Sicherheit der Zurich Platform

Zuletzt aktualisiert: 10.11.2025

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Materialien wurden für Sie mit einer Übersetzungssoftware übersetzt. Es wurden angemessene Anstrengungen unternommen, um Ihnen eine akkurate Übersetzung zu liefern. Jedoch können menschliche Übersetzer nicht durch automatisierte Übersetzungstechnologien ersetzt werden. Die Übersetzungen werden ungeprüft bereitgestellt. Es wird keinerlei Gewährleistung, weder ausdrücklich noch implizit, für die Genauigkeit, Zuverlässigkeit und Richtigkeit von Übersetzungen in andere Sprachen übernommen. Manche Inhalte wurden aufgrund der Beschränkungen der Übersetzungssoftware möglicherweise nicht präzise übersetzt. Die Ausgangssprache dieser Dokumente ist Englisch. Jegliche Diskrepanzen oder Unterschiede, die bei der Übersetzung entstehen, sind nicht verbindlich und haben keine Rechtswirkung für die Einhaltung oder Durchsetzung von Rechten.

Einige Beispiele und Grafiken, die hier dargestellt sind, dienen nur der Veranschaulichung.®ine echte Zuordnung oder Verbindung zu ServiceNow-Produkten oder -Services ist nicht beabsichtigt und sollte nicht abgeleitet werden.

ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken
sind Marken und/oder eingetragene Marken von ServiceNow, Inc., in den USA und/oder anderen Ländern. Andere Unternehmens- und
Produktnamen können Marken der jeweiligen Unternehmen sein,
denen sie zugeordnet sind.

Bitte lesen Sie die Nutzungsbedingungen für die ServiceNow-Website unter www.servicenow.com/terms-of-use.html

Automatische Übersetzung

Firmensitz
2225 Lawson Lane
Santa Clara, CA 95054
USA
(408) 501-8550

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltsverzeichnis

Instanz sichern **10**

ServiceNow Vault **12**

ServiceNow Vault erkunden 13

ServiceNow Vault konfigurieren 16

Plugins installieren 16

Geführtes Setup verwenden 17

ServiceNow Vault Konsolen-Dashboard 19

Guided Vault 21

Tools und Metriken 22

Platform-Sicherheit **26**

Security Center 28

Zielseite des Sicherheitszentrums 30

Identitäts- und Zugriffsverwaltung 32

Sicherheitskonfigurationskonsole 33

Sicherheitsüberwachungskonsole 68

Sicherheitslage-Konsole 88

Sicherheitsaufgaben 113

Sicherheitslernen 119

Sicherheitsbanner-Ankündigungen 120

Instanz-Sicherheitszentrum 121

Migration zum Sicherheitscenter 130

Sicherheitsereignisse überwachen 132

Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften 139

Suchen Sie nach falschen Sicherheitsdefinitionen 148

Überwachen Sie Instanzmetriken 149

Aktivieren Sie ISC Virtual Agent Schnittstelle 162

Härtungseinstellungen 164

Baseline-Versionen 165

Zugriffssteuerung 255

API und Webservice 330

Architektur, Design und Bedrohungsmodellierung 345

Authentifizierung 361

Geschäftslogik 397

Kommunikation 401

Konfiguration 407

Datenschutz 421

Fehlerbehandlung und -Protokollierung 425

Datei und Ressourcen 434

Schädlicher Code 443

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Management von Anwendersitzungen....445
Gespeicherte Kryptografie....463
Validierung, Bereinigung und Codierung....466
Protokollexportservice (LES)....505
Untersuchen....506
Verwalten....509
Konfigurieren....512
Verwenden....526
Referenz....528
Protokolle....529
Systemprotokolle....530
Protokollierung, Audits und Fehler....545
Geheimnisverwaltung....546
Geheimnisverwaltung Erkunden....547
Vom Client zugängliche Geheimnisse konfigurieren....552
Dashboard „Geheimnisverwaltung“....570
Codesignatur....581
Untersuchen....585
Konfigurieren....588
Codesignatur verwenden....613
Dashboard für Integrität und Status....628
Verwalten und Problembehandlung durchführen....635
Antivirus-Scanning....643
Virenschutzscans Erkunden....644
Antivirus-Scanning konfigurieren....646
Dateien in Quarantäne werden überprüft....648
Überprüfen Sie die Virenschutzaktivität....648
Wörterbuchattribute verstehen....649
HTML-Bereinigung....650
HTML-Bereinigung erkunden....651
HTML-Bereinigung wird konfiguriert....654
HTML-Bereinigung wird aktiviert....655
Aktivieren Sie die Bereinigung einzelner Felder....655
Aktivieren Sie die Protokollierung der HTML-Bereinigung....656
Auditing....657
Untersuchen....658
Auditkomponenten....659
Konfigurieren....662
Aktivieren Sie das Auditing der Aufnahmeliste für eine Tabelle....662
Ein Feld von der Prüfung ausschließen (Ausschlussliste)....663
Tabellenfeld in Auditing einschließen (Aufnahmeliste)....663
Aktivieren Sie das Auditing für eine Systemtabelle....664

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audit-Management-Konsole....664
Prüfung....666
Funktionsweise der Tabelle „Audit-Beziehungsänderung“ (sys_Audit_Relation)....667
Referenz....667
Unterschiede zwischen Audit- und Verlaufssätzen....668
Steuern Sie den Zugriff auf den Verlauf....669
Ändern Sie die Anzahl der Verlaufseinträge....670
Verlaufsliste....670
Verlaufskalender....671
Verlaufszeitleiste....673
Nachverfolgung von Änderungen an Referenzfeldern....677
Nachverfolgung von Einfügungen....677
Nachverfolgung von CI-Beziehungen....677
Strenge Sicherheitseinstellungen....679
Einstellungen Für Hohe Sicherheit Erkunden....679
Einstellungen Für Hohe Sicherheit Werden Aktiviert....690
Virtuelles privates Netzwerk (VPN)....694
Virtual Private Network (VPN) erkunden....695
VPN-Service wird aktiviert....698
Konfigurieren einer Adresse für die VPN-Kommunikation....698
Plattform-Datenschutz....699
Datenschutz Erkunden....700
Datenschutz....701
Datenschutz für Now Assist....703
Datenschutz....705
Domänentrennung....723
Unterstützte Feldtypen für die Anonymisierung....724
Datenschutzrollen....725
Datenschutz (klassisch)....727
Daten-Discovery....739
Erkunden Daten-Discovery(Klassisch)....741
Daten-Discovery Speichern....761
Datenklassifizierung....773
Datenklassifizierung Erkunden....775
Plugin-Demodaten werden installiert....776
Datenklassifizierungen werden erstellt....778
Zuweisen von Datenklassifizierungen zu Wörterbucheinträgen....779
Datenklassifizierungen werden analysiert....779
Domänentrennung....781
Verschlüsselung....783
Key Management Framework....784
Erkunden Sie das Key Management Framework....786

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren des Key Management Framework ... 794
Key Management Framework-Referenz ... 812
Schlüsselverwaltungsaktionen ... 826
Importieren Sie einen Schlüssel aus einem Webservice ... 829
Key Management Framework Gesundheit ... 832
Bereiten Sie Ihre Instanz auf die Einstellung von GlideEncrypter vor ... 834
Key-Management-Framework-Ressourcenaustausch ... 838
Infrastruktursicherheit ... 846
Passwort2-Verschlüsselung mit Key Management Framework (KMF) ... 848
Zertifikate ... 851
Zertifikate Erkunden ... 852
LDAP-Clientzertifikat wird generiert ... 854
Ein Zertifikat wird in eine Instanz hochgeladen ... 856
Feldverschlüsselung ... 857
Feldverschlüsselung erkunden ... 859
Feldverschlüsselung konfigurieren ... 861
Feldverschlüsselung verwenden ... 886
Feldverschlüsselung Enterprise ... 921
Cloud-Verschlüsselung Mit Schlüsselverwaltung ... 926
Schlüsselverwaltungsvorgänge ... 928
Quorum-Steuerungsrichtlinie ... 936
Schlüsselverwaltungstransaktionen ... 941
Protokollierung der Cloud-Verschlüsselung ... 943
Manipulationserkennung ... 946
Vollständige Datenträgerverschlüsselung ... 949
Edge Encryption ... 949
Edge Encryption erkunden ... 951
Die Edge Encryption planen ... 964
Edge Encryption Wird Installiert ... 973
Upgrade Von Edge Encryption ... 1026
Konfiguration Von Edge Encryption ... 1034
Datenbankverschlüsselung ... 1091
Datenbankverschlüsselung Erkunden ... 1092
Datenbankschlüsselrotation wird angefordert ... 1094
Datenbankverschlüsselung mit vom Kunden gesteuertem Switch ... 1095
Zugriffsverwaltung ... 1097
Zero Trust-Zugriff ... 1098
ZTA erkunden ... 1100
ZTA wird aktiviert ... 1102
Sitzungszugriffsrolle wird konfiguriert ... 1102
Systemeigenschaften ... 1104
Tutorial: Verwenden Sie ZTA ... 1107

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ZTA für Mobile ... 1111
Kontinuierliche Authentifizierung (CA) ... 1113
Domänentrennung für Service Provider ... 1143
Domänentrennung erkunden ... 1145
Anwendungssupport für die Domänentrennung ... 1163
Empfohlene Praktiken für Service Provider ... 1172
Hilfe Zur Domänentrennung ... 1213
Setup und Verwaltung ... 1214
Domain Separation Center ... 1250
Authentifizierung ... 1258
Adaptive Authentifizierung ... 1261
API-Authentifizierung ... 1325
API-Zugriffsrichtlinie ... 1339
Zertifikatbasierte Authentifizierung ... 1363
Anwenderdefinierte Instanz-URLs ... 1371
Installationsausgänge ... 1379
IP-bereichsbasierte Authentifizierung ... 1381
LDAP-Integration ... 1384
Gleichzeitige Sitzungen begrenzen ... 1452
Lokale Authentifizierung ... 1457
Multi-Faktor-Authentifizierung ... 1484
Single Sign-on (SSO) für mehrere Anbieter ... 1567
OAuth-Authentifizierung ... 1657
Persönliche Authentifizierung ... 1726
Selbstregistrierung bei ServiceNow Instanz ... 1731
Token-basierte Authentifizierung (Anwenderanmeldungen) ... 1742
Webservice – Sicherheit ... 1756
Regeln Für Zugriffssteuerungsliste ... 1761
Zugriffssteuerungslisten Erkunden ... 1762
Konfigurieren Sie eine ACL-Regel ... 1782
Kontextbezogener Sicherheitsmanager ... 1788
Erweiterte ACL-Konfiguration ... 1794
Sicherheitsattribute ... 1806
Grundlagen Der Sicherheitsattribute ... 1807
Erstellen Sie Sicherheitsattribute ... 1807
Sicherheitsattribut Umfang ... 1810
Feldabfragerollen und Einschränkungen ... 1811
Konfigurieren Sie eine Feldabfragerolle ... 1811
Konfigurieren Sie Einschränkungen Für Feldabfragen ... 1812
Skripting-Governance-Tool ... 1812
Zugriffssteuerungen für Rechneridentität ... 1814
Erstellen Sie eine Zugriffssteuerung für die Rechneridentität ... 1815

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenfilterung....1816
Erkunden Sie die Datenfilterung....1817
Aktivieren Sie die Datenfilterung....1820
Erstellen Sie Datenfilterungsregeln....1820
Erstellen Sie Betreffkriterien....1823
Debugging der Datenfiltration....1827
Sicherheitsdatenfilter....1828
Erstellen Sie einen Sicherheitsdatenfilter....1831
Standardsicherheitsfilter....1832
Sicherheitsrollen....1833
Explizite Rollen....1834
Rollen mit erhöhten Rechten....1842
Verbindung und Anmeldeinformationen....1844
Erkunden Sie Anmeldeinformationen, Verbindungen und Aliasse....1846
Erste Schritte mit Verbindungen....1862
Erste Schritte mit Anmeldeinformationen....1875
Authentifizierungsalgorithmen....1970
ServiceNow®-Zugriffssteuerung....1981
Erkunden E ServiceNow® Zugriffssteuerung....1982
Aktivieren ServiceNow® Zugriffssteuerung....1985
Konfigurieren ServiceNow® Zugriffssteuerung....1987
Audit-Protokollierung....1989
Identität....1990
Zugriffsanalyse....1991
Zugriffsanalyse Erkunden....1992
Zugriffsanalyse Verwenden....1993
Berechtigungsauswertung....2014
Häufige Fragen....2016
Zugriffssimulator....2022
Access Insights....2036
Globale Identität....2041
Föderierte ID erkunden....2042
Zugriff auf Kriterien für föderierte ID....2043
ID-Felder werden aktualisiert....2044
Identitäts- und Zugriffsaudit....2046
Identitäts- und Zugriffsaudit erkunden....2047
Ergebnisse Des Identitätsaudits....2048
Prüfbare Felder für Sicherheit....2052
Unterstützte und nicht unterstützte Felder....2056
Identity Center....2057
Identity Center Erkunden....2059

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identity Center wird aktiviert ... 2059
Identity Center für Anwender ... 2059
Identitätsmetriken für Administratoren ... 2063
Rechneridentitätskonsole ... 2063
Computeridentitätskonsole Erkunden ... 2064
Machine Identity Console Wird Aktiviert ... 2072
Mit Der Computer Identity Console ... 2073
System für domänenübergreifendes Identitätsmanagement (SCIM) ... 2073
SCIM-Anbieter ... 2074
SCIM-Client ... 2093
Zugriffsbeobachter ... 2113
Konfigurieren Sie die Zugriffsbeobachtung ... 2113
Überprüfen Sie die Protokolle des Zugriffsüberwachungsservers ... 2114
Zusätzliche Ressourcen ... 2116

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanz sichern

Die Plattformsicherheit bietet Funktionen zum Sichern der Instanz.

ServiceNow Vault



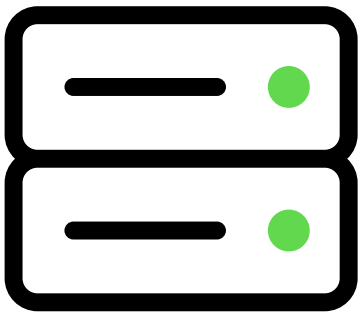
Verwenden Sie den Produktsatz von Datensicherheitstools von ServiceNow Vault, die vertrauliche Informationen während des gesamten Lebenszyklus vor nicht autorisiertem Zugriff, Beschädigung oder Diebstahl schützen.

Platform-Sicherheit



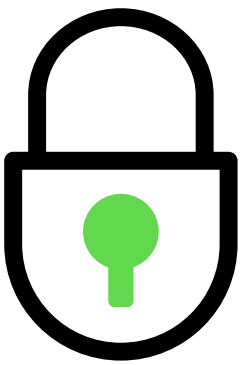
Die Plattformsicherheit bietet Funktionen zum Sichern der Instanz.

Plattform-Datenschutz



Mit Plattformdatenschutz können Sie das Vertraulichkeitsdatum in der Instanz maskieren.

Verschlüsselung



Schützen Sie Ihre sensiblen Daten, und halten Sie sich an regulatorische#Anforderungen und Standards.

Zugriffsverwaltung



Zugriffsmanagement ermöglicht Ihnen sicheren Zugriff auf die ServiceNow-Instanz.

Identität



Erfahren Sie mehr über die Identitäten in der Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Ressourcen für Plattformsicherheitsprodukte und -Lösungen



Erkunden Sie zusätzliche Plattformsicherheitsressourcen für Lerninhalte.

Automatische Übersetzung

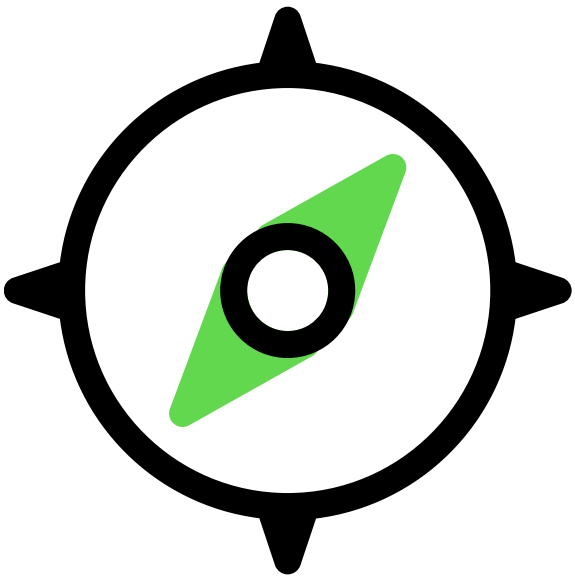
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Vault

ServiceNow Vault Bietet einen zentralen Ort zum Überprüfen und Implementieren von Sicherheitstools für erweiterte Sicherheits- und Datenschutzanforderungen.

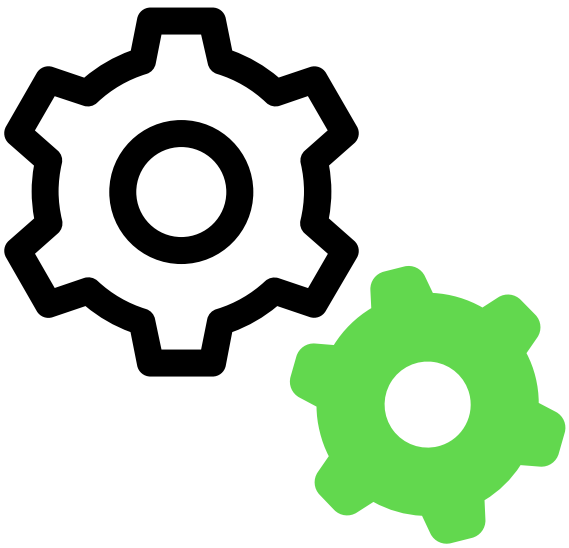
Erste Schritte

ServiceNow Vault erkunden



Erfahren Sie mehr über ServiceNow Vault Und seine Funktionen.

ServiceNow Vault konfigurieren

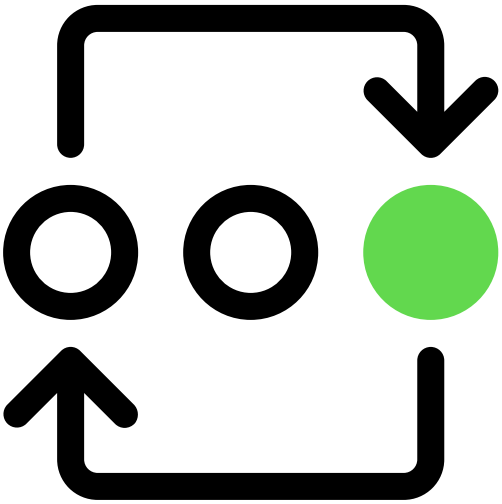


Erste Schritte mit der Installation und Konfiguration ServiceNow Vault

Automatische Übersetzung

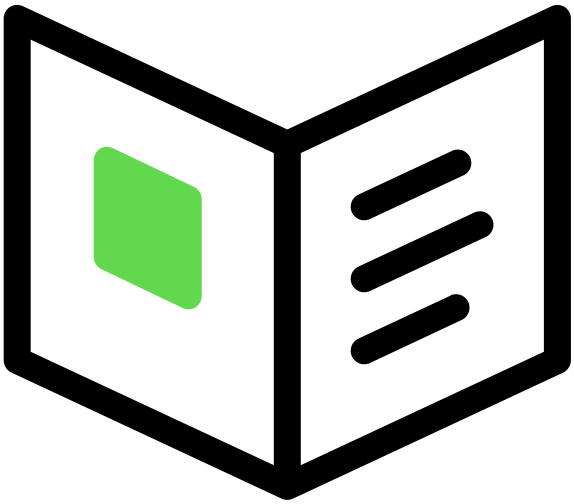
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Vault-Dashboard



Erfahren Sie, wie Sie verwenden ServiceNow Vault Dashboard zur Überprüfung Ihrer Datensicherheit.

ServiceNow Vault -Tools



Erfahren Sie mehr über die mit verwendeten Tools ServiceNow Vault

ServiceNow Vault erkunden

Erfahren Sie mehr über ServiceNow Vault, und überprüfen Sie die Vorteile, die es für Ihre Datenschutzanforderungen bieten kann.

ServiceNow Vault – Übersicht

ServiceNow Vault Ist eine Reihe von Datensicherheitstools, die vertrauliche Informationen während des gesamten Lebenszyklus vor nicht autorisiertem Zugriff, Beschädigung oder Diebstahl schützen. Sie können verwenden ServiceNow Vault Dient zum Anwenden von Schutzmaßnahmen wie Verschlüsselung, Geheimnisverwaltung und Datenschutz für die Schwärzung und Prüfung vertraulicher Informationen.

Hinweis:

ServiceNow Vault Ist ein bezahltes Plugin, das ServiceNow Mitarbeiter müssen in Ihrer Produktionsinstanz aktivieren. ServiceNow Vault Enthält die hier aufgeführten Komponenten.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste **Alle Anwendungen** in Ihrer Instanz aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Vault – Vorteile

ServiceNow Vault – Vorteile

Vorteil	Funktion	Anwender
Erhalten Sie eine umfassende ServiceNow VaultÜbersicht und Überprüfung der Metriken im Zusammenhang mit der Discovery, Klassifizierung und dem Schutz Ihrer Daten	ServiceNow Vault Konsolen-Dashboard	Plattformadministratoren
Geführte Setups, um die Verwendung von ServiceNow Vault-Tools mit Anwendungen einfach zu starten	Guided Vault	Plattformadministratoren

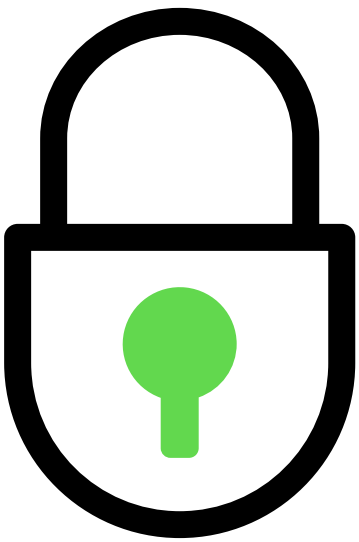
Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von ServiceNow Vault finden Sie unter:

- ServiceNow Vault Konsolen-Dashboard
- ServiceNow Vault konfigurieren
- Verwenden Sie das geführte Setup für ServiceNow Vault

ServiceNow Vault -Tools

Verschlüsselung



Schlüsselverwaltung und Feldverschlüsselung sind eine Suite von hoch konfigurierbaren Verschlüsselungsmodulen

Codesignatur

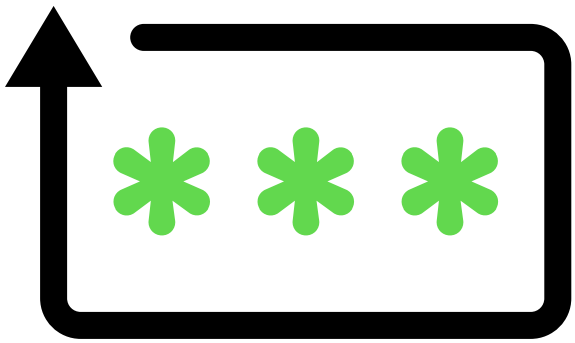


Tragen Sie zur Erhöhung der Sicherheit bei, indem Sie sensible Anwendungskonfigurationsdaten und Skripts validieren, bevor sie verwendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz



Verwenden Sie das Plugin „Datenschutz“, um personenbezogene Daten (Personally Identifiable Information, PII) aus Anwenderdaten zu entfernen, wenn sie von einer Produktionsinstanz zu einer Instanz außerhalb der Produktion migriert werden.

Daten-Discovery

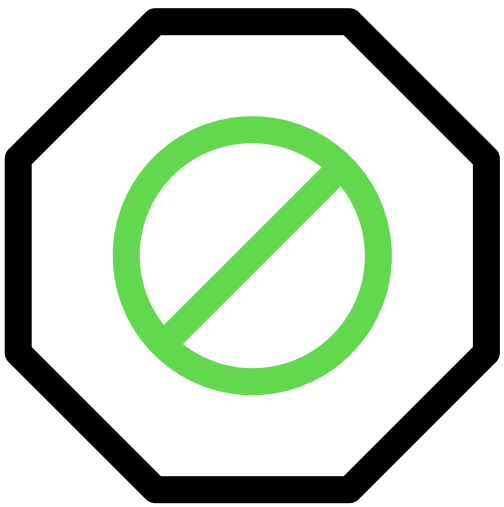


Mit dem Data Discovery-Plugin können Sie personenbezogene Daten (PII) aus Anwenderdaten finden. Die Daten können dann für weitere Sicherheitsmaßnahmen klassifiziert werden.

Protokolle



Zero Trust-Zugriff



ServiceNow Mit Sitzungszugriff können Unternehmen Anwenderberechtigungen in einer Websitzung dynamisch reduzieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbessern Sie Sicherheit, Leistung und Benutzer-Experience, indem Sie ServiceNow-Protokolldaten mit dem Log Export Service in Enterprise-Protokollanalysetools importieren.

ServiceNow Vault konfigurieren

Erfahren Sie, wie Sie installieren und konfigurieren ServiceNow Vault

Konfiguration – Übersicht

- Installieren Sie Vault-Plugins

  Erfahren Sie, wie Sie installieren ServiceNow Vault Für Ihre Instanz.

- Lernen Sie die für die Verwendung erforderlichen Rollen, und richten Sie sie ein ServiceNow Vault

- Installieren Sie Vault-Plugins

  Installieren und überprüfen Sie die Plugins, die erforderlich sind, um das Beste aus zu machen ServiceNow Vault.

Geführtes Setup zur Implementierung von ServiceNow Vault verwenden

Das geführte Setup bietet eine Reihe von Aufgaben, die Ihnen bei der Konfiguration helfen ServiceNow Vault In Ihrer ServiceNow-Instanz. Dient zum Öffnen des geführten Setups für ServiceNow Vault, Navigieren Sie zu **Alle** > **Vault** > **Vault-Konsole**an.

Weitere Informationen finden Sie unter Guided Vault.

Installieren Sie Vault-Plugins

Erfahren Sie, wie Sie die nessecary-Plugins für überprüfen und installieren ServiceNow Vault.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
ServiceNow Vault Wird am besten mit anderen ServiceNow-Sicherheitsprodukten verwendet. Installieren und konfigurieren Sie die anderen Plugins, um Ihre Tools und Metriken optimal zu nutzen.

Prozedur

1. Navigieren zu **Alle** > **Vault** > **Vault-Konsole**an.
2. Überprüfen Sie den Status Ihrer Tools.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Toolstatus

Status	Beschreibung
	Das Tool verfügt über eine eingeschränkte Zugriffslizenz. Gemeldete Metriken sind möglicherweise betroffen oder nicht verfügbar.
	Das Tool ist standardmäßig in der Plattform enthalten
	Tool hat keine Lizenz. Gemeldete Metriken sind möglicherweise betroffen oder nicht verfügbar.
	Das Tool hat vollständigen Zugriff.

3. **Wahlweise:** Wenn ein Status entweder eingeschränkt ist oder eine Lizenz benötigt, überprüfen Sie die entsprechende Installationsseite.

Toolinstallation

Tool	Installationsseite
Daten-Discovery	Daten-Discovery aktivieren
Datenklassifizierung	In der Plattform enthalten
Datenanonymisierung	Aktivieren Sie den Datenschutz **Hinweis:** Die Datenanonymisierung wird als Teil von installiert Datenschutz
Feldverschlüsselung	Feldverschlüsselung aktivieren
○ Zero Trust Access (ZTA) ○ Kontinuierliche Authentifizierung (CA)	○ Zero Trust-Zugriff Wird Aktiviert ○ Kontinuierliche Authentifizierung Wird Aktiviert

Verwenden Sie das geführte Setup für ServiceNow Vault

Verwenden Sie das geführte Setup, um eine Anwendung mit ServiceNow Vault einfach zu verwenden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Vault** > **Vault-Konsole**an.
2. In **Geführter Tresor** Wählen Sie im Abschnitt aus **Erste Schritte** Schaltfläche für Ihre Anwendung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. In **Wählen Sie App-Daten aus** Verwenden Sie die Tabelle, um die Anwendungsdaten auszuwählen, mit denen verwendet werden soll ServiceNow Vault, Wählen Sie aus **Klassen in der Vorschau anzeigen** Wenn fertig

Wählen Sie App-Datentabellenfelder aus

Bezeichnung	Beschreibung
Tabelle	Die Tabelle, in der sich die Daten befinden.
Spalte	Die Spalte, in der sich die Daten befinden
Vorhandene Klasse	Die aktuelle Klassifizierung der Daten
Empfohlene Klasse	Die empfohlene Klassifizierung für die Daten.
Anwendung	Der Anwendungsbereich der Daten

4. In **Vorschau der Datenklassifizierung** Zeigen Sie eine Vorschau Ihrer Datenklassifizierungseinstellungen an. Aktivieren Sie nach Abschluss die Option „zustimmen“, und wählen Sie aus **Wenden Sie empfohlene Klassen an** Schaltfläche.

Vorschau der Datenklassifizierungstabellenfelder

Bezeichnung	Beschreibung
Tabelle	Die Tabelle, in der sich die Daten befinden.
Spalte	Die Spalte, in der sich die Daten befinden
Endgültige Klasse	Die Klasse, die die Daten zugewiesen werden
Anwendung	Der Anwendungsbereich der Daten

5. In **Klassifizierungszusammenfassung** Überprüfen Sie die Ergebnisse der Datenklassifizierung, wählen Sie aus **Als Nächstes** Wenn fertig.

Trouble?
Verwenden Datenklassifizierung Dient zum Überprüfen von Daten, die nicht klassifiziert werden konnten.

6. In **Schützen Sie vorhandene Daten** Überprüfen Sie die Schutzrichtlinien der Daten.

Schützen Sie vorhandene Datentabellenfelder

Bezeichnung	Beschreibung
Tabelle	Die Tabelle, in der sich die Daten befinden.
Spalte	Die Spalte, in der sich die Daten befinden
Anonymisierung	Meldet, ob eine Datenanonymisierungsrichtlinie auf die Daten angewendet werden kann oder bereits angewendet wird.
Feldverschlüsselung	Meldet, ob eine Feldverschlüsselungsrichtlinie auf die Daten angewendet werden kann oder bereits angewendet wird.
Zero-Trust-Zugriff	Meldet, ob eine Zero Trust-Zugriffsrichtlinie auf die Daten angewendet werden kann oder bereits angewendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. **Wahlweise:** Sie können auswählen **Verfügbar** Überprüfen Sie, um mit der Anwendung dieser Spalten der jeweiligen Anwendungsdatenschutzrichtlinie zu beginnen Tresor t Ools und Metriken Weitere Informationen finden Sie unter .
8. In **Schützen Sie Echtzeitdaten** Überprüfen Sie Ihre Datenschutzrichtlinien in Echtzeit, und wählen Sie aus **Als abgeschlossen markieren** Wenn fertig.

Schützen Sie Echtzeitdatenfelder

Bezeichnung	Beschreibung
Name	Der Name der ???
Typ	Der Datenkanaltyp.
Anonymisierung in Echtzeit	Meldet, ob eine Echtzeitanonymisierungsrichtlinie verfügbar ist oder bereits auf die Daten angewendet wurde.

Hinweis: Echtzeitdaten werden über die gesamte Instanz und alle Anwendungen geschützt.

Ergebnis
Die ausgewählte Anwendung verfügt jetzt über klassifizierte Daten- und Schutzrichtlinien. Außerdem werden jetzt relevante Metriken an gemeldet ServiceNow Vault Konsolen-Dashboard.

ServiceNow Vault Konsolen-Dashboard

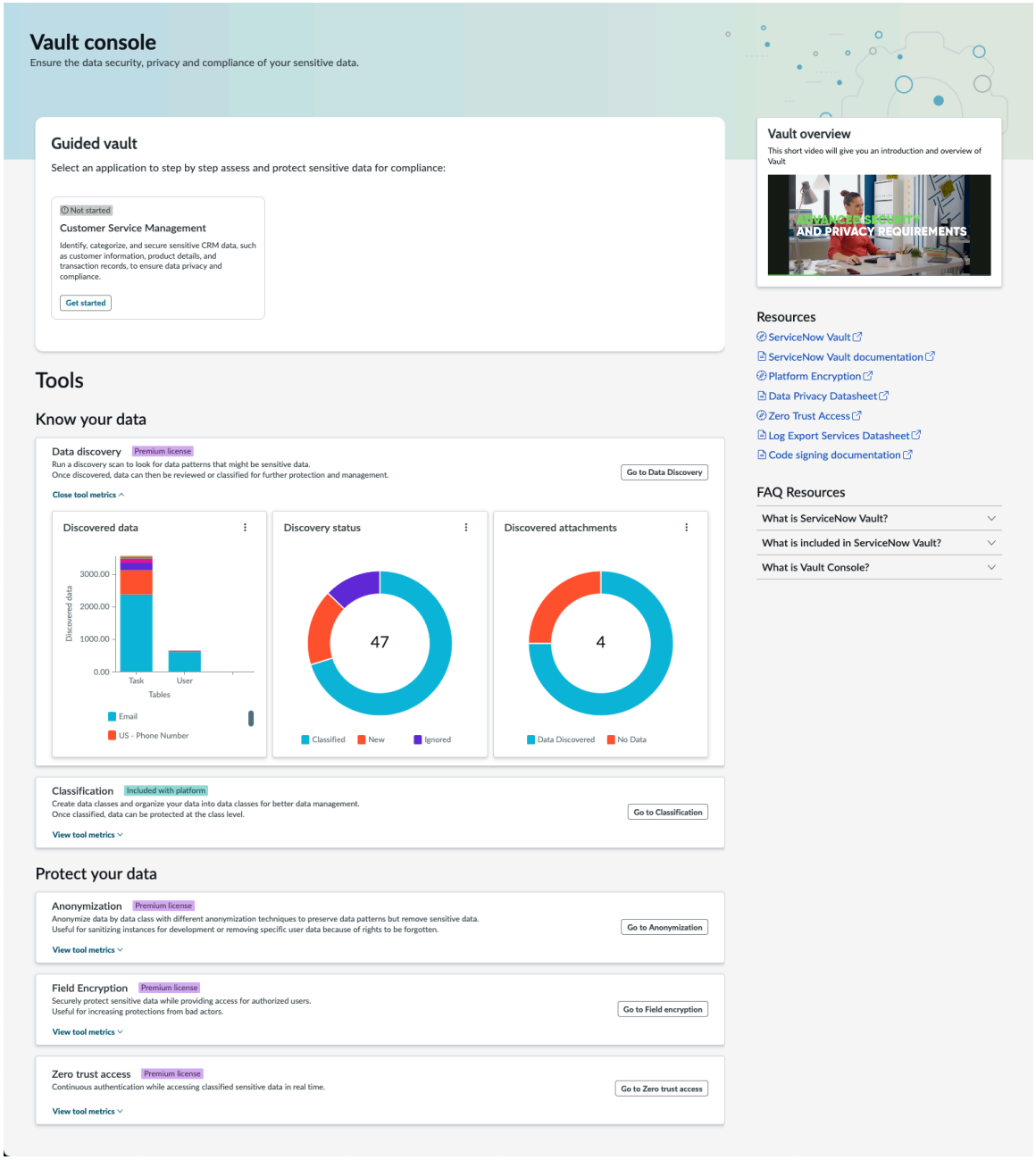
Verwenden Sie ServiceNow Vault Konsolen-Dashboard zum Nachverfolgen und Verwalten Ihrer ServiceNow Vault-Sicherheitstools.

Das Dashboard bietet eine einfache Möglichkeit, die Sicherheit, den Datenschutz und die Compliance Ihrer sensiblen Daten zu überprüfen. Das Dashboard berichtet über ServiceNow Vault Tools und ihre verschiedenen Metriken sowie geführte Setups für Anwendungen, die für kompatibel sind ServiceNow Vault.

Um auf zuzugreifen ServiceNow Vault Konsolen-Dashboard navigieren Sie zu **Alle** > **Vault** > **Vault-Konsole**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vault-Konsolen-Dashboard-Seite



Automatische Übersetzung

Abschnitt	Unterabschnitt	Beschreibung
Vault-Übersicht Und Ressourcen	Vault-Übersicht	Bietet eine Videoübersicht von ServiceNow Vault
	Ressourcen	Bietet zusätzliche Ressourcen für Hilfe bei ServiceNow Vault
	FAQ-Ressourcen	Erhalten Sie Antworten auf häufig gestellte Fragen zu ServiceNow Vault
Guided Vault	Karten für geführte Setups für Anwendungen	Wählen Sie aus **Erste Schritte** Schaltfläche auf einer Anwendungskarte, mit der begonnen werden soll ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt	Unterabschnitt	Beschreibung
		Vault Mit dieser Anwendung. Weitere Informationen zum geführten Setup finden Sie hier:Verwenden Sie das geführte Setup für ServiceNow Vault
Tresor t Ools und Metriken	Toolinformationen	Eine kurze Beschreibung und Lizenzierungsinformationen für die in verwendeten Tools ServiceNow Vault. Wählen Sie aus **Wechseln Sie zu** Schaltfläche zur Tools-Homepage wechseln. Die derzeit im Dashboard angezeigten Tools sind: • Daten-Discovery • Datenklassifizierung • Datenanonymisierung • Feldverschlüsselung • Zero Trust Access (ZTA)
	Toolmetriken	Wählen Sie die Dropdown-Liste aus, um verschiedene Metriken und Diagramme zu einem Tool zu überprüfen. **Hinweis:** Weitere Informationen zu den Metriken finden Sie auf der entsprechenden Tools-Homepage.

Guided Vault

Das geführte Vault-Setup bietet einen Schritt-für-Schritt-Prozess zum Bewerten und Schutz vertraulicher Daten für eine Anwendung.

Das geführte Vault-Setup bietet eine einfache Möglichkeit, mit der Verwendung zu beginnen ServiceNow Vault Mit Ihren Anwendungen. Das Setup verwendet die ausgewählten Anwendungsdaten. Das Setup hilft dem Anwender, die Anwendungsdaten auf Klassifizierung zu überprüfen, und hilft dann bei der Implementierung von Schutzrichtlinien für die klassifizierten Daten. Sie können die Verwendung von überprüfen ServiceNow Vault Geführtes Setup um Verwenden Sie das geführte Setup für ServiceNow Vault

Ein geführtes Setup umfasst 5 Schritte:

1. App-Daten auswählen
2. Vorschau der Datenklassifizierung
3. Klassifizierungszusammenfassung
4. Vorhandene Daten schützen
5. Echtzeitdaten schützen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach einem geführten Vault-Setup können Sie Anwendungsdatenmetriken in überprüfen **Tools** Abschnitt des Vault-Konsolen-Dashboards. Weitere Informationen finden Sie unter Tresor t Ools und Metriken.

Tresor t Ools und Metriken

Erfahren Sie mehr über die Tools und Metriken ServiceNow Vault Verwendet zum Schutz und Discovery vertraulicher Daten.

ServiceNow Vault Ist in mehrere Tools integriert, um Ihnen einen zusammenhängenden Überblick über die Sicherheit Ihrer sensiblen Daten zu bieten. Sie können den Mauszeiger über ein Widget bewegen, um weitere Einblicke in die gemeldeten Daten zu erhalten. Wählen Sie aus **Wechseln Sie zu** Schaltfläche in einem beliebigen Tool, das auf die jeweilige Seite gebracht werden soll.

Ihre Daten kennen

ServiceNow Vault Verwendet Daten-Discovery Und Datenklassifizierung Helfen Sie Ihnen, Ihre Daten zu verstehen und zu kennen.

Tools und Metriken

Tool	Metrik	Beschreibung
Discovery Verwenden Daten-Discovery Um einen Discovery-Scan auszuführen, um nach Datenmustern zu suchen, die vertrauliche Daten sein könnten. Nach der Erkennung können Daten überprüft oder klassifiziert werden, um weiteren Schutz und Verwaltung zu gewährleisten.	Erkannte Daten	Balkendiagramm mit Details zu erkannten Daten.
	Discovery-Status	Proportionen der erkannten Datenstatus
	Erkannte Anhänge	Anteile von Anhängen mit erkannten Daten.
Klassifizierung Datenklassifizierung Erstellen Sie Datenklassen und helfen Sie, Ihre Daten in Datenklassen zu organisieren, um die Verwaltung zu verbessern. Klassifizierte Daten können auf Klassenebene geschützt werden.	Klassifizierbare Daten	Anteile klassifizierbarer Daten
	Klassifizierte Daten	Anteile klassifizierter Daten

Daten schützen

ServiceNow Vault Verwendet Datenanonymisierung, Feldverschlüsselung und Zero Trust-Zugriff, um Ihre Daten zu schützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

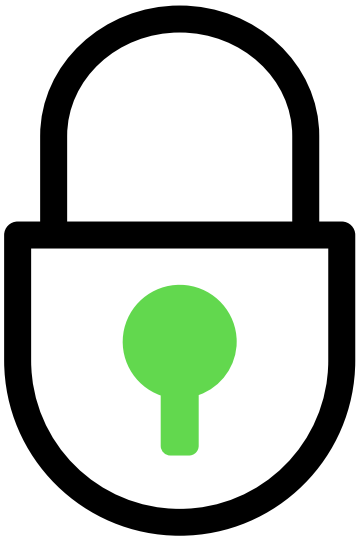
Tools und Metriken

Anonymisierung Anonymisieren Sie Daten nach Datenklasse mit verschiedenen Anonymisierungstechniken, um Datenmuster beizubehalten, aber vertrauliche Daten zu entfernen. Nützlich zum Bereinigen von Instanzen für die Entwicklung oder zum Entfernen bestimmter Anwenderdaten, da Rechte vergessen werden sollen. Metriken sind:	Echtzeitdiagramm??	
	Echtzeitdaten	Balkendiagramm, das die Menge der anonymisierten Echtzeitdaten anzeigt
	Anonymisierungslaufzeiten	
Feldverschlüsselung Schützen Sie vertrauliche Daten sicher, während Sie autorisierten Anwendern Zugriff gewähren. Nützlich, um den Schutz vor schlechten Akteuren zu erhöhen.	Status der Klassifizierung verschlüsselter Felder	Anteil der verschlüsselten Feldstatus
	Durch Feldverschlüsselung geschützte Klassen	Ein Diagramm von Klassen, die mit Feldverschlüsselung geschützt sind.
	Aktive Verschlüsselungsschlüssel	Zeigt die Anzahl der aktiven Verschlüsselungsschlüssel an. **Hinweis:** Sie benötigen Key Management Framework administratorrolle zum Anzeigen dieser Daten
Zero Trust Access (ZTA) Kontinuierliche Authentifizierung beim Zugriff auf klassifizierte sensible Daten in Echtzeit.	Klassifizierungsstatus der kontinuierlichen Authentifizierung	Anteil der Klassifizierungsstatus der kontinuierlichen Authentifizierung
	Durch kontinuierliche Authentifizierung geschützte Klassen	Zeigt die Anzahl der Klassen an, die mit kontinuierlicher Authentifizierung durch ihre Klasse geschützt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

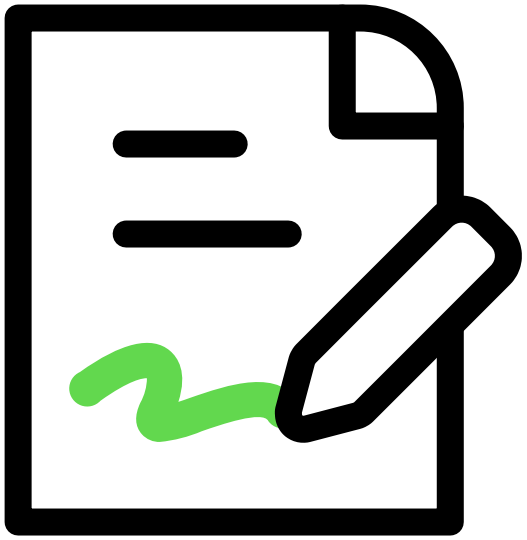
Alle ServiceNow Vault Tools

Verschlüsselung



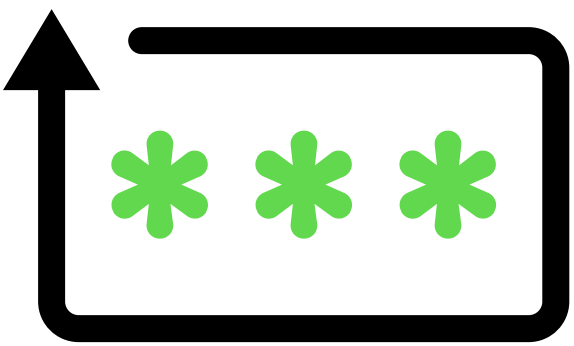
Schlüsselverwaltung und Feldverschlüsselung sind eine Suite von hoch konfigurierbaren Verschlüsselungsmodulen

Codesignatur



Tragen Sie zur Erhöhung der Sicherheit bei, indem Sie sensible Anwendungskonfigurationsdaten und Skripts validieren, bevor sie verwendet werden.

Datenschutz



Daten-Discovery



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie das Plugin „Datenschutz“, um personenbezogene Daten (Personally Identifiable Information, PII) aus Anwenderdaten zu entfernen, wenn sie von einer Produktionsinstanz zu einer Instanz außerhalb der Produktion migriert werden.

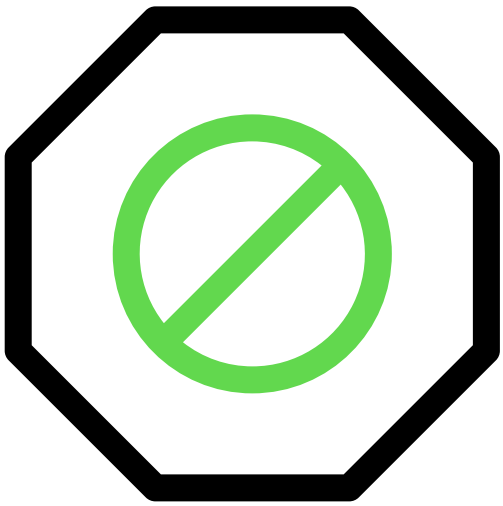
Mit dem Data Discovery-Plugin können Sie personenbezogene Daten (PII) aus Anwenderdaten finden. Die Daten können dann für weitere Sicherheitsmaßnahmen klassifiziert werden.

Protokolle



Verbessern Sie Sicherheit, Leistung und Benutzer-Experience, indem Sie ServiceNow-Protokolldaten mit dem Log Export Service in Enterprise-Protokollanalysetools importieren.

Zero Trust-Zugriff



ServiceNow Mit Sitzungszugriff können Unternehmen Anwenderberechtigungen in einer Websitzung dynamisch reduzieren

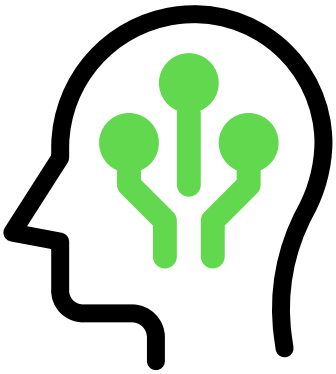
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Platform-Sicherheit

Die Plattformsicherheit bietet Funktionen zum Sichern der Instanz.

Sicherheitscenter



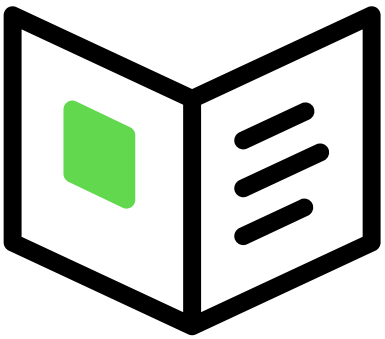
Ermöglichen Sie Administratoren, kontinuierlich die höchste Sicherheitslage aufrechtzuerhalten und einfach auf unsichere Ereignisse und Verhaltensweisen zu überwachen.

Log Export Service



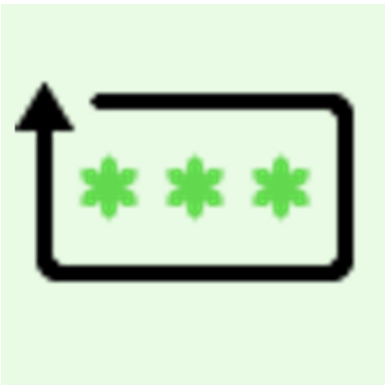
Mit dem Log Export Service (LES) können Sie Ihre Instanzsystem- und Anwendungsprotokolle nahtlos in Ihre Analysetools für Unternehmenssicherheit exportieren. Der Service bietet eine hoch skalierbare und nahezu Echtzeit-Integration mit Ihren Analysetools, die einfach einzurichten und zu warten ist.

Protokolle



Das Protokollmodul bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Ereignissen in der Instanz verwenden können.

Geheimnisverwaltung



Codesignatur



Virenschutzscanfunktionen



Automatische Übersetzung

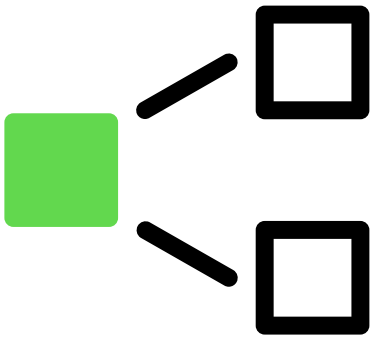
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter, die Ihren Geschäftsanforderungen entspricht.

Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen.

Verwenden Antivirus-Scanning Zum Schutz Ihrer Instanz vor Vireninfektionen, die durch Dateianhänge an Ihre Systemdatensätze wie Incidents, Probleme und Stories eingeführt werden können.

HTML-Bereinigung



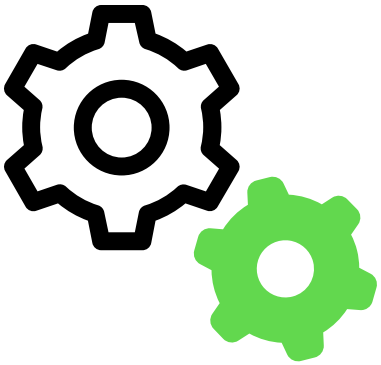
Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Auditing



Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

Strenge Sicherheitseinstellungen



Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

Virtuelles privates Netzwerk (VPN)



Härtungseinstellungen



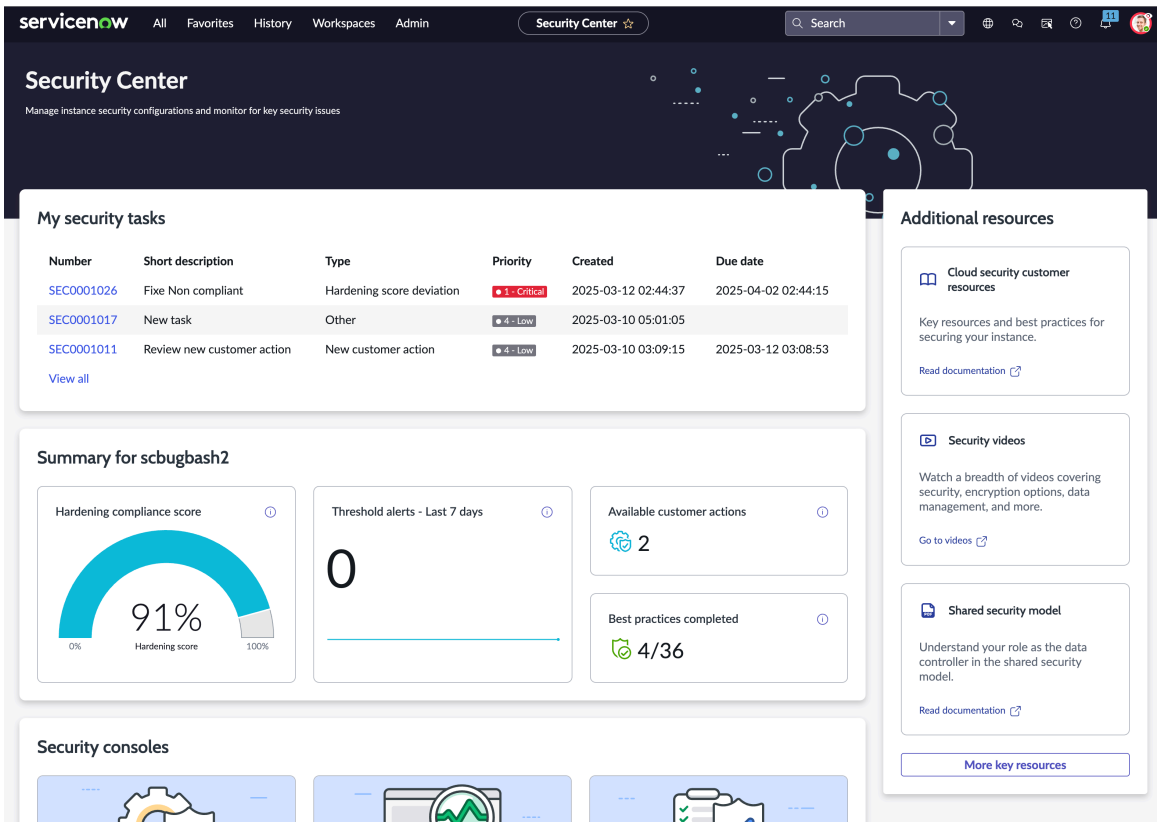
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.	Finden Sie detaillierte Beschreibungen und Compliance-Werte für den Inhalt der Sicherheitscenter-Härtungseinstellungen (SSC)	

Security Center

ServiceNow Security Center Ist eine Anwendung, die aus einer Reihe von Tools besteht, die Ihrem Unternehmen helfen, die Sicherheit Ihrer ServiceNow-Bereitstellungen aufrechtzuerhalten. Mit dem Sicherheitscenter können Sie die Sicherheitslage verbessern und die Compliance-Stufen mit einer nahtlosen Anwender-Experience stärken.



Das Sicherheitscenter ist eine kostenlose Anwendung, die Administratoren aus dem ServiceNow Store herunterladen können. Es wird standardmäßig ab dem Vancouver-Release installiert. Es wird jedes Quartal zwischen Familienveröffentlichungen auch im ServiceNow Store verfügbar gemacht, um die schnellere Einführung neuer Funktionen zu erleichtern.

Wichtig:

Das Instanzsicherheitszentrum (ISC) hat das Ende des Verkaufs im September 2024 erreicht und wird nicht mehr unterstützt oder kann nicht mehr aktiviert werden.

Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Instanz-Sicherheitszentrum an ServiceNow Security Center Migration.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Sicherheitscenter-Zielseite



Verwenden Sie die Zielseite des Sicherheitscenters, um die Informationen und Tools zu finden, die Sie zum Sichern Ihrer Instanz benötigen.

Sicherheitskonfigurationskonsole



Verwenden Sie die Sicherheitskonfigurationskonsole, um auf der Übersichtsseite einen schnellen Überblick über die Sicherheitslage Ihrer Instanz zu erhalten.

Sicherheitsüberwachungskonsole



Überwachen Sie Sicherheitsbenachrichtigungen und -Metriken, um über potenzielle Sicherheitsrisiken in Ihrer Instanz auf dem Laufenden zu bleiben.

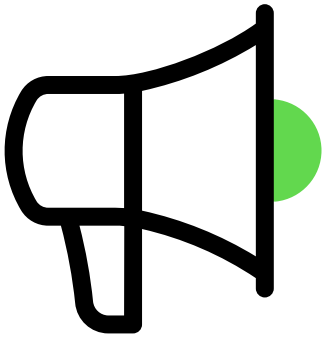
Sicherheitslage-Konsole



Verbessern Sie Ihre Sicherheitslage mit umfassender Transparenz und Schritt-für-Schritt-Anweisungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Sicherheitsbanner-Ankündigungen  Überwachen Sie Sicherheitsbenachrichtigungen und -Metriken, um über potenzielle Sicherheitsrisiken in Ihrer Instanz auf dem Laufenden zu bleiben.	

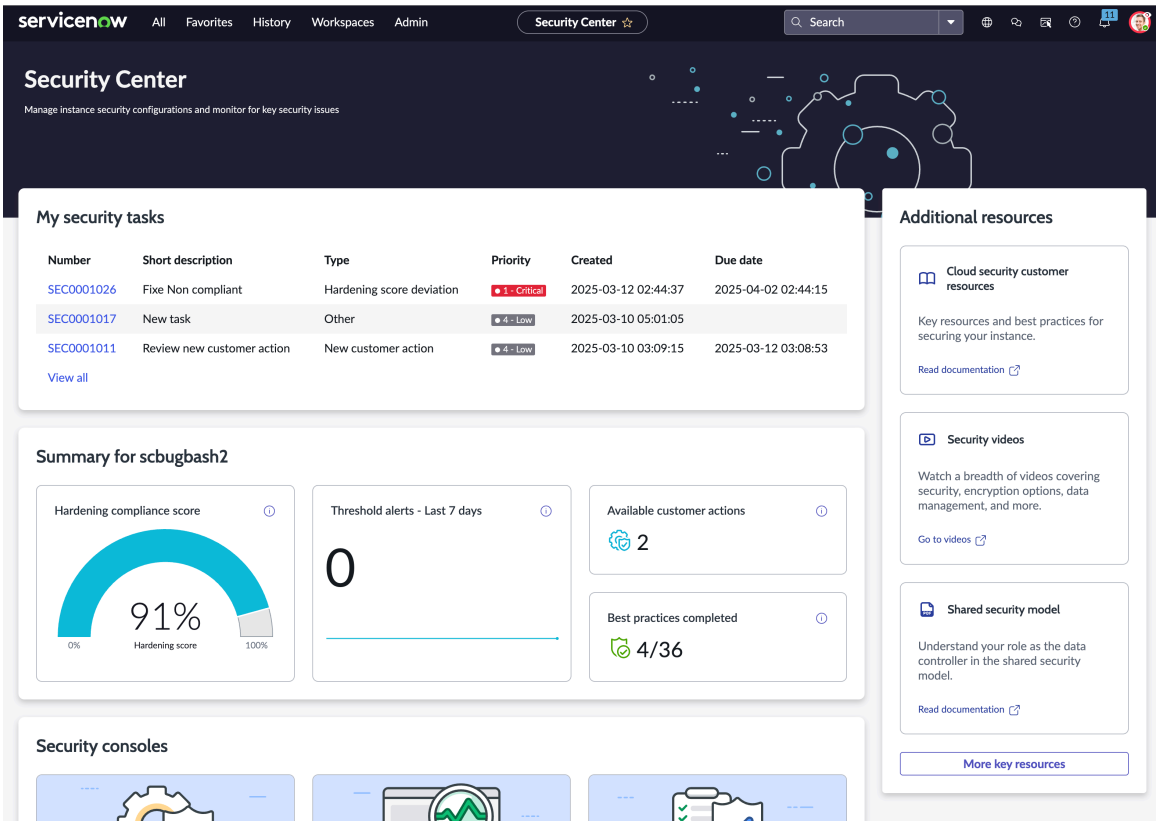
Problembehandlung und Hilfe

- Stellen Sie Fragen, und erkunden Sie andere Ressourcen für Security Center Im Abschnitt „Security Operations“ von ServiceNow Community an.
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Zielseite des Sicherheitszentrums

Verwenden Sie die Zielseite des Sicherheitscenters, um die Informationen und Tools zu finden, die Sie zum Sichern Ihrer Instanz benötigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Meine Sicherheitsaufgaben

Im Abschnitt meine Sicherheitsaufgaben wird eine Liste der Ihnen zugewiesenen Sicherheitsaufgaben angezeigt. Öffnen Sie eine Aufgabe, indem Sie die Nummer auswählen, um die Details einer Aufgabe zu überprüfen, oder wählen Sie aus **Alle anzeigen** Greifen Sie auf den Sicherheitsaufgaben-Manager zu, in dem alle Aufgaben sichtbar sind. Weitere Informationen zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Instanzzusammenfassung

Die Instanzzusammenfassung zeigt eine allgemeine Übersicht über den Status der Sicherheit Ihrer Instanz an. Wählen Sie die Informationen aus (ⓘ) Symbol auf einer beliebigen Karte, um Details zu den jeweiligen Darstellungen zu erhalten. Sie können auch eine beliebige Karte auswählen, um zum relevanten Bereich des Sicherheitszentrums zu navigieren.

Identitäts- und Zugriffsverwaltung

Verwenden Sie die Tools im Abschnitt Identitäts- und Zugriffsmanagement (IAM), um sicherzustellen, dass Ihre Daten nur für die Anwender und Prozesse zugänglich sind, die sie benötigen. Weitere Informationen zu diesen Tools finden Sie unter Identitäts- und Zugriffsverwaltung.

Sicherheitskonsolen

Wählen Sie im Abschnitt „Sicherheitskonsolen“ eine Karte aus, um zu einer der drei Sicherheitskonsolen zu navigieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sicherheitskonfigurationskonsole
- Sicherheitsüberwachungskonsole
- Sicherheitslage-Konsole

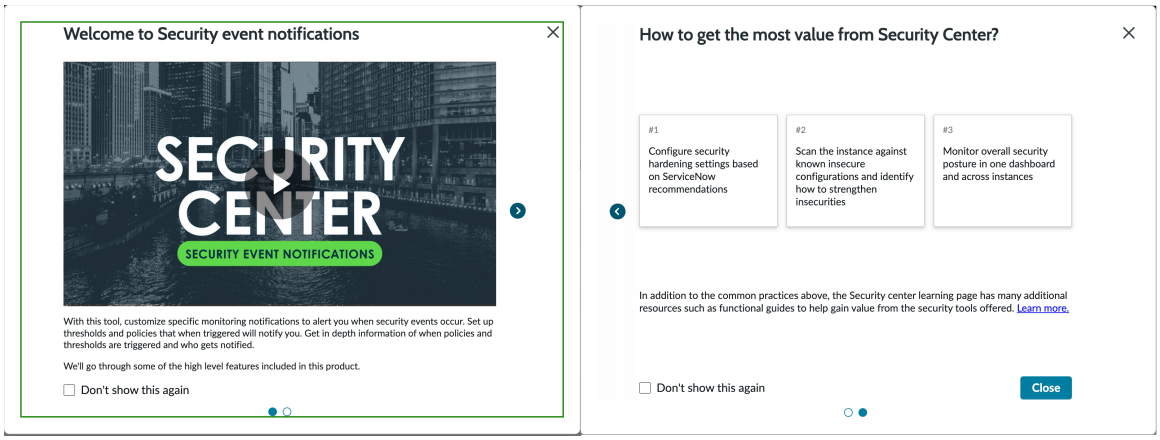
Tools

Navigieren Sie im Abschnitt „Tools“ zu den Tools, die Sie zum Verwalten der Instanzsicherheit benötigen. Diese Tools sind in drei Registerkarten organisiert, die oben im Abschnitt angezeigt werden. Wählen Sie eine Karte aus, um zum ausgewählten Tool zu navigieren.

Zusätzliche Ressourcen

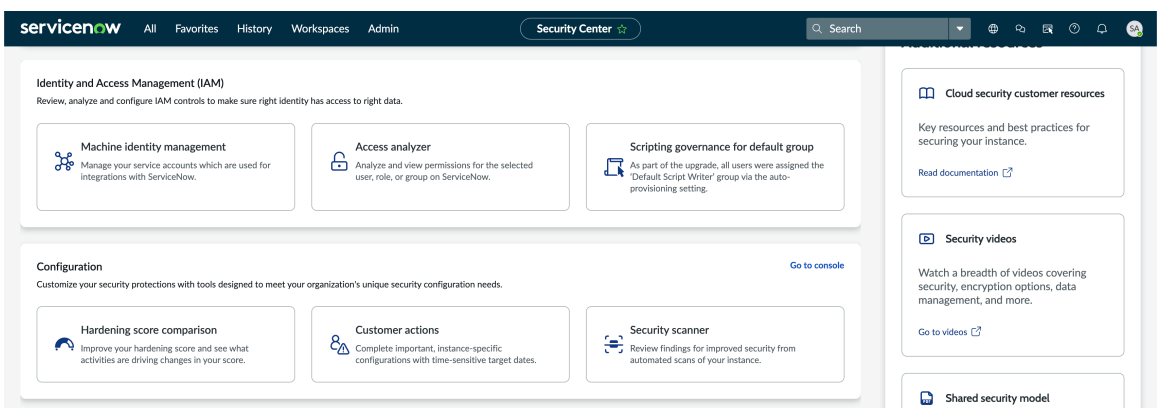
Verwenden Sie den Abschnitt „zusätzliche Ressourcen“ am Rand des Bildschirms, um zu Dokumentationen und Videos zu navigieren, die für das Lernen des Sicherheitszentrums relevant sind, sowie zu Informationen zur Verwaltung der Instanzsicherheit.

Sicherheitscenter wurde in aktualisiert Zurich Um Anleitungen zu geben, um zu verstehen, was das Tool mit seiner Verwendung tun kann. Diese Neugestaltung ist darauf zugeschnitten, sowohl neue als auch unregelmäßige Anwender des Sicherheitszentrums zu unterstützen. Im Sicherheitscenter werden neue modale Fenster angezeigt, um zu demonstrieren, wie diese Tools Ihnen helfen können, Ihre Sicherheitsziele zu erreichen.



Identitäts- und Zugriffsverwaltung

Verwenden Sie die Tools im Abschnitt Identitäts- und Zugriffsmanagement (IAM), um sicherzustellen, dass Ihre Daten nur für die Anwender und Prozesse zugänglich sind, die sie benötigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IAM besteht aus drei Tools, mit denen Sie den Zugriff auf die Daten in Ihrer Instanz verwalten können.

Identitätsmanagement Für Computer

Rechneridentitäten sind digitale Anmeldeinformationen wie Zertifikate, Schlüssel und Token. Server, Anwendungen, Container und Cloud-Services verwenden diese Identitäten, um sich gegenseitig zu authentifizieren. Verwenden Sie **Konsole Für Rechneridentität** Dient zum Verwalten der für Integrationen mit verwendeten Rechneridentitäten ServiceNow.

Zugriffsanalyse

Verwenden Sie **Analysieren Sie Zugriff und Berechtigungen** Konsole zum Anzeigen von Berechtigungen für einen ausgewählten Anwender, eine ausgewählte Rolle oder eine ausgewählte Gruppe oder zum Vergleich des Zugriffs zwischen zwei Anwendern.

Skripting-Governance für Standardgruppe

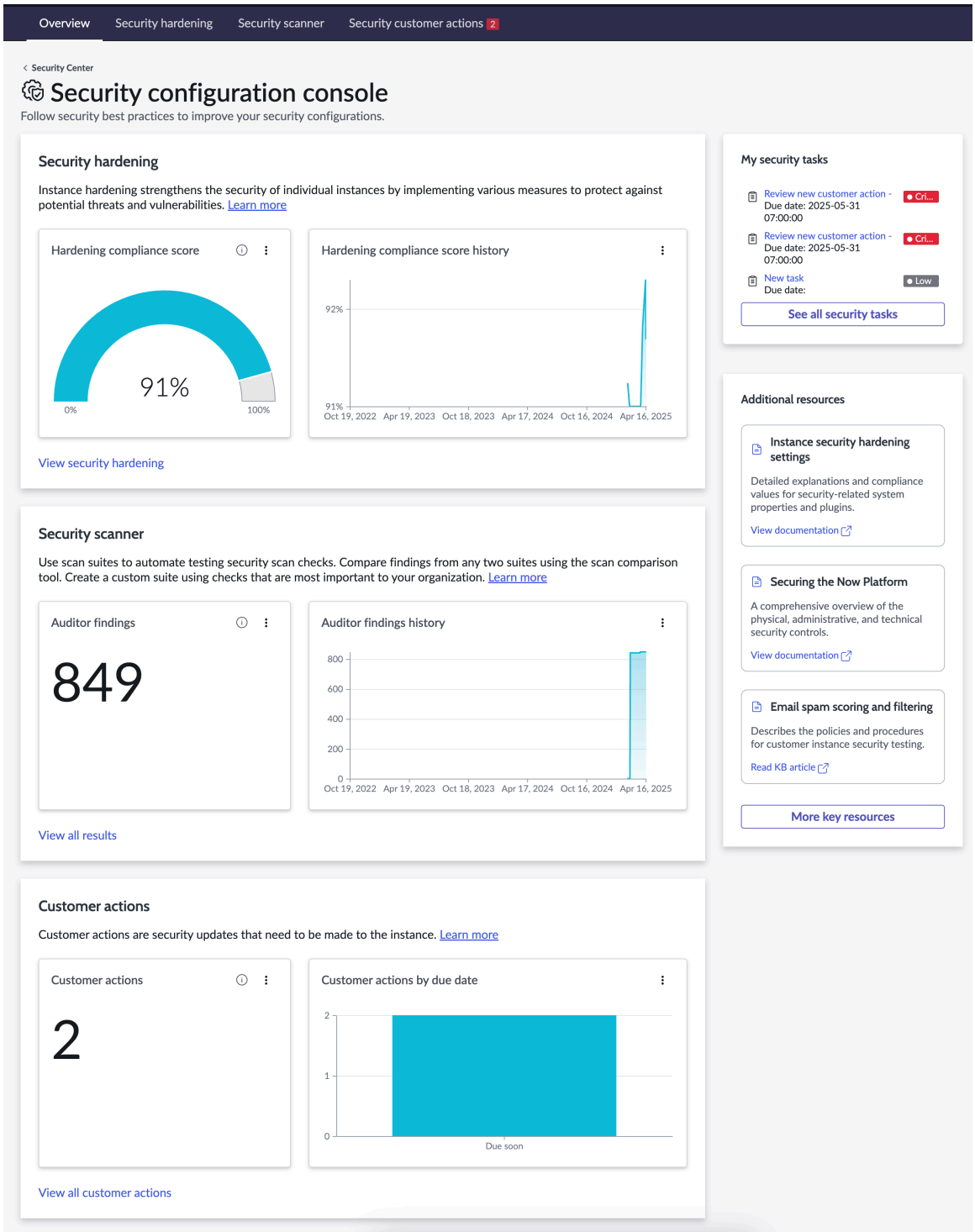
Verwenden Sie das Scripting Governance-Tool, um Einstellungen für die Gruppe „Bedingter Skriptschreiber“ zu konfigurieren. Anwendern in dieser Gruppe wird zugewiesen *snc_required_script_writer_permission*Rolle, mit der Anwender auf Skripts und skriptähnliche Felder auf der gesamten Plattform zugreifen können.

Mit den Einstellungen in dieser Konsole können Sie die automatische Zuweisung dieser Rolle aktivieren oder deaktivieren und der Gruppe Anwender manuell zuweisen. Sie können auch Informationen darüber anzeigen, wer zugewiesen ist, und Ihre Instanz scannen, um Anwender zu finden, die in einem bestimmten Zeitrahmen geskriptet haben.

Sicherheitskonfigurationskonsole

Verwenden Sie die Sicherheitskonfigurationsseite, um einen Überblick über die Sicherheitslage Ihrer Instanz zu erhalten. Zeigen Sie Ihre Compliance-Punktzahl für Härtung an, erkennen Sie grafische Trends, analysieren Sie die häufigsten nicht konformen Härtungseinstellungen, und zeigen Sie die Ergebnisse Ihrer Sicherheitsscans an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Navigationsleiste

Verwenden Sie die Leiste oben auf der Seite, um zwischen dieser Seite und dem Abschnitt „Sicherheitshärtung“, „Sicherheitsscanner“ oder „Sicherheitskundenaktionen“ des Sicherheitszentrums zu navigieren.

Sicherheitshärtung

Weitere Informationen zu Ihrer Härtungs-Compliance finden Sie im Abschnitt „Sicherheitshärtung“. Wählen Sie die Karten auf in diesem Abschnitt aus, um zu navigieren Sicherheitshärtung Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Compliance-Punktzahl für Härtung ist ein Prozentsatz, der angibt, wie eng Ihre Sicherheitseinstellungen mit den empfohlenen Einstellungen übereinstimmen. Im Abschnitt „Sicherheitshärtung“ werden dieser Prozentsatz sowie der Verlauf der Punktzahl in Ihrer Instanz im Zeitverlauf angezeigt.

Sicherheitsscanner

Überprüfen Sie die Ergebnisse automatisierter Sicherheitsscanprüfungen mithilfe des Abschnitts „Sicherheitsscanner“. Diese Prüfungen helfen Ihnen, Sicherheitsschwachstellen, Ineffizienzen und Compliance-Probleme zu finden.

Wählen Sie in diesem Abschnitt die Karten auf aus, um zur Seite „Sicherheitsscanner“ zu navigieren.

Kundenaktionen

Suchen Sie im Abschnitt Kundenaktionen nach Sicherheitsupdates, die an der Instanz vorgenommen werden können. In diesem Abschnitt wird die Anzahl der verfügbaren Aktionen und ein Diagramm angezeigt, das das Fälligkeitsdatum für diese Aktionen angibt. Wählen Sie in diesem Abschnitt die Karten auf aus, um zur Seite „Kundenaktionen“ zu navigieren.

Meine Sicherheitsaufgaben

Zeigen Sie die dringendsten Sicherheitsaufgaben an, die Ihnen zugewiesen sind. Wählen Sie eine Aufgabe aus, um ihre Details anzuzeigen, oder wählen Sie aus **Alle Sicherheitsaufgaben anzeigen** Zum Anzeigen einer vollständigen Liste von Sicherheitsaufgaben.

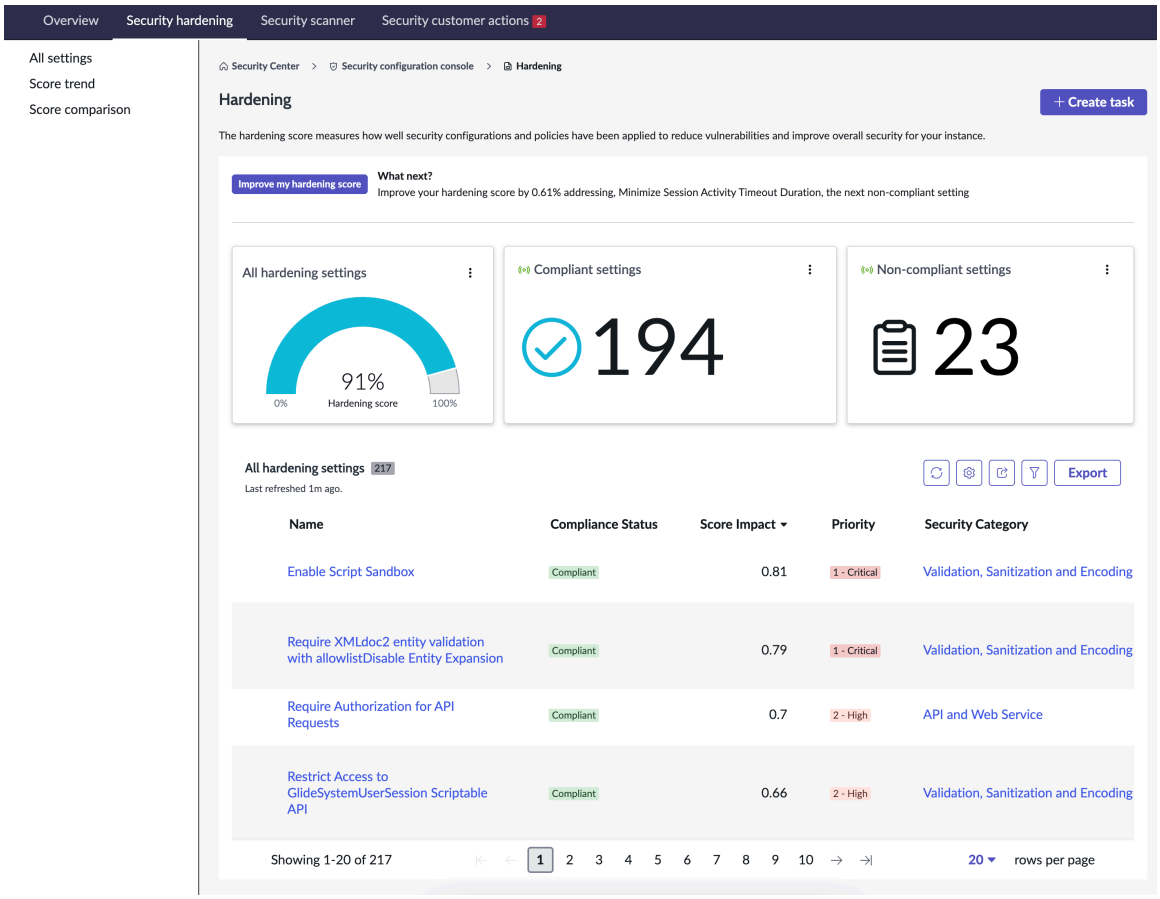
Zusätzliche Ressourcen

Verwenden Sie den Abschnitt „zusätzliche Ressourcen“ am Rand des Bildschirms, um zu Dokumentationen und Videos zu navigieren, die für das Lernen des Sicherheitszentrums relevant sind, sowie zu Informationen zur Verwaltung der Instanzsicherheit.

Sicherheitshärtung

Zeigen Sie Ihre Compliance-Punktzahl für Härtung an, vergleichen Sie sie mit vorherigen Punktzahlen, und ändern Sie die Einstellungen, um Ihre Compliance-Punktzahl und Ihre Sicherheitslage auf der Seite „Sicherheitshärtung“ zu verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Härtungseinstellungen Geben Sie empfohlene Werte für die sicherheitsbezogenen Eigenschaften und Plugins in an ServiceNow AI Platform. Das Härtungstool berechnet die Compliance-Punktzahl der Härtungseinstellung als Prozentsatz. Diese Zahl gibt an, wie konform Ihre Instanz mit den Sicherheitscenter-Härtungseinstellungen ist.

Die Formel für die Berechnung der Compliance-Punktzahl der Härtung:

- Jede Härtungseinstellung hat eine Risikopunktzahl zwischen 0 und 10. Sie können die Werte einzelner Einstellungen in anzeigen **Alle Einstellungen** Abschnitt.
- Die Punktzahl entspricht der Summe aller konformen Risikopunktzahlen geteilt durch die Summe aller Risikopunktzahlen.

Beispielsweise beträgt die Summe aller konformen Risikopunktzahlen 25,4 und die Summe aller Risikopunktzahlen 34.9. Für diese Summe beträgt die Compliance-Punktzahl (25,4 /34,9) x 100, was 72 entspricht. Diese Dezimalzahl wird auf die nächste ganze Zahl gerundet und ist daher gleich 73.

Diese Berechnung wird automatisch am ersten des Monats oder nach einer Installation oder Neuinstallation von durchgeführt ServiceNow Sicherheitscenter. Sie können eine Neuberechnung jederzeit mit auslösen **Aktualisieren Sie die Punktzahl** Schaltfläche auf dieser Seite.

Unterabschnitte zur Sicherheitshärtung

Der Abschnitt „Sicherheitshärtung“ enthält drei Unterabschnitte, die Sie am linken Rand des Bildschirms auswählen können.

Automatische Übersetzung

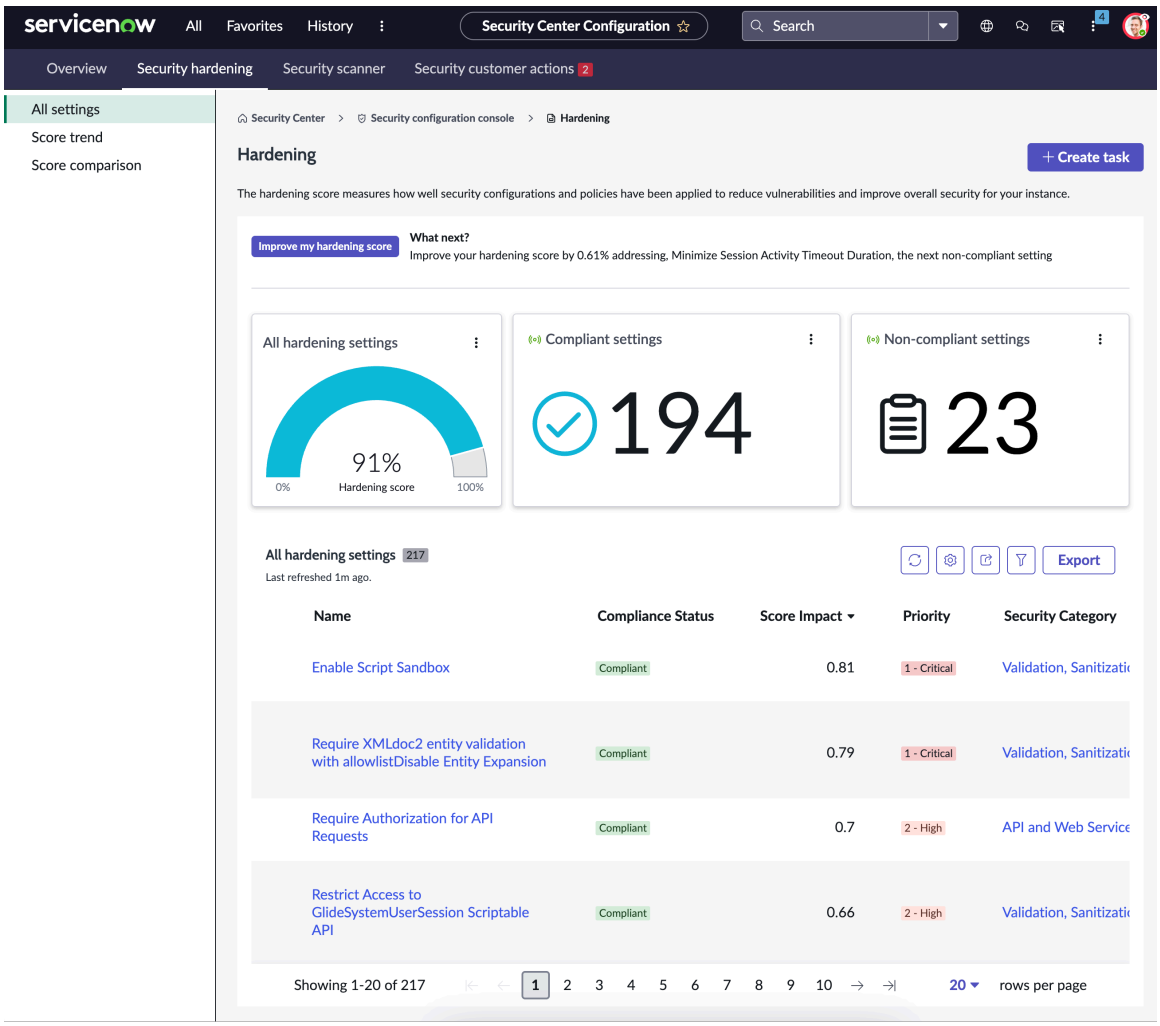
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alle Einstellungen
- Compliance-Punktzahltrend für Härtung
- Vergleich der Härtungspunktzahl

Alle Einstellungen

Überprüfen Sie alle Ihre Instanzhärtungseinstellungen, die auf einer einzigen Seite verfügbar sind.

Die **Alle Einstellungen** Seite zeigt Informationen zu allen Instanzhärtungseinstellungen an. Verwenden Sie die Schaltflächen oben rechts, um diese Informationen zu aktualisieren, zu filtern und zu exportieren.\



Verwenden Sie **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe zum Abschließen einer Kundenaktion. Diese Schaltfläche wird sowohl im angezeigt **Alle Einstellungen** Seite sowie die Seiten für einzelne Härtungseinstellungen. Details finden Sie unter Sicherheitsaufgaben.

Die folgenden Informationen zu Härtungseinstellungen finden Sie in der Liste.

Name

Name der Härtungseinstellung.

Compliance-Status

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gibt an, ob die Einstellung ordnungsgemäß gemäß der Systemempfehlung konfiguriert ist (konform) oder konfiguriert sein muss (nicht konform)

Auswirkung auf Punktzahl

Auswirkung dieser Härtungseinstellung auf Ihre Sicherheitslage, ausgedrückt als Prozentsatz. Die Summe aller Punktzahlauswirkungen ergibt 100 %.

Priorität

Die Relevanz der Einstellung: Kritisch, hoch, Mittel und Niedrig. Eine höhere Punktzahl weist auf eine größere Auswirkung und Priorität hin.

Sicherheitskategorie

Die Sicherheitskategorie der Eigenschaft. Wählen Sie die Kategorie aus, um Details anzuzeigen.

Lösungsdetails

Beschreibung der Schritte zum Beheben der Sicherheitsschwachstelle der Härtungseinstellung.

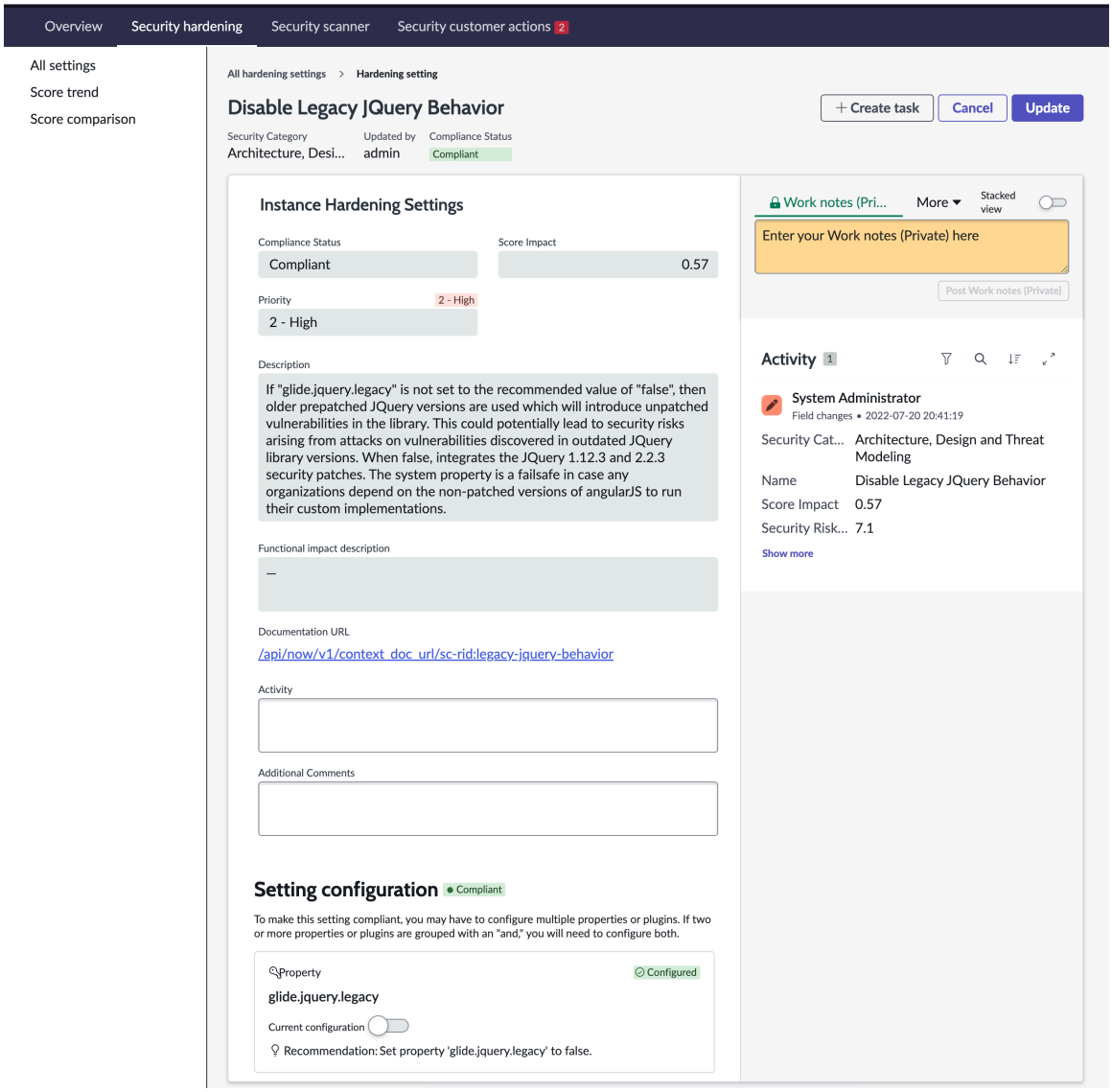
Informationen zum Konfigurieren einer Eigenschaftshärtungseinstellung finden Sie unter Erhöhen Sie die Compliance-Punktzahl für Härtung.

Details zu Härtungseinstellungen

Analysieren Sie die Details einer Härtungseinstellung, indem Sie ihren Link in der Sicherheitscenter-App auswählen.

Navigieren zu **Härtung** > **Alle Einstellungen**, Und wählen Sie dann eine Härtungseinstellung aus, die zu einer Seite im Härtungseinrichtungstool weitergeleitet werden soll, auf der die sicherheitsbezogenen Informationen angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verwenden Sie **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe zum Abschließen einer Kundenaktion. Details finden Sie unter Sicherheitsaufgaben.

Details zur Konfiguration der Härtungseinstellungen

Konfigurationsattribut	Beschreibung
Compliance-Status	Gibt an, ob die Härtungseinstellung konform ist oder nicht.
Auswirkung auf Punktzahl	Ein Prozentsatz, der angibt, wie sehr sich diese Härtungseinstellung auf Ihre Sicherheitslage auswirkt.
Priorität	Eine Zahl im Bereich von 1 bis 4, wobei 1 die stärkste Gewichtung hat, die die Stärke der Auswirkung dieser Härtungseinstellung auf Ihre Sicherheitslage angibt.
Funktionale Auswirkung	Die Auswirkung dieser Härtungseinstellung auf den Betrieb Ihrer Instanz.
Beschreibung	Eine allgemeine Übersicht über die Härtungseinstellung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details zur Konfiguration der Härtungseinstellungen (Fortsetzung)

Konfigurationsattribut	Beschreibung
Dokumentations-Url	Link zur Dokumentation für die Härtungseinstellung.
Aktivität	Benachrichtigungen über Updates im Zusammenhang mit der Härtungseinstellung.
Einstellungskonfiguration	Details zum Compliance-Status Ihrer Härtungseinstellung zusammen mit Anweisungen zur Konformität. **Hinweis:** Einige Härtungseinstellungen erfordern möglicherweise, dass Sie mehrere Eigenschaften und Plugins konfigurieren, um sie konform zu machen.

Filterhärtungseinstellungen

Vereinfachen Sie Ihren Härtungsüberprüfungsprozess mithilfe von Filtern. Diese Filter können eine Arbeitsliste von Härtungseinstellungen zur Überprüfung erstellen, die zur späteren Verwendung wiederhergestellt und für andere Anwender freigegeben werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Sicherheitscenter**an.
2. In **Sicherheitskonsolen** Wählen Sie den Abschnitt aus **Sicherheitskonfigurationskonsole** .
3. Wählen Sie aus **Sicherheitshärtung** Registerkarte.
4. Wählen Sie Aus **Alle Einstellungen** .
5. Wählen Sie aus **Filterbereich anzeigen** Schaltfläche ( ).
6. In **Filter** Fenster auswählen **Erweiterte Ansicht** .
7. Erstellen Sie einen Filter, der nur die Härtungseinstellungen anzeigt, die Sie überprüfen möchten.
8. Sobald Ihr Filter abgeschlossen ist, wählen Sie aus **Filter Speichern** .
9. Geben Sie einen Namen für Ihren Filter ein, und wählen Sie aus **Speichern** .

Hinweis: Sie können diese Liste auch anderen Anwendern zur Verfügung stellen, indem Sie Berechtigungen auf festlegen **Alle** , Oder **Gruppe** Zum Freigeben für eine bestimmte Gruppe. Diese Anwender müssen auch über die Berechtigung zur Verwendung des Sicherheitszentrums verfügen.

Nächste Maßnahme

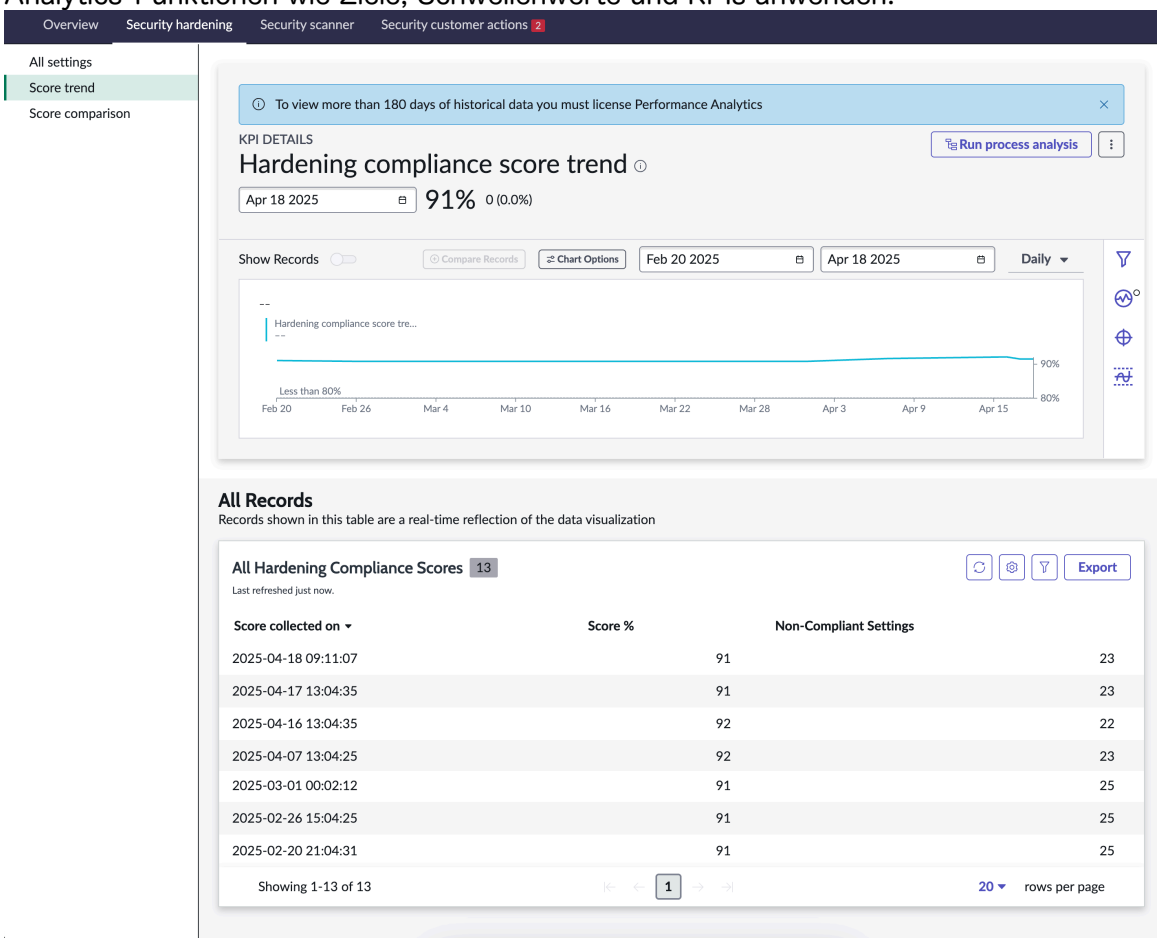
Nach dem Speichern eines Filters können Sie ihn in laden **Erweiterte Ansicht** Mit **Vorhandenen Filter verwenden** Schaltfläche.

Compliance-Punktzahltrend für Härtung

Zeigen Sie die Trends Ihrer Compliance-Punktzahl für Härtung im Zeitverlauf in einem Diagramm oder in einer Tabelle an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Trends in Ihrer Compliance-Punktzahl im Zeitverlauf an. Verwenden Sie die Datumsauswahl, um einen zu analysierenden Zeitbereich auszuwählen, um Einblicke in die Daten zu erhalten, indem Sie Performance Analytics-Funktionen wie Ziele, Schwellenwerte und KPIs anwenden.



Compliance-Punktzahldiagramm

Verwenden Sie **Diagrammoptionen** Schaltfläche, um anzugeben, welche Informationen analysiert und wie die Informationen präsentiert werden sollen.

Analyse

Wählen Sie aus der Liste der Optionen aus. Einige Optionen sind je nach ausgewähltem Diagrammtyp möglicherweise nicht verfügbar.

Zielvorgabe

Ziele, die Ihre Organisation erreichen möchte. Weitere Informationen finden Sie unter Indikatorziele .

Schwellenwert

Definiert einen normalen Punktzahlbereich für einen Indikator und warnt Sie, wenn ein bestimmtes Ereignis auftritt. Weitere Informationen finden Sie unter Indikatorschwellenwerte .

Prognose

Beschreibt die Möglichkeit, zukünftige Punktzahlen basierend auf vergangenem Verhalten zu prognostizieren. Weitere Informationen finden Sie unter Performance Analytics – Prognosen zu Punktzahlen .

Trend

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigt an, wie sich der Wert eines oder mehrerer Elemente im Laufe der Zeit ändert.

Kommentare

Zeigt Anmerkungen zu einzelnen Datenpunkten an.

Bezeichnungen

Zeigt Punktzahlen im Zusammenhang mit Visualisierungen an.

Statistik

Zeigt Statistiken im Zusammenhang mit Ihrer Compliance-Punktzahl an.

Zeitreihen

Wählen Sie aus, welche Metrik im Diagramm angezeigt werden soll.

Punktzahl

Punktzahl für den Leistungskennzahl (KPI).

Change

Änderung der Punktzahl für diesen Indikator.

Prozentuale Veränderung

Ändern Sie als Prozentsatz der Punktzahlen.

Diagrammtyp

Wählen Sie einen Diagrammtyp aus, um zu steuern, wie die von Ihnen ausgewählten Informationen visualisiert werden. Weitere Informationen finden Sie unter Anwendungsfälle für verschiedene Zeitreihenvisualisierungstypen .

Tabelle „alle Datensätze“

In der Tabelle alle Datensätze werden das Datum, an dem die Compliance-Punktzahlen erfasst wurden, die Prozentsätze der Punktzahl und die Anzahl der nicht konformen Einstellungen angezeigt. Sie können diese Tabelle als eine weitere Option verwenden, um die Sicherheitslage Ihrer Instanz zu analysieren Zeit.

Erhöhen Sie die Compliance-Punktzahl für Härtung

Erhöhen Sie Ihre Compliance-Punktzahl für Härtung, indem Sie sicherstellen, dass die Härtungseinstellungen den Empfehlungen des Systems entsprechen.

Vorbereitungen

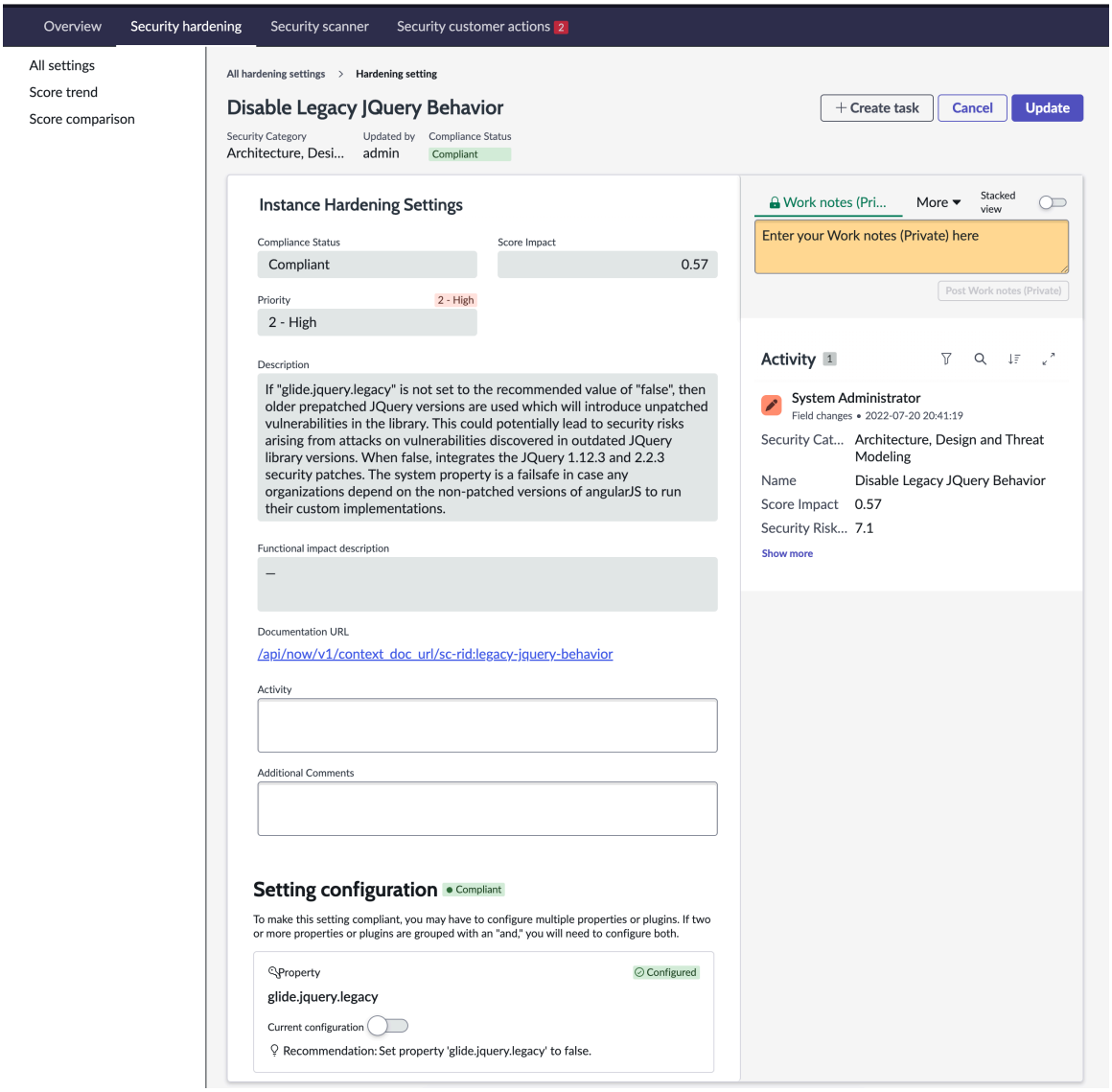
Erforderliche Rolle: Administrator

Identifizieren Sie nicht konforme Härtungseinstellungen mit den höchsten Auswirkungen auf Ihre Instanz. Überprüfen Sie sie, um zu sehen, ob Sie Systemempfehlungen einhalten können, damit Sie Ihre Compliance-Gesamtpunktzahl erhöhen können.

Prozedur

1. Navigieren zu **Härtung** > **Alle Einstellungen**an.
2. Filtern Sie die Spalte „Compliance-Status“, um nur nicht konforme Härtungseinstellungen anzuzeigen.
3. Wählen Sie Aus **Auswirkung Auf Die Punktzahl** Zum Sortieren von „am größten“ nach „am kleinsten“.
4. Wählen Sie Einstellungen aus, und überprüfen Sie die Einstellungsdetails, um zu entscheiden, ob Sie Empfehlungen einhalten möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



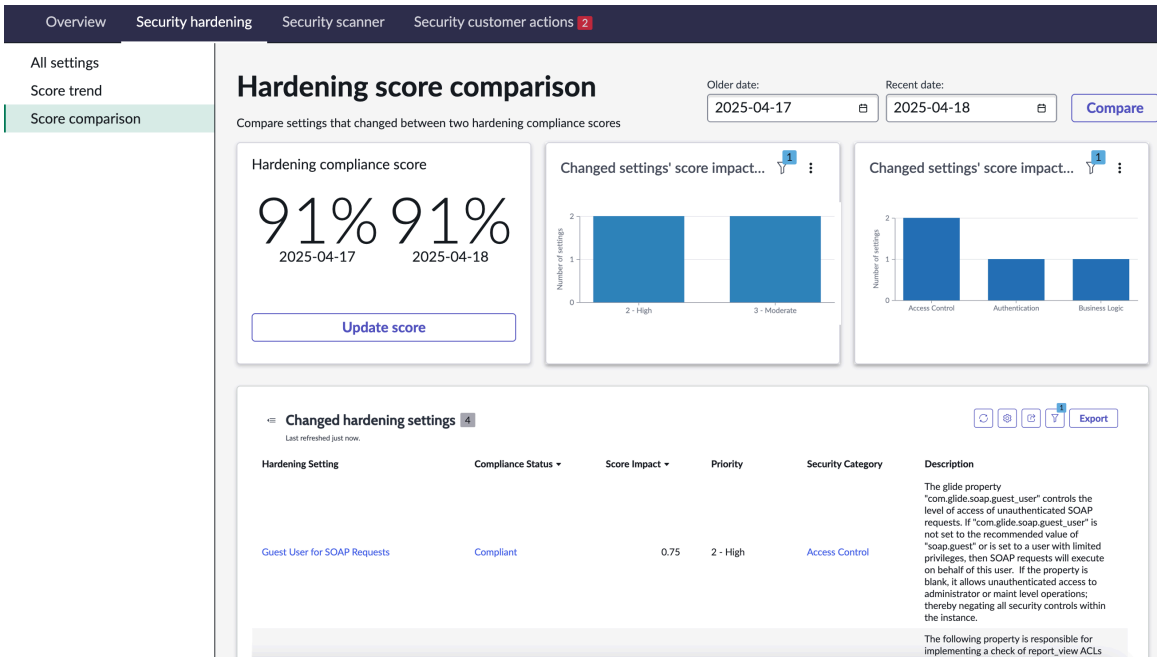
5. Machen Sie die Härtungseinstellung konform.
6. Wenn Sie eine nicht konforme Härtungspunktzahl aktualisieren, um sie konform zu machen, wechseln Sie zur Homepage, und wählen Sie aus **Aktualisieren Sie die Punktzahl** Zum Anzeigen der aktuellsten Punktzahl.
   Die Härtungspunktzahl wird aufgerundet. Eine Punktzahl von 86,75% wird auf 87 aufgerundet.

Vergleich der Härtungspunktzahl

Verschaffen Sie sich Einblick in die Integrität Ihrer Härtungseinstellungen, und verwenden Sie diese Daten, um die Sicherheitslage Ihrer Instanz zu verbessern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf dieser Seite wird eine Zusammenfassung Ihrer Härtungs-Compliance und der an Ihrer Instanz vorgenommenen Änderungen angezeigt, die sich auf diese Punktzahl auswirken.

Auf der Vergleichsseite der Härtungspunktzahl werden Härtungseinstellungen mit Änderungen des Compliance-Status zwischen den in ausgewählten Daten angezeigt **Älteres Datum** Und **Letztes Datum** Felder. Mit diesen Informationen können Sie sehen, wie sie sich auf Ihre Compliance-Punktzahl für Härtung ausgewirkt haben.

Compliance-Bewertung für Härtung

Die Karte vergleicht die Compliance-Punktzahl Ihrer Instanz an den ausgewählten Daten als Prozentsatz.

Impact auf die Punktzahl der geänderten Einstellungen nach Priorität

Zeigt die Anzahl der Härtungseinstellungen an, die ihren Compliance-Status seit der letzten Punktzahlaktualisierung geändert haben, organisiert nach Prioritätswert.

Impact auf die Punktzahl der geänderten Einstellungen nach Sicherheitsbereich

Zeigt die Anzahl der Härtungseinstellungen an, die den Compliance-Status zwischen den beiden ausgewählten Daten geändert haben, organisiert nach Sicherheitsbereich.

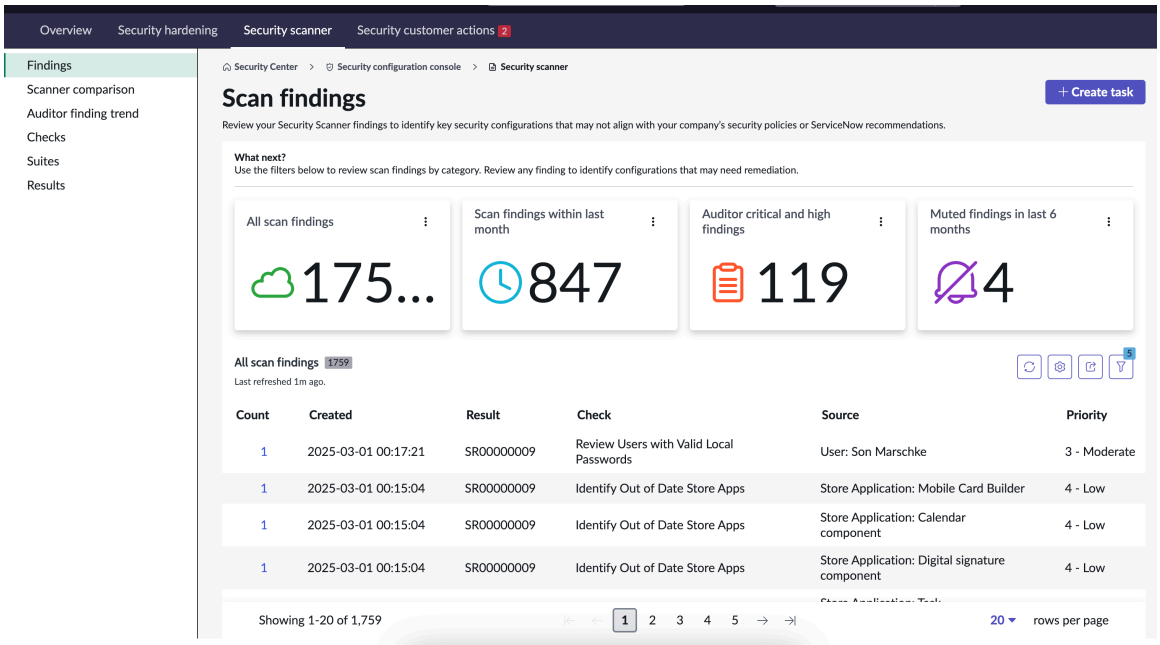
Härtungseinstellungen geändert

Zeigt die Liste der Härtungseinstellungen an, die die Compliance-Status zwischen den ausgewählten Daten geändert haben. Überprüfen Sie Einstellungen, die nicht konform wurden und Ihre Vergleichspunktzahl für Härtung verringert haben, um sie konform zu machen, um Ihre Punktzahl zu erhöhen. Weitere Informationen finden Sie unter Erhöhen Sie die Compliance-Punktzahl für Härtung.

Sicherheitsscanner

Scannen Sie Ihre Instanz anhand einer Reihe von Sicherheitsprüfungen, um Fehlkonfigurationen zu identifizieren. Das Scanner-Tool vereinfacht die Erstellung verschiedener Suites von Prüfungen für verschiedene Anwendungsfälle, sodass Sie die Ergebnisse im Laufe der Zeit analysieren können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

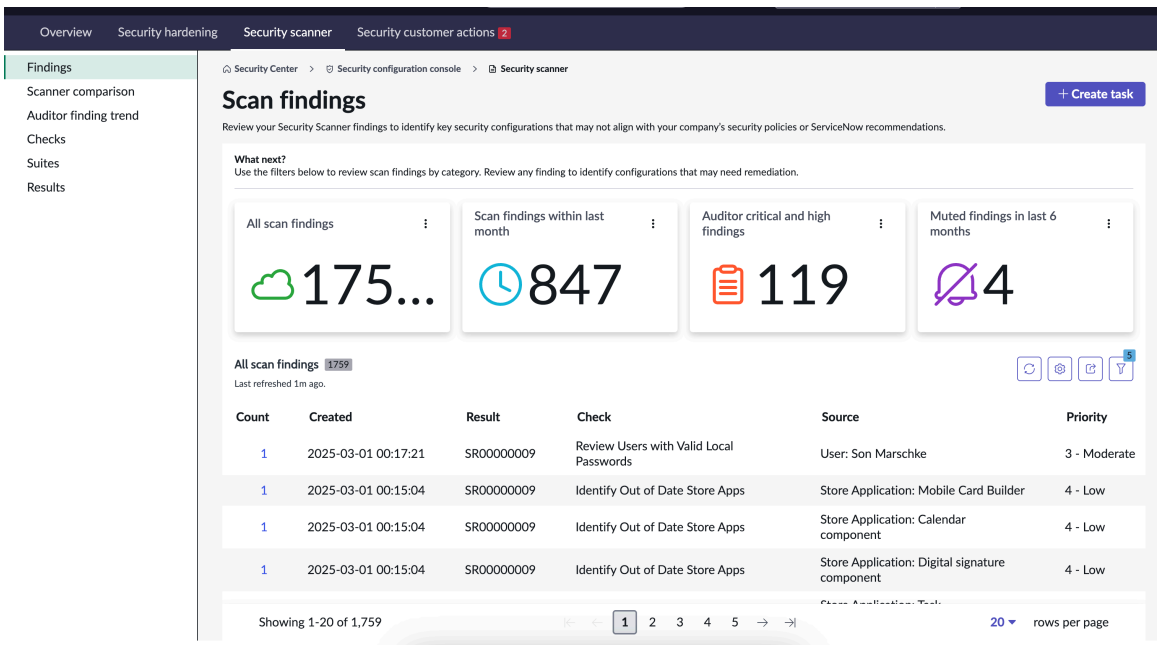


Sicherheitsscans sind eine Methode, um Ihre Instanz auf Konfigurationen zu untersuchen, die auf Probleme mit der Sicherheitsintegrität hinweisen. Mit dieser Methode können Sie Möglichkeiten zur Implementierung von Sicherheitsempfehlungen für Ihre Organisation identifizieren.

Beim Zugriff auf das Scanner-Tool ist kein Vergleich verfügbar, bis Sie die Suite auswählen, die mit mindestens zwei Scan-Ergebnissen der Suite verglichen werden soll. Sie können die Standard-Suite und -Prüfungen verwenden oder eigene anwenderdefinierte Prüfungen und Suites erstellen.

Scanfunde

Ein Ergebnis ist ein Verweis auf einen Datensatz, der gegen eine Regel aus einer Prüfung der Instanz verstoßen hat. Sie können den Quelldatensatz und die Häufigkeit finden, mit der der Datensatz die Regeln einer bestimmten Prüfung ausgelöst hat.



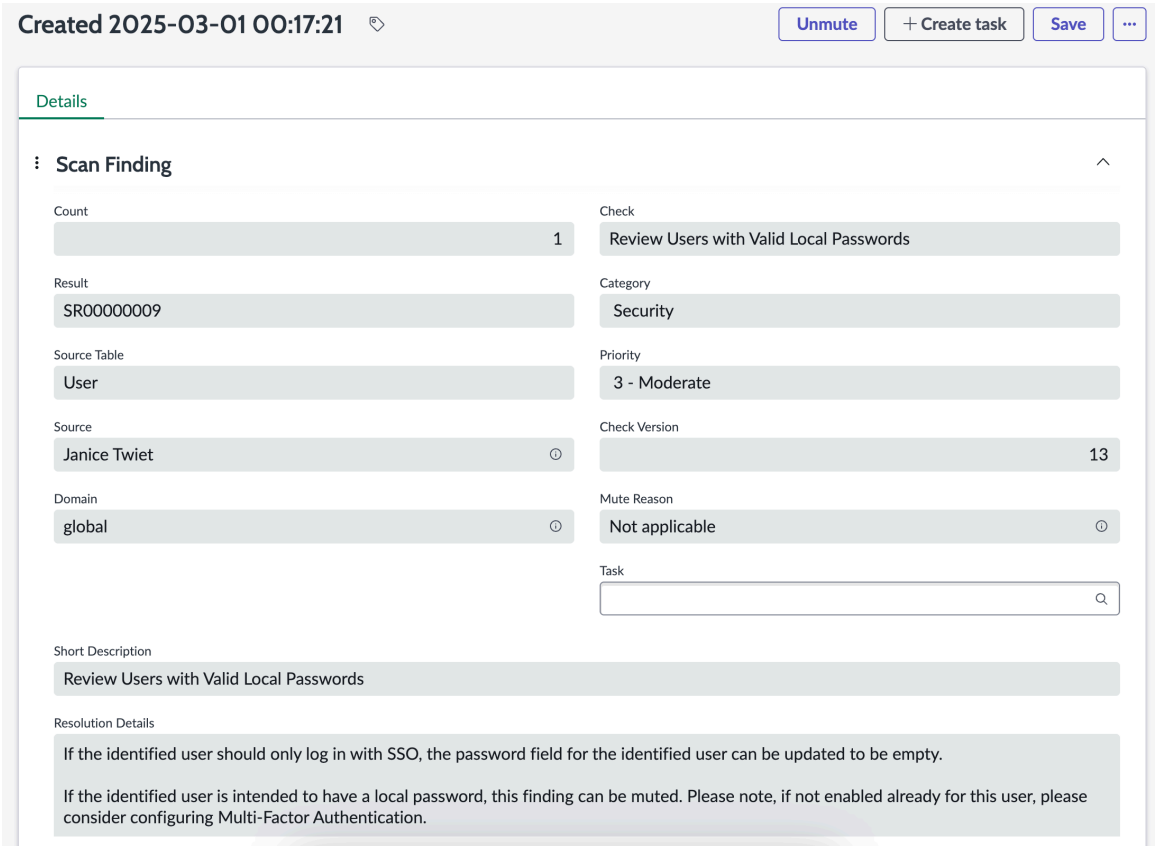
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie zu **Ergebnisse** Registerkarte zum Anzeigen von Scan-Ergebnissen in einer Liste. Die Karten über der Liste geben eine Anzahl der Ergebnisse an, die bestimmten auf der Karte aufgeführten Kriterien entsprechen. Wählen Sie eine dieser Karten aus, um die Liste so zu filtern, dass nur diejenigen angezeigt werden, die den Kriterien entsprechen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe zur Lösung eines Ergebnisses. Diese Schaltfläche wird sowohl in der Liste als auch im Ergebnisdatensatz angezeigt. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Scanfunde

Wählen Sie einen Link unter aus **Anzahl** Spalte zum Anzeigen eines Ergebnisdatensatzes, der granulare Details im Zusammenhang mit einem bestimmten Ergebnis anzeigt.



Überprüfen

Liste der Prüfungen, die dem Scan zugeordnet sind.

Kategorie

Sicherheitskategorie, die dem Scan zugeordnet ist. Zum Beispiel Zugriffssteuerung oder schädlicher Code.

Anzahl

Anzahl der Verstöße des Datensatzes gegen Prüfungsregeln.

Priorität

Schweregrad des Sicherheitsrisikos: 1 ist die höchste Priorität, 4 hingegen die niedrigste Priorität.

Ergebnis

Status und Typ des Scans.

Version überprüfen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Version der Prüfung.

Quelltabelle

Datensatz, der gegen eine Regel aus der Prüfung verstoßen hat.

Grund für Stummschaltung

Grund für das Stummschalten des Ergebnisses.

Quelle

Datum, an dem das Ergebnis erstellt wurde.

Aufgabe

Aufgabendatensatz, der dem Scan zugeordnet ist. Wird verwendet, um Aufgabenzuweisungen aus dem Ergebnis eines Datensatzes zu erleichtern.

Domäne

Auf welche Domäne der Scan angewendet wird.

Kurzbeschreibung

Kurze Erklärung des Scans.

Lösungsdetails

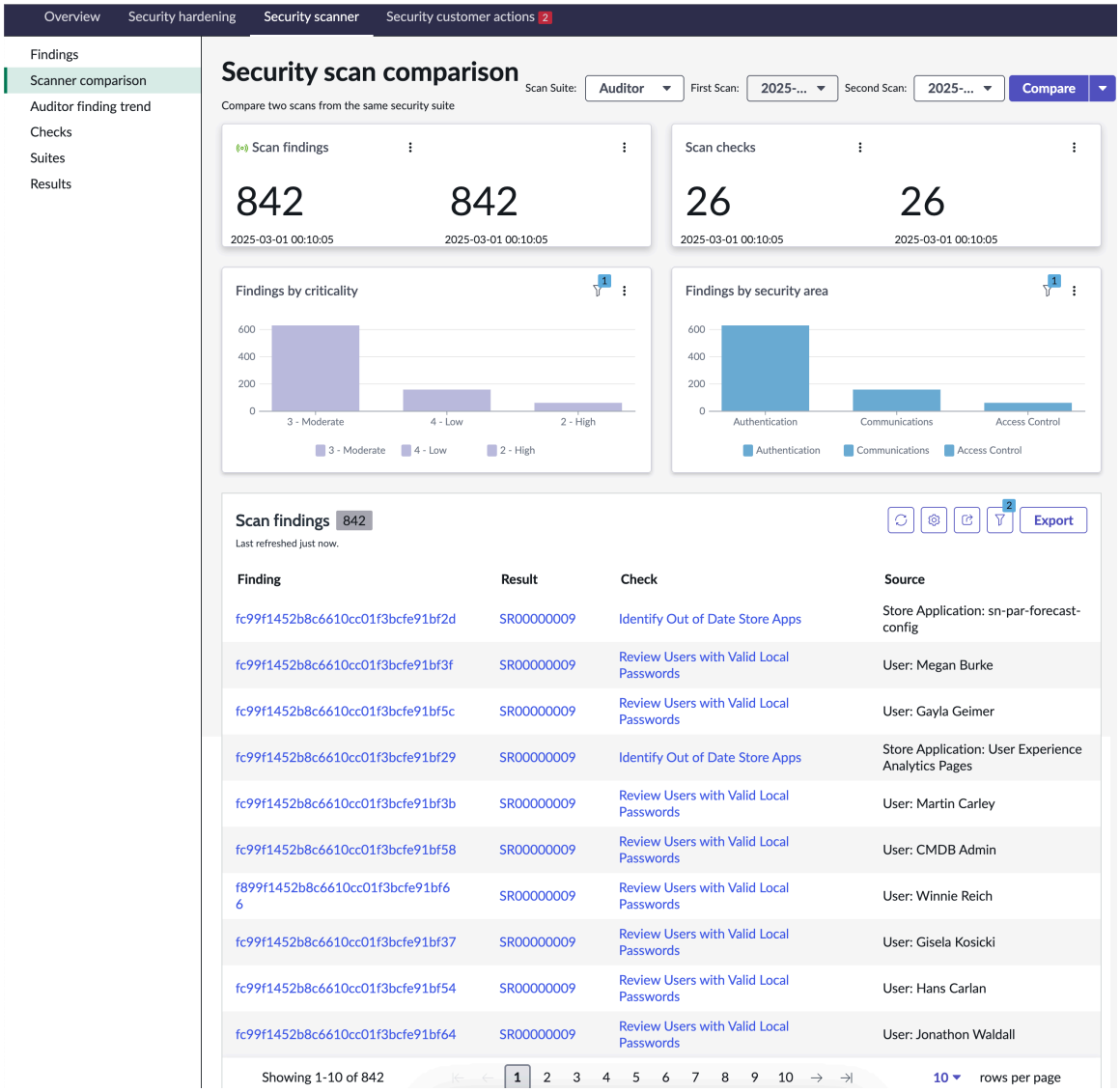
Anweisungen zur Lösung von Problemen, die vom Scan gemeldet wurden.

Ergebnisse können durch Auswahl von stummgeschaltet werden **Stummschalten/ Stummschaltung Aufheben** Schaltfläche. Wenn Sie ein Scan-Ergebnis stummschalten, werden Sie zu einem Grund für das Stummschalten des Ergebnisses aufgefordert. Ergebnisse, die in den letzten sechs Monaten stummgeschaltet wurden, sind auf der Karte „stummgeschaltete Ergebnisse“ in verfügbar **Scan-Ergebnisse** Seite.

Sicherheitsscanvergleich

Vergleichen Sie zwei Scans derselben Sicherheits-Suite, um Einblick in die Integrität Ihrer Härtungseinstellungen zu erhalten und die Sicherheitslage Ihrer Instanz zu verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wichtig: Diese Seite wird leer angezeigt, wenn Sie nicht zwei oder mehr Instanzen desselben Scans zum Vergleichen haben. Führen Sie mindestens zweimal einen Scan aus, um einen Vergleich auf dieser Seite anzuzeigen.

Wählen Sie im einen Scan aus **Scan-Suite** Liste, und wählen Sie dann eine aus **Erster Scan** Und **Zweiter Scan** Um einen Vergleich zu beginnen.

Auf der Vergleichsseite für Sicherheitsscans werden die Sicherheitsänderungen in Ihren Härtungseinstellungen zwischen dem ersten und dem zweiten Scan angezeigt. Nachfolgend finden Sie eine Erklärung für jede Karte:

Scanfunde

Anzahl der Ergebnisse im ausgewählten Scan an jedem ausgewählten Datum.

Scanprüfungen

Anzahl der Scan-Prüfungen, die im ausgewählten Scan an jedem ausgewählten Datum durchgeführt wurden.

Geänderte Ergebnisse nach Relevanz

Diagramm, das alle Ergebnisse nach Relevanz organisiert anzeigt.

Geänderte Ergebnisse nach Sicherheitsbereich

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

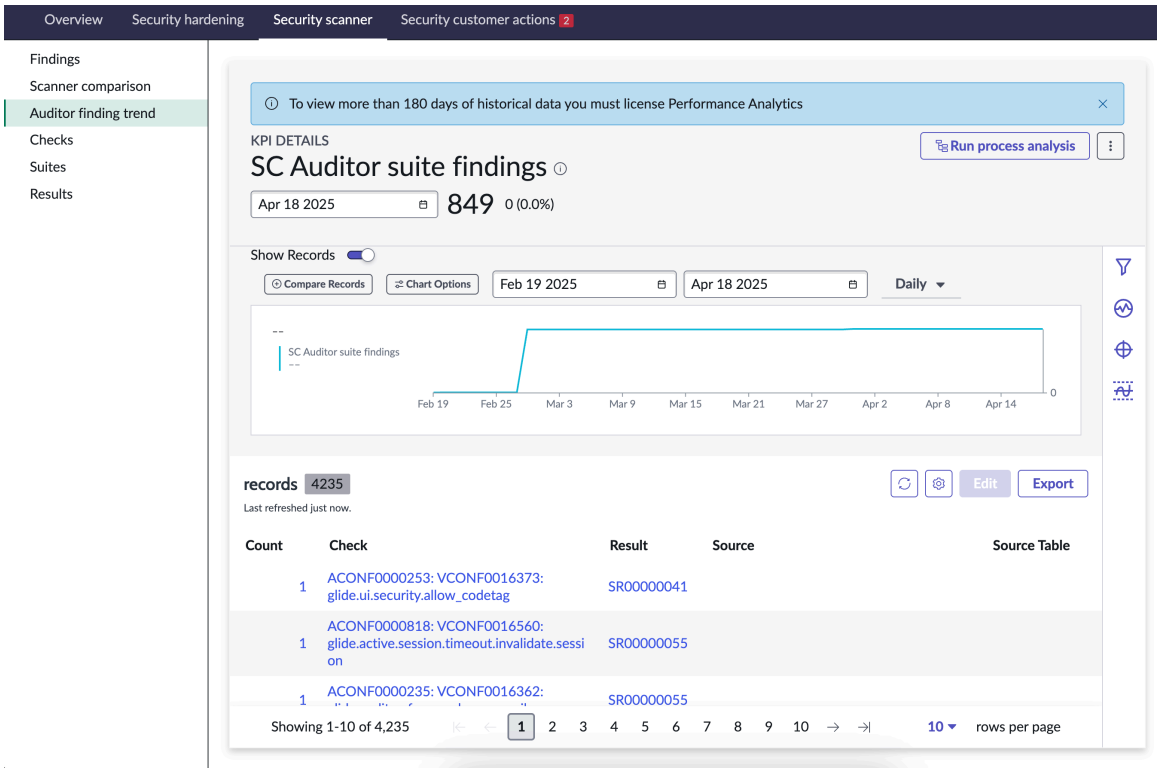
Diagramm, in dem alle Ergebnisse des organisierten Sicherheitsbereichs angezeigt werden.

Scanfunde

Liste aller Scan-Ergebnisse. Wählen Sie ein Ergebnis aus, scannen Sie ein Ergebnis oder aktivieren Sie es, um den zugehörigen Datensatz anzuzeigen und zusätzliche Details zu finden. Verwenden Sie die unteren Bereiche oben rechts, um die Liste zu filtern, zu aktualisieren oder zu exportieren.

Ergebnisse der Auditor-Suite

Überprüfen Sie die Ergebnisse der Security Center-Auditor-Suite im Zeitverlauf.



SC Auditor Suite-Ergebnisdiagramm

Auf der Seite werden die Ergebnisse der SC Auditor-Suite im Vergleich zu den beiden ausgewählten Daten angezeigt.Verwenden Sie die **Diagrammoptionen** Schaltfläche, um anzugeben, welche Informationen analysiert und wie die Informationen präsentiert werden sollen.

Analyse

Wählen Sie aus der Liste der Optionen aus. Einige Optionen sind je nach ausgewähltem Diagrammtyp möglicherweise nicht verfügbar.

Zielvorgabe

Ziele, die Ihre Organisation erreichen möchte. Weitere Informationen finden Sie unter Indikatorziele .

Schwellenwert

Definiert einen normalen Punktzahlbereich für einen Indikator und warnt Sie, wenn ein bestimmtes Ereignis auftritt. Weitere Informationen finden Sie unter Indikatorschwellenwerte .

Prognose

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibt die Möglichkeit, zukünftige Punktzahlen basierend auf vergangenem Verhalten zu prognostizieren. Weitere Informationen finden Sie unter Performance Analytics – Prognosen zu Punktzahlen .

Trend

Zeigt an, wie sich der Wert eines oder mehrerer Elemente im Laufe der Zeit ändert.

Kommentare

Zeigt Anmerkungen zu einzelnen Datenpunkten an.

Bezeichnungen

Zeigt Punktzahlen im Zusammenhang mit Visualisierungen an.

Statistik

Zeigt Statistiken im Zusammenhang mit Ihrer Compliance-Punktzahl an.

Zeitreihen

Wählen Sie aus, welche Metrik im Diagramm angezeigt werden soll.

Punktzahl

Punktzahl für den Leistungskennzahl (KPI).

Change

Änderung der Punktzahl für diesen Indikator.

Prozentuale Veränderung

Ändern Sie als Prozentsatz der Punktzahlen.

Diagrammtyp

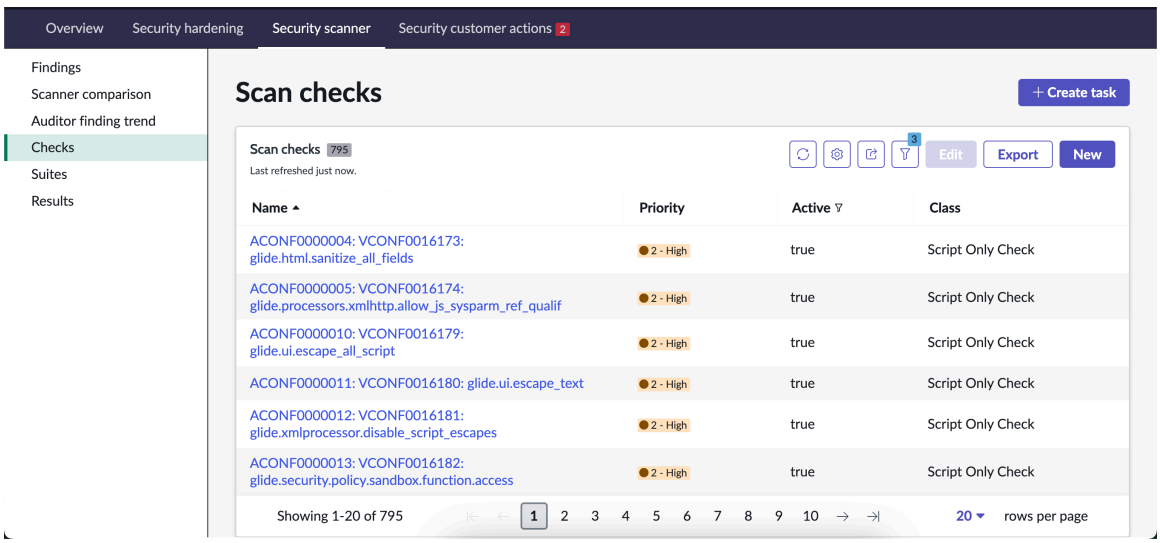
Wählen Sie einen Diagrammtyp aus, um zu steuern, wie die von Ihnen ausgewählten Informationen visualisiert werden. Weitere Informationen finden Sie unter Anwendungsfälle für verschiedene Zeitreihenvisualisierungstypen .

Datensatzliste

Listet die Prüfungen auf, die als Teil der Suite durchgeführt wurden.

Scanprüfungen

Verwenden Sie Prüfungen, um Anomalien innerhalb einer Instanz zu erkennen, die für Tabellen, Datensätze oder Metadaten ausgeführt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfungen sind Regeln, die zum Erkennen von Anomalien in einer Instanz entwickelt wurden. Wählen Sie eine Prüfung in der Liste aus, um Details anzuzeigen, einschließlich der Bewertung der Prüfung und möglicher Schritte zur Behebung des Problems, wenn die Prüfung Ergebnisse zurückgibt.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Scan-Prüfung. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

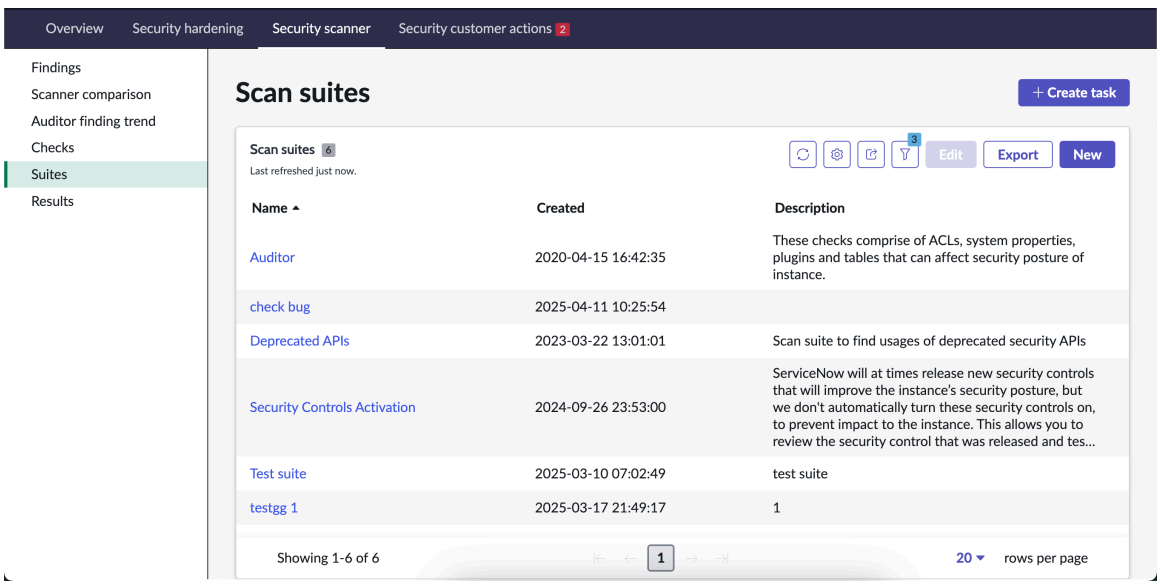
Prüfungen sind in vier Klassen unterteilt, um Probleme zu identifizieren und Sicherheitsempfehlungen für Ihre Organisation zu implementieren: Tabellenprüfungen, Spaltentypprüfungen, nur Skriptprüfungen und Linter-Prüfungen.

Klassen überprüfen

Klasse überprüfen	Beschreibung
Tabellenprüfungen	Verwenden Sie diese Prüfklasse, wenn Sie die spezifischen Tabellen und Prüfungen kennen, die Sie testen möchten.
Spaltenprüfungen	Verwenden Sie diese Prüfklasse, um die von Ihnen erstellte Regel zu implementieren, um alle Datensätze zu iterieren, die dem Zielspaltenfeldtyp entsprechen.
Skriptprüfungen	Verwenden Sie diese Prüfklasse, um Metadaten und Konfigurationen zu verifizieren und komplexe Prüfungen auszuführen, indem Sie eigene Prüfungen schreiben.
Linter-Prüfungen	Verwenden Sie diese Prüfklasse, um Probleme in einem Skript zu identifizieren. Wenn eine Linter-Prüfung für einen Datensatz ausgeführt wird, wird eine abstrakte Syntaxstruktur für seinen Code generiert, die zur Analyse von Problemen mit dem Code verwendet werden kann.

Scan-Suites

Überprüfen Sie die Details der Scan-Suites, die in Ihrer Instanz verfügbar sind.

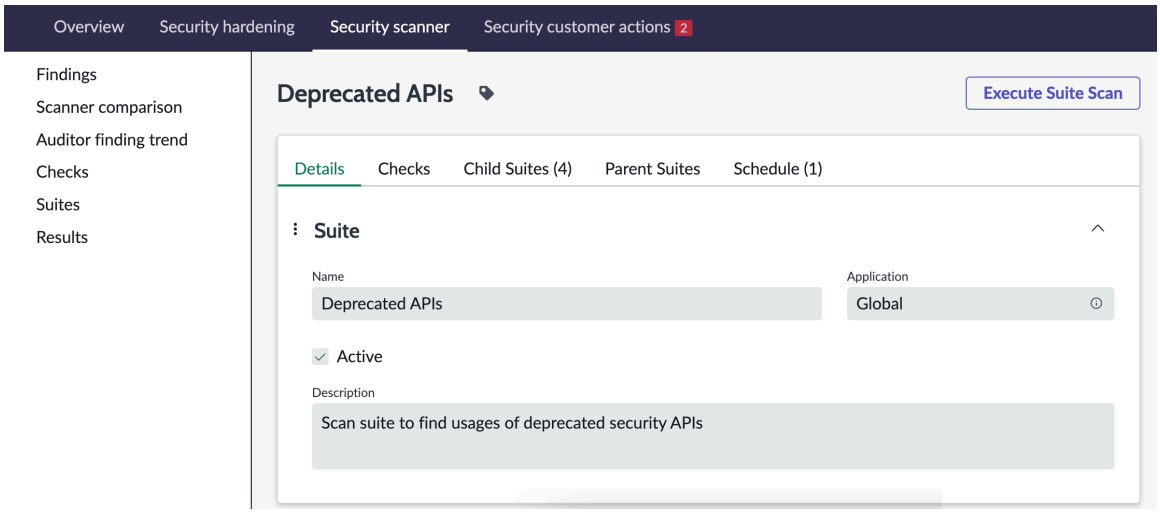


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scan-Suites sind Sammlungen von Sicherheitscenter-Prüfungen, die zusammen ausgeführt werden. Sie können Basissystem-Suites verwenden oder eigene erstellen, indem Sie eine vorhandene Suite klonen und die im Klon vorgenommenen Prüfungen aktualisieren. Details finden Sie unter Erstellen Sie eine Scan-Suite.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Scan-Suite. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Scan-Suite-Details



Wählen Sie aus **Name** Feld einer Suite zum Anzeigen der Suite-Details. Diese Seite enthält Details zu den Scan-Suites in einer Schnittstelle mit Registerkarten. Auf der Seite mit Registerkarten finden Sie diese Informationen:

Details

Details zur Suite umfassen Name, Anwendung und Beschreibung.

Überprüfungen

Liste der Prüfungen, die in dieser Suite enthalten sind. Details zu einzelnen Prüfungen sind mit denen in identisch Scanprüfungen.

Untergeordnete Suites

Liste der untergeordneten Suites, die dieser Suite zugeordnet sind. Wenn Sie diese Suite ausführen, werden auch alle untergeordneten Suites ausgeführt.

Übergeordnete Suites

Liste der Suiten, in denen diese Suite eine untergeordnete Suite ist. Wenn Sie eine übergeordnete Suite ausführen, wird diese Suite ebenfalls ausgeführt.

Zeitplan

Details der geplanten Ausführung dieser Suite.

Zugriffssteuerungen Auditor-Prüfungen

Erfahren Sie mehr über die Prüfungen, die in den Auditor-Suites für Standardzugriffssteuerungen verfügbar sind, welche Kriterien sie bewerten und wie sie verwendet werden können, um die Sicherheit Ihrer Instanz zu verbessern.

Zugriffssteuerungslisten-Regeln (ACLs) beschränken den Zugriff auf Daten, indem sie von Anwendern verlangen, eine Reihe von Anforderungen zu erfüllen, bevor sie mit ihnen interagieren können. Auditor-Prüfungen für Zugriffssteuerungen bewerten Ihre Instanz gemäß den acht in der folgenden Tabelle aufgeführten Kriterien. Verwenden Sie die Ergebnisse dieser Prüfungen, um die Sicherheit Ihrer Instanz zu verbessern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerungen Auditor-Prüfungen

Name überprüfen	Kriterien Überprüfen	Beschreibung
Alle Prozessoren vom Typ „-SCRIPT“ müssen mit CSRF-Token geschützt werden.	Sucht nach Prozessoren mit **SKRIPT** Typ, der nicht durch ein CSRF-Token geschützt ist.	Alle Prozessoren mit **SKRIPT** Der Typ muss mit einem CSRF-Token (Cross-Site Request Forgery) geschützt werden. Für diese Prozessoren muss die CSRF-Option aktiviert sein, die verhindert, dass der Prozessor ausgeführt wird, es sei denn, die Instanz verwendet ein CSRF-Token.
Anwenderkriterien „Kann beitragen“/„Kann nicht beitragen“ sind für jedes Wissen zu definieren.	Sucht nach Knowledge Base-Datensätzen, die nicht enthalten **Kann Beitragen** Oder **Kann Nicht Mitwirken** Anwenderkriterien definiert.	Jede Knowledge Base muss entweder haben **Kann Beitragen** Oder **Kann Nicht Mitwirken** Anwenderkriterien definiert. Andernfalls kann jeder Anwender Inhalte zu einer Knowledge Base beitragen, ohne dass Mitwirkkriterien definiert sind.
Leere ACLs	Sucht nach ACL-Datensätzen (Access Control List), die kein Sicherheitsattribut, keine Rolle oder haben **Öffentlich** Rolle.	ACLs werden leer gelassen oder mit verwendet **Öffentlich** Die Rolle kann offenen Zugriff auf alle von dieser ACL geschützten Inhalte gewähren.
Zugriffssteuerungen für vom Client aufrufbare Skripteinbindungen	Sucht nach vom Client aufrufbaren Skripteinbindungen, die nicht durch ACLs gesichert sind.	Alle vom Client aufrufbaren Skripteinbindungen müssen mit einer ACL mit den erforderlichen Rollen gesichert werden.
Zugriffssteuerungen für UI-Seiten	Sucht nach UI-Seiten, die nicht durch ACLs gesichert sind	Ohne eine ACL, die den Zugriff auf eine UI-Seite sichert, ist diese UI-Seite für alle angemeldeten internen Anwender zugänglich. Ohne Einschränkungen können angemeldete Anwender potenziell nicht autorisierte Änderungen vornehmen.
Zugriffssteuerungen für Tabellen	Sucht nach Tabellen ohne ACLs	Tabellen müssen mit ACLs gesichert werden. Der Zugriff auf Daten, die in Tabellen gespeichert sind, sollte nur auf Anwender beschränkt werden, die ihn benötigen.
Der Anwenderaccount darf nicht sowohl interne als auch externe Rollen haben	Sucht nach Anwenderdatensätzen mit beiden **Intern** Und **Extern** Rollen zugewiesen	Interne Anwenderrollen sind für Anwender in Ihrem Unternehmen vorgesehen. Externe Anwenderrollen sind für externe Mitarbeiter wie Kunden und Partner vorgesehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerungen Auditor-Prüfungen (Fortsetzung)

Name überprüfen	Kriterien Überprüfen	Beschreibung
Öffentlich zugängliche Knowledge Base und Artikel	Sucht nach öffentlich zugänglichen Knowledge Bases und Knowledge Base-Artikeln	Öffentlich zugängliche Knowledge Bases und Artikel sind für alle Anwender in der Instanz sichtbar. Erhöhen Sie die Sicherheit, indem Sie Knowledge Bases und Artikel auf die spezifische Zielgruppe beschränken, die sie benötigt.

Auditor-Prüfungen

Verwenden Sie die Auditor-Suite für SecureCheck, um Fehlkonfigurationen zu erkennen, die sich auf die Sicherheitslage Ihrer Instanz auswirken können.

Überprüfen Sie die Informationen

Zugriffssteuerungen Auditor-Prüfungen

Name überprüfen	Beschreibung	Scan-Ergebnistyp
Identifizieren Sie veraltete Store-Apps	Identifiziert Apps, die auf Ihrer Instanz aktiviert sind und über aktualisierte Versionen verfügen. Überprüfen Sie, ob Sie die aktuellsten Versionen von Store-Anwendungen ausführen, die Korrekturen potenzieller Sicherheitsprobleme enthalten können.	Lösung Empfohlen
Unsichere GlideRecord-Anrufe	Identifiziert Skripts, die von Endanwendern direkt aufgerufen werden können (z. B. vom Client aufrufbare Skripteinbindungen, Widgets, Prozessoren, REST-Endpunkte) Diese Skripts sollten ACLs beachten und GlideRecordSecure oder GlideRecord mit canRead, canWrite, canCreate, canDelete verwenden.	Lösung Empfohlen
Überprüfen Sie die zulässigen JavaScript-Bibliotheken	Gibt Skripts an, in denen die JavaScript-Inhaltszugriffssteuerung verwendet wird, um bestimmte JavaScript-Bibliotheken von Drittanbietern zuzulassen oder abzulehnen. Überprüfen Sie Instanzanpassungen, um sicherzustellen, dass Bibliotheken nicht verwendet werden, bevor Sie den Zugriff blockieren. Die Tabelle „Zugriffsnachverfolgung für JavaScript-Inhaltsanbieter“ [sys_js_content_Provider_Access_Tracking] kann überprüft werden, um das letzte	Lösung Empfohlen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerungen Auditor-Prüfungen (Fortsetzung)

Name überprüfen	Beschreibung	Scan-Ergebnistyp
	Datum anzuzeigen, an dem auf die Bibliothek zugegriffen wurde. **Hinweis:** Diese Prüfung kann in Instanzen ignoriert werden, die ursprünglich in Tokio oder später bereitgestellt wurden. Für Datensätze in der zugehörigen Tabelle sind standardmäßig Deny-Regeln festgelegt. In Instanzen, die ursprünglich vor Tokio bereitgestellt wurden, können in den Tabellen der JavaScript-Zugriffssteuerung zulässige Regeln vorhanden sein.	
Überprüfen Sie vom Client aufrufbare Skripteinbindungen ohne entsprechende ACL	Identifiziert vom Client aufrufbare Skripteinbindungen, die keine entsprechende ACL haben. Diese Skripts verwenden die standardmäßige ACL („*“) des aufrufbaren Clientskripts. Erstellen Sie für diese Skripts ACLs, die die entsprechenden Zugriffskriterien definieren, um sicherzustellen, dass nur erwartete Anwender mit der bereitgestellten Funktionalität interagieren können.	Lösung Empfohlen
Überprüfen Sie anwenderdefinierte Tabellen mit Datensatzerstellern und ohne Business-Regel	Identifiziert Datensatzersteller, die keine zusätzliche serverseitige Validierung haben. Diese Prüfung identifiziert anwenderdefinierte Tabellen mit einem Datensatzersteller, aber ohne zugehörige Business-Regel. Dies kann Anwendern ermöglichen, unerwartete Daten an die zugehörige Tabelle zu übermitteln.	Lösung Empfohlen
Überprüfen Sie leere ACLs	Identifiziert ACL-Datensätze, die kein Skript, keine Bedingung, kein Sicherheitsattribut oder keine Rolle oder ACLs mit haben **Öffentlich** Rolle. ACLs werden leer gelassen oder mit verwendet **Öffentlich** Die Rolle bietet offenen Zugriff auf alle von dieser ACL geschützten Inhalte.	Lösung Empfohlen
Überprüfen Sie Felder mit deaktivierter HTML-Bereinigung	Gibt HTML-Felder an, wo HTML-Bereinigung Ist inaktiv.	Lösung Empfohlen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerungen Auditor-Prüfungen (Fortsetzung)

Name überprüfen	Beschreibung	Scan-Ergebnistyp
	HTML-Bereinigung entfernt oder ersetzt potenziell schädliche Elemente und Attribute im HTML-Code. Überprüfen Sie HTML-Felder, in denen die Bereinigung inaktiv ist, um zu bestätigen, ob diese Konfiguration erforderlich ist.	
Überprüfen Sie inaktive Sicherheitsfunktionen-Plugins	Identifiziert nicht aktivierte Plugins, die zusätzliche, konfigurierbare Sicherheitskontrollen bereitstellen. Die Ergebnisse dieser Prüfung werden zu Informationszwecken bereitgestellt. Bevor Sie eines der identifizierten Plugins aktivieren, stellen Sie sicher, dass das Plugin Ihre Anwendungsfälle oder Anforderungen erfüllt. Sie können diese Ergebnisse stummschalten, wenn Sie keinen Anwendungsfall für den identifiziert haben.	Informieren
Überprüfen Sie große zulässige IP-Adressbereiche	Identifiziert IP-Adresszugriffssteuerungsbereiche, die eine große Anzahl von IP-Adressen enthalten. **Hinweis:** Wenn Sie eine große Anzahl von falsch positiven Ergebnissen sehen, sollten Sie die Variable largestExpectedCIDRBlock an Ihre spezifischen Geschäftsanforderungen anpassen. CIDR-Blöcke (Classless Inter Domain Routing) enthalten eine größere Anzahl von IP-Adressen, wenn die Anzahl abnimmt. Beispielsweise ist der CIDR-Block 8 größer (enthält mehr IP-Adressen) als die CIDR-Blockgröße 16. Überprüfen und bestätigen Sie, dass die aktuelle Konfiguration Ihren Geschäftsanforderungen entspricht.	Überprüfen und entscheiden
Überprüfen Sie öffentliche GraphQL-Schemas	Identifiziert öffentliche GraphQL-Schemas in der GraphQL-API-Tabelle [sys_graphql_Schema]. Diese Schemas können so konfiguriert werden, dass sie ohne Authentifizierung verfügbar sind. Je nach Funktionalität des	Überprüfen und entscheiden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerungen Auditor-Prüfungen (Fortsetzung)

Name überprüfen	Beschreibung	Scan-Ergebnistyp
	Endpunkts kann dies nicht authentifizierten Anwendern ermöglichen, unerwartete Aktionen auszuführen oder mit unerwarteten Daten zu interagieren.	
Überprüfen Sie öffentliche Knowledge Base-Artikel	Identifiziert Knowledge Bases und Knowledge Base-Artikel, die konfiguriert sind, um nicht authentifizierten Anwendern Zugriff zu ermöglichen. Überprüfen und bestätigen Sie, dass die aktuelle Konfiguration Ihren Geschäftsanforderungen entspricht.	Überprüfen und entscheiden
Überprüfen Sie die öffentlichen REST API-Endpunkte	Identifiziert Rest-API-Endpunkte in der Tabelle „geskriptete REST-Ressource“ [sys_WS_Operation], die so konfiguriert sind, dass sie ohne Authentifizierung verfügbar sind. Je nach Funktionalität des Endpunkts kann dies nicht authentifizierten Anwendern ermöglichen, unerwartete Aktionen auszuführen oder mit unerwarteten Daten zu interagieren.	Überprüfen und entscheiden
Überprüfen Sie die Seiten des öffentlichen Serviceportals	Identifiziert Serviceportal-Seiten, die öffentlich gemacht werden. Serviceportal-Seiten werden nicht authentifizierten Anwendern zur Verfügung gestellt, indem das Feld „öffentlich“ auf „wahr“ festgelegt wird. Überprüfen und bestätigen Sie, dass die aktuelle Konfiguration Ihren Geschäftsanforderungen entspricht.	Überprüfen und entscheiden
Überprüfen Sie öffentliche UI-Seiten	Gibt UI-Seiten an, die öffentlich gemacht werden. UI-Seiten können für nicht authentifizierte Anwender mithilfe der Seite [sys_public] verfügbar gemacht werden. Überprüfen und bestätigen Sie, dass die aktuelle Konfiguration Ihren Geschäftsanforderungen entspricht.	Überprüfen und entscheiden
Überprüfen Sie Rollen, die die Rolle „admin“ enthalten	Identifiziert alle Rollen (Tabelle „Rollen“ [sys_user_role]), die enthalten **Administrator** Rolle.	Überprüfen und entscheiden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerungen Auditor-Prüfungen (Fortsetzung)

Name überprüfen	Beschreibung	Scan-Ergebnistyp
	Die **Administrator** Die Rolle gewährt Anwendern Administratorrechte und sollte nur bei Bedarf verwendet werden. Überprüfen und bestätigen Sie, dass die aktuelle Konfiguration Ihren Geschäftsanforderungen entspricht. Wenn dies eine absichtliche Konfiguration ist, kann diese Prüfung stummgeschaltet werden.	
Überprüfen Sie UI-Seiten ohne entsprechende ACLs	Identifiziert UI-Seiten, die keine ACL für diese UI-Seite haben. UI-Seiten, die keine bestimmte ACL haben, standardmäßig auf eine generische UI-Seiten-ACL, Die unbeabsichtigten Anwendern Zugriff gewähren kann.	Lösung Empfohlen
Überprüfen Sie Anwender mit gültigen lokalen Passwörtern	Identifiziert Anwender mit lokal festgelegten Passwörtern. Anwender mit lokalen Passwörtern können mithilfe der lokalen Anmeldeinformationen über APIs mit der Instanz interagieren, auch wenn lokale Anmeldungen nicht zulässig sind. Diese Passwortkonfiguration ist erforderlich, damit Integrationsanwenderaccounts ordnungsgemäß funktionieren. Überprüfen Sie diese Anwenderaccounts, um sicherzustellen, dass sich nur beabsichtigte Anwender (z. B. Integrationsaccounts) mit lokaler Authentifizierung authentifizieren können.	Überprüfen und entscheiden
Rotieren Sie Passwörter, die mit veralteten Hashing-Algorithmen gespeichert wurden	Identifiziert Anwenderaccounts mit Passwörtern, die in früheren Versionen von erstellt wurden ServiceNow AI Platform, Der möglicherweise einen veralteten oder veralteten Hashing-Algorithmus verwendet hat. Für Accounts, die mit alten Plattformversionen erstellt wurden und ihre Passwörter nicht rotiert wurden, können weiterhin Passwörter mit einem Legacy-Hashing-Algorithmus gespeichert werden. Überprüfen Sie die erstellten identifizierten Accounts unter Berücksichtigung der Passwortzurücksetzung.	Lösung Empfohlen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssteuerungen Auditor-Prüfungen (Fortsetzung)

Name überprüfen	Beschreibung	Scan-Ergebnistyp
Datensatzersteller werden gesichert	Identifiziert unsichere Datensatzersteller. Wenn sie nicht den entsprechenden Rollen zugewiesen sind, können nicht autorisierte Anwender darauf zugreifen, wodurch möglicherweise vertrauliche Informationen offengelegt werden. Weisen Sie Datensatzerstellern entsprechende Rollen zu, um sicherzustellen, dass sie nur für Anwender zugänglich sind, die sie benötigen.	Lösung Empfohlen
Sichtbarkeit der UI-Aktion	Identifiziert UI-Aktionen, auf die ein Anwender ohne Rollen zugreifen kann, der keinen Lesezugriff auf die Tabelle hat. Diese Anwender können möglicherweise Daten in einer Tabelle ändern, auf die sie über diese UI-Aktionen keinen Zugriff haben. Stellen Sie sicher, dass UI-Aktionen nur für Anwender mit Zugriff auf die von ihnen betroffene Tabelle verfügbar sind.	Lösung Empfohlen

Erstellen Sie eine Scan-Suite

Erstellen und planen Sie eine anwenderdefinierte Suite, damit Sie die Sicherheit Ihrer Instanz für Ihre Organisation analysieren können.

Vorbereitungen

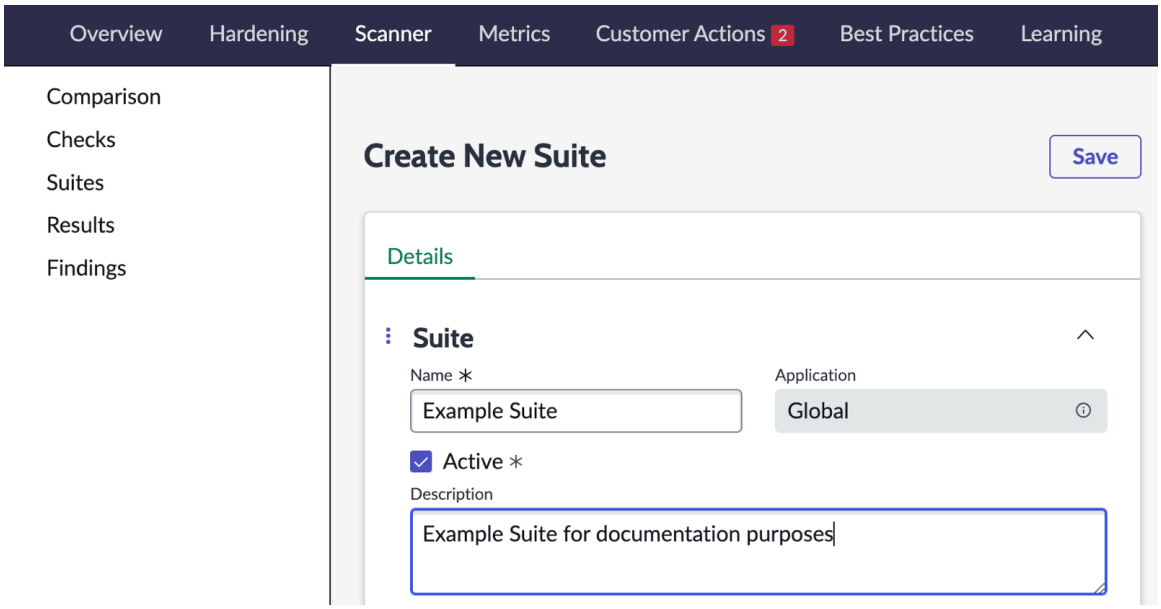
Erforderliche Rolle: administrator oder sn_vsc.security_center_viewer.

Eine Suite ist eine Sammlung von Prüfungen, die für einen Scan verwendet werden können. Zeigen Sie eine Liste der Scan-Suites an, die in einer Tabelle organisiert sind, indem Sie zu navigieren **Scanner** > **Suites**an. Erstellen Sie Ihre eigenen Suites, oder um die Standard-Suite Auditor zu verwenden. Auditor ist eine standardmäßige Basissystemsuite, die Prüfungen auf Best Practices für Sicherheit enthält. Diese Prüfungen bestehen aus Systemeigenschaften, Plugins und Tabellen, die sich auf die Sicherheitslage Ihrer Instanz auswirken können. Die folgenden Schritte zeigen, wie Sie eine Suite zusammen mit den verschiedenen Optionen erstellen, die für ihre Konfiguration verfügbar sind.

Prozedur

1. Wählen Sie im Sicherheitscenter die aus **Scanner** Registerkarte, und wählen Sie dann aus **Suiten** Im Bereich auf der linken Seite des Bildschirms.
2. In **Scan-Suites** Wählen Sie Seite aus **Neu** Schaltfläche.
3. Geben Sie eine Suite ein **Name** Und **Beschreibung** , Und wählen Sie dann aus **Speichern**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nach Auswahl **Speichern** , Konfigurationsoptionen für die Suite werden in einer Benutzeroberfläche mit Registerkarten angezeigt.

4. Wählen Sie aus **Prüfungen** Registerkarte.
   Verwenden Sie diese Registerkarte, um Ihrer Suite Prüfungen hinzuzufügen.
   a. Wählen Sie **Bearbeiten**.
   b. Wählen Sie die Prüfungen aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um es in Ihrer Suite zu platzieren.
   c. **Speichern** .
5. Wählen Sie aus **Untergeordnete Suites** Registerkarte.
   Verwenden Sie diese Registerkarte, um untergeordnete Suites hinzuzufügen. Als untergeordnete Suites hinzugefügte Suites werden ebenfalls ausgeführt.wenn diese Suite in einem Scan verwendet wird.
   a. Wählen Sie **Bearbeiten**.
   b. Wählen Sie die untergeordneten Suites aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um es in Ihrer untergeordneten Suite zu platzieren.
   c. **Speichern** .
6. Wählen Sie aus **Übergeordnete Suites** Registerkarte.
   Verwenden Sie diese Registerkarte, um übergeordnete Suites hinzuzufügen. Übergeordnete Suites, die in einem Scan ausgeführt werden, führen diese Suite ebenfalls aus.
   a. Wählen Sie **Bearbeiten**.
   b. Wählen Sie die untergeordneten Suites aus, die Sie hinzufügen möchten, und wählen Sie dann Hinzufügen (**>**), um es in Ihrer übergeordneten Suite zu platzieren.
   c. **Speichern** .
7. Wählen Sie die Registerkarte **Zeitplan**.
   Verwenden Sie diese Registerkarte, um eine Zeit für die Ausführung Ihrer Suite festzulegen.
   a. Wählen Sie **Neu**.
   b. Geben Sie Details des geplanten Scans ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Zeitfelder haben das folgende Format: Stunde:Minuten:Sekunden.

c. Speichern .

Klonen Sie die Auditor-Suite für Zugriffssteuerungen

Klonen und passen Sie die Auditor-Suite für Standardzugriffssteuerungen in Ihrer Instanz an, um eine neue Suite zu erstellen, die auf die Sicherheitspraktiken Ihrer Organisation zugeschnitten ist.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die mit Ihrer Instanz bereitgestellte Auditor-Suite für Standardzugriffssteuerungen kann nicht geändert werden. Wenn Sie jedoch Prüfungen hinzufügen, entfernen oder bearbeiten möchten, um sie den Sicherheitspraktiken Ihrer Organisation anzupassen, können Sie die Auditor-Suites für Zugriffssteuerungen duplizieren. Durch das Kopieren der Auditor-Suites für Zugriffssteuerungen können Sie sie anpassen und eine neue Suite basierend auf der Standardsuite erstellen. Die Auditor-Suites für Zugriffssteuerungen enthalten Prüfungen im Zusammenhang mit Best Practices für Sicherheit, die Systemeigenschaften, Plugins und Tabellen abdecken, die sich auf die Sicherheitslage der Instanz auswirken. Die folgenden Schritte demonstrieren, wie Sie die Auditor-Suites für Standardzugriffssteuerungen duplizieren, um sie an die Anforderungen Ihrer Organisation anzupassen.

Prozedur

1. Navigieren zu **Alle** > **Instanz-Scan** > **Suites**an.
2. Wählen Sie Aus **Neu** Und geben Sie einen Namen für Ihre Suite zusammen mit einer optionalen Beschreibung ein.
3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
4. Fügen Sie die für Ihren Scan erforderlichen Prüfungen hinzu.

   a. In **Prüfungen** Wählen Sie die Registerkarte aus **Bearbeiten** .

   b. Fügen Sie die Bedingungen hinzu.
   Um beispielsweise Scan-Prüfungen hinzuzufügen, wenden Sie die folgenden Felder, Operatoren, Werte und Bedingungen an:

   [Kategorie][ist][Sicherheit] UND [Anwendung][ist][Global]

   Zum Beispiel sollte es wie folgt aussehen: Kategorie ist „Sicherheit“ und „Anwendung“ ist „Global“ .

5. Wählen Sie Aus **Filter ausführen** .
6. Wählen Sie die Scan-Prüfungen aus, die Sie aus der Sammlungsliste der Prüfliste hinzufügen möchten, und wählen Sie dann die Schaltfläche Hinzufügen (>).
7. Wählen Sie Aus **Speichern** .
   Die Suite mit Ihren hinzugefügten anwenderdefinierten Prüfungen wurde erstellt.
8. Wählen Sie Aus **Suite-Scan Ausführen** .

Zeigen Sie die Auditor-Suite für Zugriffssteuerungen an

Zeigen Sie die Prüfungen an, die in den Auditor-Suites für Standardzugriffssteuerungen verfügbar sind, um zu verstehen, welche Prüfungen bei der Ausführung dieser Suite ausgeführt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Schritte, die Sie ausführen müssen, um auf die Auditor-Suites für Standardzugriffssteuerungen in Ihrer ServiceNow-Instanz zuzugreifen.

Prozedur

1. Wählen Sie im Sicherheitscenter die aus **Scanner** Registerkarte, und wählen Sie dann aus **Suiten** Im Bereich auf der linken Seite.
2. In **Scan-Suites** Seite auswählen **Auditor** Aus der Liste.
3. Um die Suite-Prüfungen zu überprüfen, wählen Sie aus **Prüfungen** Registerkarte.
   Sie sollten die Liste der 8 Prüfungen sehen, die für die Suite verfügbar sind.
4. Wählen Sie den Namen der Prüfung aus, die Sie analysieren möchten.
5. Analysieren Sie die Felder, die der Prüfung zugeordnet sind.

Name	Beschreibung
Name	Name der Prüfung.
Anwendung	Die Anwendung, zu der die Prüfung gehört (Sicherheitscenter).
Kategorie	Kategorie, die der Prüfung zugeordnet ist.
Priorität	Die Dringlichkeit.
Version	Versionsnummer der Prüfung.
Aktiv	Der Status der Prüfung, z. B. „aktiv“ oder „inaktiv“.
Kurzbeschreibung	Eine kurze Zusammenfassung der Prüfung.
Beschreibung	Eine umfassendere Zusammenfassung der Prüfung.
Lösungsdetails	Geminderte potenzielle Security Incidents.
Dokumentations-URL	Links zur zugehörigen Dokumentation in der Produktdokumentation oder in Knowledge Base (KB)-Artikeln.
Ausführungsbedingung	Bedingungen, die den Start der Prüfungen auslösen.
Tabelle	Die Tabelle, zu der die Prüfung gehört.
Bedingungen	Bedingte Logik, die auf die Prüfungen angewendet wird.
Erweitert	Erweiterte Konfigurationsoptionen.

Planen Sie eine Scan-Suite neu

Ändern Sie den Zeitplan Ihrer Scan-Suites entsprechend Ihren Anforderungen.

Vorbereitungen
Erforderliche Rolle: administrator, sn_vsc.security_center_viewer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Sicherheitscenter**an.
2. In **Tools** Abschnitt auswählen **Sicherheitsscanner** .
3. Wählen Sie Aus **Suiten** Im Menü am linken Rand des Bildschirms.
4. Öffnen Sie die Suite, die Sie neu planen möchten.
5. Wählen Sie die Registerkarte **Zeitplan**.
6. Wählen Sie einen vorhandenen Zeitplan aus, oder wählen Sie aus **Neu** Um einen neuen Zeitplan zu erstellen.
7. In **Geplanter Scan** Füllen Sie die Felder nach Bedarf aus.

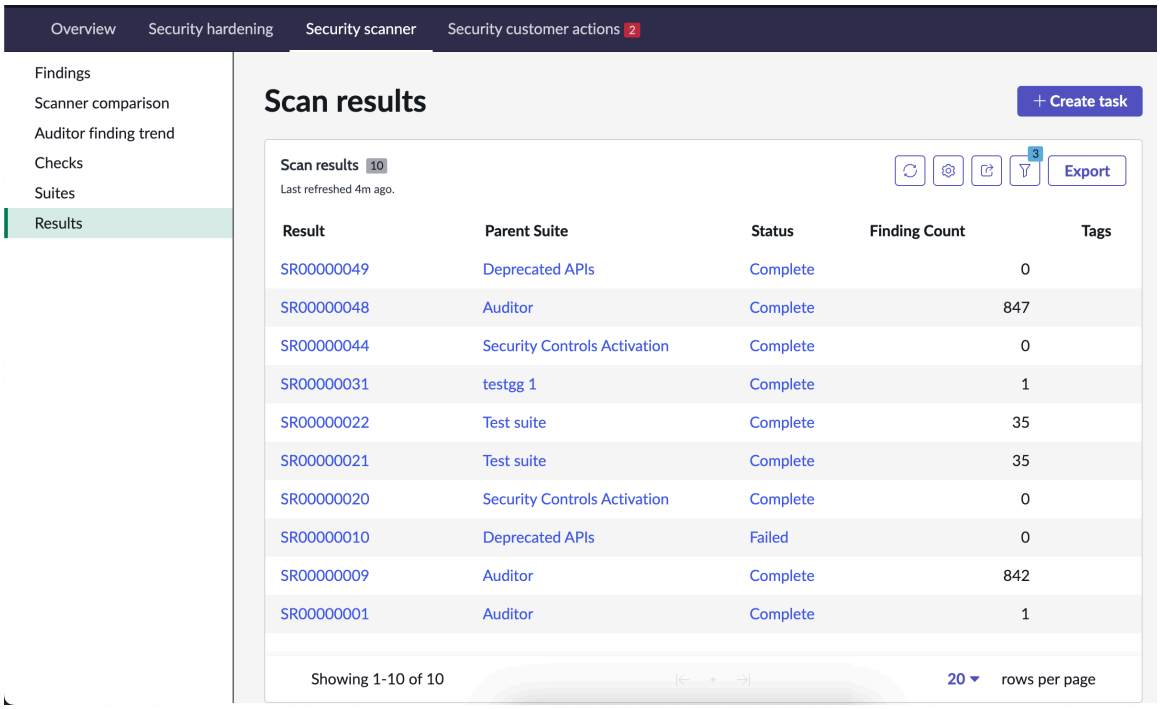
Feld	Beschreibung
Name	Name des Scan-Zeitplans
Ausführen	Wählen Sie aus, wie oft Ihre Suite ausgeführt werden soll. **Hinweis:** Zusätzliche Felder werden angezeigt, um Ihren Zeitplan zu definieren. Diese Felder variieren je nach Auswahl.
Aktiv	Gibt an, ob der Zeitplan aktiv ist. Inaktive Zeitpläne werden nie ausgeführt.
Bedingt	Auswählen, um zu aktivieren **Bedingung** Feld, in dem Sie eine geskriptete Bedingung für Ihren Zeitplan definieren können.
Bedingung	Eine geskriptete Bedingung für Ihren Zeitplan. Die Suite wird nur ausgeführt, wenn das Skript als ausgewertet wird `Wahr` .
Als ZZ ausführen	Welche Zeitzone der Zeitplan verwendet, wenn bestimmt wird, wann er ausgeführt werden soll.

Scan-Ergebnisse

Zeigen Sie Daten im Zusammenhang mit Ihren Scan-Ergebnissen in einer einzigen Ansicht an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ein Scan-Ergebnis meldet den Status und den Typ des Scans. Sie können auch alle Prüfungen anzeigen, die als Teil des Scans ausgeführt wurden, und alle anderen Informationen im Zusammenhang mit dem Scan, z. B. Fehler und Scanprotokolle.

Sie können Ihr Dashboard für Scan-Ergebnisse finden, indem Sie auswählen **Scanner** Registerkarte im Sicherheitscenter und dann auswählen **Ergebnisse** Im linken Bereich. Die Scan-Ergebnisse werden unter aufgeführt **Scan-Ergebnisse** Liste. Wählen Sie ein Ergebnis aus, um einen Drilldown durchzuführen und die Details anzuzeigen, die in Abschnitte mit Registerkarten unterteilt sind.

Details

Übersicht über die Scan-Ergebnisse, einschließlich Status, Typ und Ausführungszeit in Sekunden.

Scanfunde

Ergebnisse, die während der Ausführung der Prüfungen aufgetreten sind.

Suites

Zeigt die Suites an, die als Teil dieses Scans ausgeführt wurden.

Überprüfungen

Zeigt die Prüfungen an, die als Teil dieses Scans ausgeführt wurden.

Fehler

Zeigt die während des Scans fehlgeschlagenen Prüfungen und den Grund des Fehlers in Form einer Fehlermeldung an.

Scanprotokoll

Zeigt die Nachrichtenausgabe während des Scans an.

Scanstatistiken

Zeigt Statistiken im Zusammenhang mit dem Scan an.

Ziele

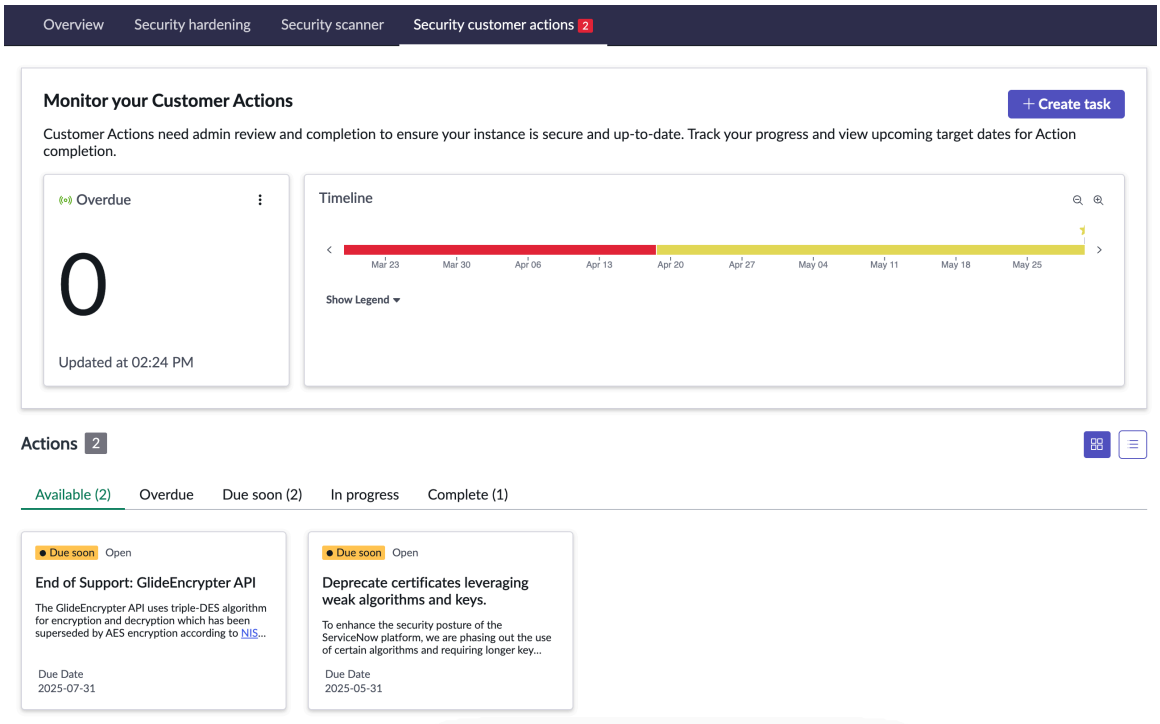
Zeigt alle Ziele an, für die die Prüfungen ausgeführt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kundenaktionen

Verwenden Sie das Kundenaktionen-Tool, um wichtige Sicherheitsupdates basierend auf Ihrer Instanz und der Konfiguration von Plugins zu implementieren.



Kundenaktionen sind empfohlene Changes für eine Instanz, die Ihnen helfen sollen, die Wichtigkeit sicherheitsbezogener Changes zu verstehen. Manuell implementierte Kundenaktionen unterscheiden sich von den automatischen Updates, die in Ihrer Instanz für den ServiceNow-Code oder die Funktionalität mit Familien-Releases oder Patches gerendert werden. Implementieren Sie Kundenaktionen, um Störungen bei der Anpassung Ihrer Instanz zu vermeiden.

Auf der Homepage „Kundenaktionen“ sehen Sie die Zeitleiste der Kundenaktionen, damit Sie priorisieren können, wann die Schritte implementiert werden sollen. Die Zeitleiste im obigen Beispiel zeigt die überfälligen Kundenaktionen und die bald fälligen Kundenaktionen. Darüber hinaus können Sie den Fortschritt Ihrer Kundenaktionen unter der Bezeichnung Updates nachverfolgen. Wählen Sie die Registerkarten aus, damit Sie die Kundenaktionen verfügbar, überfällig, bald fällig, in Bearbeitung oder Abgeschlossen sehen können.

Verwenden Sie **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe zum Abschließen einer Kundenaktion. Details finden Sie unter Sicherheitsaufgaben.

Erste Schritte:

- Greifen Sie auf dieses Tool zu, indem Sie zu navigieren **Kundenaktionen** Im Sicherheitscenter.
- Kundenaktionen sind in der Sicherheitscenter-App ab Washington DC enthalten.

Implementieren Sie Kundenaktionen

Erfahren Sie, wie Sie Kundenaktionen in Ihrer Instanz implementieren, um die Sicherheitslage zu erhöhen.

Vorbereitungen
Erforderliche Rolle: Administrator

Automatische Übersetzung

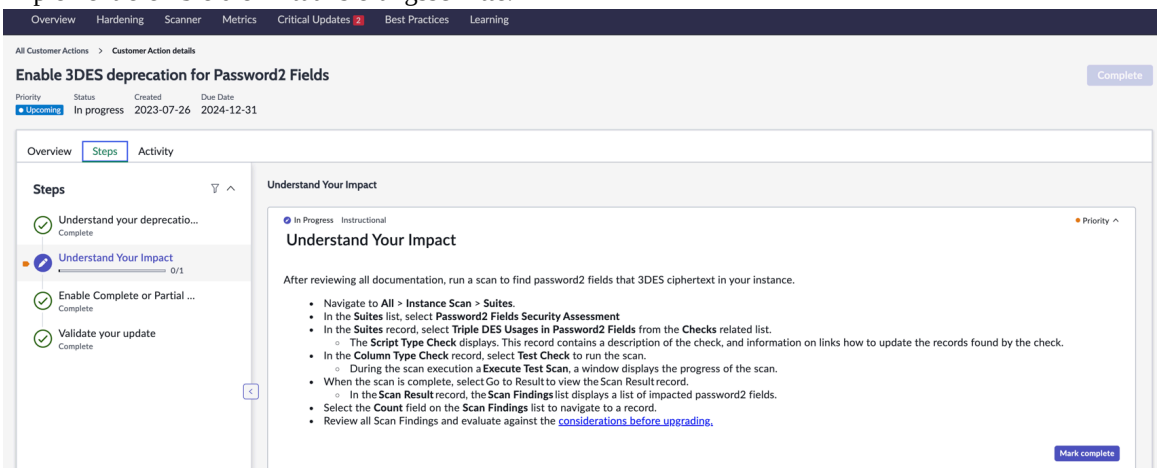
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Kundenaktionen bieten Ihnen Schritt-für-Schritt-Anweisungen, wie Sie die Änderungen in Ihrer Instanz implementieren, um Ihre Sicherheitslage zu erhöhen. Kundenaktionen ruft relevante Inhalte aus der Produktdokumentation ab, um Sie durch jeden Schritt des Implementierungsprozesses zu führen. Führen Sie die folgenden Schritte aus, um zu erfahren, wie Sie eine Kundenaktion implementieren.

Prozedur

1. Navigieren Sie zu **Kundenaktionen** App.
2. Wählen Sie eine zu implementierende Kundenaktion aus.
   Unter **Updates** Abschnitt enthält die Registerkarte verfügbar alle Kundenaktionen in Ihrer Instanz. Klicken Sie auf eine Kundenaktion unter dieser Registerkarte, um die Anweisungen anzuzeigen.
3. Lesen Sie die Übersicht, um zu erfahren, warum die Kundenaktion erforderlich ist, und um sich auf die Implementierung der Schritte vorzubereiten.
   Klicken Sie auf **Wechseln Sie zum nächsten Schritt** Um zu den Implementierungsdetails zu gelangen.
4. Implementieren Sie die Aktualisierungsschritte.



   a. Lesen Sie jede Gruppe von Anweisungen, und implementieren Sie sie in Ihrer Instanz.
   b. Klicken Sie Auf **Als abgeschlossen markieren** Wenn Sie mit einer Reihe von Anweisungen fertig sind.
   c. Wiederholen Sie die Schritte a–b, bis Sie alle Aktualisierungsschritte abgeschlossen haben.
   d. Klicken Sie auf **Abschließen**.
   Die Kundenaktion sollte in angezeigt werden **Abgeschlossen** Registerkarte.

Zeigen Sie Kundenaktionen An

Sehen Sie sich Details aller Aktivitäten im Zusammenhang mit an Ihr Kundenaktionen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

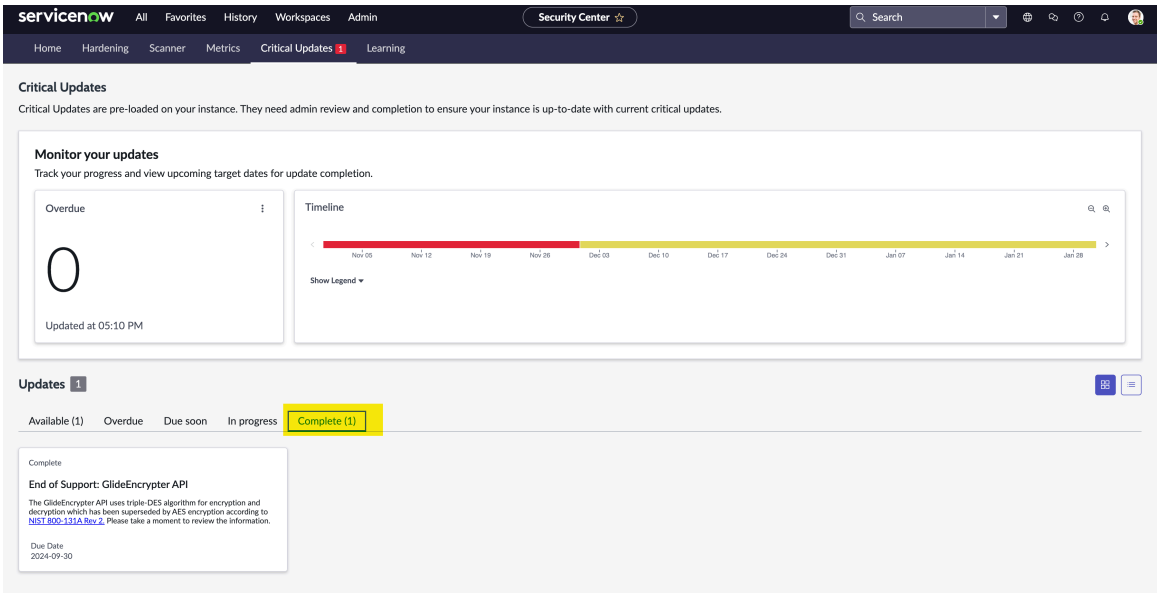
Die Aktivitäten werden von der neuesten zur ältesten aufgelistet, damit Sie zuerst die neueste Aktivität analysieren können. Jedes Update einer Aktivität wird mit einem Zeitstempel versehen, und Sie können es Verwenden Sie Suche und Filter Zum Abfragen bestimmter Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu **Kundenaktionen** App im Sicherheitscenter.
2. Navigieren Sie zu **Updates** Bezeichnung Von Kundenaktionen.
3. Klicken Sie auf einen Status, und wählen Sie dann eine Kundenaktion aus diesem Status aus.

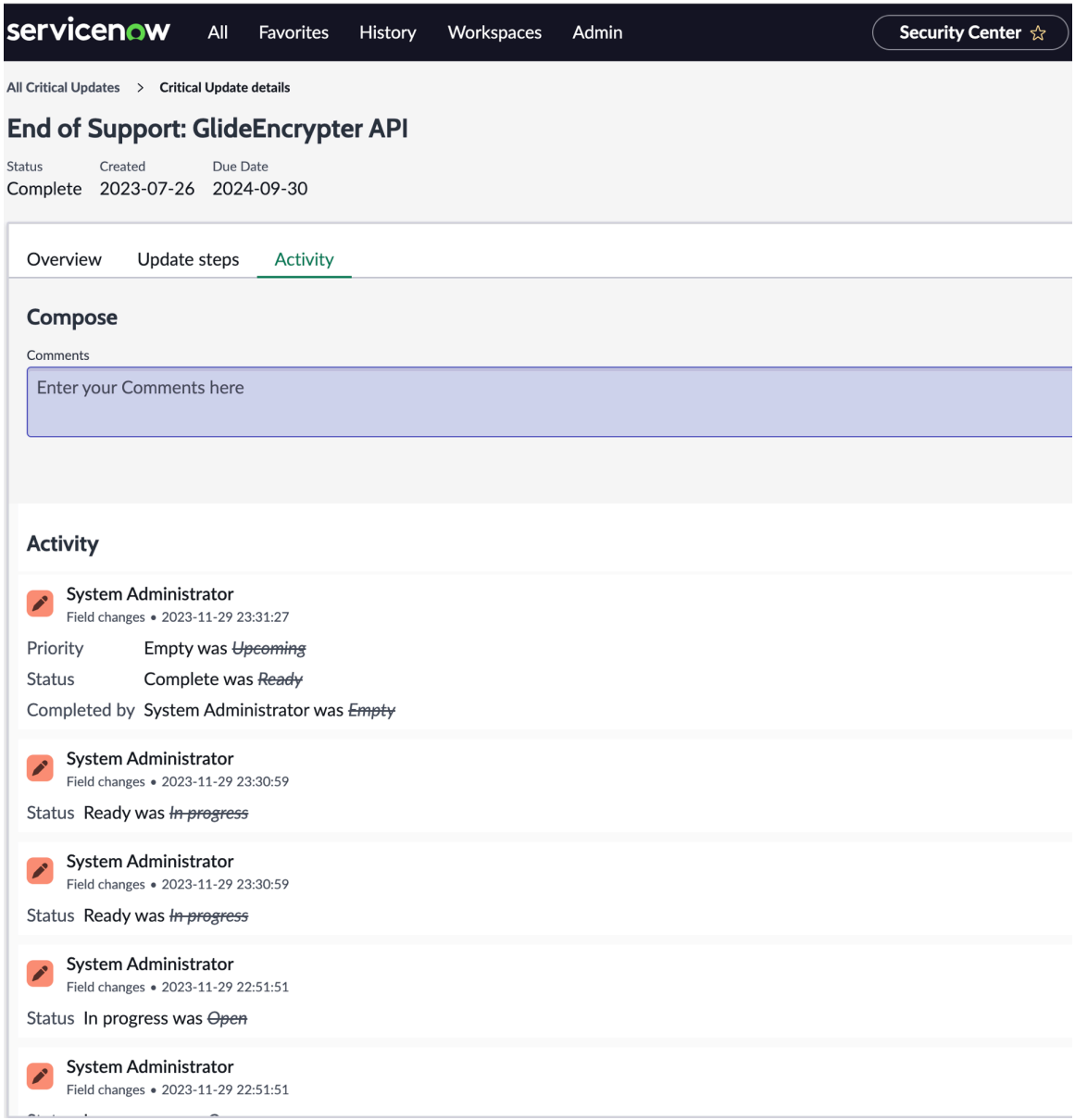
   Im folgenden Beispiel ist **Abgeschlossen** status wird ausgewählt, und dann die Kundenaktion für **Ende des Supports: GlideEncrypter-API** Ist ausgewählt.



4. Zeigen Sie die Aktivität Ihrer Kundenaktion an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

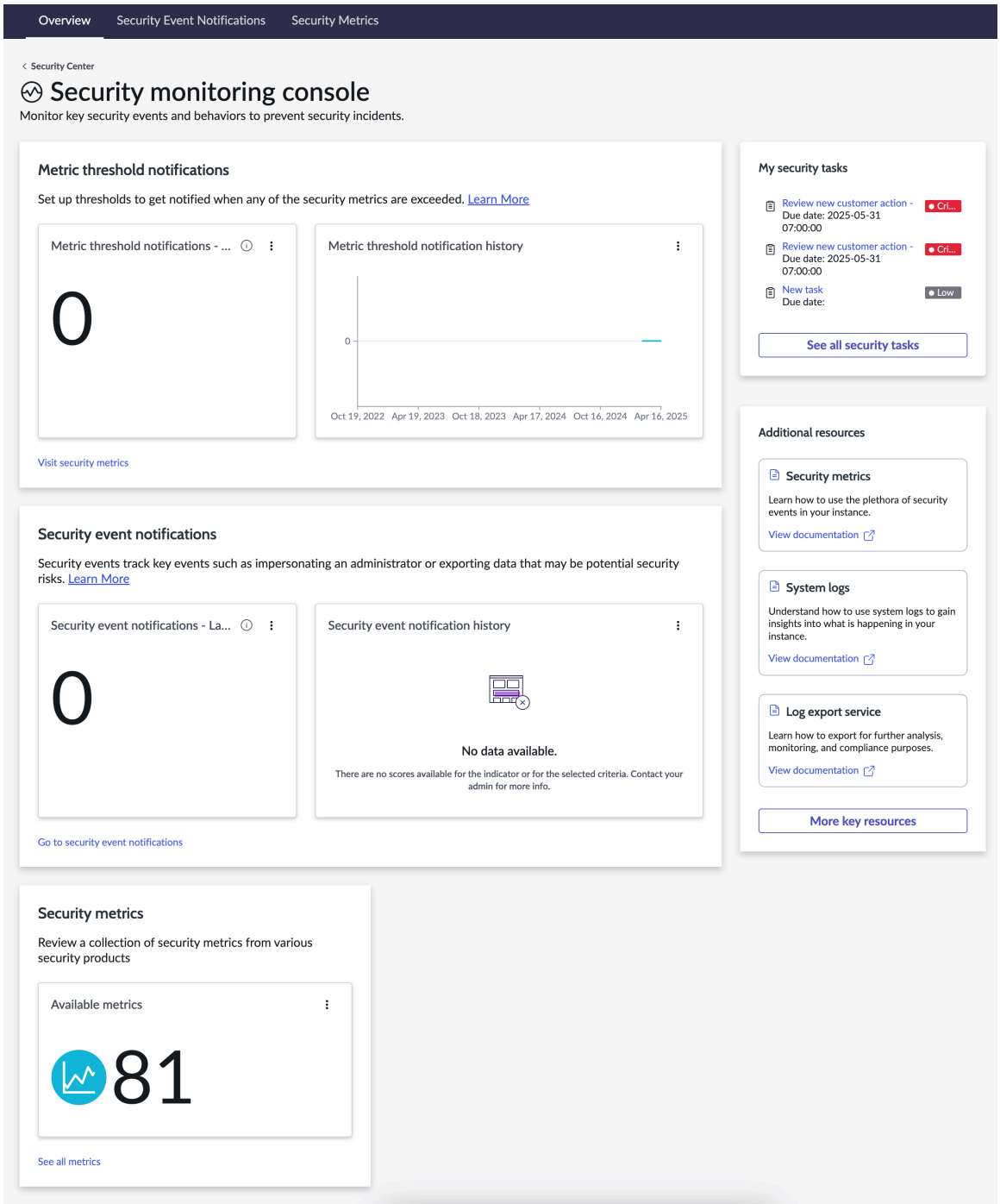


Alle Aktivitäten im Zusammenhang mit einer Kundenaktion werden automatisch aufgezeichnet. Darüber hinaus können Sie Aktivitäten zusätzliche Kommentare hinzufügen.

Sicherheitsüberwachungskonsole

Überwachen Sie Sicherheitsbenachrichtigungen und -Metriken, um über potenzielle Sicherheitsrisiken in Ihrer Instanz auf dem Laufenden zu bleiben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Sicherheitsüberwachungskonsole ist in Abschnitte unterteilt, jeweils mit Karten, die Informationen zu einem bestimmten Aspekt der Sicherheitsüberwachung enthalten. Wählen Sie die Informationen aus (ⓘ) Symbol auf einer beliebigen Karte, um Details zu den jeweiligen Darstellungen zu erhalten.

Navigationsleiste

Verwenden Sie die Leiste oben auf der Seite, um zwischen zu navigieren **Übersicht** , **Sicherheitsereignisbenachrichtigungen** , Und **Sicherheitsmetriken** Abschnitte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungen über Metrikschwellenwert

Erfahren Sie mehr über die Benachrichtigungen zu Metrikschwellenwerten in Ihrer Instanz im Benachrichtigungsbereich für Metrikschwellenwerte. Schwellenwerte definieren einen normalen Punktzahlbereich für einen Indikator und warnen Sie, wenn bestimmte Ereignisse auftreten, z. B. wenn eine Punktzahl ein Allzeithoch erreicht. In diesem Bereich wird die Anzahl der Schwellenwertbenachrichtigungen in den letzten sieben Tagen und ein Diagramm angezeigt, das die Anzahl der Schwellenwerte im Zeitverlauf anzeigt.

Wählen Sie eine der Karten aus, um die Registerkarte Sicherheitsmetriken zu öffnen, um weitere Details zu diesen Benachrichtigungen anzuzeigen.

Benachrichtigungen zu Sicherheitsereignissen

Verfolgen Sie Sicherheitsereignisse wie Identitätswechsel oder Datenexporte im Abschnitt „Sicherheitsereignisbenachrichtigungen“ nach. In diesem Bereich wird die Anzahl der Sicherheitsereignisse in den letzten sieben Tagen und ein Diagramm mit der Anzahl im Zeitverlauf angezeigt.

Wählen Sie eine der Karten aus, um die Registerkarte Sicherheitsmetriken zu öffnen, um weitere Details zu diesen Benachrichtigungen anzuzeigen.

Sicherheitsmetriken

In diesem Abschnitt wird eine Anzahl der verfügbaren Sicherheitsmetriken in Ihrer Instanz angezeigt. Überprüfen Sie eine Sammlung von Sicherheitsmetriken aus verschiedenen Sicherheitsprodukten.

Meine Sicherheitsaufgaben

Zeigen Sie die dringendsten Sicherheitsaufgaben an, die Ihnen zugewiesen sind. Wählen Sie eine Aufgabe aus, um ihre Details anzuzeigen, oder wählen Sie aus **Alle Sicherheitsaufgaben anzeigen** Zum Anzeigen einer vollständigen Liste von Sicherheitsaufgaben. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Zusätzliche Ressourcen

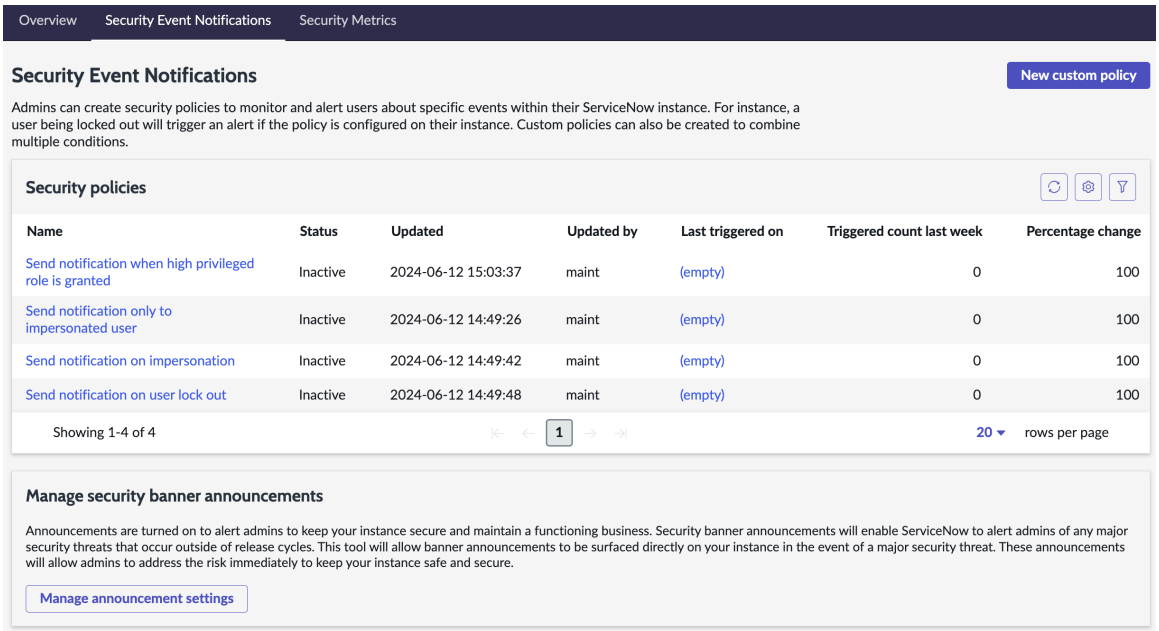
Verwenden Sie den Abschnitt „zusätzliche Ressourcen“ am Rand des Bildschirms, um zu Dokumentationen und Videos zu navigieren, die für das Lernen des Sicherheitszentrums relevant sind, sowie zu Informationen zur Verwaltung der Instanzsicherheit.

Benachrichtigungen zu Sicherheitsereignissen

Zeigen Sie die standardmäßigen Richtlinien für Benachrichtigungen zu Sicherheitsereignissen in Ihrer ServiceNow-Instanz an, verwalten und analysieren Sie sie, und greifen Sie auf die Funktionalität zum Erstellen anwenderdefinierter Richtlinien zu.

Greifen Sie über die Security Center-Homepage auf Sicherheitsereignisbenachrichtigungen zu, indem Sie öffnen **Sicherheitsüberwachungskonsole** In **Sicherheitskonsolen** Abschnitt, und wählen Sie dann aus **Sicherheitsereignisbenachrichtigungen** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Passen Sie Benachrichtigungsrichtlinien an, die E-Mail-Benachrichtigungen auslösen, wenn Anwender Aktionen in ausführen ServiceNow AI Platform Die möglicherweise unsicher sind oder eine Administratorüberwachung erfordern.

Administratoren können die Werte für die Standardrichtlinien anpassen, klonen und Standardrichtlinien bearbeiten oder eigene anwenderdefinierte Richtlinien erstellen.

Sicherheitsrichtlinien

Die Konsole „Benachrichtigungen zu Sicherheitsereignissen“ zeigt wichtige Informationen zu den Sicherheitsrichtlinien in Ihrer Instanz an. Diese Tabelle enthält Spalten, die Folgendes anzeigen:

Bezeichnung	Beschreibung
Name	Der Name der Benachrichtigungsrichtlinie für Sicherheitsereignisse.
Status	Der Status einer Richtlinie kann entweder aktiv oder inaktiv sein.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Richtlinie.
Aktualisiert von	Der Anwender, der eine Richtlinie aktualisiert hat.
Zuletzt ausgelöst am	Datum und Uhrzeit der letzten Ausführung der Richtlinie.
Ausgelöst-Anzahl letzte Woche	Die Anzahl der Auslöser, die eine Richtlinie in den letzten 7 Tagen generiert hat.
Änderung in Prozent	Die Change-Rate für wöchentliche Auslöser, berechnet als Prozentsatz. **Hinweis:** Wenn diese Richtlinie beispielsweise durchschnittlich 5 Benachrichtigungen pro Woche auslöst und sie letzte Woche 10 Mal ausgelöst hat, wäre dies ein prozentualer Anstieg um 100 %.

Wählen Sie eine Richtlinie in der Tabelle aus, um weitere Details anzuzeigen, einschließlich Übersicht, Einstellungen und Benachrichtigungsverlauf. Wählen Sie aus **Neue**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

anwenderdefinierte Richtlinie Schaltfläche zum Erstellen einer anwenderdefinierten Richtlinie, die auf die Anwendungsfälle Ihrer Organisation zugeschnitten ist.

Sicherheitsbanner-Mitteilungen verwalten

Wählen Sie Aus **Verwalten Sie Ankündigungseinstellungen** Dient zur Steuerung, ob Administratoren Bannerbenachrichtigungen auf dieser Instanz erhalten. Informationen zu diesen Ankündigungen finden Sie unter Sicherheitsbanner-Ankündigungen.

Create custom security event notification policies

Learn how to create custom security event notifications that are specific to your organization's needs. This enables you to monitor actions taken by users and groups on your instance and generate notifications for potential security risks.

Vorbereitungen

Role required: admin

Prozedur

1. Navigate to the Security Center app and select **Notifications**.
2. Select **New custom policy**.
3. Select one of the three event types that will trigger the start of the policy, and select **Create**.
4. Configure the policy.
   See Konfigurieren Sie Einstellungen für Richtlinien zur Benachrichtigung von Sicherheitsereignissen to learn how to configure your new custom security event notification policy.

Ändern Sie Richtlinien für Benachrichtigungen zu Sicherheitsereignissen

Erfahren Sie, wie Sie die Einstellungen Ihrer Richtlinien für Benachrichtigungen zu Sicherheitsereignissen ändern können.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie zum Sicherheitsereignis **Benachrichtigung** Homepage und wählen Sie eine der Richtlinien aus, die Sie ändern möchten.

   Hinweis: Sie können die Auslöser- oder Bedingungslogik für Standardrichtlinien nicht ändern. Um diese Einstellungen zu ändern, müssen Sie zuerst die Richtlinie duplizieren. Dazu wählen Sie den Abwärtspfeil neben **Aktualisieren** , Und dann auswählen **Duplikat** .

2. Wählen Sie Aus **Richtlinieneinstellungen** Zum Ändern der Einstellungen.
3. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.
4. **Wahlweise:** Wählen Sie Aus **Deaktivieren** Bis Sie bereit sind, mit dem Auslösen von Benachrichtigungen zu beginnen.
5. **Wahlweise:** Starten Sie das Auslösen von Benachrichtigungen, indem Sie auswählen **Aktivieren** .
   Siehe Konfigurieren Sie Einstellungen für Richtlinien zur Benachrichtigung von Sicherheitsereignissen Um zu erfahren, wie Sie Ihre neue anwenderdefinierte Benachrichtigungsrichtlinie für Sicherheitsereignisse konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Einstellungen für Richtlinien zur Benachrichtigung von Sicherheitsereignissen

Erfahren Sie, wie Sie Richtlinien für Benachrichtigungen zu Sicherheitsereignissen in anpassen können Security Center Um den spezifischen Anforderungen Ihrer Organisation gerecht zu werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die **Richtlinieneinstellungen** Auf der Seite können Sie die Einstellungen für eine Benachrichtigungsrichtlinie für Sicherheitsereignisse anpassen. Hier können Sie Optionen für die Ausführung der Richtlinie, die bedingte Logik und die gesendeten Benachrichtigungen anpassen.

Prozedur

1. Wählen Sie im Sicherheitscenter die Option aus **Benachrichtigungen** .
2. Wählen Sie in der Tabelle „Sicherheitsrichtlinien“ eine Benachrichtigungsrichtlinie für Sicherheitsereignisse aus, die Sie konfigurieren möchten.
   Beispiel: **Benachrichtigung senden, wenn eine Rolle mit hohen Berechtigungen gewährt wird** .
3. Wählen Sie Aus **Richtlinieneinstellungen** .
4. Konfigurieren Sie die Richtlinieneinstellungen.

Konfigurationsoptionen für Richtlinieneinstellungen

Bezeichnung	Zu konfigurierende Elemente
Zeitpunkt für Ausführung	**Auslöser** : Das Ereignis, das die Richtlinie startet.
Bedingungen	Die bedingte Logik und Bedingungen, die auf Ihre Richtlinien angewendet werden sollen. ○ **Bedingungslogik** : Zwei Optionen ▪ **Alle Bedingungen müssen erfüllt sein, um diese Richtlinie auszulösen** : Alle Bedingungen müssen gültig sein, damit die Richtlinie Benachrichtigungen senden kann. ▪ **Eine der Bedingungen muss erfüllt sein, um diese Richtlinie auszulösen** : Benachrichtigungen werden gesendet, wenn eine der Bedingungen gültig ist. ○ **Bedingung Hinzufügen** : Wählen Sie Bedingung hinzufügen aus, und geben Sie die entsprechenden Werte dafür an. Sie können eine Bedingung entfernen, indem Sie auswählen **Bedingung entfernen** .
Benachrichtigungen	Der E-Mail-Text und die E-Mail-Empfänger:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Zu konfigurierende Elemente
	○ **Benachrichtigung** : Wählen Sie eine der vordefinierten Benachrichtigungsvorlagen aus. Weitere Informationen finden Sie unter Erstellen Sie eine anwenderdefinierte E-Mail für Benachrichtigungen zu Sicherheitsereignissen. ○ **Fügen Sie Eine Benachrichtigung Hinzu** : Wählen Sie Benachrichtigung Hinzufügen. ○ **Gruppen** : Wählen Sie die Gruppe aus, die die Benachrichtigung erhalten soll. ○ **Anwender** : Wählen Sie die Anwender aus, die die Benachrichtigung erhalten sollen. Sie können eine Benachrichtigung entfernen, indem Sie auswählen **Entfernen Sie die Benachrichtigung** .

Hinweis: Wenn Sie eine Richtlinie deaktivieren möchten, wählen Sie aus **Deaktivieren** . Wenn Sie eine Richtlinie replizieren möchten, wählen Sie den Abwärtspfeil neben **Aktualisieren** (

) Schaltfläche.

5. Wählen Sie Aus **Aktualisieren** Um Ihre Einstellungen zu speichern.

Erstellen Sie eine anwenderdefinierte E-Mail für Benachrichtigungen zu Sicherheitsereignissen

Erfahren Sie, wie Sie eine anwenderdefinierte E-Mail für Sicherheitsereignisbenachrichtigungen erstellen, indem Sie neue Benachrichtigungen konfigurieren, Auslöser festlegen, Empfänger definieren und E-Mail-Inhalte mit dynamischen Ereignisfeldern erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Auswahlvorgang **Systembenachrichtigungen** > **Benachrichtigung**an.
2. Wählen Sie Aus **Neu** .
3. Geben Sie ein **Name** Für das Benachrichtigungsfeld.
4. Wählen Sie das Feld neben aus **Tabelle** Und geben Sie die Sicherheitsrichtlinienbenachrichtigung ein (`sn_vsc_Security_Policy`).
5. Konfigurieren Sie den neuen Datensatz.
   Der Datensatz enthält drei Registerkarten, die konfiguriert werden müssen: **Zeitpunkt des Sendens** , **Wer erhält** , Und **Inhalt** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte	Beschreibung
Absendezeitpunkt	Wählen Sie das Feld neben aus **Senden, wenn** Bezeichnung und wählen Sie aus **Ausgelöst** .
Empfänger	○ Wählen Sie das lokale Symbol neben aus **Anwender/Gruppen in Feldern** , Und wählen Sie beide aus **Anwender** Und **Gruppen** . Wählen Sie aus **Element Hinzufügen** Symbol (>) zum Verschieben der Felder in **Ausgewählt** Textfeld. ○ Klicken Sie mit der rechten Maustaste auf das Header-Banner des Datensatzes, und wählen Sie aus **Speichern** .)

Darin enthalten	Erstellen Sie eine E-Mail-Vorlage.
	Weitere Informationen finden Sie unter Erstellen einer E-Mail-Vorlage .
	Geben Sie Felder des Ereignisses in ein **Nachrichten-HTML** . Dies kann mithilfe von erfolgen `${event_id.FIELD_NAME}` . Hier ist ein Beispiel:
	`Role: ${event_id.role.URI_REF}`
	`Granted to: ${event_id.granted_to.URI_REF}`
	`Granted by: ${event_id.user.URI_REF}`
	`Logged at: ${event_id.sys_created_on}`
	`Security Center Notification: ${execution.policy.name}`

6. Wählen Sie **Absenden**.
7. Fügen Sie der E-Mail-Vorlage in Sicherheitsereignisbenachrichtigungen eine anwenderdefinierte Benachrichtigung hinzu.
   a. Wählen Sie im Sicherheitscenter die Option aus **Benachrichtigungen** > **Richtlinieneinstellungen**an.
   b. Navigieren Sie zu **Benachrichtigungen** Bezeichnung.
   c. Geben Sie den Namen der anwenderdefinierten Benachrichtigung ein, die Sie in erstellt haben **Benachrichtigung** Feld.

Verlauf der Sicherheitsereignisbenachrichtigungen

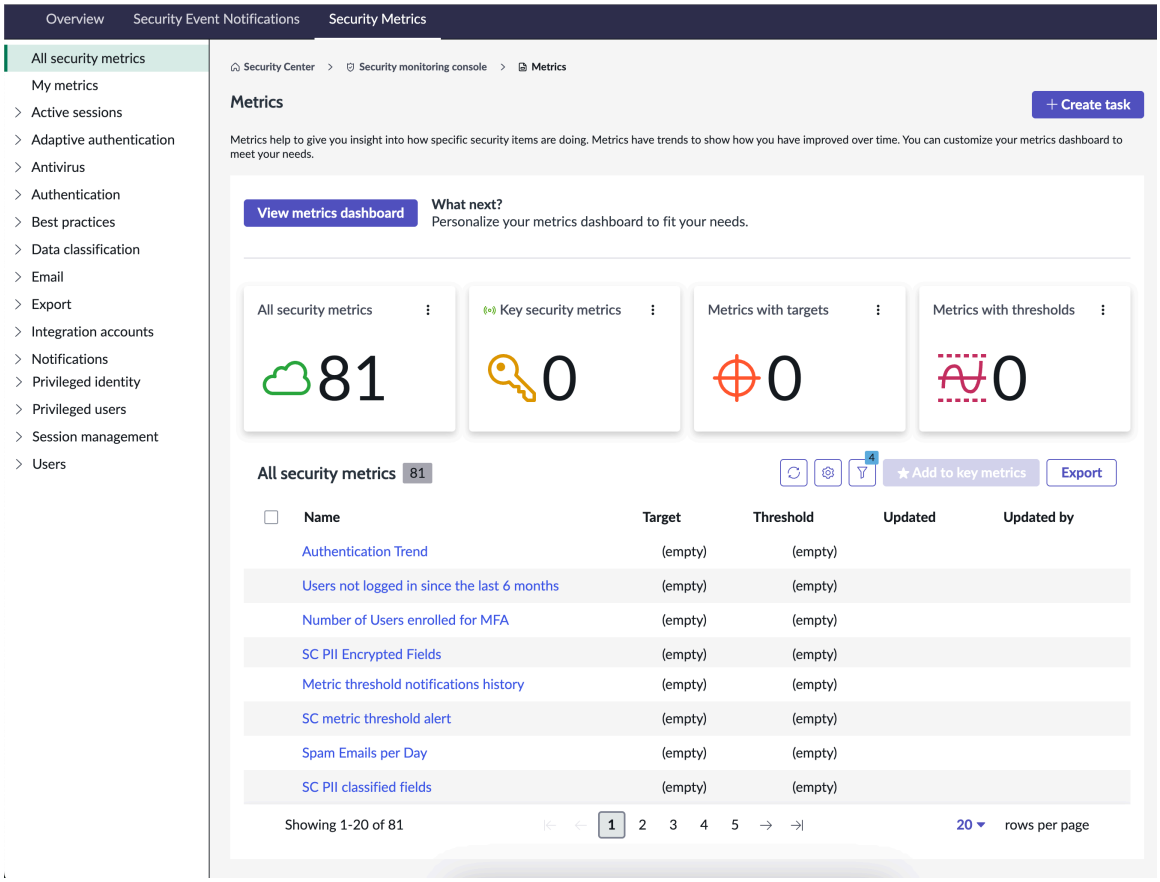
Erkunden Sie den vollständigen Verlauf der Benachrichtigungen zu Sicherheitsereignissen in Ihrer Instanz.

Die **Benachrichtigungen** Die Seite bietet einen Überblick über den Benachrichtigungsverlauf für alle Benachrichtigungsrichtlinien für Sicherheitsereignisse in Ihrer Instanz. Sie können die Daten in Diagrammen anzeigen, sie grafisch darstellen und Performance Analytics-Funktionen wie Ziele, Schwellenwerte und KPI-Signale anwenden. Alternativ können Sie die Daten in einem Tabellenformat anzeigen, sodass Sie Standardfunktionen wie Suchen, Sortieren, Filtern und Abfragen verwenden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsmetriken

Überwachen Sie über 50 verschiedene Sicherheitsmetriken, um potenzielle Sicherheitsbedrohungen oder unsicheres Verhalten zu identifizieren. Legen Sie Schwellenwerte für E-Mail-Benachrichtigungen fest, visualisieren und analysieren Sie die Daten auf mehrere Arten. Exportieren Sie die Daten, oder erstellen Sie Dashboards mit den Metriken, die für Ihre Organisation am wichtigsten sind.



Greifen Sie auf Sicherheitsmetriken im Sicherheitscenter zu, indem Sie auswählen **Sicherheitsüberwachung** Im Abschnitt „Tools“. Wählen Sie dann aus **Sicherheitsmetriken** Karte.

Dashboard „alle Sicherheitsmetriken“

Mit diesem Dashboard können Sie Metriken wie fehlgeschlagene Anmeldungen, Exporte, Identitätswechsel usw. anzeigen. Die Karten über der Liste geben eine Anzahl der Metriken an, die bestimmten auf der Karte aufgeführten Kriterien entsprechen. Wählen Sie eine dieser Karten aus, um die Liste so zu filtern, dass nur die Metriken angezeigt werden, die den Kriterien entsprechen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Dashboard „meine Metriken“

Dies ist ein anpassbares Dashboard, das Informationen zu Metriken anzeigt, die Ihnen am meisten wichtig sind. Wählen Sie Aus **Bearbeiten** Zum Anpassen Ihres Dashboards durch Hinzufügen von Visualisierungen, Filtern, Überschriften, Bildern, Rich-Text, und Listen.

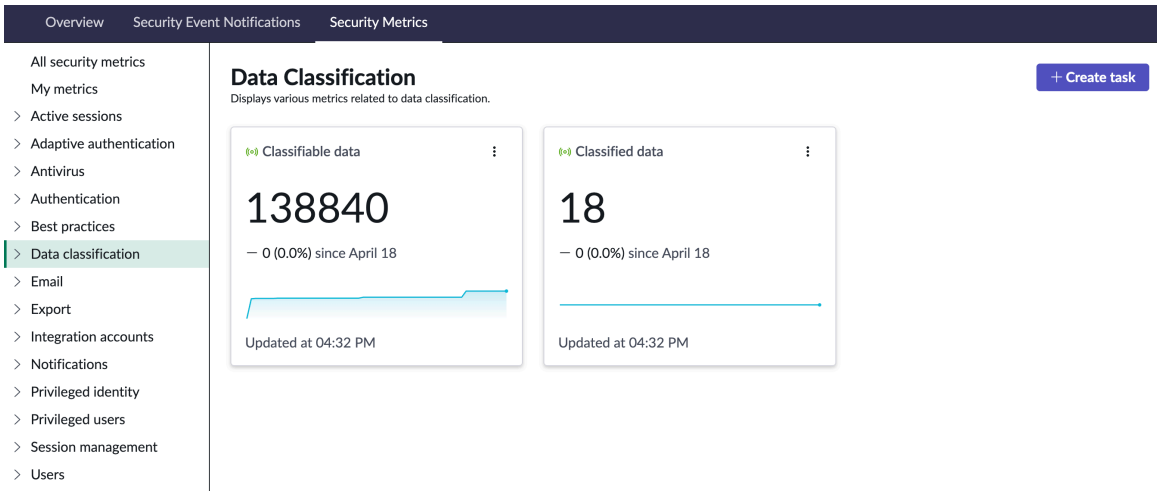
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zu den verschiedenen Möglichkeiten zum Anpassen Ihres Dashboards finden Sie unter Dashboards in Platform Analytics .

Metriken-Navigationsbereich

Im Navigationsbereich am Rand des Bildschirms werden Ihre Instanzmetriken angezeigt. Wählen Sie Aus **Alle Sicherheitsmetriken** Zum Anzeigen aller Metriken in einer einzelnen Liste. Wählen Sie eines der Elemente unter aus **Alle Sicherheitsmetriken** Der Eintrag zum Durchsuchen der Metriken, organisiert nach Kategorie.

Jede Kategorie zeigt ein Dashboard an, das der Sicherheit ähnelt **Dashboard „meine Metriken“** , Mit Karten für die Metriken in dieser Kategorie.



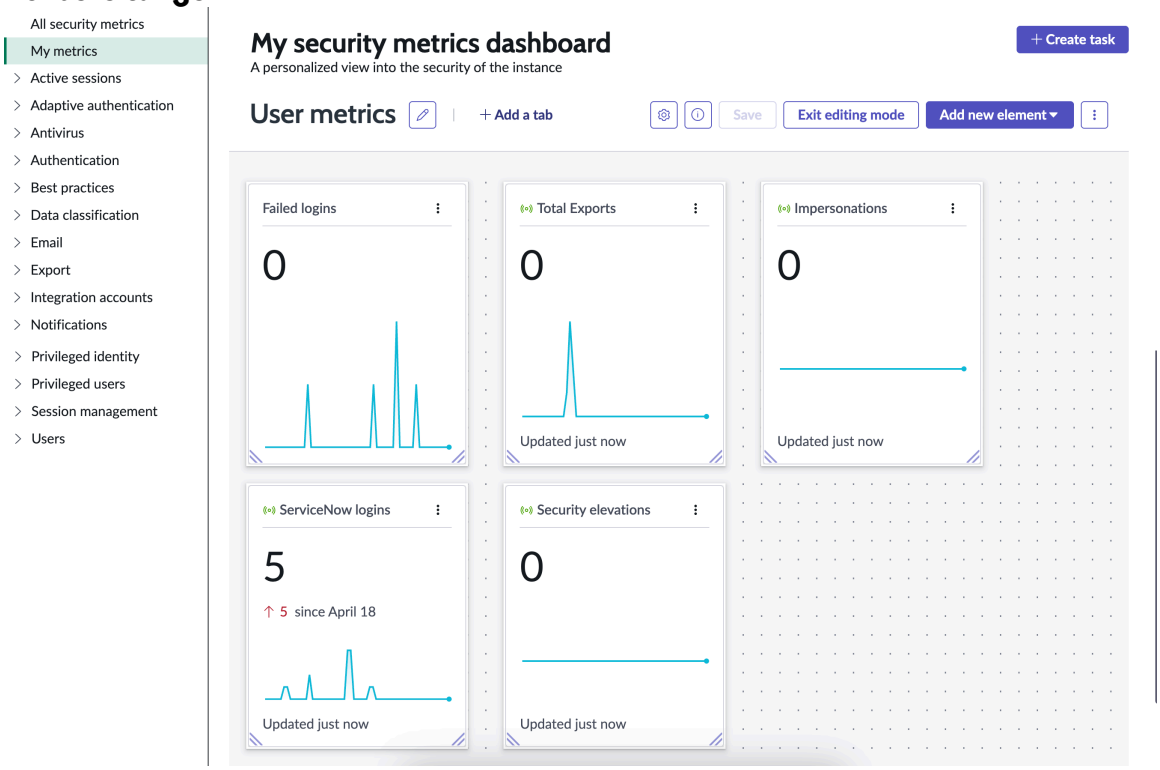
Passen Sie das Dashboard „meine Sicherheitsmetriken“ an

Entdecken Sie die Flexibilität des Dashboards „meine Sicherheitsmetriken“, das mit Metriken aus verschiedenen Quellen wie Diagrammen und Diagrammen angepasst werden kann. Passen Sie das Dashboard an die spezifischen Anforderungen Ihrer Organisation an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen



Um das Dashboard „Sicherheitsmetriken“ anzupassen, bestätigen Sie, dass Sie sich innerhalb des Anwendungsbereichs „Security Center“ befinden. Um zu diesem Bereich zu wechseln, wählen Sie aus **Anwendungsauswahl** > **Anwendungsbereich**, Und geben Sie das Sicherheitscenter ein.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Implementieren und passen Sie das Dashboard „meine Sicherheitsmetriken“ an. Fügen Sie Ihrem Dashboard Metriken und Inhalte aus einer Vielzahl von Quellen hinzu, z. B. aus Diagrammen und Diagrammen, die aus einem Bericht generiert wurden. Erfahren Sie, welche Schritte erforderlich sind, um Ihrem Dashboard eine Registerkarte hinzuzufügen, damit Sie sie an die Anforderungen Ihrer Organisation anpassen können.

Prozedur

1. Greifen Sie auf Sicherheitsmetriken im Sicherheitscenter zu, indem Sie auswählen **Sicherheitsüberwachung** Wählen Sie im Abschnitt „Tools“ aus, und wählen Sie aus **Sicherheitsmetriken** Karte.
2. Wechseln Sie in den Bearbeitungsmodus, indem Sie auswählen **Bearbeiten** .
3. Erstellen Sie eine Registerkarte, indem Sie auswählen **+Registerkarte hinzufügen** .

   Hinweis: Sie können auch eine neue Registerkarte hinzufügen, indem Sie auswählen **Plus (+)** Symbol neben einer vorhandenen Registerkarte.

4. Bearbeiten Sie den Titel Ihrer neu erstellten Registerkarte, indem Sie das Bleistiftsymbol auswählen und einen Namen eingeben.
5. Fügen Sie Ihrer Registerkarte ein Element hinzu, indem Sie auswählen **Fügen Sie ein neues Element hinzu** .
6. Wählen Sie **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. **Wahlweise:** Um das Dashboard für Anwender, Gruppen und Rollen in Ihrer Organisation freizugeben, wählen Sie aus **Menü „Weitere Aktionen“** > **Freigeben**an.

   a. Geben Sie den Namen eines Anwenders ein, für den Zugriff gewährt werden soll.

   b. Wählen Sie **Bestätigen** aus.

Konfigurieren Sie Sicherheitsmetriken, um E-Mails zu senden, wenn Schwellenwerte ausgelöst werden

Erfahren Sie, wie Sie Sicherheitsmetriken konfigurieren, damit Ihre Instanz eine E-Mail-Benachrichtigung generiert, wenn ein Schwellenwert ausgelöst wird.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie im Sicherheitscenter zu **Metriken** .
2. Wählen Sie eine Metrik aus, für die Sie in Ihrer Organisation einen Schwellenwert festlegen möchten.

   Example

   Um fehlgeschlagene Anmeldungen zu verwalten, können Sie einen Schwellenwert festlegen. Wenn die Anzahl der fehlgeschlagenen Anmeldungen diesen Schwellenwert erreicht, werden Administratoren oder Sicherheitsexperten in Ihrer Organisation benachrichtigt. Die entsprechende Sicherheitsmetrik, die in diesem Fall angestrebt werden soll, ist **users** > **Fehlgeschlagene Anmeldungen**an.
3. Wählen Sie aus **Schwellenwerte** Symbol.
4. Wählen Sie aus **Plus (+)** Symbol im Schwellenwertbereich zum Konfigurieren des Formulars.
   Die verfügbaren Optionen sind zum Festlegen der Sichtbarkeit, des Schwellenwerttyps und des Schwellenwerts.

   a. Wählen Sie für Sichtbarkeit aus **Für alle** Wenn alle die Benachrichtigung erhalten sollen, oder **Für mich** Wenn Sie nur eine Benachrichtigung erhalten möchten.

   b. In **Schwellenwerttyp** , Wählen Sie aus **Allzeithoch** .
   Dieses Feld löst die Schwellenwertbenachrichtigung aus.

   > **Hinweis:** Ein Schwellenwert darf nur eingegeben werden, wenn der **Schwellenwerttyp** Ist auf festgelegt **Kleiner als** Oder **Mehr als** .
5. Wählen Sie Aus **Speichern** Zum Erstellen des Schwellenwerts.
   Als Nächstes muss die Benachrichtigung eingerichtet werden.
6. Wählen Sie Aus **Alle** , Und Eingabetaste **Systembenachrichtigung** .
7. Navigieren zu **E-Mail** > **Benachrichtigungen**an.
8. In **Name** Spalte eingeben `*PA thre` .
   Die Schwellenwertbenachrichtigungen sind ereignisbasiert und werden in der Tabelle „PA-Schwellenwertbenachrichtigung“ eingerichtet.
9. Wählen Sie **PA Schwellenwert-Benachrichtigung** aus.
   Die Ergebnisse enthalten drei Registerkarten:

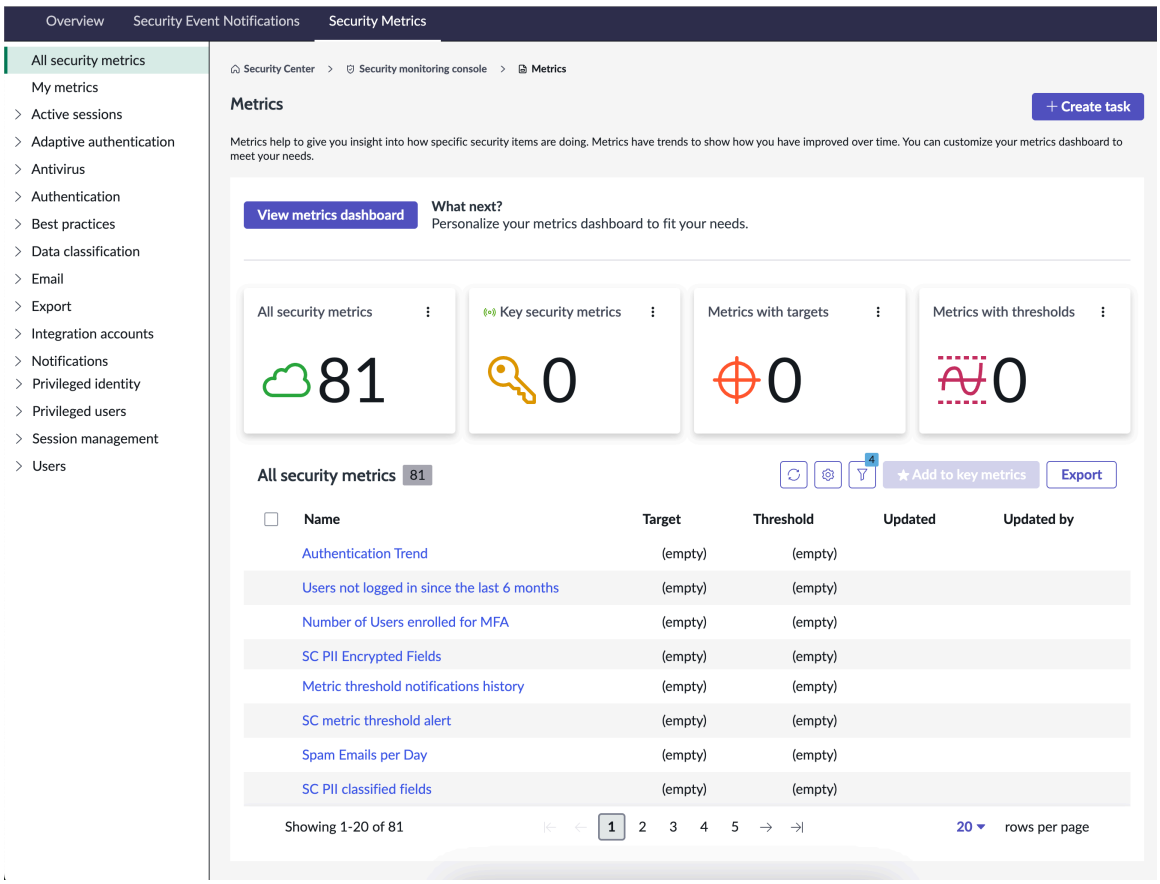
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wann gesendet werden soll: Gibt an, was geschehen muss, um die E-Mail-Benachrichtigung zu senden. In diesem Beispiel wird die E-Mail ausgelöst, sobald der zuvor von Ihnen festgelegte Schwellenwert erreicht ist.
- Empfänger: Gibt an, welche Anwender die Benachrichtigung erhalten. Sie können Anwender und Gruppen hinzufügen.
- Inhalt: Gibt die Skriptaktion an, die ein Anwender ändern kann, um die Nachricht anzupassen, die Anwender und die Gruppe erhalten. Weitere Informationen zum Erstellen von Skriptaktionen finden Sie unter Skriptaktionen .

Alle Sicherheitsmetriken

Navigieren Sie zu **Alle Sicherheitsmetriken** Zum Anzeigen einer Tabelle mit den Daten im Zusammenhang mit den Sicherheitsmetriken Ihrer Instanz.

Greifen Sie auf die Liste aller Sicherheitsmetriken in einer filterbaren Liste zu, indem Sie auf das Dashboard „Sicherheitsmetriken“ zugreifen und auswählen **Alle Sicherheitsmetriken** Option auf aus der Liste auf der linken Seite.



Wählen Sie ein beliebiges Element in der Liste aus, um Details zu jeder Metrik anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Aktive Sitzungen

Zeigen Sie die Trendlinie der aktiven Anwender in an ServiceNow AI Platform.

Auf dieser Seite werden Karten mit Informationen zu Metriken im Zusammenhang mit aktiven Sitzungen angezeigt. Jede Karte zeigt eine Trendlinie für die folgenden Metriken an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwendersitzungen: Metriken im Zusammenhang mit aktiven Anwendersitzungen in Ihrer Instanz.
- Sitzungen privilegierter Anwender: Metriken im Zusammenhang mit privilegierten Anwendern oder denen, denen zusätzliche Rollen zugewiesen wurden.

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Sicherheitsmetriken der adaptiven Authentifizierung

Verwenden Sie Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten und den Zugriff auf Ihre Instanz basierend auf den angegebenen Richtlinienbedingungen zu verweigern oder zuzulassen.

Mit Metriken der adaptiven Authentifizierung können Sie überwachen, wie die adaptive Authentifizierung in Ihrer Instanz verwendet wird. Zeigen Sie eine Zusammenfassung aller Ihrer Metriken zur adaptiven Authentifizierung an, einzelne Metriken wie Richtlinienergebnisraten oder abgelehnte IP-Adressen. Diese Seite erfordert die adaptive Authentifizierung (`com.snc.adaptive_authentication`) Plugin, damit die adaptive Authentifizierung in Ihrer Instanz verfügbar ist. Sie müssen die Authentifizierungsrichtlinie aktivieren, um die Metriken anzuzeigen. Siehe Aktivieren Adaptive Authentifizierung Und Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung Für weitere Details.

Hinweis: Diese Funktion wurde mit Version 1,2 veröffentlicht.

- Richtlinienergebnisraten: Alle erfolgreichen und fehlgeschlagenen Ereignisse der adaptiven Authentifizierung.
- Ereignisfehlerverteilung: Alle fehlgeschlagenen Ereignisse für jeden Ereignistyp.
- Ereigniserfolgsverteilung: Die erfolgreichen Ereignisse, die jedem Ereignistyp zugeordnet sind.
- Abgelehnte IP-Adressen: Die Anzahl der von der Instanz blockierten IP-Adressen zusammen mit den zugehörigen Daten.
- Authentifizierte Anwenderanmeldungen: Die Anzahl der Ereignisse, die für jeden Ereignistyp gezählt werden, mit Ausnahme des Ereignisses vor der Anmeldung.
- API-Anwenderanmeldungen: Die Anzahl der Ereignisse, die API-Authentifizierungsrichtlinien für jeden Ereignistyp zugeordnet sind.
- Authentifizierungstrend: Die Gesamtzahl der aufgezeichneten Ereignisse.
- Authentifizierte Anwender: Die Anzahl der Anwender, die für jeden Ereignistyp gezählt werden, mit Ausnahme des Ereignisses vor der Anmeldung.

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virenschutz

Zeigt den Trend an, wann Ereignisse für potenziell infizierte Dateien auftreten. Sehen Sie, wann sie erkannt, in Quarantäne gestellt, wiederhergestellt oder gelöscht werden.

Auf dieser Seite werden Karten mit Informationen zu Metriken im Zusammenhang mit Virenschutzaktivitäten in Ihrer Instanz angezeigt. Jede Karte zeigt eine Trendlinie für die folgenden Metriken an:

- Dateien in Quarantäne: Die Anzahl der Dateien, die potenziell Malware enthalten.
- Heruntergeladene Dateien: Die Anzahl der heruntergeladenen Dateien.
- Wiederhergestellte Dateien: Die Anzahl der Dateien, die wiederhergestellt wurden.
- Gelöschte Dateien: Die Anzahl der gelöschten Dateien.

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Authentifizierung

Zeigen Sie Trends für Metriken im Zusammenhang mit Authentifizierungsschemata an, z. B. Verwendung der Multifaktor-Authentifizierung (MFA), Webservice-Accounts und Nutzung biometrischer Scanner.

Auf dieser Seite werden Karten mit Informationen zu Metriken im Zusammenhang mit der Authentifizierung angezeigt. Jede Karte zeigt eine Trendlinie für die folgenden Metriken an:

- Für MFA registrierte Anwender
- Anwender, die MFA verwenden
- Nicht-MFA-Anwender mit hohen Berechtigungen
- Aktive MFA-Anwender
- Gesperrte MFA-Anwender
- Nur Webservicekonto
- X509-Zertifikate, die in 30 Tagen ablaufen
- Anwender von biometrischem Scanner/Hardware-Schlüsseln
- REST APIs ohne Zugriffsrichtlinie
- Integrationskonten ohne aktivierte Kennzeichnung für „Nur Webservice-Zugang“

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Datenklassifizierung

Greifen Sie auf die Sicherheitsmetriken für die Datenklassifizierung in Ihrer ServiceNow-Instanz zu.

Mit der Datenklassifizierung können Sie Datenklassifizierungsbezeichnungen auf vorhandene Wörterbucheinträge in einer beliebigen Tabelle anwenden. Diese Bezeichnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

helfen Ihnen, Einblicke in die Arten von Daten zu bieten, die in Ihren Instanzen gehostet werden. Verwenden Sie diese Klassifizierungen, um Datenschutzgesetze zu erfüllen und Branchenanforderungen zu erfüllen.

Siehe Datenklassifizierung Weitere Informationen finden Sie unter .

- **Klassifizierbare Daten** : Tabellen oder Spalten, die klassifiziert werden können.
- **Klassifizierte Daten** : Wörterbucheinträge, Tabellen oder Spalten, die klassifiziert sind.

Die Daten werden grafisch in einem anpassbaren Diagramm angezeigt, das detaillierte Analysen wie Festlegen von Zielen, Schwellenwerten, Trends, Statistiken oder Prognosen bietet. Die Daten sind auch als Datensätze in einer Tabelle organisiert. Weitere Informationen finden Sie unter Analytics Hub .

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Authentifizierungsmetriken

Zeigen Sie Metriken im Zusammenhang mit der Authentifizierung in Ihrer Instanz über ein Dashboard an.

Auf dieser Seite werden Karten mit Informationen zu Metriken im Zusammenhang mit der Authentifizierung angezeigt. Jede Karte zeigt eine Trendlinie für die folgenden Metriken an:

- Für MFA registrierte Anwender: Gesamtanzahl der Anwender, die für die Verwendung von MFA registriert sind.
- Anwender, die MFA-Umgehung verwenden: Gesamtanzahl der Anwender, die die Multifaktor-Authentifizierung umgehen.
- Anwender mit hohen Berechtigungen ohne MFA: Gesamtanzahl der Anwender mit hohen Berechtigungen, die MFA nicht verwenden.
- Aktive MFA-Anwender: Gesamtanzahl der MFA-Anwender, die in Ihrer Instanz aktiv sind.
- Gesperrte MFA-Anwender: Gesamtanzahl der MFA-Anwender, die in Ihrer Instanz gesperrt sind.
- Webservice-Account-Anwender: Gesamtanzahl der Anwender nur mit Webservice-Account.
- X509-Zertifikate, die ablaufen: Gesamtanzahl der X509-Zertifikate, die in den nächsten 30 Tagen ablaufen.
- Anwender des biometrischen Scanners/Hardwareschlüssels: Gesamtanzahl der Anwender, die sich mit dem biometrischen Scanner oder Hardwareschlüssel anmelden.
- REST-APIs ohne Zugriffsrichtlinie: Gesamtanzahl der Anwender, die sich ohne Zugriffsrichtlinie der REST-API anmelden.
- Kennzeichnung für „Integrationsaccounts ohne Webservice-Zugriff nur“ aktiviert: Gesamtanzahl der Anwender, die sich ohne Integration-Accounts anmelden – Kennzeichnung „nur Webservice-Zugriff“ aktiviert.

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

E-Mail

Zeigt Daten im Zusammenhang mit Spam-E-Mails an, die extern empfangen werden.

Auf der Seite wird eine Karte mit einer Trendlinie für die Spam-E-Mails angezeigt, die die Anzahl der pro Tag empfangenen Junk-Mails darstellt.

Wählen Sie die Karte aus, um zusätzliche Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Exportieren

Erkennen Sie die Daten, die häufig exportiert werden, und welche Anwender exportieren.

Auf dieser Seite werden Karten mit Informationen zu Metriken im Zusammenhang mit dem Export angezeigt. Jede Karte zeigt eine Trendlinie für die folgenden Metriken an:

- Gesamtzahl der Exporte: Gesamtanzahl der vom Anwender exportierten Tabellendatensätze.
- Klassifizierte Exporte: Gesamtanzahl der exportierten Tabellendatensätze, zusammengefasst nach der ihnen zugewiesenen Datenklassifizierung.

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Integrations-Accounts

Zeigen Sie die Trends zu den Integrationsaccounts an, die in erstellt werden ServiceNow AI Platform.

Auf dieser Seite werden Karten mit Informationen zu Metriken im Zusammenhang mit Integrationsaccounts angezeigt, die auf erstellt werden ServiceNow AI Platform. Jede Karte zeigt eine Trendlinie für die folgenden Metriken an:

- Integrationsaccounts insgesamt: Trends im Zusammenhang mit Integrationsaccounts in Ihrer Instanz.
- Aktive Integrationsaccounts: Trends im Zusammenhang mit aktiven Integrationsaccounts in Ihrer Instanz.
- Inaktive Integrationsaccounts: Trends für die Gesamtanzahl der Integrationsaccounts, die in Ihrer Instanz inaktiv sind.

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Privilegierte Identität

Analysieren Sie Daten im Zusammenhang mit Metriken für Anwender mit privilegierter Identität.

Auf dieser Seite werden Karten mit Informationen zu Metriken angezeigt, die sich auf privilegierte Identitätsanwender und ihre Aktivitäten in Ihrer Instanz beziehen. Jede Karte zeigt eine Trendlinie für die folgenden Metriken an:

- Administratoranmeldungen: Gesamtanzahl der Anmeldungen bei Anwendern der Administratorrolle.
- Identitätswechsel: Gesamtanzahl der Identitätswechsel, die von Anwendern mit der Identitätswechsel-Rolle ausgeführt wurden.
- Erhöhung: Gesamtanzahl der Sicherheitserhöhungen, die von Anwendern mit der Rolle „Security_admin“ durchgeführt wurden.
- ServiceNow-Anmeldungen: Gesamtanzahl der Anmeldungen durch ServiceNow-Mitarbeiter.
- Hinzugefügte Administratoranwender: Gesamtzahl der Anwender mit der Administratorrolle.

Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Privilegierte Anwender

Zeigen Sie die Trendlinie für die privilegierten Anwender (aktiv und inaktiv) und ihre Aktivitäten im an ServiceNow AI Platform.

Im Abschnitt „Übersicht über privilegierte Anwender“ wird die Trendlinie für die privilegierten Anwender (aktiv und inaktiv) und ihre Aktivitäten im angezeigt ServiceNow AI Platform. Privilegierte Anwender sind Anwender, denen von Administratoren zusätzliche Rollen für den Zugriff auf Funktionen wie Einstellungen für hohe Sicherheit, Import und Portal zugewiesen wurden.

Nachfolgend finden Sie eine Erklärung der privilegierten Anwender:

- Anwender insgesamt: Gesamtanzahl der Anwender in Ihrer Instanz.
- Aktive Anwender: Gesamtzahl der Anwender, die Sitzungen in Ihrer Instanz initiiert haben.
- Inaktive Anwender: Anwender, die sich nicht kürzlich bei Ihrer Instanz angemeldet haben.
- Inaktive Anwender, die nicht gesperrt sind: Anwender, die sich nicht kürzlich angemeldet haben, aber noch Zugriff auf ihren Account haben.
- Gesperrte Anwender: Anwender, die sich nicht bei ihrem Account authentifizieren dürfen.
- Neue Anwender: Anwender, die kürzlich Ihrer Instanz hinzugefügt wurden.
- Erfolgreiche Anmeldungen: Anwender, die sich erfolgreich angemeldet haben.
- Fehlgeschlagene Anmeldungen: Nicht erfolgreiche Anmeldeversuche.
- Lokale Anmeldungen, die nicht durch MFA geschützt sind: Anwender, die sich ohne MFA angemeldet haben.
- Nie angemeldete Anwender: Anwender, die sich noch nie bei Ihrer Instanz angemeldet haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwender, die sich seit dem letzten Monat nicht angemeldet haben: Anwender, die sich in den letzten 30 Tagen nicht angemeldet haben.
- Anwender, die sich in den letzten 6 Monaten nicht angemeldet haben: Anwender, die sich in den letzten 6 Monaten nicht angemeldet haben.
- Anwender, die sich seit dem letzten Jahr nicht angemeldet haben: Anwender, die sich im letzten Jahr nicht angemeldet haben.
- Passwort muss zurückgesetzt werden: Anwender, die ihr Passwort zurücksetzen müssen.
- Fehler beim Zurücksetzen des Passworts der Anwender: Anzahl der Passwortfehler pro Anwender.

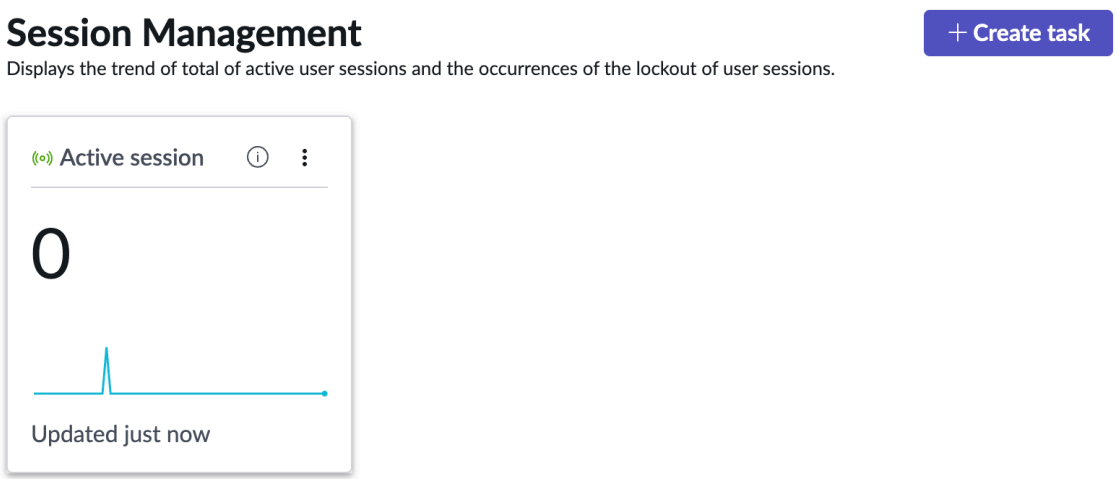
Wählen Sie die Karten aus, um die Seite für einzelne Metriken mit zusätzlichen Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Management von Anwendersitzungen

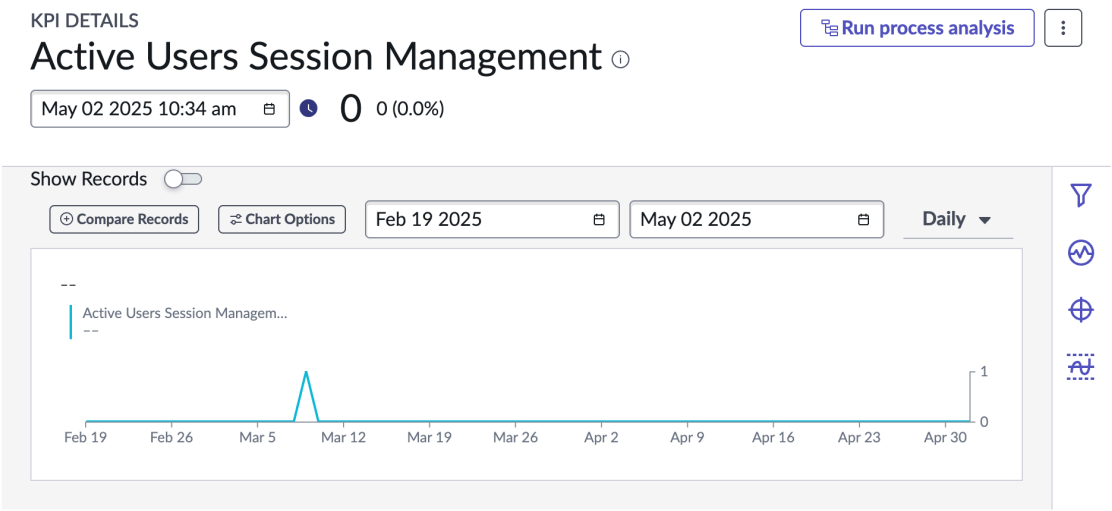
Zeigen Sie Metriken im Zusammenhang mit Anwendersitzungen und der Häufigkeit der Sperrungen der Sitzungen an.

Auf der Seite wird eine Karte mit einer Trendlinie für aktive Sitzungen angezeigt, die die Anzahl der aktiven Sitzungen in Ihrer Instanz darstellt.



Wählen Sie die Karte aus, um zusätzliche Details anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf der Detailseite können Sie die Schaltflächen am Rand des Bildschirms verwenden, um Filter, KPI-Signale, Ziele und Schwellenwerte zu konfigurieren.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Anwender

Zeigen Sie die Trendlinie für die Gesamtzahl der Anwender (aktiv und inaktiv) und ihre Aktivitäten im an ServiceNow AI Platform.

Im Abschnitt Anwenderübersicht wird die Trendlinie für die Gesamtzahl der Anwender (aktiv und inaktiv) und ihre Aktivitäten im angezeigt ServiceNow AI Platform.

Nachfolgend finden Sie eine Erklärung des Anwendertyps:

- Anwender insgesamt: Gesamtanzahl der Anwender in Ihrer Instanz.
- Aktive Anwender: Gesamtzahl der Anwender, die Sitzungen in Ihrer Instanz initiiert haben.
- Inaktive Anwender: Anwender, die sich nicht kürzlich bei Ihrer Instanz angemeldet haben.
- Inaktive Anwender, die nicht gesperrt sind: Anwender, die sich nicht kürzlich angemeldet haben, aber noch Zugriff auf ihren Account haben.
- Neue Anwender: Anwender, die kürzlich Ihrer Instanz hinzugefügt wurden.
- Erfolgreiche Anmeldungen: Anwender, die sich erfolgreich angemeldet haben.
- Fehlgeschlagene Anmeldungen: Nicht erfolgreiche Anmeldeversuche.
- Externe Anmeldungen: Authentifizierungen, die eine Drittpartei verwenden.
- Lokale Anmeldungen, die nicht durch MFA geschützt sind: Anmeldungen, die MFA nicht verwenden.
- Anwender, die sich seit dem letzten Monat nicht angemeldet haben: Anwender, die sich in den letzten 30 Tagen nicht angemeldet haben.
- Anwender, die sich in den letzten 6 Monaten nicht angemeldet haben: Anwender, die sich in den letzten 6 Monaten nicht angemeldet haben.
- Anwender, die sich seit dem letzten Jahr nicht angemeldet haben: Anwender, die sich im letzten Jahr nicht angemeldet haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

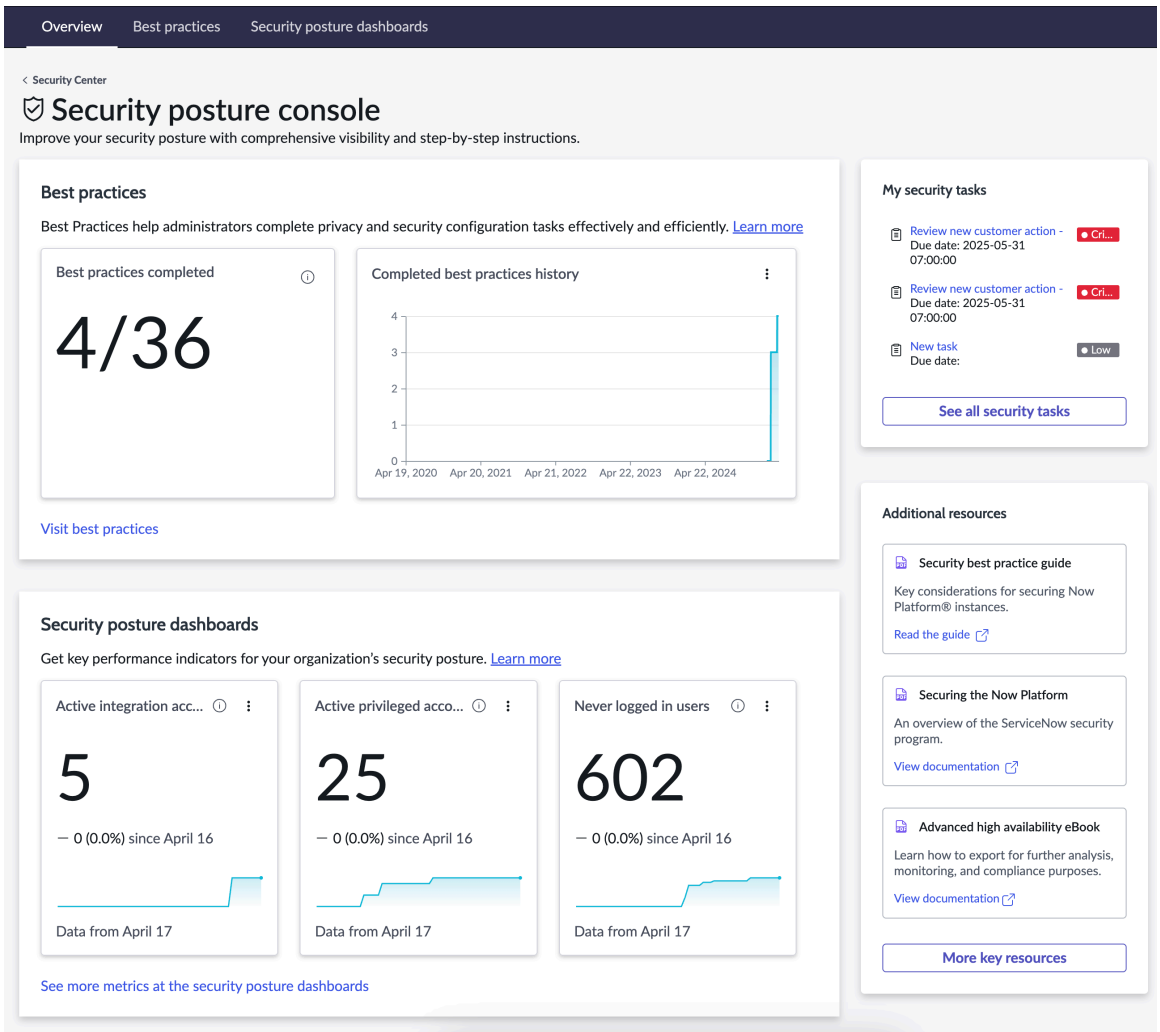
- Passwort muss zurückgesetzt werden: Anwender, die ihr Passwort zurücksetzen müssen.
- Fehler beim Zurücksetzen des Passworts der Anwender: Anzahl der Passwortfehler pro Anwender.

Wählen Sie die Karte aus, um zusätzliche Details anzuzeigen.

Wählen Sie aus **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe im Zusammenhang mit einer Metrik. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Sicherheitslage-Konsole

Verbessern Sie Ihre Fähigkeit, Sicherheitsbedrohungen zu identifizieren, darauf zu reagieren und sie wiederherzustellen, mit umfassender Transparenz und Schritt-für-Schritt-Anweisungen.



Die Sicherheitsstatus-Konsole ist in Abschnitte unterteilt, um Informationen zu Best Practices und Dashboards für die Sicherheitslage bereitzustellen. Suchen Sie nach zusätzlichen Details, indem Sie eine der Karten in diesen Abschnitten auswählen. Sie können auch die Leiste oben auf der Seite verwenden, um zwischen dieser Seite und dem Abschnitt „Best Practices und Sicherheitsstatus-Dashboards“ des Sicherheitszentrums zu navigieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practices

In diesem Abschnitt wird die Anzahl der Best Practices und die Anzahl der Anwendungen auf Ihre Instanz angezeigt. Sie können ein Diagramm sehen, das Ihre abgeschlossenen Best Practices im Laufe der Zeit anzeigt.

Dashboards zur Sicherheitslage

In diesem Abschnitt wird die Anzahl der aktiven Integrations-Accounts, aktiven privilegierten Accounts und Anwender angezeigt, die sich noch nie angemeldet haben.

Aktive Integrationsaccounts

Integrationsaccounts sind Anwenderaccounts, die Integrationen zwischen Ihrer Instanz und Anwendungen von Drittanbietern verwalten.

Aktive privilegierte Accounts

Privilegierte Anwender sind Anwender, denen von Administratoren zusätzliche Rollen für den Zugriff auf Funktionen wie Einstellungen für hohe Sicherheit, Import und Portal zugewiesen wurden.

Nie angemeldete Anwender

Anwenderaccounts, die sich noch nie bei Ihrer Instanz angemeldet haben.

Meine Sicherheitsaufgaben

Zeigen Sie die dringendsten Sicherheitsaufgaben an, die Ihnen zugewiesen sind. Wählen Sie eine Aufgabe aus, um ihre Details anzuzeigen, oder wählen Sie aus **Alle Sicherheitsaufgaben anzeigen** Zum Anzeigen einer vollständigen Liste von Sicherheitsaufgaben.

Zusätzliche Ressourcen

Verwenden Sie den Abschnitt „zusätzliche Ressourcen“ am Rand des Bildschirms, um zu Dokumentationen und Videos zu navigieren, die für das Lernen des Sicherheitszentrums relevant sind, sowie zu Informationen zur Verwaltung der Instanzsicherheit.

Best Practices für Sicherheit

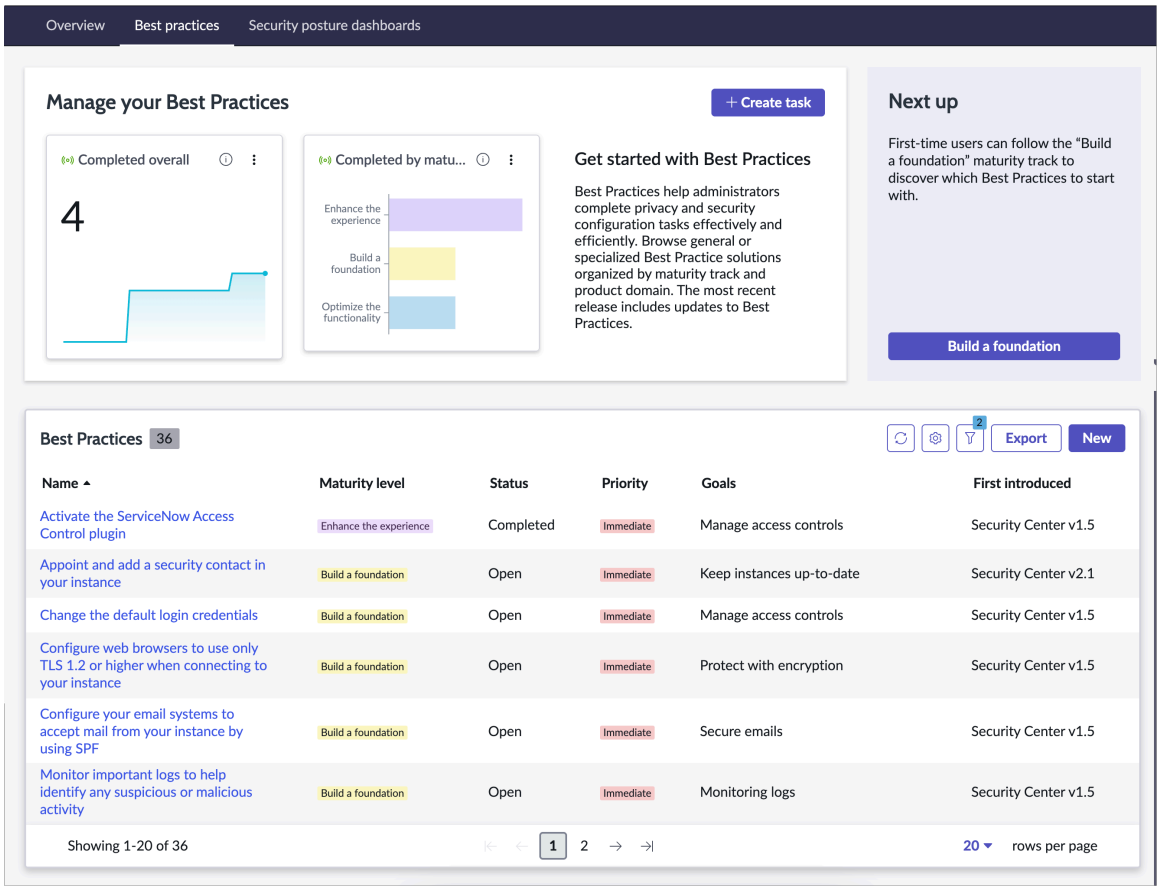
Verwenden Sie Best Practices für die Sicherheit, um Datenschutz- und Sicherheitskonfigurationsaufgaben auf Ihrem zu implementieren ServiceNow Instanz.

Identifizieren Sie Best Practices, um Ihre Sicherheitslage zu verbessern, und befolgen Sie die Schritt-für-Schritt-Anweisungen, um sie zu implementieren. BEST Practices für Sicherheit bieten Folgendes:

- Die Homepage zeigt einen Überblick über Ihren Fortschritt bei der Implementierung von Best Practices für Sicherheit. Sie können auch Listen von Best Practices für Sicherheit gemäß den Zielen Ihrer Organisation organisieren und verwalten.
- Die Übersichtsseite enthält Details zu jeder Best Practice für Sicherheit, die Schritte zu ihrer Implementierung sowie einen Datensatz aller Aktivitäten und Kommentare.
- Die Seite „Aufgabenschritte“ enthält Anweisungen zur Implementierung von Best Practices für Sicherheit.
- Auf der Aktivitätsseite wird der Verlauf der Anwender- und Systemaktionen im Zusammenhang mit Ihren Best Practices für Sicherheit nachverfolgt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Startseite für Best Practices für Sicherheit



Auf der Homepage wird ein angezeigt **Verwalten Sie Ihre Best Practices** Abschnitt, der Diagramme enthält, die einen Überblick über Ihren Fortschritt geben.

Insgesamt abgeschlossen

Zeigt eine Anzahl und Trendlinie der von Ihnen abgeschlossenen Best Practices an. Wählen Sie die Karte aus, um anzuzeigen **Insgesamt Abgeschlossen** Metrikseite in Sicherheitsmetriken.

Nach Reifegrad abgeschlossen

Zeigt ein Diagramm abgeschlossener Best Practices an, organisiert nach Reifegrad (eine Beschreibung der Reifegrade finden Sie in der Tabelle „Fortfahren"). Wählen Sie die Karte aus, um anzuzeigen **Abgeschlossen nach Reifegrad** Metrikseite in Sicherheitsmetriken.

Grundlage schaffen

Wählen Sie aus **Erstellen Sie eine Grundlage** Schaltfläche zum Filtern der Tabelle auf dieser Seite, um nur Best Practices in anzuzeigen **Erstellen Sie eine Grundlage** Reifegrad. Dies sind Änderungen mit geringerer Auswirkung, die Sie vornehmen können, um die Instanzsicherheit zu verbessern.

Eine Aufgabe erstellen

Verwenden Sie **+Aufgabe erstellen** Schaltfläche zum Erstellen einer Sicherheitsaufgabe zum Nachverfolgen oder Delegieren von Best Practice-Arbeiten. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Mit der Tabelle können Sie Filter anwenden, um gefilterte Listen zu sortieren und zu speichern, die Sie als Arbeitslisten für verschiedene Anwendungsfälle oder Rollen verwenden können. Siehe Speichern Sie eine gefilterte Liste Weitere Informationen finden Sie unter .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

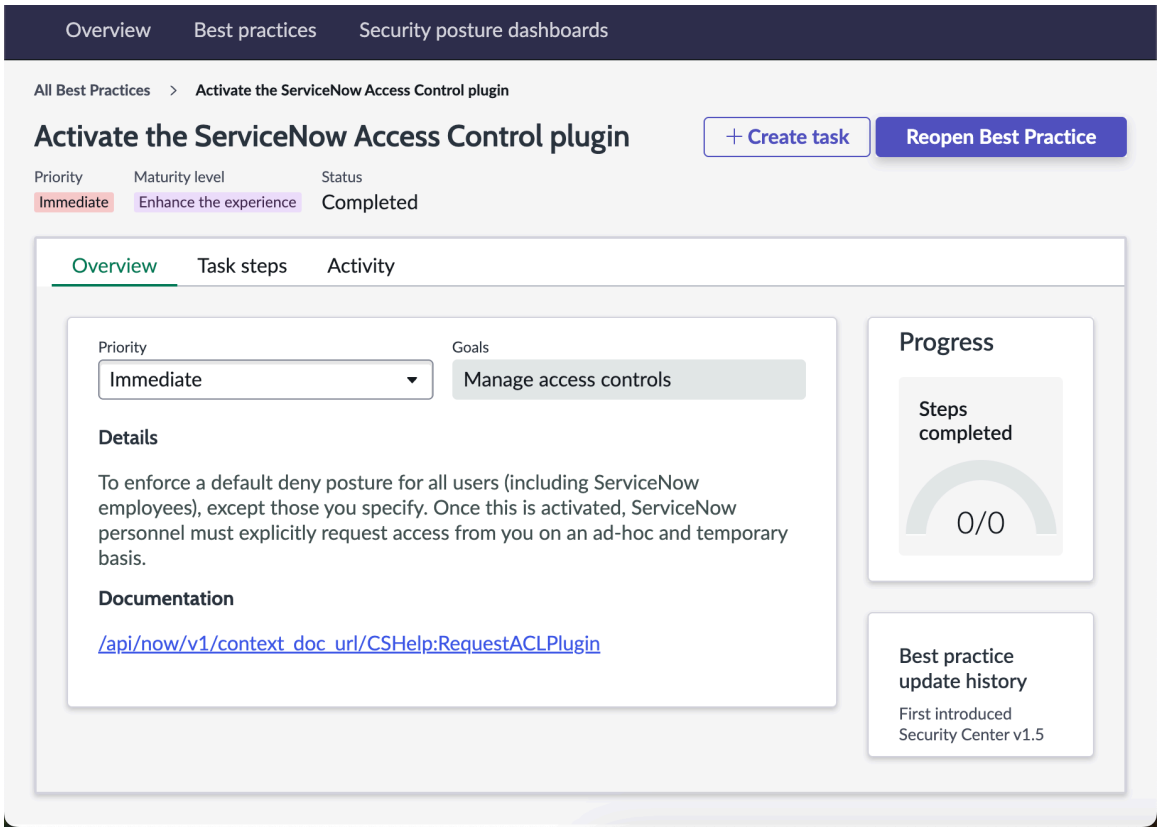
Im Folgenden finden Sie Erklärungen der Felder im Zusammenhang mit der Tabelle „Best Practices für Sicherheit“.

Zusammenfassung der Felder, die in der Tabelle „Best Practices für Sicherheit“ verwendet werden

Name	Beschreibung
Name	Wort, das zur Identifizierung einer Best Practice für Sicherheit verwendet wird.
Reifegrad	Anwendungen und Funktionen, die nach der Reihenfolge der Auswirkungen angeordnet wurden, um Ihnen messbare Ergebnisse zu liefern. Die Werte für Reifegrade sind: • Grundlage schaffen • Experience erweitern • Funktionalität optimieren • Erweiterte Funktionen hinzufügen Diese können auch als Durchforstungs-, Walk-, Run- und Fly-Phasen betrachtet werden.
Status	Aktueller Status einer Best Practice: • Öffnen • In Bearbeitung • Abgeschlossen
Priorität	Reihenfolge der Wichtigkeit für die Implementierung einer Best Practice in Ihrer Organisation: • Sofort • Später • Nicht zutreffend
Ziele	Sicherheitskategorie, auf die sich eine Best Practice bezieht: • Anfängliche Sicherheitskonfigurationen behandeln • Sichere E-Mails • Überwachungsprotokolle • Zugriffssteuerungen verwalten • Mit Verschlüsselung schützen • Instanzen auf dem neuesten Stand halten
Zuerst eingeführt	Welche Security Center-Version die Best Practice eingeführt wurde.
Geändert	Welche Security Center-Version die Best Practice geändert wurde.
Entfernt	Welche Security Center-Version die Best Practice entfernt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite mit Details zu Best Practices für Sicherheit



Wählen Sie eine Best Practice aus der Tabelle aus, um die zugehörige Seite anzuzeigen. Oben auf der Detailseite können Sie allgemeine Informationen zur Best Practice für Sicherheit anzeigen, einschließlich Priorität, Reifegrad und Status. Verwenden **Führen Sie Best Practice Aus** Schaltfläche, um die Praxis als abgeschlossen zu markieren, oder **Öffnen Sie Best Practice Erneut** Schaltfläche zum Markieren der Praxis als abgeschlossen. Verwenden Sie **+Aufgabe Erstellen** Dient zum Erstellen einer Sicherheitsaufgabe zum Nachverfolgen und Delegieren dieser Aufgabe. Details zu Sicherheitsaufgaben finden Sie unter Sicherheitsaufgaben.

Diese Seite enthält weitere Informationen zur Best Practice, unterteilt in Registerkarten:

Übersicht

Diese Registerkarte enthält **Priorität** Dropdown-Menü, in dem Sie die Best Practices für Sicherheit angeben können, die derzeit für Sie wichtig sind und nicht zutreffend sind.

Der Abschnitt „Details“ enthält Inhalte zu den Funktionen, die der Best Practice für Sicherheit zugeordnet sind, und der Dokumentationsabschnitt enthält einen oder mehrere Links, in denen Sie zusätzliche Informationen finden.

Die **Fortschritt** Die Karte auf der rechten Seite zeigt die Anzahl der abgeschlossenen Schritte vs. Die Gesamtzahl der enthaltenen Schritte. Wählen Sie Aus **Wechseln Sie zum nächsten Schritt** Um zum nächsten unvollständigen Schritt zu navigieren.

Die **BEST Practice-Aktualisierungsverlauf** Die Karte bietet einen Snapshot der Release-Informationen für die Best Practice. Sie können nachverfolgen, in welcher ServiceNow Security Center-Version die Best Practice für Sicherheit veröffentlicht wurde und in welchen Versionen sie anschließend zuletzt aktualisiert wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabenschritte

Diese Registerkarte enthält Schritt-für-Schritt-Anweisungen für die Implementierung dieser Best Practice für Sicherheit. Siehe Führen Sie eine Best Practice für Sicherheit durch Weitere Informationen finden Sie unter .

Aktivität

Auf dieser Registerkarte werden Aktivitäten mit Zeitstempel angezeigt, die von den neuesten bis den ältesten Aktivitäten aufgelistet sind. Verwenden Sie Suche und Filter, um Informationen abzufragen. Siehe Wenden Sie Filter auf die Tabelle „Best Practices für Sicherheit“ an Weitere Informationen finden Sie unter .

Führen Sie eine Best Practice für Sicherheit durch

Erfahren Sie, wie Sie eine Best Practice für Sicherheit für Ihre ServiceNow-Instanz abschließen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die folgenden Schritte aus, um Best Practices für Sicherheit in Ihrer ServiceNow-Instanz zu implementieren.

Prozedur

1. Greifen Sie auf Best Practices für Sicherheit zu, indem Sie auswählen **Alle** In Ihrer ServiceNow-Instanz und dann eingeben **BEST Practice** .
2. Wenden Sie einen Filter an, um Best Practices für die Sicherheit anzuzeigen, die implementiert werden sollen.
   a. Navigieren Sie zu **Best Practices** Tabelle in der Anwenderoberfläche.
   b. Wählen Sie das Kebab-Menü oder das Element mit drei vertikalen Punkten (⋮) In **Status** Spalte.
   c. Wählen Sie aus **Öffnen** Und **In Bearbeitung** Optionen, und wählen Sie dann aus **Anwenden** .
3. Wählen Sie den Namen einer zu implementierenden Best Practice für Sicherheit aus.
4. Wählen Sie Aus **Wechseln Sie zum nächsten Schritt** .
5. Wählen Sie einen Aufgabenschritt aus der aus **Aufgabenschritte** Liste.
6. Wählen Sie das Symbol „Caret down“ (V), um die Implementierungsanweisungen für diesen Schritt anzuzeigen.
7. Lesen Sie die Anweisungen, und implementieren Sie sie dann in Ihrer ServiceNow-Instanz.
8. Wählen Sie Aus **Schritt als abgeschlossen markieren** Wenn Sie mit der Aufgabe fertig sind.

   Hinweis: Sie können die Aufgabe überspringen, wenn Sie später darauf zurückkommen möchten oder wenn sie nicht für die Ziele Ihrer Organisation gilt. Darüber hinaus können Sie einen abgeschlossenen Aufgabenschritt erneut öffnen, indem Sie den Aufgabenschritt und dann auswählen **Schritt neu starten** .

9. Wählen Sie Aus **Führen Sie Best Practice Aus** .

Sie können eine Best Practice für Sicherheit jederzeit abschließen. Sie müssen nicht alle Schritte abschließen, und es ist in Ordnung, wenn Sie sie überspringen. Erwägen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie jedoch, einen Kommentar in die Unterregisterkarte „Aktivität“ einzufügen, wenn Sie eine Best Practice für Sicherheit abschließen, wenn Sie nicht alle Schritte für eine Audit-Referenz abgeschlossen haben.

Zeigen Sie die Aktivität einer Best Practice an

Verfolgen Sie den chronologischen Verlauf und den Zeitstempelverlauf im Zusammenhang mit einer Best Practice für Sicherheit, die Sie in Ihrer ServiceNow-Instanz abschließen, zusammen mit dem Anwender, der die Aktivität initiiert hat.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Greifen Sie auf Security Best Practices Manager zu, indem Sie auswählen **Alle** Geben Sie in Ihrer ServiceNow-Instanz Best Practice ein.
2. Wählen Sie in der Tabelle „Best Practices“ eine Best Practice für Sicherheit aus, für die Sie die Aktivität in anzeigen möchten **Name** Spalte.
3. Wählen Sie aus **Aktivität** Registerkarte.

   Beispiele für Aktivitäten, die Sie anzeigen können, umfassen Feldänderungen, z. B. wenn sich der Status einer Best Practice für Sicherheit von „Offen“ in „Abgeschlossen“ geändert hat oder wenn ein Aufgabenschritt abgeschlossen oder übersprungen wird. Darüber hinaus können Sie zusätzliche Informationen zu einer Aktivität eingeben, indem Sie einen Kommentar in das Textfeld eingeben.

Zeigen Sie Daten abgeschlossener Best Practices an

Sehen Sie sich visuelle Darstellungen der Gesamtanzahl der abgeschlossenen Best Practices oder Segmentierungen nach Reifegrad an.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Führen Sie die Aktionen aus, um Diagramme anzuzeigen, die visuelle Trends von Best Practices für die Sicherheit enthalten, die insgesamt und nach Reifegrad abgeschlossen wurden.

Prozedur

1. Greifen Sie auf die Sicherheitscenter-App zu, und navigieren Sie zu **Best Practices** Registerkarte.
2. Unter **Verwalten Sie Ihre Best Practices** Wählen Sie die Karte aus **Insgesamt abgeschlossen** Diagramm.
3. Zeigen Sie das Diagramm an, um Trends bezüglich abgeschlossener Konfigurationen für Best Practices für Sicherheit anzuzeigen.
4. Wählen Sie Aus **Abgeschlossen nach Reifegrad** Dient zum Anzeigen eines Diagramms, das Trends der Best Practices anzeigt, die nach Reifegrad abgeschlossen wurden.

Filtert die Tabelle „Best Practices für Sicherheit“

Wenden Sie Filter an, um relevantere Ergebnisse für Ihre Best Practices für Sicherheit zurückzugeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Greifen Sie auf Security Best Practices Manager zu, indem Sie auswählen **Alle** In Ihrer ServiceNow-Instanz und Eingabe von Best Practice.
2. Navigieren Sie zu **Best Practices** Tabelle und wählen Sie ein Feld aus, auf das Sie einen Filter anwenden möchten, indem Sie das Kebab-Menü oder das Feld mit drei vertikalen Punkten (⋮).

Felder	Filter
Name	Kombinieren Sie einen bedingten Operator mit einer Textzeichenfolge, um Best Practices für die Sicherheit zurückzugeben, die dem von Ihnen eingegebenen Namen entsprechen.
Reifegrad	Wenden Sie einen Filter an, um Best Practices für Sicherheit zurückzugeben, die einem oder mehreren der folgenden Reifegrade entsprechen: ○ Grundlage schaffen ○ Experience erweitern ○ Funktionalität optimieren ○ Erweiterte Funktionen hinzufügen
Status	Wenden Sie einen Filter an, um Best Practices für die Sicherheit zurückzugeben, die einem oder mehreren der folgenden Status entsprechen: ○ Leer ○ Öffnen ○ In Bearbeitung ○ Abgeschlossen
Priorität	Wenden Sie einen Filter an, um Best Practices für die Sicherheit zurückzugeben, die den folgenden Prioritäten entsprechen: ○ Leer ○ Sofort ○ Später ○ Nicht zutreffend
Ziele	Wenden Sie einen Filter an, um Best Practices für die Sicherheit zurückzugeben, die einem oder mehreren der folgenden Ziele entsprechen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Filter
	○ Anfängliche Sicherheitskonfigurationen behandeln ○ Instanzen auf dem neuesten Stand halten ○ Zugriffssteuerungen verwalten ○ Überwachungsprotokolle ○ Mit Verschlüsselung schützen ○ Sichere E-Mails **Hinweis** : Erweiterte Filter werden stan–dardmäßig auf Ziele angewendet. Um sie zu ändern, wählen Sie aus **Änderungen vorneh men** > **Erweiterte Ansicht** > **Wählen Sie Feld ziele aus** Erstellen Sie dann die restlichen Bedingungen, und wählen Sie aus **Aktuali sieren** .
Zuerst eingeführt	Kombinieren Sie einen bedingten Operator mit einer Textzeichenfolge, um Best Practices zurückzugeben, die zuerst mit der von Ihnen eingegebenen Version eingeführt wurden.
Geändert	Kombinieren Sie einen bedingten Operator mit einer Textzeichenfolge, um Best Practices für die Sicher-heit zurückzugeben, die sich in der von Ihnen einge-gebenen Version geändert haben.
Entfernt	Kombinieren Sie einen bedingten Operator mit einer Textzeichenfolge, um Best Practices für die Sicher-heit zurückzugeben, die in der von Ihnen eingegebe-nen Version entfernt wurden.

Speichern Sie einen Filter für die zukünftige Verwendung

Entdecken Sie die Schritte zum Speichern von Filtern in Ihren Best Practices für Sicherheit zur späteren Wiederverwendung.

Vorbereitungen

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie Filter in der Tabelle „Best Practices für Sicherheit“ erstellt haben, können Sie sie zur Verwendung bei der nächsten Authentifizierung bei Ihrer Instanz speichern. Wenn Sie mehr Flexibilität bei der Art der Filter wünschen, die Sie erstellen können, können Sie einen erweiterten Filter anwenden.

Prozedur

1. Wählen Sie den Filter anzeigen (Symbol für) Bereich.
2. In **Filter** Im Dialogfeld scrollen Sie nach unten, und wählen Sie aus **Erweiterte Ansicht** .
3. Erstellen Sie einen Filter, indem Sie Bedingungen hinzufügen, die ein Feld, einen Operator und Werte enthalten.
4. Wählen Sie Aus **Filter speichern**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie den Filternamen ein.
6. Wählen Sie eine Berechtigung aus.
7. Wählen Sie **Speichern**.
8. Wählen Sie Aus **Aktualisieren** Um den gespeicherten Filter auf die Tabelle „Best Practices für Sicherheit“ anzuwenden.

Verwenden Sie einen gespeicherten Filter

Entdecken Sie die Schritte für die Verwendung der Filter, die Sie für Ihre Best Practices für Sicherheit gespeichert haben.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Nachdem Sie sich von Ihrer Instanz abgemeldet haben, werden Ihre Filter auf die Standardeinstellungen zurückgesetzt. Die folgenden Schritte zeigen, wie Sie einen gespeicherten Filter abrufen, damit Sie ihn erneut auf die Tabelle „Best Practices für Sicherheit“ anwenden können.

Prozedur

1. Wählen Sie den Filterbereich anzeigen ( )-Symbol.
2. Scrollen Sie im Dialogfeld Filter nach unten, und wählen Sie aus **Erweiterte Ansicht** .
3. Wählen Sie Aus **Vorhandenen Filter verwenden** , Und wählen Sie dann einen gespeicherten Filter aus der Dropdown-Liste aus.
4. Wählen Sie Aus **Aktualisieren** Zum Anwenden des gespeicherten Filters.

Best Practices

Weitere Informationen zu den Best Practices finden Sie in der Sicherheitsstatus-Konsole.

Best Practice	Beschreibung
Aktivieren Sie ServiceNow Plugin „Zugriffssteuerung“	Verwenden Sie ServiceNow Plugin „Zugriffssteuerung“, um zu steuern, welche Mitarbeiter wann auf Ihre Instanz zugreifen können. Erzwingen einer standardmäßigen Deny-Situation für alle Anwender mit Ausnahme der von Ihnen angegebenen Anwender. Dies kann umfassen ServiceNow Mitarbeiter. Die Verwendung dieses Plugins hilft, unerwünschten Zugriff auf Ihre Instanz zu verhindern. **Hinweis:** Nach ServiceNow Die Zugriffssteuerung ist aktiviert. Mitarbeiter müssen explizit Ad-hoc und temporär Zugriff von Ihnen anfordern. Weitere Informationen zu diesem Plugin finden Sie unter ServiceNow-Zugriffssteuerung.
Kontaktperson für Sicherheit in der Instanz ernennen und hinzufügen	Wählen Sie einen Informationssicherheitskontakt in Ihrer Organisation aus, der sicherheitsbezogene Informationen vom Sicherheitsteam erhält. Dieser Kontakt ist zusätzlich zu Ihrem Administrator, der auch diese Updates erhält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	Diese Informationen können Sicherheitsprobleme, Sicherheitswarnungen oder Details zu wichtigen Software-Updates sein. Weitere Informationen zum Hinzufügen eines Sicherheitskontakts finden Sie unter KB0621516 .
Standardanmeldeinformationen ändern	Ändern Sie die Passwörter in den integrierten Anwenderaccounts Ihrer Instanz, z. B. „admin“, „ITIL“ und „Mitarbeiter“. Diese Accounts werden mit Standardpasswörtern bereitgestellt, die für Ihre Instanz eindeutig sind, sollten jedoch so bald wie möglich geändert werden. Weitere Informationen zum Ändern der Passwörter für Anwenderaccounts in Ihrer Instanz finden Sie unter Konfigurieren Sie das Passwort für einen Anwender.
Webbrowser so konfigurieren, dass bei der Verbindung mit Ihrer Instanz nur TLS 1.2 oder höher verwendet wird	Überprüfen Sie, ob Browser, die eine Verbindung zu Ihrer Instanz herstellen, die sicherere Transport Layer Security (TLS) 1,2 verwenden. Diese Änderung kann im Browser vorgenommen oder von Ihrem Web-Proxy oder einem anderen Gateway erzwungen werden. In der Dokumentation zu Ihrem Browser, Webproxy oder Gateway finden Sie Schritte zur Konfiguration dieser Produkte für die Verwendung von TLS 1,2.
E-Mail-Systeme so konfigurieren, dass sie E-Mails von Ihrer Instanz akzeptieren, indem Sie SPF verwenden	Wenn Ihre Organisation das Sender Policy Framework (SPF) verwendet, um eingehende E-Mails mit Anti-Spam-Technologie zu steuern, müssen Sie es so konfigurieren, dass E-Mails akzeptiert werden, die von Ihrer Instanz stammen. Konfigurieren Sie SPF, um die SPF-Datensätze dynamisch abzufragen. Wenn SPF keine Option ist, besteht ein anderer Ansatz darin, die E-Mail-Server-IP-Adressen Ihrer Allow-Liste hinzuzufügen. Diese Konfiguration muss überwacht werden, da die Adressen geändert werden könnten. Schritte und zusätzliche Details zu diesen Lösungen finden Sie unter KB0535456
Erwägen Sie, Dateianhänge, Uploads und Downloads einzuschränken	Beschränken Sie das Hochladen von Anhängen nach Rolle, Dateierweiterung, MIME-Typ oder Größe, um zu verhindern, dass potenziell schädliche Dateien gespeichert und dann von Ihrer Instanz bereitgestellt werden. Sie können auch steuern, welche Dateitypen heruntergeladen werden können, einschließlich nach MIME-Typ, und den Bildzugriff durch nicht authentifizierte Anwender verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	Diese Anhangsbeschränkungen werden durch Systemeigenschaften in Ihrer Instanz gesteuert. Weitere Informationen zu ihrer Konfiguration finden Sie unter Konfigurieren Sie die Systemeigenschaften des Anhangs .
Browser-SQL-Nachrichten deaktivieren	Verhindern, dass SQL-Fehlermeldungen im Webbrowser angezeigt werden. Diese Nachrichten sind für Anwender und Entwickler zwar nützlich, können jedoch von Angreifern verwendet werden, um Informationen über Ihr System zu erhalten oder ihre Versuche zu unterstützen, auf Ihre Daten zuzugreifen. Diese Nachrichten können mithilfe einer Systemeigenschaft deaktiviert werden. Weitere Informationen zu dieser Systemeigenschaft finden Sie unter Deaktivieren Sie SQL-Fehlermeldungen [Aktualisiert in Security Center 1,3 und 1,5].
Passwortlose Authentifizierung deaktivieren	Sorgen Sie für eine starke Authentifizierung, indem Sie die passwortlose Authentifizierung nach Möglichkeit deaktivieren. Ohne die passwortlose Authentifizierung zu deaktivieren, können potenzielle Angreifer Zugriff auf Ihre Instanz erhalten, indem sie einen Anwendernamen (z. B. „firstname.lastname“ oder einen Rollentitel) richtig erraten. Sie können die passwortlose Authentifizierung in Ihrer Instanz mithilfe einer Systemeigenschaft deaktivieren. Einzelheiten zu dieser Eigenschaft finden Sie unter Passwortlose Authentifizierung deaktivieren.
Tabellenauditing für wichtige oder sensible Daten aktivieren	Verfolgen Sie Änderungen an Ihren Daten mithilfe von Tabellen-Auditing. Audits verfolgen die Erstellung, Aktualisierung und Löschung aller Datensätze in der Tabelle, in der sie aktiviert ist, und ermöglichen es Administratoren, Änderungen an wichtigen oder vertraulichen Daten nachzuverfolgen. Administratoren können auch bestimmte Felder in einer Tabelle für Audits auswählen, um gezieltere Ergebnisse anzuzeigen oder die Auswirkungen auf die Leistung zu reduzieren. Details zum Auditing von Instanzen finden Sie unter Auditing. Spezifische Anweisungen zum Aktivieren von Audits für eine Tabelle finden Sie unter Auditing für eine Tabelle konfigurieren.
Daten im Ruhezustand innerhalb der Instanz verschlüsseln	Verschlüsseln Sie Ihre Daten, um ihre Vertraulichkeit und Integrität zu wahren. Daten in Ihrer Instanz können sich in der Datenbank befinden. Sie können auch die Funktionalität abonnieren, um das Datenvolumen im Back-End transparent zu verschlüsseln. Die physischen Datenträger, auf denen die Instanz ausgeführt wird, können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	auch vollständig verschlüsselt werden, um Daten bei Verlust oder Diebstahl zu schützen. Je nach Anwendungsfall und Risiken, die Sie mindern möchten, können Sie verschiedene Verschlüsselungsmethoden gleichzeitig für Daten verwenden, die in Ihrer Instanz gespeichert sind. Sie können beispielsweise Ihre Daten im Ruhezustand transparent mit Datenbankverschlüsselung in den meisten Tabellen und Cloud-Verschlüsselung für das gesamte Datenvolumen verschlüsseln. Sie können auch die vollständige Datenträgerhardware-Verschlüsselung verwenden, die auch eine dedizierte Umgebung zum Schutz vor Laufwerk- oder Serverdiebstahl erfordert. Überprüfen Sie die mit in verfügbaren Verschlüsselungsoptionen Key Management Framework.
Nutzung von starken Passwortsätzen erzwingen	Verwenden Sie Passwortrichtlinien, um Länge, Komplexität, Ablauf, Eindeutigkeit, Sperre zu erzwingen. und mehr für native und lokale Accounts in Ihrer Instanz. Verwenden Sie diese Richtlinien, um die Sicherheit zu maximieren, die Einführung langer Passphrasen zu fördern und die Verwendung einfacher Passwörter zu vermeiden. Sie können Ihre vorhandenen Richtlinien für alle integrierten externen Authentifizierungsservices wie LDAP oder SAML beibehalten. Details zur Konfiguration der Passwortrichtlinie finden Sie unter Konfigurieren Sie Ihre Passwortrichtlinie.
Automatische Accounterstellung sicherstellen	Verwenden Sie diese Funktion, um Anwenderaccounts dynamisch per E-Mail zu erstellen. Aktivieren Sie diese Funktion nur, wenn dies für Ihre Geschäftsanforderungen erforderlich ist, erst nachdem Sie eine Liste vertrauenswürdiger Domänen definiert haben, aus denen Accounts erstellt werden können. Sie können auch steuern, wie Passwörter neuen Accounts zugewiesen werden, die auf diese Weise erstellt wurden. Details zur automatischen Anwendererstellung finden Sie unter Automatische Anwendererstellung aktivieren .
Stellen Sie sicher, dass Sie sicheren Zugriff auf Knowledge Bases haben	Verwalten Sie den Zugriff auf Knowledge Bases und Artikel, um eine sichere und effiziente Informationsfreigabe zu gewährleisten. Sie können bestimmen, ob bestimmte Anwender oder Anwenderkategorien auf Knowledge Bases und Wissensartikel zugreifen können, indem Sie den Mitwirkungs- und Lesezugriff steuern. Die spezifische Konfiguration hängt von Ihren Geschäftsanforderungen ab. Erfahren Sie mehr über Ihre

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	Optionen zum Konfigurieren des Wissenszugriffs unter Verwalten des Zugriffs auf Knowledge Bases und Wissensartikel .
Sicherstellen, dass das Plugin für hohe Sicherheit installiert und aktiviert ist	Verwenden Sie das Plugin „High Security“ (HSP), um das Sicherheitsmanagement zu verbessern und entsprechende Einstellungen anzuwenden. Hohe Sicherheitseinstellungen bieten einen zentralen Speicherort für Sicherheitseinstellungen, erstellen eine eindeutige Sicherheitsadministratorrolle, eine standardmäßige Deny-Eigenschaft und andere wichtige Sicherheitsfunktionen. HSP ist standardmäßig auf allen neuen Instanzen installiert und aktiviert. Sie können die HSP-Aktivierung für ältere Instanzen anfordern, einschließlich Instanzen, für die Upgrades von einer älteren Version durchgeführt wurden. Die Aktivierung von HSP sollte erst nach sorgfältigen Tests in einer Umgebung außerhalb der Produktion erfolgen, da die Aktivierung einige grundlegende Eigenschaften und Verhaltensweisen ändert. Weitere Informationen zum Plugin für hohe Sicherheit finden Sie unter Plugin für hohe Sicherheit aktivieren [aktualisiert in Security Center 1,3].
Mit NOW-Sicherheitsressourcen vertraut machen	Sicherheitsinformationen werden ständig weiterentwickelt. Daher ist es wichtig, mit Sicherheitsressourcen auf dem Laufenden zu bleiben, um die Informationssicherheit zu gewährleisten. Verwenden Sie die folgenden Ressourcen, um über Sicherheitsressourcen auf dem Laufenden zu bleiben: • CORE-Verzeichnis: ServiceNow CORE-Compliance-Portal • Sicherung der ServiceNow KI-Plattform: Wie ServiceNow Kundendaten schützt • Instanz sichern
Sicherheitshärtung für die eigene Instanz durchführen	Verwenden Sie das Sicherheitscenter-Härtungstool, um das Risiko zu reduzieren, indem Sie Schwachstellen einschränken, die ausgenutzt werden könnten, und implementieren Sie empfohlene Einstellungen, um Ihre Instanz weiter zu sichern. Weitere Informationen zum Sicherheitscenter finden Sie unter Security Center. Überprüfen Sie die verfügbaren Härtungseinstellungen unter Härtungseinstellungen.
Patches so schnell wie möglich installieren	Installieren Sie Patches und Plattformupdates so bald wie möglich, um das höchste Sicherheitsniveau für Ihre

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	Instanz und die anderer Kunden sicherzustellen. Wenn Sie mit Updates auf dem neuesten Stand bleiben, können Sie auch kontinuierlichen Support erhalten, indem Sie die EOL-Richtlinie einhalten. Verwenden Sie das Upgrade Center, um den Prozess zu verwalten. Sicherheitsfixes werden routinemäßig für die Now Platform über die Patches und Hotfixes veröffentlicht, die Produktfunktionsupdates begleiten. Ein Upgrade, wenn neue Patches und Hotfixes verfügbar sind, trägt dazu bei, das Risiko potenzieller Schwachstellen zu reduzieren. Informationen zu Now Platform-Releases, Patches und Hotfixes finden Sie im Abschnitt „Release Notes“ der Produktdokumentation. Weitere Informationen finden Sie unter Phase 1 – .
In die MFA integrieren	Integrieren Sie die Multifaktor-Authentifizierung (MFA) von Drittparteien mit Ihrem vorhandenen SAML-IdP, um zusätzliche Anmeldesicherheit zu bieten. MFA bietet ein hohes Sicherheitsniveau, da die Authentifizierung mehrere Authentifizierungsfaktoren erfordert. Etwas, das der Anwender weiß (das Passwort), sowie etwas, das er besitzt (ein einmaliger Code, Mobiltelefon oder biometrische Attribute, z. B. ein Fingerabdruck). Weitere Informationen zur MFA-Integration finden Sie unter Multi-Faktor-Authentifizierung.
Akzeptierte E-Mail-Senderdomänen begrenzen	Steuern Sie, mit welchen Domänen und Anwendern Ihre Instanz per E-Mail kommunizieren kann, indem Sie Systemadressfilter verwenden. Diese Filter können an Ihre Anforderungen angepasst werden. Erfahren Sie, wie Sie vertrauenswürdige Domänen unter konfigurieren Legen Sie E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig fest.
Wichtige Protokolle überwachen, um dabei zu helfen, alle verdächtigen oder böswilligen Aktivitäten zu ermitteln	Das Systemprotokollmodul bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Ereignissen in der Instanz verwenden können. **Ereignisprotokolle** Ereignisprotokolle zeigen viel über die Systemaktivität auf, einschließlich Anmeldereignisse (erfolgreich oder anderweitig) und Berechtigungseskalation. **Systemprotokolle** Systemprotokolle enthalten umfassende Informationen über allgemeine Aktivitäten, einschließlich Konfigurationsänderungen, Systemfehler, Workflows und ein-/ausgehende Datenverbindungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	Hinweis: Die Ereignis- und Systemprotokolle können auch verwendet werden, um einen Audit-Pfad für alle Aktivitäten des Personals bereitzustellen. **Transaktionsprotokolle** Transaktionsprotokolle zeichnen alle Webbrowser-bezogenen Aktivitäten für eine Instanz auf und können Details zu jeder gestellten Anforderung bereitstellen. Transaktionsprotokolle können nützlich sein, um ungewöhnliche oder schädliche Aktivitäten zu identifizieren. **Tabellen-Auditing und Datensatzverlauf** Aktivieren Sie das Auditing für Datenbanktabellen. Der Datensatzverlauf ist unbefristet und ermöglicht Ihnen, Details aller seit der Erstellung an den Daten vorgenommenen Änderungen nachzuverfolgen und anzuzeigen. Standardmäßig werden nur die Tabellen „Incident“, „Problem“ und „Change“ nachverfolgt. Für andere Tabellen muss das Auditing manuell aktiviert werden. **Importprotokolle** Sie können detaillierte Informationen zur Datenimportaktivität in Ihre Instanz anzeigen, indem Sie die Importprotokolle überprüfen. Diese Protokolle enthalten Informationen zu Quelle und Status, Zeit usw. **Protokolle ausgehender Webservices** Diese zeigen die REST- und SOAP-Anforderungsaktivität an und können Ihnen helfen, das Volumen und das Ziel von Verbindungen zu externen Services nachzuverfolgen. Erfahren Sie mehr über Systemprotokolle in Systemprotokolle.
Monitor Anmeldefehlerraten überwachen und Warnungen erstellen	Überwachen Sie auf ungewöhnliche Aktivitäten wie eine hohe Anzahl fehlgeschlagener Anmeldungen, insbesondere innerhalb kurzer Zeitrahmen. Sie können Warnungen erstellen, um E-Mails zu senden, wenn ein von Ihnen definierter Schwellenwert überschritten wird. Erfahren Sie, wie Sie diese Schwellenwerte unter konfigurieren Indikatorschwellenwerte .
Sicherheitsereignisse überwachen	Überprüfen Sie **Dashboard „meine Sicherheitsmetriken“** Um die verfügbaren Sicherheitsmetriken für Ihre Instanz anzuzeigen, und legen Sie Schwellenwerte fest, um E-Mail-Benachrichtigungen für wichtige Aktivitäten zu generieren. Beispiele für bemerkenswerte Aktivitäten können sein: **Berechtigungseskalation** Unerwartete Änderungen an privilegierten Rollen wie Admin, ITIL_Admin oder anderen Rollen mit höheren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	Berechtigungen können auf verdächtige Aktionen hinweisen. **Fehlgeschlagene Anmeldungen** Ungewöhnliche Zahlen oder Muster fehlgeschlagener Anmeldungen können potenzielle Brute-Force-Versuche oder Passwortspray-Angriffe aufzeigen. **Administratoren und Benutzer mit hohen Berechtigungen hinzugefügt** Die Erstellung eines neuen Administratoraccounts sollte auf Gültigkeit überprüft werden, um Versuche eines nicht autorisierten privilegierten Zugriffs zu verhindern.
Härtungs-Compliance-Stufe Ihrer Instanz überwachen	Stellen Sie sicher, dass Ihre Instanzen mit den neuesten Sicherheitshärtungsmetriken konform sind, indem Sie das Härtungstool im Sicherheitscenter verwenden. Greifen Sie in einer Instanz außerhalb der Produktion auf dieses Tool zu. Bewerten Sie die Auswirkungen auf Ihre Umgebung. Idealerweise sollte die Punktzahl so nahe wie möglich bei 100 % mit einer Mindestpunktzahl von 83 % liegen, ohne die Produktfunktionalität zu beeinträchtigen. Weitere Informationen zum Tool für Härtungseinstellungen des Sicherheitszentrums finden Sie unter Härtungseinstellungen.
Verweisen Sie Ihre Entwickler auf den Leitfaden für sichere Codierung	Stellen Sie mithilfe sicherer Codierungspraktiken sicher, dass Ihre Instanz so sicher und gegen nicht autorisierten Zugriff geschützt ist. Der Leitfaden für sichere Codierung von ServiceNow für Instanzentwickler bietet einen Überblick über die von ServiceNow angebotenen GlideScriptable-Klassen und -Methoden im Zusammenhang mit der Anwendungssicherheit. Dieser Leitfaden soll Entwickler beim Erstellen und Ändern des Codes in der Zielinstanz unterstützen und Schulen. Lesen Sie den Leitfaden unter Leitfaden für sichere ServiceNow-Codierung für Instanzentwickler .
Entfernen Sie das Kontrollkästchen „mich speichern“	Helfen Sie, unerwünschten Zugriff auf Ihre Instanz zu verhindern, indem Sie deaktivieren **Merken Sie Sich** Funktion. Wenn diese Funktion aktiv ist, speichert sie ein Cookie auf dem Computer des Anwenders, das den Anwender bei nachfolgenden Besuchen automatisch authentifiziert. Dies kann zu Sicherheitsproblemen führen, wenn Anwender über einen unsicheren Endpunkt, z. B. einen gemeinsam genutzten Computer, auf Ihre Instanz zugreifen. Erfahren Sie mehr über diese Funktion und wie Sie sie in deaktivieren Anwendernamen speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
Zugriff auf Ihre Instanz von unbekannten IP-Adressen einschränken	Verhindern Sie nicht autorisierten Zugriff auf Ihre Instanz, indem Sie den Zugriff von IP-Adressen beschränken, die nicht mit Ihrer Organisation verbunden sind. Jeder, der versucht, über eine nicht autorisierte IP-Adresse auf die Instanz zuzugreifen, wird abgelehnt. Wenn Sie diesen Ansatz verwenden, sollten Sie erwägen, nur externe Gateway- oder Web-Proxy-Adressen sowie Adressen zuzulassen, von denen aus Ihre Anwender auf die Instanz zugreifen, einschließlich Remoteanwender. Sie können sowohl den ausgehenden als auch den eingehenden Zugriff nach IP-Adresse einschränken. Erfahren Sie in, wie Sie den Zugriff auf Ihre Instanz nach IP-Adresse einschränken können Plugin „Zugriff auf bestimmte IP-Bereiche einschränken“ [aktualisiert in Security Center 1,3].
Überprüfen ServiceNow Anleitung zu Passwortspray-Angriffen	Schützen Sie Ihre Instanz vor Passwortspray-Angriffen. Diese Angriffe versuchen, Zugriff zu erhalten, indem sie ein häufig verwendetes Passwort für mehrere Accounts nacheinander testen. Erfahren Sie mehr über Sprayangriffe und wie Sie Ihre Instanzen in davor schützen können Strategien Zur Minderung Von Passwortspray-Angriffen .
Überprüfen Sie das gemeinsam genutzte Sicherheitsmodell	Verstehen Sie Ihre gemeinsam genutzte Rolle als Kunde bei der Aufrechterhaltung der Sicherheit Ihrer Instanzen, indem Sie das Modell für geteilte Verantwortlichkeit überprüfen. Das Modell für geteilte Verantwortlichkeit definiert die Partnerschaft zwischen und dem Kunden, beide mit bestimmten Verantwortlichkeiten. Weitere Informationen finden Sie unter ServiceNow – Modell für geteilte Verantwortung .
Protokolldaten aus der Instanz zur Archivierung und als Referenz übertragen	Archivieren Sie Ihre Protokolldaten, um sie über den standardmäßigen 21-tägigen Protokollrotationszeitraum hinaus zu behalten. Diese Archivierung kann mithilfe von Webserviceanforderungen, der Datenexportfunktion, dem MID-Server oder dem Protokollexportservice aus dem Vault-Paket erfolgen. Verwenden Sie die folgenden Ressourcen, um mehr über diese Methoden zu erfahren: • Webservices • Erkunden Protokollexportservice(LES)
Verschlüsselungsmodule mit RBAC verwenden, um die	Erfahren Sie, wie Sie das Key Management Framework (KMF) verwenden, um die Daten in Ihrer Instanz mithilfe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
Datenzugriffssteuerung weiter zu verbessern	der rollenbasierten Zugriffssteuerung (RBAC) zu schützen. KMF verwendet kryptografische Module, mit denen Sie definieren können, welche Daten in Ihrer Instanz verschlüsselt werden und welche Verschlüsselungsmethode verwendet werden soll. Mit mehreren Modulen können Sie verschiedene Bereiche Ihrer Instanz mit unterschiedlichen Spezifikationen verschlüsseln. Erfahren Sie, wie KMF und seine Komponenten zum Verschlüsseln Ihrer Daten in verwendet werden Erkunden Sie das Key Management Framework. Erfahren Sie mehr über kryptografische Module in Kryptografisches Modul – Übersicht.
Verwendung der zertifikatsbasierten Authentifizierung mit Integrationsanbietern	Konfigurieren Sie Datenverkehr zu Ihren Integrationsanbietern mithilfe von REST-/SOAP-Verbindungen, um die zertifikatbasierte Authentifizierung zu verwenden. Die SSL-Zertifikatauthentifizierung (Secure Socket Layer) verschlüsselt Daten während der Übertragung und verhindert so, dass sie beim Senden gelesen werden. Weitere Informationen zu dieser Konfiguration finden Sie in Konfigurieren Sie die gegenseitige Authentifizierung.
SAML-Authentifizierung verwenden	Integrieren Sie die Multifaktor-Authentifizierung (MFA) von Drittparteien mit Ihrem vorhandenen SAML-IdP, um zusätzliche Anmeldesicherheit zu bieten. MFA bietet ein hohes Sicherheitsniveau, da die Authentifizierung mehrere Authentifizierungsfaktoren erfordert. Etwas, das der Anwender kennt (das Passwort), sowie etwas, das er besitzt (ein einmaliger Code, der von einem MFA-Token oder Mobiltelefon erstellt wird, oder biometrische Attribute, z. B. Fingerabdrücke). ServiceNow Unterstützt die direkte MFA-Integration mit lokalen Accounts, LDAP, SSO mit SAML, OIDC oder Digest. Die adaptive Authentifizierung ist eine Voraussetzung für SSO mit der MFA. MFA kann für angegebene Anwender und angegebene Rollen aktiviert und zur Anwenderfreundlichkeit konfiguriert werden. Beispielsweise können Sie erkannte Geräte für eine Anzahl von Stunden ausnehmen. Sie können Metriken für die MFA-Verwendung im Sicherheitscenter anzeigen. Erfahren Sie mehr über die SAML-Authentifizierung mit diesen Ressourcen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	• SAML 2,0-Konzepte • SAML 2,0-Konfiguration mit Multi-Provider-SSO
Verwenden Sie die Funktion „E-Mail-Filter“, um mit verdächtigen eingehenden Nachrichten umzugehen.	Erstellen Sie E-Mail-Filter, um Nachrichten herauszufiltern, die von als verdächtig markiert wurden ServiceNow Virenschutz. Zusätzlich zum Virenschutz analysiert Antivirus Protection E-Mails auf Malware und SPAM, bewertet und die Ergebnisse, die diese Informationen der Nachricht in x-Headern hinzufügen. Sie können diese Header als Kriterien für das Plugin „E-Mail-Filter“ verwenden, um bei Bedarf zu handeln. Erfahren Sie mehr über ServiceNow Virenschutzfunktion von in Antivirus-Scanning. Erfahren Sie unter, wie Sie E-Mail-Filter in Ihrer Instanz konfigurieren E-Mail-Filter .
Syslog-Probe zum Senden von Protokollen an Ihren SIEM	Verwenden Sie ServiceNow Syslog-Probe zum Senden von Protokollnachrichten von Ihrer Instanz an einen Security Information and Event Manager (SIEM). Ein SIEM ist eine Software oder ein Service von Drittanbietern, die für die Aktivitätsüberwachung und die Identifizierung von Sicherheitsereignissen verwendet werden kann. Erfahren Sie mehr über ServiceNow Syslog-Probe-Konfiguration unter Syslog-Probe .
Eigene ausgereifte E-Mail-Sicherheitsumgebung verwenden	Erwägen Sie die Verwendung Ihrer eigenen Infrastruktur (oder einer Drittpartei-Infrastruktur) zum Senden und Empfangen von instanzbezogenen E-Mails, und profitieren Sie von einer präziseren E-Mail-Kontrolle an den Grenzen. Mit Ihren eigenen SMTP-, POP3- oder IMAP-Servern können Sie steuern, wie E-Mails gefiltert und empfangen werden, bevor sie an Ihre Instanz gesendet werden. **Hinweis:** Die Konfiguration Ihrer eigenen E-Mail-Infrastruktur gilt als erweiterte E-Mail-Konfiguration und kann optional eine E-Mail-Infrastruktur von Drittanbietern über die OAuth 2,0-E-Mail-Authentifizierung verwenden. Weitere Informationen finden Sie in Ihrer eigenen E-Mail-Lieferantendokumentation und -Anweisungen.
Zugriff mit der Zugriffsanalyse validieren	Verwenden Sie ServiceNow Greifen Sie auf das Analysetool zu, mit dem Sie Berechtigungen für ausgewählte Anwender, Rollen oder Gruppen vergleichen und analysieren können. Sie können diese Informationen verwenden, um Zugriffsprobleme zu beheben, zu identifizieren, wer Zugriff auf Ihre vertraulichen Daten hat, und die richtige Zugriffsebene für Anwender in Ihrer Instanz zu bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Best Practice	Beschreibung
	Weitere Informationen zu den Vorteilen der Zugriffsanalyse finden Sie unter Zugriffsanalyse Erkunden.

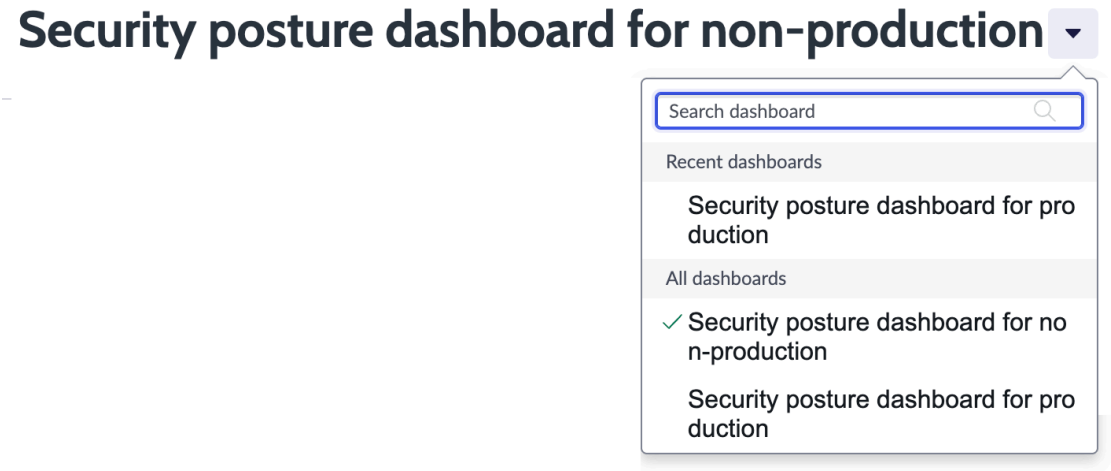
Dashboards zur Sicherheitslage

Verwenden Sie die anpassbaren Dashboards für ein- und Mehrinstanz-Sicherheitslage, um Ihre Sicherheits-KPIs zu überwachen. Diese Dashboards konsolidieren die wichtigen Informationen zur Sicherheit Ihrer Instanzen an einem zentralen Ort und enthalten eine Reihe von Basissystem-Dashboard-Widgets.

Zugriff auf die Dashboards zur Sicherheitslage

Um auf das Dashboard „Sicherheitslage“ zuzugreifen, öffnen Sie das Sicherheitscenter, indem Sie zu navigieren **Alle** > **Sicherheitscenter**an. Wählen Sie Aus **Sicherheitsstatus-Konsole** In **Sicherheitskonsolen** Abschnitt. Auf der **Sicherheitsstatus-Konsole** Seite auswählen **Dashboards zur Sicherheitslage** Oben.

Verwenden Sie den Abwärtspfeil neben **Dashboard „Sicherheitslage“** Zum Wechseln zwischen Instanz-Dashboards.



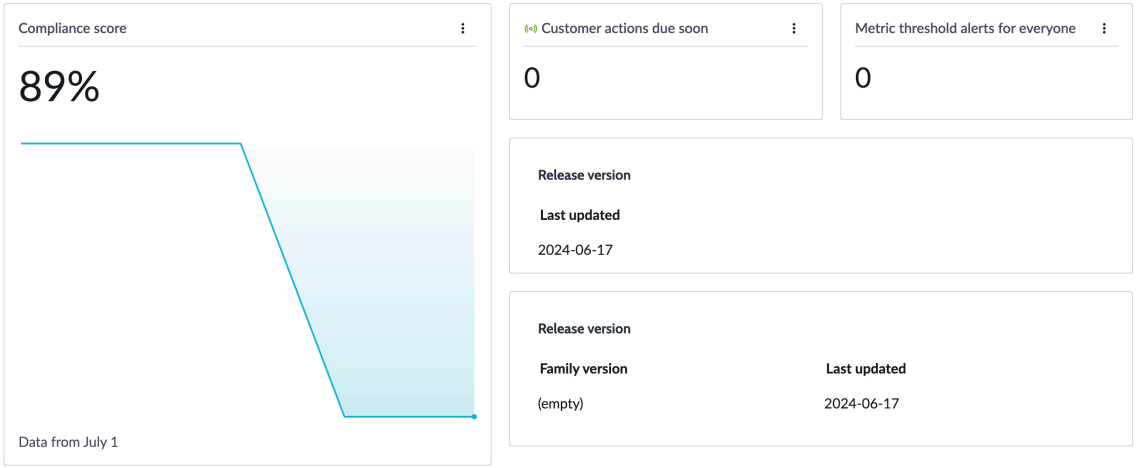
Das Dashboard ist in mehrere Abschnitte unterteilt, die Widgets enthalten, die sich auf einen Aspekt der Instanzsicherheit beziehen. Wählen Sie ein Widget im Dashboard aus, um weitere Details zu diesem Aspekt der Sicherheit Ihrer Instanz anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf einen Blick

At a glance



Die **Auf einen Blick** Abschnitt zeigt eine Übersicht über die Sicherheit einer Instanz an, z. B. Compliance-Punktzahl, fällige Kundenaktionen und Release-Informationen für die Instanz.

Compliance-Bewertung

Zeigt den Prozentsatz der Compliance-Punktzahl Ihrer Instanz im Zeitverlauf an, beginnend mit dem Datum, das am unteren Rand des Widgets ausgesät wird. Wählen Sie dieses Widget aus, um zu zu navigieren Compliance-Punktzahltrend für Härtung.

Metrikschwellenwertwarnungen für mich

Zeigt eine Anzahl der Datensätze des Metrikschwellenwertereignisses [n_vsc_metric_threshold_event] an, die dem aktuellen Anwender zugewiesen sind. Wählen Sie dieses Widget aus, um zu einer Liste dieser Datensätze zu navigieren.

Metrikschwellenwertwarnungen für alle.

Zeigt eine Anzahl von Datensätzen für nicht zugewiesene Metrikschwellenwertereignisse [n_vsc_metric_threshold_event] an. Wählen Sie dieses Widget aus, um zu einer Liste dieser Datensätze zu navigieren.

Demnächst fällige Kundenaktionen

Zeigt eine Anzahl der bald fälligen Kundenaktionen an. Wählen Sie dieses Widget aus, zu dem Sie navigieren möchten Kundenaktionen.

Von Virenschutz heruntergeladene Dateien

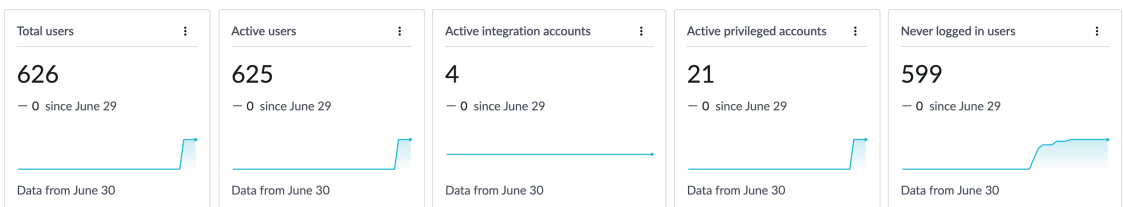
Zeigt eine Anzahl der in Ihre Instanz hochgeladenen Dateien an, die unter Quarantäne gestellt wurden. Wählen Sie dieses Widget aus, um diese Dateien in der Quarantäne anzuzeigen Virenschutz Abschnitt von Sicherheitsmetriken.

Freigabeversion

Zeigt die Familienversion der Instanz und das Datum der letzten Instanzaktualisierung an.

Anwender

Users



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Anwender** Abschnitt enthält Informationen zu den Anwendern in Ihrer Instanz. Die Widgets in diesem Abschnitt zeigen Anwenderinformationen und ein Liniendiagramm, das Änderungen an diesen Informationen im Laufe der Zeit anzeigt. Wählen Sie ein Widget aus, um weitere Details anzuzeigen.

Anwender insgesamt

Zeigt eine Anzahl von Anwendern in Ihrer Anwendertabelle [sys_user] an. Wählen Sie dieses Widget aus, um Details zu diesen Datensätzen in anzuzeigen Aktive Sitzungen Abschnitt von Sicherheitsmetriken.

Aktive Anwender

Zeigt eine Anzahl der aktiven Anwender in Ihrer Anwendertabelle [sys_user] an. Aktive Anwender sind Anwenderdatensätze, bei denen **Aktiv** Feld ist ausgewählt. Wählen Sie dieses Widget aus, um Details zu diesen Datensätzen in anzuzeigen Aktive Sitzungen Abschnitt von Sicherheitsmetriken.

Aktive Integrationsaccounts

Zeigt eine Anzahl von Integrationsaccounts in Ihrer Anwendertabelle [sys_user] an. Integrationsaccounts sind Anwenderdatensätze, in denen die **Nur Webservice-Zugriff** Feld ist ausgewählt. Wählen Sie dieses Widget aus, um Details zu diesen Datensätzen in anzuzeigen Aktive Sitzungen Abschnitt von Sicherheitsmetriken.

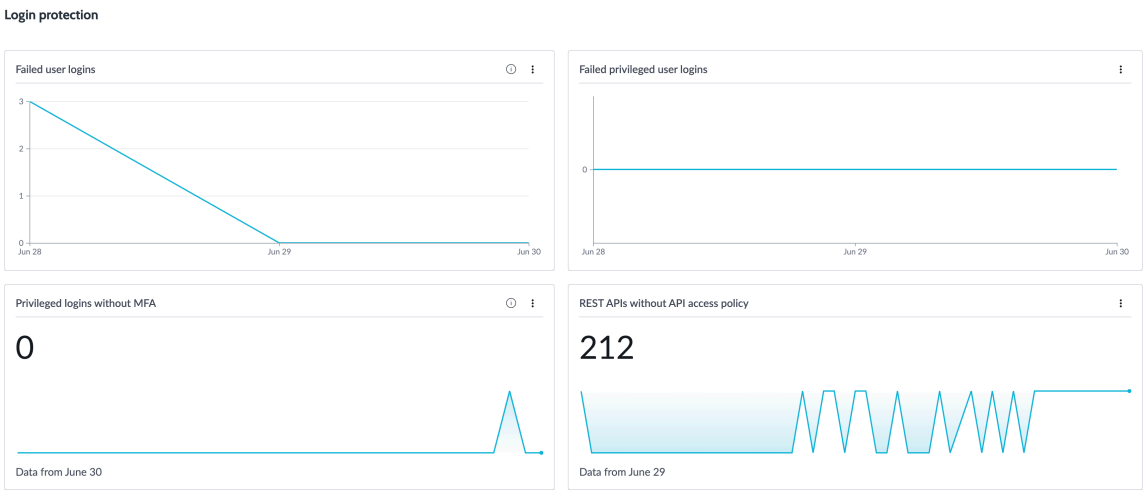
Aktive privilegierte Accounts

Zeigt eine Anzahl der aktiven privilegierten Anwender in Ihrer Anwendertabelle [sys_user] an. Privilegierte Anwender sind Anwenderdatensätze, in denen **Aktiv** Feld ist „wahr“, die **Interner Integrationsanwender** Ist falsch, und **Interner Integrationsanwender** Ist inaktiv. Wählen Sie dieses Widget aus, um Details zu diesen Datensätzen in anzuzeigen Aktive Sitzungen Abschnitt von Sicherheitsmetriken.

Nie angemeldete Anwender

Zeigt eine Anzahl von Anwendern in Ihrer Anwendertabelle [sys_user] an, die in den letzten 60 Tagen erstellt wurde und keinen Wert in haben **Zeitpunkt der letzten Anmeldung** Feld. Wählen Sie dieses Widget aus, um Details zu diesen Datensätzen in anzuzeigen Aktive Sitzungen Abschnitt von Sicherheitsmetriken.

Anmeldeschutz



Die **Anmeldeschutz** Abschnitt enthält Informationen zu fehlgeschlagenen Anmeldungen, einschließlich fehlgeschlagener Anmeldeversuche für privilegierte Anwender. Diese Widgets enthalten ein Liniendiagramm, das Änderungen an diesen Informationen im Laufe der Zeit anzeigt. Wählen Sie ein Widget aus, um weitere Details anzuzeigen.

Fehlgeschlagene Anwenderanmeldungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigt eine Anzahl der fehlgeschlagenen Anwenderanmeldungsversuche an. Wählen Sie dieses Widget aus, um zu navigieren, um Details zu fehlgeschlagenen Anmeldungen in anzuzeigen Sicherheitsmetriken.

Fehlgeschlagene Anmeldungen privilegierter Anwender

Zeigt eine Anzahl der fehlgeschlagenen Anwenderanmeldungsversuche von privilegierten Accounts an. Privilegierte Anwender sind Anwenderdatensätze, in denen **Aktiv** Feld ist „wahr“, die **Interner Integrationsanwender** Ist falsch, und **Interner Integrationsanwender** Ist inaktiv. Wählen Sie dieses Widget aus, um zu navigieren, um Details zu fehlgeschlagenen Anmeldungen in anzuzeigen Sicherheitsmetriken.

Privilegierte Anmeldungen ohne MFA

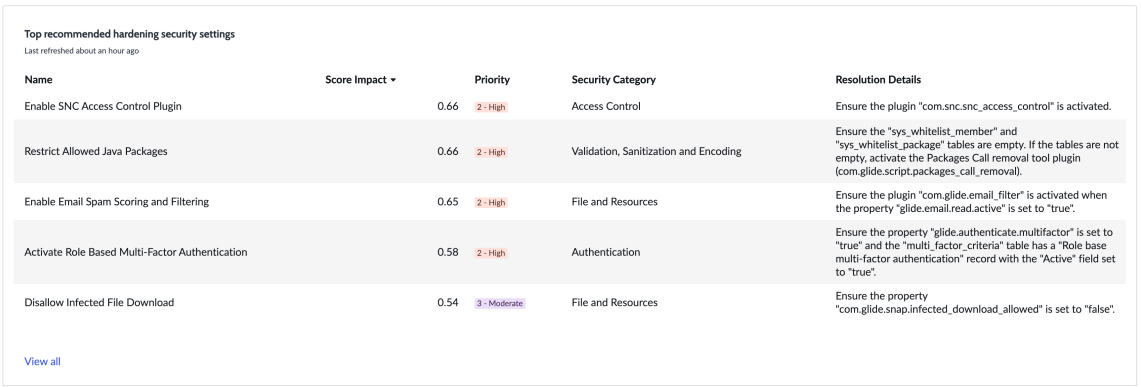
Zeigt eine Anzahl der privilegierten Accounts an, die nicht für die Multifaktor-Authentifizierung (MFA) konfiguriert sind. Wählen Sie dieses Widget aus, um zu einer Liste dieser Accounts in zu navigieren Sicherheitsmetriken.

REST APIs ohne API-Zugriffsrichtlinie

Zeigt eine Liste von REST-APIs an, die nicht durch eine API-Zugriffsrichtlinie eingeschränkt sind. Wählen Sie dieses Widget aus, um zu einer Liste dieser REST APIs in zu navigieren Sicherheitsmetriken.

Instanzhärtung

Instance hardening



Die **Instanzhärtung** Abschnitt enthält empfohlene Sicherheitseinstellungen für die Härtung, die Sie ändern können, um die Instanzsicherheit zu verbessern. Verwenden Sie diesen Abschnitt, um die Priorität und die potenziellen Auswirkungen dieser Changes anzuzeigen.

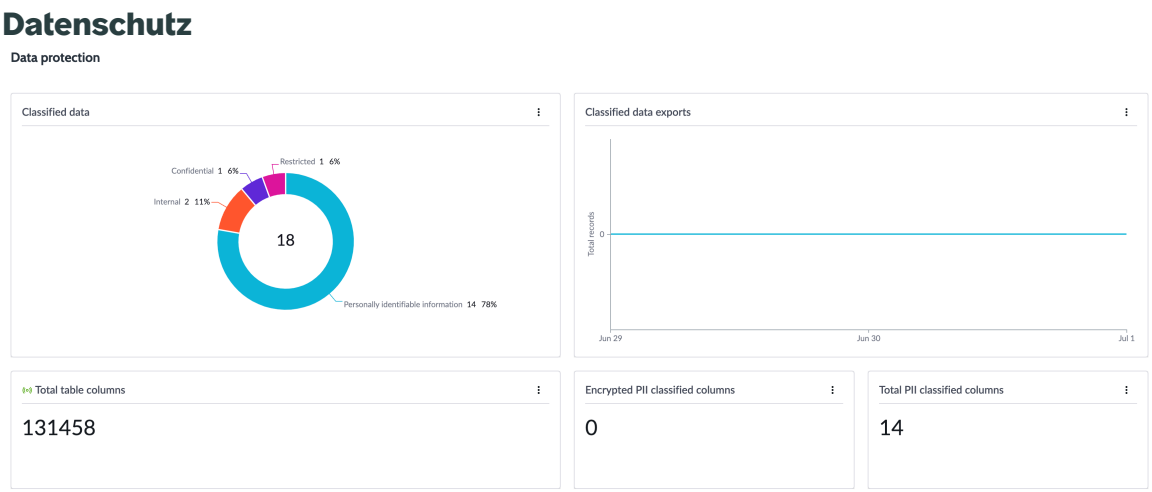
Instanztrends

Instance trends



Die **Instanztrends** Im Dashboard werden die Ergebnisse der Auditor-Scan-Suite für Zugriffssteuerungen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verwenden Sie **Datenschutz** Abschnitt, um eine Übersicht über klassifizierte Daten anzuzeigen, z. B. personenbezogene Daten. Das Dashboard verfolgt auch Exporte klassifizierter Daten.

Klassifizierte Daten

Zeigt ein Kreisdiagramm klassifizierter Daten in Ihrer Instanz an, getrennt nach Typ. Wählen Sie einen Abschnitt des Diagramms aus, um Details zu diesen Datensätzen anzuzeigen. Details zur Datenklassifizierung finden Sie unter Datenklassifizierung.

Klassifizierte Datenexporte

Zeigt eine Anzahl der klassifizierten Datensätze an, die aus Ihrer Instanz exportiert wurden. Wählen Sie dieses Widget aus, um eine Liste der klassifizierten Exporte in anzuzeigen Exportieren Abschnitt von Sicherheitsmetriken.

Gesamtzahl der Tabellenspalten

Zeigt eine Anzahl aller Spalten (Felder) in Tabellen in Ihrer Instanz an. Wählen Sie dieses Widget aus, um diese Spalten in zu überprüfen Datenklassifizierung Abschnitt von Sicherheitsmetriken.

Verschlüsselte PII-klassifizierte Spalten

Zeigt eine Anzahl der verschlüsselten Datensätze an, die als persönlich identifizierbare Informationen (PII) klassifiziert sind. Wählen Sie dieses Widget aus, um diese Datensätze in zu überprüfen Datenklassifizierung Abschnitt von Sicherheitsmetriken.

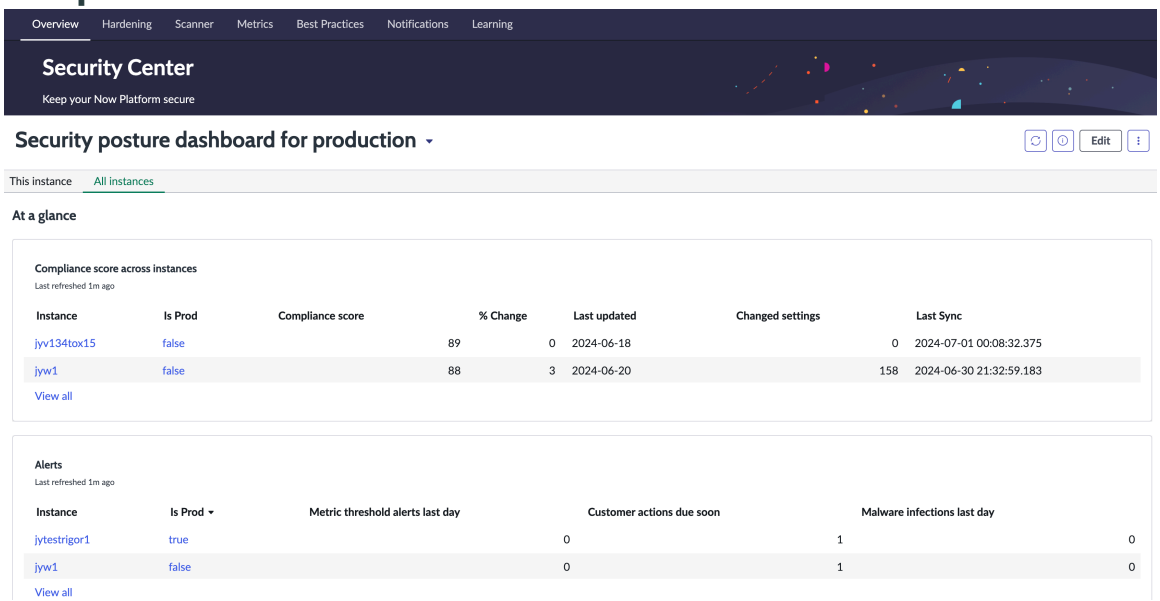
Insgesamt klassifizierte PII-Spalten

Zeigt eine Anzahl aller Datensätze an, die als persönlich identifizierbare Informationen (PII) klassifiziert sind. Wählen Sie dieses Widget aus, um diese Datensätze in zu überprüfen Datenklassifizierung Abschnitt von Sicherheitsmetriken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie mehrere Instanzen



Zeigen Sie die Sicherheitslage Ihrer nicht-Produktionsinstanzen an, ohne Ihre Produktionsinstanz mit zu verlassen **Alle Instanzen** Registerkarte oben im Dashboard. Die **Alle Instanzen** Auf der Registerkarte wird eine komprimierte Version derselben Informationen wie angezeigt **Diese Instanz** Registerkarte, enthält aber auch Daten aus allen Ihren nicht-Produktionsinstanzen.

Standardmäßig ist **Alle Instanzen** Die Registerkarte zeigt Informationen zur Produktionsinstanz, bei der Sie angemeldet sind, und zu allen Instanzen außerhalb der Produktion in allen Produktionsumgebungen an.

Sie können Instanzen hinzufügen oder entfernen, die in diesem Dashboard angezeigt werden, indem Sie Ihre Vertrauenskonfiguration ändern. Durch die Bereitstellung von Datentransparenz zwischen Instanzen können sie in Ihrem Dashboard angezeigt werden. Details zu diesem Vorgang finden Sie unter Grundlegende Vertrauenskonfiguration für Anwendungen zur Datensynchronisierung .

Dashboard-Anpassung

Das Dashboard zur Sicherheitslage der Instanz kann nicht angepasst werden, Sie können das Dashboard jedoch duplizieren, indem Sie auswählen **Weitere Aktionen** (⋮) Symbol und Auswahl **Duplikat** . Sie können das doppelte Dashboard ändern.

Sicherheitsaufgaben

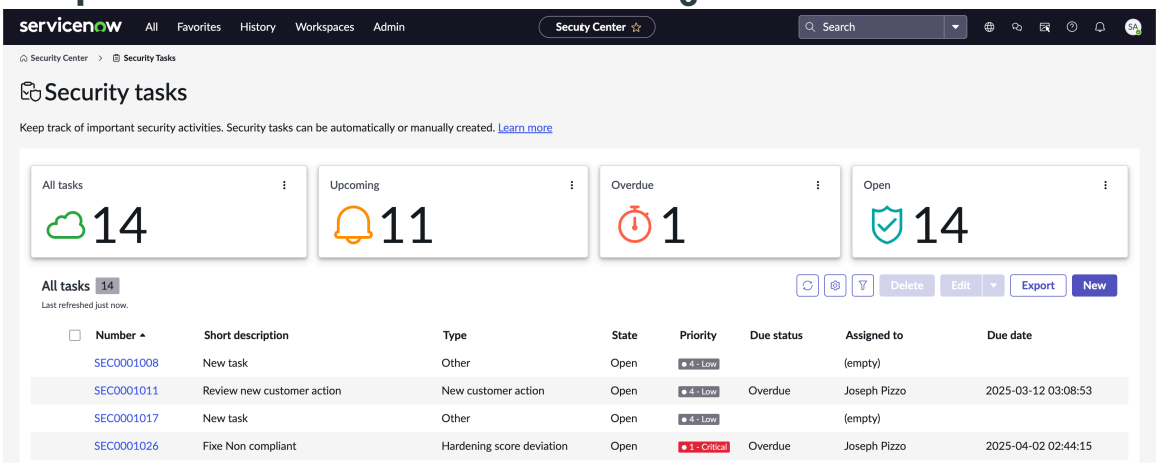
Verwenden Sie Sicherheitsaufgaben, um alle Ihre sicherheitsbezogenen Aufgaben an einem Ort zu überwachen, zu priorisieren und zuzuweisen.

Sparen Sie Zeit bei der Nachverfolgung und Organisation aller Aufgaben, die erforderlich sind, um die Sicherheitslage Ihrer Instanz mithilfe von Sicherheitsaufgaben zu verbessern und aufrechtzuerhalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen und verwalten Sie Sicherheitsaufgaben



Greifen Sie auf die Sicherheitsaufgaben zu, indem Sie zu navigieren **Alle** > **Sicherheitscenter** > **Sicherheitsaufgaben**an. Standardmäßig werden alle Aufgaben in der Liste angezeigt. Sie können anstehende, überfällige oder offene Aufgaben einfach filtern, indem Sie die Karten über der Liste auswählen. Diese Karten zeigen auch die aktuelle Anzahl der Aufgaben in jeder dieser Kategorien an. Sie können Ihren Filter weiter verfeinern, indem Sie die Filteroptionen für normale Tabellenfelder verwenden und dann die Filterschaltfläche ( ) Und dann die Schaltfläche Erweiterte Ansicht auswählen, um anwenderdefinierte Filter zu erstellen und zu speichern, die später verwendet werden sollen.

Anwenderrollen

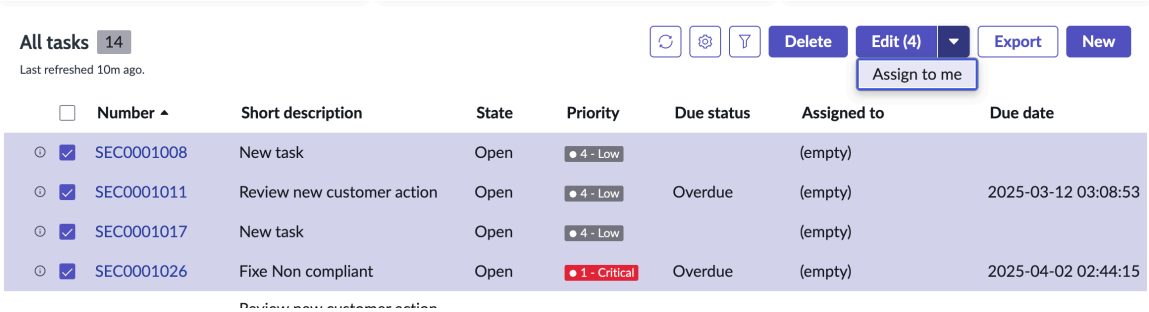
Die Sicherheitsaufgaben verwenden die folgenden Rollen:

Anwender	Erforderliche Rolle	Beschreibung
Systemadministrator	Administrator	Systemadministratoren können Sicherheitsaufgaben anzeigen, erstellen, zuweisen und löschen.
Sicherheitscenter-Viewer	sn_vsc_Security_Center_Viewer	Viewer können Sicherheitsaufgaben anzeigen, aber nicht erstellen, löschen oder bearbeiten.
Sicherheitsaufgaben-Manager	sn_vsc_Task_Manager	Sicherheitsaufgaben-Manager können an zugewiesenen Aufgaben arbeiten, Aufgabenmanager-bezogene Seiten anzeigen und Aufgaben im Sicherheitscenter erstellen und verwalten. Sie können Aufgaben anzeigen, die anderen Anwendern zugewiesen sind, aber keine Aufgaben bearbeiten, die anderen Anwendern zugewiesen sind. Aufgabenmanager können im Sicherheitscenter nicht auf Seiten ohne Aufgabenmanager zugreifen.
ITIL	ITIL	ITIL-Anwender können mit Sicherheitsaufgaben interagieren, die ihnen zugewiesen sind, können jedoch nicht alle Aufgaben anzeigen, wie dies die Rollen „Administrator“ und „Sicherheitsaufgaben-Manager“ tun.

Weisen Sie sich schnell Sicherheitsaufgaben zu

Verwenden Sie die Kontrollkästchen links neben den Elementen in der Liste, um mehrere Elemente auszuwählen. Wenn eine von mehreren Aufgaben ausgewählt ist, können Sie verwenden **Löschen** Schaltfläche zum Löschen der ausgewählten Aufgaben oder **Bearbeiten** Schaltfläche, um sich die ausgewählten Aufgaben selbst zuzuweisen.

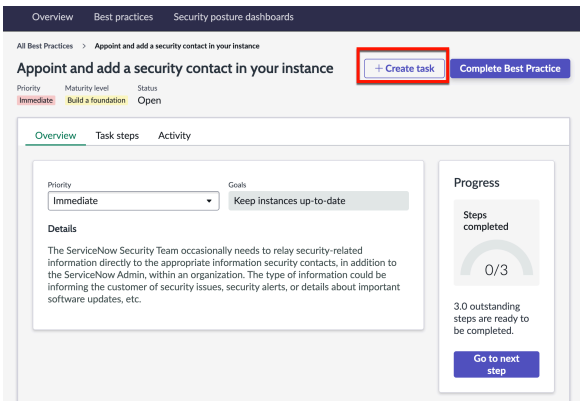
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

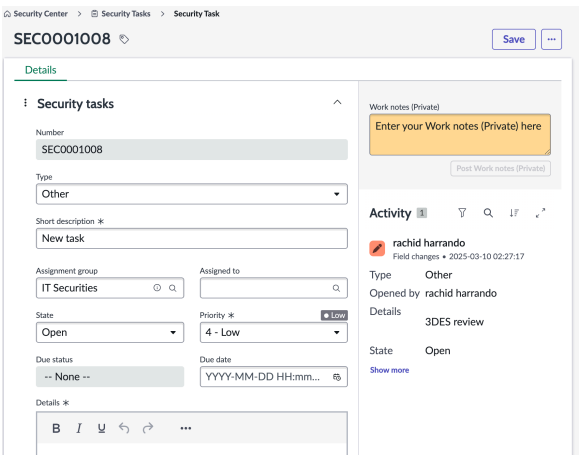


Erstellen Sie Sicherheitsaufgaben

Erstellen Sie eine Sicherheitsaufgabe mit **+Aufgabe Erstellen** Schaltfläche, die auf verschiedenen Sicherheitsseiten der Plattform verfügbar ist.

Beispielsweise kann der Administrator im Sicherheitscenter auf der Detailseite des Best Practices-Tools auswählen **+Aufgabe Erstellen** Schaltfläche zum Erstellen und Zuweisen einer Aufgabe zum Abschließen dieser Best Practice.





Automatisch generierte Aufgaben

Sicherheitsaufgaben können automatisch generiert werden. Die automatische Generierung von Sicherheitsaufgaben wird durch ein zugehöriges Ereignis ausgelöst, das auf der Plattform aufgetreten ist. Weitere Informationen zu generierten Sicherheitsaufgaben finden Sie in Automatische Generierung von Sicherheitsaufgaben.

Bearbeiten und weisen Sie Sicherheitsaufgaben zu

Bearbeiten Sie Sicherheitsaufgaben, um sie Anwendern zuzuweisen, Fälligkeitsdaten zu definieren und den Anwendern, die diese Aufgaben ausführen, zusätzliche Details bereitzustellen. Details finden Sie unter Bearbeiten Sie Sicherheitsaufgaben.

Exportaufgaben

Sie können Sicherheitsaufgaben in das Format Ihrer Wahl exportieren. Details finden Sie unter Exportieren Sie Sicherheitsaufgaben.

Automatische Generierung von Sicherheitsaufgaben

Erfahren Sie, wie und wann Ihre Instanz Sicherheitsaufgaben generiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisch generierte Sicherheitsaufgaben

Sicherheitsaufgaben können automatisch generiert werden. Die automatische Generierung von Sicherheitsaufgaben wird durch ein zugehöriges Ereignis ausgelöst, das auf der Plattform aufgetreten ist. Zum Beispiel:

Metrikschwellenwert überschritten

Eine Sicherheitsaufgabe wird für eine Metrik generiert, wenn ihr Schwellenwert überschritten wird. Es gibt nur eine offene Aufgabe für eine Metrik, auch wenn dieselbe Metrik mehrere Verstöße aufweist. Wenn eine Sicherheitsaufgabe für eine nicht eingehaltene Metrik geschlossen wird, wird eine neue Aufgabe generiert, wenn der Schwellenwert erneut überschritten wird.

Benachrichtigung zu Ereignis

Eine Sicherheitsaufgabe wird generiert, wenn eine Benachrichtigung über ein Sicherheitsereignis ausgelöst wird (erfüllt die Bedingungen der Richtlinie). Wie bei Metriken gibt es nur eine offene Aufgabe für eine Richtlinie, wobei eine neue Aufgabe generiert wird, wenn die vorherige geschlossen wird, und die Benachrichtigung wird erneut ausgelöst. Weitere Informationen zu Benachrichtigungen zu Sicherheitsereignissen finden Sie unter Benachrichtigungen zu Sicherheitsereignissen.

Abweichung der Härtungspunktzahl

Wenn die Härtungspunktzahl unter den konfigurierten Schwellenwert (Standard 3) absinkt, wird eine Sicherheitsaufgabe generiert. Wenn die Härtungspunktzahl beispielsweise 97 und am nächsten Tag 94 beträgt, wird eine Sicherheitsaufgabe erstellt, kurz nachdem die Punktzahl 94 berechnet wurde. Es wird nur eine einzelne offene Aufgabe erstellt. Die Plattform generiert keine weitere Aufgabe, wenn die Punktzahl am nächsten Tag erneut von 94 auf 91 absinkt. Weitere Informationen zu Ihrer Härtungspunktzahl finden Sie unter Compliance-Punktzahltrend für Härtung.

Kundenaktion

Eine Sicherheitsaufgabe wird generiert, wenn eine Kundenaktion installiert wird. Details zu Kundenaktionen finden Sie unter Kundenaktionen.

Bannerankündigung

Für jede neue Bannerankündigung wird eine Sicherheitsaufgabe generiert. Weitere Informationen zu Bannerankündigungen finden Sie unter Sicherheitsbanner-Ankündigungen.

Automatisch generierte Sicherheitseinstellungen

Konfigurationsoptionen für automatisch generierte Sicherheitsaufgaben finden Sie auf der Seite mit den Sicherheitscenter-Eigenschaften. Suchen Sie diese Einstellungen, indem Sie zu navigieren **Alle** > **Sicherheitscenter** > **Sicherheitscenter – Eigenschaften**an.

Automatisierte Sicherheitsaufgaben aktivieren/deaktivieren

Wenn **Ja/Nein** Feld ist ausgewählt, automatisierte Sicherheitsaufgaben sind in Ihrer Instanz aktiviert.

Schwellenwert für Verschlechterung der Härtungspunktzahl

Der Wert im Feld stellt den Betrag dar, um den die Härtungspunktzahl abwerten muss (seit der letzten täglichen Punktzahl), um eine Sicherheitsaufgabe zu generieren. Dieser Wert muss eine positive Ganzzahl sein. Der Standardwert ist 3.

Bearbeiten Sie Sicherheitsaufgaben

Erfahren Sie, wie Sie Sicherheitsaufgaben im Sicherheitscenter erstellen, bearbeiten, löschen oder exportieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin oder sn_vsc_Task_Manager

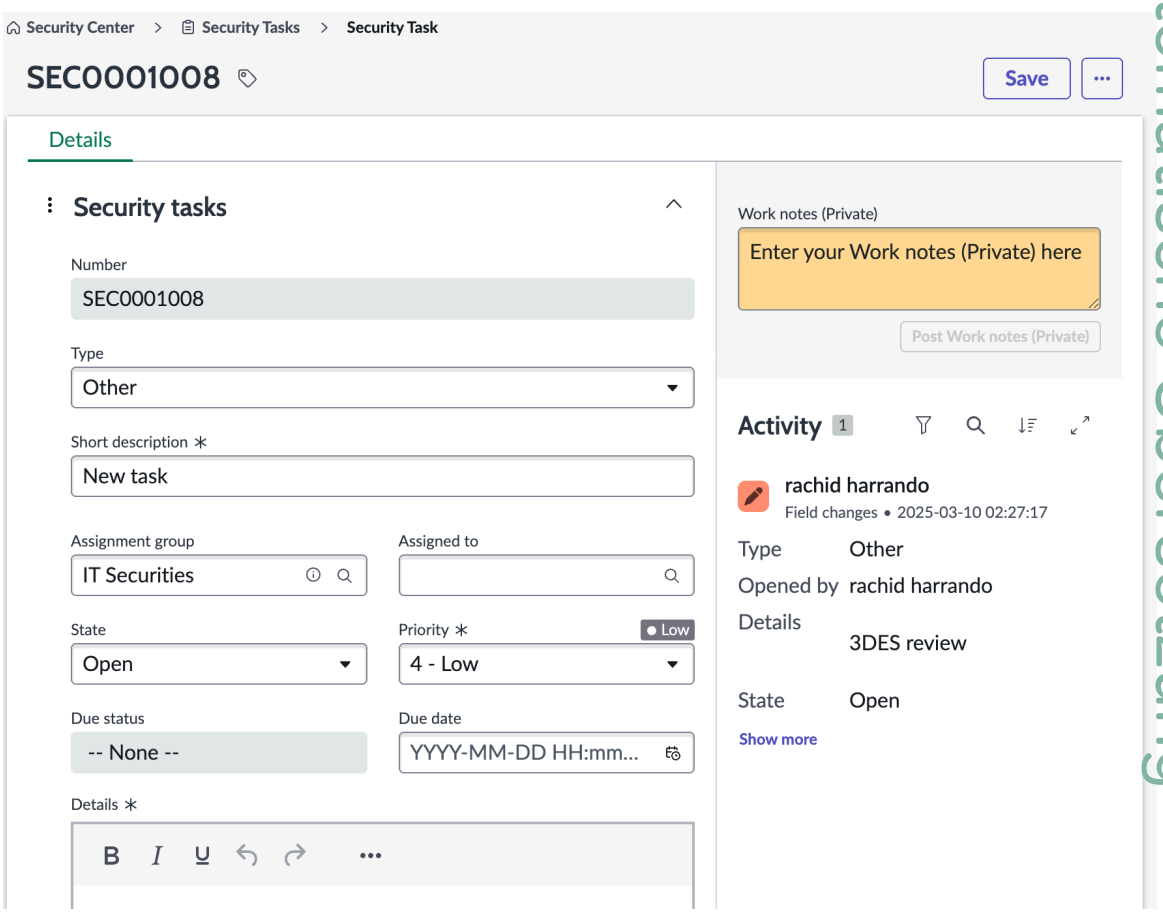
Prozedur

1. Greifen Sie auf Ihre Sicherheitsaufgabenliste zu, indem Sie zu navigieren **Alle** > **Sicherheitscenter** > **Sicherheitsaufgaben**an.
2. In der Liste „Sicherheitsaufgabe“ können Sie Ihre Sicherheitsaufgaben auf zwei Arten bearbeiten:

Bearbeiten Sie im Formular „Sicherheitsaufgabe“

Wählen Sie eine Sicherheitsaufgabennummer aus der Liste aus, um den Sicherheitsaufgabendatensatz zu öffnen und seine Details anzuzeigen. Hier können Sie Arbeitsnotizen bearbeiten, einem anderen Anwender zuweisen und hinzufügen.

Wichtig: Denken Sie daran, dass Anwender, denen Aufgaben zugewiesen sind, Administratoren sein oder über die Rolle sn_vsc_Task_Manager verfügen müssen.

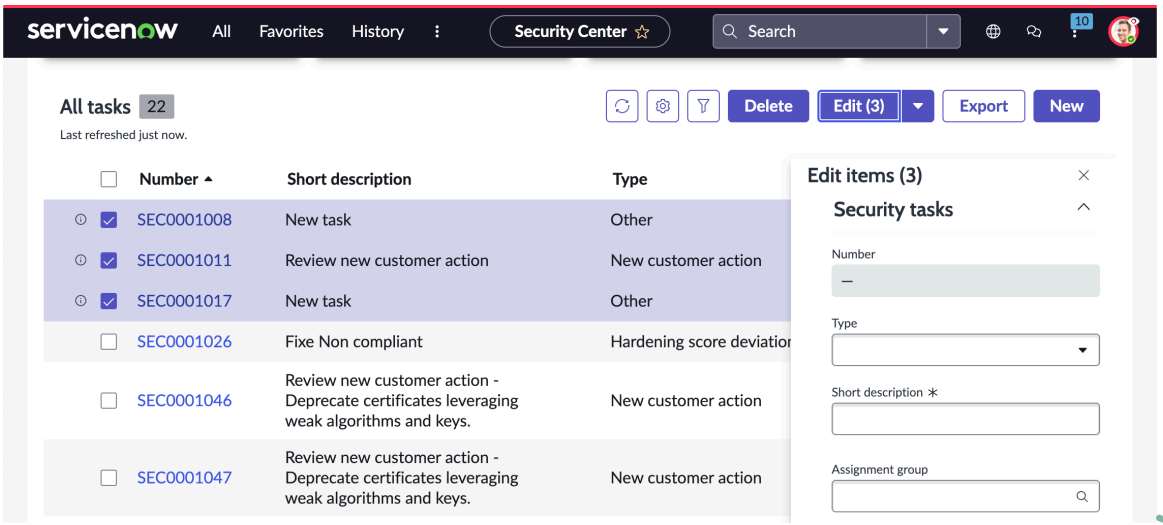


Bearbeiten Sie in der Liste „Sicherheitsaufgabe“

Wählen Sie eine oder mehrere Sicherheitsaufgaben aus, indem Sie das entsprechende Kontrollkästchen auf der linken Seite aktivieren, und wählen Sie dann aus **Bearbeiten** Schaltfläche.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Füllen Sie die Felder nach Bedarf aus:

Feld	Beschreibung
Anzahl	Automatisch generierte Nummer, die zur Identifizierung der Aufgabe verwendet wird
Typ	Wählen Sie einen Aufgabentyp aus: ○ Metrikschwellenwert überschritten ○ Neue Kundenaktion ○ Benachrichtigung zu Ereignis ○ Abweichung der Härtungspunktzahl ○ Neue Bannerankündigung
Kurzbeschreibung	Kurze Beschreibung der Aufgabe
Zuweisungsgruppe	Zuweisungsgruppe für die Aufgabe
Zugewiesen an	Person, die der Aufgabe zugewiesen ist. Dieser Anwender muss sich in der in ausgewählten Zuweisungsgruppe befinden **Zuweisungsgruppe** Und haben die *admin*Oder *sn_vsc_task_manager*Rolle.
Status	Status der Aufgabe: ○ Ausstehend ○ Offen ○ In Bearbeitung ○ Geschlossen ○ Abgebrochen
Priorität	Priorität der Aufgabe: ○ 1 – Kritisch ○ 2: Hoch ○ 3: Mittel ○ 4: Niedrig

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Fälliger Status	Gibt an, ob die Aufgabe ist **Bevorstehend** Oder **Überfällig** , Abhängig vom Datum in **Fälligkeitsdatum** Feld.
Fälligkeitsdatum	Datum und Uhrzeit, bis zu der die Aufgabe abgeschlossen sein muss.
Details	Wird verwendet, um Details, Links oder andere Informationen bereitzustellen, die Anwender über diese Aufgabe wissen müssen.
Arbeitsnotizen	Hinweise zu dieser Aufgabe. Notizen, die in dieses Feld eingegeben werden, werden mit einem Zeitstempel versehen und in der Aktivitätenliste auf der rechten Seite des Bildschirms angezeigt.
Arbeitsnotizen (privat)	Arbeitsnotizen können privat hinzugefügt werden, indem sie in dieses Feld eingegeben und ausgewählt werden **Arbeitsnotizen veröffentlichen (privat)** Schaltfläche.

4. Wählen Sie Aus **Speichern** Um den Sicherheitsaufgaben-Datensatz zu speichern, wählen Sie aus, wenn Sie einen Datensatz aus der Liste bearbeiten **Aktualisieren** .
5. **Wahlweise:** Bei Bedarf können Sie eine Aufgabe aus der Liste löschen, indem Sie auf der rechten Seite das entsprechende Kontrollkästchen aktivieren und auswählen **Löschen** , Oder im Formular, indem Sie auf das Symbol „mehr“ (...) und dann auf klicken **Löschen** .

Exportieren Sie Sicherheitsaufgaben

Erfahren Sie, wie Sie Sicherheitsaufgaben in Dateien exportieren, die Sie herunterladen und in anderer Software verwenden können.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Greifen Sie auf Ihre Sicherheitsaufgabenliste zu, indem Sie zu navigieren **Alle** > **Sicherheitscenter** > **Sicherheitsaufgaben**an.
2. Wählen Sie eine oder mehrere Sicherheitsaufgaben aus, indem Sie das entsprechende Kontrollkästchen auf der linken Seite aktivieren
3. Wählen Sie aus **Exportieren** Schaltfläche.
4. Unter **Dateityp** , Wählen Sie das Dateiformat aus, in das die Sicherheitsaufgaben exportiert werden sollen. Sie können aus Excel-, CSV-, JSON- oder PDF-Formaten auswählen.
5. Unter **Liefertyp** , Wählen Sie eine der beiden aus **Herunterladen** Oder **E-Mail** .

   Herunterladen

   Die Exportdatei wird mit Ihrem Browser heruntergeladen.

   E-Mail

   Die **E-Mail** Feld wird angezeigt. Geben Sie eine E-Mail-Adresse in ein **E-Mail** Und die Exportdatei wird an die angegebene E-Mail-Adresse geliefert.

Sicherheitslernen

Greifen Sie über eine einzelne Seite auf Sicherheitslernmaterialien zu.

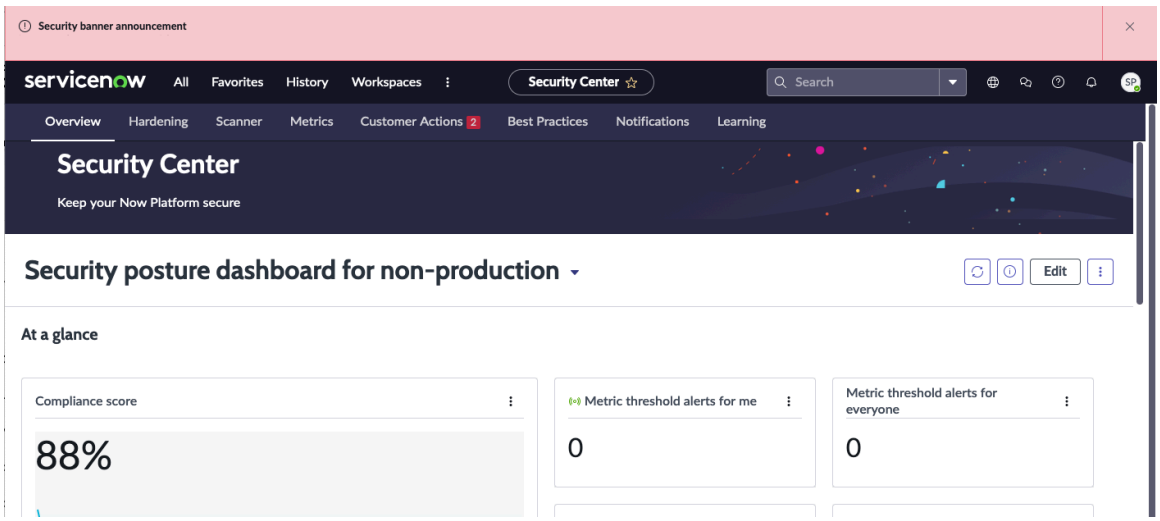
Lesen Sie Sicherheits-White Papers, E-Books, Knowledge Base-Artikel (KB), Produktdokumentation und Community-Diskussionen aus einer konsolidierten Ansicht,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

indem Sie zu navigieren **Lernen** . Der Inhalt ist nach Überschriften und beschreibenden UI-Karten organisiert, damit Sie schnell die richtige Ressource finden können.

Sicherheitsbanner-Ankündigungen

Aktivieren Sie Sicherheitsbanner-Ankündigungen, um über dringende und kritische Sicherheitswarnungen auf dem Laufenden zu bleiben, indem Sie Banner mit hoher Sichtbarkeit verwenden, die für Administratoren in der Instanz-UI sichtbar sind.

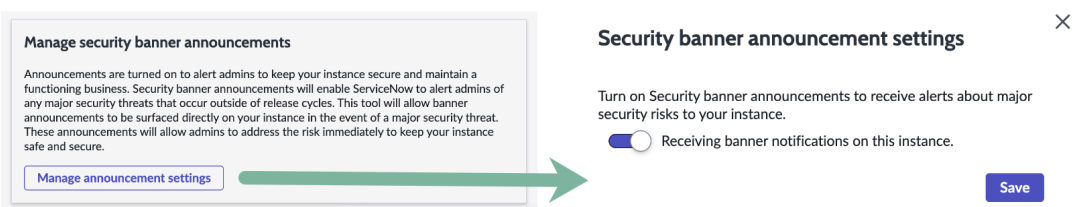


Sicherheitsbanner-Ankündigungen sind Ankündigungen, die Kundenadministratoren angezeigt werden und von gesendet werden ServiceNow, Um Sie über Korrekturen für potenzielle Sicherheitsbedrohungen, die kürzlich erkannt wurden, auf dem Laufenden zu halten. Diese Warnungen enthalten eine Zusammenfassung des Sicherheitsrisikos und einen Link, über den Sie mehr erfahren und handeln können, um Ihre Instanz zu sichern.

Administratoren können Banner schließen, indem sie die Schaltfläche „Schließen“ (x) wählen. Das Banner wird jedoch bei jeder neuen Sitzung erneut angezeigt, bis das Ablaufdatum des Banners überschritten ist. Administratoren können Banneranküngigungen deaktivieren, indem sie den Systemeigenschaftswert sn_vsc.configure_Customer_Push_action auf „falsch“ setzen.

Aktivieren oder deaktivieren Sie Sicherheitsbanner-Ankündigungen

Die Sicherheitsbanner-Funktion ist standardmäßig aktiviert. Um Sicherheitsbanner-Ankündigungen zu aktivieren oder zu deaktivieren, navigieren Sie zu **Systemsicherheit** > **Sicherheitscenter** > **Benachrichtigungen**an. Wählen Sie auf dieser Seite die aus **Verwalten Sie Ankündigungseinstellungen** Schaltfläche.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanz-Sicherheitszentrum

Überwachen Sie die Compliance-Ebene von Instanzsicherheitskontrollen, zeigen Sie Überwachungsmetriken für Sicherheitsereignisse an, und konfigurieren und verwalten Sie Instanzsicherheitseinstellungen – alles im Instanz-Sicherheitszentrum. Das Instanz-Sicherheitszentrum konsolidiert mehrere wichtige Sicherheitskomponenten in einer einzigen Steuerungskonsole, mit der Sie instanzbasierte Sicherheitsereignisse erkennen, schützen und darauf reagieren können.

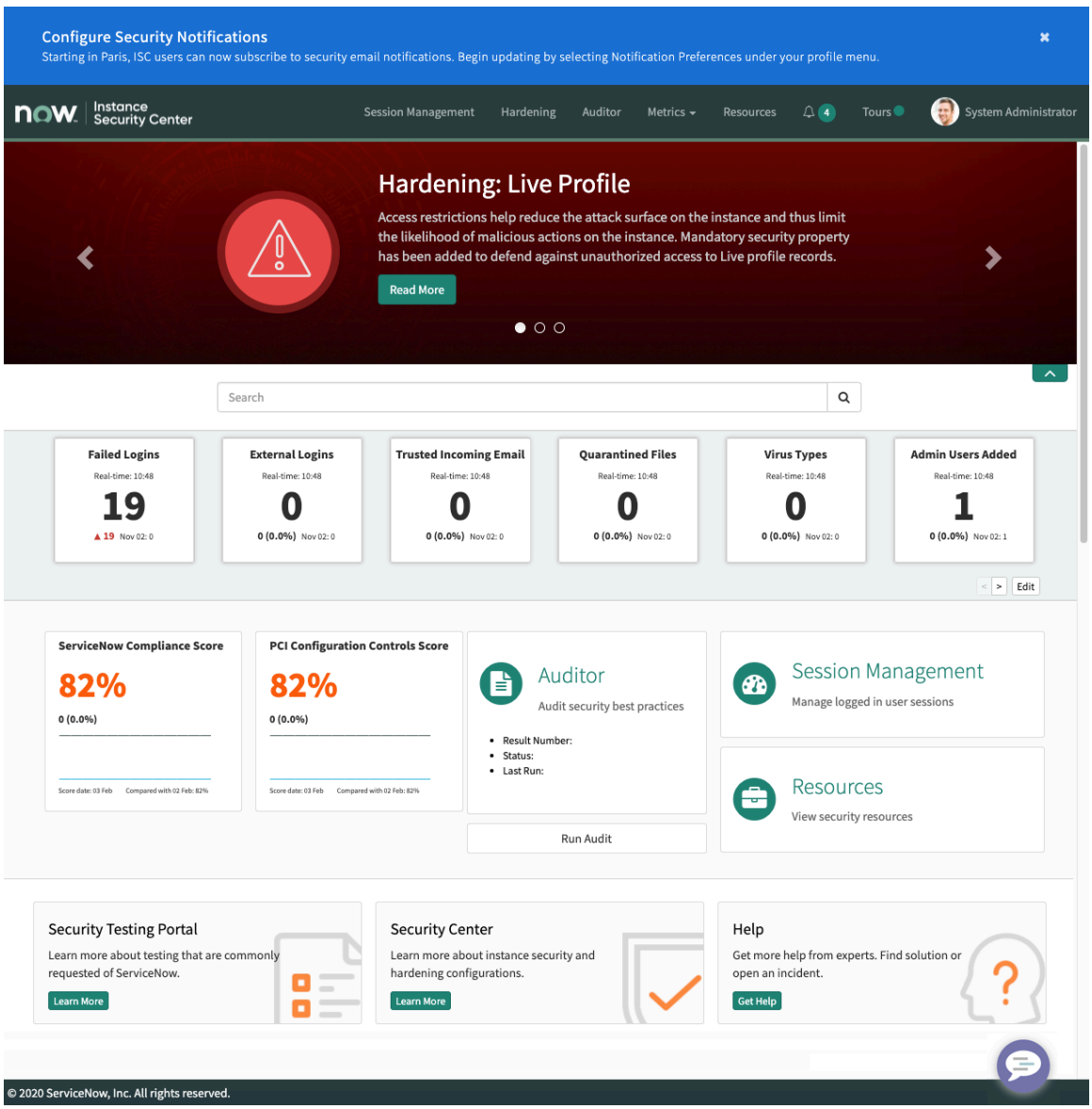
Wichtig:

Das Instanzsicherheitszentrum (ISC) hat das Ende des Verkaufs im September 2024 erreicht und wird nicht mehr unterstützt oder steht für eine neue Aktivierung zur Verfügung.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Instanz-Sicherheitszentrum an ServiceNow Security Center Migration.

Komponenten des Instanz-Sicherheitszentrums

Um auf das Instanz-Sicherheitszentrum zuzugreifen, navigieren Sie zu **Systemsicherheit** > **Instanz-Sicherheitszentrum** Oder auf der Systemadministration-Homepage.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Homepage des Instanz-Sicherheitszentrums enthält die folgenden Sicherheitskomponenten:

- Administratornachrichten
- Rotierendes Sicherheitsbanner
- Suchen
- Menüband für Sicherheitsereignis
- Tägliche Compliance-Punktzahl
- Punktzahl der PCI-Konfigurationssteuerungen
- Management von Benutzersitzungen
- Härtung
- Auditor
- Metriken (Anwender, E-Mail und Virenschutz)
- Ressourcen
- Sicherheitsbenachrichtigungen
- Touren
- Sicherheitstestportal
- Sicherheitscenter
- Hilfe
- Virtual Agent-Zugriff

Auf der Homepage des Instanz-Sicherheitszentrums können Sie die Sicherheits-Compliance-Punktzahl für Ihre Instanz anzeigen und die allgemeine Sicherheitsintegrität überwachen. Sie können dann Systemeigenschaften konfigurieren oder aktualisieren, die sich auf Ihre Instanzsicherheit beziehen, damit sie den Sicherheitsanforderungen entsprechen.

Hinweis: Das Instanz-Sicherheitszentrum unterstützt keine Domänentrennung.

Anwenderrollen

Zur Verwendung des Instanz-Sicherheitszentrums benötigen Sie die Rolle admin oder Security_Dashboard_user.

Weitere Informationen zur Verwaltung von Abonnements pro Anwender finden Sie unter Verwalten von Anwenderabonnements in Abonnement-Management. Und wenden Sie sich an Ihren Account-Vertreter.

Rollen

Erforderliche Rolle	Anwender	Vorteile
Administrator	Diese Rolle hat Zugriff auf alle Systemfunktionen, -Funktionen und -Daten, da Administratoren ACL-Regeln (Access Control List) überschreiben und alle Rollenprüfungen bestehen können. Vermeiden Sie es, diese Rolle Ihren Anwendern zuzuweisen,	Nutzen Security Center Tools zur Verbesserung der Instanzsicherheitslage und zur Überwachung sicherheitsbezogener Verhaltensweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen (Fortsetzung)

Erforderliche Rolle	Anwender	Vorteile
	wenn gezieltere Rollen verfügbar sind.	
sn_vsc.security_center_viewer	Mit dieser Rolle können Anwender, die keine Administratoren sind, die Informationen in anzeigen Security Center Nehmen Sie jedoch keine Änderungen an vor Security Center Tools oder Instanzkonfigurationen ändern sich mithilfe von Security Center Tools. Beispielsweise können Plattformbesitzer, Security Operations-Analysten oder Compliance-Stakeholder einige der in verfügbaren Sicherheits-KPIs, Sicherheitseinblicke und Sicherheitslernmaterialien anzeigen oder müssen Security Center.	Verschaffen Sie sich Einblick in Security Center Tools zur Überwachung der Instanzsicherheitslage und zur Überwachung des Sicherheitsverhaltens.

Warnung: Um sicherzustellen, dass das Instanz-Sicherheitszentrum bei jedem Upgrade aktuelle Sicherheitsinformationen erhält, passen Sie dieses Modul nicht an. Wenn Sie Sicherheitseinstellungen in Ihrer Instanz ändern, stellen Sie sicher, dass Sie sie zuerst in einer nicht-Produktionsumgebung testen.

Administratornachrichten

Nachrichten und Erinnerungen, die hauptsächlich für Administratoren gedacht sind, werden über dem rotierenden Sicherheitsbanner angezeigt.

Beispiel: A Konfigurieren Sie Sicherheitsbenachrichtigungen Die Nachricht wird angezeigt, um Administratoren daran zu erinnern, Einstellungen für Sicherheitsbenachrichtigungen zu konfigurieren, falls sie dies nicht getan haben. Außerdem wird auf die entsprechende Seite verwiesen.

Hinweis: Das Banner für Administratornachrichten wird nicht für nicht-Administratoranwender angezeigt oder wenn keine umsetzbaren Elemente für Administratoranwender vorhanden sind.

Rotierendes Sicherheitsbanner

Um Sie bei der Überwachung der Sicherheitsintegrität Ihrer Instanz zu unterstützen, werden kritische Instanzsicherheitsnachrichten im rotierenden Banner angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zwei bis drei Sicherheitsnachrichten werden normalerweise in regelmäßigen Intervallen rotiert.
- Die Punkte am unteren Rand des Banners zeigen die Gesamtzahl der aktuellen Sicherheitsnachrichten an.
- Um durch sie zu navigieren, wählen Sie die Punkte aus, oder wählen Sie die Pfeile aus, die auf beiden Seiten der Nachrichten angezeigt werden.

Die Hintergrundfarben des Banners geben den relativen Schweregrad der Nachrichten an.

Farbe	Beschreibung
Rot	Kritische Sicherheitssituation, die eine rechtzeitige Reaktion oder eine Empfehlung zum Schutz oder zur Reaktion auf kritische Sicherheitsereignisse erfordert.
Dunkelgrau	Nicht kritische Warnmeldung.
Blau	Allgemeine Informationsmeldung.

Um den Textinhalt im Banner einzuklappen oder zu minimieren, wählen Sie aus . Um den Textinhalt zu maximieren, wählen Sie ihn erneut aus.

- Wenn Sie das Instanz-Sicherheitscenter erneut verwenden, wurde der Textinhalt reduziert oder erweitert angezeigt, je nachdem, wie Sie ihn in Ihrer vorherigen Sitzung verwendet haben.
- Wenn sich der Textinhalt selbst ändert, wird er für alle Anwender als maximiert angezeigt.

Suchen

Verwenden Sie die Suchleiste, um das gesamte Instanz-Sicherheitszentrum nach Sicherheitsressourcen zu durchsuchen, die Sie beim Verständnis und Beheben von Sicherheitsproblemen unterstützen. Sie können die folgenden sicherheitsbezogenen Ressourcen durchsuchen:

- Now Support Knowledge Base Artikel
- Seiten des Instanz-Sicherheitszentrums
- Extern Now Support Links
- PA-Sicherheits-Widgets, z. B. die tägliche Compliance-Punktzahl und eingehende externe E-Mails
- Bannerinhalt

Ereignis-Menüband

Verwenden Sie das Ereignisband, um wichtige Metriken zur Überwachung von Sicherheitsereignissen für die aktuelle Instanz anzuzeigen.

- Um manuell durch die Metriken zu scrollen, wählen Sie die Pfeiltasten nach rechts oder links.
- Wählen Sie aus, um das Ereignis-Menüband zu konfigurieren **Bearbeiten** .

Weitere Informationen zum Ereignisband und zur Konfiguration finden Sie unter Sicherheitsereignisse überwachen Und Konfigurieren Sie das Sicherheitsereignis-Menüband.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tägliche Compliance-Punktzahl

Der Abschnitt „tägliche Compliance-Punktzahl“ enthält **Tägliche Compliance-Punktzahl** , **Sitzungsverwaltung** , **Härtung** , **Auditor** , Und **Ressourcen** Kacheln.

Sie verwenden die tägliche Compliance-Punktzahl, um zu messen, wie fehlerfrei Ihre Instanz aus Sicherheitssicht ist.

Die tägliche Compliance-Punktzahl ist eine Prozentpunktzahl. Sie basiert darauf, wie konform die aktuellen Einstellungen Ihrer Instanzsicherheitseigenschaften mit den in veröffentlichten Compliance-Werten sind Härtungseinstellungen.

- Weitere Informationen zu den täglichen Berechnungen der Compliance-Punktzahl und zu den Auswirkungen der Härtungseinstellungen finden Sie unter Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften.
- Die **Aktualisieren** Mit der Schaltfläche kann ein Administrator die tägliche Compliance-Punktzahl sofort neu berechnen. Weitere Informationen finden Sie unter Wie die täglichen Compliance-Punktzahlen, Trends und Diagrammdaten aktualisiert werden.

Härtung

Verwenden Sie diesen Prozess, um die spezifischen Sicherheitskonfigurationseigenschaften anzupassen, die sich auf die tägliche Compliance-Punktzahl auswirken:

1. Um auf die Seite „Compliance-Konfigurationen für Härtung“ zuzugreifen und die Instanzsicherheitshärtung durchzuführen, wählen Sie aus **Tägliche Compliance-Punktzahl** Kachel oder **Härtung** Link.
2. Geben Sie an, ob Sie alle oder nur empfohlene Sicherheitskontrollen anzeigen möchten. Wählen Sie dann die Kategorie aus, in der Sie arbeiten möchten.
3. Legen Sie jede Sicherheitskonfigurationseigenschaft in der ausgewählten Kategorie fest. Klicken Sie Auf **Weitere Informationen** Dient zum Anzeigen detaillierter Informationen für eine Eigenschaft.

Weitere Informationen zur Härtung und Optimierung von Sicherheitskonfigurationseigenschaften zur weiteren Erhöhung der Compliance finden Sie unter Passen Sie die Einstellungen für die Instanzsicherheit an, um die Compliance zu erhöhen.

Weitere Informationen zur Aktualisierung von Trend- und Diagrammdaten finden Sie unter Wie die täglichen Compliance-Punktzahlen, Trends und Diagrammdaten aktualisiert werden.

Auditor

Führen Sie den Auditor aus, um Ihre Instanz zu scannen und falsche Sicherheitsdefinitionen zu finden. Es liefert Ergebnisse, die Sie korrigieren können, um die Sicherheitslage Ihrer Instanz zu verbessern.

Um auf die Auditor-Seite zuzugreifen, wählen Sie aus **Auditor** Kachel oder **Auditor** Link. Weitere Informationen finden Sie unter Suchen Sie nach falschen Sicherheitsdefinitionen.

Management von Anwendersitzungen

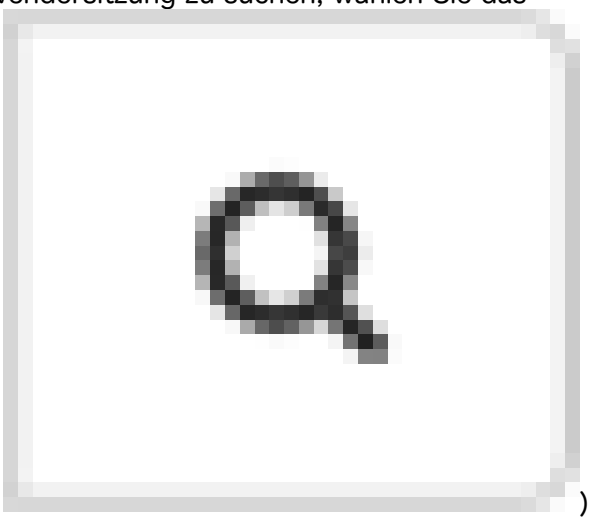
Verwenden Sie das Sitzungsmanagement, um:

- Zeigen Sie Anwenderanmeldungssitzungen an und verwalten Sie sie.
- Zeigen Sie die Anwenderanmeldesitzung des aktuellen Knotens an, mit dem Sie verbunden sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sehen Sie sich detaillierte Informationen zu jeder Sitzung an, z. B. Anwendername und IP-Adresse.
- Isolieren und sperren Sie bestimmte Anwendersitzungen, die Sicherheitsrisiken darstellen.

Um auf die Seite Sitzungsmanagement zuzugreifen, wählen Sie aus **Sitzungsverwaltung** Kachel oder Link.

Feld	Beschreibung
Anwender	Name des Anwenders, der dieser Anmeldesitzung zugeordnet ist. • Um eine bestimmte Anwendersitzung zu suchen, wählen Sie das Spotlight-Suchsymbol (), um nach Anwender, Anwenderagent-Stichwort oder IP-Adresse zu suchen. Wenn Sie beispielsweise alle aktuellen Anmeldungen über einen bestimmten Browsertyp suchen möchten, geben Sie den Browsernamen als Stichwort in ein **Anwender-Agent** Feld. • Klicken Sie auf einen Anwendernamen, um auf den Anwenderprofildatensatz zuzugreifen. Sie können das Anwenderprofil nur ändern, wenn Ihnen eine Administratorrolle zugewiesen ist. **Hinweis:** Weitere Informationen zu Anwenderprofilen finden Sie unter Erstellen Sie einen Anwender .
MFA	Kontrollkästchen, das angibt, ob Multifaktor-Authentifizierung (MFA) für den angemeldeten Anwender aktiviert ist. Weitere Informationen zu MFA finden Sie unter Multi-Faktor-Authentifizierung.
Aktiv	Kontrollkästchen, das angibt, ob der angemeldete Anwender aktiv oder inaktiv ist.
Anwenderagent	Typ des Browsers und das Betriebssystem des Geräts für die Anwenderanmeldungssitzung.
IP-Adresse	IP-Adresse des angemeldeten Anwenders.
Letzter Zugriff	Datum und Uhrzeit des letzten Zugriffs dieser Anwendersitzung auf die Instanz. **Hinweis:** Um detaillierte Informationen für eine bestimmte Anmeldesitzung anzuzeigen oder die Sitzung selbst zu sperren, wählen Sie aus **Anwender-Agent** , **IP-Adresse** , Oder **Letzter Zugriff** Felder.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken

Zeigen Sie Details für die folgenden Metriktypen an:

Typ der Metrik	Beschreibung
Benutzer	Sicherheitsmetriken, die der Anwenderaktivität in der Instanz zugeordnet sind. Um auf die Seite „Anwendermetriken“ zuzugreifen, wählen Sie aus **Metriken** Verknüpfen Sie, und wählen Sie dann aus **Anwendermetriken** .
Exportieren	Sicherheitsmetriken, die Daten zugeordnet sind, die aus der Instanz exportiert wurden. Um auf die Seite „Metriken exportieren“ zuzugreifen, wählen Sie aus **Metriken** Verknüpfen Sie, und wählen Sie dann aus **Metriken Exportieren** .
Authentifizierung	Sicherheitsmetriken, die der Authentifizierung zugeordnet sind, z. B. selten verwendete IP-Adressen, fehlgeschlagene Anmeldungen und Typen von Authentifizierungsschemata, die von Ihren Anwendern verwendet werden. Um auf die Seite „Metriken exportieren“ zuzugreifen, wählen Sie aus **Metriken** Verknüpfen Sie, und wählen Sie dann aus **Authentifizierungsmetriken** .
E-Mail	Sicherheitsmetriken, die anomalen Verhaltensweisen im Zusammenhang mit den eingehenden E-Mails an Ihre Instanz zugeordnet sind. Um auf die Seite E-Mail-Metriken zuzugreifen, wählen Sie aus **Metriken** Verknüpfen Sie, und wählen Sie dann aus **E-Mail-Metriken** .
Virenschutz	Sicherheitsmetriken, die der Virenschutz-Ereignisaktivität in der Instanz zugeordnet sind. Um auf die Seite „Antivirus-Metriken“ zuzugreifen, wählen Sie aus **Virenschutz** Kacheln Sie an, oder wählen Sie aus **Metriken** Verknüpfen Sie, und wählen Sie dann aus **Virenschutz** .

Hinweis: Weitere Informationen zur Überwachung der einzelnen Metriktypen finden Sie unter Überwachen Sie Instanzmetriken.

Ressourcen

Zugriff Now Support Knowledge Base artikel, Ressourcen und Blogs, die sich auf die Instanzsicherheit beziehen. Diese Ressourcen umfassen Sicherheitseinstellungen, Codierung, Compliance, Korrekturen und zugehörige Themen. So greifen Sie auf die Seite „Ressourcen“ zu:

1. Klicken Sie auf **Ressourcen** Kachel oder Link.
2. Wählen Sie auf der Seite „Ressourcen“ eine Kategorie aus:

Kategorie	Beschreibung
Empfohlene Richtlinien	Zugriff auf empfohlene Sicherheitsrichtlinien, einschließlich Härtungseinstellungen Und Leitfaden Für Sichere Codierung [KB0623354] Artikel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Beschreibung
Sicherheitsressourcen	Zugriff auf sicherheitsbezogene Ressourcen in Knowledge Base, Einschließlich: ○ Sicherheitstest der Kundeninstanz ○ Cloud-Sicherheits-, Trust- und Compliance-Center-KB-Artikel

Sicherheitsbenachrichtigungen

Ein Benachrichtigungs-Glockensymbol () Wird im Instanz-Sicherheitszentrum mit einer Gesamtzahl ungelesener Sicherheitsbenachrichtigungen angezeigt. Benachrichtigungen bleiben bestehen und werden in dieser Anzahl berücksichtigt, bis Sie sie als gelesen markieren.

1. Klicken Sie auf das Glockensymbol, um die ersten fünf ungelesenen Sicherheitsbenachrichtigungen anzuzeigen.

   Eine Benachrichtigung wird angezeigt, wenn **Administratoranmeldung** , **Administrator Entsperrt** , **Anmeldung Fehlgeschlagen** , **Rolle Mit Hohen Berechtigungen** , **Identitätswechsel** , **Sicherheitserhöhung** , Und **Wöchentlicher Digest** Ereignisse finden in Ihrer Instanz statt. Weitere Informationen zu diesen Sicherheitsereignissen finden Sie unter Sicherheitsereignisse überwachen.

2. Um detaillierte Informationen für ein bestimmtes Sicherheitsereignis anzuzeigen, wählen Sie die Benachrichtigung aus.

   Wenn Sie beispielsweise eine Rollenbenachrichtigung mit hohen Berechtigungen auswählen, können Sie die Tabelle „Rollen“ (sys_user_role) anzeigen. Verwenden Sie diese Tabelle, um anzuzeigen, welchen Anwendern während des Kalendertages privilegierte Rollen zugewiesen wurden. Mithilfe dieses Verlaufs können Sie feststellen, ob Rollen ordnungsgemäß zugewiesen wurden.

3. Wenn mehr als fünf ungelesene Benachrichtigungen vorhanden sind, wählen Sie aus **Zeigen Sie Alle Benachrichtigungen An** Dient zum Zugriff auf eine Seite „alle Benachrichtigungen“ mit einer Liste aller ungelesenen Benachrichtigungen.
   - Um detaillierte Informationen für ein bestimmtes Sicherheitsereignis anzuzeigen, wählen Sie die Benachrichtigung aus.
   - Um alle aufgeführten Benachrichtigungen als gelesen zu markieren, wählen Sie aus **Markieren Sie alle als gelesen** .

Hinweis: Als Administrator können Sie auch Einstellungen zum Senden bestimmter Benachrichtigungstypen für jeden Typ von Sicherheitsereignissen konfigurieren. Weitere Informationen finden Sie unter Legen Sie Einstellungen für Benachrichtigungen zu Sicherheitsereignissen fest.

Touren

Klicken Sie auf **Touren** Link zum Anzeigen einer geführten visuellen Tour durch das Instanz-Sicherheitszentrum.

- Die geführte Tour enthält nur die Sicherheitsüberwachungsfunktionen, die auf der Homepage aufgeführt sind.
- Sie enthält nicht die Sicherheitsfunktionen, auf die Sie zugreifen, wenn Sie die Kacheln oder Links auf der Homepage auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitstestportal, Sicherheitscenter und Hilfe

Die Now Support Serviceportal Ist eine zentrale Ressource, die Sie zum Verwalten von Instanzen, Aufgaben und Accounts verwenden. Sie können auch auf nützliche Ressourcen zugreifen, die Sie zur Diagnose und Lösung von Sicherheits- und technischen Problemen in Ihrer Instanz verwenden können.

Um auf diese Ressourcen zuzugreifen, wählen Sie aus **Weitere Informationen** Oder **Hilfe Erhalten** In den folgenden Kacheln:

Kachel	Beschreibung
Portal für Sicherheitstests	Zugriff auf das Sicherheits-Dashboard in Now Support Sicherheitstestportal.
Sicherheitscenter	Zugriff auf Sicherheits-Compliance in Now Support Sicherheitsportal.
Hilfe	Zugriff auf die folgenden Hilferessourcen in Now Support Sicherheitsportal: • Bitten Sie einen Experten, Antworten auf häufige Fragen zu finden. • Melden Sie ein Problem oder einen Ausfall an ServiceNow Globaler technischer Support durch Öffnen eines Falls. • Selfservice-Support-Ressourcen, einschließlich: ◦ Videos ◦ Dokumentation ◦ ServiceNow Community ◦ Knowledge Base ◦ Known Error-Portal ◦ Sicherheits-RFX-Datenbank • ServiceNow Community Fragen, die für Ihre Verwendung empfohlen werden.

Virtual Agent-Zugriff

Die Virtual Agent Ist eine Plattform für die Bereitstellung von Anwenderunterstützung durch Konversationen innerhalb einer Messaging-Schnittstelle.

Wenn die zugehörigen Plugins installiert sind, können Administratoren auf zugreifen Virtual Agent Und Natural Language Understanding(NLU) Funktionen durch Auswahl des Virtual Agent-Symbols:



Mit dieser Option können Sie die folgenden Aufgaben ausführen:

- Stellen Sie sicherheitsbezogene Fragen, und erhalten Sie dann schnelle Zusammenfassungsantworten und Referenz-Links, um mehr zu erfahren.
- Antworten im Zusammenhang mit Prozessen erhalten, z. B.:
  - Instanz-Sicherheitszentrum
  - Platform-Sicherheit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ServiceNow Sicherheitsrichtlinien
- Vertrauen, Governance und Risiko

- Suchen Sie nach sicherheitsbezogenen Ressourcen, z. B. Knowledge Base Themen in Now Support Sicherheitsportal.

Hinweis: Um mehr über die Verwendung und Aktivierung von zu erfahren Virtual Agent, Siehe:

- Virtual Agent
- Aktivieren Sie ISC Virtual Agent Schnittstelle

Instanz-Sicherheitszentrum an ServiceNow Security Center Migration

Erfahren Sie mehr über die wichtigsten Unterschiede bei der Migration von Instance Security Center (ISC) zu ServiceNow Security Center(SSC).

Wichtig:

Das Instanz-Sicherheitszentrum ist ein Legacy-Produkt, das das Ende des Verkaufs bis September 2024 erreicht. Das ServiceNow-Sicherheitszentrum ist die empfohlene Lösung, die Kunden in Zukunft annehmen sollten. Weitere Informationen finden Sie unter Verwerfungsprozess artikel (KB0867184) in der Now Support Knowledge Base.

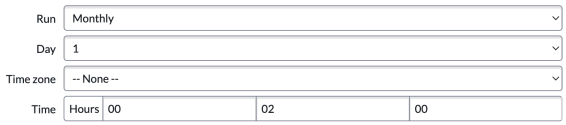
ServiceNow Security Center(SSC) ist eine Sicherheitsanwendung, die aus einer Reihe von speziell entwickelten Tools besteht, die Unternehmen dabei helfen sollen, die Sicherheit ihrer zu gewährleisten ServiceNow Bereitstellungen. Mit SSC können Unternehmen ihre Sicherheitslage verbessern, ihre Compliance-Stufen stärken und dies mit einer nahtlosen Anwender-Experience tun.

Verwenden Sie dieses Dokument, um mehr über SSC-Erweiterungen in der Funktionalität zu erfahren und zu erfahren, wie Aufgaben in SSC ausgeführt werden, die zuvor in ISC ausgeführt wurden.

Sicherheitshärtung

Funktionserweiterungen	ISC vs. SSC
Aktualisierungen der Anwenderinteraktion	• Überprüfen Sie die neueste Punktzahl, indem Sie zur Seite „Übersicht“ oder „Härtungsvergleich“ navigieren. • Aktualisieren Sie die neueste Punktzahl manuell, indem Sie zu Übersicht navigieren und Punktzahl aktualisieren auswählen. • Ändern Sie die Einstellungskonfiguration, indem Sie auf einer dieser Seiten einen Einstellungsnamenslink auswählen und dann Änderungen an vornehmen **Einstellungsdetail** Seite: ○ Übersicht ○ **Härtung** > **Alle Einstellungen** ○ **Härtung** > **Vergleich**
Legen Sie einen Zeitplan für fest, um Ihre	Mit SSC können Sie festlegen, wann das System eine Aktualisierung Ihrer Compliance-Punktzahl auslöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionserweiterungen	ISC vs. SSC
Compliance-Punktzahl neu zu berechnen	**1.** Navigieren Sie zur Tabelle geplante Skriptausführungen [sysauto_script]. **2.** Suchen und öffnen Sie SC: Compliance monatlich berechnen Datensatz. **3.** Verwenden Sie **Ausführen** , **Tag** , **Zeitzone** , Und **Zeit**Felder zum Festlegen Ihres bevorzugten Zeitplans.  **4.** Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

Sicherheits-KPIs und -Metriken

Funktionserweiterungen	ISC vs. SSC
Verbesserungen an KPIs	Mit SSC können Sie: • Zeigen Sie den Trend der Punktzahl im Zeitverlauf an. • Überwachen Sie alle KPIs und Metriken mit derselben Schnittstelle und denselben analytischen Fähigkeiten.
Erweiterungen an Metriken	SSC enthält diese Metrikerweiterungen: • Mehr als 65 Metriken wurden hinzugefügt. • Überwachen und analysieren Sie KPIs und Metriken über eine einzige Anwenderoberfläche. • Erstellen Sie Ziele und Schwellenwerte für Metriken.
Aktualisierungen der Anwenderinteraktion	Greifen Sie auf Metriken in SSC zu, indem Sie zu navigieren **Übersicht** > **Metriken**, Und dann Metrik aus dem Navigationsmenü auswählen. Alternativ können Sie zu navigieren **Alle Metriken** .

Sicherheitsscanner

Funktionserweiterungen	ISC vs. SSC
Neue Funktionalität	SSC enthält diese Funktionen: • Führen Sie Scans manuell aus, oder planen Sie, dass sie zu bestimmten Zeiten ausgeführt werden. • Erstellen Sie Ihre eigenen Scan-Prüfungen. • Erstellen Sie Ihre eigene Scan-Suite. • Vergleichen Sie die Ergebnisse von zwei Scans.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionserweiterungen	ISC vs. SSC
Erweiterte E-Mail-Funktionalität	Richten Sie E-Mail-Benachrichtigungen ein, um über Sicherheitsereignisse in Ihrer Instanz auf dem Laufenden zu bleiben.
Aktualisierungen der Anwenderinteraktion	• Führen Sie den Auditor-Scan aus, indem Sie zu navigieren **Übersicht** > **Scannen** > **Suites** Und auswählen **Auditor-Suite** Aus der Liste. • Sehen Sie sich die Scan-Ergebnisse an, indem Sie zu navigieren **Übersicht** > **Scannen** > **Ergebnisse**an.

Zusätzliche Sicherheitsfunktionen

Funktionserweiterungen	ISC vs. SSC
Funktionen zur Überwachung von Sitzungen	• Visualisieren Sie Sitzungsaktivitäten mit Analytics Hub . • Überwachen Sie die Sitzungsaktivität, indem Sie zu navigieren **Metriken** > **Sitzungen**an.
Ressourcen finden	Greifen Sie unter auf alle Lernressourcen auf einer einzelnen Seite zu **Übersicht** > **Lernen**an.

Deaktivieren Security Center Funktionen

Zum Deaktivieren Security Center Führen Sie in Ihrer Instanz die Schritte aus, die in angegeben sind KB1702514: Richtlinien zum Deaktivieren von Instanz-Sicherheitscenter-Komponenten (bei Verwendung des Sicherheitszentrums) .

Sicherheitsereignisse überwachen

Analysieren Sie die Ereignismetriken in Ihrer Instanz, um potenzielle Sicherheitsereignisse zu identifizieren und zu verhindern.

Wichtig:

Das Instanzsicherheitszentrum (ISC) hat das Ende des Verkaufs im September 2024 erreicht und wird nicht mehr unterstützt oder steht für eine neue Aktivierung zur Verfügung.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Instanz-Sicherheitszentrum an ServiceNow Security Center Migration.

Im Ereignisband, das sich auf der Instanzsicherheits-Homepage befindet, können Sie diese Metriken und die zugehörigen Details analysieren, um potenzielle Sicherheitsereignisse in der Instanz zu identifizieren.

- Für jede Ereignismetrik wird eine Einzelpunktzahl in Echtzeit angezeigt, die angibt, wie oft das Ereignis während des Tages in dieser Instanz aufgetreten ist. Diese Berichte mit einer einzelnen Punktzahl werden automatisch aktualisiert, wenn die entsprechenden Ereignisse stattfinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Jede Ereignismetrik enthält auch Compliance-Trend- und Diagramminformationen für einen Datumsbereich. Diese Informationen werden täglich aktualisiert, wenn Sie den Performance Analytics-Auftrag ausführen. Weitere Informationen finden Sie unter **Ereignistrenddetails werden analysiert** Abschnitt.

Ereignistypen

Sie können mindestens sechs der folgenden Ereignistypen überwachen. Verwenden Sie für mehr als sechs Ereignisse die Pfeiltasten nach links oder rechts unter dem Ereignisband, um durch sie zu scrollen. Informationen zum Konfigurieren des Ereignis-Menübands finden Sie unter Konfigurieren Sie das Sicherheitsereignis-Menüband.

Benachrichtigungseinstellung	Beschreibung
Administratoranmeldungen	Anzahl der Anmeldeversuche in dieser Instanz während des Kalendertages durch Anwender, die über eine zugewiesene Administratorrolle verfügen.
Administratoranwender hinzugefügt	Anzahl der Anwender mit einer Administratorrolle, die in dieser Instanz während des Kalendertages hinzugefügt wurden. Beispielsweise kann Ihre Instanz ein Sicherheitsproblem haben, wenn die Anzahl 10 beträgt, aber 4 Anwendern ist bekannt, dass sie eine Administratorrolle zugewiesen haben.
Externe eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.
Externe Anmeldungen	Anzahl der Anwender mit der zugewiesenen Rolle „snc_external“, die sich während des Kalendertages bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen normalerweise zu Wartungs-, Support-, Beratungs- oder Audit-Zwecken. Durch die Überwachung dieser Metrik können Sie überprüfen, ob die externen Anmeldeversuche legitim sind und keine potenziellen Sicherheitsprobleme darstellen. Weitere Informationen zum Zuweisen externer Anwenderrollen finden Sie unter Explizite Rollen.
Fehlgeschlagene Anmeldungen	Anzahl der versuchten Anmeldungen, die während des Kalendertages in dieser Instanz fehlgeschlagen sind. Diese Metrik kann darauf hinweisen, dass versucht wird, sich anzumelden und die Sicherheit Ihrer Instanz zu gefährden.
Identitätswechsel	Anzahl der Anmeldungen zur Identitätswechsel in dieser Instanz während des Kalendertages. Informationen zum Identitätswechsel von Anwendern finden Sie unter Identität eines Anwenders annehmen .
Dateien in Quarantäne	Anzahl der Dateien, die bei der Ausführung unter Quarantäne gestellt wurden Antivirus-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
	Scanning In dieser Instanz während des Kalendertages. Um mehr über Dateien in Quarantäne und zu erfahren Antivirus-Scanning, Siehe Virenschutzmetriken Und Antivirus-Scanning.
Erhöhungen der Sicherheit	Anzahl der Male, mit denen ein Sicherheitsadministrator die Sicherheit für Standardanwender erhöht hat, indem seine zugewiesene Anwenderrolle während des Kalendertages in eine Sicherheitsrolle mit hohen Berechtigungen geändert wurde. Diese Sicherheitsrollen mit hohen Berechtigungen umfassen oauth_admin, admin, Security_admin und Impersonator. • Diese Metrik gibt an, dass jemand versucht hat, die Sicherheit eines nicht autorisierten Anwenders zu erhöhen. Verwenden Sie diese Metrik nicht allein, um eine bestimmte Sicherheitsgefährdung zu erkennen. Behandeln Sie diese Metrik stattdessen als Hinweis darauf, dass Sie eine andere Metrik überprüfen sollten, um festzustellen, ob eine Sicherheitskompromittierung aufgetreten ist. • Weitere Informationen zur Erhöhung der Anwendersicherheit finden Sie unter Auf eine privilegierte Rolle hochstufen Und Rollen mit erhöhten Rechten.
SNC-Anmeldungen	Anzahl von Kundenservice und Support Mitarbeiter, die sich am Kalendertag mit der Hi-Hopping-Technik bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen normalerweise zu Wartungs-, Support-, Beratungs- oder Audit-Zwecken. Für Informationen zur Steuerung ServiceNow Zugriff auf Mitarbeiter im Unternehmen, siehe ServiceNow-Zugriffssteuerung .
Spam	Weitere Informationen finden Sie unter E-Mail-Metriken.
Vertrauenswürdige eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.
Nicht vertrauenswürdige eingehende E-Mail	Weitere Informationen finden Sie unter E-Mail-Metriken.
Virustypen	Anzahl der verschiedenen Arten von Antivirus-Ereignissen, die in dieser Instanz während des Kalendertages aufgetreten sind. Weitere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
	Informationen zu Antivirus-Ereignistypen finden Sie unter Virenschutzmetriken .

Ereignistrenddetails werden analysiert

Um Trenddetails für eine Ereignismetrik anzuzeigen, klicken Sie auf die Ereignisanzahl, um auf die Analytics Hub-Seite zuzugreifen. Die Details, die für die Instanz angezeigt werden, hängen vom Typ der Metrik ab.

So zeigen Sie beispielsweise eine Liste der fehlgeschlagenen Versuche auf der Seite „Sicherheits-Dashboard-Ereignisprotokolle“ an:

- Wählen Sie aus **Fehlgeschlagene Anmeldungen** Metrik.
- In Analytics Hub Seite klicken Sie auf **Datensätze Anzeigen** .
- Klicken Sie auf einen der fehlgeschlagenen Anmeldeversuche.
- Das Detail enthält den Namen des Anwenders, der versucht hat, sich anzumelden, seine IP-Adresse und den Tabellennamen, auf den er zugreifen wollte.

Sie können Ereignisschwellenwertauslöser in einrichten Core-UI Analytics Hub Oder Platform Analytics KPI-Details Dient zum Bereitstellen von Warnungen, wenn ein bestimmtes Ereignis innerhalb eines Bereichs von Punktzahlen für auftritt *Indikator*. Sie können auch Ziele festlegen, mit denen Sie die Differenz zwischen der gewünschten Punktzahl und der tatsächlichen Punktzahl eines Ereignisses visualisieren können.

Sie können beispielsweise einen Schwellenwert von festlegen `10` Für **Fehlgeschlagene Anmeldungen** Metrik. Wenn während des Tages zehn oder mehr fehlgeschlagene Anmeldeversuche auftreten, wird eine Warnung an bestimmte Sicherheitspersonal gesendet. Sie können auch ein ähnliches Ziel festlegen, das eine visuelle Hervorhebung in bietet Analytics Hub Wenn 10 fehlgeschlagene Anmeldungen an einem Tag auftreten.

Trenddaten und -Diagramme, die in der Menübandkachel „Ereignis“ und angezeigt werden Analytics Hub Werden aktualisiert, nachdem der Performance Analytics-Auftrag um 02:00 Uhr Ortszeit ausgeführt wurde. Weitere Informationen finden Sie unter Wie die täglichen Compliance-Punktzahlen, Trends und Diagrammdaten aktualisiert werden.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Now Intelligence

Analytics Hub

Performance Analytics-Ziele und -Schwellenwerte

Konfigurieren Sie das Sicherheitsereignis-Menüband

Konfigurieren Sie das Sicherheitsereignis-Menüband auf der Homepage des Instanz-Sicherheitszentrums so, dass nur die Ereignisse enthalten sind, die für die Nachverfolgung der Instanzsicherheit in Ihren Vorgängen relevant sind. Sie können auch die Reihenfolge ändern, in der die Sicherheitsereigniskacheln auf dem Menüband angezeigt werden.

Vorbereitungen

Erforderliche Rolle: Security_Dashboard_user oder admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Das Sicherheitsereignis-Menüband wird anfänglich mit einem vollständigen Satz von Standard-Sicherheitsereignissen gefüllt. Sie können sie anpassen, indem Sie die Ereignisse entfernen, die für Ihre Organisation nicht relevant sind.

- Wenn Sie beispielsweise vermuten, dass Sicherheitsprobleme auf Aktionen interner Mitarbeiter zurückzuführen sind, fügen Sie die Ereignisindikatoren Administratoranmeldungen, hinzugefügte Administratoranwender und Sicherheitserhöhungen hinzu.
- Diese Indikatoren überwachen, wie oft Anwender mit Administratorrollen versucht haben, sich anzumelden, und welche Versuche unternommen wurden, um Sicherheitsrollen zu erhöhen, wenn Administratoranwender hinzugefügt wurden.

Hinweis: Informationen zu den Typen von Sicherheitsereignissen, die im Ereignisband angezeigt werden, finden Sie unter Sicherheitsereignisse überwachen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**an.
2. Klicken Sie im Ereignisband auf **Bearbeiten** (< > Edit).
   Im Formular „Ereignisse bearbeiten“ die **Ausgewählt** Spalte enthält die Ereignisse, die bereits aufgeführt sind.
3. Um dem Ereignisband Sicherheitsereignisse hinzuzufügen, verschieben Sie sie aus dem **Verfügbar** Spalte zu **Ausgewählt** Spalte.
   Um die Reihenfolge der Ereignisse im Menüband zu ändern, wählen Sie ein Ereignis aus, und klicken Sie dann auf den Pfeil nach oben oder unten, um es an die richtige Position zu verschieben.
   - Ordnen Sie die Ereignisse in derselben sequenziellen Reihenfolge an, in der sie im Ereignisband des Instanz-Sicherheitszentrums angezeigt werden sollen.
   - Die Ereignisse, die Sie oben im platzieren **Verfügbar** Die Spalte wird sequenziell angezeigt, beginnend auf der linken Seite des Instanz-Sicherheitscenter-Ereignismenüs. Die Ereignisse, die unten in der Spalte platziert sind, werden rechts im Ereignisband angezeigt.
4. So entfernen Sie Sicherheitsereignisse aus dem Ereignisband:
   - In **Ausgewählt** Wählen Sie die Sicherheitsereignisse aus, die Sie aus dem Ereignisband entfernen möchten.
   - Verschieben Sie sie aus dem **Ausgewählt** Spalte zu **Verfügbar** Spalte.
5. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Legen Sie Einstellungen für Benachrichtigungen zu Sicherheitsereignissen fest

Konfigurieren Sie Einstellungen für die Arten von Benachrichtigungen, die Sie für das Auftreten bestimmter Sicherheitsereignisse erhalten möchten. Für jeden Typ legen Sie fest, ob Benachrichtigungen per E-Mail oder per Push-Benachrichtigung in empfangen werden sollen Now Mobile, Oder in Messaging-Anwendungen von Drittparteien wie Slack Oder Microsoft Teams.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Damit Messaging-Anwendungen von Drittparteien Sicherheitsbenachrichtigungen senden können, müssen Sie das Plugin „Messaging Notification“ (com.glide.notification.messaging) aktivieren. Einzelne Anwender müssen ihre eigenen Einstellungen konfigurieren. Weitere Informationen finden Sie unter Benachrichtigungen in Messaging-Anwendungen .

Erforderliche Rolle: admin.

Prozedur

1. Klicken Sie auf der Homepage des Instanz-Sicherheitszentrums auf das Profilmenü, und klicken Sie dann auf **Benachrichtigungseinstellungen** .

Benachrichtigungseinstellungen

Benachrichtigungseinstellung	Beschreibung
Administratoranmeldung	Senden Sie den ausgewählten Benachrichtigungstyp, wenn sich andere Anwender mit zugewiesenen Administratorrollen von einer anderen IP-Adresse bei dieser Instanz anmelden.
Admin Entsperren	Senden Sie den ausgewählten Benachrichtigungstyp, wenn ein Account für einen Anwender mit hohen Berechtigungen entsperrt wurde.
Fehlgeschlagene Anmeldung	Senden Sie den ausgewählten Benachrichtigungstyp, wenn sich andere Anwender in weniger als der in definierten Anzahl von Versuchen nicht bei dieser Instanz anmelden können `glide.user.max_unlock_attempts`Eigenschaft. Wenn Sie diese Eigenschaft nicht konfigurieren, ist der Standardwert 5. Weitere Informationen zu dieser Eigenschaft finden Sie unter Sperrung für fehlgeschlagene Anmeldeversuche angeben.
HP-Rolle hinzugefügt	Senden Sie den ausgewählten Benachrichtigungstyp, wenn einem anderen Anwender eine Sicherheitsrolle mit hohen Berechtigungen (einschließlich oauth_admin, admin, Security_admin und Identitätswechsel) gewährt wird. Weitere Informationen zur Erhöhung der Anwendersicherheit finden Sie unter Auf eine privilegierte Rolle hochstufen Und Rollen mit erhöhten Rechten.
Identitätswechsel	Senden Sie den ausgewählten Benachrichtigungstyp, wenn ein anderer Anwender Ihre Identität ausnimmt. Weitere Informationen zum Identitätswechsel von Anwendern finden Sie unter Identität eines Anwenders annehmen .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungseinstellung	Beschreibung
Erhöhung der Sicherheit	Senden Sie den ausgewählten Benachrichtigungstyp, wenn andere Anwender in dieser Instanz zu einer Sicherheitsadministratorrolle hochgestuft werden.
Wöchentlicher Digest	Senden Sie einen wöchentlichen Digest für den ausgewählten Benachrichtigungstyp. Sie enthält: ○ Eine Zusammenfassung aller Sicherheitsaktivitäten, die in dieser Instanz während der Woche stattgefunden haben. ○ Die aktuelle tägliche Compliance-Punktzahl für die Instanz.

2. Aktivieren Sie für jeden Typ von Sicherheitsereignissen die entsprechenden Kontrollkästchen, um die Art der Benachrichtigungen festzulegen, die Sie senden möchten.
Sie können mehrere Benachrichtigungsmethoden für jede auswählen.

Checkbox	Beschreibung
E-Mail	Senden Sie eine E-Mail für diesen Typ von Sicherheitsereignis.
Slack	Benachrichtigungen für diesen Typ von Sicherheitsereignis über senden Slack. **Hinweis:** Diese Spalte wird nur angezeigt, wenn Sie eingerichtet haben Slack Integration in ServiceNow AI Platform.
Teams	Benachrichtigungen für dieses Sicherheitsereignis über senden Microsoft Teams. **Hinweis:** Diese Spalte wird nur angezeigt, wenn Sie eingerichtet haben Microsoft Teams Integration in ServiceNow AI Platform.
Veröffentlichen	Push-Benachrichtigungen senden am Now Mobile Für diesen Typ von Sicherheitsereignis. **Hinweis:** Diese Spalte wird nur angezeigt, wenn Sie sich zum ersten Mal bei anmelden Now Mobile.
Alle auswählen	Wählen Sie einen bestimmten Benachrichtigungstyp für alle Typen von Sicherheitsereignissen aus. Klicken Sie beispielsweise auf **Wählen Sie Alle Aus** Befindet sich oben **E-Mail** Wenn Sie E-Mail-Benachrichtigungen für jeden Sicherheitsereignistyp erhalten möchten.

3. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften

Überprüfen Sie die Metrik für die tägliche Compliance-Punktzahl und die Sicherheitskonfigurationseigenschaften, um festzustellen, ob Ihre Instanz die vorgeschlagenen Sicherheitsanforderungen erfüllt. Sie können die tägliche Compliance-Punktzahl beeinflussen, indem Sie nicht konforme Sicherheitseigenschaften auf der Seite „Compliance-Konfigurationen für Härtung“ aktualisieren.

Wichtig:

Das Instanzsicherheitszentrum (ISC) hat das Ende des Verkaufs im September 2024 erreicht und wird nicht mehr unterstützt oder steht für eine neue Aktivierung zur Verfügung.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Instanz-Sicherheitszentrum an ServiceNow Security Center Migration.

Die tägliche Compliance-Punktzahl ist eine Prozentpunktzahl. Sie basiert darauf, wie konform die aktuellen Einstellungen Ihrer Instanzsicherheitseigenschaften mit den in veröffentlichten Compliance-Werten sind Härtungseinstellungen.

Überprüfen Sie regelmäßig die tägliche Compliance-Punktzahl Ihrer Instanz. Befolgen Sie diese Richtlinien, wenn Sie Ihre tägliche Compliance-Punktzahl bewerten:

- Größer oder gleich 90 % gibt an, dass die Instanz kritische Sicherheitskontrollen erfüllt.
- Mehr als oder gleich 50 % und weniger als 90 % zeigen ein moderates Maß an Sicherheits-Compliance an.
- Weniger als 50 % weisen auf ein niedriges Maß an Sicherheits-Compliance hin.

Passen Sie die Einstellungen für die Instanzsicherheit an, um die Compliance zu erhöhen

Auf der Seite „Konfiguration der Härtung-Compliance“ können Sie nicht konforme Sicherheitseigenschaften, die sich auf die tägliche Compliance-Punktzahl Ihrer Instanz auswirken, härten und optimieren. Ihre Verwendung stellt sicher, dass Ihre Instanz die veröffentlichten Sicherheitshärtungsstandards erfüllt und gleichzeitig die Sicherheitsanforderungen Ihres Unternehmens erfüllt.

Vorbereitungen

Erforderliche Rolle: Security_Dashboard_user oder admin.

Weitere Informationen finden Sie unter Härtungseinstellungen Inhalt für detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins in ServiceNow AI Platform.

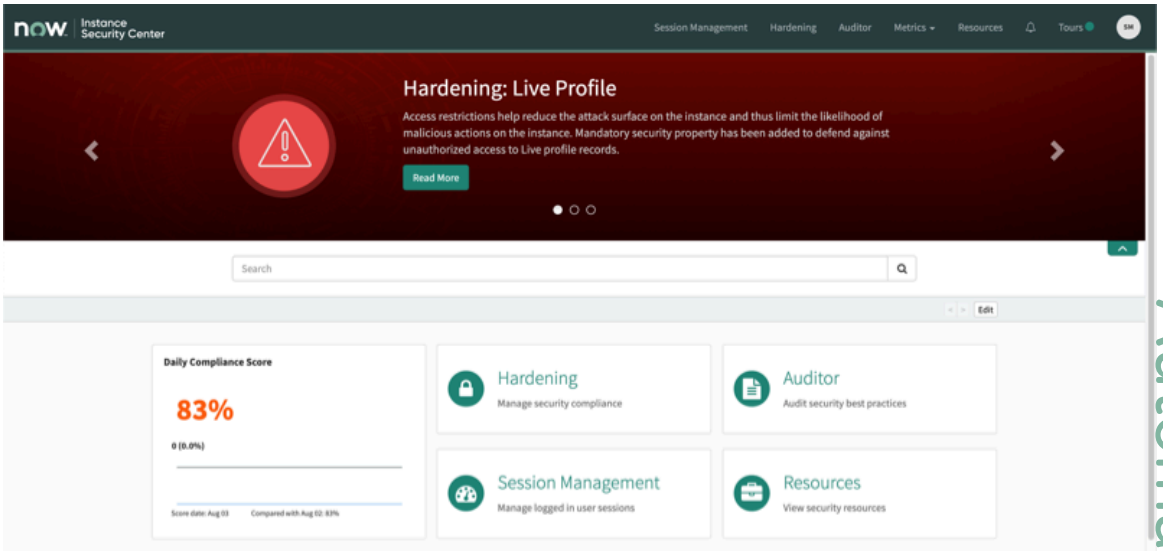
- Lesen Sie die Härtungseinstellungen für die Instanzsicherheit, wenn Sie sicherheitsbezogene Eigenschaften festlegen oder aktualisieren, auch wenn einige der Compliance-Werte möglicherweise nicht für Ihre Instanz geeignet sind.
- Wenn Sie diese Eigenschaften aktualisieren, stellen Sie sicher, dass sich die Instanz weiterhin wie erwartet verhält. Wenden Sie sich an das entsprechende interne Personal, das über das Fachwissen verfügt, um die Sicherheitsauswirkungen zu bestimmen.

Hinweis: Wenn Sie eine Administratorrolle haben, können Sie Sicherheitskontrollen anzeigen und bearbeiten. Wenn Sie über die Rolle „Security_Dashboard_user“ verfügen, können Sie Sicherheitskontrollen anzeigen, sie jedoch nicht bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**an.
2. Klicken Sie auf **Tägliche Compliance-Punktzahl** Kachel oder **Härtung** Link zum Zugriff auf die Seite „Konfiguration der Härtung-Compliance“.

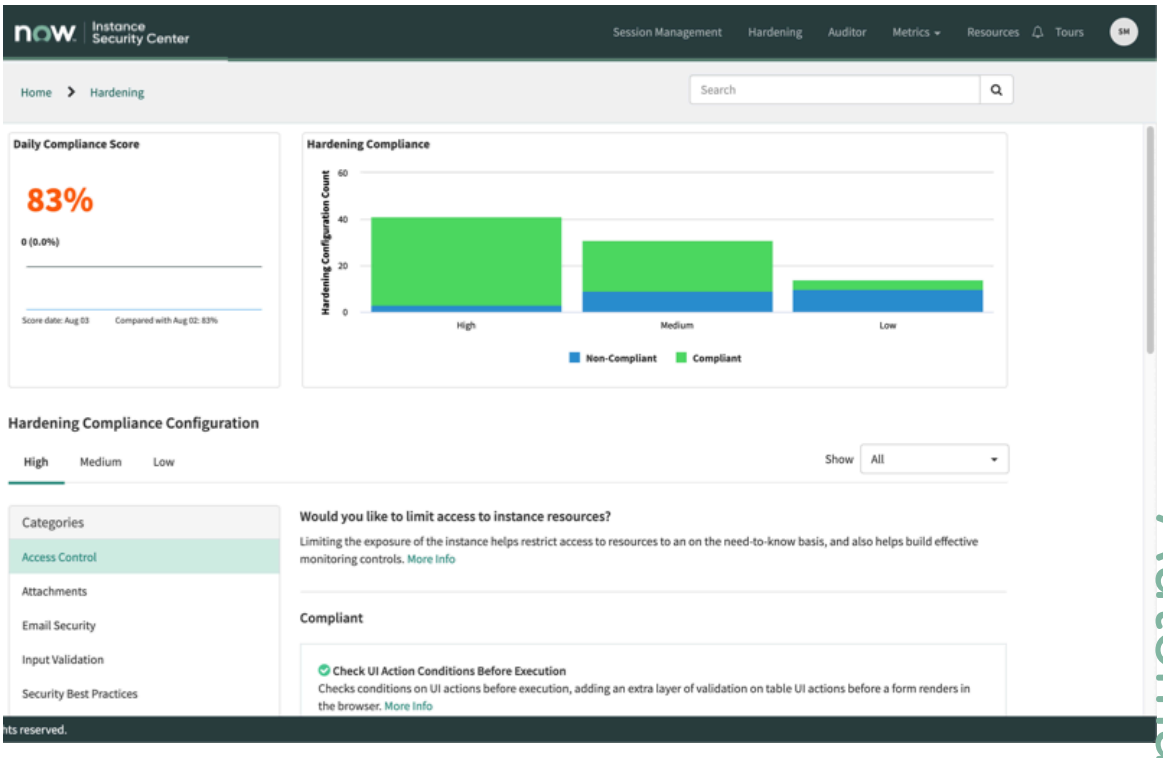


3. Zeigen Sie im Diagramm Compliance für Härtung die Statistiken für konforme und nicht konforme Sicherheitskonfigurationseigenschaften an.

Option	Bezeichnung
Konform	Anzahl der Sicherheitskonfigurationseigenschaften, die den Compliance-Werten in den Instanzsicherheitshärtungseinstellungen entsprechen. **Hinweis:** Sie können die Einstellungen für konforme Sicherheitseigenschaften in der Compliance-Konfiguration für Härtung nicht ändern. Wenn Sie dies tun möchten, müssen Sie sie in den Systemeigenschaften aktualisieren. Weitere Informationen finden Sie unter Fügen Sie eine Systemeigenschaft hinzu .
Nicht konform	Anzahl der Sicherheitskonfigurationseigenschaften, die nicht den Compliance-Werten in den Instanzsicherheitshärtungseinstellungen entsprechen. Sie können Einstellungen für nicht konforme Eigenschaften aktualisieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



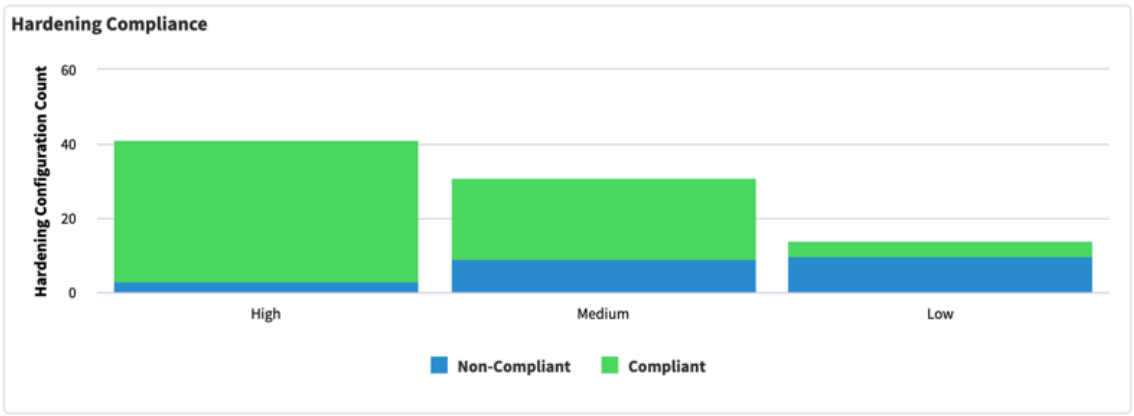
Hinweis: Um die Anzahl der konformen oder nicht konformen Sicherheitspunktzahlen über einen Datumsbereich anzuzeigen, verschieben Sie den blauen Punkt auf dem Schieberegler unter die tägliche Compliance-Punktzahl.

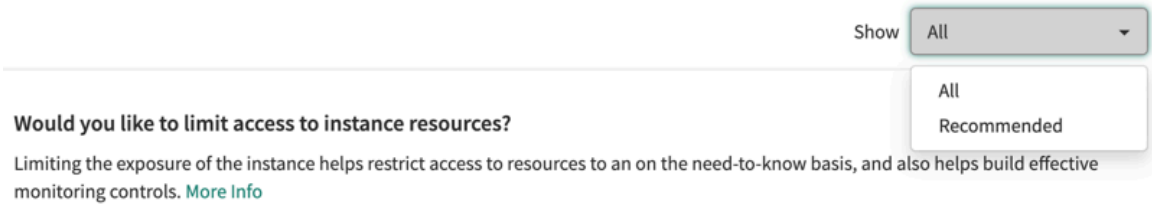
4. In **Anzeigen** Geben Sie unter dem Diagramm an, ob Sie auf alle Sicherheitskonfigurationseigenschaften oder nur empfohlene zugreifen möchten.

Option	Bezeichnung
Alle	(Standard) alle konformen und nicht konformen Sicherheitskonfigurationseigenschaften in jeder ausgewählten Kategorie.
Empfohlen	In jeder ausgewählten Kategorie werden nur empfohlene Sicherheitskonfigurationseigenschaften angezeigt. Diese Sicherheitskonfigurationseigenschaften sind eine ausgewählte Teilmenge der wichtigsten Eigenschaften, die zum Sichern von verwendet werden ServiceNow AI Platform. Betrachten Sie diese Sicherheitskonfigurationseigenschaften als die bloße Mindestanzahl von Einstellungen, die Sie festlegen müssen, um zu sichern ServiceNow AI Platform. **Hinweis:** Um Ihre Instanz vollständig zu sichern, verwenden Sie **Alle** Option. Sie enthält auch alle empfohlenen Sicherheitskonfigurationseigenschaften.

Automatische Übersetzung

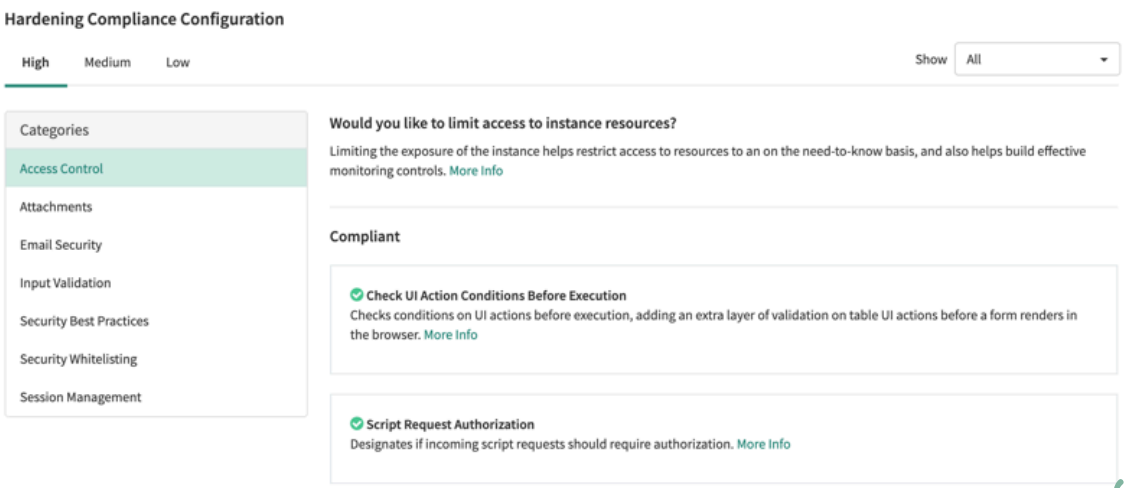
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





Automatische Übersetzung

5. In **Kategorien** Wählen Sie die Kategorie aus, die die Sicherheitskonfigurationseigenschaften enthält, auf die Sie zugreifen möchten:



Option	Bezeichnung
Zugriffssteuerung	Zugriffssteuerungen bestimmen, ob Anwenderzugriff auf eine bestimmte Ressource gewährt oder verweigert werden soll, basierend darauf, wer diese Ressourcen verwenden darf.Weitere Informationen finden Sie unter Zugriffssteuerung In den Instanzsicherheitshärtungseinstellungen.
Anhänge	Sicherheitskontrollen für Anhänge ermöglichen die Validierung eingehender Anhänge, um Ihre Instanz vor schädlichen Dateien zu schützen, die von Angreifern gesendet werden.Weitere Informationen finden Sie unter Dateimime-Typ im SOAP-Webser-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	vice „AttachmentCreator“ validieren [Neu in Security Center 1,3 und aktualisiert in 1,5] In den Instanzsicherheitshärtungseinstellungen.
E-Mail-Sicherheit	E-Mail-Sicherheit umfasst Sicherheitskonfigurationseigenschaften, die ein Administrator konfigurieren kann, um sicherzustellen, dass für alle eingehenden E-Mails die richtigen Sicherheitsrichtlinien vorhanden sind.Weitere Informationen finden Sie unter E-Mail-Spam-Bewertung und -Filterung aktivieren [aktualisiert in Security Center 1,3] In den Instanzsicherheitshärtungseinstellungen.
Eingabevalidierung	Die Eingabevalidierung enthält sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um die Eingabe fehlerhafter Daten unabhängig von der Quelle zu minimieren.Weitere Informationen finden Sie unter Validierung, Bereinigung und Codierung In den Instanzsicherheitshärtungseinstellungen.
Sichere Kommunikation	Eigenschaften für sichere Kommunikation sind diejenigen, die ein Administrator konfigurieren kann, um den HTTP-Datenverkehr zu sichern.Weitere Informationen finden Sie unter Kommunikation In den Instanzsicherheitshärtungseinstellungen.
Best Practices für Sicherheit	BEST Practices für die Sicherheit umfassen Sicherheitsaufgaben, die ein Administrator regelmäßig und innerhalb eines bestimmten Zeitintervalls ausführen sollte, und enthalten zugehörige Konfigurationseigenschaften.Weitere Informationen finden Sie unter Best Practices für Sicherheit In den Instanzsicherheitshärtungseinstellungen.
Sicherheitsaufnahmeliste	Die Sicherheitsaufschlussliste enthält sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um das Verhalten auf bekannte Aufnahmelisten zu beschränken.
Management von Benutzersitzungen	Die Sitzungsverwaltung enthält sicherheitsbezogene Eigenschaften, die ein Administrator konfigurieren kann, um eine sichere Sitzungsverwaltung in sicherzustellen ServiceNow AI Platform. Weitere Informationen finden Sie unter Management von Anwendersitzungen In den Instanzsicherheitshärtungseinstellungen

6. Konfigurieren Sie die nicht konformen Sicherheitseigenschaften in der ausgewählten Kategorie.
   - Sofern nicht anders angegeben, wird durch das Aktivieren des Schalters eine Sicherheitseigenschaft auf die empfohlene Einstellung gesetzt. Sie legen beispielsweise die meisten Steuerungen auf „wahr“ oder „falsch“ fest, einige erfordern jedoch die Eingabe eines Werts oder von Werten, z. B. einer kommagetrennten Werteliste.
   - Um auf das Thema „Dedicated Instance Security Hardening Settings“ für die Sicherheitssteuerung zuzugreifen und mehr darüber zu erfahren, klicken Sie auf **Weitere Informationen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis
Die tägliche Compliance-Punktzahl erhöht oder verringert sich je nach den Änderungen, die Sie an den nicht konformen Sicherheitssteuerungseinstellungen vornehmen.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Wie die täglichen Compliance-Punktzahlen, Trends und Diagrammdaten aktualisiert werden

Trend- und Diagrammdaten im Instanz-Sicherheitszentrum werden aktualisiert, nachdem der Performance Analytics-Auftrag um 02:00 Uhr Ortszeit ausgeführt wurde. Sie wird in der Kachel „tägliche Compliance-Punktzahl“, in den Menübändkacheln „Ereignis“ und in angezeigt Analytics Hub Seitendetail, wenn Sie auf eine der Ereigniskacheln klicken.

Der tägliche Datenverwaltungsauftrag [AppSec] ist eine regelmäßig geplante Aufgabe, die jede Nacht ausgeführt wird und die folgenden Aufgaben ausführt:

1. Überprüft, ob die Aufgaben [AppSec] tägliche Datenverwaltung und [PA AppSec] tägliche Datensammlung gültige Anwender zugewiesen wurden, wenn Sie sie zum ersten Mal planen.
   - Wenn Sie einen gültigen Anwender in eingegeben haben **Ausführen Als** Feld wird die Verarbeitung des Auftrags fortgesetzt. Ein gültiger Anwender ist ein Anwender, der nicht aus der Instanz gesperrt ist und über eine zugewiesene Administratorrolle verfügt.
   - Wenn Sie einen ungültigen Anwender eingegeben haben, wird über dem rotierenden Sicherheitsbanner im Instanz-Sicherheitszentrum eine Fehlermeldung angezeigt.

     Hinweis: Weitere Informationen zum Aktualisieren des zugewiesenen Anwenders bei der Ausführung geplanter Aufgaben finden Sie unter Erstellen oder planen Sie einen Datensammlungsauftrag .

2. Führt Geschäftslogik aus, um den Compliance-Status für die Sicherheitseigenschaften festzulegen, die Sie auf der Seite „Konfiguration der Härtung-Compliance“ konfigurieren. Weitere Informationen finden Sie unter Überprüfen Sie die tägliche Compliance-Punktzahl, und konfigurieren Sie die Einstellungen für Sicherheitseigenschaften.
3. Führt den Performance Analytics-Auftrag [PA AppSec] tägliche Datensammlung aus, um Compliance-Daten zu erfassen und die tägliche Compliance-Punktzahl zu aktualisieren.

Die tägliche Compliance-Punktzahl wird manuell aktualisiert

Wenn Ihnen eine Administratorrolle zugewiesen ist, können Sie die tägliche Compliance-Punktzahl jederzeit aktualisieren und neu berechnen, indem Sie auf klicken **Aktualisieren** .

Hinweis: Die **Aktualisieren** Die Schaltfläche wird für Anwender mit der zugewiesenen Rolle „Security_Dashboard_user“ nicht angezeigt.

- Die Funktion „Aktualisieren“ führt dieselben Aufgaben aus wie der Performance Analytics-Auftrag „tägliche Datensammlung“, führt dies jedoch in Echtzeit und nicht in einem Batch-Prozess aus.
- Sie verwenden es normalerweise, wenn Sie Aktualisierungen an der täglichen Compliance-Punktzahl durchführen möchten, um die Auswirkungen von Instanzsicherheitsaktivitäten sofort anzuzeigen.
- Es kann eine leichte Verzögerung geben, bevor die aktualisierte Punktzahl angezeigt wird.

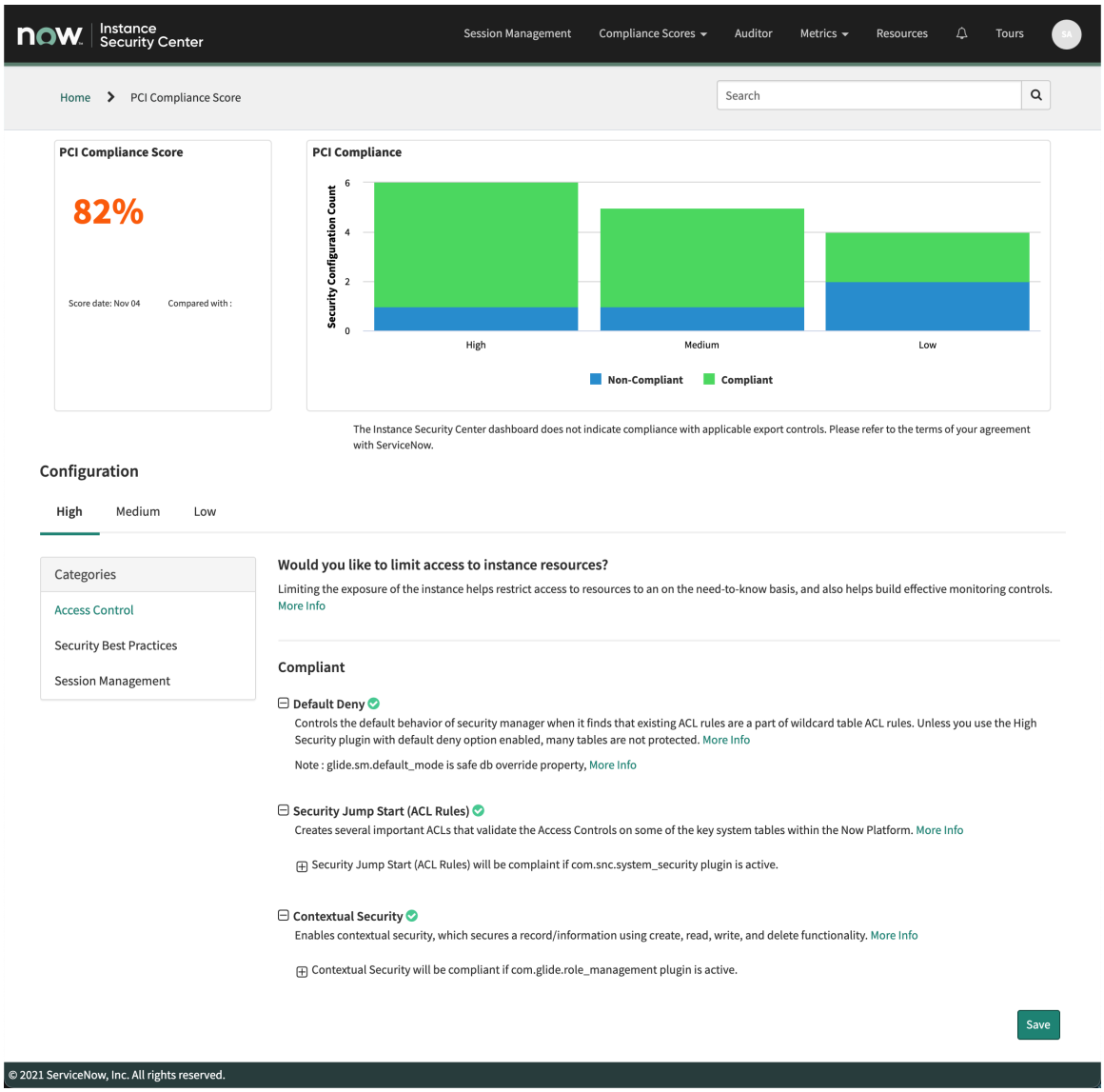
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie ein Upgrade durchführen (z. B. von London Bis Zurich), wird das Plugin „Instance Security Center“ (ISC) automatisch aktiviert. Ein bereitgestelltes Korrekturskript weist einen anwenderdefinierten Anwender automatisch ohne zugewiesene Rollen zu.

Dashboard „PCI-Compliance-Punktzahl“

Das Dashboard „PCI-Compliance-Punktzahl“ zeigt, wie Ihre Instanz den Sicherheitsstandards der Zahlungskartenbranche (PCI) entspricht. Verwenden Sie das Dashboard, um Ihre Compliance-Punktzahl anzuzeigen und Ihre Konfiguration zu ändern, um die Sicherheit zu verbessern.



Erforderliche ServiceNow AI Platform-Rollen

Security_Dashboard_user oder admin, erforderlich, um das Dashboard für die PCI-Compliance-Punktzahl anzuzeigen.

Greifen Sie auf das Dashboard „PCI-Compliance-Punktzahl“ zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**an. Klicken Sie im Instanz-Sicherheitscenter auf **Compliance-Punktzahlen** Wählen Sie im Header die Option aus **PCI-Compliance-Punktzahl** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

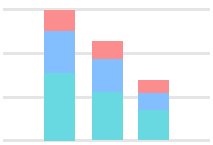
Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Sicherheits-Dashboard-Anwender (Security_Dashboard_user)	Überwachen und verwalten Sie die Compliance der Instanzsicherheit kontinuierlich.
Administrator (Administrator)	Überwachen Sie die Compliance der Instanzsicherheit kontinuierlich, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

Indikator	Beschreibung
PCI-Compliance-Punktzahl	Zeigt die Compliance-Punktzahl Ihrer Instanz als Prozentsatz an. Dieser Prozentsatz von stellt den Prozentsatz der Sicherheitskonfigurationen in Ihrer Instanz dar, die Compliance-Standards erfüllen. Der Indikator zeigt auch das Datum an, an dem die Compliance-Punktzahl berechnet wurde, und einen Vergleich mit der vorherigen berechneten Punktzahl an.

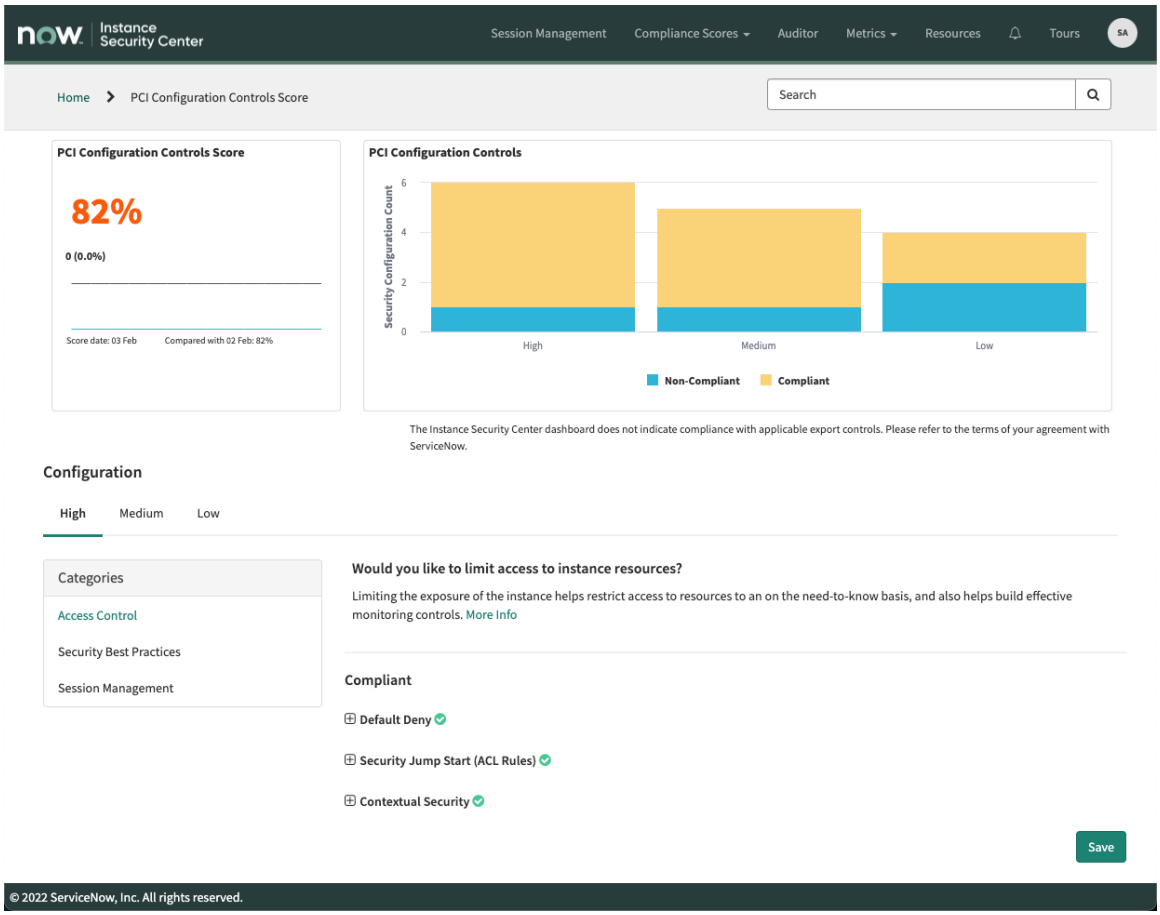
Datenvisualisierung

Titel	Typ	Quelltabelle	Beschreibung
PCI-Compliance	 Stapelbalkendiagramm	Sicherheitskonfigurationen [isc_Security_configurations]	Zeigt konforme und nicht konforme Sicherheitskonfigurationen in den Kategorien hoch, Mittel und niedrig an. Klicken Sie auf einen Bereich des Berichts, um die übereinstimmenden Sicherheitskonfigurationen anzuzeigen.

Punktzahl-Dashboard für PCI-Konfigurationssteuerungen

Verwenden Sie das Punktzahl-Dashboard für PCI-Konfigurationssteuerungen, um Ihre PCI-Konfiguration zu überprüfen und zu bestimmen, welche Sicherheitsprüfungen nicht konform sind. Sie können die Konfiguration der nicht konformen Sicherheitsprüfungen im Instanz-Sicherheitscenter ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erforderliche ServiceNow AI Platform-Rollen

Die Rolle „Security_Dashboard_user“ oder „admin“ ist erforderlich, um das Dashboard „PCI-Compliance-Punktzahl“ anzuzeigen.

Greifen Sie auf das Punktzahl-Dashboard für PCI-Konfigurationssteuerungen zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**an. Klicken Sie im Instanz-Sicherheitscenter auf **Compliance-Punktzahlen** Wählen Sie im Header die Option aus **Punktzahl der PCI-Konfigurationssteuerungen** .

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Sicherheits-Dashboard-Anwender (Security_Dashboard_user)	Überwachen und verwalten Sie die Compliance von PCI-Konfigurationssteuerungen in Ihrer Instanz kontinuierlich. Ändern Sie die PCI-Konfiguration, um Compliance sicherzustellen und die Instanzsicherheit zu verbessern.
Administrator (Administrator)	Überwachen Sie die Compliance der PCI-Konfiguration kontinuierlich, um potenzielle

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

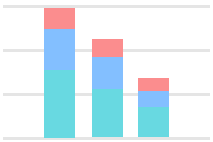
Anwender	Dashboard-Verwendung
	Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

Punktzahl der PCI-Konfigurationssteuerungen

Zeigt die Punktzahl der PCI-Konfigurationssteuerungen Ihrer Instanz als Prozentsatz an. Dieser Prozentsatz von stellt den Prozentsatz der Sicherheits-PCI-Steuerungskonfigurationen in Ihrer Instanz dar, die Compliance-Standards erfüllen. Der Indikator zeigt auch das Datum an, an dem die Compliance-Punktzahl berechnet wurde, und einen Vergleich mit der vorherigen berechneten Punktzahl an.

Datenvisualisierung

Titel	Typ	Quelltabelle	Beschreibung
PCI-Konfigurationssteuerungen	 Stapelbalkendiagramm	Sicherheitskonfigurationen [isc_Security_configurations]	Zeigt konforme und nicht konforme PCI-Steuerungskonfigurationen in den Kategorien hoch, Mittel und niedrig an. Klicken Sie auf einen Bereich des Berichts, um die übereinstimmenden Sicherheitskonfigurationen anzuzeigen.

Suchen Sie nach falschen Sicherheitsdefinitionen

Führen Sie den Auditor aus, um Ihre Instanz zu scannen und falsche Sicherheitsdefinitionen zu finden. Es liefert Ergebnisse, die Sie korrigieren können, um die Sicherheitslage Ihrer Instanz zu verbessern.

Wichtig:

Das Instanzsicherheitszentrum (ISC) hat das Ende des Verkaufs im September 2024 erreicht und wird nicht mehr unterstützt oder steht für eine neue Aktivierung zur Verfügung.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Instanz-Sicherheitszentrum an ServiceNow Security Center Migration.

Der Auditor führt eine „vollständige“ Bewertung der Instanzintegrität durch, die Ihre Systemkonfiguration analysiert. Bei Sicherheitsscans wird Ihre aktuelle Sicherheitskonfiguration mit Best Practice-Definitionen und Compliance-Werten für Sicherheitseigenschaften verglichen.

Aus Sicht der Instanzsicherheit bietet es Einblicke und Empfehlungen dazu, was Sie weiter tun sollten und wo Sie sich verbessern können. Diese Einblicke und Empfehlungen helfen Ihnen, die folgenden Fragen zu beantworten:

- Sind die entsprechenden sicherheitsbezogenen Eigenschaften festgelegt?
- Ist das Plugin „hohe Sicherheit“ aktiviert?
- Gibt es die richtigen Zugriffssteuerungsregeln?

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie den Auditor aus, und analysieren Sie die Scan-Ergebnisse

1. Um den Auditor auszuführen, klicken Sie auf **Audit** Auf der Homepage des Instanz-Sicherheitszentrums.
2. Öffnen Sie nach Abschluss die Scan-Ergebnisse, um die Sicherheitsergebnisse zu überprüfen und zu analysieren.
3. Um das Detail für ein bestimmtes Scan-Ergebnis zu überprüfen, doppelklicken Sie auf die Ergebnisnummer. Diese Informationen umfassen Status, Scan-Typ, Ausführungszeit und Fehlermeldungen.
4. Jedes Auditor-Ergebnis enthält Lösungsdetails und eine URL zu Produktinhalten, in der beschrieben wird, wie sie behandelt werden sollen. Befolgen Sie die dokumentierten Richtlinien, um die Probleme in jedem der Ergebnisse zu beheben.

Zugehörige Informationen

Härtungseinstellungen

Plugin für hohe Sicherheit aktivieren [aktualisiert in Security Center 1,3]

Regeln Für Zugriffssteuerungsliste

Überwachen Sie Instanzmetriken

Überwachen Sie Anwender-, Export-, Authentifizierungs-, E-Mail- und Virenschutzmetriken für Ihre Instanz. Sie können beispielsweise Ihre E-Mail-Sicherheit überwachen, indem Sie Metriken für Spam, externe E-Mails und eingehende E-Mails aus nicht vertrauenswürdigen und vertrauenswürdigen Domänen für Ihre Instanz überprüfen. Analysieren Sie diese Metriken, um nach anomalem Sicherheitsverhalten zu suchen, das sich auf Aktivitäten bezieht, die in Ihrer Instanz stattfinden.

Wichtig:

Das Instanzsicherheitszentrum (ISC) hat das Ende des Verkaufs im September 2024 erreicht und wird nicht mehr unterstützt oder steht für eine neue Aktivierung zur Verfügung.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Instanz-Sicherheitszentrum an ServiceNow Security Center Migration.

Anwendermetriken

Analysieren Sie Anwendermetriken, um nach anomalen Verhaltensweisen zu suchen, die sich auf bestimmte Arten von Anwenderaktivitäten in Ihrer Instanz beziehen.

Im letzten Monat/in den letzten sechs Monaten/im letzten Jahr nicht angemeldet

Gibt die Anzahl der Anwender an, die sich innerhalb des letzten Monats, innerhalb der letzten sechs Monate und innerhalb des letzten Kalenderjahres nicht bei der Instanz angemeldet haben. So zeigen Sie Anwenderdetails für eine bestimmte Metrik an:

- Klicken Sie auf die Metrik, um eine Liste der Anwender anzuzeigen, die sich während des angegebenen Zeitraums nicht bei der Instanz angemeldet haben.
- Klicken Sie auf einen Anwendernamen, um weitere Details zu diesem Anwender anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender mit Rollen mit hohen Berechtigungen

Gibt die Anzahl der Anwender mit den folgenden Rollentypen mit hohen Berechtigungen an:

Anwenderrolle	Beschreibung
Administrator	Primäre Administratorrolle, die unabhängig von Sicherheitsbeschränkungen Zugriff auf alle Systemfunktionen, -Funktionen und -Daten hat.
ais_High_Security_admin	Rolle mit erhöhten Berechtigungen, die einem Anwender den Zugriff auf Einstellungen für hohe Sicherheit für ermöglicht KI-Suche. Weitere Informationen finden Sie unter Weisen Sie Rollen zu zu zu KI-Suche Administratoren und Anwender an.
Password_Reset_admin	Administratorrolle, mit der ein Anwender den Status von Aktivitäten zum Zurücksetzen des Passworts anzeigen, potenzielle Sicherheitsbedrohungen identifizieren und die Compliance mit Passwortschutzrichtlinien überwachen kann. Weitere Informationen finden Sie unter Passwortzurücksetzung Und Passwortänderungsberichte und -Protokolle an.
Script_include_admin	Administratorrolle, die auch Zugriff auf Skripteinbindungen hat.
security_admin	Rolle mit erhöhten Berechtigungen, die es einem Anwender ermöglicht, Zugriffssteuerungen und Einstellungen für hohe Sicherheit zu erstellen und zu ändern. Weitere Informationen finden Sie unter Rolle „Security_admin“.
user_admin	Administratorrolle, die auch Anwender, Rollen, Anwendergruppen, Rollen und Abteilungszuweisungen verwalten kann.

Hinweis: Weitere Informationen zu diesen administrativen Rollentypen finden Sie unter Spezielle Administratorrollen .

So zeigen Sie Anwenderdetails für eine bestimmte Anwenderrollenmetrik an:

- Klicken Sie auf die Rollenmetrik „Anwenderanzahl“, um eine Liste der Anwender mit diesem Rollentyp mit hohen Berechtigungen anzuzeigen.
- Klicken Sie auf einen Anwendernamen, um weitere Details zu diesem Anwender anzuzeigen. Sie können dann bestimmen, ob diese sicherheitskritischen Rollen dem richtigen Personal zugewiesen sind.

Anwendertrend

Zeigt Informationen zum Anzahltrend über einen Zeitraum für die folgenden Anwendertypen an:

Anzahltyp	Beschreibung
Aktive Anwender	Anzahl der Anwender, die in der Instanz als aktiv markiert sind.
Inaktive Anwender	Anzahl der Anwender, die in der Instanz als inaktiv markiert sind.
Gesperrt	Anzahl der Anwender, die aus der Instanz gesperrt sind.

So zeigen Sie Anwenderdetails für eine bestimmte Anwenderanzahl an (z. B. gesperrte Anwender):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf **Gesperrte Anwender** Metrik.
- In Analytics Hub Seite klicken Sie auf **Datensätze Anzeigen** .
- Klicken Sie auf einen Anwendernamen, um weitere Details zu diesem Anwender anzuzeigen. Sie können dann bestimmen, ob es einen Grund gibt, aus dem diese Person gesperrt ist, und die Situation beheben.

Ereignistrend

Zeigt Informationen zum Zählungstrend für bestimmte Ereignistypen über einen Zeitraum an:

Ereignistyp	Beschreibung
Administratoranmeldung	Anzahl der Anwender mit Administratorrollen mit hohen Berechtigungen, die sich an einem bestimmten Tag angemeldet haben.
Externer Login	Anzahl der Anwender mit der zugewiesenen Rolle „snc_external“, die sich während des Kalendertages bei dieser Instanz angemeldet haben. Diese Anmeldungen erfolgen normalerweise zu Wartungs-, Support-, Beratungs- oder Audit-Zwecken. Durch die Überwachung dieser Metrik können Sie überprüfen, ob die externen Anmeldeversuche legitim sind und keine potenziellen Sicherheitsprobleme darstellen.
Anmeldung fehlgeschlagen	Anzahl der fehlgeschlagenen Anmeldeversuche an einem bestimmten Tag.
Identitätswechsel	Anzahl der an einem bestimmten Tag angemeldeten Anwender, die die Identität anderer Anwender annehmen.
Sicherheitserhöhung	Anzahl der Male, mit denen ein Sicherheitsadministrator die Sicherheit für Standardanwender erhöht hat, indem seine zugewiesene Anwenderrolle während des Kalendertages in eine Sicherheitsrolle mit hohen Berechtigungen geändert wurde. Diese Sicherheitsrollen mit hohen Berechtigungen umfassen oauth_admin, admin, Security_admin und Impersonator.
SNC-Anmeldung	Anzahl von Kundenservice und Support Wer sich an einem bestimmten Tag mit der Hi-Hopping-Technik bei dieser Instanz angemeldet hat.

So zeigen Sie Anwenderdetails für eine bestimmte Ereignisanzahl an (z. B. Identitätswechsel):

- Klicken Sie auf die Metrik „Anwenderanzahl“. Auf der Seite „Sicherheits-Dashboard-Ereignisprotokolle“ werden Ereignisprotokolle für diesen Ereignistyp aufgelistet.
- Klicken Sie auf einen Anwendernamen, um weitere Details zu diesem Ereignis anzuzeigen.

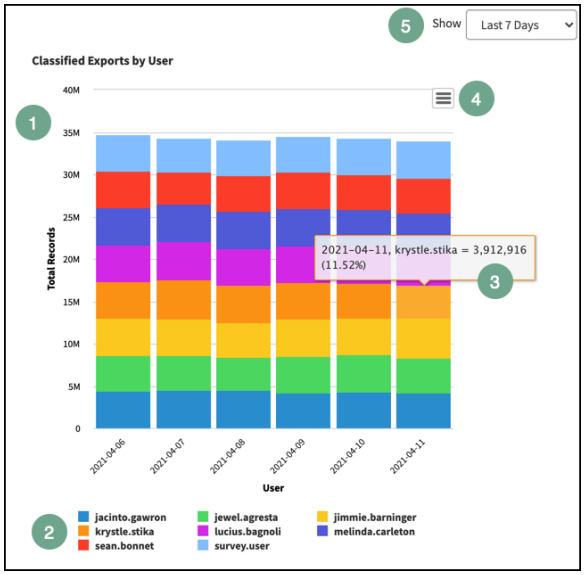
Zugehörige Informationen

Analytics Hub

Metriken exportieren

Analysieren Sie Exportmetriken, um zu sehen, welche Daten am häufigsten exportiert werden und welche Anwender die meisten Daten exportieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



1. Diagramm exportieren

In jedem Bericht wird die Anzahl der Exportereignisse nach Datum angezeigt, wobei eine farbcodierte Taste verwendet wird, um anzugeben, welche Anwender den Export durchgeführt haben. Klicken Sie auf einen farbigen Abschnitt einer Spalte, um die Liste von anzuzeigen **Ereignisse Exportieren** [isc_Export_event] Datensätze, die diesem Eintrag entsprechen.

2. Berichtsschlüssel

Der Schlüssel unten im Bericht gibt an, welche Farben welche Anwender oder Tabellen identifizieren.

3. Popup-Vorschau anzeigen

Zeigen Sie auf einen Eintrag im Diagramm, um eine Popup-Vorschau anzuzeigen. Diese Vorschau zeigt den Anwender- oder Tabellennamen sowie eine Anzahl der Exporte und einen Prozentsatz der Gesamtzahl in dieser Spalte.

4. Bildexport

Klicken Sie auf das Symbol, um den Bericht als Bild zu speichern. Sie können den Bericht im PNG- oder JPEG-Format speichern.

5. Berichtsdatumsbereich

Verwenden Sie **Anzeigen** Liste zum Anzeigen von Exporten innerhalb der letzten 24 Stunden oder innerhalb der letzten 7 Tage.

Exportieren Sie Metrikberichte

Auf der Seite „Metriken exportieren“ werden vier Berichte angezeigt.

Exporte nach Anwender

Verwenden Sie **Exporte nach Anwender** Bericht, um zu sehen, welche Ihrer Anwender die meisten Daten exportieren.

Klassifizierte Exporte nach Anwender

Verwenden Sie **Klassifizierte Exporte nach Anwender** Melden Sie sich, um zu sehen, welche Ihrer Anwender die meisten Daten exportieren, die Klassifizierungen wie vertrauliche, eingeschränkte oder persönliche Daten entsprechen. Administratoren können definieren, welche Klassifizierungen dieser Bericht in verwendet **Einstellungen** Registerkarte.

Exporte nach Tabelle

Verwenden Sie **Exporte nach Tabelle** Bericht, um zu sehen, aus welchen Tabellen am häufigsten exportiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierte Exporte nach Tabelle

Verwenden Sie **Klassifizierte Exporte nach Tabelle** Bericht, um zu sehen, aus welchen Tabellen am häufigsten exportiert werden, die Klassifizierungen wie vertrauliche, eingeschränkte oder persönliche Informationen entsprechen. Administratoren können definieren, welche Klassifizierungen dieser Bericht in verwendet **Einstellungen** Registerkarte.

Hinweis: Metrikberichte exportieren verfolgen nur Exportereignisse. Exporte aus anderen Quellen, z. B. Rest-APIs oder Workflows, werden im Rahmen dieser Funktion nicht nachverfolgt.

Metrikeinstellungen exportieren

Verwenden Sie die Konfigurationsoptionen auf der Registerkarte Einstellungen, um die Berichterstellungsergebnisse einzugrenzen.

Greifen Sie auf die Einstellungen für Ihre Exportmetriken zu, indem Sie auf klicken **Einstellungen** Registerkarte.

Konfigurationsfelder für Einstellungen

Metrikkonfigurationen exportieren

Konfiguration	Beschreibung
Klassifizierungen für Metriken	Fügen Sie diesem Feld Klassifizierungen hinzu, oder entfernen Sie sie, um zu bestimmen, welche Exporte in enthalten sind **Klassifizierte Exporte nach Anwender** Und **Klassifizierte Exporte nach Tabelle** Berichte. Diese Berichte unterstützen die folgenden Klassifizierungen: • Personenbezogene Informationen • Vertraulich • Beschränkt • Intern • Öffentlich Weitere Informationen zu Datenklassifizierungen finden Sie unter Datenklassifizierungen
Klassifizierungen für Warnungen	Fügen Sie diesem Feld Klassifizierungen hinzu, oder entfernen Sie sie, um zu bestimmen, welche Exporte Instanzsicherheitsbenachrichtigungen auslösen. Die in unterstützten Klassifizierungen **Klassifizierungen für Metriken** Feld wird hier unterstützt. Weitere Informationen zu diesen Warnungen finden Sie im Abschnitt „Sicherheitsbenachrichtigungen“ im Instanz-Sicherheitszentrum Seite. Die **Datensatzschwellenwert** Das Feld definiert die Anzahl der Datensätze, die exportiert werden, bevor Ihre Instanz ausgelöst und eine Warnung ausgelöst wird.
Datensatzschwellenwert	Anzahl des Datensatzes, den ein Anwender exportieren muss, um eine Warnung auszulösen. Um eine Warnung auszulösen, müssen diese Datensätze auch den Klassifizierungen entsprechen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikkonfigurationen exportieren (Fortsetzung)

Konfiguration	Beschreibung
	die in aufgeführt sind **Klassifizierungen für Warnungen** Feld.

Verwenden Sie **Speichern** (⌘ **+ s)** Schaltfläche zum Speichern Ihrer Einstellungen.

Authentifizierungsmetriken

Analysieren Sie Authentifizierungsmetriken, um Informationen im Zusammenhang mit der Authentifizierung anzuzeigen, z. B. selten verwendete IP-Adressen, fehlgeschlagene Anmeldungen und Typen von Authentifizierungsschemata, die von Ihren Anwendern verwendet werden.

Verwenden Sie **Authentifizierungsmetriken** Seite zum Anzeigen von Berichten zu Ihrer Authentifizierungskonfiguration. Die folgenden Berichte werden auf dieser Registerkarte angezeigt.

Hinweis: Die Seite „Authentifizierungsmetriken“ erfordert **REST API-Zugriffsrichtlinien-Plugin** Plugin (com.Glide.Rest.Policy). Weitere Informationen zu dieser Funktion finden Sie unter REST API-Zugriffsrichtlinien .

APIs ohne Authentifizierungsrichtlinien

Zeigt eine Echtzeitanzahl aller APIs ohne Zugriffsrichtlinie an

Härtung: Flow zur Account-Wiederherstellung

Härtung: Rollenbasierte MFA-Funktionseinstellung

Accounts nur für Webservice-Zugriff

Zeigt die Anzahl aller Anwenderdatensätze an, bei denen die Webservice-Zugriffsoption in aktiviert ist `User`Tabelle [sys_user].

X509-Zertifikate, die in 30 Tagen ablaufen

Zeigt eine Anzahl aller X.509-Zertifikate aus an `X.509 Certificates`[sys_certificate] Tabelle, die fällig ist, läuft in 30 Tagen ab.

Metriken der adaptiven Authentifizierung

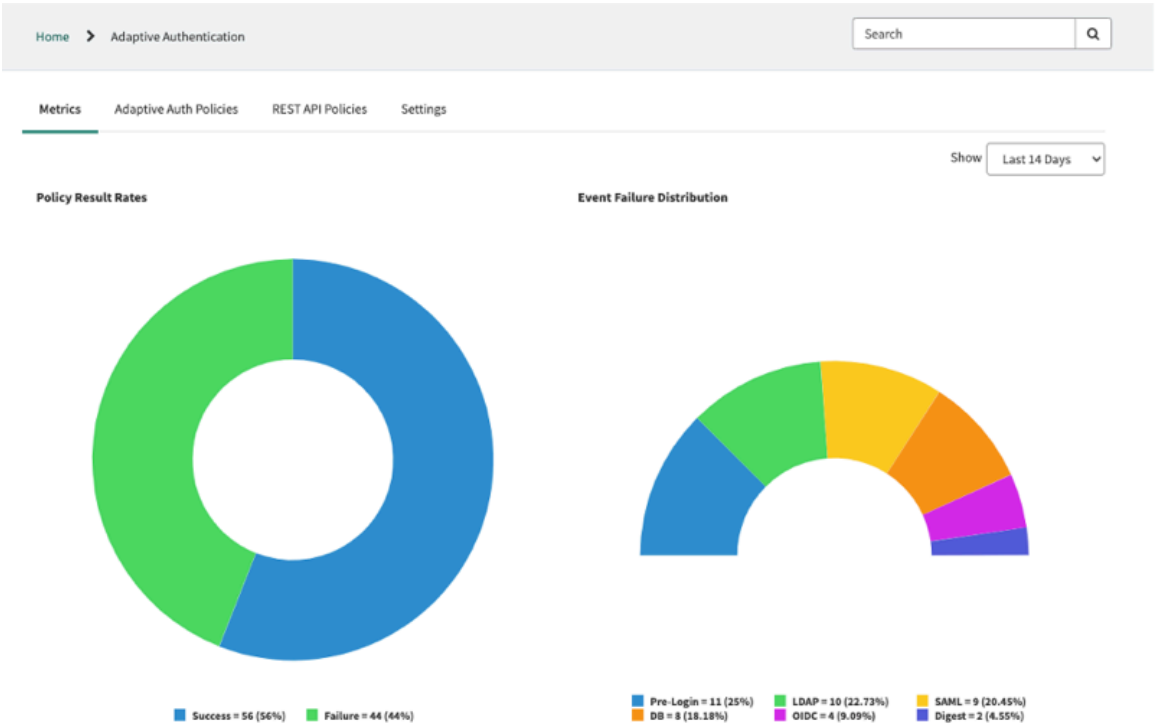
Analysieren Sie Metriken für die adaptive Authentifizierung, um zu überwachen und Einblicke in die Verwendung der adaptiven Authentifizierung in Ihrer Instanz hinzuzufügen.

Zeigen Sie Berichte, Einstellungen und Richtlinien an, die der adaptiven Authentifizierung zugeordnet sind, auf der Seite „adaptive Authentifizierungsmetriken“ an. Sicherheitsadministratoren können Berichte verwenden, um die Ergebnisse ihrer Richtlinien für adaptive Authentifizierung zu überwachen. Verwenden Sie diese Daten, um Einblicke zu erhalten und Ihre Richtlinien anzupassen, um ihre Leistung zu verbessern.

Hinweis: Die Seite „Metriken für adaptive Authentifizierung“ erfordert **Adaptive Authentifizierung** Plugin „“ (com.snc.adaptive_authentication). Weitere Informationen zu dieser Funktion finden Sie unter Adaptive Authentifizierung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken



Verwenden Sie **Metriken** Registerkarte zum Anzeigen von Berichten zu Ihrer Konfiguration der adaptiven Authentifizierung. Die folgenden Berichte werden auf dieser Registerkarte angezeigt.

- Richtlinienergebnisraten
- Ereignisfehlerverteilung
- Verteilung des Ereigniserfolgs
- Abgelehnete IP-Adressen
- Anwenderanmeldungen Für Authentifizierung
- API-Anwenderanmeldungen
- Authentifizierungstrend

Verwenden Sie **Anzeigen** Liste, um eine Zeitspanne für die angezeigten Berichte auszuwählen

Adaptive Authentifizierungsrichtlinien

Verwenden Sie **Adaptive Authentifizierungsrichtlinien** Registerkarte, um die Richtlinien und Richtlinienkontexte für die adaptive Authentifizierung in Ihrer Instanz anzuzeigen. Klicken Sie auf einen beliebigen Eintrag in diesen Listen, um den zugehörigen Datensatz anzuzeigen. Weitere Informationen zu diesen Datensätzen finden Sie unter Adaptive Authentifizierung

Einstellungen

Verwenden Sie die Registerkarte „Einstellungen“, um Systemeigenschaften der adaptiven Authentifizierung anzuzeigen und zu konfigurieren. Weitere Informationen zu diesen Eigenschaften finden Sie unter Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Metriken

Analysieren Sie Ihre E-Mail-Metriken, um nach anomalen Verhaltensweisen zu suchen, die sich auf die eingehenden E-Mails an Ihre Instanz beziehen. Wenn die Metriken beispielsweise eine Spitze in Spam-E-Mails aus bestimmten Domänen anzeigen, können Sie eingehende Aktionen definieren, die ihre Zustellung an die Instanz verhindern.

Für jede E-Mail-Metrik wird eine Anzahl für jeden E-Mail-Typ angezeigt, der während des Kalendertages an die Instanz gesendet oder gesendet wird.

Benachrichtigungseinstellung	Beschreibung
Externe eingehende E-Mail	Anzahl der eingehenden E-Mails für den Kalendertag, die von externen E-Mail-Domänen an die Instanz übermittelt wurden. **Hinweis:** Die externen E-Mail-Domänen sind die Domänen, die nicht in aufgeführt sind `security.list.internal.domains`Systemeigenschaft, da diese Eigenschaft nur Ihre internen E-Mail-Domänen nachverfolgt. Weitere Informationen zu dieser Eigenschaft finden Sie unter Verfügbare Systemeigenschaften .
Spam	Anzahl der eingehenden E-Mails für den Kalendertag, die an die Instanz übermittelt und als Spam markiert wurden. Eine Zahl, die nicht mit historischen Trends übereinstimmt, kann darauf hinweisen, dass versucht wird, die Sicherheit Ihrer Instanz zu gefährden.
Vertrauenswürdige eingehende E-Mail	Anzahl der eingehenden E-Mails an die Instanz für den Kalendertag aus E-Mail-Domänen, die als vertrauenswürdig festgelegt sind.
Nicht vertrauenswürdige eingehende E-Mail	Anzahl der eingehenden E-Mails an die Instanz für den Kalendertag aus E-Mail-Domänen, die als nicht vertrauenswürdig festgelegt sind. Sie können nicht vertrauenswürdige oder vertrauenswürdige E-Mail-Domänen im Formular „nicht vertrauenswürdige und vertrauenswürdige Domäne“ festlegen, damit Sie Ihre eingehenden E-Mails nachverfolgen können, die von ihnen gesendet werden. Informationen zum Benennen nicht vertrauenswürdiger oder vertrauenswürdiger E-Mail-Domänen finden Sie unter Legen Sie E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig fest.

Nachdem Sie auf eine E-Mail-Metrik geklickt haben, können Sie mehr über die möglichen E-Mail-Sicherheitsprobleme in Ihrer Instanz erfahren, indem Sie auf eine der folgenden Optionen klicken:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
Diagramm	Anzahl eingehender E-Mails und Anzahltrends im Zeitverlauf für den ausgewählten E-Mail-Typ (Spam, eingehende externe, nicht vertrauenswürdige oder vertrauenswürdige).
Datensätze	Einzelne E-Mail-Datensätze, die die tägliche Anzahl für den ausgewählten E-Mail-Typ beeinträchtigen.
Weitere Informationen	Zusätzliche Informationen für den ausgewählten E-Mail-Typ.

Hinweis: Die E-Mail-Metriken gelten nur für Ihre eingehenden E-Mails an die Instanz. Die Metriken gelten nicht für den normalen Datenverkehr, der über Ihre unternehmensweiten E-Mail-Server verarbeitet wird. Informationen zum Definieren eingehender Aktionen und deren Auswirkungen auf die Verarbeitung eingehender E-Mails finden Sie unter Aktionen für eingehende E-Mails .

Legen Sie E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig fest

Legen Sie bestimmte E-Mail-Domänen als nicht vertrauenswürdig oder vertrauenswürdig fest, damit Sie die Metriken für eingehende E-Mails aus diesen Quellen in Ihrer Instanz überwachen können.

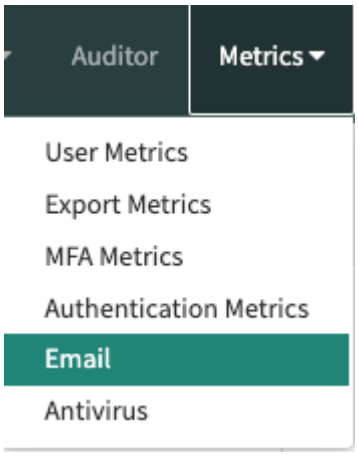
Vorbereitungen
Erforderliche Rolle: Security_Dashboard_user oder admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn nicht vertrauenswürdige oder vertrauenswürdige Domänen E-Mails an Ihre Instanz senden, wird ihre tägliche Anzahl auf der angezeigt **Nicht Vertrauenswürdige Eingehende E-Mail** Oder **Vertrauenswürdige Eingehende E-Mail** Metriken auf der E-Mail-Seite. Sie können dann E-Mail-Aktivitäten aus diesen Domänen nachverfolgen und E-Mail-Protokolle verwenden, um bestimmte eingehende E-Mails anzuzeigen. Sie können auch einen Anwender angeben, normalerweise einen Manager oder einen Sicherheitsanalyst, der benachrichtigt, wenn Aktivitäten aus der nicht vertrauenswürdigen oder vertrauenswürdigen Domäne erfolgen.

Hinweis: Die Angabe einer E-Mail-Domäne als nicht vertrauenswürdig dient nur der Sicherheitsnachverfolgung. Administratoren können auch einen Systemadressfilter einrichten, um E-Mails von nicht vertrauenswürdigen Domänen zu ignorieren. Informationen zum Filtern von E-Mails zum Blockieren ihrer Zustellung finden Sie unter Systemadressfilter .

Prozedur
1. Navigieren zu **Alle** > **Systemsicherheit** > **Instanz-Sicherheitszentrum**an.
2. Wählen Sie auf der Homepage des Instanz-Sicherheitszentrums die Option aus **E-Mail** Von **Metriken** Menü.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

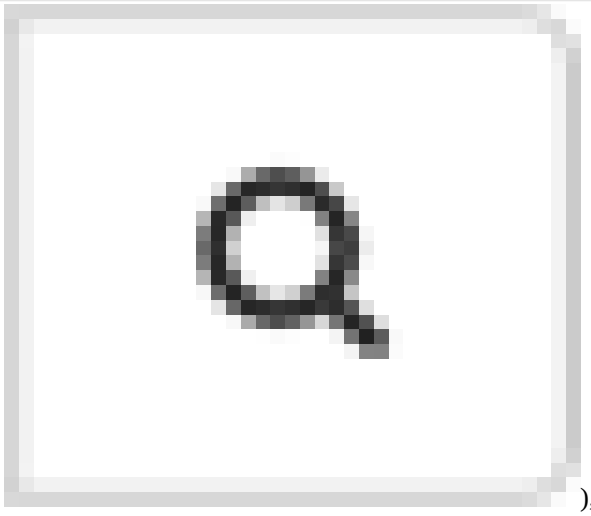


3. Klicken Sie auf der Seite E-Mail im Abschnitt nicht vertrauenswürdige und vertrauenswürdige Domänen auf **Neu** .
4. Füllen Sie im Formular die Felder aus.

Formular „nicht vertrauenswürdige und vertrauenswürdige Domäne“

Feld	Beschreibung
Domäne	Name der E-Mail-Domäne, die Sie als nicht vertrauenswürdig oder vertrauenswürdig festlegen. Geben Sie beispielsweise ein servicenow.com Zu bezeichnen ServiceNow Mitarbeiter können vertrauenswürdige E-Mails an die Instanz senden.
Kategorie	Kategorie, die angibt, ob die E-Mail-Domäne nicht vertrauenswürdig oder vertrauenswürdig ist: **Nicht vertrauenswürdige** Gibt an, dass die E-Mail-Domäne als nicht vertrauenswürdig gilt. Sie verwenden es, um Domänen zu identifizieren, die verdächtige oder E-Mails senden, die eine potenzielle Sicherheitsbedrohung an die Instanz darstellen. **Vertrauenswürdig** Gibt an, dass die E-Mail-Domäne als vertrauenswürdig gilt. Sie verwenden es, um Domänen zu identifizieren, wenn Ihre Metriken darauf hindeuten, dass die eingehenden E-Mails keine Sicherheitsbedrohungen darstellen. Wenn Sie die Domäne als vertrauenswürdig festlegen, können Sie ihre eingehende E-Mail-Aktivität im Zeitverlauf nachverfolgen.
Aktiv	Kontrollkästchen zum Aktivieren oder Deaktivieren des festgelegten Status „nicht vertrauenswürdig“ oder „vertrauenswürdig“ für die angegebene E-Mail-Domäne.
Notify	Name des Anwenders, der per E-Mail benachrichtigt werden soll, wenn Aktivität in der nicht vertrauenswürdigen oder vertrauenswürdigen Domäne auftritt. Klicken Sie auf das Spotlight-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Suchsymbol (), um nach dem Namen des Anwenders zu suchen. Verlassen Sie die **Benachrichtigen** Feld leer, wenn keine Benachrichtigungen gesendet werden sollen.

5. Wählen Sie **Speichern**.

Ergebnis

Nicht vertrauenswürdige oder vertrauenswürdige E-Mail-Domäneninformationen werden ebenfalls zu hinzugefügt **Nicht Vertrauenswürdige Und Vertrauenswürdige Domänen** Liste auf der E-Mail-Seite.

Zugehörige Informationen

Instanz-Sicherheitszentrum

E-Mail-Metriken

Virenschutzmetriken

Wenn Antivirus-Scanning Plugin ist aktiviert, Antivirus-Scanning Wird in Ihrer Instanz ausgeführt, um sie vor Vireninfektionen aus Anhängen zu schützen.

Die folgenden Metriken werden für die letzten 60 Tage der Aktivität angezeigt und ermöglichen es Ihnen, die Effektivität von zu bewerten Antivirus-Scanning Funktionen.

Antivirus-Ereignisse

Virenschutzereignisse geben die Anzahl der Virenschutzereignisse in Ihrer Instanz nach Datum an. Um auf die Antivirus-Ereignisse zuzugreifen, navigieren Sie zu **Systemsicherheit** > **Instanz-Sicherheitszentrum** Und wählen Sie die Registerkarte Metriken aus. Farbcodierte Diagrammlinien stellen die folgenden Arten von Antivirus-Ereignissen dar:

Farbe	Beschreibung
Blau	Anzahl der Dateien, die von unter Quarantäne gestellt wurden Antivirus-Scanning In diesem Fall für das angegebene Datum.
Grün	Anzahl der infizierten Dateien, die in die Instanz heruntergeladen und dann für das angegebene Datum unter Quarantäne gestellt wurden. Diese Dateien sind hauptsächlich E-Mail-Anhänge, die einen Virus- oder rouge-Code enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Farbe	Beschreibung
Gelb	Anzahl der Dateien in Quarantäne in der Instanz, die für das angegebene Datum gelöscht wurden.
Orange	Anzahl der Dateien in Quarantäne in der Instanz, die für das angegebene Datum wiederhergestellt wurden. **Hinweis:** Nach Antivirus-Scanning Führt aus und findet falsch positive Ergebnisse. Sie können eine Datei in Quarantäne wiederherstellen und sie in der Instanz zugänglich machen.

- Um auf zuzugreifen Analytics Hub Klicken Sie auf eine farbige Linie im Antivirus-Ereignisdiagramm, um die detaillierte Punktzahlkarte und Analytics-Informationen für ein bestimmtes Datum anzuzeigen. Klicken Sie beispielsweise auf die blaue Grafiklinie, um Analytics-Informationen für Dateien anzuzeigen, die für ein bestimmtes Datum unter Quarantäne gestellt wurden.
- Um die folgenden Aufgliederungen in anzuzeigen Analytics Hub Seite klicken Sie auf , Und klicken Sie dann auf:

Aufgliederung	Beschreibung
AppSec – Antivirus-Ereignisquelle	Quelle des Antivirus-Ereignisses. ○ **Beim Hochladen:** Ist aufgrund eines Uploads einer infizierten Datei aufgetreten, normalerweise eines Anhangs. ○ **Aus Quarantäne:** Ist aufgrund der Quarantäne einer infizierten Datei aufgetreten, normalerweise eines Anhangs. ○ **Beim Download:** Ist aufgrund eines Downloads einer infizierten Datei aufgetreten, normalerweise ein Anhang. ○ **Aus Datensatz:** Ist aufgrund eines infizierten Datensatzes in einer Tabelle aufgetreten.
AppSec – Antivirus-Ereignistyp	Typ des Antivirus-Ereignisses. ○ **Unter Quarantäne Gestellt:** Ist aufgrund der Quarantäne einer Datei aufgetreten, normalerweise eines Anhangs. ○ **Heruntergeladen:** Ist aufgrund eines Downloads einer Datei aufgetreten, normalerweise eines Anhangs. ○ **Wiederhergestellt:** Ist aufgrund der Wiederherstellung einer Datei in Quarantäne aufgetreten. ○ **Gelöscht:** Ist aufgrund des Löschens einer Datei in Quarantäne aufgetreten.
AppSec: Antivirus-Uploader	Name des angemeldeten Anwenders, der die Dateien hochgeladen hat, die die Quelle der von erkannten Vireninfektionen waren Antivirus-Scanning Anwendung.

Dateien in Quarantäne

Listet die infizierten Dateien in der Instanz auf, die von isoliert wurde Antivirus-Scanning:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Dateiname	Name der infizierten Datei.
Inhaltstyp	Typ des Inhalts, der in der Datei infiziert wurde. Beispiel: **Anwendung/x-dosexec** Ist eine infizierte Anwendung oder ausführbare DOS-Datei, während **Text/nur** Ist eine infizierte TXT-Datei.
Tabelle	Name der Tabelle, die die infizierte Datei enthält. Beispiel: **Incident** Wird für einen Incident-Dateidatensatz angezeigt.
Virus	Name der Datei, die von in Quarantäne gestellt wurde Antivirus-Scanning.
Erkannt	Datum und Uhrzeit der Erkennung der infizierten Datei.
Erstellt von	Name des Anwenders, der die infizierte Datei in Quarantäne gestellt hat.
Erstellt	Datum und Uhrzeit der Erstellung des Quarantänedatensatzes.
Tabellen-Sys-ID	Tabellensystembezeichner, der dem Quarantänedatensatz zugewiesen ist.

Hinweis: Sie können auch hinzufügen **Dateien In Quarantäne** Und **Virentypen** Kacheln zum Ereignis-Menüband. Weitere Informationen finden Sie unter Sicherheitsereignisse überwachen Und Konfigurieren Sie das Sicherheitsereignis-Menüband.

Zugehörige Informationen

- Antivirus-Scanning
- Antivirus-Scanning konfigurieren
- Dateien in Quarantäne werden überprüft
- Überprüfen Sie die Virenschutzaktivität
- Analytics Hub
- Performance Analytics – Aufgliederungen
- Analytics, Intelligence and Reporting

Dashboard „MFA-Metriken“

Das Dashboard „MFA-Metriken“ zeigt Informationen zur Konfiguration der Multifaktor-Authentifizierung Ihrer Instanzen an. Verwenden Sie das Dashboard, um sicherzustellen, dass Ihre MFA-Konfiguration Ihren Sicherheitsstandards entspricht.

Erforderliche ServiceNow AI Platform-Rollen

Security_Dashboard_user oder admin, erforderlich, um das Dashboard für die PCI-Compliance-Punktzahl anzuzeigen.

Greifen Sie auf das Dashboard „MFA-Metriken“ zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Systemsicherheit** > **Instanz-Sicherheitszentrum**an. Klicken Sie im Instanz-Sicherheitscenter auf **Metriken** Wählen Sie im Header die Option aus **MFA-Metriken** .

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
Sicherheits-Dashboard-Anwender (Security_Dashboard_user)	Überwachen und verwalten Sie die Compliance der Instanzsicherheit kontinuierlich.
Administrator (Administrator)	Überwachen Sie die Compliance der Instanzsicherheit kontinuierlich, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Indikatoren

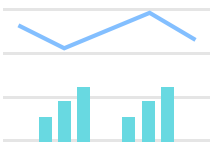
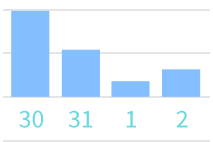
Anwender, die für MFA registriert sind

Zeigt die Gesamtzahl der Anwender in der Instanz an, die bei MFA registriert sind . Klicken Sie, um den Analytics-Hub für weitere Details zu öffnen.

Anwender, die eine MFA-Umgehung verwenden

Zeigt die Gesamtzahl der Anwender an, die die MFA-Umgehung verwenden . Klicken Sie, um den Analytics-Hub für weitere Details zu öffnen.

Datenvisualisierungen

Titel	Typ	Quelltabelle	Beschreibung
MFA-Anwender mit hohen Berechtigungen	Balken 		
MFA-Anwendertrend	 Trend		

Aktivieren Sie ISC Virtual Agent Schnittstelle

Wenn Sie die Administratorrolle innehaben, können Sie ISC aktivieren Virtual Agent Plugin „Konversationen“ (com.Glide.isc_virtualagent). Durch die Aktivierung dieses Plugins wird installiert Virtual Agent Und Natural Language Understanding(NLU Inhaltspakete, bereitstellen Virtual Agent Zugriff über das Instanz-Sicherheitszentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Wichtig:

Das Instanzsicherheitszentrum (ISC) hat das Ende des Verkaufs im September 2024 erreicht und wird nicht mehr unterstützt oder steht für eine neue Aktivierung zur Verfügung.

ServiceNow Security Center (SSC) ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Instanz-Sicherheitszentrum an ServiceNow Security Center Migration.

Die Virtual Agent Die Schnittstelle im Instanz-Sicherheitszentrum ist nur für Anwender mit kostenpflichtigen verfügbar Virtual Agent Abonnements und, die das Plugin „Glide Virtual Agent“ (com.glide.cs.chatbot) aktiviert haben. Weitere Informationen finden Sie unter Aktivieren Sie Virtual Agent .

Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Der ISC Virtual Agent Mit der Schnittstelle können Sie die folgenden Aufgaben ausführen:

- Stellen Sie sicherheitsbezogene Fragen, und erhalten Sie dann schnelle Zusammenfassungsantworten und Referenz-Links, um mehr zu erfahren.
- Erhalten Sie Antworten zu Instanzsicherheitszentrum, Plattformsicherheit, ServiceNow-Sicherheitsrichtlinien, Vertrauen, Governance, Risiko und andere Prozesse.
- Suchen Sie im Now Support-Sicherheitsportal nach sicherheitsbezogenen Ressourcen, z. B. Knowledge Base-Themen.

Plugins für ISC Virtual Agent

Plugin	Beschreibung
ISC Virtual Agent Konversationen [Com.Glide.isc_virtualagent]	Aktiviert ISC Virtual Agent Inhaltspaket für Konversationen für das Instanz-Sicherheitszentrum.
ISC NLU Modell für Virtual Agent Konversationen [Com.Glide.isc_nlu]	Aktiviert Natural Language Understanding(NLU) Inhaltspaket für das Instanz-Sicherheitszentrum.

Hinweis: Durch die Aktivierung des Plugins com.Glide.isc_virtualagent wird com.Glide.isc_nlu automatisch aktiviert. Wenn Sie jedoch zuerst das Plugin com.Glide.isc_nlu aktivieren, müssen Sie auch com.Glide.isc_virtualagent manuell aktivieren.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Härtungseinstellungen

Die ServiceNow Der Inhalt der Sicherheitscenter-Härtungseinstellungen (SSC) enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins in ServiceNow AI Platform. Sie können diese Eigenschaften mit der App „Härtungseinstellungen“ im Sicherheitscenter festlegen.

Übersicht und Zweck

Das Sicherheitscenter berechnet eine tägliche Compliance-Punktzahl, ausgedrückt als Prozentsatz, der darauf basiert, wie konform Ihre aktuellen Instanzsicherheitseinstellungen mit den Compliance-Werten in den Sicherheitscenter-Härtungseinstellungen sind.

Sie können die spezifischen Sicherheitskonfigurationseinstellungen, die sich auf die Punktzahl für Ihre Instanz auswirken können, direkt im Sicherheitscenter verwalten.

Die Konfigurationen der Härtungseinstellungen werden mit mehreren Attributen erläutert, die in der Tabelle beschrieben werden.

Details zur Konfiguration der Härtungseinstellungen

Konfigurationsattribut	Beschreibung
Übersicht	Bietet einen allgemeinen Überblick über die Empfehlung.
Konfigurationsname	Die Eigenschaft oder der Plugin-Name.
Konfigurationstyp	Beschreibt, wo die Eigenschaft außerhalb des Sicherheitszentrums konfiguriert werden kann, z. B. in Systemeigenschaften (*sys_properties_list.do*).
Datentyp	Beschreibt den Typ des Werts, der für die Konfiguration erforderlich ist. Beispiele sind „wahr/falsch“, „boolescher Wert“, „Installation“, „Plugin“, „Zeichenfolge“ usw.
Empfohlener Wert	Der Wert, der vom Sicherheitscenter zur Verbesserung der Sicherheits-Compliance in Ihrer Instanz empfohlen wird.
Standardwert	Der Wert, auf den die Konfiguration im Basissystem festgelegt ist.
Kategorie	Der Name und der Link zur Kategorie für die Härtungseinstellung.
Sicherheitsrisiko	**Schweregradpunktzahl** : Die Punktzahl gibt das potenzielle Sicherheitsrisiko für Ihre Instanz entsprechend der Wahrscheinlichkeit an, dass die Schwachstelle ausgenutzt wird. Die Sicherheitslücke wird einzeln anhand der CVSS-Punktzahl (Common Vulnerability Scoring System) auf einer Skala von berücksichtigt und bewertet **0,0** Bis **10,0** . Weitere Informationen finden Sie unter https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator .
	Schweregradbewertung pro CVSS-Punktzahl :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details zur Konfiguration der Härtungseinstellungen (Fortsetzung)

Konfigurationsattribut	Beschreibung
	• Kritisch: 9,0-10,0 • Hoch: 7,0–8,9 • Mittel: 4,0–6,9 • Niedrig: .01-3.9 • Keine: 0,0
	Sicherheitsrisikodetails : Beschreibt die Wichtigkeit der Einstellungskonfiguration und das Risiko, dass die empfohlene Konfiguration nicht verwendet wird.
Abhängigkeiten und Voraussetzungen	Zugehörige Einstellungen oder Konfigurationen, die vor oder in Verbindung mit der Härtungskonfiguration erforderlich sind.
Funktionale Auswirkung	Die Auswirkung dieser Härtungseinstellung auf den Betrieb Ihrer Instanz.
Referenzen	Links zur Konfigurationsdokumentation oder anderen hilfreichen Informationen.

Hinweis: Einige der Konfigurationen können nur bis abgeschlossen werden Kundenservice und Support Und werden als solche angegeben.

Weitere Informationen dazu, wie Sie sicherstellen, dass Ihre Instanzen die Härtungsanforderungen erfüllen, finden Sie unter Sicherheitshärtung.

Andere Ressourcen

Für Anwenderreferenz: ServiceNow AI Platform Verwaltet umfassende Informationen zu Konfigurationsfunktionen in der Produktdokumentation. Sie greifen über die in gefundenen Links auf die meisten Sicherheitsinhalte zu Instanz sichern. Weitere Informationen finden Sie unter:

- Verfügbare Systemeigenschaften
- Eigenschaften der allgemeinen Sicherheitseinstellungen
- Strenge Sicherheitseinstellungen

Baseline-Versionen der Härtungseinstellungen

Erkunden Sie, wie Baseline-Versionen für Härtungseinstellungen an Familien- und Store-Releases ausgerichtet sind.

Security Center Funktioniert, indem eine Teilmenge von Systemeigenschaften aus einer Instanz erfasst und deren Konfigurationsdetails zusammen mit den Sicherheitsauswirkungen einer Nichteinhaltung in der App angezeigt werden. Die Baseline dient als Referenzpunkt für die Systemeigenschaften, die mit jedem Release der Security Center-App erfasst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Baseline-Übersicht für Härtungseinstellungen

Sicherheitscenter-Version	Baseline-Version der Härtungseinstellung	Unterstützte Familien	Release-Datum des Stores	Standardmäßig mit installiert
SSC v1.1	Baseline v1.0	Utah, Vancouver	Mai 2023	Vancouver-Familie
SSC v1.2	Baseline v1.0	Utah, Vancouver	Aug. 2023	Nur Store
SSC v1.3	Baseline v2.0	Vancouver, Washington DC	November 2023	Washington-Familie
SSC v1.5	Baseline v4.0	Washington DC, Xanadu	Mai 2024	Xanadu
SSC v1.6	Baseline v4.0	Washington DC, Xanadu	August 2024	Nur Store
SSC V 2,0	Baseline v5.0	Xanadu, Yokohama	November 2024	Yokohama

Neue Härtungseinstellungen

Neue Härtungseinstellungen werden nach Baseline-Release aufgeschlüsselt.

Neue Härtungseinstellungen für Baseline 7,0

Mit der Security Center-Baseline-Version 7,0 wurden neue Härtungseinstellungen veröffentlicht.

- Bereichsübergreifende Berechtigungsprüfungen im Serviceportal-Formular aktivieren [Neu in Security Center 7,0]
- Abfrage-ACLs für Glide DB-Funktionen validieren [Neu in Security Center 7,0]
- Dokumentklassifizierung verwenden, um öffentlich zugängliche Dokumente einzuschränken [Neu in Security Center 7,0]
- Schreibzugriff auf Systemfelder auf Administratoranwender beschränken [Neu in Security Center 7,0]
- Genehmigung für Änderungen der Agent-basierten Office 365-Gruppenmitgliedschaft erforderlich [Neu in Security Center 7,0]
- Vertrauliche Tabellen und Felder von der Datengenerierung ausschließen [Neu in Security Center 7,0]
- Leserollen für Katalogvariablensuche erzwingen [Neu in Security Center 7,0]
- Gültige Auswahl für Abfragezeichenfolge erzwingen [Neu in Security Center 7,0]
- Eingeschränkte Bindungsfunktionalität in Fallbearer-Autorisierung [Neu in Security Center 7,0]
- Ressourcenbesitzer-Passwortanmeldeinformationen (ROPC) in OAuth 2-Tokengewährungen deaktivieren [Neu in Security Center 7,0]
- Zertifikatvertrauen erzwingen [aktualisiert in Security Center 1,3, Wurde in 2,0 entfernt , Hinzugefügt in 7,0]
- Verwendung von 3DES-Schlüsseln verhindern [Neu in Security Center 7,0]
- HTML-Links zu vertrauenswürdigen Domänen in den Beschreibungsfeldern des Impact Workspace-Moduls zulassen [Neu in Security Center 7,0]
- Stellen Sie sicher, dass die Kontextsuche keine nicht validierte Umleitung enthält [Neu in Security Center 7,0]
- HTML in den Beschreibungsfeldern des Impact Workspace-Moduls bereinigen [Neu in Security Center 7,0]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Härtungseinstellungen für Baseline-Version 6,0

Mit der Security Center-Baseline-Version 6,0 wurden neue Härtungseinstellungen veröffentlicht.

- Erzwingen Sie anwendungsspezifische ACLs nur für Anwendungsdaten
- Deaktivieren Sie die Nutzung der Legacy-JQuery-UI
- Empfehlungen für UI-Seiten mit hohem Risiko anzeigen
- Erzwingen Sie aktuelle Compliance-Anforderungen für Passwortrichtlinien bei der Anmeldung
- Verhindern, dass Anwender eine Warnung zur Umgehung der CSRF-Validierung akzeptieren [aktualisiert in Security Center 1,3 und 1,5]
- Legen Sie die minimale Passwortlänge fest [Aktualisiert im Sicherheitscenter 2,2]
- Beschränken Sie die Sitzungsdauer für Sitzungen mit hoher Sicherheit
- Deaktivieren Sie veraltete TLS-Versionen
- Deaktivieren Sie die lokale Anmeldung für Anwender mit aktiviertem Single Sign-on (SSO)
- Reduzieren Sie die zulässigen Umgehungen für das Multifaktor-Setup
- Verhindern Sie, dass der Anwender seine Identität ausnimmt, Anwendungsdaten anzuzeigen
- Ausführliche HTTP-Anforderungsprotokollierung verhindern
- Aktivieren Sie den Relaisstatus in SAML-Anforderungen, um Wiederholungsangriffe zu verhindern
- Minimieren Sie fehlgeschlagene Anmeldeversuche für Sitzungen mit hoher Sicherheit
- Wenden Sie Richtlinien für kontinuierliche Authentifizierung auf mobile Sitzungen an
- Deaktivieren Sie die Verwendung des TripleDES/3DES-Verschlüsselungsalgorithmus

Neue Härtungseinstellungen für Baseline-Version 5,0

Mit der Security Center-Baseline-Version 5,0 wurden neue Härtungseinstellungen veröffentlicht.

- ACL für HR-Lebenszyklusereignisdaten erzwingen [Neu in Security Center 2,0]
- Alle übersetzten HTML-Felder bereinigen [Neu in Security Center 2,0]
- Allow-Liste für Serviceportal-Widgets konfigurieren [Neu in Security Center 2,0]
- ACL für HR-Kerndaten erzwingen [Neu in Security Center 2,0]
- ACL für HR Virtual Agent-Daten erzwingen [Neu in Security Center 2,0]
- Allow-Liste für Tabelle „Serviceportal-Widgets konfigurieren“ [Neu in Security Center 2,0]
- Sicherheitsumfang für Serviceanwendungsinformationen erzwingen [Neu in Security Center 2,0]
- Erstellung einer leeren ACL verhindern [Neu in Security Center 2,0]
- Nicht authentifizierten Zugriff auf den eingebetteten Webclient von Virtual Agent verhindern
- Automatische Token-Bereinigung für Token-Anmeldeinformationen festlegen [Neu in Security Center 2,0]
- Globale App-Entwicklung nach Rolle einschränken [Neu in Sicherheitscenter 2,0]
- ACLs für codierte Abfrage im Widget „einfache Liste“ aktivieren [Neu im Sicherheitscenter 2,0]
- Sitzung nach Ablauf des OAuth-Tokens für ungültig erklären [Neu in Security Center 2,0]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zulässige untergeordnete MIME-Typen festlegen [Neu in Security Center 2,0]
- Identitätswechsel auf Administrator beschränken [Neu in Security Center 2,0]

Neue Härtungseinstellungen für Baseline-Version 4,0

Mit der Security Center-Baseline-Version 4,0 wurden neue Härtungseinstellungen veröffentlicht.

- Überprüfe überflüssige explizite Rollenzugriffssteuerungsbedingungen [entfernt in Security Center 1,5]
- Abfrageregeln für Arbeitsauftragsmanagement für Serviceorganisationen aktivieren [Neu in Security Center 1,5 und aktualisiert 2,0]
- Lesezugriff für Flow-Kontext einschränken [Neu in Security Center 1,5]
- Intervall für richtlinienbasierten Sitzungszugriff für mobile Aktualisierungstoken begrenzen [Neu in Security Center 1,5]
- Richtlinienbasierten Sitzungszugriff für Mobilgeräte aktivieren [Neu in Security Center 1,5]
- Verhindern, dass sich inaktive Anwender anmelden [Neu in Security Center 1,5]
- Administratorrollen für Ereignismanagement-Zuweisungsgruppe konfigurieren [Neu in Security Center 1,5]
- Sicherheitsbereich für Mitarbeiterbereich für HR-Fallmanagement erzwingen [Neu in Security Center 1,5 und aktualisiert 2,0]
- Playbook für Lizenz und Erlaubnis für den Sicherheitsumfang erzwingen [Neu in Security Center 1,5 und aktualisiert 2,0]

Neue Härtungseinstellungen für Baseline-Version 2,0

Mit der Security Center-Baseline-Version 2,0 wurden neue Härtungseinstellungen veröffentlicht.

- Stellen Sie sicher, dass ACLs der Archivtabelle aktiviert sind [Neu in Security Center 1,3 und aktualisiert in 1,5]
- Einschränkungen des Anwendungsbereichs erzwingen [Neu in Security Center 1,3 und entfernt in 1,5]
- Sicherheitsmanager für gesicherte Java aktivieren [Neu in Security Center 1,3]
- Zertifikatwiderruf verifizieren [Neu in Security Center 1,3]
- Beim Hintergrund der mobilen Anwendung muss die Zwischenablage gelöscht werden [Neu in Security Center 1,3 und aktualisiert 1,5]
- Plugin „geschützte Tabellen“ aktivieren [Neu in Security Center 1,3]
- Strikte Erhöhungsberechtigung erzwingen [Neu in Security Center 1,3]
- Lebensdauer der aktiven Sitzungen von Integrationen begrenzen [Neu in Security Center 1,3]
- Inaktive Sitzungen proaktiv für ungültig erklären [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]
- Aktivieren Sie das MID-Audit-Protokoll [Neu in Security Center 1,3 Und aktualisiert in 1,5]
- Verwendung des Vorgangs „mehrere sichere Einfügungen“ in der Importsatz-API [Neu in Security Center 1,3]
- OCSP-Prüfung bei Netzwerkfehler erzwingen [Neu in Security Center 1,3 und aktualisiert in 2,0]
- Sicherheitsregeln für die Freigabe von Dashboards erzwingen [Neu in Security Center 1,3]
- oauth-Parameter auf POST-Textkörper beschränken [Neu in Security Center 1,3]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anhangsgröße in Trainings- und Vorhersageflows für GraphQL-Endpunkte begrenzen [Neu in Security Center 1,3 und aktualisiert 1,5]
- Legacy-Verhalten für GlideRecord-Umfangsabgrenzung deaktivieren [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]
- Nutzung des Anmeldeinformationsalias erzwingen [Neu in Security Center 1,3 Und aktualisiert 1,5]
- Erforderliche jms-Connection Factorys [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]
- Anhangsgröße in Trainings- und Vorhersageflows begrenzen [Neu in Security Center 1,3 Und aktualisiert 1,5]
- Audit-Ereignisse für Protokollsitzungen [Neu in Security Center 1,3 und aktualisiert in 1,5]
- Schreibzugriff für den Zugriff auf die Seite „Servicekatalog hinzufügen“ erforderlich [Neu in Security Center 1,3]
- Aktive Sitzungszeitüberschreitungsausnahmerollen definieren [Neu in Security Center 1,3]
- Zertifikatbasierte Authentifizierung nicht erzwungen [Neu in Security Center 1,3]
- Bereichsbezogenen ACL-Zugriff für Playbooks für Informationsanforderungen erzwingen [neu in Security Center 1,3 und aktualisiert 1,5]
- Anwenderkommentare zu Artikeln ausblenden [Neu in Security Center 1,3]
- Stellen Sie sicher, dass die Erstellung/Löschung von Dashboards eine Zugriffsprüfung erfordert [Neu in Security Center 1,3 und aktualisiert in 2,0]
- Anforderungen für Geräteverschlüsselung und Passcode erzwingen [Neu in Security Center 1,3]
- Dateimime-Typ im SOAP-Webservice „AttachmentCreator“ validieren [Neu in Security Center 1,3 und aktualisiert in 1,5]
- Zertifikatwiderruf verifizieren [Neu in Security Center 1,3]
- Identitätswechsel bei ACL-Bewertung in HR-App überprüfen [Neu in Security Center 1,3 Und aktualisiert in 1,5]
- Captcha für Gast-Walk-up-Experience in der Kundenserviceanwendung [Neu in Security Center 1,3 Und aktualisiert 1,5]
- Authentifizierung für Ereignismanagement-HTTP-Prozessor anfordern [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0]
- Lebensdauer der aktiven Sitzung des Gastes begrenzen [Neu in Security Center 1,3]
- Klonen von Zielen nicht zulassen [Neu in Security Center 1,3]
- Sicherheitsrichtlinie für sichere Inhalte für svg-Dateien festlegen [Neu in Security Center 1,3]
- Validierungszeit des Anti-CSRF-Tokens [Neu in Security Center 1,3]
- Zugriff auf Knowledge Bases beschränken [Neu in Security Center 1,3]
- Umfangssicherheit für digitale Services des öffentlichen Sektors erzwingen [neu in Security Center 1,3]
- HR-Fallaktualisierungen aus persönlichen E-Mails beschränken [Neu in Security Center 1,3 Und aktualisiert 1,5]
- Lebensdauer der aktiven UI-Sitzung begrenzen [Neu in Security Center 1,3]
- Sichere Referrer-Richtlinie erzwingen [Neu in Security Center 1,3]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Härtungseinstellungen aktualisiert

Aktualisierte Härtungseinstellungen werden für jedes Baseline-Release aufgeschlüsselt.

Härtungseinstellungen für Baseline-Version 6,0 aktualisiert

Einige Härtungseinstellungen wurden mit dem Release der Security Center-Baseline-Version 6,0 aktualisiert.

Dokumentation	FTP-Anwendernamen
Nicht authentifizierten Zugriff auf den eingebetteten Webclient von Virtual Agent verhindern	• Neue Kurzbeschreibung: Nicht authentifizierten Zugriff auf den eingebetteten Virtual Agent-Webclient verhindern • Alte Kurzbeschreibung: Öffentlich zugänglicher Virtual Agent eingebetteter Webclient sn_va_Web_Client_App_embed
Erstellung einer leeren ACL verhindern [Neu in Security Center 2,0]	Regel: Skript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
ACLs für codierte Abfrage im Widget „einfache Liste“ aktivieren [Neu im Sicherheitscenter 2,0]	• CVSS-Punktzahl (Neu): 4,3 • CVSS-Punktzahl (alt): 5,3
Alle übersetzten HTML-Felder bereinigen [Neu in Security Center 2,0]	• CVSS-Punktzahl (Neu): 4,6 • CVSS-Punktzahl (alt): 8,8
HTML-Bereinigung aktivieren [aktualisiert in Security Center 1,3]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
X-Frame-options implementieren: SAMEORIGIN-Sicherheitsheader [aktualisiert in Security Center 1,3]	• CVSS-Punktzahl (Neu): 5,9 • CVSS-Punktzahl (alt): 7,1
Zugriff auf skriptfähige GlideSystemUserSession-API beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Korrektur (Neu): Stellen Sie die Eigenschaft sicher `glide.sandbox.usersession.allow_unsanitized_mess` auf festgelegt **Falsch**. Wenn für diese Eigenschaft kein Systemeigenschaftsdatensatz [sys_properties] vorhanden ist, erstellen Sie einen. • Korrektur (alt): Stellen Sie die Eigenschaft sicher `glide.sandbox.usersession.allow_unsanitized_mess` auf festgelegt **Falsch**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Klonen von Zielen nicht zulassen [Neu in Security Center 1,3]	• Beschreibung (Neu): Wenn *glide.db.clone.allow_clone_target*Ist nicht auf den empfohlenen Wert von festgelegt **Falsch** , Dann kann die Instanz als Klonziel oder als Datensatz verwendet werden, der die Instanz-URL und die Anmeldeinformationen für das Klonen angibt. Ein Systemklon ist, wenn alles in einer Datenbank von einer Instanz in eine andere kopiert wird. Dies ist ein Sicherheitsrisiko, da die Instanzdatenbank beim Klonen überschrieben werden kann, was zu Datenverlust und mangelnder Datenintegrität führt. Stellen Sie dies als Korrektur sicher *glide.db.clone.allow_clone_target*Ist auf festgelegt **Falsch** . Wenn diese Eigenschaft nicht auf den empfohlenen Wert „falsch“ festgelegt wird, kann die Instanz als Klonziel verwendet werden. Dies ist ein Sicherheitsrisiko, da die Instanzdatenbank beim Klonen überschrieben werden kann. • Beschreibung (Alt): Wenn *glide.db.clone.allow_clone_target*Ist nicht auf den empfohlenen Wert von festgelegt **Falsch** , Dann kann die Instanz als Klonziel verwendet werden. Dadurch besteht das Risiko, dass die Instanzdatenbank durch den Klonprozess überschrieben wird, was zu Integritäts- und Verfügbarkeitsverlusten führt.
oauth-Parameter auf POST-Textkörper beschränken [Neu in Security Center 1,3]	• CVSS-Punktzahl (Neu): 4,2 • CVSS-Punktzahl (alt): 7,4
Prüfung der URL-Zulässigkeitsliste erzwingen [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Beschreibung (Neu): Wenn *glide.security.url.whitelist.strict_check*Ist nicht auf den empfohlenen Wert von festgelegt **Wahr** Dann sind alle externen URLs für die Umleitung zulässig, wenn *glide.security.url.whitelist*Ist leer. Wenn *glide.security.url.whitelist*Ist nicht leer, dann sind nur externe URLs auf der weißen Liste zulässig. Daher beide Einstellungen *glide.security.url.whitelist.strict_check*Auf „wahr“ ODER „Sicherstellen“ *glide.security.url.whitelist*Ist auf einen nicht leeren Wert mit den zulässigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	externen URLs festgelegt, sodass sich die Instanz in einem sicheren Status befindet. Wenn alle externen URLs umgeleitet werden dürfen, kann ein Angreifer einen Anwender auf eine schädliche Website umleiten. • Beschreibung (Alt): Wenn *glide.security.url.whitelist.strict_check*lst nicht auf den empfohlenen Wert von festgelegt **Wahr** , Und wenn *glide.security.url.whitelist*lst nicht auf die genehmigte URL einer Organisation festgelegt, dann sind alle externen URLs zur Weiterleitung zulässig. Dies kann einem Angreifer ermöglichen, einen Anwender zu einer schädlichen Website umzuleiten. • CVSS-Punktzahl (Neu): 6,3 • CVSS-Punktzahl (alt): 8,3
Validierung der XMLdoc2-Entität mit zulässiger Entitätserweiterung anfordern [aktualisiert in Security Center 1,3]	• Wenn **Glide.stax.Whitelist_enabled** Systemeigenschaft ist in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden oder nicht auf den empfohlenen Wert festgelegt **Wahr** , Dann sind alle externen Entitäten zulässig, wenn **Glide.stax.allow_Entity_Resolution** Systemeigenschaft ist auf den Wert von festgelegt **Wahr** . Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie **Glide.stax.allow_Entity_Resolution** Systemeigenschaft zum Deaktivieren der Erweiterung externer Entitäten. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten. ◦ Wenn Sie festgelegt haben **Glide.stax.allow_Entity_Resolution** Bis **Wahr** , Alle externen Entitäten versuchen, Betreffentitäten aufzulösen oder zu erweitern, abhängig von der Einstellung von **Glide.stax.Whitelist_enabled** Eigenschaft. ◦ Wenn Sie festgelegt haben **Glide.stax.allow_Entity_Resolution** Bis **Falsch** , Alle Entitätsauflösungen und -Erweiterungen sind blockiert. Weitere Informationen zu dieser Eigenschaft

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	finden Sie unter Deaktivieren Sie die Entitätserweiterung im XMLDocument2-Streaming-Parser [Aktualisiert in Security Center 1,5]. Wenn **Glide.stax.Whitelist_enabled** Ist auf festgelegt **Wahr** , Definieren Sie eine Liste von durch Kommas getrennten FQDN in **Glide.xml.Entität.Whitelist** Eigenschaft, die die einzigen URLs sind, die mit der Verarbeitungseigenschaft der XML-Entität erreicht werden können. Weitere Informationen finden Sie unter Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0]. Angreifer können diese Schwachstelle verwenden, um Daten bei einem XXE-Angriff (External Entities Expansion) exponentiell zu erweitern und schnell alle Systemressourcen zu verbrauchen. • Beschreibung (Alt): Wenn *glide.stax.whitelist_enabled*Ist nicht auf den empfohlenen Wert von festgelegt **Wahr** , Dann sind alle externen Entitäten zulässig. Dies kann zu XXE-Angriffen (External Entities Expansion) führen. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Schützen Sie sich vor XXE-Angriffen, indem Sie eine Allow-Liste verwenden, um zu verhindern, dass Angreifer beliebige HTTP-Anforderungen aufnehmen, die der Server ausführen kann. Dies kann zu zusätzlichen Angriffen führen, die die Vertrauensbeziehung des Servers mit anderen Entitäten verwenden. Hinzufügen `http://java.sun.com/j2ee/dtds/` Auf den Wert von **Glide.xml.Entität.Whitelist** Systemeigenschaft, legen Sie dann fest **Glide.xml.Entität.Whitelist.aktiviert** Systemeigenschaft zu **Wahr** . Andere Werte als `http://java.sun.com/j2ee/dtds/` Kann in der enthalten sein **Glide.xml.Entität.Whitelist** Eigenschaft, sind jedoch für den sofort einsatzbereiten Plattformstatus unnötig. Überprüfen Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	alle zusätzlichen Werte, um festzustellen, ob sie sicher sind. **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden. • Beschreibung (alt): Wenn „Glide.xml.Entity.Whitelist“ nicht auf den empfohlenen Wert „“ festgelegt ist http://java.sun.com/j2ee/dtds/ „ Und „Glide.xml.Entity.Whitelist.enabled“ nicht auf „wahr“ festgelegt ist, kann eine schädliche externe Entität zugelassen werden, die einen XXE-Angriff verursachen kann. Ein Angreifer kann die DTD verwenden, um beliebige HTTP-Anforderungen einzubeziehen, die der Server möglicherweise ausführen kann. Dies kann zu zusätzlichen Angriffen führen, die die Vertrauensbeziehung des Servers mit anderen Entitäten verwenden. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Beschränken Sie E-Mail-Domänen für die Registrierung externer Anwender [Aktualisiert in Sicherheitscenter 1,3, 1,5 und 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Dateimime-Typ im SOAP-Webservice „AttachmentCreator“ validieren [Neu in Security Center 1,3 und aktualisiert in 1,5]	• Stellen Sie sicher, dass MIME-Typen für Anhänge validiert werden, um zu verhindern, dass gefährliche Dateien mit falschen Dateierweiterungen in Ihre Instanz hochgeladen werden. Legen Sie fest **Glide.attachment.enforce_Security_validation** Systemeigenschaft zu **Wahr** . Wenn auf festgelegt **Wahr** , Dateien werden mit der richtigen Dateityperweiterung hochgeladen. • Beschreibung (alt): Wenn „Glide.attachment.enforce_Security_validation“ nicht auf den empfohlenen Wert „wahr“ festgelegt ist, erfolgt keine Validierung für den MIME-Typ des Anhangs, und gefährliche Dateien könnten mit falschen Dateierweiterungen auf das System hochgeladen werden. Wenn diese Eigenschaft auf „wahr“ festgelegt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	ist, werden Dateien mit der richtigen Dateityperweiterung hochgeladen. Es ist eine Best Practice für Sicherheit, Dateien-Uploads mindestens mit der MIME-Typvalidierung zu validieren. • CVSS-Punktzahl (Neu): 6,7 • CVSS-Punktzahl (alt): 7,5
Definieren zulässig ServiceNow Interne IP-Adressen [aktualisiert in Security Center 1,3 Und 1,5]	• Beschreibung (Neu) verhindern, dass Instanzzugriff für eine größere Gruppe von Personen, die verwenden, unnötig gefährdet ist **glide.ip.authenticate.strict** Und **glide.ip.authenticate.allow.secured** Systemeigenschaften. Wenn **glide.ip.authenticate.strict** Systemeigenschaft ist auf festgelegt **Wahr** , Intern ServiceNow Mitarbeiter und Systeme können eingehende Verbindungen zu Ihrer Instanz nur aus wichtigen IP-Bereichen herstellen. Diese Grenzen ServiceNow Transparenz von für wichtige interne Infrastruktur in Ihrer Instanz und verhindert den Zugriff von breiter ServiceNow Mitarbeiter wie Support- und Vertriebsmitarbeiter über Unternehmensnetzwerke. Die **glide.ip.authenticate.allow.secured** Systemeigenschaft gewährt intern ServiceNow Eingehende Verbindungen, einschließlich regulärem authentifiziertem Zugriff und nicht authentifizierten Diagnoseseiten. Wenn nicht auf festgelegt **Wahr** , Dann breiter ServiceNow Interner IP-Bereich, der in definiert ist **glide.ip.authenticate.allow** Die Eigenschaft wird verwendet, um diese intern zu gewähren ServiceNow Eingehende Verbindungen. Stellen Sie sicher, dass **glide.ip.authenticate.allow.secured** Die Systemeigenschaft enthält nur vertrauenswürdige Werte und die Eigenschaft **glide.ip.authenticate.strict** Ist auf festgelegt **Wahr** . • Beschreibung (alt): Wenn „glide.ip.authenticate.strict" auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	„wahr“ festgelegt ist, können interne ServiceNow-Personelle und -Systeme nur eingehende Verbindungen zur Instanz aus wichtigen IP-Bereichen herstellen. Dieses Limit bietet ServiceNow Einblick in die Instanz in wichtige interne Infrastruktur und verhindert den Zugriff von breiteren ServiceNow-Mitarbeitern wie Support- und Vertriebsmitarbeitern über Unternehmensnetzwerke. Bei „wahr“ wird die Eigenschaft „glide.ip.authenticate.allow" verwendet, um interne eingehende ServiceNow-Verbindungen zu gewähren. Wenn nicht auf „wahr“ festgelegt, wird ein breiterer interner ServiceNow-IP-Bereich wie in „glide.ip.authenticate.allow" definiert verwendet, um interne eingehende ServiceNow-Verbindungen zu gewähren.
Deaktivieren Sie die Entitätserweiterung im XMLDocument2-Streaming-Parser [Aktualisiert in Security Center 1,5]	• Beschreibung (Neu): Deaktivieren Sie die Entitätserweiterung in Ihrer Instanz, um Ihre Instanz vor Angriffen wie der Fähigkeit, Systemdateien zu lesen, und Denial of Service zu schützen. Verwenden Sie die Systemeigenschaft, um zu verhindern, dass XML-Entitäten während der Analyse durch den Streaming-Parser (XMLDocument2) erweitert werden. Legen Sie fest **Glide.stax.allow_Entity_Resolution** Systemeigenschaft zu **Falsch** Zum Deaktivieren der Entitätserweiterung in Ihrer Instanz. Wenn diese Eigenschaft nicht in der Tabelle „Systemeigenschaften“ [sys_properties] angezeigt wird, ist der Standardwert **Wahr** . Erstellen Sie den Eigenschaftsdatensatz, und legen Sie den Wert auf fest **Falsch** Um den Wert zu ändern. • Beschreibung (alt): Wenn „Glide.stax.allow_Entity_Resolution“ nicht auf den empfohlenen Wert „falsch“ festgelegt ist, ermöglicht diese Eigenschaft das erweitern von XML-Entitäten während der Analyse durch den Streaming-Parser (XMLDocument2). Die Erweiterung der XML-Entität

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	kann zu Angriffen wie der Fähigkeit, Systemdateien zu lesen, und Denial of Service führen. • Korrektur (Neu): Stellen Sie die Eigenschaft sicher `glide.stax.allow_entity_resolution`ist in der Tabelle „sys_properties“ vorhanden und ist auf festgelegt **Falsch** . Wenn die Eigenschaft nicht in der Liste „sys_properties“ angezeigt wird, lautet der Standardwert **Wahr** . • Korrektur (alt): Stellen Sie sicher, dass die Eigenschaft „Glide.stax.allow_Entity_Resolution“ auf „falsch“ festgelegt ist.
Standardmäßig mit leeren ACLs ablehnen [aktualisiert in Security Center 1,3]	• Beschreibung (Neu): Verhindern Sie, dass der veraltete Sicherheitsmanager Ihrer Instanz Zugriff auf Ressourcen zulässt, wenn für diese Ressource keine ACLs definiert sind oder wenn nur ACLs auf Tabellenebene mit Platzhaltern vorhanden sind (z. B. `Incident.*`). Wenn der Zugriff standardmäßig zulässig ist, ist alles, für das keine expliziten ACLs festgelegt sind, anfällig für Manipulationen. Legen Sie fest **glide.sm.default_mode** Systemeigenschaftswert bis **Ablehnen** Um den Zugriff zu verweigern, wenn keine ACL-Definierungsregeln oder nur ACLs auf Tabellenebene mit Platzhaltern vorhanden sind. • Beschreibung (alt): Wenn „glide.sm.default_mode" nicht auf den empfohlenen Wert „Deny“ festgelegt ist, gewährt der veraltete Sicherheitsmanager der Instanz Zugriff auf eine Ressource, wenn für diese Ressource keine ACLs definiert sind oder nur ACLs auf Tabellenebene mit Platzhaltern. Wenn Sie dies auf „Zulassen“ festlegen, ist alles, für das keine expliziten ACLs festgelegt sind, anfällig für Manipulationen. • CVSS-Punktzahl (Neu): 6,3

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• CVSS-Punktzahl (alt): 8,8 • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Beschränken Sie den nicht authentifizierten Zugriff auf Anhänge	• Beschreibung (Neu): Sichern Sie die Images in Ihrer Instanz, um das Leck vertraulicher Informationen zu verhindern. Images in Ihrer Instanz sind über urls zugänglich, die auf enden `.iix` . Legen Sie fest **glide.image_provider.security_enabled** Systemeigenschaft zu **Wahr** Um den Zugriff auf Ihre Bilder über diese URLs zu verhindern. **Hinweis:** Diese Eigenschaft wird für Bilder aus der Anhangstabelle nicht berücksichtigt, wenn die Ursprungstabelle eine der folgenden ist: ○ Schreibwaren [sysevent_email_style] ○ Abschnitte der Willkommensseite [sys_Home] ○ Systemeigenschaften [sys_properties] Die Einschränkung sollte für nicht authentifizierte Anwender angewendet werden, da einige Anhänge vertrauliche Informationen enthalten können. • Beschreibung (alt): Wenn „glide.image_provider.security_enabled" nicht auf den empfohlenen Wert „wahr“ festgelegt ist, sind alle Bilder über urls zugänglich, die auf „.iix“ enden. Dies würde nicht authentifizierten Zugriff auf Bilder ermöglichen, was zu einem Verlust vertraulicher Informationen führen würde.
Eingebetteten HTML-Code deaktivieren [aktualisiert in Security Center 1,3]	• Beschreibung (Neu): Deaktivieren Sie die Unterstützung für die Anzeige von HTML-Code, der mit eingebettet wurde `[Code]` Tag.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Dieses Tag ermöglicht die Anzeige von gerendertem HTML in Journalfeldern und kann zu Angriffen mit Cross-Site Scripting (XSS) führen. Diese Angriffe können die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des angemeldeten Browsers ermöglichen. Angreifer können diese Skripts verwenden, um Sitzungsinformationen und vertrauliche Daten zu stehlen. Die HTML-Sprache wurde nicht so konzipiert, dass Skript von der Formatierung getrennt wird. Daher birgt das Zulassen von anwendergesteuertem HTML in jedem System ein inhärentes Risiko. Wird festgelegt **glide.ui.security.codetag.allow_script** Bis **Falsch** Ist konform und reduziert dieses Risiko erheblich, jedoch bleibt ein geringfügiges Risiko bestehen. Dadurch wird nur der Skriptteil von deaktiviert `Code` Tag, und basiert auf der Bereinigung aller bekannten Konventionen des Skripts in HTML. Legen Sie fest **glide.ui.security.allow_codetag** Systemeigenschaft zu **Falsch** Um zu verhindern, dass Journalfelder und -Formulare gerenderte HTML anzeigen. Die ServiceNow AI Platform Mildert viele Einschleusungen und standortübergreifende Angriffe durch Implementierung von Escape- und Codierungstechniken ab. Daher können Anwender keine HTML-formatierten Eingaben für Journalfelder schreiben/übermitteln. Journalfelder können jedoch Text, der in Code-Tags eingeschlossen ist, als HTML rendern. ○ Es besteht jedoch ein entsprechendes Sicherheitsrisiko. Wenn auf festgelegt `Wahr` , Böswillige Anwender können schädlichen HTML-JS-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann. ○ Legen Sie diese Eigenschaft auf fest `Falsch` Damit Administratoren verhindern können, dass Journalfelder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	HTML-Code rendern, indem sie die Unterstützung für deaktivieren [Code] Tag. • Beschreibung (alt): Deaktiviert die Unterstützung für die Einbettung von HTML-Code, der mit dem Tag [Code] erstellt wurde. Wenn „glide.ui.security.allow_codetag" nicht auf den Wert „falsch“ festgelegt ist, wird gerendertes HTML in Journalfeldern und Formularen nicht angezeigt. Wenn „glide.ui.security.allow_codetag" auf „wahr“ festgelegt wird, wenn eingebetteter HTML-Code mit angezeigt wird, kann dies zu Angriffen mit Cross-Site Scripting (XSS) führen.
Richtlinienprüfungen für Passwortzurücksetzung aktivieren [aktualisiert in Security Center 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
E-Mail-Spam-Bewertung und -Filterung aktivieren [aktualisiert in Security Center 1,3]	• Name der technischen Konfiguration (Neu): Com.Glide.email_Filter,Glide.email.read.Active • Name der technischen Konfiguration (alt): Com.Glide.email_Filter • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Excel-Formeln mit Escape-Zeichen [aktualisiert in Security Center 1,3]	• Beschreibung (Neu): Verhindern Sie, dass potenziell schädliche Formeln in Programmen wie Excel nach dem Exportieren und Öffnen der Datei ausgeführt werden, indem Sie Formeln in diesen Dateien mit Escape-Zeichen versehen. Excel-Injection tritt auf, wenn Websites nicht vertrauenswürdige Einträge in Excel-Dateien einbetten. Wenn Sie eine Tabellenkalkulationsanwendung wie Microsoft Excel oder LibreOffice-Aufruf verwenden, um eine Datei zu öffnen, werden alle Zellen, die mit +, -, = oder @ beginnen, als Formel interpretiert, sofern sie nicht ordnungsgemäß mit Escape versehen sind. Schädliche Formeln stellen ein Risiko dar, auch wenn die Tabelle keine vertraulichen Informationen enthält, da sie verwendet werden können, um den Computer des Betrachters durch Codeausführung zu gefährden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Legen Sie fest **glide.export.escape_formulas** Systemeigenschaft zu **Wahr** Um die Ausführung dieser Formeln zu verhindern. • Beschreibung (alt): Durch Festlegen der Eigenschaft „glide.export.escape_formulas" auf den empfohlenen Wert „wahr“ wird verhindert, dass potenziell schädliche Formeln in Programmen wie Excel nach dem Exportieren und Öffnen der Datei ausgeführt werden. Zellenwerte für CSV, XLS und XLSX können von Tabellenkalkulationsanwendungen als Formeln interpretiert werden, es sei denn, sie werden ordnungsgemäß mit Escape-Zeichen versehen, was zur Ausführung schädlicher Codes führen kann. • CVSS-Punktzahl (Neu): 6,4 • CVSS-Punktzahl (alt): 6,5
Beschränken Sie JSONP-Anforderungen auf vertrauenswürdige URLs [Aktualisiert in Security Center 1,3]	• Beschreibung (Neu): Erhöhen Sie die Sicherheit in Ihrer Instanz, indem Sie sicherstellen, dass nur vertrauenswürdige URLs für den Service AngularJS $http JSONP-Anforderungen zulassen/ablehnen können. JSONP-Anforderungen sind an jede URL zulässig, wenn diese Eigenschaften nicht konfiguriert und aktiviert sind. Verwenden Sie den Wert von **angular.jsonp.inclusion_list.urls** Systemeigenschaft zum Definieren einer Liste von URLs, die vertrauenswürdig sind und diesen Zweck zulassen. Legen Sie den Wert von fest **angular.jsonp.inclusion_list.enabled** Systemeigenschaft zu **Wahr** Zum Einschränken des zulässigen JSONP auf die in aufgeführten URLs **angular.jsonp.inclusion_list.urls** . • Beschreibung (alt): Diese Eigenschaft gibt vertrauenswürdige URLs für den AngularJS $http-Service an, um JSONP-Anforderungen zuzulassen/abzulehnen. Eigenschaft ist erforderlich, da dies für Kunden eine potenziell störende Änderung ist. Daher benötigen sie eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Möglichkeit, ihre vertrauenswürdigen URLs hinzuzufügen. Wenn „angular.jsonp.inclusion_list.enabled" nicht auf den empfohlenen Wert „wahr“ festgelegt ist, sind JSONP-Anforderungen an jede URL zulässig.
Plugin für SNC-Zugriffssteuerung aktivieren [aktualisiert in Security Center 1,3]	• Beschreibung (Neu): Verhindern ServiceNow Kundenservice- und Supportmitarbeiter können ohne Ihre ausdrückliche Berechtigung auf die Instanzen zugreifen, indem das Plugin „SNC Access Control“ (com.snc.snc_Access_Control) aktiviert wird. Obwohl der gesamte Zugriff auf Ihre Instanz geprüft wird, möchten Sie diesen Zugriff möglicherweise steuern. Diese Zugriffsmethode ist vollständig auditierbar und wird nachverfolgt. **Hinweis:** Andere autorisiert ServiceNow Betriebspersonal in ihrer Eigenschaft zur Unterstützung und Verwaltung des Produkts müssen administrative Aktionen für die zugrunde liegende Infrastruktur ausführen. Das Aktivieren dieses Plugins kann sich auf Support-Servicelevel und das Verfügbarkeits-SLA auswirken. Das Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeiter Zugriff auf Ihre Instanz erhalten. Aktivieren Sie das Plugin „SNC Access Control“ (com.snc.snc_Access_Control), um den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Berechtigung zu beschränken. Weitere Informationen zu dieser Funktion finden Sie unter ServiceNow-Zugriffssteuerung. Informationen zur Aktivierung finden Sie unter Aktivieren ServiceNow Zugriffssteuerung • Beschreibung (alt): Das Plugin „SNC-Zugriffssteuerung“ (com.snc.snc_Access_Control) verhindert, dass Kundenservice- und Supportmitarbeiter ohne Ihre ausdrückliche Erlaubnis auf die Instanzen zugreifen. Andere autorisierte ServiceNow Operations-Mitarbeiter, die das Produkt unterstützen und verwalten, müssen jedoch administrative Aktionen für die zugrunde liegende Infrastruktur ausführen. Diese Infrastruktur umfasst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Server und Datenbanken sowie andere Infrastrukturkomponenten, aus denen die SaaS-Lösung besteht. Diese Zugriffsmethode kann vollständig auditiert und nachverfolgt werden.mit diesem Plugin können Sie den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Berechtigung beschränken, sodass es sich auf Support-Servicelevel und das Verfügbarkeits-SLA auswirken kann. Das Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeiter Zugriff auf Ihre Instanz erhalten. • Korrektur (Neu): Stellen Sie sicher, dass das Plugin „com.snc.snc_Access_Control“ aktiviert ist. Lesen Sie die Dokumentation zum Aktivieren von um https://www.servicenow.com/docs/csh?topicname=t_ActivateSNCAccessControl.html&version=latest. • Korrektur (alt): Stellen Sie sicher, dass das Plugin „com.snc.snc_Access_Control“ aktiviert ist. • CVSS-Punktzahl (Neu): 3,3 • CVSS-Punktzahl (alt): 8,2
Timeout-Dauer für Entsperrung der fehlgeschlagenen Anmeldung maximieren [aktualisiert in Security Center 1,3]	• Name der technischen Konfiguration (Neu): glide.user.unlock_timeout_in_mins, sysevent_script_action • Name der technischen Konfiguration (alt): glide.user.unlock_timeout_in_mins • Beschreibung (Neu): Helfen Sie, Ihre Instanz vor Brute-Force-Angriffen zu schützen, indem Sie einen Zeitraum definieren, in dem ein Anwender nicht versuchen kann, sich anzumelden, nachdem er gesperrt wurde. Die **glide.user.unlock_timeout_in_mins** Die Systemeigenschaft entsperrt den Anwenderaccount nach dem im Wert angegebenen Zeitraum. Wenn kein Wert angegeben ist, entsperrt Ihre Instanz den Anwenderaccount nach dem Standardzeitraum von 15 Minuten. • Beschreibung (alt): Wenn „glide.user.unlock_timeout_in_mins" nicht auf den empfohlenen Wert von „15“ festgelegt ist, kann es einfacher sein,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Konten in einem schnelleren Zeitrahmen zu Brute-Force zu erzwingen. Mit dieser Eigenschaft wird der Anwenderaccount nach dem für die Eigenschaft glide.user.unlock_timeout_in_mins angegebenen Zeitraum entsperrt. Wenn kein Wert angegeben ist, entsperrt das System den Benutzeraccount nach dem Standardzeitraum von 15 Minuten. • Korrektur (Neu): Legen Sie fest **glide.user.unlock_timeout_in_mins** Systemeigenschaftswert auf mindestens **15** . Wenn **glide.user.unlock_timeout_in_mins** Ist nicht vorhanden, die standardmäßige Sperrzeit ist auf 15 Minuten festgelegt. Stellen Sie sicher, dass **SNC-Anwendersperrprüfung mit automatischer Entsperrung** Skriptaktion (in der Tabelle „Skriptaktion“ [sysevent_script_action] gefunden) ist vorhanden und aktiv. Die **SNC-Anwendersperrprüfung mit automatischer Entsperrung** Die Skriptaktion wird mit dem Plugin „Einstellungen für hohe Sicherheit“ (com.Glide.High_Security) installiert. • Korrektur (alt): Stellen Sie sicher, dass die Eigenschaft „glide.user.unlock_timeout_in_mins" auf mindestens „15“ festgelegt ist. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Plugin „Zugriff auf bestimmte IP-Bereiche einschränken“ [aktualisiert in Security Center 1,3]	• Name der technischen Konfiguration (Neu): Com.snc.ipauthenticator,ip_Access • Name der technischen Konfiguration (alt): Com.snc.ipauthenticator
Beschränken Sie den Zugriff auf E-Mails mit leerer Zieltabelle	• CVSS-Punktzahl (Neu): 6,5 • CVSS-Punktzahl (alt): 5,4
Herunterladbare MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]	• CVSS-Punktzahl (Neu): 6,4 • CVSS-Punktzahl (alt): 8

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Aktualisierte Version des MultiSSO-Plugins aktivieren [aktualisiert in Security Center 1,3 Und 1,5]	• Name der technischen Konfiguration (Neu): glide.authenticate.multissov2_feature.enabled • Name der technischen Konfiguration (alt): glide.authenticate.multisso.enabled,glide.authenticate.mult • Beschreibung (Neu): Wenn das Multi SSO-Plugin auf einer Instanz aktiviert ist, reduzieren Sie Sicherheitsschwachstellen, indem Sie bestätigen, dass die v2-Version aktiviert ist. Die neueste Version verbessert die Sicherheit und verfügt über weitere Funktionen, z. B. Unterstützung für Assertion Encryption und IDP-initiierte Single Logout (SLO). Wenn die neueste Version nicht aktiviert ist, können die neuen Sicherheitsfunktionen nicht verwendet werden, und die Instanz läuft Gefahr, ein veraltetes Plugin zu verwenden. Befolgen Sie die Schritte in KB0756504 Um ein Upgrade auf die neueste Version durchzuführen. Dieser Prozess umfasst das Überprüfen und Migrieren von anpassungsbezogenen Changes und das anschließende Upgrade der Version. Wenn abgeschlossen, wird **glide.authenticate.multissov2_feature.enabled** Systemeigenschaft wird automatisch festgelegt **Wahr** . • Beschreibung (alt): Wenn das Multi-SSO-Plugin auf einer Instanz aktiviert ist, sollte die v2-Version aktiviert sein. Versionen vor MultiSSOv2, einschließlich SAML 1,1 und SAML 2,0, entsprechen nicht den Best Practices und verwenden opensaml-Bibliotheksversionen mit bekannten CVEs. Wenn die bekannten CVEs in veralteten opensaml-Bibliotheken ausnutzbar waren, kann der Angreifer Nachrichten fälschen und die Authentifizierung durch XML-Signaturwicklungsangriffe umgehen, die Identität von Entitäten annehmen oder Personen-in-the-Middle-Angreifern erlauben, nicht autorisierten Zugriff auf die Plattform zu erhalten. • CVSS-Punktzahl (Neu): 0 • CVSS-Punktzahl (alt): 7,1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Verhindern, dass sich inaktive Anwender anmelden [Neu in Security Center 1,5]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Aktivieren Sie das MID-Audit-Protokoll [Neu in Security Center 1,3 Und aktualisiert in 1,5]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Stellen Sie sicher, dass ACLs der Archivtabelle aktiviert sind [Neu in Security Center 1,3 und aktualisiert in 1,5]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Aktive Sitzungszeitüberschreitungsausnahmerollen definieren [Neu in Security Center 1,3]	• CVSS-Punktzahl (Neu): 6,4 • CVSS-Punktzahl (alt): 7,1
Größe des HTTP-Antworttexts begrenzen [Neu in Security Center 1,3 Und aktualisiert 1,5]	• Beschreibung (Neu): Verhindern Außerhalb des Arbeitsspeichers Dies kann dazu führen, dass ein Anforderungsantworttext mit zu groß ist **Glide.http.response.get_body.limit.enabled** Und **Glide.http.response.get_body.limit** Systemeigenschaften. Diese Ausnahmen können Denial of Service (DOS)-Angriffe sowie andere Probleme verursachen, die Angreifern helfen können, eine Instanz zu gefährden. Wenn Sie diese Eigenschaften nicht auf die empfohlenen Werte festlegen, kann Ihre Instanz angreifbar für OutOfMemoryExceptions und Denial of Service-Angriffe werden. So schützen Sie Ihre Instanz vor diesen Sicherheitsschwachstellen: ◦ Legen Sie fest **Glide.http.response.get_body.limit.enabled** Systemeigenschaft zu **Wahr** . ◦ Stellen Sie sicher, dass **Glide.http.response.get_body.limit** Systemeigenschaft auf nicht mehr als 524.288.000 Megabyte (500 MB) festgelegt. • Beschreibung (alt): Die Eigenschaften „Glide.http.response.get_body.limit.enabled“ und „Glide.http.response.get_body.limit“ wurden eingeführt, um neue Funktionen zu aktivieren, die verhindern, dass Ausnahmen zu wenig Arbeitsspeicher ausgelöst werden, da der Antworttext der Anforderung zu groß ist. Ausnahmen zu wenig Arbeitsspeicher können Denial-of-Service-Angriffe sowie andere Probleme verursachen, die Angreifern dabei helfen können, eine Instanz zu gefährden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• CVSS-Punktzahl (Neu): 3,1 • CVSS-Punktzahl (alt): 6,4
Lebensdauer der aktiven UI-Sitzung begrenzen [Neu in Security Center 1,3]	• Beschreibung (Neu): Reduzieren Sie den Umfang potenzieller Security Incidents, indem Sie die Lebensdauer aktiver HTTP-Sitzungen verringern. Die **glide.ui.active.session.life_span** Die Systemeigenschaft erzwingt unabhängig von der inaktiven Zeitüberschreitung eine maximale Lebensdauer für aktive HTTP-Sitzungen. Eine längere maximale Lebensdauer kann einem Angreifer ermöglichen, eine gestohlene Sitzung länger zu verwenden, wodurch der Umfang eines Security Incidents erhöht wird. Der Standardwert von **0** Deaktiviert die Zeitüberschreitung aktiver Sitzungen Legen Sie fest **glide.ui.active.session.life_span** Auf einen Wert zwischen 1 und 720. Dieser Wert stellt die Zeit in Minuten dar, die HTTP-Sitzungen aktiv bleiben können. • Beschreibung (alt): Diese Konfiguration erzwingt die maximale Lebensdauer für aktive Gast-HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung. Der konfigurierte Wert ist in Minuten, und der Wert Null deaktiviert das Timeout der aktiven Sitzungen. Eine größere maximale Lebensdauer kann es einem Angreifer ermöglichen, eine gestohlene Sitzung länger beizubehalten, wodurch der Umfang eines Security Incidents erhöht wird. Diese bestimmte Eigenschaft ist auf die Zeitüberschreitung der UI-Sitzung beschränkt.

Härtungseinstellungen für Baseline-Version 5,0 aktualisiert

Einige Härtungseinstellungen wurden mit dem Release der Security Center-Baseline-Version 5,0 aktualisiert.

Die Baseline-Version 5 enthält mehrere Updates für Kurzbeschreibungen, um Stil und Konsistenz in Datensätzen zu gewährleisten. Darüber hinaus wurden viele eigenschaftsbezogene Skripts aktualisiert, um die Genauigkeit der Standardwerte in Fällen zu verbessern, in denen die Eigenschaft aus der Tabelle „sys_property“ entfernt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Autorisierung für SOAP-Anforderungen anfordern [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher `glide.basicauth.required.soap`lst vorhanden und auf den Wert „wahr“ festgelegt. Alternativ können Sie die Instanz für WS-Sicherheit konfigurieren, indem Sie die Eigenschaft „Glide.SOAP.require_WS_Security“ auf „wahr“ festlegen und der Produktdokumentation folgen, um WS-Sicherheitsprofile zu konfigurieren. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.soap`lst auf den Wert „wahr“ festgelegt. Alternativ können Sie die Instanz für WS-Sicherheit konfigurieren, indem Sie die Eigenschaft festlegen `glide.soap.require_ws_security`Auf „wahr“ und befolgen Sie die Produktdokumentation, um WS-Sicherheitsprofile zu konfigurieren.
OCSP-Prüfung bei Netzwerkfehler erzwingen [Neu in Security Center 1,3 und aktualisiert in 2,0]	• Neue Korrektur: Stellen Sie die Eigenschaft sicher `com.glide.communications.httpclient.ocsp_allow_` vorhanden und auf „falsch“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `com.glide.communications.httpclient.ocsp_allow_` auf „falsch“ festgelegt.
url für externe Inhalte deaktivieren [aktualisiert in Security Center 2,0]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher `glide.ui.url.external.content`lst vorhanden und auf den Wert „falsch“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.ui.url.external.content`lst auf „falsch“ festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Neue CVSS-Punktzahl: 7,2 • Alte CVSS-Punktzahl: 8,1 • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher *glide.xml.entity.whitelist*Ist vorhanden und ist auf „ http://java.sun.com/j2ee/dtds/ „ Und die Glide-Eigenschaft *glide.xml.entity.whitelist.enabled*Ist vorhanden und auf den Wert „wahr“ festgelegt. Wenn die Eigenschaften nicht in der Tabelle „sys_properties“ angezeigt werden, fügen Sie neue Datensätze hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.xml.entity.whitelist*Ist auf „ http://java.sun.com/j2ee/dtds/ „ Und die Eigenschaft *glide.xml.entity.whitelist.enabled*Ist auf „wahr“ festgelegt.
Nicht authentifizierte veröffentlichte Berichte deaktivieren [aktualisiert in Security Center 2,0]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher *glide.report.published_reports.enabled*Ist vorhanden und auf den Wert „falsch“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.report.published_reports.enabled*Ist auf „falsch“ festgelegt.
Richtlinienprüfungen für Passwortzurücksetzung aktivieren [aktualisiert in Security Center 2,0]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher *glide.enable.password_policy*Ist vorhanden und auf den Wert „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.enable.password_policy*Ist auf „wahr“ festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Schwellenwert für Entitätserweiterung für skriptfähige GlideXMLUtil minimieren [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.xmlutil.max_entity_expansion*Ist auf maximal 3000 festgelegt. Wenn sich die Instanz in Washington oder höher befindet, ist der implizite Standardwert 3000, wenn der Datensatz „sys_properties“ nicht vorhanden ist. Wenn sich die Instanz nicht in Washington oder höher befindet, empfiehlt es sich, dass der Instanzadministrator einen sys_properties-Datensatz mit dem Namen erstellt *glide.xmlutil.max_entity_expansion*Und der Wert 3000. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.xmlutil.max_entity_expansion*Ist auf maximal 3000 festgelegt.
Ausgehende SSLv2/SSLv3-Verbindungen deaktivieren [aktualisiert im Sicherheitscenter 1,3]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher *glide.outbound.sslv3.disabled*Ist vorhanden und auf den Wert „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.outbound.sslv3.disabled*Ist auf „wahr“ festgelegt. **Wichtig:** Der Wert für *glide.outbound.sslv3.disabled*Eigenschaft ist eine sichere Überschreibung und kann nach der Änderung nicht geändert werden.
Legacy-Verhalten für GlideRecord-Umfangsabgrenzung deaktivieren [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]	• Neue Kurzbeschreibung: Deaktivieren Sie das Legacy-Verhalten des GlideRecord-Umfangs • Alte Kurzbeschreibung: Legacy-Verhalten für GlideRecord-Umfangseinfassung aktivieren
Hochgeladene MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.security.file.mime_type.validation*Ist vorhanden und auf „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	„sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.security.file.mime_type.validation`Ist auf „wahr“ festgelegt.
Jelly JS-Interpolationsschutz für geschachtelte Ausdrücke aktivieren [aktualisiert in Security Center 2,0]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher `glide.ui.jelly.js_interpolation.protect_nested_e` vorhanden und auf den Wert „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.ui.jelly.js_interpolation.protect_nested_e` auf „wahr“ festgelegt.
SSL in LDAP-Authentifizierung aktivieren [aktualisiert in Security Center 1,5 und 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
UserCookie-Version 3,1 aktivieren [aktualisiert in Security Center 2,0]	• Neue Beschreibung: UserCookie v3 wird nur generiert, wenn Eigenschaft `glide.ui.secure.cookies.use_kmf is disabled`. UserCookie v3 ist nicht sicher, da geheimer Schlüssel für HMAC im Quellcode gespeichert und für alle Kunden identisch ist. Die schädliche Akteure unterstützen kann, diesen einen geheimen Schlüssel für Versuche zum Hijacking von Anwendersitzungen zu verwenden. Durch Festlegen der Eigenschaft `glide.ui.secure.cookies.use_kmf`Auf „wahr“ wird AnwenderCookie v3.1 verwendet, und der geheime Schlüssel wird in einem Sicherheitsspeicher wie KMF gespeichert. • Alte Beschreibung: AnwenderCookie v3 wird nur generiert, wenn Eigenschaft `glide.ui.secure.cookies.use_kmf` Ist deaktiviert. UserCookie v3 ist nicht sicher, da geheimer Schlüssel für HMAC im Quellcode gespeichert und für alle Kunden identisch ist. Die schädliche Akteure unterstützen kann, diesen einen geheimen Schlüssel für Versuche zum Hijacking von Anwendersitzungen zu verwenden. • Neue Korrektur: Stellen Sie die Eigenschaft sicher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	*glide.ui.secure.cookies.use_kmf*Ist vorhanden und auf „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.ui.secure.cookies.use_kmf*Ist auf „wahr“ festgelegt. Dies bedeutet, dass AnwenderCookie v3.1 verwendet wird und der geheime Schlüssel in einem Sicherheitsspeicher wie KMF gespeichert wird.
OTP-Lebensdauer für Passwortzurücksetzung auf 1 Stunde festlegen [aktualisiert in Security Center 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Identitätswechsel des Anwenders protokollieren [aktualisiert in Security Center 1,3 und 2,0]	• Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.sys.log_impersonation*Ist vorhanden und auf „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.sys.log_impersonation*Ist auf „wahr“ festgelegt.
Erforderliche jms-Connection Factorys [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Stellen Sie sicher, dass die Erstellung/Löschung von Dashboards eine Zugriffsprüfung erfordert [Neu in Security Center 1,3 und aktualisiert in 2,0]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher *glide.processors.check_access_before_process*Ist vorhanden und auf den Wert „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Stellen Sie den Wert von sicher *glide.processors.check_access_before_process*Ist immer „wahr“.
Inaktive Sitzungen proaktiv für ungültig erklären [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]	• Neue Korrektur: Stellen Sie die Glide-Eigenschaft sicher *glide.active.session.timeout.invalidate.session*I vorhanden und auf den Wert „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	wird, fügen Sie einen neuen Datensatz hinzu. • Alte Korrektur: Legen Sie die Glide-Eigenschaft fest *glide.active.session.timeout.invalidate.session* „wahr“.
Sicherheitsbereich für Mitarbeiterbereich für HR-Fallmanagement erzwingen [Neu in Security Center 1,5 und aktualisiert 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Playbook für Lizenz und Erlaubnis für den Sicherheitsumfang erzwingen [Neu in Security Center 1,5 und aktualisiert 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Herunterladbare MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Beschreibung: Wenn die Eigenschaft *glide.ui.attachment.force_download_all_mime_type* auf „wahr“ festgelegt, dann die *glide.ui.attachment.download_mime_types*-Eigenschaft wird überschrieben, sodass alle MIME-Typen heruntergeladen und nicht vom Browser gerendert werden. Zum Beispiel erzwingt das Herunterladen von Text/HTML, dass eine HTML-Datei als Datei auf den Client heruntergeladen und nicht inline im Browser angezeigt wird, um einen XSS-Angriff zu verhindern. XSS kann zu einer einfachen Berechtigungseskalation an höhere Rollen wie Administrator führen, in denen mehr seitliche Bewegungen erfolgen können. • Alte Beschreibung: Wenn die Eigenschaft *glide.ui.attachment.force_download_all_mime_type* nicht auf „wahr“ festgelegt, dann ist *glide.ui.attachment.download_mime_types*-Eigenschaft wird überschrieben, sodass alle MIME-Typen heruntergeladen und nicht vom Browser gerendert werden. Zum Beispiel erzwingt das Herunterladen von Text/HTML, dass eine HTML-Datei als Datei auf den Client heruntergeladen und nicht inline im Browser angezeigt wird, um einen XSS-Angriff zu verhindern. Die Fähigkeit, XSS zu verwenden, kann zu einer einfachen Berechtigungseskalation zu höheren Rollen wie Administrator führen, wo mehr seitliche Bewegungen ausgeführt werden können. • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.ui.attachment.force_download_all_mime_type* auf „wahr“ festgelegt. Wenn

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	die Eigenschaft in der Tabelle „sys_properties“ nicht vorhanden ist, ist der Standardwert „falsch“. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.ui.attachment.force_download_all_mime_type` auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Eingeschränkte herunterladbare MIME-Typen definieren [aktualisiert in Security Center 1,3, 1,5 und 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Download infizierter Dateien nicht zulassen [aktualisiert in Security Center 1,5 und 2,0]	• Neue Beschreibung: Wenn die Eigenschaft `com.glide.snap.infected_download_allowedlst` auf „wahr“ festgelegt, können Anwender auch dann nicht gescannte Anhänge herunterladen, wenn der Virenschutzservice ausgefallen oder nicht erreichbar ist. Dies bedeutet, dass es möglich ist, dass ein Anwender eine schädliche Datei herunterlädt und das Risiko besteht, den Desktop des Anwenders zu infizieren (falls auf dem Gerät kein anderer Endpunktschutz vorhanden ist). • Alte Beschreibung: Wenn `com.glide.snap.infected_download_allowedlst` nicht auf den empfohlenen Wert „falsch“ festgelegt, kann eine schädliche Datei heruntergeladen werden, die nicht gescannt wurde, was zu einem Risiko führt, den Desktop des Anwenders zu infizieren. • Neue Korrektur: Stellen Sie die Eigenschaft sicher `com.glide.snap.infected_download_allowedlst` auf „falsch“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `com.glide.snap.infected_download_allowedlst` auf „falsch“ festgelegt.
Zugriff auf skriptfähige GlideSystemUserSession-API beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Beschreibung: `gs.addErrorMessageNoSanitizationMessaging()` Und `gs.addInfoMessageNoBereinigung()` Werden in der Skriptumgebung für Protokollierung und Benachrichtigungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	verwendet. Beide sind in der Sandbox verfügbar, wenn diese Eigenschaft nicht auf den empfohlenen Wert „falsch“ festgelegt ist. Die Sandbox ist eine Skripterstellungsumgebung mit geringen Berechtigungen, die nicht authentifizierten Anwendern ohne Rolle zur Verfügung steht. Beide Methoden können verwendet werden, um einem Anwender nicht bereinigte Eingaben anzuzeigen. Das Anzeigen nicht bereinigter Eingaben für den Anwender ist gefährlich, da nicht bereinigte Eingaben gefährlichen Code enthalten können, der im Browser des Anwenders ausgeführt wird. Dies kann für traditionelle reflektierte XSS-Angriffe verwendet werden. Reflektierte XSS-Angriffe können in mehreren Szenarien verwendet werden, einschließlich Sitzungs-Hijacking. • Alte Beschreibung: Messaging in der Glide-Skripting-Sandbox wird zu Protokollierungszwecken verwendet. Durch das Aufrufen dieser nicht bereinigten Fehlerfunktion wird die Plattform reflektierten XSS-Angriffen ausgesetzt. XSS-Angriffe können eine einfache Berechtigungseskalation ermöglichen, indem Sitzungscookies einer Person gestohlen werden. Wenn `glide.sandbox.usersession.allow_unsanitized_mess` nicht auf den empfohlenen Wert „falsch“ festgelegt, dann werden die nicht bereinigten Fehlernachrichtenfunktionen verwendet `AddErrorMessageNoBereinigung` Und `AddInfoMessageNoBereinigung` Sind für Skript verfügbar.
Abfrageregeln für Arbeitsauftragsmanagement für Serviceorganisationen aktivieren [Neu in Security Center 1,5 und aktualisiert 2,0]	• Neue Beschreibung: Bei „wahr“ werden Regeln/Filter aus der Tabelle „sn_query_rule“ verwendet, um den Lesezugriff auf Tabellen im Zusammenhang mit dem Außendienst-Management (Arbeitsauftrag und Arbeitsauftragsaufgabe) für den angemeldeten Anwender über Abfragegeschäftsregeln und Lese-ACLs zu bestimmen. Bei „falsch“ werden die Datensätze nicht basierend auf Abfrageregeln gefiltert. AbfrageBusiness-Regeln fügen zusätzliche Sicherheitsvalidierungen hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Insbesondere filtert diese Eigenschaft Datensätze für Service Desk-Mitarbeiter, Qualifizierer und Dispatcher basierend auf ihrem zugewiesenen Gebiet oder ihrer Gebietsmitgliedschaft. Es empfiehlt sich, beim Lesen von Datensätzen das Prinzip der geringsten Berechtigung zu befolgen. Wenn diese Eigenschaft nicht auf „wahr“ festgelegt ist, kann das Risiko der Datengefährdung durch Außendienst-Management-Tabellen erhöht werden. • Alte Beschreibung: Bei „wahr“ werden Regeln/Filter aus der Tabelle „sn_query_rule“ verwendet, um den Lesezugriff auf Tabellen im Zusammenhang mit dem Außendienst-Management (Arbeitsauftrag und Arbeitsauftragsaufgabe) für den angemeldeten Anwender über Abfragegeschäftsregeln und Lese-ACLs zu bestimmen. Bei „falsch“ werden die Datensätze nicht basierend auf Abfrageregeln gefiltert. AbfrageBusiness-Regeln fügen zusätzliche Sicherheitsvalidierungen hinzu. Insbesondere filtert diese Eigenschaft Datensätze für Service Desk-Mitarbeiter, Qualifizierer und Dispatcher basierend auf ihrem zugewiesenen Gebiet oder ihrer Gebietsmitgliedschaft. Es empfiehlt sich, beim Lesen von Datensätzen das Prinzip der geringsten Berechtigung zu befolgen.
Beschränken Sie E-Mail-Domänen für die Registrierung externer Anwender [Aktualisiert in Sicherheitscenter 1,3, 1,5 und 2,0]	• Neue Beschreibung: Die *sn_ext_usr_reg.allowed_email_domains*Die Eigenschaft definiert, welche E-Mail-Adressen sich bei einer ServiceNow-Instanz selbst registrieren dürfen. Das Format muss eine kommagetrennte Liste zulässiger E-Mail-Domänen sein, z. B. domain1.com,domain2.com, in der E-Mails wie example@domain2.com akzeptiert werden. Wenn *sn_ext_usr_reg.allowed_email_domains*Ist nicht mit einer Liste zulässiger Domänen festgelegt, dann können Anwender mit einer beliebigen E-Mail-Adresse Accounts in den Instanzen registrieren. Wenn nicht definiert, können böswillige Akteure die Registrierung mithilfe von E-Mail-Adressen aus unerwünschten Domänen durchführen, um authentifizierten Zugriff auf die Instanz zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte Beschreibung: Die *sn_ext_usr_reg.allowed_email_domains*Die Eigenschaft definiert, welche E-Mail-Adressen sich bei einer ServiceNow-Instanz selbst registrieren dürfen. Wenn *sn_ext_usr_reg.allowed_email_domains*Ist nicht mit einer Liste zulässiger Domänen festgelegt, dann können Anwender mit einer beliebigen E-Mail-Adresse Accounts in den Instanzen registrieren. Wenn nicht definiert, können böswillige Akteure die Registrierung mithilfe von E-Mail-Adressen aus unerwünschten Domänen durchführen, um authentifizierten Zugriff auf die Instanz zu erhalten.
Domänentrennung auf Dot-Walking-Felder anwenden [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Beschreibung: Diese Eigenschaft steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie Domänentrennungsfunktionen für Dot-Walking-Felder anwenden. Wenn *glide.sys.domain.include_domain_condition_on_jo* in einer Instanz mit Domänentrennung nicht auf den empfohlenen Wert „wahr“ festgelegt, können vertrauliche Informationen offengelegt werden, die nicht für eine bestimmte Domäne freigegeben werden sollen. Es kann moderate funktionale Auswirkungen auf die Instanz haben, wenn Komponenten von den unsicheren domänenübergreifenden Abfragen abhängig sind. Instanzen sollten vor der Aktivierung in Subproduktionsumgebungen getestet werden. • Alte Beschreibung: Diese Eigenschaft steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie Domänentrennungsfunktionen für Dot-Walking-Felder anwenden. Wenn *glide.sys.domain.include_domain_condition_on_jo* in einer Instanz mit Domänentrennung nicht auf den empfohlenen Wert „wahr“ festgelegt, können vertrauliche Informationen offengelegt werden, die nicht für eine bestimmte Domäne freigegeben werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Prüfung der URL-Zulässigkeitsliste erzwingen [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.security.url.whitelist.strict_check*lst auf „wahr“ oder die Eigenschaft festgelegt *glide.security.url.whitelist*lst auf einen Wert festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.security.url.whitelist.strict_check*lst auf „wahr“ und die Eigenschaft festgelegt *glide.security.url.whitelist*lst auf einen Wert festgelegt.
Gastanwender für SOAP-Anforderungen festlegen [aktualisiert in Security Center 1,3 und 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Zugriff auf Hintergrundskript beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Beschreibung: Diese Eigenschaft enthält die erforderliche Rolle für den Zugriff auf das Modul „Skripthintergrund“. Wenn *glide.script_processor.admin*lst nicht auf den empfohlenen Standardwert „Administrator“ festgelegt, können Anwender mit einer Rolle mit niedrigeren Berechtigungen Hintergrundskripts auf der Instanz ausführen. Dies führt zu einer vollständigen Umgehung des ACL-Systems, die vollständigen Zugriff auf Tabellen ermöglicht. • Alte Beschreibung: Diese Eigenschaft enthält die erforderliche Rolle für den Zugriff auf das Skript-Hintergrundmodul. Wenn *glide.script_processor.admin*lst nicht auf den empfohlenen Wert „admin“, „Security_admin“ oder „maint“ festgelegt, können Anwender mit einer Rolle mit niedrigeren Berechtigungen Hintergrundskripts auf der Instanz ausführen. Dies führt zu einer vollständigen Umgehung des ACL-Systems, die vollständigen Zugriff auf Tabellen ermöglicht. • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.script_processor.admin*lst auf den Administrator festgelegt. Dies ist der Standardwert für Instanzen. • Alte Korrektur: Stellen Sie die Eigenschaft sicher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	*glide.script_processor.admin*lst auf die Rolle admin, Security_admin oder Maintenance festgelegt.
Zertifikatkette und Hostname verifizieren [Neu in Security Center 1,3 und aktualisiert in 2,0]	• Neue Beschreibung: Wenn die Glide-Eigenschaft *com.glide.communications.httpclient.verify_hostn* nicht auf den sicheren Wert „wahr“ festgelegt, werden Hostname und Zertifikatkette, die von Remote-Hosts während einer von der ServiceNow-Instanz initiierten TLS-Verbindung angezeigt werden, nicht validiert. Dies könnte die Sicherheit der TLS-Verbindung gefährden und Personen-in-the-Middle-Angriffe ermöglichen, bei denen die Kommunikation zwischen zwei Parteien abgefangen wird. Dies kann zur Offenlegung vertraulicher Daten führen. • Alte Beschreibung: Wenn *com.glide.communications.httpclient.verify_hostn* nicht auf „wahr“ festgelegt. Dies kann Personen-in-the-Middle-Angriffe ermöglichen, bei denen die Kommunikation zwischen zwei Parteien abgefangen wird. Wenn Sie diese Eigenschaft auf einen unsicheren Wert festlegen, wird der Zertifikatverifizierungsprozess deaktiviert, der alle Zertifizierungen in der Zertifikatkette durch Überprüfung des Widerrufsstatus bewertet. Legen Sie diese Eigenschaft auf „wahr“ fest, um zu verhindern, dass der HTTP-Client eine Verbindung zu einem potenziell schädlichen Hostnamen herstellt.
Kontrollsperrzeit für ungültige Versuche zur Passwortzurücksetzung [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: *Control Lockout Time for Invalid Password Reset Attempts* • Alte Kurzbeschreibung: *Minimize Reset Password Request Max Attempts Window Duration* • Neue Beschreibung: Die *password_reset.request.max_attempt_window*Die Eigenschaft definiert die Anzahl der Minuten, die ein Anwender warten muss, um sein Passwort zurückzusetzen oder zu ändern, nachdem die maximale Anzahl nicht erfolgreicher Versuche überschritten wurde, die mit festgelegt wurde *password_reset.request.max_attempt*

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	property. Eine kleine Anzahl von Minuten für *password_reset.request.max_attempt_window*Die Eigenschaft erhöht das Risiko, dass ein Passwort erfolgreich durch Brute-Erzwingen erzwungen wird, da eine größere Anzahl von Versuchen zur Passwortzurücksetzung unternommen werden kann. Der Standardwert von 1440 Minuten wird empfohlen. • Alte Beschreibung: Wenn *password_reset.request.max_attempt_window*Ist nicht auf den empfohlenen Wert von 1440 oder weniger festgelegt, kann Account Bruteforce ausgeführt werden, da der Account nach einer maximalen Anzahl falscher Authentifizierungsversuche nicht gesperrt wird. • Neue Korrektur: Stellen Sie die Eigenschaft sicher *password_reset.request.max_attempt_window*Ist auf 1440 oder höher festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *password_reset.request.max_attempt_window*Ist auf maximal 1440 festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Legacy-Verhalten für GlideRecord-Umfangsabgrenzung deaktivieren [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]	• Neue Kurzbeschreibung: *Disable GlideRecord Scope Fencing Legacy Behavior* • Alte Kurzbeschreibung: *Enable GlideRecord Scope Fencing Legacy Behavior* • Neue Korrektur: Legen Sie die Glide-Eigenschaft fest *glide.record.legacy_cross_scope_access_policy_i* „falsch“. Wenn nicht in der Tabelle „sys_properties“ vorhanden, ist der Standardwert „wahr“. • Alte Korrektur: Legen Sie die Glide-Eigenschaft fest *glide.record.legacy_cross_scope_access_policy_i* „falsch“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Ungültige Passwortzurücksetzungsversuche begrenzen [aktualisiert in Security Center 1,3 und aktualisiert in 2,0]	• Neue Kurzbeschreibung: *Limit Invalid Password Reset Attempts* • Alte Kurzbeschreibung: *Minimize Reset Password Request Max Attempt Allowance*

Härtungseinstellungen für Baseline-Version 4,0 aktualisiert

Einige Härtungseinstellungen wurden mit Release von aktualisiert Security Center Baseline-Version 4,0.

Die Baseline-Version 4,0 enthält mehrere Updates für Kurzbeschreibungen, um Stil und Konsistenz zwischen Datensätzen zu gewährleisten. Darüber hinaus wurden auch viele eigenschaftsbezogene Skripts aktualisiert, um die Genauigkeit des Standardwerts in Fällen zu verbessern, in denen die Eigenschaft aus der Tabelle „sys_property“ entfernt wurde.

Dokumentation	FTP-Anwendernamen
Autorisierung für SOAP-Anforderungen anfordern [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Name der neuen technischen Konfiguration: *glide.basicauth.required.soap, glide.soap.require_ws_security* • Name der alten technischen Konfiguration: *glide.basicauth.required.soap* • Neue Beschreibung: Die Glide-Eigenschaft *glide.basicauth.required.soap*Steuert, ob die Standardauthentifizierung erforderlich ist, um eine SOAP-Anforderung an eine Instanz zu stellen. Wenn *glide.basicauth.required.soap*Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, werden nicht authentifizierte Anwender, die SOAP-Vorgänge ausführen, dem SOAP.Guest-Anwender zugeordnet. Dies kann einem nicht authentifizierten Anwender ermöglichen, Vorgänge auf der Instanz auszuführen, als wäre er bei der Instanz angemeldet. Es kann zusätzliche Auswirkungen haben, wenn der Anwender in definiert *com.glide.soap.guest_user*Sind zusätzliche Rollen zugewiesen. • Alte Beschreibung: Die Glide-Eigenschaft *glide.basicauth.required.soap*Steuert, ob eine Authentifizierung erforderlich ist, um eine SOAP-Anforderung an eine Instanz zu stellen. Wenn *glide.basicauth.required.soap*Ist nicht auf den empfohlenen Wert „wahr“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	festgelegt, ist die Authentifizierung für SOAP-Anforderungen in der Instanz deaktiviert. Sie ermöglicht nicht authentifizierten Zugriff auf Vorgänge auf Administrator- oder Wartungsebene, wodurch Sicherheitskontrollen innerhalb der Instanz aufgehoben werden. • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.soap`Ist auf den Wert „wahr“ festgelegt. Alternativ können Sie die Instanz für WS-Sicherheit konfigurieren, indem Sie die Eigenschaft festlegen `glide.soap.require_ws_security`Auf „wahr“ und befolgen Sie die Produktdokumentation, um WS-Sicherheitsprofile zu konfigurieren. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.soap`Ist in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Jelly-Skript mit Escape-Zeichen [aktualisiert in Security Center 1,3 und 1,5]	• Neue Beschreibung: Mit dieser Eigenschaft werden alle in enthaltenen JS- und HTML-Zeichenfolgen mit Escape-Zeichen versehen, bevor sie in den Ausgabestrom geschrieben werden, wodurch verhindert wird, dass mehrere XSS-Probleme auftreten. Wenn `glide.ui.escape_all_script`Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, dann ist das Escape-Zeichen von Skripts, die in Jelly injiziert wurden, deaktiviert. Ohne diese Minderung wird die Plattform weit geöffnet für eine Vielzahl von Skripteinschleusungsangriffen. Ein Angreifer kann beliebige Rhino-Skripts auf der Instanz ausführen. • Alte Beschreibung: Mit der folgenden Eigenschaft werden alle in <j:jelly> ... </j:jelly> enthaltenen JS- und HTML-Zeichenfolgen mit Escape-Zeichen versehen, bevor sie in den Ausgabestrom geschrieben werden, wodurch verhindert wird, dass mehrere XSS-Probleme auftreten. Wenn `glide.ui.escape_all_script`Ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	nicht auf den empfohlenen Wert „wahr“ festgelegt, dann ist das Escape-Zeichen von Skripts, die in Jelly injiziert wurden, deaktiviert. Ohne diese Minderung wird die Plattform weit geöffnet für eine Vielzahl von Skripteinschleusungsangriffen. Ein Angreifer kann beliebige Rhino-Skripts auf der Instanz ausführen.
Verhindern, dass Anwender eine Warnung zur Umgehung der CSRF-Validierung akzeptieren [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Verhindern Sie, dass Anwender eine Warnung akzeptieren, um die CSRF-Validierung zu umgehen • Alte Kurzbeschreibung: Strikte CSRF-Token-Validierung erzwingen • Neue Beschreibung: Diese Eigenschaft verhindert, dass Anwender eine Warnung akzeptieren können, die das Senden einer potenziell schädlichen Anforderung an die Instanz ermöglicht. Diese Warnung wird angezeigt, wenn eine POST-Anforderung aufgrund eines falsch übereinstimmenden Anti-CSRF-Tokens fehlschlägt, das zu einer der anderen aktiven Sitzungen des Opfers gehört. Wenn `glide.security.csrf.strict.validation.model` nicht auf den empfohlenen Wert „wahr“ festgelegt, kann ein Angreifer einen CSRF-Angriff mithilfe eines ausgelesenen Anti-CSRF-Tokens aus einer anderen aktiven Sitzung, die zum Opfer gehört, formulieren.Eine POST-Anforderung an eine Instanz enthält ein Anti-CSRF-Token in „sysparm_ck“ oder „X-UserToken“, das der aktuellen Sitzung des Anwenders entspricht. Wenn das Anti-CSRF-Token stattdessen an eine der anderen aktiven Sitzungen des Anwenders gebunden ist, gibt die POST-Anforderung eine 302-Umleitung an Security_Interceptor.do zurück, wobei dem Anwender eine Schaltfläche „Fortfahren“ zur Verfügung steht, wenn diese Eigenschaft auf „falsch“ festgelegt ist. Wenn Sie auf diese Schaltfläche klicken, wird die Anforderung erneut an die Instanz gesendet, es sei denn, sie verfügt jetzt über ein gültiges Anti-CSRF-Token. Wenn diese Eigenschaft auf „wahr“ festgelegt ist, zeigt die 302-Weiterleitung zur Seite „Security_interceptor.do“ keine Schaltfläche „Fortfahren“ an, und der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Anwender darf die Anforderung nicht erneut übermitteln.Ein erfolgreicher CSRF-Angriff ermöglicht es einem Angreifer, jeden Vorgang effektiv auszuführen, den das Opfer ausführen kann. • Alte Beschreibung: Diese Eigenschaft aktiviert die strikte Validierung des CSRF-Tokens, wodurch die Wiederverwendung von CSRF-Token verhindert wird. Wenn *glide.security.csrf.strict.validation.mode*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, können CSRF-Token wiederverwendet werden, was eine Tür für CSRF-Angriffe öffnet. • Neue CVSS-Punktzahl: 3,7 • Alte CVSS-Punktzahl: 3,1
Authentifizierung für Ereignismanagement-HTTP-Prozessor anfordern [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0]	• Neue Kurzbeschreibung: Authentifizierung für Ereignismanagement-HTTP-Prozessor erforderlich • Alte Kurzbeschreibung: Authentifizierung für Ereignismanagement-HTTP-Prozessor erforderlich
Anti-CSRF-Token aktivieren [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0]	• Neue Beschreibung: Cross-Site Request Forgery (CSRF) ist ein Angriff, der authentifizierte Anwender zwingt, eine Anforderung an eine Webanwendung zu übermitteln, für die sie derzeit authentifiziert sind. CSRF-Angriffe nutzen das Vertrauen einer Webanwendung in einen authentifizierten Anwender aus. Diese Eigenschaft ermöglicht die Verwendung eines sicheren Tokens zur Identifizierung und Validierung eingehender Anforderungen. Dieses Token wird verwendet, um Site-übergreifende Angriffe auf Anforderungsfälschung zu verhindern. Wenn *glide.security.use_csrf_token*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, ist CSRF möglich. • Alte Beschreibung: Cross-Site Request Forgery (CSRF) ist ein Angriff, der authentifizierte Anwender zwingt, eine Anforderung an eine Webanwendung zu übermitteln, für die sie derzeit authentifiziert sind. CSRF-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Angriffe nutzen das Vertrauen einer Webanwendung in einen authentifizierten Anwender aus. Diese Eigenschaft ermöglicht die Verwendung eines sicheren Tokens zur Identifizierung und Validierung eingehender Anforderungen. Dieses Token wird verwendet, um Site-übergreifende Angriffe auf Anforderungsfälschung zu verhindern. Wenn *glide.security.use_csrf_token*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, ist CSRF möglich.
HTML-Bereinigung in Virtual Agent aktivieren [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: HTML-Bereinigung in Virtual Agent aktivieren • Alte Kurzbeschreibung: HTML-Bereinigung aktivieren • Neue Beschreibung: Diese Eigenschaft steuert, ob der HtmlSanitizerService aktiviert ist. Wenn *com.glide.cs.html.sanitizer.enabled*lst nicht auf „wahr“ festgelegt, ist im VA-Webclient ein gespeicherter Angriff auf Cross-Site Scripting (XSS) möglich. • Alte Beschreibung: Diese Eigenschaft steuert, ob der HTMLSanitezerService aktiviert ist. Wenn *com.glide.cs.html.sanitizer.enabled*lst nicht auf „wahr“ festgelegt, ist im VA-Webclient ein gespeicherter Angriff auf Cross-Site Scripting (XSS) möglich.
Internen Zugriff auf explizite externe Rollen verweigern [aktualisiert in Security Center 1,3 und 1,5]	• Name der neuen technischen Konfiguration: *glide.security.explicit_roles.enable_internal_us* • Name der alten technischen Konfiguration: *glide.security.explicit_roles.enable_internal_us* • Neue Beschreibung: Diese Eigenschaft verhindert, dass externen Anwendern die Rolle „snc_internal“ zugewiesen wird. Wenn *glide.security.explicit_roles.enable_internal_us* auf den empfohlenen Wert „wahr“ festgelegt, dann erzwingt es die Parameter des wartungsgeschützten *glide.security.explicit_roles.internal_user_blac propertyW*elche die Rolle „snc_external“ einer Liste nicht vertrauenswürdiger

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Anwenderklassen zuweist. Wenn der Wert auf „falsch“ festgelegt ist, wird der *glide.security.explicit_roles.internal_user_blac* wird ignoriert. Eine falsche Konfiguration dieser Eigenschaft erhöht das Risiko, dass ein externer Anwenderaccount Zugriff auf interne Informationen erhält. • Alte Beschreibung: Dadurch wird verhindert, dass externen Anwendern die Rolle „snc_internal“ zugewiesen wird. Wenn *glide.security.explicit_roles.enable_internal_us* nicht auf den empfohlenen Wert „wahr“ und festgelegt *glide.security.explicit_roles.internal_user_blac* Eigenschaft ist nicht auf eine Liste nicht vertrauenswürdiger Anwenderklassen festgelegt. Den angegebenen Rollen kann die Rolle „snc_internal“ anstelle der Rolle „snc_external“ zugewiesen werden. Wenn die Liste leer ist, wird allen Anwendern standardmäßig die Rolle „snc_internal“ zugewiesen. Die Eigenschaft muss mindestens die Standardrollen csm_Consumer_user, Customer_contact enthalten. Eine falsche Konfiguration dieser Eigenschaften erhöht das Risiko, dass ein externer Anwenderaccount Zugriff auf interne Informationen erhält. • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.security.explicit_roles.enable_internal_us* auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.security.explicit_roles.enable_internal_us* auf „wahr“ festgelegt und die Eigenschaft *glide.security.explicit_roles.internal_user_blac* die gefährlichen Elemente csm_Consumer_user, Customer_contact. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Autorisierung für WSDL-Anforderung anfordern [aktualisiert in Security Center 1,3 und 1,5]	• Neue Beschreibung: Wenn *glide.basicauth.required.wsdl*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, wird die Standardauthentifizierung für WSDL-Anforderungen deaktiviert. WSDL ist ein Protokoll, das zur Beschreibung von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Webservices wie Instanztabellenschemata verwendet wird und kein Mechanismus für die gemeinsame Nutzung der Daten innerhalb von Tabellen ist. Wenn Sie diese Eigenschaft auf „wahr“ festlegen, können Tabellenschemas für nicht authentifizierte Anwender offengelegt werden. • Alte Beschreibung: Wenn `glide.basicauth.required.wsdl`Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, wird die Standardauthentifizierung für WSDL-Anforderungen deaktiviert. Dies kann zur Offenlegung von Informationen an nicht authentifizierte Anwender führen. • Neue CVSS-Punktzahl: 5,3 • Alte CVSS-Punktzahl: 4,3
Prüfung der URL-Zulässigkeitsliste erzwingen [aktualisiert in Security Center 1,3, 1,5 und 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Eingeschränkte herunterladbare MIME-Typen definieren [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Kurzbeschreibung: Definieren Sie eingeschränkte herunterladbare MIME-Typen • Alte Kurzbeschreibung: Herunterladbare MIME-Typen einschränken • Neue Beschreibung: Wenn `glide.ui.attachment.download_mime_types`Enthält gefährliche Elemente wie Text/HTML, Image/svg, image/svg, image/svg +xml,Application/xml, dann können gefährliche Dateien im Browser inline gerendert werden, was zu Cross Sitte Scripting-Angriffen (XSS) führen kann. Diese Eigenschaft ist die Liste der kommagetrennten MIME-Typen für Anhänge, die im Browser nicht inline gerendert werden. Beispielsweise erzwingt das Einbeziehen von Text/HTML-Dateien, dass HTML-Dateien als Anhänge auf den Client heruntergeladen werden, anstatt sie inline im Browser anzuzeigen. Wenn Sie diese Liste ordnungsgemäß verwalten, werden Site-übergreifende Skripting-Angriffe verhindert. • Alte Beschreibung: Wenn `glide.ui.attachment.download_mime_types`Enthält gefährliche Elemente wie Text/HTML, Image/svg, image/svg, image/svg +xml,Application/xml, dann können gefährliche Dateien im Browser inline

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	gerendert werden, was zu Cross Sitte Scripting-Angriffen (XSS) führen kann. Diese Eigenschaft ist die Liste der kommagetrennten MIME-Typen für Anhänge, die im Browser nicht inline gerendert werden. Beispielsweise erzwingt das Einbeziehen von Text/HTML-Dateien, dass HTML-Dateien als Anhänge auf den Client heruntergeladen werden, anstatt sie inline im Browser anzuzeigen. Wenn Sie diese Liste ordnungsgemäß verwalten, werden Site-übergreifende Skripting-Angriffe verhindert.
HTML in Listenansichten mit Escape-Zeichen versehen [aktualisiert in Security Center 1,3 und 1,5]	• Neue Beschreibung: Diese Eigenschaft hilft, die Listenansicht von HTML-Feldern zu bereinigen. Wenn *glide.ui.escape_html_list_field*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, kann ein böswilliger Anwender HTML-Code in das Formularfeld einschleusen, um unerwünschte Skripts in verschiedenen Client-/Anwendersitzungen auszuführen. Dies könnte potenziell von Angreifern genutzt werden, um Sitzungsinformationen und vertrauliche Daten zu stehlen. • Alte Beschreibung: Die folgende Eigenschaft hilft, die Listenansicht von HTML-Feldern zu bereinigen. Wenn *glide.ui.escape_html_list_field*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, kann ein böswilliger Anwender HTML-Code in das Formularfeld einschleusen, um unerwünschte Skripts in verschiedenen Client-/Anwendersitzungen auszuführen. Dies könnte potenziell von Angreifern genutzt werden, um Sitzungsinformationen und vertrauliche Daten zu stehlen.
Beschränken Sie E-Mail-Domänen für die Registrierung externer Anwender [Aktualisiert in Sicherheitscenter 1,3, 1,5 und 2,0]	• Neue Kurzbeschreibung: E-Mail-Domänen für die Registrierung externer Anwender einschränken • Alte Kurzbeschreibung: E-Mail-Domänen für die Registrierung externer Anwender beschränken (Plugin-Anwendbarkeit: Registrierung externer Anwender) • Neue Beschreibung: Die *sn_ext_usr_reg.allowed_email_domains*Die Eigenschaft definiert, welche E-Mail-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Adressen sich bei einer ServiceNow-Instanz selbst registrieren dürfen. Wenn `sn_ext_usr_reg.allowed_email_domains`lst nicht mit einer Liste zulässiger Domänen festgelegt, dann können Anwender mit einer beliebigen E-Mail-Adresse Accounts in den Instanzen registrieren. Wenn nicht definiert, können böswillige Akteure die Registrierung mithilfe von E-Mail-Adressen aus unerwünschten Domänen durchführen, um authentifizierten Zugriff auf die Instanz zu erhalten. • Alte Beschreibung: Wenn `sn_ext_usr_reg.allowed_email_domains`lst nicht mit einer weißen Liste von zulässigen Domänen festgelegt, dann können böswillige Akteure die Registrierung mithilfe von E-Mail-Adressen aus unerwünschten Domänen durchführen. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Captcha für die Registrierung externer Anwender aktivieren [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Captcha für die Registrierung externer Anwender aktivieren • Alte Kurzbeschreibung: Captcha für Registrierung externer Anwender aktivieren (Plugin-Anwendbarkeit: Registrierung externer Anwender) • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Minimieren Sie die Ablaufdauer des Links zur Registrierung externer Anwender [aktualisiert im Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Ablaufdauer des Links zur Registrierung externer Anwender minimieren • Alte Kurzbeschreibung: Ablaufdauer des Links zur Registrierung externer Anwender minimieren (Plugin-Anwendbarkeit: Registrierung externer Anwender) • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern
Download infizierter Dateien nicht zulassen [aktualisiert in Security Center 1,5 und 2,0]	• Neue Kurzbeschreibung: Download infizierter Dateien nicht zulassen • Alte Kurzbeschreibung: Download infizierter Dateien nicht zulassen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Neue Korrektur: Stellen Sie die Eigenschaft sicher *com.glide.snap.infected_download_allowed*Ist auf „falsch“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *com.glide.snap.infected_download_allowed*Ist auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Dateimime-Typ im SOAP-Webservice „AttachmentCreator“ validieren [Neu in Security Center 1,3 und aktualisiert in 1,5]	• Neue Beschreibung: Wenn *glide.attachment.enforce_security_validation*Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, gibt es keine Validierung für den MIME-Typ des Anhangs, und gefährliche Dateien könnten mit falschen Dateierweiterungen auf das System hochgeladen werden. Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden Dateien mit der richtigen Dateityperweiterung hochgeladen. Es ist eine Best Practice für Sicherheit, Dateien-Uploads mindestens mit der MIME-Typvalidierung zu validieren. • Alte Beschreibung: Wenn *glide.attachment.enforce_security_validation*Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, gibt es keine Validierung für den MIME-Typ des Anhangs, und gefährliche Dateien könnten mit falschen Dateierweiterungen auf das System hochgeladen werden. Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden Dateien mit der richtigen Dateityperweiterung hochgeladen. Es ist eine Best Practice für Sicherheit, Dateien-Uploads mindestens mit der MIME-Typvalidierung zu validieren. • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.attachment.enforce_security_validation*Ist auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.attachment.enforce_security_validation*Ist auf „wahr“ festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
MultiSSO-Debugging deaktivieren [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Deaktivieren Sie das MultiSSO-Debugging • Alte Kurzbeschreibung: MultiSSO-Debugging deaktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
Definieren zulässig ServiceNow Interne IP-Adressen [aktualisiert in Security Center 1,3 Und 1,5]	• Name der neuen technischen Konfiguration: `glide.ip.authenticate.strict` • Name der alten technischen Konfiguration: `glide.ip.authenticate.strict,glide.ip.authentica` • Neue Beschreibung: Wenn `glide.ip.authenticate.strict`Ist auf „wahr“ festgelegt, können interne ServiceNow-Mitarbeiter und -Systeme nur eingehende Verbindungen zur Instanz aus wichtigen IP-Bereichen herstellen. Dieses Limit bietet ServiceNow Einblick in die Instanz in wichtige interne Infrastruktur und verhindert den Zugriff von breiteren ServiceNow-Mitarbeitern wie Support- und Vertriebsmitarbeitern über Unternehmensnetzwerke. Wenn auf „wahr“ festgelegt, wird `glide.ip.authenticate.allow`Die Eigenschaft wird verwendet, um interne eingehende ServiceNow-Verbindungen zu gewähren. Wenn nicht auf „wahr“ festgelegt, wird ein breiterer interner IP-Bereich von ServiceNow wie in definiert `glide.ip.authenticate.allow`Wird verwendet, um interne eingehende ServiceNow-Verbindungen zu gewähren. • Alte Beschreibung: Wenn `glide.ip.authenticate.strict`Ist auf „wahr“ festgelegt, dann sind nur in angegebene IP-Bereiche angegeben `glide.ip.authenticate.allow.secured`Kann eingehende Verbindungen zur Instanz herstellen. Diese Eigenschaft enthält eine Liste nur wichtiger interner ServiceNow-IP-Bereiche (Secure VPN, DC). Wenn `glide.ip.authenticate.allow.secured`Ist nicht auf den empfohlenen Wert oder die empfohlene Permutation von „10.0,0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0,0/17, 149.96.0,0/16, 199.91.136.0/21, 148.139.0,0/16, 127.0,0.1“ oder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	die neuere Werteliste „10.0,0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0,0/17, 149.96.0,0/16, 199.91.136.0/21, 148.139.0,0/16, 127.0,0.1, 0:0:0:0:0:0:0:1, ::1“, wodurch IPv6 localhost zu Utah hinzugefügt wird. dann kann es möglich sein, dass nicht vertrauenswürdige Quellen außerhalb des SN-Rechenzentrums und eines sicheren VPN auf sensible Überwachungsendpunkte in Instanzen zugreifen. • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.ip.authenticate.allow.secured`Enthält nur vertrauenswürdige Werte und die Eigenschaft `glide.ip.authenticate.strict`Ist auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.ip.authenticate.allow.secured`Enthält nur Werte in „10.0,0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0,0/17, 149.96.0,0/16, 199.91.136.0/21, 148.139.0,0/16, 127.0,0.1, 0:0:0:0:0:0:0:1, ::1“ und dass die Eigenschaft `glide.ip.authenticate.strict`Ist auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Deaktivieren Sie die Entitätserweiterung im XMLDocument2-Streaming-Parser [Aktualisiert in Security Center 1,5]	• Neue Kurzbeschreibung: Entitätserweiterung im XMLDocument2-Streaming-Parser deaktivieren • Alte Kurzbeschreibung: Entitätserweiterung deaktivieren • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Domänentrennung auf Dot-Walking-Felder anwenden [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Kurzbeschreibung: Domänentrennung auf Dot-Walking-Felder anwenden • Alte Kurzbeschreibung: Domänentrennung auf Dot-Walking-Felder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	anwenden (Plugin-Anwendbarkeit: Domänentrennung) • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Berechtigungen für CMDB-Modell beschränken [aktualisiert in Security Center 1,3 und 1,5]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Beim Hintergrund der mobilen Anwendung muss die Zwischenablage gelöscht werden [Neu in Security Center 1,3 und aktualisiert 1,5]	• Neue Beschreibung: Die *glide.sg.clear_pasteboard_when_backgrounded*Die Eigenschaft steuert, ob Text, der aus der mobilen ServiceNow-App kopiert wurde, in der Zwischenablage und in der Zwischenablage beibehalten wird, nachdem sich die App im Hintergrundmodus befindet. Wenn nicht auf den empfohlenen Wert „wahr“ festgelegt ist, werden vertrauliche Informationen möglicherweise an die Android- oder iOS-Zwischenablage weitergegeben, wo sie für andere Anwendungen auf dem Gerät zugänglich gemacht werden können. • Alte Beschreibung: Die Eigenschaft *glide.sg.clear_pasteboard_when_backgrounded*Steue ob Text, der aus der mobilen ServiceNow-App kopiert wurde, in der Zwischenablage/in der Zwischenablage beibehalten wird, nachdem die App nicht mehr im Fokus ist. Wenn nicht auf den empfohlenen Wert „wahr“ festgelegt ist, werden vertrauliche Informationen möglicherweise an die Android- oder iOS-Zwischenablage weitergegeben, wo sie für andere Anwendungen auf dem Gerät zugänglich gemacht werden können.
Accountwiederherstellung aktivieren [aktualisiert in Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Accountwiederherstellung aktivieren • Alte Kurzbeschreibung: Accountwiederherstellung aktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
Deaktivieren Sie SQL-Fehlermeldungen [Aktualisiert in Security Center 1,3 und 1,5]	• Neue Beschreibung: Wenn *glide.db.loguser*lst nicht auf den empfohlenen Wert „falsch“ festgelegt, dann können Endanwendern vertrauliche serverseitige Fehlermeldungen angezeigt werden. Fehlermeldungen können Stapelverfolgungen und Informationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	zur Struktur der Datenbank enthalten, die einem Angreifer das Wissen liefern könnten, das für die erfolgreiche SQL-Injection erforderlich ist, wenn die Voraussetzungen vorhanden sind. Als Tiefenverteidigung sollten diese Fehlermeldungen dem Endanwender nicht angezeigt werden. • Alte Beschreibung: Wenn *glide.db.loguser*lst nicht auf den empfohlenen Wert „falsch“ festgelegt, dann können Endanwendern vertrauliche serverseitige Fehlermeldungen angezeigt werden.
Relative Links erzwingen [aktualisiert in Security Center 1,3 und 1,5]	• Neue Beschreibung: Die *glide.cms.catalog_uri_relative*Eigenschaft erzwingt relative Links aus dem URI-Parameter in /ess/catalog.do. Wenn *glide.cms.catalog_uri_relative*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, wird die URL nicht mit der Funktion „enforceRelativeURL(url)“ bereinigt. Absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil eines Parameters oder eines Feldwerts verwendet werden, wodurch die Quellseite zu einer von Angreifern kontrollierten Website weitergeleitet wird. Diese Eigenschaft wirkt sich auf das veraltete Content Management System (CMS) aus, das durch das Serviceportal ersetzt wurde. • Alte Beschreibung: Die *glide.cms.catalog_uri_relative*Eigenschaft erzwingt relative Links aus dem URI-Parameter in /ess/catalog.do. Wenn *glide.cms.catalog_uri_relative*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, wird die URL nicht mit der Funktion „enforceRelativeURL(url)“ bereinigt. Absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil eines Parameters oder eines Feldwerts verwendet werden, wodurch die Quellseite zu einer von Angreifern kontrollierten Website weitergeleitet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Schwellenwert für Entitätserweiterung für skriptfähige GlideXMLUtil minimieren [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Kurzbeschreibung: Schwellenwert für Entitätserweiterung minimieren für skriptfähige GlideXMLUtil • Alte Kurzbeschreibung: Schwellenwert für Entitätserweiterung minimieren • Neue Beschreibung: Diese Eigenschaft steuert den maximalen Betrag der Entitätserweiterung in einem XML-Parser. Wenn *glide.xmlutil.max_entity_expansion*lst nicht auf den empfohlenen Wert von 3000 oder weniger festgelegt, kann das skriptfähige GlideXMLUtil-Analysegerät angreifbar für Denial-of-Service-Angriffe sein. • Alte Beschreibung: Diese Eigenschaft steuert den maximalen Betrag der Entitätserweiterung in einem XML-Parser. Wenn *glide.xmlutil.max_entity_expansion*lst nicht auf den empfohlenen Wert von 3000 oder weniger festgelegt, kann der XML-Parser für Denial-of-Service-Angriffe angreifbar sein. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Legacy-Verhalten für GlideRecord-Umfangsabgrenzung deaktivieren [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]	• Neue Beschreibung: GlideRecord hat bereichsübergreifenden Erstellungs-/Aktualisierungszugriff für Tabellen bereitgestellt, die nicht mit dieser Zugriffsebene konfiguriert wurden. Um zu verhindern, dass bei Kunden Anwendungen beschädigt werden, wenn dieses bereichsbezogene Zugriffsverhalten gepatcht wurde, die Eigenschaft *glide.record.legacy_cross_scope_access_policy_i* erstellt. Bei „wahr“ greift der bereichsübergreifende Zugriff auf veraltetes Verhalten zurück (unsicher). Diese Eigenschaft deaktiviert die Umfangsdefinition, sodass bereichsbezogene Apps auf globale Skriptschnittstellen zugreifen können. Es ist die beste Sicherheitspraxis, Umfangsbeschränkungen zu haben. Die Umfangsdefinition stellt sicher, dass Anwendungen nur mit explizitem Zugriff oder innerhalb ihres Umfangs auf Ressourcen zugreifen können, wobei

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	das Prinzip der geringsten Berechtigung befolgt wird. Das Deaktivieren dieser Funktion kann Auswirkungen auf Vertraulichkeit, Verfügbarkeit und Integrität haben. • Alte Beschreibung: Veraltetes Verhalten hat Erstellungs-/Aktualisierungszugriff auf Tabellen bereitgestellt, die dies nicht zulassen. Um zu verhindern, dass bei Legacy-Kunden Anwendungen beschädigt werden, wenn dieses bereichsbezogene Zugriffsverhalten gepatcht wurde, die Eigenschaft `glide.record.legacy_cross_scope_access_policy_in` erstellt. Bei „wahr“ greift der bereichsübergreifende Zugriff auf veraltetes Verhalten zurück (unsicher). Diese Eigenschaft deaktiviert die Umfangsdefinition, sodass bereichsbezogene Apps auf globale Skriptschnittstellen zugreifen können. Es ist die beste Sicherheitspraxis, Umfangsbeschränkungen zu haben. Die Umfangsdefinition stellt sicher, dass Anwendungen nur mit explizitem Zugriff oder innerhalb ihres Umfangs auf Ressourcen zugreifen können, wobei das Prinzip der geringsten Berechtigung befolgt wird. Das Deaktivieren dieser Funktion kann Auswirkungen auf Vertraulichkeit, Verfügbarkeit und Integrität haben.
Aktualisierte Version des MultiSSO-Plugins aktivieren [aktualisiert in Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins aktivieren • Alte Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins aktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
SSL in LDAP-Authentifizierung aktivieren [aktualisiert in Security Center 1,5 und 2,0]	Das Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Passwortzurücksetzung für api-Anforderungen erzwingen [aktualisiert im Sicherheitscenter 1,5]	Das Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Passwortrichtlinie bei der Anmeldung nicht anwenden [in Security Center 1,5 aktualisiert und 2,0 entfernt]	• Neue Beschreibung: Durch Festlegen der Eigenschaft `glide.apply.password_policy.on_login`Auf „falsch“ wird zum Zeitpunkt der Anmeldung keine Passwortkomplexität erzwungen. Wenn Sie die Eigenschaft

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	auf „wahr“ festlegen, wird die Passwortkomplexität erzwungen und führt zu Compliance-Problemen der Organisation. Gemäß ASVS 4,03 v2.1.9 Empfehlungen: Stellen Sie sicher, dass keine Passwortzusammensetzungsregeln vorhanden sind, die den Typ der zulässigen Zeichen einschränken. Es dürfen keine Groß- oder Kleinbuchstaben, Zahlen oder Sonderzeichen erforderlich sein. (C6) Anstelle der Durchsetzung der Passwortkomplexität empfiehlt ASVS, eine Passwortlänge von mindestens 12 Zeichen zu erzwingen. Referenz: OWASP ASVS v4.0-Authentifizierung • Alte Beschreibung: Durch Festlegen der Eigenschaft *glide.apply.password_policy.on_login*Auf „falsch“ wird zum Zeitpunkt der Anmeldung keine Passwortkomplexität erzwungen. Wenn Sie die Eigenschaft auf „wahr“ festlegen, wird die Passwortkomplexität erzwungen und führt zu Compliance-Problemen der Organisation. Gemäß ASVS 4,03 v2.1.9 Empfehlungen: Stellen Sie sicher, dass keine Passwortzusammensetzungsregeln vorhanden sind, die den Typ der zulässigen Zeichen einschränken. Es dürfen keine Groß- oder Kleinbuchstaben, Zahlen oder Sonderzeichen erforderlich sein. (C6) Anstelle der Durchsetzung der Passwortkomplexität empfiehlt ASVS, eine Passwortlänge von mindestens 12 Zeichen zu erzwingen. Referenz: OWASP ASVS v4.0-Authentifizierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Verwenden Sie keine Demozertifikate für aktive saml-Konfigurationen [Aktualisiert in Security Center 1,5]	• Neue Kurzbeschreibung: Verwenden Sie keine Demozertifikate für aktive SAML-Konfigurationen • Alte Kurzbeschreibung: Keine Demozertifikate für aktive SAML-Konfigurationen verwenden (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
SAML notBefore- oder notOnOrAfter-Einschränkungsdauer minimieren [aktualisiert in Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Einschränkungsdauer für SAML „notBefore“ oder „notOnOrAfter“ minimieren • Alte Kurzbeschreibung: Einschränkungsdauer für SAML „notBefore“ oder „notOnOrAfter“ minimieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)
Blockieren Sie abgelaufene Anti-CSRF-Token [Aktualisiert in Security Center 1,5]	• Neue Kurzbeschreibung: Abgelaufene Anti-CSRF-Token blockieren • Alte Kurzbeschreibung: Abgelaufene CSRF-Token blockieren
Captcha für Gast-Walk-up-Experience in der Kundenserviceanwendung [Neu in Security Center 1,3 Und aktualisiert 1,5]	• Neue Kurzbeschreibung: Captcha für Gast-Walk-up-Experience in Kundenserviceanwendung erforderlich • Alte Kurzbeschreibung: Captcha für Gast-Walk-up-Experience in Kundenservice-Anwendung erfordern (Plugin-Anwendbarkeit: Gast-Walk-up-Experience für Kundenservice)
Identitätswechsel bei ACL-Bewertung in HR-App überprüfen [Neu in Security Center 1,3 Und aktualisiert in 1,5]	• Neue Kurzbeschreibung: Identitätswechsel bei ACL-Auswertung in HR-App überprüfen • Alte Kurzbeschreibung: Identitätswechsel bei ACL-Auswertung in HR-App überprüfen (Plugin-Anwendbarkeit: Bereichsbezogene Human Resources-App)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
HR-Fallaktualisierungen aus persönlichen E-Mails beschränken [Neu in Security Center 1,3 Und aktualisiert 1,5]	• Neue Kurzbeschreibung: HR-Fallaktualisierungen aus persönlichen E-Mails einschränken • Alte Kurzbeschreibung: HR-Fallaktualisierungen aus persönlichen E-Mails beschränken (Plugin-Anwendbarkeit: Bereichsbezogene Human Resources-App) • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Aktivieren Sie das MID-Audit-Protokoll [Neu in Security Center 1,3 Und aktualisiert in 1,5]	• Neue Kurzbeschreibung: MID-Audit-Protokoll aktivieren • Alte Kurzbeschreibung: MID-Audit-Protokoll aktivieren (Plugin-Anwendbarkeit: MID-Server)
Nutzung des Anmeldeinformationsalias erzwingen [Neu in Security Center 1,3 Und aktualisiert 1,5]	• Neue Kurzbeschreibung: Nutzung des Anmeldeinformationsalias erzwingen • Alte Kurzbeschreibung: Nutzung des Anmeldeinformationsalias erzwingen (Plugin-Anwendbarkeit: MID-Server)
Erforderliche jms-Connection Factorys [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]	• Neue Kurzbeschreibung: Erforderliche JMS-Connection Factorys • Alte Kurzbeschreibung: Erforderliche JMS-Connection Factorys (Plugin-Anwendbarkeit: MID-Server) • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Anhangsgröße in Trainings- und Vorhersageflows begrenzen [Neu in Security Center 1,3 Und aktualisiert 1,5]	• Neue Kurzbeschreibung: Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen • Alte Kurzbeschreibung: Anhangsgröße in Trainings- und Vorhersageflows begrenzen (Plugin-Anwendbarkeit: Platform Document Intelligence)
Stellen Sie sicher, dass ACLs der Archivtabelle aktiviert sind [Neu in Security Center 1,3 und aktualisiert in 1,5]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Audit-Ereignisse für Protokollsitzungen [Neu in Security Center 1,3 und aktualisiert in 1,5]	• Neue Beschreibung: Wenn die Glide-Eigenschaft `glide.authenticate.session_access.log_audit_ever`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	auf „wahr“ festgelegt, werden Sitzungs-Audit-Ereignisse in der Tabelle „sys_Session_Access_Audit“ erstellt. Es wird empfohlen, Informationen darüber zu protokollieren, wer auf eine Sitzung zugegriffen hat, um Untersuchungen böswilliger Akteure zu unterstützen. Protokollierte Informationen umfassen Anwender, Sitzungs-ID (nicht vertraulich), IP-Adresse, Rollen und Richtlinien. • Alte Beschreibung: Wenn die Glide-Eigenschaft *glide.authenticate.session_access.log_audit_ever* auf „wahr“ festgelegt, werden Sitzungs-Audit-Ereignisse in der Tabelle „sys_Session_Access_Audit“ erstellt. Es wird empfohlen, allgemeine Informationen zum Sitzungszugriff zu protokollieren, um Untersuchungen böswilliger Akteure zu unterstützen. Protokollierte Informationen umfassen Anwender, Sitzungs-ID (nicht vertraulich), IP-Adresse, Rollen und Richtlinien.
Bereichsbezogenen ACL-Zugriff für Playbooks für Informationsanforderungen erzwingen [neu in Security Center 1,3 und aktualisiert 1,5]	• Neue Kurzbeschreibung: Bereichsbezogenen ACL-Zugriff für Playbooks für Informationsanforderungen erzwingen • Alte Kurzbeschreibung: Bereichsbezogenen ACL-Zugriff für Playbooks für Informationsanforderungen erzwingen • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Inaktive Sitzungen proaktiv für ungültig erklären [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]	• Neue Beschreibung: Die Glide-Eigenschaft *glide.active.session.timeout.invalidate.session* ob eine Sitzung mit Zeitüberschreitung proaktiv für ungültig erklärt wird, bevor der Tomcat-Container die Sitzung für ungültig erklärt. Wenn diese Eigenschaft nicht auf „wahr“ festgelegt ist, kann es ein kleines Zeitintervall geben, in dem eine Sitzung mit Zeitüberschreitung nicht für ungültig erklärt wird (mehr als 60 Sekunden, abhängig von der Warteschlangengröße). Wenn eine Sitzung gekapert wird, kann ein Angreifer während dieses kurzen Zeitraums möglicherweise eine Sitzung verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte Beschreibung: Die Glide-Eigenschaft `glide.active.session.timeout.invalidate.session` ob eine Zeitüberschreitungssitzung proaktiv vor dem Tomcat-Container für ungültig erklärt wird. Wenn diese Eigenschaft nicht auf „wahr“ festgelegt ist, kann es ein kleines Zeitintervall geben, in dem eine Sitzung mit Zeitüberschreitung nicht für ungültig erklärt wird (mehr als 60 Sekunden, abhängig von der Warteschlangengröße). Wenn eine Sitzung gekapert wird, kann ein Angreifer während dieses kurzen Zeitraums möglicherweise eine Sitzung verwenden.
Größe des HTTP-Antworttexts begrenzen [Neu in Security Center 1,3 Und aktualisiert 1,5]	• Neue Kurzbeschreibung: HTTP-Antworttextgröße begrenzen • Alte Kurzbeschreibung: Stellen Sie sicher, dass HTTP-Antworten aufgrund der Größe des Antworttexts keine OutofMemory-Ausnahme auslösen

Härtungseinstellungen für Baseline-Version 2,0 aktualisiert

Einige Härtungseinstellungen wurden mit Release von aktualisiert Security Center Baseline-Version 2,0.

Dokumentation	FTP-Anwendernamen
Anzahl gleichzeitiger interaktiver Sitzungen minimieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Gleichzeitige interaktive Sitzungsmenge minimieren • Alte Kurzbeschreibung: Glide-Authentifizierung – Max. Gleichzeitige interaktive Sitzungen
Zertifikatvertrauen erzwingen [aktualisiert in Security Center 1,3, Wurde in 2,0 entfernt , Hinzugefügt in 7,0]	• Neue Kurzbeschreibung: Zertifikatvertrauen erzwingen • Alte Kurzbeschreibung: Zertifikat-Trust
SMS-Komplexität für Passwortzurücksetzung maximieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: SMS-Komplexität für Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: SMS-Komplexität des Passworts zurücksetzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Plugin für hohe Sicherheit aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Plugin für hohe Sicherheit aktivieren • Alte Kurzbeschreibung: Plugin für hohe Sicherheit
Strikte Sicherheit von Sitzungscookies erzwingen [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Strikte Sicherheit von Sitzungscookies erzwingen • Alte Kurzbeschreibung: Cookies für sichere Sitzung
Verwenden Sie keine Demozertifikate für aktive saml-Konfigurationen [Aktualisiert in Security Center 1,5]	• Neue Kurzbeschreibung: Keine Demozertifikate für aktive SAML-Konfigurationen verwenden (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter) • Alte Kurzbeschreibung: Verwenden Sie keine Demozertifikate für aktive SAML-Konfigurationen
Deaktivieren Sie die Entitätserweiterung im XMLDocument2-Streaming-Parser [Aktualisiert in Security Center 1,5]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Zulässige Java-Pakete beschränken [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Zulässige Java-Pakete einschränken • Alte Kurzbeschreibung: Allowlist für Java-Pakete
Verschleierung der mobilen App-UI erfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Verschleierung der Mobile-App-UI erforderlich • Alte Kurzbeschreibung: UI-Obfuscation der mobilen App
Öffentlichen Zugriff auf Favoriten deaktivieren [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: Deaktivieren Sie den öffentlichen Zugriff auf Favoriten • Alte Kurzbeschreibung: Öffentlicher Zugriff auf Favoriten
JavaScript mit Escape-Zeichen versehen [aktualisiert in Security Center 1,3]	• Neue Beschreibung: Die Glide-Eigenschaft `glide.html.escape_script`Hilft bei der Bereinigung von HTML-Feldern. Wenn `glide.html.escape_script` Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, werden Eingaben für HTML-Felder (Ausgabecodierung)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	aus einem Back-End-Java-Kontext nicht bereinigt, indem eingebettetes JavaScript entfernt wird. JavaScript in HTML-Feldern kann zu gespeicherten und reflektierten XSS führen. Die Fähigkeit, XSS zu verwenden, kann zu einer einfachen Berechtigungseskalation zu höheren Rollen wie Administrator führen, wo mehr seitliche Bewegungen ausgeführt werden können. • Alte Beschreibung: Die Glide-Eigenschaft *glide.html.escape_script*Hilft bei der Bereinigung von HTML-Feldern. Wenn *glide.html.escape_script*Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, werden Eingaben für HTML-Felder (Ausgabecodierung) aus einem Back-End-Java-Kontext nicht bereinigt, indem eingebettetes JavaScript entfernt wird. JavaScript in HTML-Feldern kann zu gespeicherten und reflektierten XSS führen. Die Fähigkeit, XSS zu verwenden, kann zu einer einfachen Berechtigungseskalation zu höheren Rollen wie Administrator führen, wo mehr seitliche Bewegungen ausgeführt werden können.
Xframe-Optionen festlegen, um die Einbettung von Websites von Drittparteien zu verhindern [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Legen Sie Xframe-Optionen fest, um die Einbettung von Websites von Drittparteien zu verhindern • Alte Kurzbeschreibung: Xframe-Optionen • Neue Beschreibung: Wenn *com.glide.cs.embed.xframe_options*Ist nicht auf den empfohlenen Wert „DENY“ oder „SAMEORIGIN“ festgelegt, kann der Inhalt der Webanwendung mithilfe eines ALLOW-FROM-URI in eine Drittpartei-Website eingebettet werden. Das Zulassen nicht vertrauenswürdiger Websites von Drittparteien kann Angriffe wie Clickjacking ermöglichen. • Alte Beschreibung: Wenn *com.glide.cs.embed.xframe_options*Ist nicht auf den empfohlenen Wert „DENY“ oder „SAMEORIGIN“ festgelegt, kann der Inhalt einer Webanwendung mithilfe eines ALLOW-FROM-URI in eine Drittpartei-Website eingebettet werden. Das Zulassen nicht vertrauenswürdiger

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Websites von Drittparteien kann Angriffe wie Clickjacking ermöglichen. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
HTML in Listenansichten mit Escape-Zeichen versehen [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: HTML in Listenansichten mit Escape-Zeichen versehen • Alte Kurzbeschreibung: HTML-Escape-Zeichen
Verschleierung der klassischen mobilen App-UI erfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Verschleierung der Classic Mobile App-UI erforderlich • Alte Kurzbeschreibung: Klassische Mobile-App-UI-Obfuscation
Standardmäßig mit leeren ACLs ablehnen [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Standardmäßig ablehnen mit leeren ACLs • Alte Kurzbeschreibung: Sicherheitsmanager – Standard Deny • Neue Beschreibung: Wenn *glide.sm.default_mode*lst nicht auf den empfohlenen Wert „Deny“ festgelegt, erlaubt der veraltete Sicherheitsmanager der Instanz Zugriff auf eine Ressource, wenn für diese Ressource keine ACLs definiert sind oder nur ACLs auf Tabellenebene mit Platzhaltern. Indem Sie diese Option festlegen, dass alles, für das keine expliziten ACLs festgelegt sind, manipuliert werden kann. • Alte Beschreibung: Wenn *glide.sm.default_mode*lst nicht auf den empfohlenen Wert „Deny“ festgelegt, ermöglicht es dem Legacy-Sicherheitsmanager den Zugriff auf eine Ressource, wenn für diese Ressource keine ACLs definiert sind oder nur ACLs auf Tabellenebene mit Platzhaltern. Indem Sie diese Option festlegen, dass alles, für das keine expliziten ACLs festgelegt sind, manipuliert werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Zeitfenster für Wiederholung der Anforderung zum Zurücksetzen des Passworts maximieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Zeitdauer des Wiederholungsfensters für Anforderung zur Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: Wiederholungsfenster für Anforderung zum Zurücksetzen des Passworts
Autorisierung für XSD-Anforderungen erfordern [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Autorisierung für XSD-Anforderungen erforderlich • Alte Kurzbeschreibung: XSD-Anforderungsautorisierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.xsd`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.xsd`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Jelly-Skript mit Escape-Zeichen [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Jelly-Skript mit Escape-Zeichen versehen • Alte Kurzbeschreibung: Jelly mit Escape-Zeichen versehen
Eingehende Transaktionen doppelt prüfen [aktualisiert in Security Center 1,3]	• Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.security.strict.updates`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.security.strict.updates`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Herunterladbare Dateitypen in statischem Inhalt einschränken [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Herunterladbare Dateitypen in statischem Inhalt einschränken • Alte Kurzbeschreibung: Dateitypen-Downloadbeschränkungen aus statischem Inhalt
Autorisierung für PDF-Anforderungen anfordern [Aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für PDF-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung der PDF-Anforderung • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.pdf`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.pdf`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Hochgeladene MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: Hochgeladene MIME-Typen einschränken • Alte Kurzbeschreibung: MIME-Typbeschränkung hochladen • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Veraltetes JQuery-Verhalten deaktivieren [aktualisiert im Securty Center 1,3]	• Neue Kurzbeschreibung: Legacy-JQuery-Verhalten deaktivieren • Alte Kurzbeschreibung: Veraltetes JQuery-Verhalten
Dauer des Entsperrungsfensters für Anforderung zum Zurücksetzen des Passworts maximieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Zeitdauer des Entsperrungsfensters für Anforderung zum Zurücksetzen des Passworts maximieren • Alte Kurzbeschreibung: Fenster zum Entsperren der Anforderung zum Zurücksetzen des Passworts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
MultiSSO-Debugging deaktivieren [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: MultiSSO-Debugging deaktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter) • Alte Kurzbeschreibung: Deaktivieren Sie das MultiSSO-Debugging • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Verhalten der Produktionsinstanz erzwingen [aktualisiert in Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Verhalten der Produktionsinstanz erzwingen • Alte Kurzbeschreibung: Verhalten der Produktionsinstanz
Ungültige Passwortzurücksetzungsversuche begrenzen [aktualisiert in Security Center 1,3 und aktualisiert in 2,0]	• Neue Kurzbeschreibung: Max. Zuschuss für Passwortzurücksetzungsanforderung minimieren • Alte Kurzbeschreibung: Max. Versuche zum Zurücksetzen der Passwortanforderung
Autorisierung für CSV-Anforderungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für CSV-Anforderungen erforderlich • Alte Kurzbeschreibung: CSV-Autorisierung anfordern • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.csv`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.csv`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Dauer des Erfolgsfensters für die Anforderung zum Zurücksetzen des Passworts minimieren [aktualisiert im Securty Center 1,3]	• Neue Kurzbeschreibung: Dauer des Erfolgsfensters für Anforderung zum Zurücksetzen des Passworts minimieren • Alte Kurzbeschreibung: Erfolgsfenster der Anforderung zum Zurücksetzen des Passworts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Strikte Sicherheit der SOAP-Anforderung erzwingen [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Strikte Sicherheit der SOAP-Anforderung erzwingen • Alte Kurzbeschreibung: SOAP-Anforderung – strikte Sicherheit
Autorisierung für SOAP-Anforderungen anfordern [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Kurzbeschreibung: Autorisierung für SOAP-Anforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung der SOAP-Anforderung • Neue Beschreibung: Die Glide-Eigenschaft *glide.basicauth.required.soap*Steuert, ob eine Authentifizierung erforderlich ist, um eine SOAP-Anforderung an eine Instanz zu stellen. Wenn *glide.basicauth.required.soap*Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, ist die Authentifizierung für SOAP-Anforderungen in der Instanz deaktiviert. Sie ermöglicht nicht authentifizierten Zugriff auf Vorgänge auf Administrator- oder Wartungsebene, wodurch Sicherheitskontrollen innerhalb der Instanz aufgehoben werden. • Alte Beschreibung: Die Glide-Eigenschaft *glide.basicauth.required.soap*Steuert, ob Authentifizierung erforderlich ist, um eine SOAP-Anforderung an eine Instanz zu stellen. Wenn „Glide.basicauth.required.SOAP“ nicht auf den empfohlenen Wert „wahr“ festgelegt ist, wird die Authentifizierung für SOAP-Anforderungen in der Instanz deaktiviert. Sie ermöglicht nicht authentifizierten Zugriff auf Vorgänge auf Administrator- oder Wartungsebene, wodurch alle Sicherheitskontrollen in der Instanz außer Kraft gesetzt werden. • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.soap*Ist in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.soap*Ist auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Validierung der XMLdoc2-Entität mit zulässiger Entitätserweiterung anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: XMLdoc2-Entitätsvalidierung mit allowlistDeable-Entitätserweiterung erforderlich • Alte Kurzbeschreibung: XMLdoc2-Entitätsvalidierung mit allowlistDeable-Entitätserweiterung
Domänentrennung auf Dot-Walking-Felder anwenden [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Kurzbeschreibung: Domänentrennung auf Dot-Walking-Felder anwenden (Plugin-Anwendbarkeit: Domänentrennung • Alte Kurzbeschreibung: Domänentrennung anwenden • Neue Beschreibung: Diese Eigenschaft steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie Domänentrennungsfunktionen für Dot-Walking-Felder anwenden. Wenn *glide.sys.domain.include_domain_condition_on_joi* in einer Instanz mit Domänentrennung nicht auf den empfohlenen Wert „wahr“ festgelegt, können vertrauliche Informationen offengelegt werden, die nicht für eine bestimmte Domäne freigegeben werden sollen. • Alte Beschreibung: Diese Eigenschaft steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie Domänentrennungsfunktionen für Dot-Walking-Felder anwenden. Wenn *glide.sys.domain.include_domain_condition_on_joi* nicht auf den empfohlenen Wert „wahr“ festgelegt, dann können vertrauliche Informationen offengelegt werden, die nicht für eine bestimmte Domäne freigegeben werden sollen. • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.sys.domain.include_domain_condition_on_joi* auf „wahr“ festgelegt, wenn das Plugin „Domänentrennung“ aktiv ist. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.sys.domain.include_domain_condition_on_joi* auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Beschränken Sie JSONP-Anforderungen auf vertrauenswürdige URLs [Aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: JSONP-Anforderungen auf vertrauenswürdige URLs beschränken • Alte Kurzbeschreibung: JSONP-Aufnahmeliste anfordern • Neue Beschreibung: Diese Eigenschaft gibt vertrauenswürdige URLs für den AngularJS $http-Service an, um JSONP-Anforderungen zuzulassen/abzulehnen. Eigenschaft ist erforderlich, da dies für Kunden eine potenziell störende Änderung ist. Daher benötigen sie eine Möglichkeit, ihre vertrauenswürdigen URLs hinzuzufügen. Wenn *angular.jsonp.inclusion_list.enabled*Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, dann sind JSONP-Anforderungen an eine beliebige URL zulässig. • Alte Beschreibung: Diese Eigenschaft gibt vertrauenswürdige URLs für den AngularJS $http-Service an, um JSONP-Anforderungen zuzulassen/abzulehnen. Eigenschaft ist erforderlich, da dies für Kunden eine potenziell störende Änderung ist. Daher benötigen sie eine Möglichkeit, ihre vertrauenswürdigen URLs hinzuzufügen. Wenn *angular.jsonp.inclusion_list.enabled*) Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, dann sind jsonp-Anforderungen an eine beliebige url zulässig.
Maximale SMS-Anzahl für Passwortzurücksetzungen pro Tag minimieren [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Max. SMS für Passwortzurücksetzung pro Tag minimieren • Alte Kurzbeschreibung: SMS zum Zurücksetzen des Passworts max. Pro Tag
Verzögerungsdauer der Passwortrücksetzung maximieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Verzögerungsdauer für Passwortzurücksetzung maximieren • Alte Kurzbeschreibung: Verzögerung der Passwortverifizierung zurücksetzen • Neue Beschreibung: Wenn *password_reset.verification.delay*Ist nicht auf den empfohlenen Wert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	von 1000 oder mehr festgelegt, führt dies dazu, dass die Anmeldung anfälliger für Brute-Force-Angriffe ist. Diese Verzögerung von Millisekunden schränkt die Fähigkeit eines böswilligen Akteurs ein, mithilfe von Automatisierungstools („Bots“) zu versuchen, die Identifizierungs- oder Verifizierungsdetails von Anwendern zu erraten. • Alte Beschreibung: Wenn *password_reset.verification.delay*lst nicht auf den empfohlenen Wert von 1000 oder mehr festgelegt, führt dies dazu, dass die Anmeldung anfälliger für Brute-Force-Angriffe ist. Diese Anzahl von Millisekunden schränkt die Fähigkeit eines Hackers ein, mithilfe von Automatisierungstools („Bots“) zu versuchen, die Identifizierungs- oder Verifizierungsdetails von Anwendern zu erraten.
Autorisierung für Daten-Broker-Rest-API anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für Daten-Broker-Rest-API erforderlich • Alte Kurzbeschreibung: Daten-Broker-Rest-API-Autorisierung • Neue Beschreibung: Wenn *glide.basicauth.required.databrokerrestapiproces* nicht auf den empfohlenen Wert „wahr“ festgelegt, ist keine Standardautorisierung für alle eingehenden Daten-Broker-Rest-API-Anforderungen erforderlich. Dies kann zur Offenlegung nicht authentifizierter Informationen aus der Instanz führen. • Alte Beschreibung: Ab Utah-Release, wenn *glide.basicauth.required.databrokerrestapiproces* nicht auf den empfohlenen Wert „wahr“ festgelegt, dann ist keine Standardautorisierung für alle eingehenden Daten-Broker-Rest-API-Anforderungen erforderlich. Dies kann zur Offenlegung nicht authentifizierter Informationen aus der Instanz führen. • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.databrokerrestapiproces* in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.databrokerrestapiproces* auf Instanzen mit Utah-Release und höher auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Autorisierung für JSONv2-Anforderung anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für JSONv2-Anforderung erforderlich • Alte Kurzbeschreibung: JSONv2-Anforderungsautorisierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.jsonv2*lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.jsonv2*lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
JavaScript-Tags in eingebettetem HTML deaktivieren [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Deaktivieren Sie JavaScript-Tags in eingebettetem HTML • Alte Kurzbeschreibung: Javascript-Tags in eingebettetem HTML zulassen • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.ui.security.codetag.allow_script*lst in der Tabelle „sys_properties“ vorhanden und auf „falsch“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.ui.security.codetag.allow_script*lst auf „falsch“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Plugin „Security Jump Start“ aktivieren (ACL-Regeln) [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Sicherheits-Jump-Start-Plugin aktivieren (ACL-Regeln) • Alte Kurzbeschreibung: Sicherheits-Jump-Start-Plugin (ACL-Regeln)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Gastanwender für SOAP-Anforderungen festlegen [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: Gastanwender für SOAP-Anforderungen festlegen • Alte Kurzbeschreibung: Gastanwender für SOAP-Anforderungen
Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: Externe XML-Entitäten einschränken • Alte Kurzbeschreibung: Allowlist für URL der XML-Entitätsvalidierung
ACLs zur Steuerung von Live-Profildetails aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Aktivieren Sie ACLs, um Live-Profildetails zu steuern • Alte Kurzbeschreibung: Aktivieren Sie ACLs, um Live-Profildetails zu steuern
Zugriff auf anwenderdefinierte Journaleinträge beschränken [in Security Center 1,3 aktualisiert und 2,0 entfernt]	• Neue Kurzbeschreibung: Zugriff auf anwenderdefinierte Journaleinträge beschränken • Alte Kurzbeschreibung: Sichere anwenderdefinierte Journaleinträge • Neue Beschreibung: Wenn `glide.live_feed.custom_journal.acl_check_enable` nicht auf den empfohlenen Wert „wahr“ festgelegt, dann müssen alle Anwender alle Journaleinträge in der Lebens-Feed-Funktion anzeigen können. Wenn Sie die Eigenschaft auf „wahr“ festlegen, werden ACLs in anwenderdefinierten Journalfeldern berücksichtigt, was eine gute Funktion ist. • Alte Beschreibung: Wenn `glide.live_feed.custom_journal.acl_check_enable` nicht auf den empfohlenen Wert „wahr“ festgelegt, dann müssen alle Anwender alle Journaleinträge anzeigen können. Wenn Sie die Eigenschaft auf „wahr“ festlegen, werden ACLs in anwenderdefinierten Journalfeldern berücksichtigt, was eine gute Funktion ist.
OTP-Lebensdauer für Passwortzurücksetzung auf 1 Stunde festlegen [aktualisiert in Security Center 2,0]	• Neue Beschreibung: Diese Eigenschaft `glide.pwd_reset.onetime.token.validity`Ermöglicht, dass der Link in der E-Mail zur Passwortzurücksetzung nach der in angegebenen Anzahl von Stunden abläuft `glide.pwd_reset.onetime.token.validity property`. Die Gültigkeitszeit des Tokens

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	zur Passwortzurücksetzung sollte entsprechend der normalen Anwender-Experience so kurz wie möglich gehalten werden. Eine lange Gültigkeitsdauer für das Token zur Passwortzurücksetzung kann böswilligen Akteuren bei der Kontoübernahme helfen. • Alte Beschreibung: Diese Eigenschaft *glide.pwd_reset.onetime.token.validity*Ermöglicht, dass der Link in der E-Mail zur Passwortzurücksetzung nach der in angegebenen Anzahl von Stunden abläuft *glide.pwd_reset.onetime.token.validity*Eigenschaft Die Gültigkeitszeit des Tokens zur Passwortzurücksetzung sollte entsprechend der normalen Anwender-Experience so kurz wie möglich gehalten werden. Eine lange Gültigkeitsdauer für das Token zur Passwortzurücksetzung kann Hacker helfen, die Accountübernahme durchzuführen.
Lesezugriff delegierter Entwickler beschränken [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Lesezugriff delegierter Entwickler beschränken • Alte Kurzbeschreibung: Liste mit Lesezugriff für delegierte Entwickler
Definieren zulässig ServiceNow Interne IP-Adressen [aktualisiert in Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Definieren Sie zulässige interne ServiceNow-IP-Adressen • Alte Kurzbeschreibung: Zugriffsberechtigungsliste für IP-Adressen
SOAP-Inhaltstyp validieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Validieren Sie den SOAP-Inhaltstyp • Alte Kurzbeschreibung: Überprüfung des SOAP-Inhaltstyps • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Autorisierung für Excel-Anforderungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für Excel-Anforderungen erforderlich • Alte Kurzbeschreibung: Excel-Anforderungsautorisierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	`glide.basicauth.required.excel`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.excel`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Autorisierung für API-Anforderungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für API-Anforderungen erforderlich • Alte Kurzbeschreibung: API-Anforderungsautorisierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.api`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.api`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Schwellenwert für Entitätserweiterung für skriptfähige GlideXMLUtil minimieren [aktualisiert in Security Center 1,3, 1,5 und 2,0]	• Neue Kurzbeschreibung: Schwellenwert für Entitätserweiterung minimieren • Alte Kurzbeschreibung: Schwellenwert für Entitätserweiterung wird festgelegt
Anwender während des Prozesses zum Zurücksetzen/Ändern des Passworts benachrichtigen [in Security Center 1,5 entfernt]	• Neue Kurzbeschreibung: Anwender während des Prozesses zum Zurücksetzen/Ändern des Passworts benachrichtigen • Alte Kurzbeschreibung: Prozess für Passwortzurücksetzung/Change-Benachrichtigung • Neue Korrektur: Stellen Sie sicher, dass der Prozess zur Passwortzurücksetzung Anwender über Passwortänderung oder -Zurücksetzung benachrichtigt. • Alte Korrektur: Stellen Sie sicher, dass der Prozess zum Zurücksetzen des Passworts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	Anwender benachrichtigt, wenn das Passwort geändert oder zurückgesetzt wird.
Veraltetes AngularJS-Verhalten deaktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Legacy AngularJS-Verhalten deaktivieren • Alte Kurzbeschreibung: Veraltetes AngularJS-Verhalten
Timeout-Dauer für Entsperrung der fehlgeschlagenen Anmeldung maximieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Zeitüberschreitungsdauer für Entsperren fehlgeschlagener Anmeldungen maximieren • Alte Kurzbeschreibung: Zeitüberschreitung beim Entsperren nach fehlgeschlagenen Anmeldungen verwalten
Kennzeichnung für „nur HTTP-Cookie aktivieren“ [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Kennzeichnung für „nur HTTP-Cookie aktivieren“ • Alte Kurzbeschreibung: Kennzeichnung für „nur HTTP-Cookie“ • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
ACLs für bereichsbezogene Administratoranwendungen aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: ACLs für bereichsbezogene Administratoranwendungen aktivieren • Alte Kurzbeschreibung: ACLs der bereichsbezogenen Administratoranwendung verwalten • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
UserCookie-Version 3,1 aktivieren [aktualisiert in Security Center 2,0]	• Neue Beschreibung: UserCookie v3 wird nur generiert, wenn Eigenschaft `glide.ui.secure.cookies.use_kmf`lst deaktiviert. UserCookie v3 ist nicht sicher, da geheimer Schlüssel für HMAC im Quellcode gespeichert und für alle Kunden identisch ist. Die schädliche Akteure unterstützen kann, diesen einen geheimen Schlüssel für Versuche zum Hijacking von Anwendersitzungen zu verwenden. • Alte Beschreibung: AnwenderCookie v3 wird nur generiert, wenn die Eigenschaft glide.ui.secure.cookies.use_kmf deaktiviert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	ist. UserCookie v3 ist nicht sicher, da geheimer Schlüssel für HMAC im Quellcode gespeichert und für alle Kunden identisch ist. Die Hacker unterstützen kann, diesen einen geheimen Schlüssel für Versuche zu verwenden, Anwendersitzungen zu überführen.
Autorisierung für XML-Anforderungen anfordern [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Autorisierung für XML-Anforderungen erforderlich • Alte Kurzbeschreibung: XML-Anforderungsautorisierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.xml`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.xml`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Minimieren Sie die Ablaufdauer des Links zur Registrierung externer Anwender [aktualisiert im Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Ablaufdauer des Links zur Registrierung externer Anwender minimieren • Alte Kurzbeschreibung: Ablauf des Links zur Registrierung externer Anwender
	• Neue Kurzbeschreibung: Konvertieren Sie eingehende E-Mail-Bilder in Anhänge • Alte Kurzbeschreibung: HTML für eingehende E-Mails konvertieren
SMTP-Empfängermenge minimieren [Aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: SMTP-Empfängermenge minimieren • Alte Kurzbeschreibung: Max. SMTP-Empfänger
Aktualisierte Version des MultiSSO-Plugins aktivieren [aktualisiert in Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins aktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte Kurzbeschreibung: Aktualisierte Version des Multi-SSO-Plugins ist aktiviert • Neue CVSS-Punktzahl: 7,1 • Alte CVSS-Punktzahl: 5
Ausführung der unformatierten Datenbankabfrage deaktivieren [in Security Center 1,3 aktualisiert und 2,0 entfernt]	• Neue Kurzbeschreibung: Deaktivieren Sie die Ausführung der Rohdatenbankabfrage • Alte Kurzbeschreibung: Zugriffssteuerungsanforderungen auf Vorgangsebene • Neue Beschreibung: Mit dieser Eigenschaft kann ein Anwender unformatierte SQL-Abfragen für die Datenbank ausführen, die Zugriff auf Tabellen und Daten außerhalb der GlideRecord-Beschränkungen gewähren können. Wenn `glide.db.allow_unsafe_dbi_execute_sql`Ist nicht auf den empfohlenen Wert „falsch“ festgelegt, dann kann aufgerufen werden `dbi.executeStatement()` Aus einem Glide-Skriptfähigen. • Alte Beschreibung: Mit dieser Eigenschaft kann ein Anwender RohSQL-Abfragen für die Datenbank ausführen, die Zugriff auf Tabellen und Daten außerhalb der GlideRecord-Einschränkungen gewähren können. Wenn `glide.db.allow_unsafe_dbi_execute_sql`Ist nicht auf den empfohlenen Wert „falsch“ festgelegt, dann kann aufgerufen werden `dbi.executeStatement()` Aus einem Glide-Skriptfähigen.
XML-Markup mit Escape-Zeichen [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: XML-Markup mit Escape-Zeichen versehen • Alte Kurzbeschreibung: XML-Escape-Zeichen • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.ui.escape_text`Ist in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.ui.escape_text`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Autorisierung für RSS-Anforderungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für RSS-Anforderungen erforderlich • Alte Kurzbeschreibung: RSS-Anforderungsautorisierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.rss`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.rss`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Maximal zulässige Anhangsgröße [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Zulässige Anhangsgröße minimieren • Alte Kurzbeschreibung: Maximal zulässige Anhangsgröße
Relative Links erzwingen [aktualisiert in Security Center 1,3 und 1,5]	• Neue Beschreibung: Die `glide.cms.catalog_uri_relative`Eigenschaft erzwingt relative Links aus dem URI-Parameter in /ess/catalog.do. Wenn `glide.cms.catalog_uri_relative`lst nicht auf den empfohlenen Wert „wahr“ festgelegt, wird die URL nicht mit der Funktion „enforceRelativeURL(url)“ bereinigt. Absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil eines Parameters oder eines Feldwerts verwendet werden, wodurch die Quellseite zu einer von Angreifern kontrollierten Website weitergeleitet wird. • Alte Beschreibung: Verwenden Sie `glide.cms.catalog_uri_relative`Eigenschaft zum Erzwingen relativer Links aus dem URI-Parameter in /ess/catalog.do. Wenn `glide.cms.catalog_uri_relative`lst nicht auf den empfohlenen Wert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	„wahr“ festgelegt, wird die URL möglicherweise nicht mit der Funktion „enforceRelativeURL(url)“ bereinigt.
SMS-Codebenachrichtigung für Registrierung und Verifizierung aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: SMS-Codebenachrichtigung für Registrierung und Verifizierung aktivieren • Alte Kurzbeschreibung: SMS-Codebenachrichtigung für Registrierung und Verifizierung
HTTP-Header-Wert für Cache-Steuerung [in Security Center 1,3 aktualisiert und 1,5 entfernt]	• Neue Kurzbeschreibung: Cache-Control HTTP-Header-Wert • Alte Kurzbeschreibung: Cache-Control HTTP-Headerwert • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Internen Zugriff auf explizite externe Rollen verweigern [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Internen Zugriff auf explizite externe Rollen verweigern • Alte Kurzbeschreibung: Interne Denylist für explizite Rollen aktivieren • Neuer technischer Konfigurationsname: glide.security.explicit_roles.enable_internal_user_blacklist,g • Alter technischer Konfigurationsname: glide.security.explicit_roles.enable_internal_user_blacklist • Neue Beschreibung: Dadurch wird verhindert, dass externen Anwendern die Rolle „snc_internal“ zugewiesen wird. Wenn *glide.security.explicit_roles.enable_internal_us* nicht auf den empfohlenen Wert „wahr“ und festgelegt *glide.security.explicit_roles.internal_user_blac* Eigenschaft ist nicht auf eine Liste nicht vertrauenswürdiger Anwenderklassen festgelegt. Den angegebenen Rollen kann die Rolle „snc_internal“ anstelle der Rolle „snc_external“ zugewiesen werden. Wenn die Liste leer ist, wird allen Anwendern standardmäßig die Rolle „snc_internal“ zugewiesen. Die Eigenschaft muss mindestens die Standardrollen csm_Consumer_user,Customer_contact enthalten. Eine falsche Konfiguration dieser Eigenschaften erhöht das Risiko, dass ein externer Anwenderaccount Zugriff auf interne Informationen erhält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte Beschreibung: Diese Eigenschaft verhindert, dass externen Anwendern die Rolle „snc_internal“ zugewiesen wird. Wenn *glide.security.explicit_roles.enable_internal_us* auf den empfohlenen Wert „wahr“ festgelegt und wird dann aktiviert *glide.security.explicit_roles.internal_user_blac propertyWo*durch die Rolle „snc_external“ zugewiesen werden kann. Wenn der Wert auf „falsch“ festgelegt ist, wird er deaktiviert *glide.security.explicit_roles.internal_user_blac* • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.security.explicit_roles.enable_internal_us* auf „wahr“ festgelegt und die Eigenschaft *glide.security.explicit_roles.internal_user_blac* die gefährlichen Elemente csm_Consumer_user, Customer_contact. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.security.explicit_roles.enable_internal_us* auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Einmalige Lebensdauer von Out-of-Band-Verifizierern minimieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Einmalige Lebensdauer des Out-of-Band-Verifizierers minimieren • Alte Kurzbeschreibung: Kurze einmalige Lebensdauer des Out-of-Band-Verifizierers
Autorisierung für Skriptanforderungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für Skriptanforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung der Skriptanforderung • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.scriptedprocessor*Ist in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	`glide.basicauth.required.scriptedprocessor`Ist auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Gleichzeitige interaktive Sitzungen begrenzen [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Gleichzeitige interaktive Sitzungen begrenzen • Alte Kurzbeschreibung: Limit für Glide-Authentifizierung für gleichzeitige interaktive Sitzungen • Neue Beschreibung: Diese Eigenschaft ist für die Verwendung mit dem Limit Concurrent Sessions (`com.glide.limit.concurrent.sessions`)-Plugin. Wenn das Plugin aktiv ist und die Eigenschaft auf „falsch“ festgelegt ist, kann ein Anwender eine beliebige Anzahl gleichzeitiger interaktiver Sitzungen in einer Instanz haben. Eine größere Anzahl offener Sitzungen bedeutet, dass Sitzungs-Hijacking sehr wahrscheinlich ist. • Alte Beschreibung: Diese Eigenschaft ist für die Verwendung mit dem Limit Concurrent Sessions (`com.glide.limit.concurrent.sessions`)-Plugin. Wenn das Plugin aktiv ist und die Eigenschaft auf „falsch“ festgelegt ist, kann ein Anwender eine beliebige Anzahl gleichzeitiger interaktiver Sitzungen in einer Instanz haben. Eine größere Anzahl offener Sitzungen bedeutet, dass Sitzungs-Hijacking sehr wahrscheinlich ist.
Verhindern, dass Anwender eine Warnung zur Umgehung der CSRF-Validierung akzeptieren [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Strikte CSRF-Token-Validierung erzwingen • Alte Kurzbeschreibung: Strikte CSRF-Validierung • Neue Beschreibung: Diese Eigenschaft aktiviert die strikte Validierung des CSRF-Tokens, wodurch die Wiederverwendung von CSRF-Token verhindert wird. Wenn `glide.security.csrf.strict.validation.mode`Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, können CSRF-Token wiederverwendet werden, was eine Tür für CSRF-Angriffe öffnet. • Alte Beschreibung: Diese Eigenschaft aktiviert die strikte Validierung des CSRF-Tokens, wodurch die Wiederverwendung von CSRF-Token verhindert wird. Wenn

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	`glide.security.csrf.strict.validation.mode`Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, kann das CSRF-Token erneut verwendet werden, wodurch CSRF-Angriffe eine Tür öffnen.
Zeitüberschreitungsdauer der Sitzungsaktivität minimieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Zeitüberschreitungsdauer der Sitzungsaktivität minimieren • Alte Kurzbeschreibung: Zeitüberschreitung bei Sitzungsaktivität
HTML-Bereinigung aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: HTML-Bereinigung aktivieren • Alte Kurzbeschreibung: HTML-Bereinigung
Zugriff auf Hintergrundskript beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Beschreibung: Diese Eigenschaft enthält die erforderliche Rolle für den Zugriff auf das Modul „Skripthintergrund“. Wenn `glide.script_processor.admin`Ist nicht auf den empfohlenen Wert „admin“, „Security_admin“ oder „maint“ festgelegt, können Anwender mit einer Rolle mit niedrigeren Berechtigungen Hintergrundskripts auf der Instanz ausführen. Dies führt zu einer vollständigen Umgehung des ACL-Systems, die vollständigen Zugriff auf Tabellen ermöglicht. • Alte Beschreibung: Diese Eigenschaft enthält die erforderliche Rolle für den Zugriff auf das Skript-Hintergrundmodul. Wenn `glide.script_processor.admin`Ist nicht auf den empfohlenen Wert „Administrator“ festgelegt, kann jeder Anwender mit einer Rolle mit niedrigen Berechtigungen Hintergrundskripts auf der Instanz ausführen. Dies führt zu einer vollständigen Umgehung des ACL-Systems, die vollständigen Zugriff auf Tabellen ermöglicht • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.script_processor.admin`Ist auf die Rolle admin, Security_admin oder Maintenance festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.script_processor.admin*lst auf Administrator festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Eingebetteten HTML-Code deaktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Eingebetteten HTML-Code deaktivieren • Alte Kurzbeschreibung: Eingebetteter HTML-Code
Absolute Sitzungszeitüberschreitungsdauer minimieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Absolute Sitzungszeitüberschreitungsdauer minimieren • Alte Kurzbeschreibung: Absolute Sitzungszeitüberschreitung
Standardmäßig Authentifizierung für vom Client aufrufbare Skripteinbindungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Authentifizierung standardmäßig für vom Client aufrufbare Skripteinbindungen erforderlich • Alte Kurzbeschreibung: Datenschutz für vom Client aufrufbare Skripteinbindungen
Zugriff auf skriptfähige GlideSystemUserSession-API beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: Zugriff auf skriptfähige GlideSystemUserSession-API beschränken • Alte Kurzbeschreibung: Zugriff auf die skriptfähige GlideSystemUserSession-API
HTML-Bereinigung erzwingen [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: HTML-Bereinigung erzwingen • Alte Kurzbeschreibung: Nicht bereinigtes HTML überprüfen • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Absolute Sitzungszeitüberschreitungsdauer minimieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Absolute Sitzungszeitüberschreitungsdauer minimieren • Alte Kurzbeschreibung: Absolute Sitzungszeitüberschreitung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Rollenbasierte Multifaktor-Authentifizierung aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Rollenbasierte Multifaktor-Authentifizierung aktivieren • Alte Kurzbeschreibung: Rollenbasierte Multifaktor-Authentifizierung
SAML notBefore- oder notOnOrAfter-Einschränkungsdauer minimieren [aktualisiert in Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Einschränkungsdauer für SAML „notBefore“ oder „notOnOrAfter“ minimieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter) • Alte Kurzbeschreibung: SAML-Einschränkung „notBefore“ oder „notOnOrAfter“ • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Beschränken Sie E-Mail-Domänen für die Registrierung externer Anwender [Aktualisiert in Sicherheitscenter 1,3, 1,5 und 2,0]	• Neue Kurzbeschreibung: E-Mail-Domänen für die Registrierung externer Anwender einschränken (Plugin-Anwendbarkeit: Registrierung externer Anwender) • Alte Kurzbeschreibung: Allowlist für E-Mail-Domäne für externe Anwenderregistrierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher *sn_ext_usr_reg.allowed_email_domains*Ist nicht auf einen leeren Wert festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *sn_ext_usr_reg.allowed_email_domains*Ist nicht auf einen leeren Wert festgelegt.
Dauer des Pausierfensters zum Zurücksetzen des Passworts maximieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Zeitdauer des SMS-Pausierungsfensters zum Zurücksetzen des Passworts maximieren • Alte Kurzbeschreibung: SMS-Pause-Fenster zum Zurücksetzen des Passworts • Neue Korrektur: Stellen Sie die Eigenschaft sicher *password_reset.sms.pause_window*Ist auf 2 oder größer festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	*password_reset.sms.pause_window*lst auf 2 festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Ausgehende SSLv2/SSLv3-Verbindungen deaktivieren [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Deaktivieren Sie ausgehende SSLv2/SSLv3-Verbindungen • Alte Kurzbeschreibung: SSLv2/SSLv3 wird deaktiviert
Autorisierung für Entladeanforderungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für Entladeanforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung der Entladeanforderung • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.unl*lst in „sys_properties_table“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.unl*lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
E-Mail-Spam-Bewertung und -Filterung aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: E-Mail-Spam-Bewertung und -Filterung aktivieren • Alte Kurzbeschreibung: E-Mail-Spam-Bewertung und -Filterung
Festlegung des anfänglichen eindeutigen LDAP-Namens aufheben [in Security Center 1,3 aktualisiert und 2,0 entfernt]	• Neue Kurzbeschreibung: Festlegung des eindeutigen LDAP-Namens aufheben • Alte Kurzbeschreibung: Eindeutiger LDAP-Anfangsname
Anti-CSRF-Token aktivieren [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0]	• Neue Kurzbeschreibung: Anti-CSRF-Token aktivieren • Alte Kurzbeschreibung: Anti-CSRF-Token

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Überprüfung der AJAXGlideRecord-ACL erfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: AJAXGlideRecord-ACL-Überprüfung erforderlich • Alte Kurzbeschreibung: ACL-Überprüfung von AJAXGlideRecord wird aktiviert
Identitätswechsel des Anwenders protokollieren [aktualisiert in Security Center 1,3 und 2,0]	Regelskript: Das Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.das Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Download infizierter Dateien nicht zulassen [aktualisiert in Security Center 1,5 und 2,0]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Captcha für die Registrierung externer Anwender aktivieren [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Captcha für Registrierung externer Anwender aktivieren (Plugin-Anwendbarkeit: Registrierung externer Anwender) • Alte Kurzbeschreibung: Captcha für Registrierung externer Anwender aktivieren
Deaktivieren Sie SQL-Fehlermeldungen [Aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Deaktivieren Sie SQL-Fehlermeldungen • Alte Kurzbeschreibung: SQL-Fehlermeldungen werden deaktiviert
Ablaufdauer der Anforderung zum Zurücksetzen des Passworts minimieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Ablaufdauer der Anforderung zum Zurücksetzen des Passworts minimieren • Alte Kurzbeschreibung: Ablauf der Passwortanforderung zurücksetzen • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Kontrollsperrzeit für ungültige Versuche zur Passwortzurücksetzung [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: Maximale Fensterdauer für Anforderung zur Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: Fenster „Max. Versuche zur Passwortanforderung zurücksetzen“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Herunterladbare MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: Herunterladbare MIME-Typen einschränken • Alte Kurzbeschreibung: Herunterladbare MIME-Typ-Denylist
Excel-Formeln mit Escape-Zeichen [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Excel-Formeln mit Escape-Zeichen versehen • Alte Kurzbeschreibung: Excel-Formel mit Escape-Zeichen versehen
Plugin für kontextbezogene Sicherheit aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Plugin für kontextbezogene Sicherheit aktivieren • Alte Kurzbeschreibung: Plugin für kontextbezogene Sicherheit
Accountwiederherstellung aktivieren [aktualisiert in Security Center 1,3 Und 1,5]	• Neue Kurzbeschreibung: Accountwiederherstellung aktivieren (Plugin-Anwendbarkeit: Single Sign-on für mehrere Anbieter) • Alte Kurzbeschreibung: Accountwiederherstellung • Neue Beschreibung: Diese Eigenschaft steuert die Accountwiederherstellungsfunktion, die die Möglichkeit zur Umgehung der Single Sign-on an speziell festgelegte Administratoren bindet. Wenn *glide.sso.acr.enabled*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, bleiben die lokalen interaktiven Anmeldungen (basierend auf Anwendername oder Passwort) aktiviert, wenn Single Sign-on auf der Instanz aktiviert ist. Durch die Eliminierung lokaler interaktiver Anmeldungen wird das Risiko eines nicht autorisierten Zugriffs auf die Instanz reduziert. • Alte Beschreibung: Diese Eigenschaft steuert die Account-Wiederherstellungsfunktion. Wenn *glide.sso.acr.enabled*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, ist die Accountwiederherstellung nach Anwender-ID nicht möglich. • Neue CVSS-Punktzahl: 6,5

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte CVSS-Punktzahl: 9,1 • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Autorisierung für Importanforderungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für Importanforderungen erforderlich • Alte Kurzbeschreibung: Autorisierung der Importanforderung • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.importprocessor`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.importprocessor`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Plugin für SNC-Zugriffssteuerung aktivieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: SNC-Zugriffssteuerungs-Plugin aktivieren • Alte Kurzbeschreibung: SNC-Zugriffssteuerungs-Plugin
Gleichzeitige Sitzungen auf allen Knoten begrenzen [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Begrenzen Sie gleichzeitige Sitzungen auf alle Knoten • Alte Kurzbeschreibung: Glide-Authentifizierung – Limit gleichzeitiger Sitzungen auf allen Knoten
Autorisierung für XML-Ausgabeanforderungen anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für XML-Ausgabeanforderungen erforderlich • Alte Kurzbeschreibung: XML-Ausgabeautorisierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.xmloutputprocessor`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	`glide.basicauth.required.xmloutputprocessor`lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Escape-Skripts in Scratchpad [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Escape-Skripts in Scratchpad • Alte Kurzbeschreibung: Scratchpad mit Escape-Zeichen versehen • Neue Beschreibung: Das Scratchpad ist eine einfache Möglichkeit, Informationen auf dem Server festzulegen, auf die im Browser zugegriffen werden kann. Ein Administrator kann alles skripten, was darin enthalten sein soll, einschließlich beliebiger Daten aus beliebigen Datensätzen. Wenn `glide.ui.escape_scratchpad`lst nicht auf den empfohlenen Wert „wahr“ festgelegt, dann ist es möglich, schädliches Skript wie eine Schwachstelle für siteübergreifendes Skripting auszuführen. • Alte Beschreibung: Das Scratchpad ist eine einfache Möglichkeit, Informationen auf dem Server festzulegen, auf die im Browser zugegriffen werden kann. Ein Administrator kann alles skript, was darin enthalten sein soll, einschließlich beliebiger Daten aus beliebigen Datensätzen.if `glide.ui.escape_scratchpad`lst nicht auf den empfohlenen Wert „wahr“ festgelegt, dann ist es möglich, schädliches Skript wie eine Schwachstelle für siteübergreifendes Skripting auszuführen.
Autorisierung für WSDL-Anforderung anfordern [aktualisiert in Security Center 1,3 und 1,5]	• Neue Kurzbeschreibung: Autorisierung für WSDL-Anforderung erforderlich • Alte Kurzbeschreibung: WSDL-Anforderungsautorisierung • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.basicauth.required.wsdl`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	*glide.basicauth.required.wsdl*lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Autorisierung für SCHEMAANFORDERUNGEN anfordern [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Autorisierung für SCHEMAANFORDERUNGEN erforderlich • Alte Kurzbeschreibung: Autorisierung der SCHEMAANFORDERUNG • Neue Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.schema*lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt. • Alte Korrektur: Stellen Sie die Eigenschaft sicher *glide.basicauth.required.schema*lst auf „wahr“ festgelegt. • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
Herunterladbare MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]	• Neue Kurzbeschreibung: Herunterladbare MIME-Typen einschränken • Alte Kurzbeschreibung: Herunterladbare MIME-Typen
Protokollierung für Anwender mit niedrigen Berechtigungen in der Skript-Sandbox deaktivieren [aktualisiert im Sicherheitscenter 1,3]	• Neue Kurzbeschreibung: Protokollierung für Anwender mit niedrigen Berechtigungen in Skript-Sandbox deaktivieren • Alte Kurzbeschreibung: Glide Security Logger – keine Protokollierung für Sandbox • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
X-Frame-options implementieren: SAMEORIGIN-Sicherheitsheader [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Implementieren Sie den Sicherheitsheader X-Frame-Options: SAMEORIGIN • Alte Kurzbeschreibung: X-Frame-Options: SAMEORIGIN • Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
Zugriff auf Leistungsüberwachung einschränken [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: Leistungsüberwachungszugriff einschränken • Alte Kurzbeschreibung: ACL für Leistungsüberwachung
Ausführliche SQL-Fehlermeldungen für Importprozessor deaktivieren [aktualisiert in Security Center 1,3]	Regelskript: Skript wurde aktualisiert, um die Erkennungsgenauigkeit zu verbessern.
SMS-Ablaufdauer für Passwortzurücksetzung minimieren [aktualisiert in Security Center 1,3]	• Neue Kurzbeschreibung: SMS-Expiracy-Dauer für Passwortzurücksetzung minimieren • Alte Kurzbeschreibung: SMS-Ablauf zum Zurücksetzen des Passworts
Erstellen von Anwendern aus eingehenden E-Mails deaktivieren [aktualisiert im Securty Center 1,3]	• Neue Kurzbeschreibung: Deaktivieren Sie das Erstellen von Anwendern aus eingehenden E-Mails • Alte Kurzbeschreibung: E-Mails nach Domäne beschränken • Neue Beschreibung: Ein Administrator kann eine E-Mail-Eigenschaft festlegen, um Anwender automatisch aus eingehenden E-Mails zu erstellen. Wenn diese Eigenschaft auf den unsicheren Wert festgelegt ist, erstellt die Instanz automatisch Anwender aus eingehenden E-Mails. Jeder erstellte Anwender hat dasselbe hartcodierte Standardpasswort, was die Umgehung der Authentifizierung durch Brute Force erleichtert. • Alte Beschreibung: Ein Administrator kann eine E-Mail-Eigenschaft festlegen, um Anwender automatisch aus eingehenden E-Mails zu erstellen. Wenn diese Eigenschaft auf den unsicheren Wert festgelegt ist, erstellt die Instanz automatisch Anwender aus eingehenden E-Mails. Jeder erstellte Anwender hat dasselbe hartcodierte Standardpasswort, was die Umgehung der Authentifizierung durch Brute Force erleichtert. • Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.pop3readerjob.create_caller` Ist auf „falsch“ festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dokumentation	FTP-Anwendernamen
	• Alte Korrektur: Stellen Sie die Eigenschaft sicher `glide.pop3readerjob.create_caller`Ist auf „falsch“ festgelegt

Härtungseinstellungen gelöscht

Einige Härtungseinstellungen werden aus Sicherheitscenter-Baselines entfernt.

Härtungseinstellungen für Baseline-Version 6,0 gelöscht

Einige Härtungseinstellungen wurden mit dem Release der Security Center-Baseline-Version 6,0 entfernt.

- ACL für HR-Lebenszyklus-Ereignisdaten erzwingen
- Sicherheitsbereich für Playbook für Lizenzen und Berechtigungen erzwingen
- ACL für HR Core-Daten erzwingen
- Beschränken Sie globale Administratoren daran, bereichsbezogene App-Zugriffsbeschränkungen zu umgehen
- Legacy-AngularJS-Verhalten deaktivieren
- ACLs auf Feldebene in GlideRecordSandbox erzwingen
- Bereichssicherheit für Digitale Dienste für den öffentlichen Bereich erzwingen
- Herunterladbare Dateitypen in statischen Inhalten beschränken
- Bereichsbezogenen ACL-Zugriff für Information Request Playbooks erzwingen
- SAML-Einschränkungsdauer für „notBefore“ oder „notOnOrAfter“ minimieren
- Lesezugriff für delegierte Entwickler beschränken
- Passwortrichtlinie für alle Methoden erzwingen
- Sicherheitsbereich für Serviceanwendungsinformationen erzwingen
- Verschleierung der klassischen mobilen App-UI erfordern
- SSL in LDAP-Authentifizierung aktivieren
- Sicherheitsbereich für Mitarbeiterbereich für HR-Fallmanagement erzwingen
- Anhangsgröße in Trainings- und Vorhersage-Flows begrenzen
- Anmeldeinformationen von Willkommensseite entfernen
- ACL für HR Virtual Agent-Daten erzwingen
- Identitätswechsel für ACL-Auswertung in HR-App prüfen
- Zulässige Java-Pakete beschränken
- Erzwingen Sie Strikte Codesignaturprüfungen

Härtungseinstellungen für Baseline-Version 5,0 gelöscht

Einige Härtungseinstellungen wurden mit dem Release der Security Center-Baseline-Version 5,0 entfernt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Authentifizierung für Ereignismanagement-HTTP-Prozessor anfordern
- Beschränken Sie den Zugriff auf anwenderdefinierte Journaleinträge
- Wenden Sie bei der Anmeldung keine Passwortrichtlinie an
- Deaktivieren Sie Die Ausführung Der Abfrage Der Rohdatenbank
- HTML-Bereinigung protokollieren
- Aktivieren Sie Anti-CSRF-Token
- Erzwingen Sie Das Zertifikatvertrauen
- Heben Sie die Festlegung des eindeutigen LDAP-Initialnamens auf
- Mindestlänge von Passwörtern festlegen

Härtungseinstellungen für Baseline-Version 4,0 gelöscht

Einige Härtungseinstellungen wurden mit Release von entfernt Security Center Baseline-Version 4,0.

- Anfängliches LDAP-Passwort
- Mobile Offline-Rollen
- Zugriff auf kritische Daten durch Zero Trust-Zugriffsrichtlinien beschränken (Plugin-Anwendbarkeit: Adaptive Authentifizierung)
- Schreibgeschützte Tabellen-Allowlist Für Schreiben
- Zulässige JDBC-Probe-Vorgänge (Plugin-Anwendbarkeit: MID-Server)
- Legen Sie zulässige Domänen fest, die Anwender aus eingehenden E-Mails erstellen
- Komplexes Standardpasswort festlegen
- Zugängliche Eigenschaften in GraphQL-Allowlist
- Ursprungsübergreifende Messaging-Allowlist
- Anhangsgröße in Trainings- und Vorhersageflows für GraphQL-Enpunkte begrenzen (Plugin-Anwendbarkeit: Platform Document Intelligence)
- Allowlist „Inhaltsrollen Bearbeiten“ (Plugin-Anwendbarkeit: Communities)
- Stellen Sie sicher, dass Datenbankabfragen aufgrund der Abfragegröße keine OutofMemory-Ausnahme auslösen
- Rollenzuweisungsliste für Skriptausführung
- Allowlist Für Herunterladbaren Dateityp
- Schreibgeschützte Tabellen-Allowlist Zum Löschen
- Authentifizierung für rollenlose ACL erzwingen
- Minimieren Sie die Ablaufzeit von LDAP-Einmaltoken
- Nur vertrauenswürdige IP-Adressen für die Authentifizierung zulassen
- Legen Sie die mobile Passwortzurücksetzungs-URL
- Passwortkomplexität von Service-Accounts (Plugin-Anwendbarkeit: Service Bridge)
- Benachrichtigen Sie Anwender Während Des Prozesses Zum Zurücksetzen/Ändern Des Passworts
- Einschränkungen Des Anwendungsbereichs Erzwingen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zugriffssteuerungsanforderungen (Plugin-Anwendbarkeit: Communities)
- Allowlist Für Datensatzverlaufszugriffsrolle
- Beschränken Sie den Rollenzugriff für Anhänge
- Nur PDFs aus der vordefinierten Liste vertrauenswürdiger URLs zulassen
- Verhindern Sie das E-Mail-Senden eines einmaligen Passworts während eines LDAP-Serverausfalls
- Konvertieren Sie eingehende E-Mail-Bilder in Anhänge
- Überprüfen Sie Die Externe Explizite Rollenzugriffssteuerungsbedingung

Härtungseinstellungen für Baseline-Version 2,0 gelöscht

Einige Härtungseinstellungen wurden mit Release von entfernt Security Center Baseline-Version 2,0.

- Aktivieren Sie die Codesignatur für Anwendungskonfigurationsdaten und -Skripts
- Aktivieren Sie den Glide-KMF-Verschlüsseler
- Deaktivieren Sie die Verwendung des Verschlüsselers auf Instanzebene
- Aktivieren Sie Die Interne Denylist Für Explizite Rollen
- Direkte Einfügungen in MID-ECC-Warteschlange für Codesignaturanforderung blockieren
- Protokollieren Sie alle Felder für ausgehende HTTP-Anforderungen

Zugriffssteuerung

Die Zugriffssteuerungskategorie auditiert den Prozess zum Schutz von Ressourcen vor nicht autorisiertem Zugriff durch Gewährung und Ablehnung von Anforderungen basierend auf einem Berechtigungsmodell. Dies umfasst die Sicherstellung, dass eine Entität, die auf eine Ressource zugreift, gültige Anmeldeinformationen dazu enthält, einen klar definierten Satz von Rollen oder Berechtigungen zu erstellen und zu schützen und sicherzustellen, dass Rollen- oder Berechtigungssteuerungen vor Wiedergabe und Manipulation geschützt sind.

Zugriffssteuerungen bestimmen, ob der Zugriff auf eine bestimmte Ressource gewährt oder verweigert werden soll. Sie ermöglicht nur den Anwendern Zugriff auf Ressourcen, die sie verwenden dürfen.

Validierungszeit des Anti-CSRF-Tokens [Neu in Security Center 1,3]

Die `glide.security.csrf_previous.time_limit`Eigenschaft gibt die Zeit in Sekunden an, bis ein sicheres Token abläuft.

Wenn eine Anwendersitzung abläuft, läuft das sichere Token damit ab, es sei denn, es handelt sich um den **Die Wiederverwendung abgelaufener Token ist zulässig** Eigenschaft ist aktiviert und liegt innerhalb des von dieser Eigenschaft beschriebenen Zeitrahmens. Dieses Token wird verwendet, um Site-übergreifende Angriffe auf Anforderungsfälschung zu verhindern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.csrf_previous.time_limit`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	86400 Sekunden oder 1 Tag
Standardwert	86400 Sekunden oder 1 Tag
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt wird, wird die Tokenvalidierung deaktiviert, die verwendet wird, um Site-übergreifende Angriffe auf gefälschte Anforderungen zu verhindern.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft bestimmt die Dauer in Sekunden, bis ein sicheres Token gültig bleibt. Das sichere Token läuft ab, wenn die Anwendersitzung abläuft, es sei denn **Wiederverwendung abgelaufener Token zulassen** Eigenschaft ist aktiviert, und das Token befindet sich innerhalb des in dieser Eigenschaft angegebenen Zeitrahmens. Dieses Token verhindert Site-übergreifende Angriffe auf Anforderungsfälschung. Der Standardwert beträgt 86400 Sekunden oder 1 Tag.

Domänentrennung auf Dot-Walking-Felder anwenden [aktualisiert in Security Center 1,3, 1,5 und 2,0]

Die *glide.sys.domain.include_domain_condition_on_join*Die Eigenschaft steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie Domänentrennungsfunktionen für Dot-Walking-Felder anwenden.

Diese Eigenschaft steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie Domänentrennungsfunktionen für Dot-Walking-Felder anwenden. Wenn *glide.sys.domain.include_domain_condition_on_join*Ist in einer Instanz mit Domänentrennung nicht auf den empfohlenen Wert „wahr“ festgelegt, können vertrauliche Informationen offengelegt werden, die nicht für eine bestimmte Domäne freigegeben werden sollen. Es kann moderate funktionale Auswirkungen auf die Instanz haben, wenn Komponenten von den unsicheren domänenübergreifenden Abfragen abhängig sind. Instanzen sollten vor der Aktivierung in Subproduktionsumgebungen getestet werden.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.sys.domain.include_domain_condition_on_join*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	Boolean
Empfohlener Wert	„Wahr“, wenn die Domänentrennung installiert ist, andernfalls ist die Eigenschaft nicht vorhanden.
Standardwert	falsch
Kategorie	Zugriffssteuerung
Zweck	Steuert, ob Join-Abfragen domänengetrennte Bedingungen erhalten oder nicht, um sicherzustellen, dass sie Domänentrennungsfunktionen für Dot-Walking-Felder anwenden.
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn *glide.sys.domain.include_domain_condition_on_join* nicht auf den empfohlenen Wert von festgelegt **Wahr** , Dann können vertrauliche Informationen offengelegt werden, die nicht für eine bestimmte Domäne freigegeben werden sollen.
Referenzen	Domänentrennung für Service Provider

Blockieren Sie den Zugriff für delegierte Entwickler

Diese Konfiguration wirkt sich auf den Zugriff delegierter Entwickler aus, die Anwenderrollen über ein Skript aktualisieren. Wenn die Konfiguration konform ist, kann der Entwickler keine Datensätze aktualisieren oder in einfügen sys_user_has_role Tabelle Ohne auch Hat Die Rolle user_admin.

Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf die Funktionalität in der Instanz gewähren oder erhalten darf. Wenn die Eigenschaft Rollen enthält, können nur diese Rollen Skriptmodule ausführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.sys.security.delegateddev.block_grant_roles*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Der Wert dieser Eigenschaft wirkt sich darauf aus, ob ein delegierter Entwickler unerwarteten Zugriff auf die Funktionalität in der Instanz gewähren oder erhalten darf.
Typ	Umschalter
Standardwert	wahr
Empfohlener Wert	wahr

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsabhängigkeiten	Keine
Sicherheitsrisikobewertung	6.7
Funktionale Auswirkung	Wenn ein Anwender mit der Rolle „Delegated_Developer“ versucht, einen Datensatz in der Tabelle „sys_user_has_role“ zu ändern, aktiviert diese Eigenschaft zusätzliche Sicherheitsprüfungen für den Vorgang. Die zusätzlichen Sicherheitsprüfungen validieren, dass dem Anwender gewährt wurde User_admin Rolle, wenn versucht wird, zu erstellen oder zu aktualisieren Die Tabelle „sys_user_has_role“ . Wenn sie nicht über verfügen User_admin Rolle, wird der Zugriff verweigert. Wenn die Eigenschaft „falsch“ ist, werden diese zusätzlichen Prüfungen nicht validiert.
Sicherheitsrisiko	(Mittel) ohne entsprechende Autorisierung können nicht autorisierte Anwender auf vertrauliche Inhalte/Daten in der Instanz zugreifen.
Referenzen	Zugriffssteuerung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Blockieren Sie abgelaufene Anti-CSRF-Token [Aktualisiert in Security Center 1,5]

Blockieren Sie abgelaufene CSRF-Token, um Site-übergreifende Angriffe auf Anforderungsfälschung zu verhindern.

Übersicht

Cross-Site-Anforderungsfälschungen sind eine Art böswilliger Exploit, bei dem nicht autorisierte Befehle im Namen eines authentifizierten Anwenders ausgeführt werden.

Konfigurationsdetails

Attribut	Beschreibung
Übersicht	Steuert die Verwendung eines abgelaufenen sicheren Tokens zur Identifizierung und Validierung eingehender Anforderungen. Auf festlegen **Falsch** Verhindert, dass ein zuvor abgelaufenes Token eine eingehende Anforderung validiert.
Konfigurationsname	`glide.security.csrf_previous.allow`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	**false**
Standardwert	**true**
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	**Schweregradpunktzahl** : 6,5
	Schweregradbewertung pro CVSS-Punktzahl : Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Sicherheitsrisikodetails : Erzwingt einen starken Anti-CSRF-Mechanismus zum Schutz authentifizierter Funktionen, und eine effektive Anti-Automation oder Anti-CSRF schützt nicht authentifizierte Funktionen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Anti-CSRF-Token aktivieren [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0], Cross-Site-Anforderungsfälschung .

Überprüfen Sie die UI-Aktionsbedingungen vor der Ausführung

Verwenden Sie `glide.security.strict.actions`Eigenschaft zum Überprüfen von UI-Aktionsbedingungen in Formularen und Listen, bevor sie ausgeführt werden. Wenn Sie diese Eigenschaft auf festlegen Wahr , Fügt den UI-Aktionen der Tabelle eine zusätzliche Validierungsebene hinzu, bevor sie ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.strict.actions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um eine zusätzliche Validierungsebene für die Tabellen-UI-Aktionen sicherzustellen, bevor sie ausgeführt werden.
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	3.3
Funktionale Auswirkung	Diese Korrektur fügt nur eine zusätzliche Validierungsebene hinzu, um nach UI-Aktionen in der Zieltabelle/-Seite in der Instanz zu suchen. Solange die Zugriffssteuerungen in der Kundeninstanz entsprechend festgelegt sind, sollte dies keine Auswirkungen haben.
Sicherheitsrisiko	(Niedrig) Zugriffsanforderung wird immer aktiviert, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang validiert alle UI-Aktionen, bevor das Formular für den Endanwender gerendert wird.
Referenzen	Plugin für hohe Sicherheit

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administratorrollen für Ereignismanagement-Zuweisungsgruppe konfigurieren [Neu in Security Center 1,5]

Verwenden Sie *evt_mgmt.connector_assignment_group_admin_roles*Eigenschaft zum Festlegen, welche Rollen für den Administratorzugriff über das Zuweisungsgruppenfeld in Connector-Instanzen berechtigt sind.

Die *evt_mgmt.connector_assignment_group_admin_roles*Die Eigenschaft enthält eine kommagetrennte Zeichenfolge, die die Rollennamen angibt, die in Connector-Instanzen Administratorzugriff über das Zuweisungsgruppenfeld haben. Durch das Ändern der Standardrollen in dieser Liste können nicht autorisierte Anwender Ereignisintegrationen in der Instanz ändern. Um nicht autorisierten Zugriff auf Rollen zu verhindern, legen Sie fest *evt_mgmt.connector_assignment_group_admin_roles*Auf den Wert admin,evt_mgmt_admin,sn_SOW_srm.srm_admin. Überprüfen Sie alle zusätzlichen Rollen in der Zeichenfolge des empfohlenen Werts, um sicherzustellen, dass die Rolle eingeschlossen werden soll.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*evt_mgmt.connector_assignment_group_admin_roles*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	admin,evt_mgmt_admin,sn_SOW_srm.srm_admin
Standardwert	admin,evt_mgmt_admin,sn_SOW_srm.srm_admin
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Durch das Ändern der Standardrollen können nicht autorisierte Anwender Ereignisintegrationen in der Instanz ändern.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Gruppen werden erstellt

Allow-Liste für Serviceportal-Widgets konfigurieren [Neu in Security Center 2,0]

Erfahren Sie, wie Sie die Eigenschaft glide.service_portal.widget.allow_list sicher konfigurieren, damit die Zugriffssteuerungslisten (ACLs) für die Tabellen keine vertraulichen Informationen offenlegen.

Die *glide.service_portal.widget.allow_list*Eigenschaft identifiziert die Widgets, die auf eine beliebige Tabelle in der Instanz zugreifen können. Die Zugriffssteuerungslisten (ACLs) für diese Tabellen gelten jedoch weiterhin. Wenn die ACLs falsch konfiguriert sind oder nicht vorhanden sind, ermöglichen Widgets in dieser Liste möglicherweise den Zugriff auf diese Tabellen, wodurch möglicherweise vertrauliche Informationen offengelegt werden. Diese Eigenschaft ist nur wirksam, wenn das Widget SNCACLWidgetUtil und verwendet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

*glide.service_portal.widget.enforce_public_check*Eigenschaft ist aktiviert (auf „wahr“ festgelegt).

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.service_portal.widget.allow_list*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	array
Empfohlener Wert	Leer
Standardwert	Leer: In einigen Fällen des Kunden können einige Werte vorhanden sein.
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht mit den empfohlenen Werten konfiguriert wird, können Widgets auf eine beliebige Tabelle in der Instanz zugreifen.
Abhängigkeiten und Voraussetzungen	Für *glide.service_portal.widget.allow_list*Einstellung, die anwendbar sein soll, die *glide.service_portal.widget.enforce_public_check*Eigenschaft muss auf „wahr“ festgelegt werden.
Funktionale Auswirkung	Mit dieser Eigenschaft können Kunden auf Tabelleninformationen zugreifen, wenn das Widget auf öffentlich festgelegt und im Wert der Eigenschaft enthalten ist.

Allow-Liste für Tabelle „Serviceportal-Widgets konfigurieren“ [Neu in Security Center 2,0]

Erfahren Sie, wie *glide.service_portal.widget.table_allow_list*Eigenschaft erhöht die Sicherheit, indem Tabellen aufgelistet werden, die nicht authentifizierten Anwendern über Serviceportal-Widgets zugänglich sind, abhängig von zusätzlichen Prüfungen und spezifischen Glide-Eigenschaftseinstellungen.

Die *glide.service_portal.widget.table_allow_list*Die Eigenschaft enthält eine Liste von Tabellen, auf die nicht authentifizierte Anwender über Serviceportal-Widgets zugreifen können, die die zusätzlichen Sicherheitsprüfungen im SNCACLWidgetUtil-Skript verwenden. Diese Eigenschaft wird nur erzwungen, wenn die Glide-Eigenschaft vorhanden ist *glide.service_portal.widget.enforce_public_check*Ist auf „wahr“ festgelegt. Das Einbeziehen unnötiger Tabellen in diese Eigenschaft kann zur Offenlegung vertraulicher Informationen führen. Dennoch werden Tabellen-ACLs wie zuvor weiter ausgewertet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.service_portal.widget.table_allow_list*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den sicheren Wert festgelegt ist, können unnötige Tabellen eingeschlossen werden, was potenziell zur Offenlegung vertraulicher Informationen führen kann.
Abhängigkeiten und Voraussetzungen	Die *glide.service_portal.widget.enforce_public_check* Eigenschaft muss für auf „wahr“ festgelegt werden *glide.service_portal.widget.table_allow_list* Einstellung, die wirksam wird.
Funktionale Auswirkung	Die Tabellenliste steuert den Zugriff auf die Tabellen, aus denen das Widget Daten abrufen darf.

Internen Zugriff auf explizite externe Rollen verweigern [aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie Systemeigenschaften, um zu bestimmen, ob externen Anwendern die Rolle „snc_internal“ zugewiesen werden kann.

Verwenden Sie *glide.security.explicit_roles.enable_internal_user_blacklist* Systemeigenschaft, um zu verhindern, dass externen Anwendern zugewiesen wird *snc_internal* Rolle. Wenn diese Eigenschaft auf festgelegt ist **Wahr** , Erzwingt die Parameter des wartungsgeschützten *glide.security.explicit_roles.internal_user_blacklist* Eigenschaft. Diese Eigenschaft weist den zu *snc_external* Rolle zu einer Liste nicht vertrauenswürdiger Anwenderklassen. Wenn *glide.security.explicit_roles.enable_internal_user_blacklist* Ist auf festgelegt **Falsch** , *glide.security.explicit_roles.internal_user_blacklist* Eigenschaft wird ignoriert.

Hinweis: Instanzen ohne installierte explizite Rollen sind nicht betroffen. Ab dem Paris-Release erhalten neue Installationen von expliziten Rollen die Eigenschaft mit dem Standardwert „wahr“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.explicit_roles.enable_internal_user_blacklist`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Fallback-Wert	falsch
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 5,4 • CVSS-Punktzahl: Mittel • Eine falsche Konfiguration dieser Eigenschaft erhöht das Risiko, dass ein externer Anwenderaccount Zugriff auf interne Informationen erhält.
Abhängigkeiten und Voraussetzungen	Keine

Nicht autorisierten Zugriff auf Anforderungselemente verweigern [aktualisiert im Sicherheitscenter 1,3]

Die `glide.sc.req_for.roles.default`Die Eigenschaft definiert ein Standardverhalten für `Abrufen der Adresse` API.

Diese Eigenschaft funktioniert nur, wenn `glide.sc.req_for.roles`Hat keine Werte. Wenn `glide.sc.req_for.roles`Hat Werte, dann hat diese Eigenschaft keine Bedeutung, und Anwender mit nur definierten Rollen erhalten Zugriff auf die API.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sc.req_for.roles.default`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Wenn in der Eigenschaft keine Rollen angegeben sind, wird die vom Client aufrufbare Skripteinbindung verwendet `SkriptServiceCatalogGetLocation` Kann von jedem nicht privilegierten angemeldeten Anwender aufgerufen werden und kann die Adresse anderer Anwender im System abrufen. Diese Eigenschaft schützt diese API, damit sie nicht privilegierten Anwendern zugänglich gemacht wird.
Empfohlener Wert	verweigern
Standardwert	verweigern
Konfigurationstyp	Auswahlliste (Allow | Deny)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsrisiko	(Mittel) Wenn `glide.sc.req_for.roles.default` Ist nicht auf den empfohlenen Wert von festgelegt **Ablehnen** (Zulassen) und der Wert von `glide.sc.req_for.roles` Ist leer, kann jeder Anwender Elemente für andere Anwender anfordern, die nicht autorisierten Zugriff auf Ressourcen zulassen.
Referenzen	Vom Client aufrufbare Skripteinbindungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Empfehlungen für UI-Seiten mit hohem Risiko anzeigen

Verringern Sie die Wahrscheinlichkeit von Autorisierungsfehlern und unbeabsichtigter Offenlegung von Informationen, indem Sie Empfehlungen für UI-Seiten mit hohem Risiko anzeigen.

Verwenden Sie **glide.script.ui_page.customer_scoped.security_msgs_enabled** Systemeigenschaft, um zu bestimmen, ob Anwender, die UI-Seiten konfigurieren, Sicherheitsempfehlungen angezeigt werden sollen, wenn:

- Eine ACL fehlt
- GlideRecord/GlideDBQuery-APIs werden anstelle von GlideRecordSecure verwendet
- Die Seite ist in der Tabelle „sys_public“ als öffentlich konfiguriert

Wenn die Eigenschaft aktiviert ist, Empfehlungen, wenn die obigen Bedingungen erfüllt sind, verringern die Wahrscheinlichkeit von Autorisierungsfehlern und helfen, die unbeabsichtigte Offenlegung von Informationen zu verhindern.

Legen Sie die Systemeigenschaft fest **glide.script.ui_page.customer_scoped.security_msgs_enabled** Bis **Wahr** Um diese Empfehlungen anzuzeigen.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	glide.script.ui_page.customer_scoped.security_msgs_enabled
Plugin-Anwendbarkeit	Keine
Sicherheitsrisiko	Diese Systemeigenschaft wird auf festgelegt **Falsch** Erhöhen Sie die Wahrscheinlichkeit von Autorisierungsfehlern und unbeabsichtigter Offenlegung von Informationen.
CVSS-Punktzahl (Common Vulnerability Scoring System)	5.3
Bewertung des Common Vulnerability Scoring System (CVSS)	Mittel
Funktionale Auswirkung	Zeigt Sicherheitsempfehlungen für Anwender an, die UI-Seiten konfigurieren.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Boolean

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Basissystemwert	wahr
Fallback-Wert	wahr
Empfohlener Wert	wahr

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Deaktivieren Sie eingehende E-Mails für gesperrte Anwender

Verwenden Sie `glide.pop3.process_locked_out`Eigenschaft zur Steuerung eingehender E-Mail-Aktionen für gesperrte aktive Anwender.

Legen Sie diese Eigenschaft auf fest **Falsch** Zum Deaktivieren eingehender E-Mails für gesperrte Anwender.

Hinweis: Berücksichtigen Sie die Sicherheitsauswirkungen, die sich daraus ergeben, dass Anwender aus nicht vertrauenswürdigen Domänen zugelassen werden, und warum sie gesperrt wurden, bevor E-Mails von ihnen eingehende E-Mail-Aktionen auslösen können.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.pop3.process_locked_out`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Diese Eigenschaft steuert eingehende E-Mail-Aktionen für gesperrte Anwender.
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Sicherheitsrisiko	(Hoch) wenn Sie diese Eigenschaft auf festlegen **Wahr** , Es kann eine Offenlegung von Informationen geben, da eingehende E-Mails von Anwendern mit gesperrten Accounts empfangen würden.
Sicherheitsrisikobewertung	7,5

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Eingehende Transaktionen doppelt prüfen [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.security.strict.updates`Eigenschaft zum Aktivieren der doppelten Sicherheitsüberprüfung für eingehende Transaktionen während der Formularübermittlung. Wenn Sie diese Eigenschaft auf festlegen **Wahr** , Fügt eine zusätzliche Ebene der Tabellenvalidierung hinzu, bevor ein Formular im Browser gerendert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie die Eigenschaft sicher `glide.security.strict.updates`Ist in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.security.strict.updates`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um eine zusätzliche Ebene der Verifizierung von Anwenderberechtigungen sicherzustellen, bevor das Formular im Browser angezeigt wird.
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	Diese Korrektur fügt eine zusätzliche Validierungsebene hinzu, um auf Anwenderberechtigungen für die Zieltabelle/-Seite in der Instanz zu überprüfen. Solange die Zugriffssteuerungen in der Kundeninstanz entsprechend festgelegt sind, sollte dies keine Auswirkungen haben.
Sicherheitsrisiko	(Hoch) Sie sollten die Zugriffsanforderung immer überprüfen, wenn Transaktionen zwischen zwei Zonen stattfinden. Dieser Vorgang überprüft auf Berechtigungen, wenn das Formular angefordert wird und bevor das Formular-Rendering erfolgt.
Referenzen	

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

ACLs für bereichsbezogene Administratoranwendungen aktivieren [aktualisiert in Security Center 1,3]

Die `glide.security.scoped_administration.honor_global_acl`Bestimmt, ob eine Anwendungsverwaltungs-App Regeln für globale Zugriffssteuerungslisten (ACL) erben kann.

Diese Eigenschaft ist besonders nützlich, wenn für den Datensatzumfang keine bereichsbezogenen ACLs für Administratoranwendungen definiert sind.

Festlegen `glide.security.scoped_administration.honor_global_acl`Auf „wahr“, um zu verhindern, dass ein Anwender mit niedrigen Berechtigungen für die Anwendung potenziell auf vertrauliche Datensätze zugreifen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.scoped_administration.honor_global_acl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Steuert die ACL-Zugriffsregel in der bereichsbezogenen Administratoranwendung.
Empfohlener Wert	True
Standardwert	True
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) wenn der Eigenschaftswert „wahr“ ist und keine bereichsbezogenen ACLs für Administratoranwendungen für den Datensatzbereich definiert sind, werden die globalen ACLs berücksichtigt. Wenn dieser Wert auf „falsch“ festgelegt ist, werden ACL-Prüfungen ignoriert, wenn für den Datensatzbereich keine bereichsbezogenen ACLs für Administratoranwendungen definiert sind.
Sicherheitsrisikobewertung	3,8
Referenzen	Zugriffskontrollregeln in Anwendungsverwaltungs-Apps

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Plugins aktivieren

Abfrageregeln für Arbeitsauftragsmanagement für Serviceorganisationen aktivieren [Neu in Security Center 1,5 und aktualisiert 2,0]

Verwenden Sie `sn_fsm.use_query_rules`Eigenschaft zum Anwenden von Regeln und Filtern auf die Außendienst-Management-Tabellen.

Bei „wahr“ werden Regeln/Filter aus der Tabelle „sn_query_rule“ verwendet, um den Lesezugriff auf Tabellen im Zusammenhang mit dem Außendienst-Management (Arbeitsauftrag und Arbeitsauftragsaufgabe) für den angemeldeten Anwender durch Abfragegeschäftsregeln und Lese-ACLs zu bestimmen. Bei „falsch“ werden die Datensätze nicht basierend auf Abfrageregeln gefiltert. AbfrageBusiness-Regeln fügen zusätzliche Sicherheitsvalidierungen hinzu. Insbesondere filtert diese Eigenschaft Datensätze für Service Desk-Mitarbeiter, Qualifizierer und Dispatcher basierend auf ihrem zugewiesenen Gebiet oder ihrer Gebietsmitgliedschaft. Es empfiehlt sich, beim Lesen von Datensätzen das Prinzip der geringsten Berechtigung zu befolgen. Wenn diese Eigenschaft nicht auf „wahr“ festgelegt ist, kann das Risiko der Datengefährdung durch Außendienst-Management-Tabellen erhöht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`sn_fsm.use_query_rules`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden Regeln und Filter aus „sn_query_rule“ verwendet, um den Lesezugriff auf Außendienst-Management-Tabellen zu bestimmen, die das Prinzip der geringsten Berechtigung implementieren. Bei „falsch“ werden die Datensätze nicht basierend auf Abfragegeschäftsregeln gefiltert und können ein erhöhtes Risiko der Datengefährdung durch Außendienst-Management-Tabellen aufweisen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Bei „wahr“ werden Regeln/Filter aus der Tabelle „sn_query_rule“ verwendet, um den Lesezugriff auf zugehörige Tabellen für das Außendienst-Management zu bestimmen. Zum Beispiel Arbeitsauftrag (WO) und Arbeitsauftragstabelle (WOT) für den angemeldeten Anwender durch Abfrage von Business-Regeln und LESEN VON ACLs. Bei „falsch“ werden die Datensätze nicht basierend auf Abfrageregeln gefiltert. Durch Aktivieren dieser Eigenschaft werden die Daten gesichert, und alle Daten (wm_Task und wm_order) sind für ihre Anwender nicht sichtbar.
Referenzen	Außendienst-Management – Referenz

ACLs zur Steuerung von Live-Profildetails aktivieren [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.live_profile.details`Eigenschaft, die angibt, ob ein Anwender alle Detailfelder, z. B. Unternehmensname und Telefonnummern, in einem Live-Profil anzeigen kann.

Abhängig von der Einstellung von `glide.live_profile.details`Eigenschaft, tritt Folgendes auf:

- Wenn der Wert auf Anzeigen festgelegt ist, wird unabhängig von den für das Anwenderprofil erstellten ACLs Zugriff auf die Live-Profilinformationen gewährt.
- Wenn der Wert auf ACL festgelegt ist, wird der Zugriff auf die Live-Profilinformationen gemäß den für das Anwenderprofil erstellten ACLs eingeschränkt.
- Wenn der Wert auf Ausblenden festgelegt ist, wird der Zugriff auf die Live-Profilinformationen unabhängig von den für das Anwenderprofil erstellten ACLs eingeschränkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.live_profile.details`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Der Zweck besteht darin, nur autorisierten Anwendern den Zugriff auf die Details eines Live-Profils zu ermöglichen (z. B. Unternehmensname, Telefonnummern)
Datentyp	Auswahlliste
Empfohlener Wert	ACL
Standardwert	ACL
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	Wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Anwender auf die Live-Profildetails aller anderen Anwender zugreifen.
Sicherheitsrisiko	(Mittel) API-Anforderungen sollten Tabellen-ACLs immer berücksichtigen. Eine Einschränkung muss angewendet werden, um zu verhindern, dass nicht autorisierte Anwender auf Details eines Live-Profils zugreifen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

ACLs für codierte Abfrage im Widget „einfache Liste“ aktivieren [Neu im Sicherheitscenter 2,0]

Erfahren Sie, wie Sie festlegen `glide.service_portal.enable_acls_for_encoded_query_in_list`Eigenschaft für den sicheren Wert, um zu verhindern, dass Anwender ACL-Auswertungen (Access Control List) für eine Abfragebedingung im Widget „einfache Liste“ umgehen.

Wenn `glide.service_portal.enable_acls_for_encoded_query_in_list`Eigenschaft ist nicht auf den sicheren Wert „wahr“ festgelegt. Ein Anwender kann möglicherweise die Auswertungen der Zugriffssteuerungsliste (ACL) für eine Abfragebedingung im Widget „einfache Liste“ umgehen. Wenn die Eigenschaft auf „falsch“ festgelegt ist, wird das vorherige Verhalten wiederhergestellt, wodurch ACL-Prüfungen für eine codierte Abfrage basierend auf dem Wert des Kontrollkästchens „enforce_acl“ erzwungen werden.

Es ist eine Best Practice, ACLs in Abfragen auszuwerten, um sicherzustellen, dass ein Anwender Zugriff auf die abgefragten Felder hat, wodurch ein nicht autorisierter Datenverlust verhindert wird.

Stellen Sie sicher, dass die Glide-Eigenschaft vorhanden ist `glide.service_portal.enable_acls_for_encoded_query_in_list`Ist auf „wahr“ festgelegt. Wenn die Eigenschaft in der Tabelle „sys_properties“ nicht vorhanden ist, ist der Standardwert „wahr“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.script.fencing.cross_scope_access.shared_table_`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Diese Eigenschaft wird nicht auf den empfohlenen Wert „wahr“ festgelegt.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Das Widget „einfache Liste“ zeigt je nach Rolle des Anwenders und den zugrunde liegenden ACLs möglicherweise keine Daten an. Darüber hinaus können Anwender Sicherheitswarnungen erhalten, wenn die Abfrage „einfache Liste“ Filterbedingungen mit Eigenschaften enthält, auf die der aktuelle Anwender nicht zugreifen kann.

URL-Zulässigkeitsliste für ursprungsübergreifende iFrame-Kommunikation aktivieren

Verwenden Sie `glide.ui.concourse.onmessage_enforce_same_origin`Eigenschaft zum Aktivieren der ursprungsübergreifenden Kommunikation zwischen IFrames .

Openframe Es können nur Nachrichten aus vertrauenswürdigen Domänen verarbeitet werden, die in angegeben sind `glide.ui.concourse.onmessage_enforce_same_origin_whitelist`Eigenschaft. Weitere Informationen finden Sie unter URL-Zulässigkeitsliste für ursprungsübergreifende iFrame-Kommunikation aktivieren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.concourse.onmessage_enforce_same_origin`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Kategorie	Zugriffssteuerung
Zweck	Ermöglicht die Auflistung vertrauenswürdiger Domänen, damit sie zwischen iframes für Openframe kommunizieren können.
Empfohlener Wert	wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	wahr
Sicherheitsrisikobewertung	4.2
Funktionale Auswirkung	Wenn Sie beabsichtigte Domänen nicht auflisten, die Möglichkeit, andere Seiten in einzubetten ServiceNow AI Platform Instanzen sind möglicherweise eingeschränkt.
Sicherheitsrisiko	(Hoch) wenn eine Webseite Ereignis-Handler enthält, die keine ordnungsgemäße Ursprungsvalidierung durchführen, kann eine Webseite oder ein Skript aus einem beliebigen Ursprung mit ihr kommunizieren. Es kann auch beliebige Funktionen initiieren, die vom Ereignis-Handler ausgeführt werden.
Referenzen	OpenFrame-Übersicht

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Anti-CSRF-Token aktivieren [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0]

Verwenden Sie *glide.security.use_csrf_token*Eigenschaft, die die Verwendung eines sicheren Tokens zur Identifizierung und Validierung eingehender Anforderungen sicherstellt, die wiederum zur Verhinderung dieser Angriffe verwendet werden.

Cross-Site Request Forgery (CSRF) ist ein Angriff, der authentifizierte Anwender zwingt, eine Anforderung an eine Webanwendung zu übermitteln, für die sie derzeit authentifiziert sind. CSRF-Angriffe nutzen das Vertrauen einer Webanwendung in einen authentifizierten Anwender aus.diese Eigenschaft ermöglicht die Verwendung eines sicheren Tokens zur Identifizierung und Validierung eingehender Anforderungen. Dieses Token wird verwendet, um Site-übergreifende Angriffe auf Anforderungsfälschung zu verhindern. Wenn *glide.security.use_csrf_token* Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, ist CSRF möglich.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.use_csrf_token*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Zum Schutz der Anwendung vor potenziellen CSRF-Angriffen.
Sicherheitsrisikobewertung	8.1
Empfohlener Wert	wahr
Standardwert	wahr
Funktionale Auswirkung	Diese Korrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzanwender eine Schreibanforderung an die Instanz sendet. Jede Schreibanforderung enthält ein CSRF-Token (d. h. eine Validierungs-/CSRF-ID, die an die Anwendersitzung gebunden ist). Wenn die Anwendersitzung abläuft, läuft das sichere Token damit ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsrisiko	(Hoch) Cross Site Request Forgery ist ein erhebliches Sicherheitsrisiko, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff starten, indem er das Vertrauen eines Instanzanwenders missbraucht. Mit Hilfe von Social Engineering-Angriffen kann ein Anwender im Namen des Angreifers eine fehlerhafte Anforderung in der Instanz übermitteln.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Plugin für kontextbezogene Sicherheit aktivieren [aktualisiert in Security Center 1,3]

Aktivieren Sie das Plugin für kontextbezogene Sicherheit (`com.glide.role_management`) Plugin zum Aktivieren der kontextbezogenen Sicherheit, das einen Datensatz/Informationen mithilfe der Funktionen „Erstellen“, „Lesen“, „Schreiben“ und „Löschen“ sichert.

Nach der Installation und Aktivierung werden die Wörterbuchrollen (erstellt von einem einfachen Sicherheitsmanager) nicht mehr getestet. Stattdessen wird ServiceNow AI Platform Sucht nach ACL-Regeln für Felder und Tabellen. Sie sichert die Daten mithilfe von ACL-Regeln anstelle von traditionellen, rollenbasierten Wörterbuchregeln, die von einem einfachen Sicherheitsmanager implementiert werden. Auch wenn Sie das Wörterbuchformular konfigurieren und einem Wörterbucheintrag Rollen hinzufügen, werden die Rechte nicht geändert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	`com.glide.role_management`
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Im Gegensatz zum einfachen Sicherheitsmanager kennt der kontextbezogene Sicherheitsmanager die Systemtabellenhierarchie. Sie können potenziell verschiedene Sicherheitsregeln für ein Feld haben, je nachdem, wo es in der Hierarchie angezeigt wird.
Empfohlener Wert	Aktiv
Standardwert	Es ist kein Standardwert vorhanden, da dies ein Plugin und keine Glide-Eigenschaft ist.
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	Diese Fehlerkorrektur erzwingt die funktionale Ebene der Zugriffssteuerungen, wodurch die Anwendung die Zugriffsbeschränkungen nur basierend auf der ACL-Tabelle bestimmen kann.
Sicherheitsrisiko	(Hoch) Zugriffssteuerungen auf Funktionsebene müssen vor der Ausführung von CRUD-Vorgängen serverseitig erzwungen werden, um Instanzanwendern die entsprechende Zugriffsstufe zu gewährleisten.
Referenzen	Kontextbezogener Sicherheitsmanager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bereichsübergreifende Berechtigungsprüfungen im Serviceportal-Formular aktivieren [Neu in Security Center 7,0]

Verwenden Sie eine Systemeigenschaft, um bereichsübergreifende Berechtigungsprüfungen im Serviceportal-Formular-Widget zu erzwingen und das nicht autorisierte Abrufen von Formularen und Tabellendaten zwischen Bereichen zu verhindern.

In Yokohama Und spätere Releases erzwingen Abfragen bereichsübergreifende Berechtigungsprüfungen für die Tabelle, bevor die angegebenen sys_ID-Informationen gelesen werden.

Wenn `glide.service_portal.enforce_cross_scope_check_in_form`Eigenschaft ist auf den empfohlenen Wert von festgelegt **Wahr** , Bereichsübergreifende Berechtigungsprüfungen werden für die Tabelle erzwungen. Wenn auf festgelegt **Falsch** , Die bereichsübergreifende Berechtigungsprüfung wird nicht erzwungen.

Legen Sie fest `glide.service_portal.enforce_cross_scope_check_in_form`Systemeigenschaft zu **Wahr** Oder bestätigen Sie, dass die Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden ist. Wenn in der Tabelle „sys_properties“ kein Datensatz vorhanden ist, wird der Wert standardmäßig auf festgelegt **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.service_portal.enforce_cross_scope_check_in_form`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Ein Mangel an bereichsübergreifenden Berechtigungsprüfungen kann zu nicht autorisiertem Abrufen von Formularen und Tabellendaten zwischen Bereichen führen.
Abhängigkeiten und Voraussetzungen	Keine

ACL für HR-Lebenszyklusereignisdaten erzwingen [Neu in Security Center 2,0]

Erfahren Sie, wie Sie nicht autorisierten Zugriff auf Daten in der Anwendung Human Resources Lifecycle Events verhindern können, indem Sie überprüfen, ob dies der Fall ist `glide.enforce_security_scope.sn_hr_le property`Ist auf den gesicherten Wert festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die *glide.enforce_security_scope.sn_hr_le*Die Eigenschaft beschränkt die Zugriffssteuerungslisten (ACLs) mehrerer HR-Tabellen, sodass nur der Bereich „sn_HR_le“ berücksichtigt wird. Wenn *glide.enforce_security_scope.sn_hr_le*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, werden die Daten aus der Anwendung Human Resources: Lebenszyklusereignisse ACLs aus allen anderen Bereichen ausgesetzt, was dazu führen kann, dass nicht autorisierte Anwender auf vertrauliche Daten zugreifen. Zum Beispiel ein IT-Administrator, der Zugriff auf HR-Daten erhält.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enforce_security_scope.sn_hr_le*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den Wert „wahr“ festgelegt wird, können die Anwendungsdaten „Human Resources: Lebenszyklusereignisse“ für ACLs aus allen anderen Bereichen zugänglich gemacht werden. Dies kann dazu führen, dass nicht autorisierte Anwender auf vertrauliche Daten zugreifen.
Abhängigkeiten und Voraussetzungen	Keine

ACL für HR-Kerndaten erzwingen [Neu in Security Center 2,0]

Erfahren Sie, wie Sie konfigurieren *glide.enforce_security_scope.sn_hr_core*Eigenschaft, damit das Plugin „bereichsbezogene Human Resources-App: Core“ (com.sn_HR_Core) keine sensiblen Daten für Zugriffssteuerungslisten (ACLs) aus allen anderen Bereichen bereitstellt.

Die *glide.enforce_security_scope.sn_hr_core*Die Eigenschaft schränkt die Zugriffssteuerungslisten (ACLs) mehrerer globaler Datentabellen wie sys_attachment und sys_email so ein, dass nur der sn_HR_Core-Bereich berücksichtigt wird. Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt ist, werden Daten aus dem bereichsbezogenen Human Resources-App: Core-Plugin für ACLs aus allen anderen Bereichen verfügbar gemacht. Dies könnte beispielsweise dazu führen, dass der IT-Administrator Zugriff auf Human Resources-Daten erhält.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.enforce_security_scope.sn_hr_core`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den sicheren Wert „wahr“ festgelegt ist, werden Daten aus dem bereichsbezogenen Human Resources-App: Core-Plugin für ACLs aus allen anderen Bereichen zugänglich gemacht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Case and Knowledge Management aktivieren

ACL für HR Virtual Agent-Daten erzwingen [Neu in Security Center 2,0]

Erfahren Sie, wie Sie festlegen `glide.enforce_security_scope.sn_hr_va`Eigenschaft auf einen sicheren Wert, die Datenverluste aus der bereichsbezogenen Anwendung „Virtual Agent-Konversationen“ verhindert.

Die `glide.enforce_security_scope.sn_hr_va`Die Eigenschaft schränkt die Zugriffssteuerungslisten (ACLs) mehrerer Human Resources-Tabellen (HR) so ein, dass nur der sn_HR_va-Bereich berücksichtigt wird. Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt ist, werden Daten aus der bereichsbezogenen Anwendung Human Resources: Virtual Agent-Konversationen ACLs aus allen anderen Bereichen zugänglich gemacht. Dies könnte beispielsweise dem IT-Administrator ermöglichen, auf HR-Daten zuzugreifen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.enforce_security_scope.sn_hr_va`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den sicheren Wert „wahr“ festgelegt wird, könnten Daten aus der bereichsbezogenen Anwendung „Human Resources: Virtual Agent Conversations“ für ACLs aus allen anderen Bereichen verfügbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine

Erzwingen Sie anwendungsspezifische ACLs nur für Anwendungsdaten

Vermeiden Sie nicht autorisierten oder unerwünschten Zugriff auf Anwendungsdaten, indem Sie anwendungsspezifische Zugriffssteuerungslisten (ACLs) nur für Anwendungsdaten erzwingen.

Steuern Sie das Verhalten von Anwendungsdaten, die sich in primären Tabellen außerhalb der Anwendung befinden. Wenn diese Eigenschaften einen Wert von haben **Wahr** , Nur die anwendungsspezifischen ACLs werden für den Zugriff auf die Anwendungsdaten in diesen Tabellen ausgewertet. Nicht alle Anwendungen sind so konzipiert, dass sie in dieser Konfiguration funktionieren oder einen Systemeigenschaftsdatensatz [sys_properties] zu diesem Zweck verwenden.

Diese Systemeigenschaften verwenden **Glide.enforce_Security_scope.<scope>** Benennungsformat. Verwenden Sie beispielsweise **Glide.enforce_Security_scope.sn_HR_sp** Eigenschaft für den Bereich „Mitarbeiter-Center Core“ (sn_HR_sp). Die folgenden Anwendungsbereiche enthalten diese Eigenschaft:

- sn_doc
- sn_egd_act
- sn_egd_core
- sn_egd_Goals
- sn_em
- sn_GSM
- sn_GSM_info_req
- sn_GSM_lic_prmt
- sn_GSM_lic_prmt_ex
- sn_GSM_soc_bnfts
- sn_hc_Professional
- sn_HR_Agent_WS
- sn_HR_KI_Agents
- sn_HR_Awa
- sn_HR_Core
- sn_HR_ef
- sn_HR_er
- sn_HR_gen_ai
- sn_HR_hc
- sn_HR_le
- sn_HR_le_ent
- sn_HR_mii_Base
- sn_HR_na_galileo
- sn_HR_Pad
- sn_HR_pj
- sn_HR_sp
- sn_HR_va
- sn_HR_WS
- sn_imt_Health_Test
- sn_imt_tracing
- sn_imt_vaccine
- sn_ja
- sn_jny
- sn_lg_Contracts
- sn_lg_matter
- sn_lg_OPS
- sn_Opp_Market
- sn_Professional
- sn_svc_appl_info
- sn_svc_appl_pgm_mg
- sn_Talent_aia
- sn_Uni_req
- sn_Uni_Task

Für jede mit installierte Anwendung `glide.enforce_security_scope`Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] (z. B.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glide.enforce_security_scope.sn_hr_core), stellen Sie sicher, dass der Eigenschaftswert auf festgelegt ist **Wahr** .

Hinweis: Diese Eigenschaften können nur vom bereichsbezogenen Administrator für die spezifische Anwendung geändert werden. Wenn für die angegebene Anwendung und die jeweilige Eigenschaft kein sys_properties-Datensatz vorhanden ist, muss er erstellt werden.

Verwenden Sie dieses Skript, um zu finden, welche Eigenschaften für die Instanz aktualisiert oder erstellt werden müssen:

```
var properties = [
    'glide.enforce_security_scope.sn_uni_task',
    'glide.enforce_security_scope.sn_uni_req',
    'glide.enforce_security_scope.sn_svc_appl_info',
    'glide.enforce_security_scope.sn_professional',
    'glide.enforce_security_scope.sn_opp_market',
    'glide.enforce_security_scope.sn_lg_ops',
    'glide.enforce_security_scope.sn_lg_matter',
    'glide.enforce_security_scope.sn_lg_contracts',
    'glide.enforce_security_scope.sn_jny',
    'glide.enforce_security_scope.sn_ja',
    'glide.enforce_security_scope.sn_imt_vaccine',
    'glide.enforce_security_scope.sn_imt_tracing',
    'glide.enforce_security_scope.sn_imt_health_test',
    'glide.enforce_security_scope.sn_hr_ws',
    'glide.enforce_security_scope.sn_hr_va',
    'glide.enforce_security_scope.sn_hr_sp',
    'glide.enforce_security_scope.sn_hr_pj',
    'glide.enforce_security_scope.sn_hr_pad',
    'glide.enforce_security_scope.sn_hr_mii_base',
    'glide.enforce_security_scope.sn_hr_le',
    'glide.enforce_security_scope.sn_hr_le_ent',
    'glide.enforce_security_scope.sn_hr_hc',
    'glide.enforce_security_scope.sn_hr_gen_ai',
    'glide.enforce_security_scope.sn_hr_er',
    'glide.enforce_security_scope.sn_hr_ef',
    'glide.enforce_security_scope.sn_hr_core',
    'glide.enforce_security_scope.sn_hr_awa',
    'glide.enforce_security_scope.sn_hr_agent_ws',
    'glide.enforce_security_scope.sn_hc_professional',
    'glide.enforce_security_scope.sn_gsm_soc_bnfts',
    'glide.enforce_security_scope.sn_gsm_lic_prmt_ex',
    'glide.enforce_security_scope.sn_gsm_lic_prmt',
    'glide.enforce_security_scope.sn_gsm_info_req',
    'glide.enforce_security_scope.sn_gsm',
    'glide.enforce_security_scope.sn_em',
    'glide.enforce_security_scope.sn_egd_goals',
    'glide.enforce_security_scope.sn_egd_core',
    'glide.enforce_security_scope.sn_egd_act',
    'glide.enforce_security_scope.sn_doc',
    'glide.enforce_security_scope.sn_talent_aia',
    'glide.enforce_security_scope.sn_hr_na_galileo',
    'glide.enforce_security_scope.sn_svc_appl_pgm_mg',
    'glide.enforce_security_scope.sn_hr_ai_agents',
    'glide.enforce_security_scope.sn_hr_mii_base'
  ];
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var pm = new GlidePluginManager();

for (var i = 0; i < properties.length; i++) {
   var property = properties[i];
   var application = property.split('.')[2];
   var propertyValue = gs.getProperty(property, 'false');

   if (pm.isActive(application) && propertyValue.toLowerCase() != 'true') {
      gs.print(property);
   }
}
```

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enforce_security_scope.<scope>*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,1 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaften keinen Wert von haben **Wahr** , Die ACLs in der primären Tabelle werden weiterhin hinsichtlich des Zugriffs ausgewertet, was möglicherweise nicht autorisierten oder unerwünschten Zugriff auf Anwendungsdaten ermöglicht.
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Einschränkungen des Anwendungsbereichs erzwingen [Neu in Security Center 1,3 und entfernt in 1,5]

Verwenden Sie *glide.record.legacy_cross_scope_access_policy_in_script*Eigenschaft zur Steuerung der Berechtigungen bereichsbezogener Apps.

Wenn *glide.record.legacy_cross_scope_access_policy_in_script*Eigenschaft ist auf „wahr“ festgelegt. Bereichsbezogene Apps können APIs aufrufen, die nur für globale Apps verfügbar sein sollten. Diese Eigenschaft umgeht die beabsichtigten Zugriffssteuerungen zum Erstellen und Aktualisieren von Entwicklern für diese bereichsbezogenen Apps.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.record.legacy_cross_scope_access_policy_in_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	false
Standardwert	„Wahr“ (wenn die Eigenschaft in der Tabelle „sys_properties“ nicht vorhanden ist.)
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt ist, können bereichsbezogene Apps und delegierte Entwickler für diese bereichsbezogenen Apps Datensätze in globalen Tabellen wie Incident erstellen und aktualisieren.
Abhängigkeiten und Voraussetzungen	Keine

Leserollen für Katalogvariablensuche erzwingen [Neu in Security Center 7,0]

Verwenden Sie Systemeigenschaften, um sicherzustellen, dass nur Katalogvariablen mit einer leeren Leserolle für die Suche indiziert werden.

Wenn die Eigenschaft `glide.ais.ingestion.ignore_catalog_variables_read_roles`lst auf den empfohlenen Wert von festgelegt **Falsch** , Nur Katalogvariablen mit einer leeren Leserolle werden für die Suche indiziert. Wenn diese Eigenschaft auf festgelegt ist **Wahr** Dann werden alle Variablen für die Suche indiziert, unabhängig von den für die Variable angegebenen Leserollen.

Überprüfen Sie, ob `glide.ais.ingestion.ignore_catalog_variables_read_roles`Systemeigenschaft ist in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden oder ist vorhanden und ist auf festgelegt **Falsch** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ais.ingestion.ignore_catalog_variables_read_roles`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Zugriffssteuerung
Funktionale Auswirkung	Diese Eigenschaft wirkt sich auf die Indizierung von durchsuchbaren Inhalten aus Katalogvariablen aus, die bestimmte Rollen für den Lesezugriff erfordern.
Sicherheitsrisiko	• Schweregradpunktzahl: 2,6 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Anwender können nach Variablen suchen, auf die sie keine Leserollen für den Zugriff haben, auf die sie die Offenlegung von Informationen verursachen.
Abhängigkeiten	Keine
Referenzen	Servicekatalogvariablen

Sicherheitsregeln für die Freigabe von Dashboards erzwingen [Neu in Security Center 1,3]

Verwenden Sie *glide.cms.dashboards.sharing_with_secure_search*Eigenschaft, um zu steuern, ob Anwender Dashboards freigeben können.

Wenn *glide.cms.dashboards.sharing_with_secure_search*Eigenschaft ist nicht auf festgelegt **Wahr** , Anwender können Dashboard-Gruppen und -Rollen freigeben, auf die sie keinen Zugriff haben. Durch Aktivieren dieser Eigenschaft werden Zugriffssteuerungslisten (ACLs) beim Durchsuchen der Tabellen „sys_user“, „sys_user_role“ und „sys_user_Group“ während des Dashboardfreigabeprozesses erzwungen. Die übermäßige Freigabe eines Dashboards kann dazu führen, dass Anwender, Gruppen oder Rollen auf Daten zugreifen, für die sie keine Berechtigung zum Anzeigen haben sollten, wodurch vertrauliche Informationen möglicherweise gefährdet werden. Daher wird empfohlen, festzulegen *glide.cms.dashboards.sharing_with_secure_search*Auf „wahr“, damit Dashboards nur für diejenigen freigegeben werden, die über die entsprechenden Berechtigungen verfügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.cms.dashboards.sharing_with_secure_search*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	festgelegt wird, werden Zugriffssteuerungslisten beim Durchsuchen der Tabellen „sys_user“, „sys_user_role“ und „sys_user_Group“ nicht erzwungen. Dies kann dazu führen, dass Dashboards für nicht autorisierte Anwender freigegeben werden und vertrauliche Informationen offenlegen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Zugriffssteuerung
Funktionale Auswirkung	Diese Eigenschaft wendet Sicherheitsregeln auf die Liste der Anwender, Anwendergruppen und Rollen an, die beim Freigeben von Dashboards sichtbar sind.

Umfangssicherheit für digitale Services des öffentlichen Sektors erzwingen [neu in Security Center 1,3]

Verwenden Sie `glide.enforce_security_scope.sn_gsm`Eigenschaft, um zu steuern, wie auf die Anwendungsdaten aus der Anwendung „digitale Dienste für den öffentlichen Sektor“ zugegriffen wird.

Die ServiceNow Digitale Dienste für den öffentlichen Bereich Mit der Anwendung können Sie Anwendungen des öffentlichen Sektors entwickeln, die Beteiligte, Unternehmen und Behörden digitale Services bereitstellen.

Wenn `glide.enforce_security_scope.sn_gsm`Auf „falsch“ festgelegt ist, kann der Zugriff auf die Anwendungsdaten in den globalen Tabellen der App „digitale Services für den öffentlichen Sektor“ basierend auf den Zugriffssteuerungslisten (ACLs) dieser globalen Tabellen möglich sein. Wenn diese Eigenschaft auf „wahr“ festgelegt ist, wird der Zugriff auf Daten in globalen Tabellen nur basierend auf den ACLs ausgewertet, die direkt in der App „digitale Dienste für den öffentlichen Sektor“ geliefert werden. Wenn Sie diese Eigenschaft auf „falsch“ festlegen, kann dies zur Offenlegung von Informationen durch über zulässige ACLs führen.

Um dieses Sicherheitsrisiko zu beheben, legen Sie fest `glide.enforce_security_scope.sn_gsm`Auf „wahr“.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.enforce_security_scope.sn_gsm`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,2 • CVSS-Punktzahl: Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt wird, kann dies zur Offenlegung von Informationen durch überzulässige ACLs führen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Digitale Dienste für den öffentlichen Bereich konfigurieren

Bereichsbezogenen ACL-Zugriff für Playbooks für Informationsanforderungen erzwingen [neu in Security Center 1,3 und aktualisiert 1,5]

Verwenden Sie `glide.enforce_security_scope.sn_gsm_info_req`Eigenschaft zum Steuern des Zugriffs auf Playbook-Daten für die Playbooks-Funktion „Informationsanforderung“.

Die Information Request Playbook Mit der Anwendung können Endanwender des öffentlichen Sektors öffentliche Datensatzanforderungen übermitteln und nachverfolgen und bietet Behördendienstmitarbeitern einen vordefinierten Prozess für die Bearbeitung und Lösung dieser Anforderungen. Wenn `glide.enforce_security_scope.sn_gsm_info_req`lst nicht auf „wahr“ festgelegt, kann unerwarteter Zugriff auf Playbook-Daten für die Playbooks-Anwendung „Informationsanforderung“ gewährt werden. Legen Sie diese Eigenschaft auf „wahr“ fest, um beim Gewähren des Zugriffs nur ACLs aus dem Bereich „sn_GSM_info_req“ zu berücksichtigen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.enforce_security_scope.sn_gsm_info_req`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft auf „falsch“ festgelegt ist, werden ACLs aus allen Bereichen berücksichtigt, wenn Zugriff auf Playbook-Daten in der Umfangsmaster-Tabelle gewährt wird. Dadurch würden Playbook-Daten für Informationsanforderungen verfügbar gemacht.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	• Information Request Playbook verwenden • Konfigurieren Sie den Servicekanal für Informationsanforderungen

Strikte Erhöhungsberechtigung erzwingen [Neu in Security Center 1,3]

Verwenden Sie `glide.security.strict_elevate_privilege`Eigenschaft, die steuert, ob als privilegiert markierte Rollen manuell erhöht werden müssen, damit dem Anwender die Fähigkeiten der Rolle gewährt werden.

Legen Sie diese Eigenschaft auf „wahr“ fest, um eine zusätzliche Ebene der Sicherheitsvalidierung hinzuzufügen, wenn ein privilegierter Anwender seine Rolle erhöht.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.strict_elevate_privilege`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,7 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wann `glide.security.strict_elevate_privilege`lst auf „falsch“ festgelegt, werden Rollen, die als privilegiert markiert sind, automatisch bei einer neuen Sitzung eines Administratoranwenders hochgestuft und müssen nicht manuell hochgestuft werden (mit Ausnahme von „Security_admin“).
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft erfordert strikt, dass Benutzer der Administratorrolle Berechtigungen bei Bedarf erhöhen.

Playbook für Lizenz und Erlaubnis für den Sicherheitsumfang erzwingen [Neu in Security Center 1,5 und aktualisiert 2,0]

Verwenden Sie diese Eigenschaft, um zu bestimmen, ob nur die Zugriffssteuerungslisten (ACLs) im Plugin „Lizenz und Erlaubnis“ zur Bestimmung des Zugriffs auf den Umfang verwendet werden oder ob ACLs aus allen Bereichen berücksichtigt werden.

Wenn `glide.enforce_security_scope.sn_gsm_lic_prmt`Die Eigenschaft ist auf den empfohlenen Wert „wahr“ festgelegt. Dann werden nur ACLs im Plugin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Lizenz und Erlaubnis“ verwendet, um den Zugriff auf den Bereich zu bestimmen. Wenn diese Einstellung auf „falsch“ konfiguriert ist, werden Lizenz- und Erlaubnis-Playbooks-Daten in den Master-Tabellen des Umfangs verfügbar gemacht, da ACLs aus allen Bereichen Zugriff erhalten. Legen Sie fest, um das Datenrisiko zu reduzieren `glide.enforce_security_scope.sn_gsm_lic_prmt`Auf den empfohlenen Wert „wahr“.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.enforce_security_scope.sn_gsm_lic_prmt`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn Sie diese Einstellung auf den empfohlenen Wert „wahr“ konfigurieren, werden die Playbooks-Daten für Lizenzen und Berechtigungen in den Master-Tabellen des Umfangs gesichert, indem nur ACLs von berücksichtigt werden `sn_gsm_lic_prmt`Umfang für die Gewährung von Zugriff. Wenn Sie diese Option auf „falsch“ festlegen, werden die Playbooks-Daten für Lizenzen und Berechtigungen in den Master-Tabellen des Umfangs verfügbar gemacht, indem die ACLs aus allen Bereichen für die Gewährung des Zugriffs berücksichtigt werden. Beispielsweise kann der IT-Administrator auf Playbooks-Daten für Lizenzen und Berechtigungen zugreifen, wenn diese Einstellung „falsch“ ist.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• Playbook für Lizenzen und Berechtigungen verwenden • Anwendungsbereich

Sicherheitsbereich für Mitarbeiterbereich für HR-Fallmanagement erzwingen [Neu in Security Center 1,5 und aktualisiert 2,0]

Konfigurieren Sie das Plugin „Mitarbeiterbereich für HR-Fallmanagement“ so, dass auf Daten in den Master-Tabellen des Umfangs nur Anwender mit den richtigen Berechtigungen zugreifen können, wodurch das Prinzip der geringsten Berechtigung durchgesetzt wird.

Wenn `glide.enforce_security_scope.sn_hr_agent_ws`Das Plugin ist mit dem empfohlenen Wert „wahr“ konfiguriert. Dann werden nur die Zugriffssteuerungslisten (ACLs) im Mitarbeiterbereich für HR-Fallmanagement-Plugin verwendet, um den Zugriff auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Ressource zu bestimmen. Wenn diese Einstellung auf „falsch“ festgelegt ist, werden Mitarbeiterbereich für HR-Fallmanagement-Daten in den Master-Tabellen des Umfangs verfügbar gemacht, da den ACLs aus allen Bereichen Zugriff gewährt wird.Beispielsweise kann ein IT-Administrator auf Mitarbeiterbereich für HR-Fallmanagement-Daten zugreifen, wenn diese Einstellung auf „falsch“ festgelegt ist. Um dies zu verhindern, legen Sie fest `glide.enforce_security_scope.sn_hr_agent_ws`Auf den empfohlenen Wert „wahr“, der sicherstellt, dass das Prinzip der geringsten Berechtigung vorhanden ist, da Anwender nur auf Ressourcen zugreifen können, für die sie berechtigt sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.enforce_security_scope.sn_hr_agent_ws`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn Sie diese Einstellung auf „falsch“ konfigurieren, werden die Daten des Mitarbeiterbereichs für HR-Fallmanagement in den Master-Tabellen des Umfangs verfügbar gemacht, da die ACLs aus allen Bereichen Zugriff erhalten.
Abhängigkeiten und Voraussetzungen	Mitarbeiterbereich für HR-Fallmanagement
Funktionale Auswirkung	Wenn Sie diese Einstellung auf „wahr“ konfigurieren, wird die Ausführung globaler ACLs für eine Tabelle erzwungen, wenn bereichsbezogene ACLs für sie nicht vorhanden sind.
Referenzen	• https://owasp.org/www-project-proactive-controls/#div-numbering • Fügen Sie eine Komponente zu hinzu Mitarbeiterbereich

Sicherheitsumfang für Serviceanwendungsinformationen erzwingen [Neu in Security Center 2,0]

Verwenden Sie `glide.enforce_security_scope.sn_svc_appl`Eigenschaft, um sicherzustellen, dass die Daten in Master-Umfangstabellen gesichert sind.

Wenn `glide.enforce_security_scope.sn_svc_appl_info`Die Eigenschaft ist auf „wahr“ festgelegt. Der Zugriff auf Ressourcen innerhalb des Bereichs wird ausschließlich durch die Zugriffssteuerungslisten (ACLs) aus dem Plugin „Service Application Information“ (sn_svc_appl_info) bestimmt. Dies stellt die Sicherheit von Daten in Master-Umfangstabellen sicher, indem Zugriffsberechtigungen auf diejenigen beschränkt werden, die im Bereich „sn_svc_appl_info“ definiert sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn dieser Wert auf den unsicheren Wert „falsch“ festgelegt ist, werden ACLs aus allen Bereichen berücksichtigt, wenn Zugriff auf Daten in Master-Umfangstabellen gewährt wird, z. B. „sys_attachment“. Dies kann zu nicht autorisiertem Zugriff auf vertrauliche Informationen durch Anwender führen, die nicht über Berechtigungen für die Daten der Serviceanwendungsinformationen verfügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.enforce_security_scope.sn_svc_appl_info`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft auf den unsicheren Wert „falsch“ festgelegt ist, kann dies zu nicht autorisiertem Zugriff auf vertrauliche Daten durch Anwender führen, die keine Berechtigungen für die Daten der Serviceanwendungsinformationen haben.
Abhängigkeiten und Voraussetzungen	Das Plugin „Informationen zum Serviceantragsteller“ (`com.sn_svc_appl_info`) Muss für aktiviert sein `glide.enforce_security_scope.sn_svc_appl_info`Eigenschaft, die wirksam sein soll.

Erzwingen Sie ACLs auf Feldebene in GlideRecordSandbox

Verwalten Sie ACLs auf Feldebene in GlideRecordSandbox in Ihrer Instanz.

Verwenden Th E `glide.sandbox.fields.check_acl` Eigenschaft zum Erzwingen von ACLs auf Feldebene in GlideRecordSandbox. Ein Beispiel, in dem diese Eigenschaft angewendet wird, ist, wenn ein Anwender ein Skript wie in bereitstellen kann `sysparm_query`. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Wahr** , ACL-Einschränkungen können umgangen werden, wodurch vertrauliche Daten gefährdet werden können, z. B. `sys_user.user_password`Von einem nicht autorisierten Anwender.

Warnung: Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sandbox.fields.check_acl`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Ermöglicht die Umgehung von ACL-Einschränkungen, die vertrauliche Daten offenlegen können.
Abhängigkeiten und Voraussetzungen	Keine

Nutzung des Anmeldeinformationsalias erzwingen [Neu in Security Center 1,3 Und aktualisiert 1,5]

Erfahren Sie, wie Sie Ihre Anmeldeinformationen vor nicht autorisierter Verwendung schützen können, indem Sie die Eigenschaft MID-Server konfigurieren.

Der MID-Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die als Windows-Service oder UNIX-Daemon in Ihrem lokalen Netzwerk ausgeführt wird. MID-Server-Eigenschaften sind in der Tabelle [ecc_Agent_property] aufgeführt. Sie können in Ihrer Instanz darauf zugreifen, indem Sie zu navigieren **MID-Server** > **Eigenschaften**an. Aliasse für Anmeldeinformationen ermöglichen es einem Administrator, bestimmte Anmeldeinformationen in Discovery-Zeitplänen zu verwenden. Anmeldeinformationsaliasse bieten eine detailliertere Steuerung darüber, welche Anmeldeinformationen eine Discovery-Tabelle verwenden darf. Legen Sie fest, um diese Sicherheitslücke zu beheben `alias_filtering_behavior`Strikt, um unnötiges Aussetzen von Anmeldeinformationen mit erhöhten Berechtigungen zu verhindern. Unter MID Server-Eigenschaften finden Sie weitere Details.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`alias_filtering_behavior`
Konfigurationstyp	MID-Servereigenschaften (/ecc_Agent_property_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	strict
Standardwert	Lose
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2 • CVSS-Punktzahl: Niedrig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Sicherheitsrisikodetails: Wenn diese Härtungseinstellung nicht auf strikt festgelegt ist, werden alle Anmeldeinformationen unabhängig von ihren Aliasen für Discovery-Tabellen verwendet, was die Wahrscheinlichkeit eines nicht autorisierten Zugriffs erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• MID-Server • Anmeldeinformationsaliasse für Discovery

GroupBy-ACLs erzwingen

Konfigurieren Sie Ihre Instanz, um ACL-Prüfungen für groupby-Spalten durchzuführen.

Verwenden Sie `glide.security.groupby_acl_check`Systemeigenschaft zum Konfigurieren Ihrer Instanz zur Durchführung von ACL-Prüfungen für groupby-Spalten. Wenn diese Eigenschaft auf den empfohlenen Wert von festgelegt ist **Wahr** , Dann werden ACLs in groupby-Spalten standardmäßig berücksichtigt. Eine Tabelle `groupby_acl_check`Attribut hat Vorrang vor `glide.security.groupby_acl_check`Eigenschaft. Wenn die Eigenschaft auf festgelegt ist **Falsch** , Stellen Sie dann sicher, dass jede Tabelle, die ACL-Prüfungen für groupby-Spalten haben soll, über verfügt `groupby_acl_check`Attribut auf festgelegt **Wahr** .

Stellen Sie die Eigenschaft sicher `glide.security.groupby_acl_check`Ist auf festgelegt **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.groupby_acl_check`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Deaktiviert die ACLs-Prüfung für groupby-Spalten, was zu Informationsverlusten führen kann.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass ACLs der Archivtabelle aktiviert sind [Neu in Security Center 1,3 und aktualisiert in 1,5]

Die *glide.security.enable_archive_table_acls*Die Eigenschaft steuert, ob Zugriffssteuerungslisten (ACLs) der ursprünglichen Tabelle, der Tabelle, aus der die Archivtabelle erstellt wurde, als „falsch“ ausgewertet werden.

Die *glide.security.enable_archive_table_acls*Eigenschaft darf nicht auf „falsch“ festgelegt werden, da die ACLs der ursprünglichen Tabelle unabhängig von ihrem Wert ausgewertet werden. Sie können zusätzliche ACLs für eine Archivtabelle vermeiden, indem Sie sie nicht hinzufügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.enable_archive_table_acls*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn die Eigenschaft auf „falsch“ festgelegt ist, werden ACLs, die archivierten Tabellen hinzugefügt wurden, ignoriert. Eine Aktion, die intuitiv ist und daher zu einer Autorisierungsumgehung führen kann.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden alle aktiven Lese-ACLs in Archivtabellen berücksichtigt. Wenn keine aktiven Lese-ACLs vorhanden sind oder die Eigenschaft auf „falsch“ festgelegt ist, wird die ursprüngliche Tabelle (Tabelle, aus der Daten archiviert wurden) auf die Archivtabelle angewendet. **Hinweis:** In Archivtabellen werden nur Lese-ACLs unterstützt. Andere Vorgänge in Archivtabellen werden intern über einen Zugriffs-Handler gesteuert.

Stellen Sie sicher, dass die Erstellung/Löschung von Dashboards eine Zugriffsprüfung erfordert [Neu in Security Center 1,3 und aktualisiert in 2,0]

Die *glide.processors.check_access_before_process*Die Systemeigenschaft ermöglicht die Durchsetzung von Zugriffssteuerungslisten (ACL) zum Erstellen oder Löschen von Dashboards, wenn ein Anwender angemeldet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie die Systemeigenschaft *glide.processors.check_access_before_process* auf **true** fest. Wenn die Eigenschaft nicht in der Tabelle „Systemeigenschaften“ [sys_properties] angezeigt wird, ist der Fallback-Wert **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.processors.check_access_before_process*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Fallback-Wert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft deaktivieren, indem Sie sie auf „falsch“ festlegen, wird eine ACL-Umgehung in Dashboards aktiviert. Dadurch können alle authentifizierten Anwender mit geringen Berechtigungen Dashboards löschen und hinzufügen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft steuert die Möglichkeit, neue sys_Dashboards zu erstellen und vorhandene Dashboards zu löschen, wenn einem Anwender die erforderlichen Zugriffsrechte fehlen. Wenn der Wert auf „falsch“ festgelegt ist, können Anwender mit unangemessenen Rollen sys_Dashboard-Einträge hinzufügen und löschen (obwohl die GlideRecord-Ebene die vorhandenen ACLs erneut überprüfen sollte). Der Wert „wahr“ schränkt das Hinzufügen und Löschen von Vorgängen für Anwender ohne die erforderlichen Zugriffsrechte ein.

Vertrauliche Tabellen und Felder von der Datengenerierung ausschließen [Neu in Security Center 7,0]

Verwenden Sie Systemeigenschaften, um Tabellen und Felder aus der Datengenerierung auszuschließen, die verwendet wird, um gefälschte Datensätze basierend auf vorhandenen Daten zu generieren. Tabellen und Felder, die diesen Ausschlusslisten hinzugefügt werden, können nicht für die Datengenerierungsfunktion verwendet werden.

In enthaltene Tabellen *glide.data.generation.excluded.tables*Systemeigenschaft ist zusätzlich zu Metadatentabellen von der Datengenerierung ausgeschlossen.

Felder, die in einer kommagetrennten Liste für enthalten sind *glide.data.generation.excluded.fields.<TABLE-NAME>*Sind zusätzlich zu einem dieser Felder gegebenenfalls von der Datengenerierung ausgeschlossen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nummer
- Rollen
- sys_class_name
- sys_created_by
- sys_id
- sys_mod_count
- sys_Tags
- sys_updated_by

Überprüfen Sie die Liste der Tabellen, die in der Eigenschaft enthalten sind `glide.data.generation.excluded.tables`. Fügen Sie der kommagetrennten Liste der Tabellen alle Tabellen hinzu, die von der Datengenerierung ausgeschlossen werden sollen. Darüber hinaus werden Metadatentabellen für die Datengenerierung ignoriert.

Überprüfen Sie die Liste der Felder für jede Tabelle, indem Sie sich Eigenschaften im folgenden Format ansehen: Glide.Daten.Generierung.Ausgeschlossene.Felder.<TABLE-NAME>. Fügen Sie alle sensiblen Felder für die angegebene Tabelle als kommagetrennte Werteliste hinzu.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	• `glide.data.generation.excluded.tables` • `glide.data.generation.excluded.fields.*`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	• Kommagetrennte Liste von Tabellennamen • Kommagetrennte Liste von Feldern für eine bestimmte Tabelle
Empfohlener Wert	• Kommagetrennte Liste von Tabellennamen, die von der Datengenerierung ausgeschlossen werden sollen • Kommagetrennte Liste von Feldnamen, die für jede anwendbare Tabelle von der Datengenerierung ausgeschlossen werden sollen
Standardwert	"",""
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,6 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Für Daten in Tabellen, die in der Datengenerierungsfunktion verwendet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	werden, können echte oder falsche Werte wie von der Funktion beabsichtigt ausgefüllt werden. Sensible Werte in Tabellen, die nicht sichtbar oder repliziert sein sollen, können anderen Instanzanwendern angezeigt werden.
Abhängigkeiten und Voraussetzungen	Plugin „Datengenerierung“ wird verwendet

Verhindern, dass Anwender eine Warnung zur Umgehung der CSRF-Validierung akzeptieren [aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie `glide.security.csrf.strict.validation.mode`Eigenschaft zum Aktivieren der strikten Validierung des CSRF-Tokens. Wenn das CSRF-Token nicht übereinstimmt, wird die erneute Übermittlung der Anforderung verhindert.

Diese Eigenschaft verhindert, dass Anwender eine Warnung akzeptieren können, die das Senden einer potenziell schädlichen Anforderung an die Instanz ermöglicht. Diese Warnung wird angezeigt, wenn eine POST-Anforderung aufgrund eines falsch übereinstimmenden Anti-CSRF-Tokens fehlschlägt, das zu einer der anderen aktiven Sitzungen des Opfers gehört. Wenn `glide.security.csrf.strict.validation.mode`lst nicht auf den empfohlenen Wert „wahr“ festgelegt, kann ein Angreifer einen CSRF-Angriff mithilfe eines ausgelesenen Anti-CSRF-Tokens aus einer anderen aktiven Sitzung, die zum Opfer gehört, formulieren. Eine POST-Anforderung an eine Instanz enthält ein Anti-CSRF-Token in „sysparm_ck“ oder „X-UserToken“, das der aktuellen Sitzung des Anwenders entspricht.

Wenn das Anti-CSRF-Token stattdessen an eine der anderen aktiven Sitzungen des Anwenders gebunden ist, gibt die POST-Anforderung eine 302-Umleitung an Security_Interceptor.do zurück, wobei dem Anwender eine Schaltfläche „Fortfahren“ zur Verfügung steht, wenn diese Eigenschaft auf „falsch“ festgelegt ist. Wenn Sie auf diese Schaltfläche klicken, wird die Anforderung erneut an die Instanz gesendet, es sei denn, sie verfügt jetzt über ein gültiges Anti-CSRF-Token. Wenn diese Eigenschaft auf „wahr“ festgelegt ist, zeigt die 302-Weiterleitung zur Seite „Security_interceptor.do“ keine Schaltfläche „Fortfahren“ an, und der Anwender darf die Anforderung nicht erneut übermitteln.Ein erfolgreicher CSRF-Angriff ermöglicht es einem Angreifer, jeden Vorgang effektiv auszuführen, den das Opfer ausführen kann.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.csrf.strict.validation.mode`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Dient zum Erzwingen einer strikten Validierung des CSRF-Tokens und verhindert die Wiederverwendung.
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	(Mittel) Cross Site Request Forgery ist ein erhebliches Sicherheitsrisiko, das die Integrität der Instanzdaten verletzt. Ein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Angreifer kann den CSRF-Angriff auf jeden Instanzanwender starten, indem er das Vertrauen des Instanzanwenders missbraucht. Mit Hilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine fehlerhafte Anforderung an die Instanz senden.
Sicherheitsrisikobewertung	3,7
Funktionale Auswirkung	Diese Korrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Instanzanwender eine Schreibanforderung an die Instanz sendet. Überprüft, ob das aktuelle CSRF-Token zuvor verwendet wurde. Wenn ja, wird die Übermittlung weiterer Schreibanforderungen verhindert.
Sicherheitsrisiko	(Mittel) Cross Site Request Forgery ist ein erhebliches Sicherheitsrisiko, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff auf jeden Instanzanwender starten, indem er das Vertrauen des Instanzanwenders missbraucht. Mit Hilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine fehlerhafte Anforderung an die Instanz senden.

Zurück zu Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch Um Ihren umschlossenen Schlüssel hochzuladen.

Lesezugriff delegierter Entwickler beschränken [aktualisiert im Sicherheitscenter 1,3]

Wenn *com.glide.dd_allow_global_access_tables*Enthält nicht den empfohlenen Wert von wf_activity, wf_activity_Definition, wf_Workflow, wf_Workflow_Version, sp_Portal, sp_Widget und sp_page, dann können diese Tabellen von einem delegierten Entwickler gelesen werden. Dies kann dem delegierten Entwickler Lesezugriff auf vertrauliche Informationen gewähren.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.dd_allow_global_access_tables*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	wf_Activity, wf_activity_Definition, wf_Workflow, wf_Workflow_Version, sp_Portal, sp_Widget, sp_page
Standardwert	wf_Activity, wf_activity_Definition, wf_Workflow, wf_Workflow_Version, sp_Portal, sp_Widget, sp_page
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sicherheitsrisikodetails: Stellen Sie sicher, dass `com.glide.dd_allow_global_access_tables`lst auf wf_Activity, wf_activity_Definition, wf_Workflow, wf_Workflow_Version, sp_Portal, festgelegt sp_Widget, sp_page.

Überprüfung der AJAXGlideRecord-ACL erfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.script.secure.ajaxgliderecord`Eigenschaft zum Durchführen der ACL-Validierung (Access Control Rule), wenn serverseitige Datensätze, z. B. Tabellen, mithilfe von GlideAjax-APIs innerhalb eines Client-Skripts aufgerufen werden.

Aus Client-Skripts können beliebige Daten vom Server mit AJAXGlideRecord (abgefragt werdenGlideAjax – Client) API mithilfe einer Syntax, z. B. eines serverseitigen Glide-Datensatzes. Es ist ein leistungsstarkes und nützliches Tool in vielen Bereitstellungen.

Wenn Sie Zugriffssteuerungslisten (ACL) auf GlideAjax-API-Aufrufe anwenden möchten, können Sie nur Daten abfragen, auf die der derzeit verbundene Anwender Zugriff hat. Wenn beispielsweise ein ESS-Anwender angemeldet ist, der keine Rechte zum Lesen der Tabelle „cmn_location“ hat, würde jeder GlideAjax-API-Aufruf für diese Tabelle fehlschlagen.

Wenn ServiceNow AI Platform Wird ohne GlideAjax ACL-Aufrufüberprüfung ausgeführt. Eine API kann Informationen zurückgeben, auf die der derzeit angemeldete Anwender andernfalls nicht zugreifen konnte.

Verwenden Sie GlideRecordSecure beim Abfragen von Daten, um ein Höchstmaß an Sicherheit sicherzustellen. GlideRecord basiert auf der ACL-Durchsetzung durch Konfigurationen, während GlideRecordSecure strengere Sicherheitskontrollen anwendet. GlideRecordSecure bietet eine sicherere, sofort einsatzbereite Lösung für den Umgang mit sensiblen Daten.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.script.secure.ajaxgliderecord`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Stellen Sie sicher, dass Sicherheits-ACLs überprüft und validiert werden, auch wenn über clientseitige APIs auf die Datensätze zugegriffen wird.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	Diese Korrektur erzwingt die ACL-Beziehung mit serverseitigen Datensätzen, wenn die Anforderungen mithilfe der AJAXGlideRecord-API-Aufrufe gestellt werden. Wenn die ACL-Konfiguration nicht ordnungsgemäß konfiguriert ist, gibt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	es potenzielle Auswirkungen. Weitere Informationen zu den Auswirkungen und zur Identifizierung finden Sie unter Weitere Informationen finden Sie unter Clientseitige GlideRecord-Transaktionen (AJAXGlideRecord) auditieren und überprüfen [KB0550828] artikel in HI Knowledge Base .
Sicherheitsrisiko	(Hoch) über Client-Skripts ist es möglich, beliebige Daten vom Server über die GlideAjax-API abzufragen. Auf serverseitige Ressourcen kann ohne ordnungsgemäße Autorisierung zugegriffen werden. Die ACL-Validierung hilft der Anwendung, die Anforderung basierend auf der konfigurierten Autorisierung zu validieren.
Workaround	Stellen Sie sicher, dass richtige ACLs für Skripteinbindungen, Prozessoren und andere Entitäten erstellt werden, die von einer GlideAjax-API (AJAXGlideRecord) verwendet werden, damit sie unter ordnungsgemäßer Autorisierung ausgeführt wird. Implementieren Sie Methoden wie `CanRead ()` , `CanWrite()` , `KanErstellen ()` , Und `CanDelete ()` Dient zum Durchführen der Anwenderautorisierung, bevor mit GlideRecord auf Tabellendatensätze zugegriffen wird. Eine andere Methode ist die Verwendung von GlideRecordSecure. Die Klasse wird vom GlideRecord-Server übernommen, der die gleichen Funktionen wie GlideRecord ausführt und auch ACLs erzwingt.
Referenzen	ACLs auf AJAXGlideRecord anwenden (clientseitiger Glide-Datensatz) Diese Eigenschaft gehört zur gleichen Eigenschaftenfamilie, die die Ausführung von Skripts, die vom Client stammen, sicherstellt und einschränkt, z. B. `glide.script.allow.ajaxevaluate`. Weitere Informationen finden Sie unter Aktivieren Sie AJAXEvaluate .

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Schreibzugriff auf Systemfelder auf Administratoranwender beschränken [Neu in Security Center 7,0]

Verwenden Sie `glide.rest.table_api.admin_only_sys_fields`Systemeigenschaft zur Steuerung des Schreibzugriffs auf die vom System generierten Felder.

Die `glide.rest.table_api.admin_only_sys_fields`Eigenschaftssteuerungen Schreibzugriff auf diese Felder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sys_id
- sys_created_by
- sys_created_on
- sys_updated_by
- sys_updated_on

Wenn diese Eigenschaft auf festgelegt ist **Wahr** , Nur ein Administrator kann in diese Felder schreiben, die vom System generierte Werte sind. Wenn die Eigenschaft auf festgelegt ist **Falsch** Oder es ist in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden. Anwender, die über Erstellungs- oder Schreibzugriff auf eine Tabelle verfügen, können diese Systemwerte mit schreiben Tabellen-API .

Legen Sie die Eigenschaft fest *glide.rest.table_api.admin_only_sys_fields*Bis **Wahr** Um zu verhindern, dass nicht-Administratoranwender Systemfelder in Datensätzen aktualisieren.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.rest.table_api.admin_only_sys_fields*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Fallback-Wert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Anwender ohne die Administratorrolle können Felder wie sys_created_by oder sys_updated_on aktualisieren. Dieser Zugriff kann sich auf die Integrität der erstellten oder aktualisierten Datensatzmetadaten auswirken, sodass Datensätze so angezeigt werden, als ob sie von einem anderen Anwender erstellt oder zu einem anderen Zeitpunkt aktualisiert wurden.
Funktionale Auswirkung	Alle Integrationen oder Anwender ohne Administratorrolle, die die Tabellen-API zum Erstellen oder Aktualisieren von Datensätzen und zum Ändern dieser Felder verwenden, sind betroffen. Diese Anforderungen an die Tabellen-API legen den Abfrageparameter fest *sysparm_suppress_auto_sys_field*Bis **Falsch** Und legen Sie diese Felder im Anforderungstext fest.
Abhängigkeiten und Voraussetzungen	Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Genehmigung für Änderungen der Agent-basierten Office 365-Gruppenmitgliedschaft erforderlich [Neu in Security Center 7,0]

Aktivieren Sie den Genehmigungs-Flow zum Hinzufügen oder Entfernen von Office 365-Gruppenmitgliedern über den KI-Agent für Microsoft 365-Gruppenmitgliedschaft mithilfe einer Systemeigenschaft.

Verwenden Sie *sn_itsm_aia.office_365_group_member_approval.required*Systemeigenschaft zur Steuerung, ob der Genehmigungs-Flow zum Hinzufügen oder Entfernen von Office 365-Gruppenmitgliedern über den KI-Agent aktiviert oder deaktiviert ist. Wenn der Genehmigungs-Workflow aktiviert ist, muss ein Genehmigungsdatensatz von einem Mitglied der in angegebenen Gruppe auf „genehmigt“ festgelegt werden *sn_itsm_aia.office_365_group_member_approval.group_id*Systemeigenschaft. Wenn *sn_itsm_aia.office_365_group_member_approval.group_id*Eigenschaft ist nicht konfiguriert, die *Microsoft 365 group member approvers*Gruppe wird verwendet.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_itsm_aia.office_365_group_member_approval.required*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Fallback-Wert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,9 • CVSS-Punktzahl: Mittel • Jeder Anwender, der auf die Microsoft 365-Gruppenmitgliedschaft AI Agent zugreifen kann, kann Office 365-Gruppenmitglieder hinzufügen und aus der Azure AD-Gruppe entfernen, wenn keine ausdrückliche Genehmigung durch die angegebene Genehmigergruppe erforderlich ist. Stellen Sie sicher, dass diese Änderungen genehmigt werden, um das Risiko der Erhöhung von Berechtigungen zu reduzieren, indem Sie Mitglieder ohne entsprechende Autorisierung hinzufügen/entfernen.
Funktionale Auswirkung	Wenn *sn_itsm_aia.office_365_group_member_approval.required*Ist auf festgelegt **Wahr** , Ein Mitglied der in angegebenen Gruppe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	*sn_itsm_aia.office_365_group_member_approval.<group_id>*M den Incident genehmigen, der das Hinzufügen oder Entfernen von Office 365-Gruppenmitgliedern anfordert. Wenn *sn_itsm_aia.office_365_group_member_approval.required*lst auf festgelegt **Falsch** Dann ist keine Genehmigung erforderlich, und der KI-Agent kann den Prozess zum Hinzufügen oder Entfernen von Mitgliedern aus einer Office 365-Gruppe autonom bearbeiten.
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Verhindern Sie, dass der Anwender seine Identität ausnimmt, Anwendungsdaten anzuzeigen

Verwenden Sie Systemeigenschaften, um zu verhindern, dass ein Anwender seine Identität ausnimmt, Anwendungsdaten anzeigen kann.

Verhindern Sie, dass auf Administratorebene auf die anwendungsspezifischen Daten zugegriffen wird, die zu diesem Anwender gehören, wenn die Identität eines Accounts angenommen wird. Diese Berechtigung kann auf Anwendungsebene festgelegt werden, indem eine für die Anwendung spezifische Systemeigenschaft erstellt wird.

Diese Systemeigenschaften verwenden *<scope>.impersonateCheck*Benennungsformat (z. B. *sn_hr_core.impersonateCheck*). Erstellen Sie eine Systemeigenschaft mit einem Wert von **Wahr** Um zu verhindern, dass Anwender beim Identitätswechsel eines Accounts auf die anwendungsspezifischen Daten eines anderen Anwenders zugreifen.

Hinweis: Nicht alle Anwendungen sind so konzipiert, dass sie in dieser Konfiguration funktionieren, oder verfügen zu diesem Zweck über einen Systemeigenschaften-Datensatz [sys_properties]. Die folgenden Bereiche sind für die Verwendung mit dieser Eigenschaft konfiguriert.

- sn_Opp_Market
- sn_jny
- sn_imt_vaccine
- sn_imt_Health_Test
- sn_HR_Core
- sn_egd_Goals
- sn_egd_core
- sn_egd_act
- sn_em
- sn_Talent_aia

Für jede Anwendung mit *<scope>.impersonateCheck*Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] stellen Sie sicher, dass der Eigenschaftswert auf festgelegt ist **Wahr** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Eigenschaften können nur vom bereichsbezogenen Administrator für die spezifische Anwendung geändert werden.

Verwenden Sie dieses Skript, um zu ermitteln, welche Eigenschaften für die Instanz aktualisiert oder erstellt werden müssen:

```
var properties = [
   'sn_opp_market.impersonateCheck',
   'sn_jny.impersonateCheck',
   'sn_imt_vaccine.impersonateCheck',
   'sn_imt_health_test.impersonateCheck',
   'sn_hr_core.impersonateCheck',
   'sn_egd_goals.impersonateCheck',
   'sn_egd_core.impersonateCheck',
   'sn_egd_act.impersonateCheck',
'sn_em.impersonateCheck',
'sn_talent_aia.impersonateCheck'
];

var pm = new GlidePluginManager();

for (var i = 0; i < properties.length; i++) {
   var property = properties[i];
   var application = property.split('.')[0];
   var propertyValue = gs.getProperty(property, 'false');

   if (pm.isActive(application) && propertyValue.toLowerCase() != 'true') {
      gs.print(property);
   }
}
```

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*<scope>.impersonateCheck*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,8 • CVSS-Punktzahl: Niedrig • Ein Wert von **Falsch** Mit diesen Eigenschaften kann ein Anwender auf Administratorebene die Identität eines anderen Anwenders annehmen und mit dem Zugriff des Anwenders auf Anwendungsdaten zugreifen. Dies kann unerwünscht sein oder einen nicht autorisierten Datenzugriff in bestimmten Anwendungskontexten ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Erzwingen Sie die Validierung des oauth-Statusparameters

Konfigurieren Th E *glide.oauth.state.parameter.required*Eigenschaft, um Ihre Instanz vor standortübergreifenden Angriffen auf Anforderungsfälschung (Request Forgery, CSRF) zu schützen.

Die *glide.oauth.state.parameter.required*Mit der Eigenschaft kann der Parameter Status in einer OAuth-Anforderung für den Autorisierungscode-Flow erforderlich sein. Der Parameter Status ist ein Zeichenfolgenwert, der keine Sonderzeichen enthalten oder leer sein darf. Diese Eigenschaft wird auf festgelegt **Wahr** Stellt sicher, dass ein Angreifer während der Authentifizierung keine CSRF-Angriffe (Cross Site Request Forgery) ausführen kann, wodurch Ihre Instanz vor Angriffen durch einen Anwender geschützt wird, dessen Identität angenommen wurde.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.oauth.state.parameter.required*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,2 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Legen Sie diese Eigenschaft auf fest **Wahr** Um sicherzustellen, dass CSRF-Angriffe verhindert werden.
Abhängigkeiten und Voraussetzungen	Keine

Strikten Upload von Anwenderbildern erzwingen

Verwenden Sie *glide.security.strict.user_image_upload*Eigenschaft zum Aktivieren der Zugriffssteuerung für das Hochladen/Aktualisieren eines Profilbilds, wenn sie für einen Anwenderdatensatz ausgeführt wird.

Diese Einstellung eröffnet die Möglichkeit, dass ein nicht autorisierter Anwender ein Bild in das Profil eines anderen Anwenders hochlädt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie diese Eigenschaft auf festlegen **Wahr** , Die Tabellen-ACLs werden beim Hochladen von Fotos erzwungen, sodass nur autorisierte Anwender ein Bild hochladen können.
- Wenn Sie es auf festlegen **Falsch** , ACLs werden beim Hochladen von Bildern in das Feld „Foto“ nicht erzwungen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.strict.user_image_upload`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um das Hochladen von Anwenderbildern nur auf autorisierte Anwender zu beschränken.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	3,7
Funktionale Auswirkung	Keine Auswirkungen auf die Funktionalität, da autorisierte Anwender weiterhin Bilder in ihr Anwenderprofil hochladen können.
Sicherheitsrisiko	(Niedrig) wenn Sie diese Eigenschaft auf festlegen **Falsch** , Ein authentifizierter Anwender kann ein Bild ohne Autorisierung in den Account eines anderen Anwenders hochladen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Beschränken Sie E-Mail-Domänen für die Registrierung externer Anwender [Aktualisiert in Sicherheitscenter 1,3, 1,5 und 2,0]

Verwenden Sie `sn_ext_usr_reg.allowed_email_domains`Eigenschaft zum Auflisten zulässiger externer E-Mail-Domänen.

Die **sn_ext_usr_reg.allowed_email_Domains** Die Systemeigenschaft definiert, welche E-Mail-Adressen sich bei einer selbst registrieren dürfen ServiceNow Instanz. Das Format muss eine kommagetrennte Liste zulässiger E-Mail-Domänen sein, z. B. domain1.com,domain2.com Wo E-Mails wie example@domain2.com Wird akzeptiert. Wenn **sn_ext_usr_reg.allowed_email_Domains** Ist nicht mit einer Liste zulässiger Domänen festgelegt, dann können Anwender mit einer beliebigen E-Mail-Adresse Accounts in den Instanzen registrieren. Wenn nicht definiert, können böswillige Akteure die Registrierung mithilfe von E-Mail-Adressen aus unerwünschten Domänen durchführen, um authentifizierten Zugriff auf die Instanz zu erhalten.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`sn_ext_usr_reg.allowed_email_domains`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do), Communities-Eigenschaften
Kategorie	Zugriffssteuerung
Zweck	Listen Sie E-Mail-Domänen auf, damit Anwender-E-Mails für die Registrierung zulassen.
Empfohlener Wert	Als nicht leerer Wert festlegen
Konfigurationstyp	Zeichenfolge
Sicherheitsrisiko	(Hoch) böswillige Akteure könnten die Registrierung mithilfe von E-Mail-Adressen aus unerwünschten Domänen durchführen. Stellen Sie sicher **sn_ext_usr_reg.allowed_email_Domains** Ist nicht auf einen leeren Wert festgelegt.
Sicherheitsrisikobewertung	7,5
Referenzen	Communities

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Plugin für hohe Sicherheit aktivieren [aktualisiert in Security Center 1,3]

Wenn Sie das Plugin „hohe Sicherheit“ aktivieren, erstellt oder aktualisiert es Hunderte verschiedener Konfigurationen, um das Sicherheitsniveau in Ihrer Instanz zu steuern. Diese Konfigurationen mindern viele der Top-OWASP-Angriffe, indem sie eine strikte Zugriffssteuerung, Eingabevalidierung und Ausgabecodierung ermöglichen.

Diese Konfigurationen umfassen:

- Zugriffssteuerung
- Business-Regeln
- Systemeigenschaften
- UI-Richtlinienaktion
- Skriptaktionen
- Skripteinbindungen

Beispiel

In den Beispielen finden Sie die folgenden Eigenschaften:

Eigenschaft	Thema
glide.ui.escape_all_script	Jelly-Skript mit Escape-Zeichen [aktualisiert in Security Center 1,3 und 1,5]
glide.security.strict.actions	Überprüfen Sie die UI-Aktionsbedingungen vor der Ausführung
glide.security.csrf_previous.allow	Anti-CSRF-Token aktivieren [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Thema
glide.security.csrf.strict.validation.mode	Verhindern, dass Anwender eine Warnung zur Umgehung der CSRF-Validierung akzeptieren [aktualisiert in Security Center 1,3 und 1,5]

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	Com.Glide.High_Security
Konfigurationstyp	Systemdefinition > Plugins – Entwicklung
Kategorie	Zugriffssteuerung
Zweck	Es ist obligatorisch, dieses Plugin zu aktivieren. Es erhöht das Sicherheitsniveau einer Instanz, wodurch die Angriffsfläche reduziert wird, indem owasp Top 10-Angriffe abgemildert werden, einschließlich CSRF, XSS, Sichern von Sitzungscookies und Datei-Uploads.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	Dieses Plugin aktiviert mehrere Systemsicherheitskonfigurationen, die sich auch auf die Anwenderoberfläche und Funktionalität auswirken können.
Sicherheitsrisiko	(Hoch) viele Sicherheitskonfigurationen werden unbeabsichtigt offen gelassen, was die Tür für einige der kritischen Schwachstellen öffnen kann.
Referenzen	Einstellungen Für Hohe Sicherheit Werden Aktiviert Strenge Sicherheitseinstellungen

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Plugins aktivieren

ACLs mit Admin-Aufhebung berücksichtigen

Die `glide.security.admin.override.accessterm`Die Eigenschaft steuert Administratoren, dass sie die ACL-Auswertung nicht überschreiben können, auch wenn die Überschreibung wirksam sein soll.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.admin.override.accessterm`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Steuert, dass Administratoren die ACL-Auswertung nicht überschreiben können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	Boolean
Empfohlener Wert	True
Standardwert	True
Sicherheitsrisiko	(Niedrig) ACLs werden kumulativ ausgewertet. Wenn in einem bestimmten Feld eine Anzahl von ACLs vorhanden ist und die Option „Administratorüberschreibungen“ in einem Feld auf „falsch“ (nicht ausgewählt) festgelegt ist, gelten die effektiven Administratorüberschreibungen für alle ACLs als „falsch“.
Sicherheitsrisikobewertung	3,8
Referenzen	Regeln Für Zugriffssteuerungsliste

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Verhindern, dass sich inaktive Anwender anmelden [Neu in Security Center 1,5]

Konfigurieren Sie diese Eigenschaft, um zu steuern, ob inaktive Anwender sich in Ihrer Instanz authentifizieren können.

Legen Sie fest `glide.authenticate.only.allow.active.user.login`Eigenschaftswert auf „wahr“ (empfohlen). Dadurch wird sichergestellt, dass die Anwender in der Tabelle „sys_user“, die als inaktiv markiert sind, sich nicht bei der Instanz anmelden und gesperrt sind.

Wenn die Einstellung auf „falsch“ konfiguriert ist, können Anwender weiterhin auf die Instanz und die Daten zugreifen, auf die sie zuvor Zugriff hatten.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.only.allow.active.user.login`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt wird, können inaktive Anwender wie ein gekündigter Mitarbeiter weiterhin auf die Instanz und alle Daten zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine

Nicht authentifizierten Zugriff auf den eingebetteten Webclient von Virtual Agent verhindern

Erfahren Sie, wie Sie konfigurieren *sn_va_web_client_app_embed*Tabelle zum Blockieren des Zugriffs nicht authentifizierter Anwender auf eingebettete Webclients.

Die UI-Seite, *sn_va_web_client_app_embed*, Ein eingebetteter Webclient für Virtual Agent, enthält die Zugriffssteuerungslisten (ACLs), die in der Tabelle „sys_public“ standardmäßig als „wahr“ markiert sind. Es wurde bestätigt, dass es Anwendungsfälle gibt, in denen öffentliche Barrierefreiheit erforderlich ist, dies ist jedoch kein Standard, um sie auf standardmäßig öffentlich zugänglich festzulegen.

Wenn der eingebettete Webclient für nicht authentifizierte Anwender nicht benötigt wird, öffnen Sie *sn_va_web_client_app_embed*Datensatz (sys_ID `04b1905473222300e985658b4cf6a7ef`) In der Tabelle „öffentliche Seiten“ [sys_public], und deaktivieren Sie die Option **Aktiv** Feld zum Deaktivieren der Seite.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	**sn_va_Web_Client_App_embed**
Konfigurationstyp	UI-Seite (sys_ui_page_list.do)
Datentyp	table
Empfohlener Wert	Die **sn_va_Web_Client_App_embed** Öffentliche Seite [sys_public] (sys_ID `04b1905473222300e985658b4cf6a7ef`) Ist nicht vorhanden oder nicht aktiv.
Standardwert	Nicht verfügbar (dies ist ein Tabellenwert)
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Es wird empfohlen, die UI-Seite zu deaktivieren, *sn_va_web_client_app_embed*, Wenn für nicht authentifizierte Anwender kein eingebetteter Webclient erforderlich ist.
Abhängigkeiten und Voraussetzungen	Keine

Beschränken Sie JSONP-Anforderungen auf vertrauenswürdige URLs [Aktualisiert in Security Center 1,3]

Geben Sie vertrauenswürdige URLs für den AngularJS $http-Service an, um JSONP-Anforderungen zuzulassen oder abzulehnen.

Erhöhen Sie die Sicherheit in Ihrer Instanz, indem Sie sicherstellen, dass nur vertrauenswürdige URLs für den Service AngularJS $http JSONP-Anforderungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zulassen/ablehnen können. JSONP-Anforderungen sind an jede URL zulässig, wenn diese Eigenschaften nicht konfiguriert und aktiviert sind.

Verwenden Sie den Wert von **angular.jsonp.inclusion_list.urls** Systemeigenschaft zum Definieren einer Liste von URLs, die vertrauenswürdig sind und diesen Zweck zulassen. Legen Sie den Wert von fest **angular.jsonp.inclusion_list.enabled** Systemeigenschaft zu **Wahr** Zum Einschränken des zulässigen JSONP auf die in aufgeführten URLs **angular.jsonp.inclusion_list.urls** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*angular.jsonp.inclusion_list.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: Mittel • CVSS-Punktzahl: 5,4 • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Aktiviert JSONP-Anforderungen für eine beliebige URL.
Abhängigkeiten und Voraussetzungen	Keine

Verhindern Sie, dass Anwender Warnungen akzeptieren, um die CSRF-Validierung zu umgehen

Reduzieren Sie das Risiko von Cross-Site Request Forgery (CSRF), indem Sie verhindern, dass Anwender Warnungen akzeptieren, um die CSRF-Validierung zu umgehen.

Aktivieren Sie die strikte Validierung des CSRF-Tokens, um zu verhindern, dass CSRF-Token (Cross Site Request Forgery) wiederverwendet werden, was CSRF-Angriffe ermöglichen kann.

Legen Sie fest **glide.security.csrf.strict.validation.mode** Systemeigenschaftswert bis **Wahr** Zum Aktivieren der strikten Validierung des CSRF-Tokens. Wenn diese Eigenschaft in Ihrer Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden ist, lautet der Standardwert **Wahr** Startet in Xanadu.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	glide.security.csrf.strict.validation.mode

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Plugin-Anwendbarkeit	Keine
Sicherheitsrisiko	Die Cross-Site-Anforderungsfälschung ist ein erhebliches Sicherheitsrisiko, das die Integrität der Instanzdaten verletzt. Ein Angreifer kann den CSRF-Angriff auf jeden Instanzanwender starten, indem er das Vertrauen des Instanzanwenders missbraucht. Mit Hilfe von Social Engineering-Angriffen kann ein Benutzer im Namen des Angreifers eine fehlerhafte Anforderung an die Instanz senden.
CVSS-Punktzahl (Common Vulnerability Scoring System)	3,7
Bewertung des Common Vulnerability Scoring System (CVSS)	Niedrig
Funktionale Auswirkung	Diese Korrektur ermöglicht einen zusätzlichen Validierungsschritt, bevor der Anwender eine Schreibanforderung an die Instanz sendet. Überprüft, ob das aktuelle CSRF-Token zuvor verwendet wurde. Wenn vorhanden, wird die Übermittlung weiterer Schreibanforderungen verhindert.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Boolean
Basissystemwert	wahr
Fallback-Wert	wahr
Empfohlener Wert	wahr

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Ausführung der unformatierten Datenbankabfrage deaktivieren [in Security Center 1,3 aktualisiert und 2,0 entfernt]

Steuert, ob ein Anwender unformatierte SQL-Abfragen für die Datenbank durchführen kann.

Th E *glide.db.allow_unsafe_dbi_execute_sql*Mit der Eigenschaft können Anwender unformatierte SQL-Abfragen für die Datenbank ausführen, die Zugriff auf Tabellen und Daten außerhalb der GlideRecord-Einschränkungen gewähren können. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist *false*, Dies ermöglicht den Aufruf von *dbi.executeStatement()*Aus einem Glide-Skripttabellen, das dazu führen kann, dass schädliche SQL-Anweisungen ausgeführt werden.

Warnung: Diese Eigenschaft ist sowohl sicher als auch keine DB-Überschreibung.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.db.allow_unsafe_dbi_execute_sql*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,2 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Diese Eigenschaft wird nicht auf festgelegt **Falsch** Aktiviert den Aufruf von *dbi.executeStatement()* Aus einem Glide-Skriptfähigen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Regeln Für Zugriffssteuerungsliste

Anwenderkommentare zu Artikeln ausblenden [Neu in Security Center 1,3]

Verwenden Sie *glide.knowman.show_user_feedback* Eigenschaft, um zu steuern, ob Feedback-Kommentare sichtbar sind.

Wenn *glide.knowman.show_user_feedback* Ist nicht auf „nie“ festgelegt, sind Feedback-Kommentare in Knowledge Base-Artikeln (KB) für Anwender mit Rollen sichtbar, die in der Glide-Eigenschaft definiert sind. *glide.knowman.show_user_feedback.roles*. Da Feedback-Kommentare vertrauliche Informationen enthalten können, möchten Sie möglicherweise nicht, dass das Feedback sichtbar ist. Wenn diese Eigenschaft nicht auf „nie“ festgelegt ist, kann es Auswirkungen auf die Vertraulichkeit haben, wenn vertrauliche Informationen im Feedback offengelegt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.knowman.show_user_feedback*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Auswahlliste
Empfohlener Wert	nie
Standardwert	onload
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft nicht auf „nie“ festlegen, können vertrauliche Informationen in Feedback-Kommentaren offengelegt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Zeigt Anwenderkommentare zu KB-Artikeln basierend auf den in der Konfiguration erwähnten Auswahlmöglichkeiten an.

Standardmäßig Authentifizierung für vom Client aufrufbare Skripteinbindungen anfordern [aktualisiert in Security Center 1,3]

Standardmäßig sind vom Client aufrufbare Skripteinbindungen, die die Sichtbarkeit nicht explizit festlegen, öffentlich. Fügen Sie bei Bedarf hinzu *glide.script.ccsi.ispublic*Eigenschaft zum Aktivieren der Datenschutzsteuerung für alle vom Client aufrufbaren Skripteinbindungen, auf die öffentliche Seiten zugreifen.

Wenn Sie diese Eigenschaft hinzufügen, müssen Sie ihren Wert auf festlegen **Falsch** , Der angibt, dass alle vom Client aufrufbaren Skripteinbindungen privat sind, und ihre Sichtbarkeit auf öffentlichen Seiten ändert.

Hinweis: Sie können die Eigenschaft mit einem Wert von nicht hinzufügen **Wahr** , Oder ändern Sie den Wert von **Falsch** Bis **Wahr** . Wenn Sie versuchen, dies zu tun, wird eine Fehlermeldung angezeigt.

Bei Bedarf können Sie die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie hinzufügen `IsPublic()` Funktion.

- Die `IsPublic()` Die Einstellung hat Vorrang vor dem *glide.script.ccsi.ispublic*Eigenschaft.
- Beispiel: Wenn Sie festlegen `IsPublic()` Bis **Wahr** In einem einzelnen Skript wird es öffentlich gemacht, was den überschreibt *glide.script.ccsi.ispublic*Eigenschaft, die alle anderen vom Client aufrufbaren Skripts privat macht.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.script.ccsi.ispublic*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Wenn Sie vom Client aufrufbare Skripteinbindungen privat machen, können Gäste, die auf öffentliche Seiten zugreifen, nicht auf die vom Client aufrufbare Skripteinbindung zugreifen. Ein nicht angemeldeter Anwender kann kein privates Skript ausführen.
Empfohlener Wert	falsch
Standardwert	falsch
Sicherheitsrisikobewertung	7,5
Funktionale Auswirkung	Wenn die vom Client aufrufbaren Skripteinbindungen als öffentlich festgelegt sind (d. h. diese Eigenschaft fehlt), können nicht authentifizierte Anwender Client-Skripts ausführen. Das

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Hinzufügen der Eigenschaft schränkt die Ausführung von Skripts durch einen nicht angemeldeten Anwender ein.
Sicherheitsrisiko	(Hoch) wenn Sie diese Eigenschaft nicht hinzufügen, enthält das clientseitige Skript Umgehungs-ACLs, was zu unbeabsichtigten öffentlichen Funktionen führen kann. Wenn das Clientskript vertrauliche Informationen bereitstellt, kann dies ein negatives potenzielles Sicherheitsrisiko darstellen.
Workaround	Wird festgelegt *glide.script.ccsi.ispublic*Eigenschaft bis **Falsch** Macht alle vom Client aufrufbaren Skripteinbindungen privat. Sie können die Datenschutzeinstellung für eine einzelne vom Client aufrufbare Skripteinbindung ändern, indem Sie hinzufügen IsPublic() Funktion. Die IsPublic Die Funktion hat Vorrang vor dem *glide.script.ccsi.ispublic*Eigenschaft. Fügen Sie der Skripteinbindung die folgende Syntax hinzu: IsPublic:function(){return[wahr/falsch];},

Verhalten der Produktionsinstanz erzwingen [aktualisiert in Security Center 1,3 Und 1,5]

Konfigurieren Sie, ob Ihre Instanz wie eine Produktionsinstanz oder eine Instanz außerhalb der Produktion behandelt werden soll.

Wenn Die *glide.installation.production*Eigenschaft ist nicht auf den empfohlenen Wert von festgelegt **Wahr** , Wird die Instanz nicht als Produktionsinstanz behandelt, sodass zboot und andere potenziell gefährliche Skripts ausgeführt werden können. Wenn Sie eine Produktionsinstanz als Instanz außerhalb der Produktion auswerten, kann dies zu Informationslecks oder Denial of Service (DoS)-Angriffen führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.installation.production*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Dieser Eigenschaftswert wird auf festgelegt **Falsch** Bewirkt, dass die Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	als Instanz außerhalb der Produktion behandelt wird, wodurch zboot und andere potenziell gefährliche Skripts ausgeführt werden können.
Abhängigkeiten und Voraussetzungen	Keine

Zugriff auf Hintergrundskript beschränken [aktualisiert in Security Center 1,3 und 2,0]

Konfigurieren Th E `glide.script_processor.admin`Eigenschaft zum Festlegen der Rolle, die für den Zugriff auf das Modul „Skripthintergrund“ erforderlich ist.

Diese Eigenschaft enthält die erforderliche Rolle für den Zugriff auf das Modul „Skripthintergrund“. Wenn `glide.script_processor.admin`lst nicht auf den empfohlenen Standardwert „Administrator“ festgelegt, können Anwender mit einer Rolle mit niedrigeren Berechtigungen Hintergrundskripts auf der Instanz ausführen. Dies führt zu einer vollständigen Umgehung des ACL-Systems, die vollständigen Zugriff auf Tabellen ermöglicht.

Stellen Sie die Eigenschaft sicher `glide.script_processor.admin`lst auf den Administrator festgelegt. Dies ist der Standardwert für Instanzen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.script_processor.admin`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Administrator
Standardwert	Administrator
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,8 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Diese Eigenschaft wird nicht auf den empfohlenen Wert festgelegt **Administrator** Ermöglicht jedem Anwender die Ausführung von Hintergrundskripts für die Instanz.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschränken Sie den Zugriff auf E-Mails mit leerer Zieltabelle

Aktivieren Sie `glide.email.email_with_no_target_visible_to_all`Eigenschaft zum Einschränken des Anwenderzugriffs auf E-Mails, es sei denn, er hat die E-Mail gesendet oder hat eine Administratorrolle.

Nicht autorisierte Anwender können auf E-Mails in der Tabelle „sys_email_list“ zugreifen, für die ein Zieldatensatz fehlt. Anstatt ACLs für E-Mail-Einträge zu erzwingen, schränkt diese Eigenschaft den Zugriff nur auf den E-Mail-Absender und Anwender mit der Administratorrolle ein.

Hinweis: E-Mails, die an die Instanz gesendet und von der Instanz empfangen werden, werden in der Tabelle „sys_email_list“ angezeigt. Nur empfangene E-Mails, die mit dem Status „Fehler“ und „ignoriert“ markiert wurden, sollten jedoch eine leere Zieltabelle haben.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.email.email_with_no_target_visible_to_all`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren	Zugriffssteuerung
Zweck	Dient zum Blockieren der Anzeige von E-Mails durch den E-Mail-Client, wenn der Anwender keinen Zugriff autorisiert.
Empfohlener Wert	falsch
Standardwert	wahr
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	Anwender können keine E-Mails mehr anzeigen, in denen die Zieltabelle leer ist, es sei denn, sie sind ein Administrator oder der Absender der E-Mail.
Sicherheitsrisiko	(Mittel) wenn die Eigenschaft nicht aktiviert ist, können nicht autorisierte Anwender auf jede E-Mail zugreifen, in der das Feld target_table leer ist.
Referenzen	Erweiterte E-Mail-Eigenschaften https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Plugin „Zugriff auf bestimmte IP-Bereiche einschränken“ [aktualisiert in Security Center 1,3]

Verwenden Sie `com.snc.ipauthenticator`Plugin zum Einschränken des Zugriffs auf bestimmte IP-Bereiche. Sofern kein öffentlicher Zugriff für die Instanz vorgesehen ist, sollten Administratoren den Zugriff auf ihre zugewiesenen IP-Netzblöcke beschränken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Wenn dieses Plugin auf „wahr“ festgelegt ist, wird der Zugriff auf bestimmte IP-Bereiche eingeschränkt. Sofern kein öffentlicher Zugriff für die Instanz vorgesehen ist, sollten Administratoren den Zugriff auf ihre zugewiesenen IP-Netzblöcke beschränken. Eine Ausschlussliste (Deny) oder eine Aufnahmeliste (Allow) von IP-Adressen kann über die IP-Adresszugriffssteuerung (ip_Access_list.do) erstellt werden.

Bevor Sie diese Eigenschaft festlegen, müssen Sie die IP-bereichsbasierte Authentifizierung (com.snc.ipauthenticator) aktivieren. `com.snc.ipauthenticator`Plugin. Weitere Informationen finden Sie unter IP-bereichsbasierte Authentifizierung Und im Abschnitt Schritte zum Konfigurieren (unten).

Stellen Sie das Plugin sicher `com.snc.ipauthenticator`Ist aktiviert, und in der Tabelle „ip_Access“ ist mindestens eine aktive IP-Zugriffsrichtlinie vorhanden.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	• Com.snc.ipauthentifikator • ip_Access
Konfigurationstyp	Systemsicherheit > Zugriffssteuerung für IP-Adressen
Kategorie	Zugriffssteuerung
Zweck	Um den Bereich der IP-Adressen, die auf die Instanz zugreifen können oder nicht, zu den Listen vertrauenswürdiger und nicht vertrauenswürdiger Domänen hinzuzufügen.
Empfohlener Wert	Aktiv
Standardwert	Keine. Dies ist ein Plugin, keine Glide-Eigenschaft. Daher ist kein Standardwert vorhanden.
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	Für dieses Korrekturelement werden vom Kunden abgelehnte IP-Bereiche verwendet. Keine Auswirkung, da der Kunde die Zielliste definiert.
Sicherheitsrisiko	(Niedrig) unnötiges Risiko für die Zielinstanz im Internet sollte mithilfe der IP-Zugriffssteuerungsfunktion eingeschränkt werden.
Referenzen	IP-bereichsbasierte Authentifizierung

Schritte zum Konfigurieren

1. Stellen Sie sicher, dass das Plugin „com.snc.ipauthenticator“ aktiv ist.
2. Navigieren zu **Systemsicherheit** > **IP-Adressen-Zugriffssteuerung**an.
3. Klicken Sie Auf **Neu** Dient zum Erstellen einer Ausschlussliste (Deny) oder einer Aufnahmeliste (Allow) von IP-Adressen.
4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf Knowledge Bases beschränken [Neu in Security Center 1,3]

Die *glide.knowman.block_access_with_no_user_criteria*Die Eigenschaft wird verwendet, um den Lese-/Schreibzugriff von Anwendern auf wissensbasierte Artikel zu steuern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.knowman.block_access_with_no_user_criteria*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 9,1 • CVSS-Punktzahl: Kritisch • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt ist, kann jeder Anwender eine KB lesen und dazu beitragen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Verweigert den Zugriff auf eine Knowledge Base, wenn entweder „kann lesen“ oder „kann beitragen“ nicht angegeben ist.

Berechtigungen für CMDB-Modell beschränken [aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie *csm_cmdb_model.customer_visible_flag*Systemeigenschaft, um den Kundenzugriff auf Daten in der Tabelle „Produktmodelle“ als zusätzliche Zugriffssteuerung für das CMDB-Modell zu beschränken.

Legen Sie fest *csm_cmdb_model.customer_visible_flag*Eigenschaft bis **Wahr** So aktivieren Sie das Feld „sichtbar für Kunden“ für die unten aufgeführten Tabellen:

- Produktmodelltabelle [cmdb_model]
- Tabelle „Softwaremodelle“ [cmdb_Software_Product_model]
- Anwendungsmodelltabelle [cmdb_Application_Product_model]
- Tabelle „Verbrauchsgütermodelle“ [cmdb_Consumable_Product_model]
- Tabelle „Facility-Modelle“ [cmdb_Facility_Product_model]
- Tabelle „Hardwaremodelle“ [cmdb_Hardware_Product_model]

Diese Eigenschaft wird als festgelegt **Wahr** Blendet standardmäßig alle cmdb_model-Werte aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie die Eigenschaft auf fest **Falsch** Dient dazu, die Spalte/Atrribute „Customer_visible“ in „cmdb_model“ nicht zu berücksichtigen Tabelle Und sich auf die Basen-ACLs cmdb_model zu verlassen, die für sn_esm_user zugänglich sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`csm_cmdb_model.customer_visible_flag`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Wenn auf festgelegt di **Wahr** , Verwendet das System die Einstellung im Feld sichtbar für Kunden, um den Zugriff auf Produktmodelldaten im Kundenserviceportal zu bestimmen.
Empfohlener Wert	wahr
Standardwert	falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Mittel) jeder Anwender mit der Rolle sn_esm_user und sofort einsatzbereiten ACLs kann Berechtigungen für das CMDB-Modell haben. **Hinweis:** Diese Rolle wird tendenziell externen Anwendern gewährt. Externe Anwender könnten widerwillig Berechtigungen für das CMDB-Modell erhalten.
Referenzen	Zugriff auf Produktmodelldaten im Customer Service Portal beschränken

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Beschränken Sie den nicht authentifizierten Zugriff auf Anhänge

Verwenden Sie *`glide.image_provider.security_enabled`*Eigenschaft zur Steuerung der Sicherheitseinstellungen für Bilder. Wenn auf festgelegt **Wahr** , Bilder sind nur für authentifizierte und autorisierte Anwender sichtbar. Wenn auf festgelegt **Falsch** , Bilder sind für jeden mit einer URL zum Anhang sichtbar.

Sichern Sie die Images in Ihrer Instanz, um das Leck vertraulicher Informationen zu verhindern. Images in Ihrer Instanz sind über urls zugänglich, die auf enden `.lix` .

Legen Sie fest **glide.image_provider.security_enabled** Systemeigenschaft zu **Wahr** Um den Zugriff auf Ihre Bilder über diese URLs zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Diese Eigenschaft wird für Bilder aus der Anhangstabelle nicht berücksichtigt, wenn die Ursprungstabelle eine der folgenden ist:

- Schreibwaren [sysevent_email_style]
- Abschnitte der Willkommensseite [sys_Home]
- Systemeigenschaften [sys_properties]

Die Einschränkung sollte für nicht authentifizierte Anwender angewendet werden, da einige Anhänge vertrauliche Informationen enthalten können.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.image_provider.security_enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Verhindert den nicht authentifizierten Zugriff auf Anhänge, wenn sie mit gerendert werden `.Iix` Format.
Empfohlener Wert	wahr
Standardwert	falsch
Funktionale Auswirkung	Keine signifikanten Auswirkungen auf die Funktionalität. Die Anwender-Experience kann etwas beeinträchtigt werden, da der Anwender, der früher direkt auf .iix zugegriffen hat, eine Authentifizierung durchlaufen muss.
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • Sicherheitsrisikodetails: Einschränkung muss für nicht authentifizierte Anwender angewendet werden, da einige Anhänge vertrauliche Informationen enthalten können.
Referenzen	Verwalten von Anhängen Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Zugriff auf anwenderdefinierte Journaleinträge beschränken [in Security Center 1,3 aktualisiert und 2,0 entfernt]

Verwenden Sie `glide.live_feed.custom_journal.acl_check_enabled`Eigenschaft, die ACLs in anwenderdefinierten Journalfeldern berücksichtigt.

Wenn `glide.live_feed.custom_journal.acl_check_enabled`lst nicht auf den empfohlenen Wert „wahr“ festgelegt, dann müssen alle Anwender alle Journaleinträge in der Lebens-Feed-Funktion anzeigen können. Wenn Sie die Eigenschaft auf „wahr“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

festlegen, werden ACLs in anwenderdefinierten Journalfeldern berücksichtigt, was eine gute Funktion ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.live_feed.custom_journal.acl_check_enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Um zu steuern, welche Anwender welche Journaleinträge basierend auf ACLs sehen.
Empfohlener Wert	wahr
Standardwert	wahr
Konfigurationstyp	Boolescher Wert.
Sicherheitsrisiko	(Mittel) bei „wahr“ werden nur die anwenderdefinierten Journaleinträge, die ACL übergeben, im Live-Feed angezeigt. Andernfalls können alle Anwender alle Journaleinträge anzeigen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Lesezugriff für Flow-Kontext einschränken [Neu in Security Center 1,5]

Verwenden Sie `com.snc.process_flow.reporting.require_flow_access`Eigenschaft, die erzwingt, ob ein Anwender eine zusätzliche Zugriffsprüfung zum Lesen einer Flow-Prüfung benötigt.

Wenn `com.snc.process_flow.reporting.require_flow_access`Die Eigenschaft ist auf den empfohlenen Wert „wahr“ festgelegt. Es gibt eine zusätzliche Zugriffsprüfung für einen Anwender, der versucht, einen Flow-Kontext zu lesen. Wenn diese Eigenschaft auf „falsch“ festgelegt ist, kann es zu einer geringfügigen Offenlegung von Informationen kommen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.snc.process_flow.reporting.require_flow_access`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft auf „falsch“ festlegen, wird ihr vorhandenes

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Verhalten beibehalten. Wenn Sie diese Eigenschaft auf „wahr“ festlegen, wird die hinzugefügte Sicherheitsebene des Lesezugriffs erzwungen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft aktiviert ist, wird die Sicherheit für das Lesen von Flow-Kontextdatensätzen erhöht. Die Instanz erzwingt, dass ein Anwender, der versucht, den Flow-Kontext zu lesen, auch Lesezugriff auf den übergeordneten Flow hat.

Identitätswechsel auf Administrator beschränken [Neu in Security Center 2,0]

Die `glide.sys.permissive.impersonate`Die Eigenschaft kann verwendet werden, um zu verhindern, dass nicht-Administratorrollen die Identität anderer Anwender annehmen.

Wenn `glide.sys.permissive.impersonate`Die Eigenschaft ist auf „falsch“ festgelegt. Nur Anwender mit der Administratorrolle können die Identität anderer Anwender annehmen. Wenn diese Eigenschaft auf „wahr“ festgelegt ist, können Anwender möglicherweise Anwendungskomponenten verwenden, die APIs zur Identitätswechsel verfügbar machen, um die Identität eines Anwenders mit höheren Berechtigungen anzunehmen. Dies kann zu nicht autorisiertem Zugriff führen, wenn diese Anwendungskomponenten falsch konfiguriert sind, da nicht-Administratoranwender auf die Funktion zum Identitätswechsel zugreifen können.

Sie können die Eigenschaft auf den nicht-Standardwert festlegen, wenn nicht-Administratoranwender die Möglichkeit haben müssen, die Identität anderer Anwender anzunehmen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sys.permissive.impersonate`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,7 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „falsch“ festgelegt wird, kann ein nicht-Administrator-Anwender Anwendungskomponenten verwenden, die APIs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	verfügbar machen, sodass er die Identität eines Anwenders mit höheren Berechtigungen annehmen kann.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Nicht-Administrator-Anwender können mit einigen Anpassungen an andere Skripts und UI-Seiten auf Identitätswechsel-Funktionen zugreifen. Es ist jedoch wichtig, sicherzustellen, dass nur die richtigen Anwender Zugriff auf diese Funktionen erhalten. **Hinweis:** Wenn *glide.sys.permissive.impersonate*Ist auf „wahr“ festgelegt, nicht-Administrator-Anwender mit *impersonate*Die Rolle kann weiterhin die Identität annehmen.

Plugin „Security Jump Start“ aktivieren (ACL-Regeln) [aktualisiert in Security Center 1,3]

Aktivieren Sie den Sicherheits-Jump-Start (ACL-Regeln) (Com.snc.System_Security *com.snc.system_security*) Plugin zum Erstellen mehrerer wichtiger ACLs, die die Zugriffssteuerungen für einige der Schlüsselsystemtabellen in validieren ServiceNow AI Platform.

Diese Regeln bieten einen Starthilfe für die Sicherung vieler Systemtabellen, sodass eine Organisation eine Instanz leichter in die Produktion bringen kann. Das Plugin „Security Jump Start“ (ACL-Regeln) wird automatisch auf allen neuen Instanzen installiert.

Weitere Informationen

Attribut	Beschreibung
Plugin-ID	*com.snc.system_security*
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Aktivieren Sie das Plugin „Security Jump Start“ (ACL-Regeln), um eine ordnungsgemäße Sicherheits-Compliance zu erreichen. Es stellt einige grundlegende ACLs bereit, die Systemtabellen zuerst sichern, anstatt sie manuell für jede Systemtabelle zu erstellen, die mit der Standardbereitstellung einer Instanz geliefert wird. Diese ACLs sind hilfreich, wenn die neu erstellte Instanz schnell in die Produktion gehen muss.
Empfohlener Wert	Aktiv
Standardwert	Keine. Dies ist ein Plugin, keine Glide-Eigenschaft, daher ist kein Standardwert vorhanden. Das Plugin wird standardmäßig auf zBoot installiert (Zurücksetzungen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	Wenn dieses Plugin ohne Audit der vorhandenen ACLs in der Instanz installiert wird, hat dies erhebliche Auswirkungen auf die Funktion. Kundenkontakt und Definitionen sind erforderlich, bevor die Korrektur erfolgen kann.
Sicherheitsrisiko	(Hoch) die Zugriffssteuerung muss erzwungen werden, um den unbeabsichtigten Zugriff auf die Instanz zu sperren. ACL-Starthilferegeln wurden erstellt, um einen Ausgangspunkt für die Sicherung vieler Systemtabellen zu bieten, um es einer Organisation zu erleichtern, schnell in die Produktion zu gehen.
Referenzen	Sicherheits-Starthilfe: ACL-Regeln

Schritte zum Konfigurieren

Wenn dieses Plugin in Ihrer Instanz nicht aktiviert ist, wenden Sie sich an ServiceNow Support. Wenn Sie das Plugin zu diesem Zeitpunkt aktivieren, kann dies den Sicherheitszugriff auf Tabellen ändern, die bereits in einer Produktionsumgebung verwendet werden. Wenn ein Administrator an den neuen ACL-Regeln interessiert ist, die das Plugin bereitstellt, können Sie bei Bedarf eine oder mehrere davon manuell in einer vorhandenen Instanz erstellen. Diese Liste von ACLs kann in diesem Fall als Richtlinie verwendet werden.

Verwendung des Vorgangs „mehrere sichere Einfügungen“ in der Importsatz-API [Neu in Security Center 1,3]

Verwenden Sie `com.glide.import_set_api.insert_multiple_optimize`Eigenschaft, um zu steuern, ob `GlideRecordSecure` Oder `GlideRecord` Wird für den Vorgang „mehrere einfügen“ in der Importsatz-API verwendet.

Wenn `com.glide.import_set_api.insert_multiple_optimize`Wird dann auf den empfohlenen Wert „falsch“ festgelegt `GlideRecordSecure` Wird zum Einfügen von Datensätzen verwendet, und Zugriffssteuerungslisten (ACLs) auf Tabellenebene werden ausgewertet. Wenn diese Eigenschaft auf „wahr“ festgelegt ist, `GlideRecord` Wird zum Einfügen von Datensätzen verwendet, und ACLs auf Tabellenebene werden nicht ausgewertet. Darüber hinaus müssen Sie sicherstellen, dass die Importsatz-API „mehrere REST-Endpunkte einfügen“ (sys_ID: 3101b770ff2211105cf343d0653bf182) aktiv ist und dass Anwender die Rolle „Import_Transformer“ haben.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.import_set_api.insert_multiple_optimize`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf „falsch“ festgelegt ist, kann ein Anwender mit geringen Berechtigungen Daten in Tabellen einfügen, die außerhalb des Bereichs seiner privilegierten Rollen liegen.
Umkehrbares Verhalten	Sowohl sichere Überschreibung als auch keine DB-Überschreibung.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft optimiert die Leistung der Importsatz-API, indem GlideRecord zum Speichern von Daten verwendet wird. Wenn der Parameter festgelegt ist, muss ein Integrationsanwender über die Rolle „Import_Transformer“ verfügen, um auf die API zuzugreifen.
Referenzen	https://developer.servicenow.com/blog.do?p=/post/gliderecord-vs-gliderecordsecure

Strikte Sicherheit der SOAP-Anforderung erzwingen [aktualisiert in Security Center 1,3]

Verwenden Sie *`glide.soap.strict_security`*Eigenschaft zum Erzwingen der Webservicesicherheit.

Diese Eigenschaft verwendet eine Kombination aus:

- Herausforderung/-Antwort für Standardauthentifizierung über das HTTP-Protokoll und
- Zugriffssteuerungen auf Systemebene in Plugin „Security Jump Start“ aktivieren (ACL-Regeln) [aktualisiert in Security Center 1,3].

Wenn Sie diese Eigenschaft auf festlegen **Wahr** , Führt die folgenden Aktionen aus:

- Wenn der Anwender über die entsprechende Rolle verfügt, um den Vorgang auszuführen, überprüft er die eingehende SOAP-Anforderung für die Rollenautorisierung zur Validierung. Sie tritt während SOAP-Webservice-Aufrufen/-Anforderungen auf, die für gestellt werden ServiceNow AI Platform Tabellen beim Ausführen von ERSTELLUNGS-, LESE-, UPDATE- oder LÖSCHVORGÄNGEN.
- Überprüft die ACLs auf Systemebene beim Abrufen von Daten in Form von SOAP-Daten in der Tabelle.
- Überprüft die ACLs auf Feldebene auf CRUD-Vorgänge, die für ein Feld der Tabelle ausgeführt werden.

ACL-Prüfungen sind nur für Standard-Tabellen-API-Aufrufe und nicht für Webservices abgeschlossen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*`glide.soap.strict_security`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Zugriffssteuerung
Standardwert	wahr
Empfohlener Wert	wahr
Funktionale Auswirkung	Diese Korrektur erzwingt die Zugriffssteuerung auf Systemebene beim Abrufen von Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz. Wenn derzeit Anwender auf diese Daten zugreifen, sind sie auf Grundlage der ACL-Regeln eingeschränkt/berechtigt, auf die Daten zuzugreifen. Informationen zu den Standardrollen, die Zugriff auf die SOAP-Daten haben, finden Sie unter SOAP Web Service .
Sicherheitsrisiko	(Mittel) ohne entsprechende Autorisierung, die für die eingehenden SOAP-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Strikte Sicherheit für eingehende SOAP durchsetzen SOAP Web Service

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Erforderliche jms-Connection Factorys [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]

Die *mid.property.jms.command.allowed_factory_names*Die Eigenschaft steuert die Java Messaging Service (JMS) Connection Factorys, die der MID-Server verwenden kann.

Er ist für einige ausgewählte Fabriken vorgesehen, die von Plugins für JMS-Aktivitäten oder -Aktionen benötigt werden. Das Einbeziehen zusätzlicher Fabriken könnte ein Schritt in einer Angriffskette für Schwachstellen wie die JDNI-Einfügung sein, die auf Fähigkeiten basieren, die ein Angreifer in zulässigen Fabriken nutzen kann. Um die Möglichkeit einer ausgenutzten Schwachstelle zu verhindern, schließen Sie Fabriken nicht über die erforderlichen Standardwerte hinaus ein.

Um dieses Sicherheitsrisiko zu beheben, überprüfen Sie die Liste der Namen, die für die MID-Eigenschaft bereitgestellt werden. *mid.property.jms.command.allowed_factory_names*. Stellen Sie sicher, dass zusätzliche Java-Factory-Namen erforderlich sind, die über den Standard von ConnectionFactory, QueueConnectionFactory und TopicConnectionFactory hinausgehen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*mid.property.jms.command.allowed_factory_names*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Empfohlener Wert	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,1 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn der MID-Server (*com.glideapp.agent*) Plugin aktiv ist. Überprüfen Sie die Liste der Namen, die für die MID-Eigenschaft bereitgestellt werden *mid.property.jms.command.allowed_factory_names*. Stellen Sie sicher, dass zusätzliche Fabriknamen erforderlich sind, die über die Standardwerte ConnectionFactory, QueueConnectionFactory und TopicConnectionFactory hinausgehen.
Abhängigkeiten und Voraussetzungen	Keine

Globale App-Entwicklung nach Rolle einschränken [Neu in Sicherheitscenter 2,0]

Verwenden Sie *sn_g_app_creator.allow_global*Eigenschaft, um zu steuern, welche Anwender Anwendungen im globalen Bereich mit dem geführten Anwendungsersteller erstellen können.

Wenn *sn_g_app_creator.allow_global*lst auf den empfohlenen Wert „falsch“ festgelegt, benötigen Anwender *sn_g_app_creator.global*Rolle zum Erstellen von Anwendungen im globalen Bereich. Umgekehrt kann jeder Anwender mit der grundlegenden Rolle „sn_g_App_Creator.App_Creator“ globale Anwendungen erstellen, wenn er auf den unsicheren Wert „wahr“ festgelegt ist. Globale Anwendungen verfügen nicht über einen Umfangsschutz, sodass Entwickler Zugriff auf umfangreiche Funktionen und Funktionen haben, die über bestimmte Umfänge hinausgehen. Die Beschränkung der globalen Anwendungsentwicklung auf Anwender mit der zusätzlichen Rolle entspricht dem Prinzip der geringsten Berechtigung.

Hinweis: Diese Eigenschaft ist in Ihrer Instanz nicht vorkonfiguriert. Sie müssen diese Eigenschaft manuell entsprechend den Anforderungen Ihrer Organisation erstellen und konfigurieren.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_g_app_creator.allow_global*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,3 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt wird, kann jeder Anwender mit den s zugelassen werden `n_g_app_creator.app_creator`Rolle zum Erstellen globaler Anwendungen, die nicht dem Prinzip der geringsten Berechtigung entspricht.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Die API (/api/now/Templates) wurde erweitert, um die ACL und die Eigenschaft „Globale Anwendung erstellen“ zu validieren.

Überprüfe überflüssige explizite Rollenzugriffssteuerungsbedingungen [entfernt in Security Center 1,5]

Das Plugin „Explicit Roles“ wird empfohlen, dass alle Anwender entweder über die Rolle „snc_internal“ für den Zugriff auf interne Ressourcen oder über die Rolle „snc_external“ für den Zugriff auf externe Ressourcen verfügen.

Nach der Installation dieses Plugins wird allen vorhandenen Anwendern die Rolle „snc_internal“ zugewiesen, und vorhandene Zugriffssteuerungslisten (ACLs) werden mit den Rollenbedingungen gefüllt. Aufgrund der Automatisierungslogik oder des Eingreifens eines Instanzadministrators werden die Rollen „snc_internal“ oder „snc_external“ möglicherweise fälschlicherweise einer ACL hinzugefügt, die bereits eine strengere Rollenanforderung enthält. Da die ACL-Rollenauswertung für jeden Anwender übergeben wird, der eine Rolle enthält, die einer ACL zugeordnet ist, kann das Hinzufügen von snc_internal oder snc_external für den beabsichtigten Zweck einer ACL zu weit gefasst sein. Dies kann zu Datenverlusten führen, wenn einem Anwender mit geringen Berechtigungen Zugriff über die ACL gewährt wird.

Beispielsweise wäre es nicht erforderlich, dass sowohl die Rolle snc_internal als auch die Rolle admin derselben ACL innerhalb einer Tabelle zugeordnet werden. Die ACL soll Administratoren Zugriff gewähren. In diesem Fall ist die Rolle „snc_internal“ ein Fehler. Oder die ACL soll allen snc_internal-Anwendern Zugriff gewähren, was die Administratorrolle überflüssig macht. Wenn das Plugin „Explicit Roles“ installiert ist, überprüfen Sie die ACLs, die eine Rollenbedingung für „snc_internal“ oder „snc_external“ enthalten und gleichzeitig eine Bedingung für eine andere Rolle enthalten. Wenn die Rollen für einen bestimmten Anwendungsfall funktionieren können, sollte das Ergebnis regelmäßig überprüft werden.

Wichtig: Diese Härtungseinstellung wird im nächsten Store-Patch-Release des Security Center v1.5 und in zukünftigen Versionen entfernt. Eine Instanz-Scan-Suite mit der Bezeichnung „Suite für ACL-Konfigurationsprüfung für explizite Rollen“ ist im Washington-Release verfügbar. Wir empfehlen Ihnen, die Ergebnisse dieses neuen Instanzscans zu überprüfen.

Gastanwender für SOAP-Anforderungen festlegen [aktualisiert in Security Center 1,3 und 2,0]

Konfigurieren Sie diese Eigenschaft, um die Zugriffsebene nicht authentifizierter SOAP-Anforderungen zu steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Eigenschaft steuert die Zugriffsebene nicht authentifizierter SOAP-Anforderungen. Wenn er nicht auf den empfohlenen Wert von festgelegt ist `soap.guest`, Oder ist auf einen Anwender mit eingeschränkten Berechtigungen festgelegt, dann werden SOAP-Anforderungen im Namen des Anwenders ausgeführt. Wenn diese Eigenschaft leer ist, wird nicht authentifizierter Zugriff auf Administrator- oder Wartungsebene-Vorgänge aktiviert, wodurch alle Sicherheitskontrollen in der Instanz aufgehoben werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.soap.guest_user`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	SOAP.Gast
Standardwert	SOAP.Gast
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft auf „leer“ festlegen, wird nicht authentifizierter Zugriff auf Administrator- oder Wartungsebene-Vorgänge aktiviert.
Abhängigkeiten und Voraussetzungen	Keine

Öffentlichen Zugriff auf Favoriten deaktivieren [aktualisiert in Security Center 1,3 und 2,0]

Verwenden Sie `glide.ui.magellan.favorites.allow_public`Um anzugeben, ob nicht authentifizierte Anwender sehen dürfen **Favoriten** Im Navigator.

Öffentlicher Zugriff auf Favoriten ist konform, wenn `glide.ui.magellan.favorites.allow_public`Ist auf festgelegt **Falsch** .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.magellan.favorites.allow_public`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Steuert, ob nicht authentifizierte Anwender sehen dürfen **Favoriten** Im Navigator.
Typ	wahr/falsch
Empfohlener Wert	`false`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsabhängigkeiten	Festlegen *glide.ui.magellan.favorites.allow_public*Bis **Falsch** .
Funktionale Auswirkung	(Mittel) das Aktivieren dieser Eigenschaft dient als Schutzebene vor nicht autorisierten Anwendern.
Sicherheitsrisiko	(Mittel) wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie die Favoritenoption

Plugin für SNC-Zugriffssteuerung aktivieren [aktualisiert in Security Center 1,3]

Aktivieren Sie das Plugin „SNC-Zugriffssteuerung“ (com.snc.snc_Access_Control), um den Zugriff auf Ihre Instanzen durch zu steuern Kundenservice und Support Personal.

Verhindern ServiceNow Kundenservice- und Supportmitarbeiter können ohne Ihre ausdrückliche Berechtigung auf die Instanzen zugreifen, indem das Plugin „SNC Access Control“ (com.snc.snc_Access_Control) aktiviert wird. Obwohl der gesamte Zugriff auf Ihre Instanz geprüft wird, möchten Sie diesen Zugriff möglicherweise steuern. Diese Zugriffsmethode ist vollständig auditierbar und wird nachverfolgt.

Hinweis: Andere autorisiert ServiceNow Betriebspersonal in ihrer Eigenschaft zur Unterstützung und Verwaltung des Produkts müssen administrative Aktionen für die zugrunde liegende Infrastruktur ausführen. Das Aktivieren dieses Plugins kann sich auf Support-Servicelevel und das Verfügbarkeits-SLA auswirken. Das Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeiter Zugriff auf Ihre Instanz erhalten.

Aktivieren Sie das Plugin „SNC Access Control“ (com.snc.snc_Access_Control), um den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Berechtigung zu beschränken. Weitere Informationen zu dieser Funktion finden Sie unter ServiceNow-Zugriffssteuerung. Informationen zur Aktivierung finden Sie unter Aktivieren ServiceNow Zugriffssteuerung

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	*com.snc.snc_access_control*
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Zugriffssteuerung
Zweck	Verbietet Kundenservice und Support Mitarbeiter, die nicht auf die Instanz zugreifen
Empfohlener Wert	Aktiv
Standardwert	Keine. Dies ist ein Plugin, keine Glide-Eigenschaft, daher ist kein Standardwert vorhanden. Das Plugin ist nicht standardmäßig installiert.
Erforderliche Rolle	Der Kundenadministrator kann dieses Plugin nicht aktivieren. Sie muss explizit angefordert werden, da zum Aktivieren des Plugins erhöhte Berechtigungen erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisikobewertung	3.3
Funktionale Auswirkung	Wenn dieses Plugin inaktiv ist, alle Kundenservice und Support Mitarbeiter können auf die Instanz des Kunden zugreifen. Durch Aktivieren des Plugins kann der Kunde den Zugriff auf autorisierte beschränken Kundenservice und Support Nur Mitarbeiter.
Sicherheitsrisiko	(Hoch) unnötiges Risiko des Instanzzugriffs für eine breitere Personengruppe.
Referenzen	ServiceNow-Zugriffssteuerung

Schritte zum Konfigurieren

1. Um das Plugin anzufordern, führen Sie die Schritte unter aus Aktivieren ServiceNow Zugriffssteuerung. Kunden müssen das Plugin „SNC-Zugriffssteuerung“ (com.snc.snc_Access_Control) von HI anfordern.
2. Um die SNC-Zugriffssteuerung zu aktivieren, führen Sie die Schritte in aus Konfigurieren ServiceNow Zugriffssteuerung. Konfigurieren Sie einen Zugriffssteuerungsdatensatz, um einen oder mehrere anzugeben Kundenservice und Support Mitarbeiter, die über die Berechtigung zur Anmeldung bei Ihrer Instanz verfügen.

Dokumentklassifizierung verwenden, um öffentlich zugängliche Dokumente einzuschränken [Neu in Security Center 7,0]

Steuern Sie den öffentlichen Zugriff auf permalink verknüpfte Dokumente mithilfe von Systemeigenschaften.

Hinweis: Diese Härtungseinstellung ist nicht Teil der Härtungsbasis. Sie wird nicht auf den Sicherheitscenter-Härtungsseiten angezeigt und wirkt sich auf Ihre Härtungspunktzahl aus.

Standardmäßig enthält das Plugin „Dokumentverwaltung“ diese Klassifizierungen:

- **Öffentlich**
- **restricted**
- **confidential**
- **Keine** (Keine Klassifizierung angegeben)

Verwenden Sie `com.snc.documents.permalink.allowed_classifications`Dient zum Erstellen einer Liste von Dokumentklassifizierungen. Dokumente unter diesen Klassifizierungen (und Dokumente ohne Klassifizierung) sind für nicht authentifizierte Anwender mit einem entsprechenden Link öffentlich zugänglich.

Verwenden Sie diese Eigenschaft, um den öffentlichen Zugriff auf Dokument-Permalinks zu steuern. Zuvor waren diese Links für alle Personen mit dem Link öffentlich zugänglich. Der Wert dieser Eigenschaft hängt von Ihren spezifischen Anforderungen ab. Möglicherweise haben Sie zusätzliche anwenderdefinierte Dokumentkategorien, die dieser Eigenschaft hinzugefügt werden müssen, um öffentlichen Zugriff zu ermöglichen.

Legen Sie fest `com.snc.documents.permalink.allowed_classifications`Eigenschaftswert für eine kommagetrennte Liste von Dokumentklassifizierungen. Dokumente mit diesen Klassifizierungen sind für nicht authentifizierte Anwender öffentlich zugänglich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn diese Eigenschaft nicht in der Tabelle „Systemeigenschaften“ [sys_properties] vorhanden ist, wird standardmäßig eine leere Liste verwendet. In diesem Fall sind nur Dokumente ohne Klassifizierung für nicht authentifizierte Anwender öffentlich zugänglich. Der Standardwert dieser Eigenschaft ist **Öffentlich** , Bedeutet, dass nur Dokumente klassifiziert als **Öffentlich** Oder Dokumente ohne Klassifizierung sind nicht authentifizierten Anwendern zugänglich.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.snc.documents.permalink.allowed_classifications`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolgenliste
Empfohlener Wert	Öffentlich
Standardwert	Öffentlich
Fallback-Wert	<empty>
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Wenn dieser Eigenschaft eine Dokumentkategorie hinzugefügt wird, die Dokumente enthält, die nicht öffentlich zugänglich sein sollen, können vertrauliche Informationen für nicht authentifizierte Anwender zugänglich gemacht werden.
Funktionale Auswirkung	Wenn dieser Eigenschaft keine Dokumentkategorie hinzugefügt wird, die Dokumente enthält, die öffentlich zugänglich sein sollen, verhindert dies den Zugriff auf diese Dokumente.
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Abfrage-ACLs für Glide DB-Funktionen validieren [Neu in Security Center 7,0]

Steuert, ob Abfrage-ACLs mithilfe von Systemeigenschaften auf Glide DB-Funktionen angewendet werden.

Wenn `glide.db.encoded_query.check_function_field_query_acls`Systemeigenschaft ist auf festgelegt **Wahr** , Abfrage-ACLs (query_Range und query_match) werden standardmäßig für diese Glide DB-Funktionen validiert:

- Glidefunktion:Position
- Glidefunktion:substring
- Glidefunktion:Concat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Glidefunktion:zusammenfügen
- Glidefunktion:length

Um diese Abfrage-ACLS für zusätzliche Funktionen zu validieren, fügen Sie diese Funktionen zu hinzu *glide.db.encoded_query.force_query_range_on_functions*Systemeigenschaft.

Legen Sie fest *glide.db.encoded_query.check_function_field_query_acls*Systemeigenschaft zu **Wahr** , Oder bestätigen Sie, dass sich die Eigenschaft nicht in der Liste „Systemeigenschaften“ [sys_properties] befindet.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	• *glide.db.encoded_query.check_function_field_query_acls* • *glide.db.encoded_query.force_query_range_on_functions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	• Boolean • Zeichenfolgenliste
Empfohlener Wert	• wahr • Glidefunktion:Position, Glidefunktion:substring, Glidefunktion:concat, Glidefunktion:Coalesce, Glidefunktion:length
Standardwert	• wahr • Glidefunktion:Position, Glidefunktion:substring, Glidefunktion:concat, Glidefunktion:Coalesce, Glidefunktion:length
Fallback-Wert	• wahr • Glidefunktion:Position, Glidefunktion:substring, Glidefunktion:concat, Glidefunktion:Coalesce, Glidefunktion:length
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Wenn *glide.db.encoded_query.check_function_field_query_acls*S

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	ist vorhanden und nicht auf einen Wert von festgelegt **Wahr** , Kann ein angemeldeter Anwender Daten möglicherweise blind ableiten, was zur Offenlegung vertraulicher Informationen führt.
Funktionale Auswirkung	Anwender erwarten möglicherweise Werte aus Funktionsfeldern, werden jedoch aufgrund von ACLs blockiert, die für die Funktionsfelder erzwungen werden.
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

API und Webservice

Die API- und Webservicekategorie stellt sicher, dass Anwendungen über die entsprechende Authentifizierung, Autorisierung und Sitzungsverwaltung verfügen, validiert alle Eingaben, die eine Vertrauensgrenze überschreiten, und enthält Sicherheitskontrollen für alle API-Typen.

Bestimmte Steuerungen in dieser Kategorie adressieren die Validierung der Eingabe nach Servicetyp, z. B. XDS-Schemavalidierung für SOAP-Webservices oder Denial of Service-Schutz für GraphQL-APIs.

SOAP-Inhaltstyp validieren [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.soap.require_content_type_xml`Eigenschaft zum Aktivieren der Validierung eines Inhaltstyps als Text/XML und zum Schutz vor ungültigen SOAP-Anforderungen.

- Wenn auf festgelegt **Wahr** , ServiceNow AI Platform Validiert den Inhaltstyp als Text/XML und schützt vor ungültigen SOAP-Anforderungen.
- Wenn auf festgelegt **Falsch** , Ein beliebiger Inhaltstyp-Wert ist zulässig.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.soap.require_content_type_xml`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Schützen Sie sich vor ungültigen SOAP-Anforderungen
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Diese Korrektur ermöglicht die Validierung des SOAP-Inhaltstyps für alle eingehenden SOAP-Anforderungen. • Wenn Sie für eingehende Anforderungen einen anderen Inhaltstyp als Text/XML verwenden, kann dies zu einem potenziellen Fehler bei SOAP-Transaktionen führen. • Wenn Sie nicht den richtigen MIME-Typ verwenden, kann dies die Integrationen von Drittparteien beeinträchtigen.
Sicherheitsrisiko	(Mittel) beim Akzeptieren eingehender SOAP-Anforderungen wird die entsprechende Validierung durchgeführt, um sicherzustellen, dass der relevante Inhaltstyp als Teil der Anforderung definiert wird. Sie schränkt die ungültigen SOAP-Antworten ein, die als Sicherheitsrisiko betrachtet werden können.
Referenz	Inhaltstypen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung für PDF-Anforderungen anfordern [Aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.pdf`Eigenschaft, die angibt, ob eingehende PDF-Anforderungen eine Standardauthentifizierung erfordern sollen.

Stellen Sie die Eigenschaft sicher `glide.basicauth.required.pdf`lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.pdf`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für PDF-Anforderungen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	7,5
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird ausgeführt, während Daten aus Tabellen/Seiten in Form von PDF-Daten in der Instanz abgerufen werden. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Webservice-Importsätze .
Sicherheitsrisiko	(Hoch) ohne entsprechende Autorisierung, die für die eingehenden PDF-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Authentifizierung für Ereignismanagement-HTTP-Prozessor anfordern [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0]

Erfahren Sie, wie Sie eine sichere Standardauthentifizierung für eingehende Anforderungen des Amazon Simple Notification Service (SNS) einrichten können, wenn das Ereignismanagement-Plugin (`com.glideapp.itom.snac`) Ist aktiviert.

Wenn `glide.basicauth.required.evtmgmthttpprocessor`Eigenschaft ist nicht auf den empfohlenen Wert von festgelegt **Wahr** , Und das Ereignismanagement-Plugin (`com.glideapp.itom.snac`) Aktiv ist, ist keine Standardauthentifizierung für alle eingehenden Anforderungen des Amazon Simple Notification Service (SNS) erforderlich. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.

Um dieses Sicherheitsrisiko zu beheben, stellen Sie sicher, dass `glide.basicauth.required.evtmgmthttpprocessor`Ist auf festgelegt **Wahr** Und das `com.glideapp.itom.snac`Ist aktiv.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.basicauth.required.evtmgmthttpprocessor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	API und Webservice

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 7 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Keine Einstellung `glide.basicauth.required.evtmgmthttpprocessor`Auf den empfohlenen Wert „wahr“ festgelegt und wird nicht aktiviert `com.glideapp.itom.snac`Das Plugin bewirkt, dass die Standardauthentifizierung für eingehende SNS-Anforderungen nicht aktiviert wird. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • Zugriffssteuerung
Funktionale Auswirkung	Wenn `glide.basicauth.required.evtmgmthttpprocessor`Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, und wenn das Ereignismanagement-Plugin (com.glideapp.itom.snac) aktiv ist, ist keine Standardauthentifizierung für alle eingehenden Amazon Web Services SNS-Anforderungen erforderlich. Dies kann zu nicht authentifiziertem Zugriff auf Instanzdaten führen.

Autorisierung für SOAP-Anforderungen anfordern [aktualisiert in Security Center 1,3, 1,5 und 2,0]

Verwenden Sie `glide.basicauth.required.soap`Eigenschaft, die angibt, ob eingehende SOAP-Anforderungen eine Standardautorisierung erfordern sollen.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.soapglide.soap.require_ws_securi`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Autorisierung von SOAP-Anforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird ausgeführt, während Daten aus Tabellen/Seiten in Form von SOAP-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Anwender, der Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigt. Weitere Informationen finden Sie unter SOAP-Webservice Und Anmeldeinformationen für die MID-Server-Authentifizierung und SOAP-Anforderungen .
Sicherheitsrisiko	(Mittel) ohne entsprechende Autorisierung, die für die SOAP-Anforderungen der Datenquelle konfiguriert ist, kann ein nicht autorisierter Anwender auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung für Entladeanforderungen anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.unl`Eigenschaft (useUnloadFormat), die angibt, ob eingehende Entladeanforderungen eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.unl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung bei Entladeanforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7,5
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. Diese Authentifizierung wird beim Abrufen von Daten aus Tabellen/Seiten in Form von Entladedaten in der Instanz ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) ohne entsprechende Autorisierung, die für die Anforderungen zum Entladen der Datenquelle konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten. Stellen Sie sicher `glide.basicauth.required.unl`Ist in „sys_properties_table“ vorhanden und auf „wahr“ festgelegt.
Referenzen	Authentifizierung

Autorisierung für CSV-Anforderungen anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.csv`Eigenschaft, die angibt, ob eingehende CSV-Anforderungen (kommagetrennte Werte) eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.csv`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für CSV-Anforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7,5
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird ausgeführt, während Daten aus Tabellen/Seiten in Form von CSV-Daten in der Instanz abgerufen werden. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Daten werden aus einer CSV-formatierten Datei abgerufen .
Sicherheitsrisiko	(Hoch) ohne entsprechende Autorisierung, die für die eingehenden CSV-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte und Daten in der Zielinstanz erhalten. Stellen Sie sicher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	`glide.basicauth.required.csv`Ist in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt.
Referenzen	Webservice – Sicherheit

Autorisierung für Excel-Anforderungen anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.excel`Eigenschaft, die angibt, ob eingehende Excel-Anforderungen eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.excel`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für Excel-Anforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7,5
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird ausgeführt, während Daten aus Tabellen/Seiten in Form von Excel-Daten in der Instanz abgerufen werden. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Hoch) ohne entsprechende Autorisierung, die für die eingehenden Excel-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Autorisierung für Importanforderungen anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.importprocessor`Eigenschaft, die angibt, ob eingehende Importanforderungen eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.importprocessor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für Importanforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird beim Importieren von Datenquellen in die Instanztabellen/-Seiten durchgeführt. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Daten werden aus einer CSV-formatierten Datei abgerufen .
Sicherheitsrisiko	(Mittel) ohne entsprechende Autorisierung, die für die Datenquellen-Importanforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/ Daten in der Zielinstanz erhalten.
Referenzen	SOAP-Webservices-Sicherheit SOAP-Webservice

Autorisierung für JSONv2-Anforderung anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.jsonv2`Eigenschaft, die angibt, ob eingehende JSONv2-Anforderungen eine Standardautorisierung erfordern sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.jsonv2`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Zum Erzwingen der Autorisierung von JSONv2-Anforderungen.
Sicherheitsrisikobewertung	7,5
Empfohlener Wert	wahr
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird ausgeführt, während Daten aus Tabellen/Seiten in Form von JSON-Daten in der Instanz abgerufen werden. • Sie schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. • Erstellen Sie einen Account für einen Anwender, der Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigt. Weitere Informationen finden Sie unter JSONv2-Webservice JSONv2-Webservice .
Sicherheitsrisiko	(Hoch) ohne entsprechende Autorisierung, die für die JSON-Anforderungen der Datenquelle konfiguriert ist, kann ein nicht autorisierter Anwender auf vertrauliche Inhalte/Daten in der Zielinstanz zugreifen.
Referenzen	Authentifizierung Basic Authentication für eingehende JSONv2-Anforderungen anfordern

Autorisierung für WSDL-Anforderung anfordern [aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie `glide.basicauth.required.wsdl`Eigenschaft, die angibt, ob eingehende WSDL-Anforderungen (Web Services Description Language) eine Standardauthentifizierung erfordern sollen.

Wenn `glide.basicauth.required.wsdl`lst nicht auf den empfohlenen Wert „wahr“ festgelegt, wird die Standardauthentifizierung für WSDL-Anforderungen deaktiviert. WSDL ist ein Protokoll, das zur Beschreibung von Webservices wie Instanztabellenschemata verwendet wird und kein Mechanismus für die gemeinsame Nutzung der Daten innerhalb

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

von Tabellen ist. Wenn Sie diese Eigenschaft auf „wahr“ festlegen, können Tabellenschemas für nicht authentifizierte Anwender offengelegt werden.

Hinweis: Wenn Sie keine Standardauthentifizierung für eingehende WSDL-Anforderungen benötigen, müssen Sie die Zugriffssteuerungsregeln (ACL) ändern, damit Gastanwender auf den WSDL-Inhalt zugreifen können.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.wsdl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für WSDL-Anforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird ausgeführt, während Daten aus Tabellen/Seiten in Form von WSDL-Daten in der Instanz abgerufen werden. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Mittel) ohne entsprechende Autorisierung, die in den WSDL-Webservices konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche WSDL-Inhalte/-Daten in der Zielinstanz erhalten.
Referenzen	Webservice – Sicherheit

Autorisierung für XML-Anforderungen anfordern [aktualisiert im Sicherheitscenter 1,3]

Verwenden Sie `glide.basicauth.required.xml`Eigenschaft, die angibt, ob eingehende XML-Anforderungen eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.xml`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für XML-Anforderungen.
Sicherheitsrisikobewertung	7,5
Empfohlener Wert	wahr
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird ausgeführt, während Daten aus Tabellen/Seiten in Form von XML-Daten in der Instanz abgerufen werden. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter XML-Parser-Schritt .
Sicherheitsrisiko	(Hoch) ohne entsprechende Autorisierung, die für die eingehenden XML-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Autorisierung für XML-Ausgabeanforderungen anfordern [aktualisiert in Security Center 1,3]

Konfigurieren Sie diese Eigenschaft so, dass für alle eingehenden XMLOutputProcessor-Anforderungen eine Standardautorisierung erforderlich ist.

Wenn `glide.basicauth.required.xmloutputprocessor`Eigenschaft ist nicht auf den empfohlenen Wert von festgelegt **Wahr** , Dann ist für eingehende XMLOutputProcessor-Anforderungen keine Standardautorisierung erforderlich, was zur Offenlegung nicht authentifizierter Informationen von der Instanz führen kann.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.basicauth.required.xmloutputprocessor`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	API und Webservice
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Die Eigenschaft wird nicht auf den empfohlenen Wert festgelegt **Wahr** Kann dazu führen, dass vertrauliche Informationen aus der Instanz weitergegeben werden.
Abhängigkeiten und Voraussetzungen	Keine

Autorisierung für XSD-Anforderungen erfordern [aktualisiert im Sicherheitscenter 1,3]

Verwenden Sie *`glide.basicauth.required.xsd`*Eigenschaft, die angibt, ob eingehende XSD-Anforderungen (XML-Schemadefinition) eine Standardauthentifizierung erfordern sollen.

Stellen Sie die Eigenschaft sicher *`glide.basicauth.required.xsd`*lst in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	Glide.basicauth.erforderlich.xsd*`glide.basicauth.required.xsd`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für XSD-Anforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Diese Authentifizierung wird ausgeführt, während Daten aus Tabellen/Seiten in Form von XSD-Daten in der Instanz abgerufen werden. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter Nicht interaktive Sitzungen .
Sicherheitsrisiko	(Mittel) ohne entsprechende Autorisierung, die für die eingehenden XSD-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	Authentifizierung

Autorisierung für Skriptanforderungen anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.scriptedprocessor`Eigenschaft, die angibt, ob eingehende Skriptanforderungen eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.scriptedprocessor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für Skriptanforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	Diese Korrektur erzwingt die Authentifizierung in Form der Standardautorisierung. • Diese Authentifizierung wird während der Verarbeitung von Skriptanforderungen in der Instanz ausgeführt. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen.
Sicherheitsrisiko	(Hoch) ohne entsprechende Autorisierung, die für die eingehenden Skriptanforderungen konfiguriert ist, greift ein nicht autorisierter Anwender auf vertrauliche Inhalte/Daten in der Zielinstanz zu.
Referenzen	Authentifizierung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Autorisierung für SCHEMAANFORDERUNGEN anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.basicauth.required.schema*Eigenschaft, die eine Standardautorisierung für alle eingehenden Tabellenschema-Prozessor-Anforderungen erfordert.

Der Schebma-Prozessor für eingehende Tabellen verarbeitet eingehende Schemaanforderungen für die Plattform.

Festlegen *glide.basicauth.required.schema*Auf den empfohlenen Wert von **Wahr** Dient zum anfordern der Basisautorisierung für alle eingehenden Tabellenschema-Prozessor-Anforderungen. Legen Sie den Wert auf fest **Falsch** Keine Standardautorisierung für alle eingehenden Tabellenschema-Prozessor-Anforderungen erforderlich.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.basicauth.required.schema*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum anfordern der Basisautorisierung für alle eingehenden Tabellenschema-Prozessor-Anforderungen.
Empfohlener Wert	Wahr (Standardwert).
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Mittel) das Auslassen der Authentifizierung durch diesen Prozessor führt zu nicht authentifiziertem Zugriff auf Instanzdaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Autorisierung für RSS-Anforderungen anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.rss`Eigenschaft, die angibt, ob eingehende RSS-Anforderungen eine Standardauthentifizierung erfordern sollen.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.rss`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Dient zum Erzwingen der Standardauthentifizierung für RSS-Anforderungen.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	7,5
Funktionale Auswirkung	Diese Korrektur erzwingt eine Kombination von Authentifizierungsmethoden in Form von Standardauthentifizierung und Zugriffssteuerung auf Systemebene. • Diese Authentifizierung wird während der Verarbeitung von RSS-Anforderungen in der Instanz ausgeführt. • Er schränkt alle Gastanwender ein, die derzeit auf diese Daten zugreifen. Falls zutreffend, müssen Sie möglicherweise einen neuen Account für Anwender erstellen, die Zugriff auf diesen Inhalt mit den erforderlichen Zugriffssteuerungsberechtigungen benötigen. Weitere Informationen finden Sie unter RSS-Feed-Generator .
Sicherheitsrisiko	(Hoch) ohne entsprechende Autorisierung, die für die eingehenden RSS-Anforderungen konfiguriert ist, kann ein nicht autorisierter Anwender Zugriff auf vertrauliche Inhalte/Daten in der Zielinstanz erhalten.
Referenzen	RSS-Basic Authentication

Autorisierung für API-Anforderungen anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.api`Eigenschaft zur Verbesserung der Sicherheit für die Standardautorisierung für eingehende REST-Anforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie fest `glide.basicauth.required.api`Eigenschaft bis **Wahr** Dient zum anfordern der Autorisierung für alle REST-Anforderungen. Legen Sie die Eigenschaft auf fest **Falsch** Um die Autorisierung für alle REST-Anforderungen zu umgehen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.basicauth.required.api`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	API und Webservice
Zweck	Standardautorisierung für eingehende REST-Anforderungen.
Empfohlener Wert	Wahr (Standard)
Konfigurationstyp	Zeichenfolge
Sicherheitsrisiko	(Hoch) wenn „Glide.basicauth.required.api“ nicht auf den empfohlenen Wert „wahr“ festgelegt ist, wird die Standardauthentifizierung für die API-Anforderung deaktiviert und führt zu nicht authentifiziertem Zugriff auf Instanzdaten.
Sicherheitsrisikobewertung	8.6

Architektur, Design und Bedrohungsmodellierung

Diese breite Steuerung behandelt allgemeine Designüberlegungen und Schlüsselelemente für die Implementierung einer sicheren Anwendung. Dies deckt die Mandanten Verfügbarkeit, Integrität der Vertraulichkeitsverarbeitung, Nichtwiderlegung und Datenschutz ab. Darüber hinaus sind Elemente eines sicheren Softwareentwicklungslebenszyklus enthalten.

Zertifikatbasierte Authentifizierung nicht erzwungen [Neu in Security Center 1,3]

Die `glide.authenticate.mutual.enabled`Die Eigenschaft aktiviert die zertifikatbasierte Authentifizierung, eine Art der gegenseitigen Authentifizierung für eingehende REST-Verbindungen zu REST- und SOAP-APIs in ServiceNow AI Platform.

Die gegenseitige Authentifizierung schafft Vertrauen zwischen Server und Client, indem SSL-Zertifikate (Secure Socket Layer) ausgetauscht werden, um das Zertifikat mit einer vertrauenswürdigen Zertifizierungsstelle zu validieren. Dies ermöglicht die Verifizierung, dass eine vertrauenswürdige Quelle eine Verbindung mit herstellt ServiceNow AI Platform. Wenn diese Instanz nicht auf den empfohlenen Wert „wahr“ festgelegt ist, kann eine Instanz angreifbar für man-in-the-Middle-Angriffe (MitM) sein.

Um diese Sicherheitsbedrohung zu beheben, aktivieren Sie die gegenseitige Authentifizierung für eingehende Webservices. Wenn Sie das Plugin für die zertifikatbasierte Authentifizierung zum ersten Mal installieren (`com.glide.auth.mutual`)Für ServiceNow AI Platform, Folgen Sie dann dem Richten Sie die zertifikatbasierte Authentifizierung ein Anweisungen. Stellen Sie außerdem sicher, dass

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

*glide.authenticate.mutual.enabled*Eigenschaft ist auf „wahr“ festgelegt, um das Plugin zu aktivieren.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.mutual.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt ist, validiert die zertifikatbasierte Authentifizierung keine Zertifikate mit einer vertrauenswürdigen Zertifizierungsstelle. Dies erhöht die Wahrscheinlichkeit, dass ein schlechter Akteur eine Instanz mithilfe von MitM-Angriffen angreift.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • Zertifikatbasierte Authentifizierung • Konfigurieren Sie die gegenseitige Authentifizierung

Identitätswechsel bei ACL-Bewertung in HR-App überprüfen [Neu in Security Center 1,3 Und aktualisiert in 1,5]

Verwenden Sie *sn_hr_core.impersonateCheck*Eigenschaft, die verhindert, dass ein Anwender die Identität eines anderen Anwenders übernimmt und auf seine HR-Informationen zugreift.

Eine sichere Einstellung verhindert, dass ein Administrator die HR-Informationen eines anderen Anwenders sieht, während er die Identität verwendet. Eine unsichere Einstellung für diese Eigenschaft ermöglicht es einem Administrator, die Identität eines Anwenders anzunehmen und mit dem Zugriff des Anwenders auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zuzugreifen. Aufgrund der Art dieser Art von Daten, z. B. Informationen, die nur dem Anwender selbst zur Verfügung stehen sollten, z. B. E-Mail, wird dies nicht empfohlen. Einstellung *sn_hr_core.impersonateCheck*Bei „wahr“ ist nur der Zugriff auf HR-Informationen möglich, wenn der Anwender keine Identität eines anderen annimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`sn_hr_core.impersonateCheck`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Eine unsichere Einstellung für diese Eigenschaft ermöglicht es einem Administrator, die Identität eines Anwenders anzunehmen und mit dem Zugriff des Anwenders auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zuzugreifen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „wahr“ festgelegt ist, wird verhindert, dass ein Administrator die HR-Informationen eines anderen Anwenders sieht, während eine Identitätswechsel verwendet wird. Bei „falsch“ kann ein Administrator die Identität eines Anwenders annehmen und mit dem Zugriff des Anwenders auf HR-Daten wie Umfrageergebnisse oder Audit-Datensätze zugreifen. Aufgrund der Art dieser Art von Daten, z. B. Informationen, die nur dem Anwender selbst zur Verfügung stehen sollten, z. B. eine E-Mail, wird dies nicht empfohlen. Wenn Sie „sn_HR_Core.impersonateCheck“ auf „wahr“ festlegen, ist der Zugriff auf HR-Informationen nur dann möglich, wenn der Anwender keine Identität eines anderen annimmt.

Deaktivieren Sie die lokale Anmeldung für Anwender mit aktiviertem Single Sign-on (SSO)

Aktualisieren Sie Anwenderdatensätze, um die lokale Anmeldung für Anwender mit aktiviertem Single Sign-on (SSO) zu deaktivieren.

Anwender, die für die Verwendung der SSO-Authentifizierung konfiguriert sind, können möglicherweise auf die Instanz oder Teile der Instanz zugreifen, wenn lokale Anmeldeinformationen in gespeichert sind **User_password** Feld des Anwenderdatensatzes [sys_user]. Dieser Zugriff gilt sowohl für den interaktiven als auch für den nicht interaktiven Zugriff von Anwendern, die nicht gesperrt sind. Helfen Sie, SSO-konfigurierte Anwender daran zu hindern, lokale Anmeldeinformationen zu verwenden, um die Wahrscheinlichkeit zu reduzieren, dass gültige lokale Anmeldeinformationen gestohlen und von böswilligen Anwendern verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lesen Sie den Now Support Knowledge Base-artikel KB1649420 Anweisungen zum Identifizieren und Bearbeiten von Accounts mit aktivierter lokaler Anmeldung auf einer Instanz mit aktiviertem SSO.

Weitere Informationen

Attribut	Beschreibung
Sicherheitsrisiko	Wenn die SSO-Authentifizierung für einen Anwender aktiviert ist, ist es Best Practice, zu verhindern, dass sich dieser Anwender lokal anmeldet. Dies verringert die Wahrscheinlichkeit, dass die gültigen lokalen Anmeldeinformationen gestohlen und von einem böswilligen Anwender zur Anmeldung verwendet werden.
CVSS-Punktzahl (Common Vulnerability Scoring System)	4.2
Bewertung des Common Vulnerability Scoring System (CVSS)	Mittel
Funktionale Auswirkung	Mit SSO konfigurierte Anwender können sich mit lokalen Anmeldeinformationen anmelden.
Abhängigkeiten und Voraussetzungen	Single Sign-on muss aktiviert sein (die **glide.authenticate.multisso.enabled** Systemeigenschaft auf festgelegt **Wahr** .)
Datentyp	N/V
Basissystemwert	N/V
Fallback-Wert	N/V
Empfohlener Wert	N/V

Nicht authentifizierte veröffentlichte Berichte deaktivieren [aktualisiert in Security Center 2,0]

Deaktivieren Sie diese Eigenschaft, um zu verhindern, dass der Anwender Berichte veröffentlicht oder darauf zugreift. Diese Eigenschaft deaktiviert die Funktion „veröffentlichte Berichte“ in der Berichterstellung.

Aktivieren Sie die Veröffentlichung von Berichten, indem Sie festlegen `glide.report.published_reports.enabled`Bis **Wahr** .

Stellen Sie die Glide-Eigenschaft sicher `glide.report.published_reports.enabled`Ist vorhanden und auf den Wert „falsch“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.report.published_reports.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Deaktiviert die Funktion „veröffentlichte Berichte“ in der Berichterstellung.
Typ	wahr | falsch
Empfohlener Wert	**false**
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	Der Anwender kann keine Berichte veröffentlichen.
Sicherheitsrisiko	(Mittel) wenn diese Eigenschaft nicht aktiviert ist, können Anwender möglicherweise auf Berichte zugreifen oder diese veröffentlichen, die vertrauliche Daten offenlegen. Durch das Veröffentlichen eines Berichts wird eine URL erstellt, die jeder für den Zugriff auf den Bericht verwenden kann, einschließlich Personen, die keine Anwender sind. Wenn jemand zur URL navigiert, wird der Bericht mit aktuellen Daten aus der Instanz generiert.
Referenzen	Berichte veröffentlichen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Feld-ACLs für eingehende Abfrageanforderungen erzwingen

Verwalten Sie, wie eingehende Abfragen in Ihrer Instanz validiert werden.

Verwenden Sie *glide.export.query.enforce_field_acl*Eigenschaft, um zu überprüfen, wie eingehende Abfragen in Ihrer Instanz validiert werden. Wenn die Eigenschaft auf den empfohlenen Wert von festgelegt ist **Wahr** , Feld-ACLs werden anhand eingehender Abfragen überprüft und abgelehnt, wenn der Anwender nicht autorisiert ist. Wenn die Eigenschaft auf festgelegt ist **Falsch** , ACLs werden nicht anhand eingehender Abfragen überprüft und werden weiterhin ausgeführt, was zur Offenlegung von Informationen an nicht autorisierte Parteien führen kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.export.query.enforce_field_acl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,4 • CVSS-Punktzahl: Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Sicherheitsrisikodetails: Wenn diese Eigenschaft auf festgelegt ist **Falsch** , ACLs werden nicht anhand eingehender Abfragen überprüft, die zur Offenlegung von Informationen führen können.
Abhängigkeiten und Voraussetzungen	Keine

Lese-ACLs in Berichtsansichten erzwingen

Verwalten Sie, wie Lese-ACLs in Ihrer Instanz erzwungen werden.

Verwenden Sie *glide.report.report_view.read_acl*Eigenschaft zum Erzwingen der Lese-ACL (Tabellenebene) für Berichtsfunktionen, wenn in der Tabelle oder im Feld keine Berichtsansichts-ACL vorhanden ist. Wenn diese Eigenschaft nicht auf festgelegt ist **Erzwingen** , ACLs können umgangen werden, was zu einem Verlust vertraulicher Informationen führt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.report.report_view.read_acl*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Erzwingen
Standardwert	Erzwingen
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,1 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Diese Eigenschaft wird nicht auf festgelegt **Erzwingen** Kann dazu führen, dass ACLs umgangen werden.
Abhängigkeiten und Voraussetzungen	Keine

Abfrage-ACLs für Knowledge-Quick-Links erzwingen

Erzwingen Sie Abfrage-ACLs für Knowledge-Quick-Links mithilfe einer Systemeigenschaft.

Wenn *com.glide.security.query_acl.enabled.knowledge_quick_links*Systemeigenschaft ist auf festgelegt **Wahr** , Abfrage-ACLs werden für Knowledge Quick-Links erzwungen. Wenn diese Eigenschaft auf festgelegt ist **Falsch** , Kann ein Angreifer aufgrund des Standardverhaltens von Daten mit blinden Abfragen aufzählen und exfiltrieren GlideRecord.addEncodedQuery .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden ist, ist der sichere Standard von **Wahr** Wird verwendet. Eine dritte Option, **External_and_guests** Erzwingt Abfrage-ACLs nur für externe Anwender und Gäste.

Überprüfen Sie, ob *com.glide.security.query_acl.enabled.knowledge_quick_links*Systemeigenschaft ist auf festgelegt **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.security.query_acl.enabled.knowledge_quick_link*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge: Wird als ternärer Operator verwendet
Empfohlener Wert	wahr
Standardwert	wahr
Fallback-Wert	wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisiko: ACLs können umgangen werden, sodass Felddaten für Anwender offen gelegt werden, die nicht über die Berechtigung zum Anzeigen verfügen. Diese Offenlegung kann vertrauliche Daten enthalten, abhängig von der ausgenutzten Tabelle.
Funktionale Auswirkung	Anwender können keine bestimmten Abfragen für Felder ausführen, für die sie keinen Zugriff auf Feldebene haben.
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Abfrage-ACLs für Unterlisten, Listenanzahlen und Widget-Datentabellen erzwingen

Erzwingen Sie Abfrage-ACLs für Sublist-, Listenanzahl- und Widget-Datentabellenabfragen mithilfe von Systemeigenschaften.

Festlegen *com.glide.security.query_acl.enabled.sub_lists*Bis **Wahr** Dient zum Erzwingen von Abfrage-ACLs für Sublistabfragen, z. B. gruppierte Listen und zugehörige Listen.

Festlegen *com.glide.security.query_acl.enabled.list_count*Bis **Wahr** Dient zum Erzwingen von Abfrage-ACLs für Listenanzahlabfragen.

Festlegen *glide.security.query_acl.enabled.data_table*Bis **Wahr** Dient zum Erzwingen von Abfrage-ACLs für Widget-Datentabellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ob eine dieser Systemeigenschaften auf festgelegt ist **Falsch** , Kann ein Angreifer aufgrund des Standardverhaltens von Daten mit blinden Abfragen aufzählen und exfiltrieren `GlideRecord.addEncodedQuery` . Wenn diese Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden sind, wird der sichere Standardwert „wahr“ verwendet. Eine dritte Option, *`external_and_guests`*, Erzwingt ACLs nur für externe Anwender und Gäste.

Stellen Sie sicher, dass diese Systemeigenschaften nicht in der Tabelle „Systemeigenschaften“ [sys_properties] angezeigt oder auf festgelegt sind **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	• *`com.glide.security.query_acl.enabled.sub_lists`* • *`com.glide.security.query_acl.enabled.list_count`* • *`glide.security.query_acl.enabled.data_table`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	• wahr • true • wahr
Standardwert	• wahr • true • wahr
Fallback-Wert	• wahr • true • wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisiko: ACLs können umgangen werden, wenn Felddaten für Anwender offengelegt werden, die nicht über die Berechtigung zum Anzeigen verfügen. Dies kann je nach ausgenutzter Tabelle vertrauliche Daten enthalten.
Abhängigkeiten und Voraussetzungen	Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gültige Auswahl für Abfragezeichenfolge erzwingen [Neu in Security Center 7,0]

Verwenden Sie eine Systemeigenschaft, um sicherzustellen, dass jeder Auswahlfeldwert, wenn er über eine URL-Abfragezeichenfolge übergeben wird, eine gültige aktive Auswahl ist, wenn ein Datensatz erstellt wird.

Wenn `glide.ui.query_string.enforce_valid_choice_on_create`Systemeigenschaft ist auf festgelegt **Wahr** , Die Plattform validiert, dass ein beliebiger Auswahlfeldwert, der über eine URL-Abfragezeichenfolge (z. B. aus einem Listenfilter) übergeben wird, eine gültige aktive Auswahl ist, wenn der Datensatz erstellt wird.

Wenn ungültig, wird der Wert ignoriert, und das Feld wird auf seinen Standardwert zurückgesetzt. Wenn die Eigenschaft ist **Falsch** , Die Validierung ist inaktiv, und das System akzeptiert einen beliebigen Wert, auch ungültige oder inaktive. Diese Akzeptanz kann potenziell dazu führen, dass falsche oder unerwartete Daten in Datensätzen gespeichert werden.

Stellen Sie Sicher `glide.ui.query_string.enforce_valid_choice_on_create`lst in der Tabelle „Systemeigenschaften“ [sys_properties] vorhanden und ist auf festgelegt **Wahr** . Wenn die Eigenschaft in der Tabelle nicht vorhanden ist, ist der Fallback-Wert **Falsch** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ui.query_string.enforce_valid_choice_on_create`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Fallback-Wert	wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,2 • CVSS-Punktzahl: Niedrig • Sicherheitsrisiko: Legen Sie diese Eigenschaft auf fest **Wahr** Um sicherzustellen, dass nur gültige Auswahlmöglichkeiten für die Erstellung eines neuen Datensatzes verwendet werden. Ungültige Auswahlmöglichkeiten können zu geringfügigen und unerwarteten Datenintegritätsproblemen führen, bei denen ein Anwender einen unbeabsichtigten Wert auswählen kann.
Funktionale Auswirkung	Vorhandene Instanzen und Workflows basieren möglicherweise auf neuen Datensätzen, die basierend auf einem Filter erstellt werden, der eine ungültige oder inaktive Auswahl enthält. Verwenden Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	den folgenden Prozess, um dieses Verhalten zu beobachten: **1.** Melden Sie sich als Administratoranwender bei einer Instanz an. **2.** Erstellen Sie ein Zeichenfolgenfeld in einer beliebigen Tabelle. Beispiel: Ein Incident mit 2 Auswahlmöglichkeiten: **Test1** Und **Test2** . **3.** Erstellen Sie einen Listenfilter in der Incident-Tabelle, indem Sie das Zeichenfolgenfeld auswählen, dessen Wert auf festgelegt ist **Test2** . **4.** Wechseln Sie zum Wörterbuchfeld, und deaktivieren Sie die Auswahl **Test2** . **5.** Wechseln Sie zu dem in Schritt 3 ausgewählten Filter, und wählen Sie aus **Neu** Schaltfläche. **6.** Überprüfen Sie den Wert des Felds Zeichenfolgentyp im neu geöffneten Datensatz. Wenn die Eigenschaft auf festgelegt ist **Wahr** , Das Zeichenfolgenfeld darf keinen Wert haben oder sollte den Standardwert anzeigen. Wenn die Eigenschaft auf festgelegt ist **Falsch** (Standard) hat das Zeichenfolgenfeld den Wert auf festgelegt **Test2** .
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Definieren zulässig ServiceNow Interne IP-Adressen [aktualisiert in Security Center 1,3 Und 1,5]

Verwenden Sie `glide.ip.authenticate.strict`Eigenschaft zum Angeben von IP-Bereichen, die eingehende Verbindungen in einer Instanz herstellen können.

Verhindern Sie, dass Instanzzugriff für eine größere Gruppe von Personen, die verwenden, unnötig gefährdet ist **glide.ip.authenticate.strict** Und **glide.ip.authenticate.allow.secured** Systemeigenschaften.

Wenn **glide.ip.authenticate.strict** Systemeigenschaft ist auf festgelegt **Wahr** , Intern ServiceNow Mitarbeiter und Systeme können eingehende Verbindungen zu Ihrer Instanz nur aus wichtigen IP-Bereichen herstellen. Diese Grenzen ServiceNow Transparenz von für wichtige interne Infrastruktur in Ihrer Instanz und verhindert den Zugriff von breiter ServiceNow Mitarbeiter wie Support- und Vertriebsmitarbeiter über Unternehmensnetzwerke. Die **glide.ip.authenticate.allow.secured** Systemeigenschaft gewährt intern ServiceNow Eingehende Verbindungen, einschließlich regulärem authentifiziertem Zugriff und nicht authentifizierten Diagnoseseiten.

Wenn nicht auf festgelegt **Wahr** , Dann breiter ServiceNow Interner IP-Bereich, der in definiert ist **glide.ip.authenticate.allow** Die Eigenschaft wird verwendet, um diese intern zu gewähren ServiceNow Eingehende Verbindungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass **glide.ip.authenticate.allow.secured** Die Systemeigenschaft enthält nur vertrauenswürdige Werte und die Eigenschaft **glide.ip.authenticate.strict** Ist auf festgelegt **Wahr** .

Warnung: Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ip.authenticate.strict`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Ermöglicht ServiceNow-Mitarbeitern den Zugriff auf die Instanz nur über einen gesicherten Satz von IP-Bereichen
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	(Niedrig) wenn diese Eigenschaft nicht aktiviert ist, können ServiceNow-Mitarbeiter über alle IP-Bereiche auf die Instanz des Kunden zugreifen. Durch Aktivieren der Eigenschaft wird der Zugriff auf einen sicheren Satz von IP-Bereichen (Secure VPN, DC) eingeschränkt. **Hinweis:** Wenn Sie diese Eigenschaft auf festlegen `Wahr` , ServiceNow AI Platform Verwendet eine restriktivere `glide.ip.authenticate.allow.secured`Eigenschaft anstelle der IP-Einschränkung der Leistungsüberwachung (`glide.ip.authenticate.allow.secured`) Eigenschaft für eine Reihe von IP-Bereichen, die auf die Instanz zugreifen können.
Sicherheitsrisiko	(Niedrig) unnötiges Risiko des Instanzzugriffs für eine breitere Personengruppe.
Referenz	IP-bereichsbasierte Authentifizierung

Hinweis: Die Regel „alle ablehnen“ muss der IP-Zugriffssteuerung hinzugefügt werden, um den Zugriff von allen IP-Adressen zu beschränken, die nicht der IP-Zugriffssteuerung hinzugefügt wurden. Alle erforderlichen zulässigen IP-Adressen müssen dann der IP-Zugriffssteuerung hinzugefügt werden.

Veraltetes JQuery-Verhalten deaktivieren [aktualisiert im Securty Center 1,3]

Die `glide.jquery.legacy`Wird verwendet, um zu verhindern, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, wodurch nicht gepatchte Schwachstellen in der Bibliothek eingeführt werden.

Festlegen `glide.jquery.legacy`Auf den empfohlenen Wert von **Falsch** Um zu verhindern, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, die nicht gepatchte Schwachstellen in der Bibliothek einführen. Legen Sie den Wert auf fest **Wahr** Um vorab gepatchte JQuery-Versionen zuzulassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.jquery.legacy`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Um potenzielle Sicherheitsrisiken zu verhindern, die durch Angriffe auf Schwachstellen entstehen, die in veralteten JQuery-Bibliotheksversionen erkannt wurden.
Empfohlener Wert	Falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) verhindern, dass ältere vorab gepatchte JQuery-Versionen verwendet werden, die ungepatchte Schwachstellen in der Bibliothek einführen. Die Systemeigenschaft ist fehlersicher, wenn Organisationen auf die nicht gepatchten Versionen von AngularJS angewiesen sind, um ihre anwenderdefinierten Implementierungen auszuführen.
Sicherheitsrisikobewertung	7.1

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Legacy-Verhalten für GlideRecord-Umfangsabgrenzung deaktivieren [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]

Die `glide.record.legacy_cross_scope_access_policy_in_script`Die Eigenschaft deaktiviert die Umfangsdefinition, sodass bereichsbezogene Apps auf globale Skriptschnittstellen zugreifen können. Es wurde als Patch für den bereichsübergreifenden Zugriff von GlideRecord erstellt.

GlideRecord bot bereichsübergreifenden Erstellungs-/Aktualisierungszugriff auf Tabellen, die nicht mit dieser Zugriffsebene konfiguriert wurden. Um zu verhindern, dass bei Kunden Anwendungen beschädigt werden, wenn dieses bereichsbezogene Zugriffsverhalten gepatcht wurde, die Eigenschaft `glide.record.legacy_cross_scope_access_policy_in_script`Wurde erstellt. Bei „wahr“ greift der bereichsübergreifende Zugriff auf veraltetes Verhalten zurück (unsicher). Diese Eigenschaft deaktiviert die Umfangsdefinition, sodass bereichsbezogene Apps auf globale Skriptschnittstellen zugreifen können.

Es ist die beste Sicherheitspraxis, Umfangsbeschränkungen zu haben. Die Umfangsdefinition stellt sicher, dass Anwendungen nur mit explizitem Zugriff oder innerhalb ihres Umfangs auf Ressourcen zugreifen können, wobei das Prinzip der geringsten Berechtigung befolgt wird. Das Deaktivieren dieser Funktion kann Auswirkungen auf Vertraulichkeit, Verfügbarkeit und Integrität haben.

Legen Sie die Glide-Eigenschaft fest `glide.record.legacy_cross_scope_access_policy_in_script`Auf „falsch“. Wenn nicht in der Tabelle „sys_properties“ vorhanden, ist der Standardwert „wahr“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.record.legacy_cross_scope_access_policy_in_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	„Wahr“ (wenn die Eigenschaft in der Tabelle „sys_properties“ nicht vorhanden ist.)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Die Umfangsdefinition stellt sicher, dass Anwendungen nur mit explizitem Zugriff oder innerhalb ihres Umfangs auf Ressourcen zugreifen können, die dem Grundsatz der geringsten Berechtigung entsprechen. Das Deaktivieren dieser Funktion kann Auswirkungen auf Vertraulichkeit, Verfügbarkeit und Integrität haben.
Abhängigkeiten und Voraussetzungen	Keine

Veraltetes AngularJS-Verhalten deaktivieren [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.angular.legacy`Eigenschaft zum Schutz vor potenziellen Sicherheitsrisiken, die aus Angriffen auf Schwachstellen entstehen, die in veralteten AngularJS-Bibliotheksversionen erkannt wurden.

Festlegen `glide.angular.legacy`Auf den empfohlenen Wert von **Falsch** Um zu verhindern, dass ältere vorab gepatchte AngularJS-Versionen verwendet werden. Legen Sie die Eigenschaft auf fest **Wahr** Dient zur Verwendung älterer vorab gepatchter AngularJS-Versionen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.angular.legacy`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Die Systemeigenschaft ist fehlersicher, wenn Organisationen auf die nicht gepatchten Versionen von AngularJS angewiesen sind, um ihre anwenderdefinierten Implementierungen auszuführen.
Empfohlener Wert	Falsch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) die Verwendung älterer Versionen von AngularJS kann potenziell zu Sicherheitsrisiken aufgrund von Angriffen auf Schwachstellen führen, die in veralteten Versionen der AngularJS-Bibliothek erkannt wurden.
Sicherheitsrisikobewertung	7.1

Autorisierung für Daten-Broker-Rest-API anfordern [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.basicauth.required.databrokerrestapiprocessor`Eigenschaft, die eine Standardautorisierung für alle eingehenden Daten-Broker-Rest-API-Anforderungen erfordert.

Wenn diese Eigenschaft auf festgelegt ist **Wahr** , Dann wird die Autorisierung angewendet. Wenn auf festgelegt ist **Falsch** , Wird keine Autorisierung verwendet, was dazu führen könnte, dass vertrauliche Informationen aus Ihrer Instanz weitergegeben werden.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.basicauth.required.databrokerrestapiprocessor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,6 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Wenn die Eigenschaft auf festgelegt ist **Falsch** , Dann wird die API-Authentifizierung nicht angewendet, damit ein schlechter Akteur auf vertrauliche Daten zugreifen kann.
Abhängigkeiten und Voraussetzungen	Keine

Eingeschränkte Bindungsfunktionalität in Fallbearer-Autorisierung [Neu in Security Center 7,0]

Verwenden Sie eine Systemeigenschaft und eine eingeschränkte Bindung, um sicherzustellen, dass ein mit dieser Entität generiertes Zugriffstoken nicht für UI-Aufrufe verwendet werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie *glide.oauth.enforce_restricted_binding_for_ui*Systemeigenschaft und eingeschränkte Bindung für eine OAuth-Entität aktivieren, um zu verhindern, dass die von dieser Entität generierten Zugriffstoken für UI-Aufrufe verwendet werden (z. B. Incident_list.do).

Wenn die eingeschränkte Bindung deaktiviert ist, kann das generierte Zugriffstoken unabhängig vom Wert der Systemeigenschaft für UI-Aufrufe verwendet werden.

Stellen Sie sicher *glide.oauth.enforce_restricted_binding_for_ui*ist auf festgelegt **Wahr** Und **Token-Einschränkungen Erzwingen** Ist auf festgelegt **Wahr** In allen OAuth-Entitätseinträgen. Details zu OAuth-Entitätseinträgen finden Sie unter OAuth eingehend.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.oauth.enforce_restricted_binding_for_ui*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Fallback-Wert	falsch
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,0 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn *glide.oauth.enforce_restricted_binding_for_ui*Systemeiger ist nicht auf festgelegt **Wahr** Oder die eingeschränkte Bindung deaktiviert ist, kann ein Anwender mit dem Zugriffstoken für den Zugriff auf eine API (z. B. mobile API) eine Sitzung ausgeben und sie verwenden, um auf andere eingeschränkte Ressourcen in der Instanz zuzugreifen (z. B. Incident_list.do).
Abhängigkeiten und Voraussetzungen	Keine

Standardmäßig mit leeren ACLs ablehnen [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.sm.default_mode*Eigenschaft zur Steuerung des Standardverhaltens des Sicherheitsmanagers, wenn festgestellt wird, dass vorhandene ACL-Regeln (Access Control List) Teil von ACL-Regeln für Platzhaltertabellen sind.

Verhindern Sie, dass der veraltete Sicherheitsmanager Ihrer Instanz Zugriff auf Ressourcen zulässt, wenn für diese Ressource keine ACLs definiert sind oder wenn nur ACLs auf Tabellenebene mit Platzhaltern vorhanden sind (z. B. Incident.*). Wenn der Zugriff standardmäßig zulässig ist, ist alles, für das keine expliziten ACLs festgelegt sind, anfällig für Manipulationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie fest **glide.sm.default_mode** Systemeigenschaftswert bis **Ablehnen** Um den Zugriff zu verweigern, wenn keine ACL-Definierungsregeln oder nur ACLs auf Tabellenebene mit Platzhaltern vorhanden sind.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.sm.default_mode*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Architektur, Design und Bedrohungsmodellierung
Zweck	Die beste Sicherheitspraxis besteht darin, den Zugriff auf die Tabellen durch einen nicht autorisierten Anwender zu beschränken. • Wenn für Tabellen keine ACL-Regeln vorhanden sind, stellt diese Eigenschaft sicher, dass mindestens Platzhalter-ACLs für jeden CRUD-Vorgang validiert werden, der für die Tabelle/das Feld ausgeführt wird. • Diese Regeln schränken die Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen ein, es sei denn, der Anwender hat die Administratorrolle oder erfüllt die Anforderungen einer anderen Tabellen-ACL-Regel.
Empfohlener Wert	verweigern
Funktionale Auswirkung	Wenn Sie diese Eigenschaft auf festlegen **Zulassen** , Die ACL-Regeln für Platzhaltertabellen lassen CRUD-Vorgänge für alle Tabellen zu, es sei denn, es sind spezifische Tabellen-ACL-Regeln vorhanden, um solche Vorgänge einzuschränken. **Hinweis:** Dieses Plugin ist nicht für vorhandene Instanzen vorgesehen, da es den Sicherheitszugriff auf Tabellen ändern kann, die bereits in einer Produktionsumgebung verwendet werden.
Sicherheitsrisiko	6.3
Referenzen	Standardmäßige Deny-Eigenschaft

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Automatische Token-Bereinigung für Token-Anmeldeinformationen festlegen [Neu in Security Center 2,0]

Verwenden Sie *com.snc.platform.security.token.auth.cleanup*Eigenschaft, um sicherzustellen, dass abgelaufene API-Schlüssel und HMAC-Geheimnisse gelöscht werden, wodurch das Potenzial für die Wiederverwendung von Token eingeschränkt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn *com.snc.platform.security.token.auth.cleanup*Eigenschaft ist auf den unsicheren Wert von „falsch“ festgelegt, abgelaufene API-Schlüssel und HMAC-Geheimnisse werden nicht gelöscht, wodurch die Wiederverwendung von Token möglich ist. Wenn ein Token aufgrund von Leckage oder Gefährdung abgelaufen ist, kann seine Wiederverwendung die Instanz für jeden zugänglich machen, der das ausgelaufene Token besitzt.

Abgelaufene Token werden für die von definierte Anzahl von Tagen beibehalten *com.snc.platform.security.token.auth.days.expired.hmac_secret.is.kept*Und *com.snc.platform.security.token.auth.days.expired.api_key.is.kept*. Gültige Werte für diese Einstellungen sind Ganzzahlen von 0 oder größer. Ein Wert von 0 führt dazu, dass die abgelaufenen Token am selben Tag gelöscht werden, während eine höhere Anzahl von Tagen den Risikozeitraum erhöht. Ein Standardwert von 7 Tagen oder weniger wird empfohlen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.snc.platform.security.token.auth.cleanup, com.snc.platform.security.token.auth.days.expired.hmac_se*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	Die empfohlenen Werte sind „wahr“ und eine beliebige Ganzzahl kleiner oder gleich 7.
Standardwert	7
Kategorie	Architektur, Design und Bedrohungsmodellierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,1 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ konfigurieren, können abgelaufene API-Schlüssel und HMAC-Geheimnisse nicht gelöscht werden, was die Wahrscheinlichkeit der Wiederverwendung von Token erhöht.
Abhängigkeiten und Voraussetzungen	Keine

Authentifizierung

Die Authentifizierungskategorie deckt die Hauptelemente der modernen Authentifizierung ab, um zu bestätigen, dass eine Entität und ihre Ansprüche authentisch und korrekt sind, resistent gegen Identitätswechsel sind und das Abfangen von Passwörtern verhindern.

Der ASVS-Standard baut auf dem auf NIST 800-63b (https://pages.nist.gov/800-63-3/sp800-63b.html) Spezifikation für diesen Abschnitt.

Die Authentifizierung umfasst Passwortrichtlinie, Steuerungen und Speicherung, die ordnungsgemäße Implementierung von Authentifikatoren und die ordnungsgemäße Implementierung von Out-of-Band- oder einmaligen Verifizierern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenbasierte Multifaktor-Authentifizierung aktivieren [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.authenticate.multifactor`Eigenschaft zum Erzwingen der rollenbasierten Multifaktor-Authentifizierung (MFA) für alle Anwender, die bestimmten Rollen zugewiesen sind.

Erzwingen Sie die Multifaktor-Authentifizierung basierend auf den Rollen, die dem Anwender zugewiesen sind. Wenn einem Anwender in der Multifaktor-Rollenliste die Rollen „admin“, „Security_admin“ oder „user_admin“ zugewiesen wurden, wird MFA erzwungen.

- Legen Sie diese Eigenschaft auf fest **Wahr** Dient zum Erzwingen der rollenbasierten Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.
- Legen Sie diese Eigenschaft auf fest **Falsch** Zum Deaktivieren der rollenbasierten Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.authenticate.multifactor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Erzwingen Sie die rollenbasierte Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.
Typ	wahr/falsch
Empfohlener Wert	`true`
Sicherheitsabhängigkeiten	Aktivieren **Rollenbasierte Multifaktor-Authentifizierung** Innerhalb von **Multifaktor-Kriterientabelle** .
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	Durch Aktivieren dieser Eigenschaft wird die Experience des Anwenders verbessert. Sie fungiert als zusätzliche Schutz- und Sicherheitsebene gegen gefährdete Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Rollenbasierte Multifaktor-Authentifizierung aktivieren [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.authenticate.multifactor`Eigenschaft zum Erzwingen der rollenbasierten Multifaktor-Authentifizierung (MFA) für alle Anwender, die bestimmten Rollen zugewiesen sind.

Erzwingen Sie die Multifaktor-Authentifizierung basierend auf den Rollen, die dem Anwender zugewiesen sind. Wenn einem Anwender in der Multifaktor-Rollenliste die Rollen „admin“, „Security_admin“ oder „user_admin“ zugewiesen wurden, wird MFA erzwungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie diese Eigenschaft auf fest **Wahr** Dient zum Erzwingen der rollenbasierten Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.
- Legen Sie diese Eigenschaft auf fest **Falsch** Zum Deaktivieren der rollenbasierten Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.authenticate.multifactor`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Erzwingen Sie die rollenbasierte Multifaktor-Authentifizierung für alle Anwender, die bestimmten Rollen zugewiesen sind.
Typ	Boolean
Empfohlener Wert	`true`
Standardwert	falsch
Sicherheitsabhängigkeiten	Aktivieren **Rollenbasierte Multifaktor-Authentifizierung** Innerhalb von **Multifaktor-Kriterientabelle** .
Sicherheitsrisikobewertung	7.2
Funktionale Auswirkung	Durch Aktivieren dieser Eigenschaft wird die Experience des Anwenders verbessert. Sie fungiert als zusätzliche Schutz- und Sicherheitsebene gegen gefährdete Anmeldeinformationen.
Sicherheitsrisiko	(Mittel) wenn diese Eigenschaft nicht aktiviert ist, besteht das Risiko eines nicht autorisierten Zugriffs auf vertrauliche Daten.
Referenzen	Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Kontrollsperrzeit für ungültige Versuche zur Passwortzurücksetzung [aktualisiert in Security Center 1,3 und 2,0]

Die `password_reset.request.max_attempt_window`Die Eigenschaft steuert die Anzahl der Minuten, die ein Anwender warten muss, um sein Passwort zurückzusetzen oder zu ändern, nachdem die maximale Anzahl nicht erfolgreicher Versuche überschritten wurde, die mit festgelegt wurde `password_reset.request.max_attempt`Eigenschaft.

Die `password_reset.request.max_attempt_window`Die Eigenschaft definiert die Anzahl der Minuten, die ein Anwender warten muss, um sein Passwort zurückzusetzen oder zu ändern, nachdem die maximale Anzahl nicht erfolgreicher Versuche überschritten wurde, die mit festgelegt wurde `password_reset.request.max_attempt property`. Eine kleine Anzahl von Minuten für `password_reset.request.max_attempt_window`Die Eigenschaft erhöht das Risiko, dass ein Passwort erfolgreich durch Brute-Erzwingen erzwungen wird, da eine größere Anzahl von Versuchen zur Passwortzurücksetzung unternommen werden kann. Der Standardwert von 1440 Minuten wird empfohlen.

Stellen Sie die Eigenschaft sicher `password_reset.request.max_attempt_window`Ist auf 1440 oder höher festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.max_attempt_window`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt den Sperrzeitraum in Minuten an, nachdem die maximale Anzahl nicht erfolgreicher Versuche zur Passwortzurücksetzung erreicht wurde.
Empfohlener Wert	1440
Standardwert	1440
Konfigurationstyp	Positive Ganzzahlwerte
Sicherheitsrisiko	(Hoch) wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder weniger festgelegt ist, kann eine Account-Brute-Force durchgeführt werden, da der Account nach einer maximalen Anzahl falscher Authentifizierungsversuche nicht gesperrt wird.
Sicherheitsrisikobewertung	7,5
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Erstellen von Anwendern aus eingehenden E-Mails deaktivieren [aktualisiert im Securty Center 1,3]

Verwenden Sie `glide.user.trusted_domain`Eigenschaft zur Angabe der kommagetrennten Liste vertrauenswürdiger Domänen, die bei der Erstellung von Anwendern aus eingehenden E-Mails verwendet werden.

Ein Administrator kann eine E-Mail-Eigenschaft festlegen, um Anwender automatisch aus eingehenden E-Mails zu erstellen. Wenn diese Eigenschaft auf den unsicheren Wert festgelegt ist, erstellt die Instanz automatisch Anwender aus eingehenden E-Mails. Jeder erstellte Anwender hat dasselbe hartcodierte Standardpasswort, was die Umgehung der Authentifizierung durch Brute Force erleichtert.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.pop3readerjob.create_caller`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Empfohlener Wert	falsch
Standardwert	falsch
Sicherheitsrisikobewertung	5.4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Sobald diese Eigenschaft konfiguriert ist, akzeptiert die Instanz nur E-Mails von vertrauenswürdigen Domänen. Wenn Sie die Domäne nicht in die vertrauenswürdige Liste aufnehmen, hat dies Auswirkungen auf Gastanwender, da Accounts automatisch erstellt werden.
Sicherheitsrisiko	(Mittel) wenn die Eigenschaft nicht aktiviert ist, kann ein Angreifer eine E-Mail-Spoofing-/Spamming-Kampagne verwenden, um mehrere E-Mails zu senden, was zur Erstellung unnötigerer Gastanwender führt.
Referenzen	Konfiguration für eingehende E-Mails

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Passwortlose Authentifizierung deaktivieren

Verwenden Sie *glide.login.no_blank_password*Eigenschaft, um zu verhindern, dass Anwender sich mit leeren Passwörtern bei der NOW Platform anmelden, oder indem sie die verlassen **Passwort** Feld leer.

Selbst wenn der Administrator bewusst einen leeren Wert oder ein leeres Passwort in Anwenderdatensätzen zuweist, kann sich ein Anwender nicht anmelden, ohne einen Wert in anzugeben **Passwort** Feld.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.login.no_blank_password*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Um eine starke Authentifizierung sicherzustellen, da der Anwendername manchmal innerhalb einer Organisation leicht zu erraten ist.
Empfohlener Wert	wahr
Funktionale Auswirkung	Vorgänge dürfen keine leeren Passwörter verwenden, da dies als kritisches Sicherheitsrisiko angesehen wird. Wenn jedoch ein gültiger Fall für eine solche Nutzung vorliegt, besteht die Möglichkeit eines Ausfalls. Anwender mit leeren Passwörtern können sich nicht bei der Instanz anmelden.
Sicherheitsrisiko	(Hoch) ein Angreifer kann sich mit den Standardanwendernamen oder nach einer bestimmten Person/Gruppe (normalerweise firstname.lastname) ohne Passwort bei der Instanz anmelden. Dies wird als kritisches Sicherheitsrisiko betrachtet, da ein öffentlicher Anwender dadurch die Vertraulichkeit und Integrität der Instanzdaten verletzen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenbesitzer-Passwortanmeldeinformationen (ROPC) in OAuth 2-Tokengewährungen deaktivieren [Neu in Security Center 7,0]

Verhindern, dass OAuth 2-Token gewährt werden.

Standardmäßig können Ressourcenbesitzer-Passwortanmeldeinformationen (ROPC) OAuth 2-Token auf Ihren Instanzen gewähren, wenn eine Clientanwendung direkt ein Zugriffstoken mit einem Anwendernamen und Passwort anfordert. Wenn `glide.oauth.inbound.ropc.grant_type.disabled`lst auf festgelegt **Wahr** , ROPC ist inaktiv und kann nicht verwendet werden, um OAuth 2-Token zu gewähren.

Stellen Sie sicher, dass `glide.oauth.inbound.ropc.grant_type.disabled`Systemeigenschaft ist auf festgelegt **Wahr** . Wenn die Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden ist, lautet der Standardwert **Falsch** . Wenn diese Eigenschaft in dieser Tabelle vorhanden ist, ist sie standardmäßig auf festgelegt **Falsch** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.oauth.inbound.ropc.grant_type.disabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Fallback-Wert	falsch
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,3 • CVSS-Punktzahl: Niedrig • Wenn die Eigenschaft auf festgelegt ist **Falsch** , Die Verwendung von ROPC zum Gewähren von OAuth 2-Token ist zulässig. ROPC gilt als weniger sicher als andere Authentifizierungs-Flows, da die Anmeldeinformationen des Anwenders für die Anwendung verfügbar sind. Dies kann zu Schwachstellen in Situationen führen, in denen der Client gefährdet ist und an Schwachstellen leidet, die denen der Standardauthentifizierung ähneln. OAuth 2,1 hat ROPC veraltet.
Funktionale Auswirkung	Wenn die Eigenschaft auf festgelegt ist **Wahr** , ROPC ist inaktiv und kann nicht zum Gewähren von OAuth 2-Token verwendet werden. Dies verhindert Anwendungen, die auf die Plattform zugreifen, indem OAuth 2-Token mit ROPC gewährt wird.
Abhängigkeiten und Voraussetzungen	Das Plugin OAuth 2,0 (com.snc.platform.security.oauth) muss aktiv sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Passwortrichtlinie bei der Anmeldung nicht anwenden [in Security Center 1,5 aktualisiert und 2,0 entfernt]

Verwalten Sie, wie die Passwortkomplexität in Ihrer Instanz behandelt wird.

Durch Festlegen der Eigenschaft `glide.apply.password_policy.on_login`Bei „falsch“ wird die Passwortkomplexität zum Zeitpunkt der Anmeldung nicht durchgesetzt. Wenn Sie die Eigenschaft auf „wahr“ festlegen, wird die Passwortkomplexität erzwungen und führt zu Compliance-Problemen der Organisation.

Gemäß ASVS 4,03 v2.1.9 Empfehlungen:

„Stellen Sie sicher, dass keine Passwortzusammensetzungsregeln vorhanden sind, die den Typ der zulässigen Zeichen einschränken. Es dürfen keine Groß- oder Kleinbuchstaben, Zahlen oder Sonderzeichen erforderlich sein. (C6)"

Anstelle der Durchsetzung der Passwortkomplexität empfiehlt ASVS, eine Passwortlänge von mindestens 12 Zeichen zu erzwingen.

Siehe OWASP ASVS v4.0-Authentifizierung .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.apply.password_policy.on_login`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,4 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Wahr** Kann die Passwortkomplexität erzwingen und zu Compliance-Problemen der Organisation führen.
Abhängigkeiten und Voraussetzungen	Keine

Accountwiederherstellung aktivieren [aktualisiert in Security Center 1,3 Und 1,5]

Die `glide.sso.acr.enabled`Die Eigenschaft steuert die Account-Wiederherstellungsfunktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Festlegen *glide.sso.acr.enabled*Auf den empfohlenen Wert von **Wahr** Damit die Accountwiederherstellung nach Anwender-ID möglich ist. Legen Sie den Wert auf fest **Falsch** Um die Accountwiederherstellung nach Anwender-ID zu verhindern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.sso.acr.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Steuert die Funktion „Accountwiederherstellung nach Anwender-ID“.
Empfohlener Wert	Wahr (Standard)
Konfigurationstyp	Boolean
Sicherheitsrisiko	Kritisch (ohne diese Eigenschaft können Anwender ihren Account nicht nach UserID wiederherstellen.
Sicherheitsrisikobewertung	9,1
Referenzen	Siehe Accountwiederherstellung (ACR) Für zusätzliche Informationen.

Aktivieren Sie CAPTCHA für die Kundenregistrierung

Reduzieren Sie das Risiko von Anforderungen durch böswillige Bots, indem Sie CAPTCHA für die Kundenregistrierung aktivieren.

Verwenden Sie **sn_customerservice.captchaEnabled** Systemeigenschaft, die bestimmt, ob die CAPTCHA-Validierung für die Kundenregistrierung im Kundenservice-Management-Portal aktiviert ist. Verwenden Sie die CAPTCHA-Validierung, um zu verhindern, dass potenziell schädliche Bots automatisch Anforderungen für eine Anwendung übermitteln.

Legen Sie die Systemeigenschaft fest **sn_customerservice.captchaEnabled** Bis **Wahr** Zum Aktivieren der CAPTCHA-Validierung. Wenn sich die Eigenschaft nicht in der Tabelle „Systemeigenschaften“ [sys_properties] befindet, lautet der Standardwert **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	sn_customerservice.captchaEnabled
Plugin-Anwendbarkeit	Kundenservice-Management
Sicherheitsrisiko	Die CAPTCHA-Validierung hilft, zu verhindern, dass potenziell schädliche Bots automatisch Anforderungen für eine Anwendung übermitteln.
CVSS-Punktzahl (Common Vulnerability Scoring System)	3,7

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Bewertung des Common Vulnerability Scoring System (CVSS)	Niedrig
Funktionale Auswirkung	Die Registrierung von Anwendern kann eine negative Erfahrung haben, wenn die CAPTCHA-Validierung bestanden werden muss.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Boolean
Basissystemwert	**true**
Fallback-Wert	**true**
Empfohlener Wert	**true**

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Aktivieren Sie eine Passwortvalidierungsprüfung für die Deny-Liste

Verwalten Sie die Passwörter der Deny-Liste in der Tabelle „Ausgeschlossenes Passwort“.

Verwenden Sie *glide.enable.blacklist_password*Eigenschaft zur Überwachung von Passwörtern der Deny-Liste. Wenn die Eigenschaft auf festgelegt ist **Wahr** , Das Passwort des Anwenders wird anhand einer Liste der Passwörter der Deny-Liste überprüft, um zu verhindern, dass er ein Passwort aus einer Reihe von Passwörtern mit Verstößen verwendet. Der Administrator kann die Liste verwalten, indem er Passwörter in die Tabelle „Ausgeschlossenes Passwort“ einfügt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.enable.blacklist_password*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Authentifizierung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Schließen Sie Passwörter über Passwortrichtlinien in Ihrer Instanz aus

Captcha für die Registrierung externer Anwender aktivieren [aktualisiert in Security Center 1,3 und 1,5]

Die *sn_ext_usr_reg.captchaEnabled*Steuert, ob CAPTCHA für die Registrierung externer Anwender validiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Festlegen *sn_ext_usr_reg.captchaEnabled*Auf den empfohlenen Wert von **Wahr** Dient zur Verhinderung von Angriffen auf die automatische Account-Erstellung, bei denen CAPTCHA für die Registrierung externer Anwender erforderlich ist. Legen Sie den Wert auf fest **Falsch** Um CAPTCHA für die Registrierung externer Anwender nicht zu erfordern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*sn_ext_usr_reg.captchaEnabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Diese Eigenschaft wird verwendet, um die CAPTCHA-Validierung während der Registrierung externer Anwender in Portalen wie CSP oder Community zu aktivieren oder zu deaktivieren. Dies wird auch in Store-Apps wie VAM und CSM Gast-Walkup verwendet, um Captcha zu aktivieren/deaktivieren.
Empfohlener Wert	True
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) die Eigenschaft steuert die CAPTCHA-Aktivierung in der Registrierung externer Anwender. Der Unideal-Wert kann zu einer Sicherheitslücke führen.
Sicherheitsrisikobewertung	3,7

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Aktivieren Sie CAPTCHA bei Passwortzurücksetzung

Verwenden Sie *password_reset.captcha.ignore*Eigenschaft zum Aktivieren oder Deaktivieren der Anforderung einer CAPTCHA-Herausforderung, wenn ein Anwender sein Passwort zurücksetzt.

Festlegen *password_reset.captcha.ignore*Auf den empfohlenen Wert von **Falsch** Um eine CAPTCHA-Herausforderung für einen Anwender zum Zurücksetzen seines Passworts anzufordern. Legen Sie den Wert auf fest **Wahr** Dient zum Ignorieren der CAPTCHA-Option für eine Passwortzurücksetzung.

CAPTCHAs helfen Automatisierungsangriffe zu verhindern, indem sie den Anwender zur Eingabe einer Challenge-Antwort auffordern, die von automatisierten Systemen nicht leicht beantwortet werden kann. Wenn CAPTCHA deaktiviert ist, kann ein Angreifer bei automatisierten Angriffen auf die Funktion zum Zurücksetzen des Passworts erfolgreicher sein.

Hinweis: Diese Eigenschaft wird nur für die Automatisierung der Passwortzurücksetzung verwendet.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.captcha.ignore*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Diese Eigenschaft wird verwendet, um die CAPTCHA-Validierung während der Passwortzurücksetzung zu aktivieren oder zu deaktivieren.
Empfohlener Wert	falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Moderat) Unideal-Wert kann zu Sicherheitsschwachstellen führen.
Sicherheitsrisikobewertung	5.5

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Aktivieren Sie E-Mail-OTP für die Multifaktor-Authentifizierung

Verwalten Sie, wie die zwei-Faktor-Authentifizierung auf Ihre Instanz angewendet wird.

Verwenden Th E *`glide.authenticate.multifactor.email.otp.enabled`*Eigenschaft, die steuert, ob ein Token für die zwei-Faktor-Authentifizierung per E-Mail gesendet wird. E-Mail wird als schwacher MFA-Faktor betrachtet, auf den ein Angreifer wahrscheinlicher Zugriff erhält, um MFA zu umgehen. Indem Sie diese Eigenschaft auf festlegen **Falsch** , Das Risiko, dass ein Angreifer MFA umgeht, wenn er das Passwort eines Anwenders gefährdet hat, wird reduziert.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.multifactor.email.otp.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Reduziert das Risiko, dass ein fehlerhafter Akteur die zwei-Faktor-Authentifizierung umgeht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	E-Mail als MFA-Faktor

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinienprüfungen für Passwortzurücksetzung aktivieren [aktualisiert in Security Center 2,0]

Verwenden Sie **Glide.enable.password_Policy** Eigenschaft zum Aktivieren von Passwortrichtlinienprüfungen, wenn ein Anwender sein Passwort über die Anwenderoberfläche ändert.

Informationen zum Definieren der Passwortrichtlinie, die verwendet werden soll, sobald diese Eigenschaft aktiviert ist, finden Sie unter Aktivieren Sie Passwortrichtlinien in Ihrer Instanz. Stellen Sie die Glide-Eigenschaft sicher `glide.enable.password_policy`lst vorhanden und auf den Wert „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu.

Hinweis: Die **Glide.enable.password_Policy** Gilt nicht, wenn ein Administrator ein Passwort ändert oder einen Anwender über ein Skript hinzufügt.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.enable.password_policy`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Dient zum Anwenden der Passwortrichtlinie zum Zeitpunkt der Passwortänderung.
Empfohlener Wert	Wahr (für Passwörter mit höherer Stärke)
Sicherheitsrisikobewertung	7.4
Funktionale Auswirkung	Wenn Sie die Eigenschaft auf „wahr“ setzen, werden Passwortrichtlinienprüfungen aktiviert, wenn ein Anwender sein Passwort zurücksetzt.
Sicherheitsrisiko	(Mittel) ohne Passwortrichtlinie kann ein Anwender ein schwaches Passwort erstellen, was die Wahrscheinlichkeit erhöht, dass ein Angreifer Zugriff auf die Instanz erhält.

Schritte zum Konfigurieren

Wenn Sie diese Einstellung auf der Seite „Konfiguration der Härtung-Compliance“ im Instanz-Sicherheitszentrum konfigurieren:

1. Unter **Mittel** , Wählen Sie Aus **Sitzungsverwaltung** .
2. In **Aktivieren Sie Die Richtlinienprüfung Für Die Passwortzurück** Einstellung auswählen **Mittel** Für Passwörter mittlerer Stärke, oder **Stark** Für robustere Passwörter mit höherer Stärke. Wenn Sie eine dieser Optionen auswählen, wird festgelegt **Glide.enable.password_Policy** Eigenschaft auf „wahr“ und startet einen Workflow, der Ihre Passwortrichtlinie automatisch aktualisiert.

Darüber hinaus können Sie festlegen `glide.apply.password_policy.on_login`Systemeigenschaft zum Aktivieren von Passwortrichtlinienprüfungen zum Zeitpunkt der Anmeldung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinienbasierten Sitzungszugriff für Mobilgeräte aktivieren [Neu in Security Center 1,5]

Verwenden Sie das Plugin Zero Trust – richtlinienbasierter Sitzungszugriff, um zu steuern, ob Anwender, die sich über eine mobile App authentifizieren, ihre Rollen reduziert werden.

Mit dem Plugin Zero Trust – richtlinienbasierter Sitzungszugriff können Sicherheitsadministratoren den Anwenderzugriff in einer Sitzung basierend auf Parametern wie IP-Adresse, Standort, Identifizieren von Anbieterattributen und Anwenderattributen mit adaptiven Authentifizierungsrichtlinien reduzieren. Wenn dieses Plugin aktiviert oder auf „wahr“ festgelegt ist, werden für Anwender, die sich über ein Mobilgerät authentifizieren, ihre Rollen gemäß den Richtlinien des Plugins eingeschränkt. Instanzadministratoren möchten möglicherweise den Zugriff mit hohen Berechtigungen einschränken, wenn sich Anwender über ein Mobilgerät authentifizieren, da dies auf eine unsichere Umgebung für vertrauliche Vorgänge hinweisen könnte.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.session_access.mobile.enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Zugriffssteuerung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,7 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Härtungseinstellung auf „wahr“ festgelegt ist, wird für mobile Anmeldungen der richtlinienbasierte Sitzungszugriff in der Instanz erzwungen, und Anwender, die nicht aus einer vertrauenswürdigen Umgebung stammen oder keine vertrauenswürdigen Geräte verwenden, haben ihre Rollen mit eingeschränkten Berechtigungen. „Wahr“ ist die sichere Einstellung. Wenn diese Einstellung auf „falsch“ konfiguriert ist, wird der richtlinienbasierte Sitzungszugriff deaktiviert, und Anwender haben weiterhin die vollen Rollen, einschließlich der Rollen mit hohen Berechtigungen wie Administrator.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn der Administrator die Sitzungszugriffsrichtlinie für die Instanz konfiguriert hat, werden die Rollen von Anwendern nach der mobilen Anmeldung reduziert, wenn sie nicht aus einer vertrauenswürdigen Umgebung stammen oder ein vertrauenswürdiges Gerät verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Adaptive Authentifizierung

Aktivieren Sie den Relaisstatus in SAML-Anforderungen, um Wiederholungsangriffe zu verhindern

Reduzieren Sie das Risiko von Wiedergabeangriffen, indem Sie den Relaisstatus in SAML-Anforderungen aktivieren, um Wiedergabeangriffe zu verhindern.

Schützen Sie mit vor SAML-Wiedergabeangriffen **glide.authenticate.sso.saml2.enable_relay_state_with_id** Systemeigenschaft. Wenn diese Eigenschaft auf festgelegt ist **Wahr** , Der Relaisstatusparameter enthält die sys_ID eines Datensatzes in der Tabelle „MultiSSO-Anforderungsparameter“ [multisso_Request_Parameter], zu dem die Relaisstatus-URL umgeleitet wird.

Legen Sie die Systemeigenschaft fest **glide.authenticate.sso.saml2.enable_relay_state_with_id** Bis **Wahr** . Dies hilft, Angreifer, die Zugriff auf eine SAML-Anforderung erhalten haben, daran zu hindern, auf Ihre Instanz zuzugreifen, indem sie eine gültige Anforderung erneut übermitteln.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	glide.authenticate.sso.saml2.enable_relay_state_with_id
Plugin-Anwendbarkeit	Multi-Provider-SSO-Plugin (com.snc.integration.sso.multi.installer)
Sicherheitsrisiko	Der von dieser Systemeigenschaft aktivierte Relaisstatus hilft, Ihre Instanz vor Wiedergabeangriffen zu schützen. Durch Aktivieren der Eigenschaft können Angreifer, die Zugriff auf eine SAML-Anforderung erhalten haben, nicht auf Ihre Instanz zugreifen, indem sie eine gültige Anforderung erneut übermitteln.
CVSS-Punktzahl (Common Vulnerability Scoring System)	3,8
Bewertung des Common Vulnerability Scoring System (CVSS)	Niedrig
Funktionale Auswirkung	Wenn diese Eigenschaft auf „wahr“ festgelegt ist, enthält der Relaisstatus in einer SAML-Anforderung die sys_ID eines Datensatzes in der Tabelle „MultiSSO-Anforderungsparameter“ [multisso_Request_Parameter], die die Relaisstatus-URL enthält, zu der umgeleitet werden soll.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Boolean
Basissystemwert	wahr
Fallback-Wert	falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	wahr

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

SMS-Codebenachrichtigung für Registrierung und Verifizierung aktivieren [aktualisiert in Security Center 1,3]

Th E *password_reset.sms.use_notify*Die Eigenschaft steuert die Verwendung von SMS-Code-Benachrichtigungen für die Passwortzurücksetzung.

Wenn *password_reset.sms.use_notify* Eigenschaft ist auf den empfohlenen Wert von festgelegt **Wahr** , Der Anwender wird benachrichtigt, das Passwort mithilfe der SMS-Verifizierung und der Registrierung eines neuen Geräts zurückzusetzen, was sicherer ist als E-Mail.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.sms.use_notify*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Booelan
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Macht E-Mail zur Standardmethode für die Passwortwiederherstellung, die weniger sicher als SMS ist.
Abhängigkeiten und Voraussetzungen	Keine

SSL in LDAP-Authentifizierung aktivieren [aktualisiert in Security Center 1,5 und 2,0]

Verwalten Sie die Verschlüsselung von LDAP-Authentifizierungsanforderungen in Ihrer Instanz.

Verwenden t Er *glide.ldap.use.ssl*Eigenschaft zum Aktivieren oder Deaktivieren der TLS-Verschlüsselung für LDAP-Authentifizierungsanforderungen, die über das Netzwerk gesendet werden. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Wahr** , LDAP-Authentifizierung ist anfällig für einen man-in-the-Middle-Angriff.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ldap.use.ssl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** , Macht die LDAP-Authentifizierung für einen man-in-the-Middle-Angriff angreifbar.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Integration von Lightweight Directory Access Protocol

Erzwingen Sie aktuelle Compliance-Anforderungen für Passwortrichtlinien bei der Anmeldung

Reduzieren Sie das Risiko der Brute-Force-Kontoanmeldung, indem Sie aktuelle Compliance-Anforderungen für Passwortrichtlinien bei der Anmeldung durchsetzen.

Helfen Sie, zu verhindern, dass sich interaktive Anwender mit Passwörtern bei der -Instanz anmelden, die die aktuellen Administratoranforderungen nicht erfüllen **Glide.Apply.password_Policy.on_login** Systemeigenschaft.

Legen Sie fest **Glide.Apply.password_Policy.on_login** Systemeigenschaft zu **Wahr** Dient zum Erzwingen der aktuellen Compliance-Anforderungen für Passwortrichtlinien. Wenn diese Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden ist, lautet der Standardwert **Falsch** .

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	Glide.Apply.password_Policy.on_login
Plugin-Anwendbarkeit	Keine
Sicherheitsrisiko	Interaktive Anwender können sich weiterhin mit Passwörtern bei der Instanz anmelden, die die aktuellen Administratoranforderungen nicht erfüllen. Dies kann bedeuten, dass die Anwender über schwache Passwörter verfügen, die die aktuellen Sicherheitsanforderungen nicht erfüllen, was potenziell zu einem erhöhten Risiko von Brute-Force-Account-Anmeldungen durch einen böswilligen Anwender führt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
CVSS-Punktzahl (Common Vulnerability Scoring System)	4.4
Bewertung des Common Vulnerability Scoring System (CVSS)	Mittel
Funktionale Auswirkung	Wenn die vorhandenen Passwörter nicht mit Ihrer aktuellen Passwortrichtlinie übereinstimmen, zwingt die Aktivierung dieser Eigenschaft Anwender, die Passwörter bei ihrer nächsten Anmeldung zu ändern. Diese Eigenschaft wird automatisch auf festgelegt **Falsch** . Wert wird auf festgelegt **Wahr** Erzwingt während der Anmeldung eine Passwortrichtlinie. **Hinweis:** Das Aktivieren dieser Eigenschaft kann dazu führen, dass eine beträchtliche Anzahl von Anwendern, die nicht der neuen Passwortrichtlinie entsprechen, ihre Passwörter ändern muss.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Boolean
Basissystemwert	falsch
Fallback-Wert	falsch
Empfohlener Wert	wahr

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Anforderungen für Geräteverschlüsselung und Passcode erzwingen [Neu in Security Center 1,3]

Die *glide.sg.device_encryption_enabled*Die Eigenschaft erzwingt die Verschlüsselung des Federal Information Processing Standard (FIPS 140-2). Verschlüsselung und Passcode von Mobilgeräten stellen sicher, dass ein nicht autorisierter Anwender nicht auf den Inhalt eines Geräts zugreifen kann, auch wenn das Gerät physisch abgerufen wird.

Wenn *glide.sg.device_encryption_enabled*Ist auf „wahr“ festgelegt, überprüft die mobile ServiceNow-App, ob die Geräteverschlüsselung und der Gerätepasscode aktiviert sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sg.device_encryption_enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,2 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn Verschlüsselung oder Passcode nicht aktiviert ist, darf sich der Anwender auf Mobilgeräten nicht bei der Instanz anmelden
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn diese Eigenschaft auf „wahr“ festgelegt ist, überprüft die mobile App, ob die Geräteverschlüsselung aktiviert ist. Wenn die Verschlüsselung nicht aktiviert ist, dürfen sich Anwender auf Mobilgeräten nicht bei der aktuellen Instanz anmelden. Benutzer werden abgemeldet und sehen die folgende Warnmeldung, die angibt, dass sie eine Geräte-PIN festlegen oder das Gerät verschlüsseln und versuchen, sich erneut anzumelden. You were logged out You need a passcode in order to use this instance on this device. Go to your device's settings to set one up

Ungültige Passwortzurücksetzungsversuche begrenzen [aktualisiert in Security Center 1,3 und aktualisiert in 2,0]

Die `password_reset.request.max_attempt`Wird verwendet, um die maximale Anzahl nicht erfolgreicher Versuche zu steuern, die ein Anwender zurücksetzen oder sein Passwort ändern kann, bevor er für einen bestimmten Zeitraum gesperrt wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.max_attempt`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die maximale Anzahl nicht erfolgreicher Versuche zur Passwortzurücksetzung an, die unternommen werden können, bevor der Anwender vom Prozess zum Zurücksetzen des Passworts ausgeschlossen wird. Der Sperrzeitraum wird durch den Wert in bestimmt `password_reset.request.max_attempt_window`.
Empfohlener Wert	Auf einen positiven ganzzahligen Wert kleiner als drei festlegen. Der Standardwert ist **3**. Wenn Sie den Grenzwert für den oberen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Bereich der Eigenschaft bestimmen, berücksichtigen Sie die Aufgabe, die der Anwender ausführt.
Konfigurationstyp	Positive Ganzzahlwerte
Sicherheitsrisiko	(Hoch) wenn die Eigenschaft nicht auf den empfohlenen Wert festgelegt ist: „ **3** „ Oder einen anderen vernünftigen kleinen Wert, dann könnte es möglich sein, einen Brute-Force-Angriff auf den Prozess zum Zurücksetzen des Passworts durchzuführen.
Sicherheitsrisikobewertung	7,5
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Zeitüberschreitung beim Entsperren nach fehlgeschlagenen Anmeldungen verwalten [aktualisiert in Security Center 1,3]

Es sind zwei Skriptaktionen verfügbar, mit denen ein Websiteadministrator verwalten kann, wie oft ein Anwender ein falsches Passwort angeben kann, bevor er von gesperrt wird ServiceNow AI Platform. Sie können eine dieser Skriptaktionen aktivieren, um fehlgeschlagene Anmeldeversuche zu verwalten.

Weitere Informationen

Attribut	Beschreibung
Name Der Eigenschaft/Des Plugins	N/V
Konfigurationstyp	Systemrichtlinie > Skriptaktionen
Kategorie	Authentifizierung
Zweck	Dient zum Erzwingen einer strikten Richtlinie für fehlgeschlagene Anmeldeversuche, um ein Brute-Erzwingen von Anmeldeinformationen zu vermeiden.
Empfohlener Wert	Aktiv
Sicherheitsrisikobewertung	7.3
Funktionale Auswirkung	Diese Korrektur würde es dem Administrator der Instanz ermöglichen, schädlichen Anwenderzugriff zu überwachen und zu melden. Keine Auswirkung auf die Funktionalität, nur Änderung der Anwender-Experience.
Sicherheitsrisiko	(Mittel) Anwenden Sie eine definierte Protokollierungs- und Auditing-Strategie, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Schritte zum Konfigurieren

1. Navigieren zu **Systemrichtlinie** > **Skriptaktionen.**
2. Suchen Sie nach dem Namen *`*SNC User`*.
3. Um die Verwaltung fehlgeschlagener Anmeldeversuche zu aktivieren, ändern Sie den Status aktiv von entweder *`SNC User Lockout Check with Auto Unlock`*Oder *`SNC User Lockout Check`*Skriptaktionen von **Falsch** Bis **Wahr** .
4. Um den Zähler für fehlgeschlagene Anmeldungen nach einer erfolgreichen Anmeldung zurückzusetzen, können Sie aktivieren *`SNC User Clear`*Skriptaktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Timeout-Dauer für Entsperrung der fehlgeschlagenen Anmeldung maximieren [aktualisiert in Security Center 1,3]

Es sind zwei Skriptaktionen verfügbar, mit denen ein Websiteadministrator verwalten kann, wie oft ein Anwender ein falsches Passwort angeben kann, bevor er von gesperrt wird ServiceNow AI Platform. Sie können eine dieser Skriptaktionen aktivieren, um fehlgeschlagene Anmeldeversuche zu verwalten.

Helfen Sie, Ihre Instanz vor Brute-Force-Angriffen zu schützen, indem Sie einen Zeitraum definieren, in dem ein Anwender nicht versuchen kann, sich anzumelden, nachdem er gesperrt wurde. Die **glide.user.unlock_timeout_in_mins** Die Systemeigenschaft entsperrt den Anwenderaccount nach dem im Wert angegebenen Zeitraum. Wenn kein Wert angegeben ist, entsperrt Ihre Instanz den Anwenderaccount nach dem Standardzeitraum von 15 Minuten.

Legen Sie fest **glide.user.unlock_timeout_in_mins** Systemeigenschaftswert auf mindestens **15** . Wenn **glide.user.unlock_timeout_in_mins** Ist nicht vorhanden, die standardmäßige Sperrzeit ist auf 15 Minuten festgelegt.

Stellen Sie sicher, dass **SNC-Anwendersperrprüfung mit automatischer Entsperrung** Skriptaktion (in der Tabelle „Skriptaktion“ [sysevent_script_action] gefunden) ist vorhanden und aktiv. Die **SNC-Anwendersperrprüfung mit automatischer Entsperrung** Die Skriptaktion wird mit dem Plugin „Einstellungen für hohe Sicherheit“ (com.Glide.High_Security) installiert.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	• glide.user.unlock_timeout_in_mins (Systemeigenschaft) • Sysevent_script_action (Skriptaktion)
Konfigurationstyp	Systemrichtlinie > Skriptaktionen
Kategorie	Authentifizierung
Zweck	Dient zum Erzwingen einer strikten Richtlinie für fehlgeschlagene Anmeldeversuche, um ein Brute-Erzwingen von Anmeldeinformationen zu vermeiden.
Empfohlener Wert	• **15** Für **glide.user.unlock_timeout_in_mins** Systemeigenschaft • **Aktiv** Für **SNC-Anwendersperrprüfung mit automatischer Entsperrung** Skriptaktion.
Funktionale Auswirkung	Diese Korrektur würde es dem Administrator der Instanz ermöglichen, schädlichen Anwenderzugriff zu überwachen und zu melden. Keine Auswirkung auf die Funktionalität, nur Änderung der Anwender-Experience.
Sicherheitsrisiko	• Schweregradpunktzahl: 6,8 • Sicherheitsrisikodetails: Wenn die Eigenschaft nicht auf einen sicheren Wert konfiguriert ist und die Sperrdauer nicht aktiviert ist, kann es

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	einfacher sein, Account-Anmeldungen in einem schnelleren Zeitrahmen zu erzwingen. Dies kann es einem böswilligen Anwender ermöglichen, irgendwann nicht autorisierten Zugriff auf die Instanz zu erhalten. Auswirkungen auf die Instanz sind auf die Privilegierungen der betroffenen Anwenderanmeldung beschränkt.

Schritte zum Konfigurieren

1. Navigieren zu **Systemrichtlinie** > **Skriptaktionen.**
2. Suchen Sie nach dem Namen `*SNC User`.
3. Um die Verwaltung fehlgeschlagener Anmeldeversuche zu aktivieren, ändern Sie den Status aktiv von entweder `SNC User Lockout Check with Auto Unlock`Oder `SNC User Lockout Check`Skriptaktionen von **Falsch** Bis **Wahr** .
4. Um den Zähler für fehlgeschlagene Anmeldungen nach einer erfolgreichen Anmeldung zurückzusetzen, können Sie aktivieren `SNC User Clear`Skriptaktion.

Zeitfenster für Wiederholung der Anforderung zum Zurücksetzen des Passworts maximieren [aktualisiert in Security Center 1,3]

Die `password_reset.request.retry_window`Die Eigenschaft steuert die Anzahl der Minuten, bis die Anzahl der Versuche zur Passwortzurücksetzung aktualisiert wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.retry_window`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt die Dauer in Minuten an, bis die Anzahl der Passwortversuche aus der letzten Anforderung aktualisiert wird, bevor die Anzahl der Wiederholungen auf null zurückgesetzt wird.
Empfohlener Wert	Auf einen positiven ganzzahligen Wert von festlegen **1440** Oder mehr. Der Standardwert ist **1440** Minuten.
Konfigurationstyp	Positive Ganzzahlwerte.
Sicherheitsrisiko	(Hoch) wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder mehr festgelegt ist, kann eine Account-Brute-Force für den Prozess zum Zurücksetzen des Passworts durchgeführt werden.
Sicherheitsrisikobewertung	7,5
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dauer des Entsperrungsfensters für Anforderung zum Zurücksetzen des Passworts maximieren [aktualisiert in Security Center 1,3]

Die `password_reset.request.unlock_window`Die Eigenschaft steuert die Anzahl der Minuten, die ein Anwender nach der letzten erfolgreichen Aktion zum Entsperren des Accounts warten muss, um eine Anforderung zum Zurücksetzen zu starten.

Diese Eigenschaft steuert die Anzahl der Minuten, die ein Anwender nach der letzten erfolgreichen Entsperrung des Accounts warten muss, um eine Anforderung zum Zurücksetzen zu starten. Wenn `password_reset.request.unlock_window`lst nicht auf den empfohlenen Wert von 1440 oder mehr festgelegt, erhöht dies die Möglichkeit für einen böswilligen Akteur, das Passwort des Anwenders mithilfe automatisierter Tools zu erzwingen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.request.unlock_window`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt den Zeitraum in Minuten an, den ein Anwender nach dem erfolgreichen Zurücksetzen des Passworts warten muss, um das Passwort erneut zurückzusetzen.
Empfohlener Wert	1440
Standardwert	1440
Konfigurationstyp	Positive Ganzzahlwerte
Sicherheitsrisiko	(Hoch) wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder höher festgelegt ist, erhöht sie die Möglichkeit eines böswilligen Akteurs, den Passwortzugriff mithilfe automatischer Tools zu erzwingen.
Sicherheitsrisikobewertung	5,9
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

SMS-Komplexität für Passwortzurücksetzung maximieren [aktualisiert in Security Center 1,3]

Die `password_reset.sms.default_complexity`Die Eigenschaft steuert die Mindestgröße der SMS-Codeverifizierung, die während der Passwortzurücksetzung erforderlich ist.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`password_reset.sms.default_complexity`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Authentifizierung
Zweck	Gibt die Größe der SMS-Codeverifizierung an, die während der Passwortzurücksetzung erforderlich ist.
Empfohlener Wert	6
Standardwert	4
Konfigurationstyp	Ganzzahliger Wert größer als Null
Sicherheitsrisiko	(Niedrig) wenn die Eigenschaft nicht auf den empfohlenen Wert festgelegt ist, wird ein schwaches SMS-Validierungstoken verwendet. Dies erhöht die Wahrscheinlichkeit von Token-Erraten, was zur Kontoübernahme führen könnte.
Sicherheitsrisikobewertung	3,8

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Dauer des Pausierfensters zum Zurücksetzen des Passworts maximieren [aktualisiert in Security Center 1,3]

Verwalten Sie die Dauer in Minuten, die ein Anwender warten muss, bevor er einen neuen Code für die Passwortzurücksetzung anfordern kann.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **2** Minuten oder länger, dann kann ein böswilliger Anwender in einem kurzen Zeitfenster viele Passwortzurücksetzungs-Codes initiieren. Dies erhöht die Wahrscheinlichkeit, dass ein schlechter Akteur den SMS-Zurücksetzungscode vorhersagt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`password_reset.sms.pause_window`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	2
Standardwert	2
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,8 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Stellen Sie sicher, dass `password_reset.sms.pause_window`lst auf einen Wert von 2 oder mehr festgelegt.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verzögerungsdauer der Passwortrücksetzung maximieren [aktualisiert in Security Center 1,3]

Konfigurieren Sie die Verzögerung in Millisekunden, die ein Anwender warten muss, bevor er eine neue Anforderung zum Zurücksetzen des Passworts sendet.

Ein schlechter Akteur könnte versuchen, Anmeldeinformationen durch Verwendung von Automatisierungstools wie Bots zu erzwingen **Verzögerung der Passwortverifizierung zurücksetzen** Eigenschaft hilft bei der Verteidigung. Der Eigenschaftswert stellt die Verzögerung in Millisekunden dar, die ein Anwender warten muss, bevor er eine Anforderung zum Zurücksetzen des Passworts stellen kann. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **1000** Oder mehr: Die Anmeldung ist anfälliger für Brute-Force-Angriffe.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.verification.delay*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	1000
Standardwert	1000
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,9 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn Sie den Eigenschaftswert auf weniger als 1000 festlegen, ist Ihre Anmeldung anfälliger für Brute-Force-Angriffe.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Konfigurieren Sie das Passwort für einen Anwender

Minimieren Sie die Ablaufdauer des Links zur Registrierung externer Anwender [aktualisiert im Security Center 1,3 Und 1,5]

Verwalten Sie die Anzahl der Tage, an denen auf einen Registrierungslink zugegriffen werden kann.

Verwenden Die *sn_ext_usr_reg.Reg_link_expiration_days*Eigenschaft zum Verwalten, wer auf einen Registrierungslink zugreifen kann. Wenn der Link auf den empfohlenen Wert von festgelegt ist **3** , Ein Registrierungslink kann von einer anderen Person als dem beabsichtigten Anwender verwendet werden, wenn der Link zu einem späteren Zeitpunkt erkannt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`sn_ext_usr_reg.Reg_link_expiration_days`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	3
Standardwert	3
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: Mittel • CVSS-Punktzahl: 6,6 • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft nicht auf die Ganzzahl 3 festlegen, kann dies dazu führen, dass der Registrierungslink von einem unbeabsichtigten Anwender verwendet wird.
Abhängigkeiten und Voraussetzungen	Keine

Maximale SMS-Anzahl für Passwortzurücksetzungen pro Tag minimieren [aktualisiert im Sicherheitscenter 1,3]

Verwalten Sie die maximale Anzahl von SMS-Codes, die pro Tag vom Anwender zur Verifizierung gesendet werden.

Th E `password_reset.sms.max_per_day`Die Eigenschaft stellt die maximale Anzahl von SMS-Codes dar, die täglich von einem Anwender zur Verifizierung gesendet werden können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`password_reset.sms.max_per_day`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	10
Standardwert	10
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,9 • CVSS-Punktzahl: Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt ist **10** Oder weniger, es ist einfacher, den SMS-Code zu erzwingen.
Abhängigkeiten und Voraussetzungen	Keine

Minimieren Sie fehlgeschlagene Anmeldeversuche für Sitzungen mit hoher Sicherheit

Verringern Sie die Wahrscheinlichkeit eines Brute-Force-Angriffs, indem Sie fehlgeschlagene Anmeldeversuche für Sitzungen mit hoher Sicherheit minimieren.

Verwenden Sie **glide.zta.high_assurance.session.max.login.failed_attempts** Systemeigenschaft zur Beschränkung der Anzahl der fehlgeschlagenen Authentifizierungsversuche, die zulässig sind, bevor Anwender bei der erneuten Authentifizierung durch kontinuierliche Authentifizierung abgemeldet werden.

Legen Sie den Wert dieser Systemeigenschaft auf einen niedrigen Wert (z. B. 5) fest, um die Wahrscheinlichkeit eines Brute-Force-Angriffs zu verringern.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	glide.zta.high_assurance.session.max.login.failed_attempts
Plugin-Anwendbarkeit	Zero Trust – kontinuierliche Authentifizierung (com.snc.Zero_Trust_Continuous_authentication)
Sicherheitsrisiko	Eine hohe Anzahl zulässiger Authentifizierungsversuche erhöht die Wahrscheinlichkeit eines Brute-Force-Angriffs.
CVSS-Punktzahl (Common Vulnerability Scoring System)	3.3
Bewertung des Common Vulnerability Scoring System (CVSS)	Niedrig
Funktionale Auswirkung	Anwender werden nach der Anzahl der in der Eigenschaft ausgewählten Authentifizierungsfehler von ihren Sitzungen abgemeldet.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Ganzzahl
Basissystemwert	5
Fallback-Wert	5
Empfohlener Wert	5

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ablaufdauer der Anforderung zum Zurücksetzen des Passworts minimieren [aktualisiert in Security Center 1,3]

Die *password_reset.request.expiry*Gibt den Zeitraum in Minuten an, in dem ein Anwender den Prozess zum Zurücksetzen des Passworts ausführen muss.

Hinweis: Die Einstellung für *password_reset.request.expiry*Die Eigenschaft hat Vorrang vor der Einstellung für *glide.pwd_reset.onetime.token.validity*Eigenschaft, die einen 12-Stunden-Standard hat.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.expiry*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Gibt den Zeitraum in Minuten an, in dem ein Anwender den Prozess zum Zurücksetzen des Passworts ausführen muss.
Empfohlener Wert	Auf eine Ganzzahl von festgelegt **10** Oder weniger. Der Standardwert ist 10.
Konfigurationstyp	Ganzzahlwerte
Sicherheitsrisiko	(Mittel) wenn die Eigenschaft nicht auf den empfohlenen Wert von 10 oder weniger festgelegt ist, erhöht dies die Möglichkeit für eine andere Person, die Anforderung zu erraten und zu verwenden und zu versuchen, das Passwort zurückzusetzen.
Sicherheitsrisikobewertung	4.2
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Dauer des Erfolgsfensters für die Anforderung zum Zurücksetzen des Passworts minimieren [aktualisiert im Securty Center 1,3]

Die *password_reset.request.success_window*Die Eigenschaft steuert die Anzahl der Minuten, die ein Anwender warten muss, um sein Passwort zurückzusetzen oder erneut zu ändern, nachdem das Passwort erfolgreich zurückgesetzt wurde. Der Anwender wird gesperrt, um das Passwort für die angegebene Dauer erneut zurückzusetzen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*password_reset.request.success_window*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Gibt den Zeitraum in Minuten an, den ein Anwender nach dem erfolgreichen Zurücksetzen des Passworts warten muss, um das Passwort erneut zurückzusetzen.
Empfohlener Wert	1440
Standardwert	1440
Konfigurationstyp	Positive Ganzzahlwerte
Sicherheitsrisiko	(Hoch) wenn die Eigenschaft nicht auf den empfohlenen Wert von 1440 oder weniger festgelegt ist, erhöht sie die Möglichkeit, dass jemand anderes die Funktion zum Zurücksetzen des Passworts missbraucht, um nicht autorisierten Zugriff auf ein Anwenderkonto zu erhalten.
Sicherheitsrisikobewertung	4,9
Referenzen	Konfigurieren Sie Eigenschaften für die Passwortzurücksetzung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

SMS-Ablaufdauer für Passwortzurücksetzung minimieren [aktualisiert in Security Center 1,3]

Steuern Sie die Anzahl der Minuten, die verbleiben, bevor der SMS-Code abläuft.

Th E *password_reset.sms.expiry*Die Eigenschaft stellt die Anzahl der Minuten dar, die verbleiben, bevor der SMS-Code abläuft.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*password_reset.sms.expiry*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	5
Standardwert	5
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 5,6 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt ist **5** Oder weniger erhöht sich die Wahrscheinlichkeit, dass ein schlechter Akteur das Passwort rät und den SMS-Code zum Zurücksetzen des Passworts verwendet.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einmalige Lebensdauer von Out-of-Band-Verifizierern minimieren [aktualisiert in Security Center 1,3]

Verwalten Sie die Zeitdauer für Out-of-Band-Verifizierer.

Ein Out-of-Band-Verifizierer ist eine alternative Bereitstellungsmethode für Situationen mit einmaligem Code. Beispiel: Zurücksetzen eines Multifaktor-Tokens. Wenn diese Methode von Administratoren in aktiviert ist Multi-Faktor-Authentifizierung Plugin, ein einmaliger Code wird per E-Mail zugestellt. Legen Sie die einmaligen Out-of-Band-Verifizierer so fest, dass sie nach 10 Minuten ablaufen, um das Gültigkeitsfenster zu begrenzen. Ein größeres Zeitfenster ermöglicht mehr Zeit, bis der Code durch illegale Mittel wie Phishing, Social Engineering oder Schultersurfangriffe gefährdet wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.multifactor.onetime.code.validity`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	10
Standardwert	10
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,9 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Legen Sie einmalige Out-of-Band-Verifizierer so fest, dass sie nach 10 Minuten ablaufen. Alles, was länger ist, erhöht das Risiko, dass der Code durch einen schlechten Akteur gefährdet wird.
Abhängigkeiten und Voraussetzungen	Multi-Faktor-Authentifizierung
Referenzen	Multifaktor-Authentifizierungskriterien

SAML notBefore- oder notOnOrAfter-Einschränkungsdauer minimieren [aktualisiert in Security Center 1,3 Und 1,5]

Konfigurieren Sie diese Eigenschaft, um einen Toleranzzeitraum hinzuzufügen, in dem SAML-Anforderungen und -Antworten als gültig gelten.

Diese Eigenschaft fügt einen Toleranzzeitraum hinzu, in dem SAML-Anforderungen und -Antworten als gültig gelten. Der Eigenschaftswert stellt die Anzahl der Sekunden dar, die der hinzugefügt werden soll `NotBefore`Und `NotOnOrAfter`Einschränkungen zur Berücksichtigung von Zeitunterschieden zwischen der Uhr des Identitätsanbieters (Identity Provider, IdP) und der Uhr des Service Providers (Service Provider, SP). Diese Einschränkungen schützen vor Wiedergabeangriffen, indem Anforderungen abgelehnt werden, die nicht innerhalb des angegebenen Zeitrahmens gestellt werden. Wenn sich die IdP- und SP-Uhren erheblich unterscheiden, kann die Netzwerklatenz dazu führen, dass die SAML-Anforderung nicht autorisiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.sso.saml2.clockskew`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Weniger als 60
Standardwert	180
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,5 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Wenn Sie die Eigenschaft auf einen Wert von 60 oder höher festlegen, kann dies verhindern, dass die Einschränkungen gegen Wiedergabeangriffe schützen.
Abhängigkeiten und Voraussetzungen	Keine

Anwender während des Prozesses zum Zurücksetzen/Ändern des Passworts benachrichtigen [in Security Center 1,5 entfernt]

Verwenden t Seine Eigenschaft, mit der Endanwender Passwörter mithilfe eines Selfservice-Prozesses zurücksetzen oder ändern können.

Mit dieser Eigenschaft kann ein Endanwender ein Passwort mithilfe eines Selfservice-Prozesses zurücksetzen oder ändern. Alternativ könnte Ihre Organisation einen Prozess implementieren, der erfordert, dass ein Service Desk-Mitarbeiter Passwörter für Endanwender zurücksetzen muss. Wenn ein Prozess zum Ändern und Zurücksetzen des Passworts Anwender nicht über die Passwortaktualisierung benachrichtigt, kann ein schlechter Akteur diesen Anwender ohne sein Wissen aus seinem Account sperren. Dies würde dem schlechten Akteur mehr Zeit zur Ausführung schädlicher Aktivitäten geben. Stellen Sie sicher, dass der Prozess zur Passwortzurücksetzung Anwender über Passwortänderungen oder -Rücksetzungen benachrichtigt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`pwd_process.change, pwd_process.reset`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Ein schlechter Akteur kann einen Anwender ohne sein Wissen aus seinem Account sperren, wenn ihm keine Benachrichtigung gesendet wird, wenn eine Passwortänderung zurückgesetzt wird.
Abhängigkeiten und Voraussetzungen	Keine

Reduzieren Sie die zulässigen Umgehungen für das Multifaktor-Setup

Verringern Sie das Zeitfenster, in dem ein Account gefährdet ist, indem Sie zulässige Umgehungen für das Multifaktor-Setup reduzieren.

Reduzieren Sie die Häufigkeit, mit der ein Anwender die Anforderung zum Einrichten von Multifaktor-Passcodes überspringen kann, um das Zeitfenster zu verkürzen, in dem ein Account gefährdet ist. Multifaktor-Authentifizierung (MFA) schützt vor passwortbezogenen Angriffen oder schwachen Passwörtern, indem eine zusätzliche Form der Verifizierung erforderlich ist. Durch eine Reduzierung der Zeit, die ein Anwender dieses Setup überspringen kann, wird diese Schwachstelle verringert.

Legen Sie fest **glide.authenticate.multifactor.setup.bypass.count** Systemeigenschaft zu **0** Um zu verhindern, dass Anwender das Setup des Multifaktor-Passcodes überspringen.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	glide.authenticate.multifactor.setup.bypass.count
Plugin-Anwendbarkeit	Keine.
Sicherheitsrisiko	Die Multifaktor-Authentifizierung schützt vor passwortbezogenen Angriffen oder schwachen Passwörtern, indem eine zusätzliche Form der Verifizierung erforderlich ist. Eine hohe Anzahl zulässiger Multifaktor-Setup-Umgehungen erhöht das Risiko einer Accountkompromittierung, da der Account nicht durch Multifaktor geschützt ist. Eine geringe Anzahl zulässiger Umgehungen reduziert dieses Zeitfenster.
CVSS-Punktzahl (Common Vulnerability Scoring System)	3,9
Bewertung des Common Vulnerability Scoring System (CVSS)	Niedrig
Funktionale Auswirkung	Anwender dürfen sich nicht bei einer Instanz anmelden, ohne MFA einzurichten, wenn sie die in der Eigenschaft angegebene Anzahl der Anmeldungen überschritten haben.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	Ganzzahl
Basissystemwert	0
Fallback-Wert	0
Empfohlener Wert	0

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Entfernen Sie Anmeldeinformationen von der Willkommensseite

Ändern Sie den Standardinhalt auf der Willkommensseite, um die Standard-Anmeldeinformationen zu entfernen.

Zwei **So melden Sie sich an** Datensätze werden als Teil der Demodaten für das CMS-Plugin installiert.

Hinweis: Wenn Sie die Demodaten für eine Instanz nicht installieren, sind diese Datensätze nicht vorhanden. In diesem Fall wird die Konfiguration gemäß den empfohlenen Sicherheitspraktiken als sicherheitskonform betrachtet.

Weitere Informationen

Attribut	Beschreibung
Name	*How to login*
Konfigurationstyp	Tabelle: sys_HOME
Kategorie	Authentifizierung
Zweck	Dient zum Entfernen von Standard-Anmeldeinformationen von der Willkommensseite, die mit Demodaten hinzugefügt wurden.
Empfohlener Wert	Falsch oder null, wenn keine Demodaten verwendet wurden.
Standardwert	Keine. Dies ist eine Tabellenkonfiguration, keine Glide-Eigenschaft. Daher ist kein Wert für den Standardwert vorhanden.
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Mittel) Demodaten werden für das CMS-Plugin bereitgestellt, das zwei Standardpasswörter enthält, die auf der Willkommensseite enthalten sind. Wenn dies nicht entfernt wird, kann ein nicht autorisierter Angreifer Zugriff auf die Instanz erhalten.
Referenzen	https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107 Willkommensseiten

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Captcha für Gast-Walk-up-Experience in der Kundenserviceanwendung [Neu in Security Center 1,3 Und aktualisiert 1,5]

Das Captcha für die Gast-Walk-up-Experience verhindert, dass nicht authentifizierte Gastanwender Buchungen erstellen, indem Anwender eine Captcha-Verifizierung durchführen müssen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_guest_walkup_cs.captcha.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn CAPTCHA nicht aktiviert ist, kann dies zur automatisierten Erstellung von Spam-Terminen führen, um das System zu überfordern oder alle verfügbaren Buchungspunkte zu füllen und einen Denial of Service (DoS)-Angriff zu erstellen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft aktiviert oder deaktiviert das Captcha in den CSM-Gast-Walkup-Check-in-Widgets. Standardmäßig ist sie auf „wahr“ festgelegt.

Verschleierung der klassischen mobilen App-UI erfordern [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.ui.m.blur_ui_when_backgrounded*Eigenschaft zum Verschleieren aller Felder aus dem Snapshot, während das Image während des Background-Prozesses gespeichert wird.

Auf Android-Geräten nimmt das Android-Betriebssystem einen Screenshot zur Verwendung im Menü „aktuelle Aufgaben“ auf, wenn die Anwendung in den Hintergrund gesendet wird. Benutzer können auch manuelle Screenshots der Anwendung erstellen, die öffentlich auf dem Gerät gespeichert werden.

Auf iOS-Geräten ermöglicht das iOS-Betriebssystem auch Anwendungen das Speichern einer Bilddatei. Diese Datei stellt den letzten Bildschirm dar, der dem Anwender angezeigt wurde, wenn die Anwendung in den Hintergrund gesendet wird. Die Absicht besteht zwar darin, eine bessere Anwender-Experience zu bieten, stellt jedoch auch ein Sicherheitsrisiko dar, da die Bilder als PNG-Bilddateien gespeichert werden.

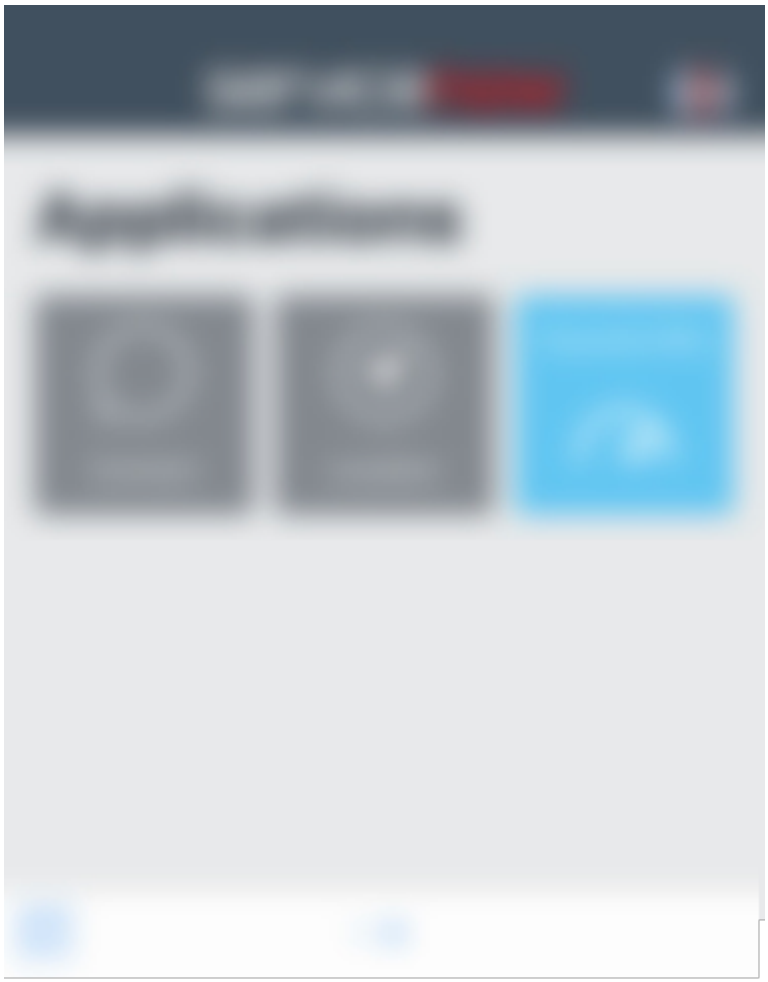
Hinweis: Diese Einstellung oder Konfiguration gilt pro Instanz, daher muss der Anwender mit der konfigurierten Eigenschaft eine Verbindung zur Instanz herstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Verschleieren aller Felder aus dem Snapshot in der ServiceNow Classic-App finden Sie unter Konfigurieren Sie die Option „Unschärfe-App“, um die Sicherheit zu verbessern .

Beispiel

Wenn Sie diese Eigenschaft auf festlegen Wahr , B Die ackground-Anwendung ist für iOS-Geräte verschleiert und für Android-iOS-Geräte gesperrt.



Weitere Informationen

Attribut	Beschreibung
Name Der Eigenschaft/Des Plugins	`glide.ui.m.blur_ui_when_backgrounded`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Authentifizierung
Zweck	Dient zum Verschleieren aller Felder aus dem Snapshot, wenn das Bild während des Background-Prozesses gespeichert wird.
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	2.4
Funktionale Auswirkung	Wenn `glide.ui.m.blur_ui_when_backgrounded`Eigenschaft ist auf festgelegt Wahr , Die nativen Apps verwenden den auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	dem Server definierten Parameter, um den Bildschirm unscharf zu machen, wenn die App in den Hintergrund wechselt. • Die von iOS und Android erstellten Screenshots werden unscharf dargestellt, wenn die App in den Hintergrund wechselt. • Die Anwender-Experience kann sich nachteilig auswirken, da sie den Inhalt nicht sehen können, wenn die App in den Hintergrund gesendet wird.
Sicherheitsrisiko	(Mittel) Ein kompromittiertes (Jailbreak) Gerät würde einem Angreifer vollständigen Zugriff auf das Dateisystem ermöglichen und auf diese Dateien/Snapshots zugreifen, in denen vertrauliche Informationen eingebettet sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Verschleierung der mobilen App-UI erfordern [aktualisiert in Security Center 1,3]

Konfigurieren Th E *glide.sg.blur_ui_when_backgrounded*Eigenschaft, damit die UI der App unscharf ist, wenn die App im Hintergrund ausgeführt wird.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Wahr** , Die Anwenderoberfläche der mobilen App ist sichtbar, wenn sie über den App-Umschalter angezeigt wird. Die Anwenderoberfläche ist auch dann sichtbar, wenn die App im Hintergrund ausgeführt wird, was Endanwendern ein niedrigeres Maß an Sicherheit und Vertraulichkeit bietet.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.sg.blur_ui_when_backgrounded*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 2,4 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wert wird auf festgelegt **Wahr** Bietet ein höheres Maß an Vertraulichkeit und Datenschutz auf dem lokalen Gerät, indem die Anwenderoberfläche unscharf dargestellt wird, wenn die App im Hintergrund ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Verschleierung der klassischen mobilen App-UI erfordern [aktualisiert in Security Center 1,3]

Legen Sie die minimale Passwortlänge fest [Aktualisiert im Sicherheitscenter 2,2]

Legen Sie eine minimale Passwortlänge fest, um Compliance-Probleme zu vermeiden und das Risiko eines erfolgreichen Brute-Force-Angriffs zu reduzieren

Erzwingen Sie eine Passwortlänge von mindestens 12 Zeichen, um Compliance-Probleme zu vermeiden und das Risiko eines erfolgreichen Brute-Force-Angriffs zu reduzieren.

Stellen Sie für jeden verwendeten Passwort-Anmeldeinformationsspeicher, der in Ihrer Instanz verwendet wird, sicher, dass eine Passwortrichtlinie durchgesetzt wird, indem Sie auswählen **Aktivieren Sie die Passwortrichtlinie** Feld im zugehörigen Datensatz in der Tabelle „Anmeldeinformationsspeicher für Passwortzurücksetzung“ [pwd_cred_Store].

Öffnen Sie als Nächstes den Datensatz in der Datensatztabelle „Passwortrichtlinie“ [password_Policy], und legen Sie fest **Mindestlänge Des Passworts** Feld bis mindestens **12** . Sie finden den zugehörigen Passwortrichtliniendatensatz im **Passwortrichtlinie** Feld des Datensatzes „Anmeldeinformationsspeicher für Passwortzurücksetzung“ [pwd_cred_Store].

Weitere Informationen zum Konfigurieren einer Passwortrichtlinie finden Sie unter Aktivieren Sie Passwortrichtlinien in Ihrer Instanz.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	Datensätze in den Tabellen „Anmeldeinformationsspeicher für Passwortzurücksetzung“ [pwd_cred_Store] und „Passwortrichtlinie“ [password_Policy].
Plugin-Anwendbarkeit	Keine
Sicherheitsrisiko	Wird festgelegt **Mindestlänge Des Passworts** Richtliniendatensätze [password_Policy] mit einem Wert von weniger als 12 können zu Compliance-Problemen führen und das Risiko erhöhen, dass ein Angreifer Passwörter erfolgreich per Brute erzwingt.
CVSS-Punktzahl (Common Vulnerability Scoring System)	5,9
Bewertung des Common Vulnerability Scoring System (CVSS)	Mittel
Funktionale Auswirkung	Die Instanz hat keine Auswirkungen bei einer Mindestlänge von 12 Passwörtern.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Ganzzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Basissystemwert	8
Fallback-Wert	8
Empfohlener Wert	12

OTP-Lebensdauer für Passwortzurücksetzung auf 1 Stunde festlegen [aktualisiert in Security Center 2,0]

Steuern Sie die Dauer des Links in der E-Mail zur Passwortzurücksetzung.

Die `glide.pwd_reset.onetime.token.validity`Die Systemeigenschaft bewirkt, dass der Link in der E-Mail zur Passwortzurücksetzung nach der in der Eigenschaft angegebenen Anzahl von Stunden abläuft. Die Gültigkeitszeit eines Passwortzurücksetzungs-Tokens sollte so kurz wie möglich gehalten werden, ohne die normale Anwender-Experience zu beeinträchtigen

Legen Sie den Eigenschaftswert auf 1 (in Stunden) fest.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.pwd_reset.onetime.token.validity`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	1
Standardwert	1
Fallback-Wert	1
Kategorie	Authentifizierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,6 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Eine längere Gültigkeitsdauer für das Token zur Passwortzurücksetzung bietet böswilligen Akteuren ein größeres Fenster, um die Kontoübernahme durchzuführen, wenn die E-Mail mit dem Token zum Zurücksetzen undicht ist oder gefährdet ist.
Abhängigkeiten und Voraussetzungen	Keine

Geschäftslogik

Diese Kategorie betrachtet die Logik und den Flow, die für jede Anwendung eindeutig sind, mit allgemeinen Sicherheitsprinzipien. Stellen Sie insbesondere sicher, dass die beabsichtigte Sequenz des Geschäftslogik-Flows nicht umgangen werden kann, dass Grenzen zum Erkennen und verhindern automatisierter Angriffe vorhanden sind und dass Schutz vor Spoofing, Manipulation, Offenlegung von Informationen und Erhöhung von Berechtigungen vorhanden ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden finden Sie einige Sicherheitskontrollen, die ein Administrator konfigurieren kann, um nicht autorisierten Zugriff auf vertrauliche Entitäten innerhalb von zu beschränken ServiceNow AI Platform.

Begrenzen Sie die maximale Anzahl von Kommentaren pro Anwender und Tag

Konfigurieren Sie *sn_kb_social_qa.max_comments_per_user_daily*Eigenschaft zum Einschränken der Anzahl der QA-Kommentare pro Tag.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **500** Oder weniger: Es gibt keine Einschränkung für die Anzahl der QA-Kommentare pro Tag, die zu einer Erschöpfung der Ressourcen führen könnten.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_kb_social_qa.max_comments_per_user_daily*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	500
Standardwert	500
Kategorie	Geschäftslogik
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn der empfohlene Wert dieser Eigenschaft nicht auf 500 oder weniger festgelegt wird, ist kein Limit für QA-Kommentare pro Tag festgelegt, was zu einer Erschöpfung der Ressourcen führen könnte.
Abhängigkeiten und Voraussetzungen	Keine

Begrenzen Sie die maximalen Abonnements pro Anwender und Tag

Konfigurieren Th E *sn_kb_social_qa.max_subscriptions_per_user_daily*Eigenschaft zum Einschränken der maximalen Anzahl von Abonnements, die ein Anwender an einem Tag abonnieren kann.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **500** Oder weniger: Es gibt keine Einschränkung für die maximale Anzahl von F&A-Fragen, die ein Anwender an einem Tag abonnieren kann. Diese keine Einschränkung kann zu einer Erschöpfung der Ressourcen führen und sich auf die Verfügbarkeit Ihrer Instanz auswirken.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_kb_social_qa.max_subscriptions_per_user_daily*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	Ganzzahl
Empfohlener Wert	500
Standardwert	500
Kategorie	Geschäftslogik
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Legen Sie den Eigenschaftswert auf maximal 500 fest, um eine Erschöpfung der Ressourcen zu verhindern.
Abhängigkeiten und Voraussetzungen	Keine

SMTP-Empfängermenge minimieren [Aktualisiert in Security Center 1,3]

Die `glide.email.smtp.max_recipients`Gibt die maximale Anzahl von Empfängern an, die die Instanz in auflisten kann **An:** Zeile für eine einzelne E-Mail-Benachrichtigung.

Festlegen `glide.email.smtp.max_recipients`Auf den empfohlenen Wert von **100 oder weniger** . Benachrichtigungen, die diese Grenze überschreiten, erstellen stattdessen doppelte E-Mail-Benachrichtigungen, die an eine Teilmenge der Empfängerliste adressiert sind. Jede E-Mail-Benachrichtigung hat dieselbe maximale Anzahl an Empfängern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.email.smtp.max_recipients`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Geschäftslogik
Zweck	Wenn diese Eigenschaft auf einen unsicheren Wert über dem Standardwert von 100 festgelegt ist, kann es zu einem Denial of Service in der Instanz kommen.
Empfohlener Wert	100
Standardwert	100
Konfigurationstyp	Ganzzahl
Sicherheitsrisiko	(Mittel) Benachrichtigungen, die diesen Grenzwert überschreiten würden, erstellen stattdessen doppelte E-Mail-Benachrichtigungen, die an eine Teilmenge der Empfängerliste adressiert sind.
Sicherheitsrisikobewertung	4,9

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitüberschreitung Bei Gastsitzungen

Verwenden Sie eine Systemeigenschaft, um die Zeitüberschreitung bei inaktiven Sitzungen für nicht authentifizierte Anwender zu steuern.

Verwenden Sie `glide.guest.session_timeout`Systemeigenschaft zum Festlegen der Zeitüberschreitungsdauer für inaktive Sitzungen (in Minuten) für nicht authentifizierte Anwender. Erhöhen Sie den Wert dieser Eigenschaft, um die Zeit zu verlängern, die Ihre Instanz Sitzungen über den Standardwert von 30 Minuten hinaus aufrechterhält. Vermeiden Sie große Zeitüberschreitungswerte, die die Anzahl der von der Instanz beibehaltenen Sitzungen erhöhen und geringfügige Verfügbarkeitsbedenken verursachen können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.guest.session_timeout`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl (in Minuten)
Empfohlener Wert	30
Standardwert	30
Fallback-Wert	0
Kategorie	Geschäftslogik
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Große Zeitüberschreitungswerte können die Anzahl gleichzeitiger Sitzungen in Ihrer Instanz erhöhen, was geringfügige Verfügbarkeitsbedenken verursacht.
Abhängigkeiten und Voraussetzungen	Keine

Validieren Sie den Remote-Host

Legen Sie die Eigenschaft auf „wahr“ fest, um zu verhindern, dass fehlerhafte Akteure interne Port-Scans in Ihrem Netzwerk verwenden.

Wenn `glide.update_set.remote.check_host`Eigenschaft ist nicht auf den empfohlenen Wert von festgelegt **Wahr** , Dann Die Testfunktion der Remote-Instanz ermöglicht interne Port-Scans. Dies ist eine Methode, die schlechte Akteure verwenden können, um Schwachstellen in einem Netzwerk zu erkennen. Es ist dann möglich, alle offenen Ports auf einem bestimmten Host aufzuzählen und in einigen Fällen Antwortdaten abzurufen, die zu Informationsverlusten oder nicht autorisiertem Datenzugriff führen können.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.update_set.remote.check_host`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Geschäftslogik
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Eigenschaft wird nicht auf den empfohlenen Wert festgelegt **Wahr** Kann es fehlerhaften Akteuren ermöglichen, interne Port-Scans zu verwenden, um Zugriff auf nicht autorisierte Daten zu erhalten.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132 Remote-Instanzen definieren

Kommunikation

Diese Steuerung stellt eine ordnungsgemäße Verschlüsselung mit starken Algorithmen und Verschlüsselungen sicher. Dies umfasst die Verwendung der empfohlenen Version von TLS für die Client-Konnektivität, die Verwendung starker Verschlüsselungs-Suites, die Verwendung vertrauenswürdiger und signierter Zertifikate, die Verschlüsselung von Verbindungen zwischen Komponenten und die Protokollierung von Verbindungsfehlern.

Zertifikatvertrauen erzwingen [aktualisiert in Security Center 1,3, Wurde in 2,0 entfernt , Hinzugefügt in 7,0]

Verwenden Sie Systemeigenschaften, um sicherzustellen, dass Zertifikatablauf und -Vertrauen für Zertifikate überprüft werden, die von ausgehenden HTTPS-Aufrufendpunkten empfangen werden, wenn keine Hostverifizierung durchgeführt wird.

Wenn `com.glide.communications.trustmanager_trust_all`lst auf festgelegt **Wahr** , Dann werden Zertifikatablauf und Vertrauen für das Zertifikat, das von einem ausgehenden HTTPS-Aufrufendpunkt empfangen wurde, nicht überprüft, wenn keine Hostverifizierung durchgeführt wird.

Überprüfen Sie, ob `com.glide.communications.trustmanager_trust_all`Systemeigenschaft ist auf den empfohlenen Wert von festgelegt **Falsch** . Dadurch wird sichergestellt, dass Ihre Instanz nur Zertifikaten vertraut, die sie anhand des JVM-Zertifikatspeichers verifizieren kann. Selbst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

signierte und vom Unternehmen signierte Zertifikate sind nicht vertrauenswürdig. Diese Eigenschaft gilt nur, wenn *com.glide.communications.httpclient.verify_hostname*lst auf festgelegt **Falsch** .

Hinweis: Die Werte für diese Eigenschaften sind Und kann nach der Änderung nicht geändert werden (sie können nicht rückgängig gemacht werden). Ändern Sie diesen Eigenschaftswert aus Sicherheitsgründen nicht. Wenn Sie weitere Fragen haben, wenden Sie sich an Kundenservice und Support.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.communications.trustmanager_trust_all*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Kommunikation
Zweck	Dient zum Erzwingen der Zertifikatvalidierung für ausgehende Anforderungen.
Empfohlener Wert	falsch
Sicherheitsrisikobewertung	5,7
Funktionale Auswirkung	Diese Korrektur erzwingt eine strikte Validierung des Felds „Zertifikat-CA“ (Certificate Authority). Wenn eine vertrauenswürdige Entität (CA) das Zertifikat ausgestellt hat, akzeptiert die Instanz es zur weiteren Verwendung.
Sicherheitsrisiko	(Mittel) aus Gründen der Vertraulichkeit und Integrität sollte die Anwendung die CA des Zertifikats validieren, bevor das Zertifikat für Transaktionsvorgänge verwendet wird.
Referenzen	Zertifikate Zertifikatkette und Hostname verifizieren [Neu in Security Center 1,3 und aktualisiert in 2,0]

Ausgehende SSLv2/SSLv3-Verbindungen deaktivieren [aktualisiert im Sicherheitscenter 1,3]

Verwenden Sie *glide.outbound.sslv3.disabled*Eigenschaft, um zu erzwingen, dass der MID-Server TLS verwendet, wenn ausgehende Verbindungen hergestellt werden, z. B. REST- und SOAP-Anforderungen. Normalerweise werden ausgehende Verbindungen von einer Instanz gezwungen, TLS anstelle von SSL zu verwenden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.outbound.sslv3.disabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Kommunikation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Um die Verwendung von „wenn TLS verwenden“ während aller ausgehenden Verbindungen von der ServiceNow-Instanz zu erzwingen.
Empfohlener Wert	wahr
Standardwert	falsch **Wichtig:** Der Wert für `glide.outbound.sslv3.disabled`Eigenschaft ist eine sichere Überschreibung und kann nach der Änderung nicht geändert werden.
Sicherheitsrisikobewertung	6.5
Funktionale Auswirkung	Diese Korrektur erzwingt die Verwendung der TLS-Protokollversion bei der Kommunikation über HTTPS. Wenn Geräte vorhanden sind, die Kunden/Anwender der Instanz verwenden und die TLS-Kommunikation nicht unterstützen, kann es zu einem potenziellen Ausfall kommen.
Sicherheitsrisiko	(Mittel) Legacy-Versionen von SSL haben sich bei Verwendung für die Implementierung einer sicheren HTTP-Shell aufgrund von clientseitigen Angriffen wie BEAST und SSL Heart Bleed als unsicher erwiesen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Verwenden Sie keine Demozertifikate für aktive saml-Konfigurationen [Aktualisiert in Security Center 1,5]

Steuert, ob Demozertifikate in SAML-Konfigurationen der Produktion verwendet werden.

Die von ServiceNow bereitgestellten Demozertifikate sollten nicht in Produktions-SAML-Konfigurationen verwendet werden, da sie unter allen Instanzen mit einer bekannten Passphrase üblich sind. Wenn eine der SAML-Eigenschaften, die einen Zertifikatschlüsselspeicher verwenden, aktiv ist (`require_signed_authnrequest`, `require_signed_logoutrequest`, Oder `encrypt_assertion`), dann sollten die Demodaten nicht verwendet werden. Da Demodaten von allen Instanzen gemeinsam genutzt werden, gibt es keine Integritätsgarantie für Anforderungen, die mit gemeinsam genutzten Zertifikaten signiert wurden. Daher kann jede vom IDP verschlüsselte Nachricht von einem ungültigen Akteur entschlüsselt werden, wenn sie abgefangen wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.sso.saml2.keystore`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	sys_ID eines anwenderdefinierten Schlüsselspeichers
Standardwert	Leere Zeichenfolge

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: 3,9 • CVSS-Punktzahl: Niedrig
Abhängigkeiten und Voraussetzungen	Keine

Deaktivieren Sie veraltete TLS-Versionen

Vermeiden Sie den Verlust oder den Verlust vertraulicher Daten, indem Sie veraltete TLS-Versionen deaktivieren.

Bestätigen Sie, dass Ihre Instanz bei der Kommunikation mit anderen Servern nur für die Kommunikation über TLS-Versionen (Transport Layer Security) 1,2 verhandelt, um zu verhindern, dass Daten über schwächere TLS 1- und TLS 1,1-Protokollversionen übertragen werden.

Legen Sie fest **com.glide.communications.disable.deprecated.tls** Bis **Wahr** Zur Verwendung nur TLS-Versionen 1,2 und höher.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	com.glide.communications.disable.deprecated.tls
Plugin-Anwendbarkeit	Keine
Sicherheitsrisiko	Die Verwendung veralteter und nicht unterstützter TLS-Versionen kann zu Verlust und Verlust vertraulicher Daten führen.
CVSS-Punktzahl (Common Vulnerability Scoring System)	4.4
Bewertung des Common Vulnerability Scoring System (CVSS)	Mittel
Funktionale Auswirkung	Wenn diese Eigenschaft auf festgelegt ist **Wahr** , Ältere unsichere Server, die ein schwächeres TLS 1- oder 1,1-Protokoll erfordern, können nicht mit Ihrer Instanz kommunizieren.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Boolean
Basissystemwert	wahr
Fallback-Wert	wahr
Empfohlener Wert	wahr

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OCSP-Prüfung bei Netzwerkfehler erzwingen [Neu in Security Center 1,3 und aktualisiert in 2,0]

Erfahren Sie, wie Sie konfigurieren `com.glide.communications.httpclient.ocsp_allow_network_error`Eigenschaft, um zu verhindern, dass fehlerhafte Akteure OCSP-Prüfungen (Online Certificate Status Protocol) umgehen.

Wenn `com.glide.communications.httpclient.ocsp_allow_network_error`lst nicht auf den empfohlenen Wert „falsch“ festgelegt, und bei der OCSP-Prüfung (Online Certificate Status Protocol) wird ein Netzwerkfehler festgestellt (z. B. eine Zeitüberschreitung oder ein Problem beim Abrufen der Widerrufsinformationen), wird die OCSP-Sicherheitsprüfung umgangen und als erfolgreich betrachtet. Dies kann einem Angreifer mit einem widerrufenen Zertifikat ermöglichen, die Infrastruktur des öffentlichen Schlüssels (PKI) und das Vertrauen des digitalen Zertifikats zu unterbrechen, die für das Web grundlegend sind. Die Verwendung widerrufener Zertifikate ist häufig ein Indikator für schädliche Aktivitäten, es sei denn, die Server sind nicht synchronisiert.

Stellen Sie die Eigenschaft sicher `com.glide.communications.httpclient.ocsp_allow_network_error`lst vorhanden und auf „falsch“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.communications.httpclient.ocsp_allow_network_er`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	wahr
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: 5,9 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft nicht auf „falsch“ festlegen, kann ein ungültiger Akteur die OCSP-Sicherheitsprüfung umgehen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft bestimmt, ob eine Anforderung für den URI des Authority Information Access (AIA) Online Certificate Status Protocol (OCSP) im Falle eines Verbindungs- oder Zeitüberschreitungsfehlers zu einem Bestanden- oder Fehlgeschlagen-Ergebnis führt. Bei „falsch“ kann der Sperrstatus des angegebenen Serverzertifikats nicht validiert werden, was zu einem Kommunikationsfehler mit diesem Endpunkt führt. Wenn ein Netzwerkfehler auftritt, wenn die Eigenschaft auf den Standardwert „wahr“ festgelegt ist, wird das Zertifikat vom Standpunkt des Widerrufs aus als gültig behandelt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatkette und Hostname verifizieren [Neu in Security Center 1,3 und aktualisiert in 2,0]

Konfigurieren Sie *com.glide.communications.httpclient.verify_hostname*Eigenschaft zur Verhinderung von man-in-the-Middle-Angriffen, indem sichergestellt wird, dass der Zertifizierungsverifizierungsprozess ausgeführt wird.

Wenn die Glide-Eigenschaft *com.glide.communications.httpclient.verify_hostname*lst nicht auf den sicheren Wert „wahr“ festgelegt, werden Hostname und Zertifikatkette, die von Remote-Hosts während einer von der ServiceNow-Instanz initiierten TLS-Verbindung angezeigt werden, nicht validiert. Dies könnte die Sicherheit der TLS-Verbindung gefährden und Personen-in-the-Middle-Angriffe ermöglichen, bei denen die Kommunikation zwischen zwei Parteien abgefangen wird. Dies kann zur Offenlegung vertraulicher Daten führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.communications.httpclient.verify_hostname*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: Hoch • CVSS-Punktzahl: 7,4 • Sicherheitsrisikodetails: Keine Einstellung *com.glide.communications.httpclient.verify_hostname*Mit dem empfohlenen Wert „wahr“ kann Ihre Instanz für man-in-the-Middle-Angriffe angreifbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Überprüft den Hostnamen und die Zertifikatkette, die von Remote-SSL-Hosts (Secure Socket Layer) dargestellt werden. Legen Sie diese Eigenschaft auf „wahr“ fest, um sich vor MITM-Angriffen (man-in-the-Middle) zu schützen. **Hinweis:** Diese Eigenschaft überschreibt *com.glide.communications.trustmanager_trust_all*, Eigenschaft.

Zertifikatwiderruf verifizieren [Neu in Security Center 1,3]

Die *com.glide.communications.httpclient.verify_revoked_certificate*Die Eigenschaft überprüft den Zertifikatwiderruf während des TLS-Handshake (Transport Layer Security), um sicherzustellen, dass Sicherheitsprüfungen nicht umgangen werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn *com.glide.communications.httpclient.verify_revoked_certificate*lst nicht auf den empfohlenen Wert von festgelegt **Wahr** , Dann wird der Zertifikatwiderruf während des TLS-Handshake nicht überprüft. TLS verschlüsselt Daten, die über das Internet gesendet werden, um sicherzustellen, dass fehlerhafte Akteure vertrauliche Informationen wie Passwörter oder Kreditkartennummern nicht sehen können. Die Umgehung des TLS-Handshake ist ein Sicherheitsrisiko, da ein Angreifer mit einem widerrufenen Zertifikat die Bereitstellung eines gültigen Zertifikats vernachlässigen und die PKI-Infrastruktur (Public Key Infrastructure, PKI) und das digitale Zertifikat-Trust unterbrechen kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.communications.httpclient.verify_revoked_certif*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Keine Einstellung *com.glide.communications.httpclient.verify_revoked_cert* der empfohlene Wert „wahr“ erreicht wird, wird der Zertifikatwiderruf während des TLS-Handshake nicht überprüft.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft muss auf „wahr“ festgelegt werden, um sicherzustellen, dass eine TLS-Sitzung (Transport Layer Security) mit einem authentischen Endpunkt gestartet wird. Wenn diese Eigenschaft auf „falsch“ festgelegt ist, wird das Zertifikat nicht überprüft, was die Sicherheit der Instanz beeinträchtigen könnte.

Automatische Übersetzung

Konfiguration

Die Kategorie „Konfiguration“ stellt sicher, dass Anwendungen über eine sichere Build-Umgebung und gehärtete Drittanbieterbibliothekskomponenten verfügen. Insbesondere muss sichergestellt werden, dass eine Build- und Bereitstellungs-Pipeline wiederholbar ist, automatisierte Tests umfasst und verhindert, dass bekannte Sicherheitsprobleme bereitgestellt werden. Dies beinhaltet, Abhängigkeiten auf dem neuesten Stand und frei von bekannten Schwachstellen zu halten.

Inhaltstypoptionen automatisch festlegen [in Security Center 1,3.3 entfernt]

Konfigurieren Sie die Eigenschaft „Inhaltstypoptionen automatisch festlegen“ in Ihrer Instanz, um MIME-Verwirrungsangriffe zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie diese Eigenschaft, um den HTTP-Header der Antwort X-Content-Type-Options zu steuern. Der HTTP-Header der Antwort „X-Content-Type-Options“ wird vom Server verwendet, um anzugeben, dass die in den Content-Type-Headern angegebenen MIME-Typen befolgt werden sollen. Wenn diese Eigenschaft auf festgelegt ist Falsch , Dann ist es für einen Angreifer möglich, MIME-Verwirrungsangriffe durchzuführen; ich f auf festgelegt Wahr Dann verhindert dieser Header, dass der Browser Dateien als alles andere als den Inhaltstyp in den HTTP-Headern interpretiert.

⚠ **Warnung:** Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.header.auto_set_x_content_type_options`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 7,3 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Kann es einem Angreifer ermöglichen, MIME-Verwirrungsangriffe durchzuführen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Systemeigenschaft hinzufügen

HTTP-Header-Wert für Cache-Steuerung [in Security Center 1,3 aktualisiert und 1,5 entfernt]

Verwenden Sie `glide.http.cache_control`Eigenschaft zum Festlegen des standardmäßigen Cache-Control-Werts in den HTTP-Antwortheadern, die ServiceNow AI Platform Sendet, wenn statische Inhaltsdaten für eine Seite angefordert werden. Beispiele für statischen Inhalt sind Bilder, CSS und JavaScript, die innerhalb für eine Seite gerendert werden.

Die `glide.http.cache_control`Die Eigenschaft legt den standardmäßigen Cache-Control-Wert in HTTP-Antwortheadern auf fest **Privat** Oder **Öffentlich** . Der Standardwert ist **Privat** .

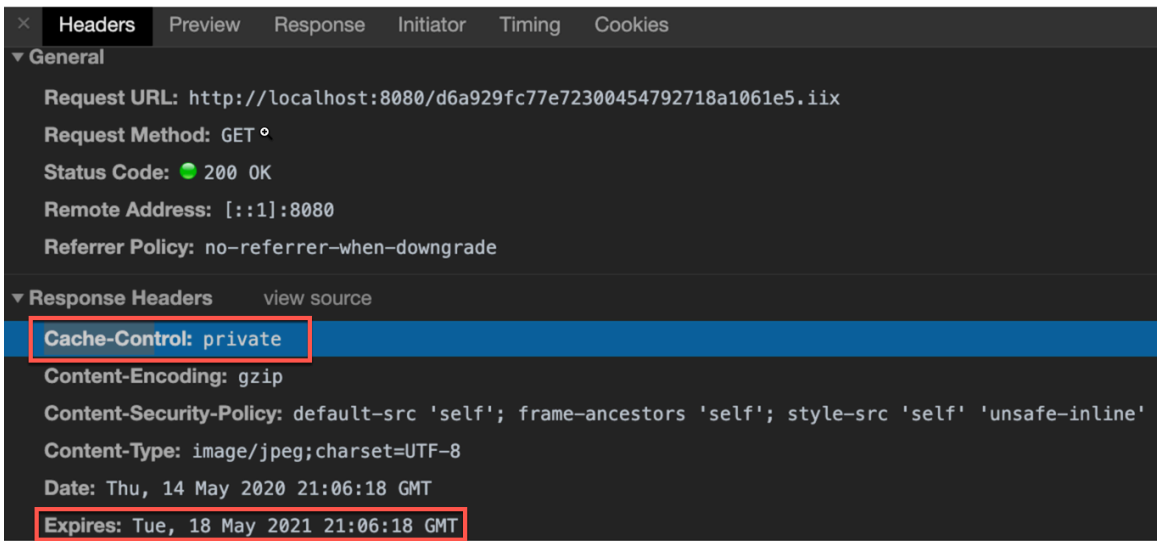
Wert	Beschreibung
Privat	Statischer Inhalt kann auf Browserebene (Client) zwischengespeichert werden, aber nicht auf Proxy-Server-Ebene.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
Öffentlich	Statische Inhalte können auf Browserebene (Client) und auf Proxy-Serverebene zwischengespeichert werden.

Der Wert „Ablauf“ in den HTTP-Antwortheadern steuert, wann der statische Inhalt abläuft, und hat einen Standardwert von 369 Tagen. Um den Standardwert manuell zu überschreiben, verwenden Sie *glide.http.expire.days*Eigenschaft.



Hinweis: Sie können verwenden *glide.http.cache*Eigenschaft, die angibt, ob die Einstellung der Cache-Control- und Ablaufwerte in HTTP-Antwortheadern aktiviert oder deaktiviert werden soll. Der Standardwert ist **Wahr** , Mit dem Sie Folgendes festlegen können:

- Cache-Control-Wert, der standardmäßig verwendet wird *glide.http.cache_control*Eigenschaft.
- Ablaufwert – Standard mit *glide.http.expire.days*Eigenschaft.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.http.cache_control*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Dient zum Konfigurieren des Werts des Cache-Control-HTTP-Antwortheaders für statischen Inhalt.
Empfohlener Wert	Privat
Standardwert	Privat
Sicherheitsrisikobewertung	4.3
Funktionale Auswirkung	Legt den standardmäßigen Cache-Control-Wert in einem HTTP-Antwortheader fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) wenn Sie diese Eigenschaft auf festlegen **Öffentlich** , Instanzen mit CDN/Proxys können statischen Inhalt zwischenspeichern und ohne Authentifizierung rendern. • **Privat** Ist eine angemessenere Einstellung für Instanzen mit CDN/Proxy-Setup. • Wenn für eine Instanz kein CDN/Proxy-Setup vorhanden ist, muss jeder Wert in Ordnung sein.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Aktivieren Sie die Konfiguration der HTTP-Antwort-Header

Reduzieren Sie das Risiko von Cookie-/sitzungsbezogenem Hijacking von Web-Apps mithilfe einer Systemeigenschaft.

Wenn *glide.http.headers_config.enabled*lst nicht auf festgelegt **Wahr** , Dann werden in der Tabelle „HTTP-Antwortheader“ [sys_response_Header] definierte Antwortheaderkonfigurationen nicht verwendet. Sicherheitsbezogene HTTP-Antwortheader enthalten die Inhaltssicherheitsrichtlinie, die XSS-bezogene Schutzmaßnahmen unterstützt. Details zu HTTP-Antwortheadern finden Sie unter HTTP-Antwortheader .

Überprüfen Sie, ob die Eigenschaft ist *glide.http.headers_config.enabled*lst auf festgelegt **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.http.headers_config.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Fallback-Wert	wahr
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 5,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisiko: Die Sicherheitsrisiken fehlender, falscher oder schwacher HTTP-Antwortheader können XSS-, CSRF- und Cookie-/Sitzungsbezogenes Hijacking von Web-Apps ermöglichen.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Deaktivieren Sie das Debugging des Chatservers

Aktivieren oder deaktivieren Sie die Systemprotokolle Ihrer Instanz, indem Sie diese Eigenschaft konfigurieren.

Verwenden Sie *glide.cs.debug*Eigenschaft, um zu verwalten, wie Ihre Instanz Systemprotokolle verarbeitet. Wenn die Eigenschaft auf den empfohlenen Wert von festgelegt ist **Falsch** , Systemprotokolle sind nicht aktiviert. Wenn auf festgelegt ist **Wahr** , Systemprotokolle sind aktiviert. Legen Sie die Eigenschaft auf fest **Wahr** Nur, wenn Sie Probleme beheben und dann deaktivieren möchten, wenn Sie fertig sind. Das Aktivieren von Systemprotokollen kann dazu führen, dass viele Nachrichten generiert werden, was die Systemprotokolle überlasten könnte. Protokollnachrichten können versehentlich vertrauliche Informationen offenlegen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.cs.debug*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 2,3 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Das Aktivieren von Systemprotokollen kann dazu führen, dass viele Nachrichten generiert werden, was das System mit Protokollnachrichten überladen könnte, die versehentlich vertrauliche Informationen offenlegen.
Abhängigkeiten und Voraussetzungen	Keine

Deaktivieren Sie die Nutzung der Legacy-JQuery-UI

Vermeiden Sie die Einführung nicht gepatchter Schwachstellen in der Bibliothek, indem Sie die Nutzung der Legacy-JQuery-UI deaktivieren.

Verhindern Sie die Verwendung älterer vorab gepatchter JQuery-UI-Versionen, die ungepatchte Schwachstellen in der Bibliothek einführen. Die Verwendung alter Versionen kann potenziell zu Sicherheitsrisiken führen, die aus Angriffen auf Schwachstellen entstehen, die in veralteten Versionen der JQuery-UI-Bibliothek erkannt wurden.

Bestätigen Sie, dass **Glide.jquery_ui.Legacy** Systemeigenschaft ist auf festgelegt **Falsch** Um zu verhindern, dass ältere vorab gepatchte JQuery-UI-Versionen verwendet werden. Diese Systemeigenschaft ist eine Ausfallsicherheit, wenn Organisationen auf die nicht gepatchten Versionen angewiesen sind, um ihre anwenderdefinierten Implementierungen auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.jquery_ui.legacy`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Fallback-Wert	wahr
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 3,9 • CVSS-Punktzahl: Niedrig • Wenn verhindert wird, dass ältere vorab gepatchte JQuery-UI-Versionen verwendet werden, kann dies zu nicht gepatchten Schwachstellen in der Bibliothek führen.
Funktionale Auswirkung	Diese Systemeigenschaft ist eine Ausfallsicherheit, wenn Organisationen auf die nicht gepatchten Versionen angewiesen sind, um ihre anwenderdefinierten Implementierungen auszuführen.
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Deaktivieren Sie das Debugging gesperrter Formularelemente

Hier ist die Beschreibung für `glide.security.explain.write.locks`.

Festlegen `glide.security.explain.write.locks`Auf den empfohlenen Wert von **Falsch** Um zu verhindern, dass Erklärungen gesperrter Formularelemente angezeigt werden. Legen Sie den Wert auf fest **Wahr** Zum Anzeigen der Erklärung gesperrter Formularelemente.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.explain.write.locks`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Begrenzt das Anzeigeverhalten von SecurityDebugger ohne Abhängigkeit von anderen Eigenschaften.
Empfohlener Wert	falsch
Standardwert	falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Niedrig) verhindert die Anzeige der Erklärung für gesperrte Formularelemente. Dies macht die Anwendung etwas sicherer, da weniger Informationen vom Sicherheits-Debugger bereitgestellt werden.
Sicherheitsrisikobewertung	3,5

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

MultiSSO-Debugging deaktivieren [aktualisiert in Security Center 1,3 und 1,5]

Die *glide.authenticate.multisso.debug*Eigenschaft steuert die Debug-Protokollierung für Multi-SSO.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.authenticate.multisso.debug*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Deaktiviert das Multi-SSO-Debuggen.
Empfohlener Wert	falsch
Standardwert	falsch
Konfigurationstyp	Boolean
Sicherheitsrisiko	(Hoch) Legen Sie die Eigenschaft auf den empfohlenen Wert „falsch“ fest, andernfalls ist MultiSSO-Debuggen aktiviert, was zu unbeabsichtigtem Verlust vertraulicher Informationen führen kann.
Sicherheitsrisikobewertung	4.0
Referenzen	Multi-Provider-SSO-Eigenschaften, -Tabellen und -Skripts

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Klonen von Zielen nicht zulassen [Neu in Security Center 1,3]

Konfigurieren Sie *glide.db.clone.allow_clone_target*Eigenschaft, um zu verhindern, dass Ihre Instanz als Klonziel verwendet wird.

Schützen Sie Ihre Instanz vor der Verwendung als Klonziel, indem Sie festlegen **Glide.DB.clone.allow_clone_target** Systemeigenschaft zu **Falsch** . Ein Systemklon kopiert alles in einer Datenbank von einer Quellinstanz in die Zielinstanz. Dies ist ein Sicherheitsrisiko, da die Instanzdatenbank auf der Zielinstanz im Klonprozess überschrieben wird, was zu Datenverlust und mangelnder Datenintegrität führt.

Legen Sie fest **Glide.DB.clone.allow_clone_target** Systemeigenschaft zu **Falsch** In Produktionsinstanzen, um zu verhindern, dass Ihre Instanz als Klonziel ausgewählt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.db.clone.allow_clone_target`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	wahr
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 4,4 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „falsch“ festgelegt wird, kann die Instanz als Klonziel verwendet werden. Dies ist ein Sicherheitsrisiko, da die Instanzdatenbank beim Klonen überschrieben werden kann.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	• Klon (veraltete UI) • Klonziel (Registrierung und Authentifizierung)
Funktionale Auswirkung	Diese Eigenschaft bietet einen zusätzlichen Schutz, der verhindert, dass eine Produktionsinstanz in geklont wird. Der Standardwert ist „falsch“ für Produktionsinstanzen und „wahr“ für Unterproduktionsinstanzen wie „dev“ oder „qa“. Damit eine Instanz als Klonziel verwendet werden kann, legen Sie diese Eigenschaft auf „wahr“ fest.

Deaktivieren Sie die Anzeige des SOAP-Fehlerstapels

Verwalten Sie, wie Stapelverfolgungen in Ihrer Instanz angezeigt werden.

Verwenden Sie `glide.soapfault.display_stack_trace`Eigenschaft zum Verwalten von Stapelverfolgungen in Ihrer Instanz. Wenn diese Eigenschaft auf konfiguriert ist **Falsch** , Dann könnten vertrauliche Informationen weitergegeben werden. Wenn auf festgelegt ist **Wahr** , Dann wird kein Stapelverlauf angezeigt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.soapfault.display_stack_trace`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Vertrauliche Informationen aus dem Stapeltrace könnten verfügbar gemacht werden.
Abhängigkeiten und Voraussetzungen	Keine

Zugriff auf Leistungsüberwachung einschränken [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.security.diag_txns_acl`Eigenschaft zum Steuern des Zugriffs auf stats.do, Threads.do, Thread_Pool_stats und Replication.do über eine nicht authentifizierte Verbindung.

Wenn Sie diese Eigenschaft auf festlegen **Wahr** , `glide.security.diag_txns_acl`Die Eigenschaft ermöglicht nur den Zugriff auf Folgendes durch den Administrator-Account:

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

Ohne diese Einstellung zu aktivieren, ist es weiterhin möglich, über eine nicht authentifizierte Verbindung auf diese Ressourcen zuzugreifen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.diag_txns_acl`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Beschränken Sie den Zugriff auf Konfigurationsseiten nur auf den Administrator-Account
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	Diese Fehlerkorrektur erzwingt, dass nur der Administratoraccount zu Protokollierungs- und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Problembehandlungszwecken Zugriff auf vertrauliche Anwendungsdaten erhält.
Sicherheitsrisiko	(Mittel) vertrauliche Daten wie Serverdetails, Threads und Prozesse, die auf dem Server ausgeführt werden, dürfen dem Endanwender ohne entsprechende Berechtigungen niemals sichtbar oder zugänglich sein.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Aktualisierte Version des MultiSSO-Plugins aktivieren [aktualisiert in Security Center 1,3 Und 1,5]

Überprüfen Sie, ob Sie v2 des MultiSSO-Plugins verwenden und ob es auf „wahr“ festgelegt ist, um Sicherheitsschwachstellen zu reduzieren.

Wenn das Multi SSO-Plugin auf einer Instanz aktiviert ist, reduzieren Sie Sicherheitsschwachstellen, indem Sie bestätigen, dass die v2-Version aktiviert ist. Die neueste Version verbessert die Sicherheit und verfügt über weitere Funktionen, z. B. Unterstützung für Assertion Encryption und IDP-initiierte Single Logout (SLO). Wenn die neueste Version nicht aktiviert ist, können die neuen Sicherheitsfunktionen nicht verwendet werden, und die Instanz läuft Gefahr, ein veraltetes Plugin zu verwenden.

Befolgen Sie die Schritte in KB0756504 Um ein Upgrade auf die neueste Version durchzuführen. Dieser Prozess umfasst das Überprüfen und Migrieren von anpassungsbezogenen Changes und das anschließende Upgrade der Version. Wenn abgeschlossen, wird **glide.authenticate.multissov2_feature.enabled** Systemeigenschaft wird automatisch festgelegt **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	glide.authenticate.multissov2_feature.enabled
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Konfiguration
Sicherheitsrisiko	Wenn die neueste Version nicht aktiviert ist, können die neuen Sicherheitsfunktionen nicht verwendet werden, und die Instanz läuft Gefahr, ein veraltetes Plugin zu verwenden
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichere Referrer-Richtlinie erzwingen [Neu in Security Center 1,3]

Verwenden Sie *com.glide.security.referrerpolicy*Eigenschaft, um sicherzustellen, dass der HTTP-Header der Referrer-Policy die entsprechende Datenebene an jeden sendet ServiceNow® Seite, um Datenlecks zu verhindern.

Wenn *com.glide.security.referrerpolicy*Die Eigenschaft ist auf Standard festgelegt. Sie stellt sicher, dass der HTTP-Header für Referrer-Policy mit der entsprechenden Ebene von gesendeten Informationen verwaltet wird, die speziell auf die zugeschnitten sind ServiceNow AI Platform® Anforderungsseite. Dies verhindert nicht autorisierte Datenlecks, die von anderen Teilen der vollständigen URL aus zugänglich sein könnten, z. B. dem Pfad und der Abfragezeichenfolge.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.security.referrerpolicy*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Standard
Standardwert	Standard
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Stellen Sie sicher, dass *com.glide.security.referrerpolicy*Eigenschaft ist auf Standard festgelegt, um das Auslaufen nicht autorisierter Daten zu verhindern.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Referrer-Richtlinie
Funktionale Auswirkung	Diese Eigenschaft steuert, wie viele Informationen über den Referrer-Header gesendet werden, wenn eine Anforderung von einer Seite gesendet wird: • Standard: Instanz kümmert sich um die Referrer-Header • Gleicher Ursprung: Vollständige Referrer-URL innerhalb der Instanz/derselben Domäne und kein Referrer an externen Ursprung senden • Ursprung: Sendet nur den Ursprung als Referrer innerhalb und außerhalb des Ursprungs • Origin-when-Cross-Origin: Vollständige Referrer-URL innerhalb der Instanz/derselben Domäne und nur den Ursprung außerhalb des Ursprungs senden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie die minimale Größe des privaten Schlüssels sicher

Verwenden Sie eine Systemeigenschaft, um die Mindestgröße des privaten Schlüssels zu bestimmen, der für die Generierung von Zertifikatsignaturanforderungen (Certificate Signing Request, CSR) mit der Anwendung „Certificate Inventory Management“ verwendet wird.

Die `sn_disco_certmgmt.private_key_size`Die Systemeigenschaft bestimmt die Mindestgröße des privaten Schlüssels, der für die CSR-Generierung mit der Anwendung „Zertifikatbestandsverwaltung“ verwendet wird. Gültige Auswahlmöglichkeiten sind 512, 1024, 2048 oder 4096.

Stellen Sie sicher, dass diese Eigenschaft auf einen Wert von 2048 oder höher festgelegt ist. Gültige Auswahlmöglichkeiten für diese Eigenschaft sind 512, 1024, 2048 oder 4096. Wenn die Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden ist oder der Wert ungültig ist, ist der Wert standardmäßig 2048.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`sn_disco_certmgmt.private_key_size`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl, die die Größe des generierten privaten Schlüssels darstellt. Verwenden Sie Werte von 512, 1024, 2048 oder 4096.
Empfohlener Wert	2048
Standardwert	2048
Fallback-Wert	2048
Kategorie	Kommunikation
Sicherheitsrisiko	• Schweregradpunktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Sicherheitsrisiko: Die Verwendung von Schlüsseln, die kleiner als 2048 sind, kann zu einer zukünftigen Offenlegung von Informationen führen, wenn der Schlüssel brute erzwungen wird. Verwenden Sie einen gültigen Wert größer oder gleich 2048, um den Schlüssel für einen längeren Zeitraum in der Zukunft nachzuweisen.
Funktionale Auswirkung	Legacy-Systeme und -Anwendungen verarbeiten möglicherweise keine Schlüssel größer oder gleich 2048.
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

X-Frame-options implementieren: SAMEORIGIN-Sicherheitsheader [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.set_x_frame_options*Eigenschaft zum Festlegen des X-Frame-Options-Antwortheaders auf SAMEORIGIN für alle UI-Seiten.

Verwenden Sie den HTTP-Antwortheader X-Frame-Options, um anzugeben, ob der Browser eine Seite in einem rendern darf <frame>Oder <iframe>. Websites können diese Funktion verwenden, um Clickjacking-Angriffe zu vermeiden, indem sichergestellt wird, dass ihre Inhalte nicht in andere Websites eingebettet werden. Ein Angreifer kann Ihre Seite in seine eigene Seite einbetten und dazu führen, dass Ihre Seitenelemente böswillig funktionieren. Der Endanwender denkt möglicherweise, dass die Seite legitim ist, da sie Ihrer Seite ähnelt. Der Endanwender kann auf Elemente wie üblich klicken, nur um schädliche Skripts oder Elemente auszuführen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.set_x_frame_options*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Konfiguration
Zweck	Um Clickjacking-Angriffe zu mindern.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	5,9
Funktionale Auswirkung	Diese Korrektur erzwingt die Einschränkung für das Rendern von ServiceNow AI Platform Anwendung in einer Drittpartei-Anwendung in Form eines iFrame. Wenn Sie über eine solche Integration verfügen, würde die Anwendung nicht in der anwenderdefinierten Drittanbieter-App gerendert.
Sicherheitsrisiko	(Mittel) mit derselben Ursprungsrichtlinie können Sie eine Domäne daran hindern, ein Skript oder eine Ressource aus anderen Domänen abzurufen. Alle modernen Browser unterstützen diese Funktionalität. Die Richtlinie validiert die Verbindung basierend auf Protokoll, Port und Host. CORS (Cross Origin Request) ist eine Änderung an derselben Ursprungsrichtlinie, die Zugriff auf Ressourcen/ Skripts aus einer anderen Domäne ermöglicht, wenn explizit als Teil des Headerwerts angegeben. • In diesem Fall steuert der Header „X-Frame-Options“, ob der ServiceNow AI Platform Die Anwendung kann auf der Website der Drittpartei gerendert werden. • Es reduziert das sensible Risiko, da der Eigenschaftswert auf festgelegt ist **SAMEORIGIN** Aktiviert das Rendern nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Verfügbare Systemeigenschaften iFrames konfigurieren

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Schreibzugriff für den Zugriff auf die Seite „Servicekatalog hinzufügen“ erforderlich [Neu in Security Center 1,3]

Verwenden Sie `glide.sc.request.add_item_write_access`Eigenschaft, um zu verhindern, dass nicht autorisierte Vorgänge für Katalogelemente ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sc.request.add_item_write_access`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn `glide.sc.request.add_item_write_access`Die Eigenschaft ist auf „falsch“ festgelegt. Jeder angemeldete Anwender kann auf die UI-Seite „Katalogelement hinzufügen“ zugreifen. Dies kann zu nicht autorisierten Vorgängen für Katalogelemente führen. Um dieses Sicherheitsrisiko zu beheben, legen Sie diese Eigenschaft auf „wahr“ fest.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wenn die Eigenschaft „wahr“ ist, muss der Anwender Schreibzugriff auf den Datensatz im Kontext der UI-Seite haben.

Xframe-Optionen festlegen, um die Einbettung von Websites von Drittparteien zu verhindern [aktualisiert im Sicherheitscenter 1,3]

Konfigurieren Sie diese Eigenschaft, um zu verhindern, dass der Inhalt einer Webanwendung in eine Drittpartei-Website eingebettet wird.

Wenn `com.glide.cs.embed.xframe_options`Ist nicht auf den empfohlenen Wert „DENY“ oder „SAMEORIGIN“ festgelegt, kann der Inhalt der Webanwendung mithilfe eines

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ALLOW-FROM-URI in eine Drittpartei-Website eingebettet werden. Das Zulassen nicht vertrauenswürdiger Websites von Drittparteien kann Angriffe wie Clickjacking ermöglichen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.cs.embed.xframe_options`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Sameursprung
Standardwert	Sameursprung
Kategorie	Konfiguration
Sicherheitsrisiko	• Schweregradpunktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert festlegen, kann der Inhalt einer Webanwendung in eine Drittpartei-Website eingebettet werden, was Angriffe wie Click-Jacking ermöglicht.
Abhängigkeiten und Voraussetzungen	Keine

Datenschutz

Die Datenschutzkategorie behandelt die Elemente Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Daten.

Die CIA-Komponenten sind:

- Vertraulichkeit: Daten werden während der Übertragung und im Ruhezustand vor nicht autorisiertem Zugriff geschützt.
- Integrität: Daten sind vor nicht autorisierter Erstellung, Löschung oder Änderung geschützt.
- Verfügbarkeit: Daten sind bei Bedarf zugänglich.

Entfernen Sie „mich speichern“

Verwenden Sie `glide.ui.forgetme`Eigenschaft zum Entfernen von **Merken Sie Sich** Aktivieren Sie das Kontrollkästchen auf der Anmeldeseite, um zu verhindern, dass Anmeldeinformationen zwischengespeichert werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.forgetme`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Datenschutz
Zweck	Um sicherzustellen, dass keine Authentifizierungsinformationen zwischengespeichert werden.
Sicherheitsrisikobewertung	3,5
Empfohlener Wert	wahr
Standardwert	wahr
Funktionale Auswirkung	Diese Korrektur würde die Anwender-Experience ändern, indem sie sie automatisch von der Instanz abmeldet, wenn ihre Sitzung abläuft. Der Ablauf der Sitzung hängt nur von dem in der Systemeigenschaft festgelegten Wert ab, wie in beschrieben Verwalten von Anwendersitzungen .
Sicherheitsrisiko	(Niedrig) wenn Sie auswählen **Merken Sie sich** Kontrollkästchen bei der Anmeldung wird ein zusätzliches Cookie auf dem Computer des Anwenders gespeichert. • Ihr Zweck besteht darin, die Sitzung für die nachfolgenden Besuche des angemeldeten Anwenders automatisch neu einzurichten. • Dies stellt ein Sicherheitsrisiko dar, da die Anwendersitzung aktiv sein kann, bis sie sich absichtlich abmelden. Die Wahrscheinlichkeit eines Angriffs für dieses Szenario erhöht sich, wenn der Endanwender den Browser unbeaufsichtigt gelassen hat oder wenn er durch einen anderen Angriff gefährdet wird.
Referenzen	Kontrollkästchen „Anwendernamen speichern“ entfernen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen

Beim Hintergrund der mobilen Anwendung muss die Zwischenablage gelöscht werden [Neu in Security Center 1,3 und aktualisiert 1,5]

Die `glide.sg.clear_pasteboard_when_backgrounded`Die Eigenschaft steuert, ob Text, der aus der mobilen ServiceNow-App kopiert wurde, in der Zwischenablage und in der Zwischenablage beibehalten wird, nachdem sich die App im Hintergrundmodus befindet. Wenn nicht auf den empfohlenen Wert „wahr“ festgelegt ist, werden vertrauliche Informationen möglicherweise an die Android- oder iOS-Zwischenablage weitergegeben, wo sie für andere Anwendungen auf dem Gerät zugänglich gemacht werden können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sg.clear_pasteboard_when_backgrounded`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt ist, werden vertrauliche Informationen möglicherweise an die Android- oder iOS-Zwischenablage weitergegeben, wo sie für andere Anwendungen auf dem Gerät zugänglich gemacht werden können.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft löscht die Zwischenablage zum Kopieren und Einfügen, wenn die ServiceNow-App in den Hintergrund verschoben wird.

HR-Fallaktualisierungen aus persönlichen E-Mails beschränken [Neu in Security Center 1,3 Und aktualisiert 1,5]

Verwenden Sie `sn_hr_core.restrict_guest_email`Eigenschaft, die steuert, ob ein Anwender mit seiner persönlichen E-Mail-Adresse auf einen HR-Fall antworten kann.

Wenn `sn_hr_core.restrict_guest_email`Die Eigenschaft ist nicht auf „wahr“ festgelegt. Ein Anwender kann eine E-Mail von einem privaten Account senden, die auf den HR-Fall verweist, der in die Arbeitsnotizen aufgenommen werden soll. Dies kann zu geringfügigen Vertraulichkeits- oder Integritätsproblemen führen, wenn die persönliche E-Mail gefährdet wird oder unsicher kommuniziert wird. Ein Administrator möchte möglicherweise die Fähigkeit von Anwendern einschränken, auf HR-Fälle über seine persönliche E-Mail-Adresse zu antworten, da er nicht sicher sein kann, dass der Anwender auf den persönlichen E-Mail-Account zugreift.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`sn_hr_core.restrict_guest_email`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregradpunktzahl: 3,5 • CVSS-Punktzahl: Niedrig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf „wahr“ festgelegt ist, kann dies zu geringfügigen Vertraulichkeits- oder Integritätsproblemen führen, wenn die persönliche E-Mail gefährdet oder unsicher kommuniziert wird.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft steuert, ob eine Antwort von einer persönlichen E-Mail-Adresse einen HR-Fall aktualisiert. Bei „wahr“ wird jede Antwort aus einer persönlichen E-Mail den Fallnotizen hinzugefügt. Bei „falsch“ werden der Fall und die Notizen nicht aktualisiert.

oauth-Parameter auf POST-Textkörper beschränken [Neu in Security Center 1,3]

Verwenden Sie `glide.oauth.allow.parameters.in.post.body.only`Eigenschaft zur Steuerung der Akzeptanz von Zugriffstoken durch die eingehende OAuth-Authentifizierung. Zugriffstoken sind vertraulich und sollten nur akzeptiert werden, wenn sie sich in einem POST-Anforderungstext befinden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.oauth.allow.parameters.in.post.body.only`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Datenschutz
Sicherheitsrisiko	• Schweregradpunktzahl: 4,2 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn `glide.oauth.allow.parameters.in.post.body.only`lst nicht auf den empfohlenen Wert von festgelegt **Wahr** , Zugriffstoken könnten im Parameter „Anforderung ABRUFEN“ vorhanden sein. Diese Zugriffstoken können in Client- und Infrastrukturprotokollen verbleiben und potenziell zur Accountübernahme führen, wenn diese Protokolle durchlaufen werden.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	• OAuth 2.0 • Verwalten Sie OAuth-Token
Funktionale Auswirkung	Stellt sicher, dass der Prozessor „oauth_token.do“ ausschließlich POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert.

Fehlerbehandlung und -Protokollierung

Die Kategorie „Fehlerbehandlung und -Protokollierung“ behandelt die Qualität und Ausführlichkeit der protokollierten Informationen, die Stakeholdern zur Verfügung gestellt werden.

Dies umfasst die Sicherstellung, dass Protokolle und Fehlermeldungen keine vertraulichen Informationen erfassen, Daten gemäß der Klassifizierung ordnungsgemäß schützen und eine angemessene Lebensdauer haben. Darüber hinaus bezieht sich diese Kategorie auf die angemessene Fehlerbehandlung und die Nichtoffenlegung sensibler Fehler für Endanwender, z. B. ausführliche Stapelverfolgungen für nicht behandelte Ausnahmen mit Sicherheitsauswirkungen.

Protokollierung für Anwender mit niedrigen Berechtigungen in der Skript-Sandbox deaktivieren [aktualisiert im Sicherheitscenter 1,3]

Verwalten Sie die Fähigkeit von Glide System, Skripts zu protokollieren, die in der Sandbox-Umgebung ausgeführt werden.

Verwenden Sie *glide.security.sandbox_no_logging*Eigenschaft zur Steuerung der Fähigkeit von Glide System, Skripts zu protokollieren, die in der Sandbox-Umgebung ausgeführt werden. Wenn *glide.security.sandbox_no_logging*lst auf festgelegt **Falsch** , Protokollierung ist für Anwender mit niedrigeren Berechtigungen verfügbar, die Sandboxed-Skripts verwenden. Dies ist eine potenzielle Sicherheitslücke, da Anwender mit niedrigen Berechtigungen Protokolle einfügen können, die es einem schlechten Akteur ermöglichen, einen Angriff potenziell zu verschleiern. Konfigurieren Sie die Eigenschaft auf **Wahr** Um zu verhindern, dass Anwender mit niedrigeren Berechtigungen, die ein Sandboxed-Skript verwenden, über Protokollierungsfunktionen verfügen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.sandbox_no_logging*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -Protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,2 • CVSS-Punktzahl: Niedrig

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Aktiviert die Protokollierung für Anwender mit niedrigeren Berechtigungen, wodurch ein schlechter Akteur einen Angriff verschleiern kann.
Abhängigkeiten und Voraussetzungen	Keine

Deaktivieren Sie das sichere Cookie-Debugging

Verwalten Sie die Protokollnachrichten im Zusammenhang mit Cookies in Ihrer Instanz.

Verwenden Th E *glide.secure_cookie.debug*Eigenschaft zum Verwalten Ihrer Protokollnachrichten im Zusammenhang mit Cookies. Wenn diese Eigenschaft auf festgelegt ist **Falsch** , Es werden keine Protokollnachrichten angezeigt. Wenn auf festgelegt ist **Wahr** , Nachrichten in SecureUserCookie Und Cookie Klassen werden protokolliert. Dies kann dazu führen, dass vertrauliche Informationen in Ihrer Instanz verfügbar gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.secure_cookie.debug*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Fehlerbehandlung und -Protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,2 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Diese Eigenschaft wird für konfiguriert **Wahr** Kann dazu führen, dass vertrauliche Informationen offengelegt werden.
Abhängigkeiten und Voraussetzungen	Keine

Deaktivieren Sie SQL-Fehlermeldungen [Aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie *glide.db.loguser*Eigenschaft zum Deaktivieren des Renderings von SQL-Fehlermeldungen in einem Browser.

Wenn *glide.db.loguser*Ist nicht auf den empfohlenen Wert „falsch“ festgelegt, dann können Endanwendern vertrauliche serverseitige Fehlermeldungen angezeigt werden. Fehlermeldungen können Stapelverfolgungen und Informationen zur Struktur der Datenbank enthalten, die einem Angreifer das Wissen liefern könnten, das für die erfolgreiche SQL-Injection erforderlich ist, wenn die Voraussetzungen vorhanden sind. Als Tiefenverteidigung sollten diese Fehlermeldungen dem Endanwender nicht angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.db.loguser`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Fehlerbehandlung und -Protokollierung
Zweck	Dient zum Deaktivieren der Anzeige von SQL-Fehlermeldungen im Browser.
Typ	Boolean
Empfohlener Wert	falsch
Standardwert	wahr
Sicherheitsrisikobewertung	3.1
Funktionale Auswirkung	Diese Korrektur deaktiviert das Rendern von SQL-Fehlermeldungen. Es gibt keine Auswirkungen auf eine Funktionalität.
Sicherheitsrisiko	(Mittel) auf einer Webseite sollten keine vertraulichen SQL-Informationen angezeigt werden, die einem Angreifer helfen könnten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Aktivieren Sie das MID-Audit-Protokoll [Neu in Security Center 1,3 Und aktualisiert in 1,5]

Das Audit-Protokoll des MID-Server-Befehls zeichnet Details wie den Befehlsnamen, den Befehlshash, den Namen der verwendeten Anmeldeinformationen und den Ausführungsstatus auf.

Nach der Aktivierung können Audit-Protokolle von Anwendern mit der Rolle „Agent_Security_admin“ in der Tabelle „ecc_Agent_Command_Audit_log“ oder durch Navigation zu angezeigt werden **MID-Server** > **Befehlsauditprotokolle**an.

Festlegen `mid.log.command_audit.enable`Auf „wahr“ in der Tabelle „MID-Servereigenschaften“ [ecc_Agent_property], um das Auditing für Befehle zu aktivieren, die vom MID-Server ausgeführt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`mid.log.command_audit.enable`
Konfigurationstyp	Datensatz der MID-Servereigenschaft [ecc_Agent_property]
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Fehlerbehandlung und -Protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,2 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Im Falle einer Sicherheitsuntersuchung kann diese Tabelle von Incident-Response-Teams verwendet werden, um die auf dem MID-Server ausgeführten Befehle zu auditieren. Ohne dieses Protokoll sind möglicherweise nicht genügend Details vorhanden, um auf Situationen wie die nicht autorisierte Accountverwendung zu reagieren.
Abhängigkeiten und Voraussetzungen	Keine

Plugin „geschützte Tabellen“ aktivieren [Neu in Security Center 1,3]

Verwenden Sie *com.glide.security.protected_table.enabled*Eigenschaft, um zu verhindern, dass Anwender mit höheren Berechtigungen an Protokolltabellen manipulieren.

Wenn *com.glide.security.protected_table.enabled*Eigenschaft ist auf festgelegt **Wahr** , Das Plugin „geschützte Tabellen“ wird verwendet, um zu verhindern, dass Anwender mit höheren Berechtigungen in einer Instanz an Protokolltabellen manipulieren. Die folgenden Protokolltabellen haben besonderen Schutz, wenn diese Eigenschaft auf festgelegt ist **Wahr** :

- Syslog (keine DB-Überschreibung)
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_Push_Notification
- Protected_table_Configuration (keine DB-Überschreibung)

Die Integrität von Protokollen ist wichtig, um schädliche Aktivitäten in einer Instanz durch einen Kundenadministrator zu bestimmen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.security.protected_table.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Fehlerbehandlung und -Protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Keine Einstellung `com.glide.security.protected_table.enabled`Mit dem empfohlenen Wert „wahr“ können Anwender mit höheren Berechtigungen in einer Instanz Protokolltabellen manipulieren.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Systemprotokolle

Alle ausgehenden HTTP-Anforderungsfelder protokollieren [im Sicherheitscenter v1.3.2 entfernt]

Konfigurieren Th E `glide.outbound_http.security.log.allow.all.fields` Eigenschaft auf „falsch“, um zu verhindern, dass sensible ausgehende HTTP-Felder im nur-Text-Format protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Falsch** , Vertrauliche ausgehende HTTP-Felder sind möglicherweise nur-Text protokolliert. Dies kann die Sicherheitslage Ihres Unternehmensnetzwerks verringern, da ausgehende Anforderungen mit vertraulichen Daten und Anmeldeinformationen in nur-Text protokolliert werden können, der unverschlüsselt ist und von Anwendern mit niedrigeren Berechtigungen angezeigt werden kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.outbound_http.security.log.allow.all.fields`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	30
Standardwert	30
Kategorie	Fehlerbehandlung und -Protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,8 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Diese Eigenschaft wird nicht auf festgelegt **Falsch** Erhöht die Wahrscheinlichkeit, dass vertrauliche ausgehende Felder im Klartext protokolliert werden, was ein Sicherheitsrisiko darstellt.
Abhängigkeiten und Voraussetzungen	Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTML-Bereinigung protokollieren [Entfernt in Sicherheitscenter 2,0]

Konfigurieren *glide.html_sanitize.discarded_log.enable* Eigenschaft, die bestimmt, ob HTML-Bereinigungsereignisse in Ihrer Instanz protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Wahr** , HTML-Bereinigungsereignisse werden nicht in protokolliert *sys_log*Tabelle. Fehlende Protokollierung kann sich negativ auf die Funktionen der automatisierten Sicherheitserkennung und -Untersuchung Ihrer Instanz auswirken.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.html_sanitize.discarded_log.enable*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -Protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,4 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert festgelegt ist **Wahr** , HTML-Bereinigungsereignisse werden nicht in protokolliert *sys_log*Tabelle, die sich auf die Funktionen der automatisierten Sicherheitserkennung und -Untersuchung auswirken könnte.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	HTML-Bereinigung wird aktiviert

Audit-Ereignisse für Protokollsitzungen [Neu in Security Center 1,3 und aktualisiert in 1,5]

Legen Sie fest *glide.authenticate.session_access.log_audit_event*Eigenschaft bis **Wahr** , Damit Sitzungs-Audit-Ereignisse in erstellt werden *sys_session_access_audit*Tabelle.

Wenn die Glide-Eigenschaft *glide.authenticate.session_access.log_audit_event*Ist auf „wahr“ festgelegt, werden Sitzungs-Audit-Ereignisse in der Tabelle „sys_Session_Access_Audit“ erstellt. Es wird empfohlen, Informationen darüber zu protokollieren, wer auf eine Sitzung zugegriffen hat, um Untersuchungen böswilliger Akteure zu unterstützen. Protokollierte Informationen umfassen Anwender, Sitzungs-ID (nicht vertraulich), IP-Adresse, Rollen und Richtlinien.

Hinweis: Die *glide.authenticate.session_access.log_audit_event*Die Systemeigenschaft ist spezifisch für den Zero Trust-Zugriff. Weitere Informationen finden Sie unter Zero Trust Access (ZTA).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.session_access.log_audit_event`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -Protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt wird, können Ereignisse nicht protokolliert werden. Dies könnte verhindern, dass Sie im Falle eines Cyberangriffs schlechte Akteure finden.
Abhängigkeiten und Voraussetzungen	Keine

Identitätswechsel des Anwenders protokollieren [aktualisiert in Security Center 1,3 und 2,0]

Konfigurieren `glide.sys.log_impersonation`Dient zur Steuerung, ob Ereignisse zur Identitätswechsel von Anwendern in Ihrer Instanz protokolliert werden.

Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Wahr** , Ereignisse, die die Identität des Anwenders annehmen, werden nicht mehr protokolliert. Das Fehlen der Protokollierung kann sich auf die Funktionen der automatisierten Sicherheitserkennung und -Untersuchung in Ihrer Instanz auswirken. Stellen Sie die Eigenschaft sicher `glide.sys.log_impersonation`Ist vorhanden und auf „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sys.log_impersonation`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -Protokollierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,4 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf festgelegt ist **Wahr** , Ereignisse, bei denen die Identität des Anwenders angenommen wird, werden nicht mehr protokolliert, was sich auf die Sicherheitserkennungs- und -Untersuchungsfunktionen Ihrer Instanz auswirken könnte.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Identität von Anwendern wird angenommen

Ausführliche HTTP-Anforderungsprotokollierung verhindern

Verhindern Sie den Zugriff auf vertrauliche Informationen, indem Sie die ausführliche Protokollierung von HTTP-Anforderungen reduzieren.

Steuern Sie die Protokollierungsstufe für ausgehende HTTP-Anforderungen, um den Zugriff auf vertrauliche Informationen wie Autorisierungsheader oder Cookies zu verhindern. Diese Informationen können wie Anmeldeinformationen für den Zugriff auf die angeforderte Ressource verwendet werden.

Die Protokollierungsebene für diese Anforderungen wird von gesteuert **Glide.outbound_http_log.override** Und **Glide.outbound_http_log.override.level** Eigenschaften. Wenn **Glide.outbound_http_log.override** Ist auf festgelegt **Wahr** , Die Protokollebene für Anforderungen und Antworten wird von gesteuert **Glide.outbound_http_log.override.level** Eigenschaft. Wenn **Glide.outbound_http_log.override.level** Ist auf festgelegt **Alle** Oder **Erhöht** , Dann werden Anforderungs- und Antwort-Header protokolliert.

Festlegen **Glide.outbound_http_log.override** Bis **Falsch** Und **Glide.outbound_http_log.override.level** Bis **Standard** . Wenn diese Eigenschaften nicht in der Tabelle „Systemeigenschaften“ [sys_properties] angezeigt werden, befinden sie sich standardmäßig in einem sicheren Status.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	• glide.outbound_http_log.override • glide.outbound_http_log.override.level
Plugin-Anwendbarkeit	Keine
Sicherheitsrisiko	Ausgehende HTTP-Anforderungsheader, die mit ausführlichen Einstellungen protokolliert wurden, können vertrauliche Informationen wie Autorisierungsheader oder Cookies enthalten. Diese Informationen können wie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Anmeldeinformationen für den Zugriff auf die angeforderte Ressource verwendet werden. Anwender mit Zugriff auf die Tabelle „Protokolle ausgehender HTTP“ [sys_outbound_http_log] können diese Informationen anzeigen. Der Schweregrad hängt davon ab, welche Art von ausgehenden Anforderungen gestellt werden.
CVSS-Punktzahl (Common Vulnerability Scoring System)	5
Bewertung des Common Vulnerability Scoring System (CVSS)	Mittel
Funktionale Auswirkung	Die **Glide.outbound_http_log.override** Mit der Systemeigenschaft können Sie die Protokollebene ausgehender HTTP-Anforderungen überschreiben. Ein Wert von **Falsch** Legt die Protokollebene standardmäßig auf „Standard“ fest. Wenn **Glide.outbound_http_log.override** Ist auf festgelegt **Wahr** , Die Protokollierungsstufe wird durch den Wert von bestimmt **Glide.outbound_http_log.override.level** Eigenschaft. Dieser Wert kann sein **Standard** , **Erhöht** , Oder **Alle** . Alle 3 sind Zeichenfolgen-/textbasierte Werte. Jeder andere Wert wird als interpretiert **Standard** . Weitere Informationen finden Sie unter Ausgehende Protokollierung konfigurieren .
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	• Boolean • Zeichenfolge
Basissystemwert	• falsch • <blank>
Fallback-Wert	• falsch • <blank>
Empfohlener Wert	• falsch • Standard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Ausführliche SQL-Fehlermeldungen für Importprozessor deaktivieren [aktualisiert in Security Center 1,3]

Konfigurieren Sie diese Eigenschaft, um zu steuern, ob ausführliche SQL-Fehlermeldungen angezeigt werden.

Wenn die Eigenschaft auf festgelegt ist **Falsch** , Wird eine ausführliche SQL-Fehlermeldung angezeigt, die vertrauliche Informationen preisgeben kann. Um dies zu vermeiden, legen Sie die Eigenschaft auf fest **Wahr** Dient zum Anzeigen einer generischen Nachricht.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.import.error_message.generic`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Fehlerbehandlung und -Protokollierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,1 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Eigenschaft wird auf festgelegt **Falsch** Aktiviert ausführliche SQL-Nachrichten, die zu Informationsverlusten führen können.
Abhängigkeiten und Voraussetzungen	Keine

Datei und Ressourcen

Die Datei- und Ressourcenkategorie stellt sicher, dass Anwendungen nicht vertrauenswürdige Dateidaten sicher verarbeiten und nicht vertrauenswürdige Daten aus nicht vertrauenswürdigen Quellen mit eingeschränkten Berechtigungen an einem geeigneten Ort speichern.

Dies umfasst Steuerungen wie das Vermeiden von Denial of Service durch große oder unerwartete Dateitypen, das Validieren des Dateityps und das verhindern von Pfaddurchläufen.

Download infizierter Dateien nicht zulassen [aktualisiert in Security Center 1,5 und 2,0]

Steuert, ob Anwender nicht gescannte Anhänge herunterladen können, wenn der Virenschutzservice ausgefallen oder nicht erreichbar ist.

Wenn `com.glide.snap.infected_download_allowed`Die Eigenschaft ist auf „wahr“ festgelegt. Anwender können auch dann nicht gescannte Anhänge herunterladen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wenn der Virenschutzservice ausgefallen oder nicht erreichbar ist. Diese Situation setzt Anwender potenziell dem Risiko aus, eine schädliche Datei herunterzuladen, wodurch die Infektion ihres Desktops riskiert wird, insbesondere wenn auf dem Gerät kein anderer Endpunktschutz installiert ist.

Stellen Sie die Eigenschaft sicher *com.glide.snap.infected_download_allowed*lst auf „falsch“ festgelegt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.snap.infected_download_allowed*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 6,7 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft nicht auf den empfohlenen Wert „falsch“ festlegen, kann Ihre Instanz schädliche Dateien herunterladen.
Abhängigkeiten und Voraussetzungen	Keine

E-Mail-Spam-Bewertung und -Filterung aktivieren [aktualisiert in Security Center 1,3]

Installieren Sie den E-Mail-Filter (*com.glide.email_filter*) Plugin zum Installieren der E-Mail-Filterung in der Instanz. Diese Filterung identifiziert vorhandene Header, sodass Sie basierend auf dem zugehörigen Header entscheiden können, was mit der E-Mail geschehen soll. Alternativ können Sie festlegen *com.glide.email_filter*Auf „falsch“.

Jede Nachricht, die über gesendet wird ServiceNow AI Platform E-Mail-Server werden auf die Wahrscheinlichkeit von Spam bewertet.

Hinweis: Wenn eine Instanz einen privaten E-Mail-Server verwendet, gilt dieses Thema nicht. Weitere Informationen finden Sie unter E-Mail-Spam-Bewertung und -Filterung.

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen:

Legen Sie die Eigenschaft *glide.email.read.active* auf „Wahr“ fest. Weitere Informationen finden Sie unter Aktivieren Sie mit Ihrem eigenen POP3-Server .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	Com.Glide.email_Filter, Glide.email.read.Active
Konfigurationstyp	Systemdefinition > Plugins
Kategorie	Datei und Ressourcen
Zweck	Zum Erzwingen von Filtern, um das Spamming von E-Mails zu vermeiden.
Empfohlener Wert	Entweder: • Die **Glide.email.lesen.aktiv** Eigenschaft bis **Falsch** • Die **Glide.email.lesen.aktiv** Eigenschaft bis **Wahr** Und aktivieren Sie **E-Mail-Filter** Plugin (com.Glide.email_Filter). Aktiv
Standardwert	Keine. Dies ist ein Plugin, keine Glide-Eigenschaft, daher ist kein Standardwert vorhanden.
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	E-Mails werden im Rahmen der Spam-Bewertung nie von der Instanz gefiltert, blockiert oder in Quarantäne gestellt. Es wird nur bewertet und dann an die Instanz gesendet. Die gesamte Filterung erfolgt innerhalb der Instanz mit dem Plugin „E-Mail-Filter“.
Sicherheitsrisiko	(Mittel) E-Mail-Filter ermöglichen Administratoren die Verwendung eines Bedingungsgenerators oder bedingten Skripts, um anzugeben, wann schädliche eingehende E-Mails von bekannten/unbekannten Absendern ignoriert werden sollen.
Referenzen	E-Mail-Filter https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Weitere Informationen zum Aktivieren eines Plugins finden Sie unter Plugins aktivieren .

Aktivieren Sie den Virenschutz-Scan

Die *com.glide.snap.enable_scan*Die Eigenschaft aktiviert die Virenschutz-Scan-Funktionalität.

Festlegen *com.glide.snap.enable_scan*Auf den empfohlenen Wert von **Wahr** Zum Aktivieren von Virenschutzscans.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`com.glide.snap.enable_scan`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Datei und Ressourcen
Zweck	Dient zum Aktivieren oder Deaktivieren der Virenschutz-Scans für die spezifische Instanz.
Empfohlener Wert	wahr
Standardwert	wahr
Datentyp	Boolean
Sicherheitsrisiko	(Hoch) Antivirus-Scans hilft, Ihre Instanz vor Vireninfektionen zu schützen, die durch Dateianhänge an Ihre Systemdatensätze wie Incidents, Probleme und Stories eingeführt werden können.
Sicherheitsrisikobewertung	7.7

Herunterladbare Dateitypen in statischem Inhalt einschränken [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.ui.strict_customer_uploaded_static_content`Eigenschaft zum Aktivieren von Einschränkungen für die Dateitypen, die heruntergeladen werden können, wenn sie mit der Funktionalität „Datei hochladen“ hochgeladen wurden.

Sie verwenden diese Eigenschaft mit `glide.ui.strict_customer_uploaded_content_types`Eigenschaft, die eine kommagetrennte Liste eingeschränkter herunterladbarer Dateitypen erstellt.

⚠ **Warnung:** Der Wert für diese Eigenschaft ist eine Überschreibung ohne DB. Sie kann nicht geändert oder überschrieben werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.strict_customer_uploaded_static_content`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Datei und Ressourcen
Zweck	Um sicherzustellen, dass Safe-Dateitypen aus der Anwendung heruntergeladen werden dürfen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	3.1
Funktionale Auswirkung	Diese Korrektur erzwingt die Einschränkung von Dateidownloads basierend auf den in angegebenen Werten `glide.ui.strict_customer_uploaded_content_types`Eigenschaft.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Niedrig) Einschränkungen des Dateidownloads sollten auf alle nicht vertrauenswürdigen Anwendereingabequellen angewendet werden.

Anhangsgröße in Trainings- und Vorhersageflows für GraphQL-Endpunkte begrenzen [Neu in Security Center 1,3 und aktualisiert 1,5]

Die `glide.platform_ml_di.max_attachment_size_graphql`Die Eigenschaft steuert die maximal zulässige Größenbeschränkung für die Rückgabe von Anhängen in GraphQL-Endpunkten von Trainings- oder Vorhersageflows.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.platform_ml_di.max_attachment_size_graphql`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	5,242,880
Standardwert	5.242.880
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert von 5.242.880 oder weniger festgelegt ist, kann die Rückgabe großer Dateien zu einem Denial of Service (DoS) führen.
Abhängigkeiten und Voraussetzungen	Keine

Anhangsgröße in Trainings- und Vorhersageflows begrenzen [Neu in Security Center 1,3 Und aktualisiert 1,5]

Die `glide.platform_ml_di.max_attachment_size`Die Eigenschaft steuert die maximal zulässige Größenbeschränkung für die Rückgabe von Anhängen in Trainings- und Vorhersageflows.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.platform_ml_di.max_attachment_size`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	4,000,000

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	4.000.000
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn *glide.platform_ml_di.max_attachment_size*lst nicht auf den empfohlenen Wert von 4.000.000 oder weniger festgelegt, kann die Rückgabe großer Dateien zu einem Denial of Service-Angriff (DoS) führen.
Abhängigkeiten und Voraussetzungen	Keine

Größe des HTTP-Antworttexts begrenzen [Neu in Security Center 1,3 Und aktualisiert 1,5]

Konfigurieren Sie *glide.http.response.get_body.limit.enabled*Und *glide.http.response.get_body.limit*Eigenschaften, vor denen Ihre Instanz geschützt werden soll *Außerhalb des Arbeitsspeichers* .

Verhindern Außerhalb des Arbeitsspeichers Dies kann dazu führen, dass ein Anforderungsantworttext mit zu groß ist **Glide.http.response.get_body.limit.enabled** Und **Glide.http.response.get_body.limit** Systemeigenschaften. Diese Ausnahmen können Denial of Service (DOS)-Angriffe sowie andere Probleme verursachen, die Angreifern helfen können, eine Instanz zu gefährden. Wenn Sie diese Eigenschaften nicht auf die empfohlenen Werte festlegen, kann Ihre Instanz angreifbar für OutOfMemoryExceptions und Denial of Service-Angriffe werden.

So schützen Sie Ihre Instanz vor diesen Sicherheitsschwachstellen:

- Legen Sie fest **Glide.http.response.get_body.limit.enabled** Systemeigenschaft zu **Wahr** .
- Stellen Sie sicher, dass **Glide.http.response.get_body.limit** Systemeigenschaft auf nicht mehr als 524.288.000 Megabyte (500 MB) festgelegt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	• **Glide.http.response.get_body.limit.enabled** • **Glide.http.response.get_body.limit**
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Datei und Ressourcen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,1 • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaften nicht auf die empfohlenen Werte festlegen, kann Ihre Instanz angreifbar sein `Außerhalb des Arbeitsspeichers` Und Denial of Service-Angriffe.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft reduziert die Wahrscheinlichkeit von `OutOfMemoryException` Weil ein Kunde versehentlich eine große Datei in den Arbeitsspeicher geladen hat.

Maximale Anzahl von Anhängen in E-Mails begrenzen

Konfigurieren Sie die Anzahl der eingehenden E-Mail-Anhänge in Ihrer Instanz.

Th E `glide.email.inbound.max_attachment_count`Die Eigenschaft steuert die maximale Anzahl eingehender E-Mail-Anhänge in Ihrer Instanz. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **30** Oder weniger, dann können eingehende E-Mails zu einer Verschlechterung der Instanzleistung führen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.email.inbound.max_attachment_count`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	30
Standardwert	30
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 5,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Das Festlegen des Eigenschaftswerts auf einen Wert über 30 kann zu Verschlechterungsproblemen führen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	E-Mail-Eigenschaften

Maximal zulässige Anhangsgröße [aktualisiert in Security Center 1,3]

Konfigurieren Die `com.glide.attachment.max_size`Eigenschaft zur Steuerung der maximalen Größe (in Megabyte), die für einen hochgeladenen Anhang zulässig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Eigenschaft steuert die maximale Größe (in Megabyte) eines hochgeladenen Anhangs. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **1024** (1 Gigabyte) oder weniger kann die Plattform große Dateien akzeptieren, die Speicher ausfüllen und zu einem Denial of Service-Angriff (DoS) führen könnten.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.attachment.max_size`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	1024
Standardwert	1024
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf festgelegt ist **1024** (1 Gigabyte) oder weniger kann die Plattform große Dateien akzeptieren, was zu einem DoS-Angriff führen kann.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Eigenschaften der Anhangsbeschränkungen

Zulässige untergeordnete MIME-Typen festlegen [Neu in Security Center 2,0]

Erfahren Sie, wie Sie konfigurieren `glide.security.mime.type.allowed_child_types`Eigenschaft für eine sichere Einstellung, damit Dateitypen die Typprüfung für Multipurpose Internet Mail Extensions (MIME) nicht bestehen. Dies reduziert das Risiko der Remotecodeausführung für eine hochgeladene Datei.

Die `glide.security.mime.type.allowed_child_types`Eigenschaft definiert die MIME-Dateitypen, die möglicherweise eine Dateierweiterung haben, die nicht mit den Daten in einer hochgeladenen Datei übereinstimmt. Dadurch können solche Dateitypen die MIME-Typprüfung umgehen. Die Eigenschaft akzeptiert eine kommagetrennte Liste von Dateityppaaren, z. B. `application/zip=application/java-archive`. Wenn in diesem Beispiel die Eigenschaft auf einen solchen Wert festgelegt ist, werden Dateien mit einem erstellt .Zip Erweiterung, die technisch sind .JAR-Datei Dateien dürfen die MIME-Typprüfung trotz der Inkonsistenz bestehen. Wenn diese Umgehung nicht ordnungsgemäß festgelegt ist, kann sie zur Remotecodeausführung einer hochgeladenen Datei führen. Daher sollte er immer auf eine leere Zeichenfolge („“) festgelegt werden, es sei denn, es entsteht ein gültiger Anwendungsfall. Wenn beispielsweise ein bestimmter MIME-Typ unter einer anderen Dateierweiterung zulässig sein muss und gemäß der Tika-Konfiguration gültig ist, werden diese Schlüssel-Wert-Paare als Teil dieses Eigenschaftswerts aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.mime.type.allowed_child_types`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	""
Standardwert	""
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,6 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn Sie diese Eigenschaft nicht auf den sicheren Wert festlegen, kann dies dazu führen, dass Dateien mit falschen Konfigurationen zur Remotecodeausführung einer hochgeladenen Datei führen.
Abhängigkeiten und Voraussetzungen	Ja, wann `glide.security.mime.type.detection.allow_child_types`Auf „wahr“ festgelegt ist, werden die Werte dieser Eigenschaft zur Validierung anhand der konfigurierten Liste der zulässigen untergeordneten MIME-Typen verwendet.
Funktionale Auswirkung	Zur Unterstützung von MIME-Typen, deren Dateierweiterungen nicht mit dem Inhalt der Dateien übereinstimmen, aber gemäß den Tika-Untertypkonfigurationen in gültig sind `tika-mimetypes.xml`.

Dateimime-Typ im SOAP-Webservice „AttachmentCreator“ validieren [Neu in Security Center 1,3 und aktualisiert in 1,5]

Die `glide.attachment.enforce_security_validation`Die Eigenschaft bestimmt, ob MIME-Dateien (Multipurpose Internet Mail Extensions) einer Validierung unterzogen werden.

Stellen Sie sicher, dass MIME-Typen für Anhänge validiert werden, um zu verhindern, dass gefährliche Dateien mit falschen Dateierweiterungen in Ihre Instanz hochgeladen werden.

Legen Sie fest **Glide.attachment.enforce_Security_validation** Systemeigenschaft zu **Wahr** . Wenn auf festgelegt **Wahr** , Dateien werden mit der richtigen Dateityperweiterung hochgeladen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.attachment.enforce_security_validation`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Datei und Ressourcen
Sicherheitsrisiko	• Schweregradpunktzahl: 6,7 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn die Eigenschaft auf „falsch“ festgelegt ist, erfolgt während des Uploads keine Validierung für MIME-Dateien. Dies könnte es ermöglichen, schädliche Dateien zu verschleiern, indem ihre Dateierweiterung geändert wird.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types
Funktionale Auswirkung	Legen Sie diese Härtungseinstellung auf „wahr“ fest, um Validierungen des MIME-Typs und der Dateierweiterung für hochgeladene Dateianhänge auszuführen. Wenn diese Eigenschaft auf „falsch“ festgelegt ist, werden keine Validierungen ausgeführt. Diese Eigenschaft ist standardmäßig auf „wahr“ festgelegt.

Schädlicher Code

Die Kategorie „schädlicher Code“ stellt sicher, dass nach besten Kräften sichergestellt wird, dass Ihr Code frei von Schwachstellen und unerwünschten Funktionen ist.

Dies umfasst die Sicherstellung einer sicheren und ordnungsgemäßen Behandlung böswilliger Aktivitäten, keine zeitbasierten Angriffe, keine ausgehenden Kommunikationen an nicht vertrauenswürdige Ziele und die Sicherstellung, dass kein nicht autorisierter oder von Angreifern kontrollierter Code enthalten ist. Diese Kategorie enthält Audit- oder Drittparteibibliotheken aus der Anwendungscodebase.

Blockieren Sie Mobilgeräte mit Rootfunktion oder Jailbreak

Sichern Sie Ihre Instanz, indem Sie verhindern, dass nicht autorisierter Zugriff von Jailbreak-Geräten erfolgt.

Verwenden Sie *`glide.sg.allow_rooted_jailbroken_device`* Eigenschaft zum Schutz Ihrer Instanz vor nicht autorisiertem Zugriff durch Jailbreak-Geräte. Wenn ein Anwender versucht, sich mit einer mobilen App bei einer Instanz zu authentifizieren, während diese Eigenschaft auf festgelegt ist **Falsch** , Erhalten sie die folgende Warnung: Dieses Gerät scheint über einen Jaildefekt zu sein und kann nicht für den Zugriff auf diese Instanz verwendet werden. Wenden Sie sich an Ihren ServiceNow-Administrator. Die App wird eingefroren, während die Warnungsnachricht angezeigt wird, und die einzige Möglichkeit, diese Nachricht zu schließen, besteht in der Auswahl **Melden Sie sich ab** . Wenn diese Eigenschaft auf festgelegt ist **Wahr** Benutzer authentifizieren sich mit einem Jailbreak-Gerät bei einer Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.sg.allow_rooted_jailbroken_device`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Schädlicher Code
Sicherheitsrisiko	• Schweregradpunktzahl: 4,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Die mangelnde Sicherheit von Jailbreak-Geräten macht sie zu einem Hauptziel für schlechte Akteure. Wenn nicht autorisierte Entitäten auf Unternehmensdaten zugreifen, kann dies die Sicherheitslage eines Unternehmensnetzwerks beeinträchtigen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Zugriffssteuerung

Codesignatur für Anwendungskonfigurationsdaten und -Skripts aktivieren [in Security Center 1,3 entfernt]

Verwalten Sie die Codesignatur für Anwendungskonfigurationsdaten und -Skripts in Ihrer Instanz.

Codesignatur kann die Sicherheit verbessern, indem vertrauliche Anwendungskonfigurationsdaten und -Skripts validiert werden, bevor sie verwendet werden. Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. Diese Verifizierung verhindert, dass schädliche Daten oder Skripts in der Instanz verwendet werden, was zu einer vollständigen Gefährdung der Instanz führen kann.

Verwenden Th E `com.snc.kmf.signature.validation.flag`Eigenschaft zum Verwalten der Codesignatur für Anwendungskonfigurationsdaten und -Skripts. Wann diese Eigenschaft auf festgelegt werden soll **Wahr** , Codesignatur ist für Anwendungskonfigurationsdaten und -Skripts aktiviert.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.snc.kmf.signature.validation.flag`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Schädlicher Code
Sicherheitsrisiko	• Schweregradpunktzahl: 6 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Wahr** Aktiviert die Codesignatur, die durch die Validierung sensibler Anwendungskonfigurationsdaten und -Skripts zur Verbesserung der Sicherheit beiträgt.
Abhängigkeiten und Voraussetzungen	Keine

Management von Anwendersitzungen

Diese Kategorie untersucht die Sicherheit des Anwendungsstatus für einen Anwender. Sitzungen müssen für jede Person eindeutig sein, nicht erraten oder geteilt werden können und nach Zeiträumen der Inaktivität oder wenn nicht erforderlich für ungültig erklärt werden. Dies umfasst Faktoren wie Cookie-Attribute für Cookie-basierte Sitzungen, Sitzungstoken-Generierung und Speicher sowie Anforderungen für die erneute Authentifizierung.

Wenden Sie Richtlinien für kontinuierliche Authentifizierung auf mobile Sitzungen an

Reduzieren Sie das Risiko von Sitzungs-Hijacking, indem Sie Richtlinien für kontinuierliche Authentifizierung auf mobile Sitzungen anwenden.

Stellen Sie sicher, dass mobile Anwender die Sitzungsfunktion mit hoher Sicherheit des Plugins „Zero Trust – kontinuierliche Authentifizierung“ verwenden, indem Sie festlegen **glide.zta.high_assurance.mobile.session.allowed** Systemeigenschaft zu **Falsch** . Um Richtlinien für kontinuierliche Authentifizierung für mobile Sitzungen zu umgehen, legen Sie diese Eigenschaft auf fest **Wahr** .

Legen Sie fest **glide.zta.high_assurance.mobile.session.allowed** Systemeigenschaft zu **Falsch** . Diese Aktion verringert das Risiko von Sitzungs-Hijacking und persistentem Zugriff, wenn eine Sitzung gefährdet wird. Wenn diese Eigenschaft nicht in der Tabelle „Systemeigenschaften“ [sys_properties] angezeigt wird, ist der Standardwert **Falsch** .

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	glide.zta.high_assurance.mobile.session.allowed
Plugin-Anwendbarkeit	Zero Trust – kontinuierliche Authentifizierung (com.snc.Zero_Trust_Continuous_authentication)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	Wenn diese Systemeigenschaft auf festgelegt ist **Wahr** , Die Sitzungsfunktion mit hoher Sicherheit wird nicht auf mobile Sitzungen angewendet. Die erneute Authentifizierung erfolgt nicht wie in Richtlinien für Sitzungen mit hoher Rolle definiert. Dies erhöht das Risiko von Sitzungs-Hijacking und persistentem Zugriff, wenn eine Sitzung gefährdet wird.
CVSS-Punktzahl (Common Vulnerability Scoring System)	3,9
Bewertung des Common Vulnerability Scoring System (CVSS)	Niedrig
Funktionale Auswirkung	Wenn auf festgelegt **Wahr** , Die Sitzungsfunktion mit hoher Sicherheit gilt nicht für mobile Sitzungen, was das Risiko von Sitzungs-Hijacking und persistentem Zugriff erhöht, wenn eine Sitzung gefährdet wird.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Boolean
Basissystemwert	falsch
Fallback-Wert	falsch
Empfohlener Wert	falsch

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Absolute Sitzungszeitüberschreitungsdauer minimieren [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.ui.user_cookie.max_life_span_in_days`Eigenschaft zum Festlegen einer maximalen Lebensdauer für Anwendercookies, die erstellt werden, wenn sich Anwender mit anmelden **Merken Sie Sich** Kontrollkästchen ausgewählt. Wenn das Cookie abläuft, Anwender, die ausgewählt haben **Merken Sie Sich** Die erneute Authentifizierung von Kontrollkästchen bei der Instanz wird erzwungen.

Dadurch kann das Anwendercookie für die Dauer der angegebenen Tage gültig sein, beginnend mit der ersten Ausgabe des Cookies. Der Standardwert ist 30 Tage, und die maximale Obergrenze beträgt 365 Tage.

Hinweis: Informationen zum Erzwingen einer maximalen Sitzungszeit für aktive Anwendersitzungen finden Sie unter Verwalten von Anwendersitzungen .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.user_cookie.max_life_span_in_days`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Zum Erzwingen von Anwendern, die ausgewählt haben **Merken Sie Sich** Kontrollkästchen zur erneuten Authentifizierung nach bestimmten Tagen.
Empfohlener Wert	Kleiner oder gleich 30
Standardwert	30 Tage
Funktionale Auswirkung	Diese Eigenschaft erzwingt eine obligatorische erneute Anmeldung, indem jegliche Art von Cookie-Rotation nach einem bestimmten Zeitraum vermieden wird.
Sicherheitsrisikobewertung	4.2
Sicherheitsrisiko	(Mittel) die unbefristet aktiven Anwendercookies stellen ein Sicherheitsrisiko dar und sollten mit einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Anwendernamen speichern

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Aktive Sitzungszeitüberschreitungsausnahmerollen definieren [Neu in Security Center 1,3]

Verwenden Sie eine Systemeigenschaft, um Rollen von Zeitüberschreitungsgrenzen für aktive Sitzungen zu befreien.

Verwenden Sie `glide.active.session.timeout.exception.roles`Systemeigenschaft zum Ausnehmen von Rollen von einem Zeitüberschreitungslimit für aktive Sitzungen. Die Zeitüberschreitungsfunktion für aktive Sitzungen trägt dazu bei, sicherzustellen, dass eine gegriffene Sitzung nicht unbegrenzt verwendet werden kann, ohne Authentifizierungsinformationen anzugeben. Es wird empfohlen, eine Ausnahme für die Zeitüberschreitungsgrenze für aktive Sitzungen nur für interne Integrations-Account-Rollen zu berücksichtigen.

Konfigurieren Sie `glide.active.session.timeout.exception.roles`Eigenschaft für Rollen, die von Zeitüberschreitungen bei aktiven Sitzungen ausgenommen werden sollen. Dieser Eigenschaftswert ist eine kommagetrennte Liste von Rollen. Der Standardwert ist `edge_encryption,mid_server,maint`.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.active.session.timeout.exception.roles`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	Edge_Encryption, Mid_Server, Wartung
Standardwert	Edge_Encryption, Mid_Server, Wartung
Fallback-Wert	Edge_Encryption, Mid_Server, Wartung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 6,4 • CVSS-Punktzahl: Mittel • Berücksichtigen Sie eine Ausnahme für die Zeitüberschreitungsgrenze für aktive Sitzungen nur für interne Integrationsaccounts-Rollen. Wenn ein Anwender Opfer eines Hijacking-Versuchs einer Sitzung ist und über eine Rolle mit einer Ausnahme verfügt, können sich Angreifer, die diese Sitzung verwenden, unbegrenzt bei dieser Sitzung authentifizieren. Dies kann die Auswirkungen eines Security Incidents erhöhen, indem einem Angreifer mehr Zeit für die Nutzung eines entführten Accounts eingeräumt wird.
Abhängigkeiten und Voraussetzungen	Keine

UserCookie-Version 3,1 aktivieren [aktualisiert in Security Center 2,0]

Verwalten Sie die Version von AnwenderCookie, die in Ihrer Instanz aktiviert ist, um die Speicherung des geheimen Schlüssels im Quellcode zu sichern.

UserCookie v3 wird nur generiert, wenn die Eigenschaft vorhanden ist `glide.ui.secure.cookies.use_kmf is disabled`. UserCookie v3 ist nicht sicher, da geheimer Schlüssel für HMAC im Quellcode gespeichert und für alle Kunden identisch ist. Die schädliche Akteure unterstützen kann, diesen einen geheimen Schlüssel für Versuche zum Hijacking von Anwendersitzungen zu verwenden. Durch Festlegen der Eigenschaft `glide.ui.secure.cookies.use_kmf`Auf „wahr“ wird AnwenderCookie v3.1 verwendet, und der geheime Schlüssel wird in einem Sicherheitsspeicher wie KMF gespeichert.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ui.secure.cookies.use_kmf`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 7,1 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Wird auf festgelegt **Falsch** Ist eine Sicherheitsschwachstelle, da

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	der geheime Schlüssel für Hash-basierte Nachrichtenauthentifizierungscodes (HMAC) im Quellcode gespeichert wird.
Abhängigkeiten und Voraussetzungen	Keine

Passwortzurücksetzung für api-Anforderungen erzwingen [aktualisiert im Sicherheitscenter 1,5]

Verwalten Sie, wie die Funktion zum Zurücksetzen des Passworts in Ihrer Instanz funktioniert.

Wenn ein Anwender für markiert ist **Passwort muss zurückgesetzt werden** , Müssen sie beim nächsten Authentifizierungsversuch ein neues Passwort angeben. Diese Eigenschaft steuert, ob die Passwortzurücksetzung vor API-Aufrufen obligatorisch ist. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Wahr** , Anwenderaccounts markiert als **Passwort muss zurückgesetzt werden** Kann weiterhin Vorgänge ausführen, indem die Tabellen-API über die Standardauthentifizierung abgefragt wird. Diese Sicherheitslücke kann Informationsverluste ermöglichen, wenn ein inaktiver Account gefährdet wird.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.api.user.reset_password.mandatory`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 8,1 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Kann zu Informationsverlusten führen, wenn ein inaktiver Account gefährdet ist.
Abhängigkeiten und Voraussetzungen	Keine

Kennzeichnung für „nur HTTP-Cookie aktivieren“ [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.cookies.http_only`Eigenschaft zum Aktivieren des Attributs „HttpOnly“ für sensible Cookies.

Verwenden Sie das Attribut HttpOnly, um Angriffe zu verhindern, z. B. siteübergreifendes Skripting, da es keinen Zugriff auf das Cookie mit einem clientseitigen Skript wie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JavaScript zulässt. Es beseitigt nicht die Risiken bei der Cross-Site-Skripting, aber einige Ausnutzungsvektoren.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.cookies.http_only`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Um das Risiko zu mindern, dass clientseitiges Skript auf das geschützte Cookie zugreift.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8
Funktionale Auswirkung	Diese Korrektur fügt eine zusätzliche HttpOnly-Kennzeichnung in Sitzungscookies hinzu, um sie vor Diebstahl zu schützen. • Wenn Sie über eine anwenderdefinierte Funktionalität verfügen, die JavaScript für den Zugriff auf das Cookie des Anwenders erfordert, wird diese Funktionalität unterbrochen. Dies sollte unter normalen Umständen nicht der Fall sein. • Die ServiceNow AI Platform Verarbeitet die Sitzungsverwaltung, und es darf kein Grund für den Zugriff eines anwenderdefinierten Skripts auf die Cookies des Anwenders geben.
Sicherheitsrisiko	(Mittel) Sitzungscookies in der Anwendung authentifizieren einen Endanwender und gewähren implizite Zugriffsberechtigungen für die Anwendung. Das bedeutet, dass sichergestellt werden muss, dass sie gestohlen oder exportiert werden. HTTP-Kennzeichnungen schützen die Sitzungscookies vor JavaScript-Einschleusungen oder Site-übergreifenden Skripting-Schwachstellen, die sie stehlen.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Sitzung nach Ablauf des OAuth-Tokens für ungültig erklären [Neu in Security Center 2,0]

Konfigurieren Sie `glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled`Eigenschaft für den sicheren Wert, um zu verhindern, dass Anwender eine Sitzung weiterhin über Cookies verwenden, nachdem das zum Erstellen der Sitzung verwendete OAuth-Token abläuft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn *glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled*Eigenschaft ist nicht auf den sicheren Wert „wahr“ festgelegt. Ein Anwender kann eine Sitzung weiterhin über Cookies verwenden, nachdem das zum Erstellen der Sitzung verwendete OAuth-Token abläuft. Dies erhöht das Risiko, dass Cookies weitergegeben werden und die Sitzung von einem böswilligen Anwender gekapert wird, um auf nicht autorisierte Ressourcen zuzugreifen. Stellen Sie sicher, dass G Lide p Roperty *glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled*lst auf „wahr“ festgelegt. Wenn der Datensatz in der Tabelle „sys_properties“ nicht vorhanden ist, ist der Standardwert „falsch“.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.oauth.post.token.expiration.cookie_aut*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	Für zboot-Instanzen ist die Eigenschaft „wahr“. Für die Update-Instanzen ist die Eigenschaft standardmäßig „falsch“.
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 5,4 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den sicheren Wert „wahr“ festgelegt ist, kann ein Anwender eine Sitzung weiterhin verwenden, auch nachdem das zum Erstellen der Sitzung verwendete OAuth-Token abgelaufen ist. Dies erhöht die Wahrscheinlichkeit, dass die Sitzung von einem böswilligen Anwender übernommen wird.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Wahr: Die Cookie-Authentifizierung wird nur berücksichtigt, bis das OAuth-Zugriffstoken abläuft. Nach Ablauf wird die Authentifizierung nicht berücksichtigt. Falsch: Die Cookie-Authentifizierung wird auch nach Ablauf des OAuth-Zugriffstoken berücksichtigt.

Anzahl gleichzeitiger interaktiver Sitzungen minimieren [aktualisiert in Security Center 1,3]

Verwenden Sie diese Eigenschaft mit dem Plugin „gleichzeitige Sitzungen begrenzen“, um die Anzahl der aktiven Sitzungen zu steuern, die von einem Anwender geöffnet werden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie **Glide-Authentifizierung – Max. Gleichzeitige Interaktive Sitzungen** Eigenschaft mit **Gleichzeitige Sitzung Begrenzen** (*com.glide.limit.concurrent.sessions*) Plugin zum Steuern der Anzahl der aktiven Sitzungen, die für einen Anwender geöffnet wurden. Der empfohlene Wert ist **1** , Wodurch die Anzahl der geöffneten Sitzungen reduziert wird (eine größere Anzahl erhöht die Wahrscheinlichkeit, dass eine Sitzung gekapselt werden könnte).

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.max.concurrent.interactive.sessions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	1
Standardwert	1
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn Sie den Standardwert der Eigenschaft größer als 1 festlegen, erhöht sich die Wahrscheinlichkeit von Sitzungs-Hijacking.
Abhängigkeiten und Voraussetzungen	Die **Gleichzeitige Interaktive Sitzungen** (*com.glide.limit.concurrent.sessions*) Plugin muss aktiv sein.
Referenzen	Gleichzeitige Sitzungen begrenzen

Gleichzeitige Sitzungen auf allen Knoten begrenzen [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.authenticate.limit.concurrent.sessions.across.all.nodes*Eigenschaft mit dem Plugin „gleichzeitige Sitzungen begrenzen“, um die Anzahl der Sitzungen zu verwalten, die auf allen Knoten nachverfolgt werden.

Wenn Gleichzeitige Sitzungen begrenzen Plugin ist aktiv, die Anzahl der offenen Sitzungen kann pro Anwender begrenzt werden. Stellen Sie sicher, dass (**Glide-Authentifizierung begrenzen Sie gleichzeitige Sitzungen auf allen Knoten** Eigenschaft) ist auf festgelegt **Wahr** Damit die Anzahl der offenen Sitzungen auf allen Knoten statt auf einem einzelnen Anwendungsknoten nachverfolgt wird. Wenn diese Eigenschaft auf festgelegt ist **Falsch** , Mehrere Sitzungen können über mehrere Knoten hinweg geöffnet sein, was die Wahrscheinlichkeit von Sitzungs-Hijacking erhöht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.limit.concurrent.sessions.across.all.r`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Bei Verwendung von **Begrenzen Sie Gleichzeitige Sitzungen** Plugin, das diese Eigenschaft auf festgelegt hat **Falsch** Ermöglicht das Öffnen mehrerer Sitzungen auf mehreren Knoten, was die Wahrscheinlichkeit einer Sicherheitsschwachstelle wie einem Sitzungs-Hijacking erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Gleichzeitige Sitzungen begrenzen

Plugin „gleichzeitige Sitzungen begrenzen“

Konfigurieren Sie das Plugin com.glide.limit.concurrent.sessions, um die Wahrscheinlichkeit von Sitzungs-Hijacking in Ihrer Instanz zu reduzieren.

Mit diesem Plugin kann ein Administrator die Anzahl der aktiven Sitzungen pro Benutzer und/oder Rolle begrenzen. Es wird empfohlen, dieses Plugin zu aktivieren und zu konfigurieren, um die Möglichkeit von Sitzungs-Hijacking zu reduzieren. Wenn dieses Plugin aktiviert und konfiguriert ist, gibt es einen Grenzwert für die Anzahl der offenen Sitzungen, die gekapselt werden können.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`com.glide.limit.concurrent.sessions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Plugin
Empfohlener Wert	com.glide.limit.concurrent.sessions aktiviert und konfiguriert
Standardwert	com.glide.limit.concurrent.sessions aktiviert und konfiguriert
Kategorie	Management von Anwendersitzungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn dieses Plugin nicht aktiv ist, besteht eine erhöhte Wahrscheinlichkeit für Sitzungs-Hijacking.
Abhängigkeiten und Voraussetzungen	Keine

Lebensdauer der aktiven Sitzung des Gastes begrenzen [Neu in Security Center 1,3]

Verwenden Sie *glide.guest.active.session.life_span*Eigenschaft zur Steuerung der Dauer der HTTP-Sitzungen eines aktiven Gastes.

Die *glide.guest.active.session.life_span*Die Eigenschaft erzwingt eine maximale Lebensdauer für aktive Gast-HTTP-Sitzungen, unabhängig von der Inaktivität der Sitzung oder der Zeit, die ein Anwender inaktiv ist, bevor die Sitzung abläuft und geschlossen wird. Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von Null wird die Zeitüberschreitung der aktiven Sitzungen deaktiviert. Ein größerer Wert könnte es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu bleiben, was die Wahrscheinlichkeit eines Security Incidents erhöht. Diese Eigenschaft ist auf Gastanwender beschränkt, die über niedrige Berechtigungen auf eine Instanz verfügen.

Legen Sie fest, um diese Sicherheitslücke zu beheben *glide.guest.active.session.life_span*Auf einen Wert größer als 0 und kleiner oder gleich 720.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.guest.active.session.life_span*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	1-720 (Minuten)
Standardwert	0
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,2 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn Sie die maximale Lebensdauer auf einen großen Wert festlegen, erhält ein schlechter Akteur mehr Zeit in einer Instanz, wenn er eine Sitzung stehlen sollte.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Diese Konfiguration erzwingt die maximale Lebensdauer für aktive Gast-HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung. Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von Null wird die Zeitüberschreitung der aktiven Sitzungen deaktiviert. Die maximale Lebensdauer muss größer als die inaktive Zeitüberschreitung sein `glide.guest.session_timeout`(Standard: 30 Minuten).

Gleichzeitige interaktive Sitzungen begrenzen [aktualisiert in Security Center 1,3]

Verwalten Sie die Anzahl der interaktiven Sitzungen in Ihrer Instanz.

Diese Eigenschaft ist für die Verwendung mit dem Limit Concurrent Sessions (`com.glide.limit.concurrent.sessions`)-Plugin. Wenn das Plugin aktiv ist und die Eigenschaft auf „falsch“ festgelegt ist, kann ein Anwender eine beliebige Anzahl gleichzeitiger interaktiver Sitzungen in einer Instanz haben. Eine größere Anzahl offener Sitzungen bedeutet, dass Sitzungs-Hijacking sehr wahrscheinlich ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.limit.concurrent.interactive.sessions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn das Plugin aktiv ist und die Eigenschaft auf festgelegt ist **Falsch** , Kann ein Anwender eine beliebige Anzahl gleichzeitiger interaktiver Sitzungen haben, was die Möglichkeit eines Sitzungs-Hijacking erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Gleichzeitige interaktive Sitzungen begrenzen [aktualisiert in Security Center 1,3]

Lebensdauer der aktiven Sitzungen von Integrationen begrenzen [Neu in Security Center 1,3]

Die `glide.integrations.active.session.life_span`Die Eigenschaft erzwingt die maximale Lebensdauer für aktive Gast-HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung. Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von Null wird die Zeitüberschreitung der aktiven Sitzungen deaktiviert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.integrations.active.session.life_span`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	0 bis 720
Standardwert	0
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,2 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Eine größere maximale Lebensdauer kann es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu verbleiben, wodurch der Umfang eines Security Incidents erhöht wird. Diese Eigenschaft ist auf Integrationen beschränkt, die über geringe Berechtigungen auf eine Instanz verfügen. Glide-Eigenschaft festlegen, `glide.integrations.active.session.life_span`Auf einen Wert von 0 und kleiner oder gleich 720.
Abhängigkeiten und Voraussetzungen	Keine

Intervall für richtlinienbasierten Sitzungszugriff für mobile Aktualisierungstoken begrenzen [Neu in Security Center 1,5]

Verwenden Sie `glide.authenticate.session_access.mobile.refresh_token_interval`Eigenschaft zur Steuerung der Dauer, die verstreichen muss, bevor ein Mobilgeräteanwender zur erneuten Authentifizierung gezwungen wird.

Ein Anwender wird nur dann zur erneuten Authentifizierung aufgefordert, wenn der Administrator die Attribute des Identitätsanbieters in der Sitzungsrichtlinie konfiguriert hat (Attribute können bei jeder Anmeldung variieren) und sich der Anwender mit Single Sign-on (SSO) authentifiziert. Der Standardwert stellt die Zeit in Sekunden dar, die ein Anwender vor der erneuten Authentifizierung hat. Ein größerer Standardwert bietet einem schlechten Akteur mehr Zeit für den Sitzungszugriff im Falle eines Sitzungs-Hijacking.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.authenticate.session_access.mobile.refresh_token_ir`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	1800 (Sekunden)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	1800 (Sekunden)
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn die ZTA-Richtlinie für die Instanz aktiviert ist, werden Anwender, die SSO während der mobilen Anmeldung verwenden, gezwungen, sich abzumelden und erneut anzumelden, nachdem der Standardwert von 1800 Sekunden (30 Minuten) veraltet ist. Wenn ein höherer Wert verwendet wird, werden Anwender gezwungen, diese verstrichene Zeit zu warten.
Abhängigkeiten und Voraussetzungen	Zero Trust: Richtlinienbasierter Sitzungszugriff
Funktionale Auswirkung	Diese Einstellung regelt die Zeit in Sekunden nach der Anmeldung, die Anwender gezwungen werden, sich von Mobilgeräten abzumelden, wenn sie Single Sign-on zur Authentifizierung verwenden, und der Administrator hat die Attribute „Provider identifizieren“ in der Sitzungszugriffsrichtlinie konfiguriert.

Lebensdauer der aktiven UI-Sitzung begrenzen [Neu in Security Center 1,3]

Die *glide.ui.active.session.life_span*Die Eigenschaft erzwingt die maximale Lebensdauer für aktive authentifizierte HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung.

Reduzieren Sie den Umfang potenzieller Security Incidents, indem Sie die Lebensdauer aktiver HTTP-Sitzungen verringern. Die **glide.ui.active.session.life_span** Die Systemeigenschaft erzwingt unabhängig von der inaktiven Zeitüberschreitung eine maximale Lebensdauer für aktive HTTP-Sitzungen. Eine längere maximale Lebensdauer kann einem Angreifer ermöglichen, eine gestohlene Sitzung länger zu verwenden, wodurch der Umfang eines Security Incidents erhöht wird. Der Standardwert von **0** Deaktiviert die Zeitüberschreitung aktiver Sitzungen

Legen Sie fest **glide.ui.active.session.life_span** Auf einen Wert zwischen 1 und 720. Dieser Wert stellt die Zeit in Minuten dar, die HTTP-Sitzungen aktiv bleiben können.

Hinweis: Die **glide.ui.active.session.life_span** Ist auf Zeitüberschreitung bei UI-Sitzung beschränkt.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.active.session.life_span*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	1-720

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Standardwert	0
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,2 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Eine größere maximale Lebensdauer könnte es einem Angreifer ermöglichen, länger in einer gestohlenen Sitzung zu bleiben, was die Wahrscheinlichkeit eines Security Incidents erhöht.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Erzwingt die maximale Lebensdauer für aktive authentifizierte HTTP-Sitzungen unabhängig von der inaktiven Zeitüberschreitung. Der konfigurierte Wert wird in Minuten angegeben. Bei einem Wert von Null wird die Zeitüberschreitung der aktiven Sitzungen deaktiviert. Die maximale Lebensdauer muss größer als die Zeitüberschreitung für Inaktivität glide.ui.session_timeout sein (Standard: 30 Minuten).

Beschränken Sie die Sitzungsdauer für Sitzungen mit hoher Sicherheit

Reduzieren Sie das Risiko der Accountübernahme in Sitzungen mit hoher Sicherheit, indem Sie die Sitzungsdauer beschränken

Reduzieren Sie das Risiko der Accountübernahme in Sitzungen mit hoher Sicherheit, indem Sie die Länge der Sitzung beschränken. Nach dem angegebenen Zeitraum müssen sich Endanwender erneut authentifizieren.

Verwenden Sie **glide.zta.high_assurance.session.timeout** Systemeigenschaft zum Festlegen einer Zeit in Minuten, nach der sich Anwender erneut authentifizieren müssen. Der Wert dieser Eigenschaft muss zwischen 1 und 480 Minuten liegen. Erwägen Sie, diesen Wert auf 30 oder niedriger zu beschränken, um das Risiko der Kontoübernahme zu reduzieren.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	glide.zta.high_assurance.session.timeout
Plugin-Anwendbarkeit	Zero Trust – kontinuierliche Authentifizierung (com.snc.Zero_Trust_Continuous_authentication)
Sicherheitsrisiko	Kürzere Sitzungslängen reduzieren das Risiko der Accountübernahme, indem Anwender gezwungen werden, sich erneut zu authentifizieren.
CVSS-Punktzahl (Common Vulnerability Scoring System)	3.3
Bewertung des Common Vulnerability Scoring System (CVSS)	Niedrig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Anwender in Sitzungen mit hoher Sicherheit müssen sich im von dieser Eigenschaft festgelegten Intervall erneut authentifizieren.
Abhängigkeiten und Voraussetzungen	Keine
Datentyp	Ganzzahl
Basissystemwert	30
Fallback-Wert	30
Empfohlener Wert	30 oder niedriger

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Inaktive Sitzungen proaktiv für ungültig erklären [Neu in Security Center 1,3 und aktualisiert in 1,5 und 2,0]

Die `glide.active.session.timeout.invalidate.session`Die Eigenschaft steuert, ob eine Zeitüberschreitungssitzung proaktiv vor dem Tomcat-Server für ungültig erklärt wird.

Wenn `glide.active.session.timeout.invalidate.session`lst nicht auf festgelegt **Wahr** , Es kann ein kleines Zeitintervall geben, in dem eine Sitzung mit Zeitüberschreitung nicht für ungültig erklärt wird (60 oder mehr Sekunden je nach Warteschlangengröße). Wenn eine Sitzung gekapert wird, kann ein Angreifer während dieses kurzen Zeitraums möglicherweise eine Sitzung verwenden. Um dieses Sicherheitsrisiko zu beheben, legen Sie fest `glide.active.session.timeout.invalidate.session`Bis **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.active.session.timeout.invalidate.session`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 4,6 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt wird, kann eine Sitzung mit Zeitüberschreitung nicht validiert werden. Dies erhöht die Wahrscheinlichkeit, dass ein schlechter Akteur eine Sitzung überführt.
Abhängigkeiten und Voraussetzungen	Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTTP-Sitzungsbezeichner rotieren

Verwenden Sie `glide.ui.rotate_sessions`Eigenschaft zum Aktivieren der Rotation der HTTP-Sitzungsbezeichner, um Sicherheitsschwachstellen zu reduzieren.

Wenn sich die Sitzungs-ID eines nicht authentifizierten Anwenders nach der Authentifizierung nicht ändert, ist eine Webanwendung für angreifbar Angriff auf Sitzungsfixierung . Ein böswilliger Anwender kann eine nicht authentifizierte Sitzung starten und dem Opfer die zugehörige Sitzungs-ID geben. Sobald sich das Opfer authentifiziert hat, gibt der böswillige Anwender diese authentifizierte Sitzung jetzt frei.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.rotate_sessions`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	Diese Korrektur hat die SessionID geändert, wenn der Anwender von der nicht authentifizierten Seite zu authentifizierten Seiten navigiert. • Wenn Sie einen Proxy verwenden oder die SessionID bei der ersten Anmeldung eines Anwenders oder für einen beliebigen Zweck hartcodieren, kann dies Auswirkungen auf die Funktionalität haben. • Wenn Sie das SAML 2,0-Plugin für die Single Sign-on-Authentifizierung verwenden, kann dies die gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigen. In diesem Fall können Sie diese Eigenschaft auf „falsch“ festlegen.
Sicherheitsrisiko	(Mittel) SessionID wird verwendet, um den Instanzanwender zu verarbeiten und zu authentifizieren, indem der Sitzungsstatus im Browser beibehalten wird. Daher gilt SessionID als vertrauliche Daten und sollte standardmäßig sicher sein. Sitzungsrotation ist eine Sicherheitssteuerung, die die Änderung der Sitzungs-ID erzwingt, wenn der Anwender von nicht authentifizierten Seiten aus navigiert, um Seiten zu authentifizieren.
Referenzen	Authentifizierung mit SAML

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzahl gleichzeitiger interaktiver Sitzungen minimieren [aktualisiert in Security Center 1,3]

Verwenden Sie diese Eigenschaft mit dem Plugin „gleichzeitige Sitzungen begrenzen“, um die Anzahl der aktiven Sitzungen zu steuern, die von einem Anwender geöffnet werden können.

Verwenden Sie **Glide-Authentifizierung – Max. Gleichzeitige Interaktive Sitzungen** Eigenschaft mit **Gleichzeitige Sitzung Begrenzen** (*com.glide.limit.concurrent.sessions*) Plugin zum Steuern der Anzahl der aktiven Sitzungen, die für einen Anwender geöffnet wurden. Der empfohlene Wert ist **1** , Wodurch die Anzahl der geöffneten Sitzungen reduziert wird (eine größere Anzahl erhöht die Wahrscheinlichkeit, dass eine Sitzung gekapselt werden könnte).

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.authenticate.max.concurrent.interactive.sessions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Ganzzahl
Empfohlener Wert	1
Standardwert	1
Kategorie	Management von Anwendersitzungen
Sicherheitsrisiko	• Schweregradpunktzahl: 3,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn Sie den Standardwert der Eigenschaft größer als 1 festlegen, erhöht sich die Wahrscheinlichkeit von Sitzungs-Hijacking.
Abhängigkeiten und Voraussetzungen	Die **Gleichzeitige Interaktive Sitzungen** (*com.glide.limit.concurrent.sessions*) Plugin muss aktiv sein.
Referenzen	Gleichzeitige Sitzungen begrenzen

Zeitüberschreitungsdauer der Sitzungsaktivität minimieren [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.ui.session_timeout*Eigenschaft, die den Wert für die Zeitüberschreitung der Aktivität in Minuten festlegt.

Die Festlegung dieser Eigenschaft hat mehrere funktionale Auswirkungen:

- Je länger die angegebene Sitzungszeitüberschreitung ist, desto größer wird der Arbeitsspeicher während einer Verarbeitungssitzung ausgelastet. Das Basissystem verwendet eine standardmäßige Zeitüberschreitungsdauer von Apache Tomcat von 30 Minuten.
- Die ServiceNow AI Platform Meldet Anwender weiterhin mit „mich speichern“ ab. Nach 30 Minuten Inaktivität in der Anwendung meldet die Plattform den Anwender automatisch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ab, sofern nicht **Merken Sie Sich** Das Kontrollkästchen auf der Anmeldeseite ist aktiviert. Der Unterschied ist, dass sie sich nicht erneut anmelden, um fortzufahren.

- Wenn Anzeigen oder Inhalte auf den Homepage von Anwendern vorhanden sind, die automatisch aktualisiert werden, wird diese Zeitüberschreitung möglicherweise nie erreicht.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.session_timeout`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Dient zum Erzwingen einer Sitzungszeitüberschreitung.
Empfohlener Wert	Vom Anwender angegebene Zeitüberschreitung in Minuten. 60 Minuten ist der empfohlene Wert, dieser Wert kann jedoch je nach Funktionalität und Sicherheitsanforderung variieren. Legen Sie diesen Wert nicht auf mehr als einen Tag fest.
Sicherheitsrisikobewertung	7,5
Funktionale Auswirkung	Diese Korrektur erzwingt den rechtzeitigen Ablauf des Anwenderaccounts. Keine Auswirkung auf die Funktionalität, die Anwender-Experience wird jedoch geändert.
Sicherheitsrisiko	(Hoch) Anwendersitzungen, die für unbestimmte Zeit aktiv sind, sind ein Sicherheitsrisiko und sollten mit einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verwalten Sie Anwendersitzungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Zeitüberschreitungsdauer des Sitzungsfensters minimieren [aktualisiert in Security Center 1,3]

Verwenden Sie `glide.ui.user_cookie.life_span_in_days`Eigenschaft zum Festlegen des Ablaufzeitraums für das Cookie „mich speichern“. Der Standardwert ist 15 Tage, und die maximale Obergrenze beträgt 30 Tage.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.user_cookie.life_span_in_days`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Management von Anwendersitzungen
Zweck	Zum Aktivieren des Standardablaufs von **Merken Sie sich** Cookie.
Datentyp	Ganzzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	15
Standardwert	15
Sicherheitsrisikobewertung	4,9
Funktionale Auswirkung	Diese Eigenschaft wird vom Endanwender aktiviert, wenn der Endanwender überprüft **Merken Sie sich** Aktivieren Sie das Kontrollkästchen auf der Anmeldeseite, und melden Sie sich bei an ServiceNow AI Platform.
Sicherheitsrisiko	(Mittel) die unbefristeten Anwendercookies sind ein Sicherheitsrisiko und sollten mit einer zeitbasierten Konfiguration ablaufen.
Referenzen	Verfügbare Systemeigenschaften Anwendernamen speichern

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Gespeicherte Kryptografie

Diese Kategorie konzentriert sich auf die Verschlüsselung gespeicherter Daten. Sie umfasst mehrere wichtige Aspekte, z. B. die Verwendung etablierter Algorithmen und kryptografischer Module, die Sicherstellung der richtigen Generierung von Pseudo-zufälligen Werten, die Implementierung der Verschlüsselung basierend auf der Datenklassifizierung und die sichere Speicherung und Isolierung von Schlüsselmaterial.

Glide-KMF-Verschlüsseler aktivieren [in Security Center 1,3.2 entfernt]

Verwalten Sie die für Passwort2-Felder in Ihrer Instanz verwendeten Verschlüsseler.

Verwenden Th E *glide.kmf.encrypter.enabled*Eigenschaft zum Festlegen des KMF-Verschlüsselers als Standardverschlüsselung für Passwort2-Felder. Diese Eigenschaft stellt sicher, dass anstelle eines veralteten Verschlüsselers starke und konforme Verschlüsselungsstandards verwendet werden. Um sicherzustellen, dass der KMF-Verschlüsseler anstelle des Legacy-Verschlüsselers verwendet wird, legen Sie diese Eigenschaft auf fest **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.kmf.encrypter.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Gespeicherte Kryptografie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,9 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Wahr** Stellt sicher, dass der KMF-Verschlüsseler anstelle des Legacy-Verschlüsselers verwendet wird.
Referenzen	Passwort2-Verschlüsselung mit Key Management Framework (KMF)

Deaktivieren Sie die Verwendung des TripleDES/3DES-Verschlüsselungsalgorithmus

Vermeiden Sie die Sicherheitsrisiken veralteter Verschlüsselungsmethoden, indem Sie die Verwendung des TripleDES/3DES-Verschlüsselungsalgorithmus deaktivieren.

Deaktivieren Sie die Verwendung von veralteten, veralteten Triple Data Encryption Standard (3DES oder Triple-DES) in Ihrer Instanz, was zu Verlust und Verlust vertraulicher Informationen führen kann.

Das National Institute of Standards and Technology (NIST) hat von der Verwendung von Triple DES (3DES) zum Verschlüsseln von Daten abgeraten. Weitere Informationen finden Sie unter NIST 800-131A Rev. 2. #3DES ist jetzt für die Verschlüsselung in staatlichen Systemen gesperrt. Künftig kann TDES nur für historische Zwecke verwendet werden, z. B. zum Entschlüsseln alter Nachrichten, zum Entpacken von Schlüsseln und zur MAC-Verifizierung.

Die **glide.security.3des.encryption.allow** Die Systemeigenschaft steuert, ob die 3DES-Verschlüsselung in Ihrer Instanz aktiviert ist. Es gibt jedoch möglicherweise mehrere Schritte, die ausgeführt werden müssen, um sicherzustellen, dass Ihre Instanz zur Einstellung bereit ist. Überprüfen KB1704481 Um weitere Informationen zum Verwerfungsprozess zu erhalten, bevor diese Eigenschaft festgelegt wird.

Weitere Informationen

Attribut	Beschreibung
Name der technischen Konfiguration	glide.security.3des.encryption.allow
Plugin-Anwendbarkeit	Keine
Sicherheitsrisiko	Die Verwendung veralteter und schwacher Verschlüsselung wie 3DES kann zu Verlust und Verlust vertraulicher Informationen führen.
CVSS-Punktzahl (Common Vulnerability Scoring System)	4.2
Bewertung des Common Vulnerability Scoring System (CVSS)	Mittel
Funktionale Auswirkung	Diese Eigenschaft wird auf festgelegt **Falsch** Hilft, zu verhindern, dass Ihre Instanz veraltete und schwache Verschlüsselung verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Dies wirkt sich auf die Speicherung von Passwort2-Daten aus. Überprüfen KB1704481 Weitere Informationen zu den funktionalen Auswirkungen der 3DES-Einstellung.
Abhängigkeiten und Voraussetzungen	Führen Sie die in beschriebenen Aufgaben aus KB1704481 Bevor Sie den Wert dieser Eigenschaft ändern.
Datentyp	Boolean
Basissystemwert	Falsch
Fallback-Wert	falsch
Empfohlener Wert	falsch

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Verwendung von 3DES-Schlüsseln verhindern [Neu in Security Center 7,0]

Deaktivieren Sie die Verwendung statischer 3DES-Schlüssel in Ihrer Instanz mit einer Systemeigenschaft.

Verwenden Sie *glide.security.3des.static_keys_usable*Systemeigenschaft zum Deaktivieren der Verwendung statischer 3DES-Schlüssel in Ihrer Instanz. Diese Eigenschaft sollte automatisch durch eine geplante Aufgabe festgelegt werden, deren Status über die Eigenschaft überprüft werden kann *glide.security.3des.removal_job_status*. In Fällen, in denen diese Eigenschaft nicht auf konfiguriert ist **Falsch** , Nachdem die geplante Aufgabe ausgeführt wurde und der Status lautet KEYS_DEACTIVATED , Die geplante Aufgabe wartet, bis diese Eigenschaft auf konfiguriert ist **Falsch** Bevor Sie mit dem Löschen der statischen 3DES-Schlüssel fortfahren.

Stellen Sie sicher, dass *glide.security.3des.static_keys_usable*lst in der Tabelle „Systemeigenschaften“ [sys_properties] vorhanden und auf einen Wert von festgelegt **Falsch** . Überprüfen KB1704481 Weitere Informationen zur Einstellung von 3DES.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.3des.static_keys_usable*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	wahr
Fallback-Wert	wahr
Kategorie	Gespeicherte Kryptografie
Sicherheitsrisiko	• Schweregradpunktzahl: 5 • CVSS-Punktzahl: Mittel • 3DES ist veraltet, und die Verwendung statischer 3DES- und 3DES-Schlüssel außerhalb der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	temporären Abwärtskompatibilität wird nicht empfohlen. Die weitere Verwendung kann zu Situationen der Offenlegung vertraulicher Informationen führen, wenn ein Anwender Zugriff auf verschlüsselte Daten erhält.
Funktionale Auswirkung	Wenn auf festgelegt **Falsch** , Es kann unwahrscheinlich sein, dass Code und Daten, die sich in der Instanz befinden, auf die sich die statischen 3DES-Schlüssel stützen, jetzt nicht zugänglich sind.
Abhängigkeiten und Voraussetzungen	Keine

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Validierung, Bereinigung und Codierung

Validierung, Bereinigung und Codierung adressieren die Eingabevalidierung, um Schwachstellen wie Cross-Site Scripting (XSS), SQL Injection und andere Angriffe zu verhindern.

Diese Steuerung stellt sicher, dass Eingabevalidierung und Ausgabecodierung vorhanden und korrekt konfiguriert sind, z. B. Codierung oder Escape-Zeichen für Ausgabedaten. Diese Kategorie enthält auch Prüfungen auf Elemente wie Deserialisierung von Objekten und positive Validierung durch Allow-Listen.

HTML-Links zu vertrauenswürdigen Domänen in den Beschreibungsfeldern des Impact Workspace-Moduls zulassen [Neu in Security Center 7,0]

Verwenden Sie eine Systemeigenschaft, um die in den Beschreibungsfeldern zulässige HTML zu bereinigen. Diese Eigenschaft beschränkt die zulässigen Links auf diejenigen aus den vertrauenswürdigen Domänen, die in der Eigenschaft aufgeführt sind.

Hinweis: Diese Härtungseinstellung ist nicht Teil der Härtungsbasis. Sie wird nicht auf den Sicherheitscenter-Härtungsseiten angezeigt und wirkt sich auf Ihre Härtungspunktzahl aus.

Das Modul „Impact Workspace“ ermöglicht HTML in einer Reihe von beschreibungsbezogenen Feldern. Wenn konfiguriert, wird *sn_impact_common.whitelisted.url_HTML_injection*Die Systemeigenschaft enthält eine kommagetrennte Liste von Domänennamen. Beschreibungsfelder für das Modul „Impact Workspace“ dürfen HREFs mit URLs nur aus den in der Eigenschaft aufgeführten Domänen enthalten.

Stellen Sie sicher, dass *sn_impact_common.whitelisted.url_HTML_injection*Die Systemeigenschaft ist auf eine kommagetrennte Liste von Domänennamen festgelegt, die die Domänen darstellen, die in HTTP-Referenz-URLs von Beschreibungsfeldern für das Impact Workspace-Modul zulässig sind.

Um HREFs in diesen Feldern nicht zuzulassen, legen Sie die Eigenschaft auf eine leere Zeichenfolge fest. Wenn die Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden ist, wird standardmäßig diese Liste verwendet: servicenow.com, service-now.com, youtube.com, google.com, youtu.be, soti.net, dpdhl.sharepoint.com, documentation.avaya.com, www.juniper.net, servicenow.sharepoint.com, servicenow-my.sharepoint.com, scaledagileframework.com .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*sn_impact_common.whitelisted.url_HTML_injection*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolgenliste
Empfohlener Wert	servicenow.com, service-now.com, youtube.com, google.com, youtu.be, soti.net, dpdhl.sharepoint.com, documentation.avaya.com, www.juniper.net, servicenow.sharepoint.com, servicenow-my.sharepoint.com, scaledagileframework.com
Standardwert	servicenow.com, service-now.com, youtube.com, google.com, youtu.be, soti.net, dpdhl.sharepoint.com, documentation.avaya.com, www.juniper.net, servicenow.sharepoint.com, servicenow-my.sharepoint.com, scaledagileframework.com
Fallback-Wert	servicenow.com, service-now.com, youtube.com, google.com, youtu.be, soti.net, dpdhl.sharepoint.com, documentation.avaya.com, www.juniper.net, servicenow.sharepoint.com, servicenow-my.sharepoint.com, scaledagileframework.com
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,4 • CVSS-Punktzahl: Mittel • Wenn der Eigenschaft eine nicht vertrauenswürdige Domäne hinzugefügt wird, werden diese Felder geöffnet, um Links zu riskanten Quellen zu enthalten, die HTML-Einschleusungsangriffe auslösen können. Das genaue Risiko hängt von der Kundeninstanz ab.
Funktionale Auswirkung	Wenn die Eigenschaft leer ist, sind im Feldtext keine HREFs zulässig, und alle HREFs werden entfernt. Alle Links, die Domänen verwenden, die nicht in der Eigenschaft aufgeführt sind, werden entfernt. Ein falscher Wert für dieses Feld kann zu beschädigten Daten für die betroffenen Felder führen.
Abhängigkeiten und Voraussetzungen	Wenn *sn_impact_common.blacklist_tags_HTML_injection*Die Systemeigenschaft enthält HTML-Tags, die HREF-Links umgeben. Dann werden alle Links innerhalb dieser Tags entfernt.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf skriptfähige GlideSystemUserSession-API beschränken [aktualisiert in Security Center 1,3 und 2,0]

Die vom Client aufrufbare skriptfähige GlideSystemUserSessionSandbox-API stellt die Methoden addErrorMessageNoSanitization und addInfoMessageNoSanitization von GlideSystemUserSession für die JavaScript-Sandbox bereit. Dadurch können alle Anwender diese Methode über ein Skript aufrufen.

`gs.addErrorMessageNoSanitizationMessaging()` Und `gs.addInfoMessageNoBereinigung()` Werden in der Skriptumgebung für Protokollierung und Benachrichtigungen verwendet. Beide sind in der Sandbox verfügbar, wenn diese Eigenschaft nicht auf den empfohlenen Wert „falsch“ festgelegt ist. Die Sandbox ist eine Skripterstellungsumgebung mit geringen Berechtigungen, die nicht authentifizierten Anwendern ohne Rolle zur Verfügung steht. Beide Methoden können verwendet werden, um einem Anwender nicht bereinigte Eingaben anzuzeigen. Das Anzeigen nicht bereinigter Eingaben für den Anwender ist gefährlich, da nicht bereinigte Eingaben gefährlichen Code enthalten können, der im Browser des Anwenders ausgeführt wird. Dies kann für traditionelle reflektierte XSS-Angriffe verwendet werden. Reflektierte XSS-Angriffe können in mehreren Szenarien verwendet werden, einschließlich Sitzungs-Hijacking.

Festlegen **glide.sandbox.usersession.allow_unsanitized_messages** Systemeigenschaft zu **Falsch** . Wenn in der Tabelle „Systemeigenschaften“ [sys_properties] kein Datensatz dieser Eigenschaft vorhanden ist, erstellen Sie einen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.sandbox.usersession.allow_unsanitized_messages`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Zugriffssteuerung
Zweck	Diese Eigenschaft schränkt den Aufruf nicht bereinigter Informations- oder Fehlermeldungen in einer Anwendersitzung im Sandkasten ein.
Typ	Boolean
Empfohlener Wert	falsch
Standardwert	wahr
Sicherheitsrisikobewertung	8.1
Funktionale Auswirkung	Wenn Sie die Eigenschaft mit dem Wert „falsch“ festlegen, wird keine Nachricht erstellt oder protokolliert, wenn diese Funktionen aufgerufen werden.
Sicherheitsrisiko	(Hoch) ohne entsprechende Bereinigung kann auf potenziell gefährliche Inhalte zugegriffen werden, und die Funktion „nicht bereinigter Fehler“ ist für Skript verfügbar.
Referenzen	Zugriffssteuerung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JavaScript-Tags in eingebettetem HTML deaktivieren [aktualisiert im Sicherheitscenter 1,3]

Verwenden Sie `glide.ui.security.codetag.allow_script`Eigenschaft zum Deaktivieren der Unterstützung für die Einbettung von HTML-JavaScript-Code, der mit dem Tag [Code] erstellt wurde.

Die ServiceNow AI Platform Mildert viele Einschleusungen und standortübergreifende Angriffe durch Implementierung von Escape- und Codierungstechniken ab. Daher können Anwender keine HTML-formatierten Eingaben für Journalfelder schreiben und übermitteln. Journalfelder können jedoch Text, der in Code-Tags eingeschlossen ist, als HTML rendern. Stellen Sie sicher, dass `glide.ui.security.codetag.allow_script`Eigenschaft ist in der Tabelle „sys_properties“ vorhanden und auf „falsch“ festgelegt.

- Es besteht jedoch ein entsprechendes Sicherheitsrisiko. Wenn auf festgelegt **Wahr** , Böswillige Anwender können schädlichen HTML-JavaScript-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Legen Sie diese Eigenschaft auf fest **Falsch** Damit Administratoren verhindern können, dass Journalfelder HTML-JavaScript-Code rendern, indem sie die Unterstützung für deaktivieren `[Code]` Tag.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.security.codetag.allow_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Schützt vor Site-übergreifendem Skripting und böswilliger Skriptausführung
Empfohlener Wert	falsch
Standardwert	falsch
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	Diese Fehlerkorrektur erzwingt das JavaScript-Escaping auf der Anwenderoberfläche und rendert die codierten Ergebnisse für den Anwender. Dies kann basierend auf der Interaktion des Instanzanwenders mit den resultierenden Daten Auswirkungen auf die Funktionalität haben.
Sicherheitsrisiko	(Hoch) die Eingabevalidierung muss in der Anwendung erfolgen, um sich vor siteübergreifenden Skripting-Angriffen zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in der Anwendersitzung im Kontext des angemeldeten Browsers. Angreifer können sie verwenden, um Sitzungsinformationen und vertrauliche Daten zu stehlen.
Referenzen	Beschränken Sie das CODE-Tag in Journalfeldern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Journalfeldeinträge als HTML rendern Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Sicherheitsmanager für gesicherte Java aktivieren [Neu in Security Center 1,3]

Die `glide.security.manager`Die Eigenschaft enthält den Java-Klassennamen des aktuellen Java-Sicherheitsmanagers.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.security.manager`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	`com.glide.sys.security.ContextualSecurityManager`
Standardwert	`com.glide.sys.security.ContextualSecurityManager`
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,2 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Wenn `glide.security.manager`lst nicht auf den empfohlenen Wert von festgelegt `com.glide.sys.security.ContextualSecurityManager`, Dann verwendet die Instanz möglicherweise einen veralteten Java-Sicherheitsmanager, dem die erwarteten Härtungsrichtlinien fehlen. Ohne diese Härtung könnte ein böswilliger Akteur mit Skriptausführungszugriff Remotecodeausführung auf der Instanz erhalten.
Abhängigkeiten und Voraussetzungen	Keine

HTML-Bereinigung erzwingen [aktualisiert in Security Center 1,3]

Verwenden Sie `com.glide.security.check_unsanitized_html`Eigenschaft zum Erzwingen des Bereinigungsverhaltens von translated_html-Feldern auf globaler Ebene für Feldzuweisungen.

HTML ist einer der Typen, die den Wörterbuchfeldern zugewiesen werden können. Das Zuweisen von HTML-Feldern zu einem beliebigen Feldtyp bietet die Möglichkeit, Inhalte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mithilfe von HTML-Tags zu formatieren (z. B. <p>, <a href>, <b>, <font>, <img>). Um schädliche Aktivitäten zu verhindern, können bestimmte HTML-Tags mithilfe einer Sperrliste nicht zulässig sein. Diese Eigenschaft verhindert, dass unzulässige Tags in den Feldern „translate_html“ in Ihrer Instanz verwendet werden.

- Legen Sie diese Eigenschaft auf fest **Erzwingen** Dient zum Erzwingen des Bereinigungsverhaltens von translated_html-Feldern.
- Legen Sie die Eigenschaft auf fest **Deaktivieren** Zum Deaktivieren der HTML-Bereinigung, um blockierte HTML-Tags in übersetzten_HTML-Feldern zuzulassen.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*com.glide.security.check_unsanitized_html*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert die Verwendung unsicherer HTML-Tags zum Schutz vor Angriffen wie siteübergreifendem Skripting.
Typ	Zeichenfolge
Empfohlener Wert	Erzwingen
Standardwert	Erzwingen
Sicherheitsrisikobewertung	7.3
Funktionale Auswirkung	Diese Korrektur erzwingt die HTML-Bereinigung auf der Anwenderoberfläche und rendert dem Anwender übersetzte HTML-Felder. Dies kann sich auf die Lesbarkeit und Formatierung auswirken.
Sicherheitsrisiko	(Hoch) die Eingabevalidierung muss in der Anwendung erfolgen, um sich vor siteübergreifenden Skripting-Angriffen zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in Anwendersitzungen im Kontext des angemeldeten Browsers. Angreifer können sie verwenden, um Sitzungsinformationen und vertrauliche Daten zu stehlen.
Referenzen	HTML-Bereinigung

Stellen Sie sicher, dass die Kontextsuche keine nicht validierte Umleitung enthält [Neu in Security Center 7,0]

Verhindern Sie mit einer Systemeigenschaft, dass Ergebnisse der Kontextsuche Referral-Links außerhalb der aktuellen Domäne enthalten.

Das Plugin „Kontextsuche“ zeigt Suchergebnisse in einem neuen Fenster mit an *cxs_new_window*UI-Seite. Diese UI-Seite enthält einen Verweislink, der durch Angabe eines Werts festgelegt werden kann *sysparm_url*. Wenn *com.snc.contextual_search.cxs_new_window.force_relative_link*Systemeigenschaft ist auf festgelegt **Wahr** , *sysparm_url*Kann nur Links enthalten, die relativ zur aktuellen Domäne sind. Diese Einschränkung verhindert, dass die UI-Seite als nicht validierte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weiterleitung zu einer von Angreifern gesteuerten Website verwendet wird. Wenn die Eigenschaft auf festgelegt ist **Falsch** , *sysparm_url*Kann mit jeder Website verknüpft werden.

Legen Sie die Eigenschaft *com.snc.contextual_search.cxs_new_window.force_relative_link* auf **true** fest. Wenn die Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden ist, lautet der Standardwert **Falsch** . Wenn die Eigenschaft in der Tabelle vorhanden ist, ist sie standardmäßig auf festgelegt **Wahr** .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.snc.contextual_search.cxs_new_window.force_relative_l*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Fallback-Wert	falsch
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 3,1 • CVSS-Punktzahl: Mittel • Wenn auf festgelegt **Falsch** , *sysparm_url*Kann mit einer beliebigen Website verknüpft werden, wodurch die UI-Seite als nicht validierte Weiterleitung zu einer von Angreifern gesteuerten Website verwendet werden kann.
Funktionale Auswirkung	Wenn auf festgelegt **Wahr** , *sysparm_url*Darf nur Links enthalten, die relativ zur aktuellen Domäne sind. Diese Einschränkung bedeutet, dass die UI-Seite immer nur mit Webseiten in der aktuellen Domäne verknüpft werden kann. Die UI-Seite soll jedoch Suchergebnisse aus der aktuellen Domäne anzeigen und sollte immer nur mit der aktuellen Domäne verknüpft werden.
Abhängigkeiten und Voraussetzungen	Das Plugin „Kontextsuche“ (com.snc.contextual_search) muss aktiv sein.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

AJAXEvaluate deaktivieren

Verwenden Sie *glide.script.allow.ajaxevaluate*Zum Schutz der System-API vor Schwachstellen bei der Ausführung von Client-Skripts durch AJAX-Aufrufe.

Zum Bearbeiten der Eigenschaft ist eine Erhöhung auf die Rolle „Security_admin“ erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.script.allow.ajaxevaluate`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um zu verhindern, dass ein Anwender Skripts als Administratorberechtigung ausführt.
Empfohlener Wert	falsch
Standardwert	falsch
Konfigurationstyp	Boolean
Funktionale Auswirkung	Diese Korrektur erzwingt das Deaktivieren des AJAXEvaluate-Prozessors. Es kann sich auf die Funktionalität auswirken, wenn Sie den AJAX-Auswertungsprozessor explizit als Teil von anwenderdefinierten Skripts verwenden.
Sicherheitsrisiko	(Hoch) der AjaxEvaluator-Prozessor führt Client-Skripts in der Sandbox aus, es gibt jedoch mehrere zusätzliche Eigenschaften, mit denen der Umfang der Aktivitäten in der Sandbox erweitert werden kann.
Sicherheitsrisikobewertung	7.3
Referenzen	Diese Eigenschaft gehört zur gleichen Eigenschaftenfamilie, die die Ausführung von Skripts, die vom Client stammen, sicherstellt und einschränkt, z. B. `glide.script.allow.ajaxevaluate`. Weitere Informationen finden Sie unter Aktivieren Sie AJAXEvaluate .

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Deaktivieren Sie die Entitätserweiterung im XMLDocument2-Streaming-Parser [Aktualisiert in Security Center 1,5]

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie `glide.stax.allow_entity_resolution`Eigenschaft zum vollständigen Deaktivieren der Erweiterung externer Entitäten. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

Deaktivieren Sie die Entitätserweiterung in Ihrer Instanz, um Ihre Instanz vor Angriffen wie der Fähigkeit, Systemdateien zu lesen, und Denial of Service zu schützen. Verwenden Sie die Systemeigenschaft, um zu verhindern, dass XML-Entitäten während der Analyse durch den Streaming-Parser (XMLDocument2) erweitert werden.

Legen Sie fest **Glide.stax.allow_Entity_Resolution** Systemeigenschaft zu **Falsch** Zum Deaktivieren der Entitätserweiterung in Ihrer Instanz. Wenn diese Eigenschaft nicht in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Systemeigenschaften“ [sys_properties] angezeigt wird, ist der Standardwert **Wahr** . Erstellen Sie den Eigenschaftsdatensatz, und legen Sie den Wert auf fest **Falsch** Um den Wert zu ändern.

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen:

- Legen Sie fest *glide.xml.entity.whitelist.enabled*Und *glide.stax.whitelist_enabled*Eigenschaften auf „wahr“. Weitere Informationen finden Sie unter Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0] Und Validierung der XMLdoc2-Entität mit zulässiger Entitätserweiterung anfordern [aktualisiert in Security Center 1,3].
- Definieren Sie eine Liste von durch Kommas getrennten FQDN in *glide.xml.entity.whitelist*Eigenschaft, die die einzigen URLs ist, die mit der Verarbeitung von XML-Entitäten erreicht werden können. Eigenschaft. Weitere Informationen finden Sie unter Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0].

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.stax.allow_entity_resolution*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen einen XML-Entitätserweiterungs-/Milliarden-Lachen-Angriff zu schützen.
Empfohlener Wert	falsch
Standardwert	wahr
Funktionale Auswirkung	Wenn für die Anpassung eine Entitätserweiterung verwendet wird, dann die ServiceNow AI Platform Blockiert möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Kritisch) ein Angreifer kann diese Schwachstelle verwenden, um Daten exponentiell zu erweitern und schnell alle Systemressourcen zu verbrauchen.
Workaround	Wenn die Anpassung eine Entitätserweiterung erfordert, legen Sie diese Eigenschaft auf „wahr“ fest, und befolgen Sie die in dokumentierten Schritte Validierung der XMLdoc2-Entität mit zulässiger Entitätserweiterung anfordern [aktualisiert in Security Center 1,3].

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen

Weitere Informationen zu OWASP-Ressourcen finden Sie unter OWASP .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

url für externe Inhalte deaktivieren [aktualisiert in Security Center 2,0]

Verwalten Sie mit Connect-Chat, wie externe Linkmetadaten in Ihrer Instanz verwendet werden.

Verwenden Sie `glide.ui.url.external.content`Eigenschaft zum Verwalten externer Linkmetadaten in Ihrer Instanz. Wenn die Eigenschaft auf den empfohlenen Wert von festgelegt ist **Falsch** , Dann werden keine Metadaten des externen Links gerendert. Wenn auf festgelegt **Wahr** Dann Connect-Chat Ruft Metadaten für externe Links aus Quellen wie YouTube oder Nachrichtenartikeln ab, um reichhaltigere Nachrichten zu rendern. Dies kann zu SSRF-Angriffen (Server Side Request Forgery) führen.

Stellen Sie die Glide-Eigenschaft sicher `glide.ui.url.external.content`Ist vorhanden und auf den Wert „falsch“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ui.url.external.content`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,2 • CVSS-Punktzahl: Hoch • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Wahr** Ihre Instanz könnte SSRF-Angriffen (serverseitige Anforderungsfälschung) ausgesetzt werden.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Connect-Chat

Herunterladbare MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]

Die `glide.ui.attachment.download_mime_types`Die Eigenschaft erzwingt, dass die angegebene Liste gefährlicher Dateitypen auf den Client heruntergeladen und nicht inline im Browser angezeigt wird.

Wenn die Eigenschaft ist `glide.ui.attachment.force_download_all_mime_types`Ist auf „wahr“ festgelegt, dann die `glide.ui.attachment.download_mime_types`Eigenschaft wird überschrieben, sodass alle MIME-Typen heruntergeladen und nicht vom Browser gerendert werden. Zum Beispiel erzwingt das Herunterladen von Text/HTML, dass eine HTML-Datei als Datei auf den Client heruntergeladen und nicht inline im Browser angezeigt wird, um einen XSS-Angriff zu verhindern. XSS kann zu einer einfachen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungseskalation an höhere Rollen wie Administrator führen, in denen mehr seitliche Bewegungen erfolgen können.

Neue Korrektur: Stellen Sie die Eigenschaft sicher `glide.ui.attachment.force_download_all_mime_types`lst auf „wahr“ festgelegt. Wenn die Eigenschaft in der Tabelle „sys_properties“ nicht vorhanden ist, ist der Standardwert „falsch“.

Hinweis: Die Rolle Security_admin ist erforderlich, um die Eigenschaft zu bearbeiten.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.attachment.download_mime_types`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Wenn Sie die Liste gefährlicher Dateitypen ordnungsgemäß verwalten, die nicht im Browser angezeigt werden können, werden Cross Site Scripting-Angriffe (XSS) verhindert.
Empfohlener Wert	Liste der anwendbaren MIME-Typen oder des empfohlenen Werts: Text/html,image/svg,image/svg+xml,Application/xml
Standardwert	Liste der anwendbaren MIME-Typen für den Standardwert: Text/html,image/svg,image/svg+xml,Application/xml
Konfigurationstyp	Zeichenfolge: Beliebige kommagetrennte Werte von Anwendungs-MIME-Typen.
Funktionale Auswirkung	Diese Korrektur erzwingt die Durchführung von Validierungsprüfungen, bevor eine Aktion ausgeführt wird, wenn Sie auf einen Anhang in klicken ServiceNow AI Platform Anwendung. Es gibt keine potenziellen Auswirkungen, aber die Anwender-Experience wird geändert.
Sicherheitsrisiko	(Mittel) Angreifer können MIME-Typen missbrauchen und unbeabsichtigte Skriptinhalte im Anhang auf der Seite des Opfers platzieren, um vertrauliche Informationen zu erfassen. Die Fähigkeit, XSS zu verwenden, kann zu einer einfachen Berechtigungseskalation zu höheren Rollen wie Administrator führen, wo mehr seitliche Bewegungen durchgeführt werden können. Füllen Sie die Eigenschaft im aktuellen Kontext mit einer Liste von kommagetrennten Anhang-MIME-Typen aus, die im Browser nicht inline gerendert werden sollen.
Sicherheitsrisikobewertung	6,4
Zugehörige Eigenschaften	• `glide.ui.attachment.force_download_all_mime_types` • `glide.ui.attachment.tables_ignore_force_download`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Referenzen	Eingeschränkte herunterladbare MIME-Typen definieren [aktualisiert in Security Center 1,3, 1,5 und 2,0].

Eingebetteten HTML-Code deaktivieren [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.ui.security.allow_codetag*Eigenschaft zum Deaktivieren der Unterstützung für die Einbettung von HTML-Code, der mit dem Tag [Code] erstellt wurde.

Deaktivieren Sie die Unterstützung für die Anzeige von HTML-Code, der mit eingebettet wurde `[Code]` Tag. Dieses Tag ermöglicht die Anzeige von gerendertem HTML in Journalfeldern und kann zu Angriffen mit Cross-Site Scripting (XSS) führen. Diese Angriffe können die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des angemeldeten Browsers ermöglichen. Angreifer können diese Skripts verwenden, um Sitzungsinformationen und vertrauliche Daten zu stehlen. Die HTML-Sprache wurde nicht so konzipiert, dass Skript von der Formatierung getrennt wird. Daher birgt das Zulassen von anwendergesteuertem HTML in jedem System ein inhärentes Risiko.

Wird festgelegt **glide.ui.security.codetag.allow_script** Bis **Falsch** Ist konform und reduziert dieses Risiko erheblich, jedoch bleibt ein geringfügiges Risiko bestehen. Dadurch wird nur der Skriptteil von deaktiviert `Code` Tag, und basiert auf der Bereinigung aller bekannten Konventionen des Skripts in HTML.

Legen Sie fest **glide.ui.security.allow_codetag** Systemeigenschaft zu **Falsch** Um zu verhindern, dass Journalfelder und -Formulare gerenderte HTML anzeigen.

Die ServiceNow AI Platform Mildert viele Einschleusungen und standortübergreifende Angriffe durch Implementierung von Escape- und Codierungstechniken ab. Daher können Anwender keine HTML-formatierten Eingaben für Journalfelder schreiben/übermitteln. Journalfelder können jedoch Text, der in Code-Tags eingeschlossen ist, als HTML rendern.

- Es besteht jedoch ein entsprechendes Sicherheitsrisiko. Wenn auf festgelegt `Wahr` , Böswillige Anwender können schädlichen HTML-JS-Code schreiben, der nach dem Rendern von Journalfeldern in einem anderen Client-Browser ausgeführt werden kann.
- Legen Sie diese Eigenschaft auf fest `Falsch` Damit Administratoren verhindern können, dass Journalfelder HTML-Code rendern, indem sie die Unterstützung für deaktivieren `[Code]` Tag.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.ui.security.allow_codetag
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Konfigurieren Sie im Instanz-Sicherheitszentrum	Ja
Zweck	Schützen Sie vor Site-übergreifendem Skripting und böswilliger Skriptausführung
Empfohlener Wert	falsch
Standardwert	wahr
Sicherheitsrisikobewertung	4.2

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Diese Korrektur erzwingt die HTML-Codierung auf der Anwenderoberfläche und rendert die codierten Ergebnisse für den Anwender. Diese Eigenschaft ist auf festgelegt `Wahr` Standardmäßig. In diesem Status zeigt Ihre Instanz gerendertes HTML in Journalfeldern und Formularen an. Wenn diese Eigenschaft auf festgelegt ist `Falsch` , HTML wird nicht ordnungsgemäß gerendert, und HTML-Tags werden möglicherweise in Journalfeldern in Formularen angezeigt. Dies kann sich nachteilig auf die Funktionalität und die Anwenderinteraktionen mit den resultierenden Daten auswirken.
Sicherheitsrisiko	(Mittel) die Eingabevalidierung muss in der Anwendung erfolgen, um sich vor siteübergreifenden Skripting-Angriffen zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des angemeldeten Browsers. Angreifer können sie verwenden, um Sitzungsinformationen und vertrauliche Daten zu stehlen.

HTML-Bereinigung in Virtual Agent aktivieren [aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie *`com.glide.cs.html.sanitizer.enabled`*Eigenschaft zum Aktivieren des HTMLSanitizerService.

Diese Eigenschaft steuert, ob der HtmlSanitizerService aktiviert ist. Wenn *`com.glide.cs.html.sanitizer.enabled`*lst nicht auf „wahr“ festgelegt, ist im VA-Webclient ein gespeicherter Angriff auf Cross-Site Scripting (XSS) möglich.

Weitere Informationen

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Attribut	Beschreibung
Eigenschaftsname	*`com.glide.cs.html.sanitizer.enabled`*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert die Anwendung vor Site-Cross-Scripting und HTML-Injection-Angriffen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8
Funktionale Auswirkung	Diese Korrektur erzwingt den HTML-Ausgabecodierungsmechanismus, bevor die Anwenderdaten an den Anwender zurückgerendert werden. Wenn der Kunde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	eine Anpassung hat, die das Rendern des HTML-Attributs oder der Inhaltsdaten beinhaltet, hat dies Auswirkungen auf die Funktionalität.
Sicherheitsrisiko	(Hoch) Anwendereingaben sollten sicher behandelt werden, wenn die Daten in der Anwendung gespeichert und verarbeitet werden. Dies reduziert clientseitige Cross-Site-Skripting-Angriffe, indem die Daten in der Ausgabe codiert werden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Jelly JS-Interpolationsschutz aktivieren

Verwenden Sie `glide.ui.jelly.js_interpolation.protect`Eigenschaft, um sicherzustellen, dass JavaScript, das auf einer Jelly-Seite ausgeführt werden soll, mithilfe der Jelly-Interpolation vor Einschleusung geschützt ist.

Wenn Sie die Eigenschaft auf festlegen **Wahr** , Eine Anwendung durchläuft eine Jelly-Skriptstruktur (geschachtelt). Er umschließt potenziell gefährliche Jelly-Ausdrücke mit einem Filter, der:

- Escape-Zeichen für ihre Ergebnisse, um sicher zu sein, oder
- Wenn ihre Sicherheit nicht garantiert werden kann, generiert eine SecurityException, da der Ausdruck, der ausgewertet wurde, ein mögliches Sicherheitsproblem darstellt.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.jelly.js_interpolation.protect`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um Angriffe auf die Ausführung böswilliger Codes zu mindern, die mit Jelly Injection auftreten können.
Empfohlener Wert	wahr
Standardwert	falsch
Sicherheitsrisikobewertung	9
Funktionale Auswirkung	Diese Eigenschaft ermittelt am besten, ob ein Ausdruck in Anführungszeichen gesetzt wird. Möglicherweise wird fälschlicherweise ein legitimer Ausdruck angegeben. In diesem Fall kann es erforderlich sein, einen Ausdruck manuell als sicher zu markieren.
Sicherheitsrisiko	(Mittel) JEXL-Injektion ist eine Form der Eingabeinschleusung, die für eindeutig ist ServiceNow AI Platform Dies kann sowohl zu Cross-Site-Anforderungsfälschung als auch zur Codeausführung führen. Das vollständige Deaktivieren des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	Schutzes kann potenziell viele P1-Sicherheitsschwachstellen öffnen.
Workaround	So markieren Sie einen Ausdruck manuell als Safe, fügen Sie dem Jelly-Ausdruck EIN SAFE-Präfix hinzu: `${SAFE:sysparm_input};` Das blinde Hinzufügen von SAFE zu jedem Ausdruck ist die falsche Methode, um das Problem anzugehen, da es eine Sicherheitslücke öffnen kann. • Fügen Sie einem Ausdruck SAFE nur hinzu, wenn Sie garantieren können, dass der Ausdruck keine Eingaben vom Client enthält. • Wenn dies der Fall ist, kann ein böswilliger Client die Auswertung von privilegiertem JavaScript veranlassen.
Referenzen	Jelly Tags Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Jelly JS-Interpolationsschutz für geschachtelte Ausdrücke aktivieren [aktualisiert in Security Center 2,0]

Verwalten Sie den Interpolationsschutz für Ihre Instanz.

Verwenden Th E *glide.ui.jelly.js_interpolation.protect_nested_expressions*Eigenschaft zum Verwalten des Interpolationsschutzes. Der Interpolationsschutz stellt sicher, dass Jelly-Ausdrücke, die in JavaScript verwendet werden, als sicher gelten müssen, indem sie entweder unter bestimmte Kategorien fallen oder im Ausdruck selbst als SICHER markiert werden. Wenn diese Minderung nicht aktiviert ist, kann ein ungültiger Akteur einen GET-Parameter an eine Jelly-Seite senden und bewirken, dass der Inhalt dieses Parameters als serverseitiges JavaScript mit Administratorrechten ausgewertet wird. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Wahr** , Schädliche Jelly-Ausdrücke, die in JavaScript interpoliert werden, sind zulässig, und ein Anwender kann Code mit einer Jelly-Vorlage ausführen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.jelly.js_interpolation.protect_nested_expressions*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Empfohlener Wert	wahr
Standardwert	falsch
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 9 • CVSS-Punktzahl: Kritisch • Sicherheitsrisikodetails: Wenn die Eigenschaft auf festgelegt ist **Falsch** , Dann sind schädliche Jelly-Ausdrücke zulässig.
Abhängigkeiten und Voraussetzungen	Keine

Relative Links erzwingen [aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie *glide.cms.catalog_uri_relative*Eigenschaft, für die relative Links vom URI-Parameter erzwungen werden sollen `/ess/catalog.do` .

Die *glide.cms.catalog_uri_relative*Eigenschaft erzwingt relative Links aus dem URI-Parameter in /ess/catalog.do. Wenn *glide.cms.catalog_uri_relative*lst nicht auf den empfohlenen Wert „wahr“ festgelegt, wird die URL nicht mit der Funktion „enforceRelativeURL(url)“ bereinigt. Absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil eines Parameters oder eines Feldwerts verwendet werden, wodurch die Quellseite zu einer von Angreifern kontrollierten Website weitergeleitet wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.cms.catalog_uri_relative*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Zum Einschränken von Versuchen, externe nicht autorisierte Inhalte zu verknüpfen.
Empfohlener Wert	wahr
Standardwert	falsch
Sicherheitsrisikobewertung	2,6
Funktionale Auswirkung	Diese Korrektur erzwingt die Validierung auf der Katalogseite, sodass nur relative URLs zulässig sind. Vorhandene Links zu externen Webanwendungen werden beschädigt.
Sicherheitsrisiko	(Hoch) absolute URLs können ein Sicherheitsrisiko darstellen, wenn sie als Teil eines Parameters oder eines Feldwerts verwendet werden. Dadurch wird die Quellseite zu einer von Angreifern kontrollierten Website weitergeleitet.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfung der URL-Zulässigkeitsliste erzwingen [aktualisiert in Security Center 1,3, 1,5 und 2,0]

Verwenden Sie `glide.security.url.whitelist`Systemeigenschaft zum Hinzufügen einer zusätzlichen Validierungsebene, um sicherzustellen, dass eine eingeführte externe URL Teil von URLs mit Einschlussliste sein soll.

Schützen Sie Ihre Anwender vor einer clientseitigen offenen Umleitung, die es Angreifern ermöglicht, Ihre Anwender auf nicht vertrauenswürdige und schädliche Seiten umzuleiten.

Wenn **glide.security.url.whitelist.strict_check** Ist nicht auf den empfohlenen Wert von festgelegt **Wahr** , Alle externen URLs sind für die Weiterleitung zulässig, solange dies der ist **glide.security.url.whitelist** Systemeigenschaft ist leer. Wenn **glide.security.url.whitelist** Ist nicht leer, dann sind nur externe URLs zulässig, die in dieser Eigenschaft aufgeführt sind.

Festlegen **glide.security.url.whitelist.strict_check** Bis **Wahr** Oder stellen Sie sicher **glide.security.url.whitelist** Ist mit den zulässigen externen URLs konfiguriert, um Ihre Instanz vor offenen Umleitungsangriffen zu schützen.

Diese Eigenschaft gilt in den folgenden Fällen:

- `/Logout.do?sysparm_goto_url={externe URL}`
- `/cms_login_redirect.do?sysparm_goto_url={External URL}`

Anwender werden zu einer externen vertrauenswürdigen Website weitergeleitet, nachdem sie sich von der Instanz abgemeldet haben:

- `/Logout_redirect.do?sysparm_url={Extern URL}`
- `/saml_redirector.do?sysparm_URI={externe URL}`

Wenn SAML aktiviert ist, wird eine Abmelde-URL des Identitätsanbieters (Identity Provider, IDP) aufgerufen.

Stellen Sie die Eigenschaft sicher `glide.security.url.whitelist.strict_check`Ist auf „wahr“ oder die Eigenschaft festgelegt `glide.security.url.whitelist`Ist auf einen Wert festgelegt.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.security.url.whitelist`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Zum Implementieren der Safe-URL-Umleitung während der Anmeldung, Abmeldung oder anderer Umleitungen. Diese Eigenschaft mindert einen der OWASP-Top-10-Angriffe, die als für ungültig erklärte Umleitungen und Weiterleitungen bezeichnet werden.
Typ	Zeichenfolge
Standardwert	wahr
Empfohlener Wert	wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Wert	Genehmigte URLs Ihrer Organisation [einige definierte FQDN (Fully Qualified Domain Name), z. B. http://www.servicenow.com]
Sicherheitsrisikobewertung	6.3
Funktionale Auswirkung	Diese Korrektur erzwingt die Validierung auf der Abmeldeseite. Dies kann sich auf die Funktion eines Anwenders einer Instanz mit einer SSO/SAML-Konfiguration auswirken.
Sicherheitsrisiko	(Hoch) die offene Umleitung auf Clientseite kann es Angreifern ermöglichen, Opfer/Anwender auf eine vom Angreifer kontrollierte Website umzuleiten, und wird als Sicherheitsrisiko betrachtet.
Referenzen	Multi-SSO (SAML 2,0) – Fehler und Korrekturen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Excel-Formeln mit Escape-Zeichen [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.export.escape_formulas*Eigenschaft zum verhindern von Excel-Injection, auch als Formelinjektion bezeichnet.

Verhindern Sie, dass potenziell schädliche Formeln in Programmen wie Excel nach dem Exportieren und Öffnen der Datei ausgeführt werden, indem Sie Formeln in diesen Dateien mit Escape-Zeichen versehen. Excel-Injection tritt auf, wenn Websites nicht vertrauenswürdige Einträge in Excel-Dateien einbetten. Wenn Sie eine Tabellenkalkulationsanwendung wie Microsoft Excel oder LibreOffice-Aufruf verwenden, um eine Datei zu öffnen, werden alle Zellen, die mit +, -, = oder @ beginnen, als Formel interpretiert, sofern sie nicht ordnungsgemäß mit Escape versehen sind. Schädliche Formeln stellen ein Risiko dar, auch wenn die Tabelle keine vertraulichen Informationen enthält, da sie verwendet werden können, um den Computer des Betrachters durch Codeausführung zu gefährden.

Legen Sie fest **glide.export.escape_formulas** Systemeigenschaft zu **Wahr** Um die Ausführung dieser Formeln zu verhindern.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.export.escape_formulas*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um die Anwendung gegen Excel- oder Formeleinschleusung zu verhindern.
Empfohlener Wert	wahr
Standardwert	falsch
Sicherheitsrisikobewertung	6,4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Funktionale Auswirkung	Böswillig erstellte Formeln können dazu verwendet werden, den Computer des Anwenders zu kapern, indem Schwachstellen in der Tabellenkalkulationssoftware ausgenutzt werden.
Sicherheitsrisiko	(Mittel) böswillige Formeln stellen ein Risiko dar, auch wenn die Einbettungstabelle keine vertraulichen Informationen enthält, da sie verwendet werden können, um den Computer des Betrachters zu gefährden.
Workaround	Alternativ sollten Sie alle nachfolgenden Leerzeichen nach Möglichkeit entfernen und alle vom Client bereitgestellten Daten auf alphanumerische Zeichen beschränken.
Referenzen	Verfügbare Systemeigenschaften

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

HTML in Listenansichten mit Escape-Zeichen versehen [aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie `glide.ui.escape_html_list_field`Eigenschaft zum Erzwingen von HTML-Escapes für HTML-Felder in einer Listenansicht.

Festlegen `glide.ui.escape_html_list_field`Bis **Wahr** Um zu verhindern, dass HTML in HTML-Feldern in der Listenansicht gerendert wird. Wenn die HTML-Bereinigung plattformweit (über Systemeigenschaft) oder nach Feld (über ein Schemaattribut) inaktiv bleibt, kann dies zu Angriffen im XSS-Stil führen. XSS-Angriffe können es einem Anwender mit geringen Berechtigungen ermöglichen, die Sitzung eines Anwenders mit hohen Berechtigungen zu übernehmen, oder das Verhalten von Standardwebanwendungen beeinträchtigen, einschließlich Umleitungen oder Defektionen.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.escape_html_list_field`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um die Anwendung vor Site-übergreifenden Skripting-Angriffen zu verhindern
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	3.1
Funktionale Auswirkung	Diese Korrektur erzwingt die HTML-Codierung auf der Anwenderoberfläche auf HTML-Parser-Ebene und rendert somit codierte Ergebnisse an den Anwender zurück. Dies kann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	basierend auf der Interaktion des Instanzanwenders mit den resultierenden Daten Auswirkungen auf die Funktionalität haben.
Sicherheitsrisiko	(Hoch) die Eingabevalidierung muss in der Anwendung erfolgen, um sich vor siteübergreifenden Skripting-Angriffen zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in Anwendersitzungen im Kontext des angemeldeten Browsers. Angreifer können sie verwenden, um Sitzungsinformationen und vertrauliche Daten zu stehlen.
Referenzen	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

JavaScript mit Escape-Zeichen versehen [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.html.escape_script*Eigenschaft zum Erzwingen des Escape-Vorgangs aus JavaScript (<script></script>) Tags in HTML-Feldern während Listenansichten.

Die Glide-Eigenschaft *glide.html.escape_script*Hilft bei der Bereinigung von HTML-Feldern. Wenn *glide.html.escape_script* Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, werden Eingaben für HTML-Felder (Ausgabecodierung) aus einem Back-End-Java-Kontext nicht bereinigt, indem eingebettetes JavaScript entfernt wird. JavaScript in HTML-Feldern kann zu gespeicherten und reflektierten XSS führen. Die Fähigkeit, XSS zu verwenden, kann zu einer einfachen Berechtigungseskalation zu höheren Rollen wie Administrator führen, wo mehr seitliche Bewegungen ausgeführt werden können.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.html.escape_script*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Dient zum verhindern von siteübergreifenden Skripting-Angriffen auf eine Anwendung.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	Diese Fehlerkorrektur erzwingt das JavaScript-Escape-Zeichen auf der Anwenderoberfläche und rendert codierte Ergebnisse für den Anwender. Dies kann sich basierend auf der Interaktion des Instanzanwenders mit den resultierenden Daten auf die Funktionalität auswirken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	(Hoch) die Eingabevalidierung muss in der Anwendung erfolgen, um sich vor siteübergreifenden Skripting-Angriffen zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des angemeldeten Browsers. Angreifer können sie verwenden, um Sitzungsinformationen und vertrauliche Daten zu stehlen.
Referenzen	Verfügbare Systemeigenschaften Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Jelly-Skript mit Escape-Zeichen [aktualisiert in Security Center 1,3 und 1,5]

Verwenden Sie `glide.ui.escape_all_script`Eigenschaft, um das Escape-Zeichen aller in Jelly injizierten Skripts zu erzwingen.

Mit dieser Eigenschaft werden alle in <j:jelly> ... </j:jelly> enthaltenen JS- und HTML-Zeichenfolgen mit Escape-Zeichen versehen, bevor sie in den Ausgabestrom geschrieben werden, wodurch verhindert wird, dass mehrere XSS-Probleme auftreten. Wenn `glide.ui.escape_all_script`Ist nicht auf den empfohlenen Wert „wahr“ festgelegt, dann ist das Escape-Zeichen von Skripts, die in Jelly injiziert wurden, deaktiviert. Ohne diese Minderung wird die Plattform weit geöffnet für eine Vielzahl von Skripteinschleusungsangriffen. Ein Angreifer kann beliebige Rhino-Skripts auf der Instanz ausführen.

⚠ **Warnung:** Gehen Sie bei der Verwendung dieser Tags vorsichtig vor. Wenn hier Anwendereingaben angezeigt werden, kann dies eine Sicherheitslücke öffnen.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.escape_all_script`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Wenn die Eigenschaft nicht auf festgelegt ist **Wahr** , Entwickler müssen für jedes anwenderdefinierte Jelly-Skript mehrere Schritte ausführen, um XSS-Probleme zu verhindern. Diese Schritte umfassen das Auffinden der Jelly-Variablen, die an den Ausgabestrom gesendet werden, um sie auf Webseiten zu rendern, und das Ausführen von Escape-Zeichen für jedes der folgenden Tags: $â {JS:Expression} $â {HTML:Expression}

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	ODER $â {JS,HTML:Expression}
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	7.3
Funktionale Auswirkung	Diese Fehlerkorrektur erzwingt Jelly-Escape auf Parser-Ebene. Dies kann Auswirkungen auf die Funktionalität auf die Anwenderinteraktion mit den resultierenden Daten haben.
Sicherheitsrisiko	(Hoch) die Eingabevalidierung muss für alle Anwendereingaben erfolgen, die in der Anwendung eingegeben werden. Dadurch können Einschleusungsangriffe auf die Plattform verteidigt und geschützt werden.
Workaround	Die Anwenderoberfläche kann betroffen sein, da einige der Skripts und HTML-Tags, die für das Rendern auf einer Webseite konzipiert sind, fehlerhaft erscheinen können. Diese Korrektur sendet die Ausgabe-codierte Seite zum Rendern an den Browser. Zum Beispiel anstelle von „Meine Zeichenfolge hier“ , Wird möglicherweise „ <u>Meine Zeichenfolge hier </u>Als <u>Tag wurde ordnungsgemäß mit Escape versehen. Fügen Sie in diesem Fall das Präfix NOESC dem Jelly-Ausdruck hinzu, um ein Escape-Escape-Zeichen für JS zu verhindern. Zum Beispiel: • Vor: ($[jvar_context_menus]); • Nach: ($[NOESC:jvar_context_menus]); • Vor: $[jvar_ui_Policy_scripts] • Nach: $[NOESC:jvar_ui_Policy_scripts] ⚠ **Warnung:** Gehen Sie bei der Verwendung dieser Tags vorsichtig vor. Wenn hier Anwendereingaben angezeigt werden, kann dies eine Sicherheitslücke öffnen.
Referenzen	Strenge Sicherheitseinstellungen Jelly Tags

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Escape-Skripts in Scratchpad [aktualisiert in Security Center 1,3]

Erfahren Sie, wie Scratchpad die Sicherheitslage Ihrer Instanz beeinflusst und wie Sie sie verwalten, damit keine schädlichen Skripts darauf ausgeführt werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Scratchpad ist eine einfache Möglichkeit, Informationen auf dem Server festzulegen, auf die Sie im Browser zugreifen können. Ein Administrator kann alles, was darin enthalten sein soll, skripten, einschließlich beliebiger Datensätze. Wenn diese Eigenschaft nicht auf den empfohlenen Wert von festgelegt ist **Wahr** , Dann ist es möglich, schädliche Skripts wie eine Schwachstelle für siteübergreifende Skripterstellung auszuführen.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.ui.escape_scratchpad*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn die Eigenschaft nicht auf den empfohlenen Wert festgelegt ist **Wahr** , Dann ist es möglich, schädliche Skripts wie eine Schwachstelle für siteübergreifende Skripterstellung auszuführen.
Abhängigkeiten und Voraussetzungen	Keine
Referenzen	Workflow-Verwaltung

XML-Markup mit Escape-Zeichen [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.ui.escape_text*Eigenschaft zum Erzwingen des Escape-Vorgangs von XML-Werten auf Parser-Ebene, bevor sie an den Browser des Clients übertragen werden.

Site-übergreifendes Skripting tritt auf, wenn ein Angreifer schädliches JavaScript in einen Einstiegspunkt einschleppt. Die Plattform/Anwendung kann das schädliche JavaScript nicht mit einem Escape-Zeichen versehen, bevor es zur Ausführung an den Browser des Opfers übertragen wird. Das Escape-Zeichen in diesem Kontext bedeutet Folgendes:

- **&** --> &
- **<** --> <
- **>** --> >
- **"** --> "
- **'** --> '
- **/** --> /

Beispiel: alert('XSS Attack');]]>

Escape-Zeichen: <script>Alert('XSS-Angriff');</script>

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass *glide.ui.escape_text*Eigenschaft ist in der Tabelle „sys_properties“ vorhanden und auf „wahr“ festgelegt.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.ui.escape_text*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Durch das Escape-XML wird sichergestellt, dass Browser das in nicht vertrauenswürdige Daten eingebettete schädliche JavaScript nicht analysieren und als JavaScript ausführen. • Ein böswilliger Anwender kann einen XSS-Angriff versuchen, um entweder die Sitzung anderer Anwender zu übernehmen oder den Anwender zu einer böswilligen Website umzuleiten. • Die NOW Platform enthält Code zum Sichern von Cookies, das Escape-Zeichen hängt jedoch davon ab, dass diese Eigenschaft auf festgelegt ist **Wahr** .
Empfohlener Wert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	Diese Korrektur erzwingt die XML-Codierung auf der XML-Parser-Ebene auf der Anwenderoberfläche. Rendert die codierten Ergebnisse für den Anwender, was sich basierend auf der Interaktion des Instanzanwenders mit den resultierenden Daten auf die Funktionalität auswirken kann.
Sicherheitsrisiko	(Hoch) die Eingabevalidierung muss in der Anwendung erfolgen, um sich vor siteübergreifenden Skripting-Angriffen zu schützen. Diese Angriffe ermöglichen die Ausführung fremder Skripts in einer Anwendersitzung im Kontext des angemeldeten Browsers. Angreifer können sie verwenden, um Sitzungsinformationen und vertrauliche Daten zu stehlen.
Workaround	Nachdem Sie diese Eigenschaft auf festgelegt haben **Wahr** , Das Rendern der HTML-Tags in der Katalogelementbeschreibung oder im Hilfetext der Katalogelementvariablen wird beendet. Möglicherweise können Sie für einige Felder keine HTML-Formatierung verwenden. Wenn jedoch *glide.ui.escape_text*Eigenschaft ist aktiviert, allen JEXL-Ausdrücken wird ein Ausgabencoder vorangestellt: ${JS:Expression}

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	${HTML:Expression} oder ${JS,HTML:Expression}

XML-Antwort mit Escape-Zeichen versehen

Verwalten Sie, wie XML-Escapes in Ihrer Instanz behandelt werden.

Verwenden Sie diese Eigenschaft, um zu verwalten, ob XML-Antworten mit Escape-Zeichen versehen werden. Wenn die Eigenschaft auf den empfohlenen Wert von festgelegt ist **Falsch** , Dann werden XML-Antworten nicht mit Escape-Zeichen versehen, was zu einem XML-Injection-Angriff führen kann. Die Injektion von unbeabsichtigtem XML-Inhalt in eine XML-Nachricht kann die beabsichtigte Logik einer Anwendung ändern.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.soaprequest.unescape_xml_response*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	falsch
Standardwert	falsch
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,4 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Diese Eigenschaft wird auf festgelegt **Falsch** Deaktiviert das XML-Escape-Zeichen, was zu einem XML-Injection-Angriff führen kann.
Abhängigkeiten und Voraussetzungen	Keine

HTML-Bereinigung aktivieren [aktualisiert in Security Center 1,3]

Verwenden Sie *glide.html.sanitize_all_fields*Eigenschaft zum Aktivieren der HTMLSanitizer-Skripteinbindung, die HTML-Eingaben basierend auf Attributen „Ausschlussliste“ und „Einschlussliste“ bereinigt, die in einem Skript konfiguriert sind.

Die für Wörterbuch/Felder verfügbaren Feldtypen umfassen HTML und übersetzte HTML. Mit diesen HTML-Eingabefeldern können Anwender HTML-formatierte Eingaben schreiben, z. B.:

<h1>Testen </h1>, Mit den einfachsten HTML-Tags wie <img>, <a href ⋯>, Und <iframe>.

Es kann eine Tür für einen böswilligen Angreifer öffnen, um schädliche Vektoren mit HTML-Tags einzuschleusen, z. B.:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">],[a href="" onclick=Alert(/xss/)] .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.html.sanitize_all_fields*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Verhindert die Anwendung vor Site-Cross-Scripting und HTML-Injection-Angriffen
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	Diese Korrektur erzwingt den HTML-Ausgabecodierungsmechanismus, bevor die Anwenderdaten an den Anwender zurückgerendert werden. Wenn der Kunde eine Anpassung hat, die das Rendern des HTML-Attributs oder der Inhaltsdaten beinhaltet, hat dies Auswirkungen auf die Funktionalität.
Sicherheitsrisiko	(Hoch) Anwendereingaben sollten sicher behandelt werden, wenn die Daten in der Anwendung gespeichert und verarbeitet werden.Dies reduziert clientseitige Cross-Site-Skripting-Angriffe, indem die Daten mit der Ausgabe codiert werden.
Workaround	Diese Eigenschaft bereinigt alle HTML-Felder im System. Wenn Sie die HTML-Bereinigung für einzelne Felder aktivieren müssen, finden Sie unter Aktivieren Sie die Bereinigung einzelner Felder . Sie können auch die Aufnahme- oder Ausschlussliste konfigurieren, um HTML-Tags und Attribute gemäß Ihrer Unternehmensrichtlinie zu bereinigen.
Referenzen	HTML-Bereinigung wird aktiviert HTML-Bereinigung

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Zulässige Java-Pakete beschränken [aktualisiert in Security Center 1,3]

Die Konfiguration dieser Eigenschaften schützt vor gefährlichen APIs, die der Skripting-Engine ausgesetzt werden.

Konfigurieren Sie die Systemtabellen, und installieren Sie das empfohlene Plugin entsprechend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn *sys_whitelist_member*Und *sys_whitelist_package*Tabelle sind keine leeren Werte, dann können gefährliche APIs für die Skripting-Engine verfügbar gemacht werden. Einträge entsprechen dem Java-Namespace, der nicht von genehmigt wurde ServiceNow Sicherheitsteams.

Installieren Sie das Tool zum Entfernen von Paketaufrufen. Details siehe Paketaufruf-Entfernungstool.

Kontakt Kundenservice und Support Zum Bearbeiten dieser Tabellen.

Weitere Informationen

Attribut	Beschreibung
Tabelle, Plugin-Name	Tabellen: • *sys_whitelist_member* • *sys_whitelist_package* Plugin: Com.Glide.script.Packages_call_removal
Konfigurationstyp	Tabellarische Konfiguration, Plugins
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Schützen Sie vor gefährlichen APIs, die der Skripting-Engine ausgesetzt sind.
Empfohlener Wert	Leer
Standardwert	Keine. Dies ist eine Tabellenkonfiguration und keine Glide-Eigenschaft, daher gibt es keinen Standardwert.
Konfigurationstyp	Tabellenliste, Plugin
Sicherheitsrisiko	(Hoch) gefährliche APIs können der Skripting-Engine ausgesetzt sein. Diese unterstützten APIs führen wahrscheinlich zu Instabilität und Unsicherheit innerhalb der Instanz.
Sicherheitsrisikobewertung	8.2

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Paketaufruf-Entfernungstool

Aktivieren und führen Sie das Paketaufruf-Entfernungstool aus (*com.glide.script.packages_call_removal*) Plugin, und überlegen Sie dann, ob jeder der vorgeschlagenen Änderungen abgeschlossen oder abgelehnt werden soll.

Das Paketaufruf-Entfernungstool ist ein Plugin, das:

- Scannt Skripts für Paketaufrufe an ServiceNow AI Platform Java-Klassen.
- Schlägt Änderungen vor, um sie durch bevorzugte GlideScriptable-Namen zu ersetzen.
- Erleichtert die Skriptänderungen.

Hinweis: Wenn dieser Datensatz ein Basissystemdatensatz ist, wird das Element mit der Empfehlung aus dem Tool als Customer_Update markiert. Es kann jedoch weiterhin nützlich sein, dieses Tool zu verwenden, da es Pakete,xxx-Aufrufe kennzeichnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Tool zum Entfernen von Paketaufrufen meldet möglicherweise einige Paketaufrufe, die in verwendet werden `sa_Mapping_ext_commands` Und `sa_custom_Operation` . Diese Paketaufrufe gehören zum MID-Server. Da keine Klassen vorhanden sind, wird der Code auf dem MID-Server ausgeführt. Wenn Sie einen der folgenden aufgeführten Paketaufrufe im Abschnitt „Fehler“ finden, markieren Sie ihn als abgelehnt (ignoriert). Das Tool meldet diesen Paketaufruf nicht erneut.

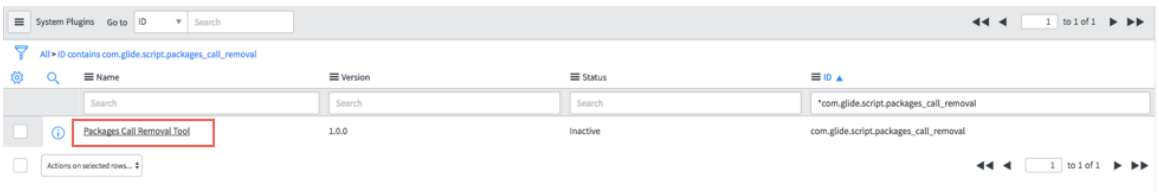
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
- `Packages.com.snc.sw.commands.HttpCallHandler;`
- `Packages.com.snc.sw.dto.ProviderType.SSH`

Weitere Informationen

Attribut	Beschreibung
Plugin-Name	Com.Glide.script.Packages_call_removal
Konfigurationstyp	Systemdefinition > Plugins
Zweck	Dient zum Entfernen/Ersetzen nicht autorisierter Paket-/Mitgliederaufrufe durch für Glide zulässige Namen (GlideScriptable), die nur autorisierten Zugriff auf Daten zulassen.
Empfohlener Wert	Aktiv
Funktionale Auswirkung	Diese Korrektur würde die Paketaufrufe durch ersetzen `GlideScriptfähig` APIs, und können sich auf die Anpassungen auswirken, die Paketaufrufe umfassen. Das Tool ersetzt Paketaufrufe nicht automatisch. Stattdessen werden Vorschläge bereitgestellt, die in der Tabelle „Packages_call_item“ gespeichert werden. Ihr Administrator kann dann entscheiden, ob der vorgeschlagene Change akzeptiert oder abgelehnt werden soll.
Sicherheitsrisiko	(Mittel) clientseitige API-Aufrufe, die zu Datenabruf oder Objektzugriff auf dem Server führen, gelten aus sicherheitstechnischer Sicht als gefährlich. Sie müssen auf Autorisierung und Einschränkung für den Zugriff auf vertrauliche Objekte validiert werden.

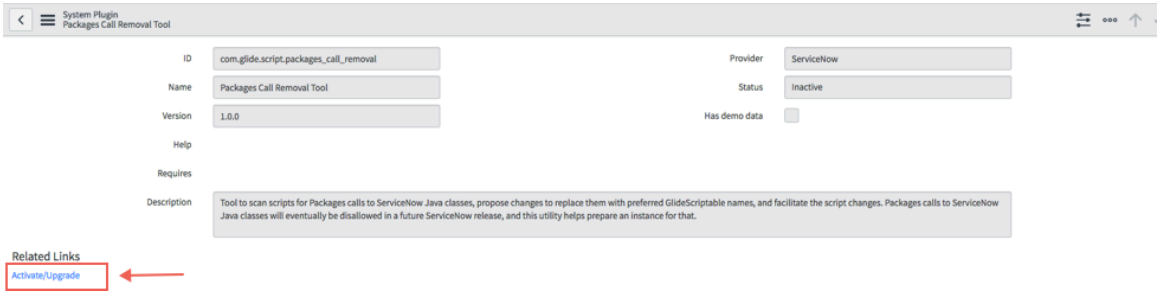
Schritte zum Konfigurieren

1. Navigieren zu **Systemdefinition** > **Plugins**

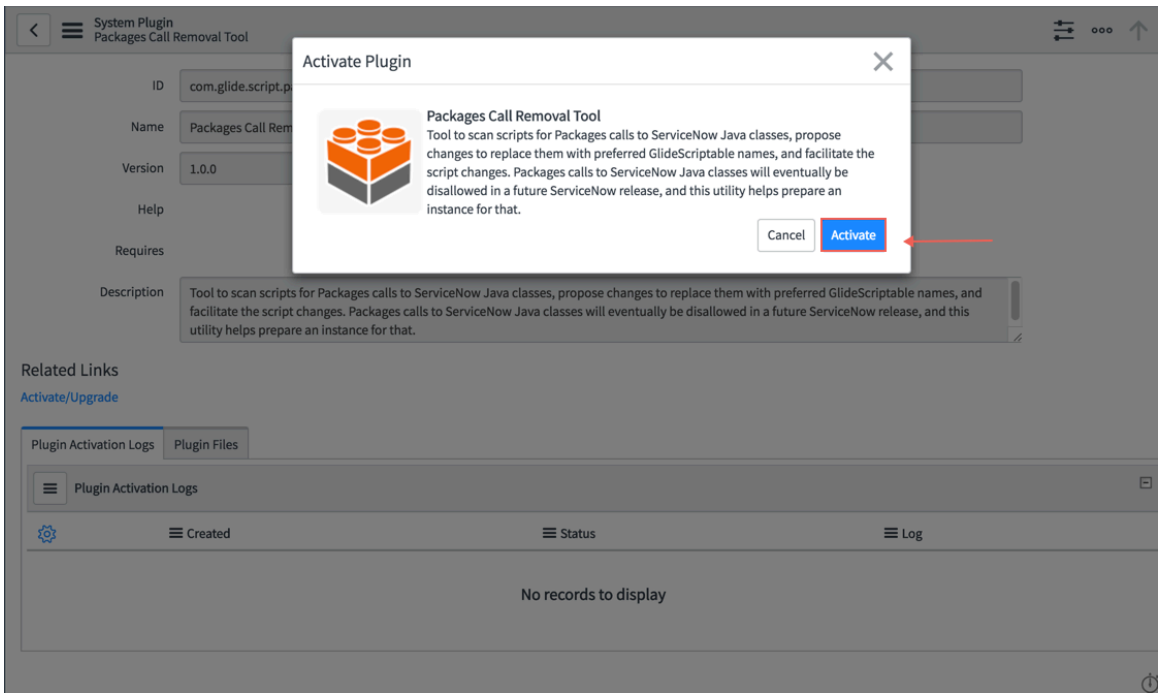


2. Suchen Sie nach der Plugin-ID = `com.glide.script.packages_call_removal`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie Auf **Aktivieren/Upgrade Durchführen** Zum Aktivieren des Plugins.



4. Führen Sie die in den Abschnitten „Schritte zum Konfigurieren“ in beschriebenen Aktionen aus, um die Aufrufe von Inklusionslisten-Paketen und Inklusionslisten-Mitgliedsmitgliedern zu überprüfen Zulässige Java-Pakete beschränken [aktualisiert in Security Center 1,3].

Festlegung des anfänglichen eindeutigen LDAP-Namens aufheben [in Security Center 1,3 aktualisiert und 2,0 entfernt]

Verwenden Sie diese Eigenschaft, um den eindeutigen Namen eines LDAP-Server-Datensatzes zu verwalten.

Diese Eigenschaft steuert den eindeutigen Namen eines LDAP-Server-Datensatzes, der beim Ausführen eines sofort einsatzbereiten Korrekturskripts (OOB) eingefügt wird. Wenn er auf den empfohlenen Wert „“ oder leer festgelegt ist, können LDAP-Serverdaten von einem Anwender mit niedrigeren Berechtigungen aufgezählt werden.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ldap.initial.dn`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Datentyp	Zeichenfolge
Empfohlener Wert	leer
Standardwert	leer
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 2,7 • CVSS-Punktzahl: Niedrig • Sicherheitsrisikodetails: Wenn Sie den Eigenschaftswert auf „“ oder leer festlegen, kann dies dazu führen, dass LDAP-Serverdaten für einen Anwender mit niedrigeren Berechtigungen zugänglich sind.
Abhängigkeiten und Voraussetzungen	Keine

Strikte Sicherheit von Sitzungscookies erzwingen [aktualisiert im Sicherheitscenter 1,3]

Verwenden Sie `glide.ui.secure_cookies`Eigenschaft, die ordnungsgemäß formatierte Cookies erfordert

Wenn Sie die Eigenschaft auf „wahr“ festlegen, lehnt Ihre Instanz eine Sitzung ab, wenn das zugehörige Cookie nicht das erwartete Format aufweist.

⚠ **Warnung:** Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.ui.secure_cookies`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Um eine sicherere Sitzungsauthentifizierung zu erreichen.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	8.8
Funktionale Auswirkung	Wenn die Eigenschaft auf „wahr“ festgelegt ist, werden falsch formatierte Cookies abgelehnt. Wenn ein solches Cookie abgelehnt wird, muss sich der Anwender erneut anmelden.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwellenwert für Entitätserweiterung für skriptfähige GlideXMLUtil minimieren [aktualisiert in Security Center 1,3, 1,5 und 2,0]

Verwenden Sie `glide.xmlutil.max_entity_expansion`Eigenschaft zum Ändern der maximalen Entitätserweiterungsgrenze auf eine kleinere Zahl.

Diese Eigenschaft steuert den maximalen Umfang der Entitätserweiterung in einem XML-Parser. Wenn `glide.xmlutil.max_entity_expansion`lst nicht auf den empfohlenen Wert von 3000 oder weniger festgelegt, kann das skriptfähige GlideXMLUtil-Analysegerät angreifbar für Denial-of-Service-Angriffe sein.

Stellen Sie die Eigenschaft sicher `glide.xmlutil.max_entity_expansion`lst auf maximal 3000 festgelegt. Wenn sich die Instanz in Washington oder höher befindet, ist der implizite Standardwert 3000, wenn der Datensatz „sys_properties“ nicht vorhanden ist. Wenn sich die Instanz nicht in Washington oder höher befindet, empfiehlt es sich, dass der Instanzadministrator einen sys_properties-Datensatz mit dem Namen erstellt `glide.xmlutil.max_entity_expansion`Und der Wert 3000.

Hinweis: 500 ist das vom auferlegte Standardminimum ServiceNow AI Platform, Der als sicherer Schwellenwert betrachtet wird.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.xmlutil.max_entity_expansion`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen XML-Entitätserweiterungen/Milliarden-Lachen-Angriffe zu schützen.
Empfohlener Wert	3000
Standardwert	100000
Sicherheitsrisikobewertung	5.3
Funktionale Auswirkung	Wenn die Anpassung eine große Entitätserweiterung verwendet, dann die ServiceNow AI Platform Blockiert möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	(Mittel) ein Angreifer kann diese Schwachstelle verwenden, um Daten exponentiell zu erweitern und schnell alle Systemressourcen zu verbrauchen.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Erstellung einer leeren ACL verhindern [Neu in Security Center 2,0]

Legen Sie fest `glide.security.empty_acl.popup_window.enabled` Eigenschaft für den sicheren Wert „wahr“, um Versuche zum Erstellen, Aktualisieren oder Speichern einer ungültigen ACL zu blockieren. Diese Einstellung stellt auch ein clientseitiges Modell zur Konfiguration einer Rolle oder eines Sicherheitsattributs für die ACL bereit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die *glide.security.empty_acl.popup_window.enabled*Die Eigenschaft bestimmt, ob Anwender, die formularbasierte Änderungen an Zugriffssteuerungslisten (ACLs) vornehmen, insbesondere sys_Security_acl, eine ungültige ACL erstellen, aktualisieren oder speichern können, die eine ungültige Datenbedingung, ein ungültiges Skript, ein Sicherheitsattribut oder eine Rollenliste aufweist . Andernfalls bleibt sie nicht konfiguriert (eine leere ACL). Ab XanaduRelease, jede leere ACL verweigert den Zugriff. In ServiceNowVersionen vor Xanadu, Eine leere ACL ermöglicht bedingungslosen Zugriff.

Wenn *glide.security.empty_acl.popup_window.enabled*Die Eigenschaft ist auf den sicheren Wert „wahr“ festgelegt, blockiert Versuche, eine ungültige oder leere ACL zu erstellen, zu aktualisieren oder zu speichern, und stellt ein clientseitiges Modell zur Konfiguration einer Rolle oder eines Sicherheitsattributs für die ACL bereit. Wenn die Eigenschaft auf den unsicheren Wert „falsch“ festgelegt ist, sind solche Versuche zulässig, und es wird kein clientseitiges Modell angezeigt.

Hinweis: Bei dieser Eigenschaft wird zwischen Groß- und Kleinschreibung unterschieden. Beispielsweise wird der Wert „wahr“ (Großbuchstabe „T“) als „falsch“ ausgewertet. Darüber hinaus funktioniert diese Eigenschaft nur, wenn das Plugin „High Security“ (com.Glide.High_Security) installiert und aktiv ist.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*glide.security.empty_acl.popup_window.enabled*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,5 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft auf „wahr“ festgelegt ist, verhindert das Popup für leere ACL-Warnungen den Anwender, eine leere ACL auf der Clientseite zu übermitteln. Wenn sie auf „falsch“ festgelegt ist, wird das Popup nicht mehr angezeigt.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Mit dieser Eigenschaft kann der Anwender das leere ACL-Warnungs-Popup aktivieren und deaktivieren.
Referenzen	Erstellung einer leeren ACL verhindern [Neu in Security Center 2,0]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingeschränkte herunterladbare MIME-Typen definieren [aktualisiert in Security Center 1,3, 1,5 und 2,0]

Verwenden Sie `glide.ui.attachment.force_download_all_mime_types`Eigenschaft zum Herunterladen von MIME-Typen und zum nicht Inline-Rendern im Browser.

Wenn `glide.ui.attachment.download_mime_types`Enthält gefährliche MIME-Typen wie Text/HTML, image/svg, image/svg, image/svg+xml,Application/xml, dann können gefährliche Dateien im Browser inline gerendert werden, was zu Cross Site Scripting-Angriffen (XSS) führen kann. Diese Eigenschaft ist die Liste der kommagetrennten MIME-Typen für Anhänge, die im Browser nicht inline gerendert werden. Beispielsweise erzwingt das Einbeziehen von Text/HTML-Dateien, dass HTML-Dateien als Anhänge auf den Client heruntergeladen werden, anstatt sie inline im Browser anzuzeigen. Durch die ordnungsgemäße Pflege dieser Liste werden Site-übergreifende Skripting-Angriffe verhindert.

Wenn `glide.ui.attachment.download_mime_types`Die Systemeigenschaft enthält keine gefährlichen MIME-Typen wie „Text/html, image/svg,image/svg+xml,Application/xml“, dann können gefährliche Dateien im Browser inline gerendert werden. Dies kann zu Angriffen mit Cross Site Scripting (XSS) führen. Diese Prüfung ist nur relevant, wenn `glide.ui.attachment.force_download_all_mime_types`Ist auf festgelegt **Falsch** .

Diese Eigenschaft ist eine Liste von kommagetrennten Anhang-MIME-Typen, die im Browser nicht inline gerendert werden. Beispiel: Einschließlich Text/HTML Erzwingt, dass HTML-Dateien als Anhänge auf den Client heruntergeladen und nicht inline im Browser angezeigt werden.

Wenn `glide.ui.attachment.force_download_all_mime_types`Ist auf festgelegt **Falsch** , Verifizieren Sie, dass `glide.ui.attachment.download_mime_types`Die Systemeigenschaft enthält die gefährlichen MIME-Typen Text/html,image/svg,image/svg+xml,Application/xml .

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.ui.attachment.force_download_all_mime_types`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Zeichenfolge (kommagetrennte Liste von MIME-Typen)
Empfohlener Wert	Text/html,image/svg,image/svg+xml,Application/xml
Standardwert	Text/html,image/svg,image/svg+xml,Application/xml
Fallback-Wert	Text/html,image/svg,image/svg+xml,Application/xml
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 6,3 • CVSS-Punktzahl: Mittel • Sicherheitsrisiko: Wenn Sie diese Liste ordnungsgemäß verwalten, können Sie Cross-Site-Skripting-Angriffe verhindern.
Abhängigkeiten und Voraussetzungen	Diese Prüfung ist nur relevant, wenn `glide.ui.attachment.force_download_all_mime_types`Ist

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	auf festgelegt **Falsch** Oder ist in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden.

Hochgeladene MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]

Verwenden Sie *glide.security.file.mime_type.validation*Eigenschaft zum Aktivieren der MIME-Typprüfung auf Uploads. Sie können aktivieren (die Eigenschaft auf festlegen **Wahr**) Oder deaktivieren (auf festlegen **Falsch**) MIME-Typvalidierung für Dateianhänge.

Voraussetzungen

Legen Sie vor dem Festlegen dieser Eigenschaft fest *glide.attachment.extensions*Eigenschaft. Nur die in angegebenen Erweiterungen *glide.attachment.extensions*Werden während des Uploads auf den MIME-Typ überprüft. Weitere Informationen finden Sie unter Dateierweiterungen beschränken .

Stellen Sie die Glide-Eigenschaft sicher *glide.ui.jelly.js_interpolation.protect_nested_expressions*Ist vorhanden und auf den Wert „wahr“ festgelegt. Wenn die Eigenschaft nicht in der Tabelle „sys_properties“ angezeigt wird, fügen Sie einen neuen Datensatz hinzu.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.security.file.mime_type.validation*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Dient zum Erzwingen der Überprüfung des MIME-Typs/ magischen Bytes während des Datei-Uploads.
Empfohlener Wert	wahr
Standardwert	wahr
Sicherheitsrisikobewertung	5.4
Funktionale Auswirkung	Diese Korrektur aktiviert die MIME-Typverifizierung für die Anhänge der Anwendung. Keine Auswirkung auf die Funktionalität, es sei denn, es besteht eine böswillige Absicht beim Hochladen der Dateien, da diese Validierung lediglich auf Fehlsynchronisierung zwischen dem MIME-Typ und den Daten überprüft.
Sicherheitsrisiko	(Mittel) um Schwachstellen wie Dateieinschluss und Uploads schädlicher Dateien zu reduzieren, sollte die MIME-Typverifizierung aktiviert sein.
Referenzen	Verwalten von Anhängen

Siehe Härtungseinstellungen Für Details zum Konfigurieren von Eigenschaften für die Härtung.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0]

Stellen Sie sicher, dass *glide.xml.entity.whitelist*Und *glide.xml.entity.whitelist.enabled*Eigenschaften sind auf die empfohlenen Werte festgelegt, um Angriffe auf externe XML-Entitäten (XXE) zu verhindern.

Schützen Sie sich vor XXE-Angriffen, indem Sie eine Allow-Liste verwenden, um zu verhindern, dass Angreifer beliebige HTTP-Anforderungen aufnehmen, die der Server ausführen kann. Dies kann zu zusätzlichen Angriffen führen, die die Vertrauensbeziehung des Servers mit anderen Entitäten verwenden.

Hinzufügen `http://java.sun.com/j2ee/dtds/` Auf den Wert von **Glide.xml.Entität.Whitelist** Systemeigenschaft, legen Sie dann fest **Glide.xml.Entität.Whitelist.aktiviert** Systemeigenschaft zu **Wahr** .

Andere Werte als `http://java.sun.com/j2ee/dtds/` Kann in der enthalten sein **Glide.xml.Entität.Whitelist** Eigenschaft, sind jedoch für den sofort einsatzbereiten Plattformstatus unnötig. Überprüfen Sie alle zusätzlichen Werte, um festzustellen, ob sie sicher sind.

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*glide.xml.entity.whitelist,glide.xml.entity.whitelist.ena*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen XXE-Angriffe zu schützen.
Empfohlener Wert	`http://java.sun.com/j2ee/dtds/`
Standardwert	`http://java.sun.com/j2ee/dtds/`
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	Wenn die Anpassung eine externe Entität verwendet, wird die Aufnahme nicht in aufgeführt *glide.xml.entity.whitelist*Eigenschaft, kann die NOW Platform die weitere Verarbeitung blockieren.
Sicherheitsrisiko	(Kritisch) ein Angreifer kann die DTD verwenden, um beliebige HTTP-Anforderungen einzubeziehen, die der Server möglicherweise ausführen kann. Dies kann zu anderen Angriffen führen, die die Vertrauensbeziehung des Servers mit anderen Entitäten verwenden.

Validierung der XMLdoc2-Entität mit zulässiger Entitätserweiterung anfordern [aktualisiert in Security Center 1,3]

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie *glide.xmlutil.max_entity_expansion*Eigenschaft zum vollständigen Deaktivieren der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterung externer Entitäten. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

Wenn die Glide-Eigenschaft ist `glide.stax.whitelist_enabled`lst in der Tabelle „Systemeigenschaften“ [sys_properties] nicht vorhanden oder nicht auf den empfohlenen Wert festgelegt **Wahr** , Dann sind alle externen Entitäten zulässig, wenn die Glide-Eigenschaft verwendet wird `glide.stax.allow_entity_resolution`lst auf den Wert von festgelegt **Wahr** .

Wenn Anpassungen keine Entitätserweiterung erfordern, verwenden Sie `glide.stax.allow_entity_resolution`Eigenschaft zum vollständigen Deaktivieren der Erweiterung externer Entitäten. Die XML-Datei schließt die Analyse ab, enthält jedoch keine internen oder externen Entitäten.

- Wenn Sie festgelegt haben `glide.stax.allow_entity_resolution`Bis **Wahr** , Alle externen Entitäten versuchen, Betreffentitäten aufzulösen oder zu erweitern, abhängig von der Einstellung von `glide.stax.whitelist_enabled`Eigenschaft.
- Wenn Sie festgelegt haben `glide.stax.allow_entity_resolution`Bis **Falsch** , Alle Entitätsauflösungen und -Erweiterungen sind blockiert. Weitere Informationen zu dieser Eigenschaft finden Sie unter Deaktivieren Sie die Entitätserweiterung im XMLDocument2-Streaming-Parser [Aktualisiert in Security Center 1,5].

Wenn **Glide.stax.Whitelist_enabled** lst auf festgelegt **Wahr** , Definieren Sie eine Liste von durch Kommas getrennten FQDN in **Glide.xml.Entität.Whitelist** Eigenschaft, die die einzigen URLs sind, die mit der Verarbeitungseigenschaft der XML-Entität erreicht werden können. Weitere Informationen finden Sie unter Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0]. Angreifer können diese Schwachstelle verwenden, um Daten bei einem XXE-Angriff (External Entities Expansion) exponentiell zu erweitern und schnell alle Systemressourcen zu verbrauchen.

Voraussetzungen

Bevor Sie diese Eigenschaft festlegen:

- Legen Sie fest `glide.xml.entity.whitelist.enabled`Und `glide.stax.whitelist_enabled`Eigenschaften bis **Wahr** . Weitere Informationen finden Sie unter Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0].
- Definieren Sie eine Liste von durch Kommas getrennten FQDN in `glide.xml.entity.whitelist`Eigenschaft, die die einzigen URLs ist, die mit der Verarbeitungseigenschaft der XML-Entität erreicht werden können. Weitere Informationen finden Sie unter Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0].

Warnung: Dies ist eine Safe-Harbor-Eigenschaft, d. h. der Wert kann nicht geändert werden, nachdem er geändert wurde. Sie kann nicht rückgängig gemacht werden.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	`glide.stax.whitelist_enabled`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Kategorie	Validierung, Bereinigung und Codierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Zweck	Diese Korrektursteuerung muss aktiviert sein, um sich gegen einen XML-Entitätserweiterungs-/Milliarden-Lachen-Angriff zu schützen.
Empfohlener Wert	wahr
Standardwert	falsch
Sicherheitsrisikobewertung	9.8
Funktionale Auswirkung	Wenn für die Anpassung eine Entitätserweiterung verwendet wird, dann die ServiceNow AI Platform Blockiert möglicherweise die weitere Verarbeitung.
Sicherheitsrisiko	Ein Angreifer kann diese Schwachstelle verwenden, um Daten bei einem XXE-Angriff (External Entities Expansion) exponentiell zu erweitern und schnell alle Systemressourcen zu verbrauchen.
Workaround	Wenn die Anpassung eine Entitätserweiterung erfordert, legen Sie diese Eigenschaft auf „wahr“ fest, und befolgen Sie die in dokumentierten Schritte Externe XML-Entitäten beschränken [aktualisiert in Security Center 1,3 und 2,0].

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Weitere Informationen zu OWASP-Ressourcen finden Sie unter OWASP .

Alle übersetzten HTML-Felder bereinigen [Neu in Security Center 2,0]

Erfahren Sie, wie Sie konfigurieren `glide.translated_html.sanitize_all_fields`Eigenschaft für den sicheren Wert, um sicherzustellen, dass alle vorhanden sind `translated_html`Elemente werden mit einer HTML-Bereinigung bereinigt.

Wenn `glide.translated_html.sanitize_all_fields`Eigenschaft ist auf „wahr“ festgelegt, alle `translated_html`Elemente werden mit einer HTML-Bereinigung bereinigt. Wenn die Eigenschaft auf „falsch“ festgelegt ist, werden nur Elemente mit dem Wörterbuchattribut verwendet `html_sanitize`Auf „wahr“ festgelegt, wird bereinigt. Diese Bereinigung trägt dazu bei, zu verhindern, dass Angreifer schädliche Inhalte einbetten, die zu Angriffen mit Cross-Site Scripting (XSS) führen könnten.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	`glide.translated_html.sanitize_all_fields`
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Validierung, Bereinigung und Codierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Sicherheitsrisiko	• Schweregradpunktzahl: 4,6 • CVSS-Punktzahl: Mittel • Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den sicheren Wert „wahr“ konfiguriert wird, werden nicht alle HTML-Elemente bereinigt, was die Wahrscheinlichkeit erhöht, dass ein schlechter Akteur schädliche Inhalte in ein Feld einbettet.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Ermöglicht Kunden den Zugriff auf Tabelleninformationen, wenn das Widget auf öffentlich festgelegt und im Wert der Eigenschaft enthalten ist.

HTML in den Beschreibungsfeldern des Impact Workspace-Moduls bereinigen [Neu in Security Center 7,0]

Bereinigen Sie HTML in den Beschreibungsfeldern, indem Sie HTML-Tags entfernen, die Quellen von HTML-Injection-Angriffen mit sind *sn_impact_common.blacklist_tags_HTML_injection*Eigenschaft.

Das Modul „Impact Workspace“ ermöglicht HTML in den folgenden Beschreibungsfeldern:

- Das Feld Customer_Notes der Tabellen sn_Impact_common_Capabilities_Map und sn_Impact_common_par_Version_Phase_App_Mapping.
- Das Feld „Manual_description“ der Tabelle „sn_Impact_Common_Manual_Capability_description“.

Wenn diese Systemeigenschaft eine kommagetrennte Liste von HTML-Tags (z. B. Skripts) enthält, werden diese Tags und ihr Inhalt aus den HTML-Teilen der aufgelisteten Felder entfernt. Das Entfernen dieser Tags hilft, HTML in den Beschreibungsfeldern zu bereinigen, indem HTML-Tags entfernt werden, die Quellen von HTML-Injection-Angriffen sind. Wenn diese Eigenschaft nicht in der Tabelle „Systemeigenschaften“ [sys_properties] festgelegt ist, wird als Wert standardmäßig eine Standardliste von abgelehnten HTML-Tags verwendet. Wenn die Eigenschaft leer ist, sind alle HTML-Tags zulässig.

Verwenden Sie *sn_impact_common.blacklist_tags_HTML_injection*Geben Sie eine kommagetrennte Liste von HTML-Tags an, die aus den Beschreibungsfeldern für das Modul „Impact Workspace“ entfernt werden. Diese Entfernung hilft, HTML-Einschleusungsangriffe zu verhindern. Diese Liste sollte mindestens den Inhalt der Standardliste enthalten. Wenn die Eigenschaft nicht in der Tabelle „Systemeigenschaften“ [sys_properties] festgelegt ist, wird standardmäßig die Liste verwendet `Skript,iFrame,object,einbetten,Form,onerror,onload,style,img,Video,Audio,Quelle,Schaltfläche` .

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	*sn_impact_common.blacklist_tags_HTML_injection*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Kategorie	Validierung, Bereinigung und Codierung
Zweck	Bereinigen Sie HTML in den Beschreibungsfeldern, indem Sie HTML-Tags entfernen, die Quellen von HTML-Injection-Angriffen sind.
Empfohlener Wert	Mindestens der Standardwert von Skript,iFrame,object,einbetten,Form,onerror,onload,style,img,Video,Audio,(
Standardwert	Skript,iFrame,object,einbetten,Form,onerror,onload,style,img,Video,Audio,(
Sicherheitsrisikobewertung	4.4
Funktionale Auswirkung	Wenn ein HTML-Tag der Standardliste hinzugefügt wird, kann dies die erforderliche HTML-Funktionalität der Beschreibungsfelder einschränken. Die genaue Auswirkung hängt von der Kundeninstanz ab.
Sicherheitsrisiko	(Mittel)
Referenzen	Strenge Sicherheitseinstellungen

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Sicherheitsrichtlinie für sichere Inhalte für svg-Dateien festlegen [Neu in Security Center 1,3]

Die *com.glide.csp.self_script_src_svg*Eigenschaft fügt hinzu **Skript-SRC keine** anweisung zum HTTP-Content-Security-Policy-Header, wenn über die Dateierweiterung Translation Memory Index (IIX) auf scalable Vector Graphics (SVGs) zugegriffen wird.

Die *com.glide.csp.self_script_src_svg*Die Eigenschaft verhindert, dass schädliche Dateianhänge, die Site Cross Scripting (XSS)-Angriffe speichern, in einer Instanz ausgeführt werden. Ohne diese Richtlinie kann ein schlechter Akteur dazu führen, dass ein Anwender beliebigen JavaScript-Code in seinem Webbrowser ausführt, was zu Sicherheitsschwachstellen wie Datenexfilterung und Sitzungsübernahme führen kann.

Weitere Informationen

Attribut	Beschreibung
Konfigurationsname	*com.glide.csp.self_script_src_svg*
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Datentyp	Boolean
Empfohlener Wert	wahr
Standardwert	wahr
Kategorie	Validierung, Bereinigung und Codierung
Sicherheitsrisiko	• Schweregradpunktzahl: 7,1 • CVSS-Punktzahl: Hoch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
	• Sicherheitsrisikodetails: Wenn diese Eigenschaft nicht auf den empfohlenen Wert „wahr“ festgelegt wird, kann ein Anwender beliebigen JavaScript-Code von einem ungültigen Akteur ausführen.
Abhängigkeiten und Voraussetzungen	Keine
Funktionale Auswirkung	Diese Eigenschaft verhindert, dass SVG-Dateien (scalable vector graphics, skalierbare Vektorgrafiken) auf externe Skripts zugreifen.

Protokollexportservice (LES)

Protokollexportservice Mit (LES) können Sie Ihre Instanzsystem- und Anwendungsprotokolle nahtlos in Ihre Analysetools für Unternehmenssicherheit exportieren.

Erste Schritte

Untersuchen



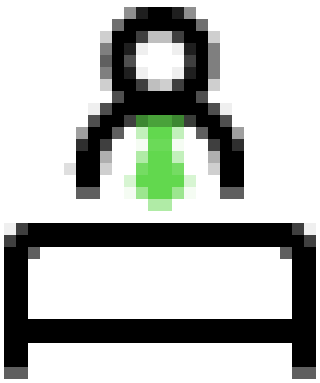
Weitere Informationen zu Log Export Service (LES)

Konfigurieren



Konfigurieren Sie LES für Kafka- und MID-Server-Verbraucher

Verwalten



Verwalten VON LES

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden	Referenz
 Überprüfen Sie Protokollberichte mit LES	 Erfahren Sie mehr über verschiedene Informationen zur App

Problembehandlung und Hilfe

- Stellen oder beantworten Sie Fragen zu Protokollexportservice (LES) in ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Informationen zum Klonen von Empfehlungen für LES, einschließlich Tabellen zum Beibehalten und Ausschließen, finden Sie unter Tabellen, die beibehalten werden sollen, um die LES-Konfiguration beizubehalten .

Erkunden Protokollexportservice(LES)

Der LES-Service bietet eine hoch skalierbare und nahezu Echtzeit-Integration mit Ihren Analysetools, die einfach einzurichten und zu warten ist. Wenn Sie neu bei LES sind, lesen Sie diesen Übersichtsabschnitt, um zu erfahren, was das Tool leisten kann.

Überprüfen Sie Ihre Berechtigungen, um festzustellen, ob Sie Zugriff auf haben Protokollexportservice.

Protokollexportservice – Übersicht

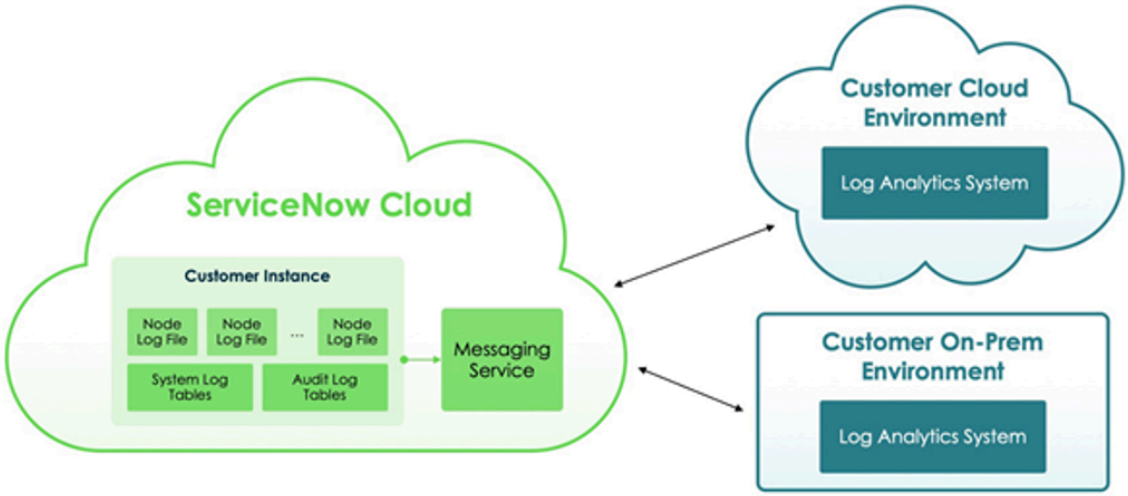
Mit dem Integrationstool können Sie Ihre analytischen Lösungen nutzen, um Folgendes auszuführen:

- Erkennen ServiceNow Sicherheitsbedrohungen und analysieren Sie Security Incidents
- Problembehandlung und Optimierung ServiceNow App-Leistung
- Überwachen und optimieren ServiceNow Anwender-Experience

LES nutzt einen ServiceNow AI Platform Fähigkeit genannt Hermes Messaging-Service, Ein Multi-Mandant-, Multi-Cluster-, Datenübertragungs- und Warteschlangenservice, der auf basiert Apache Kafka Damit kann Ihre Instanz große Mengen von Kafka-Ereignissen erstellen und verbrauchen. Apache Kafka Ist eine Open Source-Datenstreaming-Plattform, die einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zentralen Integrationspunkt für den Datenaustausch zwischen Geschäftssystemen in Ihrer Organisation bietet.



LES leitet eine Kopie der Protokollereignisse weiter, wenn sie an generiert werden Hermes Messaging-Service.

Die Hermes Messaging-Service Ist ein Multi-Mandanten-, Multi-Cluster-, Datenübertragungs- und Warteschlangenservice, der auf basiert Apache Kafka Damit kann Ihre Instanz große Mengen von Kafka-Ereignissen erstellen und verbrauchen. Die Hermes Messaging-Service Ist ein ServiceNow AI Platform Fähigkeit, die als Teil von verfügbar ist Stream Connect for Apache Kafka, Protokollexportservice(LES), und Instanzübergreifende Datenreplikation(IDR).

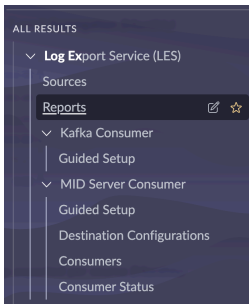
Die externen Protokollanalysesysteme können die Protokollereignisse von verwenden und verarbeiten, entweder in der Cloud oder lokal Hermes Messaging-Service. LES bietet drei Konnektivitätsoptionen zum Verbrauchen der Protokolle:

- Dediziert MID-Server: Ein dedizierter MID-Server Wird lokal oder in der Cloud installiert, die automatisch eine Verbindung mit herstellt Hermes Messaging-Service, Ruft Protokollereignisse kontinuierlich aus der IT ab und sendet sie dann über eine REST-Verbindung an die Protokollierungstools.
- Nutzen Sie den Kafka-Connector aus Ihrer Protokollanalyselösung (z. B. Splunk): Ein Kafka-Connector aus Ihrem Protokoll-Analytics-Produkt Ihrer Wahl wird lokal oder in der Cloud installiert, die automatisch eine Verbindung mit herstellt Hermes Messaging-Service, Ruft Protokollereignisse kontinuierlich aus der IT ab und sendet sie dann an Protokollanalysetools.
- Direkt über Ihr Kafka-System: Ihr Kafka-System stellt eine direkte Verbindung mit her Hermes Messaging-Service Und verwenden Sie die nativen Kafka-Protokollbefehle und -Konnektivität, um Protokollereignisse daraus abzurufen.

Hinweis: Wenn Ihre Kafka-Nachricht den konfigurierten Speicherpuffer überschreitet, gibt Hermes möglicherweise einen Fehler zurück, der angibt, dass er größer ist als der von Ihnen konfigurierte Gesamtspeicherpuffer.

Um LES zu konfigurieren und zu verwalten, müssen Sie sie über installieren ServiceNow Store. Die Anwendung LES bietet geführte Setups, die Ihnen helfen, den Service zu installieren, Seiten zur Konfiguration des Service (Protokollquellen, Verbraucher und Ziele) und Berichte, um die Erstellung und Nutzung von Protokollen zu verstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Sie können auch eine neue Quellkonfiguration erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Protokollquellenkonfiguration.

Protokollexportservice Anwender

Protokollexportservice Hat die folgenden Anwender.

Anwender	Beschreibung
Anwendungsadministrator [sn_logstoAnalytics.admin]	Diese Rolle wird zusammen mit der LES-Anwendung installiert und ermöglicht es einem nicht-Administrator, die Anwendung zu verwenden.
Systemadministrator [admin]	Die Administratorrolle ist für das Setup der LES Store-Anwendung erforderlich.

Protokollexportservice – Vorteile

Vorteil	Funktion	Anwender
Erstellen Sie eine Protokollquellenkonfiguration, um Filter für die Protokolle festzulegen	Erstellen Sie eine Protokollquellenkonfiguration	Anwendungsadministrator
Geführtes Setup für Experience für Kafka-Verbraucher	Geführtes Setup für Kafka-Verbraucher	Systemadministrator
Geführtes Setup für MID-Server-Verbraucher der Experience	Geführtes Setup für MID-Server-Verbraucher	Systemadministrator
Überprüfen Sie das Dashboard für Protokollberichte, um die Größe jedes Datenprotokolls zu analysieren	Überprüfen Sie den Protokollbericht	Systemadministrator oder Anwendungsadministrator

Empfehlungen für weitere Themen

Um mehr über die Verwendung von zu erfahren Protokollexportservice, Siehe:

- Wird Verwaltet Protokollexportservice(LES)
- Wird Konfiguriert Protokollexportservice(LES)
- Verwenden Protokollexportservice(LES)
- Protokollexportservice (LES) Referenzen

Protokollquellen

Protokollexportservice (LES) kann Protokollquellen aus einigen Systemprotokolltabellen, der Audit-Tabelle und Anwendungsknoten-Protokolldateien exportieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden sind die Protokollquellen aufgeführt, die von LES exportiert werden können.

- Systemprotokolltabellen
  - Syslog-Tabelle: Zeigen Sie Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse an, z. B. Arbeitsspeichernutzung auf dem Servercomputer
  - Tabelle „syslog_transaction“: Zeigen Sie alle Browseraktivitäten für eine Instanz an
  - Tabelle „sys_outbound_http_log“: Zeigen Sie alle Anforderungen und Antworten für ausgehende Webservices wie REST und SOAP an
- Audit-Tabelle: Verwenden Sie die Datensatzänderungen der Tabellenansicht „sys_Audit“, die an den Tabellen vorgenommen wurden, die für die Prüfung ausgewählt wurden
- Anwendungsknoten-Protokolldateien: Verwenden Sie die localhost-Protokolldateien, um Anwendungsknotenfehler anzuzeigen. Ihre Instanz hat mehrere Knoten, und jeder Knoten hat mehrere Protokolldateien.

Siehe Systemprotokolle Um mehr über das Schema und den Zweck der obigen Protokollquellen zu erfahren.

Wird Verwaltet Protokollexportservice(LES)

Verwenden Sie LES, um eine Protokollquellenkonfiguration und mehrere Themen für jeden Quelltyp zu erstellen.

Erstellen Sie eine Protokollquellenkonfiguration

Regulieren und legen Sie Filter für die weiterzuleitenden Protokolle fest, indem Sie eine Protokollquellenkonfiguration erstellen.

Vorbereitungen

Erforderliche Rolle: admin oder sn_logstoanalytics.admin

Prozedur

1. Navigieren zu **Alle** > **Log Export Service** an.
   Eine Liste der Quellkonfigurationen wird angezeigt.
2. Wählen Sie Aus **Neu** Wenn Sie eine neue Quellkonfiguration erstellen möchten.
   Sie können auch eine vorhandene Quellkonfiguration auswählen, wenn Sie sie ändern möchten.
   Das Quellformular wird angezeigt.
3. Füllen Sie die Felder im Formular aus.

Quellformular

Felder	Beschreibung
Quelltyp	Typen von Protokollquellen ○ Knotenprotokoll ○ Tabelle Weitere Informationen finden Sie unter Protokollquellen.
Protokollebene	Eine Reihe von Standard-Protokollierungsebenen, die zur Steuerung der Protokollierungsausgabe verwendet werden können. Gemäß der Konvention

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	leitet jede Ebene Protokolle mit gleichem oder höherem Schweregrad weiter. **Hinweis:** Dieses Feld ist nur sichtbar, wenn eine der folgenden Bedingungen erfüllt ist. ○ Wenn Sie Knotenprotokoll als Quelltyp auswählen ○ Wenn Sie Tabelle als Quelltyp auswählen und die Tabelle syslog ist
Akzeptiert	Gibt das Format an, in dem die Protokolle an Hermes weitergeleitet werden. Sie können entweder als JSON oder als nur-Text gesendet werden.
Tabelle	Auswahl der Tabelle für Tabellentyp-Protokolle. **Hinweis:** Dieses Feld ist nur sichtbar, wenn Sie Tabelle als Quelltyp auswählen.
Filtertyp	Bedingungen zum selektiven Weiterleiten von Protokollen. **Hinweis:** Dieses Feld ist nur sichtbar, wenn Sie entweder syslog oder sys_Audit als Tabelle auswählen.

4. Überprüfen Sie die Details der zugehörigen Liste „Quellthemen“.
   Sie können jede der Protokolltabellen überprüfen und eigene Themen erstellen.

   Hinweis: Die zugehörige Liste ist nur sichtbar, wenn Sie im Feld Filtertyp die Option Protokolltabelle auswählen.

   Der Themenname wird nicht automatisch ausgefüllt, und Sie können eigene Themen auswählen oder erstellen.

5. Wählen Sie ein Thema für die Protokolltabelle aus.

   Sie können entweder ein vorhandenes Thema auswählen oder ein neues Thema für eine Protokolltabelle erstellen.

   a. Wählen Sie Aus **Neu** Dient zum Erstellen eines neuen Quellthemas für eine Protokolltabelle. Das Formular „Quellthemen“ wird angezeigt.
   b. Wählen Sie die erforderliche Tabelle im Feld Protokolltabelle aus.
   c. Wählen Sie das Suchsymbol im Feld Thema aus.

      Hinweis: Sie können ein vorhandenes Thema aus der Liste auswählen. Sie können auch ein neues Thema erstellen, indem Sie auswählen **Neu** In der Liste „Kafka-Themen“. Siehe Erstellen Sie Quelltyp und mehrere Themen in der LES-Quelltabelle Um ein neues Kafka-Thema zu erstellen.

   d. Wählen Sie Aus **Übermitteln** Im Formular „Quellthemen“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Zeigen Sie die kürzlich erstellte Protokolltabelle und das entsprechende Thema in der zugehörigen Liste Quellthemen an.
7. Wählen Sie Aus **Übermitteln** Dient zum Erstellen einer neuen Quellkonfiguration.

Erstellen Sie Quelltyp und mehrere Themen in der LES-Quelltabelle

Verwenden Sie Protokolle für jeden Quelltyp, indem Sie mehrere Themen pro Quelltyp erstellen. Sie können jetzt die Option der anwenderdefinierten Auswahl bestimmter Themen für verschiedene Protokollquellen während des Debugging-Prozesses nutzen, ohne die anderen Protokolltabellen zu beeinträchtigen.

Vorbereitungen

Hinweis: Wenn Sie eine Protokollquelle löschen, wird das entsprechende Thema in der Tabelle „sys_kafka_topic“ nicht gelöscht. Wenn Sie die Protokollquelle erneut erstellen, kann das vorhandene Thema wiederverwendet werden, um Kontinuität zu gewährleisten und unnötige Themenneuerstellungen zu vermeiden.

Erforderliche Rolle: admin oder sn_logstoanalytics.admin

Prozedur

1. Navigieren zu **Alle** > **Export-Service protokollieren (LES)** > **Quellen**an.
2. Klicken Sie Auf **Neu** Um eine neue Quelle zu erstellen.
   Das Quellformular wird angezeigt. Zuvor war **Thema** Feld wurde automatisch ausgefüllt, sobald **Quelltyp** Ist ausgewählt. Ab Yokohama kann jeder Quelltyp sein eigenes Thema erstellen. Wird bei Auswahl von nicht standardmäßig ausgefüllt **Quelltyp** Oder **Tabelle** Name. Sie können entweder direkt aus den Kafka-Themen oder aus dem Referenzfeld erstellt werden.

   Hinweis: Da die Tabelle „sys_Audit“ mehrere Protokolltabellen enthält, wird in der Themenspalte der Quellliste kein bestimmtes Thema angezeigt. Zuvor hatten alle Quelltypen dasselbe Thema. Jetzt können Sie verschiedene Themen für verschiedene Quellen auswählen.

3. Wählen Sie das Suchsymbol aus, um zur Liste der Kafka-Themen zu wechseln.
   Die Liste der Kafka-Themen wird angezeigt.
4. **Wahlweise:** Erstellen Sie das neue Kafka-Thema mit den folgenden Schritten.

   Hinweis: Dieser Schritt gilt nur, wenn Sie ein neues Thema für einen ausgewählten Quelltyp erstellen möchten.

   a. Wählen Sie Aus **Neu** Dient zum Erstellen eines neuen Kafka-Themas für den ausgewählten Quelltyp. Das Kafka-Themenformular wird angezeigt.
   b. Füllen Sie die Felder im Formular aus.

Quellformular

Felder	Beschreibung
Name	Name des Themas, das Sie erstellen
Anwendungs-ID	Geben Sie sn_logstoAnalytics ein
Namespace	Geben Sie Den Standard-Namespace Ein
Partition	Das Partitionsfeld eines Themas in Hermes bezieht sich auf die Partitionen, in die die Daten des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Themas unterteilt sind. Es spielt eine Schlüsselrolle bei Skalierbarkeit und Parallelität

c. Wählen Sie Aus **Übermitteln** Zum Erstellen des neuen Kafka-Themas.

5. Wählen Sie aus **Quelltyp** Sie möchten für ein bestimmtes Thema erstellen.
6. Wählen Sie das erforderliche Thema aus der Liste für das ausgewählte aus **Quelltyp** .
7. Wählen Sie Aus **Übermitteln** Um den Quelltyp mit der bestimmten Auswahl zu erstellen.
   Der Quelltyp wird in der Quellliste mit dem ausgewählten Themennamen und anderen Informationen angezeigt.

Wird Konfiguriert Protokollexportservice(LES)

Verwenden Sie das geführte Setup, um die Erstkonfiguration von LES ZU durchlaufen. Das geführte Setup unterstützt Sie bei der Planung des Rollouts des Produkts und der Durchführung der Basiskonfiguration für den Go-Live.

Das geführte Setup organisiert Konfigurationsaktivitäten in Kategorien. Jede Kategorie enthält Informationen wie Planungsleitfäden, Schritte vor dem Setup und Links zu nützlichen Hilfeinhalten. Kategorien bieten auch eine Reihe von Links zu den Seiten in Ihrer Instanz, auf denen Sie die Konfiguration vornehmen. Der geführte Setup-Prozess verfolgt, was Sie abgeschlossen haben, sodass Sie anhalten und dort erneut beginnen können, wo Sie aufgehört haben.

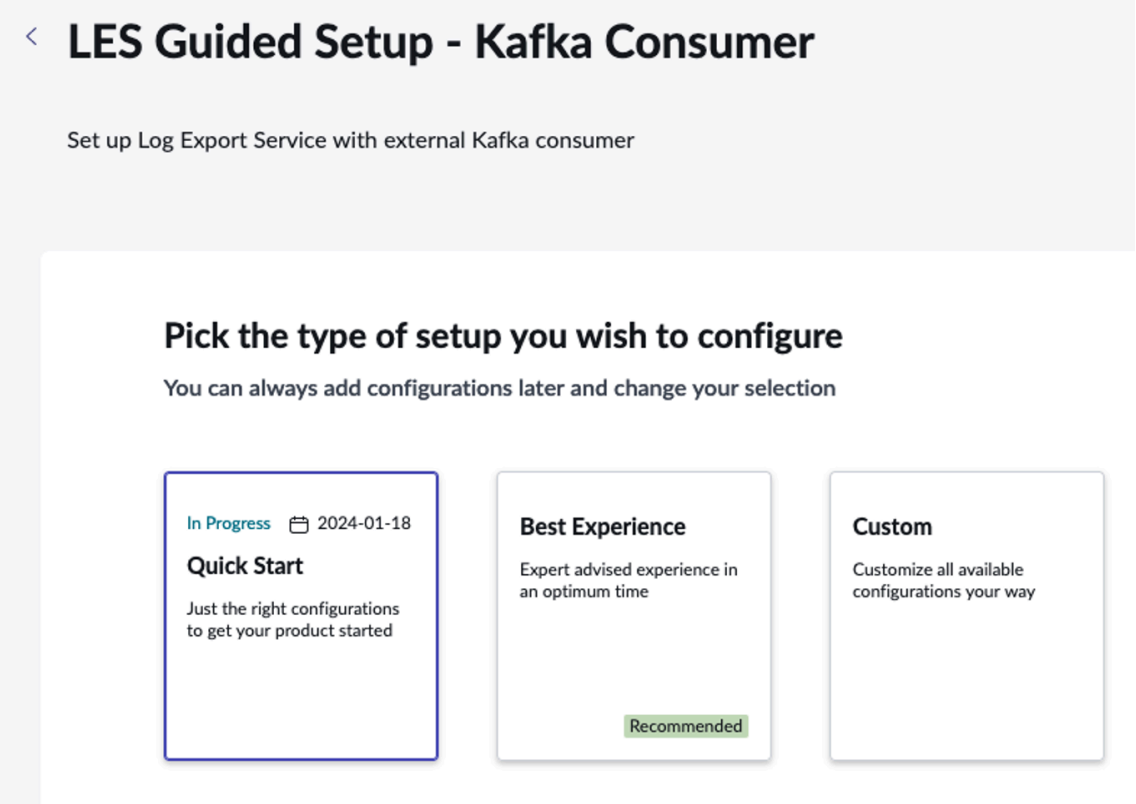
Kafka-Verbraucher

Verwenden Sie das geführte Setup, um die Erstkonfiguration von LES für Kafka-Verbraucher zu durchlaufen.

Homepage des geführten Setups

Die Homepage für das geführte Setup enthält eine Übersicht über Konfigurationstypen für Ihr geführtes Setup. Sie können Ihren Typ des geführten Setups auswählen und auswählen **Fahren Sie Fort** Um die geführten Setup-Schritte zu öffnen und mit der Konfiguration zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



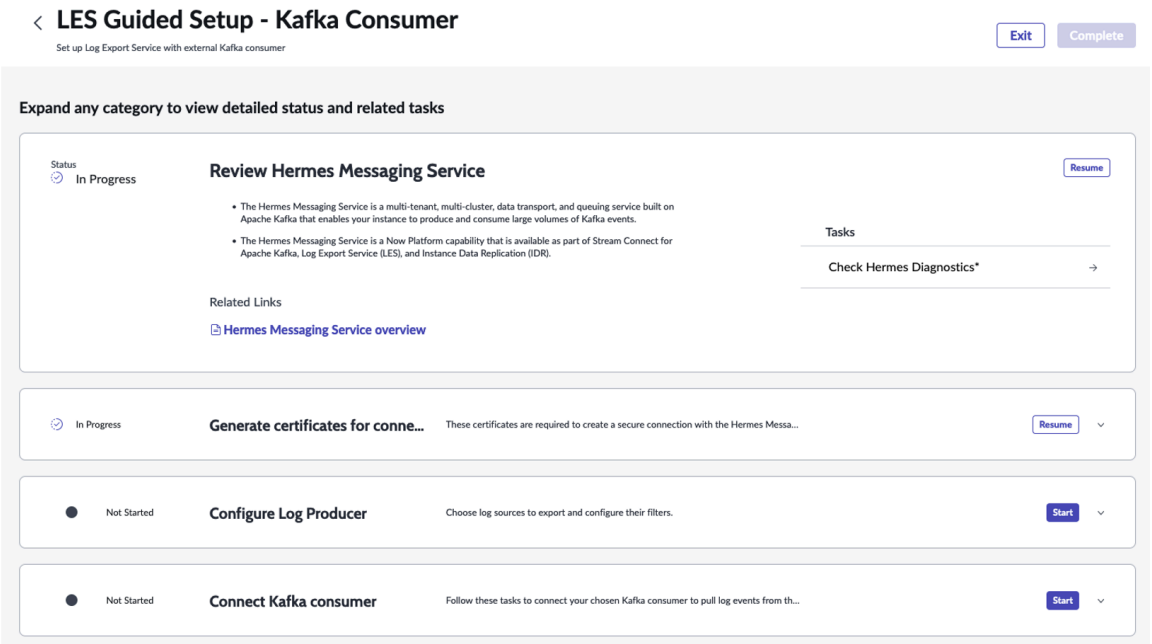
Alle drei Setups auf dieser Seite, Schnellstart/Best Experience/Anwenderdefiniert, bieten dieselben Aufgaben und Funktionen. Es ist erforderlich, die Integration zwischen der ServiceNow-Instanz und dem Analysetool für Zielprotokolle mit dem jeweiligen Administrator zu koordinieren. Der Protokollanalyseadministrator muss sein Tool so konfigurieren, dass eine sichere Verbindung mit der ServiceNow-Instanz hergestellt wird. Es wird empfohlen, den freizugeben Richten Sie eine sichere Verbindung mit ein Hermes Messaging-Service Dokument mit dem Protokollanalyseadministrator im Voraus. Auch wenn Sie eine Aufgabe als abgeschlossen markiert haben, können Sie zurückgehen und sie wieder zu „in Bearbeitung“ deaktivieren. Klicken Sie dazu zuerst auf **Bearbeiten** Feld in der oberen rechten Ecke für die Kategorie. Klicken Sie dann auf **Bearbeiten** Kontrollkästchen für die Aufgabe, die Sie deaktivieren möchten. Die **Als abgeschlossen markieren** Feld wird nicht mehr markiert.

Seite „Kategorien für geführtes Setup“

Die Seite „Kategorien“ enthält eine Übersicht und Beschreibungen der Kategorien und zugehörigen Aufgaben. Sie können entweder auf den Dropdown-Pfeil klicken, um Informationen zur Kategorie anzuzeigen, oder auf die Schaltfläche Start, um die geführten Setup-Schritte zu öffnen und mit der Konfiguration zu beginnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Führen Sie die Aufgaben in den einzelnen Kategorien aus, indem Sie die Setup-Anweisungen befolgen.

Geführtes Setup für Kafka-Verbraucher

Implementieren Sie die folgenden Schritte für ein vollständiges geführtes Setup für Kafka-Verbraucher.

Vorbereitungen

Navigieren zu **Export-Service protokollieren (LES)** > **Kafka-Verbraucher** > **Geführtes Setup**an. Wählen Sie die Art des Setups aus, das Sie konfigurieren möchten, und wählen Sie sie aus **Fahren Sie Fort** .

Hinweis: Während des Protokollexportservice Anwendungsinstallation, ServiceNow Stellt den zugrunde liegenden bereit Hermes Messaging-Service Infrastruktur. Beachten Sie, dass dieser Prozess ab dem Zeitpunkt, zu dem Sie den anfordern, bis zu ein paar Stunden dauern kann Protokollexportservice Anwendungsinstallation.

Erforderliche Rolle: Administrator

Prozedur

1. Überprüfen Hermes Messaging-Service Diagnose.

   Es wird empfohlen, dass Sie überprüfen, ob die Hermes Messaging-Service Wird mit ausgeführt Hermes Diagnosetool, das während dieses Schritts auf dem Bildschirm angezeigt wird. Wenn auf dieser Seite der Fehler „Seite nicht gefunden“ angezeigt wird, Hermes Ist nicht installiert, und wenden Sie sich an Ihren Systemadministrator.

   - Setup-Informationen: Die folgenden Bootstrap-Informationen werden verwendet, um eine Verbindung mit herzustellen Hermes Messaging-Service. „Produzenten-Bootstrap“ ist die Verbindung, die zum Senden von Nachrichten an Hermes verwendet wird, und „Verbraucher-Bootstrap 1 und 2“ werden verwendet, um Nachrichten von Hermes abzurufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Produzenten-Bootstrap
- Verbraucher-Bootstrap 1
- Verbraucher-Bootstrap 2

- Instanz-PKI: Die Komponente „Public Key Infrastructure“ (PKI) der Instanz ermöglicht es einer ServiceNow-Instanz, als Aussteller in einer X.509-Vertrauenshierarchie zu fungieren.
- Bootstrap-Konnektivität: Auswählen **Test Ausführen** Um zu bestätigen, dass der externe Client eine Verbindung zu den definierten Instanzports (Hersteller und Verbraucher) herstellen kann.
- Instanzkonnektivität: Wählen Sie Aus **Test Ausführen** Um zu bestätigen, dass die Instanz Nachrichten senden und empfangen kann.
- Themen anzeigen: Wählen Sie das aufgelistete Thema aus, um den Zeitstempel der letzten bekannten Nachricht abzurufen.

Hinweis: Sie können auf zugreifen Hermes Diagnosen in Zukunft zur Behebung potenzieller Verbindungsprobleme, indem Sie zu diesem Schritt des geführten Setups zurückkehren oder zu navigieren **Alle** > *Hermes Messaging-Service* > **Diagnosen**an.

2. Generieren Sie Zertifikate für eine sichere Verbindung mit Hermes Messaging-Service Und rufen Sie Protokollereignisse daraus ab.

   Sie werden diese Zertifikate verwenden, wenn Sie Ihr externes System verbinden.

   Richten Sie eine sichere Verbindung mit ein Hermes Messaging-Service. Siehe Richten Sie eine sichere Verbindung zum Hermes Messaging-Service für LES ein Weitere Informationen finden Sie unter . Sie benötigen diese Zertifikate für die Authentifizierung und Autorisierung im Client, der die Protokolle von Hermes abruft.

   Hinweis: Für diesen Schritt sind die Rollen „administrator“ oder „Hermes_admin“ erforderlich.

3. Protokollersteller konfigurieren: Wählen Sie Protokollquellen aus, die exportiert werden sollen, und konfigurieren Sie ihre Filter.
   Führen Sie die folgenden Aufgaben aus, um den Protokollersteller zu konfigurieren.

   - Konfigurieren Sie Protokollquellen für den Export: Erstellen Sie einen Quelldatensatz für jede der Protokollquellen, die Sie exportieren möchten.

     Hinweis: Zum Abschließen dieses Schritts sind die Rollen „administrator“ oder „sn_logstoAnalytics.admin“ erforderlich

     a. Wählen Sie Aus **Neu** In der oberen rechten Ecke

     b. Wählen Sie einen Quelltyp aus

     c. Tabelle auswählen

     d. Wählen Sie eine Protokollebene aus, die zur Steuerung der Protokollierungsausgabe verwendet werden kann

     e. Wählen Sie ein Thema aus, in das diese Protokollquelle exportiert wird, oder erstellen Sie es. Wenn Sie ein neues Thema erstellen, füllen Sie die folgenden Felder aus:

     - **Name** : Name des Themas, das Sie erstellen
     - **Anwendungs-ID** : Eingabetaste sn_logstoAnalytics

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Namespace** : Geben Sie Den Standard-Namespace Ein
- **Partition** : Das Partitionsfeld eines Themas in Hermes bezieht sich auf die Partitionen, in die die Daten des Themas unterteilt sind. Es spielt eine Schlüsselrolle bei Skalierbarkeit und Parallelität.

f. Wählen Sie ein aus **Filtertyp** Bedingung zum selektiven Weiterleiten von Protokollen.

Hinweis: Filter unterscheiden sich je nach ausgewähltem Quelltyp

g. Wählen Sie Aktualisieren
Bei erfolgreicher Erstellung wird der Name des Hermes-Themas angezeigt, in das diese Protokollquelle exportiert wird. Notieren Sie sich den Themennamen, den Sie später benötigen, wenn Sie Ihr Protokoll-Verbrauchersystem konfigurieren.

Das Feld aktiv steuert, ob diese Protokollquelle exportiert wird oder nicht. Wenn Fehler angezeigt werden, kehren Sie zur Aufgabe „Hermes-Diagnose überprüfen“ zurück, und überprüfen Sie den Hermes-Status.

- Protokollersteller validieren: Sobald Sie eine Quelle erstellt haben, aus der Protokolle erstellt werden sollen, können Sie Live-Protokolldatensätze im Thema mit anzeigen **Hermes Messaging Service** > **Hermes-Themeninspektor**an.

a. Wählen Sie Externe Themen Aus

b. Wählen Sie Themen Auflisten

c. Zeile mit Ihrem Thema aus dem vorherigen Schritt auswählen (in Quellen aufgeführt)

d. Passen Sie das Startdatum der Nachricht bei Bedarf an

e. Wählen Sie Aus **Anzeigen** Dient zum Anzeigen einer Protokollnachricht, die in das Thema exportiert wurde

4. Kafka-Verbraucher verbinden: Führen Sie diese Aufgaben aus, um den ausgewählten Kafka-Verbraucher zu verbinden, um Protokollereignisse aus Hermes abzurufen.

- Kafka-Verbraucher identifizieren: Sie haben zwei Optionen basierend auf Ihrer Log Analytics-Architektur.
  - Wenn Sie über ein eigenes Kafka-System verfügen und dieses für die Protokollzusammenfassung auswählen, können Sie über das native Kafka-Protokoll direkt eine Verbindung zum Hermes Messaging-Service herstellen.
  - Wenn Sie Ihr Protokoll-Analytics-Tool direkt mit dem Hermes Messaging-Service verbinden möchten, müssen Sie einen Kafka-Connector bereitstellen, der von Ihrem Protokoll-Analytics-System unterstützt wird (z. B. Splunk Connect für Kafka).

Hinweis: In beiden Fällen müssen Sie mit dem Administrator für diese Systeme zusammenarbeiten, um die Verbindung mit dem Hermes Messaging-Service zu koordinieren.

- Hermes-Zertifikate in Kafka-Verbrauchersystem importieren: Melden Sie sich bei Ihrem Kafka-Verbrauchersystem an, und stellen Sie sicher, dass Sie über entsprechende Administratorberechtigungen verfügen, um es zu konfigurieren und mit einem externen System zu verbinden. Importieren Sie die in der Aufgabe „sichere Verbindung mit Hermes Messaging-Service einrichten“ generierten Zertifikate in Ihren Kafka-Connector oder Kafka-Server. Befolgen Sie die Anweisungen in der Dokumentation für Ihren ausgewählten Kafka-Verbraucher.
- Kafka-Prozesse konfigurieren: Der Hermes Messaging-Service ist auf Hochverfügbarkeit ausgelegt. Zum Verbrauchen von Nachrichten von Hermes sind zwei Prozesse erforderlich. Zwei Prozesse sind erforderlich, da Hermes ein Paar von Kafka-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Clustern für Failover-Zwecke verwendet. Wenn ein Cluster ausfällt, werden Daten für den anderen Hermes-Kafka-Cluster erstellt.

In Ihrem Kafka-Verbrauchersystem müssen Sie zwei separate Verbraucherprozesse erstellen, um eine Verbindung mit beiden Hermes-Kafka-Clustern herzustellen. Für beide Prozesse geben Sie dasselbe Hermes Kafka-Thema an, Sie müssen jedoch zwei separate Bootstrap-Adressen konfigurieren:

- <instance_name>.service-now.com:4100, <instance_name>.service-now.com:4101, <instance_name>.service-now.com:4102, <instance_name>.service-now.com:4103
- <instance_name>.service-now.com:4200, <instance_name>.service-now.com:4201, <instance_name>.service-now.com:4202, <instance_name>.service-now.com:4203

Wichtige Hinweise:

- Wenn Sie über externe Systeme auf das Kafka-Thema zugreifen, müssen Sie „snc.<instance name>“ voranstellen. An das Thema, an das die Protokolle weitergeleitet werden.
- Konfigurieren Sie jeden Verbraucher mit derselben Kafka-Verbrauchergruppen-ID.
- Installieren Sie Ihre Schlüsselspeicher- und Truststore-Dateien an einem Ort, an dem Ihre Verbraucher darauf zugreifen können.
- Wenn Ihre Verbraucher dies benötigen, geben Sie die Eigenschaften der Kafka-JSON-Konverter an, um Schemas zu deaktivieren: „Key.Converter.Schemas.enable=false“, „value.Converter.Schemas.enable=false“

◦ Überprüfen, ob Kafka-Verbraucher Protokolle von Hermes abrufen: Verifizieren Sie in Ihrem ausgewählten Kakfa-Verbraucher, ob Sie Protokollereignisse aus dem Hermes Messaging-Service abrufen können.

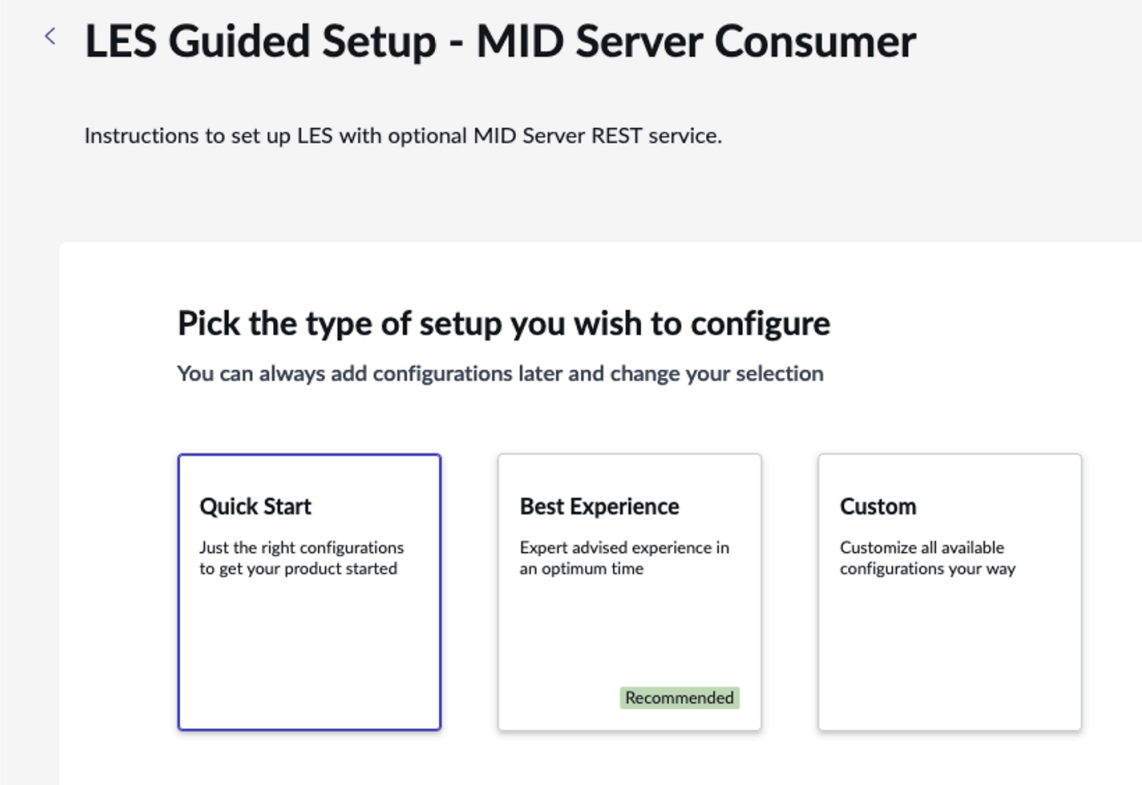
MID-Server-Verbraucher

Verwenden Sie das geführte Setup, um die Erstkonfiguration von LES für den MID-Server-Verbraucher zu durchlaufen.

Homepage des geführten Setups

Die Homepage für das geführte Setup enthält eine Übersicht über Konfigurationstypen für Ihr geführtes Setup. Sie können Ihren Typ des geführten Setups auswählen und auswählen **Fahren Sie Fort** Um die geführten Setup-Schritte zu öffnen und mit der Konfiguration zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

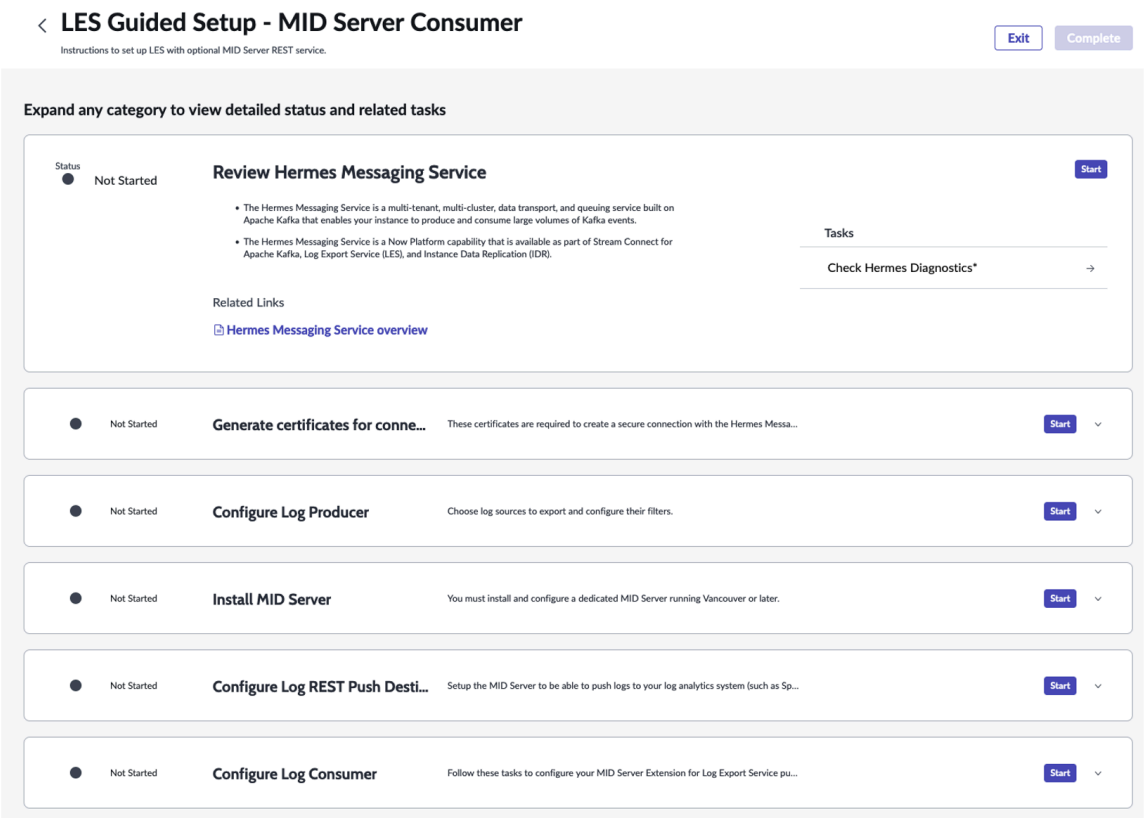


Alle drei Setups auf dieser Seite, Schnellstart/Best Experience/Anwenderdefiniert, bieten dieselben Aufgaben und Funktionen. Ein dedizierter MID-Server ist erforderlich, um Protokolle kontinuierlich von Ihrer Instanz an Ihr Protokollanalysesystem zu streamen. Der MID-Server benötigt ein einmaliges Setup, um eine sichere Verbindung zum Hermes Messaging-Service herzustellen. Auch wenn Sie eine Aufgabe als abgeschlossen markiert haben, können Sie zurück gehen und sie wieder auf „in Bearbeitung“ deaktivieren. Klicken Sie dazu zuerst auf **Bearbeiten** Feld in der oberen rechten Ecke für die Kategorie. Klicken Sie dann auf **Bearbeiten** Kontrollkästchen für die Aufgabe, die Sie deaktivieren möchten. Die **Als abgeschlossen markieren** Feld wird nicht mehr markiert.

Seite „Kategorien für geführtes Setup“

Die Seite „Kategorien“ enthält eine Übersicht und Beschreibungen der Kategorien und zugehörigen Aufgaben. Sie können entweder auf den Dropdown-Pfeil klicken, um Informationen zur Kategorie anzuzeigen, oder auf klicken **Starten** Um die geführten Setup-Schritte zu öffnen und mit der Konfiguration zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Führen Sie die Aufgaben in den einzelnen Kategorien aus, indem Sie die Setup-Anweisungen befolgen.

Geführtes Setup für MID-Server-Verbraucher

Implementieren Sie die folgenden Schritte für ein vollständiges geführtes Setup für MID-Server-Verbraucher.

Vorbereitungen

Navigieren zu **Export-Service protokollieren (LES)** > **MID-Server-Verbraucher** > **Geführtes Setup**an. Wählen Sie die Art des Setups aus, das Sie konfigurieren möchten, und wählen Sie sie aus **Fahren Sie Fort** .

Hinweis: Während des Protokollexportservice Anwendungsinstallation, ServiceNow Stellt den zugrunde liegenden bereit Hermes Messaging-Service Infrastruktur. Beachten Sie, dass dieser Prozess ab dem Zeitpunkt, zu dem Sie den anfordern, bis zu ein paar Stunden dauern kann Protokollexportservice Anwendungsinstallation.

Erforderliche Rolle: Administrator

Prozedur

1. Überprüfen Hermes Messaging-Service Diagnose.

   Es wird empfohlen, dass Sie überprüfen, ob die Hermes Messaging-Service Wird mit ausgeführt Hermes Diagnosetool, das während dieses Schritts auf dem Bildschirm angezeigt wird. Wenn auf dieser Seite der Fehler „Seite nicht gefunden“ angezeigt wird, Hermes Ist nicht installiert, und wenden Sie sich an Ihren Systemadministrator.

   - Setup-Informationen: Die folgenden Bootstrap-Informationen werden verwendet, um eine Verbindung zum Hermes Messaging-Service herzustellen. „Produzenten-Bootstrap“ ist die Verbindung, die zum Senden von Nachrichten an Hermes verwendet

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird, und „Verbraucher-Bootstrap 1 und 2“ werden verwendet, um Nachrichten von Hermes abzurufen.

- Produzenten-Bootstrap
- Verbraucher-Bootstrap 1
- Verbraucher-Bootstrap 2

- Instanz-PKI: Die Komponente „Public Key Infrastructure“ (PKI) der Instanz ermöglicht es einer ServiceNow-Instanz, als Aussteller in einer X.509-Vertrauenshierarchie zu fungieren.
- Bootstrap-Konnektivität: Auswählen **Test Ausführen** Um zu bestätigen, dass der externe Client eine Verbindung zu den definierten Instanzports (Hersteller und Verbraucher) herstellen kann.
- Instanzkonnektivität: Wählen Sie Aus **Test Ausführen** Um zu bestätigen, dass die Instanz Nachrichten senden und empfangen kann.
- Themen anzeigen: Wählen Sie das aufgelistete Thema aus, um den Zeitstempel der letzten bekannten Nachricht abzurufen.

Hinweis: Sie können auf zugreifen Hermes Diagnosen in Zukunft zur Behebung potenzieller Verbindungsprobleme, indem Sie zu diesem Schritt des geführten Setups zurückkehren oder zu navigieren **Alle** > *Hermes Messaging-Service* > **Diagnosen**an.

2. Generieren Sie Zertifikate für eine sichere Verbindung mit dem Hermes Messaging-Service, und rufen Sie Protokollereignisse daraus ab.

   Richten Sie eine sichere Verbindung zum Hermes Messaging-Service ein. Siehe Richten Sie eine sichere Verbindung zum Hermes Messaging-Service für LES ein Weitere Informationen finden Sie unter . Sie benötigen diese Zertifikate für die Authentifizierung und Autorisierung im Client, der die Protokolle von Hermes abruft.

   Hinweis: Für diesen Schritt sind die Rollen „administrator“ oder „Hermes_admin“ erforderlich.

3. Protokollersteller konfigurieren: Wählen Sie Protokollquellen aus, die exportiert werden sollen, und konfigurieren Sie ihre Filter.
   Führen Sie die folgenden Aufgaben aus, um den Protokollersteller zu konfigurieren.

   - Konfigurieren Sie Protokollquellen für den Export: Erstellen Sie einen Quelldatensatz für jede der Protokollquellen, die Sie exportieren möchten.

     Hinweis: Zum Abschließen dieses Schritts sind die Rollen „administrator“ oder „sn_logstoAnalytics.admin“ erforderlich

     Um eine neue Quelle zu erstellen, navigieren Sie zu **Log Export Service** > **Quellen**

     a. Wählen Sie Aus **Neu** In der oberen rechten Ecke

     b. Wählen Sie einen Quelltyp aus

     c. Tabelle auswählen

     d. Wählen Sie eine Protokollebene aus, die zur Steuerung der Protokollierungsausgabe verwendet werden kann

     e. Wählen Sie ein Thema aus, in das diese Protokollquelle exportiert wird, oder erstellen Sie es. Wenn Sie ein neues Thema erstellen, füllen Sie die folgenden Felder aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Name** : Name des Themas, das Sie erstellen
- **Anwendungs-ID** : Eingabetaste sn_logstoAnalytics
- **Namespace** : Geben Sie Den Standard-Namespace Ein
- **Partition** : Das Partitionsfeld eines Themas in Hermes bezieht sich auf die Partitionen, in die die Daten des Themas unterteilt sind. Es spielt eine Schlüsselrolle bei Skalierbarkeit und Parallelität.

f. Wählen Sie ein aus **Filtertyp** Bedingung zum selektiven Weiterleiten von Protokollen.

Hinweis: Die Filtertypoptionen unterscheiden sich je nach ausgewähltem Quelltyp.

g. Wählen Sie Aktualisieren
Bei erfolgreicher Erstellung wird der Name des Hermes-Themas angezeigt, in das diese Protokollquelle exportiert wird. Notieren Sie sich den Themennamen, den Sie später benötigen, wenn Sie Ihr Protokoll-Verbrauchersystem konfigurieren.

Das Feld aktiv steuert, ob diese Protokollquelle exportiert wird oder nicht. Wenn Fehler angezeigt werden, kehren Sie zur Aufgabe „Hermes-Diagnose überprüfen“ zurück, und überprüfen Sie den Hermes-Status.

- Protokollersteller validieren: Sobald Sie eine Quelle erstellt haben, aus der Protokolle erstellt werden sollen, können Sie Live-Protokolldatensätze im Thema mit anzeigen **Hermes Messaging Service** > **Hermes-Themeninspektor**an.

a. Wählen Sie Externe Themen Aus

b. Wählen Sie Themen Auflisten

c. Zeile mit Ihrem Thema aus dem vorherigen Schritt auswählen (in Quellen aufgeführt)

d. Passen Sie das Startdatum der Nachricht bei Bedarf an

e. Wählen Sie Aus **Anzeigen** Dient zum Anzeigen einer Protokollnachricht, die in das Thema exportiert wurde

4. MID-Server installieren: Sie müssen einen dedizierten MID-Server installieren und konfigurieren, auf dem Vancouver oder höher ausgeführt wird.
Führen Sie die folgenden Aufgaben aus, um den MID-Server zu installieren.

- Dedizierten MID-Server installieren: Der MID-Server, den der Protokollexport-Service verwendet, sollte nur für diesen Zweck dediziert sein und darf nicht erwartet werden, dass er andere Prozesse ausführt. Dies ist wichtig, um die rechtzeitige Bereitstellung exportierter Protokollnachrichten an Ihren REST-Endpunkt sicherzustellen. Sie können den neuen MID-Server entweder mit installieren Geführtes Setup „MID-Server verwenden“ Oder durch manuelle Installation. Befolgen Sie für die manuelle Installation die Konfigurieren Sie die Netzwerkkonnektivität des MID-Servers Dokumentation zuerst und dann die MID-Server wird installiert Dokumentation danach.
- MID-Server validieren: Sie müssen den MID-Server nach der Installation manuell validieren, damit er Automatisierungsaufgaben ausführen kann. Informationen zur Validierung des MID-Servers, den Sie für LES dedizieren, finden Sie unter MID-Server validieren

5. Protokoll-REST-Push-Ziel konfigurieren: Richten Sie den MID-Server ein, damit Protokolle an Ihr Protokoll-Analytics-System (z. B. Splunk) übertragen werden können.
Führen Sie die folgenden Aufgaben aus, um das Protokoll-REST-Push-Ziel zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MID-Eigenschaften hinzufügen: Sie müssen MID-Server-Eigenschaften hinzufügen, damit eine Verbindung zu Hermes hergestellt werden kann. Navigieren Sie zu **MID-Server** > **Eigenschaften** Und legen Sie die entsprechenden Werte für jede der unten aufgeführten Eigenschaften fest.

Name	Wert
Mid.les.kafka.ssl.Truststore.password	<password>
Mid.les.kafka.ssl.Keystore.password	<password>
Mid.les.kafka.ssl.key.password	<password>
Mid.les.kafka.ssl.Truststore.location	<your_path>/<truststore>.p12
Mid.les.kafka.ssl.Keystore.location	<your_path>/<keystore>.p12
Mid.les.kafka.ssl.Truststore.type	PKCS12
Mid.les.kafka.ssl.Keystore.type	PKCS12
mid.les.kafka.client.id	<instance_name>
mid.les.kafka.group.id	snc.<instance_name>.group1
mid.les.kafka.bootstrap.servers	<instance_name>.servicenow.com:4100,<instance_name>.servicenow.
mid.les.kafka.set2.bootstrap.servers	<instance_name>.servicenow.com:4200,<instance_name>.servicenow.

Befolgen Sie diese Hinweise, um einige der oben genannten Werte zu erhalten

- <password> ist das Passwort, das Sie für den Schlüsselspeicher und den Truststore festgelegt haben
- <your_path> ist der Dateipfad zu dem Verzeichnis, in dem Sie die heruntergeladenen Schlüsselspeicher- und Truststore-Dateien speichern. Die Zertifikate müssen sich auf dem Server befinden, auf dem Sie MID ausführen
- <instance_name> ist der Name Ihrer ServiceNow-Instanz. Wenn Sie sich nicht sicher sind, finden Sie sie in der Tabelle „sys_properties“
- Sie können die Werte für mid.les.kafka.bootstrap.servers und mid.les.kafka.set2.bootstrap.servers auf der Seite „Hermes-Diagnose“ abrufen. Navigieren zu **Hermes Messaging Service** > **Diagnosen** Und kopieren Sie die Zeichenfolgen unter Verbraucher-Bootstrap 1 bzw. Verbraucher-Bootstrap 2.

- Ziel konfigurieren: Erstellen Sie einen neuen Zielkonfigurationsdatensatz, der den REST-Endpunkt definiert, an den diese Erweiterung Protokolle weiterleitet.

  Hinweis: Zum Abschließen dieses Schritts sind die Rollen „administrator“ oder „sn_logstoAnalytics.admin“ erforderlich.

  a. Navigieren zu **Export-Service protokollieren (LES)** > **Zielkonfigurationen**

  b. Erstellen Sie einen neuen Konfigurationsdatensatz

  c. Geben Sie die URL für den gewünschten Endpunkt für die exportierten Protokollquellen an

  d. Suchen Sie nach neuen Anmeldeinformationen, oder erstellen Sie neue Anmeldeinformationen, um eine Verbindung mit Ihrem Endpunkt herzustellen. Beachten Sie beim Erstellen von Anmeldeinformationen für Ihren Endpunkt,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dass für LES nur die folgenden Anmeldeinformationstypen gültig sind: Standardauthentifizierung, OAuth, API-Schlüssel

e. Suchen oder erstellen Sie ein neues Transformationsskript. Wir werden mit dem vorgeschriebenen Skript geliefert, **SplunkTransform** Für Splunk

6. PROTOKOLLVERBRAUCHER konfigurieren: Führen Sie diese Aufgaben aus, um Ihre MID-Servererweiterung für Protokollexport-Service-Zwecke zu konfigurieren.

- LES-Verbraucherkontext konfigurieren: In diesem Schritt aktualisieren Sie den LES-Verbraucher-Datensatz so, dass er auf dem dedizierten MID-Server ausgeführt wird, den Sie gerade für den Protokollexport-Service installiert haben. Navigieren zu **MID-Server** > **Erweiterungen** > **LES-Verbraucherkontext** Und aktualisieren Sie den LES-Verbraucher-Datensatz, indem Sie die folgenden Felder festlegen:
  - Wählen Sie unter „LES Consumer“ aus, um den MID-Server-Kontextdatensatz zu öffnen
  - Wählen Sie einen bestimmten MID-Server für das Feld „Ausführen auf“ aus
  - Geben Sie den Namen des MID ein, den Sie im vorherigen Schritt für das Feld „MID-Server“ validiert haben

  Wählen Sie Aus **Aktualisieren** Zum Speichern.

  Hinweis: Wir werden mit einem vorgefertigten Kontext geliefert. Erstellen Sie keine zweite. Dies kann unbeabsichtigte Konsequenzen haben.

- Verbraucher konfigurieren: Erstellen Sie einen neuen Verbraucherdatensatz, der den Prozess darstellt, der Teil der MID-Servererweiterung des Protokollexportservice ist. Navigieren zu **Export-Service protokollieren (LES)** > **Verbraucher** Und erstellen Sie einen neuen Konfigurationsdatensatz, der das Hermes-Thema zum Abrufen von Protokollnachrichten und das Ziel angibt, an das sie weitergeleitet werden sollen. Wenn Sie auswählen **Verbraucher** Modul, zeigt Informationen zum Verbrauchernamen und zur Zielkonfiguration an.

  a. Erstellen Sie einen neuen Verbraucherdatensatz

  b. Wählen Sie ein Quellthema aus der Dropdown-Liste aus

  c. Wählen Sie die Zielkonfiguration aus

  d. Starten Sie Verbraucher

- MID-Server-Integration verifizieren: Navigieren Sie zu ☒**Export-Service protokollieren (LES)** > **Verbraucherstatus** Und zeigen Sie die#Felder Status und Statusdetails des definierten Datensatzes an. Die Informationen in diesen Feldern berichten über den aktuellen Status des auf dem MID-Server ausgeführten Prozesses, einschließlich aller Fehler, die beim Weiterleiten von Nachrichten an den REST-Endpunkt aufgetreten sind. Dies ist nur eine Statusansichtsseite. Navigieren zu **Export-Service protokollieren (LES)** > **Verbraucher** Wenn Sie einen neuen Verbraucherdatensatz erstellen möchten. #Wenn der Verbraucherstatus anzeigt, dass der Prozess gestartet wurde, sollten Sie Ihren Endpunkt überprüfen können, um die Protokolle anzuzeigen, die an ihn weitergeleitet wurden. #Darüber hinaus können Sie die Protokolle auf dem MID-Server anzeigen, um zu sehen, ob zusätzliche Details zu eventuell aufgetretenen Fehlern vorhanden sind. Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können auch die Debug-Protokollierung auf dem MID-Server aktivieren, um bei Bedarf zusätzliche Informationen zu erhalten.

Hinweis: Wenn Sie Änderungen an einem der Verbraucherdatensätze vornehmen, wird dies auf der Seite „Verbraucherstatusansicht“ angezeigt. Wenn Sie in der Liste „Verbraucherstatus“ einen Verbraucherdatensatznamen auswählen, wird das Verbraucherformular für den ausgewählten Datensatz geöffnet. Sie können dann die Name- und Zielkonfiguration des ausgewählten Datensatzes aktualisieren.

Unterstützung mehrerer Verbraucher mit eindeutigen MID-Servern

Sie können den Protokollverbrauch jetzt mit einem neuen System mit mehreren Verbrauchern genau verwalten, das dedizierte Verbraucher und MID-Server für jeden spezifischen Protokoll-Stream ermöglicht.

Das System unterstützt jetzt den Protokollverbrauch mehrerer Verbraucher, d. h. jede Protokollquelle kann separat verwendet werden und hat ein eigenes dediziertes Thema.

Zuvor wurden alle Protokolle aus demselben Thema verbraucht. Mit dem neuen Konzept für mehrere Themen können Sie jedoch mehrere Verbraucher für verschiedene Themen erstellen. Um einen Verbraucher zu erstellen, können Sie Folgendes auswählen:

- Ein bestimmtes Thema aus dem Dropdown-Menü
- Entsprechende Zielkonfiguration
- Jeweiliger Verbraucherkontext

Hinweis: Ab Zurich-Release, die **Verbraucherkontext** Ist ein neues Feld im Formular „Verbraucher“ hinzugefügt. Jeder Verbraucherkontext ist einem eindeutigen MID-Server zugeordnet.

Um mehrere Verbraucher zu erstellen, müssen Sie für jeden Verbraucher unterschiedliche Themen auswählen. Dies erfordert wiederum die Erstellung separater Verbraucherkontextdatensätze und der entsprechenden eindeutigen MID-Server.

Parallele Verarbeitung mit mehreren MID-Servern

Ein großer Vorteil dieser Architektur für mehrere Verbraucher ist die Möglichkeit, mehrere Verbraucher parallel auszuführen. Diese parallele Verarbeitung verbessert den Gesamtdurchsatz und die Effizienz der Protokollnutzung erheblich, sodass das System größere Mengen verschiedener Protokolldaten effektiver verarbeiten kann als zuvor.

Richten Sie eine sichere Verbindung zum Hermes Messaging-Service für LES ein

Sichern Sie Ihre Kafka-Themen, indem Sie einen generieren ServiceNow® Von Instanz signiertes Zertifikat.

Vorbereitungen
Einrichten von Hermes Messaging-Service Erfordert Koordination mit Ihrem Netzwerkadministrator und Ihrem Kafka-Administrator. Arbeiten Sie mit Ihrem Netzwerkadministrator zusammen, um die erforderlichen Sicherheitszertifikate zu erhalten und die erforderlichen Ports zu öffnen. Arbeiten Sie mit Ihrem Kafka-Administrator zusammen, um sicherzustellen, dass Ihre Kafka-Umgebung korrekt konfiguriert ist und Ihre Anwendungen eine Verbindung mit herstellen können Hermes Messaging-Service Mit dem Standard-Kafka-Protokoll.

Stellen Sie sicher, dass das folgende Setup vorhanden ist:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Hermes Messaging-Service Ist aktiviert. Weitere Informationen finden Sie unter Wird aktiviert Hermes Messaging-Service .
- Das Plugin „Key Management Framework“ (com.Glide.kmf.global) ist aktiviert.
- Die Tabelle „Zertifikate“ [sys_kmf_certificate] enthält einen ServiceNow CA-Stammzertifikat der Instanz.
- Die Instanz ist nicht mit einer anwenderdefinierten URL konfiguriert. Anwenderdefinierte URLs werden mit dem Instanz-PKI-Zertifikatgenerator nicht unterstützt.

Erforderliche Rolle: hermes_admin, sn_kmf.cryptographic_Manager oder admin

Details zum Zuweisen von KMF-Rollen finden Sie unter Mit Key Management Framework installierte Rollen.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatgenerator** > **Zertifikatgenerator für Instanz-PKI**an.
2. **Wahlweise:** Steuern Sie den Zugriff auf Themen, indem Sie Zugriffssteuerungslisten (ACLs) auf Namespace- oder Themenebene konfigurieren.

Option	Beschreibung
Wenden Sie ACLs auf Namespaces an	**a.** Wählen Sie Aus **Konfigurieren Sie ACLs** . **b.** Wählen Sie im Dialogfeld „Themen-ACLs“ die Option aus **Namespaces** . **c.** Geben Sie einen Namespace ein, den Sie konfigurieren möchten. **d.** Legen Sie die Berechtigungsstufe fest, indem Sie eine der folgenden Optionen auswählen **Schreibgeschützt** Oder **Le sen/Schreiben** . **e.** Wählen Sie **Hinzufügen**.
Wenden Sie ACLs auf definierte Themen an	**a.** Wählen Sie Aus **Konfigurieren Sie ACLs** . **b.** Wählen Sie im Dialogfeld „Themen-ACLs“ die Option aus **Definierte Themen** . **c.** Geben Sie ein vorhandenes Thema ein, das Sie konfigurieren möchten. **d.** Legen Sie die Berechtigungsstufe fest, indem Sie eine der folgenden Optionen auswählen **Schreibgeschützt** Oder **Le sen/Schreiben** . **e.** Wählen Sie **Hinzufügen**.

Dem Träger des Zertifikats wird Lese- oder Lese-/Schreibzugriff auf die Themen im Namespace oder im vorhandenen von Ihnen ausgewählten Thema gewährt.

3. Richten Sie die Sicherheit für ein Hermes Messaging-Service.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren Sie zurück zur Seite Instanz-PKI-Zertifikatgenerator.

b. Geben Sie ein Schlüsselspeicher-Passwort in ein **Zertifikatpasswort** Feld.

c. Wählen Sie Aus **Generieren** .
Das System generiert ein instanzsigniertes Zertifikat in der Tabelle „Zertifikate“ [sys_kmf_certificate], erstellt einen Schlüsselspeicher und erstellt einen Truststore.

Wenn eingeschränkter Anruferzugriff für den IPKI-Zertifikatgenerator nicht zulässig ist, wird ein bereichsübergreifender Zugriffsfehler angezeigt. Kontakt Kundenservice und Support Für Unterstützung beim Zulassen des eingeschränkten Anruferzugriffs. So beheben Sie dieses Problem: Kundenservice und Support Kann auf Source_scope=76f9d51369115083f4ea77aab1677cc0 in der Tabelle „eingeschränkte Anruferzugriffsberechtigungen“ [sys_Restricted_caller_Access] verweisen.

4. Speichern Sie eine Kopie des Schlüsselspeichers, indem Sie auswählen **Schlüsselspeicher Herunterladen** .
5. Speichern Sie eine Kopie des Truststore, indem Sie auswählen **Truststore Herunterladen** .
6. Kopieren Sie die Schlüsselspeicher- und Truststore-Dateien in jeden Hersteller- und Verbraucherclient, der eine Verbindung mit herstellt Hermes Messaging-Service.

Ergebnis
Sie können jetzt eine sichere Verbindung mit erstellen Hermes Messaging-Service.

Hinweis: Sie müssen den Schlüsselspeicher verwenden, den Sie mit dem Instanz-PKI-Zertifikatgenerator generiert haben, um eine Verbindung herzustellen Hermes. Anwenderdefinierte generierte Schlüsselspeicher, die nicht gemäß erstellt werden ServiceNow Dokumentation wird nicht unterstützt.

Nächste Maßnahme
.

Verwenden Protokollexportservice(LES)

Verwenden Sie LES, um das Dashboard für Protokollberichte zu überprüfen.

Überprüfen Sie den Protokollbericht

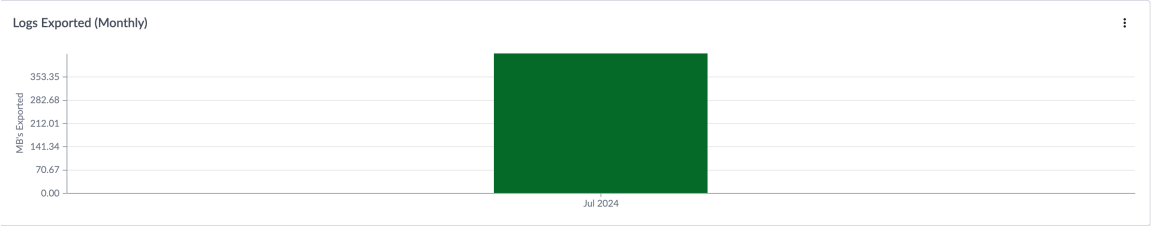
Analysieren Sie die Größe jedes Datenprotokolls, indem Sie das Dashboard für Protokollberichte überprüfen.

Vorbereitungen
Erforderliche Rolle: admin oder sn_logstoanalytics.admin

Prozedur

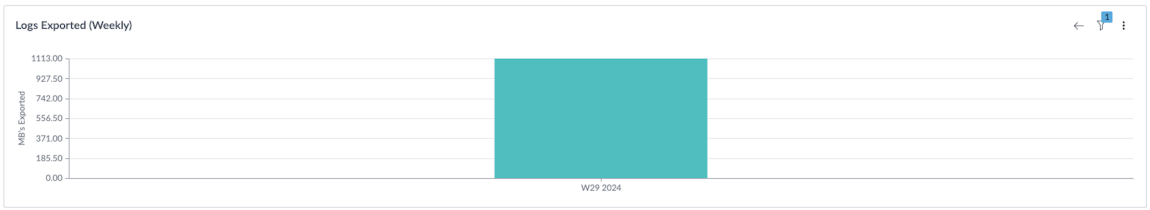
1. Navigieren zu **Alle** > **Log Export Service** > **Berichte**an.
2. Überprüfen Sie Protokolldaten in den folgenden Widgets.
   - Exportierte Protokolle (monatlich): Zeigt die pro Monat exportierten Megabyte in der anfänglichen Ansicht an. Sie können ein Drilldown des Diagramms durchführen, um die Daten für jede Woche oder tägliche Daten anzuzeigen. Sie können Daten der letzten 395 Tage anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

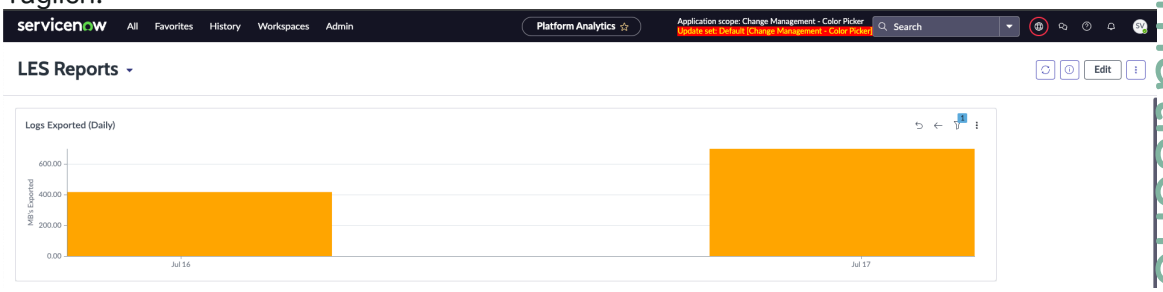


Hinweis: Klicken Sie auf die Pfeile in der oberen rechten Ecke des Widgets, um einen Drilldown für die Daten durchzuführen. Sie können auch zurück zu den übergeordneten Daten wechseln.

Wöchentlich:

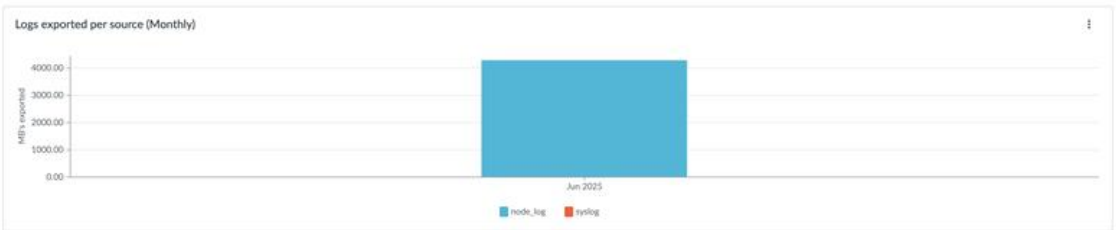


Täglich:

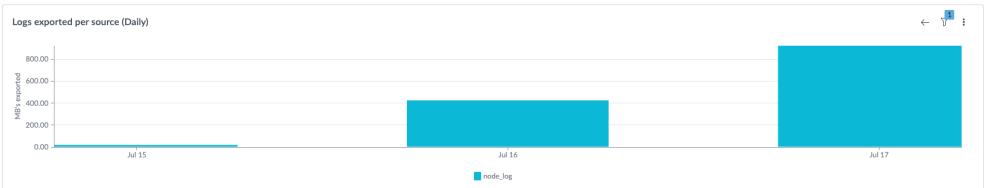


Die Daten in diesem Bericht spiegeln die Erfassung wider, die 4 Stunden zuvor durchgeführt wurde.

- Pro Quelle exportierte Protokolle (monatlich): Dieses Widget zeigt die Art der Protokolle an, die monatlich exportiert wurden. Sie können auch Drilldown durchführen, um wöchentliche und tägliche Protokolldaten anzuzeigen. Sie können Daten der letzten 395 Tage anzeigen.



Hinweis: Sie können die Quelle auswählen oder deaktivieren, aus der Sie die Daten anzeigen möchten. Die Quellen, aus denen Sie die Protokolle anzeigen können, sind: Node_log, syslog, syslog_transaction und sys_outbound_http_log.



Automatische Übersetzung

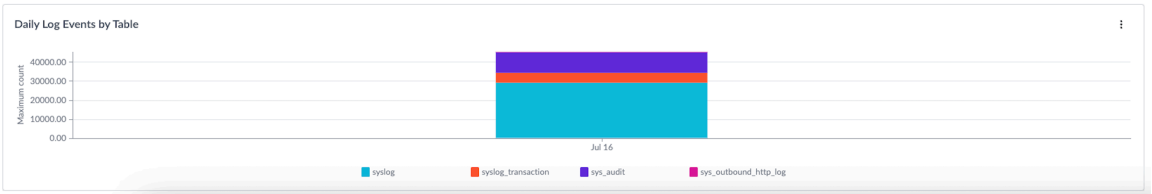
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Protokoll pro Quelle exportiert (letzte 24 Stunden): Zeigt die Daten der letzten 24 Stunden an. Das Diagramm verläuft chronologisch von links nach rechts auf einer 24-Stunden-Skala, wobei die ältesten Daten (24. Stunde) auf der rechten Seite und die neuesten Daten auf der linken Seite des Berichts positioniert sind. Sie können die Quelle auswählen oder deaktivieren, aus der Sie die Daten anzeigen möchten. Die Quellen, aus denen Sie die Protokolle anzeigen können, sind: Node_log, syslog, syslog_transaction und sys_outbound_http_log.



Hinweis: Je nach Tageszeit, zu der Sie diese Daten überprüfen, wird das Widget dynamisch aktualisiert, um genau die letzten 24 Stunden widerzuspiegeln.

- Tägliche Protokollereignisse nach Tabelle: Zeigt die Protokollereignisse an, die von den einzelnen Protokolltabellen pro Tag generiert werden. Sie können die Tabellen auswählen oder deaktivieren, aus denen Sie die Daten anzeigen möchten.



Hinweis: Die Tabellen, aus denen Sie die Protokollereignisse anzeigen können, sind: Syslog, syslog_transaction, sys_Audit und sys_outbound_http_log.

Protokollexportservice (LES) Referenzen

Alle sonstigen Informationen zu LES finden Sie im Referenzabschnitt.

Protokollexportservice Rollen

Protokollexportservice Wird mit diesen Rollen installiert.

Anwendungsadministrator [sn_logstoAnalytics.admin]

Weitere Informationen zur Verwaltung von Abonnements pro Anwender finden Sie unter Verwalten von Anwenderabonnements in Abonnement-Management Und wenden Sie sich an Ihren Account-Vertreter.

Diese Rolle wird zusammen mit der LES-Anwendung installiert und ermöglicht es einem nicht-Administrator, die Anwendung zu verwenden.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Erweitert

Gibt an, ob die Rolle eine erhöhte Rolle ist. Erhöhte Rollen werden Benutzern oder Gruppen nicht zugewiesen und müssen durch Erhöhung verwendet werden. Weitere Informationen finden Sie unter Auf eine privilegierte Rolle hochstufen.

Nein.

Besondere Erwägungen

Keine.

Systemadministrator [Administrator]

Weitere Informationen zur Verwaltung von Abonnements pro Anwender finden Sie unter Verwalten von Anwenderabonnements in Abonnement-Management Und wenden Sie sich an Ihren Account-Vertreter.

Die Administratorrolle ist für das Setup der LES Store-Anwendung erforderlich.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

- sn_templated_snip.template_snippet_admin
- sn_employee.admin
- taxonomy_admin
- sn_ace.ace_user
- sn_hr_sp.esc_admin

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Erweitert

Gibt an, ob die Rolle eine erhöhte Rolle ist. Erhöhte Rollen werden Benutzern oder Gruppen nicht zugewiesen und müssen durch Erhöhung verwendet werden. Details finden Sie unter Auf eine privilegierte Rolle hochstufen.

Nein.

Besondere Erwägungen

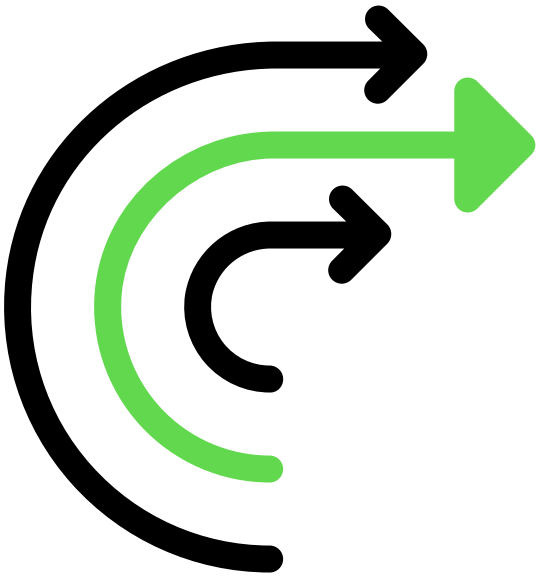
Keine.

Protokolle

Das Protokollmodul bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Ereignissen in der Instanz verwenden können.

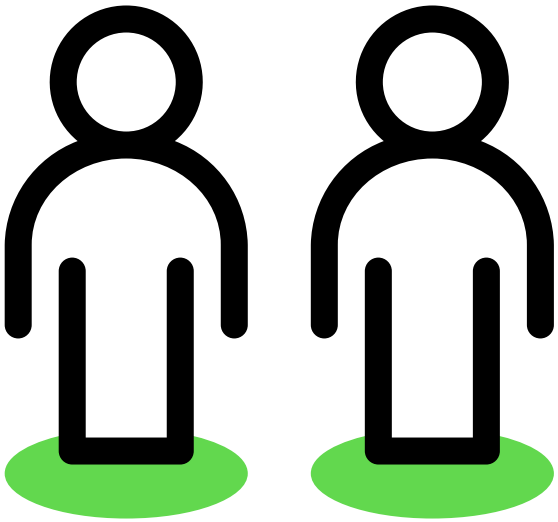
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemprotokolle



Das Modul „Systemprotokolle“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Ereignissen innerhalb der Instanz verwenden können.

Protokollierung, Audits und Fehler



Wenden Sie eine Protokollierungs- und Auditing-Strategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Systemprotokolle

Das Modul „Systemprotokolle“ bietet eine Vielzahl von Protokollen, die Sie zum Beheben und Debuggen von Transaktionen und Ereignissen innerhalb der Instanz verwenden können.

Greifen Sie über das Modul „Systemprotokolle“ auf die folgenden Protokolle zu:

Protokoll	Beschreibung
Transaktionen	Alle Anwendungsaktivitäten für eine Instanz.
E-Mail Und Veröffentlichen	Alle E-Mail-Benachrichtigungen und Push-Nachrichten, die von allen Instanzen im System gesendet werden.
Ereignisprotokolle	Alle Systemereignisse, die innerhalb des Systems auftreten.
Importieren	Datenimportaktivität innerhalb der Plattform.
Tabellenänderungen	Änderungen, die an allen Tabellen im System vorgenommen wurden.
Protokollierung für ausgehende Webservices	Alle ausgehenden Webserviceanforderungen wie REST- und SOAP-Anforderungen.
Signaturbilder	Elektronische Signaturen für das HR-Signaturpad.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokoll	Beschreibung
System	Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse, z. B. Arbeitsspeichernutzung auf dem Servercomputer.

Verwenden Sie Protokolldateibrowser Zum Durchsuchen und Herunterladen von Protokollen. Sie können auch archivierte Protokolle in durchsuchen Protokollverlauf .

Andere Protokolle

Ihre Instanz bietet zusätzlich zu den Protokollen im Modul „Systemprotokolle“ weitere Protokolle. Zum Beispiel die Systemdiagnosemodul Stellt Upgradeverlauf und Protokolle für langsame Abfragen bereit, mit denen Sie Einblicke in die Auswirkungen von Abfragen auf die Plattformleistung erhalten können. Die Tabelle „Kunden-Updates“ Zeichnet jede Änderung auf, die im System vorgenommen wird.

Systemprotokoll

Zeigen Sie Warnungen und Fehler für Instanzprozesse, Datensätze und nicht kritische Ereignisse an, z. B. Arbeitsspeichernutzung auf dem Servercomputer.

Die folgenden Informationen werden im Systemprotokoll nachverfolgt:

- Workflows
- Konfiguration
- Chats-Sitzungen
- Transaktionen für jede Ansicht jeder Seite im System, einschließlich Ladezeiten für Netzwerk, Server und Browser
- Eingehende und ausgehende E-Mail
- Im System ausgelöste Ereignisse
- Importe und Integrationen
- Systemwarnungen, Fehler und Skriptprotokolle
- Upgrade-Informationen für Plugin-Aktivierungen, Update-Sätze oder System-Upgrades

Protokolleinträge werden nur für den aktuellen Tag angezeigt. Um andere Protokolldateien anzuzeigen, verwenden Sie den Protokolldateibrowser. Dieses Protokoll enthält die folgenden Informationen für alle Vorkommen:

Systemprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Protokollierungsaktivität für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Ebene	Typ der Nachricht. Die Ebenen sind Debug, Fehler, Warnung und Informationen. • Eine Warnung ist ein Fehler, der behandelt und wiederhergestellt wurde. • Ein Fehler muss behoben werden.
Nachricht	Vom System generierte Nachricht zur Art des Vorkommens.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemprotokoll (Fortsetzung)

Feld	Beschreibung
Quelle	Name des Prozesses oder Bereichs, der vom Vorkommen betroffen ist. Beispielsweise kann die Quelle des Vorkommens E-MAIL oder Arbeitsspeicher sein.
Quellpaket	Name des Anwendungspakets, das dem Vorkommen zugeordnet ist. Klicken Sie auf den Namen, um den Datensatz der Store-Anwendung [sys_Store_App] für dieses Paket anzuzeigen.

Workflow-Protokollierung

- Jede ausgeführte Aktivität, einschließlich:
  - Datum und Uhrzeit des Starts
  - Datum und Uhrzeit des Endes
  - Status, z. B. „Fertig“, „Abgebrochen“, „Zeitüberschreitung“, Fehler
  - Ergebnis
  - Fehlerbeschreibung, wenn ein Fehler aufgetreten ist
- Übergangsverlauf, einschließlich:
  - Übergangszeit
  - Aktivität von übergegangen
  - Aktivität wurde auf übergegangen
  - Welcher Übergang ausgelöst wurde
- Workflow-Protokoll, einschließlich aller Protokollanweisungen, die dem Workflow hinzugefügt wurden

Konfigurationsinformationen

- Ausgeführte Aktion, einschließlich Einfügen, Aktualisieren und Löschen
- Kategorie des Change
- Mit dem Change aufgezeichnete Kommentare
- Name des Change
- XML-Unterschied des Change
- Update-Satz, dem der Change zugeordnet ist
- Datum und Uhrzeit des Change
- Anwender, der die Änderung vorgenommen hat
- Tabelle, in der die Änderung vorgenommen wurde
- Name des Objekts, das geändert wird
- Typ des Objekts, das geändert wird
- Zeigen Sie die Änderung an, die in vorgenommen wurde, für Änderungen an Formularen oder Listen an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transaktionsprotokolle

Das Transaktionsprotokoll zeichnet alle Browseraktivitäten für eine Instanz auf. Um das Debugging von Systemproblemen zu unterstützen, können Sie Transaktionsprotokolle nach Anwendungsbereich filtern und Transaktionen, die nur auf die Transaktionen angezeigt werden, die aus bestimmten Bereichen stammen, beschränken.

Greifen Sie auf die Transaktionsprotokolle zu, indem Sie zu navigieren **Alle** > **Systemprotokolle** > **Transaktionen**an. Das Transaktionsprotokoll enthält die folgenden Informationen für alle Aktivitäten.

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Anwendungsaktion für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Typ	Typ der aufgezeichneten Transaktion.
Erstellt von	Anwender, der diese Aktivität erstellt hat.
Ursprungsanwendung	Anwendungsbereich, aus dem die Transaktion stammt. Global wird angezeigt, wenn die Transaktion aus dem globalen Bereich stammt.
Antwortzeit	Round-Trip-Antwortzeit für die Anwendungsanforderung in Millisekunden.
Netzwerkzeit	Latenzzeit der Netzwerkantwort nach der Anforderung der Anwendung in Millisekunden.
Ausgabelänge	Größe der Ausgabezeichenfolge, die von der Instanz an die Anwendung gesendet wird, in Byte.
SQL-Anzahl	Anzahl der für diese Aktivität ausgeführten SQL Server-Befehle.
Business-Regel-Anzahl	Anzahl der für diese Aktivität ausgeführten Business-Regeln.
Business-Regel-Zeit	Verstrichene Zeit für die Ausführung der Business-Regeln für diese Aktivität.
URL	Anwendung oder Modul, die von der Client-Anwendung mit verbunden ist.
System-ID	Vom System generierter Bezeichner der Clientinstanz, die die Anforderung stellt. Diese ID wird für Clusterumgebungen verwendet, in denen mehrere Instanzen (Knoten) mit der Datenbank kommunizieren.
IP-Adresse	IP-Adresse des Clients, der die Anforderung stellt.
GZipped	Angabe, ob eine komprimierte Webseite von der Anwendung angefordert wurde.
Protokoll	HTTP-Protokoll, das von der Anwendung für diese Instanz verwendet wird.

Client-Transaktionszeiten

Das Plugin „Client-Transaktionszeiten“ verbessert die Systemprotokolle, indem zusätzliche Informationen zur Dauer der Transaktionen zwischen dem Client und dem Server bereitgestellt werden.

Sie können Leistungsprobleme bis zu ihrer Quelle nachverfolgen, indem Sie anzeigen, wo die Zeit verbraucht wird und wie die Zeit während einer Transaktion aufgewendet wurde.

Dieses Plugin erfordert Antwortzeitindikator Antwortzeitindikator Zu aktivieren und sammelt Informationen aus den folgenden Browsern:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Firefox
- Internet Explorer
- Chrome

Informationen Zu Client-Transaktionen

Durch die Installation des Plugins wird hinzugefügt *Client-Transaktionen* Modul zu *Systemprotokolle* Anwendung. Sie stellt eine Liste aller protokollierten Transaktionen zwischen Client und Server innerhalb des letzten Tages bereit:

Informationen Zu Client-Transaktionen

Feld	Beschreibung
Erstellt	Moment, in dem die Transaktion aufgezeichnet wurde.
Antwortzeit	Anzahl der ms, die der Server für die Ausführung der Transaktion ausgegeben hat.
Business-Regel-Zeit	Anzahl der ms, die von Geschäftsregeln ausgegeben wurden, die durch die Transaktion ausgelöst wurden.
SQL-Zeit	Anzahl der ms, die von der SQL-Datenbank ausgegeben werden.
Client-Antwortzeit	(Load_completion_time) – (Start_time). Dies ist einschließlich der Serverzeit.
Client-Netzwerkzeit	Anzahl der ms, die das Netzwerk ausgegeben hat, über das der Client eine Verbindung herstellt.
Browser-Zeit	Anzahl der ms, die der Browser während der Transaktion ausgegeben hat.
Clientskriptzeit	Die Anzahl der ms, die für die Ausführung von Client-Skripts aufgewendet wurden.
UI-Richtlinienzeit	Anzahl der ms, die für die Ausführung der ui-Richtlinie aufgewendet wurden.
Typ	Typ der Transaktion: • Formular • Liste • Sonstige
Tabelle	Name der angezeigten Tabelle. Beispiel: Incident, Change_Request.
Ansicht	Ansicht für dieses Formular/diese Liste.

Detaillierte Informationen Zum Client

Eine detailliertere Aufgliederung der Clientzeiten für alle Formularrenderings (aber nicht für Listen-Rendering) wird ebenfalls nachverfolgt. Um Details anzuzeigen, führen Sie einen Drilldown zu einem bestimmten Client-Transaktionsdatensatz durch, und beobachten Sie die zugehörige Liste am unteren Bildschirmrand.

Detaillierte Informationen Zum Client

Feld	Beschreibung
Reihenfolge	Reihenfolge während des Ladevorgangs, in dem dieser Vorgang aufgetreten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detaillierte Informationen Zum Client (Fortsetzung)

Feld	Beschreibung
Typ	Typ des Vorgangs.
Name	Beschreibender Name dieses bestimmten Vorgangs
Dauer	Anzahl der ms, die dieser Vorgang benötigt hat, um ihn abzuschließen.

Push-Protokolle

Lesen Sie das Push-Protokoll, um den Status von Push-Benachrichtigungen nachzuverfolgen, die in der Warteschlange zum Senden von Ihrem System stehen.

Navigieren Sie zum Anzeigen des Push-Protokolls zu **Systemprotokolle** > **Push-Benachrichtigungen**an. Anwender müssen über die Rolle Push_admin oder admin verfügen, um das Push-Protokoll anzuzeigen.

Push-Protokollfelder

Feld	Beschreibung
Anspruch	Identifikationsnummer, die von der geplanten Aufgabe generiert wird, die die Push-Benachrichtigung sendet. Diese Nummer wird auf angewendet **Anspruch** Feld, um die Konsistenz über mehrere geplante Push-Aufgaben hinweg sicherzustellen.
Nutzlast	Inhalt der Push-Benachrichtigung.
Anzahl Warteschlange	Gibt an, wie oft das System versucht hat, die Push-Benachrichtigung zu senden. Der Status der Push-Benachrichtigung bezieht sich auf die Anzahl der Warteschlangen. • Wenn die Warteschlangenanzahl länger als erwartet 0 ist, gibt es keine geplanten Aufgaben, die versuchen, die Push-Benachrichtigung zu senden. • Wenn die Warteschlangenanzahl größer als 0 und ist **Typ** Ist **Erfolg** , Dann können Sie daraus schließen, dass das System so oft versucht hat, die Push-Benachrichtigung zu senden, bevor es endgültig gesendet wurde. • Wenn die Warteschlangenanzahl 10 erreicht, versucht das System, die Push-Benachrichtigung zu senden. Die **Typ** Ändert sich in **Fehler** .
Anforderungs-ID	Eindeutige Identifikationsnummer für die Push-Benachrichtigung. Ähnlich wie die Nachrichten-ID für eine E-Mail wird die Anforderungs-ID als Korrelationstoken für die Push-Benachrichtigung verwendet.
Typ	Status, der angibt, ob die Push-Benachrichtigung gesendet wurde. Die Spalte „Typ“ kann folgende Werte haben: • **Fehler**: Die Nachricht konnte nicht gesendet werden. • **Ausstehend**: Die Nachricht wird zur Verarbeitung in die Warteschlange versetzt. • **Erfolg**: Die Nachricht wurde erfolgreich gesendet, obwohl sie nicht unbedingt vom mobilen Gerät empfangen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Geplante Aufgaben

System-E-Mail-Protokoll und Postfächer

Das System-E-Mail-Protokoll zeichnet alle E-Mails auf, die die Instanz erstellt oder empfängt. Systempostfächer sind gefilterte Ansichten dieses Protokolls.

Jede Benachrichtigungs-E-Mail, die die Instanz erstellt oder empfängt, wird in einem E-Mail-Datensatz [sys_email] aufgezeichnet. Sie können unter zu einem Protokoll dieser Datensätze navigieren **Systemprotokolle** > **E-Mails**an.

Die System-Postfächer sind gefilterte Ansichten der Tabelle „E-Mails“ [sys_email]. Die Instanz weist einem System-Postfach je nach Werten von einen E-Mail-Datensatz zu **Typ** Und **Status** Felder. Weitere Informationen finden Sie unter System-Postfächer .

Die folgenden Felder können in das Layout des Systemprotokolls und eines der System-Postfächer aufgenommen werden:

E-Mail-Protokoll

Feld	Beschreibung
Mailbox	Das System-Postfach, das diesen E-Mail-Datensatz auflistet. Die Instanz legt den Wert dieses Felds entsprechend den Werten von fest **Typ** Und **Status** Felder.
Status	Der aktuelle Status der E-Mail (Fehler, ignoriert, verarbeitet oder bereit).
Empfangstyp	Der Typ der eingehenden E-Mail (keine, Weiterleitung, Neu oder Antwort).
Typ	Der Status der E-Mail. Die Auswahlmöglichkeiten lauten wie folgt: • erhalten: Der Server hat diese E-Mail erhalten. • erhalten - ignoriert: Der Server hat diese E-Mail erhalten, sie wurde jedoch von der Instanz aufgrund von Aktionen bei eingehender E-Mail ignoriert. Normalerweise handelt es sich bei diesen E-Mails entweder um Spam oder um automatische Antworten. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - fehlgeschlagen: Der Server hat versucht, die E-Mail zu senden, und ist fehlgeschlagen. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - ignoriert: Der Server hat das Senden dieser E-Mail übersprungen. Normalerweise handelt es sich hierbei um eine E-Mail, die generiert wurde, jedoch keine Empfänger-E-Mail-Adresse hatte oder eine doppelte E-Mail ist. Weitere Informationen finden Sie im Feld „Fehlerzeichenfolge“. • senden - bereit: Die E-Mail kann gesendet werden, wurde jedoch vom Mail-Server nicht gesendet. Normalerweise bleibt eine E-Mail nur für kurze Zeit in diesem Status. • Senden – Übersetzung – bereit: Die E-Mail wird während der E-Mail-Übersetzung generiert und gesendet. Normalerweise bleibt eine E-Mail nur für kurze Zeit in diesem Status. • gesendet: Die E-Mail wurde von der Instanz ohne Fehler oder Probleme gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Protokoll (Fortsetzung)

Feld	Beschreibung
Zielvorgabe	Eine Dokument-ID-Referenz auf den Datensatz, wenn die E-Mail durch Einfügen, Aktualisieren oder Löschen eines bestimmten Datensatzes generiert wird.
Anwender	Der Name des Benutzers aus dem Benutzerdatensatz der Instanz, von der die E-Mail-Benachrichtigung gesendet wurde. **Hinweis:** Dies ist ein Zeichenfolgen-Feld.
Benachrichtigungstyp	Der Typ der Benachrichtigung. Die Auswahlmöglichkeiten lauten wie folgt: • Keiner • SMS • SMTP
UID	Die eindeutige ID der auf dem Server gespeicherten E-Mail.
Erstellt	Datum und Uhrzeit der E-Mail-Aktivität für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Gelöscht	Gibt für eingehende E-Mails an, ob die E-Mail vom E-Mail-Server gelöscht wurde.
Gewichtung	Die Gewichtung der E-Mail, die die Sendepriorität relativ zu anderen Benachrichtigungen in derselben Tabelle bestimmt.
Wichtigkeit	Ein Hinweis darauf, dass die E-Mail mit einem geänderten Wichtigkeitsgrad gesendet wurde, z. B. Dringend.
Auslösendes Ereignis und Benachrichtigung	Für E-Mails, die durch Benachrichtigungen generiert werden, eine eingebettete Liste, in der das Ereignis und die Benachrichtigung gespeichert werden, die die E-Mail erstellt haben.
Betreff	Der E-Mail-Betreff. Für Benachrichtigungen erstellen Sie den Betrefftext in **Systembenachrichtigung** > **E-Mail** > **Benachrichtigungen**an.
Fehlerzeichenfolge	Die vom E-Mail-Server erfasste Fehlerzeichenfolge, um festzustellen, warum die E-Mail nicht gesendet wurde. Dies wird nur protokolliert, wenn die E-Mail fehlgeschlagen ist.
Empfänger	Die E-Mail-Adressen der Empfänger.
Textkörper	Der Textkörper der E-Mail, der in unformatiertem HTML-Markup angezeigt wird. Verwenden Sie den zugehörigen Link „HTML-Textvorschau“, um den Nachrichtentext als gerenderten HTML-Code anzuzeigen.
Content Typ	Der E-Mail-Content Typ
Kopfzeilen	Alle in die E-Mail eingebetteten Kopfzeilen.

Ereignisprotokolle

Das Ereignisprotokoll zeichnet alle Systemereignisse auf, die innerhalb des auftreten ServiceNow AI Platform.

Dieses Protokoll enthält die folgenden Informationen für alle auftretenden Ereignisse:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignisprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit des Ereignisses für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Name	Name des Ereignisses, wie in der Ereignisregistrierung aufgeführt.
URI	HTTP-Abfrage, die das Ereignis generiert hat.
Parm1	Ereignisspezifischer Wert, der vom Ereignis und dem Empfänger abhängt.
Parm2	Ereignisspezifischer Wert, der vom Ereignis und dem Empfänger abhängt.
Tabelle	Datenbanktabelle wurde für dieses Ereignis aktiviert.
Verarbeitet	Datum und Uhrzeit des Beginns der Verarbeitung des Ereignisses. Diese Zeit spiegelt das Gebietsschema des Computers wider, auf dem die Instanz ausgeführt wird.
Verarbeitungsdauer	Zeit, die für die Verarbeitung dieses Ereignisses benötigt wurde, in Millisekunden.
Warteschlange	Name der Prozessorwarteschlange.

Importprotokolle

Das Importprotokoll zeigt Informationen zu Datenimportaktivitäten innerhalb der Plattform in einem ausführlichen Format an.

Eine detailliertere Ansicht der Importsätze, die ein bestimmtes Protokoll erstellt haben, finden Sie unter **Importsätze** > **Verlauf umwandeln**an.

Dieses Protokoll enthält die folgenden Informationen für alle Importe:

Importprotokoll

Feld	Beschreibung
Erstellt	Datum und Uhrzeit des Imports für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Ebene	Typ der angezeigten Nachricht. Für Importdateien ist die Ebene „Informationen“.
Nachricht	Vom System generierte Nachricht zum Status des Imports.
Quelle	Name der externen Quelle des Imports, z. B. eine Integration.

Systemdiagnosemodul

Die Anwendung Systemdiagnose stellt Protokolle bereit, die sich auf die Plattform beziehen.

Diese Protokolle sind verfügbar:

Upgradeverlauf

Verfolgt jedes Upgrade auf eine Instanz.

Langsame Abfragen

Bietet Einblicke in die Auswirkungen von Abfragen auf die Plattformleistung. Siehe Verwenden Sie ein langsames Abfrageprotokoll .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Kunden-Updates“

Im System vorgenommene Änderungen werden in den Kunden-Updates aufgezeichnet [sys_Update_xml] Tabelle chronologisch. Es gibt einige Ausnahmen, wie unten angegeben.

Um zu dieser Tabelle zu navigieren, geben Sie ein `sys_Update_xml.list` In den Navigationsfilter. Informationen zu Update-Sätzen finden Sie unter System-Update-Sätze .

Zu jedem Update werden die folgenden Informationen gespeichert:

Tabelle „Kunden-Updates“

Feld	Beschreibung
Name	Ein Name, der den aktualisierten Datensatz identifiziert.
Erstellt	Datum und Uhrzeit der Erstellung des Kunden-Update-Datensatzes.
Erstellt von	Der Anwender, der den Change durchgeführt hat.
Typ	Der Typ des Updates.
Aktualisiert	Datum und Uhrzeit der Aktualisierung des Kunden-Update-Datensatzes.
Aktualisiert von	Der Anwender, der die Aktualisierung durchgeführt hat.
FTP-Anwendernamen	Die Anzahl der Aktualisierungen des Datensatzes.
Zielname	Der Name des geänderten Elements.
Ansicht	Die Ansicht des Formulars, das geändert wurde, wenn es sich um eine Formularlayoutänderung handelte.
Nutzlast	Der XML-Inhalt des Datensatzes nach der Änderung.
Remote-Update-Satz	Ein Verweis auf diesen Update-Satz, wenn der Change von einem Remote-Update-Satz ausgeführt wurde.
Lokaler Update-Satz	Der Update-Satz, dem der Change zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Einige Anwendungsänderungen werden nicht durch Kundenaktualisierungsdatensätze (sys_Update_xml) dargestellt. Beispiele:

- Typen von Metadaten, bei denen updateSynch = falsch ist
- Kaskadierende Änderungen an Tabellen und Feldern, z. B. Änderungen des Anzeigenamens
- Ungelöste Metadatenreferenzen aus anderen Anwendungen (was zu keinem „Anzeigewert“ für das Element führt)
- sys_ID-Änderungen für Zusammenfügungen von Dateien
- Änderungen an Flow-/Flow-Aktionen, die „sys_documentation“ generieren können
- ua_table_license_config-Datensätze, die bei der Tabellenerstellung generiert wurden
- Aufträge, die im Hintergrund ausgeführt werden, z. B. Verarbeitung natürlicher Sprache
- Fälle, in denen sys_Update_xml manuell geändert oder entfernt wird

Weitere Informationen finden Sie unter Commit-Changes .

Protokollverlauf

Das System verwendet Tabellenrotation und Tabellenerweiterung, um ältere Protokolle zu archivieren.

Standardmäßig verwendet das System den folgenden Zeitplan, um allgemeine Protokolle zu archivieren:

Allgemeiner Protokollarchivierungszeitplan

Tabelle	Zeitplan archivieren	Rotationen	Typ
Ereignis [ecc_event]	Jeden Tag	7	Rotation
Warteschlange [ecc_Queue]	Jeden Tag	7	Rotation
Ereignis [sysevent]	Jeden Tag	7	Rotation
Protokoll [syslog]	Jede #Woche	8	Rotation
Transaktionsprotokoll [syslog_transaction]	Jede #Woche	8	Rotation
E-Mail [sys_email]	Alle 30 Tage	8	Erweiterung

Verwenden Sie den Protokolldateibrowser

Die Instanz stellt den Dienstprogramme-Protokolldateibrowser und den Protokolldateidownload bereit.

Verwenden **Systemprotokolle** > **Dienstprogramme** > **Knoten-Protokolldateibrowser** Zum Anzeigen eines Systemprotokolleintrags. Sie können mit den folgenden Filtern nach Protokolldateien suchen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokolldateibrowser

Feld	Beschreibung
Startzeit	Startdatum und -Uhrzeit des Bereichs, den Sie durchsuchen möchten, für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Sitzungs-ID	Vom System generierte Hexadezimalzeichenfolge, die die Sitzung identifiziert, die den Protokolleintrag generiert hat.
Endzeit	Enddatum und -Uhrzeit des Bereichs, den Sie durchsuchen möchten, für das Gebietsschema des Computers, auf dem die Instanz ausgeführt wird.
Nachricht	Vom System generierte Beschreibung des Vorkommens.
Ebene	Typ der angezeigten Nachricht. Die Ebenen sind Debug, Fehler, Warnung und Informationen. Eine Warnung ist ein Fehler, der behandelt und wiederhergestellt wurde. Ein Fehler muss behoben werden.
Thread-Name	Vom System generierter Bezeichner des Threads, der die Protokolldatei erstellt hat.
Maximale Zeilen	Maximale Anzahl von Datensätzen, die für einen bestimmten Filter zurückgegeben werden.

Die Instanz erstellt alle 2 Tage komprimierte Archive von Systemprotokollen und löscht Protokollarchive nach 21 Tagen.

Wichtig: Wenn ein Knoten stillgelegt wird, werden die Protokolldateien des Knotens sofort gelöscht, was bedeutet, dass sie für weitere 21 Tage nicht archiviert werden.

Sie können Protokolldateiarchive herunterladen und mit anzeigen **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**an. Wählen Sie ein Protokollarchiv aus der Liste aus, und klicken Sie dann auf **Protokoll herunterladen** Unter *Zugehörige Links* Zum Öffnen oder Speichern des Archivs.

Hinweis: Protokolldateien sind nur für den Knoten verfügbar, bei dem Sie sich derzeit angemeldet haben. Um den derzeit angemeldeten Knoten anzuzeigen, navigieren Sie zu **Systemdiagnostik** > **Statistiken**an.

Verwenden Sie die neue **Syslog-Datensätze Anzeigen** Schaltfläche in den Formularen „Transaktion“ und „aktive Transaktion“, um Systemprotokolleinträge anzuzeigen, die während der Ausführung der Transaktion generiert wurden. Eine Transaktion kann eine beliebige Anzahl von Syslog-Einträgen haben. Die mehreren Syslog-Einträge für alle Transaktionen erschweren die Verknüpfung einer Transaktion mit ihren jeweiligen Syslog-Einträgen. Die **Syslog-Datensätze Anzeigen** Die UI-Aktion hilft bei der Verknüpfung der aktiven und abgeschlossenen Transaktionen mit ihren jeweiligen Syslog-Einträgen, indem eine URL zum Abfragen der Syslog-Tabelle erstellt wird. Die Identifizierung der richtigen Syslog-Einträge für eine bestimmte Transaktion hilft beim Debugging und bei der Behebung von Sicherheitsbedenken.

Verbesserte Protokollierungssicherheit

Erkunden Sie **Zuordnung** Feld in den Knotenprotokollzeilen, um das Skript oder die Komponente zu identifizieren, das die Protokollnachricht generiert hat. Transaktionsstartzeilen enthalten das neue Feld, um den Typ der gestellten Anforderung zu identifizieren.

Mit den neuen Erweiterungen können Sie Folgendes erreichen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verfolgen Sie den Quell-Urheber jeder Protokollzeile
- Wenn die Informationen zum Urheber nicht verfügbar sind, drucken Sie den Java-Klassennamen und eine Zuordnung aus
- Zu Beginn jeder Transaktionsposition enthält sie die Transaktions-ID und den Transaktionstyp

Verwenden Sie die Transaktions-ID jeder Protokollzeile, um die in jeder Protokollzeile angegebenen Informationen zu verstehen. Sobald Sie den Transaktionstyp identifiziert haben, erhalten Sie die Informationen zum Urheber jeder Protokollzeile. Sowohl der Transaktionstyp als auch der Urheber Informationen Von jeder Protokollzeile zusammen erhalten Sie die erforderlichen Quellinformationen für jede Knotenprotokollzeile.

Hinweis: Die Skripttypen „SYS_UI_MACRO“ und „SERVICE_PORTAL_WIDGET“ in der Attribution werden nicht gemeldet.

Transaktionstypen

Im Folgenden finden Sie die Liste der Transaktionstypen:

- Liste
- Formular
- XMLHttp
- Bericht
- SOAP
- Exportieren
- Zeitplaner
- Textsuche
- Sonstige
- REST
- JSON
- AMB
- Archiv
- Batch-REST
- Instanz-Scan

Systemeigenschaften

Die folgenden Systemeigenschaften sind für die Funktion erforderlich:

- Glide.log.append.Attribution : Diese Eigenschaft ist standardmäßig aktiviert. Aktiviert/deaktiviert die Attributionsinformationen jeder Knotenzeile
- Glide.DB.log.append.classname.Attribution : Diese Eigenschaft ist standardmäßig aktiviert. Aktiviert/deaktiviert die Protokollierung der Java-Klassennamen-Attribution

Vermeiden Sie Protokollmanipulationen

Konfigurieren Sie Schutzregeln für Systemprotokolltabellen, um den Umfang der Änderung und Löschung von Anwendungsprotokolldatensätzen einzuschränken. Mit den Regeln

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können Sie die Protokollierung von Changes oder Änderungsversuchen in diesen Tabellen bestimmen.

Wenn Sie ein Security_admin sind, aktivieren Sie das Plugin „geschützte Tabellen“ (com.glide.protected_tables), mit dem die Plattform Vorgänge zum Aktualisieren, Einfügen und Löschen für die folgenden Systemprotokolltabellen einschränken kann:

- syslog
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_Push_Notification
- syslog_app_scope
- Protected_table_Configuration (Konfiguration nicht änderbar)

Hinweis: Das Plugin com.glide.protected_tables bietet nur Schutz für die oben genannten Systemprotokolltabellen. Jeder Versuch, einen Datensatz zu aktualisieren, einzufügen oder zu löschen, protokolliert eine Nachricht in der Tabelle protected_table_log.

Siehe Installieren und Konfigurieren des Plugins „Protokollschutz“ Für weitere Details.

Sie können eine der folgenden Protokollschutzstufen für jede der Systemprotokolltabellen angeben.

- Versuch blockieren und protokollieren: Blockiert Änderungen und protokolliert den Versuch
- Nur den Versuch blockieren: Blockiert jede Änderung und protokolliert den Versuch nicht
- Nur den Versuch protokollieren: Blockiert die Änderung nicht, protokolliert den Versuch jedoch
- Versuch nicht blockieren und nicht protokollieren: Blockiert die Änderung nicht und protokolliert den Versuch nicht

Die Plattform verwendet die für jede der Systemprotokolltabellen angegebenen Protokollschutzstufen, um Versuche zum Ändern eines Datensatzes nach der anfänglichen Erstellung zu blockieren und/oder zu protokollieren.

Hinweis: Wenn Sie ein Security_admin sind, können Sie die standardmäßigen Protokollschutzstufen in jeder der Systemprotokolltabellen überschreiben, um sich an die Anpassungen in Ihrer Instanz anzupassen.

Wenn versucht wurde, die Systemprotokolltabellen zu ändern, werden sie in der Tabelle protected_table_log angemeldet.

Hinweis: Wenn die Schutzstufe für eine Tabelle nicht angegeben ist, werden alle Änderungsversuche nicht in der Tabelle protected_table_log protokolliert.

Um die Plugin-Vorgänge für Tabellen im Administratorbereich zu deaktivieren, legen Sie die Eigenschaft com.glide.security.protected_table.enabled auf „falsch“ fest. Siehe Protokollschutzeigenschaft erstellen Weitere Informationen finden Sie unter .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren des Plugins „Protokollschutz“

Konfigurieren Sie die Schutzregeln für jede Tabelle und jeden Vorgang, um die Konfiguration des Protokollschutz-Plugins abzuschließen.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Geschützte Tabellen** > **Protokollschutz**an.
   Die Seite Administratorbereich wird angezeigt.

   Hinweis: Startet in Utah Release: Das Plugin „geschützte Tabellen“ ist standardmäßig installiert, aber deaktiviert.

2. Erhöhen Sie Ihre Rolle auf Security_admin, um mit der Konfiguration des Plugins fortzufahren.

   a. Wählen Sie Aus **Systemadministrator** .

   b. Wählen Sie Aus **Erhöhen Sie die Rolle** .
   Das modale Element „Rolle erhöhen“ wird angezeigt.

   c. Wählen Sie die Option Security_admin aus, um Ihre Rolle zu erhöhen, und wählen Sie aus **Aktualisieren** .

3. Konfigurieren Sie die Schutzregeln für jede Tabelle und jeden Vorgang. Die Schutzregeln gelten für das Aktualisieren, Einfügen und Löschen. Die Schutzstufen können für einige Tabellen nicht geändert werden. Die Tabellen „syslog“ und „syslog_App_scope“ haben feste Werte für den Update- und Löschschutz. Die Tabelle protected_table_Configuration hat feste Schutzwerte für alle drei Vorgänge.

   Hinweis: Für die sysevent-Tabelle können Einfügungsschutzmaßnahmen nicht auf „Blockieren“ festgelegt werden.

   Wenn Sie hatten **Auf untergeordnete Tabellen anwenden** Wenn im vorherigen Release für syslog aktiviert, werden die untergeordneten Tabellen dem Protokollschutz mit den gleichen Schutzregeln wie syslog beim Upgrade auf hinzugefügt Utah Release. Dies geschieht nur für Syslog, nicht für andere Tabellen.

4. Aktivieren Sie die Funktion, indem Sie auswählen **Aktivieren Sie Den Protokollschutz** Umschalter.

   Hinweis: Sie können dieses Plugin nur deaktivieren, indem Sie die Eigenschaft com.glide.security.protected_table.enabled in der Tabelle „sys_properties“ ändern.

Protokollschutzeigenschaft erstellen

Erstellen Sie eine Protokollschutzeigenschaft, um das Risiko von Protokollmanipulationen zu vermeiden.

Vorbereitungen
Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn `com.glide.security.protected_table.enabled`Eigenschaft ist in der Liste „Systemeigenschaften“ nicht vorhanden. Wählen Sie aus **Neu** .
   Das neue Formular für die Systemeigenschaft wird angezeigt.
2. Geben Sie die Details im Formular ein

Felder	Beschreibung
Name	Name der Eigenschaft als com.glide.security.protected_table.enabled
Anwendung	Anwendung mit der Eigenschaft.
Beschreibung	Beschreibung der Eigenschaft
Auswahlmöglichkeiten	
Typ	Werttyp: „Wahr“ oder „falsch“
Wert	Ist-Wert der Eigenschaft
Cache ignorieren	Option zum Ignorieren des Cache-Inhalts
Privat	Option, um die Eigenschaft privat zu machen ○ Leserollen ○ Schreibrollen

3. Wählen Sie Aus **Übermitteln** Um die Eigenschaft zu erstellen.

Protokollierung, Auditing und Fehler (Instanzsicherheitshärtung)

Wenden Sie eine Protokollierungs- und Auditing-Strategie an, damit Sie verdächtige Aktivitäten rechtzeitig erkennen und darauf reagieren können.

Weitere Informationen darüber, was in der Instanz protokolliert werden kann, finden Sie unter Systemprotokolle. Stellen Sie sicher, dass ein Zeitplan für die Überwachung von Systemereignissen wie Anmeldungen und fehlgeschlagenen Anmeldungen vorhanden ist, indem Sie verwenden **Systemprotokolle** > **Ereignisse**an.

SQL-Fehlermeldungen deaktivieren (Instanzsicherheitshärtung)

Verwenden Sie `glide.db.loguser`Eigenschaft zum Deaktivieren des Renderings von SQL-Fehlermeldungen in einem Browser.

Weitere Informationen

Attribut	Beschreibung
Eigenschaftsname	glide.db.loguser
Konfigurationstyp	Systemeigenschaften (/sys_properties_list.do)
Konfigurierbar im Instanz-Sicherheitszentrum	Nein
Zweck	Dient zum Deaktivieren der Anzeige von SQL-Fehlermeldungen im Browser.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
Typ	Wahr|Falsch
Empfohlener Wert	falsch
Funktionale Auswirkung	(Niedrig) diese Korrektur deaktiviert das Rendern von SQL-Fehlermeldungen. Es gibt keine Auswirkungen auf eine Funktionalität.
Sicherheitsrisiko	(Mittel) auf einer Webseite sollten keine vertraulichen SQL-Informationen angezeigt werden, die einem Angreifer helfen könnten.

Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Geheimnisverwaltung

Verwenden ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter, die Ihren Geschäftsanforderungen entspricht.

Wichtig:

Geheimnismanagement hat seinen Prozess am Ende der Lebensdauer begonnen und hat ab dem Yokohama-Release die Meilensteine für das Ende des Verkaufs und das Ende der Verlängerung erreicht. Informationen zum Speichern von Passwörtern mit bidirektionaler Verschlüsselung finden Sie unter Passwort2-Verschlüsselung mit Key Management Framework (KMF).

Geheimnisverwaltung hat zwei verfügbare Versionen. Secrets Management Core ist ohne zusätzliche Kosten auf der ServiceNow-Plattform enthalten, und Secrets Management Enterprise ist eine Premium-Abonnementversion des Produkts. Weitere Informationen zum Unterschied zwischen diesen Versionen finden Sie unter Geheimnisverwaltung Erkunden.

Untersuchen



Analysieren



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie mehr über die wichtigsten Funktionen und den Geschäftsnutzen von Geheimnisverwaltung.	Erfahren Sie mehr über das Dashboard „Geheimnisverwaltung“.
Konfigurieren  Planen Sie Ihre Kernkonfigurationen.	

Geheimnisverwaltung Erkunden

Verwenden ServiceNow Geheimnisverwaltung für eine granulare Verwaltung des Zugriffs auf Ihre Passwörter, die Ihren Geschäftsanforderungen entspricht.

Wichtig: Administratoren müssen die Rolle haben, um Module und Datensätze im Zusammenhang mit der Geheimnisverwaltung anzuzeigen. Informationen zu Geheimnisverwaltungsrollen finden Sie unter Geheimnisverwaltungsrollen.

Wählen Sie aus Core- und Enterprise-Versionen von Geheimnisverwaltung aus

Wählen Sie je nach Geschäftsanforderungen zwischen Geheimnismanagement Core und Geheimnismanagement Enterprise aus.

Das Plugin „Secret Management Core“ (com.Glide.sm.Core) ist standardmäßig verfügbar. Für die Instanz ist keine Installation zur Verwendung erforderlich. Das Plugin „Secret Management Enterprise“ ist nur mit verfügbar ServiceNow Vault v1, PROD18537-Lizenz. Wenden Sie sich an den Kundensupport, um Hilfe zum Plugin „Secret Management Enterprise“ zu erhalten.

Geheimnisverwaltung Core	Geheimnisverwaltung Enterprise
Secrets Management Core kann ohne zusätzliche Kosten auf Ihrer Instanz installiert werden. Das Plugin bietet die Möglichkeit, Geheimnisgruppen mit	Geheimnisverwaltung Enterprise enthält zusätzliche Funktionen, mit denen Administratoren Geheimnisgruppen erstellen und verwalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geheimnisverwaltung Core	Geheimnisverwaltung Enterprise
Kriterien in nicht anwenderdefinierten Tabellen zu verwenden, die in bereitgestellt werden ServiceNow Plattform, die von erstellt wurde ServiceNow Anwendungs-Engineering-Teams.	können. Enterprise bietet zusätzlich zu den in Core aufgeführten Funktionen die folgenden Funktionen. • Verwenden Sie granulare Zugriffssteuerungen, um Geheimnisgruppen basierend auf einem dieser Kriterien zu erstellen. ◦ Umfang ◦ Tabelle ◦ Spalte ◦ Datensatz • Erstellen Sie für den Client zugängliche Geheimnisse, die mit Ihrem eigenen Schlüssel verschlüsselt werden ServiceNow Zugriff nicht möglich. • Verwenden Sie das Geheimnismanagement-Dashboard, um die in Ihrer Instanz konfigurierten Geheimnisgruppen zu überprüfen und Informationen zu potenziellen Sicherheitsproblemen zu erhalten. **Hinweis:** Secrets Management Enterprise ist ein bezahltes Plugin, das ServiceNow Mitarbeiter müssen in Ihrer Produktionsinstanz aktivieren.

Verwenden Sie geheime Gruppen, um Ihre Geheimnisse zu organisieren

Verwenden Sie Geheimnisverwaltung, um Ihre Geheimnisse in Gruppen zu organisieren, und wenden Sie dann Zugriffsrichtlinien auf diese Geheimnisse auf Gruppenebene an.

Grundlegende geheime Gruppe

Diese Gruppen gelten für alle Geheimnisse in einem Bereich. Diese Geheimnisse werden durch ein gängiges kryptografisches Modul und Modulzugriffsrichtlinien entschlüsselt.

Geheime Gruppe mit Kriterien

Geheime Gruppen mit Kriterien funktionieren wie eine grundlegende geheime Gruppe, verfeinern jedoch mithilfe von Kriterien, was enthalten ist. Diese Kriterien umfassen:

- Anwendungsbereich
- Paket
- Tabelle
- Geheime Spalte
- Filterdatensatz

Geheime Gruppen des Typs können auf Instanz oder Client zugänglich gemacht werden.

Instanzseitige Geheimnisgruppen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanzseitige Geheimnisgruppen enthalten Geheimnisse, die von Ihrer Instanz entschlüsselt werden können.

Clientseitige geheime Gruppen

Clientseitige Geheimnisgruppen verwenden ein öffentliches und privates Schlüsselpaar, um sicherzustellen, dass Geheimnisse nur vom Client entschlüsselt werden können. Wenn Sie eine vom Client zugängliche Geheimnisgruppe erstellen, laden Sie den öffentlichen Schlüssel in die Instanz hoch und behalten den privaten Schlüssel auf Ihrem MID-Server bei. Die Instanz verwendet den öffentlichen Schlüssel, um Ihre Geheimnisse zu verschlüsseln, kann jedoch nur mit dem privaten Schlüssel entschlüsselt werden.

Hinweis: Weitere Informationen zu diesen Gruppentypen finden Sie unter Client-Seite verstehen Geheimnisverwaltung.

Verwenden Sie Geheimnisgruppen für eine detailliertere Steuerung

Während Passwort2 auf verfügbar ist ServiceNow Die Plattform „Geheimnisverwaltung“ bietet diese zusätzlichen Funktionen.

Granulare Zugriffssteuerungen	**Passwort2** Mit Passwort2 können Administratoren den Zugriff auf einen Anwendungsbereich steuern, den Zugriff jedoch nicht auf Elemente innerhalb des Bereichs beschränken. **Geheimnisverwaltung** Mit Geheimnisverwaltung können Administratoren den Zugriff basierend auf von ihnen definierten Kriterien einschränken. Kriterientypen können auf Kriterien wie Paket, Tabelle oder Spalte basieren.
Sicherer Speicher	Für clientseitige Geheimnisgruppen verwendet die Geheimnisverwaltung ein neues Verschlüsselungsschema. In diesem Verschlüsselungsschema ServiceNow Speichert den Verschlüsselungsschlüssel nicht. Aus diesem Grund hängt die Sicherheit Ihrer Daten nicht von ab ServiceNow Sicherheit.

Wenden Sie Modulzugriffsrichtlinien auf Ihre Gruppen an

Nachdem Sie Ihre Geheimnisse in eine geheime Gruppe gruppiert haben, können Sie Richtlinien anwenden, die festlegen, wie Sie auf Gruppenebene darauf zugreifen können. Modulzugriffsrichtlinien sind die Zugriffssteuerungsmechanismen, die Sie auf kryptografische Module anwenden, um Steuerungen auf Instanzebene zu definieren, z. B. einen Gültigkeitszeitrahmen für den kryptografischen Schlüssel. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über die Modulzugriffsrichtlinie .

Mit Geheimnisverwaltung installierte Tabellen

Geheimnisverwaltung fügt diese Tabellen hinzu oder ändert sie.

Neue Tabellen	
[sn_sm_Secret_Group]	Speichert geheime Gruppen
[sn_sm_Secret_Group_Criteria]	Speichert geheime Kriteriengruppen
[sn_sm_Secret]	Speichert umschlossene Geheimnisse

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[sn_sm_Identity_Group]	Definiert die Identitätsgruppe für die Zuordnung einer Gruppe von Identitäten zum öffentlichen Schlüssel
[sys_kmf_Wrapped_Module_key]	Speichert die umschlossenen symmetrischen kryptografischen Schlüssel
Geänderte Tabellen	
[sys_kmf_Crypto_Module]	Kryptografischer Modultyp hinzugefügt. (Kryptografisches Identitätsmodul oder kryptografisches Modul der Geheimnisgruppe)
[sys_kmf_Module_key]	• Speichert den konzeptionellen geheimen Verschlüsselungsschlüssel (ohne Schlüsselmaterial) • Speichert den öffentlichen Identitätsschlüssel
[sys_kmf_Crypto_caller_Policy]	Neuer Modulzugriffsrichtlinientyp hinzugefügt

Anwendungsfallbeispiele für Geheimnisverwaltung

Tragen Sie dazu bei, die ITOM-Discovery zu sichern

Diese Infografik zeigt eine vereinfachte Referenzarchitektur von wie ServiceNow Die Discovery von IT Operations Management (ITOM) kann von Ihrer Organisation bereitgestellt werden. Wie in der Infografik gezeigt, werden mehrere Windows- und Linux-Server mit dem MID-Server (Management, Instrumentation, and Discovery) verbunden, und mehrere MID-Server-Agents ermöglichen den Discovery-Prozess, die Configuration Management Database (CMDB) zu aktualisieren. Jede MID-Server-Transaktion erfordert eine sichere Authentifizierung. Daher ist die Verwaltung der Authentifizierungsanmeldeinformationen aus sicherheitstechnischer Sicht von entscheidender Bedeutung.

Sichere Beschleunigung der Workflow-Konnektivität mit Integration Hub

Verwenden ServiceNow Integration Hub von für die Verbindung mit verschiedenen Systemen über die automatisierte Anwendungsprogrammierschnittstelle (APIs). Jedes Mal, wenn Integration Hub über eine API eine Verbindung zu einem System herstellt, sind Anmeldeinformationen zur Authentifizierung erforderlich, um die Konnektivität herzustellen. Die Verwaltung einer Vielzahl von Anwendungen und APIs für Konnektivität erfordert eine Lösung zur Geheimnisverwaltung.

Geheimnisverwaltung ist ein wichtiger Teil der Gewährleistung der Cybersicherheit Ihrer Organisation. Sie deckt alle Prozesse und Tools im Zusammenhang mit der Erstellung, Speicherung, Übertragung und Verwaltung digitaler Anmeldeinformationen wie Verschlüsselungsschlüssel, API-Token und Passwörter ab. Um Geheimnisse sowohl sicher als auch effektiv zu verwalten, können Sie eine Core Secret Management-Richtlinie erstellen, die Standardregeln und -Verfahren für alle Phasen des Lebenszyklus eines Geheimnisses festlegt.

Client-Seite verstehen Geheimnisverwaltung

Erfahren Sie, wie Sie verwenden Geheimnisverwaltung Dient zum Verwalten des Zugriffs auf Geheimnisse und Gruppen.

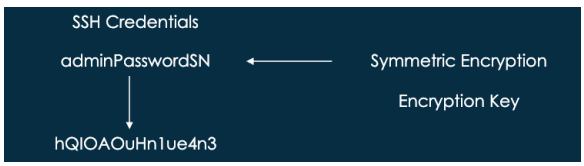
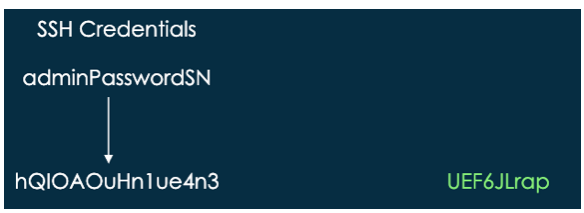
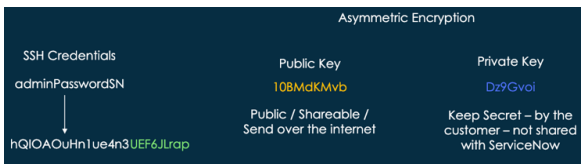
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Terminologie

Die Verwaltung clientseitiger Geheimnisse bietet eine Methode zum Verwalten von Geheimnissen ohne Proxys und ohne Angabe ServiceNow Zugriff auf Ihre entschlüsselten Daten. Um diesen Prozess zu verstehen, beginnen Sie mit den folgenden Verschlüsselungsbegriffen.

Benennung	Beschreibung
Symmetrische Verschlüsselung	Bei der symmetrischen Verschlüsselung wird ein einzelner Schlüssel zum Verschlüsseln und Entschlüsseln von Daten verwendet. Wenn Daten mit einem symmetrischen Schlüssel verschlüsselt werden, ist dieser Schlüssel alles, was zum Entschlüsseln erforderlich ist.
Symmetrischer Schlüssel	Der symmetrische Schlüssel verschlüsselt ein Geheimnis und verwandelt Ihr Klartextpasswort in unlesbaren Kryphertext.
Asymmetrische Verschlüsselung	Die asymmetrische Verschlüsselung verwendet zwei Schlüssel, einen zum Verschlüsseln und den anderen zum Entschlüsseln.
Öffentlicher Schlüssel	Der öffentliche Schlüssel ist eine Hälfte des asymmetrischen Schlüsselpaars. Dieser Schlüssel wird in Ihrer Instanz gespeichert, die den Schlüssel zum Verschlüsseln eines symmetrischen Schlüssels verwendet. Dieser verschlüsselte symmetrische Schlüssel kann nur entschlüsselt werden, wenn er mit dem privaten Schlüssel gekoppelt ist.
Privater Schlüssel	Der private Schlüssel ist eine Hälfte des asymmetrischen Schlüsselpaars. Dieser Schlüssel wird in einem Schlüsselspeicher auf Ihrem MID-Server gespeichert. ServiceNow Hat keinen Zugriff auf diesen Schlüssel. In Kombination mit dem öffentlichen Schlüssel wird das asymmetrische Schlüsselpaar verwendet, um Ihre Geheimnisse zu entschlüsseln.

Clientseitiger Verschlüsselungsprozess

Ein symmetrischer Schlüssel verschlüsselt Anmeldeinformationen (in diesem Fall ein Administratorpasswort) und ändert sie von lesbarem Klartext in verschlüsselten Kryphertext.	
Der symmetrische Schlüssel (grün dargestellt) kann auf die Anmeldeinformationen angewendet werden, um sie zu verschlüsseln oder zu entschlüsseln.	
Zu diesem Zeitpunkt beginnt die asymmetrische Verschlüsselung mit öffentlichen (gelben) und privaten (blauen) Schlüsseln.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der öffentliche Schlüssel verschlüsselt die Anmeldeinformationen zusammen mit dem symmetrischen Schlüssel. Der symmetrische Schlüssel ist jetzt geschützt und kann daher nicht zum Entschlüsseln der Anmeldeinformationen verwendet werden. Obwohl der öffentliche Schlüssel diese Verschlüsselung ausführen kann, kann er nicht allein zum Entschlüsseln verwendet werden.



Nach der Verschlüsselung mit dem öffentlichen Schlüssel wird der private Schlüssel zum Entschlüsseln der Anmeldeinformationen benötigt. Da der Kunde nur über diesen Schlüssel verfügt, sind er die einzigen, die auf die verschlüsselten Anmeldeinformationen zugreifen können.



Vom Client zugängliche Geheimnisse konfigurieren

Erfahren Sie, wie Sie Ihre Instanz so konfigurieren, dass vom Client zugängliche Geheimnisse verwendet werden.

Verwenden Sie diese Beispielimplementierung zum Konfigurieren Geheimnisverwaltung Ohne Proxys oder Geben ServiceNow Zugriff auf Ihre entschlüsselten Daten.

Weitere Informationen zur Verwendung von clientseitig Geheimnisverwaltung Informationen zum Verwalten des Zugriffs auf Passwörter und Gruppen finden Sie unter Client-Seite verstehen Geheimnisverwaltung.

Diese Anweisungen gehen davon aus, dass in Ihrem lokalen Netzwerk ein MID-Server konfiguriert ist. Informationen zu diesem Prozess finden Sie unter MID-Server .

Prozessübersicht

1. **Erstellen Sie Verschlüsselungsschlüssel und Zertifikat**

   Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat mithilfe von Terminalbefehlen in Ihrer lokalen Umgebung.

2. **Fügen Sie Ihr Zertifikat dem Trusted Key Store von ServiceNow hinzu**

   Laden Sie Ihren Schlüssel und Ihr Zertifikat in hoch ServiceNow Vertrauenswürdiger Schlüsselspeicher.

3. **Erstellen Sie eine geheime Gruppe mit Kriterien**

   Erstellen Sie eine Gruppe für Ihre Geheimnisse. Geheime Gruppen, um Ihre Geheimnisse in Gruppen zu organisieren. Mit diesen Gruppen können Sie Zugriffsrichtlinien auf diese Geheimnisse auf Gruppenebene anwenden. Ordnen Sie dann Ihre Geheimnisgruppe einer Identitätsgruppe zu, und fügen Sie Ihren MID-Server dieser Identitätsgruppe hinzu.

4. **Laden Sie das öffentliche/private Schlüsselpaar auf den MID-Server hoch**

   Laden Sie Ihr öffentliches/privates Schlüsselpaar auf Ihren MID-Server hoch. Mit diesem Schlüsselpaar kann der MID-Server Authentifizierungsanforderungen von Ihrer Instanz verarbeiten.

5. **Erstellen Sie Anmeldeinformationen, und testen Sie die Verschlüsselung der Anmeldeinformationen**

   Erstellen Sie Anmeldeinformationen, um sich bei einem Drittparteisystem zu authentifizieren, und testen Sie diese ServiceNow Auf die Anmeldeinformationen kann nicht zugegriffen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. **Konfigurieren Sie Flow Designer, um die Integration zu verwalten**

   Verwenden Sie in Ihrer Instanz Flow Designer Dient zum Verwalten einer Integration zwischen Ihrem lokalen Netzwerk und Ihrer Instanz.

7. **Testen Sie die End-to-End-Integration verschlüsselter Geheimnisse auf Clientseite**

   Testen Sie Ihre Integration, und überprüfen Sie die Ausführungsdetails, um sicherzustellen, dass Ihre Konfiguration funktioniert.

Erstellen Sie Verschlüsselungsschlüssel und Zertifikat

Erstellen Sie Verschlüsselungsschlüssel und ein Zertifikat mithilfe von Terminalbefehlen in Ihrer lokalen Umgebung.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

1. Öffnen Sie in Ihrer lokalen Umgebung Terminal (unter Mac oder Linux) oder Befehlszeile (unter Windows).
2. Verwenden Sie das -Terminal, und verwenden Sie `CD` Um in den Ordner zu wechseln, in dem Sie Ihre Verschlüsselungsschlüssel speichern möchten.
3. Geben Sie mithilfe des Terminals Folgendes ein:

   ```
   openssl req -newkey rsa:4096 -nodes -keyout sm_private_key.pem -x509 -days 365 -out sm_public_cert.pem
   ```

   Hinweis: In diesem Beispiel wird OpenSSL zum Generieren von Schlüsseln und Zertifikaten verwendet. Sie können andere vergleichbare Tools basierend auf Ihren Anforderungen ersetzen.

   Der Befehl generiert einen privaten Schlüssel und ein öffentliches Zertifikat (mit dem übereinstimmenden öffentlichen Schlüssel). Es folgt eine Reihe von Hinweismeldungen für erforderliche Informationen, beginnend mit „Ländername“.

4. Geben Sie die Eingabeaufforderungen mit den angeforderten Informationen ein.
   Die folgenden Hinweismeldungen werden angezeigt.
   - Ländername
   - Name des Bundeslands/Kantons
   - Ortsname (z. B. Stadt)
   - Organisationsname (z. B. Unternehmen)
   - Name der Organisationseinheit (z. B. Abschnitt)
   - Allgemeiner Name (z. B. vollqualifizierter Hostname)
   - E-Mail-Adresse

   Arbeiten Sie mit Ihrem Sicherheitsteam zusammen, um sicherzustellen, dass Sie die richtigen Zertifikatinformationen eingeben.

   ```
   Country Name (2 letter code) []:US
   State or Province Name (full name) []:CO
   Locality Name (eg, city) []:Boulder
   Organization Name (eg, company) []:ServiceNow
   Organizational Unit Name (eg, section) []:Product Management
   Common Name (eg, fully qualified host name) []:fake@servicenow.com
   Email Address []:fake@servicenow.com
   ```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Überprüfen Sie den Ordner, den Sie in Schritt 2 ausgewählt haben, um sicherzustellen, dass der private Schlüssel und das öffentliche Zertifikat erstellt wurden.
   Wenn Sie dieselben Dateinamen wie im Beispiel für Schritt 3 verwendet haben, sollten die folgenden Dateien angezeigt werden:
   - sm_private_key.pem
   - sm_public_cert.pem
6. Verwenden Sie im selben Ordner den folgenden Befehl:

   Wichtig: Der spezifische Befehl, der verwendet werden soll, hängt von Ihrem Betriebssystem ab.

Für Linux:	`cat sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`
Für Windows:	`sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`

   Dieser Befehl bündelt den privaten Schlüssel und das öffentliche Zertifikat in einer einzelnen Datei, die in späteren Schritten in Ihren MID-Server geladen werden können.
7. Überprüfen Sie den Ordner erneut, um sicherzustellen, dass die neue Datei mit Ihrem privaten Schlüssel (sm_Keypair_Bundle.pem) und dem öffentlichen Zertifikat erstellt wurde.

Fügen Sie Ihr Zertifikat dem Trusted Key Store von ServiceNow hinzu

Laden Sie Ihren Schlüssel und Ihr Zertifikat in hoch ServiceNow Vertrauenswürdiger Schlüsselspeicher.

Vorbereitungen

Erforderliche Rolle: Administrator

Das öffentliche Zertifikat, das Sie in diesem Beispiel erstellt haben, wird als „selbstsigniertes“ Zertifikat betrachtet (d. h. es stammt nicht von einer vertrauenswürdigen Stammberechtigung). Sie müssen das Zertifikat zu hinzufügen ServiceNow Vertrauenswürdiger Schlüsselspeicher für die Verwendung. Wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle stammt, müssen Sie diesen Schritt nicht abschließen.

Prozedur

1. Öffnen Sie in Ihrer lokalen Umgebung Terminal (unter Mac oder Linux) oder Befehlszeile (unter Windows).
2. Verwenden Sie das -Terminal, und verwenden Sie `CD` Um in den Ordner zu wechseln, in dem Sie Ihre Verschlüsselungsschlüssel erstellt haben.
3. Geben Sie im Terminal den folgenden Befehl ein:

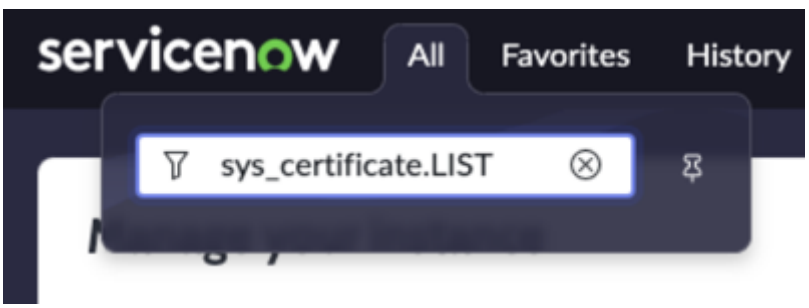
   ```
   cat sm_public_cert.pem
   ```

   Sie müssen den Inhalt Ihres öffentlichen Zertifikats anzeigen, um es in den vertrauenswürdigen Schlüsselspeicher zu kopieren. Dies `Kat` Befehl zeigt das Zertifikat an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Kopieren Sie die Zertifikatinformationen in Ihre Zwischenablage.
   Beginnen Sie mit, und schließen Sie ein `----- ZERTIFIKAT BEGINNEN------` Führen Sie und enden mit und schließen Sie die ein `----- ENDZERTIFIKAT-----` Position.
5. Auf Ihrem ServiceNow-Instanz navigieren Sie zu **X.509-Zertifikat** Liste durch Eingabe `sys_certificate.LIST` Im Navigationsfilter.



6. Wählen Sie Aus **Neu** Zum Erstellen von **X.509-Zertifikat** Datensatz.
7. Füllen Sie im Formular die folgenden Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

X.509-Zertifikatfelder

Feld	Wert
Name	Name des Zertifikats. Dieser Name kann ein beliebiger Name sein, den Sie auswählen.
Format	Wählen Sie Aus **PEM** **Hinweis:** PEM-Dateien (Privacy Enhanced Mail) sind eine Art von PKI-Datei (Public Key Infrastructure), die für Schlüssel und Zertifikate verwendet wird. Die Datensätze, die Sie in den vorherigen Schritten erstellt haben, haben diesen Dateityp.
Typ	Wählen Sie Aus **Vertrauenswürdiges Store-Zertifikat**
Kurzbeschreibung	Beschreibung des Zertifikats. Geben Sie einen Wert ein, der Sie darüber informiert, wofür dieses Zertifikat verwendet wird.
PEM-Zertifikat	Fügen Sie die Zertifikatinformationen ein, die Sie in Schritt 4 kopiert haben.

8. Wählen Sie Aus **Übermitteln** Zum Speichern des Datensatzes.

Erstellen Sie eine geheime Gruppe mit Kriterien

Erstellen Sie eine Gruppe für Ihre Geheimnisse. Geheime Gruppen, um Ihre Geheimnisse in Gruppen zu organisieren und Ihnen die Anwendung von Zugriffsrichtlinien auf diese Geheimnisse auf Gruppenebene zu ermöglichen. Ordnen Sie dann Ihre Geheimnisgruppe einer Identitätsgruppe zu, und fügen Sie Ihren MID-Server dieser Identitätsgruppe hinzu.

Vorbereitungen

Erforderliche Rolle: admin, KMF_admin, sn_secrets.secret_manager und sn_kmf.cryptographic_Manager

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen mit Kriterien**an.
2. Wählen Sie Aus **Neu** Zum Erstellen von **Geheime Gruppe mit Kriterien** Datensatz.
3. Füllen Sie im Formular die folgenden Felder aus.

Geheime Gruppe mit Kriterienfeldern

Feld	Wert
Gruppenname	Name der geheimen Gruppe. Dieser Name kann ein beliebiger Name sein, den Sie auswählen.
Geheimnistyp	Wählen Sie Aus **Vom Client zugänglich**
Autogen-Modul	Aktivieren Sie das Kontrollkästchen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Kurzbeschreibung	Beschreibung der geheimen Gruppe. Geben Sie einen Wert ein, der angibt, wofür diese Gruppe verwendet wird.
Kriteriumstyp	Wählen Sie Aus **Zieltabelle**
Zieltabelle	Wählen Sie Aus **SSH-Anmeldeinformationen [ssh_credentials]**

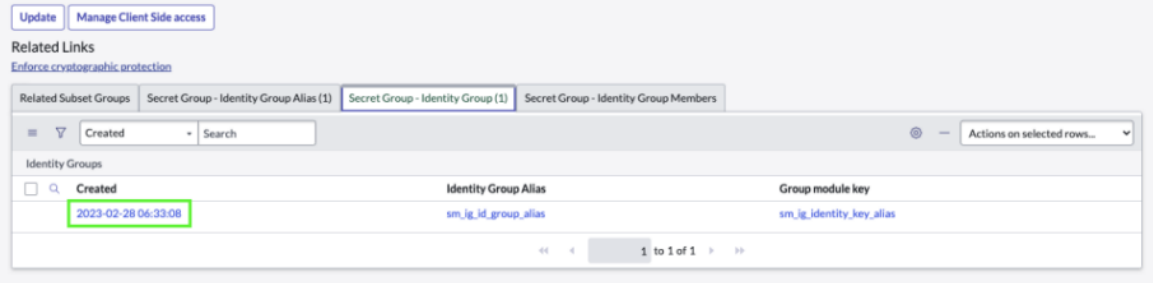
4. Wählen Sie den Formularheader aus, halten Sie ihn gedrückt (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie ihn aus **Speichern** Aus dem Kontextmenü, um den Datensatz zu speichern.
5. Stellen Sie sicher, dass **Aktiv** Kontrollkästchen ist nicht aktiviert.
6. Wählen Sie aus **Verwalten Sie den clientseitigen Zugriff** Schaltfläche zum Erstellen einer Identitätsgruppe.
   Ein **Identitätsgruppenalias** Fenster wird angezeigt.
7. Wählen Sie aus **Neu** Schaltfläche.
8. Wählen Sie das Referenzsymbol ( ) Neben **Identitätsgruppenalias** Feld.
9. In **Gruppenaliasname** Feld einen Wert eingeben.
   Dieser Name kann ein beliebiger Wert sein.
10. Wenn Sie in Schritt 9 einen eindeutigen Namen ausgewählt haben, wählen Sie aus **Übermitteln** .
11. Wählen Sie aus **Identitätsschlüssel hochladen** Schaltfläche.
    Die **Importieren Sie das Zertifikat des öffentlichen Identitätsschlüssels** Fenster wird angezeigt.
12. In **Identitätsschlüssel-Alias** Feld einen Wert eingeben.

    Wichtig: Dieser Wert kann beliebig sein, muss jedoch genau mit dem übereinstimmen, was Sie in den späteren Schritten in den MID-Server einfügen.

13. Wählen Sie Aus **Importieren**
    Die **Anhang** Fenster wird angezeigt.
14. Wählen Sie Aus **Wählen Sie die Datei aus** .
15. Wählen Sie das öffentliche Zertifikat aus, das Sie in den vorherigen Schritten erstellt haben.
    Dieses Zertifikat muss sein `sm_public_cert.pem` Datei.
16. Wählen Sie das X-Symbol, um das Fenster zu schließen.
17. Wählen Sie Aus **OK** Um zu schließen **Importieren Sie das Zertifikat des öffentlichen Identitätsschlüssels** Fenster.
    Ein Blau **Schlüssel und Zertifikate wurden erfolgreich in die Instanz importiert** Ein Banner wird angezeigt, das einen erfolgreichen Import bestätigt.
18. Wählen Sie **Absenden**.
    Die **Identitätsgruppen** Listenanzeigen.
19. Aktivieren Sie das Kontrollkästchen links neben Ihrem Identitätsgruppendatensatz in der Liste.
20. Wählen Sie aus **Ordnen Sie geheime Gruppe zu** Schaltfläche.
    Sie werden zu zurückkehren **Geheime Gruppe mit Kriterien** Datensatz. Die **Geheimnisgruppe: Identitätsgruppenalias** „ Und **Geheimnisgruppe: Identitätsgruppe** Zugehörige Listen sind sichtbar. Diese zugehörigen Listen zeigen die Datensätze an, die Sie in den vorherigen Schritten erstellt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

21. In **Geheimnisgruppe: Identitätsgruppe** Zugehörige Liste wählen Sie aus **Erstellt** Feld für den Datensatz in dieser Liste.



Ein **Identitätsgruppe** Datensatzanzeigen.

22. In **Identitätsgruppenmitglieder** Zugehörige Liste wählen Sie aus **Neu** Schaltfläche.
A **Identitätsgruppenmitglied** Datensatzanzeigen.
23. In **Mitgliedstabelle** Feld auswählen **MID-Server [ecc_Agent]** .
24. Wählen Sie das Referenzsymbol ( ) Neben **Datensatz des Identitätsgruppenmitglieds** Und wählen Sie Ihren MID-Server aus.

> **Hinweis:** Wenn Sie aktivieren **Schließen Sie alle Datensätze ein** Kontrollkästchen, alle mit Ihrer Instanz verbundenen MID-Server werden der Identitätsgruppe hinzugefügt.

25. Wählen Sie Aus **OK** Um zu schließen **Wählen Sie das Dokument aus** Fenster.
26. Wählen Sie **Absenden**.
27. Navigieren Sie zurück zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen mit Kriterien**, Und öffnen Sie den Datensatz, den Sie in Schritt 2 erstellt haben.
28. Aktivieren Sie **Aktiv** Feld.
29. Wählen Sie Aus **Aktualisieren** Zum Speichern des Datensatzes.

Laden Sie das öffentliche/private Schlüsselpaar auf den MID-Server hoch

Laden Sie Ihr öffentliches/privates Schlüsselpaar auf Ihren MID-Server hoch. Mit diesem Schlüsselpaar kann der MID-Server Authentifizierungsanforderungen von Ihrer Instanz verarbeiten.

Vorbereitungen

Erforderliche Rolle: keine

Seit ServiceNow Hat keinen Zugriff auf den privaten Schlüssel. Er kann nicht mit dem öffentlichen Schlüssel gekoppelt werden, um den symmetrischen Schlüssel zu entschlüsseln und dann die Anmeldeinformationen zu entschlüsseln. Wenn der MID-Server versucht, diese verschlüsselten Anmeldeinformationen zu verwenden, kann er die Anmeldeinformationen für die Authentifizierung ohne Zugriff auf den privaten Schlüssel nicht entschlüsseln.

In diesen Schritten laden Sie den privaten Schlüssel auf den MID-Server hoch, um den öffentlichen/privaten Schlüsselanhänger abzuschließen. Dieser Upload gewährt dem MID-Server Zugriff ohne Zuerkennung ServiceNow Zugriff.

Um dem MID-Server Zugriff auf den privaten Schlüssel zu gewähren, müssen Sie einen Befehl erstellen, der als Administrator in Powershell ausgeführt werden soll. In diesem Beispiel gilt der Befehl für die virtuelle Azure Windows-Maschine.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Stellen Sie sicher, dass das System, auf dem Sie diese Schritte ausführen, sowohl auf den MID-Server als auch auf die Schlüsselpaardatei zugreifen kann.

Prozedur

1. Suchen Sie in Ihrer lokalen Umgebung den Ordner, in dem Sie Ihr Schlüsselpaar erstellt haben Erstellen Sie Verschlüsselungsschlüssel und Zertifikat Schritte.
2. Suchen Sie den vollständigen Pfad, und kopieren Sie ihn nach `manage-certificates.bat` Datei.

   Hinweis: Diese Datei befindet sich in Ihrem MID-Server-Ordner. Je nachdem, wo Sie Ihren MID-Server-Ordner gespeichert haben, kann Ihr Pfad wie folgt aussehen:

   ```
   C:
   \Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat
   ```

3. Erstellen Sie eine Textdatei, und fügen Sie den Pfad in die Datei ein.
4. Fügen Sie in der Textdatei nach dem Pfad Folgendes hinzu:
   `-Ein Your_Identity_key_alias`

   Ersetzen `Ihre_Identität_Schlüssel_Alias` Mit dem Namen des Identitätsschlüssel-Alias, den Sie beim Hochladen Ihres öffentlichen Zertifikats erstellt haben.
5. Suchen und kopieren Sie den vollständigen Pfad in Ihre Schlüsselpaardatei.

   Hinweis: Wenn Sie die Namen in diesen Schritten verwendet haben, wird diese Datei benannt `sm_Keypair_Bundle.pem` .
6. Fügen Sie in Ihrer Textdatei diesen Pfad am Ende der Zeile hinzu, und fügen Sie einen Abstand zwischen diesem Pfad und den vorherigen Informationen hinzu.
   Der Text in Ihrer Textdatei sollte wie in diesem Beispiel aussehen:

   ```
   C:
   \Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificates.bat -a your_identity_key_alias
    C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
   ```

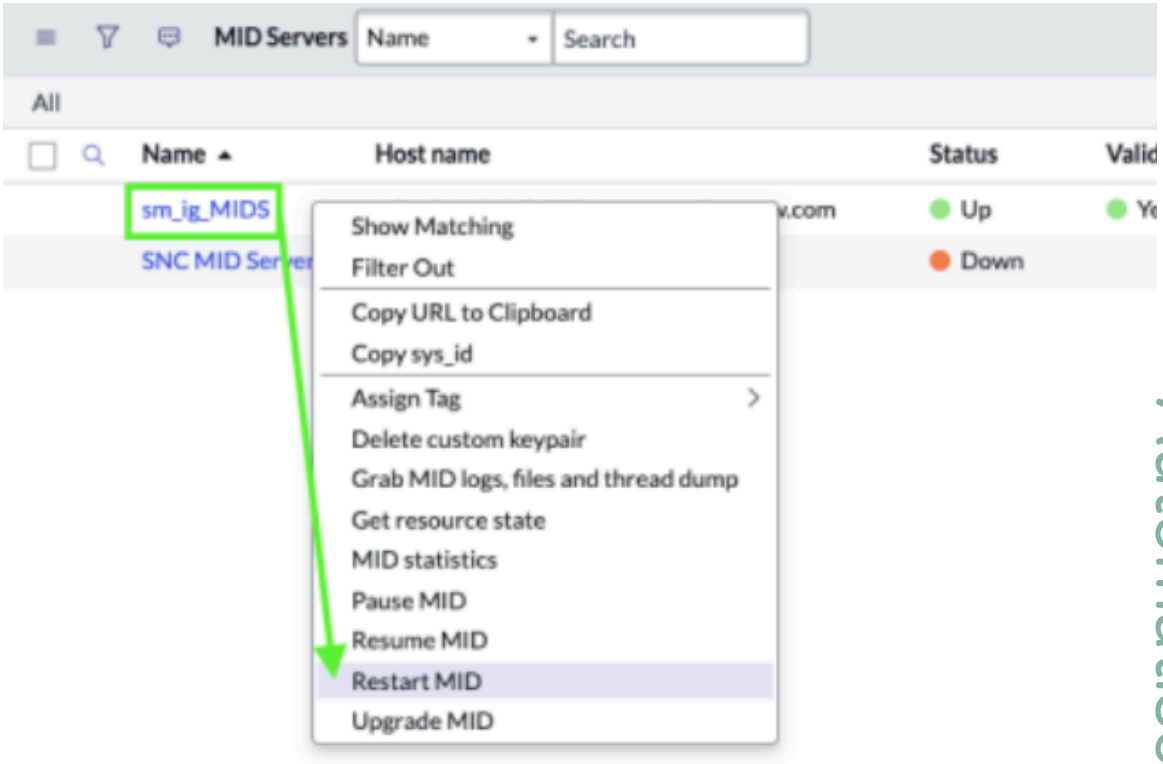
   Hinweis: In diesem Beispiel ist `sm_Keypair_Bundle.pem` Die Datei befindet sich auf dem Desktop, um den Pfad kürzer zu machen.
7. Kopieren Sie den gesamten Text Ihrer Textdatei in die Zwischenablage.
8. Suchen Sie Powershell auf Ihrem System, und wählen Sie aus **Als Administrator ausführen** Option.
9. Fügen Sie den Text aus Ihrer Textdatei in Powershell ein, und drücken Sie die Eingabetaste.
   Wenn erfolgreich, wird die folgende Meldung angezeigt:

   ```
   Installed certificate with alias: <your_identity_key_alias> into the MID keystore.
   ```

   Tipp: Wenn diese Nachricht nicht angezeigt wird, stellen Sie sicher, dass Ihr Befehl keine Fehler, Leerzeichen oder unnötige Anführungszeichen enthält. Stellen Sie sicher, dass der vollständige Pfad korrekt eingegeben ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Starten Sie Ihren MID-Server neu, indem Sie zu Ihrem MID-Server-Datensatz navigieren, mit der rechten Maustaste auf den Datensatz klicken und auswählen **Starten Sie MID neu** .



Durch einen Neustart des MID-Servers wird das hochgeladene Schlüsselpaar im MID-Schlüsselspeicher zur Verwendung mit Vorgängen synchronisiert. Warten Sie, bis der MID-Server mit dem Status neu gestartet wird **Aktiv** Und ein validierter Wert von **Ja** Bevor Sie fortfahren.

Erstellen Sie Anmeldeinformationen, und testen Sie die Verschlüsselung der Anmeldeinformationen

Erstellen Sie Anmeldeinformationen, um sich bei einem Drittparteisystem zu authentifizieren.

Vorbereitungen

Erforderliche Rolle: admin, KMF_admin, sn_secrets.secret_manager und sn_kmf.cryptographic_Manager

Wichtig: Der angemeldete Anwender des MID-Servers muss auch über die folgenden Rollen verfügen: admin, KMF_admin, sn_secrets.secret_manager und sn_kmf.cryptographic_Manager.

Prozedur

1. Navigieren Sie zu **SSH-Anmeldeinformationen** Liste durch Eingabe `ssh_credentials.list` Im Navigationsfilter.
2. Wählen Sie Aus **Neu** Um eine zu erstellen **SSH-Anmeldeinformationen** Datensatz.
3. Füllen Sie im Formular die folgenden Felder aus.

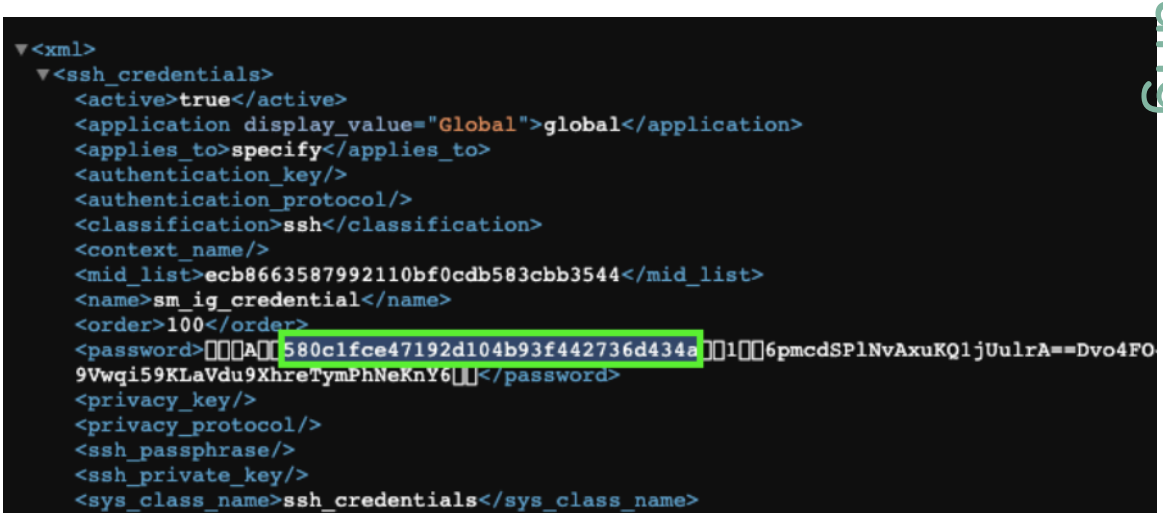
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „SSH-Anmeldeinformationen“

Feld	Wert
Name	Geben Sie einen Namen für Ihren Anmeldeinformationsdatensatz ein. Dieser Name kann ein beliebiger Wert sein.
Betrifft	Wählen Sie Aus **Bestimmte MID-Server**
MID-Server	Wählen Sie Ihren MID-Server aus.
Anwendername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort für den Anwender in ein **Anwendername** Feld.

4. Wählen Sie das Schlosssymbol ( ) Neben **Anmeldeinformationsalias** Feld.
5. Wählen Sie das Referenzsymbol ( ), um zu öffnen **Aliasse für Verbindungen und Anmeldeinformationen** Liste.
6. Wählen Sie Aus **Neu** Zum Erstellen von **Alias für Verbindungen und Anmeldeinformationen** Datensatz.
7. Geben Sie einen Namen in ein **Name** Feld.
8. Wählen Sie Aus **Anmeldeinformationen** In **Typ** Feld.
9. Wählen Sie **Absenden**.
   Sie kehren zu zurück **SSH-Anmeldeinformationen** Datensatz. In den nächsten Schritten testen Sie, ob die Anmeldeinformationen verschlüsselt sind.
10. Wählen Sie den Formularheader aus, halten Sie ihn gedrückt (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie ihn aus **XML anzeigen** .
11. Suchen Sie nach `<password>` XML-Tag innerhalb der XML.
12. Kopieren Sie die sys_ID darin `<password>` Tag in Ihrer Zwischenablage.
    Die sys_ID ist ein 32-stelliger Code, der den symmetrischen Schlüssel darstellt, der zum Verschlüsseln dieser Anmeldeinformationen verwendet wird. Das verschlüsselte Passwort, das Sie in die Tabelle „SSH-Anmeldeinformationen“ eingegeben haben, befindet sich rechts von den beiden Kästchen in derselben Zeile.

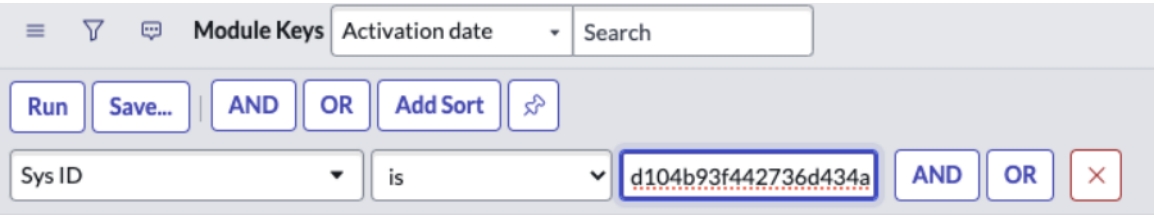


13. Navigieren Sie zu **Modulschlüssel** Liste durch Eingabe `sys_kmf_Module_key.list` Im Navigationsfilter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

14. Filtern Sie die Liste nach Datensätzen, bei denen **SYS-ID** Feld stimmt mit der sys_ID überein, die Sie in Schritt 12 kopiert haben, und wählen Sie aus **Ausführen** .



Ihre Suche sollte eine einzelne zurückgeben **Modulschlüssel** Datensatz. Dieser Datensatz zeigt, dass Sie erfolgreich einen symmetrischen Schlüssel erstellt haben und verwenden.

15. Navigieren Sie zu **Umschlossene Modulschlüssel** Liste durch Eingabe sys_kmf_Wrapped_Module_key.list Im Navigationsfilter.

16. Filtern Sie die Liste nach Datensätzen, bei denen **Krypto-Modul** Feld stimmt mit dem kryptografischen Modul überein, das Sie in den vorherigen Schritten erstellt haben, und wählen Sie aus **Ausführen** .
Ihre Suche sollte eine einzelne zurückgeben **Umschlossener Modulschlüssel** Datensatz. In dieser Liste können Sie Folgendes überprüfen:
    - Die **Umschlossenes Schlüsselmaterial** Die Spalte zeigt an, dass der symmetrische Schlüssel im Krypto-Modul (der zum Verschlüsseln der SSH-Anmeldeinformationen verwendet wird) durch den öffentlichen Schlüssel verschlüsselt wird, den Sie in die Identitätsgruppe hochgeladen haben.
    - Die **SYS-ID des umschlossenen Schlüssels** Das Feld zeigt an, dass es sich um den Schlüssel (der symmetrische Schlüssel des Krypto-Moduls) handelt, der von verschlüsselt wird **SYS-ID des umschließenden Schlüssels** (Der öffentliche Schlüssel, der in die Identitätsgruppe hochgeladen wurde).

    Wenn sich die vorherigen Felder standardmäßig nicht in Ihrer Liste befinden, können Sie sie der Liste hinzufügen, indem Sie auswählen **Personalisieren Sie die Liste** Symbol ( ).

    Hinweis: Ihre Instanz führt alle 10 Minuten einen Bereinigungsauftrag aus, der verwaiste Schlüssel entfernt und die Verbreitung nicht zugeordneter Schlüssel verhindert, nachdem Sie Ihre Anmeldeinformationen aktualisiert haben.

Konfigurieren Sie Flow Designer, um die Integration zu verwalten

Verwenden Sie in Ihrer Instanz Flow Designer Dient zum Verwalten einer Integration zwischen Ihrem lokalen Netzwerk und Ihrer Instanz.

Vorbereitungen

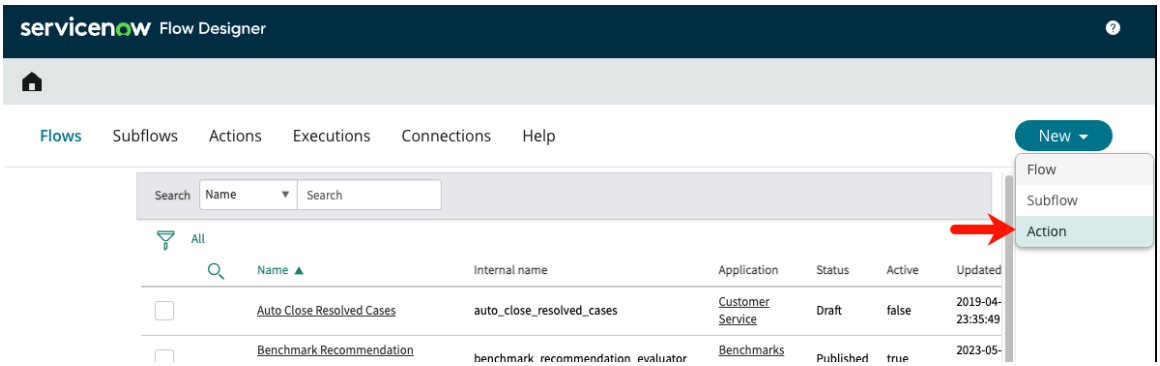
Erforderliche Rolle: admin, KMF_admin, sn_secrets.secret_manager und sn_kmf.cryptographic_Manager

In diesen Schritten erstellen Sie einen Flow Designer Workflow zum Erstellen einer Textdatei auf Ihrem lokalen System.

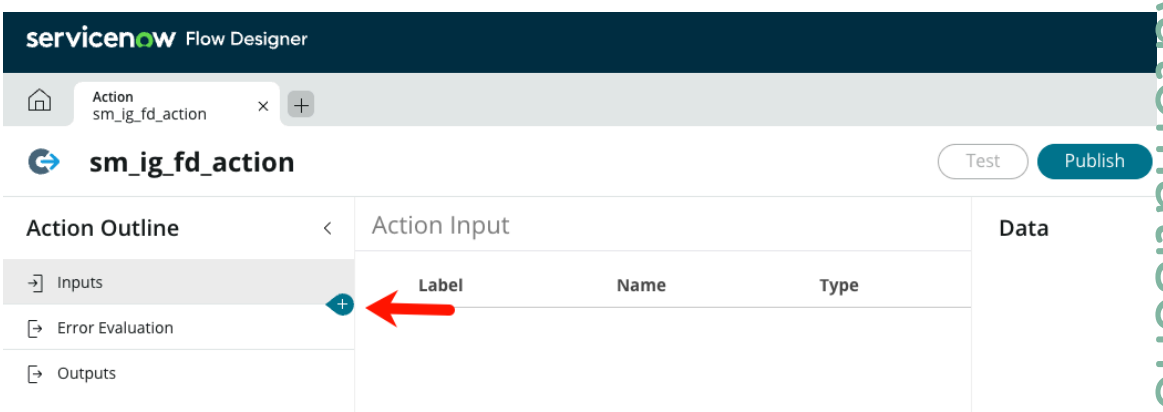
Prozedur

1. Navigieren Sie in Ihrer Instanz zu **Alle** > **Prozessautomatisierung** > **Flow Designer**an.
2. Erstellen Sie eine Aktion in ServiceNow Durch Auswahl von **Neu** Und auswählen **Aktion** .

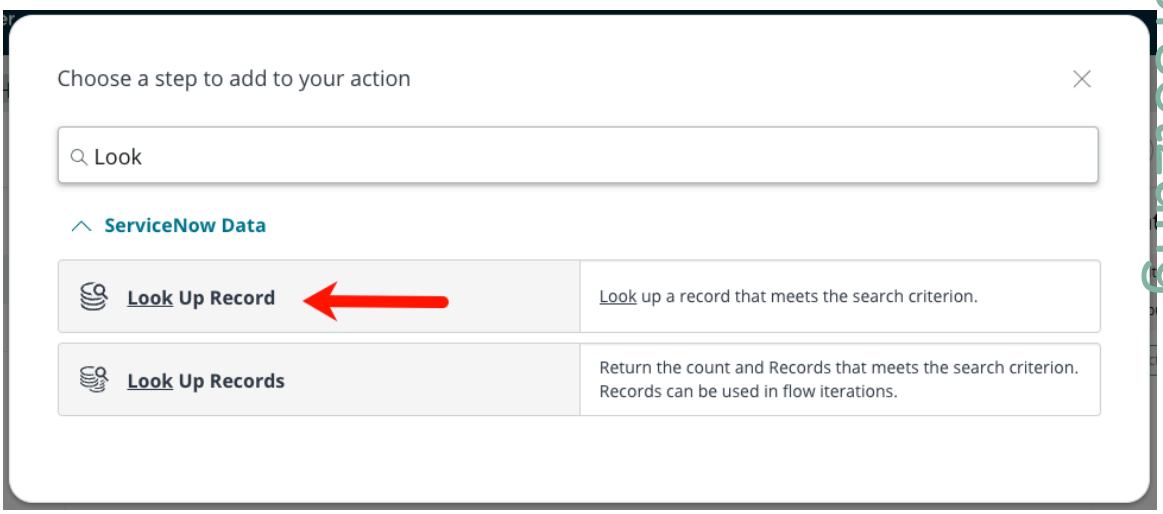
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Geben Sie einen Namen in ein **Aktionsname** Feld, und wählen Sie aus **Übermitteln** .
4. Erstellen Sie einen Schritt, indem Sie das Pluszeichen zwischen auswählen **Eingaben** Und **Fehlerauswertung** In **Aktionsstruktur** .



5. In **Wählen Sie einen Schritt aus, der Ihrer Aktion hinzugefügt werden soll** Fenster auswählen **Suchen Sie Nach Datensatz** .



6. In **Schritt „Datensatz suchen“** Abschnitt auswählen **MID-Server [ecc_Agent]** In **Tabelle** Feld.
7. Erstellen Sie einen weiteren Schritt, indem Sie das Pluszeichen unter Ihrem auswählen **Schritt „Datensatz suchen“** .
8. In **Wählen Sie einen Schritt aus, der Ihrer Aktion hinzugefügt werden soll** Fenster auswählen **SSH** .

Automatische Übersetzung

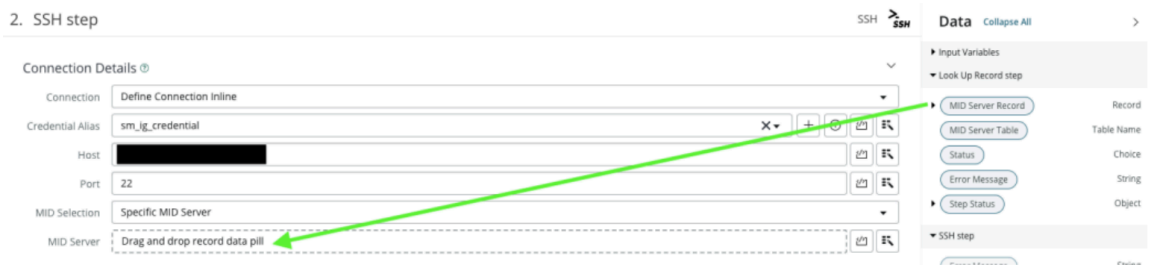
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie nicht sehen **SSH** Option müssen Sie das erforderliche Plugin aktivieren.

9. In **SSH-Schritt** Geben Sie die folgenden Informationen ein:

Feld	Wert
Verbindung	Wählen Sie Aus **Definieren Sie Die Verbindung Inline**
Anmeldeinformationsalias	Wählen Sie den Anmeldeinformationsalias für die SSH-Anmeldeinformationen aus, die in früheren Schritten erstellt wurden.
Host	Geben Sie die IP-Adresse für den Host ein, mit dem Sie über SSH eine Verbindung herstellen.
Port	Geben Sie Ein 22.
MID-Auswahl	Wählen Sie Aus **Bestimmter MID-Server** .

10. Um auszufüllen **MID-Server** Feld ziehen **MID-Server-Datensatz** Pille aus dem **Daten** Abschnitt in das Feld.



Warnung: Wenn Sie die Pille in das Feld ziehen, wählen Sie die Pille und nicht den schwarzen Pfeil neben der Pille aus.

11. In **SSH-Konfiguration** Geben Sie im Abschnitt den folgenden Wert ein **Befehl** Feld.

```
/bin/date > sm_ig_text_file.txt
```

Dieser Befehl erstellt eine Textdatei in Ihrem lokalen System mithilfe der entschlüsselten Geheimnisse vom MID-Server. Der MID-Server gewährt Zugriff auf ServiceNow Instanz (bis Flow Designer), ohne jemals zu geben ServiceNow Instanzzugriff auf das entschlüsselte Geheimnis.

Tipp: Die /Bin/date Befehl fügt das aktuelle Datum/die aktuelle Uhrzeit in die erstellte Textdatei ein. Dieser Befehl demonstriert, dass die Integration in Echtzeit stattfindet, basierend auf dem aktuellen Datum/der aktuellen Uhrzeit im Vergleich zum Zeitpunkt der Erstellung der Textdatei.

12. Wählen Sie aus **Speichern** Schaltfläche zum Speichern des Workflows.

Testen Sie die End-to-End-Integration verschlüsselter Geheimnisse auf Clientseite

Testen Sie Ihre Integration, und überprüfen Sie die Ausführungsdetails, um sicherzustellen, dass Ihre Konfiguration funktioniert.

Automatische Übersetzung

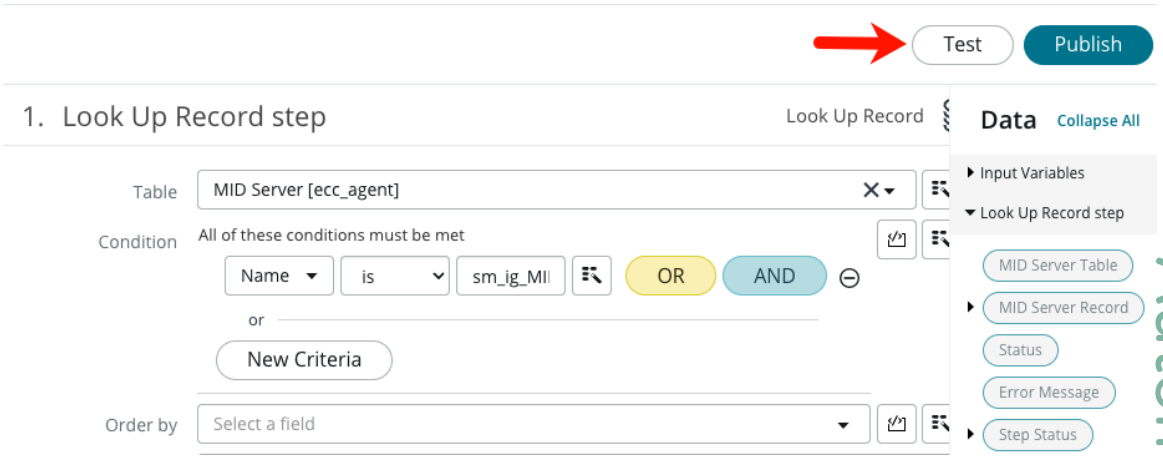
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin, KMF_admin, sn_secrets.secret_manager und sn_kmf.cryptographic_Manager

Prozedur

1. In Flow Designer Wählen Sie aus **Testen** Schaltfläche in der oberen rechten Ecke des Bildschirms.



2. In **Testaktion** Fenster auswählen **Test Ausführen** .
3. Wählen Sie Aus **Die Ausführung Ihres Tests wurde abgeschlossen. Zeigen Sie die Aktionsausführungsdetails an.**
4. Aktualisieren Sie Ihren Bildschirm, bis angezeigt wird **Testausführung: Abgeschlossen** Oben rechts im Bildschirm.
5. Wählen Sie aus **Schritte** Pfeil unten links auf dem Bildschirm.
6. Scrollen Sie nach unten, bis ein angezeigt wird **Schrittausgabedaten** Überschrift mit der folgenden Erfolgsmeldung:

```
{"Step Status";{"code";0,"message";"Success"}}
```

7. Nachdem diese Nachricht in angezeigt wurde Flow Designer, Überprüfen Sie, ob Ihre Textdatei in Ihrem lokalen System erstellt wurde.

Testen Sie Anmeldeinformationen der Windows-Verwaltungsinstrumentation, die mit der Geheimnisverwaltung verschlüsselt sind

Stellen Sie sicher, dass Ihre Windows Management Instrumentation (WMI)-Anmeldeinformationen mit Geheimnisverwaltung verschlüsselt sind, und verwenden Sie einen Integration Hub-Workflow, um End-to-End-Tests abzuschließen.

Vorbereitungen

Erforderliche Rolle: admin, KMF_admin, sn_secrets.secret_manager und sn_kmf.cryptographic_Manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Integrations-Hub Enterprise muss in Ihrer Instanz aktiv sein. Details finden Sie unter Fordern Sie an IntegrationHub Plugin .
- In Ihrer Instanz muss eine konfigurierte Geheimnisgruppe vorhanden sein. Siehe Schritte 1 bis 3, die in aufgeführt sind Vom Client zugängliche Geheimnisse konfigurieren.
- Sie müssen über konfigurierte Anmeldeinformationen verfügen, die mit Geheimnisverwaltung verschlüsselt sind. Siehe Schritte 1 bis 9, die in aufgeführt sind Erstellen Sie Anmeldeinformationen, und testen Sie die Verschlüsselung der Anmeldeinformationen.

Prozedur

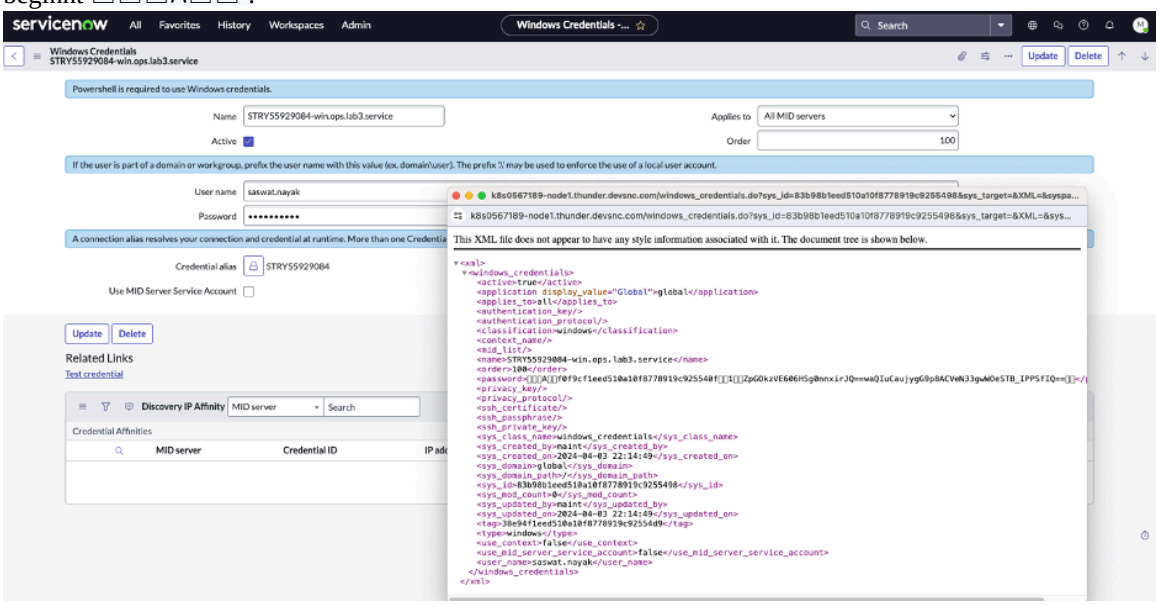
1. Bestätigen Sie, dass der gewünschte MID-Server der geheimen Gruppe zugeordnet ist.
   Öffnen Sie den Datensatz „geheime Gruppe mit Kriterien“ [sn_sm_Criteria_Secret_Group], und suchen Sie im nach Ihrem MID-Server **Geheimnisgruppe: Mitglieder Der Identitätsgruppe** Liste. Wenn Ihr MID-Server keiner Gruppe zugeordnet ist, siehe Erstellen Sie eine geheime Gruppe mit Kriterien.
2. Bestätigen Sie, dass die Anmeldeinformationen mit Geheimnisverwaltung verschlüsselt sind.

   a. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

   b. Öffnen Sie Ihren Anmeldeinformationsdatensatz.
   Stellen Sie sicher, dass Sie einen Anmeldeinformationsalias in der aufgeführt haben **Anmeldeinformationsalias** Feld. Wenn Sie noch keine erstellt haben, finden Sie weitere Informationen unter Verbindungs- und Anmeldealias erstellen.

   c. Wählen Sie den Header Ihres Anmeldeinformationsdatensatzes aus, halten Sie ihn gedrückt (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie aus **XML anzeigen** Aus der Liste.

   d. Suchen Sie in der XML-Ansicht des Datensatzes nach dem Passwort, und bestätigen Sie, dass der Wert mit beginnt □□□A□□ .



3. Erstellen Sie einen Test-Workflow in Workflow-Studio.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Prozessautomatisierung** > **Workflow-Studio**an.

b. Wählen Sie Aus **Neu** , Und wählen Sie dann aus **Aktion** Aus der Liste.

c. Geben Sie einen Namen in ein **Aktionsname** Feld.
Verlassen Sie die **Anwendung** Feld auf Global festgelegt.

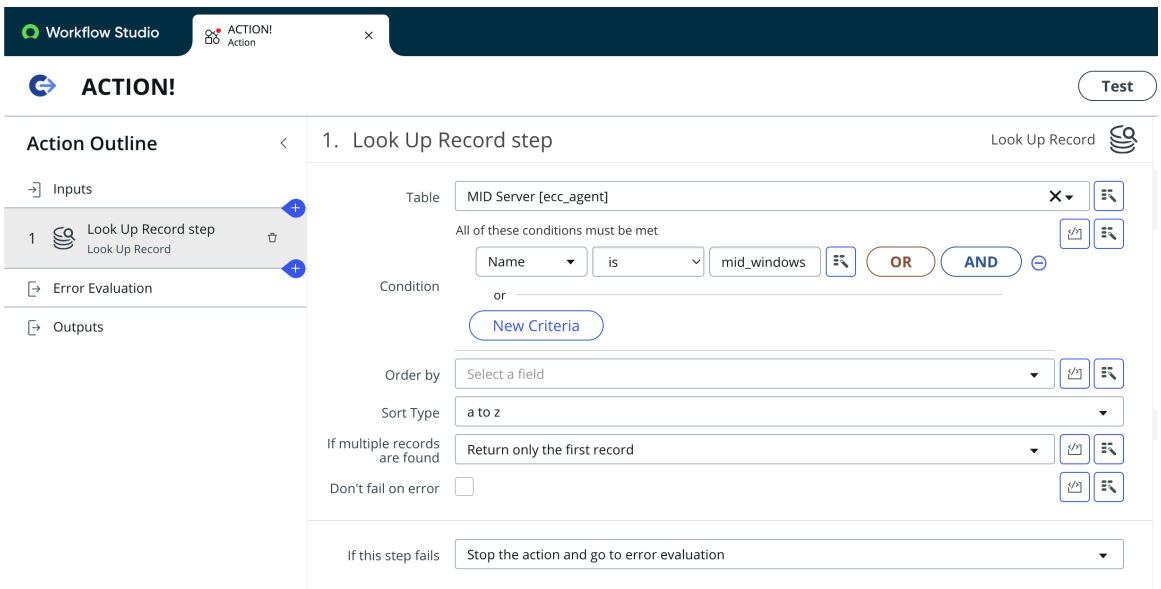
d. Wählen Sie aus **Build-Aktion** Schaltfläche.

4. Konfigurieren Sie einen Datensatzsuchschritt in Workflow-Studio.

a. In **Aktionsstruktur** , Wählen Sie die Plus-Schaltfläche, um einen neuen Schritt hinzuzufügen.
Suchen und wählen Sie aus **Suchen Sie Nach Datensatz** Schritttyp.

b. In **Tabelle** Feld auswählen **MID-Server [ecc_Agent]** .

c. Wählen Sie für die Bedingung aus **Name ist** , Gefolgt vom Namen Ihres MID-Servers.



Wichtig: Stellen Sie sicher, dass der ausgewählte MID-Server mit dem der geheimen Gruppe verknüpften Server identisch ist.

5. Konfigurieren Sie einen Datensatzsuchschritt in Workflow-Studio.

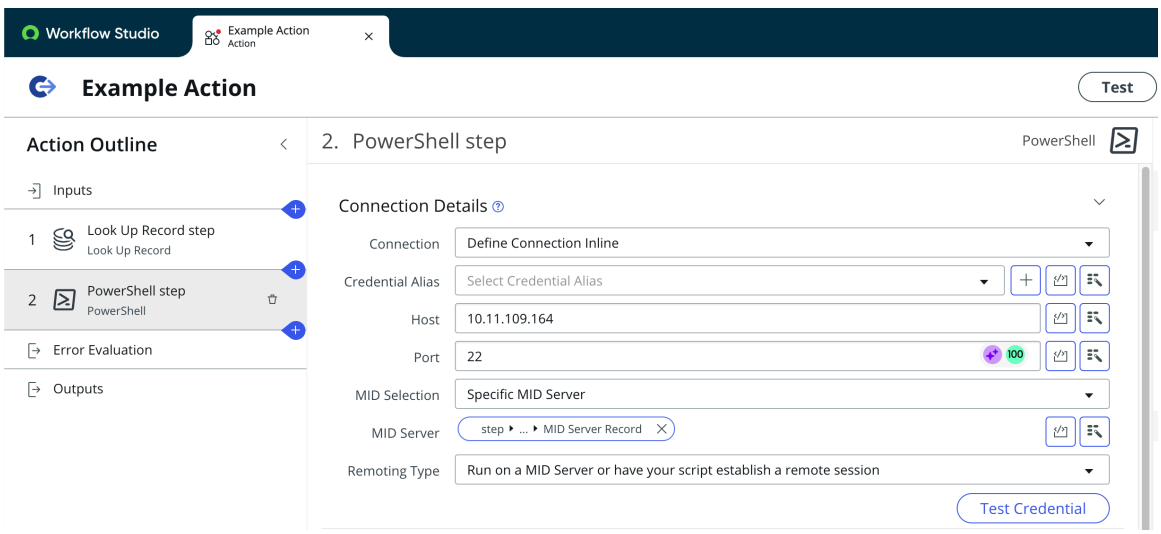
a. In **Aktionsstruktur** , Wählen Sie die Schaltfläche Plus, um einen neuen Schritt unter Ihrem Schritt „Datensatz suchen“ hinzuzufügen.
Suchen und wählen Sie aus **PowerShell** Schritttyp.

b. In **PowerShell-Schritt** Füllen Sie die Felder nach Bedarf aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PowerShell-Schrittfelder

Feld	Wert
Verbindung	Wählen Sie Aus **Definieren Sie Die Verbindung Inline**
Anmeldeinformationsalias	Wählen Sie Ihren Anmeldeinformationsalias aus
Host	Geben Sie die IP-Adresse des Windows-Zielservers ein
Port	Geben Sie Ein 22 Wenn dies nicht bereits der Standard ist.
MID-Auswahl	Wählen Sie **Spezifischer MID Server** aus.
MID-Server	Ziehen Sie in **MID-Server-Datensatz** Pille aus dem **Daten** Bereich Diese Datenpille ist in sichtbar **Daten** Bereich am rechten Rand des Bildschirms unter **Schritt „Datensatz suchen“** .
Remotingtyp	Wählen Sie Aus **Führen Sie die Ausführung auf einem MID-Server aus, oder lassen Sie Ihr Skript eine Remote-Sitzung einrichten**



6. Erstellen Sie ein Skript für Ihre Testaktion.

a. In **Skripttyp** Feld auswählen **Inline-Skript** .

b. Verwenden Sie das folgende Skript, indem Sie den Beispielpfad durch den Pfad Ihres Testhosts ersetzen.

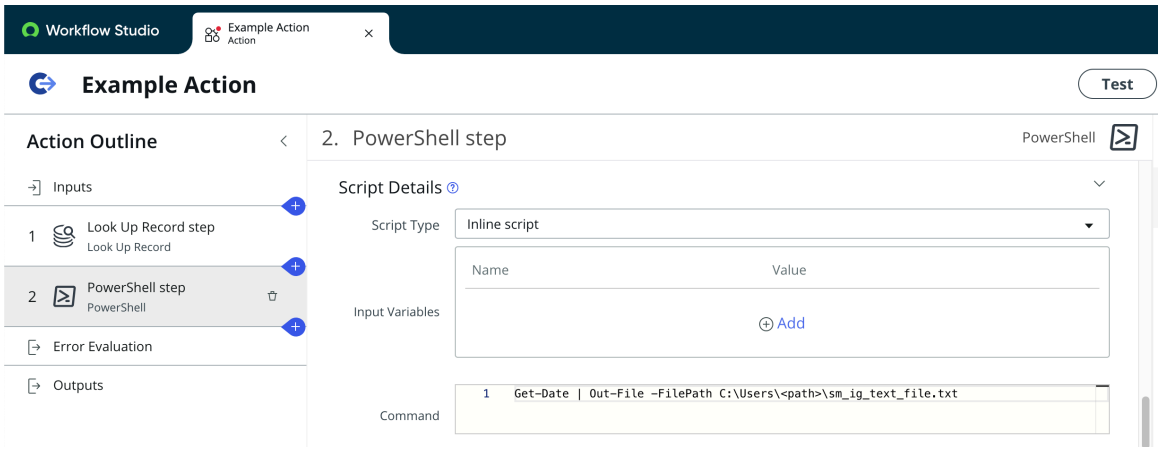
```
Get-Date | Out-File -FilePath C:\Users\<path>\sm_ig_text_file.txt
```

Automatische Übersetzung

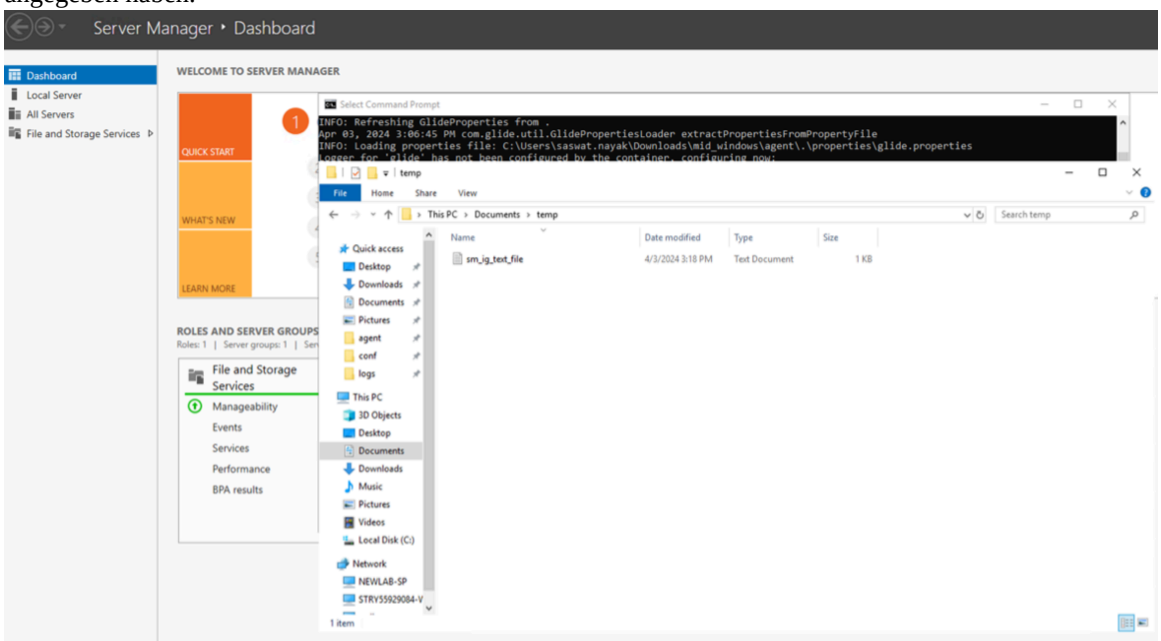
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können auch ein eigenes Skript ausführen, das Ihrer Remote-Hostkonfiguration entspricht. Es ist wichtig, zu bestätigen, dass eine Verbindung mit dem SM-verschlüsselten Wert hergestellt wurde.

c. Wählen Sie aus **Speichern** Schaltfläche zum Speichern Ihrer Aktion.



7. Wählen Sie aus **Testen** Schaltfläche zum Testen Ihrer Aktion.
8. Überprüfen Sie die Ausgabeprotokolle auf Fehlermeldungen.
9. Überprüfen Sie, ob eine Testdatei auf dem Hostserver im Dateipfad erstellt wurde, den Sie im Skript angegeben haben.



Klonen und Geheimnisverwaltung

Erfahren Sie, wie Sie Geheimnisgruppen und geheime Clientgruppen nach einem Klon neu konfigurieren.

Nachdem Sie eine Instanz geklont haben, müssen Ihre Geheimnisgruppen und Client-Geheimnisgruppen möglicherweise neu konfiguriert werden, um wie erwartet zu funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ursprung der Geheimnisgruppe	Verhalten nach einem Klon
Ursprüngliche Instanzgeheimnisgruppen aus der Zielinstanz	Funktioniert wie erwartet, nachdem das fehlende kryptografische Modul manuell importiert wurde. Weitere Informationen finden Sie unter Daten werden über XML exportiert und importiert .
Ursprüngliche geheime Clientgruppen aus Zielinstanz	Funktioniert wie erwartet, nachdem das fehlende kryptografische Modul manuell importiert wurde. Weitere Informationen finden Sie unter Daten werden über XML exportiert und importiert .
Geheime Instanzgruppen aus Quellinstanz geklont	Funktioniert nur, wenn manuell eingerichtet
Geheime Clientgruppen aus Quellinstanz geklont	Arbeiten, wenn sg/Identitätsgruppe/Alias/MID manuell konfiguriert wird

Dashboard „Geheimnisverwaltung“

Verwenden Sie das Geheimnisverwaltungs-Dashboard, um die in Ihrer Instanz konfigurierten Geheimnisgruppen zu überprüfen und sich über Sicherheitsprobleme zu informieren.

Geheime Gruppenübersicht



Die **Geheime Gruppenübersicht** Auf der Registerkarte werden Informationen zu Ihren konfigurierten geheimen Gruppen angezeigt. Verwenden Sie diese Registerkarte, um Informationen zu den Geheimnisgruppen anzuzeigen, die in Ihrer Instanz konfiguriert sind.

Geheime Gruppe nach Typ

Zeigt ein Kreisdiagramm an, das geheime Gruppen anzeigt, die in Ihrer Instanz installiert sind, gruppiert nach Geheimnistyp (Instanzseite der Clientseite).

Geheime Gruppe nach Kriteriumstyp

Zeigt ein Kreisdiagramm an, das geheime Gruppen mit Kriterien anzeigt, die in Ihrer Instanz nach dem Typ der verwendeten Kriterien konfiguriert sind.

Anzahl der inaktiven Geheimnisgruppen

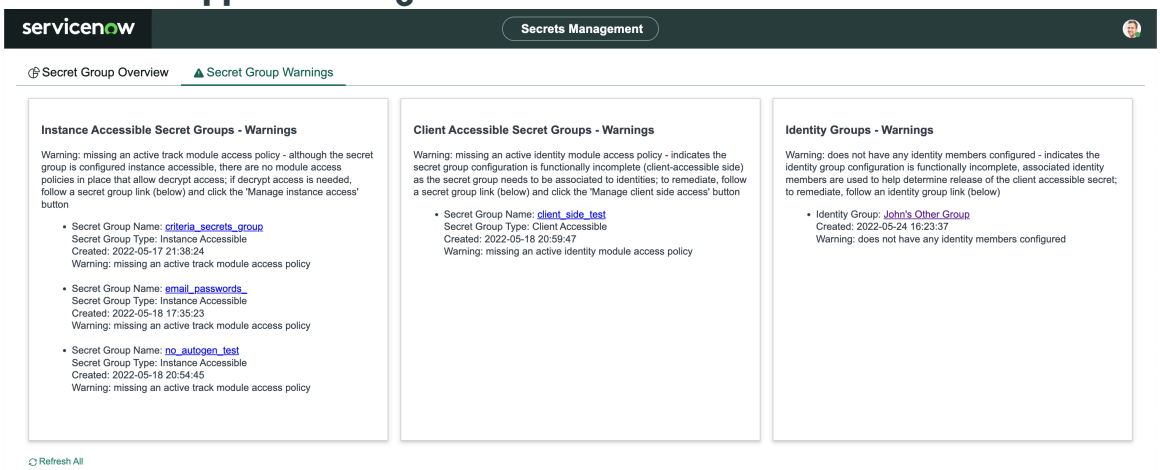
Zeigt eine Anzahl der inaktiven geheimen Gruppen an, die in Ihrer Instanz konfiguriert sind.

Anzahl der dedizierten Geheimnisse.

Zeigt eine Anzahl von Geheimnissen innerhalb grundlegender Geheimnisgruppen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geheime Gruppenwarnungen



Die **Geheime Gruppenwarnungen** Auf der Registerkarte werden Warnungen im Zusammenhang mit Ihren geheimen Gruppen und Identitätsgruppen angezeigt.

Geheime Gruppen mit Instanzzugriff – Warnungen

Diese Karte zeigt Warnungen an, wenn geheime Gruppen ohne aktive Zugriffsrichtlinien vorhanden sind. Wählen Sie einen geheimen Gruppennamen aus, um diesen Datensatz anzuzeigen.

Für Client zugängliche geheime Gruppen – Warnungen

Diese Karte zeigt Warnungen an, wenn vom Client zugängliche geheime Gruppen vorhanden sind, die keine aktive Zugriffsrichtlinie für das Identitätsmodul (Identity Module Access Policy, MAP) haben. Wählen Sie einen geheimen Gruppennamen aus, um diesen Datensatz anzuzeigen.

Identitätsgruppen – Warnungen

Diese Karte zeigt Warnungen an, wenn Identitätsgruppen vorhanden sind, für die keine Gruppenmitglieder konfiguriert sind. Wählen Sie den Namen der Identitätsgruppe aus, um den Datensatz anzuzeigen.

Hinweis: Das Geheimnismanagement-Dashboard ist Teil von Geheimnismanagement Enterprise. Secrets Management Enterprise ist ein bezahltes Plugin, das ServiceNow Mitarbeiter müssen in Ihrer Produktionsinstanz aktivieren.

Geheimnisverwaltungsrollen

Geheimnisverwaltung fügt diese Rollen hinzu.

Geheimnisadministrator [sn_Secrets.admin]

Weisen Sie anderen Anwendern nicht-Administratorrollen zu. Geheimnisadministratoren haben die gleichen Berechtigungen wie Geheimnismanager und Betrachter.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Besondere Erwägungen

Wichtig: Vermeiden Sie die Gewährung einer Administratorrolle, wenn speziellere Rollen verfügbar sind.

- Ein Anwender muss sowohl über die Rollen admin als auch Security_admin verfügen, um die Rolle sn_Secret.admin zugewiesen zu werden.
- Vermeiden Sie die Gewährung einer Administratorrolle, wenn gezieltere Rollen verfügbar sind.

Geheimnismanager [sn_secrets.secret_manager]

Gewähren Sie diese Rolle Anwendern, die eine der folgenden Funktionen ausführen müssen.

- Zeigen Sie geheime und geheime Gruppendatensätze an
- Zeigen Sie den Zugriffsverlauf und andere Informationen zur Nutzungsaktivität an
- Erstellen Sie geheime Gruppen und Filter
- Erstellen Sie geheime Anbieter
- Verschieben Sie Geheimnisse zwischen Geheimnisgruppen
- Ändern Sie die Einstellungen für geheime Gruppen und geheime Anbieter

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Wichtig: Geheimnismanager können Geheimnisse nicht im nur-Text sehen.

Geheimnisbetrachter [sn_Secrets.Viewer]

Gewähren Sie diese Rolle Anwendern, die geheime und geheime Gruppendatensätze anzeigen können müssen.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Besondere Erwägungen

Keine.

Erstellen Sie ein kryptografisches Modul der geheimen Gruppe

Erstellen Sie ein kryptografisches Modul für geheime Gruppen, um die Verschlüsselung und Entschlüsselung durchzuführen.

Vorbereitungen

Erforderliche Rolle:

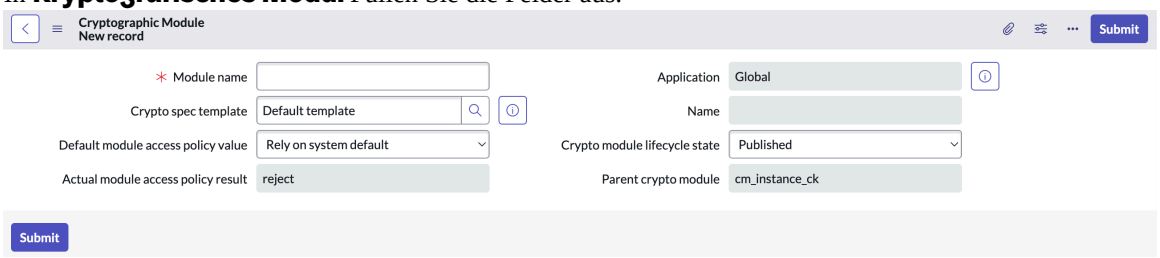
- Administrator
- sn_Secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_Manager
- sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Krypto-Modul für geheime Gruppe erstellen**an.
2. Wählen Sie den Typ des Gruppen-Krypto-Moduls aus, das Sie erstellen möchten.

Kryptografischer Modultyp	Beschreibung
Ein über die Instanz zugängliches Geheimnis-Krypto-Modul erstellen	Erstellen Sie für die Instanz zugängliche Geheimnisse, die von Ihrer Instanz entschlüsselt werden können.
Erstellt ein vom Client zugängliches geheimes Krypto-Modul	Erstellen Sie für den Client zugängliche Geheimnisse, die mit Ihrem eigenen Schlüssel verschlüsselt werden ServiceNow Zugriff nicht möglich.

3. In **Kryptografisches Modul** Füllen Sie die Felder aus.



Feld	Beschreibung
Modulname	Beschreibender Name für Ihr Modul
Anwendung	Der Anwendungsbereich, der Ihr Modul enthält. Dieses Feld wird automatisch mit dem aktuellen Modul ausgefüllt.
Krypto-Spezifikationsvorlage	**Standardvorlage** Ist standardmäßig ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name des Moduls. Dieser Name wird automatisch von basierend auf dem Anwendungs- und Modulnamen generiert.
Standardwert der Modulzugriffsrichtlinie	○ Systemvorgabe verwenden ○ Ablehnen ○ Titel
Lebenszyklusstatus kryptografisches Modul	Gibt an, ob sich das Modul in einem befindet **Entwurf** Oder **Veröffentlicht** status.
Tatsächliches Ergebnis der Modulzugriffsrichtlinie	Dieses Feld dient zu Informationszwecken und ist schreibgeschützt.
Übergeordnetes kryptografisches Modul	Das übergeordnete kryptografische Modul, das durch den kryptografischen Modultyp bestimmt wird, den Sie im vorherigen Schritt ausgewählt haben. Dieses Feld ist schreibgeschützt.

4. Wählen Sie **Absenden**.

Erstellen Sie eine grundlegende geheime Gruppe

Erstellen Sie eine grundlegende Geheimnisgruppe, um alle Geheimnisse unabhängig von ihren Kriterien zu gruppieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Grundlegende geheime Gruppen können jedes Geheimnis enthalten, das Sie ihnen hinzufügen, unabhängig von ihrer Tabelle, ihrem Umfang oder ihrer Anwendung. Nach der Erstellung fügen Sie der Gruppe manuell Geheimnisse hinzu. Um eine Gruppe speziell für alle Geheimnisse zu erstellen, die ein allgemeines Attribut wie diese teilen, erstellen Sie eine geheime Gruppe mit Kriterien gemäß den Anweisungen in Erstellen Sie eine geheime Gruppe mit Kriterien.

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**an.
2. Wählen Sie **Neu**.
3. Bei **Welche Art von Geheimnisgruppe möchten Sie erstellen?** Wählen Sie aus **Grundlegende Geheime Gruppe** .
4. In **Geheime Gruppe** Füllen Sie die Felder aus.

Geheime Gruppenfelder

Feld	Beschreibung
Gruppenname	Name für die Gruppe **Hinweis:** Geheime Gruppennamen dürfen nur Kleinbuchstaben, Zahlen und Unterstriche (_) enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geheimnistyp	Gibt an, ob die Gruppe ist **Instanz zugänglich** Oder **Vom Client zugänglich** .
Autogen-Modul	Generiert ein neues kryptografisches Modul für diese geheime Gruppe. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist standardmäßig aktiviert.
Anwendung	Die bereichsbezogene Anwendung für diesen Datensatz. Dieses schreibgeschützte Feld wird automatisch mit dem aktuellen Umfang ausgefüllt.
Kurzbeschreibung	Beschreibung der Gruppe
Krypto-Modul	Wählen Sie das kryptografische Modul aus, das mit dieser Gruppe verwendet werden soll. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist nur sichtbar, wenn **Autogen-Modul** Ist nicht ausgewählt. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über die Modulzugriffsrichtlinie **Hinweis:** Sie können die Modulzugriffsrichtlinien im Zusammenhang mit Ihrer geheimen Gruppe mit überprüfen **Verwalten Sie den Instanzzugriff** Schaltfläche.

5. Klicken Sie auf **Absenden**.

Hinweis: Wenn eine geheime Gruppe erstellt wird, ist sie standardmäßig inaktiv. Kehren Sie zum Gruppendatensatz zurück, und wählen Sie aus **Aktiv** Zum Aktivieren der Gruppe.

Erstellen Sie eine geheime Gruppe mit Kriterien

Erstellen Sie eine geheime Gruppe mit Kriterien, um Geheimnisse, die in Passwort2-Felder eingegeben werden, automatisch zu organisieren, wenn sie gemeinsame Kriterien wie Tabelle, Umfang oder Anwendung verwenden.

Vorbereitungen

Erforderliche Rolle: admin, KMF_admin, sn_secrets.secret_manager und sn_kmf.cryptographic_Manager

Geheimnisse innerhalb dieses Geheimnisgruppentyps müssen alle allgemeine Kriterien aufweisen. Erwägen Sie für Gruppen ohne diese Einschränkung, eine grundlegende geheime Gruppe zu erstellen. Erfahren Sie mehr über das Erstellen einer grundlegenden geheimen Gruppe in Erstellen Sie eine grundlegende geheime Gruppe.

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**an.
2. Wählen Sie **Neu**.
3. Bei **Welche Art von Geheimnisgruppe möchten Sie erstellen?** Prompr, wählen Sie aus **Geheime Gruppe mit Kriterien** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. In **Geheime Gruppe** Füllen Sie die Felder aus.

Geheime Gruppenfelder

Feld	Beschreibung
Gruppenname	Name für die Gruppe **Hinweis:** Geheime Gruppennamen dürfen nur Kleinbuchstaben, Zahlen und Unterstriche (_) enthalten.
Geheimnistyp	Gibt an, ob die Gruppe ist **Instanz zugänglich** Oder **Vom Client zugänglich.**
Autogen-Modul	Generiert ein neues kryptografisches Modul für diese geheime Gruppe. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist standardmäßig aktiviert.
Anwendung	Die bereichsbezogene Anwendung für diesen Datensatz. Dieses schreibgeschützte Feld wird automatisch mit dem aktuellen Umfang ausgefüllt.
Kurzbeschreibung	Beschreibung der Gruppe
Kriteriumstyp	Die Kriterien, die die Geheimnisse in dieser Gruppe teilen. ○ Umfang ○ Paket ○ Zieltabelle ○ Geheime Spalte ○ Filterdatensatz
Krypto-Modul	Wählen Sie das kryptografische Modul aus, das mit dieser Gruppe verwendet werden soll. Dieses Modul verschlüsselt und entschlüsselt Ihre Daten. Dieses Feld ist nur sichtbar, wenn **Autogen-Modul** Ist nicht ausgewählt. Weitere Informationen zu Modulzugriffsrichtlinien finden Sie unter Übersicht über die Modulzugriffsrichtlinie **Hinweis:** Sie können die Modulzugriffsrichtlinien im Zusammenhang mit Ihrer geheimen Gruppe mit überprüfen **Verwalten Sie den Instanzzugriff** Schaltfläche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Abhängig von Ihrer Konfiguration, die **Krypto-Modul** Verwendet möglicherweise einen automatisch ausgewählten Wert.

Wenn **Kriteriumstyp** Feld ist auf festgelegt Paket , Und **Autogen-Modul** Feld ist ausgewählt:	Die **Krypto-Modul** Feld ist leer und schreibgeschützt. Ein vorhandenes Password2-Submodul wird verwendet. Wenn kein Password2-Submodul gefunden wird, wird das Glide Encrypter-Modul auf Instanzebene verwendet.
Wenn **Kriteriumstyp** Feld ist auf festgelegt Paket , Und **Autogen-Modul** Feld ist deaktiviert: (Die **Autogen-Modul** Die Auswahl des Felds kann nur von Enterprise-Anwendern aufgehoben werden.)	Die **Krypto-Modul** Das Feld kann bearbeitet werden, und Administratoren können ein zu verwendendes Krypto-Modul auswählen.

5. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.

Hinweis: Wenn eine geheime Gruppe erstellt wird, ist sie standardmäßig inaktiv.

6. Nach dem Speichern des Datensatzes werden möglicherweise zusätzliche Felder angezeigt, je nachdem, wie Sie Ihre Gruppe konfiguriert haben.

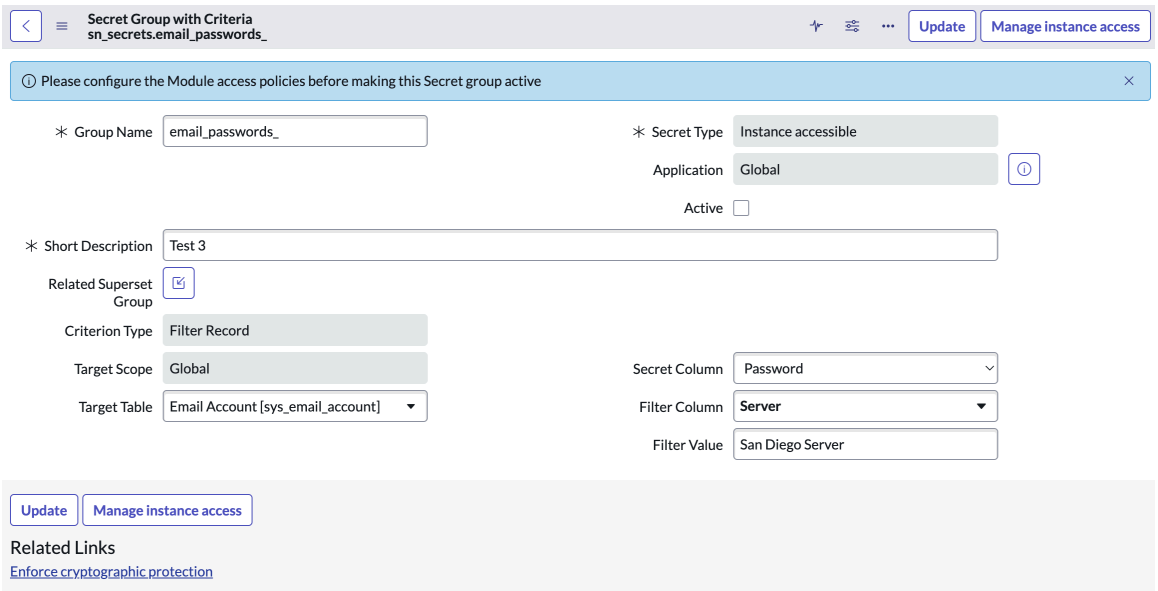
Zusätzliche geheime Gruppenfelder

Feld	Beschreibung
Zielbereich	Bereich, der von den Geheimnissen geteilt wird, die dieser Gruppe zugewiesen werden sollen. Dieses Feld ist nur verfügbar, wenn Sie auswählen Umfang In **Kriterientyp** Feld.
Zielpaket	Paket, das von den Geheimnissen geteilt wird, die dieser Gruppe zugewiesen werden sollen. Dieses Feld ist nur verfügbar, wenn Sie auswählen Paket In **Kriterientyp** Feld.
Zieltabelle	Tabelle, die von den Geheimnissen geteilt wird, die dieser Gruppe zugewiesen werden sollen. Dieses Feld ist nur verfügbar, wenn Sie auswählen Tabelle Oder Geheime Spalte In **Kriterientyp** Feld.
Zielbereich	Anwendungsbereich der in ausgewählten Tabelle **Zieltabelle** Feld. Dieses Feld ist nur sichtbar, wenn Sie auswählen Tabelle , Filterspalte , Oder Geheime Spalte In **Kriterientyp** Feld.
Geheime Spalte	Tabellenspalte, die die Pasword2-Geheimnisse enthält, die Sie in dieser Gruppe enthalten. Die in dieser Liste verfügbaren Felder werden durch die in ausgewählte Tabelle bestimmt **Zieltabelle** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn in der ausgewählten Tabelle keine Spalten vorhanden sind, die Geheimnisse enthalten, wird dieses Feld nur angezeigt – Keine -- Als Auswahl.
Spalte filtern	Die Spalte in der in ausgewählten Tabelle **Zieltabelle** Sie möchten als Filter verwenden. Dieses Feld darf kein Passwort2-Feld sein.
Filterwert	Der Wert, den Sie als Filter verwenden möchten. Dieser Filter gilt für das Feld, das in ausgewählt wurde **Filterspalte** Feld.

Example: Eine instanzzugängliche Gruppe, die alle E-Mail-Account-Passwörter für einen E-Mail-Server enthält



Nächste Maßnahme

Nach dem Erstellen Ihrer Gruppe werden alle neuen Datensätze, die den Kriterien entsprechen, verschlüsselt. Um vorhandene Datensätze mit dem kryptografischen Modul dieser Gruppe zu verschlüsseln, müssen Sie einen Sicherheitsauftrag ausführen. Details finden Sie unter Sicherheitsaufträge zur Geheimnisverwaltung ausführen.

Vom Client zugängliche Gruppen benötigen einen vom Kunden bereitgestellten öffentlichen Schlüssel, um Ihre Geheimnisse zu verschlüsseln. Schritte zum Hochladen dieses Schlüssels finden Sie unter Laden Sie einen öffentlichen Schlüssel für die Geheimnisverwaltung hoch.

Laden Sie einen öffentlichen Schlüssel für die Geheimnisverwaltung hoch

Laden Sie einen öffentlichen Schlüssel für hoch, um Ihre Geheimnisse zu verschlüsseln.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Geheimnisverwaltung** > **Geheimnisgruppen**, Und öffnen Sie den Geheimnisgruppendatensatz.
2. Wählen Sie im Datensatz die aus **Verwalten Sie Den Clientseitigen Zugriff** Schaltfläche.
   Ein neuer Identitätsgruppendatensatz wird geöffnet.
3. Wählen Sie aus **Identitätsschlüssel Hochladen** Schaltfläche.
   A **Importieren Sie das Zertifikat des öffentlichen Identitätsschlüssels** Fenster wird angezeigt.
4. Geben Sie einen Alias für Ihren Schlüssel in ein **Identitätsschlüssel-Alias** Feld.
5. Wählen Sie aus **Importieren** Schaltfläche, um den Schlüssel aus Ihrer lokalen Umgebung hochzuladen.
6. Wählen Sie aus **OK** Schaltfläche.
   Die **Gruppenmodulschlüssel** Feld verwendet den Aliasnamen des Identitätsschlüssels.
7. Wählen Sie Aus **Übermitteln** Zum Speichern des Identitätsgruppendatensatzes.

Sicherheitsaufträge zur Geheimnisverwaltung ausführen

Planen Sie einen Geheimnisverwaltungsauftrag, um Verschlüsselungsaufgaben für Geheimnisfelder in Ihrer Instanz auszuführen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin, Security_admin und sn_Secrets.admin

Um diese Schritte auszuführen, müssen Sie die Rolle „Security_admin“ erhöhen. Details zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle hochstufen

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen**an.
2. Bei **Welche Art von Sicherheitsauftrag möchten Sie erstellen?** Eingabeaufforderung, wählen Sie aus **Geheimnisverwaltungsauftrag** .
3. Füllen Sie im Formular die Felder aus.

Formular „Geheimnisverwaltungsauftrag“

Feld	Beschreibung
Name	Name des Sicherheitsauftrags
Status	Der anfängliche Auftragsstatus ist Neu. Nachdem die Aufgabe wie geplant ausgeführt wurde, wird der Status entsprechend aktualisiert
Zeitfensterstart	Startzeit für den Auftrag im 24-Stunden-Format. Die Ausführung des Auftrags beginnt zum ausgewählten Zeitpunkt.
Zeitfensterende	Endzeit für den Auftrag im 24-Stunden-Format. Wenn der Auftrag bis zu diesem Zeitpunkt nicht abgeschlossen ist, wird er während des nächsten angegebenen Verarbeitungsfensters fortgesetzt, bis der Auftrag abgeschlossen ist.
Durchsetzungsebene	Gibt an, ob sich der Auftrag auf alle Tabellen oder eine Auswahl bestimmter Tabellen oder Felder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	auswirkt. Wählen Sie aus folgenden Möglichkeiten aus: ○ Alle Tabellen ○ Bestimmte Tabellen ○ Bestimmte Felder ○ Bestimmte Pakete ⚠ **Warnung:** Auswählen von **Alle Tabellen** Die Option kann sich auf die Instanzleistung auswirken. Erwägen Sie die Planung zu Zeiten außerhalb der Spitzenzeiten.
Pakete	Die Pakete, die in diesen Auftrag aufgenommen werden sollen. Verschlüsselung wird auf ausgewählte Pakete angewendet. Diese Option wird nur angezeigt, wenn **Durchsetzungsebene** Feld ist auf festgelegt **Bestimmte Pakete**
Tabellen	Die Tabellen, die in diesen Auftrag aufgenommen werden sollen. Die Verschlüsselung wird auf alle anwendbaren Felder in den ausgewählten Tabellen angewendet. Diese Option wird nur angezeigt, wenn **Durchsetzungsebene** Ist auf festgelegt **Bestimmte Tabellen**
Felder	Die Tabellen, die in diesen Auftrag aufgenommen werden sollen. Verschlüsselung wird auf alle ausgewählten Felder angewendet. Diese Option wird nur angezeigt, wenn **Durchsetzungsebene** Ist auf festgelegt **Bestimmte Felder**
Auftragsmodus	Wählen Sie aus folgenden Möglichkeiten aus: **Password2 an Geheimnisverwaltung** Verschlüsseln Sie alle Passwort2-Felder in Ihren Geheimnisgruppen mithilfe der kryptografischen Module, die die Modulzugriffsrichtlinie jeder Gruppe definiert haben. **Geheimnisverwaltung an Password2** Verschlüsseln Sie Daten in Ihren Geheimnisgruppen mit Passwort2-Verschlüsselung erneut. Weitere Informationen zu diesem Verschlüsselungstyp finden Sie unter Passwort2-Verschlüsselung mit KMF . **Durchsetzung geheimer Gruppen** Fragt alle Daten ab, die der in ausgewählten Gruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	entsprechen sollen **Geheime Gruppe** Feld. Wenn sich alle von der Abfrage gefundenen Daten bereits in der Gruppe befinden, nimmt der Auftrag keine Änderungen vor. Wenn die Abfrage Daten findet, die sich noch nicht in der Gruppe befinden, verschlüsselt der Auftrag diese Daten innerhalb der Geheimnisgruppe erneut. **Hinweis:** Wenn die in dieser Abfrage gefundenen Daten bereits verschlüsselt sind und Ihre Instanzen diese Daten nicht entschlüsseln können, werden sie nicht verschlüsselt und der Geheimnisgruppe hinzugefügt.
Geheimnisgruppe	Geheime Gruppe, die die zu verschlüsselnden Geheimnisse enthält. Dieses Feld ist nur verfügbar, wenn **Geheime Gruppe** Ist in ausgewählt **Auftragsmodus** Feld.
Neueingabe von Daten erzwingen	
Zusammenfassung	Zeigt Informationen zum Auftragsfortschritt an. In der Zusammenfassung werden auch Datensätze angezeigt, die vom Auftrag nicht verschlüsselt werden konnten.

4. Wählen Sie **Absenden**.

Nächste Maßnahme

Der Auftrag fragt alle Daten ab, die der ausgewählten geheimen Gruppe entsprechen sollen. Wenn sich alle von der Abfrage gefundenen Daten bereits in der Gruppe befinden, nimmt der Auftrag keine Änderungen vor. Wenn die Abfrage Daten findet, die sich noch nicht in der Gruppe befinden, verschlüsselt der Auftrag diese Daten innerhalb der Geheimnisgruppe erneut. (Wenn die Instanz sie entschlüsseln kann, was bei clientseitigen verschlüsselten Geheimnissen möglicherweise nicht der Fall ist).

Codesignatur

Codesignatur erstellt digitale Signaturen für die Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. Codesignatur ist ein Modul, das als Komponente von lizenziert ist ServiceNow Vault.

Codesignatur und Circle of Trust

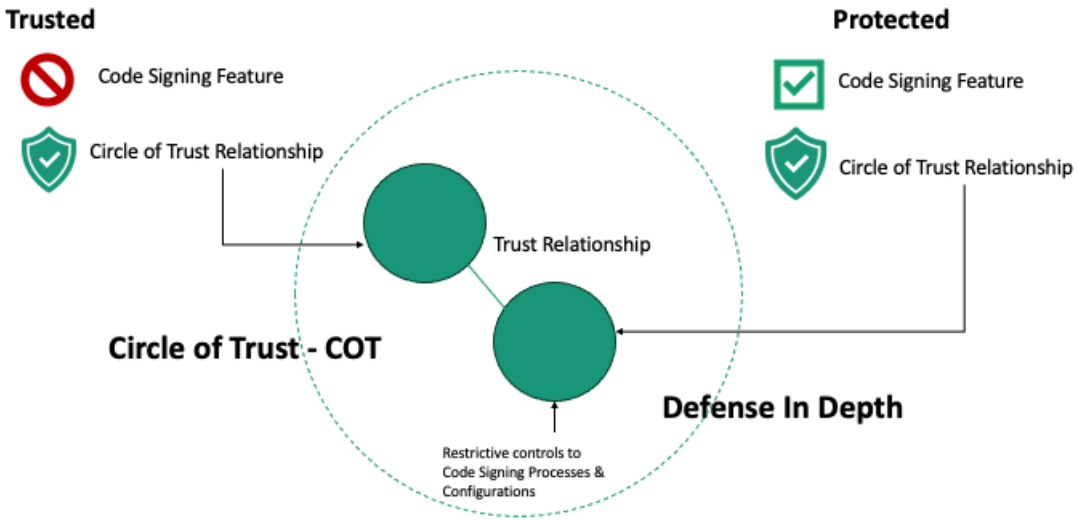
Die Circle of Trust(COT) Ist eine Voraussetzung für die Codesignatur, die eine sichere Kommunikation zwischen Ihren vertrauenswürdigen und geschützten Instanzen erstellt, um sicherzustellen, dass nur autorisierte Anwender auf die Codesignaturfunktion zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrere Sicherheitsmaßnahmen helfen, zu verhindern, dass böswillige Akteure Codesignatur deaktivieren oder missbrauchen, wenn eine geschützte Instanz gefährdet wird. Als Teil der Tiefenverteidigungsstrategie ist COT Verwendet die folgenden Komponenten:

- Steuerungen, die selbst die leistungsstärksten Administratoraccounts einschränken, werden in der geschützten Instanz eingerichtet, um Codesignaturprozesse und -Konfigurationen zu schützen.
- Vertrauenswürdige Instanzen sind erforderlich, um mit geschützten Instanzen zusammenzuarbeiten, um einzurichten Circle of Trust Beziehung. Mindestens eine vertrauenswürdige Instanz ist erforderlich, es können jedoch mehrere vertrauenswürdige Instanzen für die Zusammenarbeit mit der geschützten Instanz konfiguriert werden.

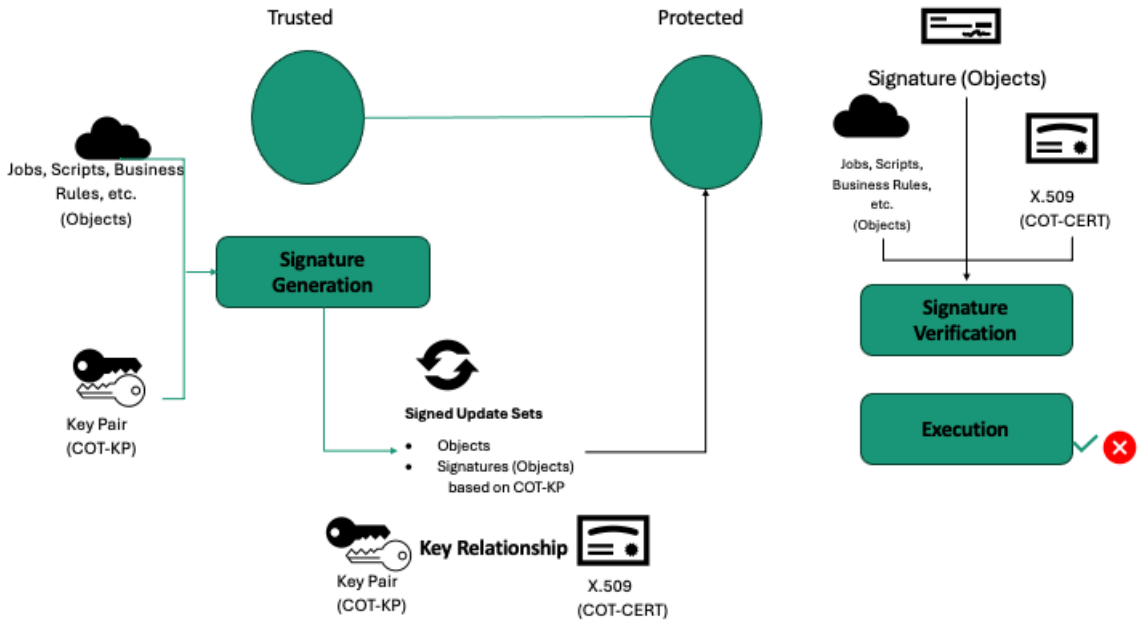
Circle of Trust – Übersicht



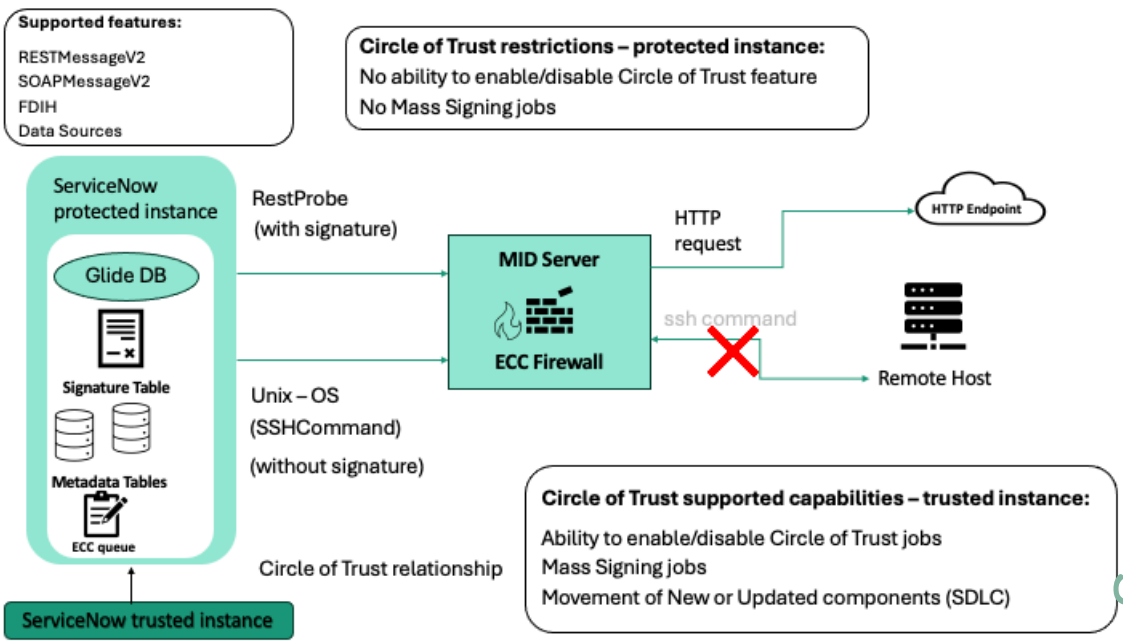
Die Circle of Trust Verwendet Aufträge, Skripts und Business-Regeln zusammen mit einem Schlüsselpaar, um Signaturen zu generieren, um Update-Sätze für die geschützte Instanz zu signieren. Wenn der Auftrag aufgerufen wird, wird die Signatur zusammen mit dem vertrauenswürdigen Zertifikat verifiziert, um geschützte Instanzaktualisierungen auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozess für vertrauenswürdige Update-Sätze



Codesignatur-Flow

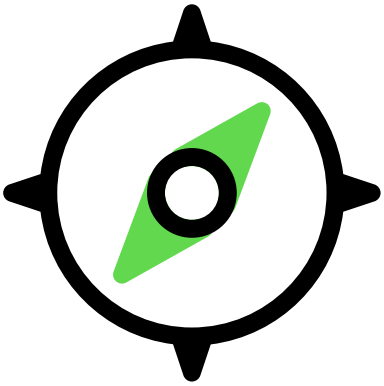


Die Circle of Trust Erfordert eine anfängliche Vertrauensbeziehung zwischen vertrauenswürdigen und geschützten Instanzen, die verhindert, dass nicht autorisierte Anwender mit beliebiger Autorisierungsstufe auf nicht genehmigte Aktivitäten zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

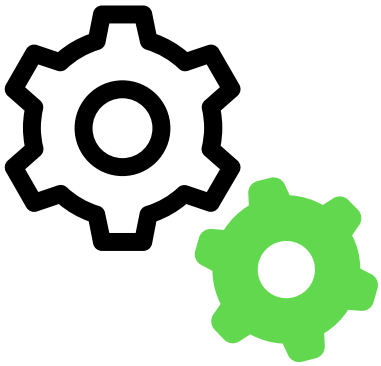
Erste Schritte

Untersuchen



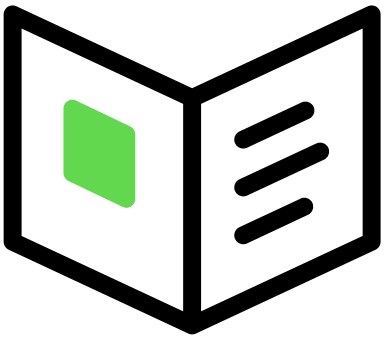
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen der Codesignatur kennen.

Konfigurieren



Aktivieren und konfigurieren Sie die Codesignatur.

Referenz



Rufen Sie Details zu Eigenschaften und zur Fehlerbehebung ab

Verwenden



Erfahren Sie, wie Sie Codesignatur verwenden, um die Authentizität und Integrität Ihrer Daten zu überprüfen.

Problembehandlung und Hilfe

- https://www.servicenow.com/community/secops/ct-p/security-operations
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur Erkunden

Die Codesignatur bietet eine kryptografische Verifizierung, um sicherzustellen, dass nur autorisierte Skripts auf MID-Servern ausgeführt werden können. Die Codesignatur verhindert, dass nicht autorisierte oder manipulierte ECC-Warteschlangendatensätze von MID-Servern verarbeitet werden, wodurch die Integrität der Integrationen zwischen ServiceNow und externen Systemen aufrechterhalten wird.

Codesignatur erstellt digitale Signaturen für Ihre Daten, die später überprüft werden, um die Authentizität und Integrität der Daten zu bestätigen. Codesignatur ist ein Modul, das als Komponente von lizenziert ist ServiceNow Vault.

Hinweis: Die Kundenservice und Support Das Team muss Zugriff auf die Codesignatur gewähren.

Codesignatur deklariert die Absicht hinter dem ausgeführten Vorgang und validiert, ob die Ressource oder der Datensatz für den beabsichtigten Zweck verwendet werden kann. Um die Codesignatur zu erleichtern, die Key Management Framework(KMF) Verwendet digitale Zertifikate und asymmetrische Verschlüsselung nach Industriestandard für digitale Signaturen.

Verwenden Sie Codesignatur intern auf Plattform- und Infrastrukturseite. Codesignatur bietet eine Möglichkeit, den Inhalt bestimmter Tabellen oder einer Teilmenge von Datensätzen in einer bestimmten Metadatentabelle zu signieren.



Codesignatur verwendet einen sicheren Circle of Trust(COT) Zwischen Ihren vertrauenswürdigen und geschützten Instanzen, um sicherzustellen, dass nur autorisierte, sichere vertrauenswürdige Instanzen auf die Codesignaturfunktion zugreifen können.

Hinweis: Codesignatur ist in der geschützten Instanz und nicht in der vertrauenswürdigen Instanz aktiviert.

Wie Codesignatur Ihre Umgebung schützt

Ohne Codesignatur ein Angreifer, der Zugriff auf erhält ServiceNow Datensätze können SQL-Anweisungen in einer geschützten Instanz ändern. Wenn der MID-Server diese Datenquellenanforderung verarbeitet, werden die schädlichen SQL-Befehle ausgeführt, was die Systemintegrität und -Sicherheit gefährden könnte.

Wenn Sie eine Circle of Trust-Architektur mit Codesignatur implementieren, erfolgt die Übertragung von Daten auf den MID-Server nach dem folgenden Verifizierungsprozess. Dieser Prozess trägt dazu bei, sicherzustellen, dass nur autorisierter Code, der aus der vertrauenswürdigen Instanz stammt, auf dem MID-Server ausgeführt werden kann. Die Prozesse reduzieren potenzielle Angriffsvektoren, die andernfalls Ihre Systeme gefährden könnten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Digitale Signaturen werden auf Datenquellen angewendet, die in der vertrauenswürdigen Instanz erstellt oder aktualisiert wurden.
2. Verwenden Sie den Codesignaturprozess, um die signierten Daten von der vertrauenswürdigen Instanz in die geschützte Instanz zu übertragen
3. Der MID-Server verifiziert die digitale Signatur für alle eingehenden Anforderungen und lehnt alle Anforderungen ohne gültige Signaturen automatisch ab.
4. Wenn der MID-Server eine Anforderung ablehnt, protokolliert er diese Ablehnung und sendet eine Benachrichtigung an die geschützte Instanz.

Vorteile der Implementierung der Codesignatur

Codesignatur bietet mehrere wichtige Vorteile:

Ausführungssteuerung

Nur kryptografisch verifizierte Skripts können auf MID-Servern ausgeführt werden

Manipulationserkennung

Alle Änderungen an signierten Datensätzen werden sofort identifiziert und blockiert.

Automatisierter Schutz

Das System verarbeitet die Durchsetzung der Sicherheit, ohne dass ein manuelles Eingreifen erforderlich ist.

Umfassende Protokollierung

Alle Fehler bei der Signaturverifizierung generieren detaillierte Audit-Datensätze.

Codesignaturvalidierung und -Aufträge

Alle Metadatentabellen mit gültigen Konfigurationen werden zum Build-Zeitpunkt mit dem Plugin „Codesignaturmetadaten“ signiert (`Com.Glide.Code_Signing`). Wenn Sie Tabellen signieren, haben Administratoranwender mit der Rolle „Sicherheitsadministrator“ Zugriff auf Codesignaturverschlüsselungsaufträge:

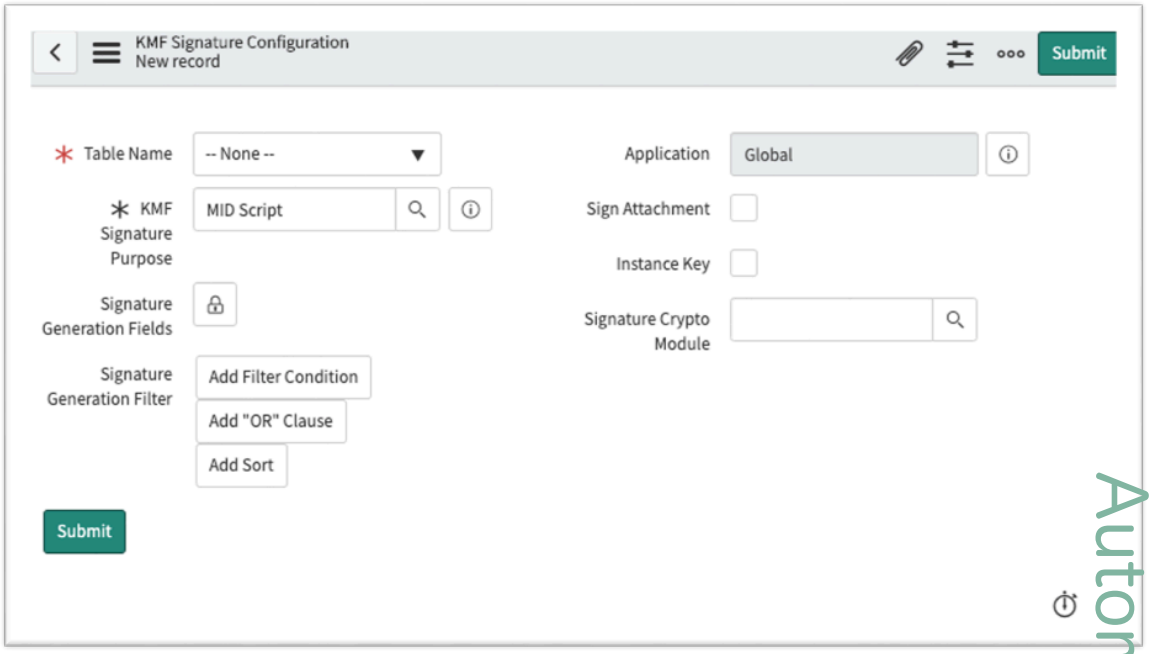
- Update-Sätze signieren.
- Massensignierungsdatensätze.
- Massensignierungsanhänge.

Update-Satz signieren

Dieser Auftrag signiert Datensätze, die einer Signaturkonfiguration im Update-Satz entsprechen. Der Auftrag fügt dem Update-Satz auch alle neuen Signaturdatensätze und Verifizierungszertifikate hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

KMF-Signaturdatensatz für Update-Satz



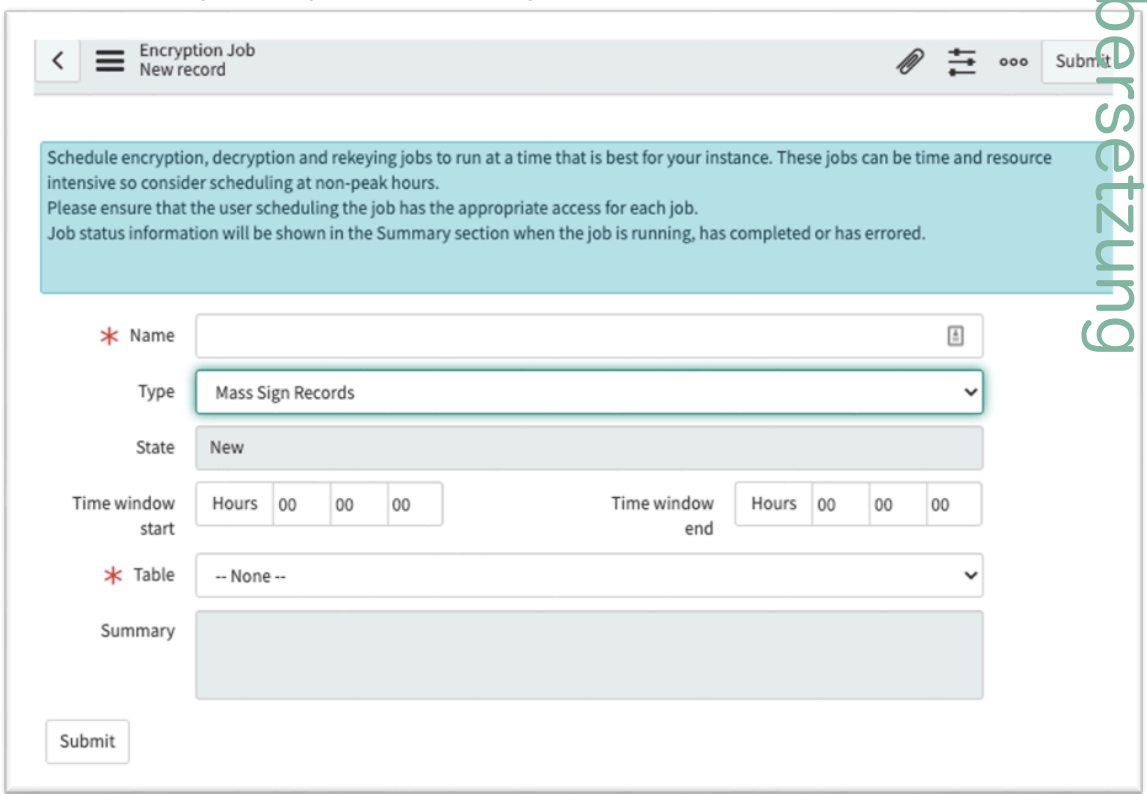
Massensignierungsdatensätze

Dieser Auftrag signiert alle Datensätze, die der Signaturkonfiguration entsprechen, die auf eine bestimmte Metadatentabelle angewendetwird.

Massensignierungsanhänge

Dieser Auftrag signiert alle Anhangsdatensätze, die an eine Tabelle angehängt sind, die einer angegebenen Signaturkonfiguration entspricht.

Verschlüsselungsauftrag zum Massen-Signieren von Datensätzen

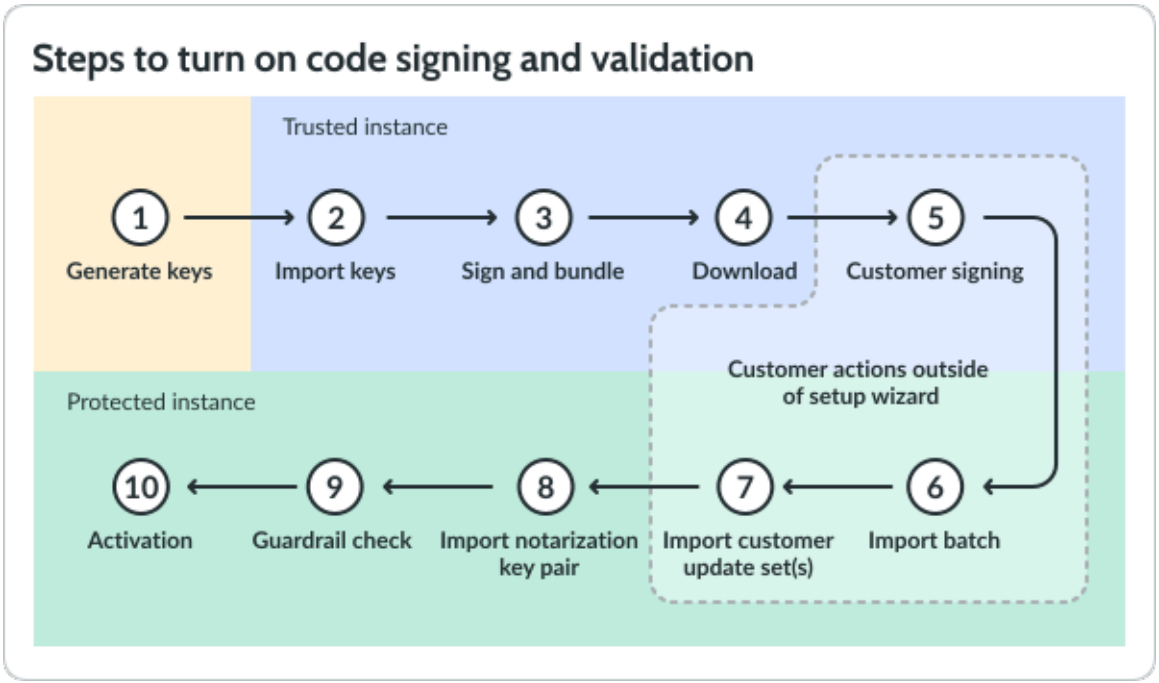


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur Wird Konfiguriert

Aktivieren und konfigurieren Sie die Codesignatur, um die Authentizität und Integrität Ihrer Daten zu überprüfen.



Codesignatur Enterprise erfordert eine anfängliche Vertrauensbeziehung zwischen vertrauenswürdigen und geschützten Instanzen, die verhindert, dass nicht autorisierte Anwender mit einer Autorisierungsstufe auf nicht genehmigte Aktivitäten zugreifen.

Lesen Sie die einzelnen Themen, um die Konfigurationsschritte zum Einrichten von abzuschließen Circle of Trust Mit Codesignatur Enterprise:

Weisen Sie die Rolle Codesignaturadministrator zu

Weisen Sie einem Anwender die Rolle „Codesignaturadministrator“ zu, um auf die Konfigurations-Experience für Codesignatur zuzugreifen.

Konfigurieren Sie Codesignatur Enterprise auf Ihrer vertrauenswürdigen Instanz

Aktivieren Sie die Codesignatur in Ihrer vertrauenswürdigen Instanz.

Laden Sie Ihre Codesignaturkonfigurationsdatei in Ihre geschützte Instanz hoch

Laden Sie die Konfigurationsdatei hoch, die in Ihrer vertrauenswürdigen Instanz generiert wurde.

Konfigurieren Sie Codesignatur Enterprise auf Ihrer geschützten Instanz

Aktivieren und konfigurieren Sie die Codesignatur in Ihrer geschützten Instanz.

Aktivieren Sie die Zertifikatvalidierung

Aktivieren Sie die Zertifikatvalidierung in Ihrer Instanz.

Codesignatur deaktivieren

Deaktivieren Sie die Codesignatur in Ihrer geschützten Instanz.

Hinweis: Dieser optionale Schritt ist nicht Teil der anfänglichen Konfiguration für Codesignatur

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weisen Sie die Rolle Codesignaturadministrator zu

Weisen Sie einem Anwender die Rolle „Codesignaturadministrator“ zu, um auf die Konfigurations-Experience für Codesignatur zuzugreifen.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- security_admin

Wichtig: Der Anwender, dem die Rolle „Codesignaturadministrator“ zugewiesen ist, muss sich im globalen Bereich befinden.

Prozedur

1. Wählen Sie eine vertrauenswürdige Instanz aus, die verwendet werden soll.
   Die vertrauenswürdige Instanz wird verwendet, um Aufträge zu erstellen, Datensätze zu signieren und andere erforderliche Aufgaben auszuführen, bevor die Signaturvalidierung für Ihre geschützte Instanz aktiviert wird.
2. Navigieren zu **Alle** > **Codesignatur** > **Administration** > **Rollenverwaltung**an.
3. Gewähren Sie einem Anwender die Rolle „Codesignaturadministrator“, indem Sie einen Anwender aus dem verschieben **Verfügbare Anwender** Liste zu **Ausgewählte Anwender** Liste.
4. Wählen Sie **Speichern**.

Wichtig: Der der Rolle zugewiesene Anwender muss sich abmelden und erneut anmelden, um Codesignaturaufgaben auszuführen.

Ergebnis

Der ausgewählte Anwender hat die Rolle Codesignaturadministrator. Ein Anwender mit dieser Rolle kann auf die Konfigurations-Experience für Codesignatur zugreifen und Anwendern andere Codesignaturrollen zuweisen.

Weitere Informationen zu Codesignaturrollen finden Sie unter Mit Codesignatur installierte Rollen.

Konfigurieren Sie Codesignatur Enterprise auf Ihrer vertrauenswürdigen Instanz

Aktivieren und konfigurieren Sie die Codesignatur in Ihrer vertrauenswürdigen Instanz.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- security_admin
- Codesigning_admin

Hinweis: Die Rolle „Codesigning_admin“ kann mit dem in beschriebenen Prozess zugewiesen werden Weisen Sie die Rolle Codesignaturadministrator zu.

- sn_kmf.cryptographic_Manager

Sie müssen mindestens ein kryptografisches Schlüsselpaar und ein Zertifikat (p12-Dateierweiterung) für die Kundensignierung und die Verwaltung von Circle of Trust

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(COT) haben. Um die Sicherheit zu verbessern, sollten Sie separate kryptografische Schlüsselpaare für die Kundensignierung und die COT-Verwaltung verwenden.

⚠ **Warnung:** Nach Abschluss dieses Prozesses haben Sie eine Konfigurationsdatei heruntergeladen, die innerhalb einer Stunde auf Ihrer geschützten Instanz installiert werden muss. Stellen Sie sicher, dass Sie nach diesem Prozess Zeit haben, um die Konfigurationsdatei in Ihre geschützte Instanz hochzuladen. Details zu diesem Prozess finden Sie unter Laden Sie Ihre Codesignaturkonfigurationsdatei in Ihre geschützte Instanz hoch.

Prozedur

1. Navigieren Sie in Ihrer vertrauenswürdigen Instanz zu **Alle** > **Codesignatur** > **Konfiguration** > **Geführtes Setup** Zum Öffnen der Konfigurationsseite für Codesignatur.
2. In **Instanztyp** Feld auswählen **Vertrauenswürdige Instanz** .
3. Wählen Sie aus **Als Nächstes** Schaltfläche.
4. In **Aktion** Feld unter **Wählen Sie die Aktion aus, die Sie ausführen möchten** , Wählen Sie aus **Aktivieren Sie die Codesignatur** .
5. Neben **Anhänge** In **Kunde signiert Schlüsselpaar und Zertifikat** Abschnittsauswahl **+Datei Hinzufügen** Zum Hochladen eines kryptografischen Schlüsselpaars (p12-Dateierweiterung) zur Verwendung für die Kundensignatur.

   Tipp: Wenn **+Datei Hinzufügen** Option ist nicht verfügbar. Stellen Sie sicher, dass Sie sich im globalen Bereich befinden und die Rolle sn_kmf.cryptographic_Manager haben.

6. In **Passwort** Geben Sie das Passwort für das hochgeladene Schlüsselpaar ein.
7. Wählen Sie **Importieren**.
8. Wählen Sie Aus **Fahren Sie Fort** Um zum nächsten Abschnitt zu wechseln.
9. Neben **Anhänge** In **COT-Administrationsschlüsselpaar und Zertifikat** Abschnittsauswahl **+Datei Hinzufügen** Zum Hochladen eines kryptografischen Schlüsselpaars (p12-Dateierweiterung) zur Verwendung für die Kundensignatur.
10. In **Passwort** Geben Sie das Passwort für das hochgeladene Schlüsselpaar ein.
11. Wählen Sie **Importieren**.
12. Wählen Sie Aus **Fahren Sie Fort** Um zum nächsten Abschnitt zu wechseln.
13. Auf der **Konfiguration Exportieren** Dateiseite auswählen **Exportieren** Zum Erstellen und Herunterladen einer Konfigurationsdatei, die zum Aktivieren der Codesignatur in Ihrer geschützten Instanz verwendet wird. Der Exportprozess lädt eine XML-Datei auf Ihren lokalen Computer herunter, um sie in den Schrittdetails in zu verwenden Konfigurieren Sie Codesignatur Enterprise auf Ihrer geschützten Instanz.

    Hinweis: Codesignatur erzwingt Grenzwerte für große Update-Sätze, um die Anwender-Experience zu verbessern. Die maximale Größe für einen Update-Satz beträgt 10.000 Datensätze.

Laden Sie Ihre Codesignaturkonfigurationsdatei in Ihre geschützte Instanz hoch

Laden Sie die Konfigurationsdatei hoch, die in Ihrer vertrauenswürdigen Instanz generiert wurde.

Vorbereitungen

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Administrator
- security_admin
- Codesigning_admin

> **Hinweis:** Die Rolle „Codesigning_admin“ kann mit dem in beschriebenen Prozess zugewiesen werden Weisen Sie die Rolle Codesignaturadministrator zu.

- sn_kmf.cryptographic_Manager

Sie benötigen auch die Konfigurationsdatei, die in den Schritten generiert wurde Konfigurieren Sie Codesignatur Enterprise auf Ihrer vertrauenswürdigen Instanz.

Prozedur

1. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
2. Wählen Sie Aus **Update-Satz aus XML importieren** Am unteren Rand des abgerufenen **Update-Sätze** Liste.
3. Wählen Sie Aus **Wählen Sie Datei** , Und wählen Sie Ihre Konfigurationsdatei (XML-Dateierweiterung) aus.
4. Wählen Sie **Hochladen** aus.
   Sie sollten sehen **Codesigning-Konfiguration** Update-Satz in **Update-Sätze Abgerufen** Liste.
5. Wählen Sie aus, und öffnen Sie **Codesigning-Konfiguration** Update-Satz.
6. Wählen Sie Aus **Vorschau Des Update-Satz-Batches Anzeigen** .
   Wenn während der Vorschau Konflikte auftreten, lösen Sie sie, indem Sie auswählen **Akzeptieren Sie das Remote-Update** Oder **Lösen Sie bekannte CS-Konflikte** .
7. Wählen Sie nach der Lösung von Konflikten aus **Update-Satz-Batch Bestätigen** .

Konfigurieren Sie Codesignatur Enterprise auf Ihrer geschützten Instanz

Aktivieren und konfigurieren Sie die Codesignatur in Ihrer geschützten Instanz.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- security_admin
- Codesigning_admin

> **Hinweis:** Die Rolle „Codesigning_admin“ kann mit dem in beschriebenen Prozess zugewiesen werden Weisen Sie die Rolle Codesignaturadministrator zu.

- sn_kmf.cryptographic_Manager

Prozedur

1. Navigieren Sie in Ihrem PPI zu **Alle** > **Codesignatur** > **Konfiguration** > **Geführtes Setup** Zum Öffnen der Konfigurationsseite für Codesignatur.
2. In **Instanztyp** Feld auswählen **Geschützte Instanz** .
3. Wählen Sie aus **Als Nächstes** Schaltfläche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie aus **Bestätigen Sie, dass der Update-Satz für die Codesignaturkonfiguration importiert und bestätigt wurde** Kontrollkästchen.
5. Wählen Sie aus **Als Nächstes** Schaltfläche.
6. Warten Sie, bis die Zertifikatinstallation abgeschlossen ist.
   Eine blaue Warnmeldung wird angezeigt, die angibt, dass Elemente aus der Konfigurationsdatei installiert werden. Die Warnung wird nach einigen Sekunden ausgeblendet, wenn die Installation abgeschlossen ist.
7. Neben **Anhänge** In **Laufzeit-/Notarisierungsschlüsselpaar und Zertifikat** Abschnittsauswahl **+Datei Hinzufügen** Zum Hochladen eines kryptografischen Schlüsselpaars (p12-Dateierweiterung) zur Verwendung für Laufzeit-/Notarisierungszwecke.
   Sie können ein Schlüsselpaar aus der vertrauenswürdigen Instanz wiederverwenden oder ein neues speziell für diese Verwendung hochladen.

   Tipp: Wenn **+Datei Hinzufügen** Option ist nicht verfügbar. Stellen Sie sicher, dass Sie sich im globalen Bereich befinden und die Rolle sn_kmf.cryptographic_Manager haben.

8. In **Passwort** Geben Sie das Passwort für das hochgeladene Schlüsselpaar ein.
9. Wählen Sie **Importieren**.
10. Wählen Sie Aus **Fahren Sie Fort** Um zum nächsten Abschnitt zu wechseln.
11. Warten Sie, während Ihre Instanz eine Schutzplanprüfung durchführt.
    Diese Prüfung scannt Ihre Instanz auf ungültige Signaturen. Dies kann einige Zeit dauern. Beenden oder aktualisieren Sie die Seite erst, wenn der Scan abgeschlossen ist.

    Dieser Workflow identifiziert Signaturen, die mit abgelaufenen oder inaktiven Zertifikaten generiert wurden, und signiert die betroffenen Datensätze erneut. Um die Leistung zu verbessern, teilt der Workflow den Prozess jetzt in mehrere Ereignisse auf und führt sie parallel aus.

12. Wenn der Scan ungültige Signaturen findet, wählen Sie aus **Bericht Herunterladen** .

    Auswählen **Bericht Herunterladen** Lädt einen Bericht herunter (`scan_report.txt`), mit dem Sie die ungültigen Signaturen untersuchen und beheben können.

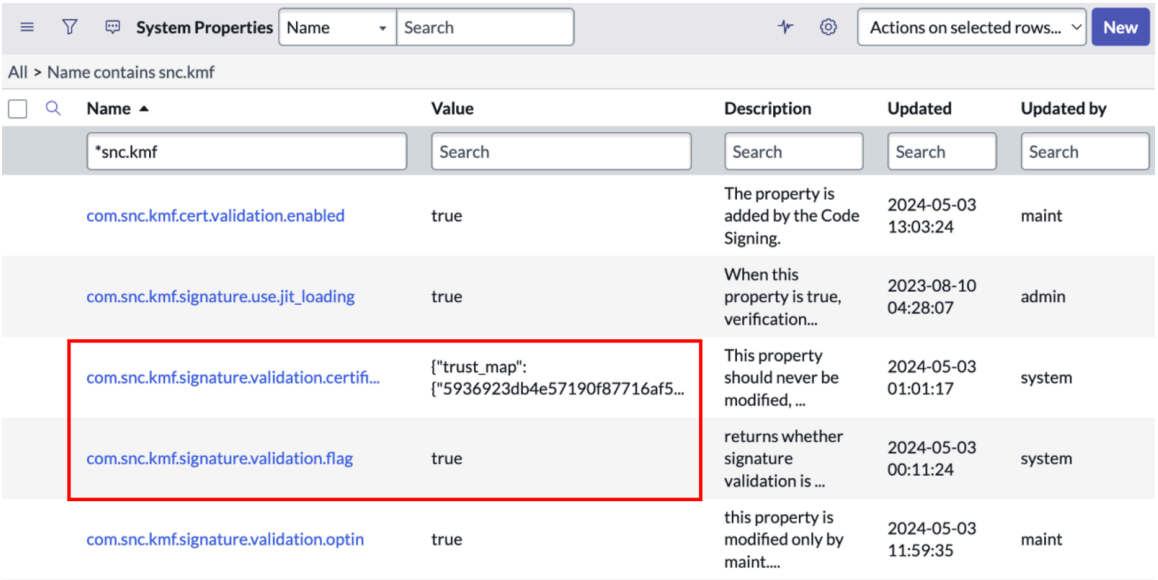
    Aktualisieren Sie nach der Behebung von Fehlern die Seite, um die Prüfung erneut auszuführen.

13. Wenn keine Fehler vorhanden sind, wählen Sie aus **Schließen Sie das Setup ab** .
14. Warten Sie, bis die Konfigurationsaufträge abgeschlossen sind.
    Ihre Instanz führt einen oder mehrere Aufträge aus, um den Konfigurationsprozess abzuschließen. Beenden oder aktualisieren Sie die Seite erst, wenn die Aufträge abgeschlossen sind. Wenn Sie fertig sind, sollte eine angezeigt werden **Codesignaturkonfiguration erfolgreich abgeschlossen** Nachricht.

Ergebnis

Die Signaturvalidierung wird jetzt in Ihrer Produktionsinstanz erzwungen. Sie können den erfolgreichen Abschluss überprüfen, indem Sie sich Ihre Systemeigenschaften ansehen. Suchen Sie nach **Com.snc.kmf.Signature.validation.Flag** Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_property], und stellen Sie sicher, dass sie einen Wert von hat **Wahr** . Überprüfen Sie, ob **Com.snc.kmf.Signature.validation.certificate_Trust** Eigenschaft hat keinen leeren Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aktivieren Sie die Zertifikatvalidierung

Schützen Sie Ihre Instanz mit zertifikatbasierter Validierung.

Vorbereitungen

Erforderliche Rolle:

- Codesigning_admin
- security_admin
- sn_kmf.cryptographic_Manager

Prozedur

1. Navigieren Sie in Ihrer vertrauenswürdigen Instanz zu **Alle** > **Codesignatur** > **Konfiguration** > **Geführtes Setup** Zum Öffnen der Konfigurationsseite für Codesignatur.
2. In **Instanztyp** Feld auswählen **Vertrauenswürdige Instanz** .
3. Wählen Sie aus **Als Nächstes** Schaltfläche.
4. In **Aktion** Feld unter **Wählen Sie die Aktion aus, die Sie ausführen möchten** , Wählen Sie aus **Aktivieren Sie die Zertifikatvalidierung** .
5. Wählen Sie aus **Als Nächstes** Schaltfläche.
6. Neben **Anhänge** In **Kunde signiert Schlüsselpaar und Zertifikat** Abschnittsauswahl **+Datei Hinzufügen** Zum Hochladen eines kryptografischen Schlüsselpaars (p12-Dateierweiterung) zur Verwendung für die Kundensignatur.

   Tipp: Wenn **+Datei Hinzufügen** Option ist nicht verfügbar. Stellen Sie sicher, dass Sie sich im globalen Bereich befinden und die Rolle sn_kmf.cryptographic_Manager haben.

7. In **Passwort** Geben Sie das Passwort für das hochgeladene Schlüsselpaar ein.
8. Wählen Sie **Importieren**.
9. Wählen Sie Aus **Fahren Sie Fort** Um zum nächsten Abschnitt zu wechseln.
10. Neben **Anhänge** In **COT-Administrationsschlüsselpaar und Zertifikat** Abschnittsauswahl **+Datei Hinzufügen** Zum Hochladen eines kryptografischen Schlüsselpaars (p12-Dateierweiterung) zur Verwendung für die Kundensignatur.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

11. In **Passwort** Geben Sie das Passwort für das hochgeladene Schlüsselpaar ein.
12. Wählen Sie **Importieren**.
13. Wählen Sie Aus **Fahren Sie Fort** Um zum nächsten Abschnitt zu wechseln.
14. In **Führen Sie vertrauenswürdige Instanzaufgaben aus** Abschnitt, warten Sie, bis alle Aufgaben abgeschlossen sind.

    Ihre Instanz generiert diese Aufgaben automatisch und führt sie aus. Wenn Sie Codesignatur vor verwendet haben Vancouver Release, Aufgaben werden erstellt und ausgeführt, um Ihre Signaturen zu aktualisieren.

    In einigen Fällen sind keine Aufgaben erforderlich. **Keine Aufgaben erforderlich** Wird auf dieser Seite angezeigt.
15. Wählen Sie Aus **Fahren Sie Fort** Um zum nächsten Abschnitt zu wechseln.
16. Auf der **Konfiguration Exportieren** Dateiseite auswählen **Exportieren** Zum Erstellen und Herunterladen einer Konfigurationsdatei, die zum Aktivieren der Codesignatur in Ihrer geschützten Instanz verwendet wird. Der Exportprozess lädt eine XML-Datei auf Ihren lokalen Computer herunter, um sie in den in beschriebenen Schritten zu verwenden Konfigurieren Sie Codesignatur Enterprise auf Ihrer geschützten Instanz.
17. Navigieren Sie in Ihrer geschützten Instanz zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
18. Wählen Sie Aus **Update-Satz aus XML importieren** Am unteren Rand des abgerufenen **Update-Sätze** Liste.
19. Wählen Sie Aus **Wählen Sie Datei** , Und wählen Sie Ihre Konfigurationsdatei (XML-Dateierweiterung) aus.
20. Wählen Sie **Hochladen** aus.
21. Kehren Sie unter zur Konfigurationsseite für die Codesignatur zurück **Alle** > **Codesignatur** > **Codesignaturkonfiguration**an.
22. Verwenden Sie den Assistenten, um Ihre Konfiguration abzuschließen, und wählen Sie die Optionen zum Abschließen der Aktivierung der Zertifikatvalidierung aus.

Quorum-Gesteuerter Zertifikatwiderruf

Quorum-gesteuerter Zertifikatwiderruf für Codesignatur Zertifikate bieten einen sicheren Mechanismus für Codesignatur Zu widerrufender administrator Codesignatur Zertifikate. Der Widerrufsprozess umfasst die Übermittlung einer Anforderung, die die Genehmigung mehrerer Stakeholder erfordert. Dieser Workflow hilft, versehentliche oder nicht autorisierte Widerrufe zu verhindern.

Dieses Thema bietet die allgemeine Prozessübersicht für das sichere Widerrufen von Zertifikaten zwischen einer vertrauenswürdigen Instanz und einer geschützten Instanz mithilfe eines quorumbasierten Genehmigungs-Workflows.

- Anforderungserstellung und -Export (vertrauenswürdige Instanz): Initiieren Sie den Widerruf eines Quorum-Zertifikats, indem Sie eine Anforderung mit den erforderlichen Konfigurationseigenschaften erstellen. Exportieren Sie den Update-Satz, der die Widerrufsanforderung und zugehörige Daten enthält. Siehe Konfiguration Der Exportwiderrufanforderung
- Import und Genehmigung (geschützte Instanz): Importieren Sie den Update-Satz in die geschützte Instanz. Genehmiger erhalten Benachrichtigungen und müssen den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigungs-Workflow abschließen, bevor das Zertifikat gelöscht wird. Siehe Importieren Sie die Konfiguration der Widerrufsanforderung

- Optionaler MID-Server-Neustart: Wenn in der Konfiguration aktiviert, werden MID-Server in der geschützten Instanz nach dem Widerruf des Zertifikats neu gestartet. Dies erzwingt eine sofortige erneute Zertifikatsynchronisierung, kann jedoch zu Datenverlust für unverarbeitete oder zwischengespeicherte Ereignisse führen. Siehe Genehmigen Sie den Zertifikatwiderruf

Hinweis:

Ihr *update set*Läuft nach dem von definierten Zeitfenster ab Com.snc.kmf.Signature.valid_window Eigenschaft. Wenn es abläuft, können Sie einen neuen signierten Update-Satz aus der vertrauenswürdigen Instanz exportieren. Dieses Gültigkeitsfenster gilt für alle Update-Satz-Vorgänge, einschließlich Export, Import und Aktivieren Codesignatur. Dieses Gültigkeitsfenster bezieht sich nicht auf das Anforderungszeitfenster, das Sie beim Erstellen der Anforderung angeben.

Konfiguration Der Exportwiderrufanforderung

Starten Sie den Zertifikatwiderrufungsprozess, indem Sie das Zertifikat auswählen, das Sie widerrufen möchten. Geben Sie die erforderlichen Konfigurationseigenschaften an. Exportieren Sie diese Transaktion als Teil eines Update-Satzes, der zur Genehmigung und Ausführung in die geschützte Instanz importiert wird.

Vorbereitungen

Erforderliche Rolle: sn_cse.Codesigning_admin, sn_cse.quorum_requester, Security_admin

Prozedur

1. Navigieren Sie in Ihrer vertrauenswürdigen Instanz zu **Alle** > **Codesignatur** > **Konfiguration** > **Geführtes Setup** Und öffnen Sie Codesignatur Konfigurationsseite.
2. In **Instanztyp** Feld auswählen **Vertrauenswürdige Instanz** .
3. Wählen Sie aus **Als Nächstes** Schaltfläche.
4. In **Aktion** Feld unter **Wählen Sie die Aktion aus, die Sie ausführen möchten** , Wählen Sie aus **Zertifikatwiderruf** .
   Die Seite „Zertifizierungswiderrufanforderung“ wird angezeigt.
5. Wählen Sie auf der Seite „Zertifikat zum Widerrufen auswählen“ das Zertifikat aus, das Sie widerrufen möchten, und wählen Sie es aus **Widerruf Initiieren** .
6. Konfigurieren Sie die Genehmigungsanforderungen für den Zertifizierungswiderruf.

   a. Geben Sie im Menü Quorum-Anforderungen die entsprechenden Informationen in die Textfelder ein.

Quorum-Anforderungseigenschaften

Eigenschaft	Beschreibung
Mindestgenehmigungen	Mindestanzahl von Genehmigern, die zum Genehmigen der Zertifikatwiderrufsanforderung erforderlich sind.
Zeitfenster	Ablaufzeit für die Widerrufsanforderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Verantwortliche Vertragsgenehmigung	E-Mail-Adresse der Anwender, die zur Genehmigung der Widerrufsanforderung berechtigt sind.

b. In **Anforderungsbeschreibung** Geben Sie den Grund für die Initiierung des Zertifikatwiderrufs ein.

c. Wählen Sie **Speichern**.
Das Menü Konfigurationsdatei exportieren wird angezeigt.

d. Wählen Sie auf der Seite „Konfigurationsdatei exportieren“ die Option aus **Exportieren** Zum Erstellen und Herunterladen einer Konfigurationsdatei, die zum Ausführen des Zertifikatwiderrufs-Workflows in Ihrer geschützten Instanz verwendet wird.

Ergebnis

Der Exportprozess lädt eine XML-Datei auf Ihren lokalen Computer herunter, um sie in den in beschriebenen Schritten zu verwenden Konfigurieren Sie Codesignatur Enterprise auf Ihrer geschützten Instanz.

Importieren Sie die Konfiguration der Widerrufsanforderung

Importieren Sie den Update-Satz in die geschützte Instanz, um den Zertifikatwiderrufungsprozess zu initiieren. Genehmiger erhalten E-Mail-Benachrichtigungen, und sie sollten den Genehmigungs-Workflow abschließen, bevor das Zertifikat widerrufen wird. Die Genehmigung bedeutet, dass die Widerrufe aus Sicherheits- und Compliance-Gründen bestätigt, autorisiert und nachverfolgbar sind.

Vorbereitungen

Erforderliche Rolle: sn_cse.Codesigning_admin, sn_cse.quorum_requester, Security_admin

Prozedur

1. Melden Sie sich bei Ihrer geschützten Instanz an, und navigieren Sie zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze** > **XML importieren**an.
   Die Seite Import XML (XML importieren) wird angezeigt.
2. Wählen Sie Aus **Wählen Sie die Datei aus** Und wählen Sie die Konfigurations-XML-Datei aus Ihrem lokalen System aus.
3. Wählen Sie **Hochladen** aus.
4. Kehren Sie unter zur Konfigurationsseite für die Codesignatur zurück **Alle** > **Codesignatur** > **Codesignaturkonfiguration**an.

   a. Überprüfen Sie die folgenden Konfigurationsdateien in **Kunden-Updates im Batch** Registerkarte.
   - Konfigurationseigenschaft Für Codesignatur (`Time_window`)
   - Konfigurationseigenschaft Für Codesignatur (`Approver_email_IDs`)
   - Konfigurationseigenschaft Für Codesignatur (`Minimum_Approvals`)
   - Konfigurationseigenschaft Für Codesignatur (`Restart_Mid_Servers`)
   - Quorum-Anforderung Für Codesignatur (`CSEQCxxxxxx`)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Codesignaturtransaktion (`CSETRANSxxxxxxxx`)
- KMF-Signaturdatensätze

b. Auswahlvorgang **Update-Satz-Vorschau bündeln** > **Commit für Update-Satz-Batch ausführen**an.

5. Kehren Sie unter zur Konfigurationsseite für die Codesignatur zurück **Alle** > **Codesignatur** > **Konfiguration** > **Geführtes Setup**an.
6. In **Instanztyp** Feld auswählen **Geschützte Instanz** Und wählen Sie aus **Als Nächstes** .
   Die **Starten oder setzen Sie Ihre Konfiguration fort** Seite wird angezeigt.
7. Wählen Sie aus **Bestätigen Sie, dass der Update-Satz für die Codesignaturkonfiguration importiert und bestätigt wurde.** Aktivieren Sie das Kontrollkästchen, und wählen Sie aus **Als Nächstes** .
   Überprüfen Sie auf der Seite Quorum Control Configuration (Quorum-Steuerungskonfiguration) die von Ihnen eingegebenen Informationen, und wählen Sie sie aus **Quorum-Genehmigung Auslösen** .
8. Wählen Sie in der geschützten Instanz aus **Status Des Zertifizierungswiderrufs** Auf der Seite Quorum-Genehmigung auslösen, um Aktualisierungen der Quorum-Steuerungsanforderungsgenehmigungen zu überprüfen.
9. Wählen Sie Aus **Genehmigerdetails** Und überprüfen Sie den Status der Quorum-Anforderungen.

Genehmigen Sie den Zertifikatwiderruf

Überprüfen und genehmigen Sie Zertifikatwiderrufsanforderungen aus den E-Mail-Genehmigungsbenachrichtigungen, die an Ihre registrierte E-Mail-Adresse gesendet werden. Überprüfen Sie die Genehmigungsbenachrichtigung, und wählen Sie aus **Klicken Sie hier, um zu genehmigen** Oder **Klicken Sie hier, um abzulehnen** Link, um auf die geschützte Instanz zuzugreifen und zu handeln. Sie können auch direkt über die E-Mail auf die Genehmigungsanforderung und die Codesignatur-Quorum-Anforderung zugreifen.

Vorbereitungen

Erforderliche Rolle: sn_cse.Codesigning_admin, Approver_user

Prozedur

1. Greifen Sie auf die geschützte Instanz zu, indem Sie den in der Benachrichtigungs-E-Mail angegebenen Links folgen.
2. Überprüfen Sie die Transaktionsanforderungen im Menü „Genehmigungen“.
3. Genehmigen Sie die Aufgabe, indem Sie auswählen **Genehmigen** .
4. Wählen Sie auf der Seite „Genehmigungsbestätigung“ die Option aus **Ja** Um auf die spezifische Quorum-Anforderung für Codesignatur zuzugreifen.
5. Überprüfen Sie Codesignatur Quorum-Anforderung und fügen Sie zusätzliche Notizen in hinzu **Kommentare** Menü, falls erforderlich.
6. Wählen Sie **Aktualisieren**.

Ergebnis

Die Codesignatur Quorum-Anforderung wurde genehmigt. Wenn Sie den Neustart des MID-Servers beim Exportieren der Widerrufsanforderung aktiviert haben, wird der MID-Server neu gestartet, damit die Anforderung aktiviert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur deaktivieren

Deaktivieren Sie die Codesignatur in Ihrer geschützten Instanz.

Vorbereitungen

Erforderliche Rolle: admin, codesigning_admin

Prozedur

1. Navigieren Sie in Ihrer vertrauenswürdigen Instanz zu **Alle** > **Codesignatur** > **Konfiguration** > **Geführtes Setup** Zum Öffnen der Konfigurationsseite für Codesignatur.
2. In **Instanztyp** Feld auswählen **Vertrauenswürdige Instanz** .
3. Wählen Sie aus **Als Nächstes** Schaltfläche.
4. In **Aktion** Feld unter **Wählen Sie die Aktion aus, die Sie ausführen möchten** , Wählen Sie aus **Deaktivieren Sie die Codesignatur** .
5. In **Exportieren Sie die Konfigurationsdatei** Bereich auswählen **Exportieren** Zum Herunterladen des Update-Satzes.
   Der Exportprozess lädt eine XML-Datei auf Ihren lokalen Computer herunter, um sie in den nächsten Schritten zu verwenden.
6. Wählen Sie **Fertig**.
7. Melden Sie sich bei Ihrer geschützten Instanz an.
8. Laden Sie Ihre Konfigurationsdateien mithilfe der Schritte in hoch Laden Sie Ihre Codesignaturkonfigurationsdatei in Ihre geschützte Instanz hoch.
9. Navigieren zu **Alle** > **Codesignatur** > **Konfiguration** > **Geführtes Setup** Zum Öffnen der Konfigurationsseite für Codesignatur.
10. In **Instanztyp** Feld auswählen **Geschützte Instanz** .
11. Wählen Sie aus **Als Nächstes** Schaltfläche.
12. Wählen Sie aus **Bestätigen Sie, dass der Update-Satz für die Codesignaturkonfiguration importiert und bestätigt wurde** Kontrollkästchen.
13. Wählen Sie aus **Als Nächstes** Schaltfläche.
14. Warten Sie, bis die Zertifikatinstallation abgeschlossen ist.
    Nach Abschluss wird A **Codesignaturkonfiguration erfolgreich abgeschlossen** Meldung wird angezeigt.

Ergebnis

Sie können den erfolgreichen Abschluss überprüfen, indem Sie sich Ihre Systemeigenschaften ansehen. Suchen Sie nach **Com.snc.kmf.Signature.validation.Flag** Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_property], und stellen Sie sicher, dass sie einen Wert von hat **Falsch** .

Laden Sie die erforderlichen Schlüsselpaare und Zertifikate für die Codesignatur

Richten Sie die Beziehung in einer festgelegten vertrauenswürdigen Instanz mithilfe der Codesignatur ein. Dieser erste Schritt lädt zwei kryptografische Schlüssel in die vertrauenswürdige Umgebung, um eine vertrauenswürdige Quelle für Updates für die Produktionsinstanz einzurichten.

Vorbereitungen

Erforderliche Rollen: Security_admin und sn_kmf.cryptographic_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der erste Schritt beim Herstellen der Beziehung besteht darin, die Vertrauensgrundlage in einer festgelegten vertrauenswürdigen Instanz mithilfe der Codesignatur einzurichten. Um diese Aufgabe auszuführen, benötigen Sie Folgendes.

- Sie müssen zwei 4096-Bit-RSA-Paar für öffentliche/private Schlüssel haben, um in kryptografische Codesignaturmodule zu laden:
  - Ein Paar für das kryptografische Modul „cm_Code_Signing“
  - Ein Paar für das kryptografische Modul „cm_Code_Attest“

  Weitere Informationen zu diesen Schlüsseln finden Sie unter Erstellen Sie Codesignaturschlüsselpaare und Zertifikate.

  Wichtig: Diese Schlüsselpaare müssen von einer öffentlichen Zertifizierungsstelle oder von der internen Zertifizierungsstelle Ihrer Organisation signiert werden. Das Zertifikat kann nicht selbstsigniert sein.

- Eine Kryptographie-Standard-Datei für öffentliche Schlüssel Nr. 12 (.p12), die Ihre Blatt- und Zwischenzertifikate enthält.

Prozedur

1. Importieren Sie Ihre Schlüssel aus dem Schlüsselspeicher.
   a. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
   b. Suchen und öffnen Sie das kryptografische Modul namens `Cm_Code_Signing` .
   c. In **Krypto-Spezifikationen** Wählen Sie den Namen der Krypto-Spezifikation aus, um sie zu öffnen.
   d. In **Importieren Sie den Schlüssel aus dem Schlüsselspeicher** Bildschirm auswählen **Schlüssel importieren** .
2. Wiederholen Sie den ersten Schritt, um das kryptografische Modul namens zu importieren `Cm_Code_Attest` .
3. In **Geben Sie Das Schlüsselspeicher-Passwort Ein** Geben Sie das Passwort für die Challenge ein, das Sie beim Generieren Ihres RSA-Zertifikats erstellt haben.

   Hinweis: Das von Ihnen erstellte Passwort für die Challenge wird hier als bezeichnet **Schlüsselspeicher-Passwort** . In anderen Teilen des Prozesses kann dies entweder als bezeichnet werden **Passwort importieren** Oder **Passwort exportieren** . In allen Fällen ist dieses Passwort dasselbe Passwort für die Herausforderung, das Sie in den vorherigen Schritten erstellt haben.

4. Wählen Sie aus **Durchsuchen** Schaltfläche neben **Importieren Sie Schlüsselspeicher/Zertifikat** .
5. Wählen Sie eine Kryptographie-Standard-Datei mit öffentlichem Schlüssel Nr. 12 (.p12) aus, die Ihr Verteilungszertifikat enthält (erwähnt im Abschnitt „bevor Sie beginnen“ oben in diesem Dokument).
6. Wählen Sie **OK**.

   Wichtig: Wenn Sie eine eigene interne Zertifizierungsstelle verwenden, müssen Sie die Zwischenzertifikate der internen Zertifizierungsstelle mit dem Prozess in den Schritten 5–6 hochladen.

   Wenn Sie Ihren Schlüssel und Ihr Zertifikat(e) erfolgreich importieren, wird eine Bestätigungsnachricht angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können überprüfen, ob der Schlüssel und die Zertifikate in Ihrer Instanz in der Tabelle „X.509-Zertifikate“ [sys_certificate] vorhanden sind. Diese Datensätze haben den Typ **Trust Store-Zertifikat** .

Sie können Ihren Schlüssel in der Tabelle „kryptografische Module“ [sys_kmf_crypto_Module] validieren.

Nächste Maßnahme

Exportieren Sie das Zertifikat in die Produktion. Details siehe Bereiten Sie Circle of Trust-Zertifikate vor.

Bereiten Sie Circle of Trust-Zertifikate vor

Erstellen Sie einen Update-Satz in der vertrauenswürdigen Umgebung, um das vertrauenswürdige Zertifikat in die Produktionsumgebung zu exportieren.

Vorbereitungen

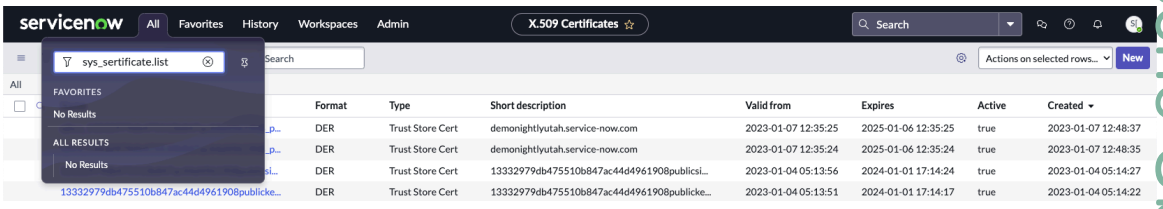
Erforderliche Rollen: admin, Security_admin

Vorbereitungen

Vertrauenswürdige Instanz

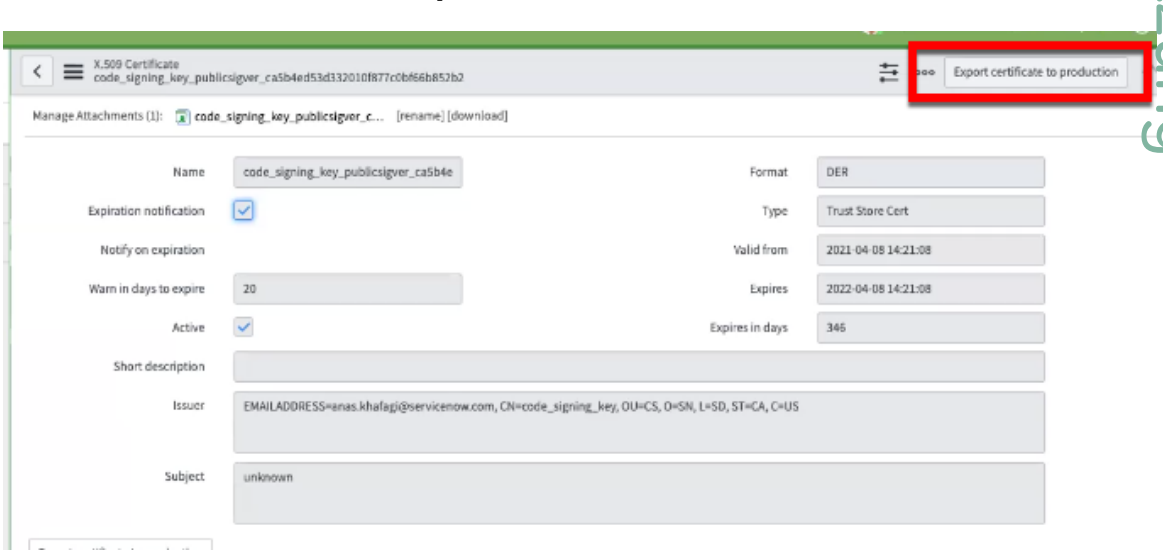
Prozedur

1. Navigieren Sie in der vertrauenswürdigen Umgebung zu **sys_certificate.list**an.



2. Öffnen Sie das zuletzt erstellte X.509-Zertifikat, das mit dem Typ generiert wurde **Trust Store-Zertifikat** . Möglicherweise müssen Sie hinzufügen **Erstellt** Feld in der Liste, um den neuesten Datensatz zu finden. Siehe Persönliche Listen .

3. Wählen Sie Aus **Zertifikat in Produktion exportieren** .



Zusammen mit dem Zertifikat wird eine Signatur erstellt.

Automatische Übersetzung

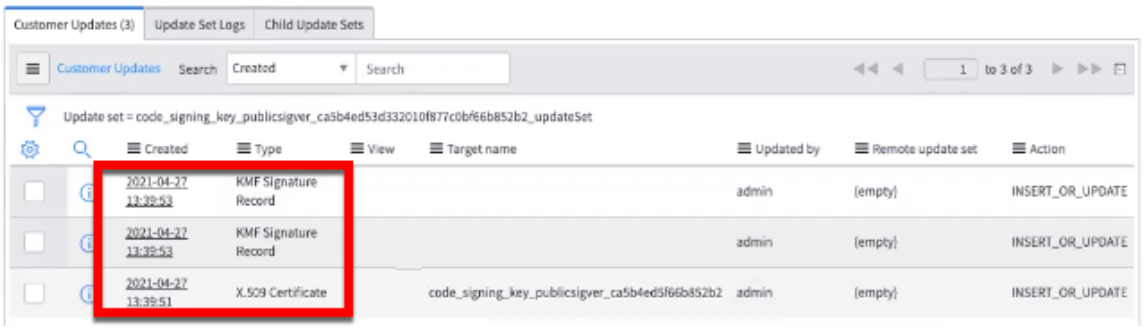
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
5. Suchen und öffnen Sie das Codesignaturupdate.

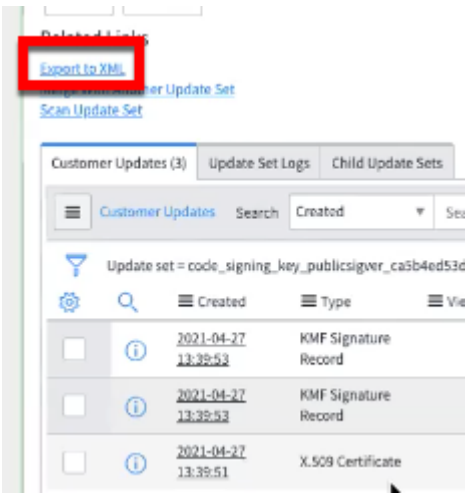
   Dieses Update beginnt mit dem Text `Code_Signing_key_publicsigver` .

   Ein neuer Code-Signatur-Update-Satz-Datensatz wurde von den vorherigen Schritten erstellt. Um diesen Datensatz zu finden, sortieren Sie die Liste mit **Erstellt von** Und suchen Sie nach Datensätzen mit in **Name** Feld.
6. Zeigen Sie die relevanten Signaturdatensätze und das X.509-Zertifikat an.

   Der Update-Satz enthält den Anhang für den Signaturdatensatz zusammen mit dem Eintrag der Signatur in der Tabelle und dem Zertifikat.



7. Wählen Sie aus **In XML exportieren** Zugehöriger Link.



8. Rufen Sie den Update-Satz in der Produktion ab.
   Details siehe Update Set abrufen .

> **Wichtig:** Wiederholen Sie diese Schritte für Ihr zweites Schlüsselpaar. Denken Sie daran, dass sowohl für die kryptografischen Module „cm_Code_Attest“ als auch „cm_Code_Signing“ ein Schlüssel vorhanden ist.

Importieren und installieren Sie Zertifikate für Circle of Trust

Rufen Sie den Update-Satz in der Produktion ab, um die Vertrauensbeziehung zwischen den beiden Instanzen herzustellen. Die Zertifikate, die erstellt wurden, um das Vertrauen in der vertrauenswürdigen Instanz darzustellen, müssen in die geschützte Instanz akzeptiert werden.

Automatische Übersetzung

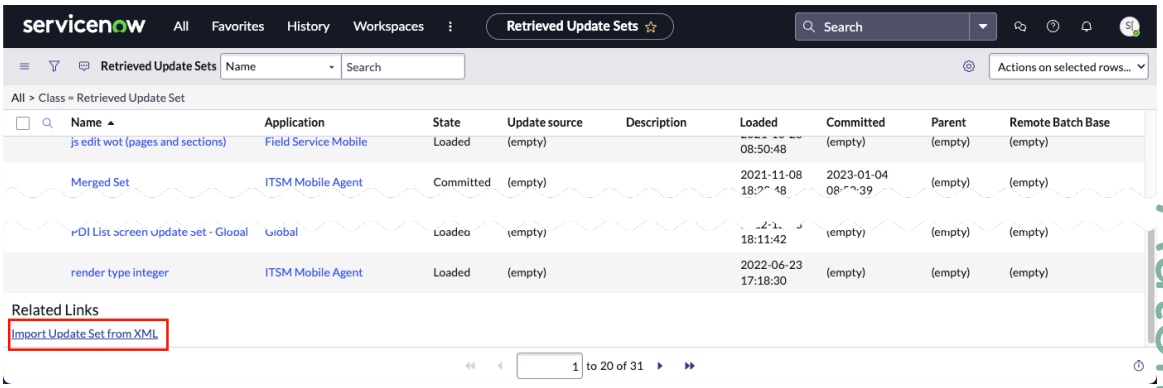
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

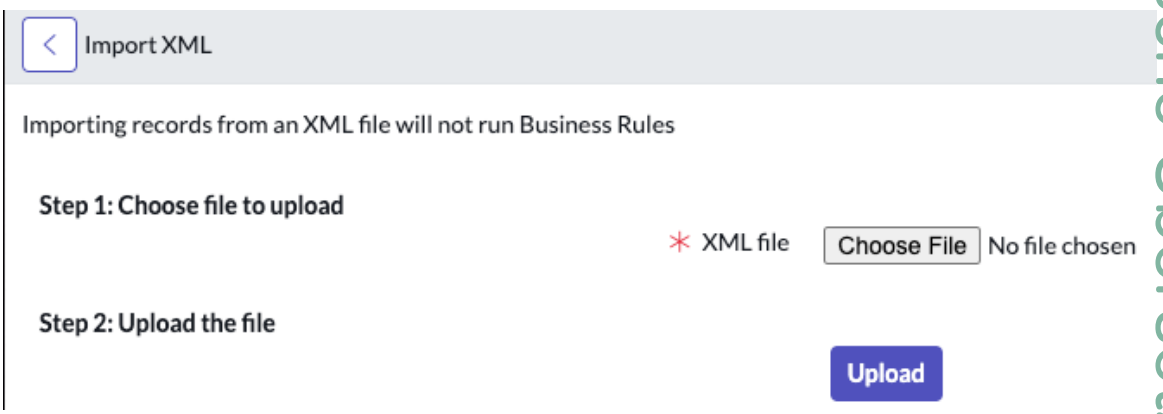
Erforderliche Rollen: admin, Security_admin

Prozedur

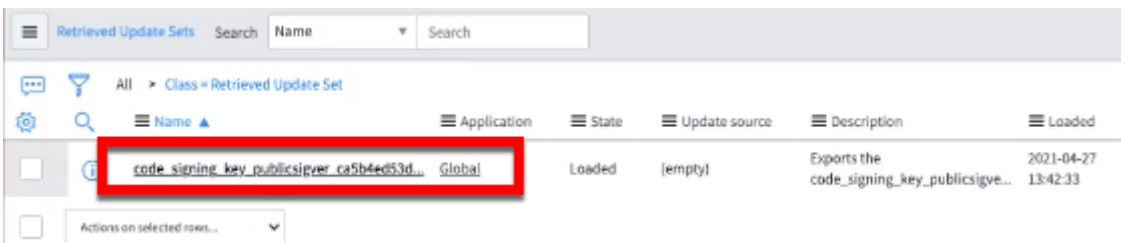
1. Navigieren Sie in der geschützten Instanz zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
2. Wählen Sie aus **Update-Satz aus XML importieren** Schaltfläche in der unteren linken Ecke des Bildschirms.



3. Wählen Sie Aus **Wählen Sie Datei** Und navigieren Sie, um die XML-Datei auszuwählen, in die Sie exportiert haben Bereiten Sie Circle of Trust-Zertifikate vor.



4. Wählen Sie **Hochladen** aus.
   Der Update-Satz für Codesignatur wird der Tabelle „abgerufene Update-Sätze“ hinzugefügt.



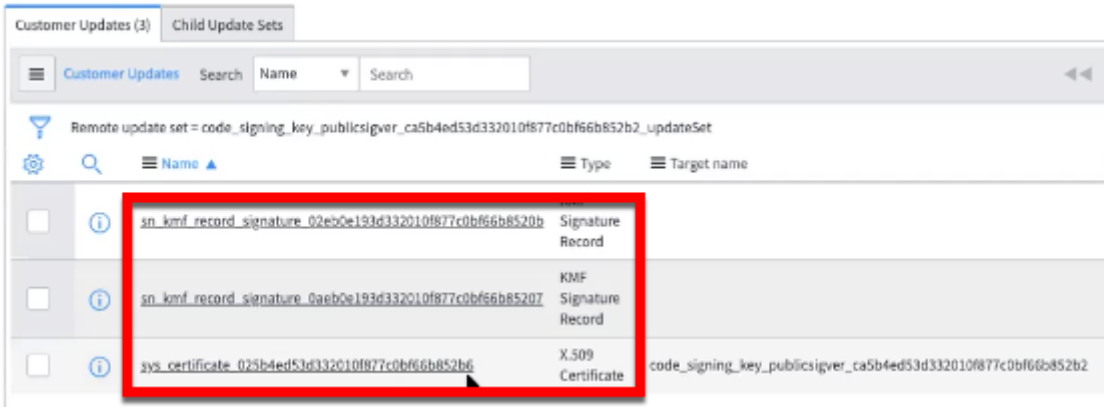
Hinweis: Wenn Ihr Update-Satz nicht angezeigt wird, filtern Sie Ihre Liste nach Datensätzen im Status „geladen“, und sortieren Sie die Liste nach **Geladen** Feld.

5. Öffnen Sie den Update-Satz-Datensatz, um sicherzustellen, dass die Tabelle „Kundenupdates“ die folgenden drei Datensätze enthält:

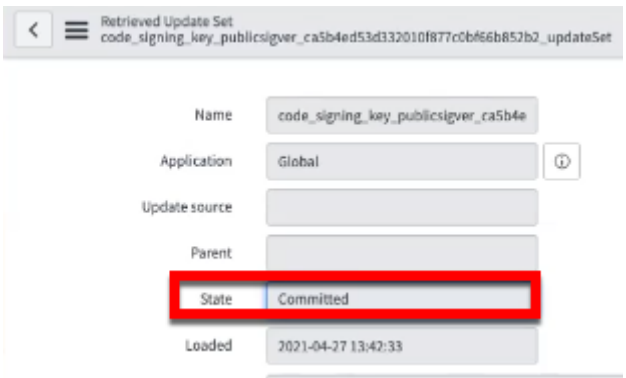
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zwei KMF Signaturdatensätze
- X.509-Zertifikat



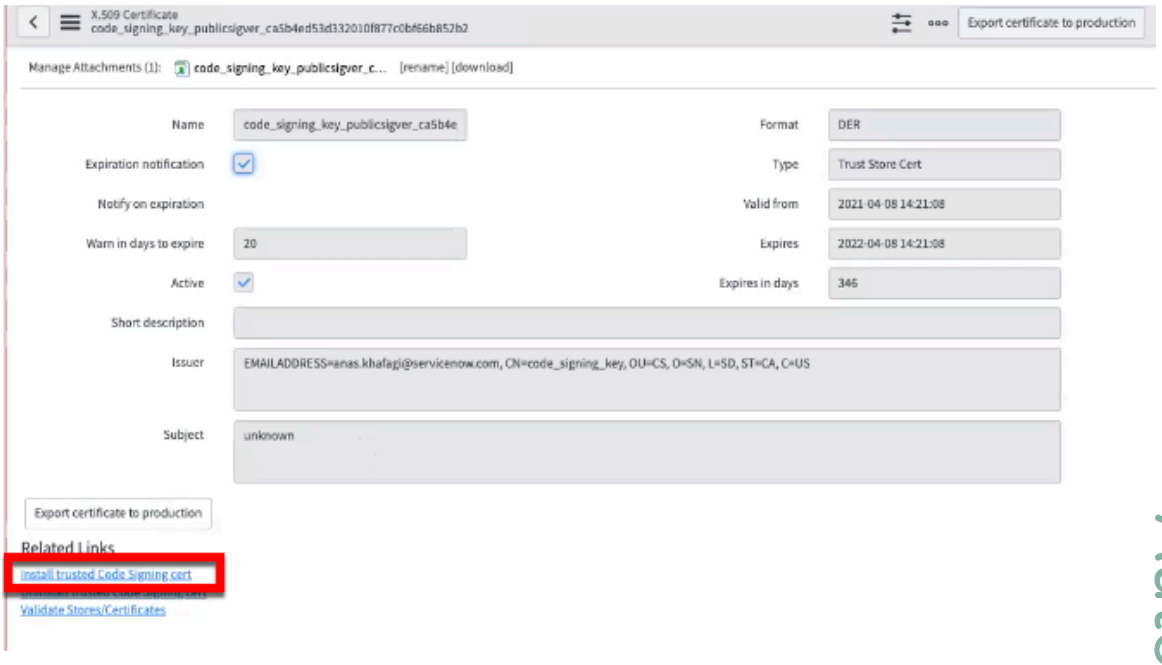
6. Wählen Sie Aus **Vorschau Des Update-Satzes Anzeigen** .
7. Wählen Sie Aus **Update-Satz Bestätigen** .



Der Abgerufene Update-Satz **Status** Wird auf „Commit“ aktualisiert.

8. Geben Sie im Navigator ein sn_kmf_Record_Signature.list Um zu öffnen **KMF-Signaturdatensätze** Liste.
9. Suchen Sie die beiden KMF Signaturdatensätze.
   Diese Datensätze sind die zuletzt erstellten Datensätze, bei denen **Zweck der KMF-Signatur** Feld hat einen Wert von Kreis des Vertrauens . Möglicherweise müssen Sie hinzufügen **Erstellt** Feld zu Ihrer Liste oder filtern Sie nach Datensätzen, die am aktuellen Datum erstellt wurden.
10. Geben Sie im Navigator ein sys_certificate.list Und öffnen Sie den Datensatz mit **Kurzbeschreibung** Wert von *Code_Signing_key* Und ein **Typ** Wert von Trust Store-Zertifikat .
11. Wählen Sie Aus **Installieren Sie das Zertifikat für vertrauenswürdige Codesignatur** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Zertifikattyp wird auf aktualisiert `Vertrauenswürdiges CodeSigning-Zertifikat` .

Wichtig: Wiederholen Sie diese Schritte für Ihr zweites Zertifikat. Denken Sie daran, dass sowohl für die kryptografischen Module „cm_Code_Attest“ als auch „cm_Code_Signing“ ein Zertifikat vorhanden ist.

Ergebnis

Die Vertrauensbeziehung wird zwischen vertrauenswürdigen und geschützten Instanzen hergestellt. Sie sind bereit, die Codesignatur zu aktivieren. Siehe Codesignatur aktivieren Um die Schritte abzuschließen.

Codesignatur aktivieren

Aktivieren Sie die Codesignatur in Ihrer vertrauenswürdigen Instanz außerhalb der Produktion, um die vertrauenswürdigen Instanzen zu identifizieren, die mit Ihrer Produktionsinstanz verknüpft sind.

Vorbereitungen

Erforderliche Rollen: Security_admin und entweder sn_kmf.crypto_Manager oder sn_kmf.admin

Als Kundenadministrator können Sie über das ServiceNow-Plugin-Portal auf das Plugin „Codesignatur“ [com.Glide.Code_Signing_Enterprise] zugreifen und installieren. Weitere Informationen zu den Anwendungsfällen der Codesignatur finden Sie unter Codesignatur Erkunden.

Warum und wann dieser Vorgang ausgeführt wird

Codesignaturaufträge mit signierten Update-Sätzen werden verwendet, um die Codesignaturfunktion ein- oder auszuschalten. Es gibt keine andere Methode für diese Funktionalität. Dieser Prozess umfasst Folgendes:

- Erstellen Sie zwei Codesignaturaufträge in der vertrauenswürdigen Instanz, einen zum Aktivieren der Codesignatur und einen zum Deaktivieren der Codesignatur.
  - Die **Aktivieren Sie** Die geplante Aufgabe startet den Prozess der MID-Server-Validierung des signierten Codes.
  - Die **Deaktivieren** Die geplante Aufgabe stoppt die MID-Server-Validierung des signierten Codes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

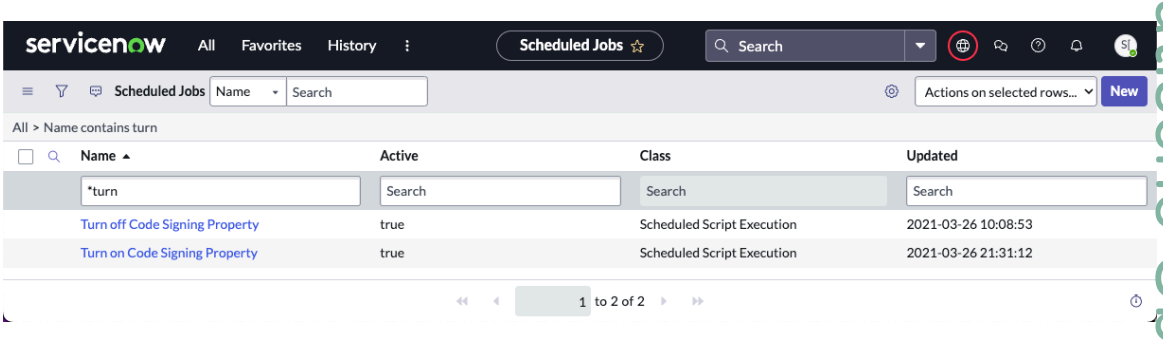
Standardmäßig gilt die Codesignatur für alle MID-Server. Wenn Sie die Codesignatur jedoch auf eine bestimmte Teilmenge von MID-Servern beschränken müssen, können Sie dies mithilfe der ECC-Firewall erreichen.

Hinweis: Beim Deaktivieren der Codesignatur wird die Systemeigenschaft auf markiert **Falsch** , Aber die Liste vertrauenswürdiger Freunde mit Codesignatur ist weiterhin verfügbar.

- Platzieren Sie **Aktivieren Sie die Codesignatureigenschaft** Auftrag in einem Update-Satz.
- Bringen Sie den Auftrag in die Produktion.
- Verwenden Sie **Aktivieren Sie die Codesignatureigenschaft** Auftrag in der Produktion, wenn die Signatur verifiziert wurde, dass sie aus einer vertrauenswürdigen Instanz stammt.

Prozedur

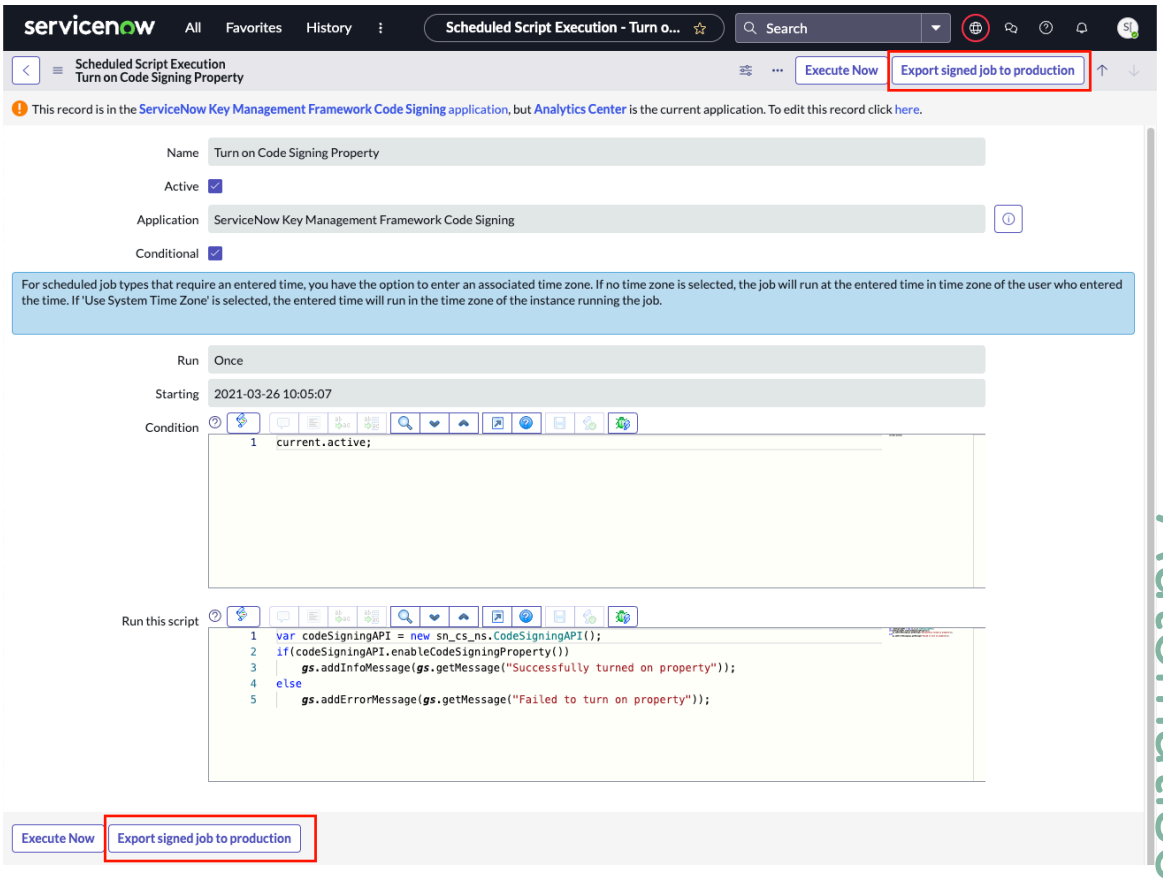
1. Navigieren Sie in Ihrer vertrauenswürdigen Instanz zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
2. Suchen Sie im Namensfeld nach „*turn“.
3. Wählen Sie Aus **Aktivieren Sie die Codesignatureigenschaft** .



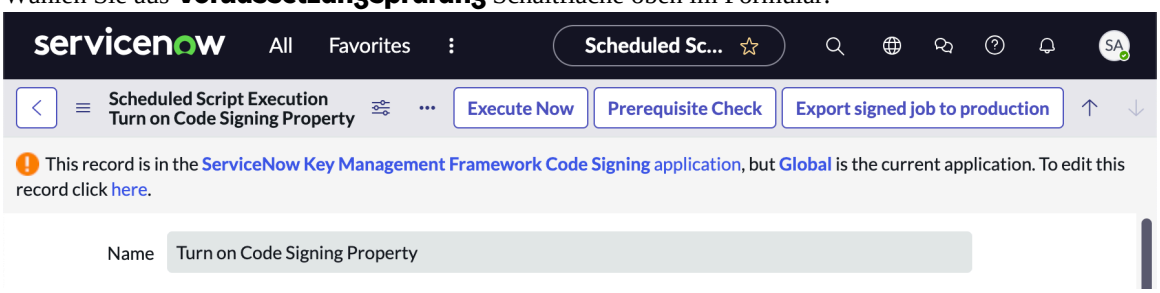
Die **Geplante Skriptausführung** Formular wird geladen. Dieses Formular enthält Informationen zum Aktivieren der Codesignatureigenschaft. Die Aufträge erstellen Update-Sätze, die die Aufträge und validierten Signaturen über den Codesignaturprozess enthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Um das Skript sofort auszuführen, signieren Sie das Zertifikat, erstellen Sie den Update-Satz, und wählen Sie aus **Signierten Auftrag in Produktion exportieren** .
   Sie können das Skript auch so konfigurieren, dass es nach einem festgelegten Zeitplan ausgeführt wird.
5. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
6. Öffnen Sie jeden Update-Satz der Codesignatureigenschaft, und wählen Sie aus **In XML exportieren** .
7. Melden Sie sich bei der Produktionsinstanz an.
8. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
9. Wählen Sie aus **Update-Satz aus XML importieren** Schaltfläche, und wählen Sie den Update-Satz für die Codesignatureigenschaft aus.
10. Wählen Sie Aus **Wählen Sie Datei** Und laden Sie die Update-Sätze hoch und bestätigen Sie sie.
11. Kehren Sie zur Liste der geplanten Aufgaben zurück, indem Sie zu navigieren **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
12. Öffnen Sie **Aktivieren Sie die Codesignatureigenschaft** Auftragsdatensatz.
13. Wählen Sie aus **Voraussetzungsprüfung** Schaltfläche oben im Formular.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

14. Wählen Sie aus **Jetzt Ausführen** Schaltfläche, nachdem die Voraussetzungsprüfung abgeschlossen ist. Die **Aktivieren Sie die Codesignatureigenschaft** Die geplante Aufgabe startet den Prozess der MID-Server-Validierung des signierten Codes.
15. Geben Sie im Navigator ein `sn_kmf_Record_Signature.list` Um zu öffnen **KMF-Signaturdatensätze** Listen Sie und filtern Sie nach Datensätzen, bei denen **Zweck der KMF-Signatur** Ist `Kreis des Vertrauens` .
    Die Vertrauensbeziehung hat die Aufträge verschoben, und wenn die Aufträge verwendet werden, wird der Signaturverifizierungsprozess ausgeführt. Wenn die Aufträge, Signaturen und Zertifikate alle Teil von sind Circle of Trust, Dann Codesignatur mit Circle of Trust Kann aktiviert werden.
16. Geben Sie im Navigator ein `sys_properties.list` Zum Öffnen der Liste der Systemeigenschaften.
17. Suchen Sie nach *`com_snc_kmf_signature.validation.flag`*Und stellen Sie sicher, dass der Wert auf festgelegt ist **Wahr** .
18. Überprüfen Sie, ob eine neue Eigenschaft vorhanden ist *`com_snc_kmf_signature.validation.certificate`*Ist in der Tabelle aufgeführt.

Systemeigenschaften

com.snc.kmf.signature.validation.certifi...	{"trust_map": {"025b4ed53d332010f877c0bf6...	string	ServiceNow Key Management Framework
com.snc.kmf.signature.validation.flag	true	true | false	Global

Verwenden Sie Circle of Trust Auftrag in der Produktion zur Verifizierung der Vertrauensbeziehung. In der Produktion kann kein direkter Auftrag ausgeführt werden, der versucht, Code zu signieren. Siehe Codesignatur Wird Konfiguriert Für Details zu Konfigurationsoptionen.

Erstellen Sie Codesignaturschlüsselpaare und Zertifikate

Erstellen Sie zwei Schlüsselpaare zu signierten Zertifikaten, um Vertrauen zwischen Ihren geschützten und vertrauenswürdigen Instanzen herzustellen.

Um Vertrauen zwischen Ihren Instanzen herzustellen, müssen Sie für jede der Schlüsselpaare und ein Zertifikat erstellen `Cm_Code_Attest` Und `Cm_Code_Signing` Kryptografische Module.

Das Erstellen von Schlüsselpaaren und Zertifikaten erfolgt mit einem kryptografischen Tool, das auf Ihrem lokalen Gerät installiert ist, z. B. dem OpenSSL-Tool. Weitere Informationen zu diesem Tool finden Sie unter https://www.openssl.org . Wenn Ihre Organisation andere kryptografische Tools wie LibreSSL oder GnuTLS verwendet, finden Sie ähnliche Schritte in der Dokumentation zu diesen Produkten.

Schlüsselpaar-Spezifikationen

Die von Ihnen erstellten Schlüsselpaare müssen diese Anforderungen erfüllen.

Typ	RSA
Schlüssellänge	4096
Signaturalgorithmus	RSASSA_PKCS1_V1_5_SHA_512

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatspezifikationen

Zertifikate müssen von einer öffentlichen Zertifizierungsstelle signiert werden.

Geben Sie anwenderdefinierte Regeln in der ECC-Firewall an

Konfigurieren Sie die ECC-Firewall (External Communication Channel) in Ihrem MID-Server Indem Sie die anwenderdefinierten Regeln angeben, um die eingehende Nachricht selektiv zuzulassen oder abzulehnen und die Codesignaturkonfiguration zu überschreiben.

Sicherheitsadministratoren können die ECC-Firewall-Tags verwenden, um die Codesignaturkonfiguration zu überschreiben und bestimmte Vorgänge für zuzulassen oder abzulehnen MID-Server. Diese anwenderdefinierten Regeln müssen in der YAML-Datei von angegeben werden, die sich unter befindet: Agent/Boot-config.yaml .

Diese Tags sind spezifisch für ein Protokoll. Die für das übergeordnete Tag angegebene Konfiguration gilt für das untergeordnete Tag. Beispiel: Wenn Http protokoll ist zulässig, Rest Und SOAP Protokolle sind ebenfalls zulässig. Diese Tabelle zeigt die verfügbaren übergeordneten und untergeordneten Tags.

Übergeordnetes Tag	Untergeordnetes Tag
DNS	
HTTP	• REST • SOAP
DIRECTORY_SERVICES	LDAP
SNMP	
SSH	• SCP • SFTP
SYSLOG	
WINDOWS	• CIM • POWERSHELL • WMI • WINRM
JAVASCRIPT	
GROOVY	
VCS	GIT
DATENBANKEN	JDBC
DATA_SOURCES	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • DISCOVERY

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnetes Tag	Untergeordnetes Tag
	• EREIGNISMANAGEMENT • HEALTH_LOG_ANALYTICS • SERVICE_MAPPING
ORCHESTRATION	

Zum Konfigurieren der anwenderdefinierten Regeln :

1. In MID-Server, Identifizieren Sie die Datei Boot-config-sample.yaml .
2. Benennen Sie die YAML-Datei in um Boot-config.yaml Und verschieben Sie die Datei an den folgenden Speicherort: Agent/Boot-config.yaml .
3. Geben Sie in der YAML-Datei die anwenderdefinierten Regeln an, und speichern Sie die Änderungen. Ein Beispiel für die YAML-Datei:

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. Starten Sie neu MID-Server.

Ändern Sie Ihre Root of Trust-Konfiguration

Vertrauen Sie Ihren eigenen Zertifikaten, und verwenden Sie sie, anstatt sich auf zu verlassen ServiceNow Erstellen Sie Zertifikate (Standard), indem Sie in „Root of Trust verwenden“ (ROT) ändern. ServiceNow Komponenten wie Skripteinbindungen, Geschäftsregeln usw. werden beim Build mit signiert ServiceNow Build-Zeitschlüssel (Verifizierungszertifikat ist der ServiceNow Zertifikat erstellen).

Vertrauensbasis wird geändert

Um den Root of Trust für diese Datensatzsignaturen zu ändern, müssen Sie den Change of Trust-Prozess befolgen.

- Generieren und migrieren Sie einen neuen Satz von Signaturen für alle bereitgestellten Komponenten mit Ihrem bereitgestellten Zertifikat.
- Deaktivieren Sie die Eigenschaft „Root of Trust“ mit einer geplanten Aufgabe.

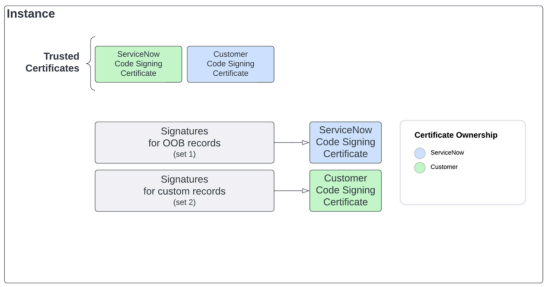
Weitere Informationen zu diesen Schritten finden Sie unter Migrieren Sie Signaturen, um ein Kundenzertifikat zu verwenden Und Deaktivieren Sie ServiceNow Root of Trust.

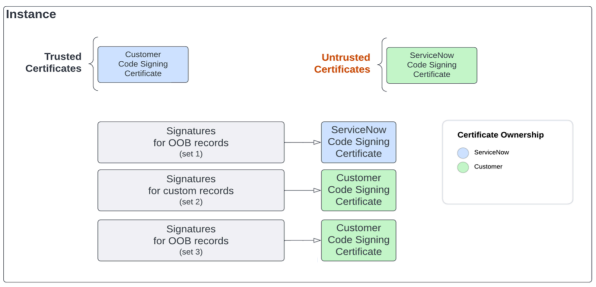
Auswirkung auf den Signaturgenerierungs- und Verifizierungsprozess

Standardmäßig werden Codesignatur-Build-Zertifikate während des Signaturverifizierungsprozesses vertrauenswürdig. Nachdem Sie diese Änderung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vorgenommen haben, akzeptiert Ihre Instanz Signaturen nur aus Ihrem eigenen Codesignaturzertifikat.





ROT-Eigenschaft auf „falsch“ festgelegt (Standard)	ROT-Eigenschaft auf „wahr“ festgelegt
• Bei der Überprüfung werden Signaturen mit Build-Zertifikaten vertrauenswürdig. • Wenn Sie beim Signieren keine Schlüssel angeben, wird der Instanzsignaturschlüssel als Sicherungsschlüssel verwendet. • Der REST-Endpunkt der Signatur *api/sn_kmf/signature/certificates*Gibt zurück ServiceNow Codesignatur-Build-Zertifikate zusammen mit anderen Zertifikaten, die in der Instanz vorhanden sind.	• Bei der Überprüfung werden Signaturen mit Build-Zertifikaten nicht vertrauenswürdig. • Wenn Sie beim Signieren keine Schlüssel angeben, wird das Signieren nicht ausgeführt. • Der REST-Endpunkt der Signatur *api/sn_kmf/signature/certificates*Ausgeschlossen ServiceNow Erstellen Sie Zertifikate (San Diego, Vancouver PKI, W PKI).

Auswirkung auf Ihren MID-Server

Wenn die ROT-Eigenschaft auf „falsch“ festgelegt ist

Wenn Sie die Eigenschaft ROT auf den Standardwert (falsch) belassen, hat dies keine Auswirkungen auf Ihren MID-Server.

Wenn Codesignatur aktiviert ist und die Eigenschaft ROT auf „wahr“ festgelegt ist

- Die *IsTrusted()* API gibt zurück Falsch Für Signaturen mit einem Build-Zertifikat.
- Die *IsTrusted()* API gibt zurück Wahr Für Signaturen mit Ihrem Zertifikat.
- Der REST-API-Aufruf für Zertifikate schließt Build-Zertifikate aus.
- Möglicherweise sehen Sie MID-Server-Probleme, z. B. Signaturvalidierung fehlgeschlagen Nachrichten in den Protokollen.

Migrieren Sie Signaturen, um ein Kundenzertifikat zu verwenden

Führen Sie einen Signaturauftrag aus, um Ihre Signaturen zu einem Kunden-Root of Trust (ROT) zu migrieren.

Vorbereitungen

Erforderliche Rolle: admin, Security_admin und sn_kmf.cryptographic_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur muss auf Ihren geschützten und vertrauenswürdigen Instanzen aktiviert sein. Sie können verifizieren, indem Sie überprüfen, ob **Com.snc.kmf.Signature.validation.Flag** Systemeigenschaft ist auf festgelegt Wahr .

Dieses Verfahren ist Teil einer Reihe von Verfahren zum Ändern eines Kunden-Root of Trust (ROT) in Ihren Instanzen. Eine Übersicht über diesen Prozess finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.

Prozedur

1. Melden Sie sich bei Ihrer geschützten Instanz an.
2. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
3. Suchen und öffnen Sie **ROT: Generieren Sie einen Aktualisierungssatz von Datensätzen, um Signaturen mithilfe des Kundenzertifikats zu migrieren** Geplante Aufgabe.
4. Wählen Sie unten im Formular aus **Jetzt Ausführen** .
5. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen**an.
6. Wählen Sie bei der Eingabeaufforderung aus **Signierauftrag** .
7. In **Signierauftrag** Füllen Sie die Felder nach Bedarf aus.

Feld	Wert
Name	Erstellen Sie einen eindeutigen Namen für Ihren Auftrag.
Typ	Wählen Sie Aus **Update-Satz Signieren** .
Tabelle	Wählen Sie den in den vorherigen Schritten erstellten Update-Satz aus. Der Update-Satz hat einen Namen, der mit beginnt Change_root_of_Trust_updateSet .

8. Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie aus **Speichern** Zum Speichern dieses Datensatzes.
9. Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie aus **Exportieren** > **XML (dieser Datensatz)** Dient zum Exportieren dieses Datensatzes als XML-Datei.
10. Melden Sie sich bei Ihrer vertrauenswürdigen Instanz an.
11. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
12. Klicken Sie mit der rechten Maustaste auf den Listenheader, und wählen Sie aus **XML importieren** .
13. In **XML importieren** Formular auswählen **Wählen Sie Datei** Und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.
14. Wählen Sie **Hochladen** aus.
15. Öffnen Sie in der Liste den importierten Sicherheitsauftrag.
16. Wählen Sie Aus **Codesignaturauftrag in die Produktion exportieren** .
    Mit dieser Aktion wird der Auftrag signiert und in einem neuen Update-Satz platziert, den Sie in Ihre geschützte Instanz importieren können.

> **Wichtig:** Nach dem Signieren des Auftrags müssen Sie die nächsten Schritte innerhalb von 10 Minuten ausführen. Wenn Sie diesen Zeitraum überschreiten, können Sie den Auftrag mit diesen Schritten erneut signieren. Dadurch wird ein weiterer signierter Update-Satz erstellt.

17. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

18. Suchen Sie den in den vorherigen Schritten erstellten Update-Satz.
    Der Name beginnt mit SIGN_UPDATE_SET_UPDATESET .
19. Wählen Sie Aus **XML exportieren** Um Ihren Update-Satz als XML-Datei zu exportieren.
20. Melden Sie sich bei Ihrer geschützten Instanz an.
21. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
22. Wählen Sie unten in der Liste aus **Update-Satz aus XML importieren** .
23. In **XML importieren** Formular auswählen **Wählen Sie Datei** Und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.
24. Wählen Sie **Hochladen** aus.
25. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**, Und öffnen Sie den Update-Satz, beginnend mit SIGN_UPDATE_SET_UPDATESET .
26. Wählen Sie Aus **Vorschau Des Update-Satzes Anzeigen** .
27. Nachdem die Vorschau abgeschlossen ist, wählen Sie aus **Update-Satz Bestätigen** .
28. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
29. Öffnen Sie den importierten Sicherheitsauftrag.
30. Wählen Sie Aus **Starten** Zum Ausführen des Sicherheitsauftrags.

    Nach Abschluss des Sicherheitsauftrags werden Informationen zum Status des Auftrags in angezeigt **Zusammenfassung** Feld.

    Wenn sich der Auftrag im Status „Fertig“ befindet, müssen alle Signaturen von Update-Satz-Datensätzen das vom Kunden bereitgestellte Zertifikat als Verifizierungszertifikat verwenden. Sie können dies in der Tabelle „KMF-Signaturdatensätze“ [sn_kmf_Record_Signature] überprüfen.

Nächste Maßnahme

Informationen zum Fortsetzen des Konfigurationsprozesses für Root of Trust finden Sie unter Deaktivieren Sie ServiceNow Root of Trust.

Deaktivieren Sie ServiceNow Root of Trust

Führen Sie eine geplante Aufgabe in Ihrer vertrauenswürdigen Instanz aus, um Root of Trust zu deaktivieren.

Vorbereitungen

Erforderliche Rolle: admin, Security_admin und sn_kmf.cryptographic_Manager

Codesignatur muss auf Ihren geschützten und vertrauenswürdigen Instanzen aktiviert sein. Sie können verifizieren, indem Sie überprüfen, ob **Com.snc.kmf.Signature.validation.Flag** Systemeigenschaft ist auf festgelegt Wahr .

Dieses Verfahren ist Teil einer Reihe von Verfahren, um in Ihren Instanzen zu einem Root of Trust (ROT) des Kunden zu wechseln. Eine Übersicht über diesen Prozess finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.

Prozedur

1. Melden Sie sich bei Ihrer vertrauenswürdigen Instanz an.
2. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
3. Öffnen Sie **Deaktivieren Sie ServiceNow Root of Trust** Geplante Aufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie aus **Signierten Auftrag in Produktion exportieren** .
5. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
6. Suchen und öffnen Sie **Deaktivieren Sie ServiceNow Root of Trust** Update-Satz.
7. Wählen Sie Aus **XML exportieren** Um Ihren Update-Satz als XML-Datei zu exportieren.
8. Melden Sie sich bei Ihrer geschützten Instanz an.
9. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
10. Wählen Sie unten in der Liste aus **Update-Satz aus XML importieren** .
11. In **XML importieren** Formular auswählen **Wählen Sie Datei** Und wählen Sie die XML-Datei aus, die Sie in den vorherigen Schritten heruntergeladen haben.
12. Wählen Sie **Hochladen** aus.
13. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**, Und öffnen Sie **Deaktivieren Sie ServiceNow Root of Trust** Update-Satz.
14. Wählen Sie Aus **Vorschau Des Update-Satzes Anzeigen** .
15. Nachdem die Vorschau abgeschlossen ist, wählen Sie aus **Update-Satz Bestätigen** .
16. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
17. Öffnen Sie die geplante Aufgabe, die im Update-Satz importiert wurde.
18. Wählen Sie aus **Jetzt Ausführen** Schaltfläche zum Ausführen des Auftrags.

Ergebnis

Durch die Ausführung der geplanten Aufgabe wird die Eigenschaft ROT auf „wahr“ festgelegt. Ihre Instanz ist so konfiguriert, dass sie den Kundenstamm des Vertrauens verwendet.

Codesignatur verwenden

Erfahren Sie, wie Sie Datensätze, Nachrichten und Anhänge signieren, um die Authentizität und Integrität Ihrer Daten zu überprüfen.

Signieren Sie die JDBC-Datenquellendatensätze in der geschützten Instanz

Verwenden Sie Update-Sätze, um die JDBC-Datenquellen zu signieren und zu validieren, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

Signieren Sie die REST- und SOAP-Nachrichten in der Produktionsinstanz

Verwenden Sie Update-Sätze, um die REST- und SOAP-Nachrichten zu signieren und zu validieren, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

Signieren Sie die Flows, Subflows und Aktionen in der geschützten Instanz

Verwenden Sie Update-Sätze, um die Flows, Subflows und Aktionen zu signieren und zu validieren, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

Signieren Sie bestimmte Datensätze oder Anhänge

Erstellen Sie einen Sicherheitsauftrag, um bestimmte Datensätze oder Anhänge anstelle aller Datensätze oder Anhänge in einer Tabelle zu signieren.

Eigenständiges Signaturtool

Verwenden Sie das eigenständige Signaturtool, um unterstützte Datensätze in zu signieren ServiceNow Anwendungen, die Ihren eigenen privaten Schlüssel verwenden.

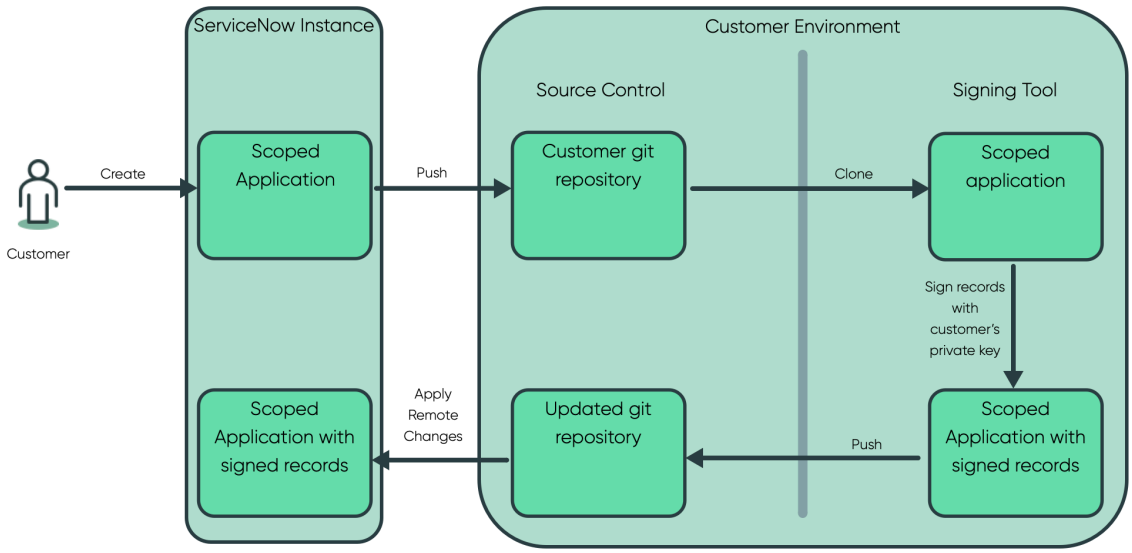
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenständiges Signaturtool

Verwenden Sie das eigenständige Signaturtool, um unterstützte Datensätze in zu signieren ServiceNow Anwendungen, die Ihren eigenen privaten Schlüssel verwenden.

Verwenden Sie das Signaturtool, um Datensätze in zu signieren ServiceNow Apps. Das Tool generiert Signaturen für Datensätze in Ihrer lokalen Umgebung mithilfe Ihres eigenen privaten Schlüssels.

Signiertool-Workflow



1. Erstellen oder wählen Sie ein vorhandenes aus ServiceNow Anwendung mit zu signierenden Datensätzen, z. B. Geschäftsregeln oder Skripteinbindungen.
2. Übertragen Sie die Anwendung in Ihr Git-Repository, das sich in Ihrer Umgebung befindet.

   Hinweis: Anwendungen können mithilfe der Quellcodeverwaltung-Integration zwischen einem Git-Repository und Ihrer Instanz synchronisiert werden. Weitere Informationen zum Konfigurieren und Verwenden dieser Integration finden Sie unter Veraltet – Quellcodeverwaltung-Integration .

3. Klonen Sie die Anwendung in Ihrer lokalen Umgebung.
4. Verwenden Sie das Signaturtool (auch in Ihrer lokalen Umgebung), um die unterstützten Datensätze aus dem geklonten zu signieren ServiceNow Anwendung mit Ihrem privaten Schlüssel. Das Signaturtool erstellt Signaturdatensätze und X.509-Zertifikatdatensätze [sys_certificate]. Weitere Informationen zur Verwendung des Signaturtools finden Sie unter Mit dem Signaturtool.
5. Übertragen Sie die aktualisierte Anwendung in Ihr Git-Repository.
6. Importieren Sie in Ihrer Instanz die aktualisierte Anwendung, indem Sie Remote-Änderungen anwenden.

Mit dem Signaturtool

Erfahren Sie, wie Sie das Signierungstool zum Signieren unterstützter Datensätze in verwenden ServiceNow Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Um diese Schritte auszuführen, müssen Sie Folgendes haben:

- A ServiceNow Anwendung, die Datensätze enthält, die signiert werden sollen.
- Ein privater Schlüssel zum Signieren von Datensätzen.
- Die `signRecords.sh` Skript in Ihrer lokalen Umgebung mit Ausführungsberechtigung.

Wichtig: Die `signRecords.sh` Das Skript ist als Teil der JAR-Datei „Signaturtool“ enthalten, die Sie anfordern müssen ServiceNow Kundensupport an.

Prozedur

1. Navigieren Sie in Ihrer lokalen Umgebung zu dem Verzeichnis, das enthält `signRecords.sh` Skript.
2. Verwenden Sie das folgende Befehlsformat, um Ihre Datensätze zu signieren:

   ```
   ./signRecords.sh -d [Path to the root directory of the ServiceNow Application to Sign] -f [Path to the Keystore file]
   ```

   Zum Beispiel:

   ```
   ./signRecords.sh -d /users/abc/ServiceNow-App-1 -f /users/abc/codesigning.p12
   ```

3. Geben Sie bei Aufforderung das Passwort für den Schlüsselspeicher ein.
   Drücken Sie die Eingabetaste, wenn kein Passwort vorhanden ist.
4. Überprüfen Sie die Ausgabe, um eine erfolgreiche Signatur zu bestätigen.

   ```
   Sep 26, 2022 2:41:09 PM com.snc.java.commands.ACommand start
   INFO: CODESIGN: executing codesigning...
   Sep 26, 2022 2:41:09 PM com.snc.core.codesigning.CodeSignerSupplier get
   INFO: CODESIGN: signing record for documentId: 65e811327702111057416efe7c5a994f
   Sep 26, 2022 2:41:11 PM com.snc.java.commands.ACommand start
   INFO: CODESIGN: codesigning successfully completed!
   ```

   Im vorherigen Ausgabebeispiel verwendete das Signaturtool die angegebene Schlüsselspeicherdatei, um den Datensatz zu signieren. Sie können auch Folgendes sehen:

   - Das Skript hat einen unterstützten Datensatz gefunden `65e811327702111057416efe7c5a994f` Und signiert.
   - Im Verzeichnis ServiceNow-App-1 wurden zwei Datensätze erstellt: `sys_certificate.xml` Und `sn_kmf_record_signature.xml` .
5. Importieren Sie die aktualisierte Anwendung zurück in Ihre Instanz, indem Sie Remote-Änderungen in anwenden Studio.
   Weitere Informationen finden Sie unter Veraltet – Remote-Changes anwenden .

Signierungstool-Argumente

Erfahren Sie mehr über die verfügbaren Argumente für das Signaturtool.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehlszeilenargumente

Argument	Erforderlich	Beschreibung
-d	Ja	Stammverzeichnis des zu signierenden Projekts. Muss Projektverzeichnis (zufällige alphanumerische 32), Datei sn_source_control.properties und eine <project_name>.iml-Datei enthalten
-f	Ja	Der Dateipfad des Schlüsselspeichers.
-a	Nein	Alias, der für den Zugriff auf einen bestimmten Eintrag im Schlüsselspeicher verwendet wird.
-c	Nein	Verketten Sie Datensatzsignaturen in einer Datei.
-k	Nein	Passwort für den Zugriff auf den im Schlüsselspeicher gespeicherten Schlüssel. Sie können dieses Passwort auch eingeben, wenn Sie dazu aufgefordert werden, anstatt innerhalb des Arguments.
-O	Nein	Signieren Sie mit einem neuen Zertifikat anstelle vorhandener sys_cert-Dateien.
-p	Nein	Passwort für den Zugriff auf den Schlüsselspeicher, wenn er über ein Passwort verfügt. Sie können dieses Passwort auch eingeben, wenn Sie dazu aufgefordert werden, anstatt innerhalb des Arguments.
-W	Nein	Löschen Sie alle vorhandenen Signaturdatensatzdateien.
-H	Nein	Zeigen Sie diese Hilfemeldung an, und beenden Sie den Vorgang.

Signieren Sie die JDBC-Datenquellendatensätze in der geschützten Instanz

Verwenden Sie Update-Sätze, um die JDBC-Datenquellen zu signieren und zu validieren, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

- Einrichten Circle of Trust Zwischen den geschützten und vertrauenswürdigen Instanzen.
- Erforderliche Rolle: Sicherheit _Admin

Hinweis:

- MID-Server Verarbeitet die Dateidatenquellen nicht, daher sind diese Datenquellen nicht codesigniert.
- LDAP-Datenquellen können nicht codesigniert werden.

Signieren Sie vorhandene Datenquellen des JDBC-Typs

Verwenden Sie Update-Sätze, um Massensignierungsaufträge in die geschützte Instanz zu übertragen.

Vorbereitungen
Erforderliche Rolle: security_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Konfigurieren Sie in der vertrauenswürdigen Instanz den KMF-Signaturauftrag, um die Datenquellen zu signieren.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie Aus **Massensignierungsdatensätze** .
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie Aus **Datenquelle** .

   d. Klicken Sie Auf **Codesignaturauftrag in die Produktion exportieren** .
   Es wird eine Bestätigungsmeldung angezeigt, dass der Update-Satz signiert ist.

   e. Exportieren Sie den generierten Update-Satz in eine XML-Datei.

2. Importieren Sie in der geschützten Instanz den Update-Satz, und bestätigen Sie ihn, um die signierten Massenaufträge aus einer vertrauenswürdigen Instanz abzurufen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

   b. Öffnen Sie den Update-Satz, der aus der vertrauenswürdigen Instanz exportiert wurde.

   c. Klicken Sie auf **Start**.
   Es wird eine Bestätigungsnachricht angezeigt, dass die Datensätze signiert sind.

Signieren Sie neue Datenquellen des JDBC-Typs

Verwenden Sie Update-Sätze, um den signierten Update-Satz in die geschützte Instanz zu übertragen.

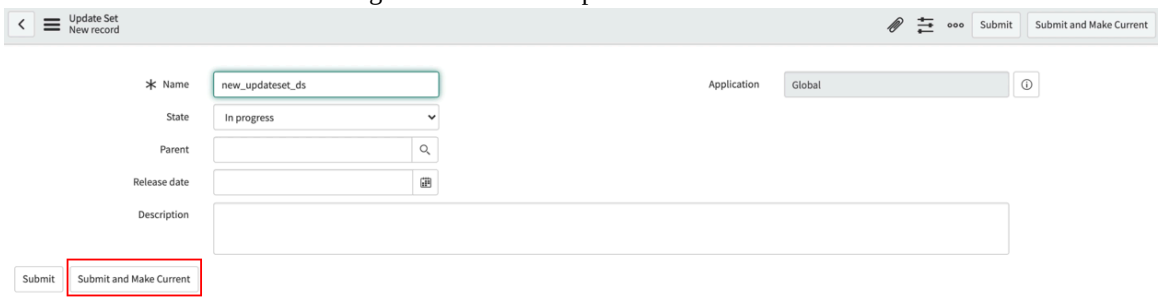
Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

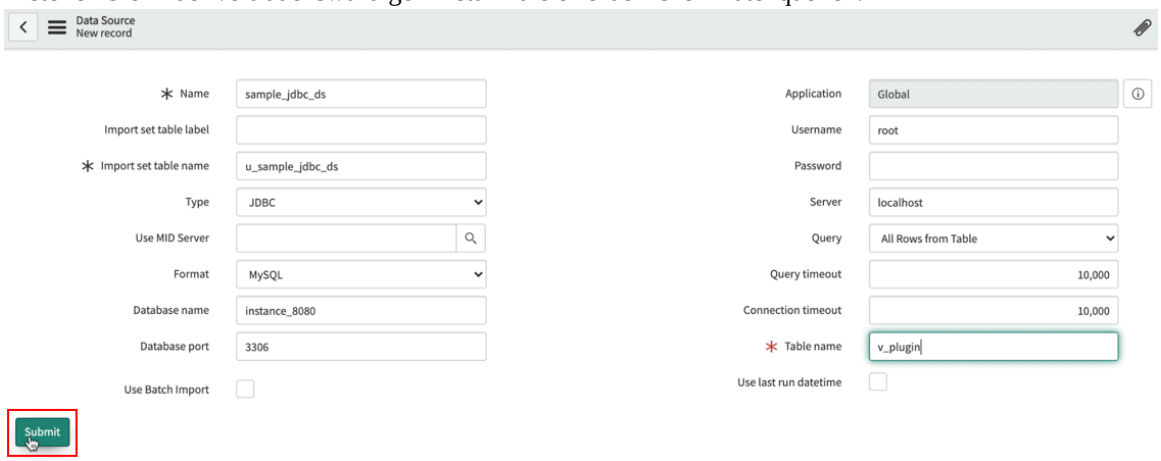
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Starten Sie in der vertrauenswürdigen Instanz einen Update-Satz.

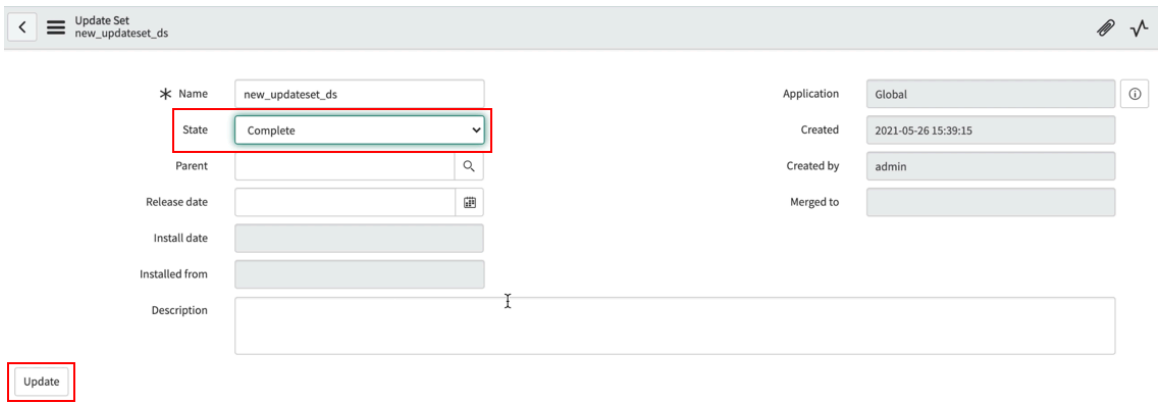


2. Erstellen Sie in der vertrauenswürdigen Instanz die erforderlichen Datenquellen.



Die Datenquellen werden dem Update-Satz hinzugefügt.

3. Ändern Sie in der vertrauenswürdigen Instanz den Status des Update-Satzes in **Abgeschlossen** Und klicken Sie auf **Aktualisieren** .



4. Signieren Sie in der vertrauenswürdigen Instanz den Update-Satz, indem Sie einen Verschlüsselungsauftrag erstellen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

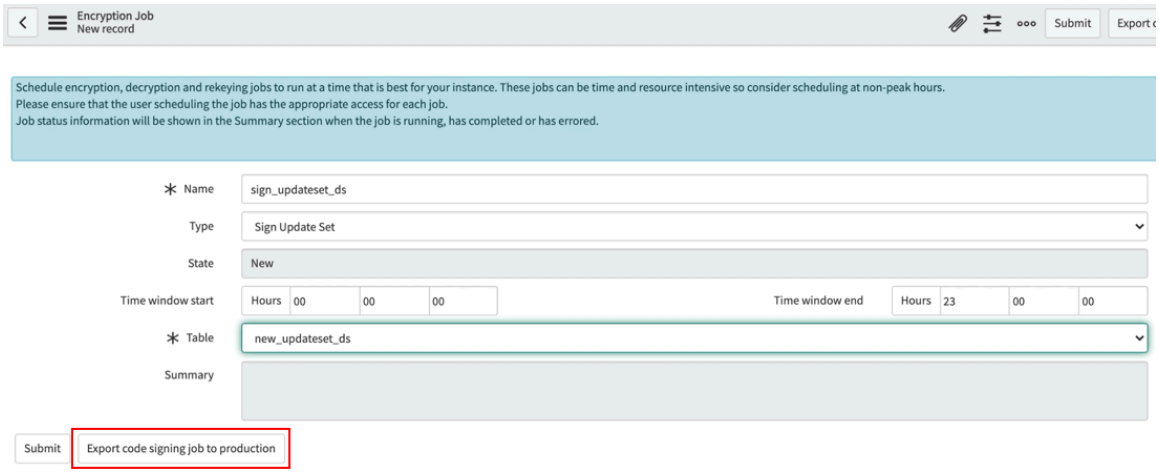
   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Automatische Übersetzung

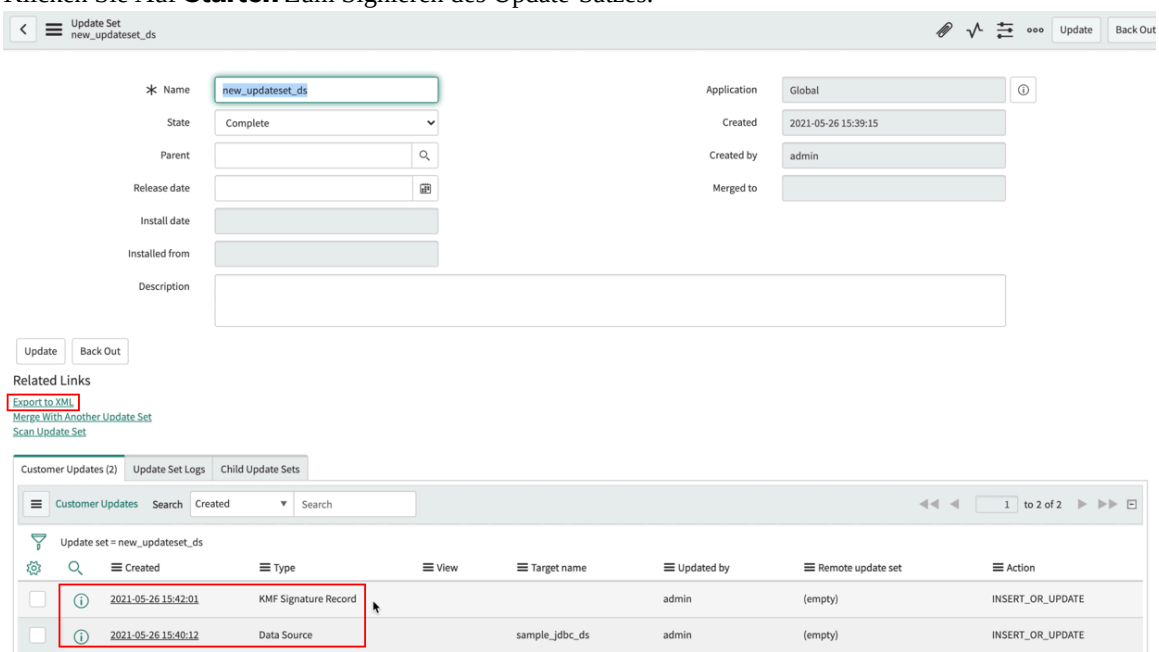
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie Aus **Update-Satz Signieren** .
Tabelle	Update-Satz, aus dem die Datensätze signiert werden sollen.



d. Klicken Sie auf **Absenden**.

e. Klicken Sie Auf **Starten** Zum Signieren des Update-Satzes.



- **Zusammenfassung** Wird aktualisiert, dass die Datensätze signiert sind.
- Der Update-Satz wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der vertrauenswürdigen Instanz den signierten Update-Satz-Datensatz, und exportieren Sie ihn in eine XML-Datei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Importieren Sie in der geschützten Instanz den signierten Update-Satz.

   a. Navigieren zu **Systemupdate-Sätze** > **Update Sets abgerufen**an.

   b. Klicken Sie auf **Update-Satz aus XML importieren** Zugehöriger Link zum Importieren des Update-Satzes, der aus der vertrauenswürdigen Instanz exportiert wird.
   Weitere Informationen finden Sie unter Importieren Sie den Schnellstart-Update-Satz, und bestätigen Sie ihn .
   Der Update-Satz wurde erfolgreich bestätigt.

Signieren Sie die REST- und SOAP-Nachrichten in der Produktionsinstanz

Verwenden Sie Update-Sätze, um die REST- und SOAP-Nachrichten zu signieren und zu validieren, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

Vorbereitungen

- Einrichten Circle of Trust Zwischen den geschützten und vertrauenswürdigen Instanzen.
- Erforderliche Rolle: security_admin

Signieren Sie die vorhandenen REST- und SOAP-Nachrichten

Signieren und validieren Sie die vorhandenen REST- und SOAP-Nachrichten, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Prozedur

1. Konfigurieren Sie in der vertrauenswürdigen Instanz den KMF-Signaturauftrag, um die UI-Aktionen zu signieren.

   a. Navigieren Sie zu KMF-Signaturkonfiguration .

   b. Füllen Sie diese Werte im Formular aus.

Formular „KMF-Signaturkonfiguration“

Feld	Beschreibung
Tabellenname	Glide-Tabellenname. Wählen Sie beispielsweise aus **UI-Aktionen [sys_ui_action]** .
KMF-Signatur-Zweck	Zweck des Signierens der Datensätze. Wählen Sie Aus **ECC-Warteschlange** .
Signaturerzeugungsfelder	Felder in der Datenquelle, die Sie signieren möchten. Wenn Änderungen an den Werten in einem oder mehreren dieser Felder vorgenommen werden, wird die zuvor generierte Signatur ungültig. Wählen Sie Aus **Name** Und **Skript** .
Signaturerzeugungsfilter	Filterkriterien, die zum Signieren der Datensätze erfüllt sein müssen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anhang signieren	Option zum Signieren des Anhangs im Glide-Datensatz.
Instanzschlüssel	Option zur Verwendung des Instanzschlüssels.

c. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.

2. Signieren Sie in der vertrauenswürdigen Instanz die erforderlichen Datensätze.

a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

b. Klicken Sie auf **Neu**.

c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie Aus **Massensignierungsdatensätze** .
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie Aus **UI-Aktion** .

d. Klicken Sie Auf **Codesignaturauftrag in die Produktion exportieren** .
Zwei lokal signierte Update-Sätze werden erstellt.

- Ein Update-Satz für die UI-Aktionskonfiguration.
- Ein weiterer Update-Satz aus dem Verschlüsselungsauftrag zum Exportieren des Codesignaturauftrags.

3. Exportieren Sie in der vertrauenswürdigen Instanz den lokalen Update-Satz in eine XML-Datei.

a. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**an.

b. Öffnen Sie den Update-Satz, den Sie für das Massensignieren der Datensätze erstellt haben.

c. Klicken Sie auf **In XML exportieren** Zugehöriger Link und speichern Sie die XML-Datei.

4. Importieren Sie in der geschützten Instanz die Update-Sätze.

a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.

b. Klicken Sie auf **Update-Satz aus XML importieren** Zugehöriger Link zum Importieren des Update-Satzes, der aus der vertrauenswürdigen Instanz exportiert wird.
Weitere Informationen finden Sie unter Importieren Sie den Schnellstart-Update-Satz, und bestätigen Sie ihn .
Der Update-Satz wurde erfolgreich bestätigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Führen Sie in der geschützten Instanz den Verschlüsselungsauftrag aus, den Sie zuvor in der vertrauenswürdigen Instanz erstellt haben, indem Sie auswählen **Starten** .
   Eine Bestätigungsnachricht wird angezeigt, in der angegeben wird, dass die Datensätze signiert sind.

Signieren Sie neue REST- und SOAP-Nachrichten

Signieren und validieren Sie die neuen REST- und SOAP-Nachrichten aus der vertrauenswürdigen Instanz, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Starten Sie in der vertrauenswürdigen Instanz einen Update-Satz.
2. Erstellen Sie in der vertrauenswürdigen Instanz die erforderlichen REST- oder SOAP-Nachrichten.
   Die Nachrichten werden dem Update-Satz hinzugefügt.
3. Ändern Sie in der vertrauenswürdigen Instanz den Status des Update-Satzes in **Abgeschlossen** Und klicken Sie auf **Aktualisieren** .
4. Signieren Sie in der vertrauenswürdigen Instanz den Update-Satz, indem Sie einen Verschlüsselungsauftrag erstellen.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie Aus **Update-Satz Signieren** .
Tabelle	Update-Satz, aus dem die Datensätze signiert werden sollen. Wählen Sie Aus **Neuen Rest V2-Update-Satz signieren – 1** .

   d. Klicken Sie auf **Absenden**.

   e. Klicken Sie Auf **Starten** Zum Signieren des Update-Satzes.

   - **Zusammenfassung** Wird aktualisiert, dass die Datensätze signiert sind.
   - Der Update-Satz wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der vertrauenswürdigen Instanz den signierten Update-Satz-Datensatz, und exportieren Sie ihn in eine XML-Datei.
6. Importieren Sie in der geschützten Instanz den Update-Satz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.

b. Wählen Sie aus **Update-Satz aus XML importieren** Zugehöriger Link zum Importieren des Update-Satzes, der aus der vertrauenswürdigen Instanz exportiert wird.
Weitere Informationen finden Sie unter Importieren Sie den Schnellstart-Update-Satz, und bestätigen Sie ihn .
Der Update-Satz wurde erfolgreich bestätigt.

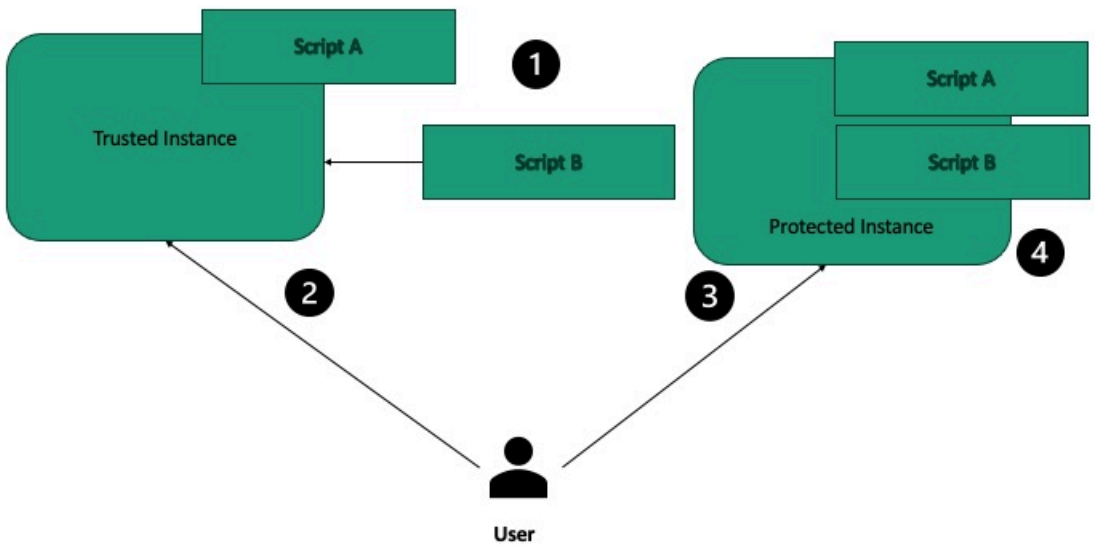
Signieren Sie bestimmte Datensätze oder Anhänge

Erstellen Sie einen Sicherheitsauftrag, um bestimmte Datensätze oder Anhänge anstelle aller Datensätze oder Anhänge in einer Tabelle zu signieren.

Beginnt in Vancouver Release: Sicherheitsadministratoren können Sicherheitsaufträge verwenden, um bestimmte Datensätze in einer Tabelle anstatt aller Datensätze in einer Tabelle zu signieren. Signieren Sie bestimmte Datensätze, um zu vermeiden, dass nicht überprüfte Codes versehentlich signiert werden.

Diese Aufträge enthalten eine angehängte Protokolldatei, die am Ende des Signaturauftrags generiert wird. Diese Protokolldatei enthält Informationen zu signierten Datensätzen und der verwendeten Signaturkonfiguration.

Signaturprozess



Dieses Diagramm zeigt ein Beispiel dafür, wie Sie den Signaturprozess verwenden können. In diesem Beispiel ein Skript mit der Bezeichnung Skript B Ist nur in der geschützten Instanz vorhanden und muss in eine vertrauenswürdige Instanz importiert werden, um signiert zu werden. Skript A Ist bereits auf beiden Instanzen vorhanden, muss nicht signiert werden. Es wurde entweder bereits überprüft und signiert oder wurde noch nicht überprüft und darf nicht signiert werden.

1. Importieren Sie den Datensatz in Ihre vertrauenswürdige Umgebung.
2. Erstellen Sie in der vertrauenswürdigen Instanz einen Signierauftrag, um den Datensatz zu signieren. Dieser Prozess ist in detailliert beschrieben Erstellen Sie einen Auftrag, um bestimmte Datensätze oder Anhänge in einer vertrauenswürdigen Instanz zu signieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Importieren Sie den signierten Signaturauftrag mit einem Update-Satz in Ihre geschützte Instanz.
4. Führen Sie in der geschützten Instanz den importierten Signierauftrag aus.

Erstellen Sie einen Auftrag, um bestimmte Datensätze oder Anhänge in einer vertrauenswürdigen Instanz zu signieren

Signieren Sie einen bestimmten Datensatz oder eine Gruppe von Datensätzen, die Sie in einer vertrauenswürdigen Instanz definieren.

Vorbereitungen

Erforderliche Rolle: Security_admin oder sn_kmf.cryptographic_Manager

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Neu erstellen**an.
2. Bei **Welche Art von Sicherheitsauftrag möchten Sie erstellen?** Eingabeaufforderung, wählen Sie aus **Signierauftrag** .
   Ein neuer **Signierauftrag** Datensatzanzeigen.
3. Füllen Sie im Formular die Felder nach Bedarf aus:

Signierauftragsfelder

Feld	Beschreibung
Name	Beschreibender Name für diesen Auftrag.
Typ	Typ des Sicherheitsauftrags. Um bestimmte Datensätze zu signieren, wählen Sie aus **Signieren Sie Bestimmte Datensätze** Option. Um bestimmte Anhänge zu signieren, wählen Sie aus **Signieren Sie Bestimmte Anhänge** .
Status	Status dieses Auftrags. Dieses Feld beginnt mit dem Wert von **Neu** . Dieses Feld ist schreibgeschützt.
Tabelle	Tabelle mit den Datensätzen oder Anhängen, die Sie signieren möchten. Wenn Sie Anhänge signieren, wählen Sie die Tabelle mit Datensätzen aus, denen die Anhänge zugeordnet sind, nicht die Tabelle „Anhang“ [sys_attachment]. **Tipp:** Überprüfen Sie die Tabelle „Key Management Framework (KMF)-Signaturdatensatz“ [sn_kmf_Record_Signature], um sicherzustellen, dass für die von Ihnen ausgewählte Tabelle nicht bereits Signaturen vorhanden sind.
Datensätze filtern	Filterbedingungen, die verwendet werden, um zu begrenzen, welche Datensätze in angezeigt werden **Wählen Sie Datensätze zum Signieren aus** Tabelle.
Datensätze zum Signieren auswählen	Liste der Datensätze in der in ausgewählten Tabelle **Tabelle** Feld, beschränkt durch Filter, der in erstellt wurde **Datensätze Filtern** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

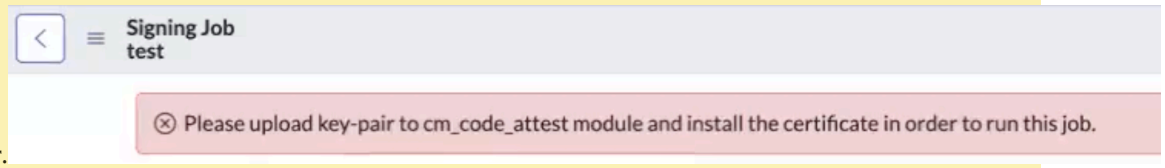
Feld	Beschreibung
	Verschieben Sie Datensätze aus dem **Verfügbar** Fenster zum **Ausgewählt** Fenster, um sie in den Signierauftrag aufzunehmen.
Zeitfensterstart	Der Beginn des Zeitfensters zur Ausführung dieses Auftrags. Der Auftrag wird nach der in dieses Feld eingegebenen Zeit ausgeführt. Ein gültiger Zeitwert ist in koordinierter Weltzeit basierend auf einer 24-Stunden-Zeitnotation.
Zeitfensterende	Das Ende des Zeitfensters zur Ausführung dieses Auftrags. Der Auftrag wird vor der in dieses Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag noch nicht abgeschlossen ist, wird der Auftrag beim nächsten Start des Fensters angehalten und fortgesetzt. Die Endzeit muss nach der Startzeit liegen. Ein gültiger Zeitwert ist in koordinierter Weltzeit basierend auf einer 24-Stunden-Zeitnotation.
Zusammenfassung	Zusammenfassung der Ausführung dieses Auftrags. Dieses Feld ist schreibgeschützt.

4. Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie aus **Speichern** .
5. Wählen Sie unten im Formular aus **Codesignaturauftrag in die Produktion exportieren** .
   Diese Aktion signiert den Signierauftrag und ist bereit für den Export.
6. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Lokale Update-Sätze**
7. Suchen und öffnen Sie den Update-Satz für Ihren Signierauftrag.
   Auf der Registerkarte „Kundenupdates“ sehen Sie, dass dieser Update-Satz den Signierauftrag und den Signaturdatensatz enthält.
8. Wählen Sie Aus **In XML exportieren** .
   Mit dieser Aktion wird eine XML-Datei erstellt, die Ihren Update-Satz auf Ihrem lokalen Gerät enthält.
9. Navigieren Sie in Ihrer Produktionsinstanz zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze** > **an.**
10. Wählen Sie unten auf der Seite die Option aus **Update-Satz aus XML importieren** .
11. Wählen Sie aus **Wählen Sie Datei** Schaltfläche, und wählen Sie die in den vorherigen Schritten erstellte XML-Datei aus.
12. Wählen Sie **Hochladen** aus.
    Ihr Update-Satz wird geladen und in angezeigt **Update-Sätze Abgerufen** Liste.
13. In **Update-Sätze Abgerufen** Öffnen Sie den Datensatz für Ihren importierten Update-Satz.
14. Wählen Sie aus **Vorschau Des Update-Satzes Anzeigen** Schaltfläche.
    Nachdem die Vorschau erfolgreich abgeschlossen wurde, wird angezeigt **Update-Satz Bestätigen** Schaltfläche wird angezeigt.
15. Wählen Sie Aus **Update-Satz Bestätigen** .
16. **Alle** > **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
17. Öffnen Sie Ihren Signierauftrag.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

18. Wählen Sie Aus **Starten** Zum Ausführen des Signaturauftrags.

> **Warnung:** Wenn das Schlüsselpaar nicht in Ihre Produktionsinstanz hochgeladen wurde, wird oben im Datensatzformular eine Warnung angezeigt. Wenn dieses Schlüsselpaar in Ihrer Instanz nicht vorhanden ist, wird die **Starten**Schaltfläche ist im Formular nicht sichtbar.



Nächste Maßnahme

Wenn abgeschlossen, wird **Zusammenfassung** Feld zeigt die Ergebnisse des Auftrags an. An Ihren Signierauftragsdatensatz mit dem Namen „Mass_Sign_Records-<sys_id>“ ist auch eine Protokolldatei angehängt. Überprüfen Sie diesen Datensatz auf Details zum Auftrag und eine Liste der sys_IDs für jeden signierten Datensatz.

Signieren Sie die Flows, Subflows und Aktionen in der geschützten Instanz

Verwenden Sie Update-Sätze, um die Flows, Subflows und Aktionen zu signieren und zu validieren, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

- Einrichten Circle of Trust Zwischen den geschützten und vertrauenswürdigen Instanzen.
- Erforderliche Rolle: security_admin

Signieren Sie den vorhandenen Flow, die Subflows und die Aktionen

Signieren und validieren Sie den vorhandenen Flow, Subflows und Aktionen, indem Sie die Codesignatur in der Produktion und vertrauenswürdigen Instanzen aktivieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Prozedur

1. Signieren Sie in der vertrauenswürdigen Instanz die Datensätze in der Tabelle „Schrittinstanz“.

   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.

   b. Klicken Sie auf **Neu**.

   c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie Aus **Massensignierungsdatensätze** .
Tabelle	Tabelle, aus der die Datensätze signiert werden sollen. Wählen Sie Aus **Schrittinstanz** .

   d. Klicken Sie Auf **Codesignaturauftrag in die Produktion exportieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zwei lokal signierte Update-Sätze werden erstellt.

- Ein Update-Satz für die KMF-Signatur.
- Ein weiterer Update-Satz aus dem Verschlüsselungsauftrag zum Exportieren des Codesignaturauftrags.

2. Exportieren Sie in der vertrauenswürdigen Instanz den lokalen Update-Satz in eine XML-Datei.
   a. Navigieren zu **Systemupdate-Sätze** > **Lokale Update-Sätze**an.
   b. Öffnen Sie den Update-Satz, den Sie für das Massensignieren der Datensätze erstellt haben.
   c. Klicken Sie auf **In XML exportieren** Zugehöriger Link und speichern Sie die XML-Datei.
3. Importieren Sie in der geschützten Instanz die XML-Datei.
   a. Navigieren zu **Systemupdate-Sätze** > **Update Sets abgerufen**an.
   b. Klicken Sie auf **Update-Satz aus XML importieren** Zugehöriger Link zum Importieren des Update-Satzes, der aus der vertrauenswürdigen Instanz exportiert wird.
   Weitere Informationen finden Sie unter Importieren Sie den Schnellstart-Update-Satz, und bestätigen Sie ihn .
   Der Update-Satz wurde erfolgreich bestätigt.
4. Führen Sie in der geschützten Instanz den Verschlüsselungsauftrag aus, den Sie zuvor in der vertrauenswürdigen Instanz erstellt haben.
   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
   b. Öffnen Sie den Verschlüsselungsauftrag, den Sie zuvor in der vertrauenswürdigen Instanz erstellt haben.
   c. Klicken Sie Auf **Starten** Um den Auftrag zu starten.
   Eine Bestätigungsnachricht wird angezeigt, in der angegeben wird, dass die Datensätze signiert sind.

Neuen Flow, Subflows und Aktionen signieren

Signieren und validieren Sie neue Flows, Subflows und Aktionen, indem Sie die Codesignatur in geschützten und vertrauenswürdigen Instanzen aktivieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Prozedur

1. Starten Sie in der vertrauenswürdigen Instanz einen Update-Satz.
2. Erstellen Sie in der vertrauenswürdigen Instanz die erforderlichen Flows, Subflows oder Aktionen, und veröffentlichen Sie sie.
   Die Flows, Subflows oder Aktionen werden dem Update-Satz hinzugefügt.
3. Ändern Sie in der vertrauenswürdigen Instanz den Status des Update-Satzes in **Abgeschlossen** Und klicken Sie auf **Aktualisieren** .
4. Signieren Sie in der vertrauenswürdigen Instanz den Update-Satz, indem Sie einen Verschlüsselungsauftrag erstellen.
   a. Navigieren zu **Systemsicherheit** > **Security-Aufträge** > **Alle**an.
   b. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Name	Name zur Identifizierung des Datensatzes.
Typ	Typ des Verschlüsselungsauftrags. Wählen Sie Aus **Update-Satz Signieren** .
Tabelle	Update-Satz, aus dem die Datensätze signiert werden sollen.

d. Klicken Sie auf **Absenden**.

e. Klicken Sie Auf **Starten** Zum Signieren des Update-Satzes.

- **Zusammenfassung** Wird aktualisiert, dass die Datensätze signiert sind.
- Der Update-Satz wird aktualisiert und enthält die Signatur.

5. Öffnen Sie in der vertrauenswürdigen Instanz den signierten Update-Satz-Datensatz, und exportieren Sie ihn in eine XML-Datei.

6. Importieren Sie in der geschützten Instanz den signierten Update-Satz.

a. Navigieren zu **Systemupdate-Sätze** > **Update Sets abgerufen**an.

b. Wählen Sie aus **Update-Satz aus XML importieren** Zugehöriger Link zum Importieren des Update-Satzes, der aus der vertrauenswürdigen Instanz exportiert wird.
Weitere Informationen finden Sie unter Importieren Sie den Schnellstart-Update-Satz, und bestätigen Sie ihn .
Der Update-Satz wurde erfolgreich bestätigt.

Dashboard für Codesignatur-Integrität und -Status

Die Codesignatur Das Dashboard für Integrität und Status bietet eine zentrale, anwenderfreundliche Ansicht von Codesignatur Integrität und Konfiguration der Umgebung. Verwenden Sie es, um Probleme zu identifizieren, die Konfigurationsgenauigkeit zu überprüfen und sichere, unterbrechungsfreie Codesignaturvorgänge zu unterstützen.

Die Codesignatur Das Dashboard „Integrität und Status“ hebt Konfigurationsprobleme hervor und enthält intuitive Anleitungen, die Ihnen helfen, sie schnell zu lösen und den Bedarf an Eskalationen zu reduzieren. Sie können das Dashboard verwenden, um dies zu überprüfen Codesignatur Konfigurationen sind korrekt eingerichtet und funktionieren sicher. Es hilft Ihnen, potenzielle Probleme zu identifizieren, die zu Fehlern führen könnten, und ermöglicht es Ihnen, den beteiligten Stakeholdern genaue Anleitungen zu geben.

Mit dem Dashboard können Sie die folgenden Parameter suchen, filtern und erneut scannen:

- Konfigurationen
- Zertifikatstatus
- Plugin-Details

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Signaturverifizierungszertifikat
- MID-Server-Setup

Um auf das Dashboard für Codesignatur-Integrität und -Status zuzugreifen, wechseln Sie zu **Alle** > **Codesignatur** > **Systemintegrität** > **Dashboard**an.

Dashboard „Übersicht“

Das Übersichts-Dashboard bietet eine zentrale Ansicht von Codesignatur Umgebung, die Echtzeiteinblicke in wichtige Komponenten und ihren Status bietet.

Im Dashboard „Übersicht“ werden die folgenden Berichte angezeigt:

Dashboard „Übersicht“

Titel	Typ	Beschreibung
Enterprise-Plugin	Textfeld	Status wichtiger Plugins und Systemeigenschaften, die für erforderlich sind Codesignatur Funktionalität. **Enterprise-Plugin** Zeigt das Core-Plugin an, das für Signierungsvorgänge erforderlich ist.
Aktivierungseigenschaft	Textfeld	Konfigurationskennzeichnung, die aktiviert Codesignatur Fähigkeiten. **Hinweis:** Diese Einstellung muss sein **Aktiv** Um zu bestätigen, dass die Codesignatur gemäß der spezifischen Anforderung funktioniert.
Signaturvalidierungsstatus	Textfeld	Gibt an, ob die Signaturvalidierung während der Codeausführung erzwungen wird, um sicherzustellen, dass nur die vertrauenswürdigen Skripts ausgeführt werden.
Signaturstatus	Kreisdiagramm	Umfassende Übersicht über alle Skriptsignaturen, einschließlich ihres aktuellen Validierungsstatus. Die Signaturen sind kategorisiert in: • **Vertrauenswürdig** Signaturen sind gültig und dem vertrauenswürdigen Codesignaturzertifikat zugeordnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard „Übersicht“ (Fortsetzung)

Titel	Typ	Beschreibung
		• **Nicht Vertrauenswürdig** Signaturen können nicht validiert werden oder sind mit einem nicht vertrauenswürdigen Verifizierungszertifikat verknüpft. • **Verwaist** Signaturen sind vorhanden, aber nicht mehr mit einem bekannten oder aktiven Zertifikat verknüpft. **Hinweis:** Verwenden Sie diese Informationen, um die Skriptintegrität zu bewerten und bei Bedarf Korrekturmaßnahmen zu ergreifen.
MID-Server-Konfigurationsstatus	Kreisdiagramm	Status und Vertrauensbeziehung aller MID-Server in Ihrer Instanz. Verwenden Sie diesen Abschnitt, um die Gesamtzahl der MID-Server anzuzeigen und ihren Status zu überprüfen. • **Aktive MID-Server** : Die Anzahl der Server, die derzeit ausgeführt werden und erfolgreich verbunden sind. • **Inaktive MID-Server** : Die Anzahl der Server, die nicht ausgeführt werden oder getrennt sind.
Signierte Datensätze nach Typ	Kreisdiagramm	Verteilung der signierten Datensätze nach Datensatztyp, die die prozentuale Abdeckung für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard „Übersicht“ (Fortsetzung)

Titel	Typ	Beschreibung
		die folgenden Kategorien anzeigt: • **Business-Regeln** : Der Prozentsatz der signierten Business-Regel-Datensätze. • **Skripteinbindungen** : Der Prozentsatz der signierten Skripteinbindungsdatensätze. • **Andere** : Der Prozentsatz der signierten Datensätze in anderen unterstützten Kategorien.
Signierte Datensätze nach Anwendung	Kreisdiagramm	Verteilung der signierten Datensätze auf verschiedene Anwendungsmodule, die den Prozentsatz der Codesignaturabdeckung anzeigt. • **Anwenderverwaltung** : Prozentsatz der signierten Datensätze im Modul „Anwenderverwaltung“. • **Formularvalidierung** : Prozentsatz der signierten Datensätze im Zusammenhang mit der Formularvalidierung. • **Andere** : Prozentsatz der signierten Datensätze in allen anderen Anwendungsmodulen.

Signaturverifizierungsstatus

Zeigen Sie den Status gültiger, ungültiger und verwaister Signaturen in verschiedenen Anwendungen an, um die Codesignaturabdeckung zu bewerten. Verwenden Sie diese Informationen, um Bereiche zu identifizieren, die möglicherweise zusätzliche Aufmerksamkeit oder Maßnahmen erfordern.

Im Dashboard „Signaturverifizierungsstatus“ werden die folgenden Berichte angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard Für Signaturverifizierungsstatus

Titel	Typ	Beschreibung
Skriptname	Textfeld	Bezeichner oder Titel, der einem bestimmten Skript im System zugewiesen ist.
Typ	Textfeld	Kategorie des Skripts im System. Es hilft, die Rolle und Funktionalität des Skripts zu definieren. Beispiel: • Business-Regel • Skripteinbindung • Client-Skript • Flow-Aktion
Anwendung	Textfeld	Modul oder Bereich im System, in dem das Skript angewendet wird. Beispiel: • Anwenderverwaltung • Bericht • Formularvalidierung • Workflow • Benachrichtigungen
Status	Textfeld	Gibt den aktuellen Verifizierungsstatus der Skriptsignatur an. • **Gültig** : Die Skriptsignatur wurde verifiziert und ist vertrauenswürdig. • **Ungültig** : Die Skriptsignatur wurde nicht verifiziert oder gilt als nicht vertrauenswürdig.
Zuletzt gescannt	Textfeld	Datum und Uhrzeit, zu der das Skript zuletzt zur Signaturverifizierung gescannt wurde, im folgenden Format: TT/MM/JJ/H:S (Tag/Monat/Jahr/Stunde:Minute)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Codesignatur-MID-Server-Konfiguration

Verwalten und konfigurieren Sie die Vertrauensbeziehungen und Zertifikateinstellungen für MID-Server.

Im Dashboard „Codesignatur-MID-Serverkonfiguration“ werden die folgenden Berichte angezeigt:

Codesignatur-MID-Server-Konfiguration

Titel	Typ	Beschreibung
MID-Server	Textfeld	Name der spezifischen MID-Server-Instanz.
Status	Textfeld	Aktueller Betriebsstatus des MID-Servers. • **Aktiv** • **Inaktiv**
Version	Textfeld	Softwareversion des derzeit verwendeten MID-Servers. Verwenden Sie diese Informationen, um: • Stellen Sie die Kompatibilität mit Ihrer Instanz sicher. • Stellen Sie sicher, dass der Server die neuesten unterstützten Funktionen und Sicherheitsupdates ausführt.
Letztes Check-in	Textfeld	Datum und Uhrzeit der letzten Kommunikation des MID-Servers mit der Instanz im folgenden Format: TT/MM/JJ/H:S (Tag/Monat/Jahr/Stunde:Minute)

Schlüsselpaar und Zertifikate

Im Dashboard „Schlüsselpaar und Zertifikate“ werden Details zu den kryptografischen Schlüsseln und digitalen Zertifikaten angezeigt, die für verwendet werden Codesignatur. Enthält Informationen wie Schlüsseltyp, Zertifikataussteller, Ablaufdatum und Gültigkeitsstatus. Verwenden Sie dieses Dashboard, um Anmeldeinformationen für Codesignaturzertifikate zu verwalten, ihre Gültigkeit zu überprüfen und sicherzustellen, dass sie sicher und vertrauenswürdig sind Codesignatur Vorgänge.

Im Dashboard „Schlüsselpaar- und Zertifikatkonfiguration“ werden die folgenden Berichte angezeigt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration von Schlüsselpaar und Zertifikaten

Titel	Typ	Beschreibung
Zertifikatname	Textfeld	Der eindeutige Bezeichner (Name), der einem digitalen Zertifikat zugewiesen ist, das für verwendet wird Codesignatur.
Krypto-Modul	Textfeld	Die kryptografische Komponente, die zum Generieren, Speichern und Verwalten privater Schlüssel für verwendet wird Codesignatur. Es stellt einen sicheren Schlüsselbetrieb sicher und hilft, vertrauliches kryptografisches Material vor nicht autorisiertem Zugriff zu schützen.
Typ	Textfeld	Die Klassifizierung des kryptografischen Schlüssels oder Zertifikats, der für verwendet wird Codesignatur. Beispiel: • ServiceNow • Drittpartei
Läuft ab	Textfeld	Datum, an dem das digitale Zertifikat abläuft und nicht mehr zur Verwendung gültig ist.
Status	Textfeld	Aktuelle Gültigkeit des digitalen Zertifikats. • **Gültig** : Das Zertifikat ist aktiv und kann für verwendet werden Codesignatur. • **Abgelaufen** : Das Zertifikat hat sein Ablaufdatum überschritten und ist nicht mehr gültig. • **Läuft Bald Ab** : Das Zertifikat nähert sich seinem Ablaufdatum. Verwenden Sie diesen Status, um proaktive Schritte für die Verlängerung zu ergreifen, um Unterbrechungen bei Codesignaturvorgängen zu vermeiden.
Kette	Textfeld	Die Zertifikatkette, die das digitale Zertifikat zusammen mit den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration von Schlüsselpaar und Zertifikaten (Fortsetzung)

Titel	Typ	Beschreibung
		Zwischen- und Stammzertifikaten enthält, die einen Vertrauenspfad einrichten. Wählen Sie Aus **Kette Anzeigen** Zum Anzeigen der Zertifikatkette.

Codesignaturkonfiguration

Im Dashboard „Codesignaturkonfiguration“ werden die Systemeigenschaften und Schlüsseleinstellungen angezeigt, die steuern Codesignatur In Ihrer Umgebung, einschließlich Kennzeichnungen und Durchsetzungsrichtlinien. Diese Einstellungen aktivieren Funktionen, erzwingen die Signaturvalidierung und definieren vertrauenswürdige Quellen.

Im Dashboard „Codesignaturkonfiguration“ werden die folgenden Berichte angezeigt:

Codesignaturkonfiguration

Titel	Typ	Beschreibung
Einstellung	Textfeld	Name einer bestimmten Konfigurationseigenschaft, die eine Funktion oder ein Verhalten im Zusammenhang mit der Codesignatur steuert. Jede Einstellung definiert, wie das System Aspekte wie Signaturvalidierung, Durchsetzung oder vertrauenswürdige Quellen behandeln soll.
Wert	Textfeld	Aktueller Status oder aktuelle Eingabe, die einer bestimmten Einstellung zugewiesen ist. Bestimmt, wie sich die Einstellung verhält. Zum Beispiel ob Codesignatur Ist aktiviert (wahr) oder deaktiviert (falsch). Der Wert wirkt sich direkt auf das System aus Codesignatur Betrieb und Durchsetzung.
Letztes Update	Textfeld	Datum und Uhrzeit der letzten Änderung der Einstellung im folgenden Format: TT/MM/JJ/H:S (Tag/Monat/Jahr/Stunde:Minute)

Codesignaturreferenz

Referenzthemen enthalten zusätzliche Informationen zum Verwalten und Beheben von Problemen mit der Codesignatur.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Codesignatur installierte Eigenschaften

Codesignatur fügt die folgenden Eigenschaften hinzu.

Problembehandlung und Zugriff auf Protokolle

Greifen Sie auf verschiedene Protokolle zu, um Probleme zu beheben und die Fehlerursachen zu identifizieren.

Mit Codesignatur installierte Eigenschaften

Codesignatur fügt die folgenden Eigenschaften hinzu.

Eigenschaft	Typ	Beschreibung
Com.Glide.Codesigning.Expanded.Tracking.enabled	Wahr|Falsch	Bei „wahr“ wird die Validierungslänge für den Metapack für ecc_Queue-Themen erhöht, die in aufgeführt sind **Com.Glide.Codesigning.extended_Tracking.topic.list** Eigenschaft. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Com.Glide.Codesigning.Expanded.Tracking.length	Ganzzahl	Ebenen der Codesignaturvalidierung, die ausgeführt werden soll, wenn Codesignatur aktiviert ist. Der Standardwert ist 3. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Com.Glide.Codesigning.extended_Tracking.topic.list	Zeichenfolge	Kommagetrennte Liste von Themen, die einer verstärkten Nachverfolgung des Metastapels unterliegen sollen. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Com.Glide.Codesigning.Tracking.Agent.validation.exclude.list	Zeichenfolge	Kommagetrennte Liste der ecc_Queue-Agents, für die die Codesignatur übersprungen werden soll
com.glide.codesigning.tracking.debug	Wahr|Falsch	Bei „wahr“ ist die Debug-Protokollierung für den Codesignaturtracker aktiviert.
Com.Glide.Codesigning.Tracking.enabled	Wahr|Falsch	Bei „wahr“ wird die Nachverfolgung der Codesignatur-Anrufer aktiviert. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Com.Glide.Codesigning.Tracking.Logging.enabled	Wahr|Falsch	Bei „wahr“ wird die Protokollierung für die Codesignaturnachverfolgung aktiviert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Typ	Beschreibung
Com.Glide.Codesigning.Tracking.unsupported_script_tracking.enabled	Wahr|Falsch	Bei „wahr“ werden ecc_Queue-Datensätze, die über nicht unterstützte Skripts eingefügt wurden (falls erkannt), nicht notariell beglaubigt. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Com.Glide.Codesigning.Tracking.validation.fail_fast	Wahr|Falsch	Bei „wahr“ schlägt die Codesignaturverifizierung beim ersten Fehler bei der Skriptvalidierung fehl, anstatt alle Skripts zu verifizieren. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Com.Glide.event_Handler.Code_Signing.Tracking	Zeichenfolge	Definiert den Ereignis-Handler, der sicherstellt, dass Kunden, die Codesignatur neu aktivieren, so sicher wie möglich konfiguriert sind. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Com.Glide.Web_Service_outbound.impl.Codesigning.Tracking	Wahr|Falsch	Bei „wahr“ wird die Nachverfolgung der SOAPMessageV2-Codesignatur aktiviert **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Com.snc.csf.Maximum_Update_size	Ganzzahl	Die maximale Anzahl von Datensätzen, die in einem Codesignatur-Update-Satz zulässig sind. Dieser Wert muss auf einen Wert zwischen 6000 und 10000 beschränkt sein. Wenn dieser Wert überschritten wird, werden mehrere Update-Sätze generiert und mit demselben übergeordneten Update-Satz verknüpft, um die Batch-Verarbeitung zu ermöglichen. Diese Einschränkung verhindert UI-Probleme, die in beschrieben werden KB0557104 .
com.snc.csf.servicenow_root_of_trust.disabled	Wahr|Falsch	Gibt an, ob die Funktion „Root of Trust“ aktiv ist. Der Standardwert ist Falsch , Bedeutet das ServiceNow Build-Zertifikate sind vertrauenswürdig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Typ	Beschreibung
		Wichtig: Diese Eigenschaft kann nur mithilfe einer signierten geplanten Aufgabe von einem Anwender mit den Rollen „Administrator“, „Sicherheitsadministrator“ und „KMF-Manager“ geändert werden. Weitere Informationen zum Ändern Ihres Stammes des Vertrauens finden Sie unter Ändern Sie Ihre Root of Trust-Konfiguration.
Com.snc.kmf.Signature.validation.optin	Wahr|Falsch	Bei „wahr“ wird die Codesignatur in Ihrer Instanz aktiviert. **Wichtig:** Diese Eigenschaft kann nur über eine Anforderung in geändert werden Kundenservice und Support.
Glide.jdbcprobeloader.Nachverfolgung	Wahr|Falsch	Schaltet die Codesignatur für JDBC-Datenquellen ein oder aus. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.
Glide.Rest.Codesigning.Nachverfolgung	Wahr|Falsch	Bei „wahr“ wird die Nachverfolgung der RESTMessageV2-Codesignatur aktiviert. **Wichtig:** Erhöhte Sicherheit ist erforderlich, um diese Eigenschaft zu ändern.

Mit Codesignatur installierte Rollen

Die Codesignatur enthält die folgenden Rollen.

Codesignatur-Administrator [Codesigning_admin]

Verwenden Sie die Codesignatur-Administratorrolle, um anderen Anwendern die Rollen „Codesigning_Manager“ und „Codesigning_Auditor“ zuzuweisen.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Besondere Erwägungen

Vermeiden Sie die Gewährung einer Administratorrolle, wenn speziellere Rollen verfügbar sind.

Codesignatur-Manager [Codesigning_Manager]

Verwenden Sie die Rolle Codesignatur-Manager, um die Signaturkonfiguration zu erstellen und zu aktualisieren und Codesignaturaufträge zu erstellen und auszuführen.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Keine.

Codesignatur-Auditor [Codesigning_Auditor]

Verwenden Sie die Rolle Codesignatur-Auditor, um Signaturkonfigurationen und Signaturaufträge anzuzeigen. Die Auditorrolle hat keinen Erstellungs- oder Schreibzugriff auf Codesignatur-Assets.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Keine.

Problembehandlung und Zugriff auf Protokolle

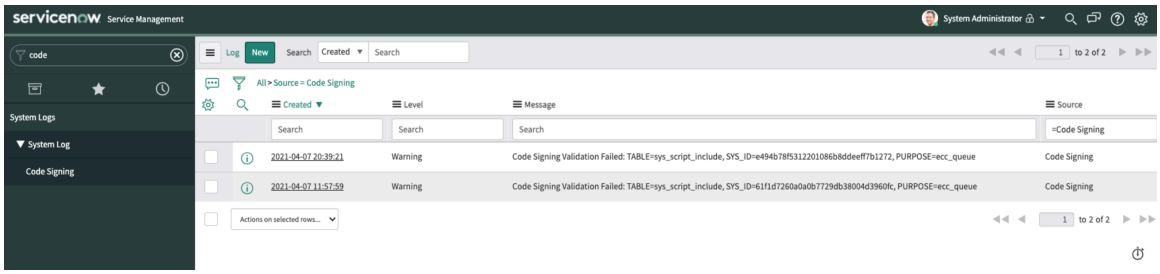
Greifen Sie auf verschiedene Protokolle zu, um Probleme zu beheben und die Fehlerursachen zu identifizieren.

Codesignaturprotokolle

Wenn einer der ECC-Warteschlangendatensätze nicht von signiert ist Codesignaturtracker-API, die nicht signierten Nachrichten und die erforderlichen Details werden im Codesignaturmodul angezeigt. Navigieren zu **Systemprotokolle** > **Systemprotokoll** > **Codesignatur** Um auf die Liste der Datensätze zuzugreifen, die nicht vertrauenswürdig sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

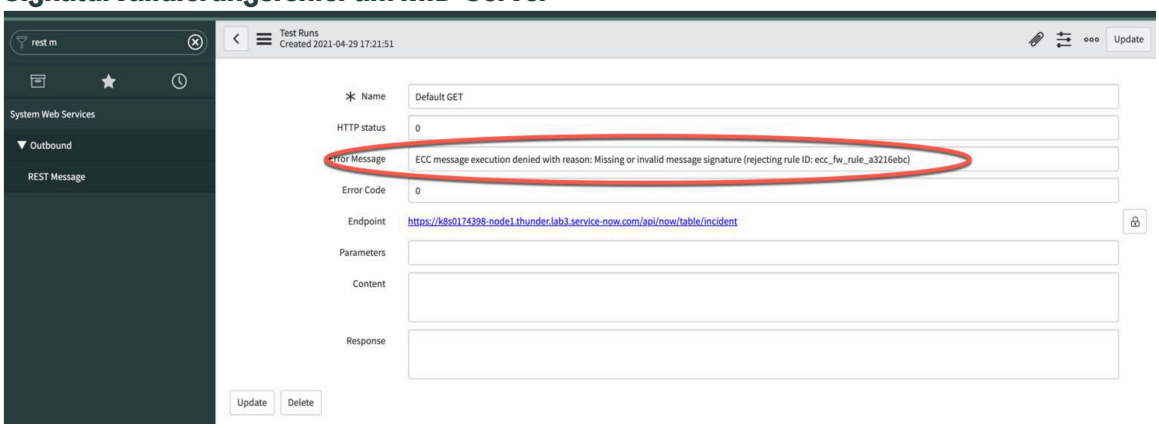


Aktivieren Sie für zusätzliche Debug-Knotenprotokolle *`com.glide.codesigning.tracking.debug`*Und legen Sie ihren Wert auf fest `Wahr` .

Fehler bei der Validierung der REST-Nachrichtensignatur für MID-Server

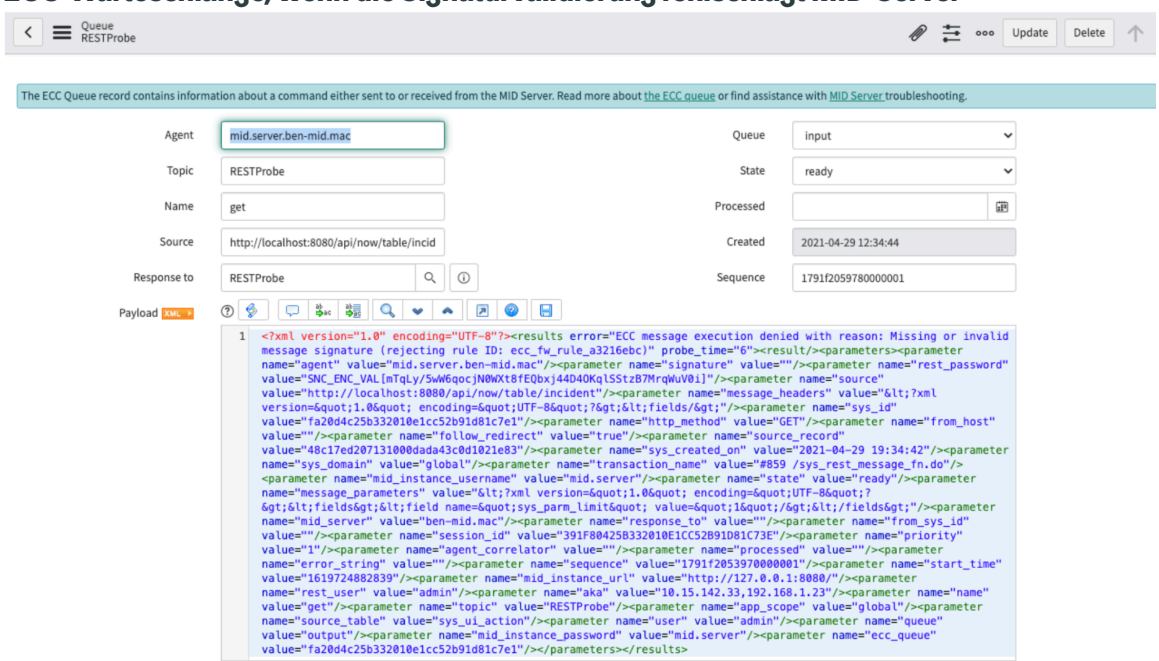
Auf die Fehlermeldung bezüglich des Signaturvalidierungsfehlers zugreifen, Indem Sie zu navigieren **System-Webservices** > **Ausgehend** > **REST-Nachricht** Und Öffnen des erforderlichen REST-Nachrichtendatensatzes.

Signaturvalidierungsfehler am MID-Server



Hinweis: Fehlermeldungen im Zusammenhang mit den ECC-Firewall-Ablehnungen beginnen mit Ausführung der ECC-Nachricht verweigert .

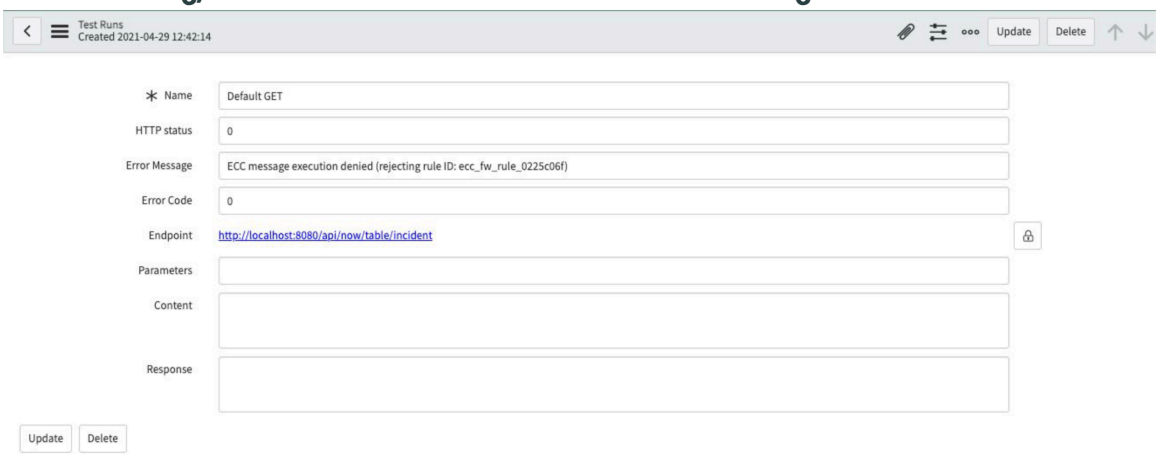
ECC-Warteschlange, wenn die Signaturvalidierung fehlschlägt MID-Server



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlermeldung, wenn die ECC-Nachricht von der Anwenderregel blockiert wird

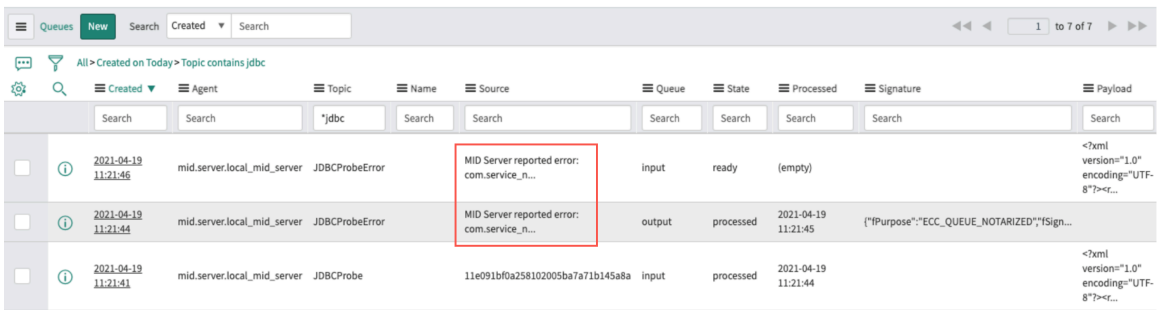


JDBC-Probe

Wenn eine JDBC-Datenquelle mit einer ungültigen oder fehlenden Signatur auf einem ausgeführt wird MID-Server, Wird eine Fehlermeldung mit den erforderlichen Details angezeigt.



Quelle Zeigt auch die Details der Fehlermeldung an.



MID-Server Protokolle

Um die detaillierte ECC-Firewall-Protokollierung zu aktivieren, erhöhen Sie die Protokollebene, indem Sie den Wert des MID festlegen Server Konfigurationsparameter, `mid.log.level`, Bis ABLAUFVERFOLGUNG . Die detaillierten Protokolle enthalten Informationen zu:

- Regelt, dass MID-Server Aus der Startkonfigurationsdatei geladen.
- Granulare Ausführungsverfolgung von Regeln.
- Bestimmte Regel, aufgrund der eine ECC-Nachricht vorliegt Ist Muss akzeptiert oder abgelehnt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn boot-config.xml Ist ungültig, MID-Server Startet nicht, und die Fehlerdetails werden in den MID-Agent-Protokollen protokolliert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antivirus-Scanning

Schützen Sie mit Antivirus-Scanning Ihre Instanz vor Virusinfektionen, die durch Dateianhänge Ihrer Systemdatensätze wie Incidents, Probleme und Storys eingeschleust werden können.

Erkunden Sie Virenschutzscans



Erfahren Sie mehr über den Wert von Virenschutzscans.

Konfigurieren Sie den Virenschutz



Erfahren Sie, wie Sie den Virenschutz konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösen Sie Infizierte Dateien Auf



Erfahren Sie, was Sie mit infizierten Dateien tun können.

Referenz für Antivirus-Scans



Erfahren Sie mehr über die Wörterbuchattribute für die Virenanalyse.

Virenschutzscans Erkunden

Schützen Sie mit Antivirus-Scanning Ihre Instanz vor Virusinfektionen, die durch Dateianhänge Ihrer Systemdatensätze wie Incidents, Probleme und Storys eingeschleust werden können.

Antivirus-Scanning Scannt Dateianhänge, die in Ihrer Anhangstabelle [sys_attachment] gespeichert sind, um Anwender vor dem Hochladen und Herunterladen infizierter Dateien zu schützen. Alle von der Plattform unterstützten Dokumenttypen werden durch Antivirus-Scanning gescannt.

Wenn Antivirus-Scanning Ist aktiviert, werden standardmäßig alle Dateianhänge in der Tabelle „Anhänge“ [sys_attachment.do] gescannt.

Die Virenschutz Plugin (com.Glide.SNAP) ist standardmäßig in Ihrer Instanz aktiviert und aktiviert. Als Administrator können Sie deaktivieren und erneut aktivieren Antivirus-Scanning Funktion in Ihrer Instanz am Umschalter, legen Sie Konfigurationsoptionen fest, und überprüfen Sie die Virenschutzaktivität in der Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Antivirus-Scanning Ist auch für Kunden in der Government Community Cloud (GCC) und in der gewerblichen Umgebung verfügbar.

  GCC-Anwender müssen die Eigenschaft (com.Glide.Snap.FED_enable_Scan) auf festlegen `Wahr` Um mit der Verwendung der Funktion zu beginnen.

  Gewerbliche Anwender müssen festlegen *`com.glide.snap.enable_scan`*Bis `Wahr` .

- HTTP- und HTTPS-Kommunikationsprotokolle werden unterstützt.
- Edge-verschlüsselte Dateien sind von diesem Scan ausgeschlossen.
- Virenschutzdefinitionen werden täglich aktualisiert.
- Dateien mit einer Dateigröße von mehr als 100 MB werden nicht gescannt.

E-Mail-Scan

Eingehende E-Mails werden vom System auf Viren gescannt E-Mail-Filter , Nicht von Antivirus-Scanning.

Feld „Dateianhang“ in einer Tabelle

Das Hinzufügen von **Dateianhang** Das Feld in einer Tabelle generiert zz_yy-Tabellen. Diese Tabellen sind dynamisch und virtuell. Sie werden automatisch generiert, wenn der Spaltentyp verwendet wird **File_attachment** Wird übergeordneten Tabellen hinzugefügt.

Erwägen Sie, ein Anwenderfoto zur Tabelle „Anwender“ hinzuzufügen und in die Formularansicht zu integrieren. Wenn ein Foto in einen Datensatz hochgeladen wird, wird der Anhang automatisch in die Tabelle „sys_attachment“ hochgeladen. Die Tabelle „sys_attachment“ ordnet das Foto der Tabelle „zz_yyUsers“ zu.

Standardmäßig werden nur Anhänge gescannt, die an zz_yylive_Profile-Tabellen angehängt sind. Zum Scannen anderer Tabellen mit dem Spaltentyp **File_attachment** Erstellen Sie die Systemeigenschaft *`com.glide.snap.scan.zz_yytables`*Und fügen Sie den Tabellennamen ein.

Beispiel

Die Tabellen „zz_yycident“ und „zz_yycase“ sind dynamische Tabellen, die erstellt werden, wenn die Spalte den übergeordneten Tabellen „Incident“ und „Case“ hinzugefügt wird. Der Eigenschaftswert muss lauten *`zz_yyincident,zz_yycase`*.

Nachdem diese Eigenschaft festgelegt wurde, werden Anhänge für die Tabellen „zz_yyincident“ und „zz_yycase“ gescannt.

Szenarien werden gescannt

Überprüfen Sie diese Upload- und Download-Szenarien, um zu verstehen, wie das System potenzielle Sicherheitsbedrohungen aus Dateien identifiziert, die an Ihre Datensätze angehängt sind.

Szenario 1: Laden Sie eine Datei hoch

1. Der Anwender lädt unwissentlich eine infizierte Datei in einen Datensatz hoch.
2. Das System scannt die Datei und verschiebt sie in die Quarantäne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Die Datei wird im Fenster Anhänge angezeigt, wo sie als nicht verfügbar markiert ist.
4. Der Anwender wählt die Datei aus, und diese Fehlermeldung wird angezeigt: Die Datei Infected_testing.txt hat den Sicherheitsscan nicht bestanden. Entfernen Sie die Datei aus dem Datensatz INC0000059, und versuchen Sie es erneut.
5. Das System sendet eine E-Mail-Benachrichtigung an den Anwender und den Virenschutz-Administrator.
6. Der Anwender schließt das Fenster Anhänge und wird zum Datensatz zurückgegeben. Die infizierte Datei wird im Header als nicht verfügbar angezeigt. Beispiel: Infizierte_testing123.txtZ [nicht verfügbar] .

Szenario 2: Laden Sie eine Datei herunter

1. Der Anwender öffnet einen Datensatz, um eine angehängte Datei herunterzuladen.
2. Der Anwender weiß nicht, dass die Datei infiziert ist, und wählt sie zum Herunterladen aus.
3. Das System scannt die Datei, verschiebt sie in die Quarantäne und zeigt eine Meldung ähnlich wie an Die Datei infected_testing123.txt hat die Sicherheitsprüfung nicht bestanden und kann nicht heruntergeladen werden.
4. Der Anwender schließt die Nachricht, und der Bildschirm wird aktualisiert und zeigt an, dass die Datei nicht verfügbar ist.
5. Das System sendet eine E-Mail-Benachrichtigung an den Anwender und den Virenschutz-Administrator.

Szenario 3: Laden Sie eine ZIP-Datei herunter

1. Ein Anwender öffnet einen Datensatz und lädt eine ZIP-Datei herunter, die an ihn angehängt ist.
2. Das System scannt die ZIP-Dateien einzeln.
3. Eine Datei besteht den Sicherheitsscan nicht und ist als nicht verfügbar markiert. Die verbleibenden Dateien wurden komprimiert und erfolgreich heruntergeladen.
4. Der Anwender öffnet die ZIP-Datei und sieht zusätzlich zur erfolgreich heruntergeladenen Datei eine Datei „error.txt“. Diese Datei enthält eine Fehlermeldung, die angibt, welche Datei nicht gescannt wurde und daher nicht in der ZIP enthalten war.
5. Der Anwender öffnet den Datensatz erneut und sieht, dass die nicht verfügbare Datei in verschoben wurde **Potenzielle Sicherheitsrisiken** Abschnitt im Fenster „Anhänge“ und kann nicht heruntergeladen werden.

Antivirus-Scanning konfigurieren

Konfigurieren Antivirus-Scanning In Ihrer Instanz und auf Tabellenebene.

Vorbereitungen

Erforderliche Rolle: Antivirus_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Antivirus-Scanning Ist standardmäßig in Ihrer Instanz aktiv, in der Anhänge automatisch gescannt werden, um Dateien zu identifizieren, die mit Viren infiziert sind. Konfigurieren Sie die Funktion, indem Sie sicherstellen, dass der Scan in Ihrer Instanz aktiviert ist, und indem Sie alle Tabellen identifizieren, die Sie vom Scan ausschließen möchten.

Prozedur

1. Navigieren zu **Alle** > **Virenschutz** > **Konfiguration**an.
2. Beachten Sie beim Konfigurieren der Funktion Folgendes.

Option	Beschreibung
Antivirus-Scanning aktivieren	Virenschutz-Scans ist aktiv und standardmäßig in der Instanz aktiviert. Ihr Umschalter ist auf die Position ein gesetzt und wird grün angezeigt. **Hinweis:** Um die Eigenschaft auf festzulegen Falsch Wenden Sie sich an den Kundensupport.
Herunterladen von Anhängen zulassen, wenn Antiviren-Scanner nicht zur Verfügung steht	Wenn diese Option auf die Position ein festgelegt ist, wird die Virenschutzprüfung umgangen, wenn eine Zeitüberschreitung beim Scanner auftritt und keine Antwort abgerufen werden kann. In dieser Situation wird der Dateidownload fortgesetzt, ohne den Scan abzuschließen. Wenn die Option deaktiviert ist, ist der Dateidownload bis zum erfolgreichen Abschluss des Scans verboten.
Liste der ausgeschlossenen Tabellen	Alle Dateianhänge, die einer Tabelle in dieser Liste zugeordnet sind, sind von der Virenschutzprüfung ausgeschlossen. Fahren Sie mit Schritt 4 fort, wenn Sie die Tabellen definieren möchten, die das System vom Scannen ausschließt.

3. Wählen Sie **Speichern**.
4. Schließen Sie Tabellen aus dem Antivirus-Scan aus, indem Sie sie zu hinzufügen **Liste der ausgeschlossenen Tabellen** .
   a. Navigieren Sie zu **Systemdefinition** # **Wörterbuch**
   b. Suchen Sie nach der Tabelle, die Sie aus dem Scan ausschließen möchten, und wählen Sie die Tabelle aus, deren Typ auf Sammlung festgelegt ist.
   c. In **Attribute** Wählen Sie die Registerkarte aus **Neu** .
   d. Hinzufügen Ausschließen_von_Antivirus_Scan Geben Sie im Feld Attribute ein Wahr In **Wert** Feld.
   e. Wählen Sie **Absenden**.

Ergebnis

Antivirus-Scanning Ist in Ihrer Instanz und in aktiviert **Liste der ausgeschlossenen Tabellen** Auf der Seite „Virenschutzkonfiguration“ werden alle Tabellen ausgefüllt, die Sie vom Scan ausgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateien in Quarantäne werden überprüft

Überprüfen Sie Dateianhänge in Quarantäne, und ergreifen Sie bei Bedarf weitere Maßnahmen.

Vorbereitungen
Erforderliche Rolle: Antivirus_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Überwachen Sie Ihre Dateieinträge in Quarantäne auf der Seite „Antivirus-Quarantäne“ in regelmäßigen Abständen, um eine der folgenden Aktionen auszuführen.

Prozedur

1. Navigieren zu **Alle** > **Virenschutz** > **Quarantäne**an.
2. Aktivieren Sie das Kontrollkästchen neben jedem Eintrag in Quarantäne, für den Sie eine verfügbare Aktion ausführen möchten.
3. Wählen Sie aus **Aktionen für ausgewählte Zeilen** Dropdown-Liste im Banner, um die Aktion auszuwählen, die für den ausgewählten Eintrag in Quarantäne ausgeführt werden soll.

Aktion	Beschreibung
Löschen	Wählen Sie diese Aktion aus, um die Datei in Quarantäne zu löschen, wenn sie von Anwendern nicht mehr benötigt wird.
Wiederherstellung	Wählen Sie diese Aktion aus, um die Datei basierend auf Ihrer Bewertung des Status oder der Anwenderanforderung wiederherzustellen. Scannen Sie die Datei jedoch mit Ihrem Virenschutzprodukt einer Drittpartei, bevor Sie sie wiederherstellen, um Virenbedrohungen zu minimieren. Nach der Wiederherstellung steht die Datei dem Anwender zum Herunterladen zur Verfügung.
Herunterladen	Wählen Sie diese Aktion aus, um die Datei für weitere Scans und Analysen auf Ihr lokales System herunterzuladen.

Ergebnis
Das System fordert eine Bestätigung an und führt die ausgewählte Aktion entsprechend Ihrer Eingabe aus.

Zugehörige Informationen

Instanz-Sicherheitszentrum

Virenschutzmetriken

Überprüfen Sie die Virenschutzaktivität

Überprüfen Sie das Antivirus-Aktivitätsprotokoll, das alle Aktivitäten nachverfolgt, die in potenziell infizierten Dateien auftreten, ab dem Zeitpunkt, an dem sie erkannt und in die Quarantäne gestellt werden.

Vorbereitungen
Erforderliche Rolle: Antivirus_admin oder admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieses Protokoll funktioniert als Bericht, der Virenschutzaktivitäten wie Discovery, Löschung und andere mögliche Dateiereignisse in Quarantäne erfasst.

Prozedur

1. Navigieren zu **Alle** > **Virenschutz** > **Aktivität**an.
2. Überprüfen Sie das Protokoll der Dateien in Quarantäne.
   Sie können die Aktionen anzeigen, die in der Spalte Ereignis für jede Datei in Quarantäne ausgeführt werden.

Nächste Maßnahme

Legen Sie fest, welche Datensätze Sie löschen, wiederherstellen, herunterladen oder im Protokoll behalten möchten. Siehe Überprüfen Sie Dateien in Quarantäne

Verstehen von Wörterbuchattributen für Antivirus-Scanning

Wörterbuchattribute ändern das Verhalten der Tabelle oder des Elements, die bzw. das der Wörterbuchdatensatz beschreibt. Als Administrator können Sie die Werte von Wörterbuchattributen festlegen, um das Verhalten der standardmäßigen Virenscans-Konfiguration zu ändern.

Wörterbuchattribute für Antivirus-Scanning

Name	Wert	Zielelement	Beschreibung
Ausschließen_von_Antivirus_Scan	wahr/falsch	Beliebige Tabelle	Bei „wahr“ werden Dateianhänge in der Tabelle vom Virenschutz-Scan ausgeschlossen. Siehe Antivirus-Scanning konfigurieren
Supress_Antivirus_email_Notification	wahr/falsch	Beliebige Tabelle	Bei „wahr“ wird das Senden von plattformgenerierten E-Mail-Benachrichtigungen gestoppt, wenn eine potenziell infizierte Datei identifiziert wird.
Suppress_Antivirus_ui_Notification	wahr/falsch	Beliebige Tabelle	Bei „wahr“ werden plattformgenerierte UI-Benachrichtigungen angehalten, wenn eine potenziell infizierte Datei identifiziert wird.

Zugehörige Informationen

Tabellen und Felder werden mithilfe von Wörterbuchattributen geändert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTML-Bereinigung

Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Erkunden Sie die HTML-Bereinigung



Erfahren Sie, wie die HTML-Bereinigungsfunktion funktioniert.

Konfigurieren Sie die HTML-Bereinigung



Konfigurieren Sie die HTML-Bereinigung.

Aktivieren Sie die HTML-Bereinigung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie, wie Sie die HTML-Bereinigung aktivieren.

HTML-Bereinigung erkunden

Entfernen Sie unerwünschten Code, und schützen Sie sich vor Sicherheitsbedrohungen wie Angriffen mit websiteübergreifendem Skripting, indem Sie HTML-Markup in HTML-Feldern und übersetzten HTML-Feldern bereinigen.

Verwenden Sie die HTML-Bereinigung, um sicherzustellen, dass HTML-Inhalte in Ihrer Instanz keine potenziell schädlichen Inhalte enthalten. Die HTML-Bereinigung funktioniert, indem HTML-Tags entfernt werden, die zur Gefährdung Ihrer Instanz verwendet werden könnten, z. B. `]]>`, `<link>`, Oder `<embed>`Tags, die verwendet werden können, um unerwünschte Skripts in Ihrer Instanz auszuführen oder Ihre Anwender zu unerwünschten Inhalten zu leiten. Safe-Tags, die die Formatierung Ihrer Inhalte steuern, werden beibehalten. Als Administrator können Sie anpassen, welche Inhalte entfernt oder beibehalten werden. Sie können auch steuern, ob die Bereinigung für alle Inhalte oder nur für von Ihnen angegebene Felder gilt.

Die HTML-Bereinigung überprüft die integrierte Aufnahmeliste auf Markup, das Sie immer beibehalten möchten. Das Desinfektionsgerät stellt bereit *`HTMLSanitizerConfig`* Skripteinbindung, mit der Administratoren die integrierte Aufnahmeliste ändern können. Elemente können auch der Ausschlussliste hinzugefügt werden, um HTML-Markup zu entfernen. Inhalte der Ausschlussliste überschreiben die Aufnahmeliste.

Die folgenden Arten von Elementen können den ein- und Ausschlusslisten hinzugefügt werden:

- Globale Attribute
- Beliebige HTML-Elemente

Hinweis: Standardmäßig sind URL-Attribute wie `Href` Und `src` Unterstützt nur diese Protokolle:

- `http`
- `https`
- `Mailto`
- `Daten`

Zum Beispiel:

```
<a href="https://community.servicenow.com/community">ServiceNow Community</a>
```

Hinweis: Um mehr über zu erfahren *`glide.html.sanitize_all_fields`*Eigenschaft, die die Verwendung der HTML-Bereinigung steuert, siehe HTML-Bereinigung aktivieren [aktualisiert in Security Center 1,3] In Instanzsicherheitshärtungseinstellungen.

Konfigurieren Sie urlAttributes und die Protokolle

Sie können urlAttributes und ihre Protokolle in konfigurieren **HTMLBereinigung** Skripteinbindung. Zum Beispiel:

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        - -
        - -
    }
```

Weil `Notizen` Befindet sich in der Aufnahmeliste in diesem Beispiel, diese URL ist nicht bereinigt:

```
<a title=“Lotus”
 href=“Notes://
ABC/X575C90019DE33/ABC594DCB76D86EB4925653E0011C4C1/ZZ90B7E2D33964749257EE
A003456FD”>Lotus</a></p>
```

Standardmäßige Aufnahmeliste

Hinweis: Die Standard-Aufnahmeliste ist eine Systemliste, auf die Anwender in der Instanz nicht zugreifen können.

```
BUILTIN_HTML_WHITELIST :{

   globalAttributes:{ attribute:["id","class","lang","title","style"],

                           attributeValuePattern:{}},

   label:{ attribute:["for"]},

   font:{ attribute:["color","face","size"]},

   a:{ attribute:["href","nohref","name","shape"]},

   img:{ attribute:["src","name","alt","border","hspace","vspace","align","height","width"},

   table:{ attribute:["border","cellpadding","cellspacing","bgcolor","background","align","no
 resize","height","width","summary","frame","rules"]},


 th:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},


 td:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},

   tr:{ attribute:["background","height","width","align","valign","char off","char"]},

   thead:{attribute:["align","valign","char off","char"]},

   tbody:{attribute:["align","valign","char off","char"]},

   tfoot:{attribute:["align","valign","char off","char"]},

   colgroup:{attribute:["align","valign","char off","char","span","width"]},

   col:{attribute:["align","valign","char off","char","span","width"]},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
p:{attribute:["align"]},
style:{attributeValuePattern:{"type":"text/css"}}
canvas:{ attribute:["height","width"]},
details:{ attribute:["open"]},
summary:{ attribute:["open","valign","char off","char"]},
button:{ attribute:["disabled","accesskey","type"]},
form:{},

input:{ attribute:["size","maxlength","checked","alt","src","type","disabled","readonly","accesskey","border","usemap"]},
select:{ attribute:["disabled","multiple","size"]},
textarea:{ attribute:["rows","cols","disabled","readonly","accesskey"]},
option:{ attribute:["disabled","label","selected"]},
div:{ attribute:["align"]},
ol:{ attribute:["start","type","square"]},
ul:{ attribute:["type","square","itemscope","itemtype","itemref"]},
li:{ attribute:["value","fb__id","itemprop"]},
span:{ attribute:["color","size","data-mce-bogus","itemprop","face"]},
br:{ attribute:["clear"]},
h3:{ attribute:["itemprop"]},
html:{ attribute:["xmlns","lang","xml:lang"]},
link:{ attribute:["rel","type","href","charset"]},
meta:{ attribute:["name","content","scheme","charset","http-equiv"]},
pre:{ attribute:["xml:space"]},
noscript:{},  h1:{},  h2:{},  h4:{},  h5:{},  h6:{},
i:{},  b:{},  u:{},  strong:{},  em:{},  small:{},  big:{},
pre:{},  code:{},  cite:{},  samp:{},  sub:{},  sup:{},
strike:{},  center:{},  blockquote:{},  hr:{},  map:{},
dd:{},  dt:{},  dl:{},  fieldset:{},  legend:{}, figure:{},  tt:{},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
body:{},  caption:{},  head:{},  title:{}, shape:{},},
```

Verwenden von Variablen und Vorlagen in HTML-Feldern

HTML-/übersetzte HTML-Felder werden standardmäßig einer HTML-Bereinigung unterzogen. Dieser Prozess bereinigt die Eingabe-HTML, um sie vor siteübergreifendem Skripting (XSS) und zugehörigen Sicherheitsangriffen zu schützen. Das Speichern von Vorlagen oder Variablen wie ${description} oder {{description}} oder ähnlichem und das Ersetzen dieser Vorlagen durch eine echte Beschreibung nach der Bereinigung reduziert die Effektivität des Bereinigungsprozesses. Dies liegt daran, dass die Bereinigung nur für die Platzhaltervorlage aufgerufen wird und nicht für den HTML-Inhalt. Das Speichern von nur HTML-Inhalten in den HTML-/übersetzten HTML-Feldern trägt zu einem effektiven Bereinigungsprozess bei.

HTML-Bereinigung wird konfiguriert

Sie müssen eine Skripteinbindung ändern, um Konfigurationsänderungen an der HTML-Bereinigung vorzunehmen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**an.
2. Öffnen **HTMLSanitizerConfig** .
3. Um der Ausschlussliste Elemente hinzuzufügen, verwenden Sie die Klasse HTML_BLACKLIST.

   Um der Aufnahmeliste Elemente hinzuzufügen, verwenden Sie die Klasse HTML_WHITELIST.

   Dieses Format verwenden:

```
HTML_XXXXLIST :{
      globalAttributes :{

         attribute:[attribute-name1,...],
         attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,...}

      },<html-element-name>:{// Same as Above},----}
```

   - *`globalAttributes`* Enthält Attribut- oder attributeValuePattern-Elemente, die global für alle HTML-Elemente gelten.
   - *`attribute`* Ist eine kommagetrennte Liste von Attributen.
   - *`attributeValuePattern`* Ist ein Wörterbuch von Attribut-zu-Attribut-Wert-regex-pattern-Paaren. Das Attribut-Wert-regex-pattern ist ein regulärer Ausdruck, der dem Attributwert entsprechen muss.

Example:
Betrachten Sie das folgende Beispiel:

```
HTML_WHITELIST:{
      globalAttributes:{
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        attribute:["id","name"],},
    img:{
        attribute:["style","align"],
        attributeValuePattern:{src:".*jpeg"}},
    iframe:{},}
```

Der Aufnahmeliste werden die folgenden Elemente hinzugefügt:

- Die ID und der Name der globalen Attribute. Dies ist eine Liste von Zeichenfolgen, die global auf alle Elemente angewendet werden können.
- Das img-Element, in dem die Attribute stilistisch und ausgerichtet sind.
- Das img-Element, bei dem das Quellattribut des Bilds eine Datei mit der Erweiterung .JPEG ist. Dies ist ein Beispiel für ein reguläres Ausdrucksmuster, das einem Attributwert entspricht.
- Das iFrame-Element.

HTML-Bereinigung wird aktiviert

Die HTML-Bereinigung bietet eine Eigenschaft zum Aktivieren oder Deaktivieren der Bereinigung für alle HTML-Felder im System.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig ist die Eigenschaft für neue Instanzen auf „wahr“ festgelegt.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein.
2. Legen Sie die Eigenschaften fest *`glide.html.sanitize_all_fields`*Und *`glide.translated_html.sanitize_all_fields`*Bis **Wahr** .

Hinweis: Weitere Informationen zu dieser Eigenschaft finden Sie unter HTML-Bereinigung aktivieren [aktualisiert in Security Center 1,3] In Instanzsicherheitshärtungseinstellungen.

Trouble?

Wenn die Eigenschaften in der Tabelle „Systemeigenschaften“ nicht vorhanden sind, können Sie sie hinzufügen.

Aktivieren Sie die Bereinigung einzelner Felder

Sie können Feldattribute verwenden, um die Desinfektionslösung für einzelne Felder zu aktivieren oder zu deaktivieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zuerst die Bereinigungseigenschaft auf „falsch“ festlegen und dann die Bereinigung pro Feld für jedes Formular aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zur Tabelle sys_properties, und legen Sie fest *glide.html.sanitize_all_fields*Bis **Falsch** .
   Dadurch wird die Bereinigung für alle HTML-Felder im System deaktiviert.
2. Navigieren Sie zu dem Formular, das das HTML-Feld enthält.
3. Klicken Sie mit der rechten Maustaste auf die HTML-Feldbezeichnung, und wählen Sie aus **Konfigurieren Sie Wörterbuch** .
   Das Formular „Wörterbucheintrag“ wird für das HTML-Feld geöffnet.
4. Geben Sie im Feld Attribute einen der folgenden Werte ein:
   - Um die Bereinigung zu deaktivieren, geben Sie ein `html_sanitize=falsch`
   - Um die Bereinigung zu aktivieren, geben Sie ein `html_sanitize=wahr`
5. Klicken Sie auf **Aktualisieren**.
6. Um die HTML-Bereinigung für übersetzte HTML-Felder zu aktivieren, legen Sie fest *glide.translated_html.sanitize_all_fields*Eigenschaft ist **Wahr** .

Aktivieren Sie die Protokollierung der HTML-Bereinigung

Wenn die HTML-Bereinigung Elemente oder Attribute entfernt, werden sie dem Systemprotokoll hinzugefügt.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können diese bereinigten Elemente überprüfen, indem Sie Ihrer Instanz-URL / syslog_list.do?sysparm_query=Source%3DHTMLSanitizer hinzufügen.

Prozedur

1. Um diese bereinigten Elemente zu überprüfen, fügen Sie hinzu `/Syslog_list.do?sysparm_query=Source%3DHTMLSanitizer` Zu Ihrer Instanz-URL.
2. Um die Protokollierung zu aktivieren oder zu deaktivieren, fügen Sie hinzu `Glide.html_bereinigen.discarded_log.enable` Eigenschaft für die Systemeigenschaften, und legen Sie den Wert auf fest **Wahr** (Aktiviert) oder **Falsch** (Deaktiviert).
   Diese Eigenschaft ist standardmäßig **true**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auditing

Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

Untersuchen



Erfahren Sie mehr über die Funktionen und Geschäftsvorteile von Auditing.

Konfigurieren



Erfahren Sie, wie Sie Auditing konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht	Referenz
	
Überprüfen Sie die Tabellen „SYS-Audit“ und „Audit-Beziehungsänderung“.	Erfahren Sie mehr über die Verlaufssätze.

Auditing Erkunden

Verfolgen Sie Datensatzänderungen in für Auditing aktivierten Tabellen. Standardmäßig verfolgt das System unter anderem Änderungen an den Incident-, Change- und Problem-Tabellen nach.

Auditing-Übersicht

Durch Aktivieren des Audits wird die Erstellung, Aktualisierung und Löschung aller Datensätze in der Tabelle nachverfolgt. Wenn Sie einzelne Felder in einer Tabelle auditieren möchten, können Sie Felder ausblenden, die Sie nicht mit einem Wörterbuchattribut nachverfolgen möchten.

Auditinformationen werden in den folgenden Tabellen gespeichert:

- Audit
- Wissen über Verlaufssätze

⚠ **Warnung:** Audits von Systemtabellen, die einen großen Datenverkehr erhalten, z. B. Workflow-Kontexte [wf_context] oder Ereignismanagement-Warnungen [em_Alert], können sich auf die Leistung auswirken. Aus diesem Grund können Sie die Tabelle „em_Alert“ nicht als Ganzes auditieren. Prüfen Sie stattdessen ausgewählte Felder des Interesses. Festlegen `audit=true`Sowohl in der Tabelle „em_Alert“ als auch in den ausgewählten Feldern. Versuchen Sie, so wenige Felder wie möglich zu auditieren.

Anwender werden überprüft

Auditing hat die folgenden Anwender.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Administrator
- security_admin

Auditleistungen

Vorteil	Funktion	Anwender
Aktivieren Sie das Tabellen-Auditing, um Änderungen an allen oder einigen Feldern der Tabelle nachzuverfolgen	Auditing für eine Tabelle konfigurieren	Administrator
Erleben Sie eine verbesserte Methode zum Definieren und Konfigurieren der Audit-Fähigkeit	Konfigurieren Sie Auditing mit der Audit-Verwaltungskonsole	Administrator
Automatisieren und vereinfachen Sie das Löschen von Audit-Daten	Richten Sie Ihre Audit-Aufbewahrung ein	security_admin

Empfehlungen für weitere Themen

Weitere Informationen zur Verwendung von Auditing finden Sie unter:

- Auditing für eine Tabelle konfigurieren
- Konfigurieren Sie Auditing mit der Audit-Verwaltungskonsole
- SYS-Audit- und Audit-Beziehungs-Change-Tabellen anzeigen
- Wissen über Verlaufssätze

Auditkomponenten

Erkunden Sie die folgenden Auditing-Komponenten, um Audittabellen, Löschungen und Ausnahmen besser zu verstehen.

Übergeordnete und untergeordnete Tabellen werden überprüft

Tabellen leiten die Audit-Kennzeichnungen nicht von übergeordneten oder untergeordneten auditierten Tabellen ab.

- Wenn Sie beispielsweise das Auditing für die Tabelle „Konfigurationselemente“ [cmdb_ci] aktivieren, werden nur CIs geprüft, die in dieser Basistabelle gespeichert sind.
- Wenn Sie das Auditing für die Tabelle „Computer“ [cmdb_ci_Computer] aktivieren, werden nur die Computer-CI-Datensätze auditiert, einschließlich aller Felder in der Tabelle „Computer“ [cmdb_ci_Computer], die aus der Tabelle „Konfigurationselemente“ [cmdb_ci] abgeleitet ist.

Auditsystemtabellen

Standardmäßig auditiert das System das Löschen eines Datensatzes aus Systemtabellen nicht. Um eine Systemtabelle zu auditieren, fügen Sie sie der Liste der Tabellen in hinzu `glide.ui.audit_deleted_tables`Eigenschaftsliste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auditieren von Löschungen aus einem Formular oder einer Liste

Standardmäßig auditiert das System das Löschen einzelner Datensätze aus einem Formular. Um Audits zu verhindern, legen Sie das Wörterbuchattribut der Tabelle fest `no_audit_delete`.

Das System auditiert Löschungen aus einer Liste, wenn dies geschieht **Audit** Ist im Tabellenwörterbuch ausgewählt, und die Tabelle ist nicht in aufgeführt `glide.db.audit.ignore.delete`Eigenschaft.

Hinweis: Standardmäßig ist `glide.db.audit.ignore.delete`Eigenschaft ist in der Tabelle „Systemeigenschaft“ [sys_properties] nicht vorhanden. Um die Eigenschaft und die zugehörigen Werte zu ändern, müssen Sie sie zuerst manuell hinzufügen. Wenn jedoch manuell hinzugefügt, werden die folgenden Standardwerte überschrieben:

```
glide.db.audit.ignore.delete =
sys_Mutex,sys_DB_Cache,sys_lucene_Block,sys_lucene_file,sys_lucene_Directory,sys_user_preferences,sys_
cmdb_instance, cmdb_sw_sw_sw_sw_sw_sdb_sdb_sw_sdb_sw_sdb_sdb_sdb_instance
sam_SW_counter_Detail
```

Weitere Informationen zum Hinzufügen von Systemeigenschaften finden Sie unter Fügen Sie eine Systemeigenschaft hinzu

Es ist zu beachten, dass die Audit-Löschungen standardmäßig aktiviert sind, unabhängig davon, ob der Datensatz aus der Formularansicht, der Listenansicht oder durch ein Skript/ eine geplante Aufgabe gelöscht wird.

Informationen geprüft

Beim Auditing werden die folgenden Datensatzänderungen nachverfolgt:

- Eindeutiger Datensatzbezeichner (sys_ID) des Datensatzes, der sich geändert hat
- Feld, das sich geändert hat
- Neuer Feldwert
- Alter Feldwert
- Gibt an, wie oft dieser Datensatz und dieses Feld aktualisiert wurden
- Datum und Uhrzeit des Change
- Anwender, der die Änderung vorgenommen hat
- Grund für den Change (wenn dem Change ein Grund zugeordnet ist)
- Interne Prüfpunkt-ID für den Datensatz, wenn der Datensatz mehrere Versionen hat.

Informationen, die von Audits ausgenommen sind

Einige Updates werden nicht auditiert, obwohl Auditing für eine Tabelle aktiviert wurde. Beispielsweise können 132 Updates im Verlauf eines Datensatzes angezeigt werden, aber nur sieben geprüfte.

Beim Auditing werden die folgenden Informationen ausgeschlossen:

- Durch ein Upgrade vorgenommene Updates.
- Aktualisierungen werden über Importsätze vorgenommen.
- Datensätze in übergeordneten oder untergeordneten Tabellen.
- Felder mit dem Wörterbuchattribut NO_Audit.
- Systemtabellen sind nicht in aufgeführt `glide.ui.audit_deleted_tables`Eigenschaftsliste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Felder, die mit dem sys_-Präfix (Systemfelder) beginnen, mit Ausnahme der Spalten sys_class_Name und sys_Domain_ID.
- UI-Seiten können manchmal Aktualisierungen an einem Datensatz auslösen, ohne ein Audit-Protokoll zu erstellen.
- Jedes Mal, wenn eine Inaktivitätsüberwachung einen Datensatz berührt. Es wird verhindert, dass möglicherweise Hunderte von Updates für einen Incident aufgeführt werden, wobei das Rauschen die nützlichen Daten übertönt.
- Manuelle Änderungen in Performance Analytics Punktzahlen.
- Update-Satz Wird Angewendet
- XML importieren

Auditieren einer Tabelle

Anweisungen zum Auditieren einer Tabelle finden Sie unter Auditing für eine Tabelle konfigurieren.

Standardmäßig verfolgt das System alle Felder in einer auditierten Tabelle. Sie können eine Teilmenge von Feldern in einer Tabelle auf eine von zwei Arten auditieren:

- Sie können das Auditing für die gesamte Tabelle aktivieren und dann die Felder ausschließen, die Sie nicht einschließen möchten. Es ist angemessen, wenn Sie die meisten, aber nicht alle Felder auditieren möchten, und als bezeichnet wird *Ausschlussliste* . Weitere Informationen finden Sie unter Ein Feld von der Prüfung ausschließen (Ausschlussliste).
- Sie können Auditing für die Tabelle aktivieren, aber nur für angegebene Felder. Dies ist angemessen, wenn Sie nur eine kleine Anzahl der Felder der Tabelle auditieren möchten und als bezeichnet wird *Aufnahmeliste* . Informationen zum Einbeziehen eines Felds in eine Aufnahmeliste finden Sie unter Tabellenfeld in Auditing einschließen (Aufnahmeliste).

Nicht abbrechbare Audit-Datensätze

Reduzieren Sie die Wahrscheinlichkeit, dass Audit-Datensätze nicht aufgezeichnet werden, wenn eine Transaktion mit der neuen Standardeinstellung abgebrochen wird.

Audits wurden so festgelegt, dass sofort ein Datensatz in derselben Transaktion mit den Schreibvorgängen des Zieldatensatzes erstellt wird. Wenn der Zieldatensatz gelöscht wird, wird das Audit weiterhin erstellt und unter beibehalten **Löschen des NCA-Test-Audits** Modul.

Hinweis: Der erweiterte Audit-Prozess ist standardmäßig aktiviert. Wenn glide.db.audit.lazy Eigenschaft ist auf festgelegt Wahr , Der erweiterte Audit-Prozess ist deaktiviert.

Vor Zurich Release: Wenn eine Transaktion abgebrochen wird, wurden bestimmte auditierbare Vorgänge nicht aufgezeichnet. Dies liegt daran, dass die Plattform einige Vorgänge zwischen der Datensatzänderung ausführt und vor der Audit-Erstellung abgebrochen wird. Jetzt werden jedoch Audits unmittelbar nach der Änderung des Datensatzes erstellt, wodurch die Wahrscheinlichkeit verringert wird, dass eine abgebrochene Transaktion den Vorgang abbricht, bevor das Audit aufgezeichnet wird.

Audits werden jetzt im selben Thread wie die Transaktion aufgezeichnet. Frühere Audits wurden in einem Hintergrund-Thread erstellt. Dieser Change definiert den Standardwert von neu glide.db.audit.lazy Eigenschaft von „wahr“ bis „falsch“. Diese Eigenschaft ist normalerweise nicht in der Eigenschaftentabelle definiert, da die meisten Instanzen den neuen Standardwert und das neue Verhalten verwenden. In einigen Instanzen ist diese Eigenschaft möglicherweise bereits vorhanden und auf „wahr“ festgelegt, was bedeutet, dass diese Instanzen diese Änderung nicht für das Audit-Verhalten verwenden können.

Hinweis: Es wird empfohlen, diese Eigenschaft zu löschen, um das Update zu nutzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auditing für eine Tabelle konfigurieren

Sie können das Tabellen-Auditing aktivieren, um Änderungen an allen oder einigen Feldern der Tabelle nachzuverfolgen.

Vorbereitungen

Hinweis: Verschlüsselte Felder werden nicht vom Design geprüft. Dieses Verhalten kann nicht konfiguriert werden.

Erforderliche Rolle: admin.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**an.
   Das System zeigt die Liste der Wörterbucheinträge an. Die Liste enthält eine Zeile für jede Tabelle sowie eine Zeile für jede Spalte (Feld) in der Tabelle.
2. Suchen Sie in der Liste der Wörterbucheinträge beispielsweise die Zeile, die der Tabelle entspricht, die Sie auditieren möchten `cmdb_ci_Computer` .
   Sie können die Zeile für die Tabelle selbst von einer Zeile für eine Spalte in der Tabelle unterscheiden, indem Sie die Zeile mit dem richtigen Tabellennamen suchen, einen leeren Eintrag für **Spalte** Name und ein **Typ** Von **Sammlung** .
3. Wählen Sie den Wörterbucheintrag für die Tabelle aus.
   Das System zeigt das Wörterbucheintragsformular an.
4. Überprüfen Sie **Audit** Kontrollkästchen.
5. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

Wenn Sie nur einige Felder in der Tabelle auditieren möchten Aktivieren Sie das Auditing der Aufnahmeliste für eine Tabelle. Wenn Sie die meisten Felder auditieren möchten, einige jedoch ausschließen möchten, finden Sie weitere Informationen unter Ein Feld von der Prüfung ausschließen (Ausschlussliste).

Aktivieren Sie das Auditing der Aufnahmeliste für eine Tabelle

Aktivieren Sie eine Tabelle, um nur die Felder zu auditieren, die Sie explizit angeben. Dies ist nützlich, wenn Sie nur eine geringe Anzahl von Feldern in einer auditierten Tabelle auditieren möchten.

Vorbereitungen

Die Tabelle muss sein Für Auditing aktiviert .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**an.
   Das System zeigt die Liste der Wörterbucheinträge an. Die Liste enthält eine Zeile für jede Tabelle sowie eine Zeile für jede Spalte (Feld) in der Tabelle.
2. Passen Sie bei Bedarf die Listenansicht an, um anzuzeigen **Attribute** Spalte.
3. Suchen Sie in der Liste der Wörterbucheinträge beispielsweise die Zeile, die der Tabelle entspricht, die Sie auditieren möchten `cmdb_ci_Computer` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Zeile für die Tabelle selbst von einer Zeile für eine Spalte in der Tabelle unterscheiden, indem Sie die Zeile mit dem richtigen Tabellennamen, einem leeren Eintrag für den Spaltennamen und einem Typ suchen `collection`.

4. In **Attribute** Feld für diese Zeile eingeben `audit_type=whitelist`.

Nächste Maßnahme
Legen Sie fest, welche Felder Sie in dieser Tabelle auditieren möchten.

Ein Feld von der Prüfung ausschließen (Ausschlussliste)

Verhindern Sie ServiceNow AI Platform Aus der Nachverfolgung einer Teilmenge von Feldern in einer auditierten Tabelle, indem diese Felder aus einem Audit ausgeschlossen werden.

Vorbereitungen
Um ein Feld in einer Tabelle von der Prüfung auszuschließen, müssen Sie zuerst haben Aktivieren Sie das Auditing für diese Tabelle .

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Fügen Sie einer Ausschlussliste einen Satz von Feldern hinzu, wenn Sie die meisten Felder in einer auditierbaren Tabelle auditieren möchten. Wenn Sie nur einige Felder auditieren möchten, folgen Sie den Anweisungen Aufnahmeauflistungsverfahren Stattdessen.

Hinweis: Das Deaktivieren des Audits für journalbasierte Felder kann sich auf die Funktionalität von Funktionen wie dem Aktivitätsformatierer auswirken. Weitere Informationen finden Sie unter KB0743142 .

Prozedur
1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**an.
2. Passen Sie bei Bedarf die Listenansicht an, um anzuzeigen **Attribute** Spalte.
3. Navigieren Sie zu der Zeile, die der Tabelle und dem Feld (Spalte) entspricht, die Sie vom Auditing ausschließen möchten.
4. In **Attribute** Geben Sie für diese Zeile die Spalte ein `No_Audit` .

Tabellenfeld in Auditing einschließen (Aufnahmeliste)

Verfolgen Sie eine Teilmenge von Feldern in einer auditierten Tabelle, indem Sie diese Felder einer Aufnahmeliste hinzufügen.

Vorbereitungen
Um Felder in einer Tabelle zu einer Aufnahmeliste hinzuzufügen, müssen Sie zuerst haben Auditing für diese Tabelle aktiviert Und Auditing der Aufnahmeliste für diese Tabelle aktiviert .

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Fügen Sie einer Aufnahmeliste einen Satz von Feldern hinzu, wenn Sie nur eine kleine Anzahl von Feldern einer auditierten Tabelle auditieren möchten. Wenn Sie die meisten Felder auditieren und nur einige ausschließen müssen, befolgen Sie die Anweisungen Ausschlusslistenverfahren Stattdessen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Lexikon**an.
2. Passen Sie bei Bedarf die Listenansicht so an, dass auch angezeigt wird **Attribute** Spalte.
3. Navigieren Sie zu der Tabelle und dem Feld (Spalte), die Sie zur Aufnahmeliste finden möchten.
4. In **Attribute** Feld eingeben `audit=true`.

Aktivieren Sie das Auditing für eine Systemtabelle

Löschungen aus Tabellen mit dem Präfix „sys_“ werden standardmäßig nicht auditiert. Um Löschungen aus diesen Tabellen nachzuverfolgen, fügen Sie den Tabellennamen zu hinzu `glide.ui.audit_deleted_tables`Eigenschaft. Durch Aktivieren des Plugins „Gelöschte Datensätze wiederherstellen“ werden dieser Eigenschaft mehrere Standardwerte hinzugefügt.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **UI-Eigenschaften**an.
2. Suchen Sie nach **Liste der Systemtabellen (beginnend mit „sys_“, kommagetrennt), für die der Löschvorgang geprüft wird** Eigenschaft.
3. Fügen Sie Tabellennamen hinzu, oder entfernen Sie sie.
   Tabellennamen müssen durch Kommas ohne Leerzeichen getrennt werden.
4. Wählen Sie **Speichern**.

Hinweis: Weitere Informationen zum Auditing finden Sie unter Verständnis der SYS-Audit-Tabelle .

Konfigurieren Sie Auditing mit der Audit-Verwaltungskonsole

Verwenden Sie das Modul „Audit-Management-Konsole“, um eine verbesserte Möglichkeit zum Definieren und Konfigurieren der Audit-Fähigkeit in Ihrer Instanz zu erhalten.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Audit-Management-Konsole**an.
   Eine Liste aller Tabellen in Ihrer Instanz wird angezeigt.

   Hinweis: Standardmäßig wird die Liste der Tabellen angezeigt, für die Audit aktiviert ist.

   Sie können auswählen **Deaktiviert** Registerkarte, um die Liste der Tabellen anzuzeigen, für die Audit deaktiviert wurde. Sie können auch die Registerkarte alle auswählen, um alle Tabellen in Ihrer Instanz mit aktivierter oder deaktivierter Audit-Option anzuzeigen.
2. Wählen Sie die Tabelle aus der Liste aus, in der Sie die Auditing-Konfigurationen aktualisieren möchten.
   Die Tabelle mit den entsprechenden Spalten wird angezeigt. Sie können auch die Gesamtzahl der Spalten in der ausgewählten Tabelle anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: **Spalten** Und **Aufbewahrung** Sind die Registerkarten, die in der Tabelle angezeigt werden.

3. Ändern Sie den Umschalter Audit je nachdem, ob Sie Audit für die ausgewählte Tabelle aktivieren oder deaktivieren möchten.

   Hinweis: Wenn Audit in einer Tabelle aktiviert ist, sind standardmäßig alle Spalten und Felder in der Tabelle aktiviert.

4. **Wahlweise:** Wählen Sie Aus **Bearbeiten Sie Den Audit-Status** Wenn Sie nicht möchten, dass alle Spalten in einer Audit-fähigen Tabelle aktiviert werden.
   Das Modal „zu bearbeitende Spalten auswählen“ wird angezeigt.
5. **Wahlweise:** Heben Sie die Auswahl der Spalten auf, die nicht aktiviert werden sollen.
   Sie können auch eine beliebige Spalte hinzufügen, indem Sie die Spalte aus der Liste der verfügbaren Spalten überprüfen.
6. Wählen Sie Aus **Speichern** Um die neuesten Änderungen zu speichern.
   Wählen Sie Aus **Löschen Sie Alle** Zum Entfernen aller aktivierten Spalten. Siehe Richten Sie Ihre Audit-Aufbewahrung ein Weitere Informationen zur Aufbewahrung von Audit-Daten.

Richten Sie Ihre Audit-Aufbewahrung ein

Verwenden Sie die Option Aufbewahrung, um das Löschen von Audit-Daten gemäß Ihren Anforderungen zu automatisieren und zu vereinfachen.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Audit-Management-Konsole**an.
2. Wählen Sie die Tabelle aus der Liste aus, in der Sie die Aufbewahrungsrichtlinie aktualisieren möchten.

   Hinweis: Standardmäßig landen Sie am Ende dieses Schritts auf der Registerkarte Spalten.

3. Wählen Sie die Registerkarte Aufbewahrung aus, um die Aufbewahrungsrichtlinie für die ausgewählten Tabellen-Audit-Daten zu aktualisieren.
   Ein Modal mit der Aufbewahrungsoption wird angezeigt.
4. Aktivieren Sie den Umschalter Audit-Datensätze automatisch löschen.
5. Wählen Sie die Dauer aus dem Dropdown-Menü Dauer aus.
   Wählen Sie Aus **Ja** Wenn Sie mit der ausgewählten Dauer fortfahren möchten. Sie können auch auswählen **Abbrechen** Wenn Sie eine andere Dauer auswählen möchten.

   Hinweis: Protokolle, die älter als die festgelegte Dauer sind, werden gelöscht und können nicht wiederhergestellt werden.

   Das Modal „Aufbewahrungsrichtlinie“ wird angezeigt und bestätigt die ausgewählte Dauer.
6. Wählen Sie Aus **Speichern** Dient zum Aktualisieren der Aufbewahrungsrichtlinie für die ausgewählte Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. **Wahlweise:** Um das Löschen von Audit-Datensätzen einer Tabelle zu deaktivieren, deaktivieren Sie den Umschalter Audit-Datensätze automatisch löschen, und wählen Sie aus **Speichern** .

> **Hinweis:** Die Audit-Datensätze, die zuvor aufgrund der ausgewählten Aufbewahrungsdauer gelöscht wurden, sind dauerhaft nicht verfügbar.

SYS-Audit- und Audit-Beziehungs-Change-Tabellen anzeigen

Die ServiceNow AI Platform Verfolgt Einfügungen und Aktualisierungen an geprüften Datensätzen in den Tabellen „SYS-Audit“ (sys_Audit) und „Audit-Beziehungsänderung“ (sys_Audit_Relation).

Die ServiceNow AI Platform Verfolgt Audit-Tabellen. Um Tabellen nachzuverfolgen, wählen Sie aus **Audit** Aktivieren Sie das Kontrollkästchen im Wörterbuchdatensatz, um den Wert auf „wahr“ festzulegen. Standardmäßig werden keine Datensätze aus Systemtabellen wie Update-Sätze-Tabellen auditiert.

> **Hinweis:** Um Leistungsprobleme und Endlosschleifen zu vermeiden, überspringt das System alle Business-Regeln oder Workflows, die durch Einfügungen in die SYS-Audit-Tabelle ausgelöst werden.

SYS-Audit-Tabellenspalten

Greifen Sie auf die SYS-Audit-Tabelle in Ihrer Instanz zu, indem Sie eingeben `sys_Audit.list` Im Navigationsfilter.

Die folgenden Spalten werden in den Datensätzen der Tabelle „sys_Audit“ angezeigt:

Feld	Beschreibung
Tabellenname	Tabelle, für die sich der Audit-Datensatz bezieht (z. B. „ `Incident` „)
Feldname	Spalte in der Tabelle, für die sich der Audit-Datensatz bezieht (z. B. „ `Assigned_to` „)
Dokumentenschlüssel	SYS_ID (eindeutiger Datensatzbezeichner) für den Ursprungsdatensatz, der dem Audit-Datensatz zugeordnet ist.
Anwender	Name des Anwenders, der den Change erstellt hat. **Hinweis:** Einige automatisierte Prozesse verwenden das System oder einen Gastanwender, um Änderungen an Datensätzen anzuwenden und nachzuverfolgen. Weitere Informationen finden Sie unter System- und Gastanwender .
Alter Wert	Alter Wert der Feldänderung, die durch diesen sys_Audit-Datensatz dargestellt wird. • Referenzfelder: Eindeutiger sys_ID-Wert des geänderten Datensatzes. • Datums- und Uhrzeitfelder: Wert in Coordinated Universal Time (UTC), wie in der Datenbank gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Neuer Wert	Neuer Wert der Feldänderung, die durch diesen sys_Audit-Datensatz dargestellt wird. • Referenzfelder: Eindeutiger sys_ID-Wert des geänderten Datensatzes. • Datums- und Uhrzeitfelder: Wert in Coordinated Universal Time (UTC), wie in der Datenbank gespeichert.

Funktionsweise der Tabelle „Audit-Beziehungsänderung“ (sys_Audit_Relation)

Die Tabelle „SYS-Audit“ [sys_Audit] verfolgt Änderungen an Referenzfeldern in Tabellen, die für das Auditing gekennzeichnet sind. Diese Aktivität enthält Journalfeldeinträge und Verlaufssätze. Die Tabelle „Audit-Beziehungsänderung“ [sys_Audit_Relation] verfolgt Beziehungsänderungen zwischen Datensätzen der Tabelle „sys_Audit“ und den Quelltabellen, aus denen die geprüften Datensätze stammen. Außerdem wird nachverfolgt, wann ein Datensatz gelöscht wurde.

-
- Jedes Mal, wenn Sie einen Datensatz in einer Tabelle auditieren, wird eine Beziehung zwischen den verschiedenen Ursprungstabellen zum Speicher erstellt, der Daten aufzeichnet. Diese Beziehungsinformationen werden in den Tabellen sys_history_Set, sys_history_line und sys_Journal gespeichert.
- Wenn Sie ein Feld löschen, das sich auf einen auditierten Tabellendatensatz bezieht, zeichnet die Tabelle „sys_Audit_Relation“ den Löschvorgang auf. Mit anderen Worten: Jedes Mal, wenn Sie einen auditierten Datensatz ändern, löscht er zuerst vergangene Elemente und erstellt dann eine Beziehung in der Tabelle „sys_Audit_Relation“ mit neuen Dokument-IDs.

Wissen über Verlaufssätze

Das System generiert automatisch Verlaufssatzdatensätze nach Bedarf aus der Audit-Tabelle, wenn ein Anwender entweder einen Datensatz erstellt oder seinen Verlauf anzeigt.

Wenn sich ein Datensatz in einer auditierten Tabelle befindet, wird sein Verlaufssatz generiert, wenn der Datensatz eingefügt wird oder wenn ein Anwender den Datensatz anzeigt.

Hinweis: Verwenden Sie keine Verlaufssätze, um Berichte zu generieren.

Mehrere Felder mit Informationen werden im Datensatz „Verlaufssatz“ erfasst, der in der Listenansicht angezeigt wird.

Listenansicht – Datensatzfelder

Feld	Eingabewert
ID	Dokument-ID für den Datensatz, dessen Verlauf aufgezeichnet wird.
Tabelle	Auditierte Tabelle für den Datensatz, dessen Verlauf aufgezeichnet wird.
Ladezeit	Zeit, die zum Generieren des Verlaufssatzes benötigt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatzfelder Für Audit-Verlauf

Feld	Eingabewert
Bezeichnung	Die Bezeichnung des Felds, das geändert wurde.
Alt	Wert vor dem Change.
Neu	Wert nach der Änderung.
Typ	Gibt an, ob der Eintrag für ein normales Feld, einen E-Mail-Datensatz oder einen Beziehungsänderungsdatensatz gilt.
Updateanzahl	Gibt an, wie oft dieses Feld geändert wurde. Der Wert -1 gibt an, wann der Datensatz erstellt oder gelöscht wurde.
Update-Zeit	Datum und Uhrzeit des Change. **Hinweis:** Die Aktualisierungszeit für automatisch generierte Verlaufspositionen stimmt nicht mit der erstellten oder aktualisierten Zeit für einen Datensatz in einer bestimmten Verarbeitungssituation überein. Wenn Sie einen Verlaufssatz eines Datensatzes zum ersten Mal anzeigen, wird ein erster Satz von Verlaufszeilendatensätzen automatisch generiert. Da Dateiänderungen in einem Upgrade nicht auditiert werden, tritt diese Datumsabweichung auf, wenn: • Sie zeigen einen Verlaufssatz an, nachdem eine Änderung an einem Datensatz vorgenommen wurde, aber • Bevor in einem zukünftigen Upgrade eine weitere Änderung daran vorgenommen wird.
Anwendername	Name des Anwenders, der den Change erstellt hat.

Verlaufssätze in einer Kalenderansicht

Nachdem Verlaufssätze aktiv sind, wird die Kontextmenüoption Verlauf anhand von Informationen aus dem Verlaufssatz und nicht aus dem ausgefüllt sys_Audit Tabelle. Aus der Perspektive des Anwenders sind dieselben Verlaufsdaten in derselben Anwenderoberfläche verfügbar, aber wie die Informationen gespeichert werden, unterscheidet sich.

Da die Verlaufsansicht eine Kalenderansicht enthält, aber nicht die normale Listenoberfläche zum Filtern und Interagieren mit den Verlaufsdatensätzen verwendet, wird Folgendes aktiviert:

- Verlaufsdaten werden gesucht und gefiltert.
- Historische Daten werden exportiert.

Verlaufssätze anzeigen

Es gibt zwei Möglichkeiten, den Verlaufssatz anzuzeigen, auf die über die Aktion „Kontextmenü“ zugegriffen werden kann **Verlauf** .

Unterschiede zwischen Audit- und Verlaufssätzen

Die Tabellen „Audit“ [sys_Audit], „Verlaufssätze“ [sys_history_Set] und „Verlauf“ [sys_history_line] speichern dieselben Daten, dienen jedoch verschiedenen Zwecken und verwalten Daten unterschiedlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audit-Tabelle [sys_Audit]

In der Tabelle „Audit“ [sys_Audit] speichert das System Verlaufsinformationen für alle Datensätze. Diese Datensätze sollen für immer aufbewahrt werden, damit Administratoren den Verlauf der geprüften Datensätze jederzeit nachverfolgen können. Wenn die Anzahl der Auditdatensätze im Laufe der Zeit zunimmt, wird es ineffizienter, die Audit-Tabelle direkt nach Verlaufsinformationen abzufragen. Es ist viel effizienter, Abfragen nur für die kleineren Teildatensätze auszuführen, für die Sie Verlaufsinformationen anzeigen möchten.

Tabelle „Verlaufssatz“ [sys_history_Set]

Die Tabelle „Verlaufssatz“ [sys_history_Set] gibt an, welche bestimmten Datensätze aus einer auditierten Tabelle Verlaufsinformationen enthalten. In der Tabelle „Verlauf“ [sys_history_line] werden die tatsächlichen Änderungen an Feldwerten gespeichert, die aufgetreten sind.

- Das System generiert automatisch Verlaufssatz- und Verlaufsdatensätze nach Bedarf aus der Tabelle „Audit“, wenn ein Anwender entweder einen Datensatz erstellt oder seinen Verlauf anfordert.
- Anstatt einen vollständigen Verlauf aller Änderungen im System zu enthalten, enthalten Verlaufssatz- und Verlaufsdatensätze nur eine aktuelle Teilmenge der Verlaufsinformationen für Datensätze, für die Anwender solche Informationen erstellt oder angefordert haben.
- Neben Audit-Daten enthalten Verlaufssätze auch die Informationen, die beim Einfügen des Datensatzes festgelegt werden, einschließlich Journalfeldeinträgen. Journalfeldeinträge, die Sie vor der Erstellung eines Datensatzes erstellen, werden auf die gleiche Weise behandelt wie Journaleinträge, die zum Zeitpunkt der Datensatzerstellung erstellt wurden. Diese Journaleinträge werden in Verlaufssätzen mit derselben Erstellungszeit angezeigt und von Daten erstellt, die der zugehörige Datensatz selbst sind.

Das System begrenzt Verlaufssatz- und Verlaufsdatensätze nach:

- Wenn Sie die Tabellenbereinigung haben, löschen Sie Verlaufssatzdatensätze, die seit 30 Tagen nicht aktualisiert wurden.
- Verwenden Sie die Tabellenrotation, um alle sieben Tage zwischen vier Verlaufstabellen zu wechseln. Das System löscht Verlaufsdatensätze, die älter als 28 Tage sind.

Wenn jemand zu einem späteren Zeitpunkt erneut Verlaufsinformationen benötigt, kann das System sie aus Auditing-Quelldatensätzen erneut generieren.

Nachdem das System Verlaufssatzdatensätze generiert hat, wird die Kontextmenüauswahl ausgewählt **Verlauf** Verwendet den Verlaufssatz anstelle von Audit-Datensätzen. Aus Sicht des Anwenders sind dieselben Verlaufsdaten in derselben Anwenderoberfläche verfügbar, die Art und Weise, wie die Informationen gespeichert werden, ist jedoch unterschiedlich.

Steuern Sie den Zugriff auf den Verlauf

Sie können einer Rolle Zugriff zum Anzeigen des Audit-Verlaufs gewähren, indem Sie eine Systemeigenschaft festlegen.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**an.
2. Wählen Sie aus `glide.history.role`Eigenschaft aus der Tabelle.
3. In `List of roles (comma-separated) that can access the history of a record`, Wählen Sie die Anwenderrollen aus, auf die Sie zugreifen möchten.
4. Wählen Sie **Speichern**.

Ergebnis

Alle Änderungen an einem Feld werden ausgelassen, wenn ein Anwender ohne Lesezugriff den Verlauf eines Datensatzes anzeigt.

Ändern Sie die Anzahl der Verlaufseinträge

Standardmäßig werden im Verlauf maximal 250 Verlaufseinträge angezeigt, Sie können diesen Wert jedoch ändern.

Vorbereitungen

Erforderliche Rolle: Administrator

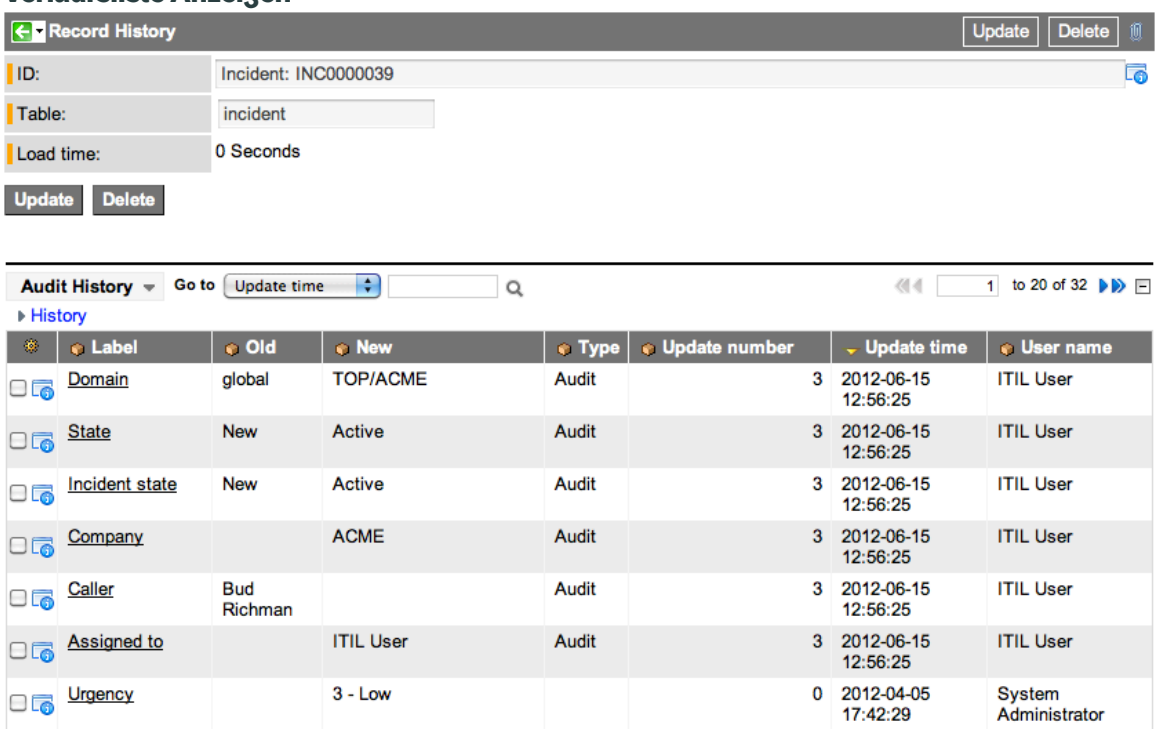
Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**an.
2. Wählen Sie die Eigenschaft `glide.history.max_entries` aus.
3. Legen Sie fest `Maximum number of field entries displayed in record history, default is 250`Wert mit einer neuen maximalen Anzahl von anzuzeigenden Einträgen.

Verlaufsliste

Die Verlaufsliste zeigt jeden Change als eigene Zeile in der Change-Liste an.

Verlaufsliste Anzeigen



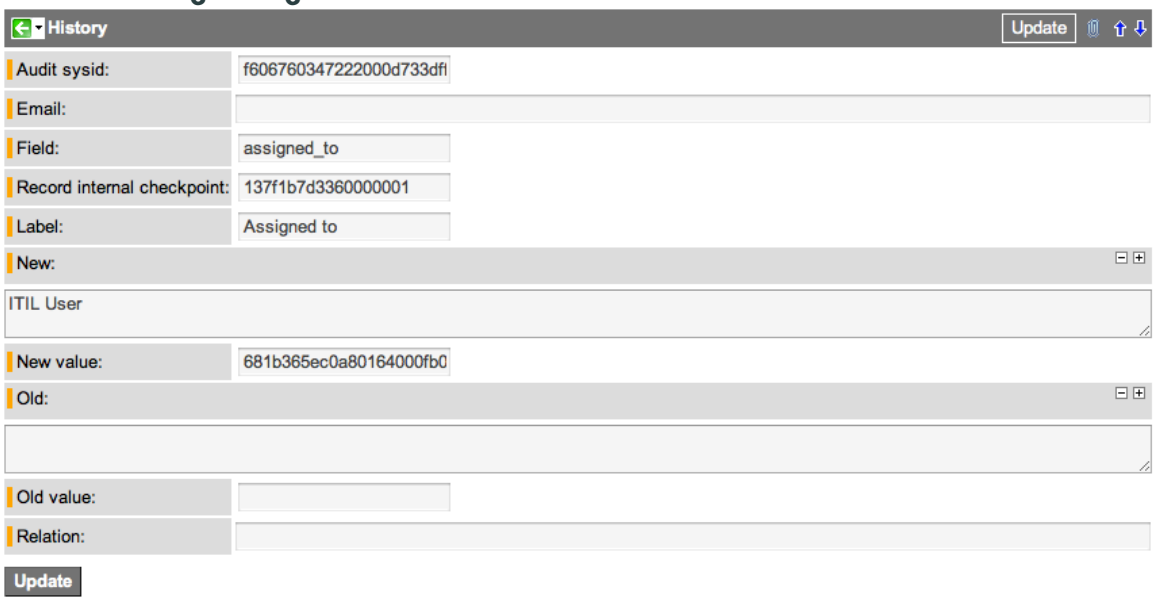
Label	Old	New	Type	Update number	Update time	User name
Domain	global	TOP/ACME	Audit	3	2012-06-15 12:56:25	ITIL User
State	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
Incident state	New	Active	Audit	3	2012-06-15 12:56:25	ITIL User
Company		ACME	Audit	3	2012-06-15 12:56:25	ITIL User
Caller	Bud Richman		Audit	3	2012-06-15 12:56:25	ITIL User
Assigned to		ITIL User	Audit	3	2012-06-15 12:56:25	ITIL User
Urgency		3 - Low		0	2012-04-05 17:42:29	System Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie auf ein Zeilenelement, um zusätzliche Details zum Change anzuzeigen.

Listenänderung Anzeigen



Anforderungen

Um eine Verlaufsliste anzuzeigen, müssen die folgenden Anforderungen erfüllt sein.

Auditing

Audits für die Tabelle müssen aktiviert sein, um eine Verlaufsliste anzuzeigen.

ACLs

Standardmäßig ist *Liste* Die Verlaufsoption ist nur für Anwender mit der Rolle „Administrator“ verfügbar. Um diese Option für nicht-Administratoren zu aktivieren, erstellen Sie eine anwenderdefinierte ACL-Regel, die Lesezugriff auf die Tabelle „Datensatzverlauf“ [sys_history_Set] gewährt.

Rollen

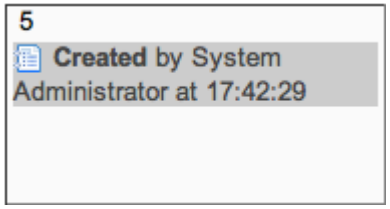
Mindestens eine der Rollen, die der Anwender hat, muss in aufgenommen werden `glide.history.role`Eigenschaft, die standardmäßig die Rolle itil enthält.

Verlaufskalender

Der Verlaufskalender zeigt die Tage an, an denen der Datensatz geändert wurde, wer die Änderung vorgenommen hat und wann.

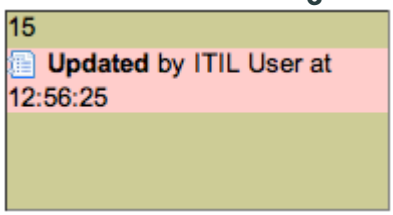
Der Verlaufskalender ist nach Update-Nummer sortiert. Jedem Anwender wird eine Farbe zugewiesen, sodass Sie auf einen Blick erkennen können, wie oft ein Datensatz von einem bestimmten Anwender geändert wurde. Zum Beispiel:

Vom Systemadministrator vorgenommene Änderungen



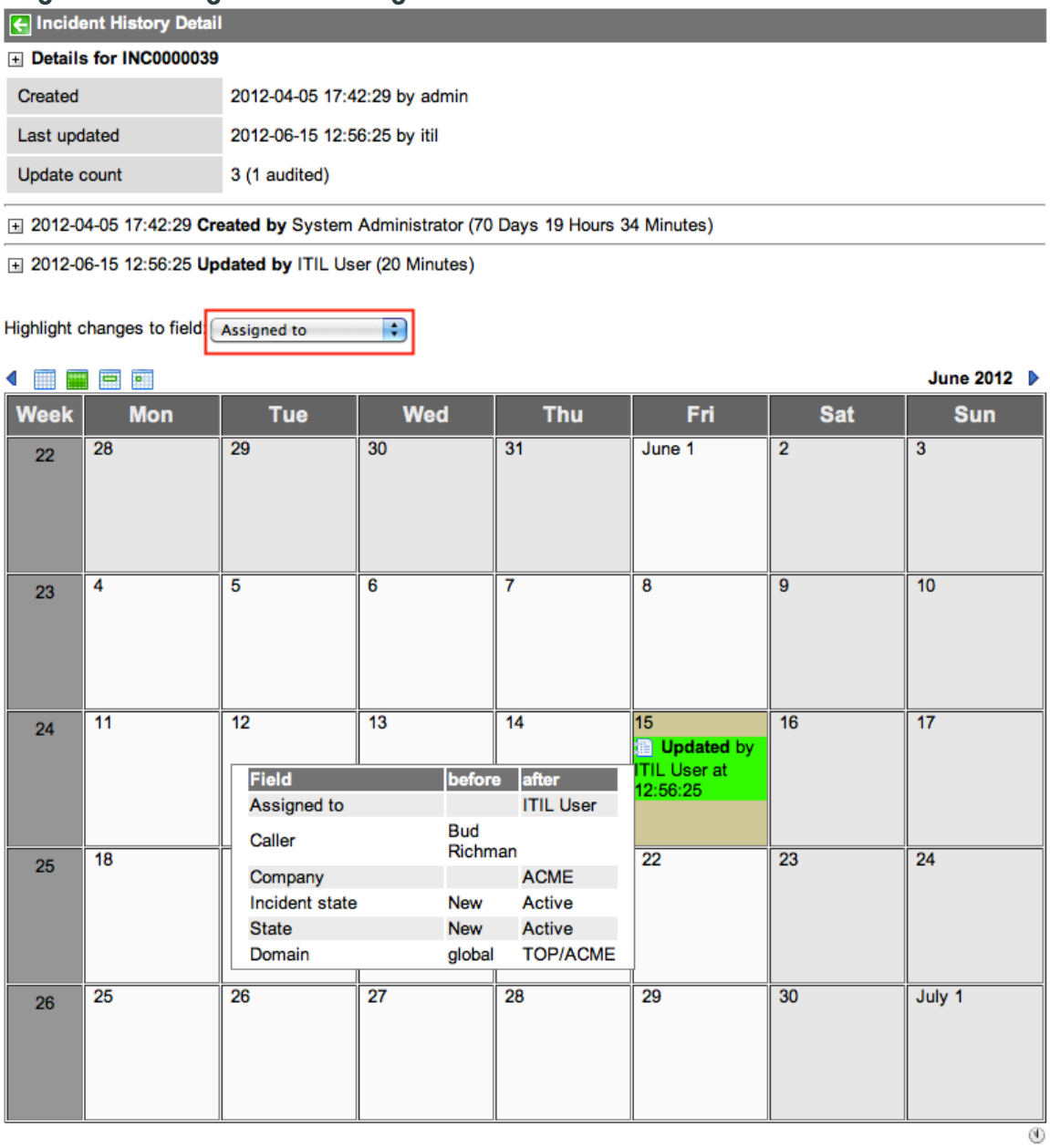
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vom ITIL-Anwender vorgenommene Änderungen



Um Änderungen an einem bestimmten Feld hervorzuheben, wählen Sie das Feld aus **Heben Sie Änderungen am Feld hervor** Auswahlfeld. Durch Auswahl eines Felds in diesem Auswahlfeld wird der Kalender geändert, um die Zeiten hervorzuheben, zu denen das Feld geändert wurde. Bewegen Sie den Mauszeiger über den Text einer hervorgehobenen Änderung, um die Änderung des Werts anzuzeigen.

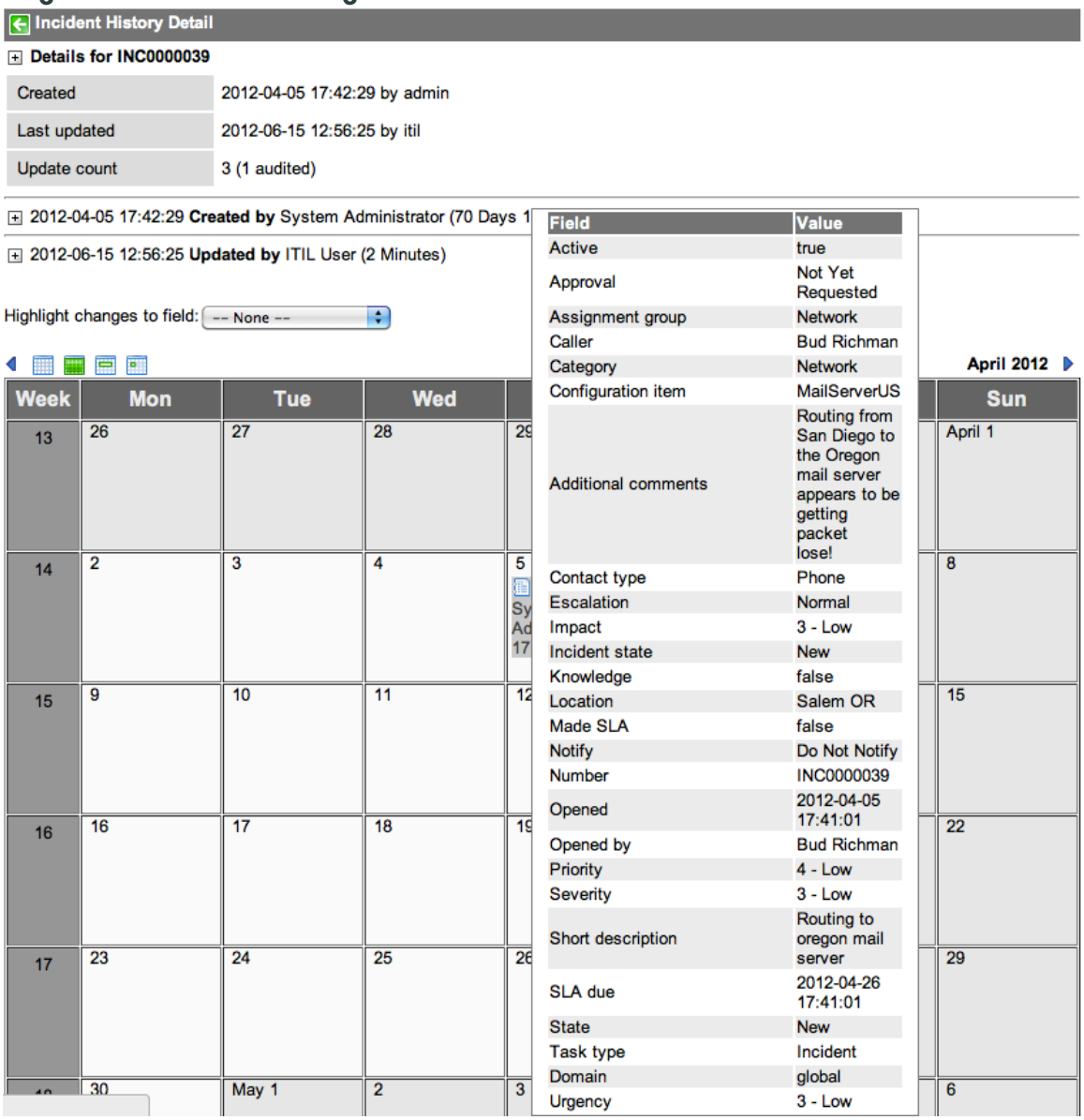
Zeigen Sie hervorgehobene Changes an



Wenn Sie den Mauszeiger über das Symbol in einem Eintrag bewegen, werden alle Wertänderungen in einem Popup angezeigt. Dies sind die gleichen Informationen, die im oberen Teil des Formulars angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Kalenderänderungen an



Sie können auf die Tagesnummer klicken, um eine Ansicht der Änderungen für diesen Tag zu erhalten. Sie können auch auf die Wochennummer links klicken, um eine Wochenansicht zu erhalten. Sie können zu und von Monat zu Monat scrollen, um Änderungen anzuzeigen.

Verlaufszeitleiste

Sie können eine Zeitleiste von Changes für ein CI und die zugehörigen Datensätze, Beziehungen, Baselines und vorgeschlagenen Changes für das CI anzeigen. Zeitleisten sind für CIs in der Tabelle „Konfigurationselement“ [cmdb_ci] oder ein untergeordnetes Element dieser Tabelle verfügbar, wenn Auditing für die Tabellen aktiviert ist.

Erforderliche Rolle: Die ACL für diese Ansicht basiert auf den in definierten Rollen `glide.history.role`Systemeigenschaft, die standardmäßig auf festgelegt ist itil . Außerdem muss der Anwender Lesezugriff auf die Tabelle „Verlaufssatz“ [sys_history_Set] haben, die standardmäßig dem Administrator gewährt wird.

Sie können eine Zeitleiste öffnen, wenn Sie den Verlauf eines CI anzeigen. Sie können den Zeitraum, den Zeitbereich und die Eigenschaften angeben, die in der Zeitleiste angezeigt werden. Sie können entweder anzeigen, was sich in einem bestimmten Change-Satz

Automatische Übersetzung

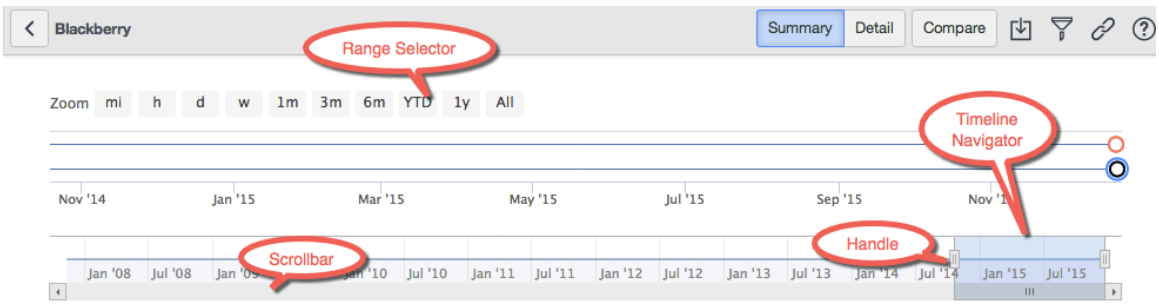
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

geändert hat, oder das gesamte CI anzeigen, um Probleme besser zu beheben. Sie können auch eine Zeitleiste von Changes an den zugehörigen Datensätzen des CI anzeigen und Snapshots des CI jederzeit exportieren und vergleichen.

CI-Changes werden durch Blasen in verschiedenen Formen und Farben entlang der Zeitleiste dargestellt. Die Form jeder Blase stellt einen anderen Change-Typ dar, und die Farbe jeder Blase gibt an, ob die Änderung gültig oder ungültig ist. CI-Baselines werden durch schwarze Kreise dargestellt, über die Sie den Mauszeiger bewegen können, um weitere Details anzuzeigen. Klicken Sie auf **?** Symbol zum Anzeigen von Blasenform- und Farbdefinitionen und zum Anzeigen von Details zum Change-Satz auf eine Blase.

Ein Change an einer Beziehung gilt nur als gültig, wenn er über das Change-Management angewendet wurde. Wenn der Change über das Framework für vorgeschlagene Changes angewendet wurde, ist er gültig. Weitere Validierungsschritte finden Sie unter Erstellen oder bearbeiten Sie ein geplantes Validierungsskript .

Zeitleistenansicht des Verlaufs



Zeitleistenblasen



Hinweis: Vorgeschlagene Changes, die kein geplantes Startdatum haben, werden zu zukünftigen Zeitpunkten platziert.

Zeitleistennavigator

Verwenden Sie die Handles an beiden Enden des Zeitleistennavigators, um den angezeigten Zeitraum zu verlängern oder zu verkürzen.

Sie können zu einem anderen Zeitraum scrollen, indem Sie auf den unteren Teil des Zeitleistennavigators klicken und den Navigator dann nach links oder rechts ziehen.

Zoom

Standardmäßig wird die Zeitleiste für den letzten Monat angezeigt. Neben **Zoom** Bezeichnung über der Zeitleiste können Sie ein anderes Zeitintervall auswählen. Sie können Intervalle von einer Minute bis zum gesamten Datenzeitraum auswählen.

Wenn während des Zeitraums viele Änderungen am CI auftreten, werden die angezeigten Blasen möglicherweise zu voll. Sie können vergrößern oder verkleinern, um die Blasen in einer der folgenden Methoden zu verteilen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ändern Sie das Zeitintervall auf der Zeitleiste. Wenn Sie das Zeitintervall verkürzen, vergrößern Sie es, und wenn Sie das Zeitintervall verlängern, verkleinern Sie es.
- Wählen Sie den Abschnitt der Zeitleiste aus, in den Sie zoomen möchten.

Eigenschaftenfilter

Sie können die angezeigten Blasen filtern. Standardmäßig werden alle Blasen angezeigt, die Änderungen an allen CI-Eigenschaften darstellen. Sie können die Ansicht so einschränken, dass nur die Blasen angezeigt werden, in denen sich ausgewählte Eigenschaften geändert haben, und Blasen ausgeschlossen werden, in denen sich nur nicht ausgewählte Eigenschaften geändert haben.

Die **Detail** Und **Zusammenfassung** Zeigt Eigenschaften in Ihrem Filterbereich an, die sich geändert haben. Die geänderten Eigenschaften sind hellblau hervorgehoben.

In **Zusammenfassung** Anzeigen können Sie alle Eigenschaften des CI oder nur Eigenschaften einschließen, die sich geändert haben. Wenn Sie alle Eigenschaften in der Zusammenfassungsansicht anzeigen möchten, werden geänderte Eigenschaften vor unveränderten Eigenschaften aufgelistet.

Zusammenfassungsansicht

Die **Zusammenfassung** Ansicht zeigt Snapshots der CIs an, die von jeder Blase dargestellt werden. Jeder Snapshot zeigt die Änderungen an den Feldern und Beziehungen des CI gemäß dem Change-Satz an. Zeigt alte und neue Werte vor und nach dem Change sowie alle Beziehungen an, die hinzugefügt oder gelöscht wurden.

Verwenden Sie **>** Und **<** Schaltflächen auf beiden Seiten der Snapshot-Anzeige, um in chronologischer Reihenfolge durch den nächsten und vorherigen Change Set-Datensatz zu scrollen.

Detailansicht

Die **Detail** Ansicht zeigt Snapshots des CI an, die den Blasen entsprechen. Jeder Snapshot enthält die Felder, die sich im Eigenschaftsfilterbereich befinden, und zeigt die geänderten Eigenschaften mit einem hellblauen Hintergrund an. Klicken Sie auf eine Blase, um den entsprechenden Snapshot des CI anzuzeigen. Die angezeigten Daten sind schreibgeschützt.

Verwenden Sie **>** Und **<** Schaltflächen auf beiden Seiten, um in chronologischer Reihenfolge durch den nächsten und vorherigen Change Set-Datensatz zu scrollen.

Zeigen Sie die Zeitleiste von Changes an zugehörigen Datensätzen an

In der Zeitleiste von Changes für einen CI-Datensatz können Sie auch eine Zeitleiste von Changes für die zugehörigen Datensätze des CI anzeigen.

Vorbereitungen

Rolle Erforderlich: administrator

- Zieltabelle: Der CI-Datensatz muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden.
- Auditing: Muss für die Tabelle aktiviert sein, die das CI enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Zeitleiste für das CI.
2. Wählen Sie aus **Zugehörige Datensätze** Symbol und wählen Sie zugehörige Datensätze aus **Liste der zugehörigen Datensätze** Zum Anzeigen.
   Klicken Sie erneut auf das Symbol „zugehörige Datensätze“, um die Zeitleiste für zugehörige Datensätze anzuzeigen.

Ergebnis

Die Zeitleiste der Changes an den zugehörigen Datensätzen des CI wird direkt über der Zeitleiste des CI angezeigt. Wenn Sie alle zugehörigen Datensätze deaktivieren, wird die Zeitleiste für zugehörige Datensätze ausgeblendet.

Nächste Maßnahme

Bewegen Sie den Mauszeiger auf einer Change-Blase in der Zeitleiste der zugehörigen Datensätze, um Details zum Change anzuzeigen, z. B. Datum und Anzahl der geänderten Eigenschaften. Wenn Sie das Zeitintervall im Fokus ändern oder vergrößern oder verkleinern, wirkt sich dies gleichzeitig auf die CI-Zeitleiste und die Zeitleiste der zugehörigen Datensätze aus.

Exportieren Sie einen Snapshot eines Konfigurationselements

Sie können einen Snapshot eines Konfigurationselements aus seiner Zeitleiste exportieren.

Vorbereitungen

Das Konfigurationselement muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden. Auditing muss für die Tabelle aktiviert sein, die das CI enthält.
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Snapshot des CI in ein XML-, PDF-Format (Portal) oder PDF-Format (Querformat) exportieren.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Basiselemente** > **Alle** Zum Öffnen der Konfigurationselementliste.
2. Öffnen Sie einen Konfigurationselementdatensatz.
3. Öffnen Sie die Zeitleiste für den Datensatz.
4. Wählen Sie die Blase aus, die die Zeit darstellt, für die Sie einen Snapshot des CI exportieren möchten.
5. Klicken Sie auf das Exportsymbol ( ).
6. Wählen Sie das Dateiformat aus, das für den Export verwendet werden soll.
   Sie können die Datei zur Anzeige in Ihr System herunterladen.

Vergleichen Sie CI-Snapshots

Sie können die Eigenschaften und Beziehungen eines CI an zwei verschiedenen Punkten in seiner Zeitleiste vergleichen.

Vorbereitungen

Das CI muss sich in der Tabelle „Konfigurationselement“ [cmdb_ci] oder einem untergeordneten Element dieser Tabelle befinden. Auditing muss für die Tabelle aktiviert sein, die das CI enthält.
Erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Zeitleiste für das CI.
2. Klicken Sie auf **Vergleichen**.
3. Wählen Sie ein aus **Starten** Datum und an **Ende** Datum.
4. Klicken Sie auf **Vergleichen**.

Nachverfolgung von Änderungen an Referenzfeldern

Administratoren können Änderungen an Anzeigewerten für Referenzfelder nachverfolgen.

Da Referenzfelder nur einen ID-Wert speichern, kann das System Änderungen normalerweise nur auditieren, wenn sich der ID-Wert ändert. Standardmäßig führt das System keine Audits durch, wenn sich der Anzeigewert eines Referenzfelds ändert.

Berücksichtigen Sie die folgende Situation. Ein Anwender ändert seinen Namen von Jane Smith in Jane Miller. Da der Anwendername der Anzeigewert für die Anwendertabelle ist, bezieht sich jeder vorherige Verweis auf Jane Smith stattdessen auf Jane Miller. Wenn der Administrator nur den Namen des vorhandenen Anwenderdatensatzes aktualisiert, zeigen Audit- und Verlaufsdatensätze nur den neuen Namen Jane Miller an. Standardmäßig bietet das System keine Möglichkeit, zwischen Änderungen zu unterscheiden, die unter dem ursprünglichen Anwendernamen vorgenommen wurden, und Änderungen, die mit dem neuen Anwendernamen vorgenommen wurden.

Wenn Ihre Auditing-Richtlinie die Nachverfolgung von Anwendernamenänderungen erfordert, können Sie:

- Erstellen Sie einen neuen Anwenderdatensatz für den neuen Namen, und deaktivieren Sie den vorherigen Anwenderdatensatz. Das System behält Audit-Datensätze für den alten Anwendernamen bei und erstellt zukünftige Audit-Datensätze mit dem neuen Anwendernamen.
- Erstellen Sie anwenderdefinierte Felder und eine Business-Regel, um den vorherigen Namen und das Datum der Namensänderung zu speichern. Das System kann diese Informationen verwenden, um die richtigen Namen in Audit- und Verlaufsdatensätzen zu erstellen.

Nachverfolgung von Einfügungen

Standardmäßig erstellt das System keine Audit-Datensätze für Einfügungen, da Einfügungen in einer typischen Instanz mehr als 80 % der Größe der Audit-Tabelle ausmachen können.

Die Nachverfolgung von Einfügungen ermöglicht eine bessere Leistung und eine viel kleinere Audit-Tabelle. Administratoren können das Auditieren von Einfügungen aktivieren, indem sie festlegen `glide.sys.audit_inserts`Eigenschaft bis *Wahr* .

Nachverfolgung von CI-Beziehungen

Änderungen an einer CI-Beziehung (CI-Beziehungen, CI/Anwenderbeziehungen oder CI/Gruppenbeziehungen) werden im Verlauf der Elemente auf beiden Seiten der geänderten Beziehung angezeigt, unabhängig davon, ob der Change manuell oder ein Ergebnis von war Discovery.

Wenn der Computer-Alpha beispielsweise eine von CI verwendete Beziehung zur Computer-Beta hat, enthält der Verlauf für Alpha einen Datensatz, wann die Beziehung zur Beta hergestellt wurde, und ebenso enthält der Verlauf für Beta einen Datensatz, wann die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehung zu Alpha hergestellt wurde. Dieses Beispiel veranschaulicht den Verlauf, der angezeigt wird, wenn einige CI-Beziehungen eingerichtet werden und dann eine der Beziehungen entfernt wird:

CI-Beziehungsverlauf

⊟ 2008-12-03 10:49:37 **Updated by** Guest (19 Hours 54 minutes ago) - CI Relationship Change

- created 2 Days 2 Hours 51 minutes earlier

Relationship	Before	After
Runs	(relationship added)	Tomcat@tomdmac
Runs	(relationship added)	MySQL Server@tomdmac

⊞ 2008-12-03 10:49:38 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Disks

⊞ 2008-12-03 10:49:43 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Active Connections

⊞ 2008-12-03 10:50:02 **Updated by** Guest (19 Hours 53 minutes ago)

⊟ 2008-12-04 06:43:39 **Updated by** Glide Maintenance (just now) - CI Relationship Change

- last activity was 19 Hours 53 minutes earlier
- created 2 Days 22 Hours 45 minutes earlier

Relationship	Before	After
Runs	MySQL Server@tomdmac	(relationship removed)

Das erstellte Aufzählungszeichen gibt das Datum an, an dem das CI, der Anwender oder die Gruppe erstellt wurde. Der Aufzählungszeichen der letzten Aktivität bezieht sich darauf, wann die Beziehungen zuletzt geändert wurden. Wenn Sie den CI-Beziehungsverlauf für einen oder alle CI-Beziehungstypen nicht anzeigen möchten, können Sie ihn deaktivieren, indem Sie die Audits für die CI-Beziehungstabellen deaktivieren (CI-Beziehung [`cmdb_rel_ci`], CI/Anwender-Beziehungstyp [`cmdb_rel_user_type`] Oder Gruppenbeziehung [`cmdb_rel_Group`]).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Strenge Sicherheitseinstellungen

Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

Erkunden Sie die Einstellung für hohe Sicherheit



Erfahren Sie mehr über die Funktionen und Geschäftsvorteile von Einstellungen für hohe Sicherheit.

Aktivieren Sie Einstellungen Für Hohe Sicherheit



Aktivieren Sie die Einstellungen für hohe Sicherheit.

Einstellungen Für Hohe Sicherheit Erkunden

Strenge Sicherheitseinstellungen schließen mehrere Sicherheitsoptionen ein, die in Ihrer Instanz verfügbar sind.

Das Modul „hohe Sicherheitseinstellungen“ wird mit dem Plugin „hohe Sicherheitseinstellungen“ aktiviert, das standardmäßig in neuen Instanzen aktiv ist. Wenn Einstellungen für hohe Sicherheit in Ihrer Instanz nicht aktiv sind, finden Sie weitere Informationen unter Aktivierung von Einstellungen für hohe Sicherheit wird angefordert . Weitere Informationen zu diesem Plugin finden Sie unter Plugin für hohe Sicherheit aktivieren [aktualisiert in Security Center 1,3] In Instanzsicherheitshärtungseinstellungen. Eigenschaften für diese Arten von Einstellungen für hohe Sicherheit sind verfügbar:

- Standardeigenschaftswerte: Um die Sicherheit auf Ihrer Plattform zu erhöhen, indem alle kritischen Sicherheitseinstellungen für die Verwaltung und das Auditing an einem Ort zentralisiert werden.
- Standardmäßige Deny-Eigenschaft: Stellt eine Sicherheitsmanager-Eigenschaft bereit, um das standardmäßige Sicherheitsverhalten für den Tabellenzugriff zu steuern.
- Sicherheitsadministratorrolle: Stellt eine Rolle bereit, um die Änderung wichtiger Sicherheitseinstellungen und -Ressourcen zu verhindern. Die Sicherheitsadministratorrolle wird nicht von der Administratorrolle übernommen und muss explizit zugewiesen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erweiterte Berechtigungen: Ermöglicht Anwendern mit der Sicherheitsadministratorrolle, im Kontext eines normalen Anwenders zu arbeiten und bei Bedarf auf eine höhere Sicherheitsrolle zu erhöhen.
- Eigenschaftszugriffssteuerungen: Ermöglicht Sicherheitsadministratoren das Festlegen der Rollen, die zum Lesen und Schreiben von Eigenschaften erforderlich sind.
- Systemprotokolle: Sind schreibgeschützt.
- Zugriffssteuerungsregeln: Steuern Sie, auf welche Daten Anwender zugreifen können und wie sie darauf zugreifen können.

Hinweis:

- Mit den Einstellungen für hohe Sicherheit wird auch automatisch das Plugin für kontextbezogene Sicherheit aktiviert, wenn es nicht bereits aktiv ist. Darüber hinaus bietet Plattformsicherheitseinstellungen – hoch Einstellungen und Funktionen im Kontext der Erhöhung der Sicherheit Ihrer Instanz.
- Der Inhalt der Instanzsicherheits-Härtungseinstellungen enthält detaillierte Beschreibungen und Compliance-Werte für die sicherheitsbezogenen Systemeigenschaften und Plugins in ServiceNow AI Platform.
- Weitere Informationen zu den einzelnen Eigenschaften finden Sie unter Härtungseinstellungen.

Es gibt zwei Möglichkeiten, Eigenschaften für hohe Sicherheitseinstellungen festzulegen oder zu ändern.

- Navigieren zu **Systemsicherheit** > **Strenge Sicherheitseinstellungen**an.

  Optionen auf der Seite „Eigenschaften für hohe Sicherheit“ sind **Ja** Oder **Nein** .

- Navigieren Sie zu **sys_properties.list** Und suchen Sie nach der Eigenschaft, die Sie festlegen oder ändern möchten.

  Optionen in der Tabelle „Systemeigenschaften“ [sys_properties.list] sind **Wahr** Oder **Falsch** .

Eigenschaftszugriffssteuerung

Wenn Einstellungen für hohe Sicherheit aktiv sind, werden in der Tabelle „Eigenschaften“ [sys_properties] zwei zusätzliche Spalten erstellt:

- **Read_roles** : Eine kommagetrennte Liste von Rollennamen, die alle Felder dieser Eigenschaft lesen dürfen.
- **Write_roles** : Eine kommagetrennte Liste von Rollennamen, die alle Felder dieser Eigenschaft schreiben/ändern dürfen.

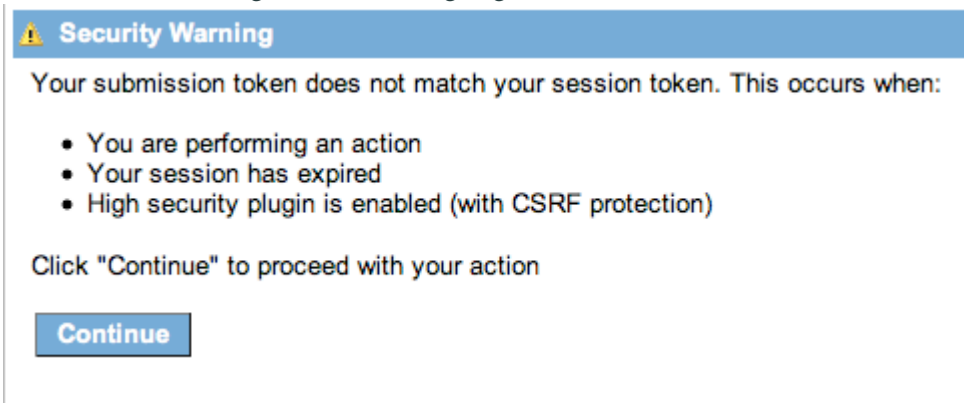
Eigenschaften, die in der Eigenschaftentabelle aufgeführt sind, haben **Read_roles** Von Administrator, und **Write_roles** Von Security_admin. Anwender mit der Administratorrolle können die Eigenschaftswerte anzeigen und lesen, müssen jedoch auf die Rolle „Security_admin“ hochgestuft werden, um sie zu ändern.

Benachrichtigungen

Durch die Aktivierung von Einstellungen für hohe Sicherheit werden auch Sicherheitswarnmeldungen aktiviert. Im Folgenden finden Sie ein Beispiel für eine Nachricht, die nach einer Genehmigung angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitswarnungsbenachrichtigung



Eigenschaften für hohe Sicherheitseinstellungen

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
glide.ui.escape_text	XML-Werte auf Parser-Ebene für die Anwenderoberfläche mit Escape-Zeichen versehen. Verhindert reflektierte und gespeicherte Cross-Site-Skripting-Angriffe. Diese Eigenschaft gilt nicht im Serviceportal. **Hinweis:** Diese Eigenschaft ist auf festgelegt **Wahr** Standardmäßig in Vancouver Und spätere Releases und können nicht von Administratoren geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.	Ja	XML-Markup mit Escape-Zeichen [aktualisiert in Security Center 1,3]
glide.ui.escape_all_script	Erzwingt alle Ausdrücke in Jelly JavaScript]]>Tags, die standardmäßig	Ja in neuen Instanzen	Jelly-Skript mit Escape-Zeichen [aktualisiert in Security Center 1,3 und 1,5]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	mit Escape-Zeichen versehen werden sollen. Erzwingt das Escape-Zeichen nur, wenn das Typattribut in der vorhanden ist]]>Tag ist leer oder wenn der Wert ist Text/javascript , Text/ecmascript , Anwendung/javascript , Anwendung/ ecmascript , Oder Application/x-javascript .		
Glide.ui.Rotation_Sessions	Rotieren Sie HTTP-Sitzungsbezeichner, um Sicherheitsschwachstel zu reduzieren. Siehe: http://www.owasp.org/index.php/Session_Management#Rota .	Ja **Hinweis:** Wenn Sie das SAML 2,0-Plugin für die Single Sign-on-Authentifizierung verwenden, legen Sie diese Eigenschaft auf Nein fest Andernfalls wird die gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigt.	HTTP-Sitzungsbezeichner rotieren
glide.ui.secure_cookies	Sichere Sitzungscookies aktivieren: Zusätzliche Cookie-Sicherheit aktivieren. Wenn **Ja** , Strikte Validierung von Sitzungscookies wird erzwungen.	Ja	Strikte Sicherheit von Sitzungscookies erzwingen [aktualisiert im Sicherheitscenter 1,3]
glide.security.password_reset.uri	Für Mobilgeräte Passwortzurücksetzung, URL, zu der		Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	der Anwender weitergeleitet wird, wenn er auf klickt **Passwort vergessen?** Schaltfläche.		
glide.security.strict.updates	Überprüfen Sie die Sicherheit eingehender Transaktionen während der Formularübermittlung erneut (Rechte werden bei der Formulargenerierung immer überprüft). **Hinweis:** Diese Eigenschaft ist auf festgelegt **Wahr** Standardmäßig in Vancouver Und spätere Releases und können nicht von Administratoren geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.	Ja	Eingehende Transaktionen doppelt prüfen [aktualisiert in Security Center 1,3]
glide.security.strict.actions	Überprüfen Sie die Bedingungen für UI-Aktionen vor der Ausführung. Normalerweise werden Bedingungen nur während des Formularrenderings überprüft.	Ja	Überprüfen Sie die UI-Aktionsbedingungen vor der Ausführung
glide.security.use_csrf_token	Aktivieren Sie die Verwendung eines sicheren Tokens, um eingehende Anforderungen	Ja	Anti-CSRF-Token aktivieren [Neu in Security Center 1,3, aktualisiert 1,5 und entfernt 2,0]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	zu identifizieren und zu validieren. Dieses Token wird verwendet, um Site-übergreifende Angriffe auf Anforderungsfälschung zu verhindern.		
glide.ui.escape_html_list_field	HTML für HTML-Felder in einer Listenansicht mit Escape-Zeichen versehen.	Ja	HTML in Listenansichten mit Escape-Zeichen versehen [aktualisiert in Security Center 1,3 und 1,5]
glide.html.escape_script	JavaScript-Tags in HTML-Feldern mit Escape-Zeichen versehen.	Ja	JavaScript mit Escape-Zeichen versehen [aktualisiert in Security Center 1,3]
Glide.ui.Vergessen	Entfernen Sie **Merken Sie sich** Kontrollkästchen auf der Anmeldeseite.	Ja	Entfernen Sie „mich speichern“
glide.smtp.auth	Authentifizieren Sie sich mit dem SMTP-Server anhand der Anwendernamen- und Passworteigenschaften. **Hinweis:** Diese Eigenschaft ist veraltet.	Ja	
Glide.SOAP.strict_Security	Erzwingen Sie strikte Sicherheit für eingehende SOAP-Anforderungen. Erfordert, dass eingehende SOAP-Anforderungen den Sicherheitsmanager für Tabellen- und Feldzugriff durchlaufen, und überprüft SOAP-Anwender auf die richtigen Rollen für	Ja	Strikte Sicherheit der SOAP-Anforderung erzwingen [aktualisiert in Security Center 1,3]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	die Verwendung des Webservice.		
Glide.basicauth.erforderlich.WSDL	Autorisierung für eingehende WSDL-Anforderungen anfordern. **Hinweis:** Wenn Sie keine Autorisierung für eingehende WSDL-Anforderungen anfordern möchten, müssen Sie die ACL-Regeln (Access Control) ändern, damit Gastanwender auf den WSDL-Inhalt zugreifen können.	Ja	Autorisierung für WSDL-Anforderung anfordern [aktualisiert in Security Center 1,3 und 1,5]
glide.basicauth.required.csv	Erfordert eine Basisautorisierung für eingehende CSV-Anforderungen an.	Ja	Autorisierung für CSV-Anforderungen anfordern [aktualisiert in Security Center 1,3]
Glide.basicauth.erforderlich.Excel	Erfordert eine Basisautorisierung für eingehende Excel-Anforderungen.	Ja	Autorisierung für Excel-Anforderungen anfordern [aktualisiert in Security Center 1,3]
Glide.basicauth.erforderlich.Importprozessor	Erfordert eine Basisautorisierung für eingehende Importanforderungen.	Ja	Autorisierung für Importanforderungen anfordern [aktualisiert in Security Center 1,3]
glide.basicauth.required.pdf	Erfordert eine Standardautorisierung für eingehende PDF-Anforderungen.	Ja	Autorisierung für PDF-Anforderungen anfordern [Aktualisiert in Security Center 1,3]
glide.basicauth.required.rss	Erfordert eine Basisautorisierung für eingehende RSS-Anforderungen.	Ja	Autorisierung für RSS-Anforderungen anfordern [aktualisiert in Security Center 1,3]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
Glide.basicauth.erforderlich.SkriptedProzessor	Erfordert eine Standardautorisierung für eingehende Skriptanforderungen.	Ja	Autorisierung für Skriptanforderungen anfordern [aktualisiert in Security Center 1,3]
Glide.basicauth.erforderlich.SOAP	Standard-Berechtigung für eingehende SOAP-Requests anfordern.	Ja	Autorisierung für SOAP-Anforderungen anfordern [aktualisiert in Security Center 1,3, 1,5 und 2,0]
Glide.basicauth.erforderlich.unl	Erfordert eine Basisautorisierung für eingehende Entladeanforderungen.	Ja	Autorisierung für Entladeanforderungen anfordern [aktualisiert in Security Center 1,3]
glide.basicauth.required.xml	Erfordert eine Basisautorisierung für eingehende XML-Anforderungen.	Ja	Autorisierung für XML-Anforderungen anfordern [aktualisiert im Sicherheitscenter 1,3]
Glide.basicauth.erforderlich.xsd	Erfordert eine Basisautorisierung für eingehende XSD-Anforderungen.	Ja	Autorisierung für XSD-Anforderungen erfordern [aktualisiert im Sicherheitscenter 1,3]
glide.cms.catalog_uri_relative	Relative Links aus dem URI-Parameter in /ess/catalog.do erzwingen. Wenn **Ja** , Nur relative URLs sind über die Seite „/ess/catalog.do“ mit zulässig *uri*Parameter. Wenn **Nein** , Alle URLs sind zulässig, was möglicherweise eine Verknüpfung mit externen nicht autorisierten Inhalten zulassen kann.	Ja	Relative Links erzwingen [aktualisiert in Security Center 1,3 und 1,5]
glide.set_x_frame_options	Aktivieren Sie diese Eigenschaft, um den X-Frame-Options-Antwortheader für alle UI-Seiten auf SAMEORIGIN	Ja	X-Frame-options implementieren: SAMEORIGIN-Sicherheitsheader [aktualisiert in Security Center 1,3]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	festzulegen. Der X-Frame-Options HTTP Response Header kann verwendet werden, um anzugeben, ob der Browser eine Seite in einem <frame> oder <iframe> rendern kann. Websites können diese Eigenschaft verwenden, um Clickjacking-Angriffe zu vermeiden, indem sichergestellt wird, dass ihre Inhalte nicht in andere Websites eingebettet werden. https://developer.mozilla.org/en/the_x-frame-options_response_header		
Glide.ui.attachment.Download_MIME_types	Eine Liste von kommagetrennten MIME-Anhangstypen, die im Browser nicht inline gerendert werden. Verhindert standortübergreifende Skripting-Angriffe. Beispiel: Text/HTML Erzwingt, dass HTML-Dateien als Anhänge auf den Client heruntergeladen und nicht inline im Browser angezeigt werden.	Text/html,image/svg,image/svg+xml	Herunterladbare MIME-Typen beschränken [aktualisiert in Security Center 1,3 und 2,0]
glide.security.groupby_acl_check	Wenn diese Eigenschaft aktiviert ist, werden ACL-Prüfungen für GroupBy-Vorgänge für die Gruppennamen basierend auf den tatsächlichen Daten	Ja	Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	aus den Gruppen durchgeführt.		
glide.security.diag_txns_acl	Wenn **Ja** , Nur der Administratoranwender oder Anwender von der zulässigen IP-Adresse kann darauf zugreifen Statistiken.do , Threads.do , Und Replikation.do .	Nein	Zugriff auf Leistungsüberwachung einschränken [aktualisiert in Security Center 1,3]
glide.ui.security.codetag.allow_script	Zulassen, dass eingebettetes HTML (mit [Code]-Tags) JavaScript-Tags enthält. **Hinweis:** Diese Eigenschaft ist auf festgelegt **Wahr** Standardmäßig in Vancouver Und spätere Releases und können nicht von Administratoren geändert werden. Wenden Sie sich für einen Anwendungsfall, bei dem die Eigenschaft geändert werden muss, an den Kundensupport.	Nein	Eingebetteten HTML-Code deaktivieren [aktualisiert in Security Center 1,3]
Glide.Skript.Allow.ajaxevaluieren	Aktivieren Sie den AJAXEvaluate-Prozessor. Die *AJAXAuswerten* API-Aufruf ermöglicht dem Client das Senden und Ausführen beliebiger Skripts auf dem Server.	Nein	AJAXEvaluate deaktivieren

Die folgenden Eigenschaften sind in der Tabelle „sys_properties“ definiert, sind jedoch auf der Seite „Einstellungen für hohe Sicherheit“ nicht sichtbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
com.glide.communications.httpclient.verify_hostname	Überprüfen Sie den Hostnamen und die Zertifikatkette, die von Remote-SSL-Hosts angezeigt werden. Schützen Sie sich vor MITM-Angriffen (man-in-the-Middle). Weitere Informationen finden Sie unter Richten Sie die Kubernetes-Spoke ein **Hinweis:** Diese Eigenschaft überschreibt die Eigenschaft com.glide.communications.trustmanager_trust_all.	wahr	Keine
Glide.basicauth.required.Schema	Erfordert Standardauthentifizierung für eingehende Tabellenschemaanforderungen.	wahr	Keine
glide.security.csrf_previous.allow	Verwendung eines abgelaufenen sicheren Tokens zulassen, um eingehende Anforderungen zu identifizieren und zu validieren. Dieses Token wird verwendet, um Site-übergreifende Angriffe auf Anforderungsfälschung zu verhindern.	falsch	Keine
glide.security.csrf_previous.time_limit	Zeit in Sekunden, bis ein sicheres Token abläuft. Ermöglicht die Kontrolle über die Gültigkeitsdauer des vorherigen CSRF-Tokens. Wenn die	86400 **Hinweis:** Wert in Sekunden. Entspricht 1 Tag.	Keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Standardwert	Härtungseinstellungen für die Instanzsicherheit
	Anwendersitzung abläuft, läuft das sichere Token mit ab, es sei denn `glide.security.csrf_previous.allow`Eigenschaft ist aktiviert und liegt innerhalb des von dieser Eigenschaft beschriebenen Zeitrahmens. Dieses Token wird verwendet, um Site-übergreifende Angriffe auf Anforderungsfälschung zu verhindern.		
glide.security.csrf.strict.validation.mode	Erzwingt die strikte Überprüfung von CSRF-Token, wobei das erneute Übermitteln der Anforderung durch Benutzer nicht erlaubt ist, wenn das CSRF-Token nicht übereinstimmt.	falsch	Verhindern, dass Anwender eine Warnung zur Umgehung der CSRF-Validierung akzeptieren [aktualisiert in Security Center 1,3 und 1,5]
com.glide.security.check_unsanitized_html	Erzwingt das Bereinigungsverhalten von translated_html-Feldern auf globaler Ebene für Feldzuweisungen.	Erzwingen	Keine

Einstellungen Für Hohe Sicherheit Werden Aktiviert

Das Plugin „hohe Sicherheitseinstellungen“ ist standardmäßig auf allen neuen Instanzen aktiv. Wenn es in Ihrer Instanz nicht aktiv ist, können Sie das Plugin anfordern.

Vorbereitungen
Erforderliche Rolle: keine

Vor Einstellungen für hohe Sicherheit werden aktiviert In einer vorhandenen Instanz:

1. Überprüfen Sie die folgenden Informationen, um das neue Verhalten zu verstehen:
   - Regeln Für Zugriffssteuerungsliste
   - Strenge Sicherheitseinstellungen
   - Standardmäßige Deny-Eigenschaft

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

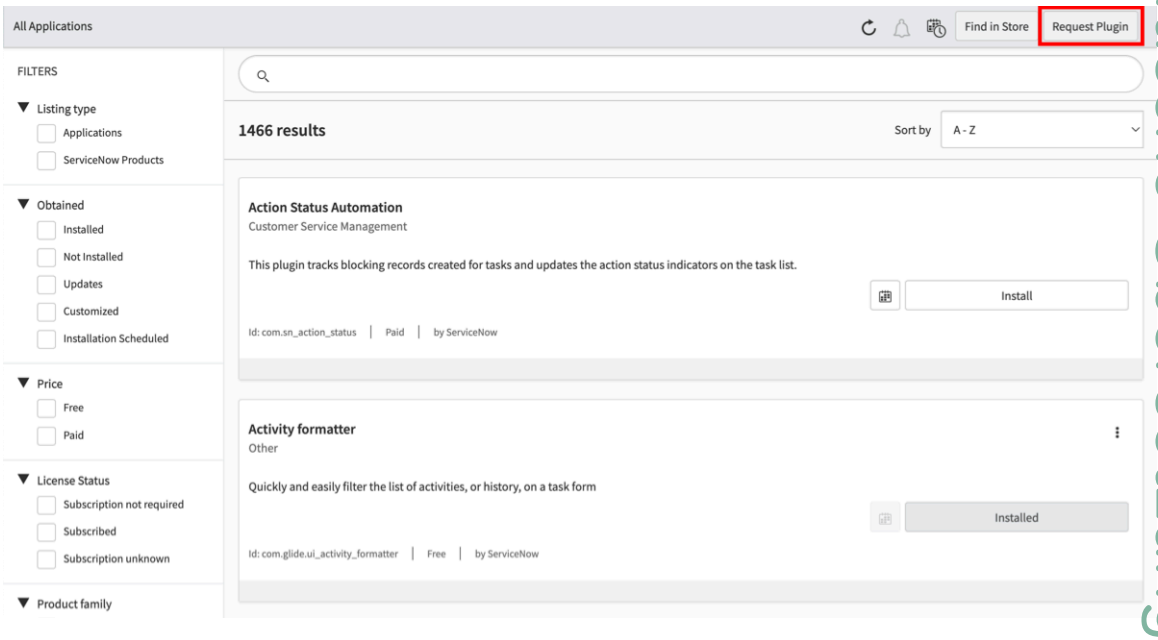
2. Aktivieren Sie das Plugin auf einer Instanz außerhalb der Produktion. Ein aktueller Klon der Produktion ist vorzuziehen.
3. Testen Sie die überarbeitete Funktionalität, insbesondere die hinzugefügten ACLs und die standardmäßige Deny-Funktionalität. Fahren Sie mit dem Testen fort, bis das System wie erwartet funktioniert. Wenn Anwender nicht auf erwartete Ressourcen zugreifen können, stellen Sie sicher, dass sie über die entsprechenden Rollen und ACL-Regeln verfügen, um ihnen Zugriff zu gewähren.
4. Erstellen Sie Update-Sätze aller erforderlichen Changes, damit Sie sie auf die Produktion anwenden können.

Hinweis: Weitere Informationen zu diesem Plugin finden Sie unter Plugin für hohe Sicherheit aktivieren [aktualisiert in Security Center 1,3] In Instanzsicherheitshärtungseinstellungen.

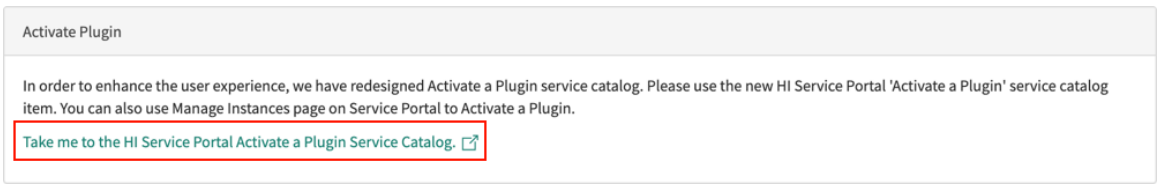
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

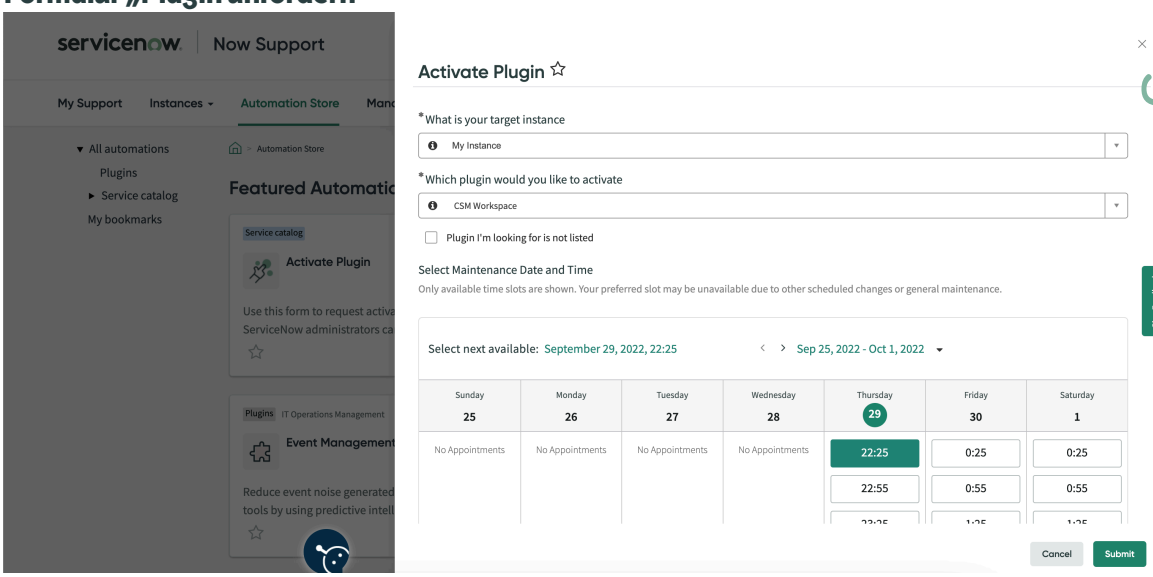
Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtuelles privates Netzwerk (VPN)

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.

Untersuchen



Erfahren Sie mehr über die Funktionen und Geschäftsvorteile eines virtuellen privaten Netzwerks.

Aktivieren



Aktives virtuelles privates Netzwerk.

Konfigurieren



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie, wie Sie ein virtuelles privates Netzwerk konfigurieren.

Virtual Private Network (VPN) erkunden

Verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Instanz mit externen Datenquellen über das Internet zu integrieren.

Meine IP-Informationen

Beim Konfigurieren einer Integration, die ein verschlüsseltes Protokoll verwendet, z. B. Lightweight Directory Access Protocol (LDAP) oder HTTPS, empfiehlt es sich, das Internet als Transportmechanismus zu verwenden.

Es kann jedoch Sicherheits- oder Netzwerkarchitekturanforderungen geben, die die Verwendung einer Site-to-Site Internet Protocol Security (IPSEC) Virtual Private Network (VPN)-Verbindung (Virtual Private Network) zwischen den Rechenzentren und Ihren Geschäftsnetzwerken vorschreiben. Das VPN unterstützt die erforderliche verschlüsselte Kommunikation zwischen der Instanz und Ihrem Netzwerk.

⚠ Warnung:

Wenn ein VPN-Tunnel initiiert wird, funktioniert er als Site-to-Site-Verbindung. Dies bedeutet, dass der Endpunkt in Ihrer Infrastruktur eine IP-Adresse erhält, die als Verschlüsselungsdomäne bezeichnet wird. Auf diese öffentliche IP kann von jeder Instanz im selben Rechenzentrum zugegriffen werden.

Wenn Sie beispielsweise einen internen Webservice haben und einen VPN-Tunnel einrichten, kann Ihre Instanz den internen Endpunkt sowie alle Ihre anderen Instanzen im selben Rechenzentrum erreichen.

VPN-Verbindungen

Die ServiceNow Die VPN-Infrastruktur verwendet Paare von Cisco Adaptive Security Appliance (ASA)-Geräten, die als VPN-Terminationspunkte dienen.

Das VPN zwischen der Instanz und Ihrem Netzwerk verwendet Ihre vorhandene Netzwerkhardware zur Unterstützung der Kommunikation. Es ist nicht erforderlich, eine Hardware zu installieren. Da jeder Kunde über eine eindeutige Konfiguration verfügt, verfügt die Instanz über eine flexible VPN-Lösung. Die Instanz hat Tunnel für Checkpoint-, Juniper-, Nortel- und andere IPSEC-VPN-fähige Geräte erstellt.

Die VPN-Verbindungen zwischen der Instanz und Ihrem Netzwerk werden erstellt, um den verschlüsselten Datenverkehr in Ihr Netzwerk zu unterstützen. Häufig verfügen Integrationen, die VPN verwenden, nicht über Verschlüsselung als Teil des zugrunde liegenden Protokolls. Beispiel: LDAP Über VPN versus LDAPS über das Internet und HTTP über VPN versus HTTPS über das Internet.

Das Netzwerk lässt keine eingehende Integration von ServiceNow oder Datenverkehr von Endanwendern zu ServiceNow zu, eine VPN-Verbindung zu passieren. Diese eingeschränkte Kommunikation umfasst den Zugriff von Endanwendern auf die Plattform, die Verwaltung der Plattform, Webservices-Integrationen und andere Integrationen, die für die Verwendung von konfiguriert sind MID-Server . Die gesamte eingehende Kommunikation mit der Instanz muss über das Internet mithilfe von HTTPS erfolgen. Diese Konfiguration stellt einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verschlüsselten Kommunikationskanal bereit. Der Verschlüsselungskanal erfüllt zusammen mit der IP-Zugriffssteuerung die Sicherheitsanforderungen für diesen Datenverkehr-Flow.

Adressen für VPN-Kommunikation

Um Konflikte oder Überschneidungen mit internen zu verhindern ServiceNow In Netzwerken oder mit anderen internen IP-Adressschemata in Ihrem Netzwerk muss für den gesamten getunnelten Datenverkehr in der Verschlüsselungsdomäne auf beiden Seiten des Tunnels nicht-RFC-1918-Adressen verwendet werden.

ServiceNow Stellt eine einzelne IP-Adresse für die Quelle von Abfragen in Ihrem Netzwerk bereit. Sie müssen NAT (Network Address Translation), nicht-RFC-1918-Adressen für jeden Host angeben, der in Ihre Instanz integriert wird. Diese öffentlichen Adressen müssen im Besitz Ihrer Organisation sein. Drittparteiadressen können nicht in Tunneln verwendet werden. Außerdem darf die Verschlüsselungsdomäne nicht die IP-Adresse des VPN-Peers enthalten.

Redundante Tunnel

Es gibt zwei Möglichkeiten, Redundanz für Ihre Tunnel zu erstellen:

- Verwenden Sie dieselbe Verschlüsselungsdomäne hinter Ihren Kollegen. Dies ist die bevorzugte Methode.
- Verwenden einer anderen Verschlüsselungsdomäne hinter jedem Peer.

Bei der ersten Methode müssen Sie hinter jedem Ihrer Kollegen dieselbe NAT-Adresse angeben, um einen Verbindungspfad mit dieser Adresse zu Ihrem Server zu erstellen. Der Pfad zu Ihrem Server kann derselbe physische Computer oder ein Spiegel sein, der identische Services bereitstellt. Mit dieser Methode verwendet Ihre Instanz dieselbe IP-Adresse, um eine Verbindung zu Ihren Servern herzustellen, unabhängig davon, ob Ihr primärer oder sekundärer Tunnel aktiv ist. Wenn Sie mehr als einen Server haben, befolgen Sie dasselbe Schema für Ihre zusätzlichen Server. Diese Methode bietet Ihren Anwendern die meiste Transparenz und wird empfohlen.

Die zweite Methode erfordert eine Konfiguration in Ihrer Instanz, um die Redundanz bereitzustellen. Wenn der Tunnel beispielsweise für LDAP verwendet wird, können Sie redundante LDAP-Server in Ihrer Instanz bereitstellen. Beachten Sie, dass für diese Methode eine Zeitüberschreitung bei der Verbindung zum ersten konfigurierten LDAP-Server erforderlich ist, bevor die Instanz versucht, eine Verbindung zum sekundären Server herzustellen. Aufgrund dieser zusätzlichen Zeitverzögerung sollte diese Lösung nur implementiert werden, wenn die erste Option nicht erreichbar ist. Beachten Sie auch, dass nicht alle Services für redundant in Ihrer Instanz konfiguriert werden können. Wenn Sie einen VPN-Tunnel für etwas anderes als LDAP verwenden und Redundanz erforderlich ist, überprüfen Sie, ob Ihre Konfiguration mehrere Adressen unterstützen kann, oder sehen Sie sich die erste Option oben an.

Alternativen zur Verwendung eines VPN

Diese Alternativen bieten eine einfachere Möglichkeit, Ihre Instanz mit den Ressourcen in zu verbinden ServiceNow Rechenzentren und bieten eine bessere Verschlüsselung. Darüber hinaus können Sie alle Probleme vermeiden, die VPN-Ausfallzeiten verursachen könnten, z. B. die Nichtverfügbarkeit Ihrer Instanz für Anwender, wenn ein Problem mit dem VPN-Tunnel auftritt.

Single Sign-on und MID-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erwägen Sie, eine Kombination aus Single Sign-on (SSO) für die Authentifizierung und dem MID-Server für die Synchronisierung von Anwenderdaten zu verwenden, anstatt ein VPN zu verwenden, um Ihren LDAP-Server mit Ihrer Instanz zu verbinden. Erwägen Sie für andere Integrationen als LDAP die Verwendung einer zertifikatbasierten Verschlüsselung.

Sie können den LDAP-Listener auf einem MID-Server verwenden, um Ihre Anwendertabelle nahezu in Echtzeit zu synchronisieren.

Der Vorteil dieses Ansatzes besteht darin, dass keine Firewall-Löcher, Routen, VPN-Tunnel oder andere spezielle Netzwerkeinstellungen konfiguriert und verwaltet werden müssen. Die SSO/MID-Server-Lösung ist die flexibelste, sicherste und kosteneffektivste Methode, um die vollständige LDAP-Integration zu erreichen.

LDAP über SSL

Eine weitere Alternative zur Verwendung eines VPN-Tunnels besteht darin, LDAP over SSL (LDAPS) direkt über das Internet zu konfigurieren. Sie können einen schreibgeschützten Domänencontroller konfigurieren und die Instanz in Ihrer DMZ sperren, indem Sie nur die Quelladressen der Instanz und die Zielports Ihrer Wahl verwenden. Da die Ports für LDAP in Ihrer Instanz konfigurierbar sind, können Sie bei Bedarf eine Portadressübersetzung (PAT) durchführen. Mit LDAPS steuern Sie das Zertifikat, das über einen verschlüsselten Kanal in die Instanz hochgeladen wird (siehe Ein Zertifikat wird in eine Instanz hochgeladen). Die Pakete können ohne das Zertifikat nicht verschlüsselt oder entschlüsselt werden.

Der Vorteil dieses Ansatzes besteht darin, dass er einen stärkeren Verschlüsselungs- und Entschlüsselungsmechanismus bietet. Ein VPN kann den Datenverkehr zwischen den beiden Peers im Internet nur mit einem koordinierten vorab freigegebenen Schlüssel verschlüsseln und entschlüsseln, ähnlich einem Passwort. LDAPS bietet einen längeren verschlüsselten Pfad, End-to-End, auf Anwendungsebene und ein Zertifikat, das viel komplizierter ist als ein vorab freigegebener Schlüssel, den der IPSec-Tunnel verwendet.

VPN-Setup

Ab dem Zeitpunkt, zu dem eine VPN-Anforderung übermittelt wird, dauert es normalerweise eine Woche oder weniger, bis der VPN-Build abgeschlossen ist. Zur Unterstützung der Redundanzanforderungen Ihrer Instanz und Ihrer Organisation werden mindestens zwei und maximal vier VPNs bereitgestellt (vom aktiven Standort zu Ihrem aktiven Standort oder vom aktiven Standort zu Ihrem DR-Standort usw.).

Es empfiehlt sich, die Verschlüsselungsdomäne so spezifisch wie möglich zu gestalten. Idealerweise umfasst die Verschlüsselungsdomäne nur die spezifischen Hosts, die für die Integrationen erforderlich sind. Eine große Verschlüsselungsdomäne kann Möglichkeiten für die Weiterleitung von Diskrepanzen (VPN versus Internet) schaffen.

Um das VPN zu erstellen, führt die Instanz Folgendes aus:

1. Stellt die VPN-Peer- und Host-Adressen aus jedem Rechenzentrum bereit.
2. Erstellt die erforderliche VPN-Konnektivität von zwei Rechenzentren in Ihr Netzwerk. Zur Unterstützung von Redundanzanforderungen und Notfallwiederherstellungsanforderungen (DR) können die VPNs von zwei Rechenzentren in zwei Netzwerken bereitgestellt werden.

Die Instanz unterstützt nicht das Erstellen mehrerer VPN-Tunnel in einem Kundennetzwerk, um eine Verbindung zu mehreren geografischen Regionen oder Tochterunternehmen herzustellen. Sie sollten eine standortübergreifende Weiterleitung, Datenverkehrsverteilung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

oder Datenverkehrsgestaltung in Ihrem eigenen internen Netzwerk durchführen, anstatt über mehrere VPN-Tunnel zu verfügen.

VPN-Service wird aktiviert

Verwenden Sie für alle VPN-Anforderungen, einschließlich Bereitstellung, Änderungen oder allgemeine Fragen, das Formular „Servicekatalog-VPN-Anforderung“.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie zu https://support.servicenow.com/now?draw=case.
2. Wählen Sie aus **Automatisierungsspeicher** Registerkarte.
3. Verwenden Sie die Struktur auf der linken Seite, um zu navigieren **Alle Automatisierungen** > **Servicekatalog** > **Cloud-Infrastruktur**an.
4. Wählen Sie Aus **VPN-Anforderungen**
5. Wählen Sie den entsprechenden VPN-Anforderungstyp aus.
6. Beantworten Sie die Fragen.
   Fragen variieren je nach ausgewähltem Anforderungstyp.
7. Klicken Sie auf **Absenden**.

Ergebnis

Sobald Ihre Anforderung übermittelt wurde, ServiceNow Arbeitet mit Ihren Netzwerktechnikern zusammen, um zu testen und zu validieren, dass das VPN Datenverkehr erfolgreich übergibt. Um sicherzustellen, dass Ihre Fragen rechtzeitig beantwortet werden, beantworten Sie während dieses Prozesses VPN-bezogene Fragen.

Konfigurieren einer Adresse für die VPN-Kommunikation

Um Konflikte oder Überschneidungen mit internen zu verhindern ServiceNow In Netzwerken oder mit internen IP-Adressschemata eines anderen Kunden erfordert die Instanz, dass für den gesamten getunnelten Datenverkehr in der Verschlüsselungsdomäne Adressen verwendet werden, die nicht-RFC-1918-Adressen auf beiden Seiten des Tunnels sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Instanz stellt eine einzelne IP-Adresse für die Quelle von Abfragen in Ihrem Netzwerk bereit.

Prozedur

Geben Sie NAT (Network Address Translation), nicht-RFC-1918-Adressen für jeden Host an, der in die Instanz integriert wird.

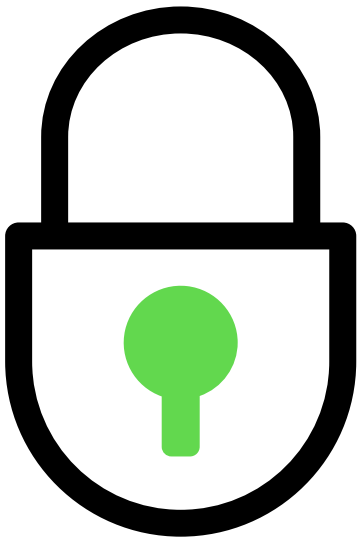
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plattform-Datenschutz

Mit Privacy können Sie vertrauliche Daten in der Instanz maskieren.

Anwendungen speichern

Datenschutz



Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren.

Daten-Discovery

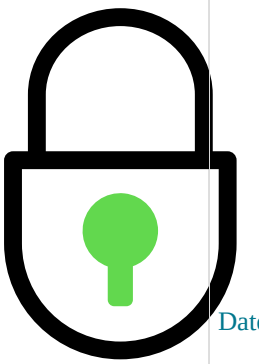


Identifizieren Sie mithilfe der Datenerkennung vertrauliche Daten innerhalb einer Instanz, um sie zu klassifizieren, zu schützen oder Berichte über sie zu erstellen.

Plugins

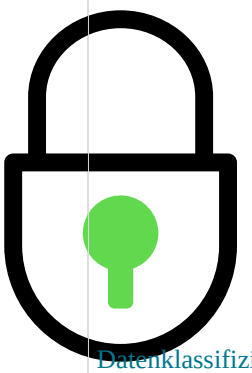
Datenschutz

(klassisch)



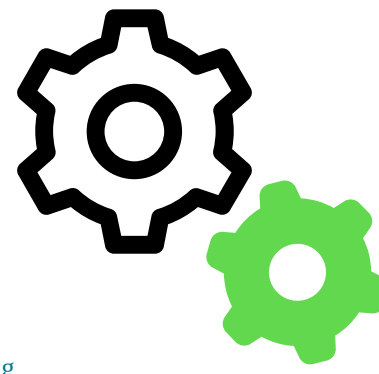
Datenanonymisierung

Die Datenanonymisierung bietet eine Möglichkeit, Daten einfach zu



Datenklassifizierung

Gruppieren Sie Daten mithilfe vordefinierter



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie das Legacy-Plugin „Datenschutz (Classic)“.	transformieren, sodass sie nicht identifizierbar sind und den Datenschutzbestimmungen besser entsprechen.	oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

Datenschutz Erkunden

Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren. Nachdem sie anonymisiert wurden, gelten sie nicht mehr als persönliche Daten, die Vorschriften unterliegen.

Erklärt die Wichtigkeit des Datenschutzes und die Schritte, die Unternehmen ergreifen können, um vertrauliche Informationen durch Klassifizierung und Anonymisierung zu schützen. Mit der Anwendung „Datenschutz-Store“ geben wir einen Überblick über das Haupt-Dashboard und die Fähigkeiten.

Entwickler müssen mit Daten in Instanzen außerhalb der Produktion arbeiten, um sicherzustellen, dass ihre Implementierungen wie erwartet funktionieren. Der Import von Daten aus Ihrer Produktionsinstanz ist zwar eine nützliche Möglichkeit, die Produktion zu simulieren, stellt jedoch ein Sicherheitsrisiko dar. Administratoren können den Datenschutz verwenden, um Entwicklern Daten bereitzustellen, die keine privaten Informationen enthalten, damit sie in einer Umgebung außerhalb der Produktion sicher arbeiten können.

Datenklassifizierung

Identifizieren und klassifizieren Sie Ihre sensiblen Daten gemäß vordefinierten Kriterien, die durch den Grad der Vertraulichkeit der Datentypen in Ihrer Instanz bestimmt werden. Die Vertraulichkeitsstufen der Daten helfen bei der Bestimmung, wie jeder Typ klassifizierter Daten behandelt werden soll. Es gibt mehrere vordefinierte Klassen mit Datenschutz auf Basisebene. Verwenden Sie den Abschnitt „Klassifizierung“ von „Datenschutz“, um Daten in Ihrer Instanz zu bezeichnen und zu gruppieren. Fügen Sie Klassen hinzu, zeigen Sie die Datenklassenstruktur an, und klassifizieren Sie Daten. Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ.

Erklärt, wie Daten mit der Datenschutzspeicher-Anwendung klassifiziert werden.

Anonymisierung von Anwenderdaten

Als Administrator definieren Sie, ob alle Informationen für alle Anwender oder für eine Teilmenge von Anwendern anonymisiert werden sollen. Bei der Anonymisierung werden die Daten für die ausgewählten Anwenderdatensätze durch zufällige Werte oder Werte ersetzt, die Sie definieren. Beim Ersetzen von Werten kann die Datenstruktur mit verschiedenen Techniken beibehalten werden.

Erklärt, wie Daten mit der Datenschutzspeicher-Anwendung anonymisiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz

Verwenden Datenschutz Dient zum Klassifizieren vertraulicher Daten, zum Entfernen von personenbezogenen Daten aus Anwenderdaten in einer Produktionsinstanz und zum Anonymisieren von Daten in nicht-Produktionsinstanzen.

Hinweis: Sie können auch das Legacy-Plugin verwenden Datenschutz (klassisch).

Installationsdetails

Auf Ihrer Instanz müssen die folgenden Anwendungen installiert sein:

- Datenschutz (Classic) [com.Glide.Data_privacy]
- Datenschutz [sn_dp_Store_App]
- Daten-Discovery [sn_Data_Discovery]
- Daten-Discovery-APIs [com.Glide.Data_Discovery]

So funktioniert die Installation:

- Durch die Installation der Datenschutz-Store-App werden die Daten-Discovery-Store-App, das Datenschutz-Plugin (Classic) und das Datenklassifizierungs-Plugin automatisch installiert.
- Durch die Installation der Store-App „Daten-Discovery“ wird das Plugin „Daten-Discovery-APIs“ automatisch installiert

Überlegungen

- Nur klassifizierte Daten können anonymisiert werden. Informationen zu Datenklassen und Klassifizierung finden Sie unter Datenklassifizierung (Klassisch) oder Datenklassifizierung Store-App.
- Personenbezogene Daten in Protokollen und andere Auditdaten werden nicht anonymisiert.
- Nur strukturierte Daten können anonymisiert werden. Unstrukturierte Daten, z. B. Journalfelder, Kommentare, Anhänge und andere Felder, in denen Teiltext personenbezogene Daten darstellen kann, sind nicht anonymisiert. Weitere Informationen finden Sie unter Unterstützte Feldtypen für die Anonymisierung.
- Integrationen mit SSO-Systemen (Single Sign-on) können Anwenderinformationen aus ihren Quell-of-Truth-Systemen erneut synchronisieren. Es ist kein Mechanismus vorhanden, um die Dauerhaftigkeit der Deidentifizierung von sys_user-Daten sicherzustellen. Informationen zur Anwenderverwaltung und zu sys_users finden Sie unter Anwenderverwaltung .

Datenschutz

Mit Data Privacy können Sie vertrauliche Daten klassifizieren und anschließend personenbezogene Daten (PII) aus Benutzerdaten in einer Produktionsinstanz entfernen und Daten in Nicht-Produktionsinstanzen anonymisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz Erkunden



Erfahren Sie mehr über Datenschutz.

Konfigurieren Sie Den Datenschutz



Erfahren Sie, wie Sie Datenschutz konfigurieren.

Rollen im Datenschutz



Rufen Sie Details zu Rollen im Datenschutz ab.

Erweiterte Datenschutzfunktionen



Erfahren Sie mehr über die erweiterten Funktionen des Datenschutzes.

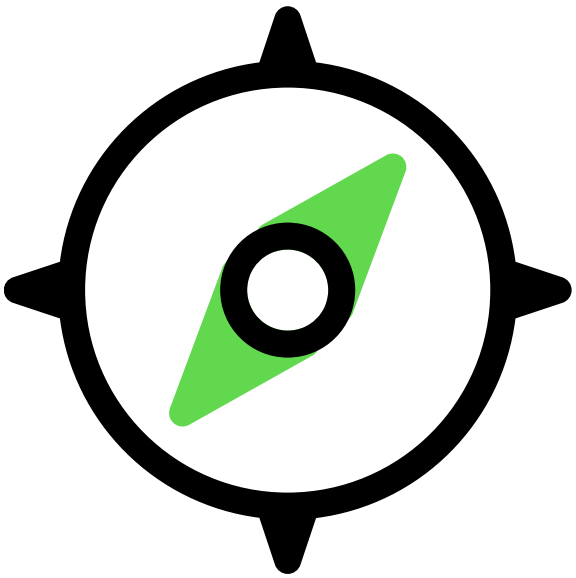
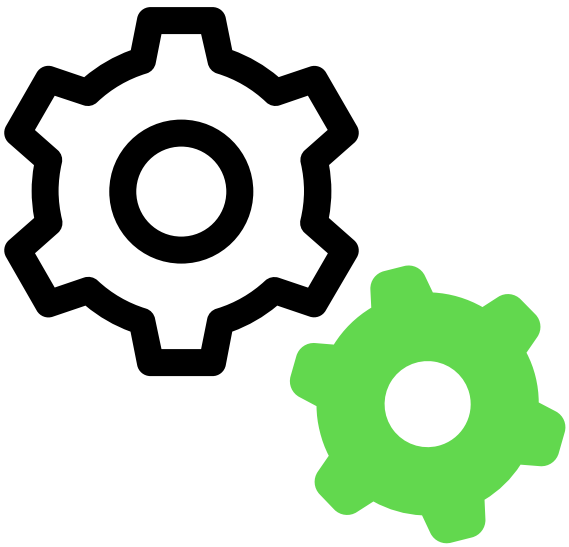
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz für Now Assist

Richten Sie ein, und konfigurieren Sie, wie vertrauliche Daten aus generativen KI-Hinweismeldungen erkannt und anonymisiert werden.

Erste Schritte

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über Datenschutz für Now Assist	Konfigurieren Sie den Datenschutz für Now Assist

Hinweis: Datenschutz für Now Assist erkennt und maskiert vertrauliche Daten basierend auf regulatorischen Mustern und unterstützt keine kontextbezogenen Datenmuster (Modelltyp).

Datenschutz für Now Assist erkunden

Weitere Informationen Datenschutz Für Now Assist Verbessert Ihre Fähigkeit, vertrauliche Daten zu schützen.

Datenschutz Für Now AssistÜbersicht

Sensible Daten wie Alter, Telefonnummer und andere personenbezogene Daten können maskiert werden, damit sie nicht aus generativen KI-Hinweismeldungen verarbeitet werden. Platzhaltertext und anonymisierte Daten werden stattdessen mit dem Prompt gesendet, und diese Werte werden durch den Originaltext ersetzt, nachdem die Antwort des Large Language Learning Module (LLM) empfangen wurde. Diese bidirektionale Maskierung stellt sicher, dass Endanwender genaue Antworten erhalten, vertrauliche Daten jedoch nicht dem LLM zugänglich gemacht werden.

Bei der Konfiguration gibt es einige Überlegungen Datenschutz Für Now Assist. Informationen zu Konfigurationsdetails finden Sie unter Datenschutz für Now Assist konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Datenschutz Für Now Assist Erkennt und maskiert vertrauliche Daten basierend auf Mustern des regulären Ausdrucks und unterstützt keine kontextbezogenen Datenmuster (Modelltyp)

Datenschutz für Now Assist konfigurieren

Konfigurieren Sie eine erweiterte Datenschutzkonfiguration, um personenbezogene Daten (PII) in Anwendungen der generativen KI zu deidentifizieren.

Vorbereitungen

Auf Ihrer Instanz müssen die folgenden Anwendungen installiert sein:

- Datenschutz (Klassisch) [com.Glide.Data_privacy]
- Datenschutz [sn_dp_Store_App]
- Daten-Discovery [sn_Data_Discovery]
- Daten-Discovery APIs[com.Glide.Data_Discovery]

Durch die Installation der neuesten Version des Generative KI-Controllers wird die Datenschutz-Store-App (sn_dp_Store_App) automatisch installiert. Die Datenschutz-Store-App installiert automatisch die Daten-Discovery-Store-App [sn_Data_Discovery], das Plugin „Datenschutz (Classic)(com.Glide.Data_privacy)“ und das Daten-Discovery APIs [com.Glide.Data_Discovery].

Erforderliche Rolle: Now_Assist_Data_privacy_admin

Wichtig: Sie benötigen keine vollständige aktive Lizenz zum Konfigurieren Datenschutz Für Now Assist.

Prozedur

1. Navigieren zu **Alle** > **Datenschutz (klassisch)** > **Erweiterte Konfiguration der Datenschutzrichtlinie**an.
   Wenn Sie zuvor den Handler für sensible Daten verwendet haben, um Daten für generative KI zu deidentifizieren, wird möglicherweise bereits eine Datenschutzrichtlinie konfiguriert. Ihre zuvor konfigurierten regulären Ausdrücke wurden im Rahmen Ihres Upgrades migriert. Wenn Sie bereits eine Datenrichtlinie für haben Now Assist, Fahren Sie mit Schritt 6 fort.
2. Wählen Sie **Neu**.
3. Geben Sie einen Namen für die Datenschutzrichtlinie ein.
4. In **Datenkanal** Feld den zu verwendenden Datenkanal auswählen.

Kanal	Beschreibung
Datenkit	Daten, die KI-Modelle zur Auswertung verwenden, werden durch Erkennung und de-Identifizierung sensibler Daten bereinigt
Datenextraktion	Daten werden vor dem Senden an das Modelltraining bereinigt
Now Assist	Daten werden vor dem Senden an den GenAI-Controller bereinigt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Festlegen **Aktiv** Bis `Wahr` , Und wählen Sie dann aus **Übermitteln** Zum Erstellen der erweiterten Richtlinienkonfiguration.
   Für jeden Datenkanal kann jeweils nur eine Richtlinienkonfiguration aktiv sein. Um eine neue erweiterte Richtlinienkonfiguration zu aktivieren, müssen Sie festlegen **Aktiv** Bis `Falsch` Für alle anderen Richtlinienkonfigurationen in diesem Datenkanal.
6. Nachdem Sie zur Liste der erweiterten Richtlinienkonfigurationen weitergeleitet wurden, öffnen Sie den von Ihnen erstellten Datensatz.
   Öffnen Sie den vorhandenen Datensatz mit dem Now Assist-Datenkanal, wenn bereits einer vorhanden ist.
7. Wählen Sie aus, um ein Datenmuster hinzuzufügen, um die Identifizierung aufzuheben **Wählen Sie Datenmuster Aus**.
8. **Wahlweise:** Informationen zum Erstellen eines eigenen Datenmusters finden Sie unter Konfigurieren Daten-Discovery Muster.
9. Wählen Sie Ihre Datenmuster aus, und wählen Sie dann aus **Speichern** .

Ergebnis

Daten, die von den in den Datenmustern ausgewählten regulären Ausdrücken erfasst werden, werden für generative KI-Anwendungen deidentifiziert. In diesem Beispiel ist die Richtlinie so konfiguriert, dass sie eine Reihe aktiver Datenmuster erfasst und dann den Datenkanal für die Datenextraktion verwendet.

Datenschutz

Die Datenschutz-Store-App ist eine Next Experience-Aktualisierung für Datenklassifizierung und Datenschutz mit modernem Look, Haptik und Benutzerfreundlichkeit. Die Datenschutz-Store-App wird ab Utah unterstützt.

Der Datenschutz besteht aus mehreren Komponenten: Übersicht, Klassifizierung und Anonymisierung.

Übersicht

Verwenden Sie den Abschnitt Übersicht als Ausgangspunkt für die Verwaltung Ihrer Daten- und Datenschutz-Compliance. Details siehe Datenschutzübersicht.

Klassifizierung

Datenklassifizierung ist der Prozess der Organisation von Daten in Kategorien, die das Abrufen, Sortieren und Speichern für die zukünftige Verwendung erleichtern. Die Verwendung eines Klassifizierungssystems hilft, sich auf die Anforderungen an Vertraulichkeits- und Sicherheitsrichtlinien zu konzentrieren. Klassifizieren Sie Daten, die für die Anonymisierung verwendet werden sollen. Informationen zu Datenklassen und Klassifizierung finden Sie unter Datenklassifizierung.

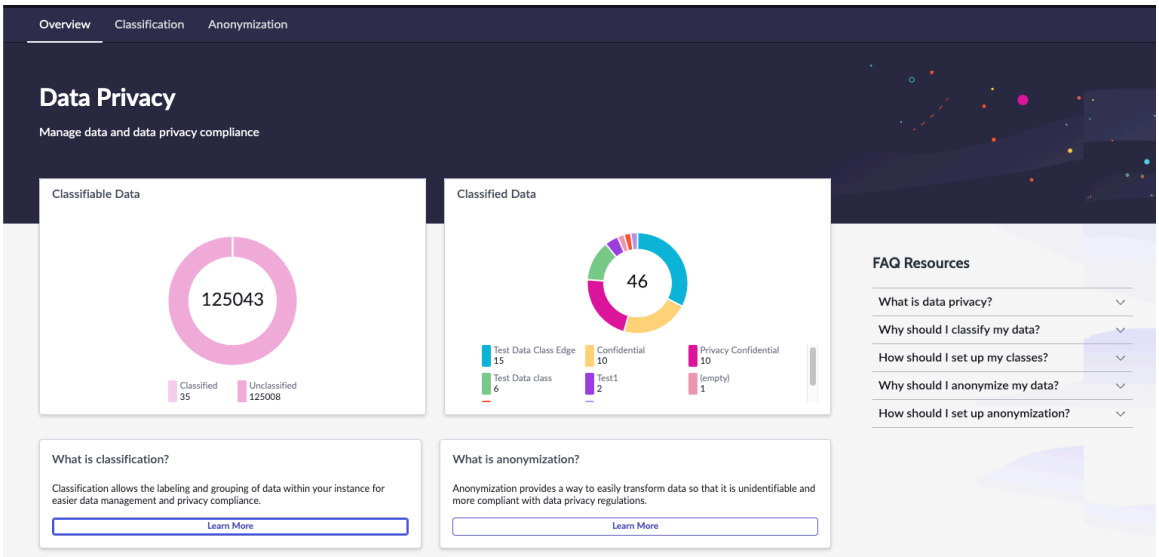
Datenschutzübersicht

Die Übersicht-Homepage ist ein Ausgangspunkt für die Verwaltung Ihrer Daten- und Datenschutz-Compliance.

Das Dashboard Übersicht berichtet über den aktuellen Status von Datenklassifizierungen und Anonymisierungsaufträgen in Ihrer Instanz. Sie können Ihre Daten im Dashboard „Übersicht“ anzeigen, um zu sehen, wie viele Daten klassifiziert werden können, welche Datenklassen verfügbar sind, wie viele Daten in jeder Klasse vorhanden sind und wie viele

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten sie in den Anonymisierungsaufträgen enthalten. Die klassifizierten Daten sind in verschiedene Kategorien unterteilt. Wenn Sie eine Unterkategorie in einem der beiden Diagramme auswählen, wird die Kategorie dem Gesamtdiagramm hinzugefügt oder entfernt, und die Anzahl wird angepasst.



Klassifizierbare Daten

Zeigt die Gesamtzahl der Datensätze in der Instanz an, die klassifiziert werden können. Die Anzahl wird in die Gesamtzahl der klassifizierten Daten und die Gesamtzahl der nicht klassifizierten Daten aufgeschlüsselt. Dies gibt Administratoren einen schnellen Überblick über potenzielle Klassifizierungsmöglichkeiten.

Klassifizierte Daten

Zeigt die Gesamtzahl der Datensätze in der Instanz an, die klassifiziert wurden. Die Anzahl wird in die Gesamtzahl der klassifizierten Daten für jede zugewiesene Datenklasse aufgeschlüsselt. Dies vermittelt ein schnelles Verständnis, wie viele Daten in den einzelnen Bereichen klassifiziert wurden.

Anonymisierungsaufgaben

Zeigt Datenschutzaufträge an, die derzeit von Aufträgen verarbeitet werden, die in Ihrer nicht-Produktionsinstanz für Anwender- und Datenklassenaufträge abgeschlossen wurden.

Weitere Informationen

Die **Weitere Informationen** Abschnitte bieten einen schnellen Überblick über das Verständnis der Klassifizierung und Anonymisierung sowie eine einfache Möglichkeit, mit dem Prozess zu beginnen.

FAQ-Ressourcen

Greifen Sie in Produktlernressourcen über Klassifizierung oder Anonymisierung zu, um zusätzliche Informationen zu erhalten, wie Sie Ihre Instanz mit Datenschutz sichern können.

Datenklassifizierung

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

Datenklassifizierung Aktiviert Unterstützung für:

- Transparenz der Arten von Daten, die auf einem gehostet werden ServiceNow AI Platform Instanzen.
- Compliance mit Datenschutzgesetzen und Erfüllung von Vorschriften für Branchen wie Finanzdienstleistungen und Herstellung medizinischer Geräte.

Datenklassifizierungen

Die Datenklassifizierung ist ein eigenständiger Prozess, bei dem Sie Datenklassifizierungen manuell auf vorhandene Wörterbucheinträge in einer beliebigen Tabelle anwenden. Weitere Informationen finden Sie unter Datenwörterbuchtabellen .

- Sie klassifizieren Daten so, wie Sie es für Ihr Unternehmen als angemessen finden, und Sie können die verfügbaren Datenklassen nach Bedarf ändern.
- Wenn Sie Daten klassifizieren, können Sie die vordefinierten Datenklassifizierungen verwenden oder eigene erstellen. Obwohl die Verwendung vordefinierter Datenklassifizierungen optional ist, wird empfohlen, dies als Ausgangspunkt zu tun. Diese vordefinierten Datenklassifizierungen sind in Demodaten enthalten, die Sie in Ihrer Instanz installieren können.
- Wenn Sie eigene Datenklassifizierungen erstellen, können Sie auch ein abgestuftes hierarchisches System mit übergeordneten und untergeordneten Datenklassifizierungen entwerfen.

Hinweis: Datenklassifizierung Unterstützt Domänentrennung, und die Tabelle „Data_classification“ selbst ist prozessgetrennt. Weitere Informationen finden Sie unter Domain Separation und Datenklassifizierung.

Anwendungsfälle

Die allgemeine Datenschutzverordnung (DSGVO) ist eine Verordnung der Europäischen Union, deren Zweck darin besteht, Einzelpersonen die Kontrolle über ihre eigenen personenbezogenen Daten zu geben. Sie können Datenklassifizierungen wie personenbezogene Informationen verwenden, um zu identifizieren, wo personenbezogene Daten in Ihrer Instanz gespeichert werden. Durch die Anwendung der entsprechenden Sicherheitsmechanismen zum Schutz dieser personenbezogenen Daten vor dem Auslaufen erfüllt Ihre Organisation die DSGVO-Anforderungen.

Wenn Sie Kundeninformationen in speichern ServiceNow AI Platform, Verwenden Sie bei Bedarf den Klassifizierungscode für personenbezogene Daten (Personally Identifiable Information, PII), um Daten nachzuverfolgen, die den lokalen Datenschutzgesetzen unterliegen.

Sie können eine eingeschränkte Datenklassifizierung auf Mitarbeitertabellenspalten anwenden, die vertrauliche Mitarbeiterinformationen wie Sozialversicherungsnummern (SSN) speichern. Administratoren und Auditoren können dann das Übersichts-Dashboard verwenden, um zu bestätigen, dass Sie Datenklassifizierungen den richtigen Spalten zugewiesen haben. Sie können auch die Klassifizierungsdetails für eingeschränkte Informationstypen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Datenklassifizierungen

Erstellen Sie Ihre eigenen anwenderdefinierten Datenklassifizierungen in der Tabelle [Data_classification], die Sie dann bestimmten Spalten in bestimmten Tabellen zuweisen können. Erstellen Sie neue Datenklassen, um den Klassifizierungsprozess zu starten.

Vorbereitungen

Erforderliche Rolle: Data_classification_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz** > **Klassifizierung**an.
2. Wählen Sie Aus **+Datenklasse hinzufügen** .

   Hinweis: Das Basissystem enthält mehrere Datenklassen.

3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Klassenname	Name der Datenklassifizierung.
Übergeordnete Klasse	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung keiner übergeordneten Datenklassifizierung untergeordnet ist.
Beschreibung	Beschreibung der Datenklassifizierung.

4. Klicken Sie auf **Absenden**.
   Die neue Datenklasse wird hinzugefügt. Wenn die Datenklasse ein untergeordnetes Element ist, wird sie unter dem übergeordneten Element in der linken Navigationsleiste aufgeführt.

Daten klassifizieren

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Weisen Sie Datenklassifizierungen bestimmten Tabellenspalten in der Tabelle „Wörterbuch“ [sys_dictionary] zu. Wenn Sie Datenklassifizierungen zuweisen, werden Einträge in der Tabelle „Wörterbuch-Datenklasse“ [m2m_dictionary_dataclass] erstellt, die Sie dann im Dashboard „Übersicht“ überprüfen können.

Vorbereitungen

Erforderliche Rolle: Data_classification_admin, admin

Prozedur

1. Wählen Sie Aus **Neu** Dient zum Zuweisen von Daten aus einer zu klassifizierenden Tabelle.
2. Wählen Sie die Datenklasse aus der Dropdown-Liste aus.
3. Wählen Sie die Datensätze aus, die die zu klassifizierenden Tabellen und Spalten widerspiegeln.
   Wählen Sie zusätzliche Zeilen aus, die pro Seite in der Tabelle angezeigt werden sollen, um die Suche nach einer bestimmten Tabelle zu vereinfachen.
4. Wählen Sie Aus **Klassifizieren Sie Daten** .
   Die Daten werden unter dem Klassifizierungsnamen in der Tabelle „klassifizierte Daten“ klassifiziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Zeigen Sie die Daten in Excel, CSV, JSON oder PDF an oder exportieren Sie sie.
   Wählen Sie aus, die Daten im ausgewählten Format herunterzuladen oder per E-Mail zu erhalten.

Datenanonymisierung

Die Anonymisierung bietet eine Möglichkeit, Daten einfach umzuwandeln, sodass sie nicht identifizierbar sind und den Datenschutzbestimmungen besser entsprechen.

Administratoren können den Anonymisierungsprozess sowohl in Produktions- als auch in nicht-Produktionsinstanzen durchführen. Datenschutz kann in Produktionsinstanzen verwendet werden, um Anwender zu deidentifizieren. Die Anonymisierung von Datenklassen sollte nur mit Instanzen außerhalb der Produktion verwendet werden. Dadurch wird sichergestellt, dass Daten wie E-Mail-Adressen oder physische Adressen durch ähnlich formatierte, aber anonymisierte Versionen ersetzt werden.

Administratoren können die Anonymisierung auch im Rahmen ihrer Prozesse zur allgemeinen Datenschutzverordnung (DSGVO) zum Recht auf Vergessenheit (RTBF) verwenden, um Anwenderinformationen zu anonymisieren. Weitere Informationen finden Sie unter https://gdpr-info.eu/art-17-gdpr/ .

Verwenden Sie den Abschnitt „Anonymisierung“ des Datenschutzes, um Datenschutzrichtlinien und -Techniken zu erstellen und anzuzeigen und Massenzuweisungen für Datenschutz durchzuführen. Zeigen Sie alle Aufträge mit Beschreibung, verwendeter privater Richtlinie und Status an. Um auf den Anonymisierungsabschnitt zuzugreifen, muss ein Administrator zuerst die Rollen „Data_privacy_admin“ und „Data_privacy_processor“ erhöhen.

Anonymisierungstechniken

Anonymisierungstechniken sind Optionen, die Sie auswählen, um zu bestimmen, wie Ihre Daten anonymisiert werden. Sie müssen eine Anonymisierungstechnik erstellen, die im Anonymisierungsauftrag referenziert werden soll. Siehe Erstellen Sie Anonymisierungstechniken Um eine Datenschutztechnik einem zugeordneten zuzuordnen **Konfiguration der Anonymisierungstechnik** .

Anonymisierungsrichtlinien

Konfigurieren Sie eine Anonymisierungsrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden. Siehe für Erstellen Sie Anonymisierungsrichtlinien Details.

Anonymisierungsaufträge

Anonymisierungsaufträge verwenden alle diese Komponenten, um Ihre Daten zu anonymisieren. Weitere Informationen zu diesen Aufträgen finden Sie unter Erstellen Sie einen Anonymisierungsauftrag.

Erstellen Sie Anonymisierungstechniken

Erstellen Sie eine Konfiguration für die Datenschutztechnik, um anzupassen, wie der Datenschutz Ihre Daten anonymisiert.

Vorbereitungen
Erforderliche Rolle: Data_privacy_admin und admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erhöhen Sie die Höhe auf **Data_privacy_admin** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**an.
3. Wählen Sie Aus **Zeigen Sie Techniken an** .
   Es stehen mehrere vordefinierte Techniken zur Auswahl.

Technik	Beschreibung
Selektives Ersetzen	Diese Technik ersetzt Zeichenfolgendaten selektiv. Alle Zeichen zwischen den Start- und Endindizes der Eingabe werden durch das von Ihnen ausgewählte Zeichen ersetzt. Sie können Zeichen angeben, die von der Maskierung ausgeschlossen werden sollen: ○ Start_index: Technik maskiert Daten ab dem angegebenen Zeichen. Wenn leer gelassen, beginnt die Maskierung mit dem ersten Zeichen. ○ End_index: Technik maskiert Daten vom Anfang der Zeichenfolge bis zum angegebenen Zeichen. Wenn leer gelassen, endet die Maskierung mit dem letzten Zeichen. ○ EXCLUDE_CHAR: Definieren Sie ein Zeichen, das von der Maskierung ausgeschlossen werden soll. ○ Replacement_char: Definieren Sie ein Zeichen, das für die Maskierung verwendet wird. Wenn keine angegeben ist, werden standardmäßig Sternchen (*) verwendet.
Statisches Ersetzen	Diese Technik tauscht Werte mit statischen Werten aus. Zeichenfolgen-, Zahlen- und Datumsdaten können diese Technik verwenden: ○ DATE_Time_VALUE: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format JJJJ-MM-TT HH:mm:ss. ○ Date_value: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format JJJJ-MM-TT. ○ Number_value: Ersetzen Sie Zahlenwerte durch diese Zahl. ○ String_value: Ersetzen Sie Zeichenfolgenwerte durch diesen Text. ○ Number_type: Akzeptiert eine Ganzzahl
Zufälliges Ersetzen	Diese Technik tauscht Werte mit zufällig generierten Werten aus. Zeichenfolgen- und Zahlendaten können diese Technik verwenden.
Entfernen	Diese Technik entfernt Werte und ersetzt sie durch leere (null) Werte.
Keine Aktion	Diese Technik ist ein Platzhalter. Wenn diese Option ausgewählt ist, werden keine Felder geändert.
Selektives Ersetzen durch X	Transformiert Zeichenfolgendaten und ersetzt selektiv sensible Zeichen durch den Buchstaben X. **Hinweis:** Standardtechnik für Datenmuster in Erkunden Daten-Discovery(Klassisch).
Anonymisierung von Datenmustern	Anonymisiert nur erkannte Datenmuster in unstrukturierten Datenfeldern, wobei der zugrunde liegende Kontext intakt bleibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Technik	Beschreibung
	Hinweis: Einstellungen für diese Technik verweisen auf Einstellungen der Anonymisierungstechnik für Datenmuster in Erkunden Daten-Discovery(Klassisch).

4. Wählen Sie Aus **Fügen Sie eine anwenderdefinierte Technik hinzu** , Wenn keine vordefinierte Technik verwendet wird.
5. Füllen Sie die Felder im aus **Passen Sie die Technik an** Formular.

Feld1	Beschreibung
Basistechnik	Wählen Sie eine vordefinierte Technik aus, da anwenderdefinierte Techniken auf den vordefinierten Techniken basieren.
Technikname	Geben Sie einen Namen für die Technik ein.
Technikbeschreibung	Geben Sie eine Beschreibung für die Technik ein.

6. Wählen Sie **Weiter**.
7. Geben Sie die Technikparameter ein.
   Die verfügbaren parametrisierten Werte hängen davon ab, welche Datenschutztechnik Sie ausgewählt haben. Es sind keine parametrisierten Werte für vorhanden **Keine Aktion** Und **Entfernen** Techniken.

Parametrisierte Datenschutzwerte für die Basistechniken

Basistechnik	Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
Selektives Ersetzen	End_index	Die Technik maskiert Daten vom Anfang der Zeichenfolge bis zum angegebenen Zeichen. Wenn leer gelassen, endet die Maskierung mit dem letzten Zeichen.	(leer)
Selektives Ersetzen	EXCLUDE_CHAR	Zeichen zum Überspringen der Maskierung. In diesem Wert kann nur ein einzelnes Zeichen verwendet werden. Wenn mehrere eingegeben werden, wird das erste Zeichen verwendet.	(leer)
Selektives Ersetzen	Replacement_char	Zeichen, das beim Ersetzen von Werten durch selektives Ersetzen verwendet werden soll.	Ein Sternchen (*) Wird verwendet, wenn kein anderer Wert eingegeben wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basistechnik	Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
Selektives Ersetzen	Start_index	Technik maskiert Daten, die mit dem angegebenen Zeichen beginnen.	Wenn leer gelassen, beginnt die Maskierung mit dem ersten Zeichen.
Statisches Ersetzen	Date_time_value	Ersetzen Sie Datums- und Uhrzeitwerte durch dieses Datum. Verwenden Sie das Format JJJJ-MM-TT HH:mm:ss.	1988-11-11 10:10:10
Statisches Ersetzen	Date_value	Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format JJJJ-MM-TT.	1988-11-11
Statisches Ersetzen	Number_value	Ersetzen Sie Zahlenwerte durch diese Zahl.	1234567
Statisches Ersetzen	string_value	Ersetzen Sie Zeichenfolgenwerte durch diesen Text.	TEXT123
Zufälliges Ersetzen	Preserve_Data_length	Auf festlegen **Wahr** Dient zum Beibehalten der Datenlänge. Deidentifizierte Daten haben die gleiche Länge wie die ursprünglichen Daten.	True

8. Wählen Sie Aus **Erstellen Sie Eine Anwenderdefinierte Technik** .
   Ihre anwenderdefinierte Technik wird den Anonymisierungstechniken hinzugefügt.

Nächste Maßnahme

Siehe Erstellen Sie Anonymisierungsrichtlinien Dient zum Konfigurieren einer Anonymisierungsrichtlinie, um anzugeben, welche Techniken bei der Anonymisierung Ihrer Daten verwendet werden.

Erstellen Sie Anonymisierungsrichtlinien

Konfigurieren Sie eine Anonymisierungsrichtlinie, um anzugeben, welche Techniken bei der Anonymisierung Ihrer Daten verwendet werden.

Vorbereitungen

Die Datenschutzkonfiguration definiert je nach Anwendungsfall Tabellen, sys_user und andere sowie Spalten, die deidentifiziert werden sollen, und gibt parametrisierte Typen der Techniken an, die beim Deidentifizieren von Daten verwendet werden sollen.

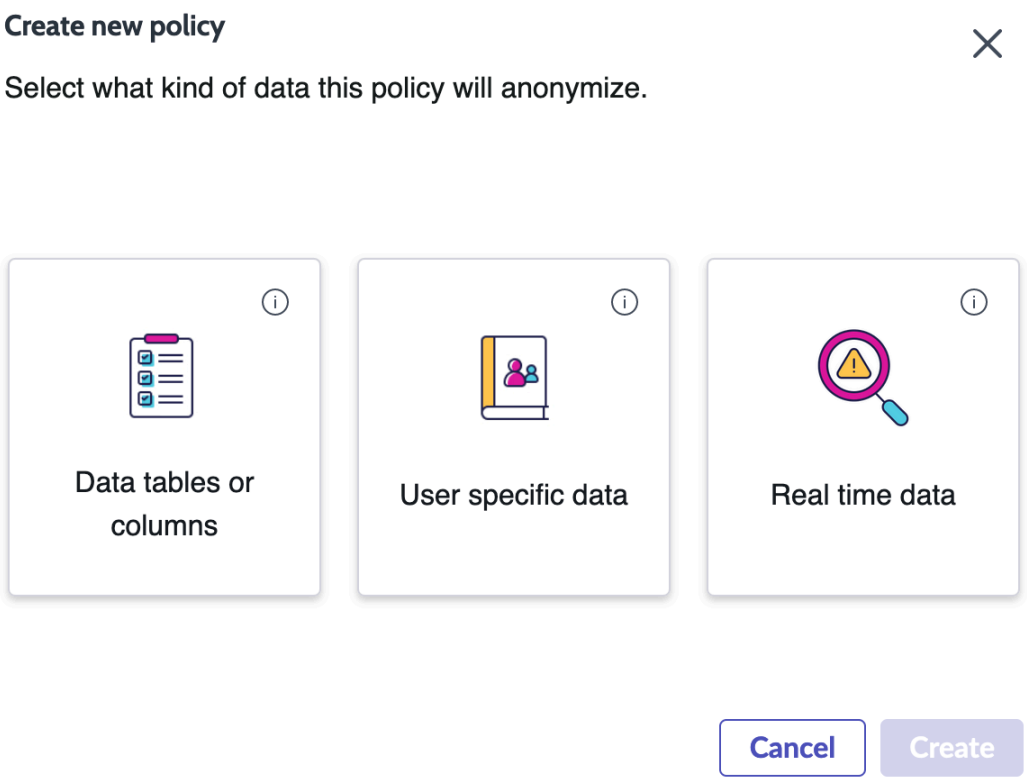
Hinweis: Um eine Datenschutzkonfiguration abzuschließen, müssen Sie zuerst eine Konfiguration der Datenschutztechnik konfigurieren. Weitere Informationen finden Sie unter Erstellen Sie Anonymisierungstechniken.

Erforderliche Rolle: Data_privacy_admin und admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erhöhen Sie die Höhe auf **Data_privacy_admin** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**an.
   Alle Anonymisierungsrichtlinien werden angezeigt. Veröffentlichte Richtlinien sind verfügbar, um den Anonymisierungsauftrag zu planen.
3. Wählen Sie Aus **Erstellen Sie eine neue Richtlinie** .
4. Wählen Sie diese Option aus, um entweder zu anonymisieren **Datentabellen oder -Spalten** , **Anwenderspezifische Daten** , Oder **Echtzeitdaten** .



Datentyp	Beschreibung
Datentabellen oder -spalten	Datensätze, die der Datenrichtlinie entsprechen, werden anonymisiert.
Bestimmte Anwenderdaten	Wählen Sie eine Gruppe von Anwendern oder Anwendergruppen aus, die anonymisiert werden sollen.
Echtzeitdaten	Anonymisieren Sie Echtzeiteinträge für einen Satz von Spalten.

Datenschutzrichtlinien können nur für klassifizierte Daten gelten. Weitere Informationen zur Datenklassifizierung finden Sie unter Datenklassifizierung.

5. Wählen Sie **Erstellen** aus.
   Zum Abschließen der Richtlinie sind sequenzielle Schritte erforderlich. **Definieren Sie Details** Und **Techniken zuweisen** . **Wählen Sie Anwenderreferenz aus** Ist auch erforderlich, wenn die Richtlinie für anwenderspezifische Daten definiert wird.

Automatische Übersetzung

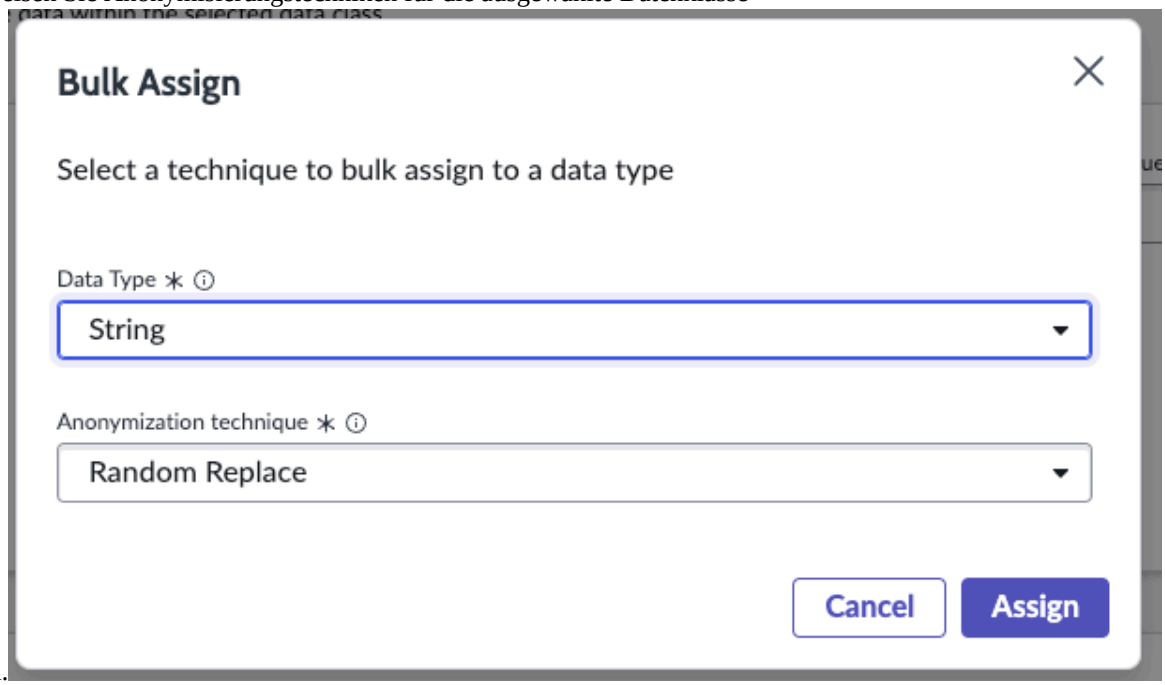
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Definieren Sie die Details für die neue Anonymisierungsrichtlinie.
   - Geben Sie den Richtliniennamen in ein **Name** Und die Richtlinienbeschreibung in **Beschreibung** Feld.
   - Definieren Sie, welche Kanäle die Richtlinie und die Kanalpriorität in automatisch aktivieren **Aktivierungskanäle**
   - In **Datenklasse** Feld die Datenklasse auswählen, die mit dieser Richtlinie verwendet werden soll.
   - Aktivieren oder deaktivieren Sie die Echtzeit-Datenanonymisierung. Siehe Schritt 8, wenn die Echtzeitdatenanonymisierung aktiviert ist

   Hinweis: Wenn Sie keinen Eintrag anonymisieren, wählen Sie aus **DoNothing** Technik, anstatt den Eintrag leer zu lassen. Richtlinien mit leeren Werten im Feld Konfiguration der Datenschutztechnik können nicht ausgeführt werden, wenn sie in Datenschutzaufträgen verwendet werden.

   Nach der Auswahl einer Datenklasse wird das Formular Techniken zuweisen für jeden Datensatz angezeigt, der für die definierte Datenklasse zurückgegeben wird.

7. Weisen Sie Anonymisierungstechniken für die ausgewählte Datenklasse zu.

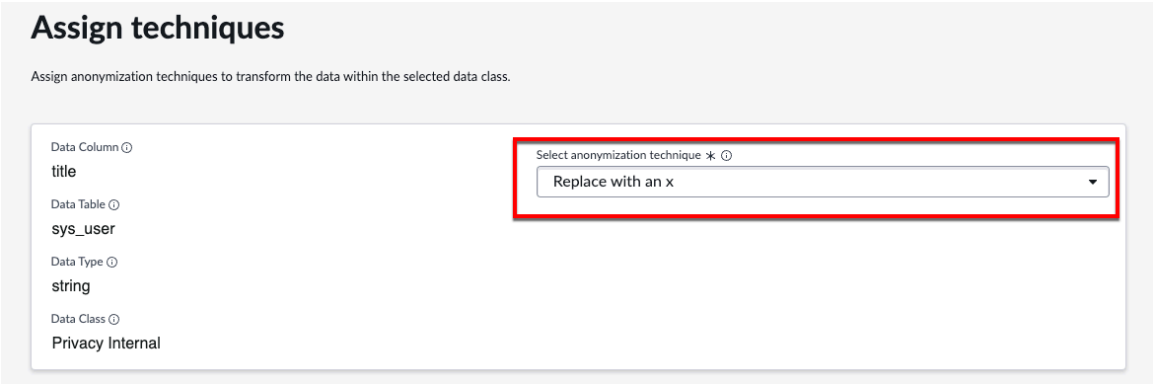


Option	Beschreibung
Wählen Sie Aus Massenzuweisung Von Techniken	Wendet die Anonymisierung auf alle Datensätze in der ausgewählten Datenklasse an. Wählen Sie den Datentyp und die Anonymisierungstechnik aus, die auf alle Einträge mit dem ausgewählten Datentyp angewendet werden sollen. Wiederholen Sie diesen Schritt für zusätzliche Massenzuweisungen verschiedener Datentypen. Siehe Unterstützte Feldtypen für die Anonymisierung Für eine Liste von Datentypen.
Wählen Sie eine aus Anonymisierungstechnik Für jeden Datenspaltendatensatz	Ihre Datenschutzverarbeiter-Anwender können auswählen, welche Datensätze beim Erstellen von Datenschutzaufträgen anonymisiert werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Wenden Sie die Anonymisierung einzeln auf jeden Datensatz in der ausgewählten Datenklasse an.



8. **Wahlweise:** Geben Sie untergeordnete Tabellen ein, die gescannt werden sollen.
   Untergeordnete Tabellen des übergeordneten Elements werden anonymisiert. Wenn eine Tabelle keine untergeordneten Elemente hat, ist diese Option nicht verfügbar.

   Warnung: Ein übergeordneter Auftrag schlägt fehl, wenn ein untergeordneter Auftrag fehlschlägt.

9. **Wahlweise:** Wenn die Anonymisierung von Datenmustern ausgewählt ist, wählen Sie die zu verwendende Anonymisierungstechnik aus.
10. **Wahlweise:** Legen Sie die Reihenfolge für Datenmuster fest.
11. **Wahlweise:**

    Tipp: Verwenden Sie **Testen** Funktion zum Testen von Beispieleingaben. Sie können Metriken aus dem Ergebnis überprüfen, z. B. Scan-Zeit, Ergebnis und erkannte Muster.

    Wählen Sie aus **Testen** Schaltfläche zum Testen der Richtlinie.

12. **Wichtig:** Alle Tabellen müssen einen richtigen sys_dictionary-Eintrag haben.

    Wählen Sie **Speichern**.

13. Wählen Sie Aus **Veröffentlichen** Dient zum Aktualisieren der Anonymisierungsrichtlinie für die Planung und zur Rückgabe an Anonymisierungsrichtlinien.

    Hinweis: Nur veröffentlichte Richtlinien können für die Planung von Anonymisierungsaufträgen verwendet werden.

Nächste Maßnahme

Erstellen Sie einen Anonymisierungsauftrag.

Klonanforderung für Datenanonymisierung konfigurieren

Die Integration des Datenschutzklons wird mithilfe eines PostClone-Skripts konfiguriert, um Datenschutzaufträge für konfigurierte Richtlinien im Ziel zu erstellen und auszuführen. Nach der Ausführung des Skripts sehen Anwender deidentifizierte Daten und haben keinen Zugriff auf die ursprünglichen Daten.

Vorbereitungen

Das Datenschutz-PostClone-Skript wird mit der Aktivierung des Datenschutz-Plugins (sn_dp_Store_App) installiert. Details siehe Aktivieren Sie den Datenschutz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Data_privacy_clone_processor, Data_privacy_admin und admin

Prozedur

1. Aktivieren Sie das Datenschutz-Plugin (sn_dp_Store_App) in der Quellinstanz.
   Das Datenschutz-PostClone-Skript ist installiert.
2. Erhöhen Sie die Höhe auf **Data_privacy_admin** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
3. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**an.
4. Wählen Sie Aus **Erstellen Sie eine neue Richtlinie** .
   Details siehe Erstellen Sie Anonymisierungsrichtlinien.
5. Wählen Sie Aus **Datentabellen oder -Spalten** .
6. Wählen Sie **Erstellen** aus.
7. Geben Sie einen Namen ein, und wählen Sie eine Datenklasse aus.
8. Wählen Sie bis aus **Aktivieren Sie die Richtlinie während des Klonens** .
9. Wählen Sie die Richtlinienreihenfolge aus, die ausgeführt werden soll, wenn mehrere Klonrichtlinien vorhanden sind.
   Ein Datenschutzauftrag für die PostClone-Konfiguration mit einer höheren Anwendungsreihenfolge kann vor einem anderen Auftrag mit niedrigerer Reihenfolge beginnen, wenn der Auftrag mit der höheren Reihenfolge keine Tabelle enthält, die sich auf einen anderen Auftrag mit niedrigerer Reihenfolge bezieht.
10. Wählen Sie **Fortsetzen**.
11. Schließen Sie die Richtlinienkonfiguration ab, und veröffentlichen Sie die Richtlinie.
12. Sichern Sie Datenschutzkonfigurationen.
13. Planen Sie den Anonymisierungsauftrag.
    Details siehe Erstellen Sie einen Anonymisierungsauftrag.
14. Senden Sie als Datenschutzadministrator eine Klonanforderung.

Ergebnis

Das Datenschutz-PostClone-Skript wird auf der Zielinstanz ausgeführt, und das PostClone-Skript erstellt einen Datenschutz-Verbundauftragsdatensatz auf der Zielinstanz.
Der Verbundauftrag erstellt und führt einen Datenschutzauftrag für jede nach dem Klonen durchgeführte Richtlinie in Anwendungsreihenfolge in der Zielinstanz aus. Die Sicherungsquelle wird in die Zielinstanz geklont. Das PostClone-Skript für Datenschutz erstellt und führt Datenschutzaufträge für konfigurierte Richtlinien in der Zielinstanz aus.

Der Prozessor für den erhöhten Datenschutz-Klon kann sich bei der Zielinstanz anmelden und den Status des verbündeten Auftrags nach dem Klonen in den Feldern dp_federated_Job.list und dp_Job.list überwachen.

Erstellen Sie einen Anonymisierungsauftrag

Konfigurieren Sie einen Datenschutzauftrag in Ihrer Produktionsinstanz, um anonymisierte Daten in Ihrer nicht-Produktionsinstanz für Anwender- und Datenklassenaufträge zu verwenden.

Vorbereitungen

Der Datenschutzauftrag unterstützt zwei Anwendungsfälle zur Deidentifizierung:

- Vertrauliche Daten bestimmter sys_users
- Vertrauliche Daten einer bestimmten Datenklasse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Data_privacy_processor und admin

Prozedur

1. Erhöhen Sie die Höhe auf **Data_Privacy_Processor** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Anonymisierung**an.
3. Wählen Sie in einer Anonymisierungsrichtlinie aus **Aufgabe planen** Für die Richtlinie, die im Auftrag verwendet werden soll.
   Eine Richtlinie muss sich im Status „veröffentlicht“ befinden, um einen Anonymisierungsauftrag zu planen.

   ⚠ **Warnung:** Anonymisierungsaufträge sind äußerst destruktiv und können nur beim Rollback rückgängig gemacht werden. Überprüfen Sie alle Informationen, z. B. die verarbeiteten Datensätze und Tabellen, bevor Sie eine Aufgabe planen.

4. Füllen Sie die Felder des Formulars aus.

Felder für Datenschutz-Auftrag

Feld	Beschreibung
Richtlinie verwendet	Schreibgeschützter Name der ausgewählten Datenschutzrichtlinienkonfiguration, die für diesen Auftrag verwendet werden soll. Bearbeiten Sie die Richtlinie, um zusätzliche Informationen zur Richtlinie anzuzeigen. Weitere Informationen zu Konfigurationen der Datenschutzrichtlinie finden Sie unter Erstellen Sie Anonymisierungsrichtlinien.
Stellenbeschreibung	Beschreibung des Auftrags.
Startzeit	Der Beginn der Zeit, in der dieser Auftrag ausgeführt werden soll **HH:MM:SS** .
Endzeit	Das Ende des Zeitfensters, in dem dieser Auftrag ausgeführt werden soll **HH:MM:SS** . Die Endzeit muss nach der Startzeit liegen. Der Auftrag wird vor der in dieses Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag noch nicht abgeschlossen ist, wird der Auftrag beim nächsten Start des Fensters angehalten und fortgesetzt.
Probelauf	Führen Sie den Auftrag als Test aus. Bei der Ausführung dieses Auftrags sind keine Datensätze betroffen. Ergebnisse werden in angezeigt **Aufträge** Liste, als ob der Auftrag ausgeführt wurde. ℹ **Hinweis:** **Probelauf** Muss deaktiviert sein, wenn ein Datenschutzauftrag mit Rollback konfiguriert wird. Details siehe Rollback des Datenschutzauftrags.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Art der Anwenderauswahl	Wählen Sie entweder Anwender oder Gruppen aus, die anonymisiert werden sollen.
Wählen Sie Anwender/Gruppen aus	Wählen Sie einen bestimmten Satz von Anwendern oder Gruppen aus, die in diesem Auftrag anonymisiert werden sollen. Unterstützt bis zu 1000 Anwender. **Hinweis:** Dieses Pflichtfeld wird nur angezeigt, wenn die ausgewählte Datenschutzrichtlinienbedingung eine Auswahl von Anwenderdatensätzen erfordert.

5. **Wichtig:** Alle Tabellen müssen vor der Planung und während ihrer Aufgabe einen richtigen sys_dictionary-Eintrag haben.

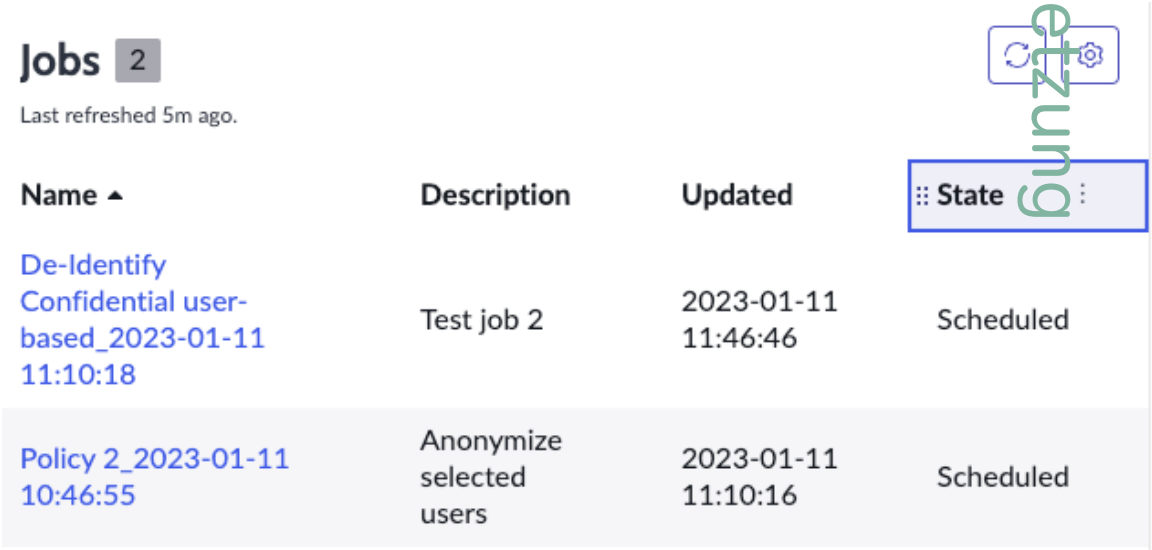
Wählen Sie Aus **Aufgabe planen** Im Formular, um die Anonymisierung in die Auftragswarteschlange zu platzieren.

Der Auftrag wird zwischen den in ausgewählten Zeiten ausgeführt **Startzeit** Und **Endzeit** Felder. Wenn der Auftrag während des Start- und Endzeitfensters nicht abgeschlossen wurde, wird der Auftrag beim nächsten Start des Zeitfensters fortgesetzt.

Ein Auftrag kann nur einmal ausgeführt werden, auch wenn **Probelauf** Ist ausgewählt. Um einen Auftrag basierend auf derselben Richtlinie erneut auszuführen, wählen Sie aus **Aufgabe planen** Und füllen Sie das Formular mit denselben Feldwerten aus.

Warnung: Anonymisierungsaufträge für verschlüsselte Spalten können Sie alle verschlüsselten Spalten entschlüsseln und erneut verschlüsseln, auf die der Auftrag ausgerichtet ist. Um dies zu verhindern, wählen Sie aus **Keine Aktion** Als Richtlinientechnik.

Der Auftrag wird in aufgeführt



AufträgeBereich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name des Anonymisierungsauftrags.
Beschreibung	Beschreibung des Anonymisierungsauftrags.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung des Auftrags.
Status	Status des Datenschutzauftrags: ○ **Geplant** : Standardstatus für neue Aufträge. ○ **Abgeschlossen** : Der Auftrag hat die ausgewählten Daten erfolgreich anonymisiert. ○ **Abgebrochen** : Der Auftrag wurde manuell abgebrochen. ○ **Fehler** : Beim Speichern des Auftrags ist ein Problem aufgetreten. Planen Sie den Auftrag neu, oder erstellen Sie einen neuen Auftrag. Wenn der Fehler weiterhin besteht, können Probleme mit der Konfiguration auftreten. ○ **Rollback wird ausgeführt** : Der Auftrag wurde so festgelegt, dass die Anonymisierung zurückgesetzt wird. ○ **Rollback abgeschlossen** : Das Rollback des Anonymisierungsauftrags wurde erfolgreich abgeschlossen. Ein schreibgeschütztes Feld.

6. Wählen Sie einen Auftrag aus der aus **Aufträge** Bereich zum Öffnen der Auftragszusammenfassung. Nachdem eine Aufgabe geplant wurde, wird **Auftrag Abbrechen** Und **Anhalten** Schaltflächen werden in der Auftragszusammenfassung angezeigt.

Zusätzliche Felder für geplante Aufgaben

Feld	Beschreibung
Geschätzte Anzahl der Datensätze	Die geschätzte Anzahl der Datensätze, auf die sich dieser Probelauftrag vor der Ausführung auswirkt. Ein schreibgeschütztes Feld
Gesamtzahl der verarbeiteten Datensätze	Die Gesamtzahl der einzelnen Datensätze, die von diesem Auftrag betroffen sind. Ein schreibgeschütztes Feld.
Gesamtzahl der verarbeiteten Datentabellen	Die Gesamtanzahl der von diesem Auftrag verarbeiteten Datentabellen. Ein schreibgeschütztes Feld.
Verbleibende Zeit bis zum Rollback	Die verbleibende Zeit, für die ein abgeschlossener Datenanonymisierungsauftrag zurückgesetzt und die Daten deanonymisiert werden können. Ein schreibgeschütztes Feld.
Gesamtanzahl der verarbeiteten Anwender	Die Gesamtzahl der einzelnen Anwenderdatensätze, die dieser Auftrag betrifft. Ein schreibgeschütztes Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Auftrag abbrechen	Wählen Sie diese Option aus, um den Anonymisierungsauftrag abzubrechen. Diese muss vor der Startzeit des Auftrags ausgewählt werden. Wenn diese Option ausgewählt ist, wird der Auftragsstatus in aktualisiert `Abgebrochen` .
Pause	Wählen Sie diese Option aus, um den Auftrag anzuhalten und die Aufzeichnung rückgängig zu machen, wenn Rollback ausgewählt wurde. Nach Ablauf von drei Tagen wird für Rollback-Kontexte eine Warnmeldung angezeigt. Diese muss nach der Startzeit des Auftrags und vor der Endzeit des Auftrags ausgewählt werden. Wenn diese Option ausgewählt ist, wird der Auftragsstatus in aktualisiert `Angehalten` .
Fortfahren	Startet einen angehaltenen Auftrag neu. Rollback wird für fortgesetzte Aufgaben nicht unterstützt, wenn sie angehalten werden. Brechen Sie den Auftrag ab, und erstellen Sie einen Datenschutzauftrag. Die Aufzeichnung verwendet einen nicht abgelaufenen Rollback-Kontext. Wenn diese Option ausgewählt ist, wird der Auftragsstatus in aktualisiert `Geplant` .
Exportieren	Lädt eine PDF-Datei mit den Details zum Datenschutzauftrag herunter.

Aktivieren Sie parallele Aufträge für die Datenanonymisierung

Verwenden Sie parallele Aufträge, um die Ausführungszeit Ihres Anonymisierungsauftrags zu reduzieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur
Standardmäßig werden Datenklassen- und anwenderbasierte Anonymisierungsaufträge mit einem einzelnen Thread ausgeführt. Für Datenklassen- und anwenderbasierte Aufträge können mehrere Threads aktiviert werden. Darüber hinaus werden beim Klonen verwendete Verbundaufträge standardmäßig parallele Aufträge mit 3 Mitarbeitern verwendet.

1. Geben Sie im Navigationsfilter ein `sys_properties.list` .
2. Erstellen Sie die Eigenschaft `Com.Glide.Data_privacy.max_parallel_Worker`
3. **Wahlweise:** Um die Anzahl der verbundenen parallelen Worker für Jobs anzupassen, bearbeiten Sie `dp.max_concurrent_clone_item_Worker` Eigenschaft.
4. Verifizieren Sie **Typ** Ist `Ganzzahl` .
5. **Wichtig:** Es wird empfohlen, mit einer kleinen Anzahl von Mitarbeitern pro Knoten (2 oder 3) zu beginnen.

   Geben Sie die Anzahl der parallelen Job Worker in ein **Wert** Feld bis zu 5.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anonymisierung in Echtzeit

Verwenden Sie die Richtlinie Real Time Anonymization (RTA), um Dateneinträge in Echtzeit zu anonymisieren.

Echtzeitanonymisierung – Übersicht

Anwender erstellen eine RTA-Richtlinie, indem sie Echtzeitanonymisierung im auswählen Seite „Anonymisierungsrichtlinien“ , Und dann den entsprechenden Datenkanal auswählen. Sie können beispielsweise verwenden Virtual Agent Mit Echtzeitanonymisierung: Erstellen Sie eine Anonymisierungsrichtlinie mit Virtual Agent Als ausgewählt **Datenkanal** .

Spalten aus dem Zieltabellen Kann für RTA ausgewählt werden, woraufhin Aktive Datenmuster Werden verwendet und ihre Richtlinien auf alle gültigen Datensatzeinträge in den Spalten angewendet, die für RTA bestimmt sind. Wenn ein Eintrag mit einem aktiven Datenmuster übereinstimmt, ist er zugeordnet Anonymisierungstechnik Wird für die Anonymisierung verwendet.

Tipp: Informationen zum Ändern der Anonymisierungstechnik finden Sie unter Konfigurieren Daten-Discovery Muster.

Fehler bei der Echtzeit-Anonymisierung

Wenn eine RTA-Richtlinie fehlschlägt, können Sie ihren Status mit überprüfen Fehler bei der Echtzeit-Anonymisierung Tabelle.

Fehler bei der Echtzeit-Anonymisierung

Überprüfen Sie Fehler bei der Echtzeitanonymisierung (RTA).

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz (Klassisch)**an.
2. Überprüfen Sie die RTA-Fehler in der Tabelle.

Feldtitel	Beschreibung
Tabellenspalte	Die Tabellenspalte, in der der Fehler aufgetreten ist.
Fehlergrund	Kategorie der Fehlerursache.
Details zum Fehlergrund	Kurzbeschreibung, die die Fehlerursache zusammenfasst.
Datenschutzkonfiguration	Die fehlgeschlagene RTA-Datenschutzkonfiguration.
Datensatz	Der spezifische Datensatz, der fehlgeschlagen ist.
Tabellenname	Tabelle, in der der Fehler aufgetreten ist.
Zeitstempel	Zeit des Fehlers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie den Datenschutz

Datenschutz umfasst Datenklassifizierung und Anonymisierung und wird über installiert ServiceNow Store.

Vorbereitungen

Zur Verwendung der Datenanonymisierung muss zunächst Datenschutz (Classic) mit aktiviert werden ServiceNow Vault Berechtigung. Weitere Informationen finden Sie unter Datenschutz aktivieren (Klassisch).

Hinweis: Durch die Installation der Datenschutz-Store-App werden die Daten-Discovery-Store-App, das Datenschutz-Plugin (Classic) und das Datenklassifizierungs-Plugin automatisch installiert.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** > **Datenschutz**an.
2. Suchen Sie die Anwendung über die Filterkriterien und die Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie eine Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.

   (Optional) Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für häufige Anwendungsfälle veranschaulichen. Das Laden von Demodaten wird empfohlen, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

   Wichtig: Wenn Sie die Demodaten nicht während der Installation laden, stehen sie nicht zum späteren Laden zur Verfügung.
6. Wählen Sie **Installieren** aus.

Datenschutz für Virtual Agent

Sie können den Datenschutz verwenden, um vertrauliche Daten und personenbezogene Daten während einer Virtual Agent-Konversation zu erkennen und zu maskieren.

Vorbereitungen

Erforderliche Rolle: Virtual_Agent_Data_privacy_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie Datenschutz, um vertrauliche Daten und personenbezogene Daten während einer Virtual Agent-Konversation zu erkennen und zu maskieren. Datenschutz ersetzt den abgeschriebenen Handler für sensible Daten, siehe Verwerfungsprozess [KB0867184] Weitere Informationen finden Sie unter . Der Setup-Prozess kann variieren, je nachdem, ob der Handler für sensible Daten zuvor installiert und konfiguriert wurde.

Hinweis: Wenn Sie zuvor den Handler für sensible Daten konfiguriert haben, werden Ihre Einstellungen als Richtlinie zum Datenschutz migriert. Weitere Informationen finden Sie unter Erstellen Sie Anonymisierungsrichtlinien.

Prozedur

1. Navigieren zu **Alle** > **Konversations-Schnittstellen** > **Einstellungen**an.
2. Unter **Erkennung sensibler Daten** , Wählen Sie aus **Alle anzeigen** .
   Wenn die Schaltfläche lautet **Rufen Sie Datenschutz ab** , Sie müssen das Datenschutz-Plugin installieren, um fortzufahren. Siehe Datenschutz aktivieren (Klassisch) Weitere Informationen finden Sie unter
3. Legen Sie den Schieberegler auf fest **Aktiv** .
4. **Wahlweise:** Wenn Datenschutz noch nicht installiert ist, werden Sie aufgefordert, das Datenschutz-Plugin zu installieren, um fortzufahren (siehe) Datenschutz aktivieren (Klassisch) Weitere Informationen finden Sie unter .
5. Wählen Sie den entsprechenden Konversations-Flow aus:
   a. Anfordernde Person zu Service Desk-Mitarbeiter: Erkennen und maskieren Sie vertrauliche Daten, die von der anfordernden Person in eingegeben wurden Mitarbeiterchat Konversation.
   b. Service Desk-Mitarbeiter zu anfordernder Person: Erkennen und maskieren Sie vertrauliche Daten, die vom Service Desk-Mitarbeiter in eingegeben wurden Mitarbeiterchat Konversation.
   c. Anfordernde Person an Virtual Agent– Erkennen und maskieren Sie vertrauliche Daten, die von der anfordernden Person während eines eingegeben wurden Virtual Agent Konversation.

   Hinweis: Sie müssen mindestens einen Konversations-Flow auswählen.
6. Wählen Sie Aus **In Datenschutz verwalten** .
   Wenn Sie den Handler für sensible Daten bereits konfiguriert haben, werden Ihre Einstellungen als Richtlinie zum Datenschutz migriert
7. Erstellen Sie eine neue Datenschutzrichtlinie für Virtual Agent, siehe Erstellen Sie Anonymisierungsrichtlinien Weitere Informationen zu Datenschutzrichtlinien.

Domänentrennung und Datenschutz

Domänentrennung wird für nicht unterstützt Datenschutz . Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung.

Zugehörige Informationen

Domänentrennung für Service Provider

Unterstützte Feldtypen für die Anonymisierung

Überprüfen Sie, welche Feldtypen beim Anonymisieren von Daten unterstützt werden.

Hinweis: Nicht alle klassifizierten Feldtypen sind für die Anonymisierung verfügbar.

Einige Feldtypen mit hohem Risiko sind standardmäßig deaktiviert, wie in der Tabelle beschrieben. Weitere Informationen zu Feldern finden Sie unter Feldtypen .

Unterstützte Feldtypen für die Anonymisierung

Feldtyp	Standardmäßig verfügbar
Audio	Nein
Bedingung	Nein
Bedingungszeichenfolge	Nein
currency	Ja
Dezimalzahl	Ja
due_date	Ja
Gleitkommazahl	Ja
glide_date	Ja
Glide_date_time	Ja
Glide_duration	Nein
Glide_time	Ja
HTML	Nein
icon	Nein
Ganzzahl	Ja
ip_addr	Nein
ip_address	Nein
Journal	Ja
journal_input	Ja
journal_list	Ja
Lang	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldtyp	Standardmäßig verfügbar
Name_Werte	Nein
percent_complete	Nein
Phone_NUMBER_e164	Ja
Preis	Ja
Zeichenfolge	Ja
String_Full_utf8	Ja
Übersetzt_html	Nein
Übersetzt_Text	Nein
URL	Nein
user_image	Nein
Video	Nein
Wiki_Text	Nein

Datenschutzrollen

Datenschutz fügt diese Rollen hinzu.

Datenschutzadministrator

Die Datenschutzadministratorrollen sind eine Administratorrolle, die zum Erstellen von Datenschutztechniken und -Richtlinien verwendet wird.

Datenschutzadministrator [Data_privacy_admin]

Enthält Rollen

Keine

Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Ja

Überlegungen

Vermeiden Sie es, diese Rolle Ihren Anwendern zuzuweisen, wenn gezieltere Rollen verfügbar sind.

Um die Rolle „Datenschutzadministrator“ zuzuweisen, erhöhen Sie den Anwender auf die Rolle „Sicherheitsadministrator“, um die Rolle hinzuzufügen.

Datenschutz-Auditor

Der Datenschutz-Auditor ist eine schreibgeschützte Rolle, die zum Anzeigen von Datenschutzdatensätzen verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz-Auditor [Data_privacy_Auditor]

Enthält Rollen

Keine

Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Nein

Überlegungen

Keine

Klonprozessor für Datenschutz

Benutzer mit der Prozessorrolle „Datenschutz-Klon“ können Datenschutzaufträge der Datenklasse erstellen und ausführen.

Prozessor für Datenschutz-Klon [Data_privacy_clone_processor]

Enthält Rollen

Keine

Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Ja

Überlegungen

Keine

Datenschutzprozessor

Anwender mit der Rolle „Datenschutzprozessor“ erstellen und führen Datenschutzaufträge in der Anwendertabelle [sys_user] aus.

Datenschutzverarbeiter [Data_privacy_processor]

Enthält Rollen

Keine

Gruppen zugewiesen

Keine

Abonnement

Nein

Erweitert

Ja

Überlegungen

Keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenschutz (klassisch)

Datenschutz (Classic) ist eine Legacy-Anwendung, die Datenklassifizierung, Techniken und Aufträge zur Anonymisierung personenbezogener Daten bereitstellt.

Datenschutz Klassisch

Hinweis: Dieser Abschnitt bezieht sich auf Datenschutz (Classic). Siehe Datenschutz Für die neueste aktuelle Store-Version.

Datenschutz aktivieren (Klassisch)

Sie können das Datenschutz-Plugin (com.Glide.Data_privacy) für aktivieren Platform-Sicherheit Wenn Sie die Administratorrolle innehaben. Die Anwendung enthält Demodaten und zugehörige Installationen ServiceNow® Store Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

Wichtig: Dieser Abschnitt bezieht sich auf Datenschutz (Classic). Siehe Datenschutz Für die neueste aktuelle Store-Version.

Datenschutz erfordert ein separates Abonnement vom Rest des ServiceNow AI Platform®.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste „Alle Anwendungen“ in Ihrer Instanz aktivieren.

Hinweis: Vor dem Kauf eines Abonnements können Sie Datenschutz (Classic) und Daten-Discovery mit einem 30-tägigen Testzeitraum bewerten. Nach Ablauf Ihrer Testversion können Sie ohne Lizenz keine Daten mehr erkennen oder Anonymisierungsaufträge in ausführen.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Datenschutz installiert:

- Plugins
- Rollen
- Tabellen

Weitere Informationen finden Sie unter Mit Datenschutz installiert (Classic).

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Datenschutz“ (com.Glide.Data_privacy).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Mit Datenschutz installiert (Classic)

Erfahren Sie mehr über die mit dem Datenschutz-Plugin (com.Glide.Data_privacy) installierten Komponenten.

Installierte Tabellen

Tabelle	Beschreibung
Datenschutz-Verbundauftrag [dp_Federated_Job]	Verbundaufträge für Datenschutz
Datenschutzauftrag [dp_Job]	Datenschutzaufträge
Datenschutzauftrag [dp_Job_Summary]	Zusammenfassungen des Datenschutzauftrags
Datenschutztechnik [dp_technique]	Datenschutztechniken
Primärer Referenzlink [dp_primary_reference]	Primäre Referenzlinks
Technik für klassifiziertes Datenschutzfeld [dp_field_technique]	Techniken für klassifiziertes Datenfeld
Datenschutzkonfiguration [dp_Configuration]	Datenschutzkonfigurationen
Konfiguration der Datenschutztechnik	Datenschutztechniken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[dp_Technik_mit_Parametern]	
Parameter für Datenschutztechnik [dp_Technik_mit_Parameter]	Datenschutztechniken mit Parametern
Parameterwert für Datenschutztechnik [dp_Technik_mit_Parameter_Wert]	Parameterwerte, die in Datenschutztechniken mit Parametern verwendet werden.

Konfiguration des Datenschutzes (Classic)

Erfahren Sie, wie Sie Datenschutztechniken und -Richtlinien erstellen und Datenschutzaufträge erstellen und ausführen.

Wichtig: Dieser Abschnitt bezieht sich auf Datenschutz (Classic). Siehe Datenschutz Für die neueste aktuelle Store-Version.

Datenschutztechniken

Datenschutztechniken sind Optionen, die Sie auswählen, um zu bestimmen, wie Ihre Daten anonymisiert werden. Sie müssen eine Datenschutztechnik erstellen, auf die im Datenschutzauftrag verwiesen werden soll. Siehe Erstellen Sie eine Konfiguration der Datenschutztechnik Um eine Datenschutztechnik einem zugeordneten zuzuordnen **Konfiguration der Datenschutztechnik** .

Datenschutzrichtlinien

Konfigurieren Sie eine Datenschutzrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden. Details siehe Erstellen Sie eine Datenschutzrichtlinie.

Datenschutzaufträge

Datenschutzaufträge verwenden alle diese Komponenten, um Ihre Daten zu anonymisieren. Weitere Informationen zu diesen Aufträgen finden Sie unter Konfigurieren Sie einen Datenschutzauftrag.

Erstellen Sie eine Konfiguration der Datenschutztechnik

Erstellen Sie eine Konfiguration für die Datenschutztechnik, um anzupassen, wie der Datenschutz Ihre Daten anonymisiert.

Vorbereitungen
Erforderliche Rolle: Data_privacy_admin und admin

Prozedur

1. Erhöhen Sie die Höhe auf **Data_privacy_admin** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Konfiguration der Datenschutztechnik**an.
3. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. In **Name** Geben Sie einen Namen für die Konfiguration Ihrer Datenschutztechnik ein.
5. In **Datenschutztechnik** Feld eine Datenschutztechnik auswählen.

Datenschutztechniken

Technik	Beschreibung
Keine Aktion	Diese Technik ist ein Platzhalter. Wenn diese Option ausgewählt ist, werden keine Felder geändert.
Zufälliges Ersetzen	Diese Technik tauscht Werte mit zufällig generierten Werten aus. Zeichenfolgen- und Zahlendaten können diese Technik verwenden.
Selektives Ersetzen	Diese Technik ersetzt Zeichenfolgendaten selektiv. Alle Zeichen zwischen den Start- und Endindizes der Eingabe werden durch das von Ihnen ausgewählte Zeichen ersetzt. Sie können Zeichen angeben, die von der Maskierung ausgeschlossen werden sollen: ○ Start_index: Technik maskiert Daten ab dem angegebenen Zeichen. Wenn leer gelassen, beginnt die Maskierung mit dem ersten Zeichen. ○ End_index: Technik maskiert Daten vom Anfang der Zeichenfolge bis zum angegebenen Zeichen. Wenn leer gelassen, endet die Maskierung mit dem letzten Zeichen. ○ EXCLUDE_CHAR: Definieren Sie ein Zeichen, das von der Maskierung ausgeschlossen werden soll. ○ Replacement_char: Definieren Sie ein Zeichen, das für die Maskierung verwendet wird. Wenn keine angegeben ist, werden standardmäßig Sternchen (*) verwendet.
Statisches Ersetzen	Diese Technik tauscht Werte mit statischen Werten aus. Zeichenfolgen-, Zahlen- und Datumsdaten können diese Technik verwenden: ○ DATE_Time_VALUE: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format JJJJ-MM-TT HH:mm:ss. ○ Date_value: Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format JJJJ-MM-TT. ○ Number_value: Ersetzen Sie Zahlenwerte durch diese Zahl. ○ String_value: Ersetzen Sie Zeichenfolgenwerte durch diesen Text.
Entfernen	Diese Technik entfernt Werte und ersetzt sie durch leere (null) Werte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Zuvor unterstützter Wert **Ersetzen** Ist veraltet und umbenannt **Ersetzen – Veraltet** Und sollten nicht verwendet werden.

6. Klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie auf **Speichern** Im Kontextmenü. Nachdem der Datensatz gespeichert wurde, wird **Parametrisierte Datenschutzwerte** Liste wird angezeigt.
7. Verwenden Sie die Datensätze in **Parametrisierte Datenschutzwerte** Liste, um die Konfiguration Ihrer Datenschutztechnik anzupassen.
   Die verfügbaren parametrisierten Werte hängen davon ab, welche Datenschutztechnik Sie ausgewählt haben. Es sind keine parametrisierten Werte für vorhanden **Keine Aktion** Und **Entfernen** Techniken.

Parametrisierte Datenschutzwerte für selektives Ersetzen

Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
CHAR_to_replace	Zeichen, das beim Ersetzen von Werten durch selektives Ersetzen verwendet werden soll.	*
End_index	Die Technik maskiert Daten vom Anfang der Zeichenfolge bis zum angegebenen Zeichen. Wenn leer gelassen, endet die Maskierung mit dem letzten Zeichen.	(leer)
EXCLUDE_CHAR	Zeichen zum Überspringen der Maskierung. In diesem Wert kann nur ein einzelnes Zeichen verwendet werden. Wenn mehrere eingegeben werden, wird das erste Zeichen verwendet.	(leer)
Start_index	Technik maskiert Daten, die mit dem angegebenen Zeichen beginnen.	1

Parametrisierte Datenschutzwerte für Ersetzen

Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
Date_time_value	Ersetzen Sie Datums- und Uhrzeitwerte durch dieses Datum. Verwenden Sie das Format JJJJ-MM-TT HH:mm:ss.	1988-11-11 10:10:10
Date_value	Ersetzen Sie Datumswerte durch dieses Datum. Verwenden Sie das Format JJJJ-MM-TT.	1988-11-11
Number_value	Ersetzen Sie Zahlenwerte durch diese Zahl.	1234567
Preserve_Data_length	Auf festlegen **Wahr** Dient zum Beibehalten der Datenlänge. Deidentifizierte Daten haben	wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameterwert für Datenschutztechnik	Beschreibung	Standardwert
	die gleiche Länge wie die ursprünglichen Daten.	
string_value	Ersetzen Sie Zeichenfolgenwerte durch diesen Text.	TEXT123
Use_random_generated_value	Auf festlegen **Wahr** Zum Ersetzen von Daten durch zufällig generierte Werte. Nur Zeichenfolgen- und Zahlendaten können durch zufällige Werte ersetzt werden. Diese Option überschreibt statische Werte.	falsch

8. Klicken Sie auf **Speichern**.

Erstellen Sie eine Datenschutzrichtlinie

Konfigurieren Sie eine Datenschutzrichtlinie, um anzugeben, welche Datenschutztechniken bei der Anonymisierung Ihrer Daten verwendet werden.

Vorbereitungen

Die Datenschutzkonfiguration definiert je nach Anwendungsfall Tabellen, sys_user und andere sowie Spalten, die deidentifiziert werden sollen, und gibt parametrisierte Typen der Techniken an, die beim Deidentifizieren von Daten verwendet werden sollen.

Hinweis: Um eine Datenschutzkonfiguration abzuschließen, müssen Sie zuerst eine Konfiguration der Datenschutztechnik konfigurieren. Weitere Informationen finden Sie unter Erstellen Sie eine Konfiguration der Datenschutztechnik.

Erforderliche Rolle: Data_privacy_admin und admin

Prozedur

1. Erhöhen Sie die Höhe auf **Data_privacy_admin** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
2. Navigieren zu **Systemsicherheit** > **Datenschutz (klassisch)** > **Konfiguration der Datenschutzrichtlinie**an.
3. Wählen Sie **Neu**.
4. In **Name** Geben Sie einen Namen für Ihre Konfiguration der Datenschutzrichtlinie ein.
5. In **Datenklasse** Feld die Datenklasse auswählen, die mit dieser Richtlinie verwendet werden soll.
   Datenschutzrichtlinien können nur für klassifizierte Daten gelten. Weitere Informationen zur Datenklassifizierung finden Sie unter Datenklassifizierung .
   Nachdem Sie eine Datenklasse ausgewählt haben **Techniken Für Klassifiziertes Datenschutzfeld** Und **Primäre Referenz-Links Zum Datenschutz** Listen werden im Formular angezeigt.
6. **Wahlweise:** Wählen Sie Aus **Auf alle Daten in Klasse anwenden** Dient zum Anwenden der Anonymisierung auf alle Daten in der ausgewählten Datenklasse.
   Wenn Sie dieses Feld nicht auswählen, können Ihre Datenschutzverarbeiter-Anwender auswählen, welche Anwender beim Erstellen von Datenschutzaufträgen anonymisiert werden sollen. Wenn Sie dieses Feld auswählen, ist diese Option nicht verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Beim Klonen anwenden** : Diese Option wird verfügbar. Wenn diese Option ausgewählt ist, wird die Datenschutzkonfiguration während des Klons von Datenschutz ausgeführt.
- **Anwendungsreihenfolge** : Ein Datenschutzauftrag für die PostClone-Konfiguration mit einer höheren Anwendungsreihenfolge kann vor einem anderen Auftrag mit niedrigerer Reihenfolge beginnen.

> **Wichtig:** Vermeiden Sie die Erstellung mehrerer Datenschutzrichtlinien mit derselben Anwendungsreihenfolge, da die resultierende Verarbeitungsreihenfolge für diejenigen mit derselben Reihenfolge inkonsistent ist.

7. **Wahlweise:** Wählen Sie Aus **Unterstützt Rollback** Um die Möglichkeit zu aktivieren, die Daten aus einem Datenschutzauftrag zu deanonymisieren.
   Weitere Informationen finden Sie unter Setzen Sie einen Datenschutzauftrag zurück.
   Nach Auswahl **Unterstützt Rollback** Beim Erstellen eines Datenschutzauftrags ist die Option zum Zurücksetzen des Auftrags verfügbar.
8. Wählen Sie aus **Techniken Für Klassifiziertes Datenschutzfeld** Registerkarte zum Anzeigen von **Techniken Für Klassifiziertes Datenschutzfeld** Liste.
9. Wählen Sie einen Eintrag in aus **Tabelle** Feld zum Öffnen von **Konfiguration Der Datenschutztechnik** Feld für jeden Listeneintrag.
   Die **Techniken Für Klassifiziertes Datenschutzfeld** In der Liste werden alle Daten angezeigt, die in Ihrer ausgewählten Datenklasse anonymisiert werden sollen. Für jeden dieser Einträge müssen Sie eine Datenschutztechnik auswählen, die angewendet werden soll.
10. Wählen Sie ein aus **Konfiguration Der Datenschutztechnik** Anzuwenden.

> **Wichtig:** Wenn Sie keinen Eintrag anonymisieren, wählen Sie aus **DoNothing** Technik, anstatt den Eintrag leer zu lassen. Richtlinien mit leeren Werten in **Konfiguration Der Datenschutztechnik** Feld kann nicht ausgeführt werden, wenn es in Datenschutzaufträgen verwendet wird.

11. Wählen Sie Aus **Übermitteln** Oder **Speichern** Zum Speichern des Datensatzes.

Nächste Maßnahme

Konfigurieren Sie einen Datenschutzauftrag.

Konfigurieren Sie einen Datenschutzauftrag

Konfigurieren Sie einen Datenschutzauftrag in Ihrer Produktionsinstanz, um anonymisierte Daten in Ihrer nicht-Produktionsinstanz für Anwender- und Datenklassenaufträge zu verwenden.

Vorbereitungen

Der Datenschutzauftrag unterstützt zwei Anwendungsfälle zur Deidentifizierung:

- Vertrauliche Daten bestimmter sys_users
- Vertrauliche Daten einer bestimmten Datenklasse.

Erforderliche Rolle: Data_privacy_processor und admin

Prozedur

1. Erhöhen Sie die Höhe auf **Data_Privacy_Processor** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
2. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Datenschutzauftrag**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie in der Liste Datenschutzaufträge auf **Neu** .
4. Füllen Sie die Felder des Formulars aus.

Felder für Datenschutz-Auftrag

Feld	Beschreibung
Name	Name des Jobs
Beschreibung	Beschreibung des Auftrags.
Datenschutzkonfiguration	Die für diesen Auftrag zu verwendende Konfiguration der Datenschutzrichtlinie. Weitere Informationen zu Konfigurationen der Datenschutzrichtlinie finden Sie unter Erstellen Sie eine Datenschutzrichtlinie.
Häufigkeit	○ **Einmal Ausführen** : Der Auftrag wird einmal im angegebenen Zeitfenster ausgeführt. ○ **Wöchentlich** : Der Auftrag wird jeden Tag des ausgeführt **Wochentag** Feld im angegebenen Zeitfenster. ○ **Monatlich** : Der Auftrag wird jeden Tag des Monats ausgeführt, wie in eingegeben **Tag des Monats** Feld im angegebenen Zeitfenster.
Anwender	Wählen Sie die Anwender oder Anwendergruppe aus, die in diesem Auftrag anonymisiert werden sollen. Bis zu 1000 Anwender einer Gruppe können verarbeitet werden. **Hinweis:** Dieses Feld wird nur angezeigt, wenn die ausgewählte Datenschutzrichtlinienbedingung eine Auswahl von Anwenderdatensätzen erfordert.
Probelauf	Führen Sie den Auftrag als Test aus. Bei der Ausführung dieses Auftrags sind keine Datensätze betroffen. Ergebnisse werden in angezeigt **Zusammenfassung** Feld, als ob der Auftrag ausgeführt wurde. **Hinweis:** **Probelauf** Muss deaktiviert sein, wenn ein Datenschutzauftrag mit Rollback konfiguriert wird. Details siehe Setzen Sie einen Datenschutzauftrag zurück.
Status	Status des Datenschutzauftrags: ○ **Abgeschlossen** : Auftrag erfolgreich abgeschlossen. ○ **Bereit zum Planen** : Standardstatus für neue Aufträge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Rollback wird ausgeführt** : Der Auftrag wurde so festgelegt, dass die Anonymisierung zurückgesetzt wird. ○ **Rollback abgeschlossen** : Das Rollback des Anonymisierungsauftrags wurde erfolgreich abgeschlossen. ○ **Mit Fehlern abgeschlossen** : Der Auftrag wurde abgeschlossen, weist jedoch Fehler auf. Weitere Informationen finden Sie unter Protokolle des Datenschutzauftrags. ○ **Fehler** : Auftrag wurde nicht abgeschlossen und weist einen Fehler auf. Siehe Protokolle des Datenschutzauftrags Weitere Informationen finden Sie unter Ein schreibgeschütztes Feld.
Geschätzte Anzahl der Datensätze	Die geschätzte Anzahl der Datensätze, die sich auf diese Aufgabe auswirken. Ein schreibgeschütztes Feld.
Zusammenfassung	Ein schreibgeschütztes Feld, das die Ergebnisse des Auftrags anzeigt, wenn Sie ihn ausführen.
Zeitfensterstart	Der Beginn des Zeitfensters zur Ausführung dieses Auftrags. Der Auftrag wird nach der in dieses Feld eingegebenen Zeit ausgeführt. Ein gültiger Zeitwert ist in koordinierter Weltzeit basierend auf einer 24-Stunden-Zeitnotation.
Zeitfensterende	Das Ende des Zeitfensters zur Ausführung dieses Auftrags. Der Auftrag wird vor der in dieses Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag noch nicht abgeschlossen ist, wird der Auftrag beim nächsten Start des Fensters angehalten und fortgesetzt. Die Endzeit muss nach der Startzeit liegen. Ein gültiger Zeitwert ist in koordinierter Weltzeit basierend auf einer 24-Stunden-Zeitnotation.

5. Klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie im Kontextmenü die Option **Speichern** aus.
   Nach dem Speichern des Datensatzes wird **Aufgabe Planen** Und **Auftrag Löschen** Schaltflächen werden angezeigt.
6. Klicken Sie Auf **Aufgabe Planen** Um Ihren Auftrag auszuführen.
   Der Auftrag wird zwischen den in ausgewählten Zeiten ausgeführt **Zeitfensterstart** Und **Zeitfensterende** Felder. Wenn der Auftrag während des Start- und Endzeitfensters nicht abgeschlossen wurde, wird der Auftrag beim nächsten Start des Zeitfensters fortgesetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Ein Auftrag kann nur einmal ausgeführt werden, auch wenn **Probelauf** Ist ausgewählt. Um denselben Auftrag erneut auszuführen, erstellen Sie einen Datenschutzauftrag mit denselben Feldwerten.

7. **Wahlweise:** Wählen Sie eine der folgenden Funktionen aus:
   - **Auftrag Abbrechen** : Bricht den Datenschutzauftrag ab.
   - **Anhalten** : Hält die Auftrags- und Rollback-Aufzeichnung an, wenn ein Rollback ausgewählt wurde. Nach Ablauf von drei Tagen wird für Rollback-Kontexte eine Warnmeldung angezeigt. Details siehe Setzen Sie einen Datenschutzauftrag zurück.
   - **Fortsetzen** : Startet einen angehaltenen Auftrag neu. Rollback wird für fortgesetzte Aufgaben nicht unterstützt, wenn sie angehalten werden. Brechen Sie den Auftrag ab, und erstellen Sie einen Datenschutzauftrag. Die Aufzeichnung verwendet einen nicht abgelaufenen Rollback-Kontext.

Rollback des Datenschutzauftrags

Datenbankänderungen werden für Aktionen wie Aufträge und Skripts erfasst, damit die Änderungen zurückgesetzt werden können. Setzen Sie einen Datenschutzauftrag zurück, wenn menschlicher Fehler versehentlich falsche Anwenderinformationen anonymisiert. Durch das Rollback werden die Daten aus dem Datenschutzauftrag deanonymisiert.

Übersicht

- Rollback ist auf einige Tage beschränkt, je nach konfigurierter Ablaufdauer des RollbackContext des neuen RollbackType *`REDACT`*. Nach Ablauf des RollbackContext, der einem Datenschutzauftrag zugeordnet ist, ist die Rollback-Funktion für diesen Auftrag nicht mehr verfügbar.
  - Ein Rollback-Kontext aus der de-Anonymisierung wird standardmäßig drei Tage lang gespeichert.
  - Die standardmäßige Ablaufzeit kann vom Datenschutzadministrator in auf einen Wert größer als eins festgelegt werden **RollbackContext** Des neuen **RollbackType** *`REDACT`*. Legen Sie den Wert in der Systemeigenschaft Glide fest *`glide.rollback.expiration_days_redact`*. Weitere Informationen finden Sie unter Rollback durchführen und Wiederherstellung löschen .

    Weitere Informationen zum Hinzufügen oder Erstellen einer Systemeigenschaft finden Sie unter Systemeigenschaft hinzufügen .

    Für zusätzliche Informationen.
- Rollback ist für Datenschutzaufträge verfügbar, die sich im Status „Abgeschlossen“, „Abgebrochen“ oder „Fehler“ befinden.
- Für jeden erfolgreichen sys_user-Deanonymisierungsauftrag, der mit einer Datenschutzrichtlinie mit aktivierter Rollback-Unterstützung konfiguriert ist, wird ein Rollback-Kontext erstellt. Pro Datenschutzauftrag kann maximal ein Rollback-Kontext vorhanden sein.

Setzen Sie einen Datenschutzauftrag zurück

Setzen Sie einen Datenschutzauftrag in Ihrer Instanz außerhalb der Produktion zurück, die anonymisierte Daten aus Ihrer Produktionsinstanz verwendet, auf einen Status, bevor Sie eine Datenklasse oder einen Anwenderauftrag deidentifizieren.

Vorbereitungen

Erforderliche Rolle: Data_privacy_admin oder Data_privacy_processor und admin

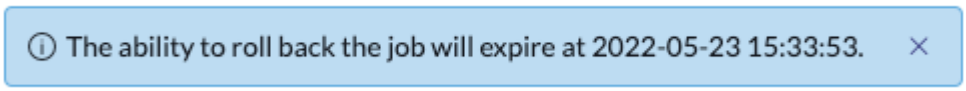
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erhöhen Sie die Höhe auf **Data_Privacy_Processor** Oder **Data_privacy_admin** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
2. Navigieren zu **Alle** > **Systemsicherheit** > **Datenschutz** > **Datenschutzauftrag**an.

   Hinweis: Im Voraus muss eine Konfiguration der Datenschutzrichtlinie erstellt werden, die das Rollback unterstützt. Erstellen Sie eine Datenschutzrichtlinie.

3. Erstellen Sie einen Datenschutzauftrag, und wählen Sie eine Datenschutzkonfiguration aus, die das Rollback unterstützt.
   Weitere Informationen finden Sie unter Konfigurieren Sie einen Datenschutzauftrag.
4. Planen Sie den Auftrag für die Datenanonymisierung.
   - Nachdem der Auftrag ausgeführt wurde, werden die Daten für die ausgewählte Konfiguration anonymisiert.
   - Im Auftrag wird eine Meldung angezeigt, die über die Ablaufzeit informiert. Innerhalb des Ablaufzeitraums können Sie den Auftrag zurücksetzen.

5. Erhöhen Sie die Höhe auf **Data_Privacy_Processor** Rolle.
6. Öffnen Sie den Datenschutzauftrag, der zurückgesetzt werden soll.
7. Wählen Sie Aus **Rollback** Zum Deanonymisieren der Daten.

Datenschutz-Klon

Wenn Kundendaten aus einer Quelle in eine Zielinstanz geklont werden, normalerweise von der Produktion in eine nicht-Produktion, werden vertrauliche Daten in der Zielinstanz deidentifiziert.

Wichtig: Dieser Abschnitt bezieht sich auf Datenschutz (Classic). Siehe Datenschutz Für die neueste aktuelle Store-Version.

Ein Datenschutzadministrator konfiguriert Richtlinien nach dem Klonen. Nachdem das Post-Klon-Skript in der Zielinstanz abgeschlossen ist, sehen die Anwender deidentifizierte Daten und haben keinen Zugriff auf die ursprünglichen Daten. Datenschutzadministratoren können Deidentifizierungsrichtlinien konfigurieren, die beim Klonen auf die Zielinstanz angewendet werden, um sicherzustellen, dass die Zielinstanz keine ursprünglichen vertraulichen Daten enthält. Für die Richtlinie wird eine Reihenfolge im Verhältnis zu anderen auszuführenden Richtlinien angegeben.

Hinweis: Das Klonen von Datenschutz ist in selbst gehosteten Instanzen nicht verfügbar.

Der Datenschutz-Klon hat die folgenden zusätzlichen Attribute:

- Das Datenschutz-Plugin erstellt das Post-Klon-Skript, das auf der Zielinstanz ausgeführt werden soll.
- Datenschutzaufträge, die für die PostClone-Konfiguration erstellt wurden, können parallel ausgeführt werden, wenn sie nicht dieselben Tabellen betreffen.
- Ein Datenschutzauftrag für die PostClone-Konfiguration mit einer höheren Anwendungsreihenfolge kann vor einem anderen Auftrag mit niedrigerer Reihenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beginnen, wenn der Auftrag mit der höheren Reihenfolge keine Tabelle enthält, die sich auf einen anderen Auftrag mit niedrigerer Reihenfolge bezieht.

- Mit dem Datenschutz-Plugin werden Datenschutztabellen standardmäßig im Tabellensatz „Datenerhalt klonen“ festgelegt.
- Beim Versuch, eine Datenschutztabelle (dp_[table]) zum Klonen von Ausschlusstabellen hinzuzufügen, wird eine Warnung angezeigt, diese Tabelle darf nicht ausgeschlossen werden.

Klonanforderung für Datenschutz konfigurieren

Die Integration des Datenschutzklons wird mithilfe eines PostClone-Skripts konfiguriert, um Datenschutzaufträge für konfigurierte Richtlinien im Ziel zu erstellen und auszuführen. Nach der Ausführung des Skripts sehen Anwender deidentifizierte Daten und haben keinen Zugriff auf die ursprünglichen Daten.

Vorbereitungen

Erforderliche Rolle: Data_privacy_clone_processor, Data_privacy_admin und admin

Prozedur

1. Aktivieren Sie das Datenschutz-Plugin (sn_dp_Store_App) in der Quellinstanz.
   Das Plugin kann nur von installiert werden Kundenservice und Support.
   Das Datenschutz-PostClone-Skript ist installiert.
2. Erhöhen Sie die Höhe auf **Data_privacy_admin** Rolle.
   Weitere Informationen zur Rollenerhöhung finden Sie unter Auf eine privilegierte Rolle hochstufen .
3. Navigieren zu **Systemsicherheit** > **Datenschutz** > **Konfiguration der Datenschutzrichtlinie**an.
4. Erstellen Sie eine Datenschutzrichtlinienkonfiguration.
   Wählen Sie Aus **Auf alle in der Datenklasse anwenden** Und **Beim Klonen anwenden** . Weitere Informationen finden Sie unter Erstellen Sie eine Datenschutzrichtlinie.
5. Sichern Sie Datenschutzkonfigurationen.
6. Senden Sie als Datenschutzadministrator eine Klonanforderung.

Ergebnis

Das Datenschutz-PostClone-Skript wird auf der Zielinstanz ausgeführt, und das PostClone-Skript erstellt einen Datenschutz-Verbundauftragsdatensatz auf der Zielinstanz.
Der Verbundauftrag erstellt und führt einen Datenschutzauftrag für jede nach dem Klonen durchgeführte Richtlinie in Anwendungsreihenfolge in der Zielinstanz aus. Die Sicherungsquelle wird in die Zielinstanz geklont. Das PostClone-Skript für Datenschutz erstellt und führt Datenschutzaufträge für konfigurierte Richtlinien in der Zielinstanz aus.

Der Prozessor für den erhöhten Datenschutz-Klon kann sich bei der Zielinstanz anmelden und den Status des verbündeten Auftrags nach dem Klonen in den Feldern dp_federated_Job.list und dp_Job.list überwachen.

Protokolle des Datenschutzauftrags

Überprüfen Sie Fehler aus Datenschutzaufträgen.

Vorbereitungen

Wichtig: Dieser Abschnitt bezieht sich auf Datenschutz (Classic). Siehe Datenschutz Für die neueste aktuelle Store-Version.

Erforderliche Rolle: Data_privacy_admin, Data_privacy_clone_processor, Data_privacy_processor, Data_privacy_Auditor

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie **Datenschutzauftragsprotokolle** Dient zum Überprüfen fehlgeschlagener Discovery-, Klassifizierungs- und Anonymisierungsaufträge.

Prozedur

1. Navigieren zu **Systemsicherheit** > **Datenschutz (Klassisch)** > **Protokolle des Datenschutzauftrags**an.
2. Überprüfen Sie die Tabelle

Tabelle „Datenschutzauftragsprotokolle“

Bezeichnung	Beschreibung
Erstellt	Wer oder was den Protokolleintrag erstellt hat
Ebene	Der Schweregrad des Fehlers
Nachricht	Beschreibung der Fehlerursache
Quelle	Plugin-Quelle des Fehlers
Typ	Der Typ des aufgetretenen Fehlers
Code	Fehlercode, der aufgetreten ist
Auftragstabellenname	Die Tabelle, in der sich der Auftrag befindet
Auftrags-ID	Die Auftrags-ID
Zieltabellenname	Tabelle, in der der Auftrag ausgeführt wird
Zieltabellenspalte	Spalte, in der der Auftrag ausgeführt wird
Zieltabellen-Datensatz	Zeichnen Sie den ausgeführten Auftrag auf

Daten-Discovery

Verwenden Daten-Discovery Dient zum Identifizieren vertraulicher Daten in einer Instanz, z. B. Kreditkarteninformationen, E-Mails oder Sozialversicherungsnummern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie Die Daten-Discovery



Erfahren Sie mehr über Daten-Discovery.

Konfigurieren Sie Die Daten-Discovery



Erhalten Sie Hilfe beim Konfigurieren der Daten-Discovery.

Rollen in Daten-Discovery



Erfahren Sie mehr über Rollen in Daten-Discovery.

Daten-Discovery-Ergebnisse



Überprüfen Sie Die Daten-Discovery-Ergebnisse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Daten-Discovery(Klassisch)

Verwenden Daten-Discovery Dient zum Identifizieren vertraulicher Daten in einer Instanz, z. B. Kreditkarteninformationen, E-Mails oder Sozialversicherungsnummern.

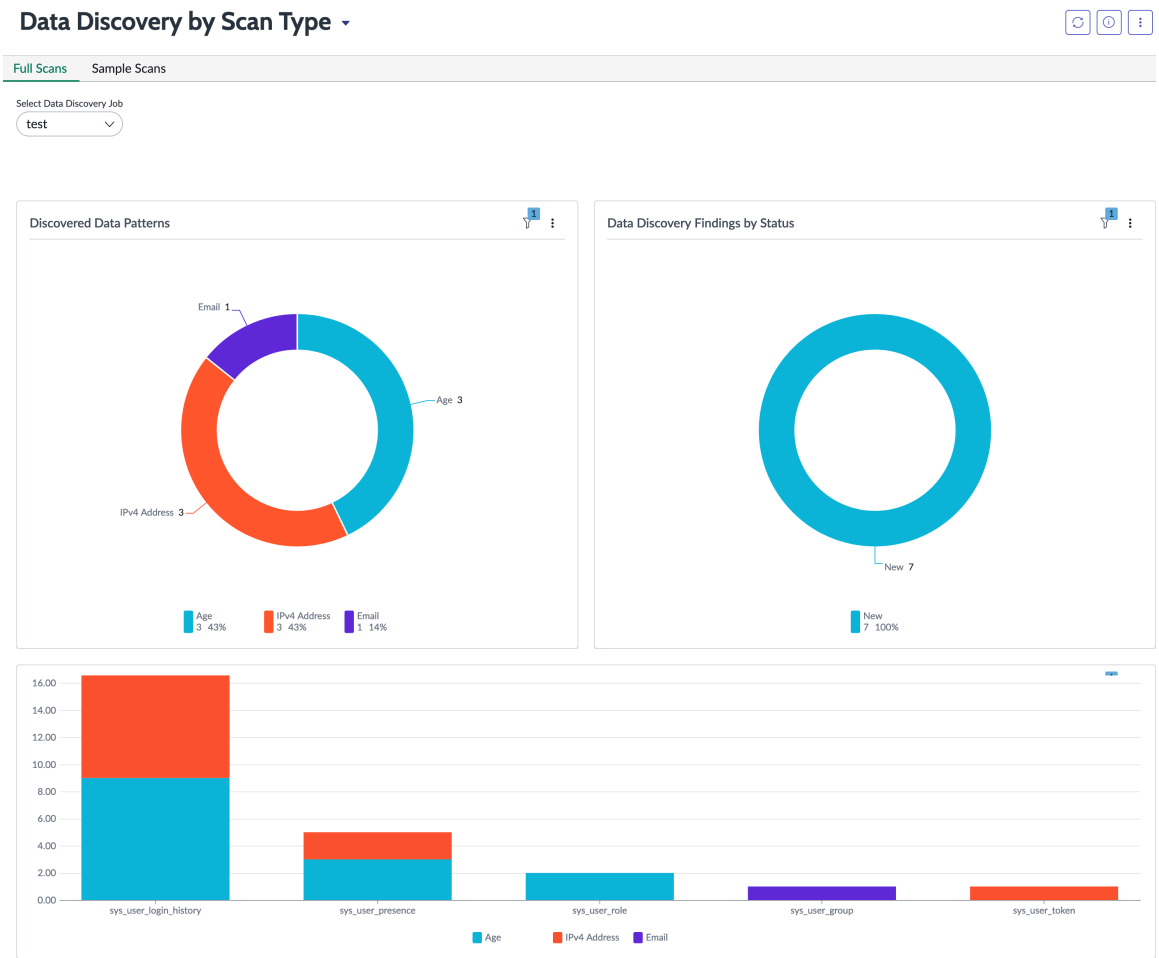
Daten-Discovery Führt einen anwenderdefinierten Satz von Aufträgen für eine Reihe von Tabellen aus. Die Aufträge suchen nach vertraulichen Informationen, und melden sie zur Überprüfung im Daten-Discovery Dashboard. Eine geplante Aufgabe verwendet automatisch alle aktiven Datenmuster und Zieltabellen, wenn sie ausgeführt wird.

Daten-Discovery Enthält auch vorab zugewiesene Rollen mit unterschiedlichen Zugriffsebenen auf Daten.

Zugriff auf das Dashboard von Daten-Discovery

Navigieren zu **Alle** > **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Dashboard** Um anzuzeigen Daten-Discovery Dashboard und zur Überprüfung Ihrer aktuellen Stellenergebnisse.

Daten-Discovery-Dashboard



Erkannte Datenmuster

Tipp: Wählen Sie einen Datensatz aus, um weitere Informationen anzuzeigen und weitere Maßnahmen für die Ergebnisse zu ergreifen. Siehe Daten-Discovery Auftragsergebnisse Für mehr.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Diagramm „erkannte Datenmuster“ zeigt die Anzahl und den Prozentsatz der derzeit erkannten Datenmuster an. Wählen Sie einen Abschnitt aus, um weitere Aktionen auszuführen.

Daten-Discovery-Ergebnisse nach Status

Das Diagramm „Daten-Discovery-Ergebnisse“ überprüft die Anzahl und den Prozentsatz der derzeit erkannten Datenmuster nach ihrem Status.

Erkannte Tabellen

Die erkannten Tabellen heben hervor, in welchen Tabellen sich derzeit erkannte Daten befinden, und ihr Datenmuster.

Spalten mit erkannten Daten

Der Abschnitt „Spalten mit erkannten Daten“ überprüft derzeit erkannte Daten anhand ihrer Spalte.

Daten-Discovery aktivieren

Die Anwendung wird installiert Daten-Discovery Und zugehörig ServiceNow® Store Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen
Die Daten-Discovery erfordert ein separates Abonnement vom Rest des ServiceNow AI Platform.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste „Alle Anwendungen“ in Ihrer Instanz aktivieren.

Hinweis:

Bevor Sie ein Abonnement kaufen, können Sie die Funktion in einer Instanz außerhalb der Produktion kostenlos testen, indem Sie sie über den Now Support Servicekatalog anfordern.

Durch die Installation der Store-App „Daten-Discovery“ wird das Plugin „Daten-Discovery-APIs“ automatisch installiert

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit der Daten-Discovery installiert:

- Rollen
- Tabellen

Weitere Informationen zu den installierten Rollen und Tabellen finden Sie unter Daten-Discovery Rollen Und Standarddatenmuster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Daten-Discovery“ (sn_Data_Discovery).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Klassifizieren Sie Daten in Daten-Discovery Seite „Ergebnisse“

Klassifizieren Sie vertrauliche Daten, die von allen erfolgreichen Aufträgen über gefunden wurden Daten-Discovery Ergebnisse.

Vorbereitungen

Erforderliche Rollen: Data_Discovery_admin

Ein Auftrag muss eine erfolgreiche Ausführung abschließen, bevor Ergebnisdaten als klassifiziert erscheinen können.

Warum und wann dieser Vorgang ausgeführt wird

Die Daten-Discovery Die Seite „Ergebnisse“ zeigt alle Dateneinträge an, die von einem Auftrag gefunden wurden. Auf der Seite „Ergebnisse“ können Sie die Einträge überprüfen und einer Klassifizierung zuordnen.

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery (Klassisch)** > **Daten-Discovery-Ergebnisse**an.
2. Wählen Sie den Eintrag aus, den Sie klassifizieren möchten.
3. In Daten-Discovery Liste „Ergebnisse“ auswählen **Klassifizieren** .
4. Wählen Sie die Datenklassen aus, die Sie den Tabelleneinträgen zuordnen möchten.
5. Wählen Sie Aus **Klassifizieren** .

Daten-Discovery Aufträge

Daten-Discovery Überprüft Ihre Zielinformationen mithilfe anwenderdefinierter Datenmuster und Zieltabellen.

Daten-Discovery Funktioniert, indem zuerst eine Aufgabe in geplant wird **Daten-Discovery-Auftrag** Abschnitt. Wenn eine geplante Aufgabe ausgeführt wird, werden alle aktiven Datenmuster in den aktuellen Zieltabellen gesucht. Weitere Informationen zum Erstellen und Konfigurieren von Daten-Discovery Auftrag, siehe Konfigurieren Sie ein Daten-Discovery Auftrag.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Beispiel-Scan-Aufträge – Scan bis zu 10.000 Datensätze werden pro Tabelle und Muster gescannt.

Warnung: Wenn ein Auftrag zweimal in kurzer Zeit ausgeführt wird, kann die Anzahl der gescannten Zeilen für die zweite Ausführung 0 zurückgeben.

Daten-Discovery Datenmuster

Die **Datenmuster** Der Abschnitt zeigt alle aktuellen Datenmuster an, sowohl aktiv als auch inaktiv. Ein Datenmuster ist ein regulärer Ausdruck, der zum Abgleichen vertraulicher Daten verwendet wird. Weitere Informationen zum Zugriff auf Datenmuster und zum Konfigurieren dieser Muster finden Sie unter Konfigurieren Daten-Discovery Muster. Die **Aktive Datenmuster** Abschnitt zeigt nur aktive Muster an. Inaktive Muster werden nicht angezeigt.

Zieltabellen

Die **Zieltabellen** Abschnitt listet alle Tabellen auf, die für einen Auftrag verarbeitet werden können. Um auf die Zieltabellen zuzugreifen, wählen Sie aus **Zieltabellen** .

Die folgenden Tabellen werden nicht unterstützt:

- sr
- Sysx
- v
- sh$
- syslog
- ua
- UsageAnalytics
- ecc
- Klon
- Jrobin
- PA
- sla_Repair_log
- Scan
- gcf
- fm_log
- log
- np$
- sn_data_discovery
- dp_Configuration
- dp_Federated_Job
- dp_Field_technique
- dp_Job
- dp_Job_Summary
- dp_primary_reference

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- dp_technique
- Data_classification
- m2m_dictionary_dataclass

Granulare Konfiguration

Die Granulare Konfiguration Das Tool ermöglicht spezifischere und fein abgestimmte Steuerungen für die Erkennung vertraulicher Daten in einer Tabelle. Es gibt jedoch wichtige Unterschiede in seinem Betrieb im Vergleich zu einem herkömmlichen Daten-Discovery-Auftrag. Eine granulare Konfiguration scannt nur die angegebenen Spalten einer Tabelle für die Discovery und meldet ihre Ergebnisse nach dem Datensatz. Für Ergebnisse aus dem Scan von granularen Konfigurationen, als granulare Ergebnisse bezeichnet, sind ihre Aktionen pro Datensatz angegeben und die Rolle „Data_privacy_admin“ muss anonymisiert werden.

Konfigurieren Sie ein Daten-Discovery Auftrag

Konfigurieren Sie ein Daten-Discovery Auftrag und Status laufender Aufträge überprüfen. A Daten-Discovery Auftrag definiert, wann ein Muster in einer Zieltabelle ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: Data_Discovery_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery (Klassisch)** > **Daten-Discovery-Auftrag**an.
2. In Daten-Discovery Auftragsliste, wählen Sie aus **Neu** .
3. Auf der Daten-Discovery Formular „Auftragsfelder“: Füllen Sie die Felder aus.

Daten-Discovery Auftragsfelder

Feld	Beschreibung
Name	Name des Jobs
Beschreibung	Beschreibung des Auftrags.
Scantyp	Anzahl der zu scannenden Einträge. Mögliche status: ○ **Beispiel** : Scannt 10.000 Einträge. ○ **Inkrementell** : Scannt nach Mustern vertraulicher Daten in neuen oder geänderten Datensätzen. Dieser Scan-Typ ist wiederkehrend. ○ **Voll** : Scannt alle Einträge.
Richtlinie	Die in diesem Auftrag zu verwendende Daten-Discovery-Richtlinie. Weitere Informationen finden Sie unter Daten-Discovery-Richtlinien.
Anhänge scannen	Scannt Anhänge nach Mustern für vertrauliche Daten. Bilder, die unter PDF- oder DOC-Dateien eingebettet sind, werden nicht auf vertrauliche Daten gescannt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Warnung: Diese Funktion erfordert das Senden Ihrer Daten an eine kontrollierte ServiceNow-Umgebung. Bestätigen Sie vor der Aktivierung, dass Sie den zusätzlichen Nutzungsbedingungen für die Verwendung dieser Funktion zugestimmt haben.
Kontext	Auftragsdetails zu gescannten Mustern, Treffer in Zieltabellen und verstrichene Zeit.
Status	Status von Daten-Discovery Auftrag. Mögliche status: ○ **Bereit zum Planen** : Standardstatus für neue Aufträge. ○ **Geplant** : Die Ausführung der Aufgabe ist geplant. ○ **In Bearbeitung** : Auftrag wird aktiv ausgeführt. ○ **Abgeschlossen** : Auftrag wurde erfolgreich ausgeführt. ○ **Fehler** : Die Ausführung des Auftrags wurde aufgrund eines Fehlers angehalten. ○ **Abgebrochen** : Der Auftrag wurde abgebrochen. ○ **Angehalten** : Der Auftrag wurde angehalten.
Zusammenfassung	Zeigt die Ergebnisse des Auftrags an, nachdem Sie ihn ausgeführt haben.
Startdatum	Legt das Startdatum für den Auftrag fest.
Zeitfensterstart	Der Beginn des Zeitfensters zur Ausführung dieses Auftrags. Der Auftrag wird nach der in dieses Feld eingegebenen Zeit ausgeführt. Die in eingegebene Zeit **Zeitfensterstart** Das Feld muss vor der in eingegebenen Zeit erfolgen **Zeitfensterende** Feld. **Hinweis:** Ein gültiger Zeitwert ist in koordinierter Weltzeit basierend auf einer 24-Stunden-Zeitnotation.
Zeitfensterende	Das Ende des Zeitfensters zur Ausführung dieses Auftrags. Der Auftrag wird bis zu der in dieses Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag dieses Mal nicht abgeschlossen ist, wird der Auftrag angehalten und beim nächsten Start des Fensters fortgesetzt. Die in eingegebene Zeit **Zeitfensterende** Das Feld muss nach der in eingegebenen Zeit erfolgen **Zeitfensterstart** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Ein gültiger Zeitwert ist in koordinierter Weltzeit basierend auf einer 24-Stunden-Zeitnotation.

4. Wählen Sie **Absenden**.
   Die **Aufgabe Planen** Und **Aktualisieren** Schaltflächen werden angezeigt.
5. Wählen Sie Aus **Aufgabe Planen** Um Ihren Auftrag auszuführen.
   Der Auftrag wird zwischen den in ausgewählten Zeiten ausgeführt **Zeitfensterstart** Und **Zeitfensterende** Felder. Wenn der Auftrag während des Start- und Endzeitfensters nicht abgeschlossen wurde, wird der Auftrag beim nächsten Start des Zeitfensters fortgesetzt.
6. **Wahlweise:** Wählen Sie eine der folgenden Funktionen aus:
   - **Auftrag Abbrechen** : Bricht den Auftrag ab.
   - **Anhalten** : Hält den Auftrag an.
   - **Fortsetzen** : Startet einen angehaltenen Auftrag neu.

Anhang wird gescannt Daten-Discovery Aufträge

Anhang wird gescannt Daten-Discovery Ermöglicht Ihnen das Scannen, Erkennen und Berichten über vertrauliche Daten in Dateianhängen.

Sensible Daten wie Sozialversicherungsnummern, Kreditkartennummern und andere personenbezogene Daten sind häufig in Dateianhängen enthalten. Daten-Discovery Beauftragt das Scannen von Anhängen, ermöglicht Ihnen das Erkennen und Melden vertraulicher Daten in bestimmten Anhängen.die Funktion zum Scannen von Anhängen ist nur für geplante Scans verfügbar.

Warnung: Diese Funktion erfordert das Senden Ihrer Daten an eine kontrollierte ServiceNow-Umgebung. Wenden Sie sich an Ihren Account und Ihre Supportteams, um die Funktion zum Scannen von Anhängen zu aktivieren

Einschränkungen

- Eingebettete Bilder und Anhänge in PDF- und Dokumentdateien werden nicht auf vertrauliche Daten gescannt.
- Dateien müssen kleiner als 10 MB sein.
- Support ist für die folgenden Dateitypen verfügbar:
  - PDF
  - DOKUMENT (X)
  - TXT
  - XLS
  - CSV

Konfigurieren Daten-Discovery Muster

Konfigurieren Sie ein Daten-Discovery Muster erstellen und aktuelle Muster überprüfen. A Daten-Discovery Muster definiert den regulären Ausdruck, der zum Abgleichen von Daten mit einer Zieltabelle verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Data_Discovery_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Daten-Discovery** > **Alle Datenmuster**an.
2. In Daten-Discovery Musterliste auswählen **Neu** .
3. In Daten-Discovery Formular „Auftragsfelder“: Füllen Sie die Felder aus.

Daten-Discovery Auftragsfelder

Feld	Beschreibung
Interner Umfang	Umfang des Musters.
Beschreibung	Beschreibung des Auftrags.
Name	Name des Datenmusters.
Anwendung	Anwendungsbereich des Musters.
Ausdruck	Regulärer Ausdruck, der zum Erkennen des Datenmusters verwendet wird. **Hinweis:** Die Ausdruckslänge muss weniger als 1000 Zeichen betragen.
Stichwort (Optional)	Ein bestimmtes Wort (oder Wörter, die durch Kommas getrennt sind), nach dem um einen Ausdruck gesucht werden soll. Muss mit verwendet werden **Stichwortnähe** **Hinweis:** Ein Stichwort kann verwendet werden, um nach zusätzlichem Kontext für ein Muster zu suchen. Beispielsweise kann die Verwendung eines Stichworts helfen, zwischen einem Geburtsdatum und einem Einstellungsdatum zu unterscheiden, wenn sie dieselbe Formatierung FÜR MM/TT/JJ aufweisen.
Stichwort-Nähe (Optional)	Wie weit der Ausdruck entfernt ist, um nach Stichwörtern zu suchen. Muss mit verwendet werden **Stichwort** **Hinweis:** Der Standardwert ist 30, der obere Grenzwert von 64
Konfiguration der Datenschutztechnik	Für das Muster verwendete Datenschutztechnik
Synthetic-Wert	Liste der Werte, die für die Muster ersetzt werden
Typ	Typ des Musters ○ **Lokal** : Das Muster basiert auf dem regulären Ausdruck ○ **Modell** : Verwendet KI/ML-Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Absenden**.
   - Die **Testen** Mit der Schaltfläche können Sie Ihren regulären Ausdruck testen, bevor Sie die Datenmusterliste übermitteln.

Das Datenmuster muss als aktiv festgelegt werden, um mit geplanten Aufgaben verwendet werden zu können.

5. Navigieren zu **Systemsicherheit** > **Daten-Discovery** > **Aktive Datenmuster**an.
6. In Daten-Discovery Liste „aktive Muster“ auswählen **Bearbeiten** .
7. Wählen Sie die Musterliste aus **Verfügbare Listen** Und verschieben Sie sie nach **Ausgewählte Listen** .

Standarddatenmuster

Überprüfen Sie die regulären Ausdrücke des Standarddatenmusters, die in enthalten sind Daten-Discovery. Diese Standarddatenmuster können verwendet werden, um Tabelleneinträge für eine weitere Klassifizierung zu filtern.

Im Folgenden sind Standardmuster für die Daten-Discovery verfügbar.

Name	Beschreibung	Regulärer Ausdruck	Stichwörter	Beispiele
Alter	Alter einer Person zwischen 0-99	\B([0-9]|[1-9][0-9]|1[012][0-9])\b	age	**Übereinstimmung** 24 **Nicht übereinstimmend** • 103 • -2
Geburtsdatum	Geburtsdatum im Format TT/MM/JJJJ	\B[0-3]?[0-9]/[0-3]?[0-9]/(?:[0-9]{2})?[0-9]{2}\b	geburtsdatum, Geburtstag, Geburtsdatum	**Übereinstimmung** • 06/18/2012 • 1/1/19
E-Mail	Standard-E-Mail-Adresse	\B[\W!#$%&'*+/=?`{\|}~^]+(?:\.[\W!#$%&'*+/=?`{|}~^-]+)*@(?:[A-ZA-Z0-9-]+\.)+[a-ZA-Z]{2,6}\b		**Übereinstimmung** • johndoe@emailserver.com • historyprofessor@college **Nicht übereinstimmend** • notanemail.com • Bademail@.org
Fahrzeugidentifizierungsnummer (VIN)	Eine Fahrzeugidentifizierungsnummer	\B[A-HJ-NPR-Z0-9]{17}\b		**Übereinstimmung** AHUYA31581L000000
IP-Adresse	Standard-IP-Adresse	**4-stellige IP** \B(?:(?:25[0-5]|2[0-4]		**Übereinstimmende 4-stellige IP** 102.28.46.103

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Regulärer Ausdruck	Stichwörter	Beispiele
		[0-9]| [01]? [0-9] [0-9]?)\.) {3} (?:25[0-5]| 2[0-4] [0-9]| [01]? [0-9] [0-9] [0-9]?)\b **6-stellige IP** \B((?: [0-9A-Fa-f] {1,4} (?: [0-9A-Fa-f] {1,4})*)?: (?: [0-9A-Fa-f] {1,4} (?:: [0-9A-Fa-f] {1,4})*))| (?: [0-9A-FA-F] {1,4} {7} 1,4		**Übereinstimmende 6-stellige IP** 914b:d45a:61ea:6346:59bc:3085
Kreditkarte: Visa	Visa-Kreditkartennummer	\b4[0-9]{12}(?:[0-9]{3})?\b		**Übereinstimmung** 4444434342424242
Kreditkarte: American Express	American Express-Kreditkartennummer	\b3[47][0–9]{13}\b		**Übereinstimmung** 378225246366005
Kreditkarte: Mastercard	Mastercard-Kreditkartennummer	\B(?:5[1-5][0-9]{2}| 222[1-9]|22[3-9] [0-9]|2[3-6][0-9] {2}|27[01][0-9]| 2720)[0-9]{12}\b		**Übereinstimmung** 5555444455554444
Kreditkarte: Diners Club	Diners Club-Kreditkartennummer	\b3(?:0[0-5]|[68] [0-9])[0-9]{11}\b		**Übereinstimmung** 3056930009020004
Kreditkarte: Erkennen	Discovery-Kreditkartennummer	\b6(?:011|5[0-9] {2})[0-9]{12}\b		**Übereinstimmung** 6011025690875424

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Regulärer Ausdruck	Stichwörter	Beispiele
Kreditkarte: CCV	Sicherheitsnummer der Kreditkarte	\B[0–9]{3,4}\b	cvv, Verifizierungscode, Sicherheitscode	**Übereinstimmung** 124
Kreditkarte: Ablaufdatum	Ablauf der Kreditkarte im Format MM/JJJJ	\B([1-9])|(0[1-9]|1[0-2])\/?([0-9]{4}|[0-9]{2})\b	Ablauf, exp	**Übereinstimmung** • 02/2027 • 04/23 **Nicht übereinstimmend** 03/9
USA: Sozialversicherungsnummer	Sozialversicherungsnummer der US-Bürger	\B(?!666|000|9\d{2})\d{3}-(?!00)\d{2}-(?!0{4})\d{4}\b		**Übereinstimmung** 001-22-111
USA: Telefonnummer	Telefonnummer (USA) **⚠ Warnung:** Verwendet nicht die US-Telefonvorwahl.	\B\(?([0-9]{3})\)?[-.]?([0-9]{3})[-.]?([0-9]{4})\b		**Übereinstimmung** 2065550199 **Nicht übereinstimmend** 1 555 238 0199
USA: Reisepassnummer	9-stellige US-Reisepassnummer	\B[a-ZA-Z0-9]\\d{8}\b		**Übereinstimmung** 770022122
USA: Steuernummer	Steuernummer des US-Steuerzahlers	\B(9\d{2})([\-]?)([7]\d|8[0-8])([\-]?)(\d{4})\b		**Übereinstimmung** 927 70 5828
USA: California State Führerscheinnummer	Führerscheinnummer des Bundesstaats Kalifornien, USA	\B[a-ZA-Z]\d{7}\b		**Übereinstimmung** A0002144
USA: Bankleitzahl	Nummer der US-Bankweiterleitung (ABA)	\B((0[0-9])|(1[0-2])|(2[1-9])|(3[0-2])|(6[1-9])|(7[0-2])|80)([0-9]{7})\b		**Übereinstimmung** 125210305

Konfigurieren Daten-DiscoveryZieltabelle

Fügen Sie Zieltabellen hinzu, die in verwendet werden sollen Daten-DiscoveryAufträge. Nur Zieltabellen werden auf Datenmuster gescannt.

Vorbereitungen
Erforderliche Rolle: Data_Discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Daten-DiscoveryAuftrag wird ausgeführt. Er wird für alle Zieltabellen mit allen aktiven Mustern ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Auswahlvorgang **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Zieltabellen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie Ihre Zieltabelle in aus **Tabellenname** Feld.
4. Wählen Sie **Absenden**.

Aktivieren Sie parallele Aufträge für Daten-Discovery

Verwenden Sie parallele Aufträge, um Ihre zu reduzieren Daten-Discovery Ausführungszeit des Auftrags.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur
Standardmäßig Daten-Discovery Führt Aufträge mit einem einzelnen Thread aus. Für können mehrere Threads aktiviert werden Daten-Discovery Vollständige Scans.

1. Geben Sie im Navigationsfilter ein `sys_properties.list` .
2. Erstellen Sie die Eigenschaft `Com.Glide.Data_Discovery.max_concurrent_item_Worker`
3. Verifizieren Sie **Typ** Ist Ganzzahl .
4. **Wichtig:** Es wird empfohlen, mit einer kleinen Anzahl von Mitarbeitern pro Knoten (2 oder 3) zu beginnen.

   Geben Sie die Anzahl der parallelen Job Worker in ein **Wert** Feld bis zu 5.

Daten-Discovery Rollen

Sie können zuweisen Daten-Discovery Rollen, um den Anwenderzugriff auf bestimmte Datentypen zu beschränken.

Daten-Discovery-Administrator [sn_Data_Discovery.Data_Discovery_admin]

Datenmuster und zugehörige Aufträge anzeigen, erstellen und ändern.

- Datenmuster:
  - Erstellen
  - Lesen
  - Aktualisieren
  - Löschen
- Aktive Datenmuster:
  - Löschen
  - Lesen
- Aufträge:
  - Erstellen
  - Lesen
  - Aktualisieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Löschen
- Zeitplan
- Pause
- Fortfahren
- Abbrechen

- Zieltabellen:
  - Erstellen
  - Lesen
  - Schreiben
- Granulare Konfiguration:
  - Erstellen
  - Lesen
  - Aktualisieren
  - Löschen
- Granulare Ergebnisse:
  - Erstellen
  - Lesen
  - Aktionen

Hinweis: Anwender mit dieser Rolle dürfen nur die Aktion „Ignorieren“ ausführen

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

- Data_classification_Auditor
- Data_classification_admin
- sn_Data_Discovery.Data_Discovery_api_Processor

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Administratoren wird diese Rolle bei der Produktinstallation automatisch zugewiesen.

Hinweis: Vermeiden Sie die Gewährung einer Administratorrolle, wenn speziellere Rollen verfügbar sind.

Auditor für Datenerkennung [sn_Data_Discovery.Data_Discovery_Auditor]

Lesen Sie Datenmuster und Zieltabellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datenmuster lesen
- Aktive Datenmuster lesen
- Lesen Daten-Discovery Aufträge
- Zieltabellen lesen
- Überprüfen Sie die granulare Konfiguration
- Überprüfen Sie die granularen Ergebnisse

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Keine.

Datenklassifizierungsadministrator [Data_classification_admin]

Lesen Sie Datenmuster, Discovery-Aufträge und die Tabelle „Data_classification“, wenn ein aktiviertes bestimmtes Musterergebnis klassifiziert wird.

Enthält Rollen

Die Rolle „Datenklassifizierung“ enthält die Liste der Rollen, die in der Rolle „Data_classification_Auditor“ enthalten sind.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Hinweis: Weitere Informationen zur Administratorrolle „Datenklassifizierung“ finden Sie unter Wird Installiert Datenklassifizierung Plugin-Demodaten.

Daten-Discovery Auftragsergebnisse

Die Daten-Discovery Die Seite „Ergebnisse“ zeigt Details zu den von einem Auftrag gefundenen Daten an. Sie können die Seite „Ergebnisse“ verwenden, um die Ergebnisse eines Auftrags zu überprüfen und mit der Klassifizierung von Daten zu beginnen.

Die Daten-Discovery Die Seite „Ergebnisse“ zeigt die folgenden Details nach einem abgeschlossenen Auftrag an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Wörterbucheintrag	Spalte der Zieltabelle, in der sich die Daten befanden
Tabelle	Zieltabelle, in der die Daten gefunden wurden
Datenmuster	Datenmuster, das zum Suchen der Daten verwendet wird
Anzahl der Übereinstimmungen von Datenmustern	Anzahl der Dateneinträge, die dem Datenmuster entsprechen
Gesamtanzahl der Zeilenscans	Anzahl der während des Auftrags gescannten Zeilen
Prozentsatz der übereinstimmenden Zeilen	Prozentsatz der Zeilen in der Zieltabelle, die dem Datenmuster entsprechen
Daten-Discovery Auftrag	In der Zieltabelle verwendeter Auftrag
Status	Status des Eintrags

Nachdem Sie ausgeführt haben Daten-Discovery Auftrag, die Ergebnisse haben den Status Neu. Wenn keine Aktion erforderlich ist, können Sie die Daten in Ruhe lassen, wodurch der Status automatisch auf „ignoriert“ gesetzt wird. Andernfalls können Sie die Daten klassifizieren, z. B. indem Sie anwenderdefinierte Datenklassifizierungen erstellen, um die Datenanonymisierung mit vorzubereiten Datenklassifizierung Tool.

Granulare Ergebnisse

Anwender können auswählen **Verfolgen Sie Granulare Ergebnisse** Aktion zur Verwendung von Granulare Ergebnisse Seite, um Aktionen für bestimmte erkannte Datensätze auszuführen. Weitere Informationen finden Sie unter Granulare Ergebnisse.

Verfügbare Schutzmaßnahmen

Wählen Sie aus **Verfügbare Schutzmaßnahmen** Schaltfläche zum Überprüfen von Einträgen, die den Service, den Status, die Notizen und das letzte Einchecken steuern. Ab Xanadu Diese Funktion unterstützt nur Feldverschlüsselung.

Auf Protecton-Services kann auch über das Dashboard zugegriffen werden. Weitere Informationen zum Dashboard finden Sie unter . Daten-Discovery.

Konsolidieren Sie Ergebnisse

Auftragsergebnisse können mit konsolidiert werden **Konsolidieren Sie Ergebnisse** Schaltfläche. Auftragsergebnisse, die von zwei separaten Aufträgen geteilt werden, werden dann unter dem zuletzt ausgeführten Auftrag konsolidiert.

Hinweis: Nur abgeschlossene vollständige Scanaufträge können konsolidiert werden

Klassifizieren Sie Daten in Daten-Discovery Seite „Auftragsergebnisse“

Klassifizieren Sie Daten in Daten-Discovery Direkt über die Ergebnisseite eines Auftrags.

Vorbereitungen
Erforderliche Rolle: Data_Discovery_admin und admin

Ein Auftrag muss eine erfolgreiche Ausführung abschließen, bevor Ergebnisdaten als klassifiziert erscheinen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Gehe zu **Systemsicherheit** > **Daten-Discovery** > **Daten-Discovery-Auftrag**an.
2. Wählen Sie den Eintrag aus, den Sie klassifizieren möchten.
3. In Daten-Discovery Liste „Ergebnisse“ auswählen **Klassifizieren** .
4. Wählen Sie die Datenklassifizierungen aus, die Sie den Tabelleneinträgen zuordnen möchten.
5. Wählen Sie Aus **Klassifizieren** .

Daten-Discovery Unterstützte Datentypen

Überprüfen Sie, welche Feldtypen bei Verwendung von unterstützt werden Daten-Discovery.

Hinweis: Nicht alle Feldtypen, die klassifiziert wurden, sind für verfügbar Daten-Discovery.

Einige Feldtypen mit hohem Risiko sind standardmäßig deaktiviert, wie in der Tabelle beschrieben. Weitere Informationen zu Feldern finden Sie unter Feldtypen .

Unterstützte Feldtypen für die Daten-Discovery

Feldtyp	Standardmäßig verfügbar
Audio	Nein
Bedingung	Nein
Bedingungszeichenfolge	Nein
currency	Ja
Dezimalzahl	Ja
due_date	Ja
Gleitkommazahl	Ja
glide_date	Ja
Glide_date_time	Ja
Glide_duration	Nein
Glide_time	Ja
HTML	Nein
icon	Nein
Ganzzahl	Ja
ip_addr	Nein
ip_address	Nein
Journal	Ja
journal_input	Ja
journal_list	Ja
Lang	Ja
Name_Werte	Nein
percent_complete	Nein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldtyp	Standardmäßig verfügbar
Phone_NUMBER_e164	Ja
Preis	Ja
Zeichenfolge	Ja
String_Full_utf8	Ja
Übersetzt_html	Nein
Übersetzt_Text	Nein
URL	Nein
user_image	Nein
Video	Nein
Wiki_Text	Nein

Scannen mit granularer Konfiguration

Granularer Scan kann verwendet werden, um bestimmte Tabellenspalten für Discovery zu scannen. Traditionell Daten-Discovery Aufträge scannen die gesamte Tabelle, um Daten zu erkennen, während granulare Scans bestimmte Spalten der Tabelle anvisiert und dadurch mehr Kontrolle über den Discovery-Prozess bietet

Vorbereitungen

Erforderliche Rolle: admin, sn_Data_Discovery_admin, Data_privacy_admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Daten-Discovery (Klassisch)** > **Granulare Konfiguration**an.
2. In **Granulare Konfigurationen** Liste, wählen Sie aus **Neu** .
3. In **Granulare Konfiguration** Füllen Sie die Felder aus.

Granulare Konfigurationsfelder

Feld	Beschreibung
Wörterbucheintrag	Zu scannende Spalte.
Tabelle	Zu scannende Tabelle.
Spaltenbezeichnung	Bezeichnung der zu scannenden Spalte
Startpunkt des Scans	Vertrauliche Daten werden nur für den Tag und nach dem Scan-Startpunkt erkannt. **Hinweis:** Wenn der Scan-Startpunkt leer gelassen wird, werden alle Einträge in der Spalte gescannt. Wenn der Scan-Startpunkt geändert wird, wird der Scan zurückgesetzt, um mit dem neu konfigurierten Zeitstempel zu beginnen.
Aktiv	Aktivieren Sie diese Option, um die granulare Konfiguration zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Absenden**.
   Untergeordnete Elemente erweiterbarer Tabellen können für die Konfiguration ausgewählt werden.
5. **Wahlweise:** Wählen Sie die granulare Konfiguration für die übergeordnete Tabelle aus **Wählen Sie Untergeordnete Tabellen Aus** Und wählen Sie untergeordnete Tabellen zum Scannen aus.

Ergebnis

Die spezifische Spalte der Zieltabelle wird für Discovery gescannt. Granularer Scan verwendet Datenmuster Von **Aktive Datenmuster** . Sie können die Ergebnisse überprüfen und unter Maßnahmen ergreifen **Alle** > **Systemsicherheit** > **Daten-Discovery (Klassisch)** > **Granulare Ergebnisse**an. Weitere Informationen finden Sie unter Granulare Ergebnisse.

Granulare Ergebnisse

Granulare Ergebnisse können mit dem Tool granulare Ergebnisse überprüft werden.

Granulare Ergebnisse Werden Überprüft

Granulare Ergebnisse Wird verwendet, um bis zu 500 Ergebnisse von zu überprüfen Granulare Konfigurationen . Bei 500 Ergebnissen wird das Scannen granularer Konfigurationen angehalten, bis eine Aktion ausgeführt wird.

Spaltenbezeichnung	Beschreibung
Datensatz	Erkannter Datensatz.
Tabelle	Übergeordnete Tabelle des Datensatzes.
Spalte	Spalte des Datensatzes, in dem vertrauliche Informationen erkannt wurden.
Datenmuster	Muster, das zum Erkennen des Datensatzes verwendet wird.
Aktion	Aktion für Ergebnisse. Zum Ändern auswählen **Wichtig:** Die Rolle Data_privacy_admin ist erforderlich, um die Aktion Anonymisieren für einen Datensatz auszuführen. **Prüfung** Die Überprüfung des Datensatzes steht aus. Dies wird neuen granularen Erkennungen zugewiesen. **Ignorieren** Für den Datensatz wird keine Aktion ausgeführt **Anonymisieren** Datensatz wird anonymisiert.
Status	Status des Datensatzes. **Neu** Status, der dem Ergebnis zugewiesen ist, wenn es erstmals gemeldet wird **Verarbeitet**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spaltenbezeichnung	Beschreibung
	Wenn die vom Anwender ausgewählte Aktion erfolgreich auf das Ergebnis angewendet wurde **Hinweis:** Verarbeitete Ergebnisse werden vor dem Löschen 3 Tage lang in der Tabelle „granulare Ergebnisse“ gespeichert **Manuelle Überprüfung** Beim Anwenden der vom Anwender ausgewählten Aktion ist ein Fehler aufgetreten. **Warnung:** Ergebnisse in der manuellen Überprüfung sollten von Anwendern gelöscht werden, nachdem sie entsprechende Aktionen ergriffen haben.

Warnung: Rollback wird für die Anonymisierung, die durch granulare Ergebnisse ausgelöst wird, nicht unterstützt.

Kontextbasierte Discovery

Verwenden Sie die kontextbasierte Discovery, um vertrauliche Daten zu erkennen, die keinen festen Mustern folgen.

Daten-Discovery unterstützt die Verwendung eines Modells für benannte Entitäten (NER) Um Daten wie Namen, Organisationen, Nationalitäten und politische Zugehörigkeiten zu erkennen. Datenmuster mit dem Typ **Modell** Verwenden Sie diese Funktion, siehe Mustertyp in Konfigurieren Daten-Discovery Muster Für weitere Details.

Warnung: Diese Funktion erfordert eine Lizenzprüfung vom Kunden, bevor sie aktiviert wird.

Die KI-modellbasierte Discovery unterstützt standardmäßig 5 Muster.

Kontextbezogene Discovery-Muster

Muster	Beschreibung	Beispieltext	Übereinstimmender Text
Person	Der Name der Person(n)	John Doe kam auf einen Kaffee vorbei.	Max Mustermann
Nationalität, religiöse oder politische Gruppen (NRPs)	Nationale, religiöse und politische Zugehörigkeit.	Er war Amerikaner.	Amerikanisch
Standort	Adressen oder Standortinformationen	Er war in New York	New York
Date_Time	Daten- und Uhrzeitinformationen	Er kam heute um 9:30 Uhr.	Heute 9:30 Uhr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontextbezogene Discovery-Muster (Fortsetzung)

Muster	Beschreibung	Beispieltext	Übereinstimmender Text
Organisation	Organisationsnamen	Er arbeitet bei ServiceNow.	ServiceNow

Hinweis: Die KI-modellbasierte Discovery unterstützt nur Englisch für die Verwendung mit Anonymisierung in Echtzeit(RTA) für Tabellen und Datenkit-Kanal .

Daten-Discovery-Richtlinien

Verwenden Daten-Discovery Richtlinien zum Scannen bestimmter Tabellen und Aktivieren spaltenbasierter Aufträge.

Daten-Discovery Mit Richtlinien können Sie feingranulierte Kontrolle über die Definition bestimmter Datenmuster, Tabellen und Spalten haben, die in einen Auftrag aufgenommen werden sollen. Darüber hinaus können Sie mithilfe von Richtlinien mehrere Discovery-Auftragseinstellungen gleichzeitig erstellen, anstatt eine globale Konfiguration. Sie können Ihren überprüfen Daten-Discovery Richtlinien, indem Sie zu navigieren **Alle** > **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Daten-Discovery-Richtlinien**an.

Hinweis: Wenn für eine Richtlinie keine Spalten ausgewählt sind, werden alle Spalten der Zieltabelle gescannt

Siehe Erstellen Sie einen Daten-Discovery Richtlinie Um zu erfahren, wie Sie einen erstellen Daten-Discovery Richtlinie.

Erstellen Sie einen Daten-Discovery Richtlinie

Erstellen Sie einen Daten-Discovery Richtlinie für granulare Kontrolle über Ihren Daten-Discovery Aufträge.

Vorbereitungen

Erforderliche Rolle: admin, sn_Data_Discovery_admin, Data_privacy_admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Daten-Discovery (klassisch)** > **Daten-Discovery-Richtlinien**an.
2. Wählen Sie aus **Neu** Schaltfläche.
3. Füllen Sie das Formular aus.

Daten-Discovery-Richtlinie

Bezeichnung	Beschreibung
Name	Name der Richtlinie
Zielspalte(n)	Wählen Sie die Zielspalten aus, die in der Richtlinie verwendet werden sollen **Hinweis:** Wenn keine Spalten ausgewählt sind, werden alle Spalten der Zieltabelle gescannt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Beschreibung
Zieltabelle	Wählen Sie die Zieltabelle aus, die in der Richtlinie verwendet werden soll
Aktiv	Bestimmt, ob die Richtlinie aktiv oder inaktiv ist **Hinweis:** Standardmäßig ist aktiv
Datenmuster	Das Datenmuster, das die Richtlinie verwendet.

4. Wählen Sie **Absenden**.

Ergebnis

Wählen Sie die Richtlinie aus, wenn Sie eine erstellen Daten-Discovery Aufträge.

Daten-Discovery Speichern

Erkennen und verfolgen Sie vertrauliche Daten in einer ServiceNow-Instanz

Daten-Discovery-Speicher

Verwenden Daten-Discovery Um vertrauliche Daten in Ihrer Instanz zu erkennen. Scannen Sie nach strukturierten sensiblen Daten wie Kreditkartennummern, Telefonnummern, Sozialversicherungsnummern usw. Beginnen Sie schnell, indem Sie sofort einsatzbereite allgemeine Datenmuster verwenden, oder erstellen Sie eigene, um eine granulare Experience zu erhalten. Für unstrukturierte und häufig kontextbasierte sensible Daten wie Namen, Adressen usw. können Sie KI und maschinelles Lernen zur Unterstützung der Identifizierung verwenden

Daten-Discovery Store-Übersicht

Verschaffen Sie sich einen Überblick über Ihre Daten-Discovery-Metriken und einen Ausgangspunkt für die Verwendung der zugehörigen Tools.

Daten-Discovery Richtlinie

Überprüfen Sie die aktuellen Daten-Discovery-Richtlinien, und konfigurieren Sie sie.

Daten-Discovery-Quellen

Zeigen Sie die Datenmuster und Zieltabellen an, die derzeit von Ihren Discovery-Aufträgen verwendet werden

Daten-Discovery Geplante Discovery

Planen und überprüfen Sie Discovery-Aufträge, einschließlich Discovery-Aufträge für granulare Spalten.

Daten-Discovery Store-Übersicht

Verschaffen Sie sich Einblick in vertrauliche Daten in Ihrer Instanz, und arbeiten Sie an der Implementierung von Sicherheitsmaßnahmen, um den Verlust oder die Offenlegung vertraulicher Daten zu verhindern.

Die **Übersicht** Die Registerkarte bietet einen einfachen Ausgangspunkt für die Verwendung von Daten-Discovery und zeigt wichtige Discovery-Metriken und -Ergebnisse an. Navigieren zu **Alle** > **Daten-Discovery** > **Übersicht** Um mit der Verwendung der Registerkarte zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Discovery-Richtlinie, und planen Sie den Discovery-Auftrag

Sie können mit beginnen Daten-Discovery Mit den empfohlenen Aktionselementen. Wählen Sie Aus **Richtlinie Erstellen** Um zu definieren, welche Muster sensibler Daten identifiziert werden sollen und wie sie behandelt werden sollen. Siehe Daten-Discovery Richtlinie Weitere Informationen zum Erstellen einer neuen Richtlinie. Wählen Sie Aus **Aufgabe Planen** Dient zum Planen von Daten-Discovery-Aufträgen, die Ihre Instanz nach vertraulichen Informationen durchsuchen. Siehe Daten-Discovery Geplante Discovery Weitere Informationen zum Planen eines neuen Discovery-Auftrags.

Daten-Discovery-Zusammenfassung

Sie können auf einen Blick wichtige überprüfen Daten-Discovery Metriken. Darüber hinaus können Sie die Diagramme auswählen, um weitere Detailinformationen anzuzeigen. Weitere Informationen zum Überprüfen von Discovery-Ergebnissen finden Sie unter Überprüfen Sie die Discovery-Ergebnisse.

Erkannte Daten

Ein Balkendiagramm, das die Klassifizierungen und die Menge der erkannten Daten überlagert. Er fasst zusammen, wo und wie viele Instanzen von personenbezogenen Daten in verschiedenen Tabellen in Ihrer Instanz erkannt wurden, kategorisiert nach Datenmustertypen.

Discovery-Status

Ein Ringdiagramm, das die Proportionen des aktuellen Status aller erkannten Muster anzeigt – ob es sich um neue Ergebnisse handelt, die einer Überprüfung ausstehen, klassifiziert oder als ignoriert markiert wurden

Erkannte Daten und letzte Aufträge

In diesem Abschnitt können Sie neu erkannte Daten und aktuelle Discovery-Aufträge überprüfen. Eine detailliertere Überprüfung dieser Tabellen und ihres Inhalts finden Sie unter Daten-Discovery Geplante Discovery

an.

Daten-Discovery Richtlinie

Verwenden Daten-Discovery Richtlinien, um zu definieren, welche Muster sensibler Daten identifiziert werden sollen und wie sie behandelt werden sollen.

Die **Richtlinie** Registerkarte von Daten-DiscoveryÜberprüft aktuelle Discovery-Richtlinien. Zeigen Sie zusätzliche Details einer Richtlinie an, indem Sie auswählen **Zeigen Sie Details an** Schaltfläche. Bearbeiten, löschen und ändern Sie den Status aktueller Richtlinien, indem Sie die drei Punkte auswählen ⋮. Informationen zum Erstellen einer neuen Richtlinie finden Sie unter Neue Richtlinie erstellen.

Neue Richtlinie erstellen

Erstellen Sie einen Daten-Discovery Richtlinie zum Scannen von Tabellen auf Datenmuster.

Vorbereitungen
Erforderliche Rolle: Discovery.admin

Prozedur

1. Navigieren zu **Alle** > **Daten-Discovery** > **Richtlinie**an.
2. Wählen Sie aus **Erstellen Sie eine neue Richtlinie** Schaltfläche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bearbeiten oder löschen Sie eine vorhandene Richtlinie, indem Sie die drei Punkte auswählen ⋮ Symbol.

3. Füllen Sie die Felder des Popup-Fensters aus.

Formular „neue Discovery-Richtlinie“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Richtlinie ein
Datenmuster	Wählen Sie aus, nach welchen Mustern für sensible Daten gescannt werden soll. Sie können mehrere Datenmuster auswählen **Hinweis:** KI/ML-modellbasierte Datenmuster erfordern eine zusätzliche Lizenz und unterliegen zusätzlichen Nutzungsbedingungen.
Wählen Sie Anwendertabellen und -Spalten aus	Überprüfen Sie die zu scannenden Tabellen **Hinweis:** Alle ausgewählten Tabellenspalten werden standardmäßig gescannt. Sehen Sie sich den folgenden Schritt an, um Ihre Auswahl auf bestimmte Spalten einzugrenzen
Ausgewählte Tabellen und Spalten	Zeigt eine Liste der derzeit ausgewählten Tabellen und Spalten für die Richtlinie an

4. **Wahlweise:** Wählen Sie den Pfeil aus › Symbol zum Anzeigen und Auswählen bestimmter Spalten der Tabelle.
5. Wählen Sie **Speichern**.

Ergebnis

Standardmäßig wird die neue Richtlinie auf festgelegt **Aktiv** . Wählen Sie die drei Punkte aus ⋮ Symbol und wählen Sie aus **Deaktivieren Sie die Richtlinie** / **Aktivieren Sie die Richtlinie** Um den Status zu ändern.

Daten-Discovery-Quellen

Erstellen Sie die Datenmuster, die in verwendet werden sollen, und wählen Sie sie aus Daten-Discovery, Und welche Tabellen gescannt werden sollen.

Die **Quellen** Registerkarte von Daten-Discovery Hilft Ihnen, alle Ihre Datenmuster zu überprüfen, festzulegen, welches Muster für Scans verwendet werden soll, und die zu scannenden Tabellen auszuwählen.

Alle Muster

Die **Alle Muster** Tabelle listet alle aktuellen Muster auf. Beachten Sie, dass inaktive Muster in dieser Liste angezeigt werden.siehe Erstellen Sie ein neues Datenmuster Zum Erstellen eines neuen Datenmusters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Muster müssen aktiv sein, um in Discovery-Aufträgen verwendet werden zu können.

Tabelle „alle Muster“

Bezeichnung	Beschreibung
Name	Name des Datenmusters.
Ausdruck	Regulärer Ausdruck, der zum Erkennen des Datenmusters verwendet wird.
Stichwort	Ein bestimmtes Wort (oder Wörter, die durch Kommas getrennt sind), nach dem um einen Ausdruck gesucht werden soll.
Stichwortnähe	Wie weit der Ausdruck entfernt ist, um nach Stichwörtern zu suchen.
Konfiguration der Datenschutztechnik	Für das Muster verwendete Datenschutztechnik

Aktive Muster

Die **Aktive Muster** Tabelle listet alle aktuell aktiven Datenmuster auf. Siehe Wählen Sie aktive Datenmuster aus Um zu erfahren, wie ein Muster auf „aktiv“ festgelegt und von Discovery-Aufträgen verwendet wird.

Tabelle mit aktiven Mustern

Bezeichnung	Beschreibung
Name	Name des Datenmusters.
Ausdruck	Regulärer Ausdruck, der zum Erkennen des Datenmusters verwendet wird.
Stichwort	Ein bestimmtes Wort (oder Wörter, die durch Kommas getrennt sind), nach dem um einen Ausdruck gesucht werden soll.
Stichwortnähe	Wie weit der Ausdruck entfernt ist, um nach Stichwörtern zu suchen.
Konfiguration der Datenschutztechnik	Für das Muster verwendete Datenschutztechnik

Zieltabellen

Die **Zieltabellen** Tabelle listet alle Tabellen auf, die derzeit für Discovery-Aufträge ausgewählt sind. Siehe Wählen Sie Zieltabellen aus Zum Auswählen von Tabellen zur Verwendung in Discovery-Aufträgen.

Zieltabellen-Tabelle

Bezeichnung	Beschreibung
Tabellenname	Name der Tabelle
Anzeigename	Der Anzeigename der Tabelle (wird in der Berichterstellung verwendet)
Anwendung	Der Anwendungsbereich der Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein neues Datenmuster

Erstellen Sie eine neue Daten-Discovery Muster speichern.

Vorbereitungen
Erforderliche Rolle: Discovery.admin

Prozedur

1. Navigieren zu **Alle** > **Daten-Discovery** > **Quellen**an.
2. Wählen Sie Aus **Alle Muster** Im Navigationsbereich.
3. Wählen Sie aus **Erstellen Sie neu** Schaltfläche.
4. Füllen Sie das Formular aus.

Formular „Neues Datenmuster“

Feld	Beschreibung
Beschreibung	Beschreibung des Musters.
Name	Name des Datenmusters.
Ausdruck	Regulärer Ausdruck, der zum Erkennen des Datenmusters verwendet wird. **Hinweis:** Die Ausdruckslänge muss weniger als 1000 Zeichen betragen.
Stichwort	Ein bestimmtes Wort (oder Wörter, die durch Kommas getrennt sind), nach dem um einen Ausdruck gesucht werden soll. Muss mit verwendet werden **Stichwortnähe** **Hinweis:** Ein Stichwort kann verwendet werden, um nach zusätzlichem Kontext für ein Muster zu suchen. Beispielsweise kann die Verwendung eines Stichworts helfen, zwischen einem Geburtsdatum und einem Einstellungsdatum zu unterscheiden, wenn sie dieselbe Formatierung FÜR MM/TT/JJ aufweisen.
Stichwortnähe	Wie weit der Ausdruck entfernt ist, um nach Stichwörtern zu suchen. Muss mit verwendet werden **Stichwort** **Hinweis:** Der Standardwert ist 30, der obere Grenzwert von 64
Konfiguration der Datenschutztechnik	Für das Muster verwendete Datenschutztechnik
Synthetic-Wert	Liste der Werte, die für die Muster ersetzt werden
Typ	Typ des Musters
Anwendung	Anwendungsbereich des Musters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Umfang	Umfang des Musters.

5. **Wahlweise:** Wählen Sie aus **Testen** Schaltfläche zum Testen Ihrer regulären Ausdrücke bei Bedarf.
6. Wählen Sie **Absenden**.

Ergebnis

Das neue Datenmuster muss als aktiv festgelegt werden, um in Discovery-Aufträgen verwendet werden zu können. Weitere Informationen finden Sie unter Wählen Sie aktive Datenmuster aus.

Wählen Sie aktive Datenmuster aus

Wählen Sie die aktiven Datenmuster aus, für die verwendet werden soll Daten-Discovery Aufträge.

Vorbereitungen

Erforderliche Rolle: Discovery.admin

Prozedur

1. Navigieren zu **Alle** > **Daten-Discovery** > **Quellen**an.
2. Wählen Sie Aus **Aktive Muster** Im Navigationsbereich.
3. Wählen Sie die Schaltfläche **Bearbeiten**.
4. Überprüfen Sie die zu aktivierenden Muster. Sie werden auf der rechten Seite des Popups angezeigt.
5. **Wahlweise:** Wählen Sie Muster aus, und ziehen Sie sie, um sie neu anzuordnen.

Hinweis:

Die Reihenfolge der Datenmuster bestimmt auch die Reihenfolge der Anonymisierungstechniken, die für die Anonymisierung von Datenmustern angewendet werden.

6. Wählen Sie aus **Speichern** Schaltfläche.

Wählen Sie Zieltabellen aus

Wählen Sie Zieltabellen aus, die in Discovery-Aufträgen verwendet werden sollen.

Vorbereitungen

Erforderliche Rolle: Discovery.admin

Prozedur

1. Navigieren zu **Alle** > **Daten-Discovery** > **Quellen**an.
2. Wählen Sie Aus **Zieltabellen** Im Navigationsbereich.
3. Wählen Sie die Schaltfläche **Bearbeiten**.
4. Überprüfen Sie die Tabellen, die als Ziel festgelegt werden sollen. Sie werden auf der rechten Seite des Popups angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Zieltabellen scannen alle Spalten, sofern nicht anders angegeben In Richtlinie .

5. Wählen Sie aus **Speichern** Schaltfläche.

Ergebnis

Ausgewählte Tabellen werden jetzt als Ziel ausgewählt Geplante Discovery-Aufgaben .

Daten-Discovery Geplante Discovery

Richten Sie Daten-Discovery-Aufträge ein, und planen Sie sie, um Ihre Instanz nach vertraulichen Informationen zu durchsuchen.

Discovery-Aufträge

Die **Discovery-Aufträge** Tabelle listet alle Discovery-Aufträge auf. Siehe Erstellen Sie einen Discovery-Auftrag Dient zum Erstellen eines neuen Discovery-Auftrags.

Discovery-Aufgabentabelle

Name	Name des Auftrags
Beschreibung	Die Auftragsbeschreibung
Fertigstellungsgrad	Der Prozentsatz des Abschlusses des Auftrags
Scantyp	Scan-Typ des Auftrags. Mögliche status: • **Beispiel** : Scannt 10.000 Einträge. • **Voll** : Scannt alle Einträge.
Startdatum	Das Startdatum des Auftrags
Aktualisiert	Zeitpunkt der letzten Aktualisierung des Auftrags.
Status	Status von Daten-Discovery Auftrag. Mögliche status: • **Bereit zum Planen** : Standardstatus für neue Aufträge. • **Geplant** : Die Ausführung der Aufgabe ist geplant. • **In Bearbeitung** : Auftrag wird aktiv ausgeführt. • **Abgeschlossen** : Auftrag wurde erfolgreich ausgeführt. • **Fehler** : Die Ausführung des Auftrags wurde aufgrund eines Fehlers angehalten. • **Abgebrochen** : Der Auftrag wurde abgebrochen. • **Angehalten** : Der Auftrag wurde angehalten.
Ausführen	Wie oft die Ausführung der Aufgabe geplant ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Ergebnisse

Die **Discovery-Ergebnisse** Tabelle listet alle erkannten Ergebnisse aus Discovery-Aufträgen auf. Siehe Überprüfen Sie die Discovery-Ergebnisse Dient zum Überprüfen und Klassifizieren von Ergebnissen aus Discovery-Aufträgen.

Discovery-Ergebnistabelle

Bezeichnung	Beschreibung
Wörterbucheintrag	Spalte der Zieltabelle, in der sich die Daten befanden
Tabelle	Zieltabelle, in der die Daten gefunden wurden
Datenmuster	Datenmuster, das zum Suchen der Daten verwendet wird
Anzahl der Übereinstimmungen von Datenmustern	Anzahl der Dateneinträge, die dem Datenmuster entsprechen
Gesamtanzahl der Zeilenscans	Anzahl der während des Auftrags gescannten Zeilen
Prozentsatz der übereinstimmenden Zeilen	Prozentsatz der Zeilen in der Zieltabelle, die dem Datenmuster entsprechen
Daten-Discovery-Auftrag	In der Zieltabelle verwendeter Auftrag
Status	Status des Eintrags

Granulare Konfiguration

Die **Granulare Konfiguration** Tabelle listet alle granularen Discovery-Aufträge auf. Siehe Erstellen Sie einen granularen Auftrag Um zu erfahren, wie Sie einen granularen Discovery-Auftrag erstellen.

Granulare Konfigurationstabelle

Bezeichnung	Beschreibung
Tabelle	Tabelle des granularen Discovery-Auftrags
Spaltenbezeichnung	Spaltenbezeichnung des granularen Discovery-Auftrags
Startpunkt des Scans	Vertrauliche Daten werden nur für den Tag und nach dem Scan-Startpunkt erkannt. **Hinweis:** Wenn der Scan-Startpunkt leer gelassen wird, werden alle Einträge in der Spalte gescannt.
Aktiv	Der Status des granularen Discovery-Auftrags.

Granulare Ergebnisse

Die **Granulare Ergebnisse** Tabelle listet alle granularen Ergebnisse aus granularen Discovery-Aufträgen auf. Siehe Überprüfen Sie die granularen Ergebnisse Dient zum Überprüfen der Ergebnisse von granularen Discovery-Aufträgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle der granularen Ergebnisse

Bezeichnung	Beschreibung
Datensatz	Erkannter Datensatz
Tabelle	Übergeordnete Tabelle des Datensatzes
Datenmuster	Muster, das zum Erkennen des Datensatzes verwendet wird
Aktion	Aktion, die für den Datensatz ausgeführt werden soll **Prüfung** Die Überprüfung des Datensatzes steht aus. Dies wird neuen granularen Erkennungen zugewiesen **Ignorieren** Für den Datensatz wird keine Aktion ausgeführt **Anonymisieren** Datensatz wird anonymisiert
Status	Der Status des Datensatzes **Neu** Status, der dem Ergebnis zugewiesen ist, wenn es erstmals gemeldet wird **Verarbeitet** Wenn die vom Anwender ausgewählte Aktion erfolgreich auf das Ergebnis angewendet wurde **Hinweis:** Verarbeitete Ergebnisse werden vor dem Löschen 3 Tage lang in der Tabelle „granulare Ergebnisse“ gespeichert **Manuelle Überprüfung** Beim Anwenden der vom Anwender ausgewählten Aktion ist ein Fehler aufgetreten **Warnung:** Ergebnisse in der manuellen Überprüfung sollten von Anwendern gelöscht werden, nachdem sie entsprechende Aktionen ergriffen haben.

Erstellen Sie einen Discovery-Auftrag

Erstellen und planen Sie einen neuen Daten-Discovery-Store-Auftrag.

Vorbereitungen
Erforderliche Rolle: Discovery.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Daten-Discovery** > **Geplante Discovery**an.
2. Wählen Sie Aus **Discovery-Aufträge** Im rechten Navigationsbereich.
3. Füllen Sie das Formular aus.

Formular „neue Discovery planen“

Feld	Beschreibung
Name	Name des Jobs
Beschreibung	Beschreibung des Auftrags.
Scantyp	Anzahl der zu scannenden Einträge. Mögliche status: ○ **Beispiel** : Scannt 10.000 Einträge. ○ **Voll** : Scannt alle Einträge.
Richtlinie auswählen	Die für die geplante Aufgabe zu verwendende Richtlinie.
Startdatum	Legt das Startdatum für den Auftrag fest.
Zeitfensterstart	Der Beginn des Zeitfensters zur Ausführung dieses Auftrags. Der Auftrag wird nach der in dieses Feld eingegebenen Zeit ausgeführt. Die in eingegebene Zeit **Zeitfensterstart** Das Feld muss vor der in eingegebenen Zeit erfolgen **Zeitfensterende** Feld. **Hinweis:** Ein gültiger Zeitwert ist in koordinierter Weltzeit basierend auf einer 24-Stunden-Zeitnotation.
Zeitfensterende	Das Ende des Zeitfensters zur Ausführung dieses Auftrags. Der Auftrag wird bis zu der in dieses Feld eingegebenen Zeit ausgeführt. Wenn der Auftrag dieses Mal nicht abgeschlossen ist, wird der Auftrag angehalten und beim nächsten Start des Fensters fortgesetzt. Die in eingegebene Zeit **Zeitfensterende** Das Feld muss nach der in eingegebenen Zeit erfolgen **Zeitfensterstart** Feld. **Hinweis:** Ein gültiger Zeitwert ist in koordinierter Weltzeit basierend auf einer 24-Stunden-Zeitnotation.

4. Wählen Sie aus **Zeitplan** Schaltfläche.

Überprüfen Sie die Discovery-Ergebnisse

Klassifizieren Sie Daten im Daten-Discovery-Speicher

Vorbereitungen

Erforderliche Rolle: Discovery.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Gehe zu **Alle** > **Daten-Discovery** > **Geplante Discovery**an.
2. Wählen Sie Aus **Discovery-Ergebnisse** Im rechten Navigationsbereich.
3. Überprüfen Sie die zu klassifizierenden Einträge.
   Wählen Sie aus **Bearbeiten** Schaltfläche zum Bearbeiten der Klassifizierung ausgewählter Einträge.
4. Wählen Sie aus **Klassifizieren** Schaltfläche.

   Hinweis: Wählen Sie aus **Verfügbare Schutzmaßnahmen** Schaltfläche zum Überprüfen der Schutzoptionen für klassifizierte Daten.

5. Wählen Sie die Datenklassifizierungen aus, die Sie den Tabelleneinträgen zuordnen möchten.
6. Wählen Sie Aus **Klassifizieren** .

Ergebnis

Die ausgewählten Daten sind jetzt klassifiziert.

Erstellen Sie einen granularen Auftrag

Scannen Sie bestimmte Tabellenspalten im Daten-Discovery-Speicher.

Vorbereitungen

Erforderliche Rolle: Discovery.admin

Prozedur

1. Navigieren zu **Alle** > **Daten-Discovery** > **Geplante Discovery**an.
2. Wählen Sie Aus **Granulare Konfiguration** Im rechten Navigationsbereich.
3. Wählen Sie **Neu erstellen**.
4. Füllen Sie das Formular aus.

Erstellen Sie ein neues granulares Konfigurationsformular

Feld	Beschreibung
Tabelle	Die zu scannende Tabelle
Spaltenbezeichnung	Die zu scannende Spalte
Startpunkt des Scans	Vertrauliche Daten werden nur für den Tag und nach dem Scan-Startpunkt erkannt. **Hinweis:** Wenn der Scan-Startpunkt leer gelassen wird, werden alle Einträge in der Spalte gescannt. Wenn der Scan-Startpunkt geändert wird, wird der Scan zurückgesetzt, um mit dem neu konfigurierten Zeitstempel zu beginnen.

5. Festlegen **Aktiv** Schieberegler.
6. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis
Ein granularer Scan ist für die Zieltabelle und -Spalte geplant. Nach der Ausführung können Sie dies tun Überprüfen Sie die Scan-Ergebnisse .

Überprüfen Sie die granularen Ergebnisse

Überprüfen Sie granulare Ergebnisse im Daten-Discovery-Store

Vorbereitungen
Erforderliche Rolle: Discovery.admin

Prozedur

1. Navigieren zu **Alle** > **Daten-Discovery** > **Geplante Discovery**an.
2. Wählen Sie Aus **Granulare Ergebnisse** Im rechten Navigationsbereich.
3. Überprüfen Sie die Tabelleneinträge.

Spaltenbezeichnung	Beschreibung
Datensatz	Erkannter Datensatz.
Tabelle	Übergeordnete Tabelle des Datensatzes.
Datenmuster	Muster, das zum Erkennen des Datensatzes verwendet wird.
Aktion	Aktion für Ergebnisse. Zum Ändern auswählen **Wichtig:** Die Rolle Data_privacy_admin ist erforderlich, um die Aktion Anonymisieren für einen Datensatz auszuführen. **Prüfung** Die Überprüfung des Datensatzes steht aus. Dies wird neuen granularen Erkennungen zugewiesen. **Ignorieren** Für den Datensatz wird keine Aktion ausgeführt **Anonymisieren** Datensatz wird anonymisiert.
Status	Status des Datensatzes. **Neu** Status, der dem Ergebnis zugewiesen ist, wenn es erstmals gemeldet wird **Verarbeitet** Wenn die vom Anwender ausgewählte Aktion erfolgreich auf das Ergebnis angewendet wurde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spaltenbezeichnung	Beschreibung
	Hinweis: Verarbeitete Ergebnisse werden vor dem Löschen 3 Tage lang in der Tabelle „granulare Ergebnisse“ gespeichert **Manuelle Überprüfung** Beim Anwenden der vom Anwender ausgewählten Aktion ist ein Fehler aufgetreten. **Warnung:** Ergebnisse in der manuellen Überprüfung sollten von Anwendern gelöscht werden, nachdem sie entsprechende Aktionen ergriffen haben.

Warnung:

Rollback wird für die Anonymisierung, die durch granulare Ergebnisse ausgelöst wird, nicht unterstützt.

Datenklassifizierung

Gruppieren Sie Daten mithilfe vordefinierter oder benutzerdefinierter Datenklassifizierungen nach Typ. Wenn Ihnen die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ zugewiesen wurde, können Sie verschiedene Datenklassen verwalten oder den aktuellen Status verschiedener Datentypen innerhalb der Instanz visuell analysieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie Die Datenklassifizierung



Erfahren Sie mehr über die Datenklassifizierung.

Konfigurieren Sie Die Datenklassifizierung



Erstellen und konfigurieren Sie eigene Datenklassen.

Referenz für Datenklassifizierung



Erfahren Sie, wie die Datenklassifizierung mit Demodaten funktioniert.

Analysieren Sie Datenklassifizierungen



Erfahren Sie, wie Sie Datenklassifizierungen analysieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenklassifizierung Erkunden

Untersuchen Sie die Datenklassifizierung.

Datenklassifizierung Aktiviert Unterstützung für:

- Transparenz der Arten von Daten, die auf einem gehostet werden ServiceNow AI Platform Instanzen.
- Compliance mit Datenschutzgesetzen und Erfüllung von Vorschriften für Branchen wie Finanzdienstleistungen und Herstellung medizinischer Geräte.

Datenklassifizierungen

Die Datenklassifizierung ist ein eigenständiger Prozess, bei dem Sie Datenklassifizierungen manuell auf vorhandene Wörterbucheinträge in einer beliebigen Tabelle anwenden. Weitere Informationen finden Sie unter Datenwörterbuchtabellen .

- Sie klassifizieren Daten so, wie Sie es für Ihr Unternehmen als angemessen finden, und Sie können die verfügbaren Datenklassen nach Bedarf ändern.
- Wenn Sie Daten klassifizieren, können Sie die vordefinierten Datenklassifizierungen verwenden oder eigene erstellen. Obwohl die Verwendung vordefinierter Datenklassifizierungen optional ist, wird empfohlen, dies als Ausgangspunkt zu tun. Diese vordefinierten Datenklassifizierungen sind in Demodaten enthalten, die Sie in Ihrer Instanz installieren können. Weitere Informationen finden Sie unter Wird Installiert Datenklassifizierung Plugin-Demodaten Und Mit installierte Komponenten Datenklassifizierung Demodaten.
- Wenn Sie eigene Datenklassifizierungen erstellen, können Sie auch ein abgestuftes hierarchisches System mit übergeordneten und untergeordneten Datenklassifizierungen entwerfen.

Übersichts-Dashboard

Verwenden Sie das Übersichts-Dashboard, um zu verstehen, wie Ihre aktuellen Datentabellen verschiedenen Datenklassifizierungen zugeordnet sind. Sie können auch analysieren, wie Ihre globalen, regionalen und internationalen Anwender unterschiedliche Ansätze für die Datenklassifizierung benötigen, was die Verwendung oder den Zugriff auf Daten betrifft. Sie können den Inhalt und das Layout des Übersichts-Dashboards auch an Ihre Anforderungen anpassen.

Informationen zur Verwendung der verfügbaren geskripteten APIs und REST APIs zum Anwenden der Klassifizierungsmetadaten in vorhandenen Prozessen, Workflows und Anwendungen finden Sie unter:

- Datenklassifizierung: REST API
- DCManager: Global
- ScopedDCManager: Bereichsbezogen

Hinweis: Datenklassifizierung Unterstützt Domänentrennung, und die Tabelle „Data_classification“ selbst ist prozessgetrennt.

Anwendungsfälle

Die allgemeine Datenschutzverordnung (DSGVO) ist eine Verordnung der Europäischen Union, deren Zweck darin besteht, Einzelpersonen die Kontrolle über ihre eigenen personenbezogenen Daten zu geben. Sie können Datenklassifizierungen wie personenbezogene Informationen verwenden, um zu identifizieren, wo personenbezogene

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten in Ihrer Instanz gespeichert werden. Durch die Anwendung der entsprechenden Sicherheitsmechanismen zum Schutz dieser personenbezogenen Daten vor dem Auslaufen erfüllt Ihre Organisation die DSGVO-Anforderungen.

Wenn Sie Kundeninformationen in speichern ServiceNow AI Platform, Verwenden Sie bei Bedarf den Klassifizierungscode für personenbezogene Daten (Personally Identifiable Information, PII), um Daten nachzuverfolgen, die den lokalen Datenschutzgesetzen unterliegen. Wenn Sie Demodaten installieren, wird dieser Klassifizierungscode automatisch auf angewendet Sicher Sicherheitsrelevante Felder in der Anwendertabelle [sys_user]. Weitere Informationen finden Sie unter:

- Mit installierte Komponenten Datenklassifizierung Demodaten
- Zuweisen von Datenklassifizierungen zu Wörterbucheinträgen

Sie können eine eingeschränkte Datenklassifizierung auf Mitarbeitertabellenspalten anwenden, die vertrauliche Mitarbeiterinformationen wie Sozialversicherungsnummern (SSN) speichern. Administratoren und Auditoren können dann das Übersichts-Dashboard verwenden, um zu bestätigen, dass Sie Datenklassifizierungen den richtigen Spalten zugewiesen haben. Sie können auch die Klassifizierungsdetails für eingeschränkte Informationstypen anzeigen.

Wird Installiert Datenklassifizierung Plugin-Demodaten

Wenn Sie ein Upgrade auf oder installieren Zurich(Und höher), die Datenklassifizierung Das Plugin „“ (com.Glide.Data_classification) wird automatisch aktiviert. Sie sollten die Demodaten, die mit dem Plugin geliefert werden, jedoch manuell installieren. Es enthält mehrere wichtige vordefinierte Datenklassifizierungen und weist eine davon auch bestimmten Tabellenspalten „Anwender“ [sys_user] in Ihrer Instanz zu.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Unabhängig davon, ob Sie Demodaten installieren, wird aktiviert Datenklassifizierung Das Plugin fügt die folgenden Anwenderrollen in Ihrer Instanz hinzu:

- Data_classification_admin: Kann alle Aspekte von verwalten Datenklassifizierung Anwendung, einschließlich Einrichtung und Zuweisung der Datenklassifizierung.
- Data_classification_Auditor: Audit möglich Datenklassifizierung Codezuweisungen an Anwendertabellen und -Spalten.

Wichtig: Hinweis zur Verwendung durch Kunden:

Alle Entscheidungen im Zusammenhang mit der Implementierung dieser Anwendung unterliegen der alleinigen Entscheidung des Kunden. Kunden bestätigen und stimmen zu, dass die Verwendung der Anwendung keine Darstellung von ServiceNow hinsichtlich der Compliance mit Gesetzen oder Vorschriften ist und dass jede vorgeschlagene Sprache, ein Feld oder eine Klassifizierung, die standardmäßig mit der Anwendung bereitgestellt wird, keine rechtliche Beratung durch ServiceNow darstellt.

Kunden bleiben allein für die Einhaltung ihrer rechtlichen Verpflichtungen nach geltendem Recht verantwortlich, einschließlich (aber nicht beschränkt auf) Datenschutz-, Sicherheitsanforderungen und Datenschutzgesetzen, und sind verantwortlich für die Konfiguration und Durchführung aller erforderlichen Änderungen an dieser Anwendung, einschließlich (aber nicht beschränkt auf) Vorlagen, um die Anforderungen der Kunden zu erfüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach Datenklassifizierung Plugin mithilfe der Filterkriterien und der Suchleiste.
   Ein Installiert Die Nachricht wird angezeigt, nachdem Sie das Plugin gefunden haben.
3. Klicken Sie auf das Symbol mit drei vertikalen Punkten, und wählen Sie dann aus **Reparieren** Um auf das Dialogfeld „Plugin aktivieren“ zuzugreifen.
4. Wählen Sie Aus **Demodaten laden** , Und klicken Sie dann auf **Reparieren** .

Mit installierte Komponenten Datenklassifizierung Demodaten

Wenn Sie die Demodaten installieren, die in enthalten sind Datenklassifizierung Plugin „“ (com.Glide.Data_classification), in Ihrer Instanz werden verschiedene Arten von Komponenten installiert. Diese Komponenten umfassen vordefinierte Datenklassifizierungen und Codezuweisungen für bestimmte Anwenderspalten [sys_user}.

Datenklassifizierungen installiert

Datenklassifizierung	Beschreibung
Vertraulich	Vertrauliche Daten, die sich bei Gefährdung negativ auf den Betrieb auswirken können.
Intern	Interne Daten sind nicht für die öffentliche Offenlegung vorgesehen.
Personenbezogene Informationen	Auch bekannt als PII. Daten, die potenziell zur Identifizierung einer bestimmten Person verwendet werden könnten.
Öffentlich	Daten, die der Öffentlichkeit frei zugänglich gemacht werden können.
Beschränkt	Sehr vertrauliche Unternehmensdaten, die bei Gefährdung das Unternehmen einem finanziellen oder rechtlichen Risiko aussetzen könnten.

Datenklassifizierung Zuweisungen

Tabelle	Zugewiesene Spalte	Zugewiesene Datenklassifizierung
sys_user	Postleitzahl	Personenbezogene Informationen
sys_user	first_name	Personenbezogene Informationen
sys_user	E-Mail	Personenbezogene Informationen
sys_user	city	Personenbezogene Informationen
sys_user	Zweiter_Name	Personenbezogene Informationen
sys_user	Straße	Personenbezogene Informationen
sys_user	mobile_phone	Personenbezogene Informationen
sys_user	last_name	Personenbezogene Informationen
sys_user	country	Personenbezogene Informationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Zugewiesene Spalte	Zugewiesene Datenklassifizierung
sys_user	Geschlecht	Personenbezogene Informationen
sys_user	name	Personenbezogene Informationen
sys_user	Foto	Personenbezogene Informationen
sys_user	Status	Personenbezogene Informationen
sys_user	home_phone	Personenbezogene Informationen

Datenklassifizierungen werden erstellt

Erstellen Sie Ihre eigenen anwenderdefinierten Datenklassifizierungen in Datenklassifizierung Tabelle [Data_classification], die Sie dann bestimmten Spalten in bestimmten Tabellen zuweisen können.

Vorbereitungen

Erforderliche Rolle: Data_classification_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Datenklassifizierung** > **Datenklassen**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Klassifizierungsname	Name der Datenklassifizierung.
Beschreibung	Beschreibung der Datenklassifizierung.
Übergeordnet	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung keine übergeordneten zu untergeordneten Datenklassifizierungen ist.
Anwendung	Anwendungsbereich für diese Datenklassifizierung.

4. Wenn diese Datenklassifizierung ein übergeordnetes Element für untergeordnete Datenklassifizierungen sein soll, klicken Sie auf **Neu** .
   Wenn Sie keine untergeordneten Datenklassifizierungen erstellen möchten, überspringen Sie diesen Schritt.
5. Füllen Sie die Felder des Formulars aus.

Titel

Feld	Beschreibung
Klassifizierungsname	Name der untergeordneten Datenklassifizierung.
Beschreibung	Beschreibung der Klassifizierung der untergeordneten Daten.
Übergeordnet	Name der übergeordneten Datenklassifizierung, der diese Datenklassifizierung untergeordnet ist. Lassen Sie das Feld leer, wenn diese Datenklassifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	keine übergeordneten zu untergeordneten Datenklassifizierungen ist.
Anwendung	Anwendungsbereich für diese untergeordnete Datenklassifizierung.

6. Klicken Sie auf **Absenden**.

Zuweisen von Datenklassifizierungen zu Wörterbucheinträgen

Weisen Sie Datenklassifizierungen bestimmten Tabellenspalten in der Tabelle „Wörterbuch“ [sys_dictionary] zu. Wenn Sie Datenklassifizierungen zuweisen, werden Einträge in der Tabelle „Wörterbuch-Datenklasse“ [m2m_dictionary_dataclass] erstellt, die Sie dann im Dashboard „Übersicht“ überprüfen können.

Vorbereitungen

Erforderliche Rolle: Data_classification_admin und admin

Prozedur

1. Geben Sie im Navigationsbereich ein `sys_dictionary.list` .
2. Wählen Sie unter Wörterbucheinträge jedes der Elemente aus, denen Sie bestimmte Datenklassifizierungen zuweisen möchten.
3. Nachdem Sie die Elemente ausgewählt haben, klicken Sie auf **Aktionen für ausgewählte Zeilen** , Und wählen Sie dann aus **Klassifizieren** .

   Hinweis: Um zuvor zugewiesene Datenklassifizierungen für ausgewählte Wörterbuchelemente zu löschen, können Sie auswählen **Klassifizierung löschen** .

4. Wenn das Dialogfeld „Zuweisen an Datenklasse“ angezeigt wird, wählen Sie die Datenklassifizierungen aus, die Sie Ihren ausgewählten Wörterbuchelementen zuweisen möchten, und klicken Sie dann auf **Klassifizieren** .

   Warnung: Dadurch werden alle vorhandenen Klassifizierungen für die ausgewählten Wörterbuchelemente überschrieben.

   Sie können nach Bedarf mehrere Datenklassifizierungen auswählen.

   Weitere Informationen finden Sie unter Datenwörterbuchtabellen .

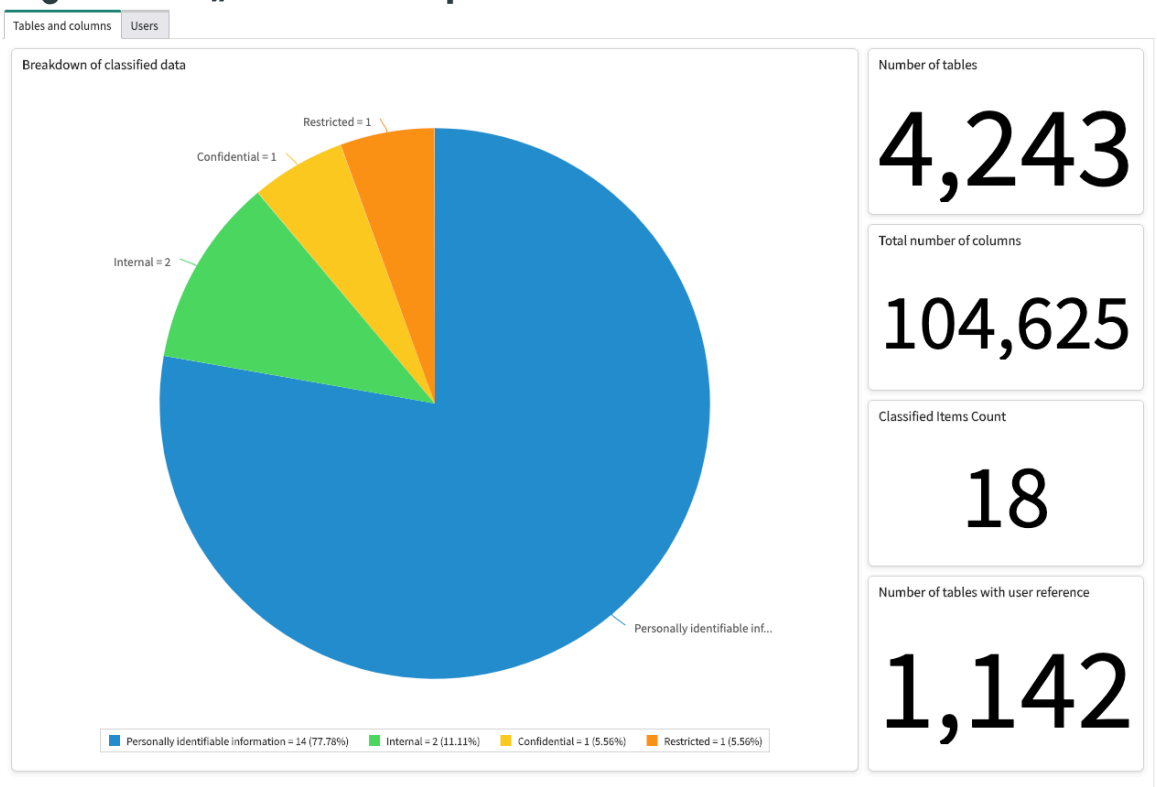
Datenklassifizierungen mit dem Übersichts-Dashboard analysieren

Das Dashboard „Übersicht“ zeigt den aktuellen Status der Datenklassifizierungen in Ihrer Instanz und die Verteilung Ihrer Anwender nach Standort an.

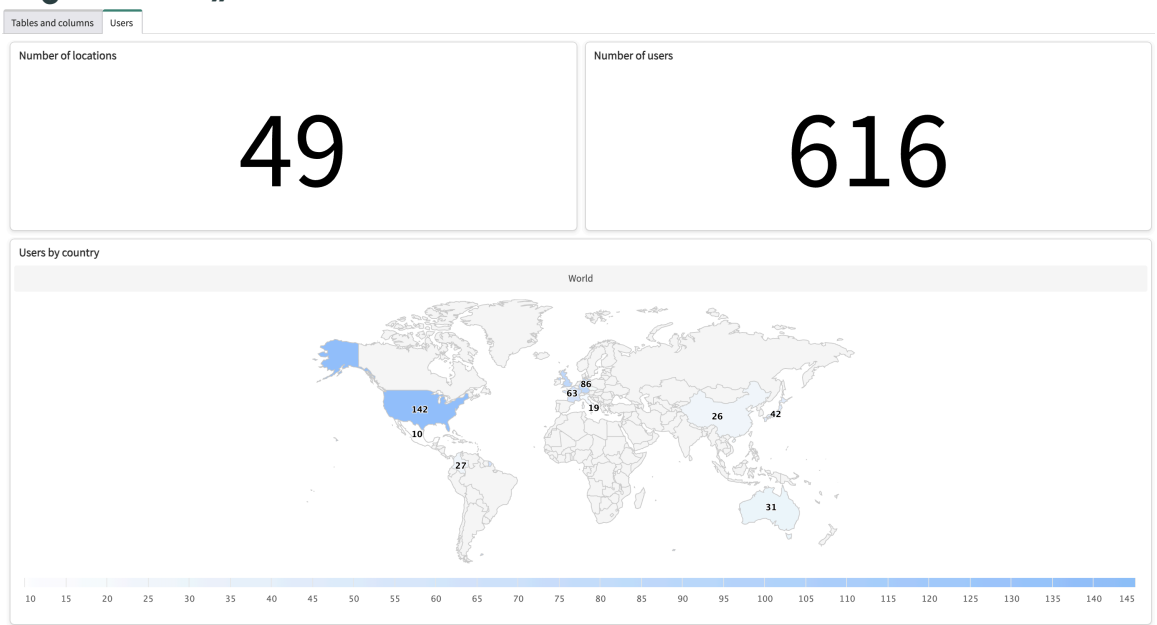
Wenn Sie über die Rolle „Datenklassifizierungsadministrator“ oder „Auditor“ verfügen, können Sie die aktuelle Vertraulichkeit von Instanzdaten visualisieren, was zur Erhöhung der Sicherheit und Compliance mit Datenschutzgesetzen beiträgt. Durch die Verwendung des Felds Standort in Anwenderdatensätzen ordnen Administratoren Anwender in verschiedenen Regionen mit unterschiedlichen Datenschutzbestimmungen zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Tabellen und Spalten“



Registerkarte „Anwender“



Erforderliche ServiceNow AI Platform-Rollen

- Data_classification_admin: Verwaltet alle Aspekte von Datenklassifizierung Anwendung, einschließlich Setup der Datenklassifizierung und Zuweisung.
- Data_classification_Auditor: Audits Datenklassifizierung Codezuweisungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

Zusätzliche Beispiele dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden würden, finden Sie unter Anwendungsfälle in Datenklassifizierung.

Anwender	Dashboard-Verwendung
Data_classification_admin	Bestätigen Sie, dass Sie Datenklassifizierungen den richtigen Feldern in Ihrer Instanz zugewiesen haben.
Data_classification_Auditor	Auditieren Sie die Zuverlässigkeit und Sicherheit von Daten in Ihrer Instanz.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Aufgliederung klassifizierter Daten	Ringdiagramm	m2m_dictionary_dataclass	Bietet eine Aufgliederung der Instanzdatenklassifizierungen nach Datenklasse, insgesamt angezeigt in der Mitte.
Gesamtanzahl Tabellen	Einzelne Punktzahl	sys_dictionary	Gesamtanzahl der Datentabellen im gesamten Wörterbuch.
Gesamtsummenspalten	Einzelne Punktzahl	sys_dictionary	Gesamtanzahl der klassifizierten Datenspalten im gesamten Wörterbuch.
Anwenderreferenzspalten	Einzelne Punktzahl	sys_dictionary	Gesamtanzahl der Anwenderreferenzspalten im Wörterbuch.
Anzahl Anwenderstandorte	Einzelne Punktzahl	sys_user	Gesamtzahl der eindeutigen Standorte, die für Anwender gefunden wurden
Anwenderanzahl	Einzelne Punktzahl	sys_user	Gesamtzahl der Anwenderdatensätze in Ihrer Instanz.
Anwender nach Land	Karte	sys_user	Aufgliederung der Anwenderdatensätze nach Land.

Domain Separation und Datenklassifizierung

Domänentrennung wird für unterstützt Datenklassifizierung . Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufe: Erweitert

- Enthält alle Aspekte von **Standard** Und **Standard** Supportstufen.
- Ein datengesteuerter Prozess ermöglicht es Service Provider-Kunden, die Geschäftslogik basierend auf definierten Anwendungsfällen zu ändern. Diese Konfigurationen sind UI-basiert und ausfallsicher, sodass Konfigurationen von einem Kunden sich nicht auf einen anderen auswirken können.
- Mandanten der Instanz müssen die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter für sich selbst konfigurieren können. Diese Logik und diese Parameter würden für die normale Funktion der Anwendung erwartet.

Beispiel-Anwendungsfall: Mandanten-Kunden einer gemeinsam genutzten Umgebung müssen in der Lage sein, Änderungen an der Auswirkungs-, Dringlichkeits- und Prioritätsmatrix vorzunehmen, um die Priorität in ihrer Domäne festzulegen.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung.

So funktioniert Domain Separation in Datenklassifizierung

Für die Domänentrennung verwendet die Anwendung Prozesstrennung für Datenklassifizierung Tabelle [sys_Data_classification]. Für die Tabelle „Wörterbuch-Datenklasse“ [m2m_dictionary_dataclass] wird Datentrennung verwendet. Weitere Informationen zur Daten- und Prozesstrennung finden Sie unter Domänentrennung erklärt .

Zugehörige Informationen

Domänentrennung für Service Provider

Automatische Übersetzung

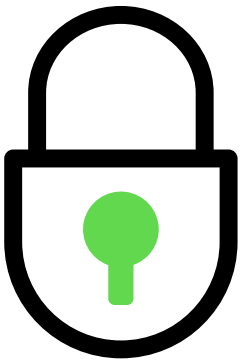
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

servicenow

Verschlüsselung

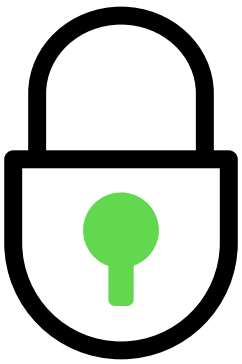
Schützen Sie Ihre sensiblen Daten, und halten Sie sich an regulatorische#Anforderungen und Standards.

Key Management Framework



Verwenden Sie das Key Management Framework (KMF), um die Ausführung kryptografischer Vorgänge in Ihrer ServiceNow-Instanz vollständig anzupassen und zu verwalten.

Feldverschlüsselung



Verwenden

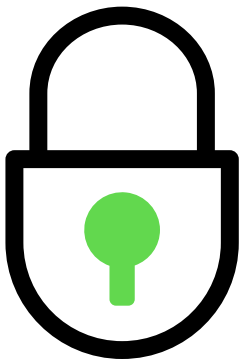
Feldverschlüsselung

Ermöglicht und verweigert den Zugriff auf verschlüsselte Daten basierend auf der Anwenderrolle.

Feldverschlüsselung

Enthält grundlegende Schlüsselverwaltung mit Verschlüsselungsmodulen.

Feldverschlüsselung Enterprise



Verwenden

Feldverschlüsselung

Ermöglicht und verweigert den Zugriff auf verschlüsselte Daten basierend auf der Anwenderrolle.

Feldverschlüsselung

Enthält grundlegende Schlüsselverwaltung mit Verschlüsselungsmodulen.

Cloud-Verschlüsselung

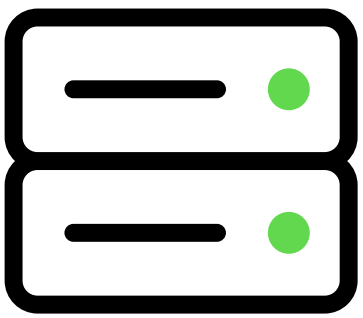


Verschlüsseln Sie Ihre Instanzdatenbank mit Blockverschlüsselung zusammen mit verbesserter Schlüsselverwaltung.

Berechtigungspaket für Plattformverschlüsselung

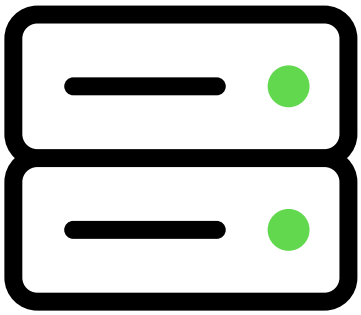
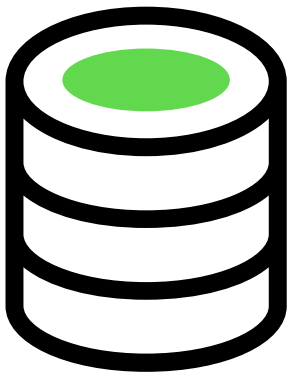


Vollständige Datenträgerverschlüsselung (FDE)



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Führen Sie ein Upgrade auf unbegrenzte Nutzung durch Feldverschlüsselung Enterprise , Cloud-Verschlüsselung und Datenbankverschlüsselung.	Die vollständige Datenträgerverschlüsselung wendet die Verschlüsselung nur auf das gesamte Speichersystem innerhalb des Datenbankservers an. Da dies die einzige Komponente ist, die Kundendaten speichert.
Edge Encryption	**Zertifikate**	**Datenbankverschlüsselung**
		
Verschlüsselt vertrauliche Daten in Ihrem Unternehmen, bevor Daten über das Internet an Ihre ServiceNow-Instanz gesendet werden. Daten bleiben im Ruhezustand in der Instanz verschlüsselt.	Verwenden Sie Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.	Verschlüsseln Sie alle gespeicherten Daten in Echtzeit, um Daten online und offline ohne Verlust der Funktionalität zu schützen.

Key Management Framework

Verwenden Sie Key Management Framework(KMF) Zum Generieren, Austauschen, Speichern, Verwenden und Ersetzen der kryptografischen Schlüssel, die zum Verschlüsseln und Entschlüsseln vertraulicher Daten auf Ihrem verwendet werden ServiceNow Instanz.

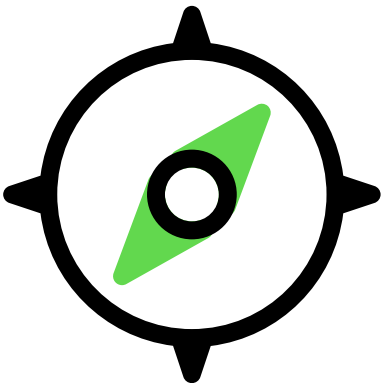
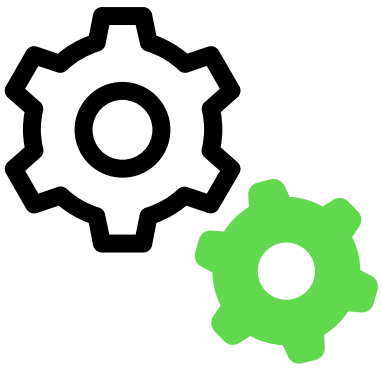
Schlüsselverwaltung bezieht sich auf die Aktivitäten, die an der Verarbeitung Ihrer kryptografischen Schlüssel und zugehörigen Sicherheitsparameter während des Lebenszyklus des Schlüssels beteiligt sind. Key Management Framework Basiert auf National Institute of Standards and Technology (NIST) 800-57 Richtlinien. Gemäß diesen Richtlinien können Sie verwenden KMF An:

- Weisen Sie dedizierte Rollen für kryptografische Verwaltung und Vorgänge, Audits und Integration zu.
- Erstellen Sie kryptografische Module, um kryptografische Spezifikationen für eindeutige kryptografische Zwecke und Schlüsseltypen zu konfigurieren.
  - Symmetrischer Schlüssel: Verschlüsselung und Entschlüsselung, Schlüsselumbruch und -Entpackung und Authentifizierung
  - Asymmetrischer Schlüssel: Generierung und Verifizierung digitaler Signaturen, Verschlüsselung und Entschlüsselung, Schlüsselumbruch und -Entpackung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

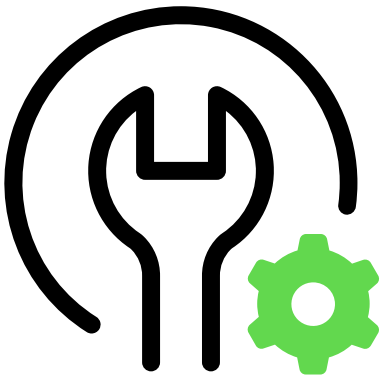
- Verwalten Sie Ihren Schlüssellebenszyklus, um Schlüssel zu generieren, zu rotieren, zu widerrufen und anzuhalten, einschließlich Unterstützung mehrerer schlüssellebenszyklusstatus
- Erstellen Sie Modulzugriffsrichtlinien (Zuordnungen), um Zugriffssteuerungen zu erzwingen und nur Anwendern und Skripts Zugriff zu gewähren, die Sie auswählen.
- Schützen Sie Ihre kryptografischen Schlüssel mit dem Federal Information Processing Standard (FIPS) 140-2-L3 Hardware Root of Trust (rot), der Public Key Infrastructure (PKI), der Schlüsselhierarchie und der Umschlagverschlüsselung.
- Weisen Sie Anwendern die Auditing-Rolle zu, damit sie Auditinformationen wie Statistiken zur Schlüsselnutzung anzeigen können.

Erste Schritte

Erkunden Sie das Key Management Framework	Konfigurieren des Key Management Framework	Key Management Framework-Referenz
		
Erfahren Sie mehr über die Komponenten des Key Management Framework und wie Sie sie verwenden, um zu verwalten, wie kryptografische Vorgänge in Ihrer Instanz ausgeführt werden.	Erstellen und verwalten Sie Schlüsselverwaltungskomponenten, um anzupassen und zu verwalten, wie kryptografische Vorgänge auf Ihrem ausgeführt werden ServiceNow Instanz.	Erstellen und verwalten Sie Schlüsselverwaltungskomponenten, um anzupassen und zu verwalten, wie kryptografische Vorgänge auf Ihrem ausgeführt werden ServiceNow Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen des Key Management Framework



Verwenden Sie KMF-Funktionen, um#Schlüssel zu verwalten, zu widerrufen oder zu rotieren, um vertrauliche Daten mit den neuesten Verschlüsselungsmaterialien und Lebenszyklusvorgängen zu sichern.

Aktivierungsinformationen

Die ServiceNow Das Abonnementpaket „Platform Encryption“ ist eine gewerbliche Gruppenberechtigung, die umfasst Key Management Framework, Feldverschlüsselung Enterprise, Cloud-Verschlüsselung, Und Datenbankverschlüsselung.

Feldverschlüsselung Enterprise Ist die unbegrenzte Lizenz von Feldverschlüsselung. Die Feldverschlüsselung Das Enterprise-Plugin ist mit der Aktivierung des Plugins com.glide.now.platform.encryption verfügbar. Weitere Informationen finden Sie unter Abonnementpaket für Verschlüsselung und Schlüsselverwaltung .

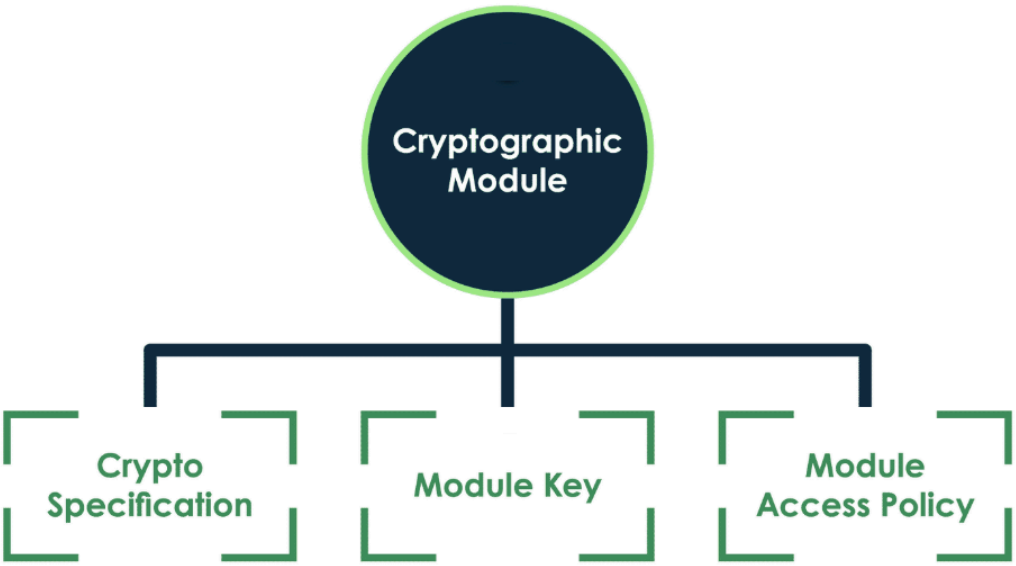
Hinweis: KMF Unterstützt keine Domänentrennung, kann jedoch mit lokalen Instanzen verwendet werden.

Erkunden Sie das Key Management Framework

Erfahren Sie mehr über die Komponenten von Key Management Framework(KMF), und wie Sie sie verwenden, um zu verwalten, wie kryptografische Vorgänge in Ihrer Instanz ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten des Key Management Framework



Key Management Framework Besteht aus den folgenden Komponenten.

Kryptografische Module

KMF konzentriert sich auf die Verwaltung kryptografischer Module. Diese Module fungieren als übergeordneter Datensatz für die anderen Komponenten. Sie definieren, welche Daten in Ihrer Instanz verschlüsselt werden und welche Verschlüsselungsmethode verwendet werden soll. Mit mehreren Modulen können Sie verschiedene Bereiche Ihrer Instanz mit unterschiedlichen Spezifikationen verschlüsseln.

Sie können beispielsweise ein Modul erstellen, um die Daten in Ihrer Human Resources-Anwendung für Anwender mit einer bestimmten Rolle zu sichern. Sie können dann ein weiteres Modul erstellen, um Incident-Beschreibungen zu verschlüsseln, die für bestimmte Anwender sichtbar sind, basierend auf einem von Ihnen erstellten Skript.

Modulzugriffsrichtlinien werden gefunden, indem Sie zu navigieren **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an. Weitere Informationen zu diesen Modulen finden Sie unter Kryptografisches Modul – Übersicht.

Modulschlüssel

Kryptografische Schlüssel sind Zeichenfolgen, die in der Kryptografie verwendet werden. Wenn sie zusammen mit einem kryptografischen Algorithmus verwendet werden, können sie Ihre Daten codieren oder decodieren. Diese Schlüssel werden von den kryptografischen Spezifikationen verwendet, die Ihren Modulen zugewiesen sind. Sie können einen von generierten Schlüssel verwenden ServiceNow, Oder laden Sie Ihren eigenen Schlüssel hoch.

Sie können auf die Modulschlüssel für ein kryptografisches Modul in zugreifen **Modulschlüssel** Zugehörige Liste in kryptografischen Moduldatensätzen. Weitere Informationen zu Modulschlüsseln finden Sie unter Schlüssel auf Instanzebene im Key Management Framework.

Kryptografische Spezifikationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine kryptografische Spezifikation definiert Algorithmen, die zum Verschlüsseln Ihrer Daten verwendet werden. Diese Algorithmen verwenden einen kryptografischen Schlüssel, um Ihre Daten zu codieren oder zu decodieren. Das Zuweisen einer kryptografischen Spezifikation zum Modul bestimmt, wie die diesem Modul zugewiesenen Daten verschlüsselt werden.

Sie können auf die Modulschlüssel für ein kryptografisches Modul in zugreifen **Krypto-Spezifikationen** Zugehörige Liste in kryptografischen Moduldatensätzen. Weitere Informationen zu Modulschlüsseln finden Sie unter Übersicht über kryptografische Spezifikationen.

Modulzugriffsrichtlinien

Modulzugriffsrichtlinien (Maps) sind die Zugriffssteuerungen, die Sie auf Ihre kryptografischen Module anwenden. Verwenden Sie diese Richtlinien, um zu bestimmen, welche Anwender und Skripts auf Daten zugreifen können, die von einem kryptografischen Modul verschlüsselt werden.

Suchen Sie nach Modulzugriffsrichtlinien, indem Sie auswählen **Zeigen Sie Zugriffsrichtlinien an** Link in kryptografischen Moduldatensätzen. Weitere Informationen finden Sie unter Übersicht über die Modulzugriffsrichtlinie.

Key Management Framework-Workflow

1. Weisen Sie KMF-Rollen zu

Administratoren müssen damit beginnen, sich selbst die Rolle sn_kmf.admin zuzuweisen. Mit dieser Rolle können Sie KMF-Funktionen verwenden und anderen Anwendern KMF-Rollen zuweisen.

2. Konfigurieren Sie KMF-Einstellungen

Konfigurieren Sie Ihre Feldverschlüsselungseinstellungen, um entweder bereitgestellte Schlüssel oder eigene kundenbereitgestellte Schlüssel (CSK) für die Verschlüsselung auszuwählen.

3.Erstellen Sie kryptografische Module

Verwenden Sie kryptografische Module, um einen Satz von Daten in Ihrer Instanz auszuwählen, die verschlüsselt werden sollen. In späteren Schritten weisen Sie eine kryptografische Spezifikation zu, um zu bestimmen, wie diese Daten verschlüsselt werden, und eine Modulzugriffsrichtlinie, um zu bestimmen, wer die Daten entschlüsseln kann.

4. Erstellen Sie eine kryptografische Spezifikation

Die kryptografische Spezifikation definiert eine Verschlüsselungsmethode. Nach der Zuweisung an ein Modul definiert es, wie die diesem Modul zugewiesenen Daten verschlüsselt werden.

5. Erstellen Sie Modulzugriffsrichtlinien

Nachdem Sie Module zum Sichern Ihrer Daten erstellt haben, erstellen Sie Modulzugriffsrichtlinien, um zu steuern, welche Anwender und Skripts auf die verschlüsselten Daten zugreifen können.

6. Erstellen Sie eine Lebenszyklusrichtlinie für kryptografische Module

Diese Richtlinien legen Beschränkungen für kryptografische Module fest, z. B. wie lange ein kryptografischer Schlüssel gültig ist. Diese Richtlinien können Ihre kryptografischen Module schützen, indem sie ihr Risiko beschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile des Key Management Framework

Leistung	Funktion	Anwender
Schützen Sie Ihre vertraulichen und proprietären Daten.	Verschlüsselung und Schlüsselverwaltung	Alle
Halten Sie Compliance mit ein NIST 800-57 Richtlinien. Diese Richtlinien werden vom National Institute of Standards and Technology bereitgestellt, um das Cybersicherheitsrisiko für Ihre Netzwerke und Daten zu reduzieren.	Verschlüsselung und Schlüsselverwaltung	Sicherheitsadministratoren
Verwenden Sie das Key Management Framework, um Ihre kryptografischen Schlüssel zu generieren, hochzuladen, anzuzeigen und zu verwalten. Verwenden Sie die Schlüsselrotation für die manuelle oder geplante Rotation Ihrer Schlüssel, um die Sicherheit zu erhöhen.	Key Management Framework	Sicherheitsadministratoren

Kryptografisches Modul – Übersicht

Die Key Management Framework(KMF) Konzentriert sich auf die Verwaltung kryptografischer Module. Verwenden Sie diese Module, um einen kryptografischen Mechanismus auszuwählen und zu definieren, wo sie auf Ihre Instanz angewendet werden.

Kryptografische Module sind das Herzstück von KMF. Sie definieren die spezifischen kryptografischen Mechanismen, die für kryptografische Vorgänge für einen bestimmten Anwendungsfall verwendet werden.

Sie möchten beispielsweise die Daten in Ihrer Human Resources-Anwendung mit einem AES-CBC mit einem 256-Bit-symmetrischen Schlüssel sichern. Zu diesem Zweck können Sie ein Modul erstellen.

Kryptografische Module unterstützen auch die Verwaltung des Schlüssellebenszyklus. Sie können Ihre kryptografischen Schlüssel erstellen, rotieren und Ihre Verschlüsselungsmethode definieren. Kryptografische Module bestehen aus den folgenden Komponenten:

Kryptografische Spezifikation

Definiert, welcher Algorithmus für die Verschlüsselung verwendet werden soll und woher der Schlüssel stammt. Alle Schlüssel verwenden den Advanced Encryption Standard with Cipher Block Chaining (AES CBC), Sie können jedoch entweder 128 oder 256 Bit auswählen. Diese Spezifikation deckt sowohl asymmetrische als auch symmetrische schlüsselbasierte kryptografische Vorgänge ab.

Hinweis: Die symmetrische Verschlüsselung verwendet einen einzelnen Schlüssel für die Verschlüsselung und Entschlüsselung. Die asymmetrische Verschlüsselung verwendet ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung.

Kryptografische Schlüssel

Der Schlüssel, den Ihr Modul zum Codieren oder Decodieren kryptografischer Daten verwendet. Dieser Schlüssel kann von Ihrer Instanz oder einem vom Kunden bereitgestellten Schlüssel generiert werden, den Sie erstellen und hochladen.

Modulzugriffsrichtlinien

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

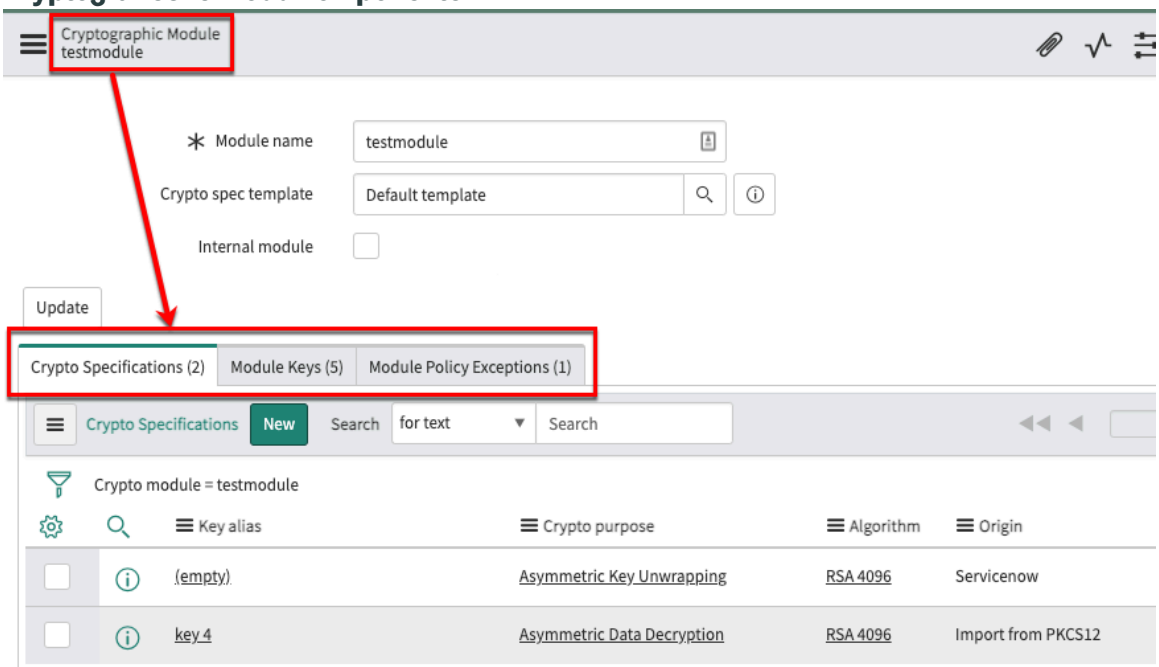
Modulzugriffsrichtlinien sind die Zugriffssteuerungsmechanismen, die einschränken, ob Daten verschlüsselt oder entschlüsselt werden können.

Modulrichtlinienausnahmen

Ein Steuerungsmechanismus zum Definieren von Ausnahmen für eine Modulzugriffsrichtlinie.

Der folgende Bildschirm zeigt diese allgemeinen Komponenten in einem kryptografischen Modul:

Kryptografische Modulkomponenten



Details zum Erstellen kryptografischer Module finden Sie unter Erstellen Sie ein kryptografisches Modul.

Übersicht über kryptografische Spezifikationen

Die kryptografische Spezifikation ist die Komponente, die Aspekte Ihres kryptografischen Moduls definiert, einschließlich seines kryptografischen Zwecks und des zu verwendenden Verschlüsselungsalgorithmus.

Kryptografische Spezifikationen können auf einen angegebenen kryptografischen Zweck zugeschnitten werden und sowohl asymmetrische als auch symmetrische schlüsselbasierte kryptografische Vorgänge abdecken. Die Auswahl eines kryptografischen Zwecks bietet weitere Auswahlmöglichkeiten, insbesondere für eine Reihe unterstützter Algorithmen und Schlüssellängenkonfigurationen.

Kryptografische Zwecke, Algorithmen und Schlüsselinformationen

Kryptografischer Zweck	Algorithmus	Wichtige Informationen
Asymmetrische Datenentschlüsselung	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Asymmetrische Datenverschlüsselung	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Asymmetrischer Schlüssel Wird Entpackt	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kryptografische Zwecke, Algorithmen und Schlüsselinformationen (Fortsetzung)

Kryptografischer Zweck	Algorithmus	Wichtige Informationen
Asymmetrisches Schlüsselumbruch	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Signaturerzeugung	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Signaturverifizierung	RSA	Asymmetrisch: 2048-Bit-, 3072-Bit- und 4096-Bit-Schlüssel
Symmetrische Authentizität	HMAC	Symmetrisch: 256-Bit-, 384-Bit- und 512-Bit-Schlüssel
Symmetrische Datenverschlüsselung/-Entschlüsselung*	AES-CBC *	Symmetrisch: 128-Bit-, 192-Bit-, 256-Bit-Schlüssel
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM **	
Symmetrisches Umwickeln/Entpacken Des Schlüssels*	AES-CBC *	Symmetrisch: 128-Bit-, 192-Bit-, 256-Bit-Schlüssel
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM **	

* AES-CBC unterstützt Optionen zur Wahrung der Gleichstellung. Feldverschlüsselung Enterprise Verwendet AES-CBC.

** AES-GCM verfügt über integrierte Datenintegrität.

Die Konfiguration dieser Parameter wird in behandelt Erstellen Sie ein kryptografisches Modul.

Übersicht über die Modulzugriffsrichtlinie

Modulzugriffsrichtlinien (Maps) sind Zugriffssteuerungen, die Sie auf Ihre kryptografischen Module anwenden. Verwenden Sie diese Zugriffsrichtlinien, um zu entscheiden, welche Anwender und Skripts auf Daten zugreifen können, die von einem kryptografischen Modul verschlüsselt werden.

Modulzugriffsrichtlinien

Hinweis: Zur Verwendung von ist ein Abonnement erforderlich Feldverschlüsselung Enterprise Funktionalität. Siehe Feldverschlüsselung aktivieren Weitere Informationen zu finden Feldverschlüsselung Enterprise.

Modulzugriffsrichtlinien werden mit eingeführt Key Management Framework(KMF) Im Basissystem.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriffsrichtlinien erweitern die rollenbasierten Bezeichnungen, die mit den Verschlüsselungsmodulen bereitgestellt wurden. Modulzugriffsrichtlinien können auf folgenden basieren:

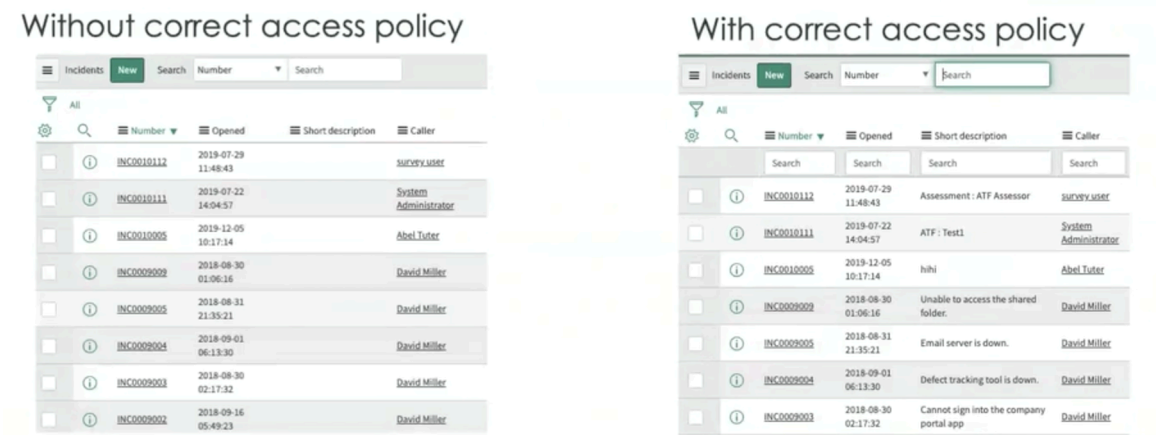
- Standard (Umfang)
- Rolle
- Systemanwender
- Skript
- Ressourcenaustausch

Hinweis: Details siehe Key-Management-Framework-Ressourcenaustausch.

In einem kryptografischen Modul müssen Sie die richtigen Modulzugriffsrichtlinien konfigurieren, um den Zugriff auf verschlüsselte Daten zu ermöglichen. Ohne eine Modulzugriffsrichtlinie, die einem kryptografischen Modul zugeordnet ist, sind verschlüsselte Daten für Anwender nicht sichtbar, und zugehörige Felder und Spalten in Listen werden als leer angezeigt.

In diesem Beispiel blendet das Fehlen einer Modulzugriffsrichtlinie im Feld verschlüsselte Kurzbeschreibung den Inhalt für alle Anwender aus, die auf die Incident-Tabelle zugreifen. Wenn eine Modulzugriffsrichtlinie vorhanden ist, können nur Anwender mit einer bestimmten Rolle die verschlüsselten Daten sehen.

Verschlüsselte Kurzbeschreibungen mit und ohne Modulzugriffsrichtlinien



Hinweis: Die Daten in der Spalte werden auch für Anwender ohne die richtige Rolle, die in der Modulzugriffsrichtlinie angegeben ist, leer angezeigt.

Siehe Erstellen Sie eine Modulzugriffsrichtlinie Für Setup.

Autogen-Richtlinien

Autogen-Richtlinien werden automatisch basierend auf der standardmäßigen Modulzugriffsrichtlinie generiert, die für das angegebene kryptografische Modul definiert ist. Wenn keine Richtlinien auf granularer Ebene definiert sind, wenn das System oder ein Skript versucht, auf das angegebene kryptografische Modul zuzugreifen, werden diese globalen Richtlinien generiert und angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Automatische Richtlinienregeln werden nicht für geplante Aufgabentypen oder Feldverschlüsselungsmodule (Module, in denen sich das übergeordnete Modul befindet) angewendet Feldverschlüsselung).

Schlüssel auf Instanzebene im Key Management Framework

Erfahren Sie mehr über Key Management Framework(KMF) Schlüsselstruktur, die Umschlagverschlüsselung verwendet, um sicherzustellen, dass alle Plattformschlüssel unter sind KMF Die Verwaltung wird durch eine Schlüsselkette geschützt. Kundendatenverschlüsselungsschlüssel (CDEKs) erstellt von KMF Sind auch in dieser Struktur enthalten

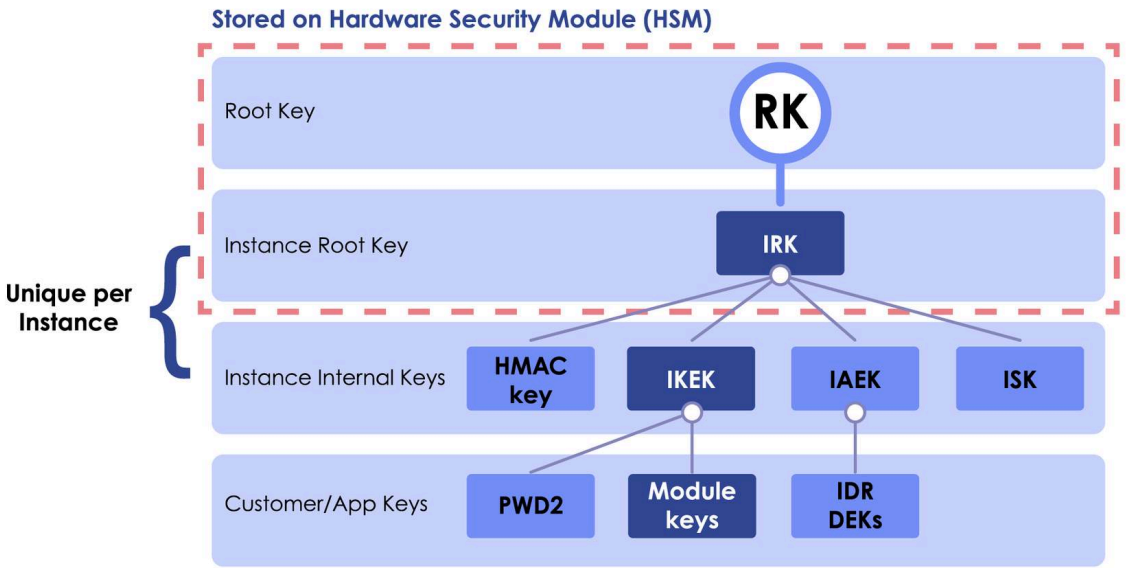
an.

KMF-Schlüsselspeicherarchitektur

Die KMF Die Schlüsselstruktur verwendet das SafeNet KeySecure Hardware Security Module (HSM). Das HSM ist physisch und elektronisch manipulationssicher, um die zu erfüllen Sicherheitsstandard FIPS 140-2-L3 . KMF Verwendet Umschlagverschlüsselung, um sicherzustellen, dass alle Plattformschlüssel unter KMF Die Verwaltung wird durch eine Schlüsselkette geschützt, einschließlich der Modulschlüssel, die von generiert werden können KMF.

Umschlagverschlüsselung

Umschlagverschlüsselung ist die Praxis, einen Schlüssel mit einem anderen Schlüssel zu verschlüsseln, auch als Umbruch bezeichnet. Modulschlüssel werden durch den Instanzschlüssel-Verschlüsselungsschlüssel (IKEK) verschlüsselt, der wiederum durch den Instanzstammschlüssel (IRK) verschlüsselt wird, der schließlich durch den Stammschlüssel (Root Key, RK) verschlüsselt wird. Da auf das IRK nur vom HSM zugegriffen werden kann, muss das IKEK zur Entschlüsselung hochgeladen werden.



Auf Instanzebene KMF Definiert mehrere Schlüssel, die intern für unterschiedliche kryptografische Zwecke im verwendet werden ServiceNow AI Platform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Tabelle enthält Beispiele für eine Teilmenge der verfügbaren Schlüssel, die von verwaltet und geschützt werden KMF.

Schlüssel	Standort	Beschreibung
Stammschlüssel (RK)	Hardware-Sicherheitsmodell (HSM)	Stammschlüssel, der zum Entschlüsseln des IRK verwendet wird.
Instanz-Stammschlüssel (IRK)	HSM	Ein für Ihre Instanz eindeutiger Schlüssel, der zum Umhüllen der Verschlüsselung mehrerer interner Instanzschlüssel verwendet wird.
Instanz-HMAC-Schlüssel (IHK)	Instanz	Das IHK ist pro Instanz eindeutig und wird intern für Zwecke des Hash-basierten Message Authentication Code (HMAC) verwendet. Das IHK hilft bei der Überprüfung der Authentizität und Integrität von Modulschlüsseln und wird entweder in KeySecure oder im Dateischlüsselspeicher eingeschlossen.
Instanzschlüssel-Verschlüsselungsschlüssel (IKEK)	Instanz	Das IKEK umschließt die Modulschlüssel und wird entweder in KeySecure oder den Dateischlüsselspeicher eingeschlossen.
Asymmetrischer Verschlüsselungsschlüssel für Instanz (IAEK)	Instanz	Ein für Ihre Instanz eindeutiger Schlüssel, der intern für asymmetrische Verschlüsselungszwecke verwendet wird. Das IAEK wird verwendet, um während vertrauliche Nachrichten zwischen einer Instanz zu übertragen Key Exchange Oder Instanzübergreifende Datenreplikation Verbrauchergenehmigung.
Instanzsignaturschlüssel (ISK)	Instanz	Ein für Ihre Instanz eindeutiger Schlüssel, der intern zu Signierungszwecken verwendet wird.
Password2 (PW2)	Instanz	Mit KMF, Der Schlüssel für PW2 Felder werden vollständig von verwaltet KMF.
Kundendaten-Verschlüsselungsschlüssel (CDEK)	Instanz	Verschlüsselungsschlüssel, die über erstellt wurden KMF Sind von IKEK-Umschläge verschlüsselt.
Datenverschlüsselungsschlüssel für Instanzdatenreplikation (IDR) (DEK)	Instanz	Bestimmte Verschlüsselungsschlüssel, die für den IDR-Prozess verwendet werden.

Konfigurieren des Key Management Framework

Erstellen und verwalten Sie Schlüsselverwaltungskomponenten, um anzupassen und zu verwalten, wie kryptografische Vorgänge auf Ihrem ausgeführt werden ServiceNow Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuweisen Key Management Framework Rollen

Administratoren mit der Rolle „Security_admin“ können zuweisen Key Management Framework(KMF) Administratoren, die wiederum andere zuweisen können Key Management Framework Rollen.

Vorbereitungen

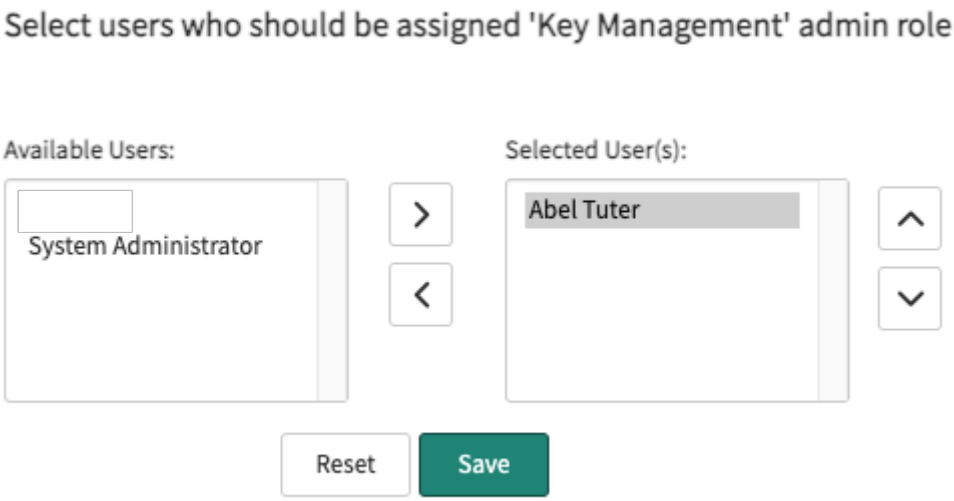
Erforderliche Rolle: admin und security_admin

Sie müssen die Rolle Security_admin erhöhen, bevor Sie zuweisen KMF administratorrolle. Anweisungen dazu finden Sie unter Auf eine privilegierte Rolle hochstufen.

Wichtig: KMF Zur Verwendung von sind Rollen erforderlich Key Management Framework. Anwender ohne KMF Rollen können nicht auf Listen, Tabellen und Module zugreifen, die zum Konfigurieren der Schlüsselverwaltung verwendet werden.

Prozedur

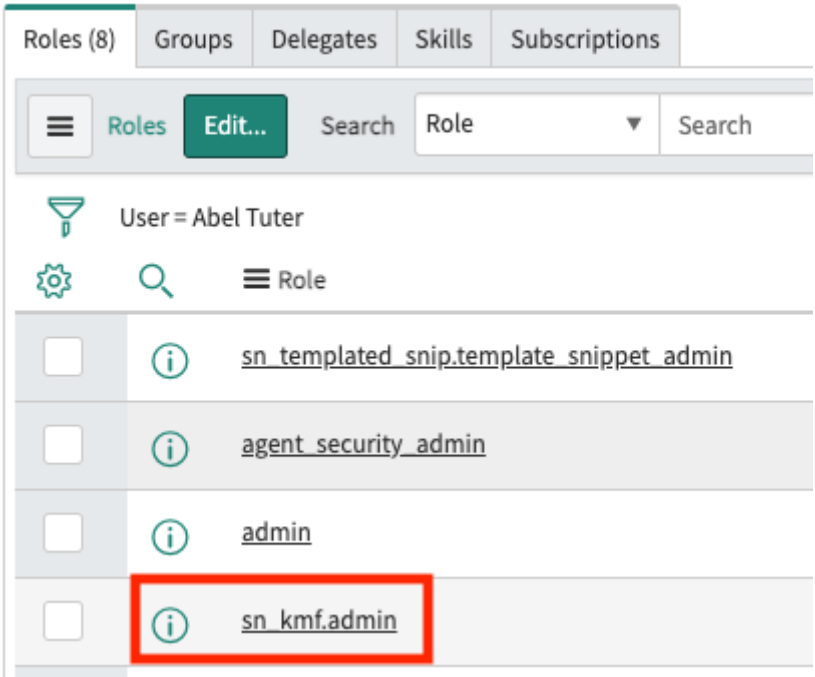
1. Erhöhen Sie die Rolle „Sicherheitsadministrator“.
2. Navigieren zu **Anwenderadministration** > **Anwender** Und wählen Sie den Anwender aus, der sein soll KMF administrator.
3. Wenn der Anwender nicht bereits über die Rollen admin und Security_admin verfügt, wählen Sie aus **Bearbeiten** Fügen Sie unter der zugehörigen Liste Rollen hinzu **Administrator** Und **Security _admin** .
4. Navigieren zu **Systemsicherheit** > **Administration der Schlüsselverwaltung**an.
5. Wählen Sie den Anwender aus, der Sie sein möchten KMF administrator in **Verfügbare Anwender** Und verschieben Sie sie in die **Ausgewählte Anwender** Spalte.



6. Wählen Sie **Speichern**.
7. Navigieren zu **Anwenderadministration** > **Anwender** Und wählen Sie den Anwender aus, dem Sie gerade die KMF-Administratorrolle zugewiesen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

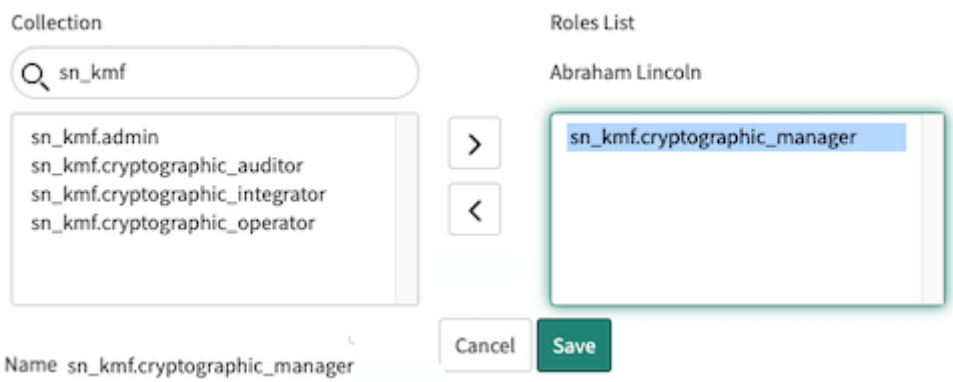
Dieser Anwender hat jetzt die Rolle sn_kmf.admin in der zugehörigen Liste „Rollen“. Dieser Anwender kann jetzt andere KMF-Rollen zuweisen.



Nächste Maßnahme

Wenn Sie über die KMF-Administratorrolle verfügen, führen Sie die folgenden Schritte aus, um andere KMF-Rollen zuzuweisen:

1. Navigieren zu **Anwenderadministration** > **Anwender** Und wählen Sie den Anwender aus, für den Sie eine andere KMF-Rolle haben möchten, z. B. KMF Cryptographic Manager.
2. Klicken Sie in der zugehörigen Liste Rollen auf **Bearbeiten** Und wählen Sie die KMF-Rollen aus, die Sie den Anwendern zuweisen möchten. Alle KMF-Rollen beginnen mit `sn_kmf` .



Nächste Maßnahme

Um mehr über die verfügbaren zu erfahren KMF Rollen, siehe Mit Key Management Framework installierte Rollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen

Konfigurieren Sie die zu verwendenden Feldverschlüsselungseinstellungen ServiceNow Bereitgestellte Schlüssel oder eigene vom Kunden bereitgestellte Schlüssel (CSK) für die Verschlüsselung auf dem ServiceNow AI Platform.

Vorbereitungen

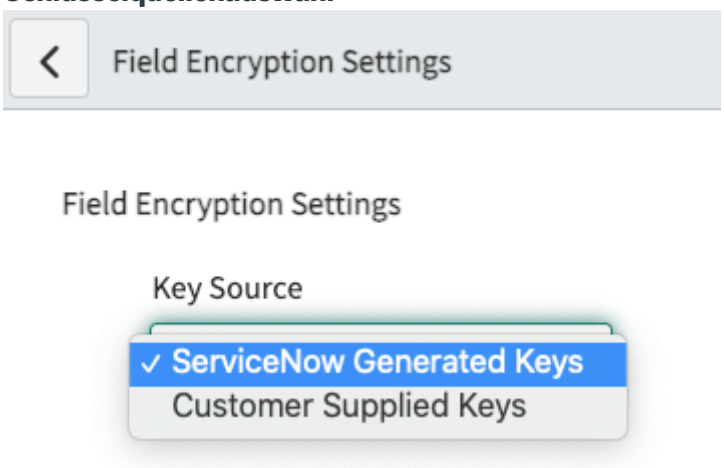
Vom Kunden bereitgestellte Schlüssel werden nur mit unterstützt Feldverschlüsselung Enterprise.

Erforderliche Rolle: sn_kmf.cryptographic_Manager und Security_admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Einstellungen für Feldverschlüsselung**an.
2. Wählen Sie im Feld Verschlüsselungseinstellungen eine der Optionen aus **Von ServiceNow generierte Schlüssel** Oder **Vom Kunden Bereitgestellte Schlüssel** Von **Schlüsselquelle** Liste.

Schlüsselquellenauswahl



Mit dieser Option wird geändert Com.Glide.Encryption.cle_kmf.key_Source Eigenschaft zu entweder **Von ServiceNow generierte Schlüssel** Oder **Vom Kunden Bereitgestellte Schlüssel** .

3. Wählen Sie **Speichern**.

Nächste Maßnahme

- Wenn Sie eigene vom Kunden bereitgestellte Schlüssel verwenden, finden Sie weitere Informationen unter Mit vom Kunden bereitgestellte Schlüssel werden verwendet Feldverschlüsselung Enterprise.
- Wenn Sie verwenden ServiceNowAngegebene Schlüssel. Beginnen Sie mit der Erstellung Ihres kryptografischen Moduls. Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul.

Erstellen Sie ein kryptografisches Modul

Erstellen Sie ein kryptografisches Modul, um die für kryptografische Vorgänge verwendeten Mechanismen zu definieren. Nachdem Sie das Modul erstellt haben, erstellen Sie eine kryptografische Spezifikation, in der Sie einen Algorithmus für die Verschlüsselung definieren und einen Schlüssel generieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Wenn Sie eigene Schlüssel bereitstellen, wechseln Sie zu Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch.

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird

In diesem Verfahren werden Optionen beschrieben, die mit verfügbar sind KMF In ServiceNow Plattformbasissystem. Feldverschlüsselung Enterprise Funktionalität ist nur verfügbar, wenn `com.glide.now.platform.encryption` Plugin ist aktiv. Siehe Feldverschlüsselung aktivieren Weitere Informationen zum Abrufen von Feldverschlüsselung Enterprise. Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul für Feldverschlüsselung.

Hinweis: Datensätze des kryptografischen Moduls [sys_kmf_crypto_Module] können nicht gelöscht werden.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Neu erstellen**an.
2. Füllen Sie die Felder des Formulars aus.

Kryptografische Modulfelder

Feld	Beschreibung
Modulname	Alphanumerische Zeichenfolge, auf die beim Ausführen von Skripts verwiesen werden soll.
Krypto-Spezifikationsvorlage	Wählen Sie aus **Standard** Vorlage zum Erstellen des kryptografischen Moduls, da sie Zuordnungen unterstützter Algorithmen für Krypto-Spezifikationen enthält.
Standardwert der Modulzugriffsrichtlinie	○ Auf Systemstandard verlassen: ○ Ablehnen ○ Titel
Tatsächliches Ergebnis der Modulzugriffsrichtlinie	Ablehnen oder nachverfolgen, basierend auf dem Standardrichtlinienwert oder dem bei der Erstellung der Modulzugriffsrichtlinie ausgewählten Wert.
Name	Krypto-Modulname, dem der Name des Anwendungsbereichs vorangestellt ist.
Lebenszyklusstatus des Krypto-Moduls	Der Lebenszyklus bezieht sich auf die Erstellung, Verwendung und Deaktivierung eines kryptografischen Moduls. Auf festlegen **Entwurf** Anfänglich während der Konfiguration. Wenn Sie das Modul verwenden, legen Sie dieses Feld auf fest **Veröffentlicht** . Die Standardvorlage wird automatisch auf „veröffentlicht“ festgelegt.

3. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

⚠ Warnung:

Für Anwender mit Legacy-Verschlüsselungsunterstützung:

Wenn Sie die nicht-Enterprise-Version von verwenden Feldverschlüsselung, Sie sind auf fünf Module beschränkt. Wenn Sie diesen Grenzwert überschritten haben, erhalten Sie die folgende Warnung:

Diese Einfügung überschreitet die Anzahl der veröffentlichten Module für Feldverschlüsselung Berechtigt für das Abonnementprodukt. Das Enterprise-Abonnement für Feldverschlüsselung Ist für zusätzliche Module erforderlich. Wenden Sie sich an Ihr Account-Team.

Nach erfolgreicher Übermittlung wird Ihr kryptografisches Modul in der Tabelle „kryptografische Module“ aufgeführt. Das System stellt dem Namen den Bereich vor, um Konflikte mit anderen bereichsbezogenen Anwendungen zu vermeiden. Beispiel: Wenn Sie ein Modul mit dem Namen erstellt haben `Mein_Krypto_Modul` Im globalen Anwendungsbereich wird der Name als gespeichert `Global.my_crypto_Module` .

Nächste Maßnahme

Erstellen Sie eine kryptografische Spezifikation

an.

Erstellen Sie eine kryptografische Spezifikation

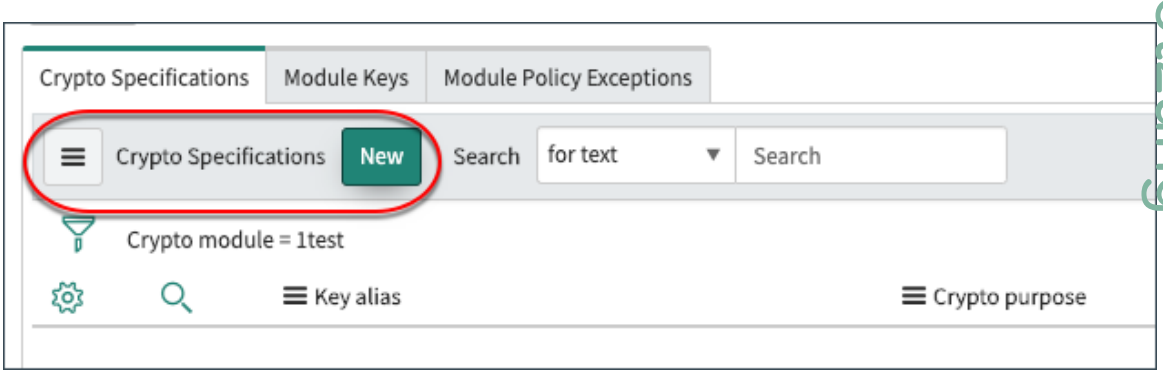
Nachdem Sie ein kryptografisches Modul erstellt haben, erstellen Sie eine kryptografische Spezifikation, um die Modulalgorithmen zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Prozedur

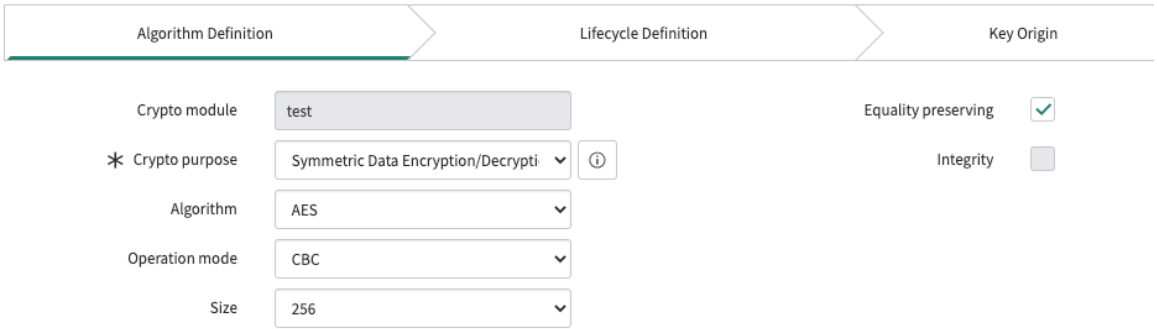
1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie das kryptografische Modul für die Definition aus, um die Konfigurationsoptionen zu öffnen.
3. Auf der **Krypto-Spezifikationen** Wählen Sie die Registerkarte aus **Neu** .



4. Füllen Sie das Formular „Algorithmusdefinition“ aus.
   Details siehe Übersicht über kryptografische Spezifikationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Bildschirm „Algorithmusdefinition“ wird geöffnet. Wählen Sie Optionen für die Schlüsselgenerierung aus. Wiederholen Sie diesen Schritt, um mehrere Schlüssel für das ausgewählte Krypto-Modul zu generieren.

Algorithmusdefinitionsfelder

Feld	
Krypto-Modul	Schreibgeschützt. Name des ausgewählten kryptografischen Moduls wird angezeigt.
Kryptografischer Zweck	Wählen Sie den Zweck dieses Moduls aus. Sie können ihn beispielsweise für Datenverschlüsselung, Signaturgenerierung oder Schlüsselumbruch verwenden. Die verfügbaren Algorithmen werden basierend auf dem ausgewählten Krypto-Zweck angepasst. Details siehe Übersicht über kryptografische Spezifikationen.
Algorithmus	Typ des Algorithmus, der zum Erreichen des Krypto-Zwecks verwendet wird. Der Algorithmus steuert auch den Schlüsselursprung. Passt sich automatisch basierend auf dem ausgewählten Krypto-Zweck an. Übersicht über kryptografische Spezifikationen Für Details.
Betriebsmodus	Dieses Feld kann basierend auf dem ausgewählten Krypto-Zweck angezeigt werden.
Größe	Wählen Sie die Bitgröße aus.
Hash	Dieses Feld wird basierend auf dem ausgewählten Algorithmus verfügbar.
Gleichstellungserhaltung	Aktiviert die nicht deterministische Verschlüsselung. Diese Option wird angezeigt, wenn Sie auswählen **Symmetrische Datenverschlüsselung/-Entschlüsselung** Mit **AES** Und in **Verschlüsselungsblockverketten (CBC)** Modus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	
	Wenn Sie diese Option auswählen, sind die codierten Daten jedes Mal identisch, wenn dieselben Daten erneut verschlüsselt werden. Die nicht deterministische Verschlüsselung unterstützt das Filtern einer Liste verschlüsselter Daten mit Gleichheitsvergleichsoperatoren nicht.
Integrität	Der GCM-Betriebsmodus bietet Integrität.

5. Wählen Sie **Weiter**.
   Die Krypto-Spezifikation wird basierend auf den ausgewählten Algorithmen in der Tabelle „Schlüssellebenszyklus“ aufgeführt.

Nächste Maßnahme

Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus“ aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Siehe Konfigurieren Sie Schlüssel-lebenszyklusstatus Für Details zum Vervollständigen der Lebenszyklusdefinition für den Schlüssel.
- Wählen Sie Aus **Als Nächstes** Dient zum Erstellen eines kryptografischen Schlüssels. Sehen Sie sich eine der folgenden Aufgaben für die Schlüsselgenerierung an:
  - Generieren Sie einen kryptografischen ServiceNow-Schlüssel.
  - Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
  - Importieren Sie das Schlüsselpaar zum Umwickeln/Entpacken.

Konfigurieren Sie Schlüssel-lebenszyklusstatus

Nachdem Sie eine kryptografische Spezifikation erstellt haben, können Sie die Lebenszyklusaktionen für die Schlüssel in Ihrer Instanz konfigurieren.

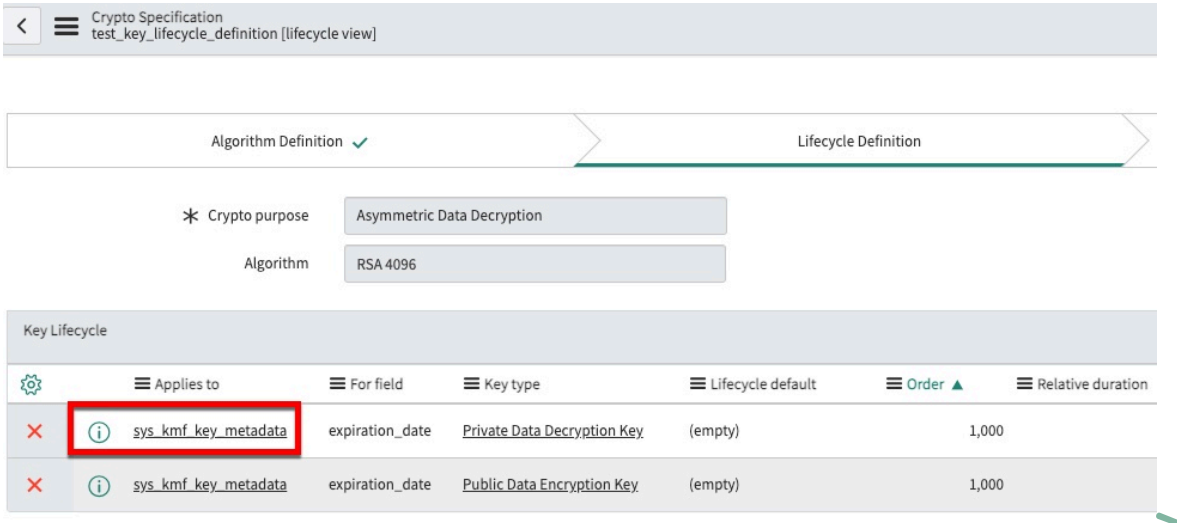
Vorbereitungen

Erforderliche Rolle: sn_kmf.admin

Prozedur

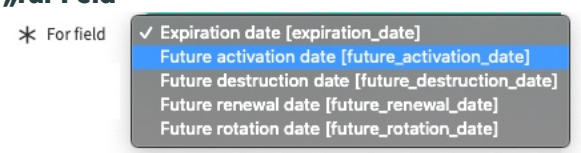
1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie das kryptografische Modul aus, um den Lebenszyklus eines Schlüssels zu konfigurieren.
3. Wählen Sie auf der Registerkarte Krypto-Spezifikationen einen Schlüsselalias aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

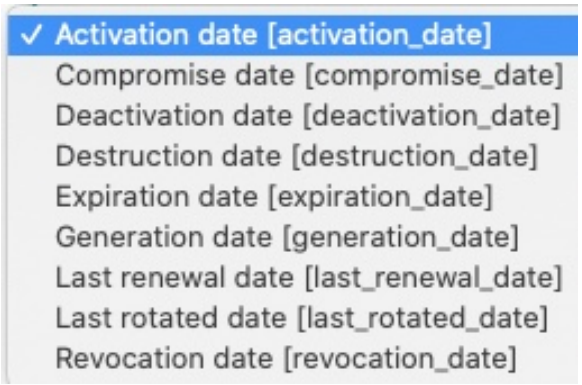


4. Wählen Sie **Weiter**.
   Das Feld Lebenszyklusvorlage wird geladen. Standardwerte für den Schlüssellebenszyklus werden basierend auf den ausgewählten Algorithmen für die definierte kryptografische Spezifikation erstellt.
5. Wählen Sie einen Schlüssellebenszyklus aus **Gilt für** Spalte im Schritt „Lebenszyklusdefinition“ für die Krypto-Spezifikation.

Schlüssel-Lebenszyklusfelder

Feld	Beschreibung
Betrifft	Ausgewählter Schlüssel, für den der Lebenszyklus gilt.
Für Feld	Wählen Sie den Typ der Steuerung für den Schlüssel aus, für den der Lebenszyklus gilt. **Schlüssel-Lebenszyklusmanagement-Werte „für Feld“** 
Typ	Wählen Sie aus, ob die Bewertung für den Schlüssellebenszyklus ein relativer Wert oder ein absoluter Wert ist: ○ **Relativ** : Geben Sie einen Wert ein, der von anderen Dateneinträgen im System abhängt, z. B. Schlüsselgenerierung, Aktivierung und Deaktivierung. ○ **Absolut** : Geben Sie einen genauen Wert ein, z. B. ein Datum.
Lebenszyklusstandard	Schreibgeschützt. Zeigt einen Wert an, wenn festgelegt.
Reihenfolge	Geben Sie die Sequenz ein, in der der Schlüssel-Lebenszyklusstatus für die Krypto-Spezifikation verarbeitet werden soll.
Typ relative Dauer	Dauer des Lebenszyklus: **Jahre** , **Monate** , Oder **Tage** .
Relative Dauer	Anzahl der Jahre, Monate oder Tage, die der Schlüssel gültig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Relativer Betrieb	**Vor** Oder **Nach** .
Relativ zu	Feld, zu dem die Dauer relativ ist. Zeigt an, ob eine relative Dauer oder ein Vorgang ausgewählt ist. 

Generieren Sie einen kryptografischen ServiceNow-Schlüssel

Gehen Sie wie folgt vor, um einen hochzuladen und zu konfigurieren ServiceNow Kryptografischer Schlüssel zum Verschlüsseln vertraulicher Daten.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird

Kryptografische Manager haben die Möglichkeit, zu verwenden ServiceNow Bereitgestellte Schlüssel oder eigene vom Kunden bereitgestellte Schlüssel (CSK) für die Verschlüsselung auf dem ServiceNow AI Platform Mit Feldverschlüsselung Enterprise. Informationen zu CSK finden Sie unter Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.

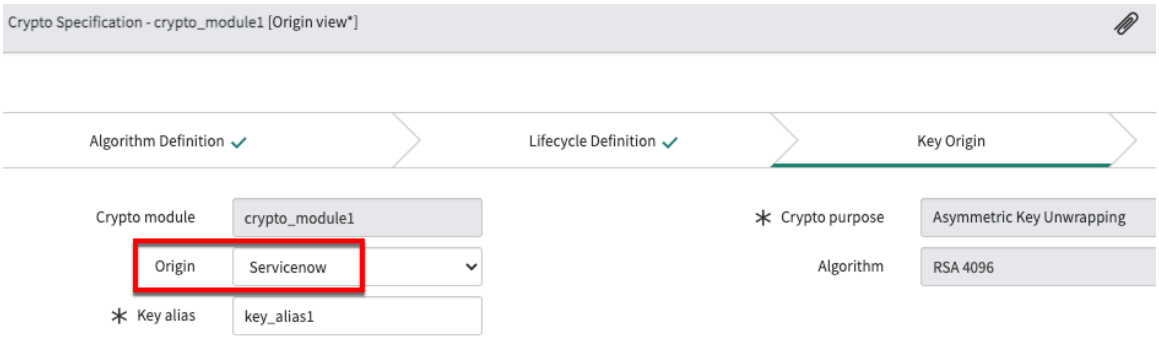
Prozedur

1. Legen Sie die Feldverschlüsselungseinstellungen so fest, dass von ServiceNow generierte Schlüssel verwendet werden.
   Details siehe Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen.
2. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
3. Wählen Sie das entsprechende kryptografische Modul aus, um die Detailseite des kryptografischen Moduls zu öffnen.
4. Wählen Sie die Zeile für den Schlüssel-Alias-Eintrag auf der Registerkarte Krypto-Spezifikationen aus.
   Wenn noch kein Schlüssel generiert wurde, ist das Feld „Schlüsselalias“ leer.
5. Wählen Sie Aus **Als Nächstes** Um zur Registerkarte Schlüsselursprung der Krypto-Spezifikationskomponenten zu navigieren.
   Die Registerkarte Lebenszyklusdefinition wird zusammen mit der Tabelle „Schlüssellebenszyklus“ angezeigt und kann überprüft oder bearbeitet werden. Details siehe Konfigurieren Sie Schlüssel-lebenszyklusstatus.

Automatische Übersetzung

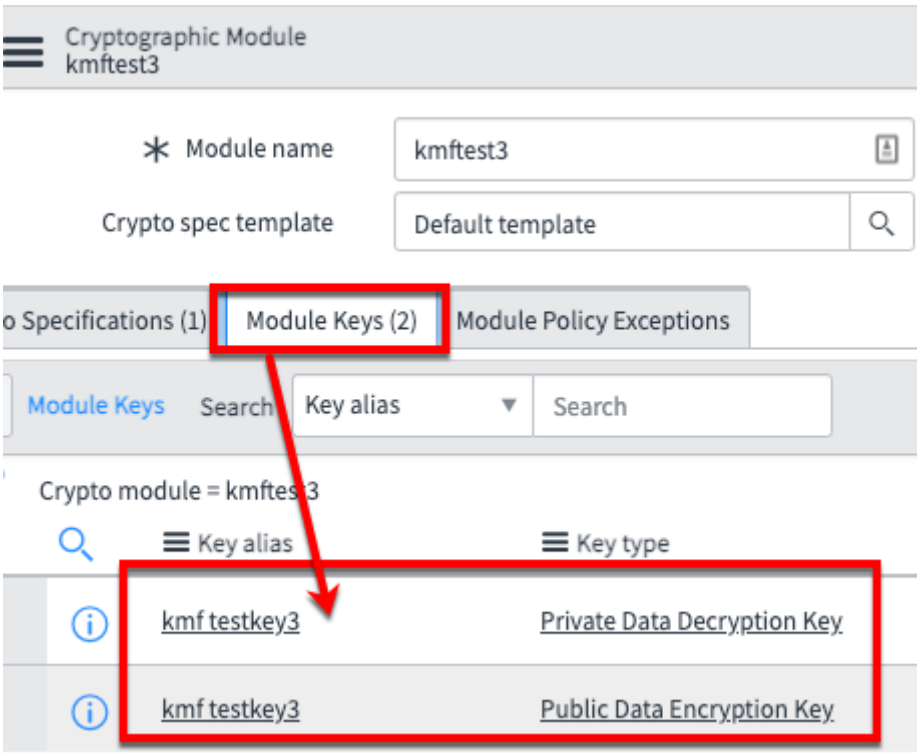
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie Aus **Servicenow**Im Feld



Ursprung.
Dieses Feld variiert je nach den Feldverschlüsselungseinstellungen aus Schritt 1 und dem ausgewählten Algorithmus. Informationen zur Verwendung eines importierten Schlüssels finden Sie unter Importieren Sie das Schlüsselpaar zum Umwickeln/Entpacken. Siehe Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel Wenn Sie Ihren eigenen Schlüssel verwenden.

7. Geben Sie einen Anzeigenamen für den Schlüssel-Alias ein.
8. Wählen Sie Aus **Als Nächstes** Um zur Registerkarte Schlüsselerstellung zu wechseln.
9. Wählen Sie Aus **Schlüssel Generieren** .
   Nachdem Sie den Schlüssel generiert haben, wird das Formular „kryptografisches Modul“ neu geladen und zeigt die kryptografische Spezifikation an.
10. Wählen Sie aus **Modulschlüssel** Registerkarte zum Anzeigen der Schlüssel.
    Sichere Informationen für den Schlüssel werden auf der Registerkarte Modulschlüssel zusammen mit der Anzahl der Schlüssel gespeichert, die für die kryptografische Spezifikation vorhanden sind.



11. Wählen Sie einen Schlüssel aus, um Schlüsselverwaltungsaktionen auszuführen.
    Details siehe Schlüsselverwaltungsaktionen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Modulzugriffsrichtlinie

Erstellen Sie Modulzugriffsrichtlinien, um zu entscheiden, welche Anwender und Skripts auf Daten zugreifen können, die von einem kryptografischen Modul verschlüsselt werden.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager oder sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird

Feldverschlüsselung Unterstützt rollenbasierte Modulzugriffsrichtlinien und zusätzliche Konfigurationsoptionen werden mit verfügbar CLE_Ent) Funktionalität.

- Konfigurieren Sie den spezifischen kryptografischen Vorgang in Modulzugriffsrichtlinien für kryptografische Module, die symmetrische Vorgänge unterstützen. Beispielsweise kann ein Anwender Daten verschlüsseln, aber nicht Daten entschlüsseln.
- Legen Sie einen standardmäßigen Modulzugriffsrichtlinienwert oder gemäß einem kryptografischen Modul fest.
- Ordnen Sie Skriptversionen zu, in denen Änderungen am Skript nachverfolgt werden, und machen die Skriptrichtlinie ungültig, was eine bessere Sicherheit für Skripttyp-Modulzugriffsrichtlinien bietet.

CLE_Ent Die Funktionalität ist mit einem kostenpflichtigen Abonnement verfügbar. Informationen zu unterstützten Funktionen und Optionen, die für jedes Angebot verfügbar sind, finden Sie unter . Weitere Informationen finden Sie unter Feldverschlüsselung Enterprise.

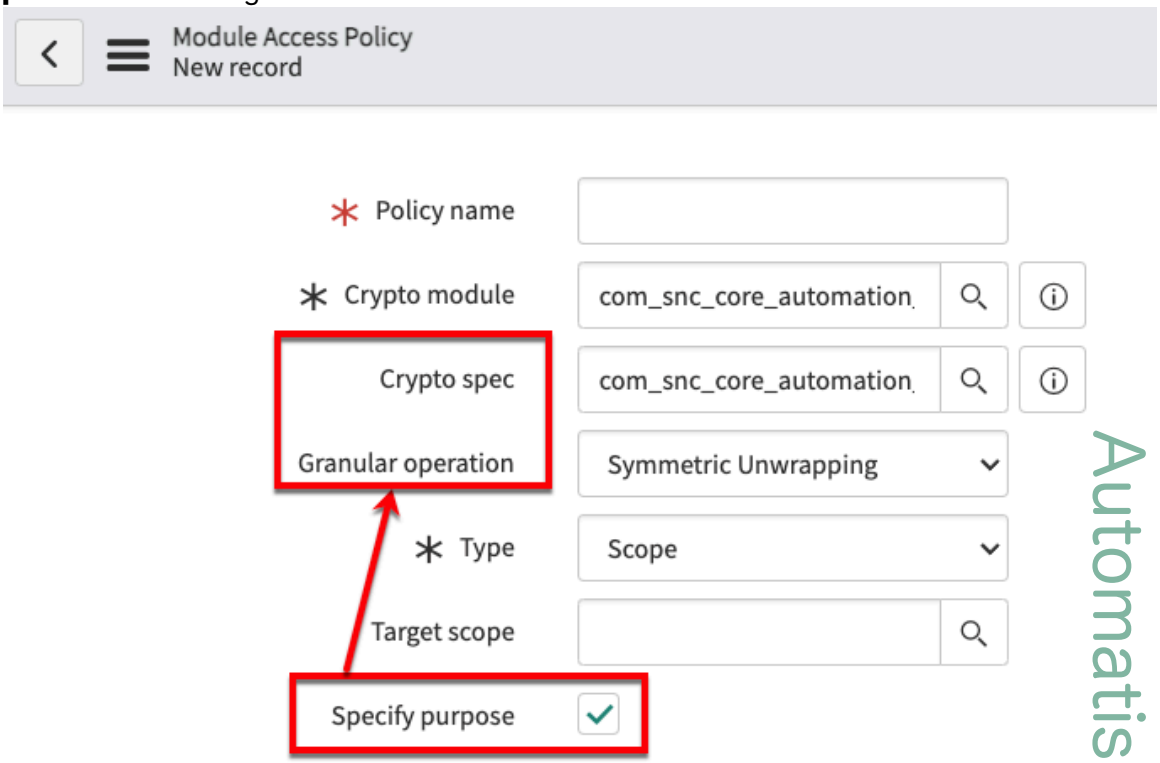
Hinweis: Das Standardverhalten der Modulzugriffsrichtlinien (Maps) ist „Ablehnen“, um nicht autorisierten Zugriff zu verhindern, es sei denn, dies ist explizit in KARTENDATENSÄTZEN deklariert.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle** .
   Wenn Sie kein kryptografisches Modul erstellen, das für die symmetrische Datenverschlüsselung/-Entschlüsselung konfiguriert ist, wird eine automatisch generierte Modulzugriffsrichtlinie erstellt und in der Tabelle aufgeführt.
2. Wählen Sie **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie Aus **Geben Sie den Zweck an** Um einen auszuwählen **Krypto-Spezifikation** Und legen Sie fest **Granularer**



Submit

Vorgang.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mit kryptografischen Spezifikationen für die symmetrische Datenverschlüsselung/-Entschlüsselung und das symmetrische Wrapping/-Entpacken **Granularer Vorgang** Das Feld ist verfügbar, wenn Sie auswählen **Geben Sie den Zweck an** Kontrollkästchen.



3. Füllen Sie das Formular aus.

Felder für Modulzugriffsrichtlinien

Feld	Beschreibung
Richtlinienname	Geben Sie einen Namen für die Richtlinie ein.
Krypto-Modul	Wählen Sie das Suchsymbol ( ), um ein Modul auszuwählen.
Krypto-Spezifikation	Wählen Sie beim Generieren der Modulzugriffsrichtlinie eine kryptografische Spezifikation aus, oder erstellen Sie sie. Dieses Feld wird verfügbar, wenn **Geben Sie den Zweck an** Das Kontrollkästchen ist aktiviert.
Granularer Vorgang	Wählen Sie den kryptografischen Zweck für die kryptografische Spezifikation aus. Die verfügbaren Werte hängen vom Typ der ausgewählten kryptografischen Spezifikation ab. Weitere Informationen zu Krypto-Zwecken finden Sie unter .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	○ **Umfang** : Steuert den Zugriff nach Anwendungsbereich. ○ **Systemanwender** : Ermöglicht Systemanwendern den Zugriff auf Krypto-Module. ○ **Skript** : Zugriff nach Skript steuern. Weitere Informationen finden Sie unter ○ **Rolle** : Steuert den Zugriff nach Anwenderrolle. ○ **Ressourcenaustausch** : Steuern Sie den Zugriff mit Ressourcenaustausch. Weitere Informationen finden Sie unter . **Hinweis:** Nur der Rollentyp wird mit unterstützt Feldverschlüsselung. Alle anderen Typen sind mit verfügbar Feldverschlüsselung Enterprise.
Zielbereich	Feld ist als Bezeichner für sichtbar **Umfang** Typ. Bezieht sich auf die Funktionalität für die Richtlinie. Wählen Sie die Anwendungen im Suchmenü aus. **Hinweis:** Der Zielbereich wird nicht unterstützt und kann nur mit festgelegt werden Feldverschlüsselung Enterprise
Zielrolle	Feld ist als Bezeichner für sichtbar **Rolle** Typ. Rolle, für die diese Richtlinie gilt.
Skripttabelle Zielskript	Diese Felder werden angezeigt, wenn Sie auswählen **Skript** Als Typ. Feld ist als Bezeichner für sichtbar **Skript** Typ. Wählen Sie eine Tabelle aus, für die diese Richtlinie gilt. Dokument, für das diese Richtlinie gilt. Wählen Sie aus **Tabellenname** Und dann das zugehörige Dokument für die Richtlinie. Wenn ein Skript zum ersten Mal ein kryptografisches Modul aufruft, wird der Zugriff auf das Modul verweigert, und der Entwickler erhält einen Fehler. Dieser Fehler gibt dem Modulbesitzer die Möglichkeit, den Zugriff auf das Modul zu gewähren oder zu verweigern.
Ressourcenaustausch: ○ Krypto-Spezifikation ○ Genehmigungstyp ○ Zielinstanz-Host	Diese Optionen werden angezeigt, wenn Sie als Typ auswählen. Ressourcenaustausch Wird sowohl von KMF als auch von unterstützt, wenn das übergeordnete Modul ist **Column_level_Encryption** . Wählen Sie die Krypto-Spezifikation, einmalig oder wiederkehrend und die URL der Zielinstanz aus. Weitere Informationen finden Sie unter .
Identitätswechsel	In rollenbasierten Modulzugriffsrichtlinien können Anwender über eine Identitätswechsel-Sitzung auf verschlüsselte Daten zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Anwender, z. B. Administratoren, die Identität anderer Anwender annehmen, werden solche Modulzugriffsrichtlinien mit Identitätswechsel angewendet.
Zweck angeben	Wählen Sie diese Option aus, um das Feld kryptografische Spezifikation als verfügbares Feld für die Richtlinie umzuschalten.
Aktiv	Wählen Sie diese Option aus, um die Richtlinie zu aktivieren.
Ergebnis	Wählen Sie eine der folgenden Optionen aus: ○ **StrictAblehnen** Lehnt den Zugriff unter allen Umständen ab. ○ **Ablehnen** Lehnt Anwender mit ab **Zielrolle** Oder **Zielbereich** Von Zugriff auf dieses kryptografische Modul, es sei denn, eine andere Richtlinie gewährt ihnen Zugriff. ○ **Nachverfolgen** Um den Zugriff auf das Modul zu ermöglichen und die Verwendung zu überwachen.

4. Wählen Sie **Absenden**.

Warnung:

Für Anwender mit Legacy-Verschlüsselungsunterstützung:

Wenn Sie die nicht-Enterprise-Version von verwenden Feldverschlüsselung, Sie sind auf fünf Module beschränkt. Wenn Sie diesen Grenzwert überschritten haben, erhalten Sie die folgende Warnung:

Diese Einfügung überschreitet die Anzahl der veröffentlichten Module, die für zulässig sind Feldverschlüsselung Berechtigt für das Abonnementprodukt. Das Enterprise-Abonnement für Feldverschlüsselung Ist für zusätzliche Module erforderlich. Wenden Sie sich an Ihr Account-Team.

5. Wählen Sie den Richtliniennamen aus, der dem kryptografischen Modul zugeordnet ist, das Sie untersuchen möchten.
Zugriffsrichtlinie für Skripttyp-Modul verwenden:

Eine Modulzugriffsrichtlinie wird basierend auf der Standardzugriffseinstellung automatisch generiert, wenn das Skript ausgeführt wird. Dem Modulnamen ist vorangestellt Autogen- . Zum Beispiel die Modul – Testrichtlinie Modul ist als aufgeführt Autogen-Modul-Testrichtlinie In der Spalte Richtlinienname.

Im Formular kryptografische Anruferrichtlinie wird die von Ihnen ausgewählte Anruferrichtlinie aufgelistet. Das Feld Zielbereich gibt den Umfang des Skripts an, das versucht, das Modul zu verwenden. Weitere Informationen finden Sie unter .

Hinweis: Mit sind maximal fünf Modulzugriffsrichtlinien zulässig Feldverschlüsselung. Konfigurationsoptionen finden Sie unter .

Erstellen Sie eine granulare Rollenmodulzugriffsrichtlinie für die symmetrische Verschlüsselung

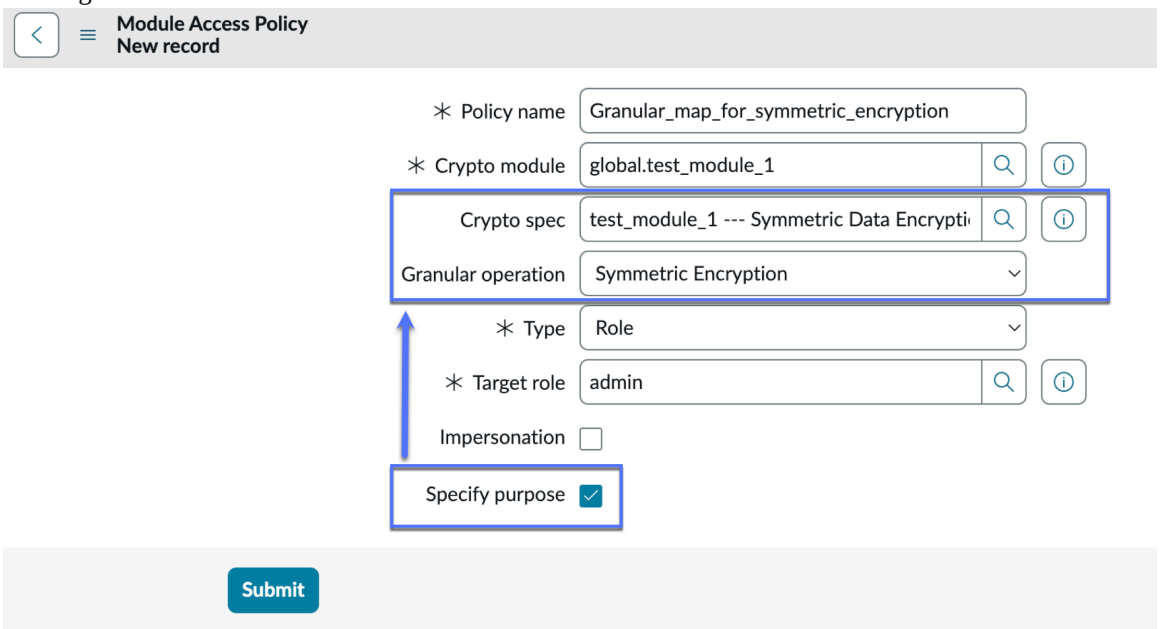
Erstellen Sie eine granulare Rollenmodulzugriffsrichtlinie (MAP), um Daten zu sichern, während Anwender, die keiner bestimmten ZUORDNUNG zugewiesen sind, Formulare für einen öffentlichen Datensatz übermitteln können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**an.
2. Wählen Sie **Neu**.
3. Geben Sie einen Namen für die Richtlinie ein.
4. Wählen Sie aus **Krypto-Modul** Auf die Sie Zugriff gewähren.
5. Wählen Sie die entsprechende aus **Zielrolle** .
6. Aktivieren Sie das Feld Zweck angeben, und geben Sie die Details zum Zweck in die neu angezeigten Felder wie folgt ein:



- **Krypto-Spezifikation** : Wählen Sie die zu verwendende Krypto-Spezifikation aus.
- **Granularer Vorgang** : Wählen Sie in der Dropdown-Liste Symmetrische Verschlüsselung aus.

7. Wählen Sie aus **Aktiv** Feld.
8. Für **Ergebnis** Wählen Sie aus **Nachverfolgen** .

Ergebnis
Mit der granularen ROLLENZUORDNUNG kann ein Anwender, der keiner KARTE zugewiesen ist, öffentliche Datensatzformulare übermitteln, während Daten gesichert werden.

Erstellen Sie eine Lebenszyklusrichtlinie für kryptografische Module

Erstellen Sie eine Lebenszyklusrichtlinie für kryptografische Module, um Beschränkungen für kryptografische Module festzulegen, z. B. wie lange der Schlüssel gültig ist. Erstellen Sie Richtlinien, um kryptografische Module zu schützen, indem Sie deren Gefährdung beschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird
Eine Lebenszyklusrichtlinie für kryptografische Module ist eine Richtlinie auf Instanzebene. Je größer das Risiko eines kryptografischen Schlüssels ist, desto wahrscheinlicher kann er gefährdet werden. Schützen Sie Schlüssel, indem Sie einschränken, wie lange die Schlüssel verwendet werden können und wer sie verwenden kann.

Die folgenden Funktionen steuern kryptografische Module:

- Instanzrichtlinien legen Grenzen für die Instanz fest. Wenn Sie beispielsweise in einer Instanzrichtlinie angeben, dass das Ablaufdatum nie mehr als zwei Jahre nach dem Aktivierungsdatum liegen darf, können Sie die Lebenszyklusregeln nicht verwenden, um ein Ablaufdatum fünf Jahre nach dem Aktivierungsdatum festzulegen.

- Mit Instanzlebenszyklusvorlagen können Sie verschiedene Richtlinien für verschiedene Schlüssel festlegen. Vorlagen bieten standardmäßige Lebenszyklusregeln für kryptografische Module, sodass sie nicht für jedes Modul neu erstellt werden müssen. Sie können beispielsweise andere Ablaufdaten für symmetrische Datenverschlüsselungsschlüssel festlegen als für Umschließungsschlüssel für öffentliche Schlüssel.

- Lebenszyklusregeln wirken sich direkt auf die Schlüssel aus. Wenn Sie beispielsweise in den Lebenszyklusregeln angeben, dass das Ablaufdatum zwei Jahre nach dem Aktivierungsdatum liegen soll, laufen Schlüssel zwei Jahre nach dem Aktivierungsdatum ab.

Prozedur
1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Lebenszyklusrichtlinien** > **Instanzrichtlinien**an.
2. Auswahlvorgang **Neu**an.
3. Füllen Sie das Formular aus.

Felder für kryptografische Lebenszyklusrichtlinien

Feld	Beschreibung
Betrifft	Schreibgeschützt. Der Schlüssel, für den der Lebenszyklus gilt.
Aktiv	Wählen Sie diese Option aus, um die Richtlinie zu aktivieren.
Richtlinienbedingung	Bedingte Anweisungen, die angeben, wann das kryptografische Modul aktiviert, verlängert, deaktiviert und gelöscht werden soll.
Ergebnis	**Ablehnen** Um den Zugriff auf das kryptografische Modul zu widerrufen, oder **Nachverfolgen** Um den Zugriff auf das kryptografische Modul zu ermöglichen und die Verwendung zu überwachen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Wenn Sie dieser Lebenszyklusrichtlinie Ausnahmen auf Modulebene hinzufügen möchten, finden Sie unter Erstellen Sie Modullebenszyklus-Richtlinienausnahmen.

Erstellen Sie Modullebenszyklus-Richtlinienausnahmen

Erstellen Sie eine Modulrichtlinienausnahme, um die Lebenszyklusrichtlinie eines Schlüssels nur für eine bestimmte in einer Instanz zu ändern.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager und sn_kmf.admin

Ausnahmen gelten nur für dieses Modul und nicht für die gesamte Instanz. Ein Administrator hat beispielsweise so konfiguriert, dass symmetrische Schlüssel auf Instanzebene auf ein Jahr beschränkt werden. Auf Modulebene kann eine Ausnahme von zwei Jahren gemacht werden.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module Alle**an.
2. Wählen Sie das kryptografische Modul aus, das die Richtlinienausnahmen verwendet.
3. Wählen Sie in der Tabelle kryptografisches Modul die aus **Modulrichtlinienausnahmen** Registerkarte
4. Auswahlvorgang **Neu**an.
5. Füllen Sie das Formular aus.

Felder für Modulrichtlinienausnahmen

Feld	Beschreibung
Krypto-Modul	Name des ausgewählten Moduls. Dieses Feld ist schreibgeschützt.
Betrifft	Der angegebene Schlüssel wird automatisch ausgefüllt.
Schlüsseltyp	Schlüsseltyp, auf den sich die Ausnahmerichtlinien beziehen. **Hinweis:** Sie können nur einen einzelnen Schlüsseltyp auswählen, pro kryptografischem Modul können jedoch mehrere Ausnahmerichtlinien erstellt werden.
Richtlinienbedingung	Anpassbare Bedingung, die bestimmt, wann die Richtlinienausnahme gilt.
Ergebnis	Das Ergebnis, das auftritt, wenn die Bedingung in **Richtlinienbedingung** Feld ist erfüllt. ○ **Ablehnen** Lehnt die Verwendung des Schlüssels ab. ○ **Nachverfolgen** Ermöglicht die Verwendung des Schlüssels.

6. Auswahlvorgang **Absenden** Soll an die Tabelle „kryptografisches Modul“ zurückgegeben werden.

Key Management Framework-Referenz

Die Key Management Framework Mit der (KMF) API/UX können Sie die Ausführung kryptografischer Vorgänge auf Ihrem vollständig anpassen und verwalten ServiceNow Instanz. Die ServiceNow Key Management Framework Bietet eine sichere und umfassende Schnittstelle für instanzseitige Verwaltungsservices für kryptografische Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

schlüssellebenszyklusstatus des Key Management Framework

KMF unterstützt mehrere status des Lebenszyklus kryptografischer Schlüssel durch die Durchsetzung bestimmter zulässiger Aktionen. Beispielsweise können nur Schlüssel, die sich im Status „aktiv“ befinden, vollständig für ihren beabsichtigten kryptografischen Zweck verwendet werden. Die folgende Tabelle enthält weitere Details zu den unterschiedlichen status des Schlüssellebenszyklus.

Mit Key Management Framework installierte Rollen

Die Key Management Framework(KMF) Führt bestimmte Rollen für kryptografische Modul- und Schlüsselverwaltungskonfigurationen ein.

Visualisierung der Modulzugriffsrichtlinie

Verwenden Sie die Visualisierung der Modulzugriffsrichtlinie, um alle relevanten kryptografischen Modulinformationen auf einer einzelnen UI-Seite anzuzeigen.

Debugger für Modulzugriffsrichtlinie

Verwenden Sie den Debugger für Modulzugriffsrichtlinien, um Protokollierungsinformationen zu überprüfen und zu verstehen, warum Ihren Anwendern Zugriff auf einen Verschlüsselungskontext gewährt wird oder nicht.

Abonnementpaket für Verschlüsselung und Schlüsselverwaltung

Mit Schlüsselverwaltung, Feldverschlüsselung Wird ohne zusätzliche Gebühr auf die hoch konfigurierbaren Verschlüsselungsmodule aktualisiert. Sie haben auch die Möglichkeit, ein Upgrade auf die Lizenz für unbegrenzte Nutzung durchzuführen. Abonnieren Sie das neue Verschlüsselungsberechtigungspaket Plattformverschlüsselung, das enthält Feldverschlüsselung Enterprise Und Cloud-Verschlüsselung.

schlüssellebenszyklusstatus des Key Management Framework

KMF unterstützt mehrere status des Lebenszyklus kryptografischer Schlüssel durch die Durchsetzung bestimmter zulässiger Aktionen. Beispielsweise können nur Schlüssel, die sich im Status „aktiv“ befinden, vollständig für ihren beabsichtigten kryptografischen Zweck verwendet werden. Die folgende Tabelle enthält weitere Details zu den unterschiedlichen status des Schlüssellebenszyklus.

Status oder Aktion des Schlüssellebenszyklus	Beschreibung
Aktiv	Der aktive Schlüssel wird zum Generieren neuer Inhalte verwendet, z. B. zum Verschlüsseln oder Signieren. Für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul kann nur ein aktiver Schlüssel vorhanden sein.
Gefährdet	Kompromittierte Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln oder Signieren, können jedoch weiterhin verwendet werden, um den Zweck vorhandener Inhalte zu identifizieren, z. B. Entschlüsselung oder Verifizierung. Mehrere Schlüssel können im gefährdeten Status zum Widerruf in einer bestimmten kryptografischen Spezifikation in einem kryptografischen Modul vorhanden sein. Jeder aktive oder ausgesetzte Schlüssel kann in einen gefährdeten Status verschoben werden.
Deaktiviert	Jeder aktive Schlüssel kann deaktiviert werden. Für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul können mehrere Schlüssel in einem deaktivierten Status vorhanden sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status oder Aktion des Schlüssellebenszyklus	Beschreibung
	Wenn der Schlüssel beispielsweise gedreht wird, wird der aktuell aktive Schlüssel deaktiviert. Deaktivierte Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln und Signieren, können jedoch weiterhin verwendet werden, um Zwecke vorhandener Inhalte zu identifizieren, z. B. Entschlüsselung oder Verifizierung. **Hinweis:** Gefährdete und widerrufene Schlüssel werden als deaktivierte Schlüssel behandelt.
Zerstört	Wenn ein Schlüssel zerstört wird, wird das Schlüsselmaterial dauerhaft entfernt und kann nicht mehr für kryptografische Zwecke verwendet werden. Jeder deaktivierte Schlüssel kann mithilfe der Lebenszyklusautomatisierung gelöscht werden, wenn er im konfigurierten festgelegten Zeitrahmen nicht verwendet wurde. Es können mehrere Schlüssel in einem zerstörten Status für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul vorhanden sein. **Warnung:** Auf Daten, die einem zerstörten Schlüssel zugeordnet sind, kann nicht mehr zugegriffen werden. Daher ist bei der Ausführung einer Aktion zum Löschen eines Schlüssels mit äußerster Vorsicht vorzugehen.
Generiert	Mehrere Schlüssel können im generierten Status für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul vorhanden sein. Ein generierter Schlüssel kann in einen aktiven Status verschoben werden, wenn für die angegebene kryptografische Spezifikation kein aktiver Schlüssel vorhanden ist. Der erste generierte Schlüssel wird automatisch auf „aktiv“ gesetzt. **Hinweis:** Wenn die Möglichkeit besteht, einen neuen Schlüssel zu generieren, wird ein neuer Schlüssel generiert und aktiviert, obwohl Schlüssel in einem generierten Status für die angegebene kryptografische Spezifikation vorhanden sind.
Erneuert	Ein aktiver Schlüssel mit einem Ablaufdatum kann beliebig oft verlängert werden, um den Lebenszyklus des Schlüssels zu verlängern. **Hinweis:** Die Differenz zwischen Aktivierungsdatum und Ablaufdatum wird berechnet, und das Ablaufdatum wird um diese Dauer ab dem aktuellen Tag verschoben.
Fortfahren	Die UI-Aktion ist für ausgesetzte Schlüssel verfügbar, um sie in einen aktiven Status zurückzuversetzen, wenn für die angegebene kryptografische Spezifikation kein anderer aktiver Schlüssel vorhanden ist.
Widerrufen	Jeder aktive oder ausgesetzte Schlüssel kann in den Status „Widerrufen“ verschoben werden. Widerrufene Schlüssel können nicht zum Generieren neuer Inhalte verwendet werden, z. B. zum Verschlüsseln oder Signieren, können jedoch weiterhin verwendet werden, um den Zweck vorhandener Inhalte zu identifizieren, z. B. zur Entschlüsselung oder Verifizierung.

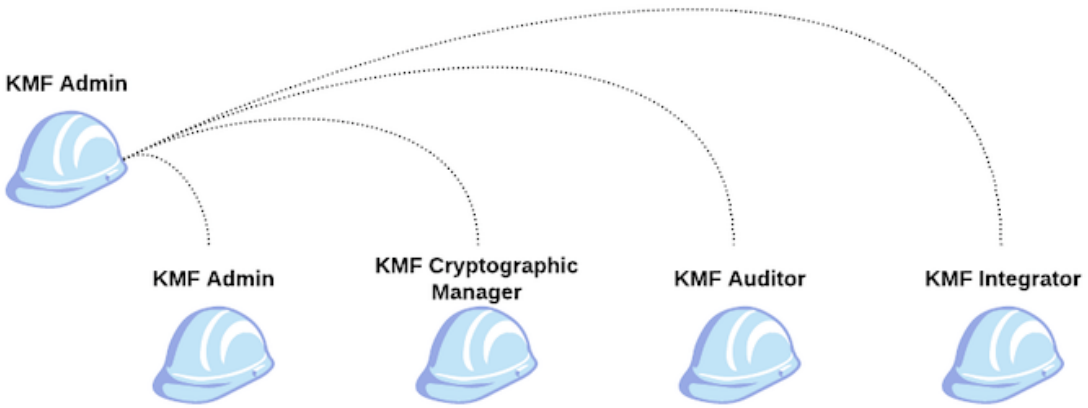
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status oder Aktion des Schlüssellebenszyklus	Beschreibung
	Mehrere Schlüssel mit widerrufenem Status können für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul vorhanden sein.
Rotiert	Schlüsselrotation führt dazu, dass der aktuell aktive Schlüssel deaktiviert und ein anderer Schlüssel aktiviert wird. Wählen Sie den neuen aktiven Schlüssel aus den folgenden Optionen aus: • Generierung eines neuen Schlüssels. • Zeigen Sie auf einen vorhandenen importierten Schlüssel. Jeder aktive Schlüssel kann rotiert werden.
Angehalten	Für eine bestimmte kryptografische Spezifikation in einem kryptografischen Modul können mehrere Schlüssel im Status „angehalten“ vorhanden sein. Wenn der Schlüssel angehalten wird, kann der Schlüssel fortgesetzt und in einen aktiven Status versetzt werden, wenn kein anderer aktiver Schlüssel für diese kryptografische Spezifikation vorhanden ist.

Mit Key Management Framework installierte Rollen

Die Key Management Framework(KMF) Führt bestimmte Rollen für kryptografische Modul- und Schlüsselverwaltungskonfigurationen ein.

Wichtig: KMF Zur Verwendung von sind Rollen erforderlich Key Management Framework. Anwender ohne KMF Rollen können nicht auf Listen, Tabellen und Module zugreifen, die zum Konfigurieren der Schlüsselverwaltung verwendet werden.



KMF-Administrator [sn_kmf.admin]

Weist anderen Anwendern Rollen zu, um Vorgänge rund um ServiceNow auszuführen Key Management Framework.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Wichtig: Vermeiden Sie die Gewährung einer Administratorrolle, wenn speziellere Rollen verfügbar sind.

- Diese Rolle wird über den in angezeigten Prozess zugewiesen Zuweisen Key Management Framework Rollen.
- Anwender mit dieser Rolle müssen auch über admin und Security_admin verfügen
- Sie müssen über diese Rolle verfügen, um#KMF-Rollen zuzuweisen, und können darüber hinaus alle Funktionen des KMF-kryptografischen Managers ausführen.

Kryptografischer KMF-Manager [sn_kmf.cryptographic_Manager]

Erstellen, lesen und aktualisieren Sie Vorgänge für kryptografische Module (Zuordnung von Schlüsseln zu kryptografischen Nutzungs- und Algorithmuskonfigurationen) und Modulzugriffsrichtlinien. Außerdem können KMF-Kryptografiemanager Schlüsselverwaltungsvorgänge (generieren, rotieren, widerrufen) und Lebenszyklusvorgänge durchführen.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Diese Rolle kann einem Anwender nur von einem KMF-Administrator zugewiesen werden.

Kryptografischer KMF-Auditor [sn_kmf.cryptographic_Auditor]

Zeigen Sie kryptografische Modulinformationen, Schlüsselmetadaten und lebenszyklusbezogene Details sowie Informationen zur Modulzugriffsrichtlinie (MAP) an.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Besondere Erwägungen

Diese Rolle kann einem Anwender nur von einem KMF-Administrator zugewiesen werden.

Kryptografischer KMF-Integrator [sn_kmf.cryptographic_Integrator]

Integrieren Key Management Framework Mit externen Schlüsselspeichern oder Systemen.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Diese Rolle kann einem Anwender nur von einem KMF-Administrator zugewiesen werden.

Kryptografischer KMF-Operator [sn_kmf.cryptographic_Operator]

Greifen Sie auf einen Teil von zu ServiceNow Key Management Framework Schlüssellebenszyklus: Verlängerung, Rotation, Widerruf.

Enthält Rollen

Liste der Rollen, die in der Rolle enthalten sind.

Keine.

Gruppen

Liste der Gruppen, denen diese Rolle standardmäßig zugewiesen ist.

Keine.

Besondere Erwägungen

Keine.

Zuweisen KMF Rollen

Zuweisen KMF Rollen für Administratoren, die wiederum andere zuweisen können KMF Rollen.

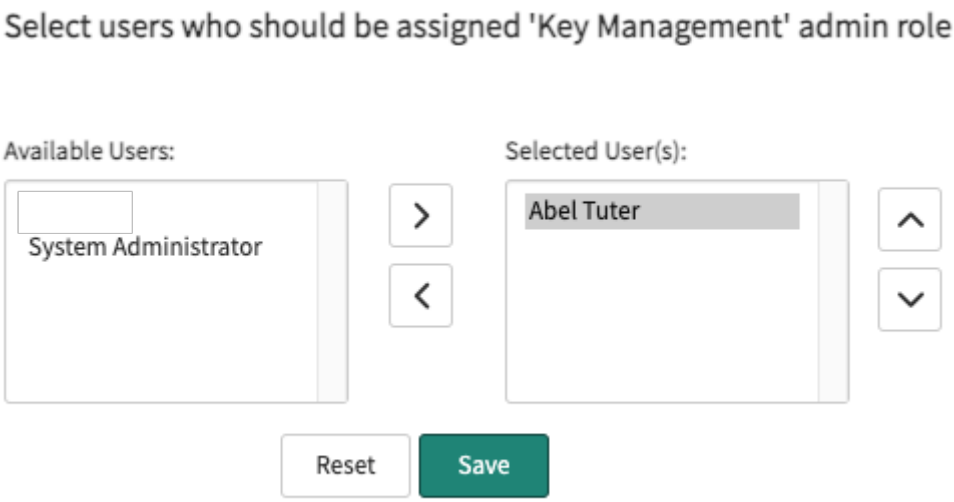
Vorbereitungen
Erforderliche Rolle: admin und security_admin

Sie müssen die Rolle Security_admin erhöhen, bevor Sie zuweisen KMF administratorrolle. Anweisungen finden Sie unter Auf eine privilegierte Rolle hochstufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

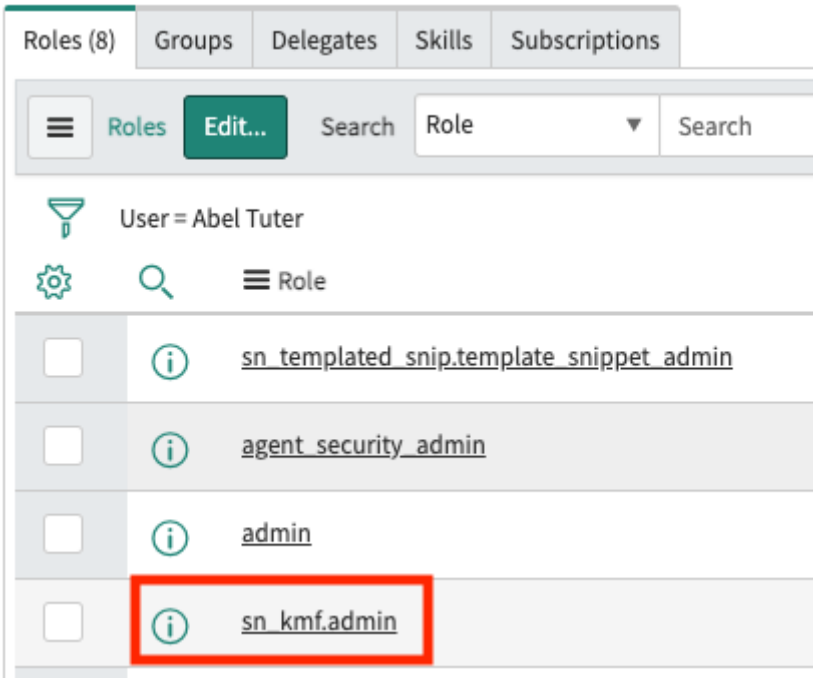
1. Erhöhen Sie die Rolle „Sicherheitsadministrator“.
2. Navigieren zu **Anwenderadministration** > **Anwender** Und wählen Sie den Anwender aus, der sein soll KMF administrator.
3. Stellen Sie sicher, dass der Anwender bereits über die Rollen admin und Security_admin verfügt. Wenn nicht, wählen Sie aus **Bearbeiten** Fügen Sie unter der zugehörigen Liste Rollen hinzu **Administrator** Und **Security _admin** .
4. Navigieren zu **Systemsicherheit** > **Administration der Schlüsselverwaltung**an.
5. Wählen Sie den Anwender aus, der Sie sein möchten KMF administrator in **Verfügbare Anwender** Und verschieben Sie sie in die **Ausgewählte Anwender** Spalte.



6. Wählen Sie **Speichern**.
7. Navigieren zu **Anwenderadministration** > **Anwender** Und wählen Sie den Anwender aus, dem Sie gerade die Rolle sn_kmf.admin zugewiesen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

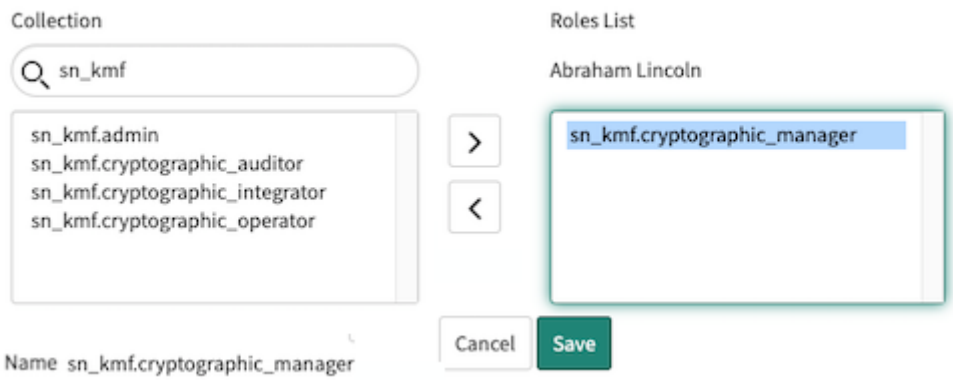
Der Anwender hat die Rolle sn_kmf.admin in **Rollen** Zugehörige Liste und kann andere KMF-Rollen zuweisen.



Nächste Maßnahme

Wenn Sie über die KMF-Administratorrolle verfügen, führen Sie die folgenden Schritte aus, um andere KMF-Rollen zuzuweisen:

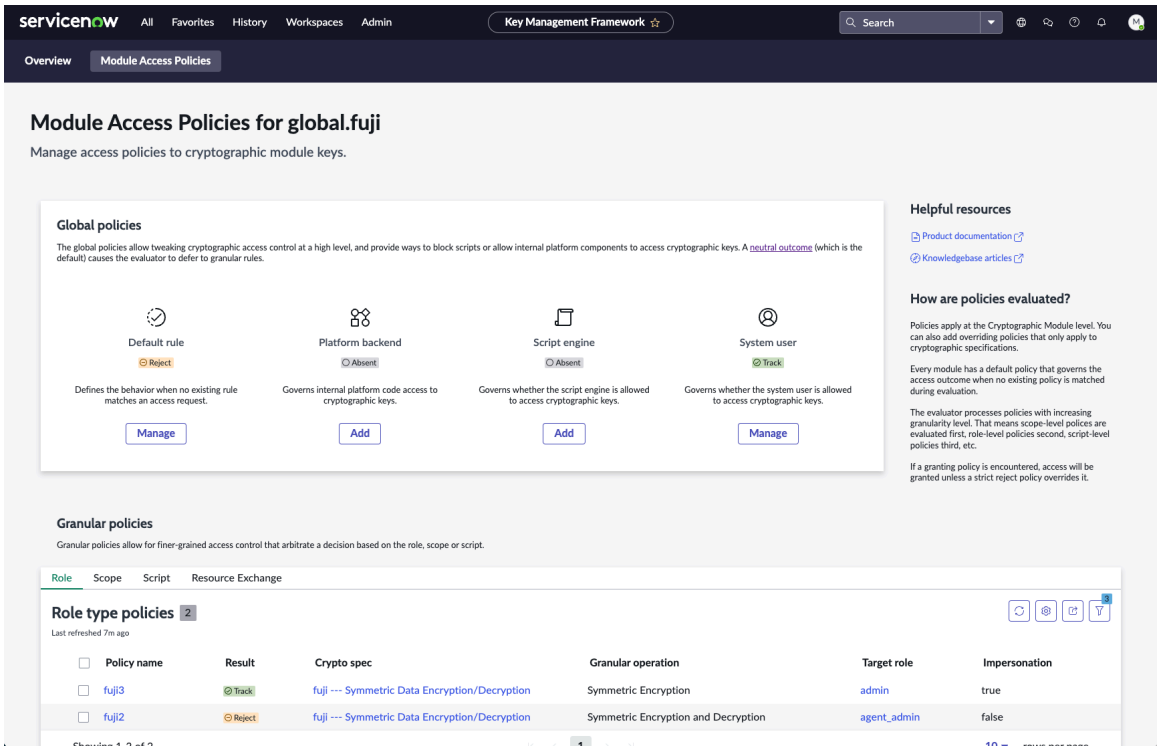
1. Navigieren zu **Anwenderadministration** > **Anwender** Und wählen Sie den Anwender aus, für den Sie eine andere KMF-Rolle haben möchten, z. B. KMF Cryptographic Manager.
2. Wählen Sie in der zugehörigen Liste Rollen die Option aus **Bearbeiten** Und wählen Sie die KMF-Rollen aus, die Sie den Anwendern zuweisen möchten. Alle KMF-Rollen beginnen mit `sn_kmf` .



Visualisierung der Modulzugriffsrichtlinie

Verwenden Sie die Visualisierung der Modulzugriffsrichtlinie, um alle relevanten kryptografischen Modulinformationen auf einer einzelnen UI-Seite anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Key Management Framework-Administratoren und kryptografische Manager können die UI-Seite der Modulzugriffsrichtlinie verwenden, um alle Zugriffssteuerungsmechanismen anzuzeigen, die sich auf ein einzelnes kryptografisches Modul beziehen. Verwenden Sie die auf dieser UI-Seite gesammelten Informationen, um zu bestimmen, wer Zugriff auf verschlüsselte Informationen in Ihrer Instanz hat.

Anwender mit *sn_kmf.admin*Oder *sn_kmf.cryptographic_manager*Rollen können auf die UI-Seite der Modulzugriffsrichtlinienvisualisierung zugreifen, indem sie zu navigieren **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.

Ergebnisbezeichnungen

Modulzugriffsrichtlinien enthalten ein **Ergebnis** Feld, das bestimmt, ob Zugriff auf das ausgewählte kryptografische Modul gewährt werden soll. Auf der UI-Seite wird eine Bezeichnung für Elemente auf der UI-Seite basierend auf dem Wert dieses Felds angezeigt.

UI-Bezeichnung	Ergebnisfeldwert	Definition
Track	*Track* oder *Allow*	Zugriff wird allen Anwendern gewährt, einschließlich Skripts.
Reject	*Reject*	Der Zugriff wird verweigert, es sei denn, es wurde eine Zugriffsrichtlinie für das Nachverfolgungsmodul gefunden.
StrictReject	*StrictReject*	Zugriff wurde verweigert.

Automatische Übersetzung

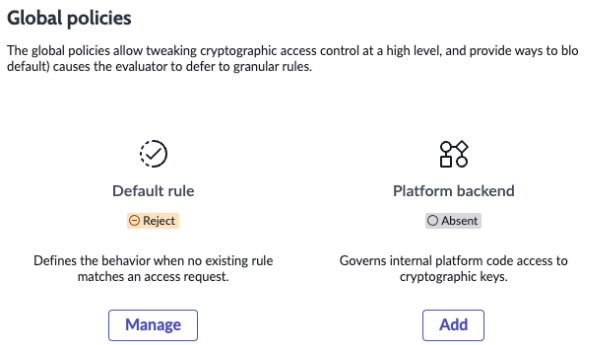
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Bezeichnung	Ergebnisfeldwert	Definition
○ Absent	*N/A*	Die Modulzugriffsrichtlinie ist in der Instanz nicht vorhanden. Zugriff wird allen verweigert.

Globale Richtlinien

Verwenden Sie **Globale Richtlinien** Abschnitt zum Überprüfen der Modulzugriffsrichtlinien, die den Zugriff auf Plattformebene steuern.

Wählen Sie aus **Verwalten** Schaltfläche unter einer der Richtlinien, um zu diesem Richtliniendatensatz zu navigieren. Wenn die Richtlinie nicht vorhanden ist, wird ein **Hinzufügen** Die Schaltfläche wird unter diesem Eintrag angezeigt. Wählen Sie aus **Hinzufügen** Schaltfläche zum Navigieren zu einem neuen Richtliniendatensatz, in dem Sie die Richtlinie definieren können.

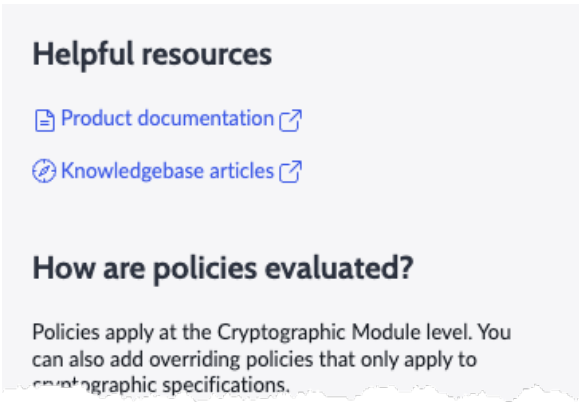


Richtlinie	Definition
Standardregel	Die Standardregelrichtlinie definiert das Verhalten, wenn keine vorhandene Regel einer Zugriffsanforderung entspricht.
Plattform-Back-End	Die Plattform-Back-End-Richtlinie steuert den internen Plattformcodezugriff auf kryptografische Schlüssel.
Skriptmodul	Die Skript-Engine-Richtlinie regelt, ob die Skript-Engine auf kryptografische Schlüssel zugreifen darf.
Systemanwender	Die Systemanwenderrichtlinie regelt, ob der Systemanwender Zugriff auf kryptografische Schlüssel hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hilfreiche Ressourcen

Verwenden Sie **Hilfreiche Ressourcen** Abschnitt mit Links zur Produktdokumentation, relevanten Wissensartikeln und einer kurzen Beschreibung, wie Modulzugriffsrichtlinien auf der Plattform ausgewertet werden. Weitere Informationen zur Auswertung von Modulzugriffsrichtlinien finden Sie unter Debugger für Modulzugriffsrichtlinie.

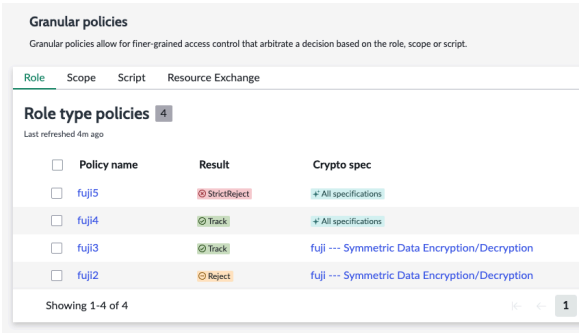


Granulare Richtlinien

Verwenden Sie **Granulare Richtlinien** Abschnitt zum Anzeigen von Listen von Modulzugriffsrichtlinien, getrennt nach Richtlinientyp. Verwenden Sie die Registerkarten über der Liste, um eine anzuzeigende Richtlinienkategorie auszuwählen.

- Rolle
- Umfang
- Umfang und Domäne (wenn Domänentrennung aktiv ist)
- Skript
- Ressourcenaustausch (wenn das kryptografische Modul ein Password2 oder ist Feldverschlüsselung Untermodul)
- Identität (wenn Geheimnismanagement Enterprise aktiv ist)

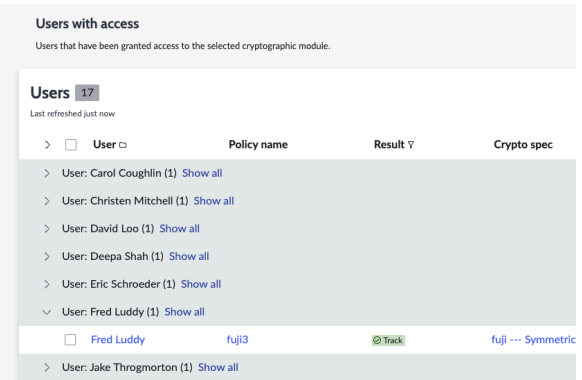
Standardmäßig werden in jeder Liste nur aktive Richtlinien angezeigt. Verwenden Sie das Filtersymbol, um den Standardfilter für die Liste zu ändern.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender mit Zugriff

Verwenden Sie **Anwender mit Zugriff** Abschnitt zum Anzeigen einer Liste aller Anwender, die Zugriff auf das ausgewählte kryptografische Modul haben. Die Liste ist nach Anwender gruppiert, da einzelne Anwender mehrere Rollen haben können, die Zugriff auf ein kryptografisches Modul gewähren.

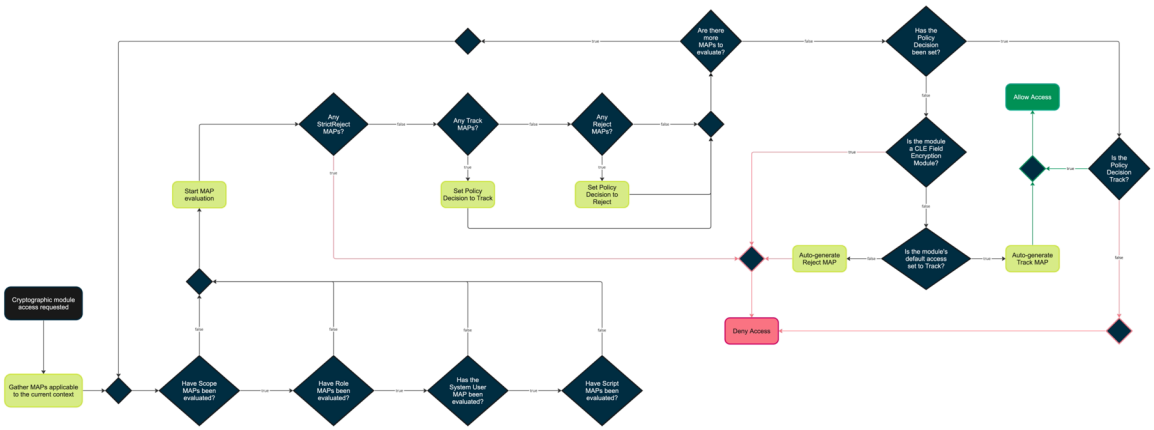


Debugger für Modulzugriffsrichtlinie

Verwenden Sie den Debugger für Modulzugriffsrichtlinien, um Protokollierungsinformationen zu überprüfen und zu verstehen, warum Ihren Anwendern Zugriff auf einen Verschlüsselungskontext gewährt wird oder nicht.

Modulzugriffsrichtlinien (Maps) definieren Steuerungen auf Instanzebene für den Zugriff auf kryptografische Module. Anrufer (z. B. ein Anwender oder Skript) benötigen expliziten Zugriff, um ein kryptografisches Modul für die Verschlüsselung und Entschlüsselung zu verwenden. Verwenden Sie den Debugger, um zu sehen, welche Richtlinien ausgewertet werden, wenn ein Anrufer versucht, auf ein kryptografisches Modul zuzugreifen. Sie können auch den Debugger verwenden und erfahren, warum Zugriff gewährt wird oder nicht.

Dieses Flussdiagramm zeigt, wie Ihre Instanz Anforderungen für den Zugriff auf ein kryptografisches Modul auswertet.



Steuern Sie den Zugriff auf die Debug-Protokolle

Der Zugriff auf die Debug-Protokolle des Modulzugriffs wird durch die Rolle bestimmt. Anwender mit `sn_kmf.admin`Und `sn_kmf.cryptographic_manager`Rollen haben Zugriff auf den Debugger. Gewähren Sie mithilfe von Zugriff auf andere Rollen `glide.kmf.module_access_policies.debugger.authorized.roles`Systemeigenschaft. Der Wert dieser Eigenschaft ist eine kommagetrennte Liste von Rollen, die auf die Debug-Protokolle zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren oder deaktivieren Sie den Debugger

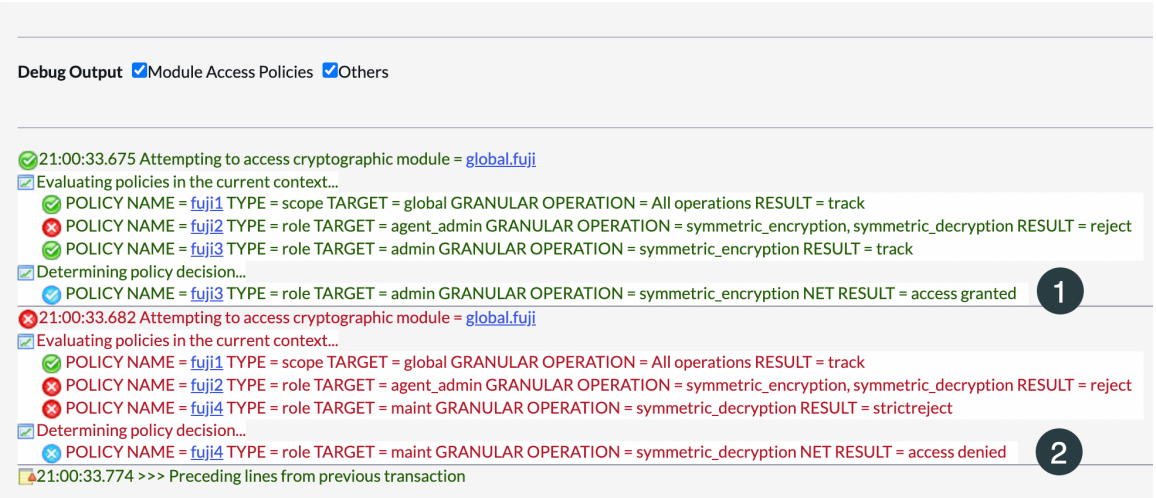
Um Debug-Protokollierungsnachrichten für Modulzugriffsrichtlinien zu aktivieren, navigieren Sie zu **Alle** > **Diagnosen** > **Sitzung debuggen** > **Modulzugriffsrichtlinien debuggen** > **an.**

Wenn Sie das Debugging abgeschlossen haben, können Sie die Protokollierungsnachrichten deaktivieren, indem Sie zu navigieren **Alle** > **Diagnosen** > **Sitzung debuggen** > **Alle deaktivieren** > **an.**

Greifen Sie auf die Protokolle zu

Navigieren Sie nach dem Aktivieren des Debugging zu einer Seite, die eine KARTENAUSWERTUNG auslöst, um die KARTEN-Debug-Protokolle anzuzeigen. Debug-Nachrichten werden unten auf der Seite angezeigt.

Tipp: Sie können Identitätswechsel verwenden, um Probleme beim Zugriff für andere Anwender zu beheben. Weitere Informationen zum Identitätswechsel finden Sie unter Identität von Anwendern wird angenommen . Um die Debug-Protokolle aus der Perspektive eines anderen Anwenders anzuzeigen, stellen Sie sicher, dass Ihre Modulzugriffsrichtlinien mit dem verwendet werden `role`Typ hat **Identitätswechsel** Feld als festgelegt **Wahr** .



In diesem Beispiel ruft ein Anrufer zwei Zugriffsanforderungen auf Global.fuji Kryptografisches Modul. Eine symmetrische Verschlüsselung, die gewährt wird, und eine symmetrische Entschlüsselung, die verweigert wurde.

Protokolleinträge verstehen

Debugging-Informationen werden in diesem Format strukturiert.

1. In dieser ersten Zeile wird das kryptografische Modul angezeigt, das die Zugriffsanforderung empfängt.
2. Die Zeilen zwischen der ersten und der letzten Zeile zeigen die ausgewerteten Karten in der Reihenfolge an, in der sie ausgewertet wurden, und enthalten Namen, Typ, Ziel, granularen Vorgang und Ergebnis.
3. In der letzten Zeile werden die Richtlinienentscheidung (falls zutreffend) und das Nettozugriffsergebnis für den Anrufer angezeigt (ob dem Anrufer Zugriff gewährt wird).

Jede Zeile beginnt mit einem Symbol, das den Nachrichtentyp angibt.

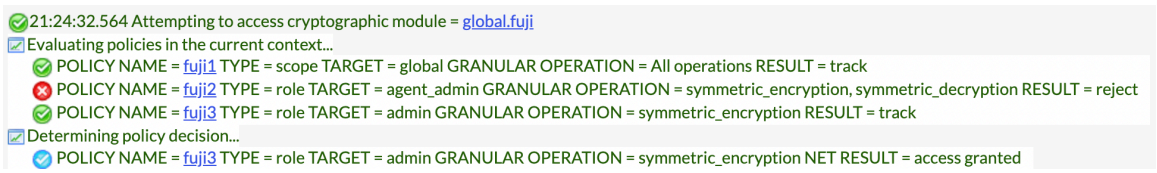
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachrichtensymbole

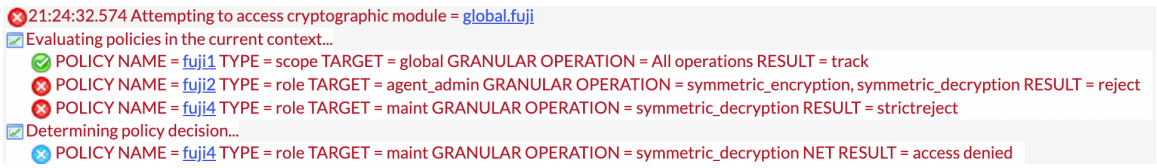
Symbol	Nachrichtentyp
	Informationsmeldung
	Die Modulzugriffsrichtlinie gewährt Zugriff
	Die Modulzugriffsrichtlinie verweigert den Zugriff
	Anrufer erhält Zugriff
	Dem Anrufer wird der Zugriff verweigert
	Keine Modulzugriffsrichtlinie zum Auswerten vorhanden

Debug-Protokollbeispiele

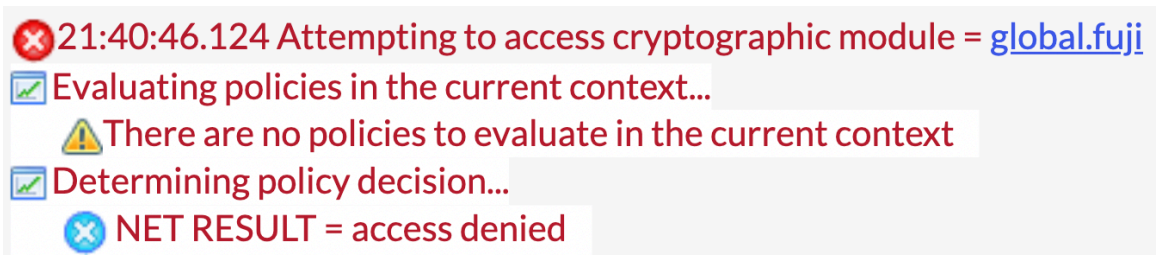
Nachricht „Zugriff gewährt“



Nachricht „Zugriff verweigert“



Zugriff verweigert (keine Modulzugriffsrichtlinien zum Auswerten vorhanden



Zugriff verweigert (unzureichende Berechtigungen)



Abonnementpaket für Verschlüsselung und Schlüsselverwaltung

Mit Schlüsselverwaltung, Feldverschlüsselung Wird ohne zusätzliche Gebühr aktualisiert, um hoch konfigurierbare Verschlüsselungsmodule einzuschließen. Sie können auch optional ein Upgrade auf die Lizenz für unbegrenzte Nutzung durchführen. Abonnieren Sie das neue Verschlüsselungsberechtigungspaket Plattformverschlüsselung, das enthält Feldverschlüsselung Enterprise Und Cloud-Verschlüsselung.

Feldverschlüsselung Funktionen

Feldverschlüsselung Mit Verschlüsselungsmodulen sind kostenlos in Ihrer Instanz und enthalten enthalten NIST 800-57 Schlüsselverwaltung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Funktionen der Plattformverschlüsselungsgruppe

Die Plattformverschlüsselungsgruppe fügt die folgenden Funktionen und Angebote hinzu:

- Verschlüsselung.
- Cloud-Verschlüsselung Mit Schlüsselverwaltung.

Zusätzliche Information

Weitere Informationen zur Schlüsselverwaltung finden Sie unter Erkunden Sie das Key Management FrameworkErkunden Sie das Key Management Framework.

Schlüsselverwaltungsaktionen

Eine der Kernfunktionen von KMF besteht darin, die Fähigkeit#zur Verwaltung von#Schlüsseln bereitzustellen, z. B. das Widerrufen oder Drehen von Schlüsseln. #KMF schützt vertrauliche Daten ordnungsgemäß mit den neuesten Verschlüsselungsmaterialien und Lebenszyklusvorgängen.

Die folgende Tabelle enthält eine Zusammenfassung der wichtigsten Lebenszyklusvorgänge und Verwaltungsaktionen. Der Zweck des kryptografischen Moduls wird auf die Daten mit der kryptografischen Modulkonfiguration angewendet und hat keine Auswirkungen auf die Daten.

Schlüsselverwaltungsaktion	Beschreibung
Schlüssel generieren	Generiert#einen#neuen Schlüssel für das angegebene#kryptografische Modul. Ein erster generierter Schlüssel ist auf festgelegt `Aktiv` .
Schlüssel drehen	Deaktiviert#den aktuellen#Schlüssel und#generiert einen neuen#. Der#neue#Modulschlüssel wird auf aktuell#(aktiv) festgelegt.
Schlüssel widerrufen	Markiert#den aktuellen Schlüssel#- und Lebenszyklusstatus als widerrufen. Das kryptografische Modul generiert automatisch einen neuen Schlüssel für neue Daten und setzt den Schlüsselstatus auf „aktiv“. Widerrufen bedeutet, dass der Schlüssel nicht mehr für die Verschlüsselung verwendet wird. Es kann jedoch weiterhin für die Entschlüsselung verwendet werden. Sie können keinen Schlüssel löschen.
Schlüssel anhalten	Markiert#den aktuellen Schlüssel als angehalten. ##Setzen Sie den ausgesetzten#Schlüssel manuell fort, oder widerrufen#Sie den ausgesetzten Schlüssel, um#einen neuen Modulschlüssel zu generieren, bevor Sie das kryptografische Modul erneut verwenden.
Schlüssel fortsetzen	Markiert einen ausgesetzten Schlüssel als aktiven Schlüssel.
Schlüssel verlängern	Verlängert die Lebensdauer des aktuellen Schlüssels. Die **Verlängern** Die Schaltfläche wird unter den folgenden Umständen verfügbar: • Ihnen ist die Rolle „kryptografischer Manager“ zugewiesen. • Der Lebenszyklusstatus ist entweder in markiert **Aktiv** Oder **Verlängert** . • In der Modullebenszyklusdefinition wird ein Ablaufdatum festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüssel anzeigen und verwalten

Überprüfen Sie den Status eines Schlüssels, um weitere Schlüsselaktionen zu bestimmen, z. B. wann ein aktueller Schlüssel verlängert, rotiert, ausgesetzt, deaktiviert oder gelöscht werden soll.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie ein kryptografisches Modul aus.

   Das Formular <module-name> des kryptografischen Moduls wird angezeigt.
3. Wählen Sie auf der Registerkarte Modulschlüssel den Schlüsselalias aus, um den Schlüsselstatus im Formular „Lebenszyklus-<key name>“ zu überprüfen.
4. Überprüfen Sie das Formular, da alle Felder schreibgeschützt sind.

Schlüsselfelder für kryptografischen Lebenszyklus

Feld	Beschreibung
Generierungsdatum	Zeigt das Datum an, an dem der Schlüssel generiert wurde.
Aktivierungsdatum	Zeigt das Datum an, an dem der Schlüssel aktiviert wurde.
Letztes Verlängerungsdatum	Zeigt das Datum an, an dem der Schlüssel zuletzt verlängert wurde.
Letztes Rotationsdatum	Zeigt das Datum an, an dem der Schlüssel zuletzt gedreht wurde.
Deaktivierungsdatum	Zeigt das Datum an, an dem der Schlüssel deaktiviert wurde.
Zerstörungsdatum	Zeigt das Datum an, an dem der Schlüssel gelöscht wurde.
Status des Schlüssellebenszyklus	Zeigt den Status des Schlüssellebenszyklus an.
Künftiges Aktivierungsdatum	Zeigt das zukünftige Aktivierungsdatum des Schlüssels an.
Künftiges Verlängerungsdatum	Zeigt das zukünftige Datum der Schlüsselverlängerung an.
Künftiges Rotationsdatum	Zeigt das zukünftige Datum für die Schlüsselrotation an.
Künftiges Zerstörungsdatum	Zeigt das zukünftige Datum an, an dem der Schlüssel gelöscht wird.
Ablaufdatum	Zeigt das Datum an, an dem der Schlüssel abläuft.

5. Um eine Aktion für den Schlüssel auszuführen, wählen Sie eine der folgenden Optionen aus, um sofort wirksam zu werden:
   - **Schlüssel widerrufen**: Wählen Sie diese Option aus, um den Schlüssel zu deaktivieren und einen neuen Schlüssel zu generieren. Geben Sie den Grund ein, warum Sie den Schlüssel widerrufen.
   - **Schlüssel rotieren**: Wählen Sie diese Option aus, um den aktuellen Schlüssel zu deaktivieren und einen neuen Schlüssel an seiner Stelle zu generieren. Der neue Schlüssel wird in der Tabelle „Modulschlüssel“ aufgeführt, und die Nummer der Schlüsselversion wird um 1 erhöht. Weitere Informationen finden Sie unter .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Schlüssel aussetzen**: Wählen Sie diese Option aus, um den aktuellen Schlüssel zu deaktivieren.
- **Schlüssel Fortsetzen** : Wählen Sie diese Option aus, um einen ausgesetzten Schlüssel als aktiven Schlüssel zu markieren. Diese Option ist nur verfügbar, nachdem der aktive Schlüssel angehalten wurde.

Schlüssel rotieren

Um die Sicherheit zu erhöhen, können Sie Ihre kryptografischen Schlüssel nach einem vordefinierten Zeitplan rotieren. Die Schlüsselrotation erfolgt, wenn Sie einen Verschlüsselungsschlüssel stilllegen und diesen alten Schlüssel durch Generieren eines neuen kryptografischen Schlüssels ersetzen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

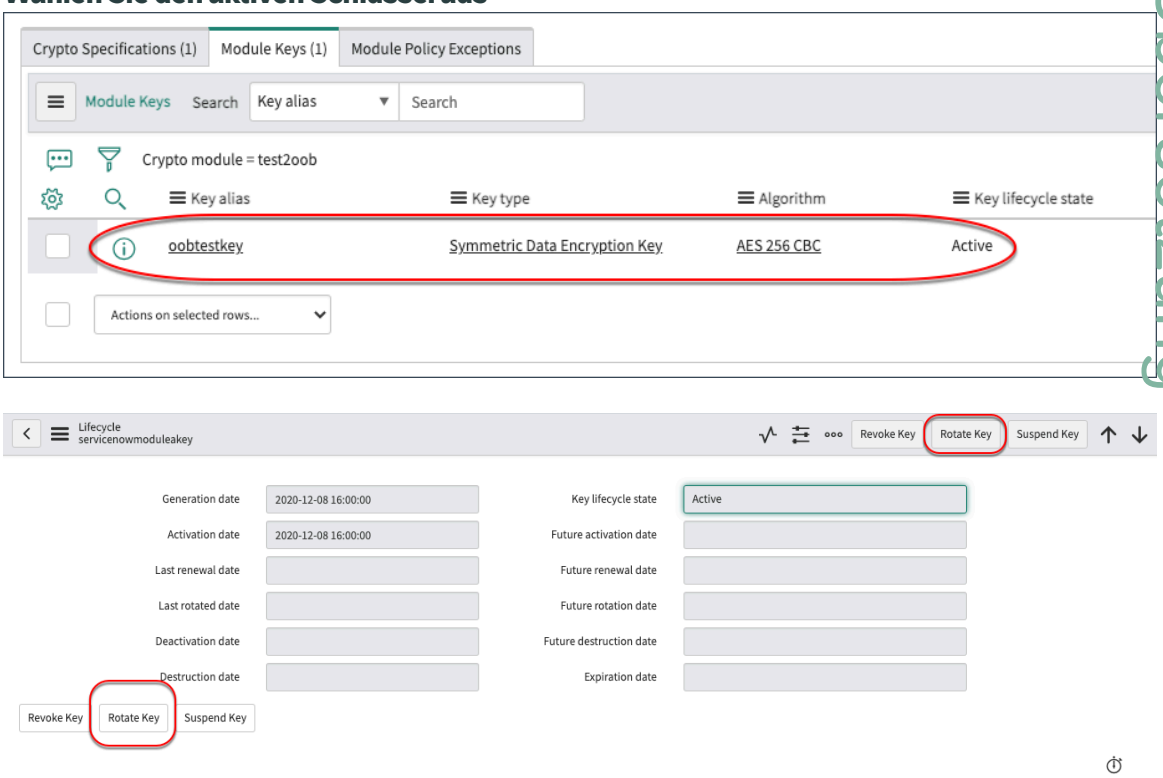
Warum und wann dieser Vorgang ausgeführt wird

Verschlüsselungsmodule unterstützen im Gegensatz zu Verschlüsselungskontexten eine Neuverschlüsselung von Datensätzen für die erneute Verschlüsselung mit einem neuen Schlüssel. Im Folgenden wird gezeigt, wie Sie einen Schlüsselrotationsvorgang manuell für ein kryptografisches Modul ausführen.

Prozedur

1. Navigieren zu **Schlüsselverwaltung** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie das kryptografische Modul für die Schlüsselrotation aus.
3. Auf der **Modulschlüssel** Wählen Sie die Taste aktiv aus.

Wählen Sie den aktiven Schlüssel aus



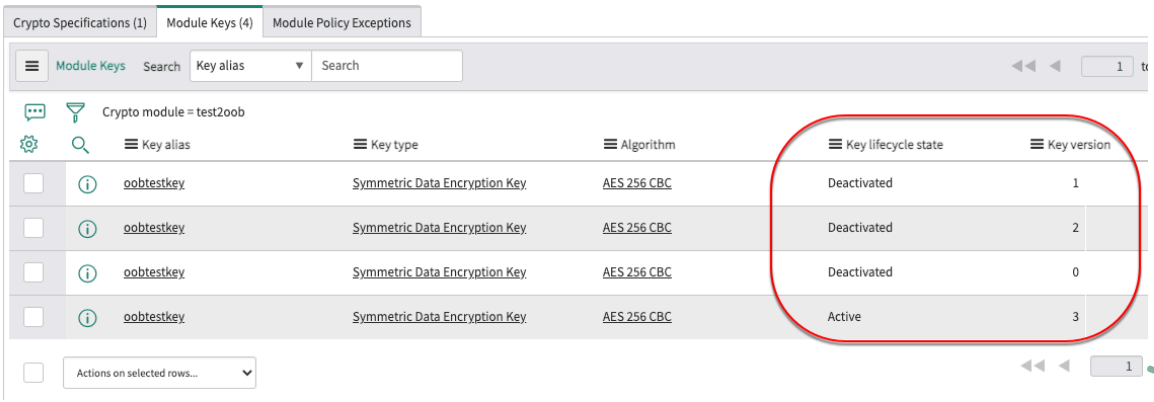
4. Wählen Sie Aus **Schlüssel Rotieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Status des Schlüssellebenszyklus ändert sich in „deaktiviert“. Die **Datum der letzten Rotation** , **Deaktivierungsdatum** , Und **Schlüsselversion** Felder werden aktualisiert.

5. Zurück zu **Kryptografisches Modul** > **Modulschlüssel** .



In der Tabelle ist ein zusätzlicher Modulschlüssel aufgeführt. Der neu rotierte Schlüssel wird zu „aktiv“, und der letzte Schlüssel ist „deaktiviert“.

Importieren Sie einen Schlüssel aus einem Webservice

Laden Sie einen externen Kundenschlüssel sicher in Ihre Instanz hoch, indem Sie einen Schlüssel aus einem Webservice importieren (z. B. die Schlüssel-REST-API). Sowohl symmetrische als auch asymmetrische öffentliche Schlüssel können in ein Ziel importiert werden KMF Kryptografisches Modul.

Der zu importierende Schlüssel (der Zielschlüssel) muss mit einem umschließenden Schlüssel verschlüsselt werden, bevor er in das kryptografische Zielmodul der Instanz hochgeladen wird. Dieser umschließende Schlüssel ist die öffentliche Komponente eines öffentlichen/privaten Schlüsselpaars, das in der Instanz vorhanden sein muss. Der Schlüssel ist eine Voraussetzung, bevor der umschlossene Zielschlüssel über „aus Webservices importieren“ hochgeladen werden kann.

Diese beiden separaten Verfahren (Importieren des umschließenden Schlüsselpaars und Importieren des umschlossenen Zielschlüssels aus einem Webservice) werden in der folgenden Dokumentation beschrieben. Dieses Schlüsselpaar muss generiert und hochgeladen werden, damit es im internen kryptografischen Modul des Schlüsselimports der Instanz verfügbar ist.

Hinweis: In diesem Beispiel wird OpenSSL für die Schlüssel- und Zertifikatgenerierung und das Postman-API-Testtool verwendet, um die REST-API-Verwendung anzuzeigen. Ersetzen Sie andere vergleichbare Tools basierend auf Ihren Unternehmensanforderungen.

Importieren Sie das Schlüsselpaar zum Umwickeln/Entpacken

Konfigurieren Key Management Framework Importieren Sie Einstellungen, bevor Sie einen Schlüssel importieren.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird
In diesem Beispiel wird OpenSSL für die Schlüssel- und Zertifikatgenerierung verwendet. Ersetzen Sie andere vergleichbare Tools basierend auf Ihren Unternehmensanforderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

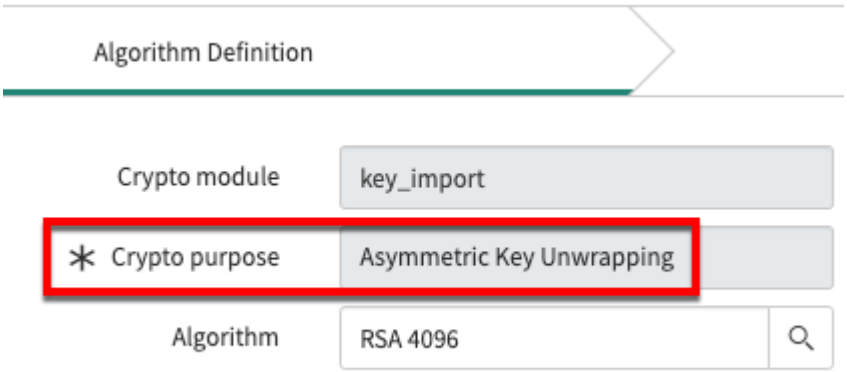
1. Verwenden Sie in Ihrer lokalen Umgebung das Terminal, um ein Zertifikat zu erstellen.
   Beispiel: `openssl REQ -x509 -sha256 -nodes -days 365 -newkey rsa:4096 -keyout wrapping_private.key -out Wrapping_public.crt`

   Dieses Zertifikat ist eine öffentliche Komponente, die einen Schlüssel enthält. Das Zertifikat wird zum Umschließen eines symmetrischen AES-Schlüssels verwendet.

2. Verwenden Sie in Ihrer lokalen Umgebung das Terminal, um einen Schlüsselspeicher zu erstellen, der ein öffentliches Zertifikat (mit dem Umschließungsschlüssel) und einen privaten Entpackungsschlüssel enthält.
   Beispiel: `openssl pkcs12 -Export -in Wrapping_public.crt -inkey wrapping_private.key -Name „Wrapping_key_alias“ -out Wrapping_Keystore.p12`

3. Navigieren Sie in Ihrer Instanz zu **Alle** > **Schlüsselverwaltung** > **Einstellungen importieren** > **Schlüsselimporteinstellungen**an.

4. Überprüfen Sie im Abschnitt „Algorithmusdefinition“ **Krypto-Zweck** Ist auf festgelegt *`Asymmetrischer Schlüssel Wird Entpackt`*.



5. Wählen Sie einen entsprechenden Algorithmus aus, der am asymmetrischen Schlüsselmaterial für den importierten Schlüsselspeicher ausgerichtet ist.
   Weitere Informationen finden Sie unter Übersicht über kryptografische Spezifikationen.

6. Wählen Sie **Weiter**.

7. In **Lebenszyklusdefinition** Abschnitt auswählen **Als Nächstes** Um fortzufahren.

8. In **Schlüsselursprung** Wählen Sie entweder aus **Importieren Sie aus PKCS12** Oder **Import aus BCFKS** In **Ursprung** Feld.

   Hinweis: Wenn Sie den Beispielschlüsselspeicher aus Schritt 1 verwenden, wählen Sie aus **Importieren Sie aus PKCS12** .

9. Geben Sie ein **Schlüsselalias** Um den Schlüssel zu identifizieren.
   Dieser Alias muss mit dem Schlüsselalias (oder „Anzeigename“) übereinstimmen, der beim Generieren des hochzuladenden Zertifikats oder Schlüsselspeichers angegeben wurde. Wenn Sie das obige Beispiel fortsetzen, wäre dies `Wrapping_key_alias` .

10. Wählen Sie **Weiter**.
    Die **Schlüsselerstellung** Abschnitt enthält einen **Schlüssel Importieren** Link, der ein Dialogfeld zum Hochladen des Schlüsselspeichers anzeigt. Wenn Sie das Beispiel fortsetzen, wäre dies `Wrapping_Keystore.p12` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importieren Sie einen umschlossenen Schlüssel aus einem Webservice

Laden Sie Ihren umschlossenen Schlüssel mithilfe der Funktionalität „Schlüssel aus Webservice importieren“ in ein kryptografisches Modul hoch. Das Beispiel verwendet einen symmetrischen Schlüssel. Ähnliche Schritte können verwendet werden, um einen asymmetrischen Schlüssel zu importieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager (Modulkonfiguration), sn_kmf.cryptographic_Operator (Standardauthentifizierung für REST-Vorgang)

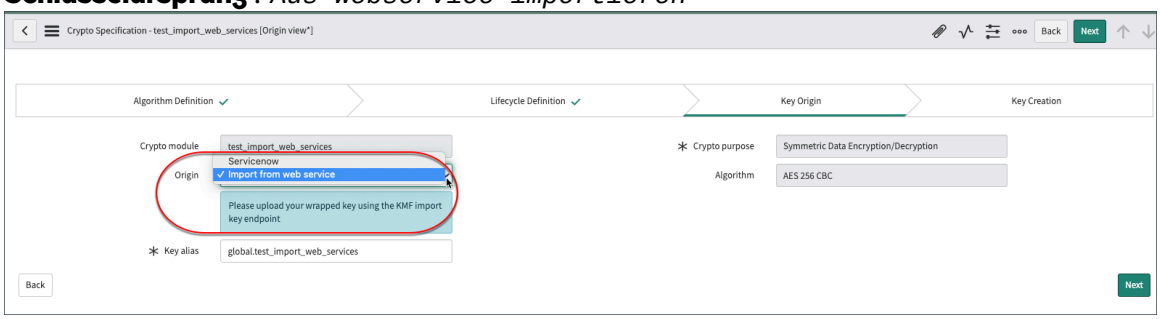
Warum und wann dieser Vorgang ausgeführt wird

KMF Der Zugriff auf den Importschlüssel-Endpunkt ist erforderlich, um den Schlüsselimport abzuschließen.

In diesem Beispiel wird OpenSSL zum Generieren von Schlüsseln und Zertifikaten verwendet. Sie können andere vergleichbare Tools basierend auf Ihren Anforderungen ersetzen.

Prozedur

1. Umschließen Sie Ihren symmetrischen Schlüssel mithilfe des Terminals auf Ihrem lokalen Gerät mit dem Schlüsselimport-Modul „öffentlicher Schlüssel umschließender Schlüssel“.
   Beispiel: `openssl pkeyutl -crypt -pubin -inkey public_Wrapping_key.pem -in symmetric_key.bin -pkeyopt rsa_Padding_Mode:oaep -pkeyopt rsa_oaep_md:sha256 -out wrapped_symmetric_key.txt`
   In diesem Beispiel wird eine umschlossene Schlüsseldatei mit dem Namen erstellt `wrapped_symmetric_key.txt` .
2. Erstellen Sie ein kryptografisches Modul, das an die API gebunden werden soll.
   Weitere Informationen finden Sie unter oder.
3. Fügen Sie eine kryptografische Spezifikation mit den folgenden Auswahlen hinzu.
   - **Krypto-Zweck** : *`Symmetrische Datenverschlüsselung/-Entschlüsselung`* .
   - **Schlüsselursprung** : *`Aus Webservice importieren`*

   Weitere Informationen finden Sie unter oder .
4. Führen Sie eine aus *`HTTP-POST-Anforderung`* Zum Import von einem Webservice-REST-Endpunkt.

Option	Wert/Format
URL des Endpunkts	*`https://<instance>/api/sn_kmf/key/Import?cryptoSpecSysID=<sys_id_of_crypto_spec>`* .

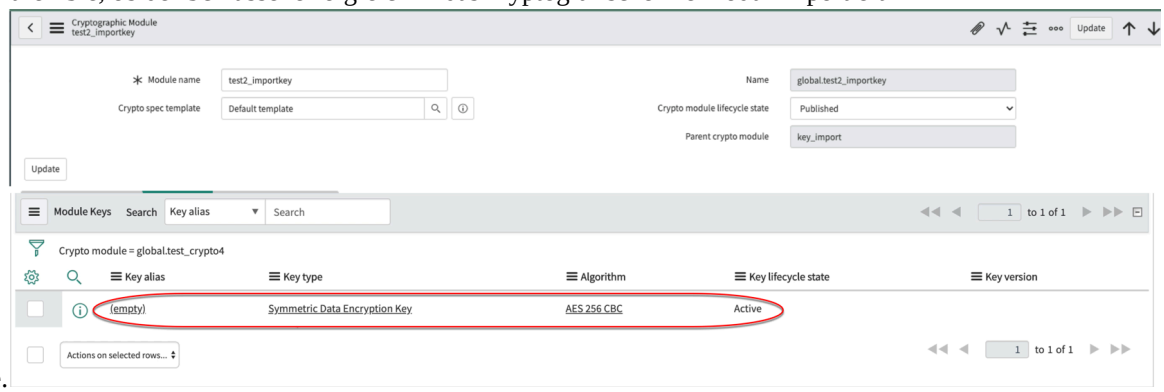
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wert/Format
CryptoSpecSysID-Parameter	Die `sys_ID` Der neu erstellten Kryp–to-Spezifikation. **Tipp:** Klicken Sie mit der rechten Maustaste auf den Header der Krypto-Spezifikation, um zu kopieren `sys_ID` .
Header-Inhaltstyp	Anwendungs-/Octet-Stream.
Textkörper	Muss eine Dateianhangbinäre und den öffentlichen Schlüssel zum Importieren (Wrapped_symmetric_-key.txt) enthalten.
Import aus Webservice-REST-Endpunkt	Verwendet die Standardauthentifizierung von `<username/password>` . **Hinweis:** Stellen Sie sicher, dass der de-signierte Anwender über die Rolle sn_kmf_-cryptographic_Operator verfügt.

Der erfolgreiche Import des öffentlichen Schlüssels führt zu einer HTTP-Antwortnachricht mit `Status 200` .

5. Überprüfen Sie, ob der Schlüssel erfolgreich in das kryptografische Zielmodul importiert wurde.



Key Management Framework Gesundheit

Greifen Sie auf Informationen zum Status des Status bei Bedarf für zu Key Management Framework. Warn- und Fehlfunktionsfehler enthalten eine detaillierte Meldung.

Vorbereitungen

Erforderliche Rolle: sn_kmf_Cryptographic Auditor oder sn_kmf_admin oder sn_kmf_Cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird

Jede Komponente von Key Management Framework Ist umrissen und meldet die folgenden Status und Farben:

- Grün/funktionsfähig: Die Komponente ist funktionsfähig, keine Fehler zu melden.
- Grau/deaktiviert: Die Komponente ist inaktiv, daher wird keine Integritätsprüfung durchgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Gelb/verschlechtert: Warnung, die Komponente funktioniert, aber Verzögerungen/ vorübergehende Probleme sind anfällig.
- Rot/Störung: Ein schwerwiegender Fehler verhindert den Betrieb der Komponente, was wahrscheinlich zu Teilausfällen führt.

Komponenten können Unterkomponenten mit einzelnen Berichten enthalten, und ihr eigener Integritätsstatus wirkt sich wie folgt auf das übergeordnete Element aus:

- Wenn alle Unterkomponenten inaktiv sind, wird das übergeordnete Element als inaktiv angezeigt. Inaktive Unterkomponenten wirken sich nicht auf die Integrität ihrer übergeordneten Elemente aus.
- Wenn eine oder mehrere Unterkomponenten verschlechtert oder fehlerhaft sind, wird die übergeordnete Integrität als verschlechtert angezeigt.
- Wenn alle Unterkomponenten als fehlerhaft melden, meldet das übergeordnete Element auch als fehlerhaft.

Weitere Informationen zu Unterkomponenten finden Sie unter Schlüssel auf Instanzebene im Key Management Framework.

Hinweis: Integritätsprüfungen werden alle 15 Sekunden ausgeführt. Aktualisieren Sie die Integritätsseite, um den Bericht erneut auszuführen.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > > **Diagnosen**an.
2. Überprüfen Sie die folgenden Integritätsstatusinformationen:

Diagnoseinformationen

Kategorie	Details
Schlüssel sicher	Überprüft, ob eine Verschlüsselung versucht wird.
Dateischlüsselspeicher	Überprüft, ob ein Abrufversuch des Instanz-Stammschlüssels (IRK) stattfindet. **Hinweis:** Der Dateischlüsselspeicher ist eine Offline-Alternative zu Key Secure, die für lokale Instanzen und Entwicklerinstanzen verwendet wird.
GlideEncrypter	Überprüft, ob ein kryptografisches Modul, eine Spezifikation und ein Schlüssel auf Instanzebene von GlideEncrypter vorhanden sind. **Hinweis:** GlideEncrypter ist eine skriptfähige Komponente, die eine transparente Verschlüsselung von ermöglicht Password2Felder und andere veraltete Verschlüsselungsnutzungen über den Key Management Framework.
Instanzschlüssel-Verschlüsselungsschlüssel (IKEK)	Überprüft, ob der Schlüssel aus dem Dateischlüsselspeicher oder KeySecure abgerufen werden kann.
HMAC-Schlüssel der Instanz	Überprüft, ob der Schlüssel aus dem Dateischlüsselspeicher oder KeySecure abgerufen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Details
Vault-PKI	Überprüft die Vault-Konnektivität, um zu überprüfen, ob der Instanzasymmetrische Verschlüsselungsschlüssel (IAEK) und der Instanzsignaturschlüssel (ISK) verwendbar sind und aus dem Vault abgerufen werden können.
EJBCA PKI	Überprüft die LDAP-Konnektivität, um zu überprüfen, ob IAEK und ISK nutzbar sind und aus Cache und LDAP abgerufen werden können.
Instanz-PKI	Überprüft den Dateischlüsselspeicher und KeySecure auf einen Schlüssel und ob das Zertifikat vorhanden ist und mit dem symmetrischen Schlüssel übereinstimmt. **Hinweis:** Instanz-PKI ist nur für Instanzen in einem verfügbar ServiceNow Rechenzentrum.

Wenn Sie Hilfe bei der Fehlerbehebung benötigen, wenden Sie sich an Kundenservice und Support.

Bereiten Sie Ihre Instanz auf die Einstellung von GlideEncrypter vor

Verwenden Sie ein Instanz-Scan-Skript, um GlideEncrypter-API-Aufrufe in Ihrer Instanz zu finden und zu entfernen. Das Entfernen dieser Aufrufe ist ein notwendiger Schritt, um die 3DES-Verschlüsselung in Ihrer Instanz als veraltet zu setzen.

Vorbereitungen

Erforderliche Rolle: Administrator

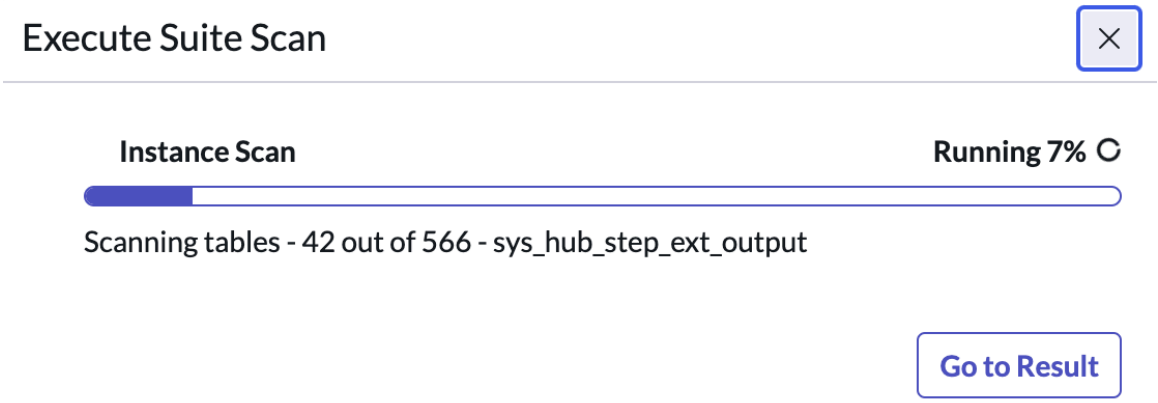
Für die GlideEncrypter-API ist ab dem Zurich-Release von geplant ServiceNow. Das Entfernen von GlideEncrypter-Aufrufen aus Ihrem Skript ist auch ein notwendiger Schritt, bevor die 3DES-Verschlüsselung in Ihrer Instanz als veraltet festgelegt wird.

Prozedur

1. Navigieren zu **Alle** > **Instanz-Scan** > **Suites**an.
2. In **Suiten** Liste, wählen Sie aus **GlideEncrypter** Um die Datensätze mit GlideEncrypter-Nutzungen zu identifizieren.
3. In **Suiten** Datensatz auswählen **Suite-Scan Ausführen** .
4. In **Suites Jetzt Scannen** Fenster auswählen **Vollständige Instanz** , Und wählen Sie dann aus **Scan Ausführen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

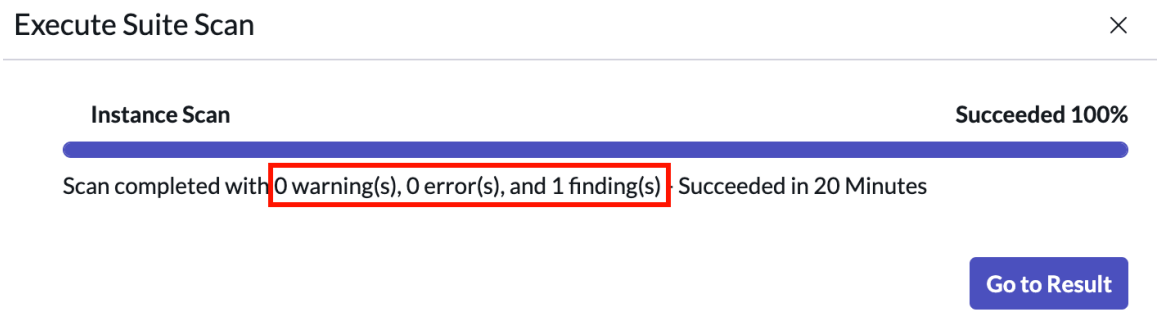
Der Suite-Scan wird ausgeführt. Während der Scan-Ausführung a **Testscan Ausführen** , Ein Fenster zeigt den Fortschritt des Scans



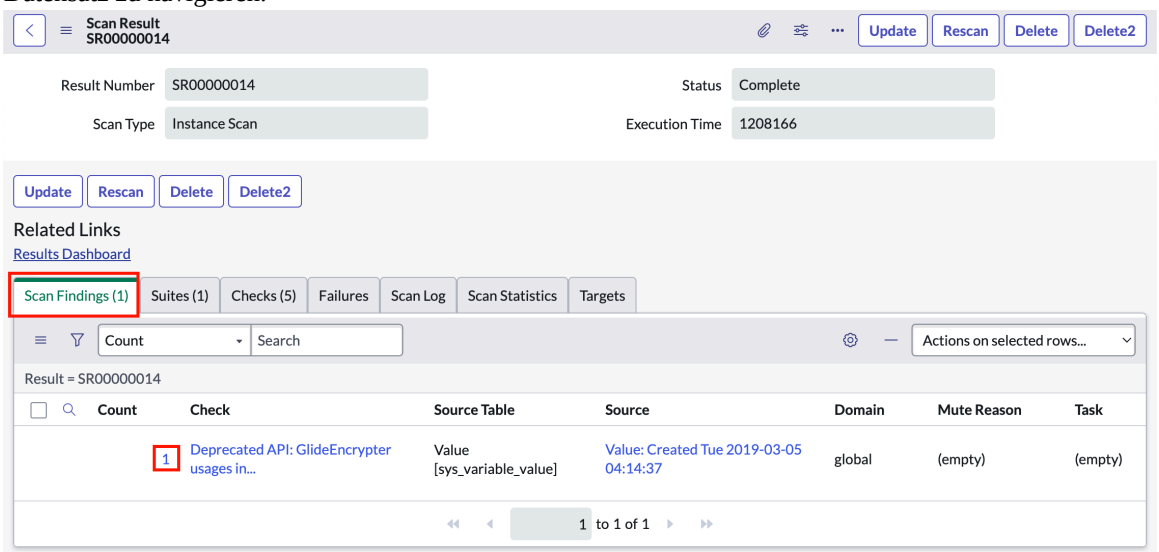
an.

Hinweis: Dieser Scan überprüft nur Datensätze, die vom Kunden erstellt oder geändert wurden.

5. Wenn der Scan abgeschlossen ist, wählen Sie aus **Wechseln Sie zum Ergebnis** Um anzuzeigen **Scan-Ergebnis** Datensatz.



6. In **Scan-Ergebnis** Datensatz, wählen Sie aus **Anzahl** Feld auf der **Scan-Ergebnisse** Liste, um zu einem Datensatz zu navigieren.



7. Ändern Sie alle Skripts im Datensatz, der verwendet **GlideEncrypter** API.
Für Details zu Alternativen zu **GlideEncrypter** , Siehe Alternativen zu veralteten GlideEncrypter-APIs .

8. Nach dem Entfernen **GlideEncrypter** Aufrufe aus Ihren Skripts. Führen Sie den Scan erneut aus, um sicherzustellen, dass keine Aufrufe der API verbleiben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

GlideEncrypter-Nutzung von 3DES für Passwort2-Felder als veraltet festlegen

GlideEncrypter-Einstellung

Erfahren Sie, wie Sie Legacy-GlideEncrypter-Aufrufe verwenden aus den Skripts in Ihrer Instanz entfernen können.

GlideEncrypter-Verfügbarkeit in der Zurich Release

Die Verfügbarkeit von GlideEncrypter in der Zurich Das Release hängt davon ab, ob Ihre Instanz in einem vorherigen Release erstellt oder von einem vorherigen Release aktualisiert wurde.

Neue Instanzen

In neuen Instanzen, die in erstellt wurden Zurich Oder später wurde diese API standardmäßig deaktiviert. Alle Basissystemskripts wurden aktualisiert und verwenden keine Aufrufe dieser API mehr.

Aktualisierte Instanzen

Zurich Instanzen, die von einem vorherigen Release aktualisiert wurden, können weiterhin die Legacy-GlideEncypter-API verwenden, aber die API wurde aktualisiert, um die AES256-GCM-Verschlüsselung über zu verwenden Key Management Framework. Diese Änderung ersetzt die Verwendung des Legacy-3DES-Verschlüsselungsstandards, um den NIST-Richtlinien zu entsprechen, während alle Skripts, die noch GlideEncrypter verwenden, ausgeführt werden können.

Aktivieren oder deaktivieren Sie GlideEncrypter

Die Verfügbarkeit von GlideEncrypter wird von gesteuert *glide.security.glideencrypter.allow*Systemeigenschaft. Diese Systemeigenschaft ist auf festgelegt **Falsch** Standardmäßig in „Neu“ Zurich Instanzen und können nicht aktualisiert werden. In Instanzen, die auf aktualisiert wurden Zurich, Diese Eigenschaft kann von Administratoren mit der Rolle „Security_admin“ geändert werden.

Die Systemeigenschaft glide.security.glideencrypter.allow

Wert	Verhalten
wahr	Bei „wahr“ kann GlideEncypter weiterhin in Skripts aufgerufen werden, verwendet jedoch die AES256-GCM-Verschlüsselung über Key Management Framework.
falsch	Bei „falsch“ werden GlideEncrypter-Aufrufe zurückgegeben `Null` , Und Administratoren sehen diesen Fehler: `Unsupported call to GlideEncrypter. Details: GlideEncrypter is deprecated and now returns null, please refer KB1320986`

GlideEncrypter-Nutzung von 3DES für Passwort2-Felder als veraltet festlegen

Deaktivieren Sie die Verwendung des 3DES-Verschlüsselungsstandards für GlideEncrypter in Ihrer Instanz. Stellen Sie sicher, dass Ihre Instanz den sichereren Advanced Encryption Standard (AES) ausschließlich für die Verschlüsselung und Entschlüsselung Ihrer Passwort2-Daten verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beginnt in Rome, Passwort2-Daten werden mit geschützt Key Management Framework, Der den moderneren AES-Algorithmus (Advanced Encryption Standard) verwendet. Einige Konfigurationen und Fallbacks in der Passwort2-Logik können jedoch weiterhin den 3DES-Algorithmus für die Verschlüsselung und Entschlüsselung verwenden.

In Vancouver Release können Administratoren den 3DES-Algorithmus vollständig als veraltet festlegen. Nach Abschluss dieser Änderung verwendet Ihre Instanz AES-Verschlüsselung ausschließlich für alle Verschlüsselungs- und Entschlüsselungsaufgaben im Zusammenhang mit Passwort2-Daten. Diese Änderung bietet eine bessere Instanzsicherheit als die 3DES-Verschlüsselung und ist erforderlich, um NIST-konform zu bleiben.

Überlegungen vor der Einstellung

Passwort2-Daten werden zwischen Instanzen übertragen

Beim Übertragen von Passwort2-verschlüsselten Texten in andere Instanzen müssen Sie dies sicherstellen KMF Key Exchange Ist zwischen Quell- und Zielinstanzen aktiviert. Diese Konfiguration stellt sicher, dass die Schlüssel, die zum Verschlüsseln von Passwort2-Texten verwendet werden, auf beiden Instanzen verfügbar sind, um die mit Passwort2 verschlüsselten Texte zu entschlüsseln. Berücksichtigen Sie vor der Einstellung von 3DES die folgenden Anwendungsfälle, die sich auf Passwort2-Daten zwischen Instanzen auswirken können.

- Wenn Sie Anwendungen in Ihrer Instanz haben, die Passwort2-Daten verwenden, stellen Sie dies sicher KMF Ressourcenaustausch Ist auf dieser Instanz installiert. KMF Ressourcenaustausch Stellt sicher, dass Schlüssel auf Instanzebene, die zum Verschlüsseln der Passwort2-Daten in der Quellinstanz verwendet werden, in den Zielinstanzen zur Entschlüsselung verfügbar sind. Weitere Informationen finden Sie unter Key-Management-Framework-Ressourcenaustausch.
- Wenn Sie Passwort2-Daten über XML oder Datenquellen exportieren möchten, stellen Sie sicher, dass die Zielinstanz über verfügt KMF Key Exchange Aktiviert. Diese Konfiguration stellt sicher, dass die Schlüssel auf Instanzebene, die zum Verschlüsseln der Passwort2-Daten in der Quellinstanz verwendet werden, in den Zielinstanzen zur Entschlüsselung verfügbar sind. Weitere Informationen zu dieser Konfiguration finden Sie unter Schlüsselaustausch Für Schlüsselmanagement-Framework.

> **Wichtig:** Die obigen Beispiele sind häufigere Szenarien. Wenn Sie jedoch eine andere Methode zur Übertragung von verschlüsseltem Passwort2-Text zwischen Instanzen verwenden, müssen Sie konfigurieren KMF Ressourcenaustausch Um sicherzustellen, dass die Zielinstanz Passwort2-Daten entschlüsseln kann.

Downgrade einer Instanz nach der 3DES-Einstellung

Folgendes gilt nur für Instanzen, die Passwort2-Felder mit einer Eingabelänge von mehr als 125 Zeichen aufweisen und die 3DES-Verschlüsselung bereits veraltet ist.

Dient zum Downgrade einer Instanz auf eine frühere Veröffentlichung als Vancouver Führen Sie über Instanzklonen die folgenden Schritte aus, bevor Sie den Klon initiieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Überprüfen Sie, ob die Datenaufbewahrung so konfiguriert ist, dass Passwort2-Felddaten erhalten bleiben.
2. Wenn ja, wenden Sie sich an, bevor Sie einen Klon anfordern ServiceNow Unterstützung zum Deaktivieren der 3DES-Einstellung. In **Grund** Feld „Downgrade-Voraussetzung für Passwort2-Support klonen“ verwenden.

Veraltete Passwort2-Felder

Ihre Instanz verwendet 3DES-Verschlüsselung, um Passwort2-Daten in Legacy-Daten (vor- Rome) Passwort2-Daten. Nachdem die 3DES-Verschlüsselung veraltet ist, ist diese Option nicht mehr verfügbar. Wenn Sie diese Funktion weiterhin benötigen, fordern Sie eine teilweise Einstellung an (Details finden Sie im nächsten Abschnitt).

So setzen Sie 3DES als veraltet fest

Nachdem Sie die vorherigen Anwendungsfälle überprüft haben, verwenden Sie den Knowledge Base-artikel KB1704481 für einen Schritt-für-Schritt-Prozess, um die Verwendung des DES DES- oder Triple-DES-Algorithmus in der Instanz sicher zu verwerfen. Weitere Informationen finden Sie unter KB1704481 .

Wichtig: Sie müssen zum Sicherheitsadministrator hochstufen, um anzuzeigen **Sicherheits-Compliance** Modul und führen Sie diese Schritte aus. Details zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle hochstufen.

Nach der Einstellung von GlideEncrypter

Nach Abschluss des Ablehnungsprozesses gelten die folgenden Informationen für Ihre Instanz.

- Passwort2-Felder unterstützen weiterhin die Entschlüsselung (aber keine Verschlüsselung) von 3DES-verschlüsselten Daten.
- Vorhandene 3DES-verschlüsselte Daten in Passwort2-Feldern bleiben unverändert, bis der Feldwert von einem Anwender oder Workflow aktualisiert wird.
- Jede Aktualisierung des Werts eines Passwort2-Felds entfernt 3DES-verschlüsselten Text und ersetzt ihn durch den von verschlüsselten Text KMF Mit AES.
- In einigen Situationen kann Ihre Instanz beim Speichern von Passwortdaten einen Fehler anzeigen:

  Aktion abgebrochen: Der Passwortwert kann aufgrund eines technischen Problems nicht gespeichert werden. Hilfe finden Sie in KB1296997.

  Wenn dieser Fehler angezeigt wird, lesen Sie die Supportinformationen im Knowledge Base-artikel KB1296997 .

Key-Management-Framework-Ressourcenaustausch

ServiceNow® Ressourcenaustausch Ist ein KMF Funktion, mit der Sie Ressourcen zwischen Instanzen sicher austauschen können.

Terminologie

Bei Verwendung von Ressourcenaustausch, Verweisen Sie auf die folgende Terminologie:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenaustausch Terminologie

Name	Beschreibung
Ressourcenaustausch	Der Prozess zum Austausch von Ressourcen über Instanzen hinweg.
Key Exchange (KE)	Der Prozess zum Austausch von Schlüsseln über Instanzen.
Schlüsselquelleninstanz (Schlüsselquelle)	Die Instanz, die die Schlüssel besitzt.
Schlüsselzielinstanz (Schlüsselziel)	Die Instanz, die die Schlüssel anfordert.

Übersicht

Ressourcenaustausch Verwendet KMF Kryptografische APIs zur Bereitstellung von Vertraulichkeit, Integrität, Authentifizierung und Nichtwiderrede. Derzeit Ressourcenaustausch Unterstützt Key Exchange Funktionalität. Weitere Informationen finden Sie unter Schlüsselaustausch Für Schlüsselmanagement-Framework.

Schlüsselaustausch Für Schlüsselmanagement-Framework

KMF Key Exchange Ist eine Teilsatzfunktion von KMF Ressourcenaustausch. Key ExchangeÜberträgt verschlüsselte Daten sicher über mehrere Instanzen.

Übersicht über Key Exchange

Key Exchange Überträgt Schlüssel sicher über Instanzen hinweg.

KMF Key Exchange Bietet Kunden eine sichere Möglichkeit zum Austausch KMF Schlüssel zwischen Instanzen. Ein Anwendungsfall ist der Datenklonprozess. Mit Key Exchange, Krypto-Modulschlüssel werden während des Datenklonens von kopiert KMF Komponenten. Kryptografische Module, Modulschlüsselspezifikationen und Modulzugriffsrichtlinien sind im Klonprozess enthalten. Übertragung von Schlüsseln ist nicht enthalten.

Diese Funktionalität ist in enthalten Key Management Framework, Die in enthalten ist ServiceNow AI Platform Verschlüsselungsabonnementpaket. Weitere Informationen zu diesem Produkt finden Sie unter Key Management Framework.

Key Exchange verwenden

Administratoren, die verwenden KMF Für Feldverschlüsselung Kann verwenden Key Exchange Zum Klonen der Schlüssel zwischen Produktionsinstanzen beim Klonen von Daten. Beim Klonen von Daten muss der Administrator/ KMF Kryptografischer Manager kann Folgendes ausführen:

- Tauschen Sie alle Schlüssel in die anderen Instanzen aus.
- Tauschen Sie bestimmte Schlüssel einmal oder regelmäßig mit der anderen Instanz aus.
- Senden Sie Bedarfsanforderungen von der Zielinstanz an die Schlüsselquellinstanz.
- Tauschen Sie Schlüssel von Quelle zu Ziel aus, um den verschlüsselten Text erneut zu verschlüsseln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwalten Sie die Ablaufzeit der Anforderung mit der Möglichkeit, Schlüssel zu löschen oder die Schlüsselaustauschanforderung abzulehnen, wenn die Anforderung abgelaufen ist.
- Nachdem die Anforderung abgeschlossen und der Schlüssel importiert wurde, wird der verwendete Schlüssel als abgelaufen festgelegt und mit einem Zeitstempel versehen.
- Geben Sie den verschlüsselten Chiphertext für die Zielinstanz erneut ein, die mit Schlüsseln aus der Quelle verschlüsselt wurde.

Unterstützte Modi

Key Exchange Unterstützt mehrere Modi auf der Krypto-Spezifikationsebene des Verschlüsselungsmoduls:

Modus	Beschreibung
Automatisch (keine Konfiguration, Standardverhalten)	Alle Schlüssel werden während des Datenklonvorgangs ohne zusätzliche Konfiguration automatisch übermittelt.
Konfigurierbar (einmaliges Konfigurations-Setup)	Der Administrator konfiguriert die Schlüssel, die während des Datenklonvorgangs gesendet werden sollen.
Manuell (Person in der Schleife)	Der Administrator sendet eine Anforderung bei Bedarf für die Zielinstanz an die Quelle. Die Anforderung muss von einem Administrator auf der Schlüsselquellinstanz genehmigt werden.
Neuschlüssel (automatisierte Anforderung)	Der Administrator wählt während des Setup-Prozesses für das Klonen die Option „Neuschlüssel eingeben“ aus.

Konfigurieren Sie Den Schlüsselaustausch

Key Management Framework(KMF) Generiert automatische Schlüsselaustauschanforderungen für unterstützte kryptografische Module während der Neuinstallation oder des Upgrades der Instanz. Verwaltet den Datenverschlüsselungsschlüssel lokal für die Instanz.

Vorbereitungen

Ein kryptografisches Modul mit einem Schlüssel muss vor der Verwendung sowohl in den Ziel- als auch in den Quellinstanzen erstellt werden Key Exchange.

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird

Key Exchange Anforderungen werden von der Zielinstanz initiiert.

Der automatische Schlüsselaustausch ist standardmäßig aktiv, wenn eine Instanz geklont wird, in der die Eigenschaft in die Zielinstanz geklont wird. Zusammen mit KMF, Konfigurieren Sie Systemeigenschaften, um zu verwalten, wie Schlüssel während eines Instanzklons behandelt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Automatischen Schlüsselaustausch deaktivieren:** Legen Sie fest *glide_encryption.auto_key_exchange.enabled*Eigenschaft bis **Falsch** Für wiederkehrende Klonanforderungen.
- **Senden Sie Anforderungen zum automatischen Schlüsselaustausch** : Legen Sie diese Eigenschaft auf fest **Wahr** .

Wichtig: Die Basissystemeigenschaft ist auf festgelegt **Wahr** Standardmäßig ist der automatische Schlüsselaustausch beim Klonen einer Instanz aktiviert. Dieser Wert muss auf festgelegt werden **Falsch** Wenn Sie verwenden Geben Sie den verschlüsselten Text mit Schlüsselaustausch erneut ein Oder die Funktion „Wiederkehrender Schlüsselaustausch“. Weitere Einzelheiten erhalten Sie unter Wiederkehrender Schlüsselaustausch – Walkthrough.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen** > **Neu**an.
2. Füllen Sie im Formular die Felder aus.

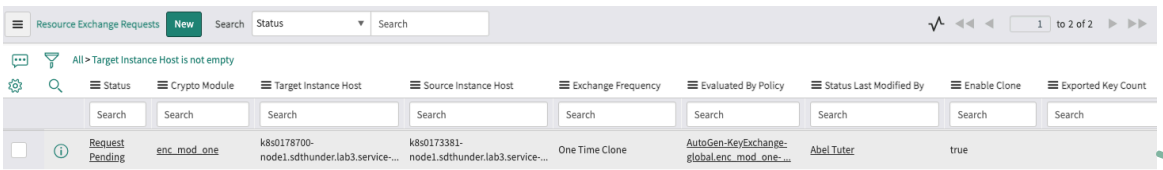
Ressourcenaustausch Anforderungsformularfelder

Name	Beschreibung
Austauschhäufigkeit	○ **Ad-Hoc** : Sendet Anforderungen von der Schlüsselzielinstanz an die Quellinstanz. Geben Sie die sys_ID der Instanz und die Host-Informationen für die Quelle ein. Nicht unterstützt mit Neuschlüssel des Schlüsselaustauschs. ○ **Einmaliger Klon** : Einmaliger Austausch der Schlüssel aus den Quell-Krypto-Spezifikationen an die Zielinstanz. ○ **Wiederkehrender Klon** : Tauschen Sie Schlüssel aus den ausgewählten Quell-Krypto-Spezifikationen an die Zielinstanz in einem definierten wiederkehrenden Klon.
<Source or Target> Sys_ID der Instanz	○ **Ad-Hoc** : Geben Sie die sys_ID für die Quellinstanz ein, von der die Schlüssel angefordert werden sollen. ○ **Einmaliger Klon** , **Wiederkehrender Klon** : Geben Sie die sys_ID für die Zielinstanz ein, die die Anforderungen sendet. **Tipp:** Geben Sie Ein `Statistiken.do` Im Anwendungsnavigator, um die Instanz-ID zu suchen.
<Source or Target> Instanzhost	Geben Sie den Hostspeicherort oder den Namen der Quell- oder Zielinstanz ein. **Tipp:** Zum Beispiel `instanceA.service-now.com`
Krypto-Spezifikationen	Die Schlüssel aus der Krypto-Spezifikation in einem Krypto-Modul definieren die zu klonenden Schlüssel. Sowohl für einmalige als auch für wiederkehrende Klonanforderungen erstellt Ihre Instanz automatisch einen **Ressourcenaustausch** Modulzugriffsrichtlinie. Sie müssen eine Richtlinie nicht manuell konfigurieren. **Hinweis:** Wählen Sie das Symbol „Suchen mit Liste“ ( ), um die verfügbaren kryptografischen Spezifikationen zu durchsuchen.
Aktivieren Sie die erneute Eingabe	Option zum Aktivieren der automatischen Neueingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

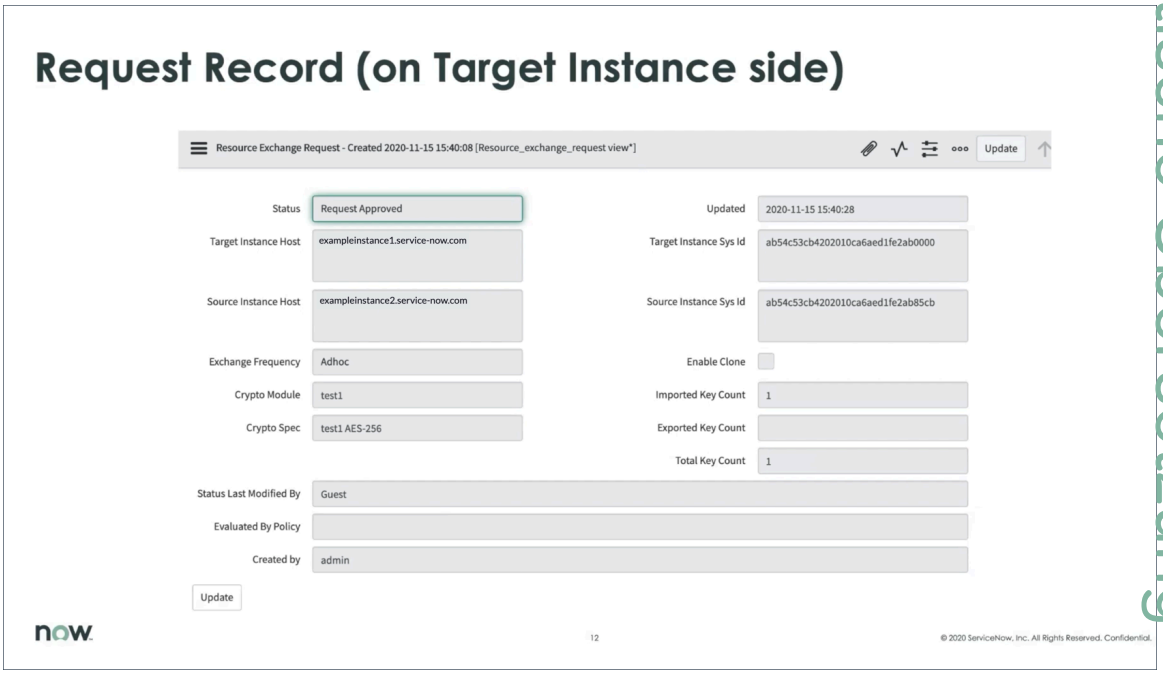
Name	Beschreibung
nach dem Import des Schlüssels	

3. Wählen Sie **Absenden**.
   Wenn erfolgreich, wird oben im Formular eine Bestätigung angezeigt. Die Tabelle „Anforderungen“ wird mit einem Eintrag von aktualisiert **Anforderung Ausstehend** Sowohl in der Quellinstanz als auch in der Zielinstanz. Öffnen Sie den Anforderungsdatensatz, um den Status der Anforderung, die Anzahl der importierten Schlüssel und die Gesamtschlüsselanzahl auf dem Ziel- oder Quellhost anzuzeigen.



4. Die ausstehende Anforderung wird in der Quellinstanz akzeptiert, um den Austausch abzuschließen.

   Beim Klonen wird die Modulzugriffsrichtlinie in der Quellinstanz aufgerufen, um die Anforderung automatisch zu genehmigen und Schlüssel an das neu geklonte Ziel zu senden.



Ergebnis

Nachdem ein Schlüsselaustausch versucht wurde, aktualisiert Ihre Instanz außerhalb der Produktion *protected.script.values.kmf.rekeyed*Systemeigenschaft. Diese Eigenschaft ist in der Tabelle „Systemeigenschaften“ [sys_properties] sichtbar, nachdem ein Schlüsselaustausch versucht wurde. Wenn die Verschlüsselung mit dem ausgetauschten Schlüssel erfolgreich ist, hat diese Eigenschaft einen Wert von **Wahr** . Andernfalls hat die Eigenschaft einen Wert von **Falsch** . Wenn der Wert „falsch“ ist, versucht die Instanz am nächsten Tag erneut, die Verschlüsselung durchzuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geben Sie den verschlüsselten Text mit Schlüsselaustausch erneut ein

Ressourcenaustausch Unterstützt die erneute Eingabe von verschlüsseltem Text in der Zielinstanz, die mit Schlüsseln aus der Quelle verschlüsselt wurde. Die Aktivität zum erneuten Schlüssel wird im Schlüssellebenszyklus nachverfolgt.

Übersicht

Administratoren, die verwenden KMF Für Feldverschlüsselung Kann verwenden Key Exchange Dient zum erneuten Verschlüsseln kryptografischer Schlüssel zwischen Produktionsinstanzen beim Klonen von Daten. Ein aktiver Schlüssel muss zuerst in der Zielinstanz für die erneute Schlüsselerstellung verfügbar sein, da eine erneute Schlüsselerstellung einen aktiven Schlüssel erfordert. Ein Verschlüsselungsauftrag wird automatisch erstellt und vom System ausgeführt, um den Quellschlüssel zu rotieren und neu zu verschlüsseln und den Chiffriertext erneut zu verschlüsseln.

Verwenden Key Exchange So führen Sie Folgendes aus:

- Legen Sie einen Ablaufzeitrahmen für die erneute Schlüsselerstellung fest.

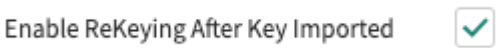
  Wenn die Anforderung abgelaufen ist, wird die Anforderung abgelehnt, und der Schlüssel wird gelöscht.

- Automatisieren Sie die erneute Eingabe von verschlüsseltem Chiffriertext, der mit Schlüsseln aus Quellinstanzen verschlüsselt wurde.

  Ein neuer geklonter Krypto-Schlüssel wird verwendet, um den verschlüsselten Text in der Zielinstanz erneut zu verschlüsseln.

- Der Zweck der Neuschlüssel wird während des Klonvorgangs eingerichtet und als Teil des Klons automatisiert.
- Die Aktivität zum erneuten Schlüssel wird auf nachverfolgt **Modulschlüssel** Registerkarte des kryptografischen Moduls. Greifen Sie auf den Status des Schlüssellebenszyklus und die Schlüsselversion für die Schlüsselaktivität zu. Weitere Informationen finden Sie unter Schlüssel rotieren.

Konfigurieren Sie ein Key Exchange Und wählen Sie aus **Aktivieren Sie Die Erneute Eingabe Nach Dem Import Des Schlüssels** Kontrollkästchen für Aktivierung. Details siehe Konfigurieren Sie Den Schlüsselaustausch.



Wiederkehrender Schlüsselaustausch – Walkthrough

Verwenden Sie diese Führung, um einen wiederkehrenden Schlüsselaustausch in Ihrer Instanz mit und einzurichten Ressourcenaustausch.

Vorbereitungen

Erforderliche Rollen: sn_kmf.cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird

Dieses Beispiel zeigt, wie eine Zielinstanz Schlüssel von einer Hostinstanz anfordert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

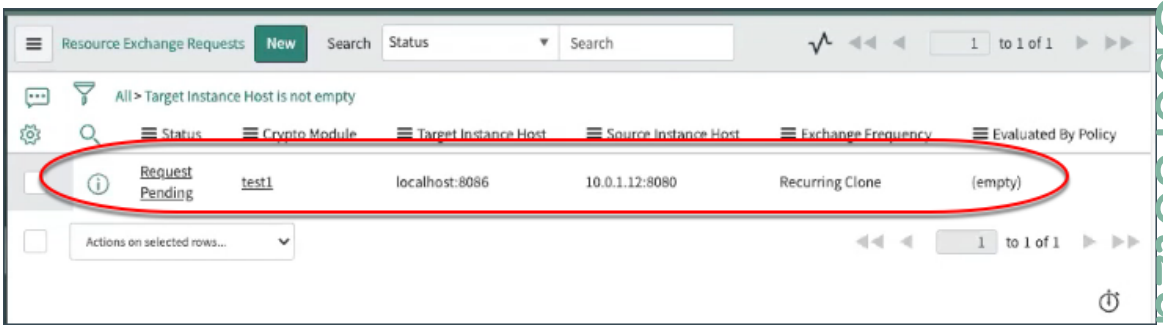
- Bevor Sie dieses Verfahren ausführen können, müssen Sie eine Instanz klonen. Siehe Systemklon Weitere Informationen finden Sie unter .
- **Automatischer Schlüsselaustausch** : Die Basissystemeigenschaft *glide_encryption.auto_key_exchange.enabled*lst **Wahr** Standardmäßig, d. h. beim Klonen einer Instanz ist automatisch aktiviert. Die Eigenschaft wird in die Zielinstanz geklont.
- Deaktivieren Sie automatisch, indem Sie die Eigenschaft auf festlegen **Falsch** .

Prozedur

1. Erstellen Sie in der Quellinstanz ein Krypto-Modul, oder greifen Sie mithilfe von column_level_Encryption auf ein vorhandenes Krypto-Modul zu, und richten Sie die verschlüsselten Feldkonfigurationen für die Verschlüsselung von Chiffriertext für ein Key Exchange.
   Weitere Informationen finden Sie unter und.
   a. Stellen Sie sicher, dass Schlüssel im Krypto-Modul generiert wurden.

   Hinweis: Ihre Instanz erstellt automatisch eine Modulzugriffsrichtlinie bei der Ausführung der Klonanforderung.

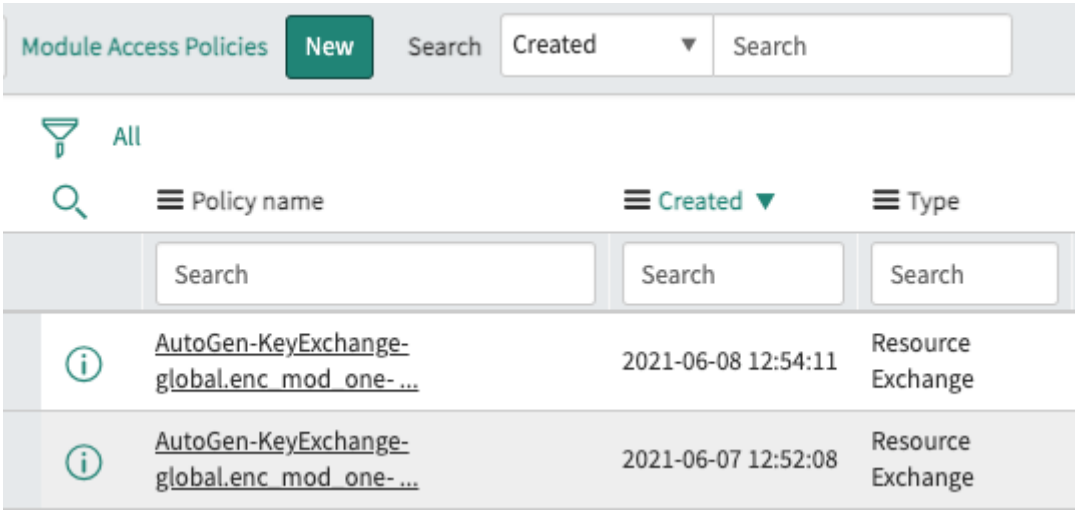
2. Navigieren Sie in der geklonten Instanz zu **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen** > **Neu**an.
3. Füllen Sie das Formular aus, und wählen Sie aus **Wiederkehrender Klon** Als Austauschfrequenz.
4. Navigieren Sie in der Zielinstanz des Klons zu **Schlüsselverwaltung** > **Ressourcenaustausch-Anforderungen**an.
   Die Anforderung von der Hostinstanz wird in der Tabelle angezeigt.



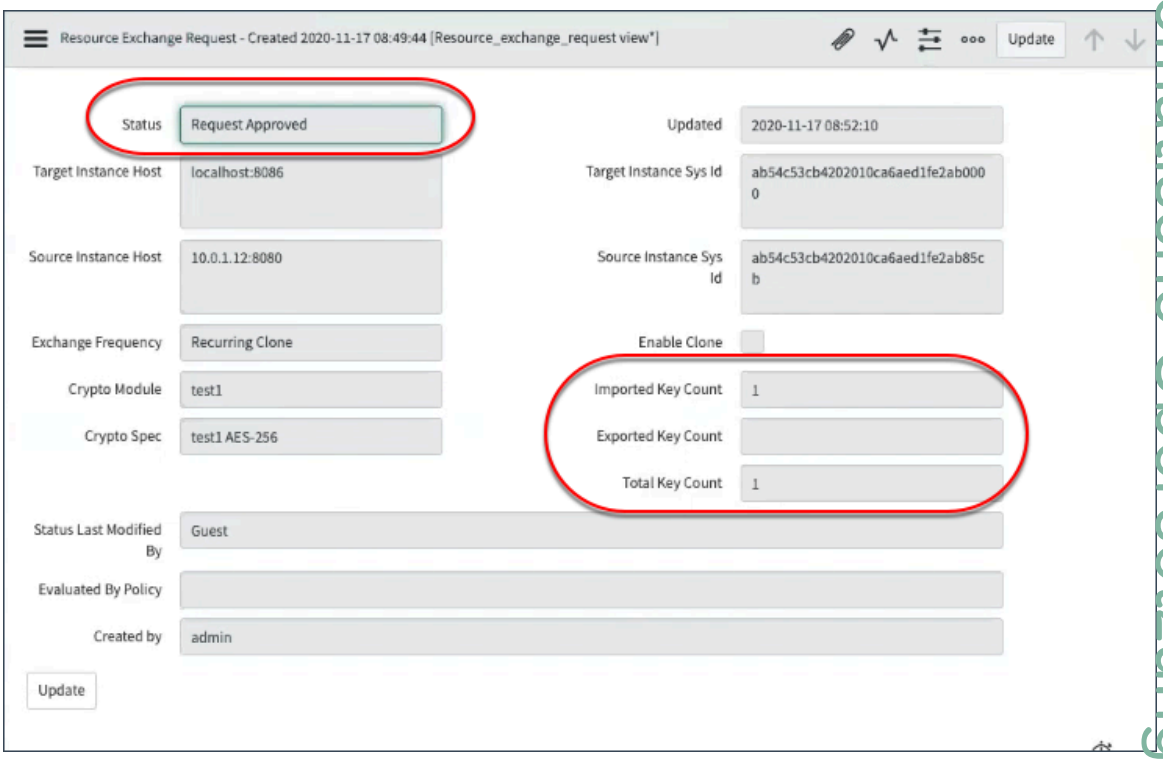
Wichtig: Sowohl für einmalige als auch für wiederkehrende Klonanforderungen erstellt Ihre Instanz automatisch eine Modulzugriffsrichtlinie. Sie müssen eine Richtlinie nicht manuell konfigurieren. Beim Klonen wird diese Richtlinie in der Quellinstanz aufgerufen, um die Anforderung automatisch zu genehmigen und Schlüssel an das neu geklonte Ziel zu senden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



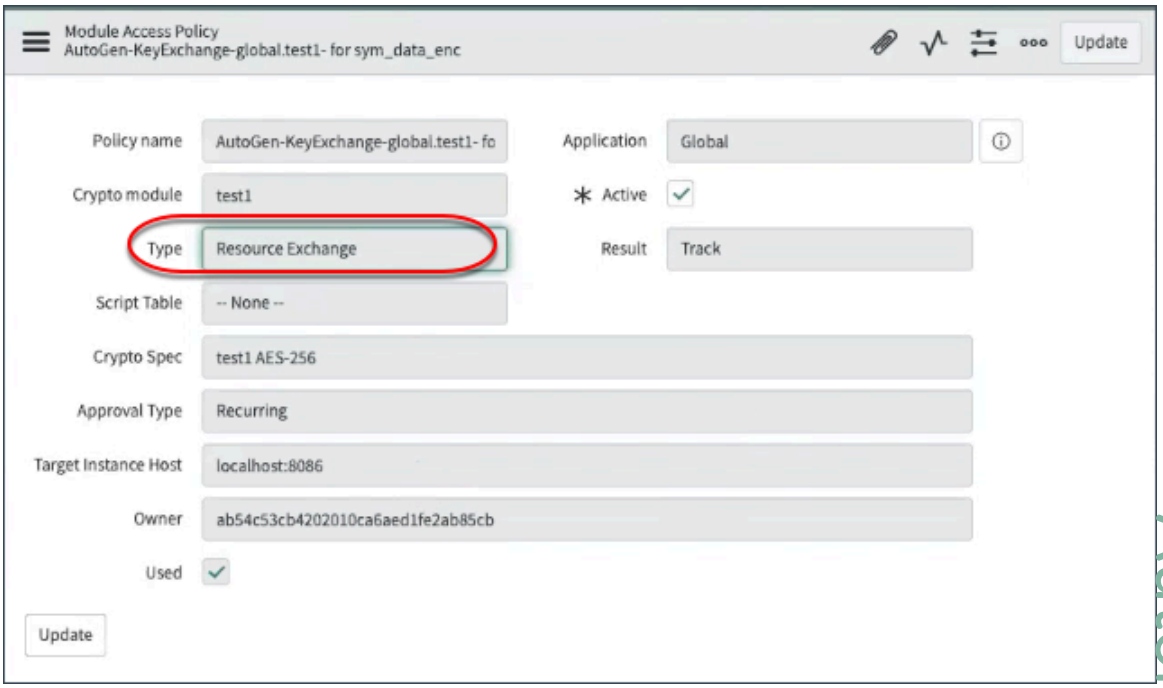
Im Formular „Anforderungen“ wird der Status in aktualisiert **Anforderung Genehmigt** Und **Anzahl Der Importierten Schlüssel** Feld wird im Datensatz angezeigt.



Automatische Übersetzung

5. Kehren Sie zur Hostinstanz zurück.
6. Zeigen Sie den Anforderungsdatensatz an, um die Anzahl der exportierten Schlüssel anzuzeigen.
7. Zeigen Sie den Datensatz der Modulzugriffsrichtlinie an, um anzuzeigen, dass **Typ** Ist Ressourcenaustausch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Ressourcenaustausch Unterstützt auch die erneute Eingabe von verschlüsseltem Text in der Zielinstanz. Weitere Informationen finden Sie unter .

Ergebnis

Nachdem ein Schlüsselaustausch versucht wurde, aktualisiert Ihre Instanz außerhalb der Produktion `protected.script.values.kmf.rekeyed`Systemeigenschaft. Diese Eigenschaft ist in der Tabelle „Systemeigenschaften“ [sys_properties] sichtbar. Wenn die Verschlüsselung mit dem ausgetauschten Schlüssel erfolgreich ist, hat diese Eigenschaft einen Wert von **Wahr** . Andernfalls hat die Eigenschaft einen Wert von **Falsch** . Wenn der Wert „falsch“ ist, versucht Ihre Instanz am nächsten Tag erneut, die Verschlüsselung durchzuführen.

Infrastruktursicherheit

Verwenden Sie Infrastruktursicherheitstools, um Zertifikate zu erstellen, hochzuladen und zu verwalten, die Ihre Instanz zum Verschlüsseln des Datenverkehrs vom Client zum Server verwendet.

Das Plugin „Infrastruktursicherheit“ stellt die Tools bereit, die Sie zum Verwalten der TLS-Verschlüsselungen und Zertifikate (Transport Layer Security) verwenden können. Ihre Instanz verwendet TLS, um Datenverkehr vom Client zu Ihrem Server zu verschlüsseln.

Wählen Sie die in Ihrer Instanz verwendeten Verschlüsselungen aus

Mit **TLS-Seite** , Administratoren können konfigurieren, welche Rechenzentrums-Verschlüsselungen in ihrer Instanz verwendet werden sollen, und die Reihenfolge auswählen, in der Verschlüsselungen versucht werden.

Generieren Sie eigene Zertifikate, und laden Sie sie hoch

Verwenden Sie die Sicherheitstools der Infrastruktur, um eigene Zertifikatsignierungsanforderungen zu generieren, die von der Zertifizierungsstelle Ihrer Wahl signiert werden können. Dann können Sie die Tools verwenden, um das signierte Zertifikat in den Lastenausgleichsmodul Ihrer Instanz hochzuladen.

Überwachen Sie den Status Ihrer Verschlüsselungen und Zertifikate

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie **TLS-Einstellungen** Und **SYOC-Einstellungen** Seiten zum Anzeigen des Status der Änderungen, die Sie an Ihren Verschlüsselungen und Zertifikaten vorgenommen haben.

Installieren Sie das Plugin „Infrastruktursicherheit“

Installieren Sie ServiceNow Plugin „Infrastruktursicherheitseinstellungen“ (com.glide.infrastructure_security), um mit der Verwendung dieser Funktionen zu beginnen. Weitere Informationen zur Plugin-Aktivierung finden Sie unter Aktivieren Sie ein Plugin .

Aktivieren Sie nach der Installation des Plugins die SYOC-Funktionalität (Sign Your Own Security), indem Sie festlegen *sn_infra_sec.syoc.enabled*Systemeigenschaft zu Wahr .

Hinweis: Wenn *sn_infra_sec.syoc.enabled*Eigenschaft ist in Ihrer Instanz nicht verfügbar. Sie müssen sie erstellen. Details zu diesem Vorgang finden Sie unter Systemeigenschaft hinzufügen .

Generieren Sie eine Zertifikatsignierungsanforderung

Verwenden Sie die Seite Certificate Signing (CSR) generieren, um eine Zertifikatsignierungsanforderung zu erstellen, um vom Kunden signierte Zertifikate für Ihren Instanz-Lastenausgleichsmodul zu unterstützen.

Vorbereitungen

Erforderliche Rolle: Administrator

Das Plugin „Infrastruktursicherheit“ (com.glide.infrastructure_security) muss installiert sein, um diese Schritte auszuführen. Siehe Infrastruktursicherheit Für Details zu diesem Plugin.

Informationen zur Verwendung anwenderdefinierter URLs mit ServiceNow, Siehe Legen Sie eine anwenderdefinierte URL als Instanz-URL fest.

Prozedur

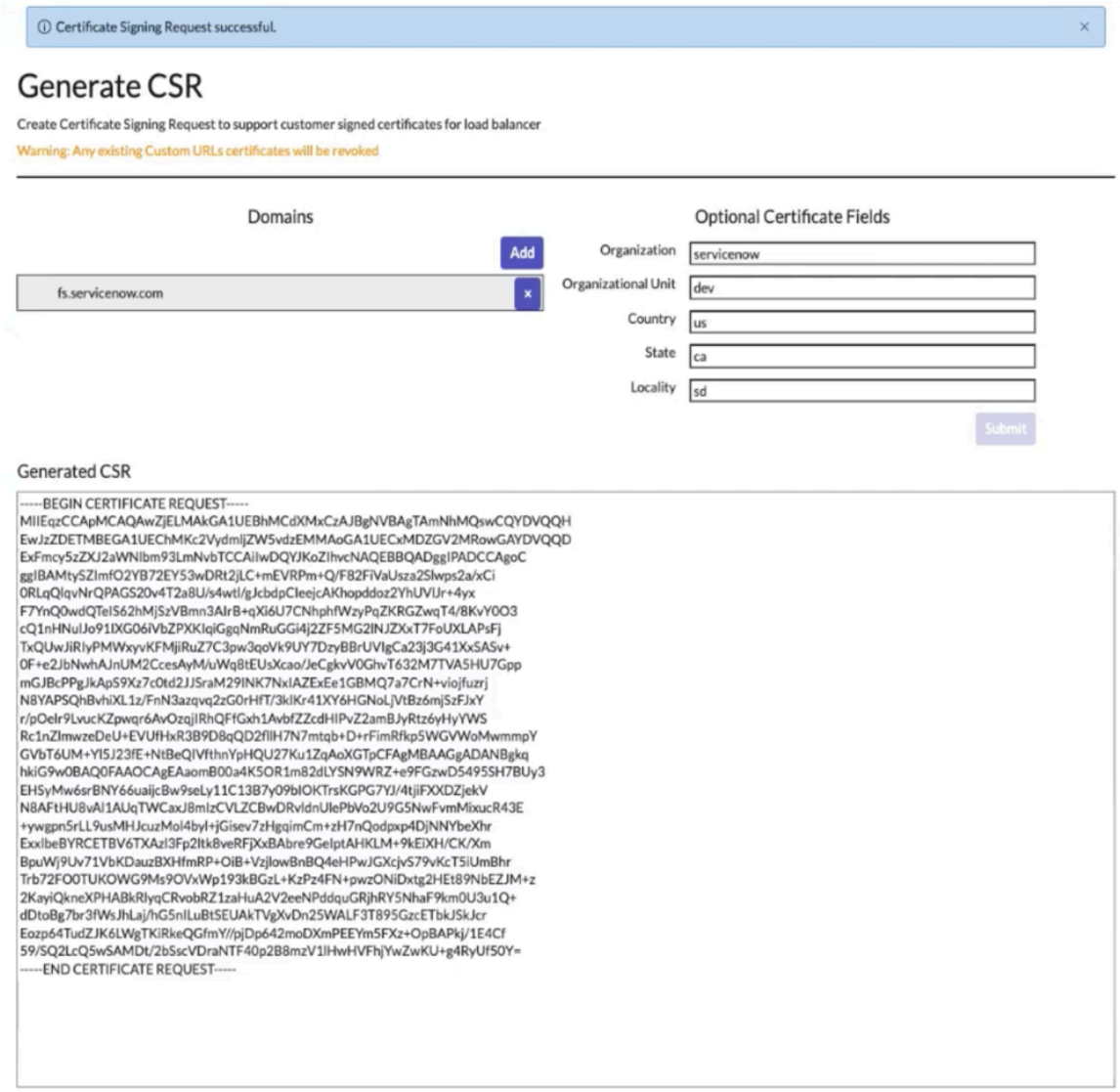
1. Navigieren zu **Alle** > **Sicherheitseinstellungen der Infrastruktur** > **CSR generieren**an.
2. Fügen Sie Ihrer Anforderung eine oder mehrere Domänen hinzu.
   a. Wählen Sie aus **Hinzufügen** Schaltfläche unter **Domänen** Überschrift.
   b. Geben Sie im Popup-Fenster die Domäne ein, und wählen Sie aus **OK** .
   c. Wiederholen Sie diese Schritte nach Bedarf, um weitere Domänen hinzuzufügen.

   Hinweis: Domänen können entfernt werden, indem Sie links neben jedem Domäneneintrag auf die Schaltfläche X klicken.
3. Geben Sie im alle Informationen ein, die in Ihre Anforderung aufgenommen werden sollen **Optionale Zertifikatfelder** .
4. Wählen Sie **Absenden**.

Warnung: Sie können keine Anforderung übermitteln, während eine andere Anforderung generiert wird. Wenn dieses Problem auftritt, wird der Fehler „Ressource in Konflikt“ angezeigt. Brechen Sie zur Verarbeitung die aktuelle Anforderung ab, oder warten Sie, bis die aktuelle Anforderung verarbeitet wird, bevor Sie eine weitere senden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach Auswahl **Übermitteln** , Ihre Instanz generiert die Zertifikatsignierungsanforderung. Die Anforderung wird in angezeigt **CSR generiert** Feld.



5. Kopieren Sie den Inhalt von **CSR generiert** Feld.

Passwort2-Verschlüsselung mit Key Management Framework (KMF)

Unterstützt von Key Management Framework, Verwenden Sie Password2(2-fach verschlüsselt) Feldtyp zum Verschlüsseln und Entschlüsseln anwenderdefinierter Felder mit Aufgabentrennung, Schlüsselschutz und Lebenszyklusmanagement. Es funktioniert gemäß den NIST 800-57-Richtlinien und bietet FIPS 140-2-L3-Schutz.

Password2 Ist ein Textfeld, in dem Passwörter mit bidirektionaler Verschlüsselung gespeichert werden. Die bidirektionale Verschlüsselung speichert Passwörter als sicheren verschlüsselten Wert, der innerhalb der Instanz entschlüsselt werden kann.

Tipp: Beginnt in Vancouver Release können Administratoren die 3DES-Verschlüsselung für Password2-Felder zugunsten des neueren Advanced Encryption Standard (AES) als veraltet festlegen. Details finden Sie unter GlideEncrypter-Nutzung von 3DES für Passwort2-Felder als veraltet festlegen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

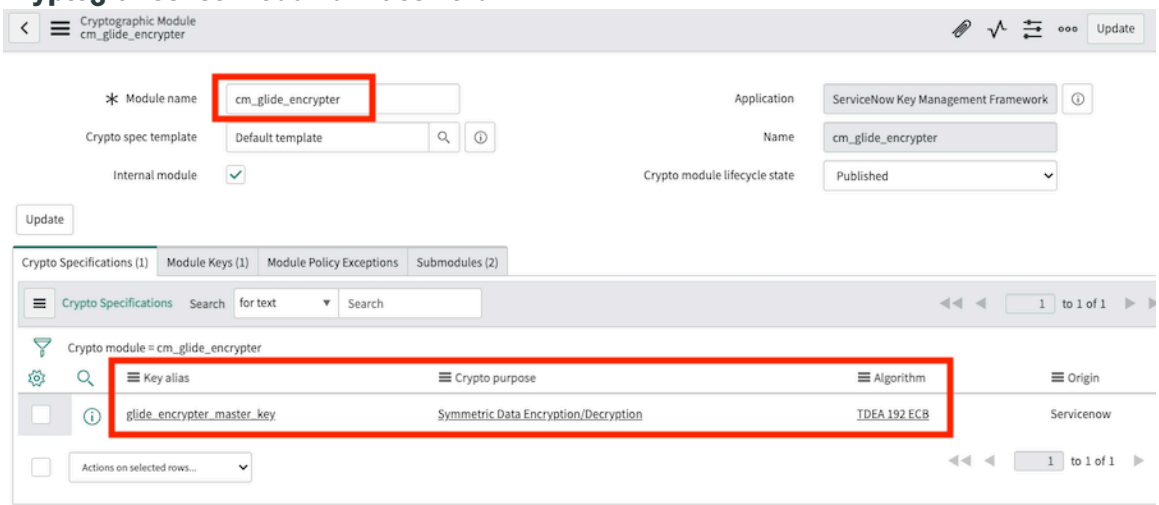
Aktivierung

Password2 Die Funktionalität ist standardmäßig aktiv. Sie wird von gesteuert `glide.kmf.encrypter.enabled`Eigenschaft, die auf festgelegt ist **Wahr** Für alle neuen Instanzen und Upgrades. Sie müssen nicht aktivieren Feldverschlüsselung Enterprise Zu verwenden Password2.

Funktionsweise von Password2

Die Key Management Framework Stellt ein übergeordnetes kryptografisches Modul des Basissystems bereit **Cm_Glide_encrypter** . Dieses Modul bietet eine kryptografische Spezifikation und einen Schlüssel, der Kann Legacy entschlüsseln Password2 Felder.

Kryptografisches Modul für Password2



Dieses Modul „cm_Glide_encrypter“ kann Submodule mit jeweils eigenem Modulschlüssel und eigener Spezifikation haben. Wenn ein Submodul mit demselben Anwendungsbereich wie die Anwendung vorhanden ist, in der Password2 Feld ist , verwendet das System das Submodul. Beispiel: Wenn eine Tabelle in ServiceNow® Kundenservice Die Anwendung verfügt über ein Untermodul, und Sie schreiben Informationen in ein Password2 Feld in einer Tabelle in Kundenservice Anwendungsbereich, ruft der kryptografische Prozess auf Kundenservice Submodul. Der Prozess verwendet auch den Schlüssel dieses Submoduls für die Verschlüsselung und Entschlüsselung mit einem eindeutigen AES 256 GCM-Verschlüsselungsschlüssel. Ein Submodul pro Anwendungsbereich ist zulässig. Übergeordnetes Modul wird nicht immer für den globalen Bereich verwendet. Im Allgemeinen verwenden neue Felder instance_level_Glide_encrypter.

Hinweis: Sie können in keine eigenen Submodule erstellen Zurich. Submodule werden in verschiedenen Anwendungs-Plugins auf bereitgestellt ServiceNow AI Platform. Sie können Schlüssel in Submodulen rotieren, aber nicht das übergeordnete Modul „cm_Glide_encrypter“.

Domänentrennung und lokale Kunden

KMF Password2 Unterstützt keine Domänentrennung. Sie können verwenden Password2 Mit lokalen Instanzen.

Veraltet Password2 Und die aktuelle Password2

In Zurich, Die vorhandene Password2 Feld wurde aktualisiert.

Die aktuelle Implementierung von Password2:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwendet Key Management Framework In Übereinstimmung mit NIST 800-57 Richtlinien für Schlüsselumschließungen und -Bereitstellungen FIPS 140-2-L3 Schutz für die gesamte Schlüsselhierarchie.
- Enthält Fähigkeiten zum Erstellen dedizierter und eindeutiger Elemente KMF Password2 Submodule für bestimmte Anwendungen, die Kontrolle über den Anwendungsbereich bieten. Jedes Submodul verfügt über einen eigenen eindeutigen AES 256 GCM-Verschlüsselungsschlüssel.

Passwort2-Felder in Skripts

Beim Zugriff auf Password2 Felder mit einem Skript: Führen Sie das Skript unter demselben Umfang wie der Tabellenbereich aus. Verwenden SetDisplayValue() Zum Verschlüsseln Password2 Werte und GetDecryptedValue() Zum Entschlüsseln und Lesen des Werts.

Hinweis: Verwenden Sie nicht GlideEncrypter() API auf Password2 Felder.

Dieses Beispielskript zeigt Ihnen, wie Sie verschlüsseln Mein@Passwort In der Spalte „Passwort2“ der Tabelle „table_XYZ“.

```
var  gr =  new GlideRecord('table_xyz');
gr.pwd2column_name.setDisplayValue('my@Password');

gr.insert();
```

Wichtig: Sie können nicht verwenden SetValue() API für Password2 Feld.

Dieses Beispielskript zeigt, wie Sie dasselbe Feld entschlüsseln, um den Wert abzurufen:

```
var  gr =  new GlideRecord('table_xyz');
gr.query();
gr.next();
var ge=gr.getElement('pwd2column_name');
var ged1 = ge.getDecryptedValue();
```

Wichtig: Die GetDecryptedValue() API ist nicht im Bereich enthalten. Es ist global verfügbar.

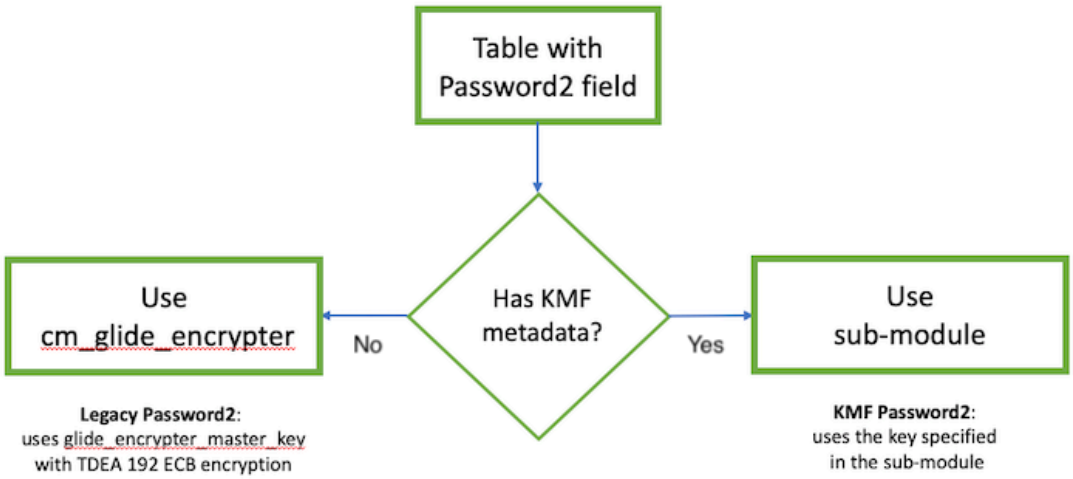
1. Wenn Sie Daten in einem verschlüsseln Password2 Feld bestimmt das System den Umfang der Anwendung, in der Password2 Feld befindet sich.
2. Das System sucht dann nach einem Untermodul von **Cm_Glide_encrypter** Übergeordnetes Modul mit demselben Umfang wie die Anwendung, wenn die Eigenschaft auf festgelegt ist *true*.

   Hinweis: Wenn ein Submodul mit demselben Umfang vorhanden ist, verwendet es die Submodulspezifikation und den Schlüssel, um die Verschlüsselung durchzuführen.

Diese Abbildung erklärt, wie Ihre Instanz Daten in entschlüsselt Password2 Felder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Passwort2-Entschlüsselungs-Flow



KMF Password2 Migrationsauftrag

Für Kunden, die ein Upgrade von vorherigen Releases durchführen, wird ein Migrationsauftrag bereitgestellt. Es werden Daten verwendet, die mit einem Legacy verschlüsselt sind Password2 Verschlüsselung und erneute Verschlüsselung mit dem Schlüssel in einem KMF Password2 Submodulschlüssel. Die erneute Verschlüsselung gilt nur für Tabellen mit Password2 Felder in Anwendungsbereichen, für die auch Submodule für diesen Bereich erstellt wurden. Zum Beispiel ein Legacy Password2 Feld in **XYZ_example** Anwendung (mit **XYZ_example** Anwendungsbereich) wird nur dann erneut verschlüsselt, wenn ein Submodul für den vorhanden ist **XYZ_example** Anwendungsbereich ist unter dem übergeordneten Modul „cm_Glide_encrypter“ vorhanden.

Die KMF Password2 Verschlüsselungsschlüssel im Submodul sind in geschützt (Umschlag verschlüsselt) KMF Schlüsselhierarchie.

Zertifikate

Ihre Instanz erfordert Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen von Zertifikaten kennen.

Konfigurieren



Planen Sie Ihre Kernkonfigurationen.

Hochladen



Planen und richten Sie die Anwendung ein.

Zertifikate Erkunden

Ihre Instanz erfordert Zertifikate, um sichere Verbindungen herzustellen und Signaturen zu validieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikate werden für Funktionen verwendet, z. B.:

- LDAPS
- Gegenseitige Authentifizierung des ausgehenden Webservice
- Webservice – Sicherheit
- MID Server

Um ein Zertifikat zu verwenden, müssen Sie ein Zertifikat für den gesicherten Server oder Client generieren oder erwerben und es in eine Instanz hochladen.

LDAP-Zertifikate

Ein SSL-Zertifikat ist erforderlich, damit die Instanz eine LDAP-über-SSL-Verbindung (LDAPS-Protokoll) mit einem LDAP-Server herstellt.

Die Instanz akzeptiert zwei Arten von LDAP-Zertifikaten:

Zertifikat	Typ	Erforderlich für
LDAP-Serverzertifikat	Beliebiger unterstützter Typ	Alle LDAP-Konfigurationen
LDAP-Clientzertifikat	Java-Schlüsselspeichertyp	Gegenseitige Authentifizierung

Wenn mehrere Serverzertifikate vorhanden sind, versucht die Instanz nacheinander jedes Serverzertifikat, bis der LDAP-Server die Verbindung zulässt. Wenn Sie mehrere LDAP-Server verwenden, müssen Sie das SSL-Zertifikat für jeden LDAP-Server angeben.

Für die gegenseitige Authentifizierung muss der Client zusätzlich zum Server ein Zertifikat vorlegen. Wenn Ihr LDAP-Server gegenseitige Authentifizierung erfordert, müssen Sie auch das Client-Zertifikat Ihres LDAP-Servers in einem Java-Schlüsselspeicher-Typzertifikat angeben.

Zertifikatkriterien

Ein gültiges Zertifikat muss diese Kriterien erfüllen:

- Das Zertifikat kann eine Schlüsselgröße von bis zu 2048 Bit haben.
- Das Zertifikat muss eine der folgenden Dateierweiterungen haben:

Erweiterung	Beschreibung
DER	Die *Eindeutige Codierungsregeln* Format ist eine binäre Nachrichtenübertragungssyntax. Dieses Format unterstützt auch die Dateierweiterungen .CER und .CRT.
CER	Zertifikatdateierweiterungen für Zertifikate mit dem Format Distinguished Encoding Rules.
CRT	Zertifikatdateierweiterungen für Zertifikate mit dem Format Distinguished Encoding Rules.
PEM	Die *Datenschutz – Erweiterte E-Mail* Das Format ist ein Base-64-codiertes DER-Zertifikat, das zwischen „----- ZERTIFIKAT BEGINNEN------ „ Und „------- ENDZERTIFIKAT----- „ Textzeichenfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatvertrauen

Standardmäßig vertraut Ihre Instanz nur Zertifikaten einer Zertifizierungsstelle (Certificate Authority, CA), die in der Java Virtual Machine (JVM) erkannt wurde. Selbst signierte und vom Unternehmen signierte Zertifikate sind nicht vertrauenswürdig.

Hinweis: Weitere Informationen zu den Eigenschaften, die sich auf die Verwendung von Zertifikaten auswirken, finden Sie unter In Instanzsicherheitshärtungseinstellungen.

LDAP-Clientzertifikat wird generiert

Generieren Sie ein LDAP-Clientzertifikat für die gegenseitige Authentifizierung mit OpenSSL. Die endgültige Ausgabe ist ein PKCS#12-Zertifikat, das in einem Java-Schlüsselspeicher gespeichert ist.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Siehe OpenSSL-Dokumentation Weitere Informationen zum Generieren von Zertifikaten. Diese Schritte setzen voraus, dass Sie Zugriff auf OpenSSL haben.

Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein.

Prozedur

1. Generieren Sie ein selbst signiertes Clientzertifikat.

   Example

   Dieser Befehl erstellt beispielsweise ein Clientzertifikat test1-cert.crt basierend auf dem privaten Schlüssel test1-key.key.

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout test1-key.key -out
    test1-cert.crt
   ```

2. Konvertieren Sie sowohl die Zertifikatdatei als auch den privaten Schlüssel in PKCS#12 (eine Datei mit der Erweiterung .pfx oder .p12).

   Example

   Dieser Befehl konvertiert beispielsweise das Clientzertifikat und den privaten Schlüssel in ein PKCS#12-Zertifikat namens test1-certificate.pfx.

   ```
   openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key -in test1-cert.crt
   ```

3. Generieren Sie den Java Key Store, und importieren Sie die pkcs12-Datei in ihn.

   Example

   Dieser Befehl importiert beispielsweise das Zertifikat in den Java-Schlüsselspeicher test1.jks.

   ```
   keytool -importkeystore -srckeystore test1-certificate.pfx -srcstoretype PKCS12
    -destkeystore test1.jks
   ```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Laden Sie das Zertifikat hoch In der Schlüsselspeicherdatei (`test1.jks`) Zur Instanz.

Hinweis:

Wenn Sie ein Zertifikat mit der Erweiterung .jks in eine lokale Instanz hochladen und die Fehlermeldung „kein gültiges Zertifikat zum Verarbeiten des Anwendungs-Uploads gefunden“ erhalten, verwenden Sie stattdessen ein Zertifikat mit der Erweiterung .pfx.

Nächste Maßnahme

Ein Zertifikat wird in eine Instanz hochgeladen

Serverzertifikat wird generiert

Sie können Keytool verwenden, um eine neue Java-Schlüsselspeicherdatei zu generieren, eine Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) zu erstellen und den privaten Schlüssel, das öffentliche Zertifikatpaar und die signierten Zertifikate in den Schlüsselspeicher zu importieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Siehe Java-Keytool-Dokumentation Weitere Informationen zum Generieren von Schlüsseln und CSRs.

Geben Sie diese Befehle in einer Befehlszeilenschnittstelle ein:

Prozedur

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

Example

Dieser Befehl erstellt beispielsweise einen Schlüsselspeicher mit dem Namen my.Keystore und generiert einen privaten Schlüssel mit dem Namen myDomain innerhalb des Schlüsselspeichers.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

Example

Dieser Befehl generiert beispielsweise eine CSR mit dem Namen „mydomain.csr“ oder den mydomain-Schlüssel.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Importieren Sie einen Stamm oder ein Zwischenprodukt *Zertifizierungsstelle* , Oder CA-Zertifikat für den Java-Schlüsselspeicher.

Example

Dieser Befehl importiert beispielsweise das CA-Zertifikat für Thawte. Dieser Befehl geht davon aus, dass Thwate die CA war, die die CSR signiert hat.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. Importieren Sie ein signiertes primäres Zertifikat in den Java-Schlüsselspeicher.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example
Dieser Befehl importiert beispielsweise das signierte Zertifikat mydomain.crt in den Schlüsselspeicher.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

5. Laden Sie das Zertifikat in der Schlüsselspeicherdatei (my.Keystore) in die Instanz hoch.

Nächste Maßnahme
Ein Zertifikat wird in eine Instanz hochgeladen

Ein Zertifikat wird in eine Instanz hochgeladen

Fügen Sie der Instanz ein Zertifikat aus dem Zertifikatmodul hinzu.

Laden Sie ein Zertifikat in eine Instanz hoch

Laden Sie ein Zertifikat in eine Instanz hoch.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Zertifikat auf dem ADFS-Server aktualisiert wird, müssen Sie auch ein aktualisiertes Zertifikat in die Instanz hochladen.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Zertifikate**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für das Zertifikat an.
Ablaufbenachrichtigung	[Optional] Wählen Sie aus, ob Sie eine Benachrichtigung senden möchten, wenn das Zertifikat abläuft.
Aktiv	Wählen Sie aus, ob die Instanz dieses Zertifikat für sichere Kommunikationen und Signaturanforderungen verwenden soll.
Kurzbeschreibung	[Optional] Geben Sie eine Textbeschreibung des Zertifikats ein, z. B. den anfordernden Personen- oder Servernamen.
Format	Wählen Sie das Zertifikatformat aus. Die Instanz unterstützt die Formate PEM und DER.
Typ	Wählen Sie den Zertifikatcontainer aus. Die Instanz erkennt Zertifikate aus Truststores, Java-Schlüsselspeicher und PKCS#12-Schlüsselspeicher.
PEM-Zertifikat	Geben Sie den Base-64-codierten PEM-formatierten Text ein, der das DER-Zertifikat enthält. Die Instanz decodiert das Zertifikat, um auszufüllen **Gültig ab** ,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Läuft Ab , **Läuft in Tagen ab** , **Aussteller** , Und **Betreff** Felder.

4. Wählen Sie **Absenden**.

   Während des Uploads extrahiert das Modul die schreibgeschützten Eigenschaften des Zertifikats und zeigt sie in diesen Feldern an:

   - Gültig ab Datum
   - Ablaufdatum
   - Bearbeiter
   - Betreff des Zertifikats

5. Wählen Sie Aus **Validiert Speicher/Zertifikate** Um zu überprüfen, ob das Zertifikat korrekt ist. Wenn die Instanz Fehler mit dem Zertifikat oder Schlüsselspeicher erkennt, wird eine Fehlermeldung angezeigt.

Ein vertrauenswürdiges Serverzertifikat wird hochgeladen

Durch Hochladen des vertrauenswürdigen Serverzertifikats des Service Providers stellt die Instanz sicher, dass eine Verbindung zu einem gültigen und sicheren Service hergestellt wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Instanz validiert ausgehende Webserviceaufrufe mithilfe des vom Service Provider bereitgestellten Zertifikats.

Prozedur

1. Erstellen Sie einen neuen Zertifikatdatensatz mit dem Typ **Trust Store-Zertifikat** .
2. Führen Sie eine der folgenden Aktionen aus:
   - Hängen Sie das im Format DER-Zertifikat des Service Providers an.
   - Kopieren Sie das Zertifikat im PEM-Format des Service Providers, und fügen Sie es in ein **PEM-Zertifikat** Feld.

Feldverschlüsselung

Schützen Sie verschlüsselte Daten in Ihrer Instanz mit vor nicht autorisierten Anwendern, Skripts oder Systemprozessen Feldverschlüsselung.

Feldverschlüsselung Ist ein Verschlüsselungsprodukt, das auf basiert ServiceNow Key Management Framework. Feldverschlüsselung Ermöglicht die Verschlüsselung bestimmter Felder oder Anhänge in einer Instanz. Verwenden Feldverschlüsselung In Kombination mit Cloud Encryption und Zugriffssteuerungslisten (ACLs), um vertrauliche Informationen vor angemeldeten Anwendern zu schützen, die nicht zum Anzeigen berechtigt sind.

Feldverschlüsselung Hat zwei verfügbare Versionen.

Feldverschlüsselung Starter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldverschlüsselung Starter ist in enthalten ServiceNow Plattform kostenlos und unterstützt Verschlüsselung für eine begrenzte Anzahl von Feldern.

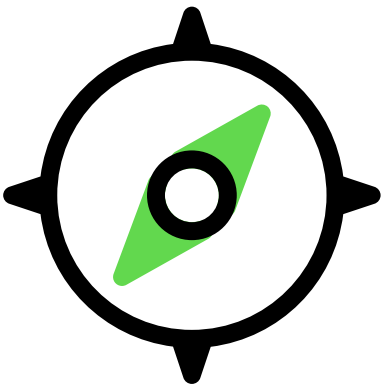
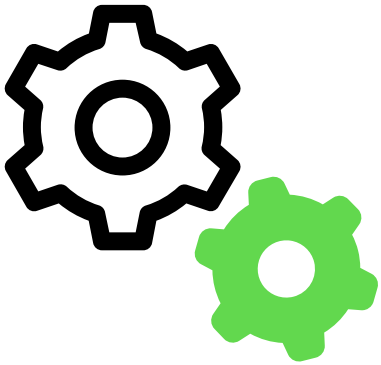
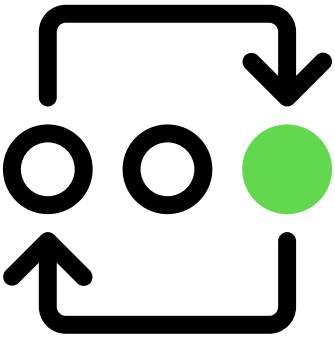
Feldverschlüsselung Enterprise

Feldverschlüsselung Enterprise ist eine Premium-Abonnementversion des Produkts, die für Kunden verfügbar ist, die abonnieren ServiceNow Tresor, Plattformverschlüsselung oder Feldverschlüsselung Enterprise.

Weitere Informationen zum Unterschied zwischen diesen Versionen finden Sie unter Feldverschlüsselung erkunden.

Feldverschlüsselung Ersetzt Verschlüsselung auf Spaltenebene Produkt verfügbar in Xanadu Und frühere Releases.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über die Vorteile der Starter- und Enterprise-Versionen von Feldverschlüsselung.	Erfahren Sie, wie Sie aktivieren und konfigurieren Feldverschlüsselung Enterprise, Und verwalten Sie die Migration über Verschlüsselungsunterstützung oder Verschlüsselung auf Spaltenebene.	Verwenden Feldverschlüsselung Dient zum Verwalten des Zugriffs auf verschlüsselte Daten in Ihren Instanzen

an.

Hilfreiche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

ServiceNow Community

ServiceNow Community

Customer Success Center

Customer Success Center

Entwickler

developer.servicenow.com

Impact

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

http://impact.servicenow.com

ServiceNow University

ServiceNow-Universität

Jetzt erstellen

Now Create

Partner

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

ServiceNow

https://www.servicenow.com/

ServiceNow Store

https://store.servicenow.com/

Support

https://support.servicenow.com/now

Known Error-Portal

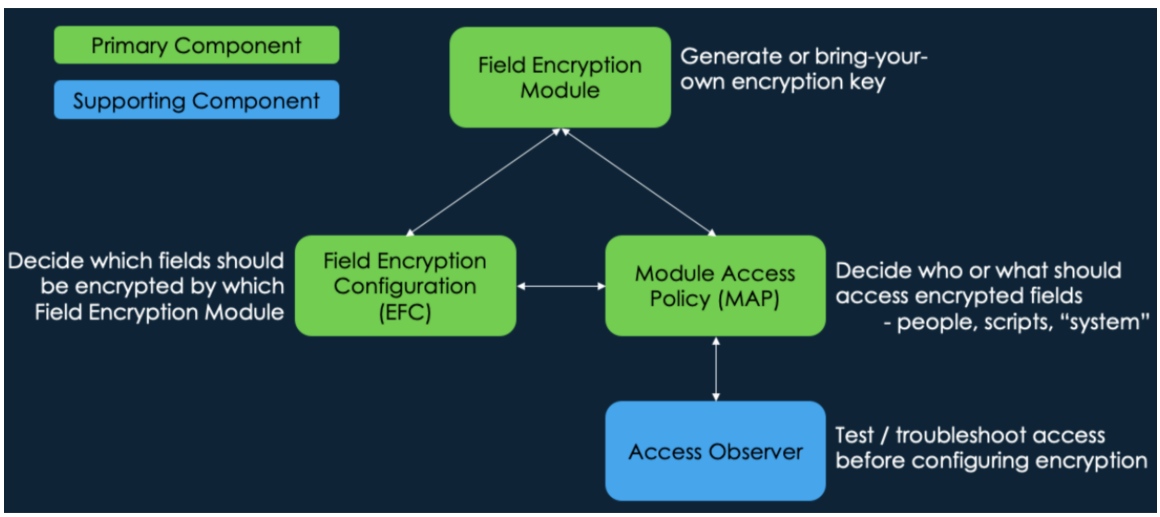
Feldverschlüsselung erkunden

Erfahren Sie mehr über die Details von Feldverschlüsselung Starter und Feldverschlüsselung Enterprise

Verschlüsselungsgestützte Zugriffssteuerung

Standardmäßig Feldverschlüsselung Blockiert alle Anwender, Skripts und Systemprozesse am Zugriff auf verschlüsselte Daten. Jedoch Feldverschlüsselung Verfügt über eine Zugriffssteuerungsfunktion, die in Kombination mit Zugriffssteuerungslisten (Access Control Lists, ACLs) verwendet wird, um sicherzustellen, dass nur die richtigen Anwender, Skripts oder Systemprozesse auf verschlüsselte Daten zugreifen können.

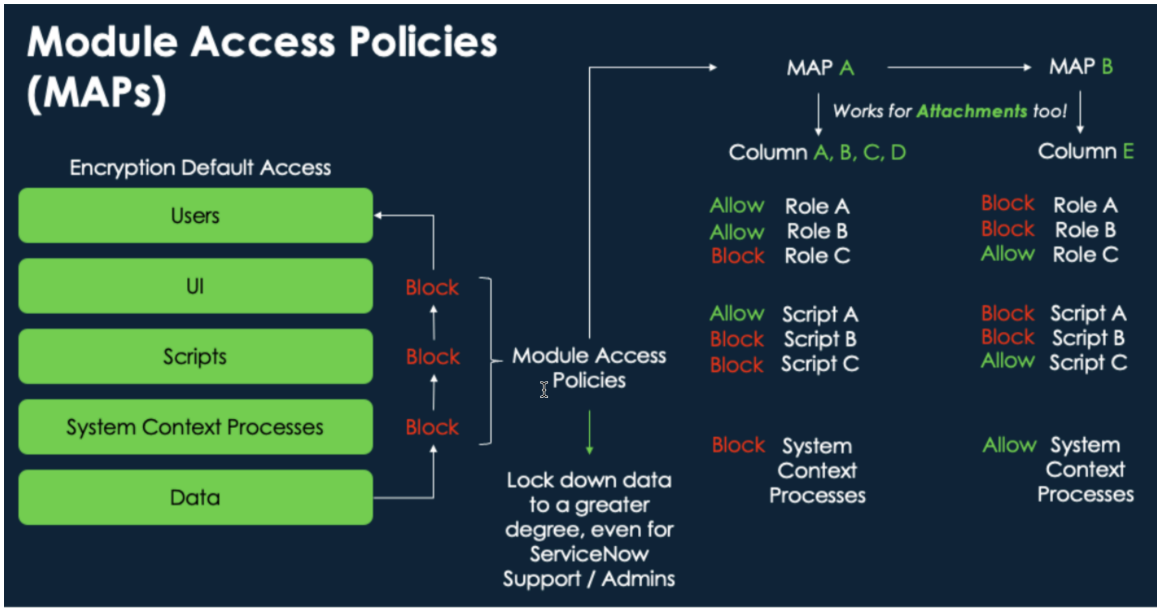
Sie können konfigurieren Feldverschlüsselung Zugriffssteuerungsfunktion von durch eine Kombination von Feldverschlüsselung Module, verschlüsselte Feldkonfigurationen und Modulzugriffsrichtlinien. Die nächste Abbildung zeigt, wie diese drei Komponenten zusammenarbeiten.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriffsrichtlinien (im nächsten Bild angezeigt) zeigen, wie Anwender, Skripts oder Systemprozesse berechtigt werden können, auf verschlüsselte Daten zuzugreifen (standardmäßig sind die verschlüsselten Daten jedoch für jeden Zugriff in der Instanz gesperrt).



Unterschiede zwischen Feldverschlüsselung Starter und Feldverschlüsselung Enterprise

Der Funktionssatz unterscheidet sich zwischen Feldverschlüsselung Starter und Feldverschlüsselung Enterprise.

Funktion	Feldverschlüsselung Starter	Feldverschlüsselung Enterprise
Anzahl der verschlüsselten Felder	Bis zu 5 verschlüsselte Felder	Keine Einschränkung für die Anzahl der verschlüsselten Felder
Anhangsverschlüsselung	Nein	Ja
Schlüsselverwaltung	Keine (Kontakt ServiceNow Unterstützung für Schlüsselrotation)	Verwalten Sie Schlüssel aus Ihrer Instanz ohne Beteiligung von ServiceNow Support
Unterstützte Datentypen	Alle unterstützten Datentypen	Alle unterstützten Datentypen
Anzahl der Feldverschlüsselungsmodule	Keine Einschränkung	Keine Einschränkung
Anzahl der Modulzugriffsrichtlinien	Keine Einschränkung	Keine Einschränkung

Feldverschlüsselung Anwender

Anwender

Anwender	Beschreibung
Key Management Framework (KMF)Admin oder KMF Cryptographic Manager	Diese Rollen werden verwendet, um Elemente von zu konfigurieren Feldverschlüsselung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung
	• Feldverschlüsselung Module und Modulschlüssel • Kryptografische Spezifikationen • Modullebenszyklusrichtlinien • Verschlüsselte Feldkonfigurationen für Felder und Anhänge • Modulzugriffsrichtlinien (Zuordnungen) • Konfiguriert, umschließt und lädt vom Kunden bereitgestellte Schlüssel (für) hoch Feldverschlüsselung Enterprise) • Konfiguriert Access Observer und überprüft Access Observer-Protokolle. • Planen Sie die Massenverschlüsselung, -Entschlüsselung oder -erneute Schlüsselerstellung
Kryptografischer KMF-Operator	Konfiguriert Eigenschaften für vom Kunden bereitgestellte Schlüssel

Feldverschlüsselung Und Datensatzverlauf

Ändert sich an Feldern, die mit verschlüsselt wurden Feldverschlüsselung Werden im Aktivitätenstrom für den Datensatz oder in der Tabelle „Datensatzverlauf“ [sys_history_Set] nicht nachverfolgt.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Feldverschlüsselung finden Sie unter:

- Feldverschlüsselung konfigurieren
- Feldverschlüsselung verwenden

Feldverschlüsselung konfigurieren

Erfahren Sie, wie Sie aktivieren und konfigurieren Feldverschlüsselung Und verwalten Sie die Migration über Verschlüsselungsunterstützung.

Feldverschlüsselung aktivieren

Erfahren Sie, wie Sie entweder oder aktivieren Feldverschlüsselung Enterprise.

Rollen, die zum Konfigurieren der Feldverschlüsselung erforderlich sind

Erfahren Sie mehr über die Rollen, die zum Konfigurieren erforderlich sind Feldverschlüsselung.

Migration von Verschlüsselungsunterstützung

Verwenden Sie geplante Aufgaben, um Ihre Schlüssel und verschlüsselten Daten von Legacy-Verschlüsselungsunterstützung zu zu migrieren Feldverschlüsselung Enterprise. Details zu diesem Prozess finden Sie unter Migrieren zu Feldverschlüsselung Enterprise

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ändern Sie die Einstellungen für die Anhangverschlüsselung

Verbessern Sie die Sicherheit, indem Sie verhindern, dass Anwender unverschlüsselte Dateien anhängen. Details finden Sie unter Verhindern Sie, dass Anwender unverschlüsselte Dateien anhängen.

Feldverschlüsselung aktivieren

Aktivieren Sie entweder Feldverschlüsselung Starter oder Feldverschlüsselung Enterprise.

Vorbereitungen

Erforderliche Rolle: Administrator

ServiceNow Wurde ersetzt Verschlüsselung auf Spaltenebene Mit Feldverschlüsselung Beginnt in Yokohama Release.

In Yokohama Release, Kunden, die zuvor nicht verwendet haben Verschlüsselung auf Spaltenebene Kann beginnen, beides zu verwenden Feldverschlüsselung Starter oder Feldverschlüsselung Enterprise Unter der neuen Berechtigungsstruktur.

Kunden, die verwendet haben Verschlüsselung auf Spaltenebene In früheren Releases und wer mit beginnen möchten Feldverschlüsselung, Haben die folgenden Optionen:

Feldverschlüsselung Starter

Verschlüsselung auf Spaltenebene Starterkunden können installieren Feldverschlüsselung Starter ohne erneute Implementierung. Feldverschlüsselung Der Starter übernimmt die vorhandene Konfiguration und fügt nahtlos neue Funktionen hinzu.

> ⚠ **Warnung:** Es gibt Unterschiede in der Berechtigung zwischen Verschlüsselung auf Spaltenebene Starter und Feldverschlüsselung Starter. Vor der Installation Feldverschlüsselung Starter: Stellen Sie sicher, dass Ihre Konfiguration den Berechtigungen entspricht. Für Informationen zu Berechtigungen für Feldverschlüsselung Starter, siehe Feldverschlüsselung erkunden.

Feldverschlüsselung Enterprise

Verschlüsselung auf Spaltenebene Enterprise-Kunden sollten mit ihren Account-Teams zusammenarbeiten, um sicherzustellen, dass sie über die richtige Berechtigung für verfügen Feldverschlüsselung Enterprise. Sobald dies geschieht, wird Feldverschlüsselung Enterprise Das Plugin kann in ihren Instanzen installiert werden.

> ℹ **Wichtig:** Verschlüsselung auf Spaltenebene Enterprise gewährt nicht automatisch eine Berechtigung für Feldverschlüsselung Enterprise, Da es sich um ein anderes, aber Ersatz-Produkt handelt.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**
2. Unter **Durchsuchen Sie Ihre lizenzierten Anwendungen und Plugins** , Suchen nach `Feldverschlüsselung` .
   Bei der Suche sollte das Plugin angezeigt werden. Wenn Sie ein Abonnement für erworben haben Feldverschlüsselung Enterprise, Sie können dieses Plugin auch verfügbar sehen.

> ℹ **Wichtig:** Zum Aktivieren Feldverschlüsselung Enterprise, Sie müssen zuerst ein Abonnement erwerben. Ihr Account Manager kann das Plugin in den Produktions- und nicht-Produktionsinstanzen Ihrer Organisation aktivieren, im Allgemeinen innerhalb weniger Tage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie oder aus Feldverschlüsselung Enterprise, Und wählen Sie dann aus **Installieren** .

> **Hinweis:** Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Rollenanforderungen für Feldverschlüsselung

Erfahren Sie mehr über die Rollen, die zum Konfigurieren erforderlich sind Feldverschlüsselung.

Für die Verwaltung sind die folgenden Rollen erforderlich. Seit basiert auf Key Management Framework, Es gibt Rollen, die für beide gemeinsam sind.

- Administrator
- Sicherheitsadministrator
- KMF-Administrator
- KMF Cryptographic Manager

Vollständige Details zu Details zu Rollen finden Sie unter Mit Key Management Framework installierte Rollen.

Administrator und Sicherheitsadministrator

Benutzer müssen über die Administratorrolle verfügen, um zur Sicherheitsadministratorrolle zu wechseln. Sie benötigen die Rolle „Sicherheitsadministrator“, um Aufgaben mit hoher Sicherheit auszuführen, z. B. Konfigurationen für verschlüsselte Felder und Konfiguration von Access Observer.

Administratoren können mit diesem Verfahren zum Sicherheitsadministrator hochstufen.

1. Wählen Sie in Ihrem Profilbild oben rechts auf dem Bildschirm aus.
2. Wählen Sie im Dropdown-Menü die Option aus **Erhöhen Sie Die Rolle** .
3. Wählen Sie Aus **Sicherheitsadministrator** .
4. Wählen Sie **Speichern**.

KMF-Administrator

Anwender mit der Administratorrolle können Anwender mit diesem Prozess der KMF-Administratorrolle zuweisen:

1. Navigieren zu **Alle** > **Systemsicherheit** > **Administration der Schlüsselverwaltung**an.
2. Von **Verfügbare Anwender** Einen Anwender, der die Rolle „KMF-Administrator“ benötigt, in die verschieben **Ausgewählte Anwender** Liste.
3. Wählen Sie **Speichern**.

> **Wichtig:** Um Sicherheitsprobleme zu vermeiden, sollten Sie vermeiden, die KMF-Administratorrolle mehreren Anwendern zu gewähren. Vermeiden Sie die Zuweisung dieser Rolle an Anwender, wenn speziellere Rollen verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

KMF Cryptographic Manager

Benutzer mit der Rolle „KMF Cryptographic Manager“ können Vorgänge für kryptografische Module und Modulzugriffsrichtlinien erstellen und aktualisieren. KMF-Kryptografiemanager können auch Schlüsselverwaltungs- und Lebenszyklusvorgänge durchführen.

Verwenden Sie den folgenden Prozess, um diese Rolle einem Anwender zuzuweisen.

1. Navigieren zu **Alle** > **Systemsicherheit** > **Anwender**an.
2. Wählen Sie einen Anwender aus, der konfiguriert werden muss Feldverschlüsselung.
3. In **Rollen** Zugehörige Liste, wählen Sie aus **Bearbeiten** .
4. Suchen Sie nach sn_kmf.kryptografischer Manager Und fügen Sie die Rolle des ausgewählten Anwenders hinzu.
5. Wählen Sie **Speichern**.

Konfigurieren Feldverschlüsselung Module

Erfahren Sie, wie Sie konfigurieren Feldverschlüsselung Module.

Vorbereitungen

Erforderliche Rolle: KMF-Administrator oder KMF Cryptographic Manager

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Feldverschlüsselungsmodule**an.
2. Wählen Sie **Neu**.
3. Füllen Sie im Modul-Formular die hier angezeigten Felder aus.

Feld	Wert
Modulname	Wählen Sie einen Namen für das Modul aus. Dieser Name wird beim Ausführen von Skripts referenziert.
Krypto-Spezifikationsvorlage	Wird automatisch mit ausgefüllt **Standardvorlage** . Diese Vorlage wird verwendet, um das kryptografische Modul zu erstellen, das Zuordnungen vieler kryptografischer Zwecke zu kryptografischen Spezifikationen und empfohlenen Algorithmen enthält.
Anwendung	Der Anwendungsbereich für dieses Modul. Dieses Feld wird automatisch mit der aktuellen Anwendung gefüllt.
Name	Dieser Name wird automatisch generiert. Dies ist der Modulname, dem der Name des Anwendungsbereichs vorangestellt ist, um Konflikte mit anderen bereichsbezogenen Anwendungen zu vermeiden. Beispiel: Wenn Sie ein Modul mit dem Namen erstellen Mein_Krypto_Modul Im globalen Anwendungsbereich wird der Name als gespeichert Global.my_crypto_Module .
Lebenszyklusstatus Des Krypto-Moduls	Der Begriff „Lebenszyklus“ bezieht sich auf die Erstellung, Verwendung und Deaktivierung eines kryptografischen Moduls. Legen Sie diesen Wert auf fest **Entwurf** Anfänglich während der Konfiguration. Legen Sie sie auf fest **Veröffentlicht** Zur aktiven Verwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Hinweis: Die Standardvorlage wird automatisch auf festgelegt **Veröffentlicht** .
Übergeordnetes Krypto-Modul	Für Feldverschlüsselung, Stellen Sie sicher, dass dieser Wert auf festgelegt ist **Column_level_Encryption** .

4. Wählen Sie **Absenden**.

Nächste Maßnahme

Konfigurieren Sie den Zweck, den Algorithmus, die Schlüssellänge, den Modus und den Ursprung Ihres Verschlüsselungsschlüssels in Kryptografische Spezifikationen für Feldverschlüsselung.

Kryptografische Spezifikationen für Feldverschlüsselung

Verwenden Sie kryptografische Spezifikationen, um Zweck, Algorithmus, Schlüssellänge, Modus und Ursprung Ihres Verschlüsselungsschlüssels zu definieren.

Vorbereitungen

Erforderliche Rolle: KMF-Administrator oder KMF Cryptographic Manager

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren zeigt, wie generierte Schlüssel konfiguriert werden. Ein Datenverschlüsselungsschlüssel (bekannt als Modulschlüssel) wird automatisch ausgefüllt, sobald Sie die Krypto-Spezifikationen konfiguriert haben.

Informationen zur vom Kunden bereitgestellten Schlüsselkonfiguration finden Sie unter Konfigurieren Sie vom Kunden bereitgestellte Schlüssel für Feldverschlüsselung Enterprise.

Prozedur

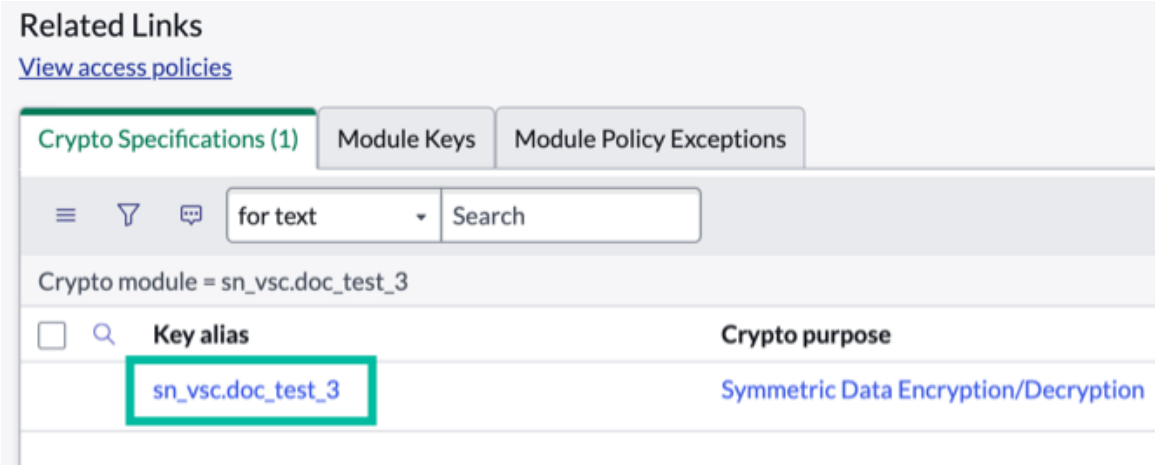
1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Feldverschlüsselungsmodule**an.
2. In **Kryptografische Module** Liste öffnen Sie den Moduldatensatz, den Sie konfigurieren möchten.

   Hinweis: Die in der Liste angezeigten Namen werden an den Umfang angehängt, z. B. Global. [Name des Feldverschlüsselungsmoduls] .

3. In **Krypto-Spezifikationen** Zugehörige Liste öffnen Sie den kryptografischen spezifischen Datensatz, indem Sie unter den Namen auswählen **Schlüsselalias** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die Felder im Formular „kryptografische Spezifikationen“ nach Bedarf aus.

Hinweis: Die Felder sind in Abschnitte unterteilt. Wählen Sie aus **Als Nächstes** Oder **Zurück** Schaltflächen zum Navigieren zwischen Abschnitten.

Abschnitt	Feld	Beschreibung
Algorithmusdefinition	Krypto-Modul	Zeigt den Namen des ausgewählten kryptografischen Moduls an.
	Kryptografischer Zweck	Der Zweck des ausgewählten Algorithmus, Schlüssels, Länge und Modus. Für Feldverschlüsselung, Dieses Feld ist schreibgeschützt und hat einen Wert von **Symmetrische Datenverschlüsselung/-Entschlüsselung** .
	Algorithmus	Wählen Sie einen Algorithmustyp aus, der zum Erreichen des kryptografischen Zwecks verwendet wird. Die verfügbaren Optionen werden gefiltert, um sie an dem ausgewählten kryptografischen Zweck auszurichten.
Lebenszyklusdefinition	Betrifft	Zeigt den ausgewählten Schlüssel an, für den der Lebenszyklus gilt.
	Für Feld	Wählen Sie den Typ der Steuerung für den Schlüssel aus, den Sie für den Lebenszyklus anwenden möchten. ○ Ablaufdatum ○ Künftiges Aktivierungsdatum ○ Künftiges Zerstörungsdatum ○ Künftiges Verlängerungsdatum ○ Künftiges Rotationsdatum
	Schlüsseltyp	
	Lebenszyklusstandard	
	Reihenfolge	Reihenfolge, in der der Schlüssel-Lebenszyklusstatus für die Krypto-Spezifikation verarbeitet werden soll. Niedrigere Werte werden vor höheren Werten ausgeführt.
	Relative Dauer	Anzahl der Jahre, Monate oder Tage, die der Schlüssel gültig ist.
	Typ relative Dauer	Dauertyp des Lebenszyklus. Wählen Sie aus **Jahre** , **Monate** , Oder **Tage** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt	Feld	Beschreibung
	Relativer Betrieb	Wählen Sie Aus **Vor** Oder **Nach** .
	Relativ zu	Wählen Sie ein Feld aus, zu dem die Dauer relativ ist. ○ Aktivierungsdatum ○ Datum der Gefährdung ○ Deaktivierungsdatum ○ Zerstörungsdatum ○ Ablaufdatum ○ Generierungsdatum ○ Letztes Verlängerungsdatum ○ Letztes Rotationsdatum ○ Sperrdatum **Hinweis:** Dieses Feld arbeitet mit dem in ausgewählten Wert zusammen **Relativer Vorgang** Feld.
	Typ	Wählen Sie aus, ob der Wert für den Schlüssellebenszyklus relativ oder absolut ist. **Relativ** Geben Sie einen Wert ein, der von anderen Dateneinträgen im System abhängt, z. B. Schlüsselgenerierung, Aktivierung und Deaktivierung. **Absolut** Geben Sie einen genauen Wert ein, z. B. ein Datum.
Schlüsselursprung	Krypto-Modul	Zeigt den Namen des ausgewählten kryptografischen Moduls an.
	Quelle	Gibt an, ob der Schlüssel vom Kunden stammt oder vom Kunden bereitgestellt wird. ○ Wählen Sie für Starter aus **Servicenow** ○ Wählen Sie für Enterprise die Option aus **Servicenow** Oder **Vom Kunden Bereitgestellt**
	Schlüssel-Alias	Name des kryptografischen Moduls mit dem Bereich, der an die Vorderseite des Namens angehängt ist.
	Kryptografischer Zweck	Zeigt den Zweck des ausgewählten Algorithmus, Schlüssel, Länge und Modus an. Für Feldverschlüsselung, Dieses Feld ist schreibgeschützt und hat einen Wert von **Symmetrische Datenverschlüsselung/-Entschlüsselung** .
	Algorithmus	Zeigt den Algorithmus an, der zum Erreichen des Krypto-Zwecks verwendet wird.
Schlüsselerstellung	Krypto-Modul	Zeigt den Namen des ausgewählten kryptografischen Moduls an.
	Schlüssel-Alias	Zeigt den Namen des kryptografischen Moduls an, dessen Umfang an die Vorderseite des Namens angehängt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt	Feld	Beschreibung
	Schlüssel generieren	Wählen Sie diesen Link aus, um Ihren Datenverschlüsselungsschlüssel zu generieren, wenn Sie einen generierten Schlüssel und keinen vom Kunden bereitgestellten Schlüssel verwenden.
	Schlüssel automatisch generieren	Wenn Sie nicht auswählen **Schlüssel generieren** Link, wird automatisch ein Datenverschlüsselungsschlüssel generiert, wenn Daten zum ersten Mal mit dem kryptografischen Modul verschlüsselt werden müssen.
	Kryptografischer Zweck	Zeigt den Zweck des ausgewählten Algorithmus, Schlüssel, Länge und Modus an. Für Feldverschlüsselung, Dieses Feld ist schreibgeschützt und hat einen Wert von **Symmetrische Datenverschlüsselung/-Entschlüsselung** .
	Quelle	Zeigt den Wert an, der während ausgewählt wurde **Schlüsselursprung** Abschnitt.
	Algorithmus	Zeigt den Algorithmus an, der zum Erreichen des Krypto-Zwecks verwendet wird.

5. Wählen Sie Aus **Wechseln Sie Zum Krypto-Modul** Um zu Ihrem Moduldatensatz zurückzukehren. Im Moduldatensatz befindet sich jetzt ein Eintrag in **Modulschlüssel** Zugehörige Liste. Die **Schlüsselalias** Feld in **Krypto-Spezifikationen** Die zugehörige Liste ist jetzt leer, da der Schlüsselalias in den neuen Modulschlüssel verschoben wurde.

Nächste Maßnahme

Informationen zur Verwendung eines vom Kunden bereitgestellten Schlüssels finden Sie unter Konfigurieren Sie vom Kunden bereitgestellte Schlüssel für Feldverschlüsselung Enterprise.

Modulschlüssel für Feldverschlüsselung

Auf der Registerkarte „Modulschlüssel“ werden Informationen auf Zusammenfassungsebene zu Ihren Feldverschlüsselungsdaten-Verschlüsselungsschlüsseln angezeigt. Sie können den Schlüsselalias, den Schlüsseltyp, den Algorithmus, den Status des Schlüssellebenszyklus und die Schlüsselversion anzeigen.

Zugriff auf Modulschlüsselinformationen

Greifen Sie über Datensätze in der Tabelle „kryptografisches Modul“ [sys_kmf_crypto_Module] auf Ihre Modulschlüssel zu. In einem kryptografischen Modul-Datensatz können Sie auswählen **Schlüsselalias** Feld in Datensätzen in **Modulschlüssel** Zugehörige Liste.

Die verfügbaren Informationen hängen von der Version von ab Feldverschlüsselung Sie sind in Ihrer Instanz aktiv.

Feldverschlüsselung Starter

Verwenden Feldverschlüsselung Starter, können Sie wichtige Nutzungs-Audit-Daten anzeigen.

Feldverschlüsselung Enterprise

Sie können manuelle Schlüsselvorgänge wie verlängern, Widerrufen, Rotieren oder Anhalten ausführen und gleichzeitig wichtige Nutzungs-Audit-Daten anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulschlüsselinformationen

Informationen zu Ihren Modulschlüsseln werden im Modulschlüsseldatensatz in den hier aufgeführten Feldern angezeigt. Diese Felder sind schreibgeschützt und werden nur zu Informationszwecken verwendet.

Feld	Beschreibung
Generierungsdatum	Wann der Modulschlüssel generiert wurde
Aktivierungsdatum	Wann der Modulschlüssel aktiviert wurde.
Letztes Verlängerungsdatum	Wann der Modulschlüssel zuletzt verlängert wurde.
Letztes Rotationsdatum	Wann der Modulschlüssel zuletzt rotiert wurde.
Deaktivierungsdatum	Wann der Modulschlüssel deaktiviert wurde.
Zerstörungsdatum	Wann der Modulschlüssel zerstört wurde.
Künftiges Aktivierungsdatum	Wann der Modulschlüssel aktiviert wird.
Künftiges Verlängerungsdatum	Wann der Modulschlüssel verlängert wird.
Künftiges Rotationsdatum	Wann der Modulschlüssel rotiert wird.
Künftiges Zerstörungsdatum	Wann der Modulschlüssel gelöscht wird.
Schlüssel-Lebenszyklusstatus	Aktueller Status des Modulschlüssels.

Modullebenszyklus-Richtlinienausnahmen für Feldverschlüsselung

Verwenden Sie Modullebenszyklus-Richtlinienausnahmen, um den Lebenszyklus Ihrer Modulschlüssel anzupassen.

Vorbereitungen

Erforderliche Rolle: KMF-Administrator oder KMF Cryptographic Manager

Warum und wann dieser Vorgang ausgeführt wird

Modullebenszyklus-Richtlinienausnahmen ändern die Lebenszyklusrichtlinie von Feldverschlüsselung Module aus der standardmäßigen Lebenszyklusrichtlinie auf Instanzebene. Wenn Sie beispielsweise symmetrische Schlüssel so konfiguriert haben, dass sie auf Instanzebene auf ein Jahr beschränkt sind, können Sie eine Modullebenszyklus-Richtlinienausnahme für einen bestimmten erstellen Feldverschlüsselung Modul, damit der Schlüssel zwei Jahre lang aktiv bleibt.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Feldverschlüsselungsmodule**an.
2. Wählen Sie den Feldverschlüsselungsmoduldatensatz aus, für den eine Modullebenszyklus-Richtlinienausnahme erforderlich ist.
3. Wählen Sie im Datensatz des Feldverschlüsselungsmoduls die Option aus **Neu** In **Modulrichtlinienausnahmen** Zugehörige Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die Felder im Formular „Schlüssel-Lebenszyklusrichtlinie“ nach Bedarf aus.

Feld	Beschreibung
Krypto-Modul	Zeigt den Namen des Feldverschlüsselungsmoduls an, das diese Richtlinienausnahme verwendet.
Betrifft	Der angegebene Schlüssel wird automatisch ausgefüllt.
Schlüsseltyp	Wählen Sie den Schlüsseltyp aus. Ausnahmerichtlinien beziehen sich auf einen bestimmten Schlüssel. Pro können mehrere Ausnahmerichtlinien erstellt werden Feldverschlüsselung Modul.
Richtlinienbedingung	Erstellen Sie qualifizierende Bedingungen aus dem Dropdown-Menü, und füllen Sie die zusätzlichen Einschränkungskriterien aus.
Ergebnis	Wählen Sie Aus **Ablehnen** Um die Verwendung des Schlüssels oder abzulehnen **Nachverfolgen** Um die Verwendung zu ermöglichen, wenn die Kriterien erfüllt sind.

5. Wählen Sie **Absenden**.

Konfigurieren Sie vom Kunden bereitgestellte Schlüssel für Feldverschlüsselung Enterprise

Bringen Sie Ihren eigenen Datenverschlüsselungsschlüssel auf die Plattform, anstatt den mit zu verwenden ServiceNow Generiert.

Vorbereitungen

Erforderliche Rolle: KMF-Administrator oder KMF Cryptographic Manager

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie verwenden Feldverschlüsselung Enterprise, Sie können Ihren eigenen Datenverschlüsselungsschlüssel für die Plattform verwenden, anstatt einen von generierten Schlüssel zu verwenden ServiceNow.

Sie müssen einen symmetrischen Schlüssel haben, der außerhalb von generiert wurde ServiceNow. Die Beispiele in diesem Dokument basieren auf OpenSSL. Weitere Informationen zu OpenSSL finden Sie unter https://www.openssl.org . Wenn Sie andere kryptografische Tools wie LibreSSL oder GnuTLS verwenden, finden Sie ähnliche Schritte in der Dokumentation zu diesen Produkten.

Prozedur

1. Führen Sie in einer Befehlszeile auf Ihrem Computer (Beispiel: Terminal) den folgenden Befehl aus: `openssl-Rand -hex 32 -out mykey.bin` .
   Speichern Sie `mykey.bin` Datei, die in den folgenden Schritten verwendet wird.
2. Navigieren Sie in Ihrer Instanz zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Einstellungen für Feldverschlüsselung**an.
3. Ändern Sie **Schlüsselquelle** Feld von **Von ServiceNow generierte Schlüssel** Bis **Vom Kunden Bereitgestellte Schlüssel** .
4. Wählen Sie **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Verwenden Sie den symmetrischen Schlüssel, den Sie in Ihrer Instanz erstellt haben, indem Sie die folgenden Schritte ausführen:

1. Konfigurieren Sie Eigenschaften für den vom Kunden bereitgestellten Schlüssel
2. Schließen Sie Ihren vom Kunden bereitgestellten Schlüssel ein
3. Laden Sie Ihren vom Kunden bereitgestellten Schlüssel hoch

Konfigurieren Sie Eigenschaften für den vom Kunden bereitgestellten Schlüssel

Überprüfen Sie die Systemeigenschaften für den flüchtigen öffentlichen Wrapping-Schlüssel, den Ihre Instanz zum Entpacken von vom Kunden bereitgestellten Schlüsseln verwendet.

Vorbereitungen

Erforderliche Rolle: KMF-Administrator oder KMF-kryptografischer Operator

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen Ihren symmetrischen Datenverschlüsselungsschlüssel mit umschließen ServiceNow Flüchtiger öffentlicher Wrapping-Schlüssel, bevor Sie ihn in Ihre Instanz hochladen können.

Wenn Ihr Schlüssel in Ihre Instanz hochgeladen wird, wird er von der Instanz mithilfe der privaten Seite des öffentlichen Schlüssels entpackt.

Sie können Systemeigenschaften in Ihrer Instanz verwenden, um die Schlüsselauffüllung, die Größe des flüchtigen Schlüsselpaars und einen Gültigkeitszeitraum des Schlüssels für diesen flüchtigen öffentlichen Schlüssel zu definieren.

Systemeigens	Beschreibung	Standardwert
Glide.kmf.ephemeral_key_padding	Schlüsselauffüllung für den flüchtigen Schlüssel.	OAEPWithSHA256AndMGF1Padding OAEP SHA256, SHA1 wird jedoch unterstützt.
Glide.kmf.ephemeral_key_size	Schlüsselgröße des flüchtigen Schlüsselpaars.	4096 4096 Bit, aber 2048 Bit werden ebenfalls unterstützt.
Glide.kmf.ephemeral_key_validity_period	Zeitraum, für den das flüchtige Schlüsselpaar gültig ist.	02:00:00 2 Stunden

Prozedur

Kontakt ServiceNow Unterstützen Sie, wenn Sie eine dieser Eigenschaften ändern müssen.

Hinweis: Diese Systemeigenschaften sind für Administratoren nicht sichtbar und werden nicht in der Liste „Systemeigenschaften“ [sys_properties] angezeigt. Verwenden Sie die Tabelle oben, um die Standardwerte anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Sobald Ihre Eigenschaften entsprechend Ihren Anforderungen konfiguriert sind, fahren Sie mit fort Schließen Sie Ihren vom Kunden bereitgestellten Schlüssel ein.

Schließen Sie Ihren vom Kunden bereitgestellten Schlüssel ein

Umschließen Sie Ihren symmetrischen Datenverschlüsselungsschlüssel mit einem flüchtigen öffentlichen Umschließungsschlüssel, bevor Sie ihn in Ihre Instanz hochladen können.

Vorbereitungen

Erforderliche Rolle: KMF-Administrator oder KMF-kryptografischer Operator

Sie müssen einen symmetrischen Datenverschlüsselungsschlüssel in einem haben `.Bin` Um diese Schritte auszuführen. Anweisungen zu diesem Prozess finden Sie unter Konfigurieren Sie vom Kunden bereitgestellte Schlüssel für Feldverschlüsselung Enterprise.

Wichtig: Ihr symmetrischer Datenverschlüsselungsschlüssel muss ein Binärformat (.BIN) aufweisen. Wenn ein anderes Format verwendet wird, wird die folgende Fehlermeldung angezeigt:

Validierung des Tokens fehlgeschlagen. Fügen Sie das unveränderte Token erneut an.

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum Ändern optionaler Eigenschaften, die die Größe, den Auffüllalgorithmus und den Gültigkeitszeitraum des Schlüssels steuern, finden Sie unter Konfigurieren Sie Eigenschaften für den vom Kunden bereitgestellten Schlüssel.

Sie benötigen ein kryptografisches Tool, um Ihren Schlüssel einzuschließen. Das Beispiel in diesem Dokument verwendet OpenSSL 1,1. Weitere Informationen zu OpenSSL finden Sie unter https://www.openssl.org . Wenn Sie andere kryptografische Tools wie LibreSSL oder GnuTLS verwenden, finden Sie ähnliche Schritte in der Dokumentation zu diesen Produkten.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Feldverschlüsselungsmodule**an.
2. Öffnen Sie ein Feldverschlüsselungsmodul, das Sie zuvor erstellt haben.

   Hinweis: Wenn Sie noch kein Feldverschlüsselungsmodul erstellt haben, können Sie eines mit den Schritten in erstellen Konfigurieren Feldverschlüsselung Module.

3. In **Modul** Zugehörige Liste öffnen Sie den kryptografischen spezifischen Datensatz, indem Sie unter den Namen auswählen **Schlüsselalias** .
4. Wählen Sie aus **Als Nächstes** Schaltfläche, bis Sie erreichen **Schlüsselursprung** Abschnitt.
5. Überprüfen Sie, ob **Ursprung** Feld hat einen Wert von **Vom Kunden bereitgestellten Schlüssel hochladen** .
   Wenn dies nicht der Fall ist und Sie diesen Wert nicht auswählen können, lesen Sie die Schritte 3–5 in Konfigurieren Sie vom Kunden bereitgestellte Schlüssel für Feldverschlüsselung Enterprise.
6. In **Schlüsselalias** Feld erstellen Sie einen Alias.
   Ihr Schlüssel verwendet diesen Alias, sobald er hochgeladen wurde.
7. Wählen Sie **Weiter**.
8. Wählen Sie den Link im aus **Umschließenden Schlüssel herunterladen** Feld.

   A `Token_publickey` Dateien werden auf Ihren Computer heruntergeladen. Benennen Sie diese Datei nicht um.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Entpacken und öffnen Sie auf Ihrem lokalen Computer Token_publickey Ordner.
   In diesem Ordner sollten eine Import-Token-Datei (.txt) und eine öffentliche Schlüsseldatei (.PEM) angezeigt werden.
10. Verschieben Sie Ihren von Ihnen generierten symmetrischen Datenverschlüsselungsschlüssel in diesen Ordner.
11. Kopieren Sie den Namen von Token_publickey Datei in Ihre Zwischenablage.
12. Öffnen Sie eine Terminalsitzung, und navigieren Sie zu Token_publickey Ordner.
13. Geben Sie den folgenden Befehl ein:

Wichtig: Ersetzen Sie den Text in Klammern (<>) durch Ihre spezifischen Dateinamen und Informationen. Verwenden Sie die folgende Tabelle mit Beispielen für Schlüsselumwicklungsbefehle als Leitfaden.

```
openssl-pkeyutl -encrypt -pubin -inkey publickey_<keyname>. PEM -in <keyname.bin> -out Wrapped_key_Material -pkeyopt rsa_padding_Mode: oaep -pkeyopt rsa_oaep_md:sha<128 oder 256>
```

Beispiele für Schlüsselumbruch-Befehl

Richtungen	Befehl	Beispiel
Geben Sie „publickey_<keyname>.PEM“ ein	openssl-pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM	openssl pkeyutl -encrypt -pubin -inkey publickey_567898643ffff.PEM
Geben Sie den Namen Ihres symmetrischen Datenverschlüsselungsschlüssels ein	-in <keyname.bin>	-in mykey.bin
Geben Sie den Befehl <-out> ein, um anzugeben, ob das umschlossene Schlüsselmaterial 128-Bit oder 256-Bit sein soll	-Out Wrapped_key_Material -pkeyopt rsa_Padding_Mode:oaep -pkeyopt rsa_oaep_md:sha256	NA

Nächste Maßnahme
Jetzt, da Ihr Schlüssel umgebrochen ist, können Sie ihn mithilfe des Verfahrens in in Ihre Instanz hochladen Laden Sie Ihren vom Kunden bereitgestellten Schlüssel hoch.

Laden Sie Ihren vom Kunden bereitgestellten Schlüssel hoch

Laden Sie Ihren umschlossenen symmetrischen Datenverschlüsselungsschlüssel in Ihre Instanz hoch, um mit der IT-Arbeitsverschlüsselung zu beginnen.

Vorbereitungen
Erforderliche Rolle: KMF-Administrator oder KMF Cryptographic Manager

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Wenn Sie keinen eigenen Schlüssel angeben möchten, können Sie die Schritte in ausführen Konfigurieren Feldverschlüsselung Module Zur Verwendung von ServiceNow. Sie können einen vom Kunden bereitgestellten Schlüssel nicht widerrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Feldverschlüsselungsmodule**an.
2. Öffnen Sie ein Feldverschlüsselungsmodul, in dem Sie Ihren Schlüssel verwenden möchten.
3. In **Modul** Zugehörige Liste öffnen Sie den kryptografischen spezifischen Datensatz, indem Sie unter den Namen auswählen **Schlüsselalias** .
4. Wählen Sie aus **Als Nächstes** Schaltfläche, bis Sie erreichen **Schlüsselursprung** Abschnitt.
5. Überprüfen Sie, ob **Ursprung** Feld hat einen Wert von **Vom Kunden bereitgestellten Schlüssel hochladen** .
   Wenn dies nicht der Fall ist und Sie diesen Wert nicht auswählen können, lesen Sie die Schritte 3–5 in Konfigurieren Sie vom Kunden bereitgestellte Schlüssel für Feldverschlüsselung Enterprise.
6. Bestätigen Sie, dass Sie einen Wert in haben **Schlüsselalias** Feld.
7. Wählen Sie **Weiter**.
8. Wählen Sie aus **Vom Kunden bereitgestellten Schlüssel hochladen** Link.
   Dieser Link sollte unter angezeigt werden **Umschließenden Schlüssel herunterladen** Link, den Sie als Teil des Umschließens Ihres Schlüssels ausgewählt haben.
9. Wählen Sie Aus **Durchsuchen** , Und wählen Sie zwei Dateien aus:
   a. Die Datei Wrapped_key_Material
   b. Die Datei „Importtoken“
10. Wählen Sie **OK**.

Ergebnis

In einer Bestätigungsnachricht wird ein erfolgreicher Upload des vom Kunden bereitgestellten Schlüssels angezeigt. Der Schlüssel ist auch in aufgeführt **Modulschlüssel** Zugehörige Liste mit **Ursprung** Von Vom Kunden bereitgestellter Schlüssel .

Jetzt, da Ihr Verschlüsselungsschlüssel konfiguriert ist, können Sie mit der Angabe beginnen, welche Felder und Anhänge verschlüsselt werden. Details finden Sie unter Konfigurieren Sie verschlüsselte Feldkonfigurationen für Felder oder Anhänge.

Konfigurieren Sie verschlüsselte Feldkonfigurationen für Felder oder Anhänge

Erstellen Sie eine verschlüsselte Feldkonfiguration, um anzugeben, welche Felder in einer Tabelle verschlüsselt werden und ob diese Tabellenanhänge verschlüsselt sind.

Vorbereitungen

Erforderliche Rolle: KMF-Administrator oder KMF Cryptographic Manager, Sicherheitsadministrator

Sie müssen über ein konfiguriertes Feldverschlüsselungsmodul mit verfügen ServiceNow Oder vom Kunden bereitgestellter Schlüssel. Wenn Sie noch kein Modul konfiguriert haben, finden Sie unter Konfigurieren Feldverschlüsselung Module.

Prozedur

1. Stellen Sie sicher, dass Sie sich im selben Anwendungsbereich wie die Tabelle befinden, die Sie verschlüsseln möchten.
2. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Neu**.
4. In **Verschlüsselte Feldkonfiguration** Formular, Felder in den Feldern nach Bedarf.

Feld	Wert
Typ	Wählen Sie entweder aus **Spalte** Oder **Anhang** **Hinweis:** Die Anhangsverschlüsselung ist nur mit verfügbar Feldverschlüsselung Enterprise.
Tabelle	Wählen Sie die Tabelle aus, deren Felder oder Anhänge verschlüsselt sind.
Spalte	Wenn Sie ausgewählt haben **Spalte** In **Typ** Wählen Sie die zu verschlüsselnden Felder aus. **Hinweis:** Wenn das Feld, das Sie verschlüsseln möchten, nicht verfügbar ist, ist es möglicherweise kein unterstützter Typ. Die unterstützten Feldtypen sind: ○ Zeichenfolge (einschließlich vollständiger UTF-8) ○ Datum ○ Datum/Uhrzeit ○ URL ○ HTML ○ Journal ○ Übersetzt ○ E-Mail ○ Telefon
Aktiv	Gibt an, ob die Konfiguration aktiv ist. **Wichtig:** Wenn aktiv, verschlüsselt Ihre Instanz aktiv neue Daten in den ausgewählten Feldern oder Anhängen. Anwender haben keinen Zugriff auf diese Daten, es sei denn, sie haben die Berechtigung über eine zugeordnete Modulzugriffsrichtlinie. Überprüfen Sie nicht, ob das Feld noch nicht bereit ist, mit der Verschlüsselung und Durchsetzung von Modulzugriffsrichtlinien zu beginnen. Um sicherzustellen, dass Verlaufsdaten verschlüsselt werden, nachdem eine verschlüsselte Feldkonfiguration aktiv ist, müssen Sie einen Massenverschlüsselungsauftrag für die Spalte ausführen. Weitere Informationen finden Sie unter „Massenverschlüsselung, Entschlüsselung oder erneute Schlüsselerstellung planen“. .
Krypto-Modul	Das Feldverschlüsselungsmodul, das von dieser verschlüsselten Feldkonfiguration verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Methode	Wählen Sie Aus **Einzelnes Modul** Um sicherzustellen, dass alle Felder oder Anhänge durch ein einzelnes Feldverschlüsselungsmodul verschlüsselt werden. Wählen Sie Aus **Mehrfachmodul** Damit verschiedene Feldverschlüsselungsmodule für verschiedene Zeilen in einer Spalte oder verschiedene Anhänge verwendet werden können. Weitere Informationen zur Konfiguration mit mehreren Modulen finden Sie unter .
Algorithmusgleichstellung Beibehalten	Zeigt an, ob **Gleichstellungserhaltung** Ist im Feld Verschlüsselungsmodul aktiviert, das in ausgewählt ist **Krypto-Modul** Feld.

5. Wählen Sie **Absenden**.

Konfigurieren Sie Konfigurationen für verschlüsselte Felder mit mehreren Modulen

Erstellen Sie eine verschlüsselte Feldkonfiguration, die mehr als ein Verschlüsselungsmodul verwendet.

Vorbereitungen

Erforderliche Rolle: KMF-Administrator oder KMF Cryptographic Manager, Sicherheitsadministrator

Sie müssen über ein konfiguriertes Feldverschlüsselungsmodul mit verfügen ServiceNow Oder vom Kunden bereitgestellter Schlüssel. Wenn Sie noch kein Modul konfiguriert haben, finden Sie unter Konfigurieren Feldverschlüsselung Module.

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie mehrere Verschlüsselungsmodule für eine einzelne verschlüsselte Feldkonfiguration, um verschiedene Zeilen innerhalb einer Spalte (oder verschiedene Anhänge in derselben Tabelle) mit verschiedenen Modulschlüsseln zu verschlüsseln. Beispielsweise können Anwender mit verschiedenen Rollen Daten in derselben Tabelle verschlüsseln, aber trotzdem daran gehindert werden, die verschlüsselten Daten der anderen zu entschlüsseln.

⚠ Warnung:

Beachten Sie diese Einschränkungen für die Konfiguration von verschlüsselten Feldern mit mehreren Modulen, bevor Sie fortfahren:

- Die Massenverschlüsselung wird für Konfigurationen verschlüsselter Felder mit mehreren Modulen nicht unterstützt.
- Sie können eine Feldkonfiguration nicht von einem Mehrfachmodul in ein einzelnes Modul ändern. Stattdessen müssen Sie die Feldkonfiguration für mehrere Module deaktivieren und ein neues einzelnes Modul erstellen.
- Welcher Modulschlüssel eine Feldkonfiguration mit mehreren Modulen verwendet, wird vom ersten Anwender bestimmt, der Daten in ein Feld eingibt. Da das Feldverschlüsselungsmodul für jeden Datensatz festgelegt ist, können Felder in einer Liste durch verschiedene Feldverschlüsselungsmodule verschlüsselt werden. Innerhalb eines einzelnen Datensatzes kann das Feld jedoch nur von einem Feldverschlüsselungsmodul verschlüsselt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Stellen Sie sicher, dass Sie sich im selben Anwendungsbereich wie die Tabelle befinden, die Sie verschlüsseln möchten.
2. Bestätigen Sie, dass die Feldverschlüsselungsmodule erstellt wurden, die Sie verwenden möchten. Wenn Sie dies nicht getan haben, lesen Sie unter Konfigurieren Feldverschlüsselung Module.
3. Bestätigen Sie, dass jedes Ihrer Module über eine Modulzugriffsrichtlinie verfügt. Wenn Sie dies nicht getan haben, lesen Sie unter Konfigurieren Sie Modulzugriffsrichtlinien für die Feldverschlüsselung.
4. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**an.
5. Öffnen von Erstellen Sie einen verschlüsselten Feldkonfigurationsdatensatz.
6. In **Methode** Feld auswählen **Mehrere Module** .
7. Wählen Sie Aus **Spalte** Oder **Anhang** In **Typ** Feld, je nach Bedarf.
8. Wählen Sie eine Tabelle in aus **Tabelle** Feld und Spalte in **Spalte** Feld, falls zutreffend.
9. Wählen Sie **Absenden**.

Ergebnis

Nachdem der Datensatz gespeichert wurde, und **Aktiv** Feld ist aktiviert, neue Daten, die für das angegebene Feld erstellt wurden, werden mit dem Modulschlüssel des entsprechenden Feldverschlüsselungsmoduls verschlüsselt. Wenn ein Anwender mit der Rolle in der Modulzugriffsrichtlinie „A“ in die angegebene Tabelle schreibt, werden die Daten mit dem Modulschlüssel des Feldverschlüsselungsmoduls „A“ verschlüsselt. In diesem Fall können nur Anwender mit derselben Rolle diese Daten entschlüsseln.

Example: Verschlüsseln der Spalte „Kurzbeschreibung“ in der Incident-Tabelle mithilfe einer Konfiguration mit mehreren verschlüsselten Feldern

1. Erstellen Sie zwei Feldverschlüsselungsmodule, die in diesem Beispiel auf A und B verwiesen werden.
2. Erstellen Sie für jedes Feldverschlüsselungsmodul eine Modulzugriffsrichtlinie (Zuordnungen A und B).
   a. Gewähren Sie Anwendern mit einer HR-Rolle für Feldverschlüsselungsmodul A Zugriff auf Modulzugriffsrichtlinie A.
   b. Gewähren Sie Anwendern mit der Rolle „Vertrieb“ für Feldverschlüsselungsmodul B Zugriff auf Modulzugriffsrichtlinie B.
3. Erstellen Sie einen verschlüsselten Feldkonfigurationsdatensatz, der die Spalte Kurzbeschreibung in der Incident-Tabelle angibt, und stellen Sie sicher, dass Sie auswählen **Mehrere Module** In **Methode** Feld.
4. Haben zwei Anwender:
   - Eines mit der HR-Rolle im Zusammenhang mit der ZUORDNUNG A und dem Feldverschlüsselungsmodul A (Anwender A)
   - Eine mit der Vertriebsrolle im Zusammenhang mit ZUORDNUNG B und Feldverschlüsselungsmodul B (Anwender B)

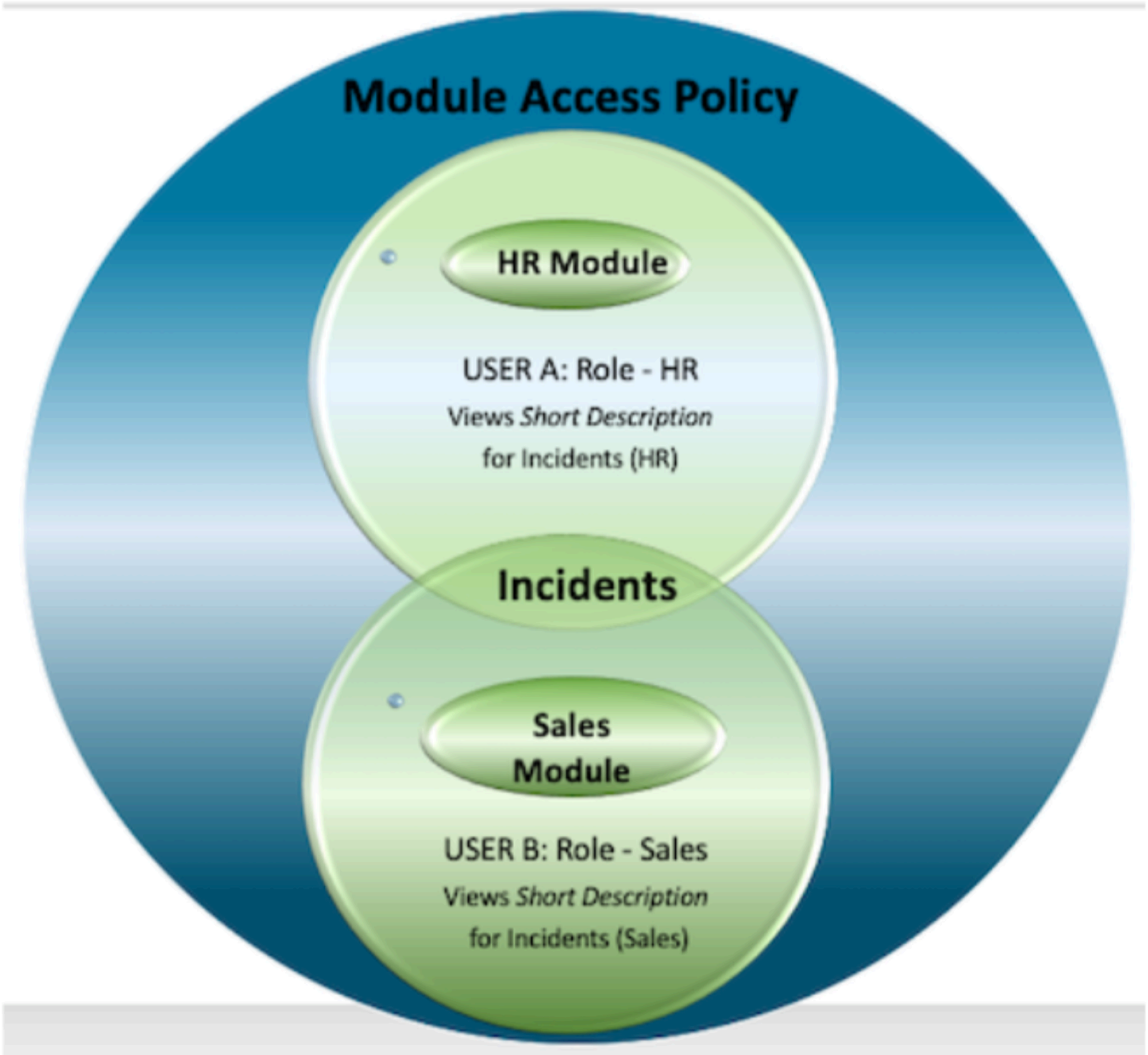
   Erstellen Sie einen Incident-Datensatz mit einem Kurzbeschreibungswert. Lassen Sie beide Anwender die Liste der Incidents anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Die Kurzbeschreibung für den von Anwender A erstellten Incident-Datensatz wird mit dem Schlüssel für Feldverschlüsselungsmodul A verschlüsselt

b. Die Kurzbeschreibung für den von Anwender B erstellten Incident-Datensatz wird mit dem Schlüssel für Feldverschlüsselungsmodul B verschlüsselt

5. Anwender mit den Rollen HR und Vertrieb haben Zugriff auf Incidents. Nur ein Anwender mit der HR-Rolle kann die Kurzbeschreibung für die Incidents entschlüsseln und anzeigen, die von Anwender A erstellt wurden (der die HR-Rolle innehatte). Nur Anwender mit der Rolle „Vertrieb“ können die Kurzbeschreibungen für die Incidents entschlüsseln und anzeigen, die von Anwender B (der die Rolle „Vertrieb“ hat) erstellt wurden.



Konfigurieren Sie Modulzugriffsrichtlinien für die Feldverschlüsselung

Erstellen Sie eine Modulzugriffsrichtlinie, um zu steuern, welche Anwender, Skripts oder Systemprozesse Daten verschlüsseln oder entschlüsseln können, die von einem Feldverschlüsselungsmodul verschlüsselt werden.

Vorbereitungen
Erforderliche Rolle: KMF-Administrator oder KMF Cryptographic Manager, Sicherheitsadministrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie benötigen ein veröffentlichtes Feldverschlüsselungsmodul, um diesen Prozess verwenden zu können. Wenn Sie dies nicht getan haben, lesen Sie unter Konfigurieren Feldverschlüsselung Module.

Warum und wann dieser Vorgang ausgeführt wird

Modulzugriffsrichtlinien (Maps) sind die Zugriffssteuerungen, die Sie auf Ihre Feldverschlüsselungsmodule anwenden, um zu definieren, welche Anwender, Skripts oder Systemprozesse Daten verschlüsseln oder entschlüsseln können. Konfigurieren Sie Zuordnungen für Anwender (über Rollen), Skripts oder Prozesse, die im Systemkontext ausgeführt werden. Ohne eine ZUORDNUNG können Anwender, Skripts oder Systemprozesse Daten nicht verschlüsseln oder entschlüsseln, was dazu führen kann, dass End-to-End-Workflow-Prozesse nicht ordnungsgemäß funktionieren.

Zuordnungen sind von Zugriffssteuerungslisten (ACL) getrennt, können jedoch in Kombination mit ihnen verwendet werden. Siehe Feldverschlüsselung erkunden Um weitere Informationen zum Zweck hinter Karten zu erhalten.

Für Feldverschlüsselung Enterprise, Überprüfung Um zu planen, für welche Anwender, Skripts oder Systemprozesse eine ZUORDNUNG erforderlich ist.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular „Modulzugriffsrichtlinie“ nach Bedarf aus.

Feld	Beschreibung
Richtlinienname	Name Ihrer KARTE
Krypto-Modul	Wählen Sie das Feldverschlüsselungsmodul aus, das von dieser ZUORDNUNG gesteuert werden soll.
Krypto-Spezifikation	Optional. Wählen Sie eine neue kryptografische Spezifikation für diese ZUORDNUNG aus, oder erstellen Sie sie. Dieses Feld wird nur angezeigt, wenn **Geben Sie Den Zweck An** Feld ist aktiviert.
Typ	Entscheiden Sie, wer oder was Zugriff auf diese ZUORDNUNG haben soll, um Daten zu verschlüsseln oder zu entschlüsseln. **Umfang** Alles innerhalb des angegebenen Anwendungsbereichs hat Zugriff auf diese ZUORDNUNG. **Rolle** Nur Anwender mit der bestimmten Rolle können auf diese ZUORDNUNG zugreifen. **Skript** Stellen Sie sicher, dass ein angegebenes Skript auf diese ZUORDNUNG zugreifen kann. **Systemzugriff** Ermöglicht Prozessen, die im „Systemkontext“ ausgeführt werden, den Zugriff auf diese ZUORDNUNG.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Ressourcenaustausch Ermöglicht den Zugriff der Ressourcenaustauschfunktion auf diese ZUORDNUNG. Weitere Informationen dazu, wie diese verschiedenen Arten von KARTEN funktionieren, finden Sie unter Feldverschlüsselung erkunden.
Zielbereich	Wählen Sie einen Bereich aus, für den diese ZUORDNUNG gilt. Dieses Feld wird nur angezeigt, wenn **Typ** Feld ist auf festgelegt **Umfang** .
Geben Sie Den Zweck An	Optional. Aktivieren Sie diese Option, um anzuzeigen **Krypto-Spezifikation** Feld im Formular. Aktivieren Sie diese Option, um granulare Vorgänge zu konfigurieren, z. B. können einige Anwender verschlüsseln, aber nicht entschlüsseln.
Granularer Vorgang	Optional. Wählen Sie den kryptografischen Zweck für die Krypto-Spezifikation aus. Die verfügbaren Werte hängen vom Typ der ausgewählten Krypto-Spezifikation ab. Sie können beispielsweise angeben, dass diese ZUORDNUNG nur Anwendern das Verschlüsseln, aber nicht das Entschlüsseln oder umgekehrt oder beides erlaubt. Dieses Feld wird nur angezeigt, wenn ein Wert in vorhanden ist **Krypto-Spezifikation** Feld. ○ Wenn ein Anwender Zugriff zum Verschlüsseln, aber nicht zum Entschlüsseln hat, wird das Feld im Bearbeitungsmodus angezeigt, und die eingegebenen Daten werden als Sternchen angezeigt. ○ Wenn ein Anwender über Entschlüsselungszugriff verfügt, aber keinen Verschlüsselungszugriff hat, zeigt das Feld die entschlüsselten Daten im schreibgeschützten Modus an. ○ Wenn ein Anwender Zugriff zum Verschlüsseln und Entschlüsseln hat, sind sowohl Lese- als auch Schreibfunktionen für das verschlüsselte Feld verfügbar.
Zielrolle	Wählen Sie aus, welche Rolle Zugriff auf diese ZUORDNUNG haben soll. Dieses Feld wird nur angezeigt, wenn **Typ** Feld ist auf festgelegt **Rolle**
Skripttabelle	Wählen Sie aus, welcher Skripttyp für diese ZUORDNUNG gilt: ○ Zugriffssteuerung ○ Aktivitätsdesigner ○ Business-Regel ○ Aktion Für Eingehende E-Mails ○ Datensatzersteller ○ Geplante Skriptausführung ○ Skripteinbindung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ UI-Aktion ○ Widget ○ Workflow-Aktivität Dieses Feld wird nur angezeigt, wenn **Typ** Feld ist auf festgelegt **Skript** .
Zielskript	Wählen Sie das spezifische Skript der in ausgewählten Typtabelle aus **Skripttabelle** Feld, das Zugriff auf diese ZUORDNUNG haben soll. Dieses Feld wird nur angezeigt, wenn **Typ** Feld ist auf festgelegt **Skript** .
Überprüfen Sie Die Skriptversion	Wenn diese Option ausgewählt ist, überprüft das System die Version des Skripts, das mit der in angegebenen Version ausgeführt wird **Zielskript** Feld. Wenn sich die Versionen unterscheiden, wird der Administrator benachrichtigt. Dieses Feld wird nur angezeigt, wenn **Typ** Feld ist auf festgelegt **Skript** .
Freigabetyp	Wählen Sie entweder aus **Einmal** Oder **Wiederkehrend** : **Einmal** Ermöglicht die einmalige sichere Freigabe des symmetrischen Datenverschlüsselungsschlüssels im zugehörigen Feldverschlüsselungsmodul für die Zielinstanz. **Wiederkehrend** Ermöglicht es, dass der symmetrische Datenverschlüsselungsschlüssel im zugehörigen Feldverschlüsselungsmodul wiederkehrend sicher für die Zielinstanz freigegeben wird. Dieses Feld wird nur angezeigt, wenn **Typ** Feld ist auf festgelegt **Ressourcenaustausch** .
Zielinstanz-Host	Geben Sie die URL für die Zielinstanz ein, an die der symmetrische Datenverschlüsselungsschlüssel im zugehörigen Feldverschlüsselungsmodul gesendet wird. Dieses Feld wird nur angezeigt, wenn **Typ** Feld ist auf festgelegt **Ressourcenaustausch** .
Identitätswechsel	Wenn diese Option aktiviert ist, erhält ein Anwender, der die Identität eines anderen Anwenders übernimmt, alle KARTENBERECHTIGUNGEN von beiden Anwendern. Wenn diese Option deaktiviert ist, verfügt ein Anwender, der die Identität eines anderen Anwenders übernimmt, nur über ZUORDNUNGSBERECHTIGUNGEN, die ihm vor der Identitätswechsel gewährt wurden.
Aktiv	Aktivieren Sie diese Option, um diese ZUORDNUNG zu aktivieren.
Ergebnis	Wählen Sie eine der folgenden Optionen aus: **Titel**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Ermöglicht den Zugriff auf die KARTE und überwacht die Verwendung. **Ablehnen** Lehnt den Zugriff ab, es sei denn, eine andere ZUORDNUNG gewährt Zugriff. **StrictReject** Lehnt den Zugriff unter allen Umständen ab, auch wenn eine andere KARTE Zugriff gewährt.

4. Wählen Sie **Absenden**.

Migrieren zu Feldverschlüsselung Enterprise

Geplante Aufgaben migrieren Ihre Schlüssel und verschlüsselten Daten von Verschlüsselungsunterstützung zu Feldverschlüsselung Enterprise.

Sie können die geplanten Aufgaben überprüfen, indem Sie zu navigieren **Systemsicherheit** > **Strenge Sicherheitseinstellungen** > **Security-Aufträge**:

- **AutoKeyMigration** : Migriert Verschlüsselungskontextschlüssel zu Key Management Framework(KMF) Kryptografische Modulschlüssel.
- **Automatische Datenmigration** : Migriert Daten, die Sie bereits zur Verwendung von verschlüsselt haben KMF Kryptografischer Modulschlüssel.

Sie können ändern, wann diese geplanten Aufgaben ausgeführt werden, und sie jederzeit anhalten oder neu starten.

Überprüfen Sie, ob die verschlüsselten Feldkonfigurationen Ihre neu migrierten Modulschlüssel verwenden, indem Sie zu navigieren **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**an. Suchen Sie nach den folgenden Elementen:

- Die **Methode** Feld ist **Einzelnes Modul** .
- Die **Krypto-Modul** Das Feld wird mit dem Namen des kryptografischen Moduls ausgefüllt, das das System automatisch erstellt. Sie können dieses Modul und die Modulzugriffsrichtlinie überprüfen, die beide aktiv und veröffentlicht sind.

Feldverschlüsselung Enterprise Und Systemklone

Wenn Feldverschlüsselung Enterprise Ist auf Ihrer Instanz installiert, wird im Rahmen des Klonprozesses automatisch ein neuer Verschlüsselungsschlüssel für das Feldverschlüsselungsmodul auf der Zielkloninstanz generiert. Diese Schlüssel werden für alle Module generiert, auf die der Anwender Zugriff hat und für die noch kein Schlüssel vorhanden ist.

Daher können Feldverschlüsselungsmodule in der Zielkloninstanz zwei Modulverschlüsselungsschlüssel vorhanden sein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

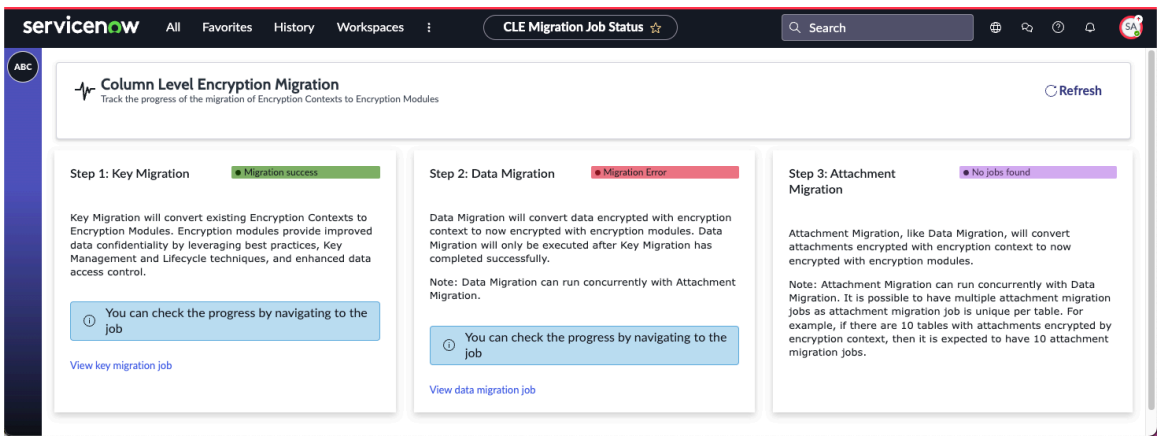
- Ein aktiver Modulverschlüsselungsschlüssel. Dies ist der neue Schlüssel, der nach dem Klonen generiert wird, solange das Modul für den Anwender zugänglich ist und keine vorherigen Schlüssel hat.
- Ein deaktivierter Schlüssel des Verschlüsselungsmoduls (aus der automatisierten Schlüsselaustauschübertragung

  Der aktive Modulverschlüsselungsschlüssel wird verwendet, um eingefügte Daten nach Bedarf in der Zielkloninstanz zu verschlüsseln. Das deaktivierte Modul wird verwendet, um vorhandene Daten zu entschlüsseln, die als Teil des Systemklons geklont wurden.

  Um einen einzelnen Schlüssel zum Entschlüsseln und Verschlüsseln aller Daten zu verwenden, können Sie einen Modul-Neuschlüsselauftrag ausführen. Weitere Informationen zum erneuten Codieren von Modulaufträgen finden Sie unter Planen Sie Massenverschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge .

Feldverschlüsselung Migrationsstatusseite

Verwenden Sie die Migrationsstatusseite, um die Migration von Verschlüsselungskontexten zu Verschlüsselungsmodulen nachzuverfolgen.

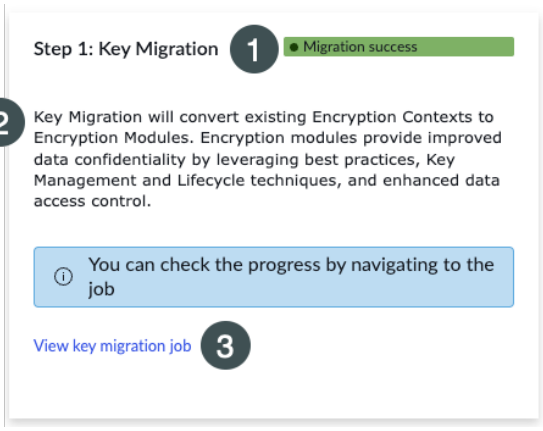


Die Feldverschlüsselung Die Migrationsseite zeigt den Status der Schritte an, die bei der Migration von Verschlüsselungskontexten zu Verschlüsselungsmodulen erforderlich sind. Jeder der drei Abschnitte zeigt den Status eines bestimmten Prozessschritts an.

Seitenabschnittskarten

Die Seite enthält drei Karten, die die Schritte im Migrationsfortschritt darstellen. Diese Karten werden angezeigt:

- (1) der Status des aktuellen Schritts. Dieser Status zeigt an, ob der Schritt erfolgreich abgeschlossen wurde oder ob keine Aufträge zum Verarbeiten vorhanden sind.
- (2) Eine Beschreibung des aufgelisteten Schritts.
- (3) Ein Link zum entsprechenden Verschlüsselungsauftragsdatensatz [sys_Mass_Encryption_Job].



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Migrieren Sie von Edge Encryption zu Feldverschlüsselung

Migrieren Sie von Edge Encryption zu Feldverschlüsselung Um die neuesten Sicherheitsfunktionen zu nutzen.

Migrationsprozess

Dieses Thema umfasst die folgenden Schritte:

1. Migrieren Sie Spalten und Anhänge von Edge Encryption nach Feldverschlüsselung.
2. Beenden und deaktivieren Sie Edge Encryption-Proxy-Server.
3. Detokenisieren Sie Ihre Daten
4. Entschlüsseln Sie Servicekatalog-Elementvariablen.

Einschränkungen

- Feldverschlüsselung Unterstützt derzeit die Tokenisierung von Daten nicht auf dieselbe Weise wie Edge Encryption. Daten, die über Edge Encryption tokenisiert werden, müssen in eine verschlüsselte Feldkonfiguration für aufgenommen werden Feldverschlüsselung.
- Feldverschlüsselung Unterstützt derzeit die Verschlüsselung von Servicekatalog-Elementvariablen nicht.

Konfigurieren Feldverschlüsselung Für Ihre Edge-verschlüsselten Felder

Bevor Sie Ihre vorhandenen Edge-verschlüsselten Felder zu migrieren Feldverschlüsselung, Sie müssen die Feldverschlüsselung für diese Felder konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Dieser Prozess setzt voraus, dass Sie über vorhandene Edge-verschlüsselte Felder verfügen, zu denen Sie migrieren möchten Feldverschlüsselung.

Prozedur

1. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Kryptografische Module** > **Alle** > **an.**
2. Wählen Sie in der Liste kryptografische Module die Option aus **Neu** .
3. Füllen Sie diese Felder im Formular aus.

Feld	Wert
Name	Wählen Sie einen beschreibenden Namen aus
Krypto-Spezifikationsvorlage	Standardvorlage
Lebenszyklusstatus kryptografisches Modul	Veröffentlicht
Übergeordnetes kryptografisches Modul	Column_level_Encryption

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. In **Krypto-Spezifikationen** Zugehörige Liste: Öffnen Sie den Datensatz in der Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. In **Krypto-Spezifikation** Datensatz auswählen **Als Nächstes** Dreimal, um die Abschnitte Algorithmusdefinition, Lebenszyklusdefinition und Schlüsselursprung abzuschließen.
   Sie müssen keine Felder in diesen Abschnitten ändern.
7. In **Schlüssel Generieren** Wählen Sie das Feld aus **Schlüssel Generieren** Link zum Generieren eines Schlüssels.
8. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfiguration**an.
9. Wählen Sie in der Liste der verschlüsselten Feldkonfiguration die Option aus **Neu** .
10. Füllen Sie diese Felder im Formular aus.

Feld	Wert
Typ	Wählen Sie Spalte oder Anhang aus, je nachdem, was Sie verschlüsseln möchten.
Krypto-Modul	Wählen Sie das kryptografische Modul aus, das Sie in früheren Schritten erstellt haben.
Tabelle	Wählen Sie die Tabelle aus, die die Daten enthält, die verschlüsselt werden sollen.
Methode	Wählen Sie Aus `Einzelnes Modul`
Spalte	Wählen Sie die Spalte (Feld) in der Tabelle aus, die verschlüsselt werden soll.

Hinweis: Die zu verschlüsselnden Daten werden durch die Felder Tabelle und Spalte bestimmt. Diese Felder sollten die Tabelle und Spalte (Feld) sein, in der Sie derzeit Edge Encryption verwenden.

11. Wählen Sie **Absenden**.
12. Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**an.
13. Wählen Sie **Neu**.
14. Füllen Sie diese Felder im Formular aus.

Feld	Wert
Richtlinienname	Wählen Sie einen beschreibenden Namen aus
Krypto-Modul	Wählen Sie das kryptografische Modul aus, das Sie in früheren Schritten erstellt haben.
Typ	Wählen Sie Aus `Rolle`
Zielrolle	Wählen Sie eine zu verwendende Rolle aus. Diese Rolle muss Daten in der Spalte verschlüsseln und entschlüsseln können.
Ergebnis	Wählen Sie die gewünschte Aktion aus.

15. Wählen Sie **Absenden**.
16. Um Ihre Konfiguration zu überprüfen, navigieren Sie zu der Tabelle, mit der Sie verschlüsselt werden möchten Feldverschlüsselung, Und öffnen Sie einen Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um beispielsweise auf die Anwendertabelle [sys_user] zuzugreifen, geben Sie ein sys_user.list In den Navigationsfilter.

Das Feld, das Sie in den vorherigen Schritten für die Verschlüsselung ausgewählt haben, hat jetzt ein Schlosssymbol neben der Feldbezeichnung.

Ergebnis
Das Feld „Edge Encrypted“ kann zur Feldverschlüsselung migriert werden. Um weitere Felder zu konfigurieren, wiederholen Sie die vorherigen Schritte für jedes dieser Felder.

Verhindern Sie, dass Anwender unverschlüsselte Dateien anhängen

Ändern Sie die Eigenschaft com.Glide.Encryption.enable_attachment_key_ui, um zu verhindern, dass Ihre Anwender mit Zugriff auf einen Verschlüsselungsmodulschlüssel unverschlüsselte Anhänge anhängen.

Vorbereitungen
Erforderliche Rolle: security_admin

Sie müssen die Rolle „Security_admin“ ausführen, um diese Schritte auszuführen. Anweisungen finden Sie unter Auf eine privilegierte Rolle hochstufen

Standardmäßig können Anwender, die Zugriff auf einen Verschlüsselungsmodulschlüssel haben, unverschlüsselte Anhänge hochladen. Verwenden Sie *com.glide.encryption.enable_attachment_key_ui*Systemeigenschaft zum Ändern dieses Verhaltens.

Beim Anhängen sehen Ihre Anwender eine UI-Auswahl in Datensätzen, die eine verschlüsselte Feldkonfiguration mit mehreren Modulen aufweisen. Wenn diese Eigenschaft auf „falsch“ festgelegt ist, sehen Anwender keine Option mehr, einen Anhang nicht zu verschlüsseln.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen und öffnen Sie in der Liste der Systemeigenschaften die Systemeigenschaft.
3. Legen Sie fest **Wert** Der Eigenschaft bis Falsch .

Feldverschlüsselung verwenden

Verwenden Feldverschlüsselung Dient zum Verwalten des Zugriffs auf verschlüsselte Daten in Ihren Instanzen.

Es gibt zwei Methoden zum Verschlüsseln von Felddaten:

- Einzelnes Modul: Ermöglicht die Datenverschlüsselung mithilfe eines einzelnen Verschlüsselungsmoduls in einer deterministischen Methode.
- Mehrfachmodul: Ermöglicht die Datenverschlüsselung mit mehreren Verschlüsselungsmodulen in einer nicht deterministischen Methode. Zeilenbedingungen sind die neue und bevorzugte Methode zum Anwenden mehrerer Module auf ein Feld. Zeilenbedingungen wenden die Multimodul-Fähigkeit deterministisch an.

Verwenden Sie die zugehörigen Links, um Informationen zu allgemein zu finden Feldverschlüsselung Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellen Sie ein kryptografisches Modul für Feldverschlüsselung

Erstellen Sie eine kryptografische Spezifikation für Feldverschlüsselung

Konfigurieren Sie erweiterte Algorithmen für Feldverschlüsselung Enterprise

Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel

Felder und Anhänge werden verschlüsselt

Feldverschlüsselung Enterprise Beispiele

Erstellen Sie ein kryptografisches Modul für Feldverschlüsselung

Erstellen Sie einen Feldverschlüsselung Kryptografisches Modul zum Definieren der für kryptografische Vorgänge verwendeten Mechanismen.

Vorbereitungen

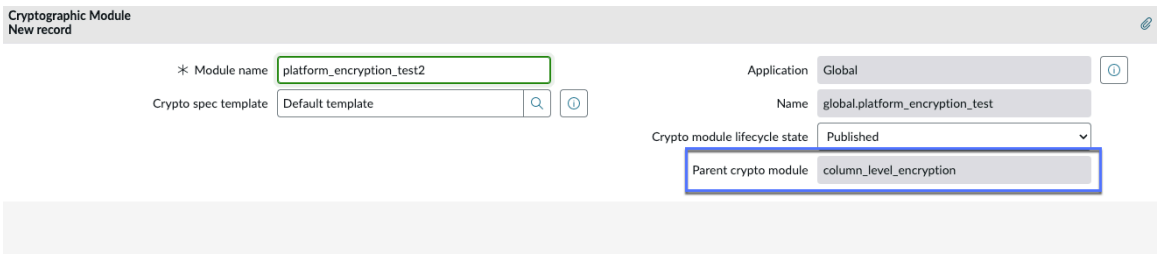
Erforderliche Rolle: sn_kmf.cryptographic_Manager oder sn_kmf_admin, Security_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

In diesem Verfahren werden Optionen beschrieben, die mit verfügbar sind Feldverschlüsselung Mit dem Basissystem und zusätzlichen Konfigurationsoptionen, die mit verfügbar werden Feldverschlüsselung Enterprise Funktionalität. Feldverschlüsselung Enterprise Ist mit einem kostenpflichtigen Abonnement verfügbar. Siehe Abonnementpaket für Verschlüsselung und Schlüsselverwaltung Für unterstützte Funktionen und Optionen, die für jedes Angebot verfügbar sind. Siehe Feldverschlüsselung aktivieren Weitere Informationen zum Abrufen von Feldverschlüsselung Enterprise.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselungsmodule** > **Neu**an.



2. Füllen Sie im Formular die Felder aus.

Formular „kryptografisches Modul“

Feld	Beschreibung
Modulname	Alphanumerische Zeichenfolge, auf die beim Ausführen von Skripts verwiesen werden soll.
Krypto-Spezifikationsvorlage	Standardvorlage, die zum Erstellen des kryptografischen Moduls verwendet wird, das Zuordnungen vieler kryptografischer Zwecke zu Krypto-Spezifikationen und empfohlenen Algorithmen enthält.
Anwendung	Der ausgewählte Anwendungsbereich.
Name	Der Name des Verschlüsselungsmoduls wird dem Namen des Anwendungsbereichs vorangestellt, um Konflikte mit anderen bereichsbezogenen Anwendungen bei der Modulerstellung zu vermeiden. Beispiel: Wenn Sie ein Modul mit dem Namen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	erstellt haben Mein_Krypto_Modul Im globalen Anwendungsbereich wird der Name als gespeichert Global.my_crypto_Module .
Lebenszyklusstatus kryptografisches Modul	Die Bedingung *Lebenszyklus* Bezieht sich auf die Erstellung, Verwendung und Deaktivierung eines kryptografischen Moduls. Auf festlegen **Entwurf** Anfänglich während der Konfiguration. Wenn Sie das Modul verwenden, legen Sie auf fest **Veröffentlicht** . Die Standardvorlage wird automatisch auf festgelegt **Veröffentlicht** .
Übergeordnetes kryptografisches Modul	Das übergeordnete Element wird automatisch als ausgefüllt **Column_level_Encryption** .

3. Klicken Sie auf **Absenden**.

   Nach erfolgreicher Übermittlung wird Ihr kryptografisches Modul in der Tabelle „kryptografische Module“ aufgeführt.

   Warnung:

   Für Anwender mit Legacy-Verschlüsselungsunterstützung:

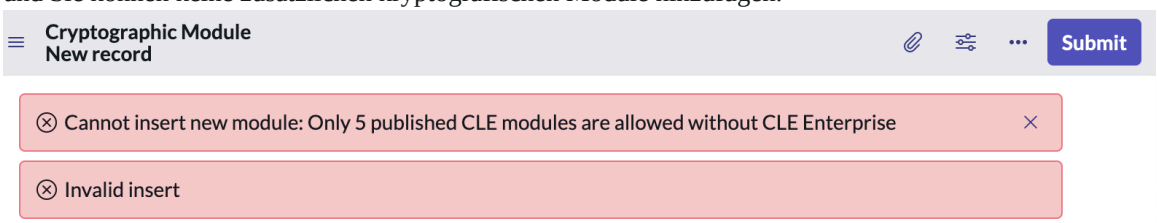
   Wenn Sie die nicht-Enterprise-Version von verwenden Feldverschlüsselung, Sie sind auf fünf beschränkt Felder . Wenn Sie diesen Grenzwert überschritten haben, erhalten Sie die folgende Warnung:

   Diese Einfügung überschreitet die Anzahl der veröffentlichten Felder Grenzwert für Feldverschlüsselung#Berechtigt für das Abonnementprodukt. Das Enterprise-Abonnement für Feldverschlüsselung Ist für zusätzliche erforderlich Felder . Wenden Sie sich an Ihr Account-Team.

   Eine standardmäßige kryptografische Spezifikation wird erstellt, wobei der Krypto-Zweck auf symmetrische Datenverschlüsselung/-Entschlüsselung und der Algorithmus AES 256 CBC festgelegt ist. Wählen Sie den Algorithmus für Updates aus.

4. Klicken Sie zum Öffnen der Konfigurationsoptionen auf das neu erstellte kryptografische Modul.

   Hinweis: Maximal fünf Feldverschlüsselung Felder Sind vor dem Upgrade auf zulässig Feldverschlüsselung Enterprise. Eine Fehlermeldung wird angezeigt, und Sie können keine zusätzlichen kryptografischen Module hinzufügen.



Nächste Maßnahme

Erstellen Sie eine kryptografische Spezifikation für Feldverschlüsselung.

Mehrere Verschlüsselungsmodule verwenden

Mehrere Verschlüsselungsmodule ermöglichen die Verschlüsselung von Daten mit mehr als einem Verschlüsselungsmodul. Wenn jedes Modul beispielsweise eine eigene Zugriffsrichtlinie basierend auf einer Rolle hat, können Anwender mit verschiedenen Rollen Daten in derselben Tabelle verschlüsseln, die jedoch verwendet wird, um zu verhindern, dass sie die verschlüsselten Daten des anderen anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt zwei Möglichkeiten, Daten mit mehreren Verschlüsselungsmodulen in der Plattform zu verschlüsseln:

- Zeilenbedingungen: Ermöglicht Administratoren, das zu verwendende Verschlüsselungskrypto-Modul zu definieren. Diese Option bietet einen deterministischen Ansatz und ermöglicht mehrere Verschlüsselungsfeldkonfigurationen (EFCs) für eine einzelne Spalte. Sie können verschiedene Datensätze für ein Feld oder einen Anhang verschlüsseln, indem Sie eindeutige Verschlüsselungsschlüssel für bestimmte Felder konfigurieren. Dies wird durch die Zuweisung mehrerer Verschlüsselungsfeldkonfigurationen (Encryption Field Configurations, EFCs) erreicht. Zeilenbedingungen sind die bevorzugte Methode zum Verschlüsseln von Daten mit mehreren Modulen. Weitere Informationen finden Sie unter Daten mithilfe von Zeilenbedingungen verschlüsseln.
- Mehrere Module: Ermöglicht Anwendern, das Krypto-Modul zum Verschlüsseln von Daten zu verwenden. Da mehrere Module davon abhängen, dass der Anwender das richtige Krypto-Modul zum Verschlüsseln der Daten auswählt, ist diese Konfiguration nicht deterministisch und gilt als Legacy und nicht bevorzugt, auch wenn die Funktion derzeit noch verfügbar ist. Weitere Informationen finden Sie unter Verschlüsseln Sie Daten mit der Funktion „mehrere Module“.

Daten mithilfe von Zeilenbedingungen verschlüsseln

Verschlüsseln Sie Felder mit mehreren Feldverschlüsselungsmodulen mithilfe von Zeilenbedingungen, um die zu verschlüsselnden Daten und die zugehörigen Verschlüsselungsschlüssel zu definieren. Zeilenbedingungen können auch verwendet werden, um die Anwender zu definieren, die über den Bedingungsgenerator Zugriff haben.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager oder sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Bei der Verwendung von Zeilenbedingungen gelten die folgenden Richtlinien:

- Zeilenbedingungen werden nur für verschlüsselte Spalten und Anhänge unterstützt.
- Massenverschlüsselung ist bei Verwendung der Methode „mehrere Verschlüsselungsmodule“ nicht verfügbar.
- Sie können ein Feld mit mehreren Verschlüsselungsmodulen nicht ändern, um ein einzelnes Verschlüsselungsmodul zu verwenden.
- Zeilenbedingungen ermöglichen die Verschlüsselung von Daten im Hauptdatensatz. Dot-Walking wird im Bedingungsgenerator nicht unterstützt.
- Zeilenbedingungen werden von den folgenden Servicekatalog-Tabellen nicht unterstützt:
  - Optionen [sc_item_Option]
  - Antwort auf Frage [question_answer]
  - Antwort auf mehrzeilige Frage [sc_Multi_row_question_answer]

Das Feld wird vom Verschlüsselungsmodul des ersten Anwenders verschlüsselt, der Daten eingegeben hat. Da das Verschlüsselungsmodul pro Datensatz festgelegt ist, können Felder in einer Liste verschiedene Verschlüsselungsmodule haben. Innerhalb eines einzelnen Datensatzes kann das Feld von nur einem Modul verschlüsselt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie mehrere kryptografische Module und eine Zugriffsrichtlinie für jedes Modul.

   Stellen Sie sicher, dass Sie den verschiedenen kryptografischen Modulen über die Zugriffsrichtlinien verschiedene Rollen gewähren.

2. Navigieren zu **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen** > **Neu**an.

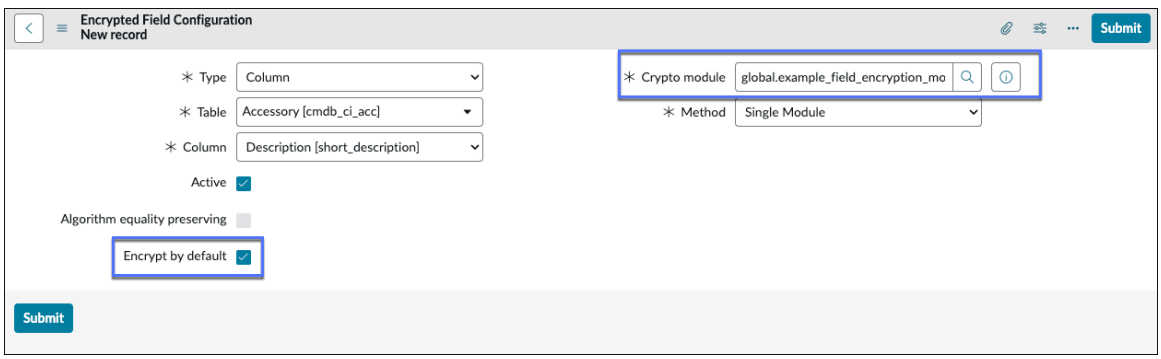
   Weitere Informationen zu verschlüsselten Feldkonfigurationen finden Sie unter Legen Sie verschlüsselte Feldkonfigurationen fest.

3. Wählen Sie aus **Tabelle** Und **Spalte** In der Tabelle, die Sie verschlüsseln möchten.
4. Wählen Sie Aus **Standardmäßig verschlüsseln** Zum Verschlüsseln gespeicherter Datensätze, die keine definierte Zeilenbedingung erfüllen.

   Wenn Sie diese Option auswählen, stellen Sie sicher, dass Sie auswählen **Krypto-Modul** Zur Verwendung als standardmäßiges Verschlüsselungsmodul.

   Wenn dieses Kontrollkästchen nicht aktiviert ist und hinzugefügte Datensätze keine Zeilenbedingung erfüllen, werden sie nicht verschlüsselt.

   Beispielsweise kann eine Zeilenbedingung definiert werden, um Datensätze zu verschlüsseln, um zu erklären, dass das Feld „Abteilung“ im Datensatz gleich „IT“ ist. Dann werden die Datensätze, in denen das Feld „Abteilung“ nicht gleich „IT“ ist, nur verschlüsselt **Standardmäßig verschlüsseln** Ist ausgewählt.



5. Wählen Sie **Absenden**.
6. Navigieren Sie zum Bedingungsgenerator **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen** Und wählen Sie die neue verschlüsselte Feldkonfiguration (EFC) aus.
7. Wählen Sie **Neu**.
8. Definieren Sie Zeilenbedingungen, indem Sie die erforderlichen Felder ausfüllen.
9. Wählen Sie **Absenden**.

Ergebnis

Hinweis: Wiederholen Sie diesen Vorgang nach Bedarf, um sicherzustellen, dass die Anzahl der Zeilenbedingungen Ihre erforderlichen Encryption Crypto Modules (ECMs) erfüllt. Wenn im ECM-Setup standardmäßig verschlüsselt ausgewählt wird, muss auch eine Zeilenbedingung eingerichtet werden, um das ausgewählte Standard-ECM zu definieren.

Neu erstellte Daten für das angegebene Feld werden mit dem Schlüssel für das relevante Modul verschlüsselt. Wenn ein Anwender mit der in der Zugriffsrichtlinie von Modul A

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angegebenen Rolle in die angegebene Tabelle schreibt, werden die Daten mit dem Schlüssel von Modul A verschlüsselt. Nur Anwender mit derselben Rolle können die Daten lesen.

Example:
In diesem Beispiel wird erläutert, wie das Feld Kurzbeschreibung in der Incident-Tabelle verschlüsselt wird. Dieses Beispiel funktioniert ähnlich, wenn Sie ein anderes Feld in einer Tabelle verschlüsseln möchten.
Zum Verschlüsseln der Kurzbeschreibung gehen Sie wie folgt vor:

1. Erstellen Sie zwei Feldverschlüsselungsmodule A und B.
2. Erstellen Sie für jedes Modul eine Modulzugriffsrichtlinie (MAP), und definieren Sie den Zugriff wie folgt:
   a. Modul A: Für Anwender mit einer HR-Rolle.
   b. Modul B: Für Anwender mit einer Vertriebsrolle.
3. Erstellen Sie einen EFC-Datensatz (Encrypted Field Configuration).
   a. Navigieren zu **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen** > **Neu**an.
   b. Wählen Sie Aus **Incident** Im Feld Tabelle.
   c. Wählen Sie Aus **Kurzbeschreibung** Im Feld Spalte.
   d. Wählen Sie aus **Standardmäßig verschlüsseln** Box, wenn Sie sicherstellen müssen, dass alle Datensätze, die außerhalb der Bedingungsgeneratorkriterien liegen, weiterhin durch das standardmäßige Feldverschlüsselungsmodul verschlüsselt werden.
   Wenn Sie diese Option nicht auswählen, werden alle Datensätze, die außerhalb der Bedingungsgeneratorkriterien liegen, nicht verschlüsselt.

      Geben Sie das Standard-Krypto-Modul in zugehörige ein **Krypto-Modul** Feld.

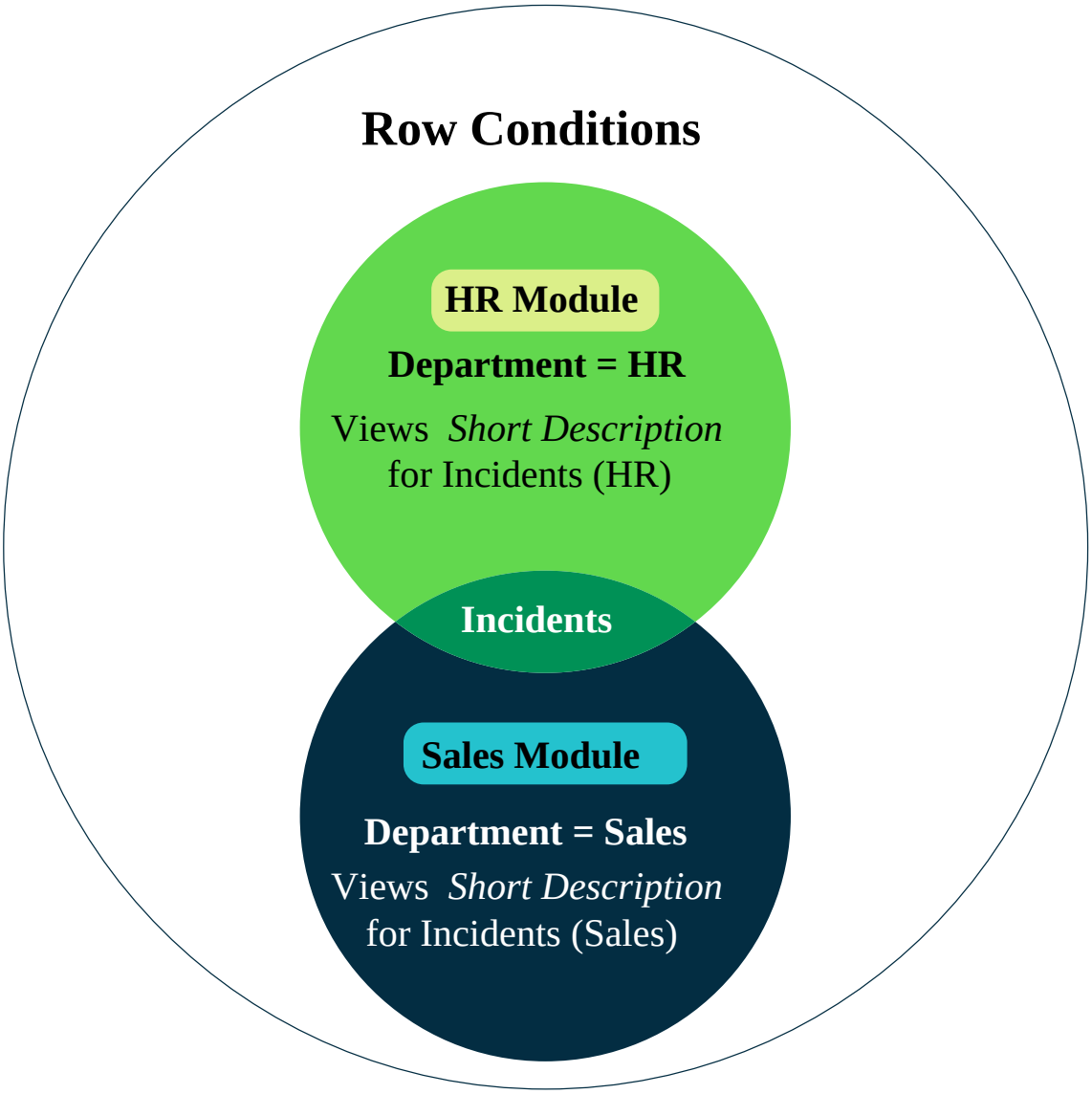
   e. Wählen Sie **Absenden**.
4. Erstellen Sie die Zeilenbedingungen.
5. Führen Sie den entsprechenden Verschlüsselungsauftrag aus:
   - Massenverschlüsselung: Führen Sie diesen Auftrag aus, wenn eine neue Zeilenbedingung erstellt wird.
   - Massenwiedergabe: Führen Sie diesen Auftrag aus, wenn eine vorhandene Zeilenbedingung geändert wird.

   Weitere Informationen finden Sie unter Planen Sie Massenverschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge.
6. Lassen Sie einen Anwender aus Modul A und einen Anwender aus Modul B einen Incident mit einer Kurzbeschreibung erstellen. Lassen Sie beide Anwender die Liste der Incidents anzeigen.

Die Kurzbeschreibung für den Incident, der vom Anwender mit der HR-Rolle erstellt wurde, wird durch den Schlüssel für Modul A verschlüsselt. Die Kurzbeschreibung für den Incident, der vom Anwender mit der Vertriebsrolle erstellt wurde, wird durch den Schlüssel für Modul B verschlüsselt

Alle Anwender mit den Rollen HR und Vertrieb haben Zugriff auf Incidents. Jedoch kann nur ein Anwender mit der HR-Rolle die Kurzbeschreibung für Incidents entschlüsseln und anzeigen, die von einem anderen Anwender mit der HR-Rolle erstellt wurden. Ebenso können nur Anwender mit der Rolle „Vertrieb“ die Kurzbeschreibungen für die Incidents entschlüsseln und anzeigen, die vom Anwender B erstellt wurden, der die Rolle „Vertrieb“ innehatte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nächste Maßnahme
Führen Sie einen der folgenden Vorgänge aus:

- Planen Sie einen **Massenverschlüsselung** Auftrag zum Aktualisieren der Verschlüsselung des Bedingungsfelds.
- Wenn Sie eine vorhandene Zeilenbedingung ändern, führen Sie eine aus **Massenwiedergabe** Auftrag zum Verschlüsseln der erforderlichen Daten mit dem aktualisierten Verschlüsselungsmodul.

Siehe Planen Sie Massenverschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge

Verschlüsseln Sie Daten mit der Funktion „mehrere Module“

Verschlüsseln Sie Daten mit mehr als einem Verschlüsselungsmodul, sodass der Anwender bestimmen kann, welche Schlüssel für bestimmte Zeilen in den verschlüsselten Daten verwendet werden.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_Manager oder sn_kmf.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die Option „mehrere Module“ wird als nicht deterministisch betrachtet und ist nicht die bevorzugte Methode, da der Anwender bestimmt, welcher Schlüssel für einen bestimmten Datensatz verwendet werden soll. Die Möglichkeit, mehrere Module für eine Spalte zu verwenden, wird durch Zeilenbedingungen ersetzt. Weitere Informationen finden Sie unter Mehrere Verschlüsselungsmodule verwenden. Diese nicht deterministische Implementierung wird weiterhin unterstützt, da sie zuerst erstellt wurde und noch verwendet wird. Es wird jedoch bevorzugt, Zeilenbedingungen für neue Anwendungsfälle mit mehreren Modulen zu verwenden.

Hinweis: Nur die Verschlüsselung in Spalten unterstützt mehrere Module. Anhangsverschlüsselung nicht Massenverschlüsselung ist bei Verwendung der Methode „mehrere Verschlüsselungsmodule“ nicht verfügbar.

Sie können ein Feld mit mehreren Verschlüsselungsmodulen nicht ändern, um ein einzelnes Verschlüsselungsmodul zu verwenden.

Das Feld wird vom Verschlüsselungsmodul des ersten Anwenders verschlüsselt, der Daten eingegeben hat. Da das Verschlüsselungsmodul pro Datensatz festgelegt ist, können Felder in einer Liste verschiedene Verschlüsselungsmodule haben. Innerhalb eines einzelnen Datensatzes kann das Feld von nur einem Modul verschlüsselt werden.

Prozedur

1. Erstellen Sie mehrere Feldverschlüsselungsmodule und eine Modulzugriffsrichtlinie (MAP) für jedes Modul.

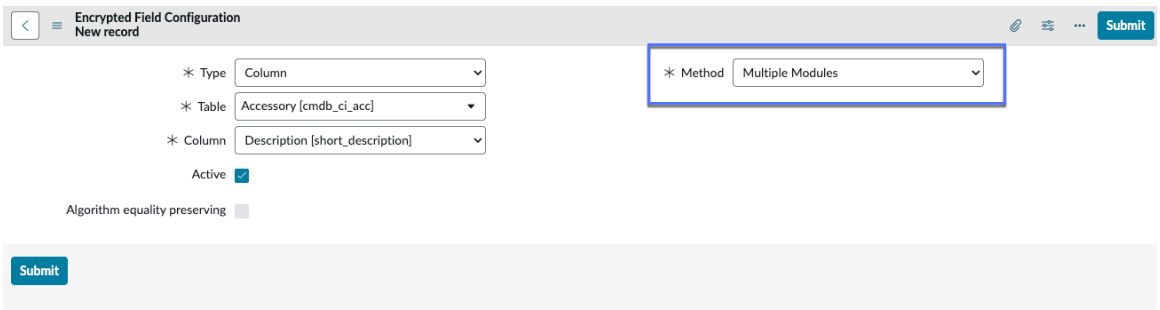
   Stellen Sie sicher, dass Sie den verschiedenen kryptografischen Modulen über die Zugriffsrichtlinien verschiedene Rollen gewähren.

2. Navigieren zu **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen** > **Neu**an.

   Weitere Informationen zu verschlüsselten Feldkonfigurationen finden Sie unter Legen Sie verschlüsselte Feldkonfigurationen fest.

3. In **Typ** Feld, müssen Sie auswählen **Spalte** .
   Die Anhangsverschlüsselung unterstützt nicht mehrere Module.

4. Wählen Sie Aus **Mehrere Module** In **Methode** Feld.



5. Wählen Sie aus **Tabelle** Und **Spalte** In der Tabelle, die Sie verschlüsseln möchten.

6. Wählen Sie **Absenden**.

Ergebnis

Neu erstellte Daten für das angegebene Feld werden mit dem Schlüssel des entsprechenden Moduls verschlüsselt. Wenn ein Anwender mit der in der Zugriffsrichtlinie von Modul A angegebenen Rolle in die angegebene Tabelle schreibt, werden die Daten mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dem Schlüssel von Modul A verschlüsselt. Nur Anwender mit derselben Rolle können die Daten lesen.

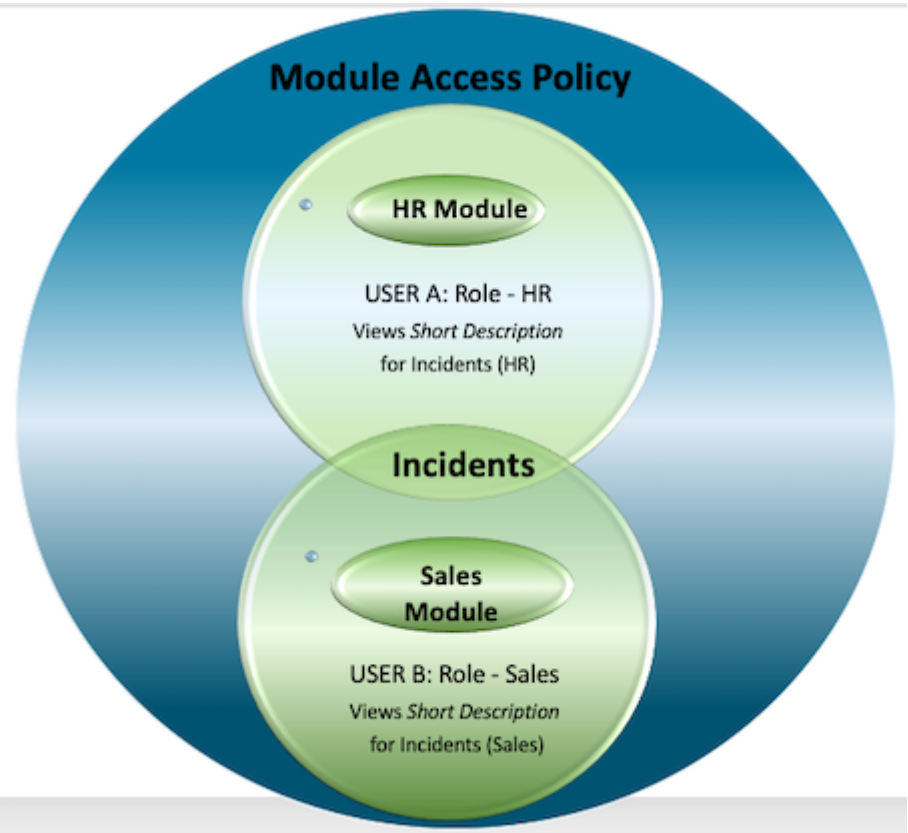
Example:
Zum Verschlüsseln der Spalte Kurzbeschreibung in der Incident-Tabelle. Sie würden Folgendes tun:

1. Erstellen Sie zwei kryptografische Module A und B.
2. Erstellen Sie für jedes Modul eine Modulzugriffsrichtlinie.

   Gewähren Sie Benutzern mit einer HR-Rolle für Modul A Zugriff. Gewähren Sie Benutzern mit der Rolle „Vertrieb“ für Modul B Zugriff.
3. Erstellen Sie einen verschlüsselten Feldkonfigurationsdatensatz, der die Spalte Kurzbeschreibung in der Incident-Tabelle angibt, und stellen Sie sicher, dass Sie auswählen **Mehrere Module** In **Methode** Feld.
4. Haben Sie zwei Anwender, einen mit der HR-Rolle (Anwender A) und einen mit der Vertriebsrolle (Anwender B), erstellen Sie einen Incident mit einer Kurzbeschreibung, und lassen Sie beide Anwender dann die Liste der Incidents anzeigen.

   Die Kurzbeschreibung für den Incident, der vom Anwender mit der HR-Rolle erstellt wurde, wird durch den Schlüssel für Modul A verschlüsselt. Ebenso wird die Kurzbeschreibung für den Incident, der vom Anwender mit der Vertriebsrolle erstellt wurde, durch den Schlüssel für Modul B verschlüsselt

   Obwohl alle Anwender mit den Rollen HR und Vertrieb Zugriff auf Incidents haben, kann nur ein Anwender mit der HR-Rolle die Kurzbeschreibung für die Incidents entschlüsseln und anzeigen, die von Anwender A erstellt wurden, der die HR-Rolle innehatte. Ebenso können nur Anwender mit der Rolle „Vertrieb“ die Kurzbeschreibungen für die Incidents entschlüsseln und anzeigen, die vom Anwender B erstellt wurden, der die Rolle „Vertrieb“ innehatte.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine kryptografische Spezifikation für Feldverschlüsselung

Nachdem Sie ein kryptografisches Modul erstellt haben, greifen Sie auf die entsprechende kryptografische Spezifikation zu, um den Algorithmus zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager oder sn_kmf_admin und Security_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

In diesem Verfahren werden Optionen beschrieben, die mit verfügbar sind Feldverschlüsselung Mit dem Basissystem und zusätzlichen Konfigurationsoptionen, die mit verfügbar werden Feldverschlüsselung Enterprise Funktionalität. Feldverschlüsselung Enterprise Die Funktionalität ist mit einem kostenpflichtigen Abonnement verfügbar. Siehe Abonnementpaket für Verschlüsselung und Schlüsselverwaltung Für unterstützte Funktionen und Optionen, die für jedes Angebot verfügbar sind. Siehe Feldverschlüsselung aktivieren Weitere Informationen zum Abrufen von Feldverschlüsselung Enterprise.

Eine kryptografische Spezifikation wird vom System erstellt, wenn Sie ein kryptografisches Modul für erstellen Feldverschlüsselung Enterprise.

Prozedur

1. Navigieren zu **Systemsicherheit** > **Feldverschlüsselungsmodule** > **Alle**an.
2. Wählen Sie das kryptografische Modul aus, um die Konfigurationsoptionen zu öffnen.
   Informationen zum kryptografischen Modul werden oben auf dem Bildschirm angezeigt. Eine symmetrische Krypto-Spezifikation für Datenverschlüsselung/-Entschlüsselung wird automatisch mit einem AES 256 CBC-Algorithmus erstellt.
3. Wählen Sie die Krypto-Spezifikation aus der Tabelle aus, um die Algorithmusdefinition zu öffnen.
   Für Feldverschlüsselung Enterprise Siehe Konfigurieren Sie erweiterte Algorithmen für Feldverschlüsselung Enterprise.
4. Klicken Sie Auf **Als Nächstes** Um auf den Schlüssellebenszyklus zuzugreifen.

Nächste Maßnahme

Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus“ aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Siehe Konfigurieren Sie Schlüssel-lebenszyklusstatus Für Details zum Vervollständigen der Lebenszyklusdefinition für den Schlüssel.
- Klicken Sie Auf **Als Nächstes** Dient zum Erstellen eines kryptografischen Schlüssels. Details zu diesem Vorgang finden Sie unter Generieren Sie einen kryptografischen ServiceNow-Schlüssel.

Konfigurieren Sie erweiterte Algorithmen für Feldverschlüsselung Enterprise

Erstellen Sie eine kryptografische Spezifikation, um den Algorithmus für ein kryptografisches Modul zu definieren. Passen Sie die Verschlüsselungsspezifikationen mit erweiterten Optionen an, die für verfügbar sind Feldverschlüsselung Enterprise.

Vorbereitungen

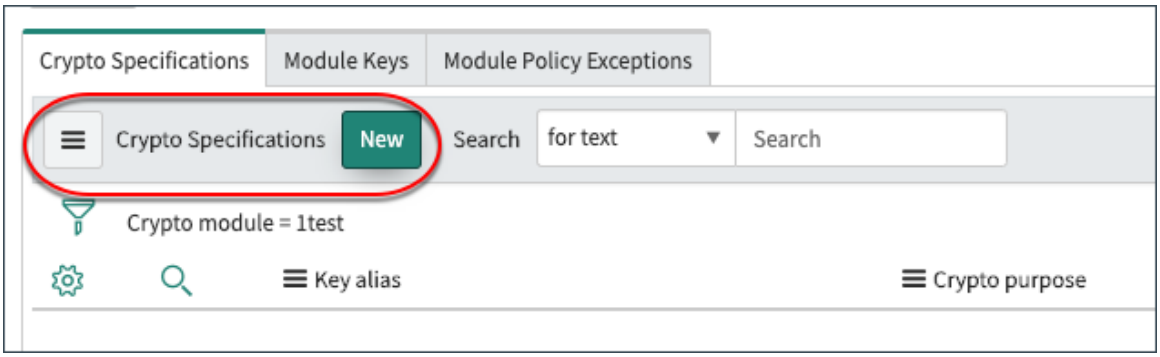
Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Auf der **Krypto-Spezifikationen (#)** Klicken Sie auf die Registerkarte **Neu** .



2. Füllen Sie im Formular die Felder aus.

Formular „Algorithmusdefinition“

Feld	Beschreibung
Krypto-Modul	Name des ausgewählten kryptografischen Moduls wird ausgefüllt.
Kryptografischer Zweck	Der Wert ist **Symmetrische Datenverschlüsselung/-Entschlüsselung** Für Feldverschlüsselung Enterprise.
Algorithmus	Der Wert ist **AES** Für Feldverschlüsselung Enterprise.
Betriebsmodus	Der Wert ist **CBC** Für Feldverschlüsselung Enterprise.
Größe	Mögliche Werte sind **256** Und **128** . **Hinweis:** Die 256-Bit-Größe ist für die Verschlüsselung am besten geeignet und wird für die symmetrische Datenverschlüsselung/-Entschlüsselung für verwendet Feldverschlüsselung Enterprise.
Gleichstellungserhaltung	Option zum Aktivieren der deterministischen Verschlüsselung. **Hinweis:** Wenn Sie diese Option auswählen, muss der verschlüsselte Wert eines Felds gleich sein, wenn der Feldwert gleich bleibt. Option zum Aktivieren **Symmetrische Datenverschlüsselung/-**

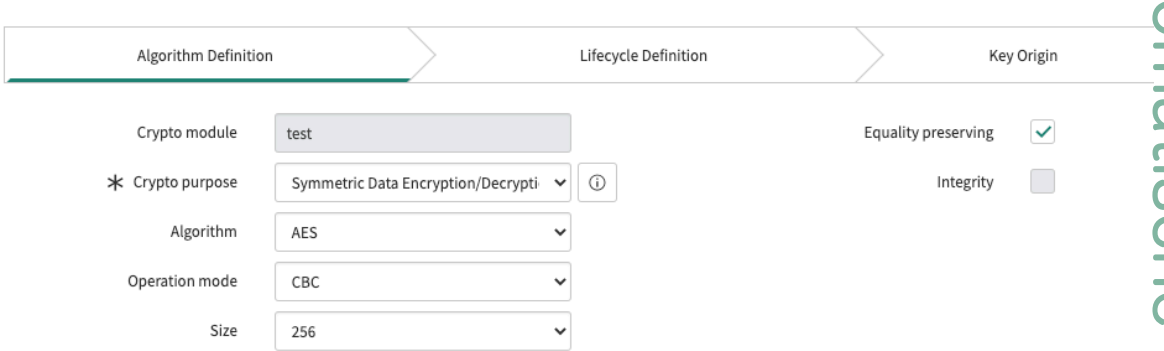
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Entschlüsselung Mit **AES** In **Verschlüsselungsblockverketten (CBC)** Modus.
Integrität	Option zum Bereitstellen von Integrität im GCM-Vorgang und gilt nicht für Feldverschlüsselung Enterprise Funktionalität.

3. Klicken Sie auf **Absenden**.

Das folgende Beispiel zeigt die AES CBC-256-Verschlüsselung. Wenn Feldverschlüsselung Enterprise Ist aktiv und das übergeordnete Modul ist column_level_Encryption. Als Krypto-Zweck gilt nur die symmetrische Datenverschlüsselung/Entschlüsselung AES CBC-256. Details siehe Übersicht über kryptografische Spezifikationen.



Nächste Maßnahme
Führen Sie einen der folgenden Vorgänge aus:

- Wählen Sie einen Eintrag in der Tabelle „Schlüssellebenszyklus“ aus, um das Verhalten des Schlüssellebenszyklus zu definieren. Siehe Konfigurieren Sie Schlüssel-lebenszyklusstatus Für Details zum Vervollständigen der Lebenszyklusdefinition für den Schlüssel.
- Wählen Sie Aus **Als Nächstes** Dient zum Erstellen eines kryptografischen Schlüssels. Sehen Sie sich eine der folgenden Aufgaben für die Schlüsselgenerierung an:
  - Generieren Sie einen kryptografischen ServiceNow-Schlüssel.
  - Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
  - Importieren Sie das Schlüsselpaar zum Umwickeln/Entpacken.

Mit vom Kunden bereitgestellte Schlüssel werden verwendet Feldverschlüsselung Enterprise

Sie können Ihren eigenen vom Kunden bereitgestellten Schlüssel anstelle von verwenden ServiceNow® Vom System generierte Schlüssel.

Wichtig: Diese Themen wenden nur Instanzen mit an Feldverschlüsselung Enterprise, Die nur mit verfügbar ist `com.glide.now.platform.encryption` Plugin. Siehe Feldverschlüsselung aktivieren Weitere Informationen zum Abrufen dieses Plugins.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Feldverschlüsselung Enterprise Sie können Ihre eigenen Schlüssel für die Verschlüsselung verwenden. Administratoren können verwenden ServiceNow® Bereitgestellte Schlüssel oder eigene vom Kunden bereitgestellte Schlüssel (CSK) für die Verschlüsselung auf dem ServiceNow AI Platform.

Wichtig: Um die vom Kunden bereitgestellte Schlüsseloption verwenden zu können, benötigen Sie einen eigenen kryptografischen Schlüssel.

Sobald Sie Ihren Schlüssel haben, können Sie ihn in Ihren Instanzen verwenden, indem Sie diese Schritte ausführen.

1. **Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel**

   Es gibt drei Systemeigenschaften, die die Größe, den Auffüllalgorithmus und den Gültigkeitszeitraum des umschließenden RSA-Schlüsselpaars definieren. Überprüfen Sie diese Eigenschaften, und passen Sie ihre Werte an, wenn die standardmäßig nicht Ihren Anforderungen entspricht.

2. **Schließen Sie Ihren vom Kunden bereitgestellten Schlüssel ein**

   Verwenden Sie ein kryptografisches Tool, um Ihren Schlüssel wie OpenSSL zu umschließen, um den symmetrischen Schlüssel für die Verschlüsselung mit dem heruntergeladenen öffentlichen Schlüssel zu umschließen.

Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch

Laden Sie den umschlossenen Schlüssel Ihres Kunden hoch, und konfigurieren Sie das kryptografische Modul, um Ihren Schlüssel für die Verschlüsselung in Ihrer Instanz zu verwenden.

Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel

Wenn Feldverschlüsselung Enterprise Das Plugin ist aktiviert. Sie können Systemeigenschaften verwenden, um die Schlüsselauffüllung, die Größe des flüchtigen Schlüsselpaars und einen Gültigkeitszeitraum des Schlüssels Ihrer vom Kunden bereitgestellten Schlüssel zu definieren.

Feldverschlüsselung Enterprise Mit der Schlüsselverwaltung können Sie den gesamten Schlüssellebenszyklus Ihrer Datenverschlüsselungsschlüssel verwalten. Optional können Sie in Ihrer Umgebung generierte Datenverschlüsselungsschlüssel sicher austauschen.

Mit der Plattformverschlüsselung mit Schlüsselverwaltung können Sie den gesamten Schlüssellebenszyklus Ihrer Datenverschlüsselungsschlüssel verwalten. Optional können Sie in Ihrer Umgebung generierte Datenverschlüsselungsschlüssel sicher austauschen.

Systemeigenschaften zum Definieren von Schlüsselpaarattributen

Wenn Sie einen eigenen Schlüssel angeben, müssen Sie ihn mit dem öffentlichen RSA-Schlüssel umschließen. Drei Eigenschaften definieren die Größe, den Auffüllungsalgorithmus und den Gültigkeitszeitraum des umschließenden RSA-Schlüsselpaars:

- `glide.kmf.ephemeral_key.key_padding` Steuert das Schlüsselauffüllschema für den flüchtigen Schlüssel. Das Standardschema ist OAEP SHA256, SHA1 wird jedoch auch unterstützt.
- `glide.kmf.ephemeral_key.key_size` Steuert die Schlüsselgröße des flüchtigen Schlüsselpaars. Der Standardwert ist 4096 Bit, aber 2048 Bit werden ebenfalls unterstützt.
- `glide.kmf.ephemeral_key.key_validity_period` Definiert den Zeitraum, für den das flüchtige Schlüsselpaar gültig ist. Der Standardwert ist zwei Stunden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem der Datenverschlüsselungsschlüssel in die Instanz importiert wurde, schützt ein sicherer Wrapping-Schlüssel neue Modulschlüssel in der Instanz. Der umschließende Schlüssel ist ein Instanzschlüssel-Verschlüsselungsschlüssel (IKEK), der von einem Hardware-Sicherheitsmodul (HSM) auf SafeNet KeySecure generiert wird. Siehe Schlüssel auf Instanzebene im Key Management Framework Für Details in Schlüsseltypen.

Fahren Sie mit fort Schließen Sie Ihren vom Kunden bereitgestellten Schlüssel ein.

Schließen Sie Ihren vom Kunden bereitgestellten Schlüssel ein

Umbrechen Sie den symmetrischen Schlüssel, der für die Verschlüsselung verwendet werden soll, mit dem heruntergeladenen öffentlichen Schlüssel.

Vorbereitungen

Hinweis: In diesem Verfahren werden Optionen beschrieben, die mit verfügbar sind KMF Basissystem und Optionen, mit denen verwendet werden soll Feldverschlüsselung Enterprise Funktionalität. Feldverschlüsselung Enterprise Funktionalität ist nur verfügbar, wenn `com.glide.now.platform.encryption` Plugin ist aktiv. Siehe Feldverschlüsselung aktivieren Weitere Informationen zum Abrufen von Feldverschlüsselung Enterprise.

Einige der Schritte in diesem Dokument erfordern die Verwendung eines kryptografischen Tools, das auf Ihrem lokalen Gerät installiert ist. Die Beispiele in dieser Aufgabe verwenden das OpenSSL-Tool. Weitere Informationen zu diesem Tool finden Sie unter https://www.openssl.org . Wenn Sie andere kryptografische Tools wie LibreSSL oder GnuTLS verwenden, finden Sie ähnliche Schritte in der Dokumentation zu diesen Produkten.

- Ändern Sie optionale Eigenschaften, die die Größe, den Auffüllalgorithmus und den Gültigkeitszeitraum des Schlüssels steuern. Weitere Informationen finden Sie unter Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.
- Sie benötigen Ihren symmetrischen Schlüssel (.BIN) für die Verschlüsselung.

  Wichtig: Ihr Schlüssel muss im Binärformat vorliegen. Wenn ein anderes Format verwendet wird, wird ein verwendet Validierung des Tokens fehlgeschlagen. Fügen Sie das unveränderte Token erneut an. Fehlermeldung wird angezeigt.

- Sie benötigen ein kryptografisches Tool, um Ihren Schlüssel einzuschließen. In diesem Beispiel wird OpenSSL 1,1 verwendet.

Erforderliche Rolle: sn_kmf.cryptographic_Manager oder sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Key Management Framework** > **Kryptografische Module** > **Alle**an.
2. Wählen Sie das kryptografische Modul aus, das Sie für den vom Kunden bereitgestellten Schlüssel aus der zugehörigen Liste Krypto-Spezifikationen erstellt haben.
3. Sie werden zu weitergeleitet **Schlüsselerstellung** Schritt.
4. Wenn Sie den umschließenden Schlüssel noch nicht heruntergeladen haben, klicken Sie auf den Link, um herunterzuladen `Token_publickey<id>.zip` Datei und speichern Sie sie an demselben Speicherort wie Ihr Schlüssel.

   Hinweis: Benennen Sie den heruntergeladenen nicht um `Token_publickey<id>` Datei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Entpacken Sie die Datei in Ihr lokales Netzwerk.
   Die ZIP-Datei enthält zwei Dateien, ein Import-Token und einen öffentlichen Schlüssel .PEM Zertifikat. Umschließen Sie Ihren symmetrischen Schlüssel mit dem öffentlichen Schlüssel, um ihn zu verschlüsseln.
6. Kopieren Sie den Namen von *Token_publickey* Datei in Ihre Zwischenablage.
7. Verwenden Sie von einer Befehlszeile aus die kopierte *Token_publickey* Dateiname zum Öffnen des Ordners der entpackten Dateien als Platzhalter für den umschlossenen Schlüssel.
8. Bearbeiten Sie dieses Skript, indem Sie die Beispiele durch die Namen Ihrer Krypto-Dateien ersetzen.

```
"downloads user.name$ cd token_publickey_<token>
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM
-in <keyname.bin>
-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt
 rsa_oaep_md:sha<128 or 256> "
```

Weitere Informationen finden Sie in den Befehlen zum Umschließen von Schlüsseln in der folgenden Tabelle.

Schlüsselumwicklungsbefehle

Richtungen	Befehl	Beispiel
Öffnen Sie das Dateiverzeichnis, in das Sie das Wrapping-Token heruntergeladen haben.	`cd`	cd-Token_publickey123456789
Fügen Sie den Namen des ein Publickey.PEM Zertifikat.	`openssl pkeyutl -encrypt -pubin -inkey`	Publickey_586798643ffff.PEM
Fügen Sie hier den Namen Ihres Schlüssels ein.	`-in`	mykey.bin
Geben Sie den Befehl <-out> ein, und geben Sie an, ob der Schlüssel 128 Bit oder 256 Bit ist.	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	N/V

9. Führen Sie den Befehl aus.
   Eine Systemmeldung wird angezeigt Token_Publickey_<keynumber> . Der Schlüssel und wird generiert *Wrapped_key_Material* Datei wurde dem Verzeichnis hinzugefügt.
10. Laden Sie den umschlossenen Schlüssel hoch.

Nächste Maßnahme

Zurück zu Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch Um Ihren umschlossenen Schlüssel hochzuladen.

Konfigurieren Sie den vom Kunden bereitgestellten Schlüssel, und laden Sie ihn hoch

Sie können Ihren eigenen vom Kunden bereitgestellten Schlüssel anstelle von verwenden ServiceNow® Vom System generierte Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rollen: Security_admin, sn_kmf.cryptographic_Manager

Wenn Sie KEINE eigenen Schlüssel bereitstellen, müssen Sie dieses Verfahren nicht ausführen. Dient zum Erstellen eines kryptografischen Moduls mit ServiceNow® Schlüssel, wechseln Sie zu Erstellen Sie ein kryptografisches Modul Oder Erstellen Sie ein kryptografisches Modul für Feldverschlüsselung.

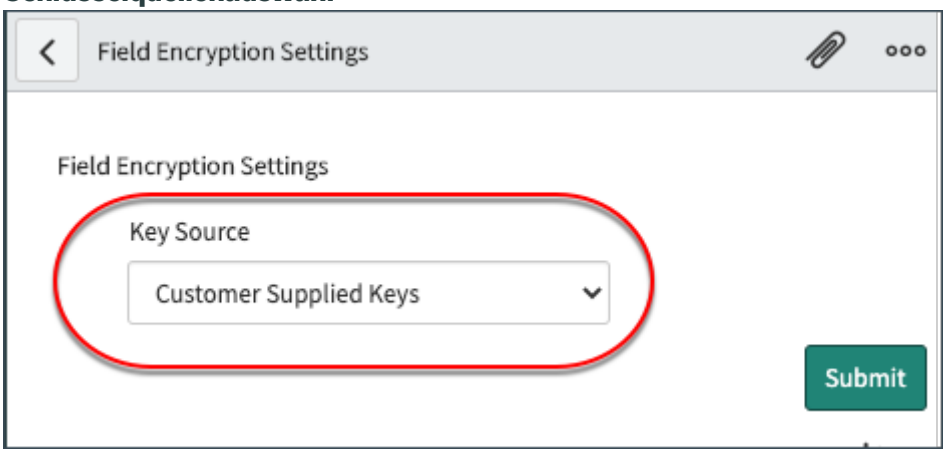
Hinweis: Dieses Verfahren gilt nur für Feldverschlüsselung Enterprise Funktionalität. Weitere Informationen finden Sie unter Feldverschlüsselung aktivieren.

Wichtig: Sie können einen vom Kunden bereitgestellten Schlüssel nicht widerrufen.

Prozedur

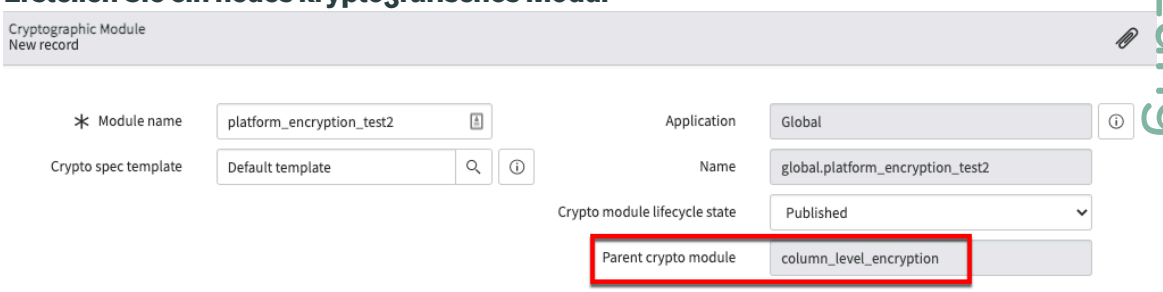
1. Navigieren zu **Alle** > **Systemsicherheit** > **Einstellungen für Feldverschlüsselung** Und verifizieren Sie das **Vom Kunden Bereitgestellte Schlüssel** Ist ausgewählt.

Schlüsselquellenauswahl



2. Wählen Sie **Absenden**.
3. Zurück zu **Systemsicherheit** > **Feldverschlüsselungsmodule** > > **Neu erstellen**an.

Erstellen Sie ein neues kryptografisches Modul



4. Füllen Sie das Formular „kryptografisches Modul“ wie folgt aus:

Kryptografische Modulfelder

Feld	Beschreibung
Modulname	Geben Sie einen Namen für das Modul ein.

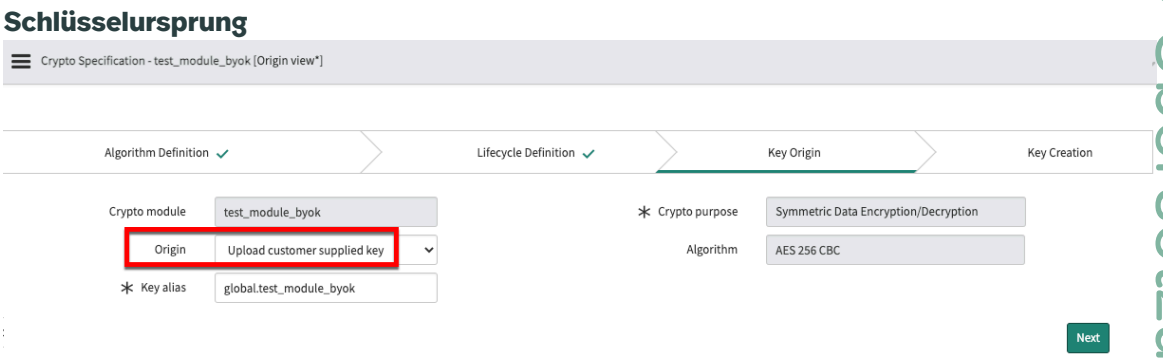
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Krypto-Spezifikationsvorlage	Die standardmäßige kryptografische Vorlage ist ausgewählt.
Name	Füllt automatisch basierend auf dem Modulnamen aus und stellt dem Namen den Bereich voran, um sicherzustellen, welche Anwendung angewendet wird. In diesem Fall wird der globale Bereich angewendet.
Lebenszyklusstatus kryptografisches Modul	Auswahlvorgang **Veröffentlicht** Zum Aktivieren des Krypto-Moduls.
Übergeordnetes kryptografisches Modul	Das übergeordnete Modul **Column_level_Encryption** Wird automatisch ausgewählt, wenn vom Kunden bereitgestellte Schlüssel und Verschlüsselungsmodule verwendet werden.

5. Wählen Sie **Absenden**.
6. Wählen Sie das neu erstellte kryptografische Modul aus der Tabelle aus.
   In **Krypto-Spezifikationen** Zugehörige Liste wählen Sie den automatisch generierten Schlüsselalias mit dem AES 256 CFB-Algorithmus aus.

   Das System füllt den Krypto-Zweck und den Algorithmus für aus Feldverschlüsselung Automatisch und springt zu **Schlüsselursprung** Phase.
7. Beachten Sie das **Vom Kunden bereitgestellten Schlüssel hochladen** Ist **Ursprung** Und **Schlüsselalias** Ist bereits ausgefüllt.



8. Wählen Sie Aus **Als Nächstes** Um zu wechseln **Schlüsselerstellung** Phase.

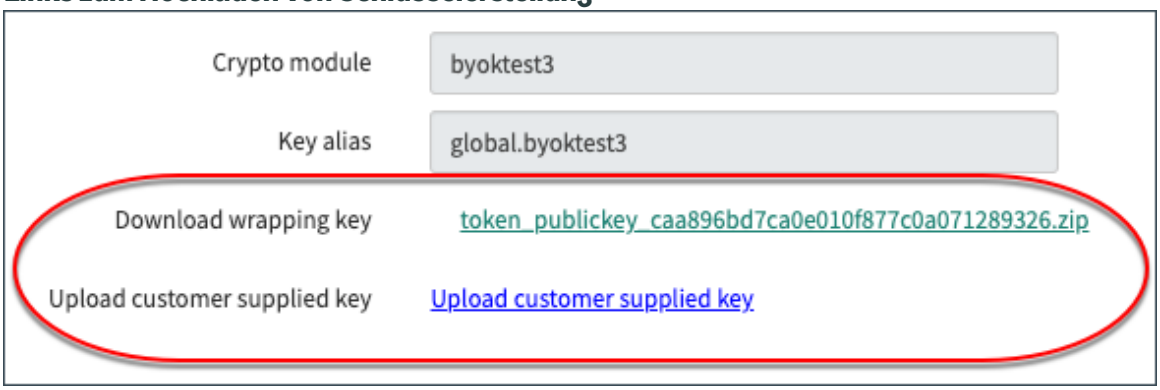
   Es gibt zwei Links:

   - **Umschließenden Schlüssel herunterladen** Lädt den Schlüssel in eine ZIP-Datei herunter, die ein Import-Token und ein öffentliches Schlüsselzertifikat enthält. `.PEM` Datei. Verwenden Sie das Importtoken, um die erfolgreiche Schlüsselumwicklung gemäß der Sicherheitsspezifikation für die Instanz zu überprüfen. Verwenden Sie das öffentliche Schlüsselzertifikat `.PEM` Datei zum sicheren Umschließen des vom Kunden bereitgestellten Schlüssels, bevor er zusammen mit dem Token hochgeladen wird.
   - **Vom Kunden bereitgestellten Schlüssel hochladen** Öffnet den Dateibrowser, um das Token und den verschlüsselten Schlüssel auszuwählen, den Sie umgebrochen haben.

Automatische Übersetzung

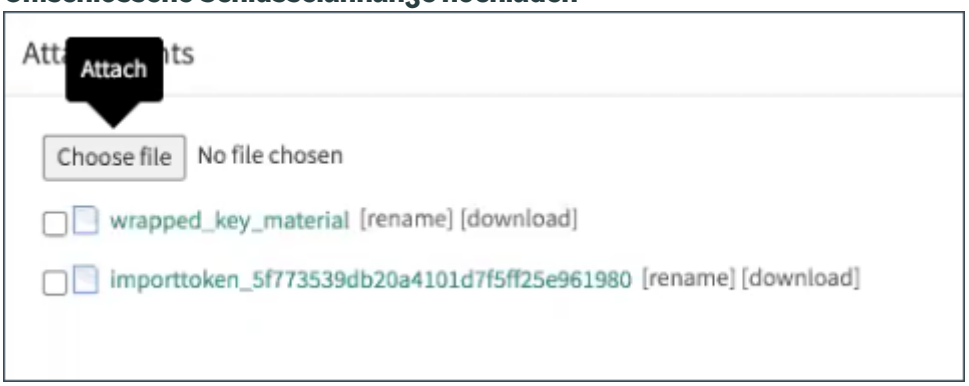
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Links zum Hochladen von Schlüsselerstellung



9. Wählen Sie Aus **Umschließenden Schlüssel herunterladen** Zum Speichern des Tokens.
   Speichern Sie das Token an demselben Zielspeicherort, da der Schlüssel auf Ihrem System gespeichert ist. Benennen Sie das heruntergeladene Token nicht um.
10. Führen Sie den BYOK-Befehl auf einem Terminal aus, um den Schlüssel einzuschließen.
    Weitere Informationen finden Sie unter Schließen Sie Ihren vom Kunden bereitgestellten Schlüssel ein.
11. Wählen Sie Aus **Vom Kunden bereitgestellten Schlüssel hochladen** .
12. Wählen Sie Aus **Durchsuchen** Um die beiden Dateien auszuwählen, den umschlossenen Schlüssel und die Tokendatei.
    Im Fenster Anhänge werden die beiden Dateien angezeigt.

Umschlossene Schlüsselanhänge hochladen



Wählen Sie bei Bedarf eine Datei aus, die entfernt und erneut hochgeladen werden soll.

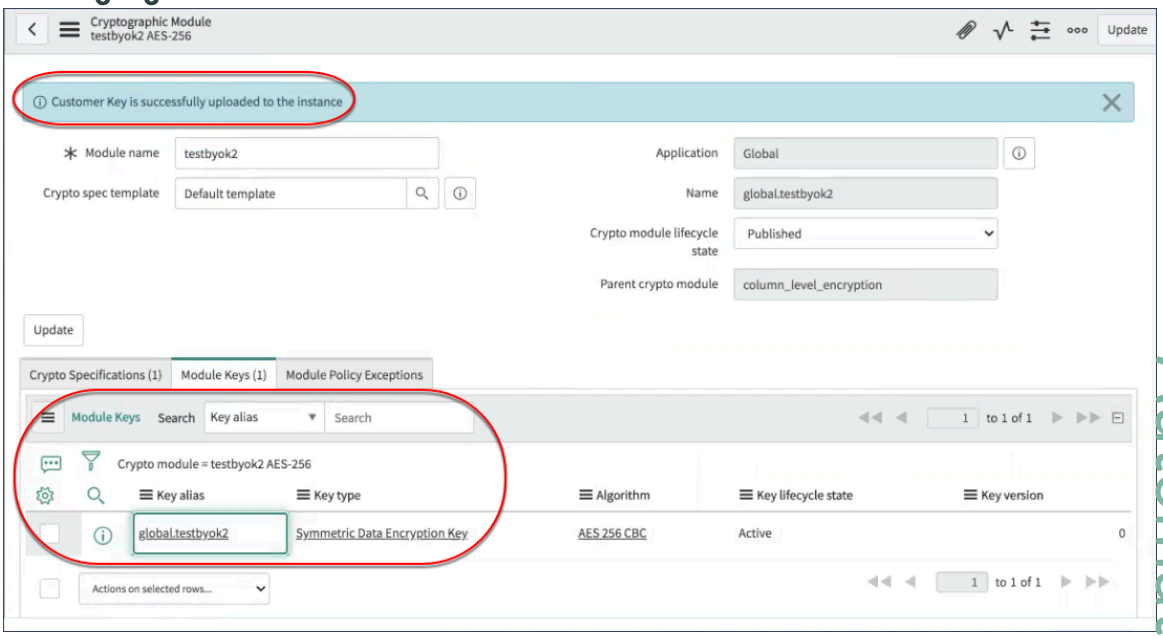
13. Wählen Sie **OK**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie kehren zum Bildschirm „kryptografisches Modul“ zurück. Eine Bestätigungsnachricht wird für einen erfolgreichen Upload des Kundenschlüssels angezeigt. Der Schlüssel wird auch in der zugehörigen Liste Modulschlüssel aufgeführt.

Bestätigung des Schlüsselhochladens



Nächste Maßnahme

Nachdem Sie nun die Konfiguration Ihres kryptografischen Moduls mit dem vom Kunden bereitgestellten Schlüssel abgeschlossen haben, fahren Sie mit fort Erstellen Sie eine Modulzugriffsrichtlinie

Felder und Anhänge werden verschlüsselt

Sobald kryptografische Module erstellt wurden, kann ein Sicherheitsadministrator die Konfiguration verschlüsselter Felder (EFC) definieren und ein Feld oder einen Anhang in einer Tabelle verschlüsseln.

So verschlüsseln Sie Felder

Hinweis: Verschlüsselte Felder werden nicht vom Design geprüft. Dieses Verhalten kann nicht konfiguriert werden.

1. Geben Sie die Schlüsselquelle an: ServiceNow Generierte Schlüssel oder Ihre vom Kunden bereitgestellten Schlüssel (eigenen Schlüssel mitbringen) **Systemsicherheit** > **Einstellungen für Feldverschlüsselung**an.
2. Nachdem Sie die Schlüsselquelle angegeben haben, erstellen Sie ein kryptografisches Modul, oder verwenden Sie ein vorhandenes kryptografisches Modul. Beginnen Sie mit Erstellen Sie ein kryptografisches Modul Für Anweisungen.

   Hinweis: Wenn Sie vom Kunden bereitgestellte Schlüssel verwenden, befolgen Sie die Anweisungen in Erstellen Sie ein kryptografisches Modul für Feldverschlüsselung Und Konfigurieren Sie Eigenschaften für vom Kunden bereitgestellte Schlüssel.

3. Erstellen Sie eine verschlüsselte Feldkonfiguration, um zu definieren, wo die Verschlüsselung angewendet wird. Hier geben Sie die Zieltabelle an, und wählen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aus, ob eine Spalte oder Anhänge innerhalb der Tabelle verschlüsselt werden sollen. Informationen zu den ersten Schritten finden Sie unter Legen Sie verschlüsselte Feldkonfigurationen fest.

Hinweis: Siehe Feldverschlüsselung Enterprise Beispiele Dies veranschaulicht, wie Felder und Anhänge mit vom Kunden bereitgestellten Schlüsseln verschlüsselt werden.

Legen Sie verschlüsselte Feldkonfigurationen fest

Konfigurieren Sie, welche Tabellenspalten oder Anhänge das System mithilfe eines vorkonfigurierten kryptografischen Moduls verschlüsselt.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_Manager und Security_admin, oder erhöhen Sie die Rolle auf den Sicherheitsadministrator.

Warum und wann dieser Vorgang ausgeführt wird
Stellen Sie sicher, dass Sie sich im richtigen Anwendungsbereich befinden, damit Sie die Tabellen in diesem Bereich sehen können.

Nur Anwender mit Zugriff auf das in dieser Konfiguration verwendete kryptografische Modul können die Daten in der verschlüsselten Tabellenspalte lesen oder auf den Anhang zugreifen.

- Wenn ein Anwender Schreibzugriff, aber keinen Lesezugriff hat, wird das Feld im Bearbeitungsmodus angezeigt, und die eingegebenen Daten werden als Sternchen angezeigt.
- Wenn ein Anwender Lesezugriff, aber keinen Schreibzugriff hat, zeigt das Feld die entschlüsselten Daten im schreibgeschützten Modus an.
- Wenn ein Anwender alle Zugriffsrechte hat, ist im verschlüsselten Feld sowohl Lese- als auch Schreibfunktionen verfügbar.

Siehe Erstellen Sie ein kryptografisches Modul Oder Erstellen Sie ein kryptografisches Modul für Feldverschlüsselung Um zu beginnen.

Wichtig:

Nach dem Verschlüsseln einer Spalte werden alle neuen Daten, die in die Spalte eingefügt werden, automatisch verschlüsselt. Daten, die in der Spalte vorhanden waren, bevor die Verschlüsselung aktiv war, werden jedoch nicht automatisch verschlüsselt.

Um Daten zu verschlüsseln, die vor der Verschlüsselung der Spalte vorhanden waren, müssen Sie einen separaten Massenverschlüsselungsauftrag ausführen. Weitere Informationen zur Massenverschlüsselung finden Sie in Führen Sie eine Massenverschlüsselung oder -Entschlüsselung aus.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen** > **Neu**an.
2. Wählen Sie **Neu**.
3. Füllen Sie das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	**Spalte** Zum Verschlüsseln einer Tabellenspalte oder **Anhang** Zum Verschlüsseln aller Anhänge einer Tabelle. Typen von verschlüsselten Daten sind: ○ Zeichenfolgentext (vollständiges UTF-8) ○ Anhänge ○ Datum, Datum/Uhrzeit: **Hinweis:** Sie können Verschlüsselungsfeld-Konfigurationen zum Verschlüsseln der vorhandenen Datums- und Datums-/Uhrzeitfelder erstellen. Sie können eine neue Verschlüsselungskonfiguration nur einer übergeordneten Tabelle hinzufügen. Sie können einer untergeordneten Tabelle keine neue Verschlüsselungskonfiguration hinzufügen. ○ URL ○ HTML ○ Journal ○ Übersetzt
Tabelle	Tabelle, deren Felder oder Anhänge verschlüsselt werden sollen.
Spalte	Spalte (Feld), die verschlüsselt werden soll, wenn Sie ausgewählt haben **Spalte** Als Typ.
Aktiv	Wählen Sie diese Option aus, um die Konfiguration als aktiv zu markieren. Deaktivieren Sie diese Option, wenn die Konfiguration noch nicht verwendet wird.
Krypto-Modul	Das kryptografische Modul, für das die verschlüsselte Feldkonfiguration gilt.
Methode	Wählen Sie Aus **Einzelnes Modul** Zum Festlegen der Feldkonfiguration für ein Modul. Wählen Sie Aus **Mehrere Module** Für rollenbasierten Zugriff, der sich über mehr als ein kryptografisches Modul erstreckt. **Einzelnes Modul** Verwenden Sie diese Option, um alle Anhänge mit einem einzelnen Modul zu verschlüsseln. Ihre Anwender benötigen Zugriff auf dieses Modul, andernfalls können sie keine Anhänge hochladen. **Mehrere Module** Verwenden Sie diese Option, damit Anwender beim Hochladen von Anhängen ein Modul auswählen können. Benutzer mit Zugriff auf mindestens ein Modul können ein Modul auswählen, das für die Verschlüsselung verwendet werden soll. Benutzer ohne Modulzugriff können unverschlüsselte Anhänge hochladen.
Mit Algorithmus Verschlüsselte Beibehaltung	Gibt an, ob das von Ihnen ausgewählte Krypto-Modul bereits für die Unterstützung der nicht deterministischen Verschlüsselung konfiguriert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
[Schreibgeschützt]	Dies bedeutet, dass die Verschlüsselung jedes Mal unterschiedlich ist, wenn dieselben Daten mehr als einmal verschlüsselt werden.

4. Wählen Sie **Absenden**.

Skriptzugriff für kryptografische Module

Skripts können ausgeführt werden, um auf eine kryptografische Modulrichtlinie für einen kryptografischen Zweck zuzugreifen.

Für Key Management Framework, Richtlinien können basierte Skripts sein. Wenn eine Zugriffsrichtlinie für den Skriptzugriff ausgelöst wird, kann das Back-End-Skript die Modulrichtlinienaktionen aus dem Skript ausführen.

Kryptografische Module können einen oder mehrere Verschlüsselungszwecke unterstützen, z. B. asymmetrische Datenentschlüsselung und symmetrische Datenentschlüsselung. Jeder kryptografische Zweck erfordert die Generierung eines Verschlüsselungsschlüssels und einen definierten kryptografischen Zweck.

Beachten Sie beim Ausführen einer Verschlüsselungsskriptanforderung Folgendes:

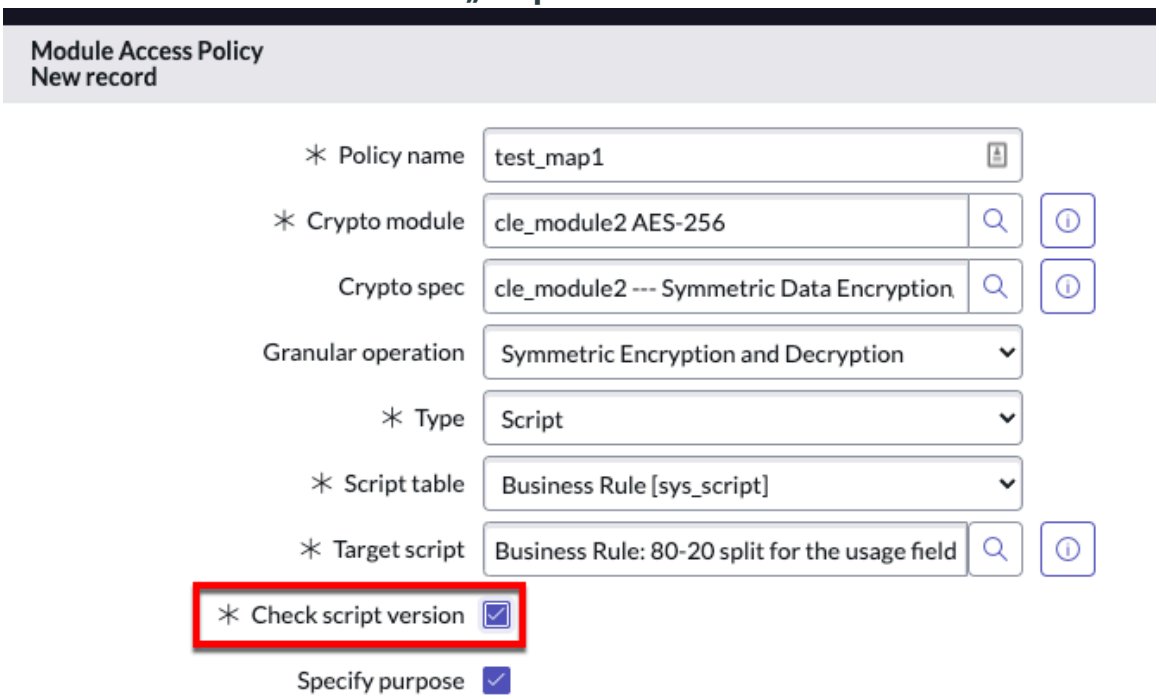
- Der referenzierte kryptografische Zweck muss im kryptografischen Modul definiert werden.
- Für das kryptografische Modul muss ein aktiver generierter Schlüssel vorhanden sein.
- Der Modulzugriffsrichtlinientyp muss auf festgelegt sein **Skript** .

Skriptversion überprüfen

Beim Erstellen einer Modulzugriffsrichtlinie, die auf den Skripttyp festgelegt ist, ist eine Option verfügbar, um die Integrität der Skriptversion zu validieren, auf die zugegriffen wird. Nur die zugewiesene Version des Skripts darf auf die Verschlüsselungsmodule zugreifen. Wenn **Überprüfen Sie die Skriptversion** Das Kontrollkästchen ist in der Modulzugriffsrichtlinie aktiviert. Jedes Mal, wenn das Skript ausgeführt wird, führt das System einen Versionsvergleich durch. Wenn das Skript geändert wurde, wird der Anwender benachrichtigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie das Kontrollkästchen „Skriptversion“



Konfigurieren Sie den Skriptzugriff auf verschlüsselte Daten

Führen Sie ein Skript aus, um die kryptografische Modulrichtlinie für einen kryptografischen Zweck auszuführen. Spezifischer Lese- (Entschlüsseln/Entpacken) oder Schreibzugriff (Verschlüsseln, Umbrechen) kann basierend auf der Granularität des Modulzugriffsrichtlinienvorgangs definiert werden.

Vorbereitungen

Erforderliche Rolle: sn_kmf.cryptographic_Manager

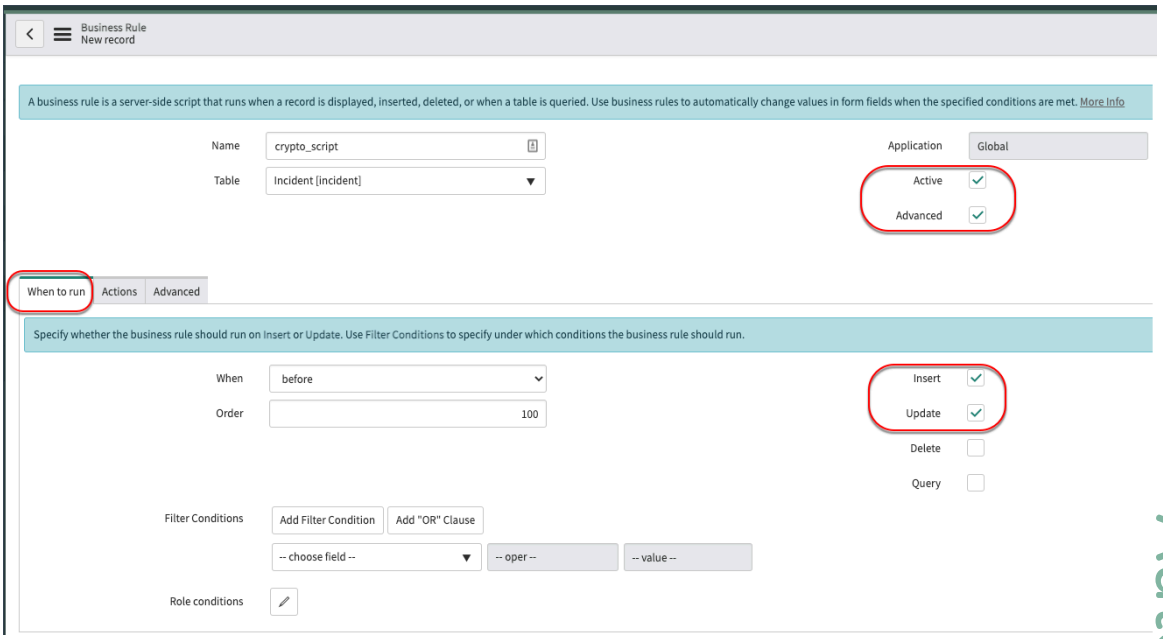
Warum und wann dieser Vorgang ausgeführt wird

Anwendungsbeispiele sind Business-Regeln und Skripteinbindungen. Dieses Verfahren verwendet ein Skript für Business-Regeln.

Prozedur

1. Erstellen Sie ein kryptografisches Modul mit dem symmetrischen Datenverschlüsselungs-/Entschlüsselungsalgorithmus.
   Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul. Der spezifische Zugriff auf die Daten oder Anhänge wird mit einer Modulzugriffsrichtlinie mit den folgenden Merkmalen gesteuert:
   - Symmetrische Verschlüsselung: Das Skript kann Daten verschlüsseln, aber die Daten können nicht entschlüsselt werden.
   - Symmetrische Entschlüsselung: Das Skript kann hochgeladene verschlüsselte Daten oder Anhänge entschlüsseln, aber Daten oder Anhänge können nicht verschlüsselt werden.
   - Symmetrische Verschlüsselung und Entschlüsselung: Das Skript kann Daten oder Anhänge sowohl verschlüsseln als auch entschlüsseln.
2. Navigieren zu **Systemdefinition** > **Business-Regeln**an.
3. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



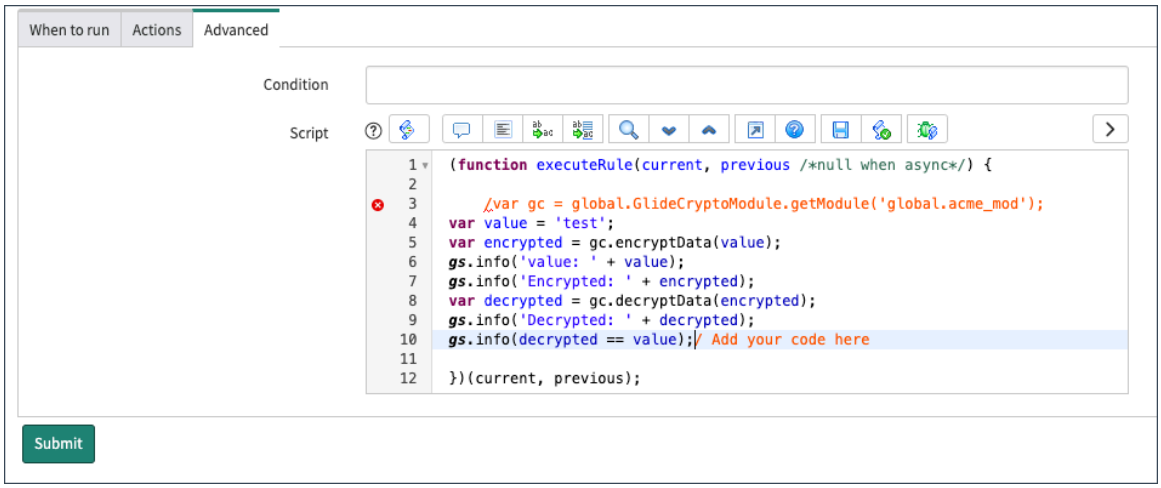
4. Füllen Sie das Formular im aus **Zeitpunkt der Ausführung** Registerkarte und geben Sie das Skript in ein **Erweitert** Registerkarte:

Business Rule-Felder

Feld	Beschreibung
Name	Geben Sie einen Namen für die Business Rule ein.
Tabelle	Wählen Sie Aus **Incident [Incident]** Aus der Dropdown-Liste.
Anwendung	**Global** Ist standardmäßig ausgewählt.
Aktiv	Markieren Sie die Regel als **Aktiv** .
Erweitert	Aktivieren Sie das Kontrollkästchen, um erweiterte Optionen anzuzeigen.
Registerkarte „Ausführungszeitpunkt“	Auf der **Zeitpunkt der Ausführung** Registerkarte aktivieren **Einfügen** Und **Aktualisieren** Felder.

Registerkarte „Erweitert“	Auf der **Erweitert** Fügen Sie den folgenden Skripttext in Zeile 3 ein:
	`//`
	`var gc =`
	`global.GlideCryptoModule.getModule('global.acme_mod');`
	`var value = 'test';`
	`var encrypted = gc.encryptData(value);`
	`gs.info('value: ' + value);`
	`gs.info('Encrypted: ' + encrypted);`
	`var decrypted = gc.decryptData(encrypted);`
	`gs.info('Decrypted: ' + decrypted);`
	`gs.info(decrypted == value);`
	Hinweis: Weitere Informationen finden Sie im Bild „Registerkarte „Business-Regeln – Erweitert“.

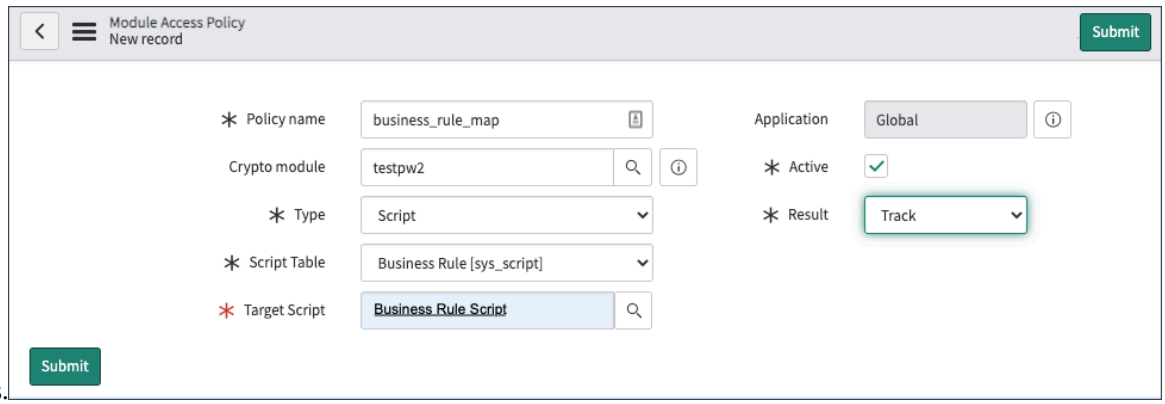
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.
6. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle** .

   Hinweis: Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

7. Klicken Sie auf **Neu**.
8. Füllen Sie das Formular aus.



Felder für Modulzugriffsrichtlinien

Feld	Beschreibung
Richtlinienname	Geben Sie einen Namen für die Richtlinie ein.
Krypto-Modul	Klicken Sie auf das Suchsymbol, um ein Modul mit dem symmetrischen Datenverschlüsselungs-/Entschlüsselungsalgorithmus auszuwählen.
Typ	Wählen Sie Aus **Skript** Dient zur Steuerung des Zugriffs nach Skript.
Skripttabelle	Wählen Sie einen Wert aus der Dropdown-Liste „Skripttabelle“ aus. Wählen Sie für dieses Beispiel aus **Business-Regel [sys_script]** .
Zielskript	Wählen Sie das Skriptdokument für die Richtlinie aus. Wählen Sie aus **Tabellenname** Und dann das zugehörige Dokument für die Richtlinie. Wählen Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	in diesem Beispiel die Business-Regel aus, die Sie in den vorherigen Schritten erstellt haben.
Aktiv	Wählen Sie diese Option aus, um die Richtlinie zu aktivieren.
Ergebnis	Um dem Skript Zugriff auf das Modul zu gewähren, wählen Sie aus **Nachverfolgen** In **Ergebnis** Feld.

9. Klicken Sie auf **Absenden**.
   Die Modulzugriffsrichtlinie für das Skript ist jetzt im System verfügbar.

Zeigen Sie abgelehnte Anforderungen zur Nutzung kryptografischer Module an

Zeigen Sie kryptografische Module an, die Verschlüsselungsanforderungen von Skripts aufgrund nicht unterstützter Verschlüsselungsmechanismen abgelehnt haben.

Vorbereitungen
Erforderliche Rolle: sn_kmf.cryptographic_Manager

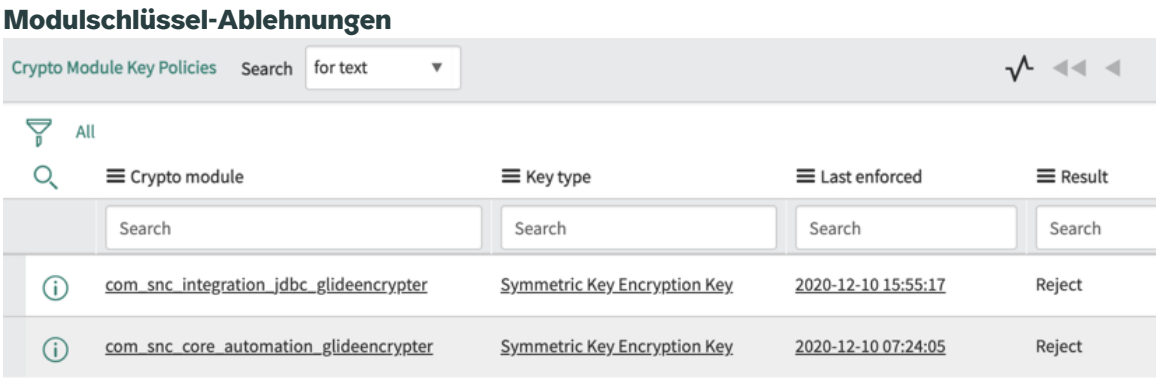
Warum und wann dieser Vorgang ausgeführt wird
Kryptografische Module können einen oder mehrere Verschlüsselungszwecke unterstützen, z. B. asymmetrische Datenentschlüsselung und symmetrische Datenentschlüsselung. Auf verschlüsselte Daten kann nur basierend auf der Modulzugriffsrichtlinie zugegriffen werden. Wenn ein Skript versucht, ein kryptografisches Modul für einen nicht im Modul definierten Zweck zu verwenden, kann das Skript nicht auf die verschlüsselten Daten zugreifen.

Im folgenden Beispiel wurde einem kryptografischen Modul ein kryptografischer Zweck zugewiesen, dafür wurde jedoch nie ein Schlüssel generiert.

Prozedur

Navigieren zu **Alle** > **Schlüsselverwaltung** > **Modulschlüssel-Richtlinien** > **Modulschlüssel-Ablehnungen**an.

Eine Liste der kryptografischen Module, die abgelehnte Anforderungen zusammen mit dem im entsprechenden Skript verwendeten Verschlüsselungsschlüssel angezeigt werden.



Hinweis: Wenn ein anderes Skript versucht, dasselbe kryptografische Modul mit demselben Schlüsseltyp zu verwenden, der Wert für **Zuletzt erzwungen** Updates. Eine andere Zeile wird nicht generiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Beispiel hat das erste Modul bei 2020-02-10_15:55:17 eine Anforderung abgelehnt, da der Schlüssel von module1 gefährdet ist. Bei 2020-02-10_07:24:05 hat das zweite Modul eine Anforderung abgelehnt, da der Schlüssel des zweiten Moduls angehalten ist.

Um Skripts die Berechtigung zur Verwendung des Verschlüsselungsmoduls bei der nächsten Ausführung zu gewähren, erstellen Sie eine Modulzugriffsrichtlinie für die Skriptverschlüsselung. Weitere Informationen finden Sie unter Konfigurieren Sie den Skriptzugriff auf verschlüsselte Daten.

Planen Sie Massenverschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge

Planen Sie Verschlüsselungs-, Entschlüsselungs- und Neuschlüsselaufträge so, dass sie zu einem Zeitpunkt ausgeführt werden, der für Ihre Instanz am besten geeignet ist.

Vorbereitungen

Verschlüsselungs-, Entschlüsselungs- und Neuschlüsselaufträge können Zeit- und ressourcenintensiv sein. Erwägen Sie daher die Planung außerhalb der Spitzenzeiten. Stellen Sie außerdem sicher, dass der Anwender, der den Auftrag plant, über den entsprechenden Zugriff für jeden Auftrag verfügt.

Erforderliche Rolle: sn_kmf.cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird

Massenverschlüsselung und -Entschlüsselung ist auch über das Formular „verschlüsselte Feldkonfigurationen“ verfügbar. Siehe Führen Sie eine Massenverschlüsselung oder -Entschlüsselung aus für Anweisungen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Security-Aufträge**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Planungsformular aus.

Feld	Beschreibung
Name	Name des Verschlüsselungs-, Entschlüsselungs- oder Neuschlüsselungsauftrags.
Typ	Auftragstyp: ○ **Schlüsselmigrationskontext zu Modul:** Massenmigration von Verschlüsselungskontextschlüsseln zu Verschlüsselungsmodulen, einschließlich der Erstellung von Datensätzen für Modulzugriffsrichtlinien für Zugriffssteuerungen für die Verschlüsselungsmodule ○ **Datenmigrationskontext zu Modul** : Migriert von Verschlüsselungskontexten verschlüsselte Daten zu Verschlüsselungsmodulen ○ **Massentschlüsselungsanhang** : Entschlüsselt alle verschlüsselten Anhänge in Datensätzen für eine einzelne Tabelle, die Sie in definieren **Tabelle** Feld. ○ **Massenverschlüsselungsanhang** : Verschlüsselt alle Anhänge in Datensätzen für eine einzelne Tabelle, die Sie in definieren **Tabelle** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Massenverschlüsselung** : Verschlüsselt jeden bereits vorhandenen Wert in der definierten Spalte/dem in der Feldverschlüsselungskonfiguration verwendeten Feld ○ **Massenentschlüsselungsmodul** : Entschlüsselt alle bereits vorhandenen Werte in der definierten Spalte/dem definierten Feld, die in der Feldverschlüsselungskonfiguration mit einzelnem Modul verwendet wird. ○ **Mehrfachmodul Für Massenentschlüsselung** : Entschlüsselt alle bereits vorhandenen Werte in der definierten Spalte/dem definierten Feld, die in der Feldverschlüsselungskonfiguration mit mehreren Modulen verwendet wird. ○ **Massenwiedergabe** : Verschlüsselt alle bereits vorhandenen Werte in der definierten Spalte/dem definierten Feld, die in der Feldverschlüsselungskonfiguration verwendet wird, erneut mit dem aktuell aktiven Schlüssel für das Modul. ○ **Migrieren Sie den Anhangskontext zum Modul** : Verschlüsselt alle bereits vorhandenen Anhänge in der Tabelle, die im Feld „Verschlüsselungskonfiguration“ definiert ist. Alle Anhänge, die zuvor mit einem Kontext verschlüsselt wurden, werden mit dem Modul erneut verschlüsselt.
Status	Der anfängliche Auftragsstatus ist Neu. Nachdem die Aufgabe wie geplant ausgeführt wurde, wird der Status entsprechend aktualisiert.
Zeitfensterstart	Startzeit für den Auftrag im 24-Stunden-Format.
Zeitfensterende	Endzeit für den Auftrag im 24-Stunden-Format.
Tabelle	Tabelle, die verschlüsselt oder entschlüsselt werden soll.
Feld	Feld, das verschlüsselt oder entschlüsselt werden soll.
Zusammenfassung	Auftragsstatusinformationen, wenn der Auftrag ausgeführt wird, abgeschlossen wurde oder Fehler aufweist.

Hinweis: Aufgrund des Systemaufwands sollten Sie Massenverschlüsselungs-, Entschlüsselungs- und Neuschlüsselaufträge so planen, dass sie außerhalb der Spitzenzeiten ausgeführt werden. Die ServiceNow AI Platform Führt den Auftrag zwischen aus **Zeitfensterstart** Und **Zeitfensterende** . Wenn der Auftrag in einem Verarbeitungsfenster nicht abgeschlossen ist, wird er während des nächsten angegebenen Verarbeitungsfensters fortgesetzt, bis die gesamte Verarbeitung abgeschlossen ist.

4. Klicken Sie auf **Absenden**.
5. Nachdem Sie eine Aufgabe geplant haben, können Sie Folgendes tun.
   - Klicken Sie Auf **Auftrag Abbrechen** Um einen laufenden Auftrag abzubrechen.
   - Klicken Sie Auf **Starten** Um einen Auftrag sofort zu starten.
   - Klicken Sie Auf **Aktualisieren** Um alle Änderungen zu speichern, die Sie am Auftragszeitplan vornehmen.
   - Klicken Sie Auf **Löschen** Um die geplante Aufgabe zu löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie eine Massenverschlüsselung oder -Entschlüsselung aus

Sie können eine Massenverschlüsselung für Verschlüsselungskonfigurationen sowie eine Massenentschlüsselung ausführen, um zuvor verschlüsselte Werte zu entschlüsseln.

Vorbereitungen
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch geplante Aufgaben für die Massenverschlüsselung und -Entschlüsselung erstellen. Siehe Planen Sie Massenverschlüsselungs-, Entschlüsselungs- und Neuschlüsselungsaufträge für Anweisungen.

Massenverschlüsselung und -Entschlüsselung sind nur verfügbar, wenn eine verschlüsselte Feldkonfiguration das einzelne kryptografische Modul verwendet. Die Massenentschlüsselung ist sowohl für die einzelne als auch für mehrere Verschlüsselungsmethoden verfügbar.

Hinweis: Sie sollten die Massenverschlüsselung und -Entschlüsselung nur außerhalb der Spitzenzeiten ausführen, da die Vorgänge Ressourcen- und zeitintensiv sind.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Feldverschlüsselung** > **Verschlüsselungsfeld-Konfigurationen**an.
2. Öffnen Sie die verschlüsselte Feldkonfiguration für das Feld, das Sie Massenverschlüsseln oder entschlüsseln möchten.
3. Wählen Sie unter zugehörige Links eine verfügbare Option aus.
   - **Planen Sie einen Massenentschlüsselungsauftrag**
   - **Massenverschlüsselungsauftrag planen**
4. Bestätigen Sie Ihre Auswahl im Dialogfeld.

Ergebnis
Wenn eine Massenverschlüsselung ausgeführt wird, werden alle Werte mit dem im Datensatz der verschlüsselten Feldkonfiguration definierten Verschlüsselungsmodul verschlüsselt. Wenn Sie eine Massenentschlüsselung ausführen, werden nur Felder entschlüsselt, die mit einem Verschlüsselungsmodul verschlüsselt wurden, auf das Sie Zugriff haben.

Anhänge zur Verschlüsselung hochladen

Schützen Sie vertrauliche Dateien, indem Sie Datensatzanhänge mithilfe von Feldverschlüsselungs- und Zeilenbedingungen verschlüsseln.

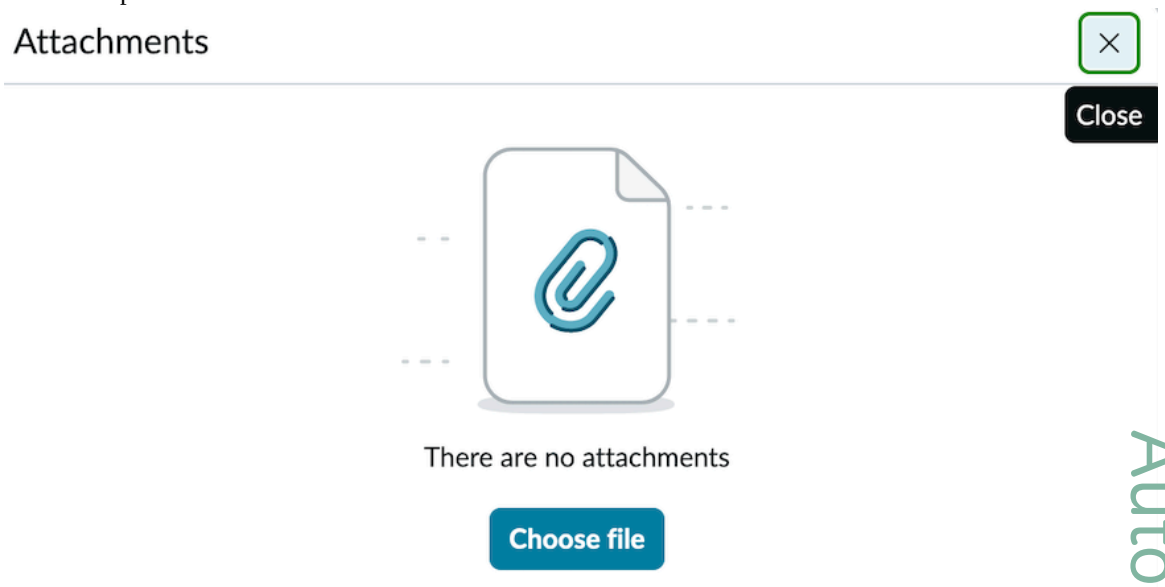
Vorbereitungen
Erforderliche Rolle: Jede Rolle, die an der vom Administrator erstellten Modulzugriffsrichtlinie (MAP) ausgerichtet ist.

Prozedur

1. Zu einem Datensatz navigieren.
2. Wählen Sie aus **Verwalten Sie Anhänge** Büroklammersymbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. In **Anhänge** Wählen Sie im das Modul aus, mit dem verschlüsselt werden soll **Mit Modul verschlüsseln**Dropdown-



Optionen. 

Hinweis:

Wenn der Konfiguration des Verschlüsselungsfelds Zeilenbedingungen hinzugefügt wurden, wird diese Option nicht angezeigt. Der Anhang wird dann automatisch mit dem in der Zeilenbedingung definierten Modul verschlüsselt. Ebenso wird diese Dropdown-Option nur angezeigt, wenn das Symbol „Anhänge verwalten“ verwendet wird, und nicht, wenn der Anhang per Drag-and-Drop hinzugefügt wird.

4. Wählen Sie Aus **Wählen Sie die Datei aus** Um den Anhang zu suchen und auszuwählen **Öffnen** Um es anzuhängen.

Ergebnis

Angehängte Dateien werden oben im Formular angezeigt. Verschlüsselte Anhänge werden durch ein Schlosssymbol gekennzeichnet. Nur Anwender mit dem Verschlüsselungsmodul zum Anzeigen verschlüsselter Dateien werden aufgelistet.

Feldverschlüsselung Enterprise Beispiele

Diese Beispiele führen Sie durch die Verschlüsselung von Feldern und Anhängen mit vom Kunden bereitgestellten Schlüsseln.

Feldverschlüsselung Enterprise Walk-through

Diese Walk-through zeigt Ihnen, wie Sie ein Feld in Ihrer Instanz mit verschlüsseln Feldverschlüsselung Enterprise Mit Key Management Framework(KMF). Außerdem erfahren Sie, wie Sie Ihren eigenen Schlüssel verwenden.

Vorbereitungen

Hinweis: Dieses Verfahren gilt nur für Feldverschlüsselung Enterprise Funktionalität. Siehe Feldverschlüsselung aktivieren Weitere Informationen zum Abrufen von Feldverschlüsselung Enterprise.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin oder security_admin

Hinweis: Security_admin ist eine privilegierte Rolle. Details zur Verwendung privilegierter Rollen finden Sie unter Auf eine privilegierte Rolle hochstufen

Warum und wann dieser Vorgang ausgeführt wird

Diese Walkthrough beginnt mit einer Instanz, in der Sie Ihren persönlichen kryptografischen Schlüssel bereits erstellt und hochgeladen haben. Sie könnten verwenden ServiceNow Schlüssel, aber in diesem Beispiel wird ein vom Kunden bereitgestellter Schlüssel verwendet.

Nachdem der Schlüssel in einem kryptografischen Modul gespeichert wurde, können Sie mit der Konfiguration von Feldern in Ihrer Instanz beginnen, z. B. Gehaltsnummern oder Sozialversicherungsnummern, die von bestimmten Anwendern eingeschränkten Zugriff haben. Geben Sie im Feld verschlüsselte Konfiguration an, welches autorisierte Personal auf vertrauliche Daten zugreifen kann.

In dieser Aufgabe werden zwei Szenarien demonstriert. Ein Beispiel verschlüsselt **Kurzbeschreibung** Feld in einem Incident für Anwender, die nicht berechtigt sind, die sensiblen Daten anzuzeigen.

Anhänge können auch verschlüsselt werden und nur für Anwender sichtbar sein, denen Zugriff gewährt wird, oder für alle Anwender, die nicht an der Anzeige der Daten gehindert sind. Siehe Walkthrough zur Anhangsverschlüsselung Zum Verschlüsseln eines Anhangs.

Prozedur

1. Stellen Sie sicher Feldverschlüsselung Enterprise Ist aktiviert.
2. Erstellen Sie ein kryptografisches Modul für column_level_Encryption.
   Siehe Erstellen Sie ein kryptografisches Modul für Feldverschlüsselung Erstellen Sie ein kryptografisches Modul Weitere Informationen finden Sie unter .
3. Navigieren zu **Systemsicherheit** > **Verschlüsselungsfeld-Konfigurationen**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie im Formular die Felder aus.

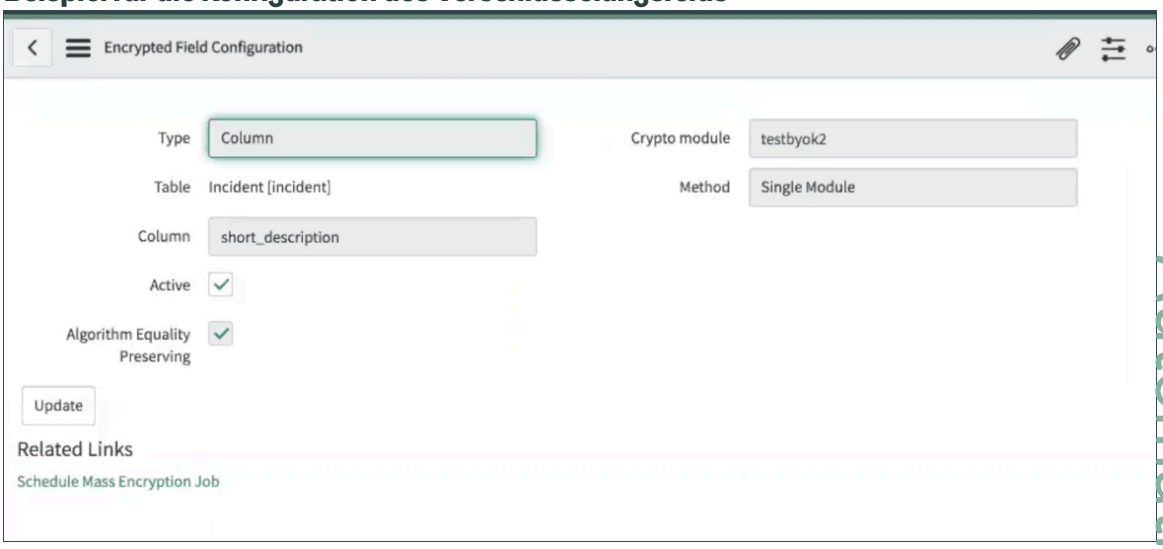
Verschlüsseltes Feldkonfigurationsformular

Feld	Beschreibung
Typ	**Spalte** Ist erforderlich, um Ihren persönlichen Schlüssel zu verwenden.
Tabelle	Tabelle, in der die vertraulichen Informationen gespeichert werden. Wählen Sie für dieses Beispiel aus **Incident [Incident]** .
Spalte	Spalte oder spezifische Informationen, die das zu verschlüsselnde vertrauliche Datum darstellt. Wählen Sie für dieses Beispiel aus **Short_description** .
Aktiv	Zu markierende Option **Aktiv** Dient zur Verwendung der Feldkonfiguration.
Algorithmusgleichstellung Beibehalten	Die Option ist automatisch ausgewählt.
Krypto-Modul	Modul, das Sie zur Verwendung mit dem persönlichen Schlüssel erstellt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Methode	Die **Einzelnes Modul** Die Option wird verwendet, um die Richtlinien für ein Modul anzuwenden. **Mehrere Module** Wird verwendet, um die Richtlinien auf mehrere Module anzuwenden.

Beispiel für die Konfiguration des Verschlüsselungsfelds



6. Klicken Sie auf **Absenden**.

Richten Sie eine Modulzugriffsrichtlinie ein, um Zugriff auf das kryptografische Modul zuzuweisen. Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

7. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > > **Neu erstellen** > **an.**
8. Füllen Sie im Formular die Felder aus.

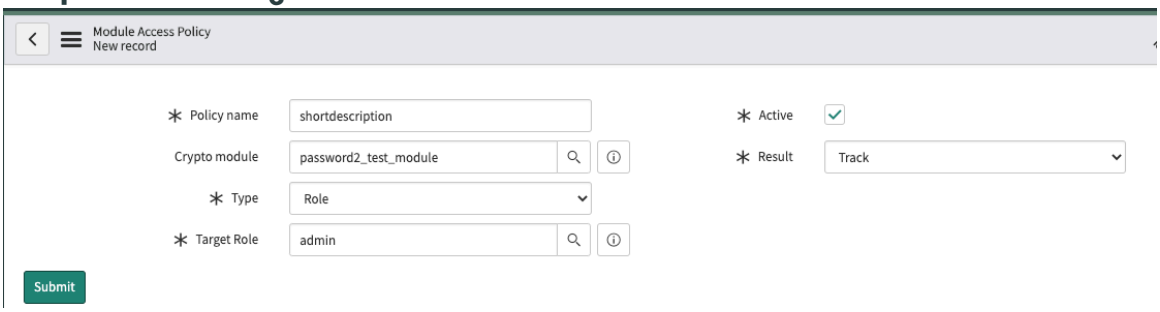
Formular für Modulzugriffsrichtlinie

Feld	Beschreibung
Richtlinienname	Name für die Richtlinie, z. B. Kurzbeschreibung .
Krypto-Modul	Krypto-Modul, das Sie zum Verschlüsseln Ihres Schlüssels erstellt haben.
Typ	Typ der Zugriffsbezeichnung für die Krypto-Richtlinie. Verwenden **Rolle** Um nur den Anwendern Zugriff auf das verschlüsselte Feld zu gewähren, die über die zugewiesene Rolle verfügen.
Zielrolle	Die Rolle, die Zugriff auf das verschlüsselte Feld hat. Wählen Sie für dieses Beispiel aus **Administrator** .
Aktiv	Option zum Aktivieren der Modulzugriffsrichtlinie.
Ergebnis	Die **Nachverfolgen** Mit der Option wird der Zugriff auf das Feld für die ausgewählte Rolle aktiviert. (Um den Zugriff auf dieses Feld für die ausgewählte Rolle einzuschränken, wählen Sie aus **Ablehnen** Oder **Strikte Ablehnung** .)

Automatische Übersetzung

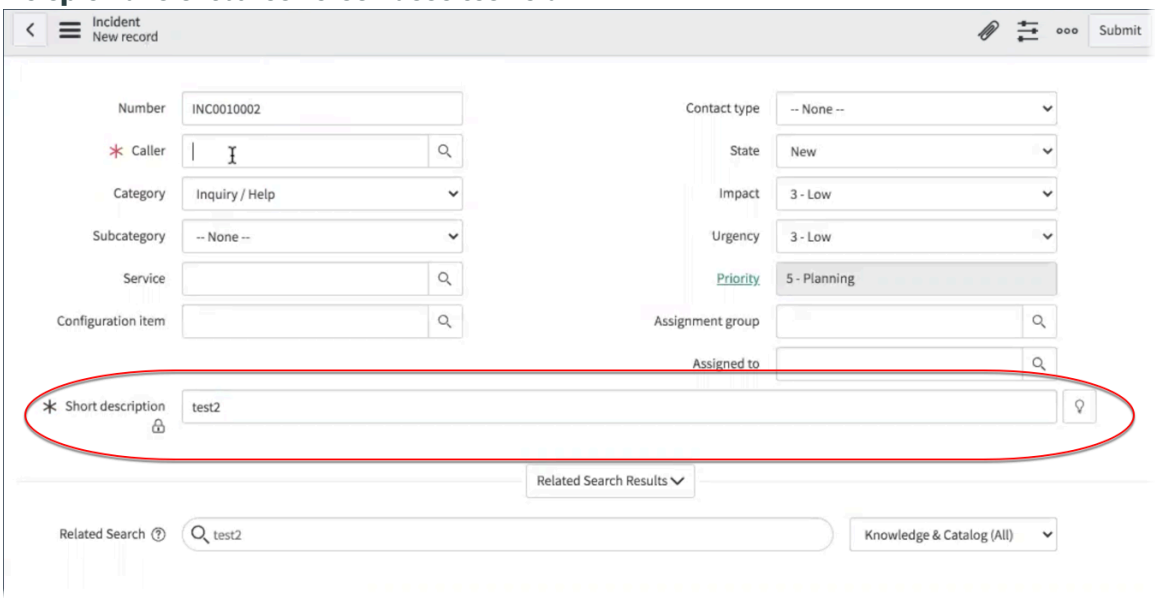
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Modulzugriffsrichtlinie



9. Klicken Sie auf **Absenden**.
10. Navigieren Sie als Anwender mit der Rolle sn_kmf.admin zu **Incident** > **Neu**an.

Beispiel für sichtbares verschlüsseltes Feld



Sie können jetzt das Feld Kurzbeschreibung basierend auf der Konfiguration der Modulzugriffsrichtlinie anzeigen.

Hinweis: Die Rolle sn_kmf.admin wurde Anwenderzugriff auf das verschlüsselte Feld Kurzbeschreibung gewährt, indem die Modulzugriffsrichtlinie auf festgelegt wurde **Nachverfolgen**. Beachten Sie das Sperrsymbol ( ) Unter dem Feldnamen, der angibt, dass das Feld ein verschlüsseltes Feld ist.

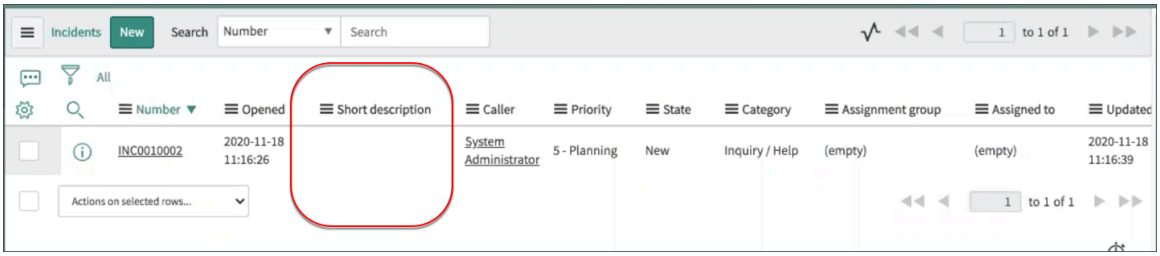
Sie können jetzt auf zugreifen **Incidents** Modul als Endanwender zum Testen der Konfiguration des verschlüsselten Felds.

11. Melden Sie sich als Anwender an, damit die verschlüsselten Daten im Feld „konfiguriert“ nicht angezeigt werden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselte Daten auf Feldebene



Wenn Sie auf die Incident-Nummer zugreifen, sind die Daten in der Kurzbeschreibung nicht sichtbar.

Ergebnis

Sie haben Ihren symmetrischen Schlüssel erfolgreich verwendet, um den Zugriff auf ein bestimmtes Feld mit zu steuern Feldverschlüsselung Enterprise.

Walkthrough zur Anhangsverschlüsselung

Diese Walk-through zeigt Ihnen, wie Sie einen Anhang in Ihrer Instanz mit verschlüsseln Feldverschlüsselung Enterprise Mit Key Management Framework(KMF). Außerdem erfahren Sie, wie Sie Ihren eigenen Schlüssel verwenden.

Vorbereitungen

Hinweis: Dieses Verfahren gilt nur für Feldverschlüsselung Enterprise Funktionalität. Siehe Feldverschlüsselung aktivieren Weitere Informationen zum Abrufen von Feldverschlüsselung Enterprise.

Erforderliche Rolle: Kryptografischer kmf-Manager

Warum und wann dieser Vorgang ausgeführt wird

Diese Walkthrough beginnt mit einer Instanz, in der Sie Ihren vom Kunden bereitgestellten kryptografischen Schlüssel bereits erstellt und hochgeladen haben. Sie könnten den Schlüssel verwenden, aber in diesem Beispiel wird ein vom Kunden bereitgestellter Schlüssel verwendet.

Laden Sie vertrauliche Anhänge in Ihre Instanz hoch, und beschränken Sie den Zugriff bestimmter Anwender. Verwenden Sie die verschlüsselte Feldkonfiguration, um anzugeben, welche autorisierten Mitarbeiter auf vertrauliche Daten zugreifen können.

Wir zeigen Ihnen, wie Sie Anhänge so verschlüsseln, dass sie nur für Anwender sichtbar sind, denen Zugriff gewährt wird, oder für alle Anwender sichtbar sind, die nicht an der Anzeige der Daten gehindert sind. In diesem Beispiel beschränken wir eine bestimmte Rolle davon, auf einen Anhang in zuzugreifen **Incidents** Modul.

Hinweis: Obwohl Sie mehrere Module mit verwenden können Feldverschlüsselung Enterprise, Die Anhangsverschlüsselung muss einzelne Module verwenden.

Prozedur

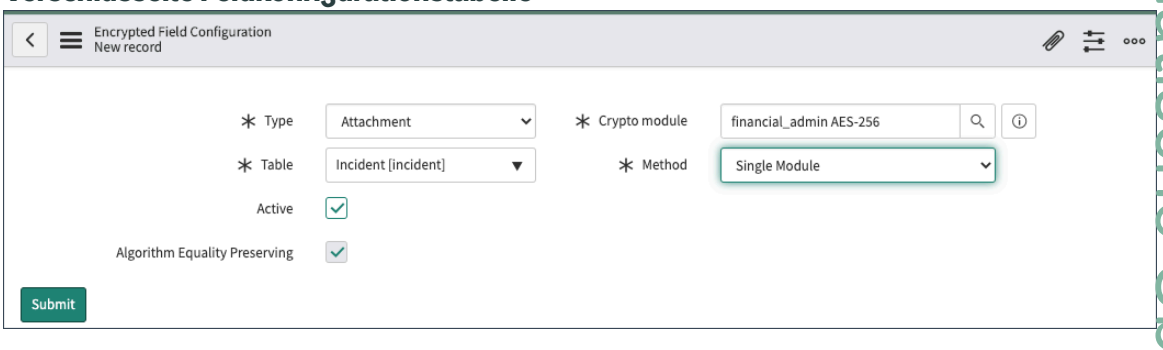
1. Stellen Sie sicher Feldverschlüsselung Enterprise Ist aktiviert.
2. Erstellen Sie ein kryptografisches Modul.
   Weitere Informationen finden Sie unter Erstellen Sie ein kryptografisches Modul für Feldverschlüsselung.
3. Navigieren zu **Systemsicherheit** > **Verschlüsselungsfeld-Konfigurationen**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie das Formular aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselte Feldkonfigurationsfelder

Feld	Beschreibung
Typ	Wählen Sie Aus **Anhang** Dient zur Verwendung Ihres persönlichen Schlüssels zum Verschlüsseln eines Anhangs aus dem ausgewählten **Tabelle** Wählen Sie für dieses Beispiel aus **Incident** .
Tabelle	Wählen Sie die Tabelle aus, um auf die vertraulichen Informationen zuzugreifen. Wählen Sie für dieses Beispiel aus **Incident [Incident]** .
Aktiv	Markieren **Aktiv** Um die Feldkonfiguration verwenden zu können.
Algorithmusgleichstellung Beibehalten	Bei Auswahl von Feldverschlüsselung Enterprise, Dieses Feld ist basierend auf der ausgewählten Tabelle sichtbar.
Krypto-Modul	Wählen Sie das Modul aus, das Sie zur Verwendung mit dem persönlichen Schlüssel erstellt haben.
Methode	Die **Einzelnes Modul** Die Option wird verwendet, um die Richtlinien für ein Modul anzuwenden. **Mehrere Module** Wird verwendet, um die Richtlinien auf mehrere Module anzuwenden.

Verschlüsselte Feldkonfigurationstabelle



6. Klicken Sie auf **Absenden**.

Richten Sie eine Modulzugriffsrichtlinie ein, um Zugriff auf das kryptografische Modul zuzuweisen. Siehe Erstellen Sie eine Modulzugriffsrichtlinie Für zusätzliche Informationen.

7. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**an.
8. Klicken Sie auf **Neu**.
9. Füllen Sie das Formular aus:

Felder für Modulzugriffsrichtlinie

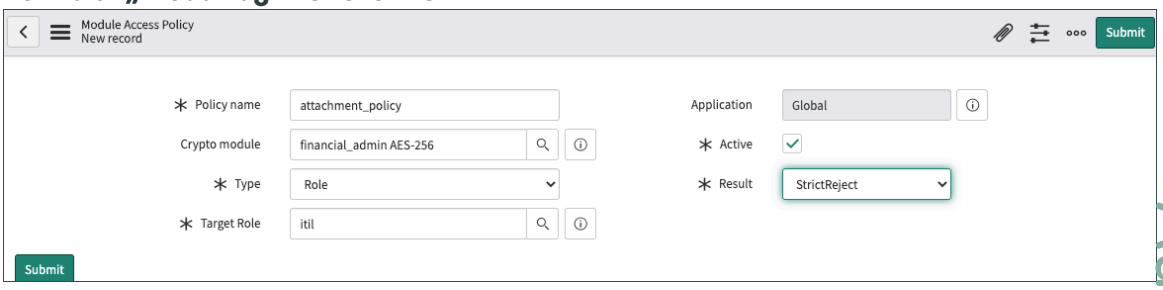
Feld	Beschreibung
Richtlinienname	Geben Sie einen Namen für die Richtlinie ein, z. B. „Anhangrichtlinie“.
Krypto-Modul	Wählen Sie das Krypto-Modul aus, das Sie zum Verschlüsseln Ihres Schlüssels erstellt haben.
Typ	Wählen Sie Aus **Rolle** Dient zum Einschränken des Zugriffs auf das verschlüsselte Feld von Anwendern mit der zugewiesenen Rolle.
Zielrolle	Wählen Sie die Rolle aus, die keinen Zugriff auf das verschlüsselte Feld hat. Wählen Sie für dieses Beispiel aus **itil** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

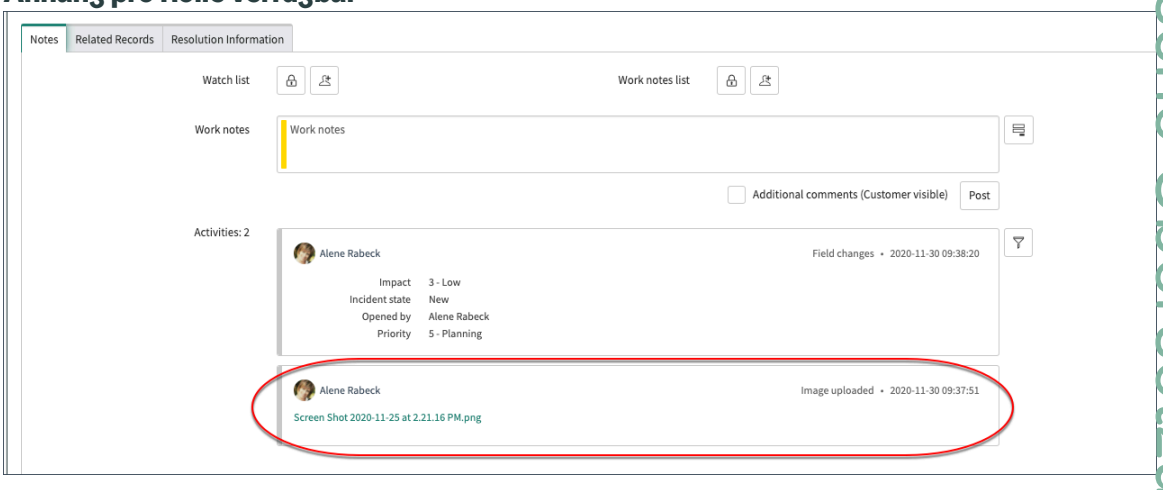
Feld	Beschreibung
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Modulzugriffsrichtlinie verwenden zu können.
Ergebnis	Wählen Sie Aus **Strikte Ablehnung** Dient zum Steuern des Zugriffs auf den Anhang von der ausgewählten Rolle. (Um Zugriff für die ausgewählte Rolle zu gewähren, wählen Sie aus **Nachverfolgen** .)

Formular „Modulzugriffsrichtlinie“



10. Klicken Sie auf **Absenden**.
11. Navigieren Sie als Administrator oder als Person, die den Incident erstellt hat, zu **Incidents** Und fügen Sie einen Anhang zu hinzu **Aktivitäten** Auf der **Notizen** Zugehörige Liste.

Anhang pro Rolle verfügbar



12. Melden Sie sich als Anwender an, der den Zugriff auf den verschlüsselten Anhang eingeschränkt hat.
13. Öffnen Sie den Incident, und scrollen Sie zu **Aktivitäten:** Abschnitt.
    Der Link zum Öffnen des Anhangs ist für Anwender mit der eingeschränkten Rolle nicht zugänglich.
14. Sie haben jetzt erfolgreich Ihren vom Kunden bereitgestellten Schlüssel verwendet, um den Zugriff auf einen bestimmten Anhang mit zu steuern Feldverschlüsselung Enterprise.

Feldverschlüsselung Enterprise

Feldverschlüsselung Enterprise Verwendet Key Management Framework(KMF), damit Sie anpassen und verwalten können, wie Felder und Anhänge in Ihrer Instanz verschlüsselt und entschlüsselt werden. Zur Verwendung ist ein Abonnement erforderlich Feldverschlüsselung Enterprise.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: In diesem Thema wird die Enterprise-Version von behandelt Feldverschlüsselung. Für Informationen zur Standardversion von Feldverschlüsselung, Oder Informationen zu den Unterschieden zwischen den beiden Versionen finden Sie unter Feldverschlüsselung erkunden.

Feldverschlüsselung Enterprise Ist mit begründet Feldverschlüsselung Und verwendet Key Management Framework Und seine volle Unterstützung wichtiger Verwaltungsfunktionen. Feldverschlüsselung Enterprise Bietet Schlüsselschutz und Schlüssellebenszyklusmanagement für die Feldverschlüsselung auf Anwendungsebene. Alle Schlüssel werden mit einer Schlüsselhierarchie geschützt, die letztendlich in FIPS (Federal Information Processing Standards) 140-2-L3 Hardware Security Modules (HSM) verwurzelt ist.

Feldverschlüsselung Enterprise Ermöglicht Ihnen, zu verwalten, wie unterstützte Felder gemäß verschlüsselt und entschlüsselt werden NIST 800-57 Praktiken. Außerdem wird die aktuellste Version der Verschlüsselung auf Feldebene verwendet, einschließlich Integration für ordnungsgemäßen Schutz und Verwaltung von Schlüsseln.

Insbesondere Feldverschlüsselung Enterprise Verwendet KMF Verschlüsselungsmodule, die Ihnen mehr Kontrolle über die serverseitige Verschlüsselung gewähren. KMF Verifiziert den ordnungsgemäßen Schutz von Datenverschlüsselungsschlüsseln mithilfe der Schlüsselhierarchie und der Umschlagverschlüsselung. Ihre Instanz verschlüsselt Daten über von Ihnen konfigurierte kryptografische Module. Sie können für jedes Modul eine Zugriffsrichtlinie erstellen, dann kryptografische Spezifikationen und Zugriffsrichtlinien konfigurieren und die Steuerung des Schlüssellebenszyklus-Managements steuern.

Feldverschlüsselung Enterprise Unterstützt Modulzugriffsrichtlinien basierend auf:

- Umfang
- Rolle
- Skript
- Ressourcenaustausch
- Systemanwender

Weitere Informationen finden Sie unter Erstellen Sie eine Modulzugriffsrichtlinie.

Hinweis: Für Details zu den unterstützten Funktionen von Feldverschlüsselung Und wie Sie aktualisieren und abonnieren Feldverschlüsselung Enterprise Berechtigung siehe Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

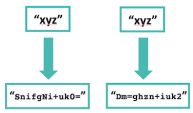
Verschlüsselungsbegriffe

Benennung	Beschreibung
Schlüsselverwaltung 	Unterstützung für Schlüsselverwaltung Grundlegend zu Feldverschlüsselung Enterprise Ist das Key Management Framework (KMF). Erhalten Sie die folgenden Fähigkeiten: • Key-Lebenszyklusmanagement. • Schlüsselrotation. Details siehe Schlüssel rotieren. • Schlüsselschutz und Schlüsselgenerierung mit FIPS 140-2-L3 Hardware Security Modules (HSMs).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benennung	Beschreibung
	• Trennung von Rollen und Aufgaben. • Die sichere Übertragung von Datenverschlüsselungsschlüsseln zwischen Instanzen, z. B. Produktions- und nicht-Produktionsinstanzen. • Vom Kunden bereitgestellte Schlüssel (CSK) mit Schlüsselumwicklung. • Nicht deterministische Verschlüsselung. • Massenverschlüsselung/-Entschlüsselung. • Audit des Schlüsselzugriffs/der Schlüsselverwendung. Details siehe Key Management Framework-Referenz.
Vom Kunden bereitgestellter Schlüssel  	Support für vom Kunden bereitgestellte Schlüssel Einer der größten Vorteile von Feldverschlüsselung Enterprise Ist, dass Sie eigene Schlüssel für die Verschlüsselung verwenden können. Administratoren können verwenden ServiceNow Bereitgestellte Schlüssel oder eigene vom Kunden bereitgestellte Schlüssel (CSK) für die Verschlüsselung auf dem ServiceNow AI Platform®. Sie können auch den Schlüssellebenszyklus verwalten und entscheiden, wann die Schlüssel widerrufen, rotiert und deaktiviert werden sollen. Nachdem Sie vom Kunden bereitgestellte Schlüssel aktiviert und ein kryptografisches Modul erstellt haben, laden Sie ein Token und einen öffentlichen flüchtigen Schlüssel herunter. Sie verwenden das Token und den öffentlichen Schlüssel, um Ihren Schlüssel einzuschließen und dann in die Instanz hochzuladen. Informationen zur Verwendung von vom Kunden bereitgestellten Schlüsseln finden Sie unter Konfigurieren Sie die Feldverschlüsselungseinstellungen, um den Schlüsseltyp auszuwählen Und Mit vom Kunden bereitgestellte Schlüssel werden verwendet Feldverschlüsselung Enterprise.
Feldverschlüsselung 	Unterstützung für Feldverschlüsselung und Anhangsverschlüsselung Sowohl die Feldverschlüsselung als auch die Anhangsverschlüsselung verwenden kryptografische Module und Zugriffsrichtlinien über verschlüsselte Feldkonfigurationen. Das Formular „Konfiguration verschlüsselter Felder“ wird verwendet, um einen Verschlüsselungstyp von auszuwählen *Spalte* Oder *Anhang* Verschlüsselung. Siehe Legen Sie verschlüsselte Feldkonfigurationen fest Für weitere Informationen und unterstützte Feldtypen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benennung	Beschreibung
Nicht deterministische Verschlüsselung 	Unterstützung für nicht deterministische Verschlüsselung Feldverschlüsselung Enterprise Unterstützt *Nicht deterministisch* Verschlüsselung für verbesserte Sicherheit. Wenn das System dieselben Daten mehrmals verschlüsselt, unterscheiden sich die Chiffriertexte jedes Mal. Die nicht deterministische Verschlüsselung ist mit der AES-Verschlüsselung (Advanced Encryption Standard) mit Cipher Block Chaining (CBC) verfügbar. Sie können diese Funktion über die Option Gleichheitserhaltung in der Phase „Algorithmusdefinition“ der kryptografischen Spezifikation aktivieren. Erstellen Sie eine kryptografische Spezifikation für ein Krypto-Modul, definieren Sie einen Algorithmus für die Verschlüsselung, und generieren Sie den Schlüssel. Siehe Erstellen Sie ein kryptografisches Modul Zum Definieren der Mechanismen, die für kryptografische Vorgänge verwendet werden, und für weitere Informationen zum Aktivieren der nicht deterministischen Verschlüsselung.
Ressourcenaustausch 	Ressourcenaustausch Feldverschlüsselung Enterprise Schlüsselinstanz für Instanz auf sichere Weise mit verwenden KMF Kryptografische APIs zur Bereitstellung von Vertraulichkeit, Integrität, Authentifizierung und Nichtwiderrede. Ressourcenaustausch Ist ein KMF Funktion, mit der Sie Ressourcen zwischen Instanzen sicher austauschen können. Details siehe Key-Management-Framework-Ressourcenaustausch.

Hinweis: Wenn Sie nicht aktivieren möchten Feldverschlüsselung Enterprise, Können Sie weiterhin verwenden Feldverschlüsselung. Siehe Feldverschlüsselung erkunden Für Informationen.

Feldverschlüsselung Enterprise Unterstützt lokale Kunden. Domänentrennung wird nicht unterstützt.

Unterstützung für zusätzliche verschlüsselte Felder

Die Standardversion von Feldverschlüsselung Ist auf fünf verschlüsselte Spalten beschränkt. Feldverschlüsselung Enterprise Unterstützt eine unbegrenzte Anzahl verschlüsselter Spalten.

Unterstützte Feldinformationen

Die folgenden Feldtypen können verschlüsselt werden:

- Anhänge
- Datum
- Datum/Uhrzeit
- E-Mail
- HTML

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Journal
- Journaleingabe
- Journalliste
- Telefon
- Zeichenfolgentext
- Übersetztes Feld
- Übersetzte HTML
- Übersetzter Text
- URL

Anhangsverschlüsselung

Anhangsverschlüsselung standardmäßig

Kunden, die verwenden Feldverschlüsselung Anhänge werden standardmäßig in Tabellen verschlüsselt, die den aktiven EFC-Typ (Encrypted Field Configuration) haben `Attachment`.

Diese durch die EFC-Konfiguration definierte Standardverschlüsselung bedeutet, dass Administratoren nicht manuell deklarieren müssen, dass ein Anhang beim Hochladen für diese Tabellen verschlüsselt werden soll.

Administratoren können Anwendern das Anhängen unverschlüsselter Dateien verhindern

Details finden Sie unter Verhindern Sie, dass Anwender unverschlüsselte Dateien anhängen.

Deaktivieren Sie die Standardverschlüsselung

Wenn Anhänge nicht standardmäßig basierend auf der EFC-Konfiguration verschlüsselt werden sollen, können Sie diese Option deaktivieren, indem Sie sich an wenden ServiceNow Support.

Um diese Funktion zu deaktivieren, erstellen Sie einen Supportfall mit ServiceNow Unterstützen und diese Aussage in einen Kommentar zum Falldatensatz einfügen:

„Ich [Kundenname] habe verstanden, dass ich Frage ServiceNow Deaktivieren einer empfohlenen Best Practice für Sicherheit für Anhänge und die [Kundenunternehmen] jedes zusätzliche Risiko im Zusammenhang mit der Konfiguration und Verwendung unverschlüsselter Anhänge in übernimmt ServiceNow Anwendung.“

API-Support

Feldverschlüsselung Enterprise Aktualisiert `SetDisplayValue()` Und `SetValue()` APIs, damit sie verschlüsselte Daten für verschlüsselte Felder einfügen können. Es wird auch aktiviert `GetDisplayValue()` Und `GetValue()` Um Klartextwerte zurückzugeben.

Das folgende Skript veranschaulicht diese API-Änderungen, wenn die Kurzbeschreibung des Incidents verschlüsselt wird:

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

Bei Verwendung von `GetValue()` Um verschlüsselten Text zu erhalten, gibt Ihr Skript den verschlüsselten Text nicht mehr zurück. Ihr Skript gibt den nur-Text zurück, vorausgesetzt, der Anwender hat Zugriff auf das kryptografische Modul. `GetValue()` Gibt den verschlüsselten Text für Anwender zurück, die keinen Zugriff auf das kryptografische Modul haben.

Cloud-Verschlüsselung Mit Schlüsselverwaltung

ServiceNow® Cloud-Verschlüsselung Bietet verschlüsselten Speicher für die Datenbank mithilfe von Blockverschlüsselung zusammen mit verbesserter Schlüsselverwaltung. Cloud-Verschlüsselung Ist mit verfügbar ServiceNow® Abonnementpaket für Plattformverschlüsselung.

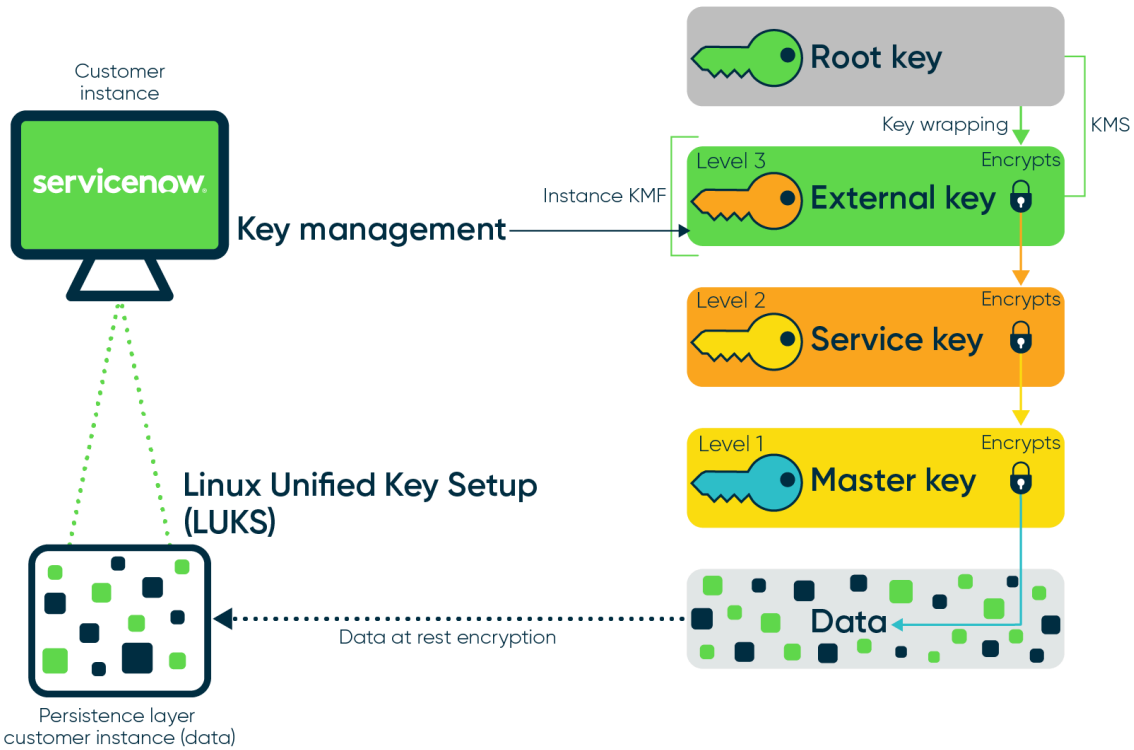
Cloud-Verschlüsselung Angebote:

- Aufgabentrennung.
- Rotation von ServiceNow Verwaltete Schlüssel.
- Vom Kunden verwaltete Schlüsseloption.

> **Hinweis:** Ziehen Sie diese Option in Betracht, wenn Ihre Organisation erfordert, dass Sie Schlüsselmaterial verwenden, das von Ihren eigenen kryptografischen Tools oder Bibliotheken, einem Enterprise Key Management System oder einem Hardware Security Module (HSM) generiert wurde. Details siehe Schlüsselverwaltungsvorgänge.

Das folgende Diagramm zeigt, wie Cloud-Verschlüsselung Funktioniert.

Cloud-Verschlüsselung – Übersicht



Die Cloud-Verschlüsselung Das Schlüsselverwaltungsmodul besteht aus den folgenden Untermodulen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schlüsselverwaltungsvorgänge:
  - Greifen Sie auf die Liste der Schlüssel zu.
  - Führen Sie Schlüsselrotationsvorgänge aus.
  - Ziehen Sie den vom Kunden verwalteten Schlüssel zurück.
- Schlüsselverwaltungstransaktionen:

  Referenzieren Sie alle Transaktionen, die für die verwendeten Schlüssel aufgetreten sind.

  Verwenden Sie Ihren eigenen vom Kunden verwalteten Schlüssel für die Verschlüsselung.

Unter bestimmten Umständen können Sie sich für eine Anforderung zum Zurückziehen des Schlüssels entscheiden, wenn Sie einen vom Kunden verwalteten Schlüssel verwenden. Dazu müssen Sie die optionale Add-on-SKU „Cloud Encryption zurückziehen und neu bereitstellen“ lizenzieren und dann anfordern, dass die Schlüsselwiderrufungsfunktion von aktiviert wird Kundenservice und Support Teammitglied.

Die Option Einstellungen für Quorum-Steuerungsrichtlinie wird verfügbar, wenn die Rückzugsfunktion aktiviert ist. Andernfalls ist das Modul nicht im Menü sichtbar. Diese Funktion kann nur aktiviert werden, wenn vom Kunden verwaltete Schlüssel verwendet werden. Mit dieser Richtlinie können Einstellungen für die Quorum konfiguriert werden, wenn die Rückzugsfunktion aktiviert ist. Weitere Informationen zu dieser Funktion finden Sie unter Quorum-Steuerungsrichtlinie.

Cloud-Verschlüsselung Unterstützt Produktions- und nicht-Produktionsinstanzen für MariaDB- und RaptorDB-Datenbanken. Cloud Encryption wird in unterstützt ServiceNow Commercial Cloud, Government Customer Cloud (GCC) Pod 101 und ServiceNow Geschützte Plattform – Australien (SPP-AU).

Lizenzierung und Aktivierung Cloud-Verschlüsselung

Für Informationen zur Lizenzierung Cloud-Verschlüsselung, Siehe Abonnementpaket für Verschlüsselung und Schlüsselverwaltung.

Für lizenzierte Kunden mit neuen Instanzen umfasst die neue Instanzbereitstellung Cloud-Verschlüsselung.

Für lizenzierte Kunden mit vorhandenen Instanzen, um anzufordern, dass eine Instanz nach verschoben wird Cloud-Verschlüsselung, Befolgen Sie die Anweisungen in KB1117369 . Sie müssen über die Rolle „Kundenadministrator“ oder „Partneradministrator“ verfügen, um das Servicekatalogelement anzufordern, um die Cloud-Verschlüsselung in Ihrer Instanz zu aktivieren. Das Aktivieren dieser Funktion erfordert ein einstündiges Wartungsfenster.

Cloud Encryption-UI

Wenn Cloud Encryption aktiviert ist, ist die Cloud Encryption-Anwenderoberfläche (UI) für den Anwender Security_admin sichtbar, wenn dieser Anwender die Rolle sn_kmf.admin hat.

Dient zum Zugreifen auf die Cloud Encryption-UI durch Suchen nach **Cloud-Verschlüsselungsschlüsselverwaltung** In der Navigationsleiste. Navigieren Sie zu **Schlüsselverwaltungsvorgänge** Abschnitt, in dem Informationen zu Verschlüsselungsschlüsseln angezeigt werden, z. B. Details zum aktiven Schlüssel und ob Cloud Encryption für die Instanz aktiviert ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselverwaltungsvorgänge

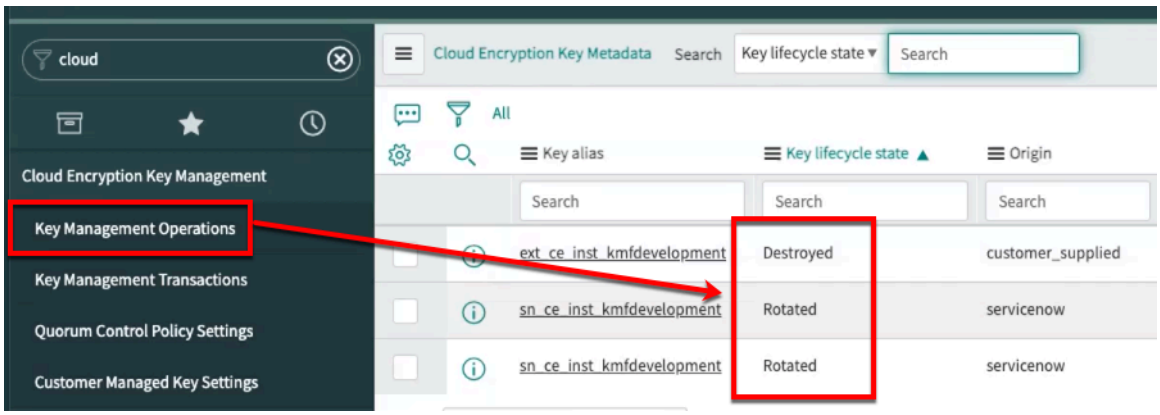
Das Untermodul „Schlüsselverwaltungsvorgänge“ bietet Zugriff zum Anzeigen und Verwalten aller mit verwendeten Verschlüsselungsschlüssel ServiceNow Cloud-Verschlüsselung.

Erste Schritte mit Cloud Encryption

status des Schlüssellebenszyklus

Im System ist jeweils nur ein aktiver Schlüssel vorhanden. Wenn Sie einen Schlüssel auswählen, greifen Sie auf die Aktivität für den ausgewählten Schlüssel zu, z. B. welche Schlüssel gedreht oder zurückgezogen wurden, und den entsprechenden Zeitstempel.

Der Status des Schlüssellebenszyklus wird entsprechend dem durchgeführten Schlüsselverwaltungsvorgang aktualisiert.



Siehe Rotieren Sie einen von ServiceNow verwalteten Schlüssel Oder Rotieren Sie einen vom Kunden verwalteten Schlüssel Für Details.

Hinweis: Der Schlüsselrotationsprozess kann bis zu 20 Minuten dauern.

Rotieren Sie einen von ServiceNow verwalteten Schlüssel

Rotieren Sie den aktiven Cloud-Verschlüsselung ServiceNow Verwalteter Schlüssel.

Vorbereitungen

Erforderliche Rollen: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Wichtig: Wenn Sie vom Kunden verwaltete Schlüssel verwenden, finden Sie weitere Informationen unter Rotieren Sie einen vom Kunden verwalteten Schlüssel.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**an.
   Die Cloud-Verschlüsselung Schlüsselmetadatenliste wird geladen. Alle in Ihrer Instanz verwendeten Schlüssel werden aufgelistet. Es kann jeweils nur ein Schlüssel aktiv sein.

   Wenn Sie auf zugreifen Cloud-Verschlüsselung Modul zum ersten Mal sind Schlüsseleinträge verfügbar, nachdem eine erste Schlüsselrotation durchgeführt wurde. A ServiceNow Verwalteter Schlüssel ist der Standard im System.

2. Wählen Sie den aktiven Schlüssel aus der Tabelle aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Tabelle „Schlüsseldefinition“ wird mit allgemeinen Informationen zu angezeigt ServiceNow Generierter Schlüssel.

3. Wählen Sie aus **Schlüssel Rotieren** Schaltfläche.
   Eine Benachrichtigung wird mit der Option angezeigt, die Schlüsselrotation fortzusetzen oder den Vorgang abzubrechen.
4. Wählen Sie Aus **OK** Zum Drehen des Schlüssels.
   Oben auf der Seite „Schlüsseldefinition“ wird eine Bestätigungsmeldung angezeigt.
5. Kehren Sie zum Bildschirm „Key Management Operations“ zurück, um zu aktualisieren Cloud-Verschlüsselung Schlüsselmetadatentabelle.
   Einträge werden für den aktuell aktiven Schlüssel und den Schlüssel aufgelistet, der generiert wird, um anstelle des aktuell aktiven Schlüssels zu rotieren. Siehe schlüssellebenszyklusstatus des Key Management Framework Für die verschiedenen verfügbaren status.

   Der aktive Schlüssel wird mit einer Schlüsselversion von aufgeführt `0` Und der generierte Schlüssel hat eine Version von `1` .
6. Öffnen Sie den Eintrag für den ursprünglichen Schlüssel, um die Schlüsselverwaltungstransaktionen anzuzeigen.
   Weitere Informationen finden Sie unter Schlüsselverwaltungstransaktionen Weitere Informationen finden Sie unter .
   Der zuvor aktive Schlüssel, Version `0` , Wurde auf den Status des Schlüssellebenszyklus von aktualisiert `Rotiert` Und der neue Schlüssel, Version `1` Ist `Aktiv` .

Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor

Führen Sie die folgenden Schritte aus, um Ihren vom Kunden verwalteten Schlüssel für den Upload in Ihre Instanz vorzubereiten.

Vorbereitungen

Erforderliche Rollen: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Warum und wann dieser Vorgang ausgeführt wird

Für einen vom Kunden verwalteten Schlüssel können Sie eine beliebige kryptografische Bibliothek oder HSM verwenden, um Ihren Schlüssel zu generieren. Dieser Schlüssel muss ein AES-256-Bit-Schlüssel sein und von einem Cloud Encryption-Wrapping-Zertifikat mit einem RSAES_OAEP_SHA_256-Verschlüsselungsschema umwickelt werden.

Hinweis:

Wenn Sie das kryptografische OpenSSL-Tool zum Generieren Ihres Schlüssels verwenden, muss die OpenSSL-Version Version Version 1,1.1x oder höher sein.

Wenn Sie Ihren vom Kunden verwalteten Schlüssel mit erstellen und umschließen Windows, Sie müssen den umschlossenen Schlüssel über Bash-Shell-Supportanwendungen wie Git Bash generieren.

Prozedur

1. Generieren Sie einen zufälligen Wert, der als symmetrischer AES-256-Bit-Schlüssel mit OpenSSL verwendet werden soll.

   Mit OpenSSL können Sie diesen Schlüssel beispielsweise mit generieren `openssl-Rand 32` Befehl.

   Aus Kompatibilitätsgründen muss Ihr symmetrischer Schlüssel die folgenden Attribute aufweisen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Wert
Schlüsseltyp	AES-Algorithmus (Advanced Encryption Standard) – basierter symmetrischer Schlüssel.
Schlüsselgröße	256 Bit (32 Byte)
Schlüsselumschließungsanforderung	○ RSA-Verschlüsselungsalgorithmus ○ Optimaler asymmetrischer Verschlüsselungsabstand (OAEP) ○ SHA-256-Hash-Funktion (RSAES_OAEP_SHA_256) ○ Codiert mit Base64-Algorithmus

2. Speichern Sie den Schlüssel in einer Datei.
   Zum Beispiel der OpenSSL-Befehl `openssl-Rand 32 > plaintext_key.bin` Generiert einen 32-Byte-Schlüssel und speichert ihn in einer Datei mit dem Namen `plaintext_key.bin` .

   Wichtig: Speichern Sie diese Datei zur späteren Referenz sicher. Dieser Schlüssel wird mit dem öffentlichen Schlüssel zum Hochladen umschlossen.

3. Extrahieren Sie den öffentlichen Schlüssel aus der heruntergeladenen Wrapping-Zertifikatdatei aus Ihrer Instanz:

   ```
   openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
   ```

   Hinweis: Informationen zum Herunterladen des Wrapping-Zertifikats finden Sie unter .

4. Umschließen Sie den generierten Schlüssel mit dem öffentlichen Schlüssel, der mit dem umschließenden Zertifikat heruntergeladen wurde, mithilfe des Algorithmus RSAES_OAEP_SHA_256:

   ```
   cat plaintext_key.bin | openssl pkeyutl -encrypt -inkey public_key.pem -pubin -pkeyopt
    rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 | openssl base64 -A -out
    wrapped_key.txt
   ```

   Eine in diesem Befehl angegebene Datei enthält einen umschlossenen vom Kunden verwalteten Schlüssel, der SN für den CMK-Prozess bereitgestellt werden kann.

Wechseln Sie zwischen ServiceNow- und vom Kunden verwalteten Schlüsseln

Wechseln Sie zwischen vom Kunden verwaltetem Schlüssel oder einem ServiceNow Verwaltete Schlüssel zur Verwendung in ServiceNow Cloud-Verschlüsselung.

Standardmäßig ist Ihre Instanz für die Verwendung konfiguriert ServiceNow Verwaltete Schlüssel, und ServiceNow Die Generierung des Verschlüsselungsschlüssels ist aktiv. Administratoren können jedoch vom Kunden verwaltete Schlüssel verwenden. Sie können auch zu zurückkehren ServiceNow Verwaltete Schlüssel.

Rotieren Sie einen vom Kunden verwalteten Schlüssel

Rotieren Sie Ihren vom Kunden verwalteten Schlüssel in Ihre Instanz, nachdem Sie Ihren vom Kunden verwalteten Schlüssel für eingepackt haben Cloud-Verschlüsselung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rollen: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**an.
   Die **Cloud-Verschlüsselungsschlüsselmetadaten** Liste wird geladen. Alle Schlüssel, die in Ihrer Instanz verwendet wurden, werden aufgelistet.
2. In **Cloud-Verschlüsselungsschlüsselmetadaten** Liste öffnen Sie den Datensatz für Ihren aktiven Schlüssel.
   Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel aus, der einen hat **Status des Schlüssellebenszyklus** Von `Aktiv` . In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. Wählen Sie im Schlüsseldefinitionsdatensatz die aus **Schlüssel Rotieren** Schaltfläche.
4. In **Vom Kunden verwalteten Schlüssel hochladen** Fenster Führen Sie die aufgeführten Schritte aus.

   a. Wählen Sie Aus **Wrapping-Zertifikat Herunterladen** .
   Die *`public_certificate....zip`* Lädt auf Ihren lokalen Computer herunter und wird zum Umschließen des vom Kunden verwalteten Schlüssels verwendet.

   > ⚠ **Warnung:** Vermeiden Sie potenzielle zertifikatbezogene Probleme, indem Sie das umschließende Zertifikat jedes Mal herunterladen, wenn Sie zu einem vom Kunden verwalteten Schlüssel wechseln oder zu einem vom Kunden verwalteten Schlüssel wechseln.

   b. Wählen Sie Aus **Durchsuchen** Um Ihren vom Kunden verwalteten Schlüssel hochzuladen, suchen und wählen Sie Ihren umschlossenen Verschlüsselungsschlüssel aus.
   Um eine andere Datei auszuwählen, wählen Sie die Datei aus, und wählen Sie aus **Entfernen** .

   c. Schließen Sie das Fenster „Anhänge“.

   d. Wählen Sie Aus **OK** Um Ihren Schlüssel hochzuladen.
   Wenn der Schlüssel das richtige Format hat, wird eine Bestätigungsmeldung angezeigt. Andernfalls wird eine Fehlermeldung angezeigt. Die Schlüsseldatei wird an den Schlüsseldefinitionsdatensatz angehängt.

   In der Tabelle „Schlüsselverwaltungstransaktionen“ werden die Schritte zum Herunterladen des Zertifikats und zum Hochladen von Schlüsseln aufgeführt. Siehe Schlüsselverwaltungstransaktionen Für Details zu den Anforderungsschritten.

5. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** Um die Liste der Schlüssel anzuzeigen.
   In der Liste der Schlüssel wird ein neuer Datensatz für Ihren vom Kunden verwalteten Schlüssel angezeigt. Dieser neue Schlüssel hat einen **Ursprung** Wert von **Customer_provided** Und befindet sich in **Aktiv** status. Ihr vorheriger Schlüssel befindet sich in **Rotiert** status.

Wechseln Sie zu einem vom Kunden verwalteten Schlüssel

Verwenden Sie Ihren vom Kunden verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Um zu einem vom Kunden verwalteten Schlüssel zu wechseln, müssen Sie einen umwickelten vom Kunden verwalteten Schlüssel haben, der im Rahmen dieser Schritte hochgeladen werden kann. Details zur Vorbereitung dieses Schlüssels für den Upload finden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie unter Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor. Nach dem Hochladen Ihres Schlüssels initiiert dieser Prozess eine Schlüsselrotation zu Ihrem neuen Schlüssel.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**an.
2. In **Cloud-Verschlüsselungsschlüsselmetadaten** Liste öffnen Sie den Datensatz für Ihren aktiven Schlüssel.
   Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel aus, der einen hat **Status des Schlüssellebenszyklus** Von Aktiv . In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. In **Zugehörige Links** Wählen Sie im Abschnitt des Formulars aus **Wechseln Sie Zum Vom Kunden Verwalteten Schlüssel** Link.
4. In **Wechseln Sie zum vom Kunden verwalteten Schlüssel** Wählen Sie das Dialogfeld aus **Verwalteten Schlüssel Hochladen** Schaltfläche.
5. In **Vom Kunden Verwalteten Schlüssel Hochladen** Dialogfeld führen Sie die aufgeführten Schritte aus.

   a. Wählen Sie Aus **Wrapping-Zertifikat Herunterladen** .

   > ⚠ **Warnung:** Vermeiden Sie potenzielle zertifikatbezogene Probleme, indem Sie das umschließende Zertifikat jedes Mal herunterladen, wenn Sie zu einem vom Kunden verwalteten Schlüssel wechseln oder zu einem vom Kunden verwalteten Schlüssel wechseln.

   b. Wählen Sie Aus **Durchsuchen** , Und befolgen Sie die Anweisungen, um Ihren Schlüssel von Ihrem Gerät auszuwählen und hochzuladen.

   c. Wählen Sie Aus **Wechseln Sie zum vom Kunden verwalteten Schlüssel** .

   Eine Anforderung wird von der Instanz generiert, um zu Ihrem vom Kunden verwalteten Schlüssel zu wechseln. Im aktuellen Formular sehen Sie, dass **Schlüssel-Lebenszyklusstatus** Des ursprünglich aktiven Schlüssels hat sich in geändert **Rotiert** .
6. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** Um die Liste der Schlüssel anzuzeigen.
   In der Liste der Schlüssel wird ein neuer Datensatz für Ihren vom Kunden verwalteten Schlüssel angezeigt. Dieser neue Schlüssel hat einen **Ursprung** Wert von **Customer_provided** Und befindet sich in **Aktiv** status.

Ergebnis

Ihre Instanz verwendet jetzt Ihren vom Kunden verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

> ⓘ **Wichtig:** Stellen Sie sicher, dass eine Kopie Ihres Verschlüsselungsschlüssels für Schlüsselverwaltungsvorgänge immer an einem sicheren Ort verfügbar ist. Ohne diesen Schlüssel ist Ihre Instanz möglicherweise nicht zugänglich.

Wechseln Sie zu einem von ServiceNow verwalteten Schlüssel

Wechseln Sie von einem vom Kunden verwalteten Schlüssel zurück zu einem verwalteten Schlüssel für ServiceNow Cloud-Verschlüsselung.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung**an.
2. In **Cloud-Verschlüsselungsschlüsselmetadaten** Liste öffnen Sie den Datensatz für Ihren aktiven Schlüssel.
   Wenn Sie mehrere Schlüssel haben, wählen Sie den Schlüssel aus, der einen hat **Status des Schlüssellebenszyklus** Von Aktiv . In Ihrer Instanz ist nur ein aktiver Schlüssel vorhanden.
3. In **Zugehörige Links** Wählen Sie im Abschnitt des Formulars aus **Wechseln Sie zum von ServiceNow verwalteten Schlüssel** Link.
4. In **Wechseln Sie zum von ServiceNow verwalteten Schlüssel** Wählen Sie das Dialogfeld aus **Wechseln Sie zum von ServiceNow verwalteten Schlüssel** Schaltfläche.
   Eine Anforderung wird von der Instanz generiert, um zu wechseln ServiceNow Verwalteter Schlüssel. Im aktuellen Formular sehen Sie, dass **Schlüssel-Lebenszyklusstatus** Des ursprünglich aktiven Schlüssels hat sich in geändert **Rotiert** .
5. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Vorgänge der Schlüsselverwaltung** Um die Liste der Schlüssel anzuzeigen.
   In der Liste der Schlüssel wird ein neuer Datensatz für angezeigt ServiceNow Verwalteter Schlüssel ist . Dieser neue Schlüssel hat einen **Ursprung** Wert von **ServiceNow** Und befindet sich in **Aktiv** status.

Schlüsselrotation planen

Legen Sie einen Zeitplan für die automatische Rotation von fest ServiceNowVerwaltete Schlüssel. Bei diesem Prozess wird ein Verschlüsselungsschlüssel automatisch stillgelegt und der alte Schlüssel durch einen neu generierten kryptografischen Schlüssel ersetzt. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, kann dieser Zeitplan eine Erinnerung an die manuelle Rotation Ihrer anwenderdefinierten Schlüssel bereitstellen.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Einstellungen für geplante Schlüsselrotation**an.
2. Wählen Sie aus **Aktivieren Sie die geplante Schlüsselrotation** Kontrollkästchen.
3. Füllen Sie die verbleibenden Felder basierend auf Ihren Geschäftsanforderungen aus.

Einstellungen für geplante Schlüsselrotation

Feld	Beschreibung
Anzahl der Monate zwischen Schlüsselrotationen (maximal 60 Monate)	Anzahl der Monate zwischen Schlüsselrotationen. Dieser Wert ist 12 Standardmäßig und kann maximal betragen 60 Monate.
Wochentag für die Schlüsselrotation	Wochentag, an dem die Schlüsselrotation durchgeführt wird.
Uhrzeit für die Schlüsselrotation	Uhrzeit, zu der die Schlüsselrotation durchgeführt wird.
Datum und Uhrzeit der nächsten Schlüsselrotation	Datum und Uhrzeit der nächsten geplanten Schlüsselrotation. Dieser Wert kann nicht direkt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	bearbeitet werden und wird automatisch basierend auf Ihren Auswahlmöglichkeiten berechnet.
Angabe, wie viele Tage vor der Schlüsselrotation die Erinnerung gesendet werden soll (maximal 15 Tage)	Anzahl der Tage vor dem Datum Ihrer Schlüsselrotation, die Ihre Instanz Benachrichtigungen sendet.
E-Mail-Benachrichtigungen werden an die folgende Liste Ihrer genehmigten Sicherheitsadministratoren gesendet	Liste der Anwender, die Benachrichtigungen für die Schlüsselrotation erhalten. Die **Systemadministrator** Befindet sich standardmäßig in dieser Liste.

4. Wählen Sie **Absenden**.
   Nachdem Sie Absenden ausgewählt haben, wird oben im Formular eine Benachrichtigung angezeigt. Die Benachrichtigungen bestätigen Ihre Schlüsselrotation und den Benachrichtigungszeitplan.

⚠ Warnung:

Jede geplante Schlüsselrotation hat eine eindeutige Signatur, die die Integrität eines Auftrags sicherstellt und nicht autorisierte Änderungen erkennt. Die Signatur für eine geplante Aufgabe ist für jede Instanz eindeutig. Beim Klonen eines geplanten Schlüsselrotationsauftrags aus einer Quellinstanz A in eine Zielinstanz B schlägt die geplante Aufgabe in Instanz B fehl. In diesem Fall können Sie die Signatur erneut erstellen, indem Sie die Auswahl aufheben und dann erneut auswählen **Aktivieren Sie die geplante Schlüsselrotation** Kontrollkästchen. Weitere Informationen zu diesem Problem finden Sie unter KB1247113 .

Ziehen Sie einen vom Kunden verwalteten Schlüssel zurück

Nachdem die vom Kunden verwaltete Funktion zum Zurückziehen des Schlüssels aktiviert wurde, wird auf der Seite „Schlüsselverwaltungsvorgänge“ ein Widerrufsvorgang verfügbar. Die Vorgänge „Schlüssel zurückziehen“ und „Quorum-Genehmigung“ können ebenfalls verwaltet werden.

Vorbereitungen

Erforderliche Rollen: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Dieser Abschnitt gilt nur, wenn Sie eine lizenzierte Cloud Encryption-Bereitstellung zurückziehen und erneut bereitstellen, ein optionales Add-on für Cloud-Verschlüsselung.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > > **Vorgänge der Schlüsselverwaltung**an.
2. Wählen Sie den aktiven vom Kunden verwalteten Schlüssel aus der Tabelle aus.
   Die Tabelle „Schlüsseldefinition“ wird mit allgemeinen Informationen zu Ihrem Kundenschlüssel angezeigt. Eine Funktion zum Zurückziehen des Schlüssels ist jetzt verfügbar.
3. Wählen Sie aus **Schlüssel Zurückziehen** Zum Auslösen des Widerrufsvorgangs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

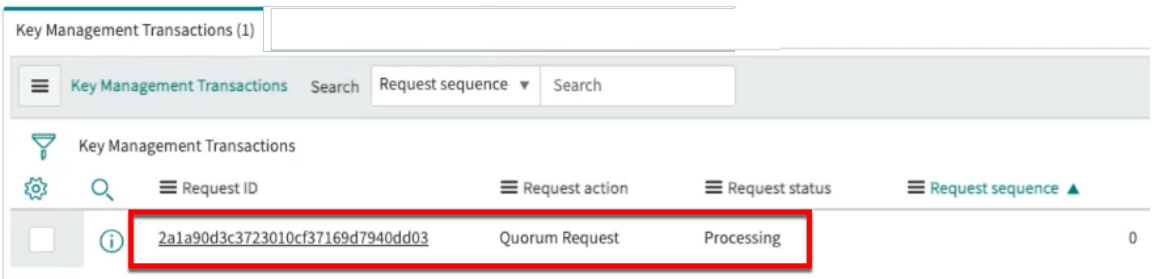
Warnung:

Eine Warnmeldung zum Zurückziehen des Schlüssels wird angezeigt. Das Zurückziehen des Schlüssels löst ein Herunterfahren Ihrer Instanz aus, bis ein Wiederherstellungsvorgang mit dem zurückgenommenen Schlüssel ausgeführt wird.

Gefahr: Sie können nur einen Wiederherstellungsvorgang mit demselben Schlüssel ausführen, der zurückgezogen wurde. Wenn Sie zu einem anderen Schlüssel rotieren möchten, müssen Sie dies tun, nachdem Sie den zurückgenommenen Schlüssel wiederhergestellt haben.

Wenn der zurückgenommene vom Kunden verwaltete Schlüssel nicht innerhalb des Zeitrahmens wiederhergestellt wird, für den er festgelegt wurde ServiceNow Behält Sicherungen bei (weitere Informationen finden Sie in der SOP „Sicherung und Wiederherstellung“ [Standard Operating Procedure]). Auf Ihre Instanzdatenbanksicherungen kann nicht mehr zugegriffen werden. Auf diese Weise verlorene Sicherungsdaten können nicht wiederhergestellt werden.

4. Wählen Sie Aus **OK** Zum Zurückziehen des Schlüssels.
   Wählen Sie Aus **Abbrechen** Wenn Zweifel an der Funktion zum Zurückziehen des Schlüssels bestehen. Sie kehren zum Bildschirm „Schlüsseldefinition“ zurück, und eine Bestätigungsmeldung wird angezeigt.
5. Aktualisieren Sie die Seite „Schlüsseldefinition“, um die ausstehende Widerrufsanforderung anzuzeigen.



Wenn die Quorum-Steuerungsrichtlinie aktiviert wurde, muss der Genehmigungs-Workflow erfolgreich abgeschlossen werden, um den Schlüsselzurückzug abzuschließen. Details siehe Verwalten Sie Die Quorum-Steuerung.

Stellen Sie einen vom Kunden verwalteten Schlüssel erneut bereit

Nach Abschluss eines Schlüsselrückzugsvorgangs muss Ihr vom Kunden verwalteter Schlüssel erneut in Ihre Instanz bereitgestellt werden.

Vorbereitungen

Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Hinweis: Dieser Abschnitt gilt nur, wenn Sie lizenzierte Cloud Encryption zurückziehen und erneut bereitstellen.

Prozedur

1. Wechseln Sie zu Now Support Und navigieren Sie zu **Servicekatalog** > **Katalog** > **Instanzenverwaltung** > **Instanzwiederherstellung: Verwalteten Schlüssel Erneut Bereitstellen**an.
2. Klicken Sie auf **Anforderung**.
3. In **Instanzwiederherstellung: Verwalteten Schlüssel Erneut Bereitstellen** Wählen Sie Ihre Instanz im aus **Wählen Sie Instanz Aus** Dropdown-Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Laden Sie das Wrapping-Zertifikat herunter, indem Sie auf klicken **Zertifikat wird umgebrochen** Text.

   ⚠ **Warnung:** Sie müssen jedes Mal ein neues Wrapping-Zertifikat herunterladen, wenn Sie einen vom Kunden verwalteten Schlüssel rotieren oder hochladen.

5. Bereiten Sie Ihren Schlüssel für den Upload vor.
   Details zu diesem Vorgang finden Sie unter Bereiten Sie Ihren vom Kunden verwalteten Schlüssel vor.

6. In **Schritt 4** Klicken Sie auf Abschnitt **Durchsuchen und hochladen** Um Ihren umschlossenen Schlüssel von Ihrem lokalen Gerät hochzuladen.
   Nachdem Ihr Schlüssel hochgeladen wurde, wird der Schlüssel unter angezeigt **Folgende Datei wurde erfolgreich hochgeladen** . Wenn Sie den Schlüssel erneut hochladen müssen, klicken Sie auf **Entfernen Sie die Datei** Und laden Sie Ihren Schlüssel erneut hoch, wie in den vorherigen Schritten beschrieben.

7. Klicken Sie Auf **Schlüssel drehen** Um die erneute Versorgung abzuschließen.

Quorum-Steuerungsrichtlinie

Die Quorum-Steuerungsrichtlinie gibt die Mindestanzahl der Genehmigungen an, die unter der Gesamtzahl der ausgewählten Genehmiger erforderlich sind, um das Quorum für den vom Kunden verwalteten Schlüssel zu erreichen.

⚠ **Warnung:** Sie müssen einen rechtlichen Nachtrag unterzeichnen, um die Funktion zum Zurückziehen des Schlüssels zu aktivieren. Die Option Einstellungen für Quorum-Steuerungsrichtlinie wird verfügbar, wenn die Rückzugsfunktion aktiviert ist. Andernfalls ist das Modul nicht im App-Menü sichtbar. Nach dem Zurückziehen des Schlüssels ist Ihre Instanz nicht mehr verfügbar, bis der Verschlüsselungsschlüssel erneut bereitgestellt wurde und wieder aktiv ist.

Unter bestimmten Umständen möchten Sie möglicherweise einen Schlüsselwiderruf erstellen. Sie müssen zuerst die Funktion zum Zurückziehen des Schlüssels von anfordern Kundenservice und Support.

Die Quorum-Steuerungsrichtlinie gibt die Mindestanzahl der Genehmigungen an, die unter der Gesamtzahl der ausgewählten Genehmiger erforderlich sind, um das Quorum für den vom Kunden verwalteten Schlüssel zu erreichen. Beispielsweise gibt es insgesamt fünf Genehmiger, aber nur vier Genehmigungen sind erforderlich, um das Quorum zu erreichen. Wenn vier Genehmigungen eingeholt werden, wird die Widerrufsanforderung verarbeitet und der Schlüssel zurückgezogen.

Immer wenn ein Rückzugsvorgang in einer Gruppe ausgeführt wird, die für die Quorum-Genehmigung aktiviert ist, wird ein Workflow für die Quorum-Genehmigung ausgelöst. Eine E-Mail-Benachrichtigung wird an alle Anwender gesendet, die die Genehmigung erteilen können. Aufgaben werden auch in den Accounts der Genehmiger generiert, die sie im Dashboard sehen, wenn sie sich bei anmelden ServiceNow Account.

Die Anwender können Genehmigungen über die Seite „Instanz“, „E-Mail“ oder „Schlüsselverwaltungsvorgänge“ erteilen. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erreicht ist.

Sobald die Mindestanzahl von Genehmigern erreicht ist, ist das Quorum erreicht, und der Schlüsselzurückzug wird ausgelöst. Der Widerruf wird durchgeführt und protokolliert, einschließlich der Namen der Anwender, die die Anforderung genehmigt haben.

Siehe Konfigurieren Sie Die Richtlinieneinstellungen Für Die Quorum-Steuerung Für Setup-Details.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Die Richtlinieneinstellungen Für Die Quorum-Steuerung

Führen Sie die folgenden Schritte aus, um die Richtlinieneinstellungen für die Quorum-Steuerung zu konfigurieren.

Vorbereitungen

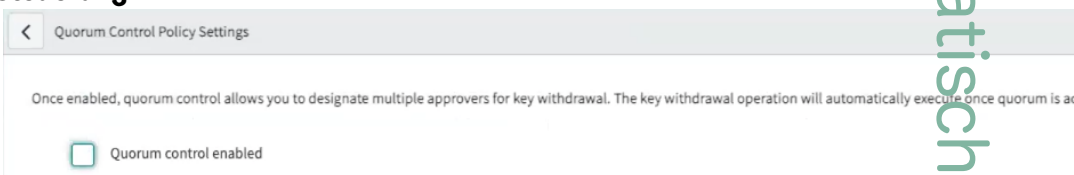
Erforderliche Rollen: sn_kmf.admin

Warum und wann dieser Vorgang ausgeführt wird

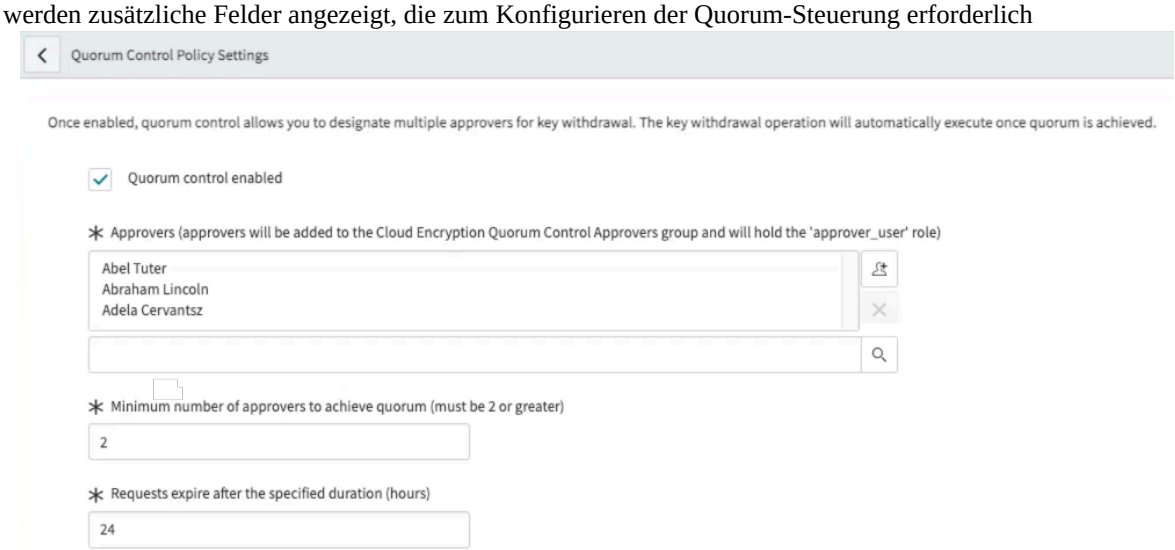
⚠ **Warnung:** Sie müssen einen rechtlichen Nachtrag unterzeichnen, um die Funktion zum Zurückziehen des Schlüssels zu aktivieren. Die Option Einstellungen für Quorum-Steuerungsrichtlinie wird verfügbar, wenn die Rückzugsfunktion aktiviert ist. Andernfalls ist das Modul nicht im App-Menü sichtbar. Nach dem Zurückziehen des Schlüssels ist Ihre Instanz erst verfügbar, wenn der Verschlüsselungsschlüssel erneut aktiv ist.

Prozedur

1. Fordern Sie die Funktion zum Zurückziehen des Schlüssels von an Kundenservice und Support.
2. Navigieren zu **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Einstellungen für Quorum Control-Richtlinie**an.
3. Wählen Sie aus **Quorum-Steuerung**



aktiviertKontrollkästchen.
Es werden zusätzliche Felder angezeigt, die zum Konfigurieren der Quorum-Steuerung erforderlich



sind.

4. Füllen Sie die Felder aus, um das Formular auszufüllen.

Feld	Beschreibung
Verantwortliche Vertragsgenehmigung	Bestimmen Sie die Mitglieder des Quorums aus der Liste der Anwender. Wählen Sie das Schlosssymbol Zum Öffnen des Anwenderverzeichnisses. Die Anzahl der auswählbaren Genehmiger ist nicht begrenzt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Mindestanzahl von Genehmigern, um das Quorum zu erreichen	Geben Sie die Mindestanzahl von Genehmigern an, die zum Erreichen des Quorums erforderlich sind. Wenn beispielsweise neun Genehmiger ausgewählt sind, können mindestens fünf für Quorum konfiguriert werden. Wenn fünf Genehmigungen im System empfangen werden, ist die Quorum erreicht, und der Vorgang „Zurückziehen“ wird gestartet. **Hinweis:** Die Mindestanzahl der erforderlichen Genehmiger beträgt zwei.
Anforderungen laufen nach der angegebenen Dauer (Stunden) ab.	Legen Sie einen numerischen Wert in Stunden fest, der die maximale Zeitzuteilung für die Mindestanzahl von Genehmigungen darstellt, die abgerufen werden sollen. Nach Ablauf des Zeitrahmens laufen auch die Quorum-Anforderungen ab. Eine neue Quorum-Anforderung ist erforderlich, um mit einer Widerrufsanforderung fortzufahren.

5. Klicken Sie auf **Absenden**.
   Eine Bestätigungsnachricht wird angezeigt.

Nächste Maßnahme
Die Widerrufsaktionen sind in verfügbar Schlüsselverwaltungsvorgänge.

Verwalten Sie Die Quorum-Steuerung

Nachdem ein Workflow für einen Rückzugsvorgang ausgelöst wurde, können Quorum-Aktionen über die Seite „Schlüsselverwaltungsvorgänge“ verwaltet werden. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erreicht ist.

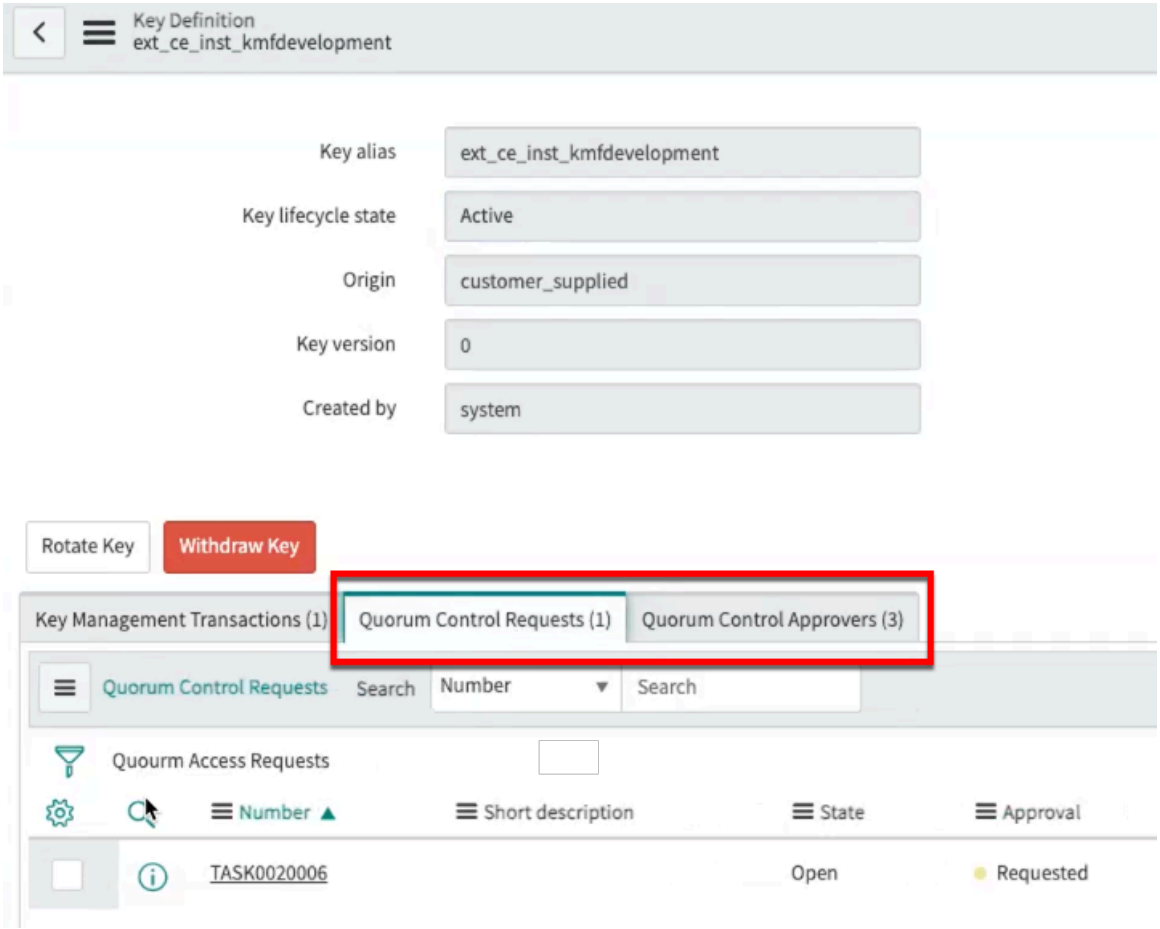
Vorbereitungen
Erforderliche Rolle: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Wenn das Quorum entweder genehmigt oder abgelehnt wurde, erhält die anfordernde Person des Schlüsselwiderrufs eine E-Mail, in der angegeben wird, ob das Quorum erreicht oder abgelehnt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Führen Sie die Schritte aus, um einen in gefundenen, vom Kunden verwalteten Schlüssel zurückzuziehen Schlüsselverwaltungsvorgänge.
2. Zeigen Sie an `Quorum-Steuerungsanforderungen` Und `Quorum Control-Genehmiger`Registerkarten, die aktiviert wurden.

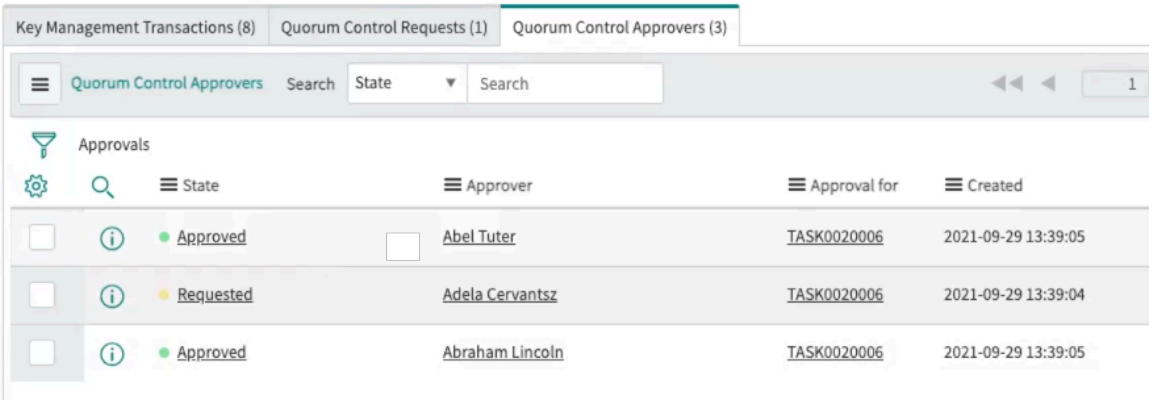


3. Öffnen Sie die **Quorum Control-Anforderungen** Registerkarte zum Anzeigen der tatsächlich erstellten Anforderung.
   - Status:
     - Offen: Die Aktion zum Zurückziehen des Schlüssels wartet auf die Erfüllung des Quorums.
     - Abgeschlossen: Das Quorum wurde erfüllt und kann keine weitere Aktion für diese bestimmte Quorum-Anforderung darstellen.
   - Genehmigung:
     - Angefordert: Genehmigungs-E-Mails wurden gesendet, und der Workflow wurde ausgelöst, um das Quorum zu erreichen.
     - Genehmigt: Der Schlüssel wird zurückgezogen, und die Instanz wird heruntergefahren.
     - Abgelehnt: Die Quorum-Anforderung wird abgebrochen, und mit dieser Anforderung wird keine weitere Aktion ausgeführt. Eine neue Widerrufsanforderung ist erforderlich, um den Schlüssel zurückzuziehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Öffnen Sie die Registerkarte Quorum Control Approvers (Quorum Control Approvers), um die Liste der Genehmiger und den Status der Genehmigungsanforderung



anzuzeigen.

Status:

- Angefordert: Der Genehmiger hat noch keine Maßnahmen für die Genehmigungsanforderung ergriffen.
- Genehmigt: Die Anforderung wurde entweder über die E-Mail oder die Genehmigungsseite genehmigt.

5. Wählen Sie aus **Schlüsselverwaltungstransaktionen** Registerkarte zum Anzeigen des Fortschritts des Anforderungsschritts für den Zurückziehen des Schlüssels.
   - Schritt 0: Quorum-Anforderung: Die tatsächliche Quorum-Anforderung. Die Quorum-Anforderung muss abgeschlossen werden, um die Schritte zum Zurückziehen des Schlüssels auszulösen.
   - Schritt 1 – Schlüsselrückzug: Der Schlüsselrückzug-Schritt. Dies besteht aus den Schritten zwei bis sieben.
   - Schritt 2 – Request_Preparation: Erstellt eine Anforderung zum Auslösen sowie das Umschließen und die Rotation.
   - Schritt 3 – Request_Integrity_Check: Validiert, dass die Anforderung legitim und sicher ist.
   - Schritt 4 – Request_validation: Validiert, dass eine Anforderung in Bearbeitung ist. Es kann jeweils nur eine Rotationsanforderung verarbeitet werden.
   - Schritt 5 – hsm_key_delete: Ruft KeySecure auf, um den aktiven Schlüssel zu löschen.
   - Schritt 6 – key_metadata_WELECT: Konvertiert den Lebenszyklusstatus der aktiven Schlüsselmetadaten in „zerstört“.
   - Schritt 7 – Post_Reduction: Ruft zum Herunterfahren der Instanz auf.

Automatische Übersetzung

Genehmigen oder verweigern Sie eine Quorum-Steuerungsanforderung

Genehmigen oder verweigern Sie eine Quorum-Steuerungsanforderung aus Schlüsselverwaltungstransaktionen.

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Quorum-Anforderung erstellt wurde, ist die Mindestanzahl von Genehmigungen für die Mitglieder erforderlich. Nachdem ein Workflow für einen Rückzugsvorgang ausgelöst wurde, können Quorum-Aktionen mit mehreren Methoden verwaltet werden. Die Anwender können Genehmigungen über die Seite „Schlüsselverwaltungsvorgänge“, „meine Genehmigungen in der Instanz“ oder direkt über die Anforderungs-E-Mail erteilen. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erreicht ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Verfahren wird beschrieben, wie Sie eine Quorum-Anforderung auf der Seite „Schlüsselverwaltungsvorgänge“ genehmigen oder ablehnen.

Vorbereitungen
Erforderliche Rollen: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Prozedur

1. Navigieren zu **Alle** > **Cloud-Verschlüsselungsschlüssel-Verwaltung** > **Transaktionen der Schlüsselverwaltung** > **Quorum Control-Genehmiger**an.
2. Wählen Sie Ihren Anwendernamen aus der Tabelle aus.
3. Genehmigen oder verweigern Sie die Anforderung.

Genehmigen oder verweigern Sie eine Quorum-Anforderung

Wenn eine Quorum-Anforderung erstellt wurde, ist die Mindestanzahl von Genehmigungen für die Mitglieder erforderlich. Nachdem ein Workflow für einen Rückzugsvorgang ausgelöst wurde, können Quorum-Aktionen mit mehreren Methoden verwaltet werden. Die Anwender können Genehmigungen über die Seite „Schlüsselverwaltungsvorgänge“ erteilen. **Meine Genehmigungen** In der Instanz oder direkt aus der Anforderungs-E-Mail. Der Vorgang zum Zurückziehen des Schlüssels wird blockiert, bis das Quorum erreicht ist.

Vorbereitungen
Erforderliche Rollen: sn_kmf.admin oder sn_kmf.cryptographic_Manager

Schlüsselverwaltungstransaktionen

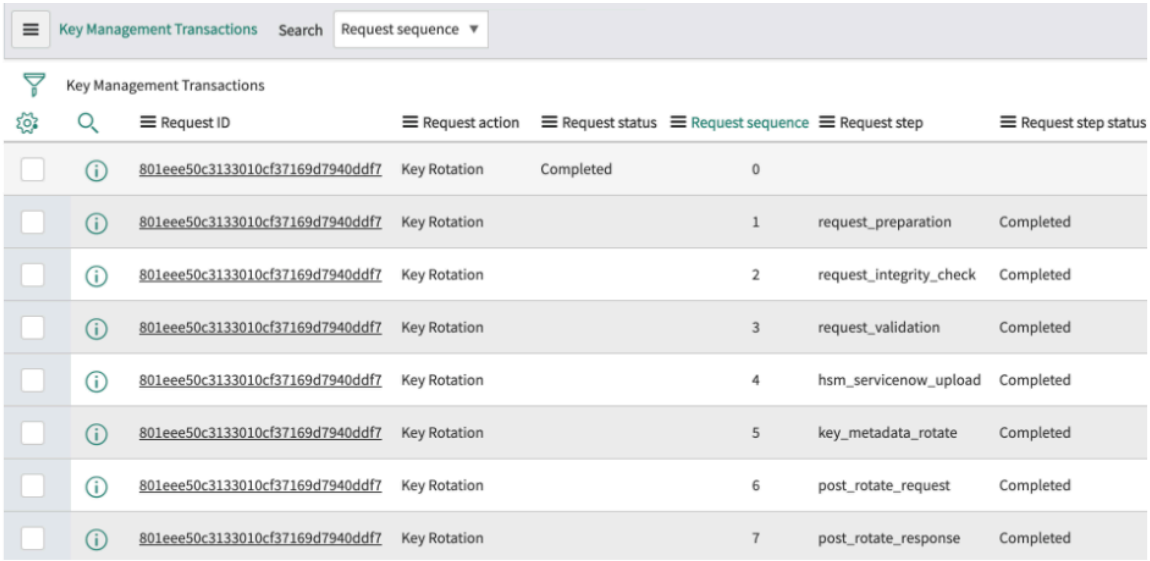
Das Untermodul Schlüsselverwaltungstransaktionen zeigt alle Transaktionen an, die für die Schlüssel in aufgetreten sind ServiceNow Instanz.

- Eine Schlüsseltransaktion wird wie folgt definiert:
  - Besteht aus mehreren Anforderungsschritten.
  - Eine einzelne `Anforderungs-ID` Wird für alle Anforderungsschritte freigegeben.
  - Der erste Schritt, Anforderungssequenz 0, einer Transaktion gibt den aktuellen Status der Gesamttransaktion an.

    Wie in der folgenden Abbildung zu sehen, hat der erste Schritt 0 einen Gesamt `Anforderungsstatus` Von abgeschlossen.
- Folgendes kann für die Transaktion durch den einzelnen Anforderungsschritt identifiziert werden:
  - Die Reihenfolge der einzelnen Schritte in einer Transaktion kann anhand der Sequenznummer für den Schritt identifiziert werden.
  - Der Status jeder Transaktion ist durch den Status des Anforderungsschritts sichtbar.
  - Wenn Schritte über den ersten Schritt hinaus fehlschlagen, hat die gesamte Transaktion den Status Fehlgeschlagen. Wenn alle Schritte abgeschlossen sind, wird auch der Transaktionsstatus „Abgeschlossen“ angezeigt.

Der folgende Bildschirm ist ein Beispiel für die Art von Informationen, die mit angezeigt werden ServiceNow Schlüsselrotation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In der folgenden Tabelle werden die Feldinformationen angezeigt, die auf der Seite „Schlüsselverwaltungstransaktionen“ verfügbar sind.

Transaktionen der Schlüsselverwaltung

Feld	Beschreibung
Anforderungs-ID	Eindeutige vom System generierte ID für die ausgeführte Aktion eine Anforderungs-ID wird für alle Anforderungsschritte freigegeben.
Anforderungsaktion	Zeigt die Aktion für den ausgeführten Schlüsselvorgang an.
Anforderungsstatus	• Verarbeitung: Eine Anforderung wurde eingegeben, aber noch nicht abgeschlossen. • Abgeschlossen: Die Anforderung wurde erfolgreich abgeschlossen. • Fehlgeschlagen: Ein Problem ist aufgetreten, und der Prozess wurde nicht abgeschlossen. **Hinweis:** Kontakt Kundenservice und Support Und geben Sie die Anforderungsnummer an, bei der der Fehler aufgetreten ist.
Schlüssel-Alias	Alphanumerischer Eintrag.
Status des Schlüssellebenszyklus	Siehe schlüssellebenszyklusstatus des Key Management Framework Für Definitionen.
Quelle	• ServiceNow Schlüssel • Vom Kunden verwalteter Schlüssel
Schlüsselversion	Wenn sich ein Schlüssel dreht, erhöht sich die Versionsnummer.
Anforderungssequenz	Zeigt die Reihenfolge an, in der eine Anforderung im System verarbeitet wird.
Anforderungsschritt	Zeigt an, ob während der Schlüsselrotation ein Schritt im System verarbeitet wird. Die Menge und der Inhalt der Schritte variieren je nach Typ des ausgeführten Schlüsselvorgangs.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transaktionen der Schlüsselverwaltung (Fortsetzung)

Feld	Beschreibung
	1. Request_Preparation: Erstellt eine Anforderung zum Auslösen sowie das Umschließen und die Rotation. 2. Request_Integrity_Check: Validiert, ob die Anforderung legitim und sicher ist. 3. Request_validation: Validiert, dass eine Anforderung in Bearbeitung ist. Es kann jeweils nur eine Rotationsanforderung verarbeitet werden. 4. Attachment_Process: Extrahiert das umschlossene Schlüsselmaterial aus dem Anhang. (Zusätzlicher Schritt beim Rotieren eines vom Kunden verwalteten Schlüssels.) 5. hsm_<key type>_Upload: Lädt das umschlossene Schlüsselmaterial in HSM, KeySecure hoch. 6. Key_metadata_Rotation: Generiert die neuen Schlüsselmetadaten. 7. Post_Rotation_Request: Sendet eine Anforderung zur Durchführung der Schlüsselrotation. 8. Post_Rotation_response: Antwort zum Durchführen der Schlüsselrotation basierend auf der Anforderung von der Kundeninstanz. **Hinweis:** Geben Sie den Anforderungsschritt an Kundenservice und Support Dient zum Analysieren des Statusfortschritts, falls ein Anforderungsschritt nicht abgeschlossen wird.
Anforderungsschritt-Status	• Abgeschlossen: Rotation ist erfolgreich. • Fehlgeschlagen: Rotation ist nicht erfolgreich. **Hinweis:** Geben Sie den Anforderungsschritt an Kundenservice und Support Dient zum Analysieren des Statusfortschritts, falls ein Anforderungsschritt nicht abgeschlossen wird.

Protokollierung der Cloud-Verschlüsselung

Erfahren Sie mehr über Protokollierungsoptionen für Cloud-Verschlüsselung.

Protokollierungstabellen für Cloud-Verschlüsselung

Verwenden Sie diese Tabellen, um Protokollierungsinformationen im Zusammenhang mit Cloud Encryption-Transaktionen in Ihrer Instanz zu finden.

Tabelle	Beschreibung
Cloud-Verschlüsselungsmetadaten [Dare_key_metadata]	Cloud Encryption-Metadaten erfasst wichtige Metadaten für das Lebenszyklusmanagement. In dieser Tabelle finden Sie wichtige Informationen zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	Lebenszyklus, Status und Version. Diese Tabelle wird nach jedem Schlüsselvorgang aktualisiert.
Schlüsselverwaltungstransaktionen [Dare_key_Request]	Schlüsselverwaltungstransaktionen erfasst Schlüsselverwaltungstransaktionsinformationen. In dieser Tabelle finden Sie die Protokollierung für jeden Schritt einer Transaktion. Die Tabelle zeichnet Fehlerinformationen für eine Transaktion in auf **Fehlermeldung** Feld.
SYS-Audits[sys_Audit]	Die Tabelle „SYS-Audits“ erfasst Einfügungen und Aktualisierungen für alle geprüften Datensätze in Ihrer Instanz. In dieser Tabelle finden Sie Änderungen an Datensätzen in Ihrer Instanz, wann die Änderungen vorgenommen wurden und welcher Anwenderaccount die Änderung initiiert hat.

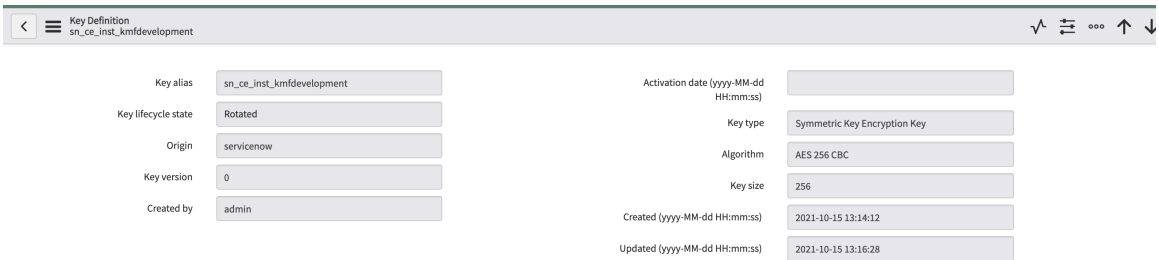
Überwachen Sie Schlüsselrotationsvorgänge

Verwenden Sie die Tabelle „Cloud Encryption Key Metadata“ [Dare_key_metadata], um Informationen zum Lebenszyklus Ihres Schlüssels zu finden. In dieser Tabelle finden Sie Informationen wie Ursprung, Aktivierungsdatum, Status und Version Ihrer Schlüssel.

Verwenden Sie die Tabelle „Schlüsselverwaltungstransaktionen“ [Dare_key_Request], um Transaktionen wichtiger Vorgänge zu überwachen. In dieser Tabelle finden Sie alle Anforderungen im Zusammenhang mit Ihren Schlüsseln, einschließlich Status, Status und Prozessschritt, in dem sich die Anforderung befindet. Abgeschlossene Anforderungen werden in dieser Tabelle mit beibehalten **Abgeschlossen** Status.

Dieses Beispiel zeigt einen Schlüsselrotationsvorgang. Während dieses Vorgangs wird der Status des alten Schlüssellebenszyklus von „aktiv“ in „rotiert“ und der Versionsstatus von „aktiv“ in „deaktiviert“ aktualisiert.

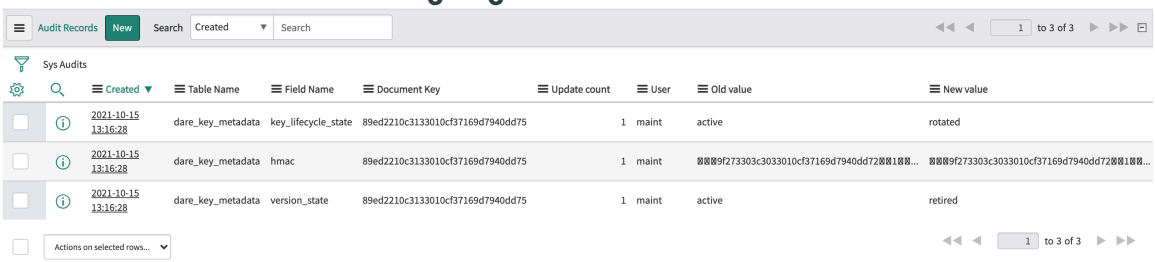
Schlüsseldefinition für einen rotierten Schlüssel



In der Tabelle „SYS-Audits“ [sys_Audit] können Administratoren Änderungen anzeigen, die an Datensätzen in der Tabelle „Cloud-Verschlüsselungsschlüssel-Metadaten“ [Dare_key_metadata] vorgenommen wurden. Administratoren können sehen, welche Datensätze wann aktualisiert wurden. Die Protokolleinträge erfassen auch das geänderte Feld sowie die alten und neuen Werte.

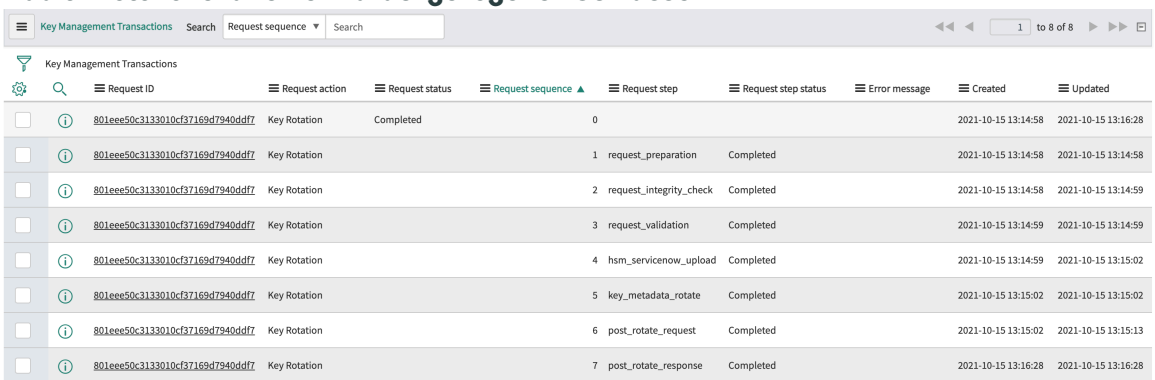
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audit-Protokolle für einen zurückgezogenen Schlüssel



Administratoren können die Datensätze in der Tabelle „Cloud-Verschlüsselungsschlüssel-Metadaten“ [Dare_key_metadata] anzeigen. In den folgenden Audit-Datensätzen wurde der Anforderungsstatus von „Verarbeitung“ in „Abgeschlossen“ geändert.

Audit-Protokolle für einen zurückgezogenen Schlüssel

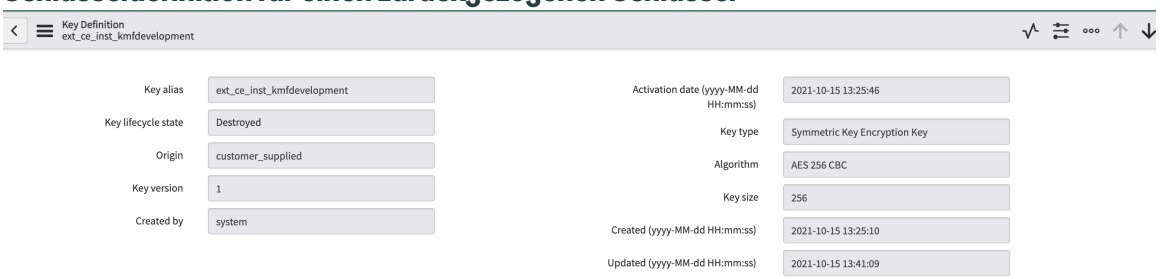


Protokollierung für Vorgänge zum Zurückziehen des Schlüssels

Protokollierungsinformationen zum Zurückziehen des Schlüssels werden in der Tabelle „Audits“ [sys_Audit] gespeichert. Diese Protokollierungsinformationen enthalten Informationen darüber, wer den Schlüsselwiderruf initiiert hat und wann der Widerruf stattgefunden hat.

Dieses Beispiel zeigt einen Vorgang zum Zurückziehen des Schlüssels. Während dieses Vorgangs wird der Status des Schlüssellebenszyklus von „generiert“ in „aktiv“ und „zerstört“ aktualisiert. Die Schlüsselversion wird von „unbekannt“, „aktiv“ und „deaktiviert“ aktualisiert.

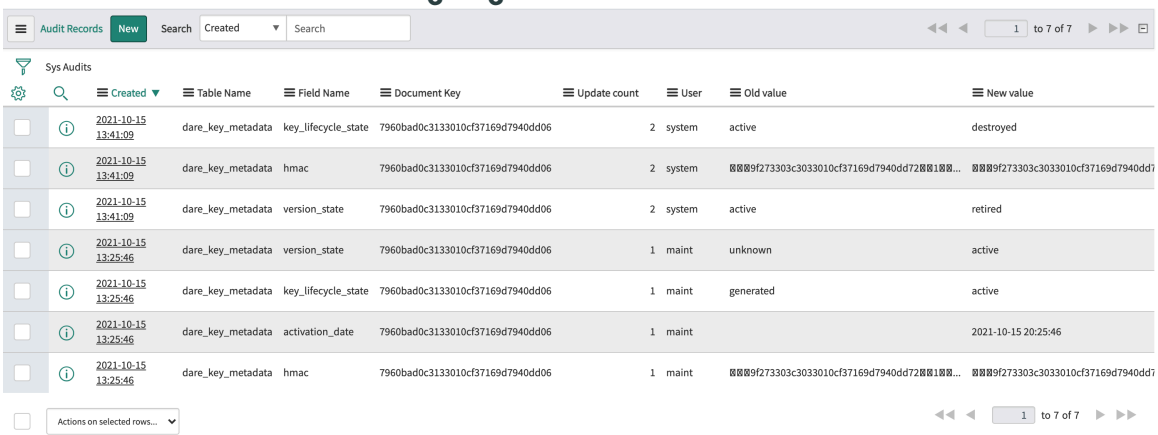
Schlüsseldefinition für einen zurückgezogenen Schlüssel



Wenn Sie sich die Tabelle „SYS-Audits“ [sys_Audit] ansehen, können Administratoren die Tabelle „Cloud Encryption Key Metadata“ [Dare_key_metadata] ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audit-Protokolle für einen zurückgezogenen Schlüssel



Audit Records | New | Search | Created | Search | 1 to 7 of 7

Sys Audits

Created	Table Name	Field Name	Document Key	Update count	User	Old value	New value
2021-10-15 13:41:09	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	2	system	active	destroyed
2021-10-15 13:41:09	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	2	system	▯▯▯9f273303c3033010cf37169d7940dd72▯▯1▯▯...	▯▯▯9f273303c3033010cf37169d7940dd7
2021-10-15 13:41:09	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	2	system	active	retired
2021-10-15 13:25:46	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	1	maint	unknown	active
2021-10-15 13:25:46	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	1	maint	generated	active
2021-10-15 13:25:46	dare_key_metadata	activation_date	7960bad0c3133010cf37169d7940dd06	1	maint		2021-10-15 20:25:46
2021-10-15 13:25:46	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	1	maint	▯▯▯9f273303c3033010cf37169d7940dd72▯▯1▯▯...	▯▯▯9f273303c3033010cf37169d7940dd7

Actions on selected rows... | 1 to 7 of 7

Manipulationserkennung

Verwenden Sie die Manipulationserkennung, um die Sicherheit zu verbessern, indem Sie nicht autorisierte Änderungen an Ihren Quorum-Steuerungseinstellungen erkennen.

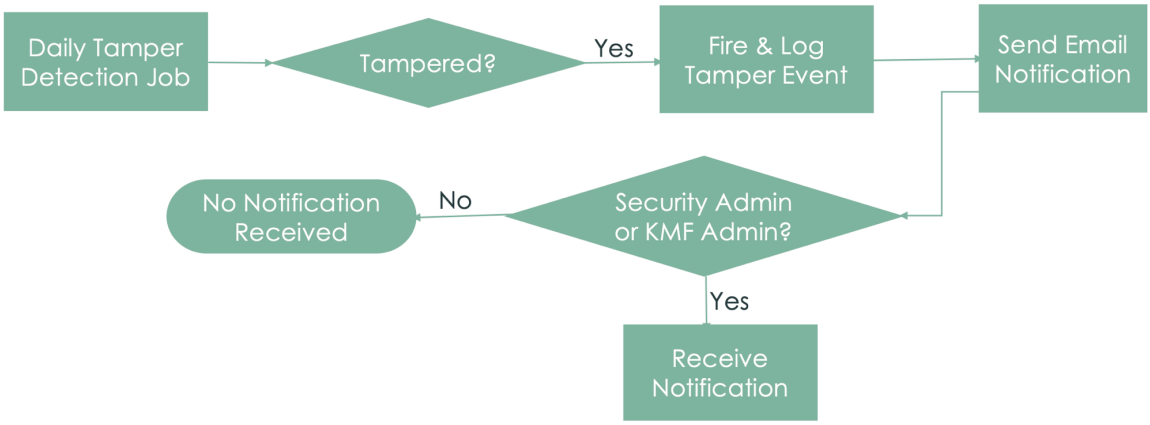
Manipulationserkennungsprozess

Wenn diese Option aktiviert ist, validiert die Manipulationserkennung Ihre Quorum-Steuerungseinstellungen, indem sie auf nicht autorisierte Änderungen (Manipulation) überprüft. Die Manipulationserkennung verwendet HMAC (Hash-based Message Authentication Code).

1. Wenn eine Einstellung geändert oder erstellt wird, erstellt Ihre Instanz einen HMAC. Der HMAC basiert auf dem Wert des Einstellungsdatensatzes (Dare_property).
2. Immer wenn Ihre Instanz diese Einstellungen verwendet, validiert die Manipulationserkennung sie mithilfe des HMAC.
3. Wenn die Einstellung erfolgreich validiert wird, kann sie von der Plattform verwendet werden, andernfalls nicht.

Manipulationserkennung wird täglich in Ihrer Instanz ausgeführt

Die Manipulationserkennung überprüft Ihre Einstellungen anhand einer täglichen geplanten Aufgabe auf Manipulationen und meldet Validierungsfehler in Ihrem Knoten und Sicherheitsprotokollen. Manipulationserkennung sendet eine Benachrichtigung an die Sicherheits- und KMF-Administratoren bei Validierungsfehlern.

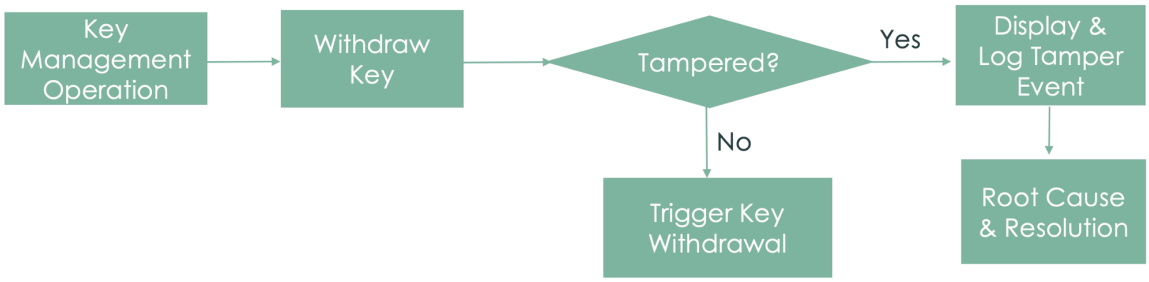


Manipulationserkennung wird ausgeführt, bevor ein Schlüssel zurückgezogen wird

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Manipulationserkennung validiert auch Ihre Eigenschaften, wenn Sie einen Schlüsselwiderruf anfordern. Wenn Ihre Einstellungen die Validierung nicht bestehen, wird der Schlüsselzurückzug nicht ausgeführt. In diesem Fall müssen Sie Validierungsprobleme lösen, bevor der Schlüsselzurückzug konkurrieren kann.



Manipulationen werden identifiziert

Die Manipulationserkennung aktualisiert Ihre Protokolle, wenn die Validierung fehlschlägt.

Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validiert, werden diese Fehler in Ihren Knoten- und Sicherheitsprotokollen angezeigt. Der Protokolleintrag enthält die sys_ID des Einstellungsdatensatzes (Dare_property), bei dem die Validierung fehlgeschlagen ist.

```
2022-06-28 13:45:46 (582) Default-thread-5
 B6FAC1F6C3D01110CF37169D7940DD6E txid=231c4d72c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 776e3200c3210110900b169d7940dd76 failed HMAC validation

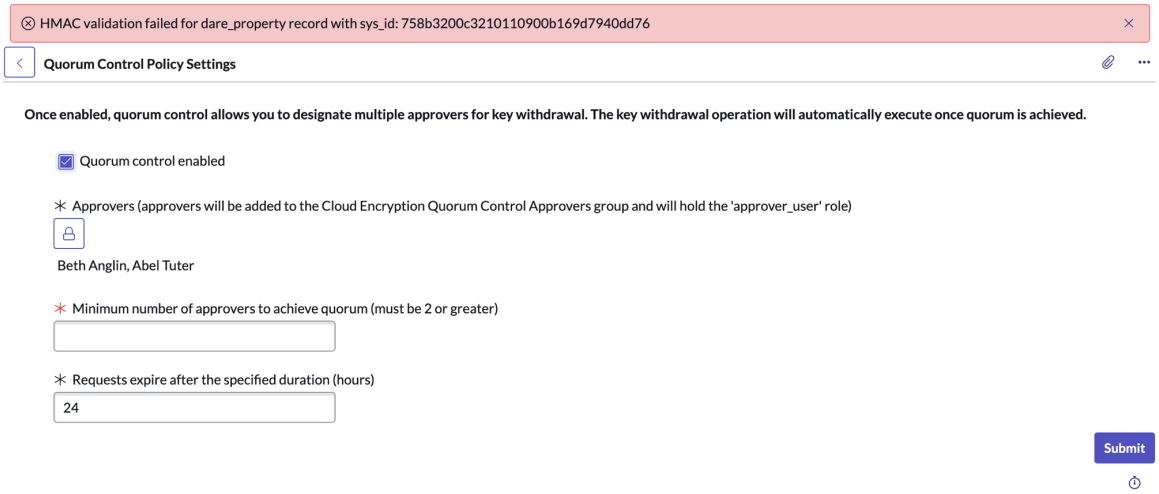
2022-06-28 13:47:35 (264) Default-thread-8
 B6FAC1F6C3D01110CF37169D7940DD6E txid=8e8cc972c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 758b3200c3210110900b169d7940dd76 failed HMAC validation
```

Die Protokollierung zeigt Informationen ähnlich wie diese Beispiele an, wenn die Validierung fehlschlägt. Erfolgreiche Validierungen werden nicht in den Protokollen angezeigt.

Die Manipulationserkennung zeigt eine Warnmeldung auf der Seite mit den Einstellungen für die Quorum-Steuerung an

Wenn die Validierung einer Quorum-Steuerungseinstellung fehlgeschlagen ist, wird eine Warnung angezeigt, wenn Sie die Seite mit den Einstellungen für die Quorum-Steuerungsrichtlinie in Ihrer Instanz anzeigen. Die Warnung enthält die sys_ID des Einstellungsdatensatzes (Dare_property), bei dem die Validierung fehlgeschlagen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Manipulationserkennung sendet Benachrichtigungen an Anwender mit dem *Security Admin*Und *KMF Admin*Rollen

Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validiert, erhalten Ihre Sicherheitsadministratoren und KMF-Administratoren eine Benachrichtigung ähnlich wie in diesem Beispiel.

Subject: IMPORTANT: Cloud Encryption Properties Tampering Detected

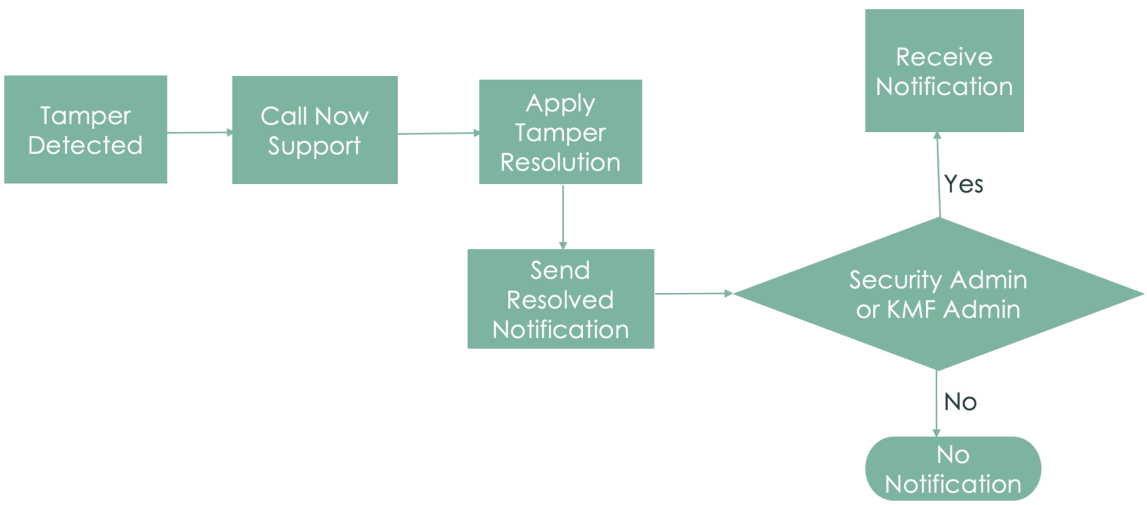
The following list of Cloud Encryption properties appear to have been tampered.
Contact ServiceNow support for additional information and how to correct this issue.

Tampered properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000109_q5pzYMS7hcgHXAoUhipc

Beheben von Manipulationsproblemen mit ServiceNow Support

Wichtig: Fehler bei der Validierung der Manipulationserkennung können nur mit Unterstützung von gelöst werden ServiceNow Support.

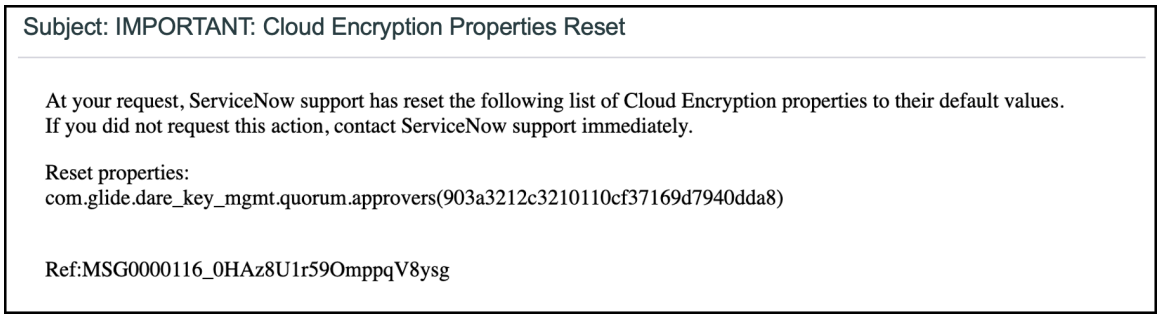


Wenn die Manipulationserkennung eine Ihrer Quorum-Steuerungseinstellungen nicht validiert, wenden Sie sich an ServiceNow Unterstützung für Unterstützung bei der Lösung des Problems. Nachdem ein Support-Mitarbeiter den Validierungsfehler gelöst hat, erhalten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheits- und KMF-Administratoren eine Benachrichtigung, dass das Problem gelöst wurde.



Subject: IMPORTANT: Cloud Encryption Properties Reset

At your request, ServiceNow support has reset the following list of Cloud Encryption properties to their default values.
If you did not request this action, contact ServiceNow support immediately.

Reset properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000116_0HAz8U1r59OmppqV8ysg

Vollständige Datenträgerverschlüsselung

Full Disk Encryption (FDE) wendet die Verschlüsselung nur auf das gesamte Speichersystem innerhalb des Datenbankservers an, da dies die einzige Kundendatenspeicherungskomponente ist. FDE schützt nur vor physischem Verlust oder Diebstahl von Speichergeräten. Wenn verschlüsselte Festplattenserver eingeschaltet sind und Daten bereitstellen, bietet die Verschlüsselung keinen zusätzlichen Schutz.

Vollständige Datenträgerverschlüsselung

Die vollständige Datenträgerverschlüsselung kann für stark regulierte Organisationen relevant sein, kann jedoch erhebliche Kosten für einen Kunden verursachen ServiceNow Bereitstellung. Maßnahmen vorhanden bis ServiceNow Die Minimierung des Verlusts oder Diebstahls von Speichergeräten kann ebenfalls ein Faktor bei der Auswahl sein.

Von ServiceNow AI Platform Perspektive, alle Daten-Flows in entschlüsselt.

In gewerblichen Umgebungen wird eine vollständige Datenträgerverschlüsselung (Full Disk Encryption, FDE) mit FIPS 140-validierter Hardware oder Speichergeräten verwendet, die zusammen mit einer validiert werden ServiceNow Dedizierte Hardwareoption gegen zusätzliche Kosten. FDE gilt für die Hardware selbst und bietet daher eine Verschlüsselung im Ruhezustand für alle Daten, die in jeder Ihnen zugewiesenen Instanz gespeichert sind.

Weitere Informationen zur Auswahl von FDE und dedizierten Hardwareoptionen erhalten Sie von ServiceNow Vertreter.

Edge Encryption

ServiceNow® Edge Encryption ™ Verschlüsselt vertrauliche Daten in Ihrem Unternehmen, bevor sie über das Internet an Ihren gesendet werden ServiceNow Instanz (im Flug verschlüsselt), in der sie im Ruhezustand verschlüsselt bleibt.

Wichtig:

Edge Encryption wurde ab November 2024 in den Status „Ende des Vertriebs“ versetzt und befindet sich ab dem Yokohama-Release in der Phase „Ende der Verlängerung“.

ServiceNow Plattformverschlüsselung ist die empfohlene Lösung für die Zukunft. Weitere Informationen finden Sie unter Edge Encryption – Ende der Verlängerung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



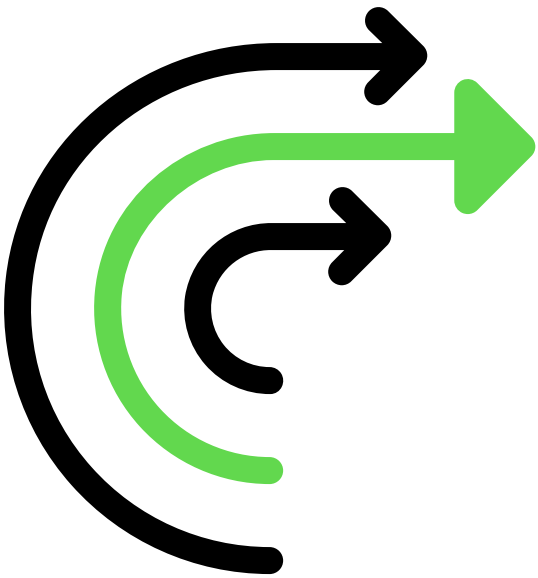
Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von Edge Encryption.

Planen



Erfahren Sie, wie Sie Edge Encryption planen.

Installieren



Installieren Sie Edge Encryption.

Upgrade Von Edge Encryption

Upgrade



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie mehr über das Upgrade von Edge Encryption.

Konfigurieren



Erfahren Sie, wie Edge Encryption konfiguriert wird.

Edge Encryption erkunden

Edge Encryption Ist ein Netzwerkverschlüsselungssystem, das sich in Ihrem Netzwerk befindet und vertrauliche Daten verschlüsselt und entschlüsselt, während sie zwischen Ihrem Rechenzentrum und dem übertragen werden ServiceNow Cloud.

Edge Encryption – Beschreibung

Auch als „clientseitige“ Verschlüsselung bezeichnet, erfordert Edge, dass der gesamte bidirektionale Anwenderdatenverkehr über Proxys geleitet wird, die in Ihrer Infrastruktur verwaltet werden. Sie haben die volle Kontrolle über Ihre Schlüsselverwaltung, da die Schlüssel in Ihrem Proxy in Ihrer Infrastruktur gespeichert werden. Die ServiceNow AI Platform Der verschlüsselte Text kann nicht entschlüsselt werden, um auf Ihre Schlüssel zuzugreifen.

Die Edge Encryption Die Funktion ist eine zusätzliche Kostenoption, mit der Sie die End-to-End-Verschlüsselung Ihrer Daten und die Schlüsselverwaltung steuern können. Edge Encryption Verwendet eine von bereitgestellte Proxy-Anwendung ServiceNow Und von Ihnen in Ihrem eigenen Netzwerk installiert. Diese Proxy-Anwendung tokenisiert angegebene Datenmuster oder verschlüsselt Zeichenfolgenfelder, Datumsfelder, Datums-/Uhrzeitfelder und Anhangsdaten, bevor sie von Ihrer Umgebung an Ihre Instanz gesendet werden. Die Proxy-Anwendung entschlüsselt auch dieselben Daten, wiederum nur in Ihrem eigenen Netzwerk, mit Schlüsseln, die nur in Ihrem eigenen Netzwerk gespeichert sind.

Die relevanten Verschlüsselungsschlüssel und die Konfiguration sind nur auf dem Edge-Proxy in Ihrem Netzwerk vorhanden und für nicht sichtbar ServiceNow. Die Daten werden ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dem Zeitpunkt verschlüsselt, zu dem sie Ihre Umgebung verlassen, und erst beim Abrufen entschlüsselt. Zu keinem Zeitpunkt sind die Daten in nur-Text von zugänglich ServiceNow Systeme oder Personal.

Edge Encryption – Benutzer

Nur ein Anwender, der sich über einen Proxy-Server in Ihrem Netzwerk bei der Instanz angemeldet hat, kann verschlüsselte Daten in Klartext anzeigen. Ebenso kann nur ein Security_admin-Anwender, der über einen Proxy-Server in Ihrem Netzwerk bei einer Instanz angemeldet ist, konfigurieren und verwalten Edge Encryption.

Da sich der Proxy-Server in Ihrem Netzwerk befindet, besitzen und verwalten Sie die Verschlüsselungsschlüssel, und sie werden nie an die Instanz gesendet. Infolgedessen ServiceNow Zeigt vertrauliche Daten nie in Klartext an.

Zusätzlich zur Edge-Proxy-Konfiguration und -Verwaltung von Regeln sind Sie für die üblichen Anforderungen des Betriebs eines Servers in Ihrer Umgebung (einschließlich Hosting, Weiterleitung, Sicherung, DNS-Konfiguration usw.) verantwortlich, um Ihre Edge-Proxys zu aktivieren und zu unterstützen.

Verschlüsselung und Tokenisierung

Edge Encryption Unterstützt sowohl die Verschlüsselung (durch Verschlüsselungskonfigurationen) als auch die Tokenisierung (durch Verschlüsselungsmuster), um Ihre vertraulichen Informationen zu schützen.

Verschlüsselungskonfigurationen

Sie können einzelne Felder mithilfe von Verschlüsselungskonfigurationen verschlüsseln. Edge Encryption Unterstützt AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel. Edge Encryption Unterstützt die Verschlüsselungstypen „Standard“, „Gleichberechtigung erhalten“ und „Reihenfolge beibehalten“.

Zusätzlich zu Anhängen können Sie die folgenden Feldtypen verschlüsseln:

- Datum
- E-Mail
- Datum/Uhrzeit
- HTML
- IP-Adresse
- Journal
- Journaleingabe
- Mehrzeiliger Text
- Einzeiliger Text
- Zeichenfolge
- URL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn dem Aktivitätsstrom ein Journal Feld hinzugefügt wird, das für die Verschlüsselung markiert ist, werden alle Benutzereingaben in das Feld im Aktivitätsstrom verschlüsselt.

Multi-Byte-Zeichen innerhalb der unterstützten Feldtypen können verschlüsselt werden.

Sie können auch die folgenden Servicekatalog-Variablentypen verschlüsseln:

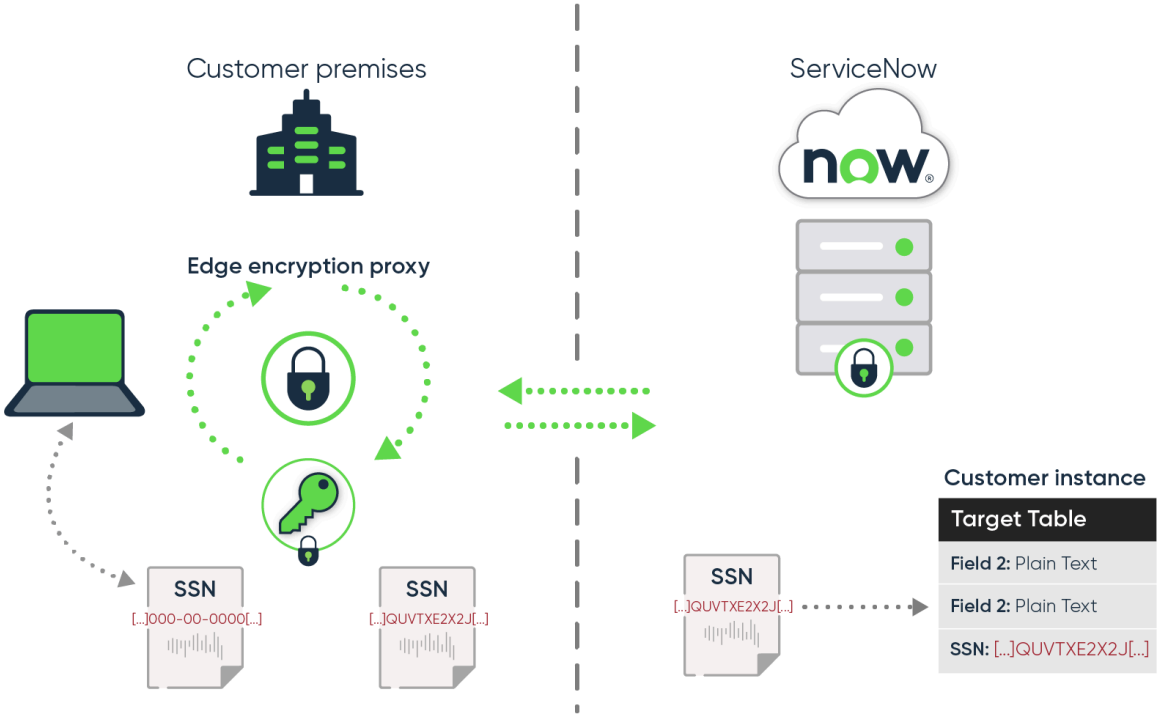
- Zeichenfolgentypen
  - Einzeiliger Text
  - Mehrzeiliger Text
  - Breite einzeilige Textzeile
- Datum
- Datum/Uhrzeit
- URL
- E-Mail
- HTML
- IP-Adresse

Verschlüsselungsmuster

Sie können Verschlüsselungsmuster verwenden, um Zeichenketten zu tokenisieren, die regulären Mustern wie Sozialversicherungs- und Kreditkartennummern entsprechen. Verschlüsselungskonfigurationen sollten zwar die primäre Verschlüsselungsmethode sein, verwenden Sie jedoch Verschlüsselungsmuster als Ergänzung, um vertrauliche Informationen außerhalb verschlüsselter Felder zu schützen.

Hinweis: Der Edge Encryption Proxy-Server erfordert nur eine MySQL-Datenbank in Ihrem Netzwerk, wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden. Klartextwerte werden in der Proxy-Datenbank in Ihrem Netzwerk gespeichert. Aus diesem Grund ist es wichtig, dass Sie Ihre Proxy-Datenbank schützen und regelmäßig sichern. Empfehlungen finden Sie unter Komponenten der Edge Encryption.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Edge Encryption auf ServiceNow AI Platform

Edge Encryption Fungiert als Gateway zwischen Ihrem Browser und Ihrem ServiceNow Instanz. Der Datenverkehr Ihres Browsers wird durch das Gateway auf dem Weg zur ServiceNow-Instanz. Das Gateway wiederum ist so konfiguriert, dass ausgehende Daten, die zur Verschlüsselung markiert sind, verschlüsselt werden. Eingehender Datenverkehr wird über das Gateway entschlüsselt, und der Endbenutzer sieht im Browser Klartext. Der Vorteil dieser Implementierung in Bezug auf die Sicherheitskontrolle besteht darin, dass die Verschlüsselung und die Schlüsselverwaltung extern über ServiceNow erfolgen.

Vor- und Nachteile

Wie mit Feldverschlüsselung Enterprise Und Feldverschlüsselung, Edge Encryption Erzwingt aufgrund der zusätzlichen Sicherheit einige Funktionseinschränkungen innerhalb einer Instanz. Der lokale Edge-Proxy bietet jedoch im Vergleich zur Verschlüsselung auf Spaltenebene auch einige zusätzliche Funktionen in Bezug auf die Sortierung.

Vorteile:

- Edge Encryption Bietet absolute Kontrolle darüber, wer Ihre Informationen sieht, und verhindert Datenschutzverletzungen.
- Informationen verbleiben auf Ihrem Proxy-Server und lassen Ihr Netzwerk nie unverschlüsselt.
- Informationen werden während der Übertragung verschlüsselt, bevor sie überhaupt erreicht werden ServiceNow Instanz.
- Sie halten und verwalten alle Ihre eigenen Verschlüsselungsschlüssel. Niemand sonst, nicht einmal ServiceNow Mitarbeiter, können auf Ihre Schlüssel zugreifen.
- Sie können die Stärke des Verschlüsselungsalgorithmus auswählen: AES-128 oder AES-256.
- Edge Encryption Enthält die Möglichkeit, Zeichenfolgentext, Datums- und Datums-/Uhrzeitfelder, Anhänge, URLs und Journale zu verschlüsseln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Edge Encryption Bietet die Standard-, Gleichzeitigungs- und Ordnungsbewahrungsverschlüsselung von Daten, die sich in der Datenbank und der Instanz befinden.
- Mit Verschlüsselungsregeln können Sie anwenderdefinierte Skripts schreiben, die dem Proxy-Server genau mitteilen, was verschlüsselt werden soll und wo diese verschlüsselten Informationen in der Instanz gespeichert werden sollen. Diese Skripts sind nützlich, wenn die Datenstruktur nicht genau mit übereinstimmt ServiceNow Instanz.
- Mit Verschlüsselungsmustern können Sie Informationen wie Passwörter tokenisieren.

Nachteile:

- Edge Encryption Erfordert einen zusätzlichen Netzwerk-Hop durch den Edge-Proxys-Cluster und zusätzliche Verarbeitung, was den Datenverkehr verzögern kann. Die hinzugefügte Verarbeitungsverzögerung von Edge Encryption Anwendung ist im Vergleich zum Netzwerk-Hop vernachlässigbar.
- Die Verwaltung eigener Verschlüsselungsschlüssel kann komplex und zeitaufwändig sein.
- Sie können maximal zwei Schlüssel verwalten, ohne flexibel zu sein, verschiedene Schlüssel für verschiedene Teilmengen von Spalten/Daten oder für verschiedene Rollen usw. zu definieren
- Edge Encryption Hat den Nebeneffekt, dass der Server oder die Plattform die Daten nicht entschlüsseln kann, um Manipulationen der entschlüsselten Daten durchzuführen. Folglich Funktionalität und Datenverarbeitung im ServiceNow AI Platform Kann beim Verschlüsseln von Spalten mit Edge Encryption eingeschränkt sein.

Was Sie wissen sollten, bevor Sie beginnen

Da Verschlüsselung und Tokenisierung die Art Ihrer Daten ändern, kann Edge Encryption sich auf andere Instanzprozesse auswirken. Vor der Verwendung Edge Encryption, Überdenken Sie sorgfältig die Auswirkungen auf Ihre Instanz.

Da der Proxy-Server in Ihrem Netzwerk installiert und verwaltet wird, erfordert Edge Encryption eine Netzwerkadministration und -verwaltung. Überprüfen Sie die Netzwerkanforderungen, um eine reibungslose Implementierung sicherzustellen.

Überprüfen Sie die folgenden Themen, um die Auswirkungen von Edge Encryption auf Ihre Instanz zu verstehen:

- Die Edge Encryption planen
- Edge Encryption – Systemanforderungen
- Umgebungsgröße Ihrer Edge Encryption anpassen
- Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen
- Edge Encryption Einschränkungen
- Schlüsselverwaltung für Edge Encryption

Komponenten der Edge Encryption

Edge Encryption Besteht aus Edge Encryption Proxy-Server, der auf einem Server in Ihrem Netzwerk ausgeführt wird, und der Edge Encryption Plugin, das auf installiert sein muss ServiceNow Instanz. Wenn Sie Verschlüsselungstypen oder Verschlüsselungsmuster mit Ordnungserhaltung verwenden, muss auch eine Proxy-Datenbank in Ihrem Netzwerk installiert sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Proxy-Anwendung

Beim Durchlaufen von Edge Encryption Proxy-Server, die Edge Encryption Mit dem Plugin können Sie angeben, welche Felder, Muster und Anhänge verschlüsselt werden sollen. Sie können auch Verschlüsselungsregeln verwalten, um bestimmte Anforderungen zu verschlüsseln und Massenverschlüsselungsaufträge zu planen.

Proxy-Server

Die Edge Encryption Der Proxy-Server verwendet Verschlüsselungsregeln, um in einer HTTP-Anforderung zu identifizieren, was ggf. verschlüsselt werden muss, und verschlüsselt sie, bevor die Anforderung an die Instanz weitergeleitet wird. Für die Entschlüsselung Edge Encryption Der Proxy-Server überprüft die HTTP-Antworten auf verschlüsselte Daten und entschlüsselt sie, bevor die Antwort an den Client zurückgesendet wird. Damit diese Entschlüsselung erfolgt, müssen alle HTTP-Anforderungen und -Antworten über laufen Edge Encryption Proxy-Server. Diese HTTP-Anforderungen umfassen alle Anforderungen, die von einem Browser stammen, sowie alle SOAP- oder REST-Anforderungen.

Proxy-Datenbank

Wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden, verlassen sich Ihre Proxy-Server auf eine MySQL-Datenbank, die sich in Ihrem Netzwerk befindet. Alle Proxy-Server in Ihrem Netzwerk müssen dieselbe Datenbank verwenden.

Diese Tabellen sind in der Proxy-Datenbank enthalten.

Proxy-Datenbanktabellen

Name	Beschreibung
db_id	Eindeutige Datenbank-ID
edge_token_map	Verschlüsselungsmusterdaten
token_map	Ordnungserhaltende Verschlüsselungsdaten

Sichern Ihrer Proxy-Datenbank

Da Verschlüsselungsmuster von der Tokenisierung abhängen, werden Klartextwerte in Ihrer Proxy-Datenbank gespeichert. Wenn die Datenbank verloren geht, können Klartextwerte nicht wiederhergestellt werden. Es ist wichtig, dass Sie regelmäßige Sicherungen pflegen. Um Datenverlust zu vermeiden, sichern Sie Ihre Proxy-Datenbank gemäß ServiceNow Empfehlungen.

- Sichern Sie Ihre Datenbank alle 24 Stunden.
- Bewahren Sie die binären Protokolldateien der MySQL-Datenbank für mindestens zwei Tage auf. Nachdem eine Sicherung wiederhergestellt wurde, können Sie das binäre Protokoll verwenden, um die seit der letzten Sicherung verlorenen Daten wiederherzustellen.

Edge Encryption Clients

Edge Encryption Verwendet drei Clients, um die Instanz darüber zu informieren, dass der Proxy ausgeführt wird, um Anforderungen zwischen dem Proxy und der Instanz zu synchronisieren und alle Endanwenderanforderungen nach einer potenziellen Verschlüsselung an die Instanz weiterzuleiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client	Beschreibung
Heartbeat-/Keepalive-Client	Ist dafür verantwortlich, alle 5 Sekunden eine Anforderung an die ServiceNow-Instanz zu senden, um der Instanz mitzuteilen, dass dieser Proxy hochgefahren und ausgeführt wird. Die Anforderungen steuern das Feld Last_response_on in der Edge-Proxy-Tabelle und steuern folglich den Status des Proxys. Wenn Ihr System Probleme beim Senden der Anforderungen hat oder wenn die Anforderungs- oder Anforderungsverarbeitung verzögert wird, kann die Instanz den Proxy als nicht reagierend markieren, auch wenn die anderen Clients (einschließlich des Clients für Anwenderdatenverkehr) aktiv sind. Dieser Client steuert auch den Onlinestatus des Proxy in der Instanz. Die *edgeencryption.proxy.keepalive.interval*Die Eigenschaft steuert die Abfragerate für diesen Client. Der Standardwert ist 5 (Sekunden).
Abruf/Synchronisierung des Clients	Für verschiedene Anforderungen sendet der Proxy an die Instanz, um sie in der Edge Encryption-Konfiguration zu synchronisieren (z. B. welche Tabelle, Spalte oder Anhang verschlüsselt werden soll, Schlüssel, Aufträge, Regeln und Tokenisierungsmuster). Die *edgeencryption.config.poll.interval*Die Eigenschaft steuert die Abfragerate für diesen Client. ⚠ **Warnung:** Ändern Sie diese Einstellung nicht. Das Ändern der Standardeinstellung des Proxy-Abfrageintervalls kann zu Verzögerungen bei der Synchronisierung führen, wenn die Edge Encryption-Einstellungen in der Instanz aktualisiert werden.
Standard-/Anwenderdatenverkehr-Client	Für alles andere verarbeitet dieser Client alle Endanwenderanforderungen und leitet sie nach einer potenziellen Verschlüsselung an die ServiceNow-Instanz weiter. Dieser Client verarbeitet auch Antworten von der Instanz und leitet sie nach einer potenziellen Entschlüsselung an den Endanwender weiter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselverwaltung für Edge Encryption

Sie sind für die Bereitstellung und Verwaltung der von Edge Encryption verwendeten Verschlüsselungscodes verantwortlich.

Dieses Thema bezieht sich auf Schlüssel für Edge Encryption Produkt. Wenn Sie nach Informationen zum Key Management Framework suchen, das mit verwendet werden kann Feldverschlüsselung, Siehe Key-Management-Framework .

Wenn Sie Verschlüsselungscodes erhalten und erstellen, die die von Edge Encryption verwendeten Verschlüsselungsarten unterstützen, beachten Sie Folgendes:

- Soll AES 128-Bit oder AES 256-Bit verwendet werden? Sie müssen einen Standard-AES 128-Bit-Verschlüsselungsschlüssel definieren, auch wenn er nicht verwendet wird.
- Gibt an, ob Dateisystem, Java-Schlüsselspeicher oder Enterprise Key Management (EKM) verwendet werden soll.
- Wann müssen die Verschlüsselungsschlüssel rotiert werden?
- Wann und ob ein Massenverschlüsselungsauftrag verwendet wird, um Daten mit dem neuen Schlüssel erneut zu verschlüsseln.

Vor dem Entfernen eines Schlüssels aus den Proxy-Konfigurationsdateien und dem Schlüsselspeicher müssen unbedingt alle Daten in der Instanz entschlüsselt werden, die den Schlüssel verwendet. Sie können dies tun, indem Sie einen neuen Verschlüsselungscode hinzufügen und einen Auftrag zur Massenrotation von Schlüsseln planen.

Schlüsselspeicher

Edge Encryption unterstützt die folgenden Arten der Schlüsselspeicherung.

Dateispeicher

Schlüssel werden in einer Datei in einem Dateisystem gespeichert, auf das der Edge Encryption Proxy Zugriff hat. In einer Datei gespeicherte Verschlüsselungsschlüssel werden nicht verschlüsselt. Der Schutz dieser Dateien liegt also in Ihrer Verantwortung.

Java KeyStore

Schlüssel werden im JCEKS KeyStore von Java gespeichert. Ein Java KeyStore ist durch ein Passwort geschützt. Daher ist es sicherer als das Speichern von Schlüsseln in einer Datei im Dateispeicher. Ein einzelner Java KeyStore kann mehrere Schlüssel speichern. Die Schlüssel werden durch einen Schlüsselalias identifiziert, wodurch die Verwaltung mehrerer Schlüssel vereinfacht wird.

Enterprise Key Management (EKM)

Schlüssel werden mit den Schlüsselverwaltungssystemen SafeNet KeySecure oder Unbound Technology gespeichert und abgerufen.

Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen keystore.jceks im Verzeichnis Schlüsselspeicher geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.

Hinweis: Wenn Sie einen anderen Schlüsselspeicher als das Basissystem Java JCEKS KeyStore verwenden, müssen Sie den öffentlichen Schlüssel ServiceNow in Ihren Schlüsselspeicher importieren. Der öffentliche Schlüssel-Alias ist *servicenow*.

Zusätzlich zu den Verschlüsselungsschlüsseln wird im Java JCEKS KeyStore das RSA-Schlüsselpaar zum digitalen Signieren der in der Instanz gespeicherten Verschlüsselungskonfigurations- und Verschlüsselungsregeln und das digitale Zertifikat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gespeichert, das der Proxy Edge Encryption verwendet, um eine sichere Verbindung mit den Browsern und allen anderen Clients herzustellen.

SafeNet-Schlüsselversionsverwaltung für Edge Encryption

Verwenden Sie die SafeNet-Schlüsselversionsverwaltung, um das Wechseln der Schlüssel zu vereinfachen. Anstatt für jeden neuen Schlüssel einen Alias zu erstellen, behält die SafeNet-Schlüsselversionsverwaltung denselben Alias bei und erhöht die Version.

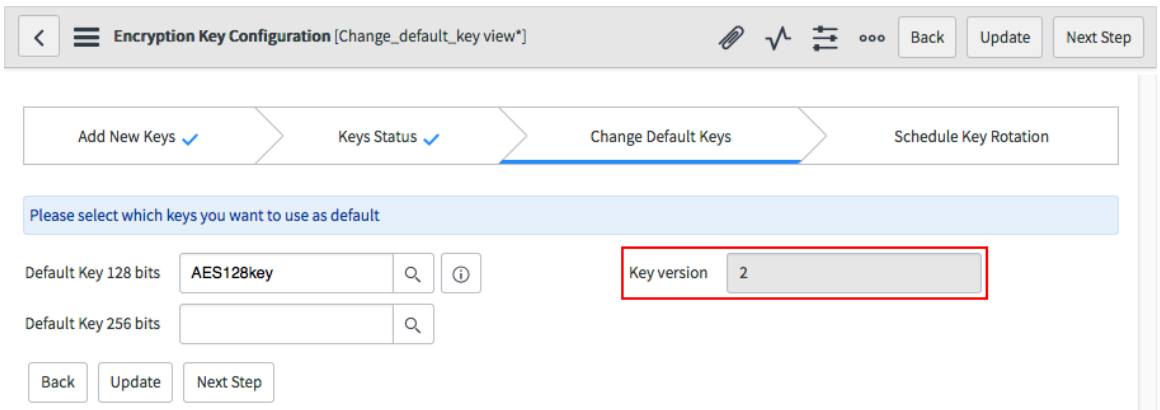
Sie müssen die Schlüsselversion in SafeNet einrichten, bevor Sie die SafeNet-Schlüsselversion auf dem Edge-Proxy-Server konfigurieren können.

Hinweis: Edge-Proxys, die vor installiert wurden London Release-Unterstützung für SafeNet-Schlüssel, aber keine SafeNet-Schlüsselversionsverwaltung. Wenn Sie versehentlich einen versionierten Schlüssel auf einem verwenden Kingston Oder ein früherer Proxy, wenn Sie ein Upgrade auf durchführen London Oder neuere Version, die London Oder später erkennt der Proxy dieses Problem, und um einen potenziellen Datenverlust zu verhindern, wird der Proxy nicht gestartet.

Sie müssen zunächst einen Auftrag für eine Massenschlüsselrotation oder einen einzelnen Schlüsselrotationsauftrag planen, um den alten SafeNet versionierten Schlüssel durch einen nicht versionierten Schlüssel zu ersetzen, und dann bei Bedarf einen neuen SafeNet versionierten Schlüssel erstellen. Dieser neue versionierte Schlüssel kann sicher mit verwendet werden London Oder später Proxy, und Sie können den Proxy neu starten.

Konfiguration des Verschlüsselungsschlüssels

Bei Verwendung von mit SafeNet versionierten Schlüsseln enthält der Abschnitt „Ändern des Abschnitts Standardschlüssel im Formular zur Konfiguration des Verschlüsselungsschlüssels“ neue Felder für die **Schlüsselversion** der standardmäßigen 128-Bit- und 256-Bit-Schlüssel. Die Felder für die **Schlüsselversion** sind ausgegraut und können nicht bearbeitet werden.



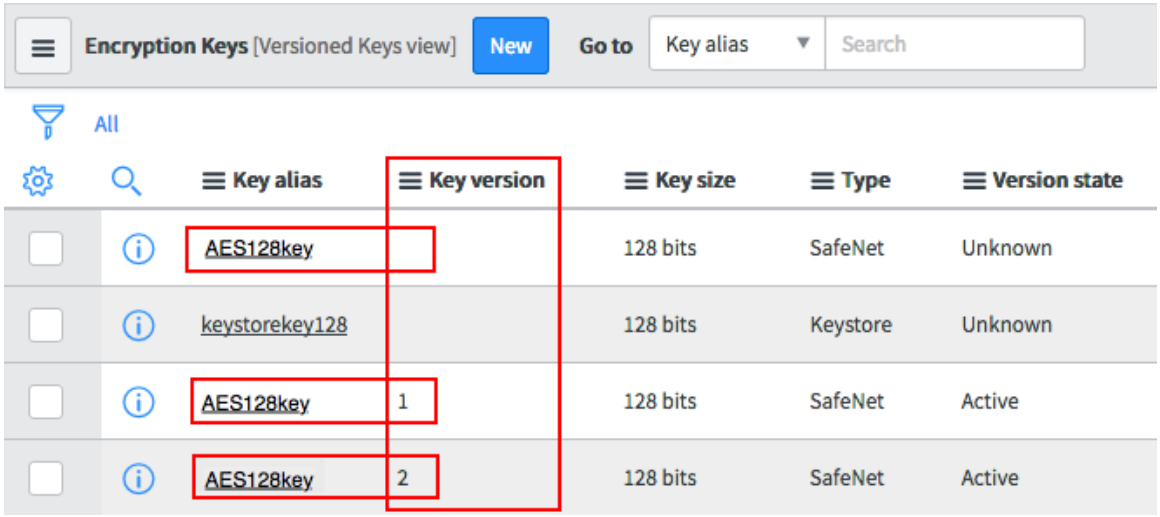
Hinweise zu Verfahren siehe Verschlüsselungsschlüssel für die Instanz konfigurieren.

Versionierte Schlüssel

Wenn Sie versionierte SafeNet-Schlüssel verwenden, wenn Sie zu navigieren **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Alle Schlüssel**, Versionierte Schlüssel enthalten **Schlüsselversion** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Für die ersten Einträge, die Sie im Abschnitt „Standardschlüssel ändern“ des Formulars „Konfiguration der Verschlüsselungsschlüssel“ vornehmen, wird keine Versionsnummer angezeigt. Wenn der Proxy-Server einen Schlüssel von SafeNet anfordert, fügt das System eine neue Zeile für den Aliasnamen und die **Schlüsselversion** hinzu.

Im obigen Beispiel ist **AES128key** dreimal aufgeführt:

- Die erste Auflistung ohne angegebener **Schlüsselversion** ist der erste Eintrag.
- Die zweite Auflistung mit **1** in der Spalte **Schlüsselversion** ist die erste Version des von SafeNet zurückgegebenen Schlüssels.
- Die dritte Auflistung mit **2** in der Spalte **Schlüsselversion** ist die zweite Version des von SafeNet zurückgegebenen Schlüssels.
- Da andere Versionen des Schlüssels von SafeNet zurückgegeben werden, werden neue Zeilen hinzugefügt, um die jetzt verwendete **Schlüsselversion** aufzuzeichnen.

Verschlüsselungskonfigurationen und -muster

Mit Edge Encryption können Felder verschlüsselt und Zeichenketten tokenisiert werden.

Verschlüsselungskonfigurationen

Sie können einzelne Felder mithilfe von Verschlüsselungskonfigurationen verschlüsseln. Edge Encryption Unterstützt 128-Bit-AES-Verschlüsselungsschlüssel. Wenn die Dateien der JCE-Richtlinie für uneingeschränkte Stärke der Java Cryptography Extension (JCE) installiert sind, Edge Encryption Unterstützt 256-Bit-AES-Verschlüsselungsschlüssel für jeden Verschlüsselungstyp. Edge Encryption Unterstützt die folgenden Arten von Verschlüsselungskonfigurationen.

Standardverschlüsselung

Der verschlüsselte Wert eines Felds unterscheidet sich jedes Mal, wenn das Feld verschlüsselt wird, auch wenn der Feldwert gleich bleibt. Standardverschlüsselung ist die robusteste Form der Verschlüsselung. Felder, die Standardverschlüsselung verwenden, können nicht sortiert, gruppiert oder gefiltert werden.

Gleichstellungserhaltende Verschlüsselung

Der verschlüsselte Wert eines Felds ist derselbe, wenn der Feldwert derselbe bleibt. Unterstützt Gleichstellungsvergleiche und Gruppieren nach Operationen in einem Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn für ein Feld, das bereits Daten enthält, die gleichstellungserhaltende Verschlüsselung ausgewählt wird, werden bei der Gruppierung nach Aktion für das Feld möglicherweise keine Felder mit demselben Wert gruppiert, wenn eines verschlüsselt ist und das andere nicht.

Ordnungserhaltende Verschlüsselung

Verwendet Token und Verschlüsselung, um Daten in Ihrer Proxy-Datenbank zu sichern. Unterstützt Gleichstellungsvergleiche, Gruppieren nach Operationen und die Möglichkeit der Datensortierung. Der ordnungserhaltende Verschlüsselungstyp wird nur unterstützt, wenn eine MySQL-Datenbank für den Edge Encryption Proxy-Server konfiguriert ist.

Hinweis: Wenn die ordnungserhaltende Verschlüsselung verwendet wird und die Proxy-Datenbank inaktiv ist, können Aktualisierungen an Feldern mit ordnungserhaltender Verschlüsselung vorgenommen werden. Die Sortierreihenfolge ist jedoch beim Versuch, Daten anhand dieser Felder zu sortieren, nicht korrekt. Gruppen funktionieren ebenfalls nicht wie erwartet. Wenn die Proxy-Datenbank wieder betriebsbereit ist, planen Sie einen Auftragstoken-Reparaturauftrag ein, um fehlende Token zu reparieren.

Verschlüsselungstypen

Die folgenden Verschlüsselungstypen sind gemäß abnehmender Sicherheitsqualität aufgeführt.

Verschlüsselungstyp	Beschreibung
Standard AES 256	Felder können nicht gefiltert, sortiert oder verglichen werden.
Standard AES 128	Felder können nicht gefiltert, sortiert oder verglichen werden.
Gleichstellungserhaltung von AES 256	Felder können mit Gleichstellungsvergleichen gefiltert werden.
Gleichstellungserhaltung von AES 128	Felder können mit Gleichstellungsvergleichen gefiltert werden.
Ordnungserhaltung von AES 256	Felder können sortiert und Gleichstellungsfilterung verwendet werden. Erfordert die Verwendung einer MySQL-Datenbank in Ihrem Netzwerk.
Ordnungserhaltung von AES 128	Felder können sortiert und Gleichstellungsfilterung verwendet werden. Erfordert die Verwendung einer MySQL-Datenbank in Ihrem Netzwerk.

Verschlüsselungsmuster

Sie können vertrauliche Daten in Zeichenfolgen mithilfe von Verschlüsselungsmustern schützen. Sobald ein Verschlüsselungsmuster gespeichert und aktiviert ist, identifiziert der Edge Encryption Proxy-Server Zeichenfolgen, die dem Muster in Anforderungen entsprechen. Nach der Suche wird die Klartextzeichenfolge in der Proxy-Datenbank gespeichert und in der Instanz durch ein Token ersetzt. Verwenden Sie Verschlüsselungsmuster, um Zeichenketten zu kennzeichnen, die regulären Mustern entsprechen, z. B. Sozialversicherungs- und Kreditkartennummern. Wir empfehlen, dass Verschlüsselungskonfigurationen die primäre Verschlüsselungsmethode sind. Verwenden Sie jedoch Verschlüsselungsmuster als Ergänzung, um vertrauliche Informationen zu finden und zu schützen, die außerhalb verschlüsselter Felder gefunden werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der Edge Encryption Proxy-Server erfordert nur eine MySQL-Datenbank in Ihrem Netzwerk, wenn Sie ordnungserhaltende Verschlüsselungs- oder Verschlüsselungsmuster verwenden. Klartextwerte werden in der Proxy-Datenbank in Ihrem Netzwerk gespeichert. Aus diesem Grund ist es wichtig, dass Sie Ihre Proxy-Datenbank schützen und regelmäßig sichern. Empfehlungen finden Sie unter Komponenten der Edge Encryption.

Zugehörige Informationen

Felder mit Verschlüsselungskonfigurationen verschlüsseln

Zeichenketten mithilfe von Verschlüsselungsmustern tokenisieren

Mit Edge Encryption installiert

Edge Encryption installiert Tabellen zum Speichern verschlüsselungsbezogener Daten, Systemeigenschaften zum Konfigurieren des Standardverhaltens und die Rolle edge_encryption zur Verwaltung von Edge Encryption.

Mit Edge Encryption installierte Tabellen

Edge Encryption fügt die folgenden Tabellen hinzu.

Edge Encryption-Konfiguration [sys_Encryption_Configuration]

Enthält verschlüsselte Felder und Tabellen, für die Anhänge verschlüsselt werden.

Edge Encryption-Regel [sys_Encryption_rule]

Enthält für jede Regel einen Datensatz. Eine Regel hat einen Namen, die Bedingung für deren Verwendung, ein Skript und ein Auftragsfeld.

Edge Encryption – Ungültiges Einfügeprotokoll [sys_Edge_Encryption_invalid_insert_log]

Enthält Protokollnachrichten, die für Versuche erstellt wurden, unverschlüsselte Daten in einem verschlüsselten Feld zu speichern.

Edge Encryption-Proxy [sys_Encryption_Proxy]

Enthält Informationen zur Verschlüsselungs-Proxy-Anwendung.

Edge-Proxy-Verschlüsselungstyp [sys_Proxy_Encryption_type]

Wird zum Aktivieren und Deaktivieren von Verschlüsselungstypen im Verschlüsselungsformular verwendet.

Ausführung des Verschlüsselungsauftrags [sys_Encryption_Job_Execution]

Unterstützt Aufträge zur Massenverschlüsselung.

Ausführungsblock des Verschlüsselungsauftrags [sys_Encryption_Job_Execution_Chunk]

Unterstützt Aufträge zur Massenverschlüsselung.

Geplanter Verschlüsselungsauftrag [sysauto_Encryption_Job]

Listet geplante Aufträge für die Verschlüsselung, Entschlüsselung, Schlüsselrotation, Auftragstokenreparatur und Datenbankwiederherstellung auf.

Konfiguration des Verschlüsselungsschlüssels [sys_Encryption_key_Configuration]

Listet die Standard-Verschlüsselungsschlüssel auf.

Verschlüsselungsschlüssel [sys_Encryption_key]

Listet die verfügbaren Schlüssel und Schlüsselattribute auf.

Proxy-Verschlüsselungsschlüssel [sys_Encryption_Proxy_key]

Listet Proxy-Verschlüsselungsschlüssel auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Edge Encryption installierte Eigenschaften

Edge Encryption fügt die folgenden Eigenschaften hinzu.

Hinweis: Um die Tabelle „Systemeigenschaften“ [sys_properties] zu öffnen, geben Sie im Navigationsfilter `sys_properties.list` ein.

glide.edge.pattern.disallowed.chars

Eine Liste von Zeichen, die in Mustern nicht zulässig sind.

- **Typ**: eine Zeichenkette einer durch Komma getrennten Liste von Werten
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

glide.edge.pattern.min.size

Die minimal zulässige Mustergröße. Das Erlauben kleinerer Muster bedeutet, mehr Übereinstimmungen zu finden, was den Aufwand erhöht.

- **Typ**: Zahl
- **Standardwert**: 5
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.logging.destination

Wo Nachrichten protokolliert werden.

- **Typ**: Zeichenfolge
- **Standardwert**: Datei
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.logging.verbosity

Die zu verwendende Protokollierungsstufe.

- **Typ**: Zeichenfolge
- **Standardwert**: Info
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.encryption.proxy.buildtag

Die in Ihrer Instanz registrierte Proxy-Version.

- **Typ**: Zeichenfolge
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

sn_edge_encryption.cleartext.allowed

Bei „Wahr“ kann Klartext in einem verschlüsselten Feld gespeichert werden. Dies geschieht, wenn ein Benutzer auf die Instanz zugreift, ohne den Edge Encryption Proxy zu verwenden. Bei „Falsch“ verhindert das System, dass Klartext in einem verschlüsselten Feld gespeichert wird.

- **Typ**: Boolesch
- **Standardwert**: false
- **Speicherort**: Tabelle „Systemeigenschaften“ [sys_properties]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Edge Encryption planen

Die erfolgreiche Implementierung von Edge Encryption erfordert Planung und Vorbereitung.

Beantworten Sie die folgenden Fragen bereits in der Planungsphase.

- Welche Felder sollen verschlüsselt werden?
- Welche Verschlüsselungstypen sollen verwendet werden?
- Wie viele Edge Encryption Proxys werden benötigt? Empfehlungen und Überlegungen finden Sie unter Umgebungsgröße Ihrer Edge Encryption anpassen.
- Wo befindet sich die MySQL-Datenbank, wenn ein ordnungserhaltender Verschlüsselungstyp oder ein Verschlüsselungsmuster verwendet werden soll?
- Welches Schlüsselmanagementsystem soll verwendet werden?

Systemadministratoren, Netzwerkadministratoren und Mitglieder des Sicherheitsteams haben unterschiedliche Aufgaben bei der Implementierung von Edge Encryption zu erfüllen.

- Systemadministratoren benötigen die Sicherheitsadministratorrolle. Der Systemadministrator muss:
  - Die Edge Encryption Proxy-Anwendung herunterladen.
  - Ein Edge Encryption Benutzerkonto für die Proxys einrichten, die zur Verbindung mit der Instanz verwendet werden sollen. Dem Benutzer muss die Rolle edge_encryption zugewiesen werden.
  - Die Verschlüsselungsschlüssel konfigurieren und die Standardschlüssel festlegen.
  - Edge Encryption auf der Instanz konfigurieren.
  - Verschlüsselungsaufträge planen.
  - Edge Encryption überwachen.
  - Verschlüsselungsregeln erstellen und bearbeiten.
- Ihr Netzwerkadministrator muss:
  - Die Edge Encryption Proxy-Anwendung installieren.
  - Die Netzwerkadressen für die Proxy-Server und die Proxy-Datenbank kennen, die zur Aufrechterhaltung der Verschlüsselungs- und Verschlüsselungsmuster verwendet wird.
  - Die Proxy-Datenbank installieren, die zur Aufrechterhaltung der Verschlüsselung und Verschlüsselungsmuster verwendet werden soll.
  - Die Proxy-Anwendung starten und stoppen.
  - Die Verschlüsselungsverwaltung durchführen.
  - Bestimmen, wie Benutzer zu Verschlüsselungs-Proxy-Anwendungen zugeordnet werden. Dies kann mit DNS-Einstellungen oder Routing-Regeln erfolgen und ist netzwerkspezifisch.
  - Mehrere Proxy-Server verwalten.
  - Load-Balancer-Pools und -Einstellungen konfigurieren.
- Ihr Sicherheitsadministrator muss die Verschlüsselungstypen festlegen, die jedem Feld zugewiesen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge Encryption – Systemanforderungen

Sie können ausführen Edge Encryption Proxy-Anwendung auf Servern oder virtuellen Computern, die auf Microsoft Windows- oder Linux-Betriebssystemen ausgeführt werden. Stellen Sie für eine optimale Leistung sicher, dass Ihre Konfiguration diese Anforderungen erfüllt.

Java-Anforderungen

Der Hostcomputer, der installiert oder ausgeführt wird Edge Encryption Der Proxy-Server muss eine unterstützte Java-Version beibehalten. Aktuell unterstützte Versionen sind Java 11.0.6 oder höher in der 11.x-Versionsreihe

Hinweis: Java 8 wird ab nicht mehr unterstützt Utah Release. Aktualisieren Sie Ihre Umgebung mit Edge Encryption Proxy für Java 11, bevor Sie versuchen, zu installieren Utah Version von Edge Encryption Proxy.

Hinweis: Java lässt Schlüssel mit unbegrenzter Stärke nicht automatisch zu. Sie müssen die Verwendung von AES 256-Bit-Verschlüsselung speziell aktivieren.

Unterstützung für OpenJDK

Die ServiceNow AI Platform Unterstützt OpenJDK Version 11.

Mindestkonfiguration für Proxy-Server

Ein Proxy-Server erfordert diese Mindestkonfiguration:

- 4 GB RAM pro Proxy-Server (6 GB werden für die meisten Bereitstellungen empfohlen).

  Hinweis: Der Proxy-Server-Host benötigt mindestens 1 GB RAM mehr als der Proxy-Server. Der Proxy-Server-Host benötigt die zusätzliche 1 GB für Betriebssystemservices. Wenn Sie beispielsweise einen Proxy-Server für die Verwendung von 4 GB RAM konfigurieren, müssen Sie mindestens 5 GB RAM auf dem Proxy-Server-Host installieren.

  Da der Proxy-Server mindestens 4 GB Arbeitsspeicher benötigt, werden 32-Bit-JREs und 32-Bit-Betriebssysteme ab dem Release London nicht mehr unterstützt.

- CPU mit mindestens 3 GHz (CPU mit 4 Kernen, die für optimale Leistung bevorzugt wird).
- Mehrere einem Load Balancer nachgeschaltete Proxy-Server. Die Anzahl der benötigten Proxy-Server hängt von der Anzahl der Anwendungsknoten, der Anzahl gleichzeitiger Anwender und der Anzahl der für das Failover erforderlichen Server ab. Weitere Informationen finden Sie unter Umgebungsgröße Ihrer Edge Encryption anpassen.
- Fähigkeit, je nach Serverauslastung und Ressourcenverfügbarkeit gleichzeitig mit anderen Services auszuführen.

Von Proxy-Servern unterstützte Systeme

Die folgenden Systeme werden unterstützt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstütztes System	Beschreibung
Windows Server 2012, 2012-R2, 2016 und 2019 Editionen	• Virtuelle Maschinen oder physische Hardware • 64-Bit-Systeme
Linux	• Virtuelle Maschinen oder physische Hardware • 64-Bit-Systeme Auf 64-Bit-Linux-Systemen muss die 32-Bit GNU C-Bibliothek (glibc) installiert werden. Der Installationsbefehl für CentOS lautet Installieren Sie glibc.i686 .

Proxy-Server-Versionsanforderungen

Behalten Sie Ihr Edge Encryption Proxy-Version ist mit synchronisiert ServiceNow Instanzversion (z. B. derselbe Major-Release Tokyo). Um Ausfallzeiten während des Upgradeprozesses zu vermeiden Edge Encryption Proxy ist abwärtskompatibel. Es ist jedoch wichtig, so bald wie möglich ein Upgrade durchzuführen, um sicherzustellen, dass Anwender auf neue Funktionen und wichtige Fehlerkorrekturen zugreifen können.

Verbindungsanforderungen des Proxy-Servers

Der Proxy-Server, auf dem die Edge Encryption-Anwendung ausgeführt wird, muss mit den Computern in Ihrem Netzwerk kommunizieren können. Stellen Sie sicher, dass der Proxy-Server über folgende Netzwerkprivilegien verfügt:

Netzwerkberechtigung	Beschreibung
Firewall-Zugriff	Konfigurieren Sie Firewalls zwischen dem Proxy-Server und den Client-Geräten, um eine Verbindung zuzulassen. Wenn Ihr Netzwerk eine demilitarisierte Zone (DMZ) verwendet, um Ihrem LAN (Local Area Network) eine zusätzliche Sicherheitsebene hinzuzufügen, und wenn Ihre Netzwerksicherheitsprotokolle den Portzugriff innerhalb des Netzwerks auf die DMZ beschränken, müssen Sie möglicherweise einen Proxy-Server auf einem Computer innerhalb der DMZ bereitstellen.
Netzwerkzugriff	Konfigurieren Sie jeden Client, damit der Proxy-Server eine Verbindung mit ihm herstellen kann. Wenn Sie aufgrund der Netzwerksicherheit keine neuen Computer konfigurieren können, die eine Verbindung zu den Clients herstellen können, installieren Sie den Proxy-Server auf einem vorhandenen Computer mit Verbindungsberechtigungen.
Instanzzugriff	Stellen Sie sicher, dass der Proxy-Server über Netzwerkzugriff auf die Instanz verfügt. Stellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkberechtigung	Beschreibung
	Sie sicher, dass Sie das Proxy-Servernetzwerk so konfigurieren, dass Datenverkehr über TCP-Port 443 zulässig ist.
Netzwerkaccount	Installieren Sie den Proxy-Server entweder mit einem lokalen Administrator oder einem Domänenadministrator.

Anforderungen an das Datenbanksystem für die Ordnungserhaltung und die Tokenisierung

Um die Reihenfolge beizubehalten, müssen Sie eine Oracle MySQL-Datenbank für konfigurieren Edge Encryption Proxy-Server. Durch die Verschlüsselung, die die Reihenfolge bewahrt, kann jeder Vergleichsvorgang direkt auf verschlüsselte Daten angewendet werden, ohne dass die Daten zuerst entschlüsselt werden müssen. Mit Verschlüsselungsmustern können Sie Zeichenfolgenmuster durch Token ersetzen (als Tokenisierung bezeichnet), bevor sie an die Datenbank gesendet und in der Datenbank gespeichert werden. Verwenden Sie aufgrund der Größe der MySQL-Datenbank einen dedizierten Proxy-Server, um die Datenbank für Ordnungserhaltung und Tokenisierung auszuführen.

Die Mindestanforderungen für das Datenbanksystem umfassen:

MySQL-Datenbank	Anforderung
Version	MySQL-Datenbankversionen 5,7 und 8,0 **Hinweis:** MySQL-Versionen 5,5 und 5,6 werden nicht mehr getestet und haben das Ende des Supports erreicht.
BS	64-Bit-Systeme
CPU	CPU mit 2 oder mehr GHz (CPU mit 4 Kernen, die für optimale Leistung bevorzugt wird)
RAM	16 GB
Datenträger	Storage Area Network (SAN) oder lokaler Speicher (RAID 10 empfohlen)
Größe	Wird durch die Anzahl der potenziellen Datensätze multipliziert mit der Datensatzgröße bestimmt. Weitere Informationen finden Sie unter Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen.
Konfiguration	Hochverfügbarkeits-Cluster. Wenn Sie sich nicht sicher sind, wie Sie Ihren MySQL-Server konfigurieren, wenden Sie sich an MySQL Für Konfigurationsinformationen.

Umgebungsgröße Ihrer Edge Encryption anpassen

Die Auswahl der Anzahl von Proxy-Servern für Ihre Umgebung ist von hoher Bedeutung. Berücksichtigen Sie die Anzahl der Benutzer, die Redundanzanforderungen und die akzeptable Latenzzeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Redundanz

Verwalten Sie redundante Proxy-Server für den Fall eines Hardwarefehlers. Proxy-Server sollten einem Load Balancer nachgeschaltet sein, um einen funktionalen Pfad für alle Benutzer bereitzustellen, wenn ein Proxy-Server nicht erreichbar ist. Stellen Sie sicher, dass immer mindestens zwei Proxy-Server verfügbar sind.

Größe

Die Größe bezieht sich auf die Anzahl der Proxy-Server, die erforderlich sind, um zusätzliche Latenzzeiten zu vermeiden, die durch die Verschlüsselung von Daten entstehen. Je nach Verwendung möchten Sie möglicherweise die Latenzzeit reduzieren, indem Sie zusätzliche Proxy-Server hinzufügen. Wenn beispielsweise regelmäßige Massenverschlüsselungen ausgeführt werden, fügen Sie zur Handhabung der Last zusätzliche Proxy-Server hinzu oder führen Sie die Massenverschlüsselungen bei geringer Benutzerlast durch. Außerdem beeinflusst die Hardware, auf der der Proxy-Server ausgeführt wird, die Leistung und Latenz. Proxy-Server, die auf Hardware mit schnelleren CPUs, mehr CPUs und mehr RAM laufen, haben einen höheren Durchsatz als langsamere, begrenzte Systeme.

In den folgenden Richtlinien wird davon ausgegangen, dass der Proxy-Server mindestens die Mindesthardwareanforderungen erfüllt. So bestimmen Sie die Anzahl der Proxy-Server:

- Erwägen Sie, für jeweils zwei Anwendungsknoten in der Instanz einen Proxy-Server einzurichten.
- Richten Sie aus Gründen der Redundanz mindestens zwei Proxy-Server hinter einem Load Balancer ein.
- Fügen Sie für jeweils 500 gleichzeitige Benutzer einen zusätzlichen Proxy-Server hinzu.
- Fügen Sie je nach gewünschter Redundanz weitere Proxy-Server für das Failover hinzu.

Für eine Instanz mit 2.000 Benutzern sollten Sie beispielsweise mindestens fünf Proxy-Server einem Load Balancer nachgeschaltet sein. Diese Berechnung umfasst einen Proxy-Server für jeweils 500 Benutzer und einen zusätzlichen Proxy-Server für Failover. Bestimmen Sie im Voraus, wann Sie sich einem Schwellenwert von 500 Benutzern nähern, und platzieren Sie einen anderen Proxy-Server im Load-Balancer-Pool.

Load Balancers

Um Anforderungen zu verteilen und die Antwortzeit des Servers zu verbessern, verteilen Sie Proxy-Server in einem Load-Balancer-Pool. Konfigurieren Sie Load Balancer für die Verwendung nach der Methode der „wenigsten Verbindungen“. Diese Methode verbindet Anfragen mit dem Proxy-Server mit den wenigsten aktiven Verbindungen, wodurch die Überlastung eines einzelnen Proxys verhindert wird.

CPU-Auslastung

Da Datenverschlüsselung und Tokenisierung CPU-intensive Operationen erfordern, sind CPU-Spitzen während der Datenverschlüsselung normal und zu erwarten. Wenn die CPU-Auslastung mehrere Minuten lang über 80 % liegt, bedeutet dies wahrscheinlich, eine zu hohe Auslastung des Proxy-Servers. In diesem Fall erhöht sich die Latenz für den Zeitraum, in dem die CPU-Auslastung hoch ist. Wenn die Latenz bestehen bleibt, kann das Hinzufügen eines weiteren Proxy-Servers zur Verringerung der Latenz beitragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsspeicher

Der Proxy-Server muss über mindestens 4 GB RAM verfügen (empfohlen sind 6 GB). Legen Sie die anfänglichen und oberen Speichergrenzen des Proxy-Servers auf die empfohlenen Einstellungen fest.

Die Größe der Datenbank für die Ordnungserhaltung und Tokenisierung berechnen

Wenn Sie ordnungserhaltende Verschlüsselung oder Verschlüsselungsmuster verwenden, bestimmen Sie die Größe Ihrer MySQL-Datenbank, indem Sie die Anzahl der potenziellen Datensätze mit der Datensatzgröße multiplizieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie eine dedizierte Maschine, um die Datenbank für die Ordnungserhaltung und die Tokenisierung auszuführen. Führen Sie die Datenbank nicht auf derselben Hardware wie der Proxy-Server aus.

Prozedur

1. Bestimmen Sie die potenzielle Anzahl von Datensätzen, die Felder enthalten können, die mit auftragserhaltender Verschlüsselung verschlüsselt sind.
   a. Multiplizieren Sie die Anzahl der Verschlüsselungskonfigurationen mithilfe der auftragserhaltenden Verschlüsselung mit der Anzahl der Datensätze, auf die jede Konfiguration angewendet wird.
   b. Um Wachstum zu ermöglichen, multiplizieren Sie das Ergebnis mit drei.
2. Multiplizieren Sie das Ergebnis aus Schritt 1 mit 1.536.
   1.536 ist die durchschnittliche Größe eines Datensatzes in Bytes.
3. Wenn Sie Verschlüsselungsmuster verwenden, führen Sie die Schritte 1 und 2 für Datensätze mit Token aus, und fügen Sie das Ergebnis zur Summe hinzu.

Ergebnis

Der berechnete Wert ist die empfohlene Größe in Bytes für Ihre auftragserhaltende und tokenisierende Datenbank.

Edge Encryption Einschränkungen

Edge Encryption wirkt sich auf Systemfunktionen aus. Bewerten Sie sorgfältig die Auswirkungen der Verschlüsselung eines Feldes.

Feldtypeinschränkungen

Sie können nur die folgenden Feldtypen verschlüsseln:

- Datum
- E-Mail
- Datum/Uhrzeit
- HTML
- IP-Adresse
- Journal

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Journaleingabe
- Mehrzeiliger Text
- Einzeiliger Text
- Zeichenfolge
- URL

Sie können die folgenden Feldtypen nicht verschlüsseln:

- Auswahlfelder
- Virtuelle Felder
- Felder in Systemtabellen, mit Ausnahme bestimmter Felder in sys_user
- Systemfelder in Tabellen
- Nummerieren Sie Felder oder Felder, die einem automatischen Nummerierungsschema zugeordnet sind
- Jeder andere Feldtyp, der oben nicht aufgeführt ist

Zusätzliche Einschränkungen:

- Wenn ein Journalfeld verschlüsselt ist, wird **Veröffentlichen** Die Schaltfläche ist inaktiv, auch wenn mehrere Journalfelder vorhanden sind und nur eines dieser Felder verschlüsselt ist.
- Verschlüsselte Felder sind in nicht verfügbar **Wechseln Sie zu** Und Header-Filterfelder.
- Beim Verschlüsseln von Feldern, die als Index verwendet werden, können Sie nur Verschlüsselungstypen mit Reihenfolgeerhaltung und Gleichheitserhaltung verwenden. Indizierte Felder können nicht mit dem Standardverschlüsselungstyp verschlüsselt werden.

Weitere Informationen finden Sie unter Feldtypen .

Filter- und Suchbeschränkungen

Standardverschlüsselung

Wenn Sie ein Feld Zeichenfolge, Datum, Datum/Uhrzeit oder URL mit einer standardmäßigen verschlüsselten Feldkonfiguration als linken Operanden in einem Filter auswählen, sind keine Filteroptionen verfügbar.

Gleichstellungserhaltende Verschlüsselung

Wenn Sie ein Feld „Zeichenfolge“, „Datum“, „Datum/Uhrzeit“ oder „URL“ mit einer gleichheitsbewahrenden verschlüsselten Feldkonfiguration als linken Operanden in einem Filter auswählen, sind die folgenden Operatoren verfügbar:

- **ist**
- **ist nicht**
- **Ist leer**
- **ist nicht leer**

Ordnungserhaltende Verschlüsselung

Wenn Sie ein Zeichenfolgenfeld mit einer reihenerhaltenden verschlüsselten Feldkonfiguration als linken Operanden in einem Filter auswählen, sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zusätzlich zu die folgenden Operatoren verfügbar **Ist** , **Ist nicht** , **Ist leer** , Und **Ist nicht leer** :

- **größer als**
- **weniger als**

Wenn Sie ein Datums- oder Datums-/Uhrzeitfeld mit einer reihenerhaltenden verschlüsselten Feldkonfiguration als linken Operanden in einem Filter auswählen, sind zusätzlich zu die folgenden Operatoren verfügbar **Ist** , **Ist nicht** , **Ist leer** , Und **Ist nicht leer** :

- **Nach**
- **Vor**
- **Nach oder am**
- **Vor oder am**

Datums- und Datums-/Uhrzeitauswahl

Verwenden Sie für Datumsfelder die Datumsauswahl, um das Datum anzugeben:



Verwenden Sie für Datums-/Uhrzeitfelder die Datums- und Uhrzeitauswahl, um Datum und Uhrzeit anzugeben:



Listenbedingungsfilter

Die **Übereinstimmungen Anzeigen** Und **Herausfiltern** Optionen werden in Listen unterstützt. Nur genaue Übereinstimmungen werden zurückgegeben oder herausgefiltert.

Hinweis: Das Hinzufügen verschlüsselter Felder in Bedingungsfiltern wird in Skripts wie UI-Richtlinien und Business-Regeln unterstützt.

Konfigurationseinschränkungen

Einschränkungen und Verhalten von Verschlüsselungskonfigurationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nachdem Sie ein Feld zu hinzugefügt haben Edge Encryption Konfigurationstabelle, Sie können den Konfigurationsdatensatz nicht löschen. Wenn Sie ein Feld nicht mehr verschlüsseln möchten, deaktivieren Sie den Datensatz in der Edge Encryption-Konfigurationstabelle und planen Sie einen Verschlüsselungsauftrag zum Entschlüsseln der Daten.
- Wenn ein Feld in einer übergeordneten Tabelle als verschlüsselt markiert ist, wird das Feld auch in allen geerbten Tabellen verschlüsselt. Beispiel: Wenn **Kurzbeschreibung** Feld in der Aufgabentabelle wird verschlüsselt, dann der Inhalt von **Kurzbeschreibung** Feld in der Incident-Tabelle sind verschlüsselt.
- Wenn ein von einer übergeordneten Tabelle geerbtes Feld als verschlüsselt markiert ist, kann das Feld in der übergeordneten Tabelle nicht verschlüsselt werden. Beispiel: Wenn **Kurzbeschreibung** In der Incident-Tabelle ist als verschlüsselt markiert, dann ist **Kurzbeschreibung** In der Aufgabentabelle kann nicht verschlüsselt werden. In diesem Beispiel können Sie verschlüsseln **Kurzbeschreibung** In der Problemtabelle.
- Wenn ein Feld mit einer definierten Verschlüsselungskonfiguration in ein beliebiges Format exportiert wird, enthält die Ausgabe auch dann verschlüsselte Werte, wenn sie über den Proxy-Server exportiert werden.
- Sie können keine Daten in ein Feld mit einer definierten Verschlüsselungskonfiguration importieren.
- Sie können geerbte Datums- und Datums-/Uhrzeitfelder nicht verschlüsseln. Datums- oder Datums-/Uhrzeitfelder, die von einer übergeordneten Tabelle geerbt wurden, werden nicht in aufgeführt **Spalte** Feld-Dropdown-Liste, und Sie können keine Datums- oder Datums-/Uhrzeitverschlüsselungskonfigurationen für diese Felder erstellen.
- Sie können eine Zeichenfolge oder ein URL-Feld nur aus einer übergeordneten Tabelle oder einer untergeordneten Tabelle verschlüsseln, aber nicht aus beiden.

Instanzeinschränkungen

Auswirkung der Verwendung Edge Encryption In der Instanz:

- Die Back-End-Logik kann verschlüsselte Daten nicht verarbeiten. Wenn die Instanz verschlüsselte Daten enthält, werden alle Business-Regeln, Back-End-Skripts oder Back-End-Funktionen, die auf der Auswertung der Daten im verschlüsselten Feld basieren, nicht ordnungsgemäß ausgeführt.

  Hinweis: Daten, die mit einer gleichstellenden oder ordnungspolitischen Verschlüsselung verschlüsselt werden, bestehen im Vergleich zu einem identischen verschlüsselten Wert weiterhin Gleichwertigkeitsprüfungen.

- Da die E-Mail-Verarbeitung von den E-Mail-Systemen direkt an die Instanz erfolgt und den Edge-Proxy nicht passieren kann, können Daten, die per E-Mail gesendet oder gesendet werden, vom Edge-Proxy nicht verschlüsselt oder entschlüsselt werden.
  - Daten und Anhänge in eingehenden E-Mails sind nicht verschlüsselt.
  - Daten und Anhänge in ausgehenden E-Mails bleiben verschlüsselt und können nicht entschlüsselt werden.
- Auf dem Server ausgeführte Skripts können verschlüsselte Daten nicht ändern.
- Globale Suche wird nicht unterstützt. Da die globale Suche versucht, sowohl verschlüsselte als auch Klartextdaten zu durchsuchen, sind die Ergebnisse möglicherweise nicht wie erwartet.
- Verschlüsselte Daten können nicht kopiert und in einen Datensatz eingefügt werden, in dem das Feld nicht verschlüsselt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Abhängig vom ausgewählten Verschlüsselungstyp wird die Benutzeroberflächenfunktionalität für die verschlüsselten Felder reduziert. Beispielsweise kann die Möglichkeit zum Vergleichen, Gruppieren, Sortieren und Suchen beeinträchtigt werden Generell gilt: Je stärker die gewählte Verschlüsselung, desto mehr Funktionalität wird eingeschränkt.
- Mit Ausnahme von Java-Schlüsselspeicher, SafeNet und Unbound Technology wird keine Verwaltung von Verschlüsselungsschlüsseln von Drittanbietern unterstützt.
- Obwohl mehrere Proxy-Server, die mit einer einzelnen Instanz verbunden sind, unterstützt werden, sind die Verwaltung und Überwachung von Verschlüsselungs-Proxy-Clustern nicht verfügbar. Jeder Proxy muss separat verwaltet werden.
- Systemkonfigurationen wie Auslastung und Anzahl der verschlüsselten Felder können sich auf die Leistung der verschlüsselten Felder auswirken.
- Der Edge Encryption Proxy-Server kann nur eine Verbindung zu einer einzelnen Instanz herstellen.
- Wenn Ihre Instanz eine Oracle-Datenbank verwendet und das Feld Zeichenfolge, das Sie als verschlüsselt markieren, mehr als 2925 Zeichen enthält, kann dieses Feld nicht sortiert werden, auch wenn die Verschlüsselung für die Beibehaltung der Reihenfolge ausgewählt ist.
- Wenn Ihre Instanz eine Oracle-Datenbank verwendet, ist Unicode AL32UTF8 der einzige unterstützte Zeichensatz.
- Verschlüsselte Daten können nicht in Berichten verwendet werden.
- Edge Encryption Kann nicht mit Datenarchivierung verwendet werden.
- Edge Encryption-Proxys können keine Anforderungen verschlüsseln, die die Batch-REST-Anforderungs-API verwenden. Wenn Sie Edge Encryption-Proxys verwenden, deaktivieren Sie REST Batching, indem Sie festlegen `Glide.uxf.disable_Rest_Batching` Systemeigenschaft auf „wahr“.

Edge Encryption Wird Installiert

Sie können einen Edge Encryption Proxy manuell oder mithilfe des interaktiven Installers Edge Encryption installieren.

Java-Anforderungen

Der Hostcomputer, der installiert oder ausgeführt wird Edge Encryption Der Proxy-Server muss eine unterstützte Java-Version beibehalten. Aktuell unterstützte Versionen sind Java 17.0.3 oder höher in der 17.x-Versionsreihe.

Hinweis: Java 11 wird ab dem Yokohama-Release nicht mehr unterstützt. Aktualisieren Sie Ihre Umgebung mit Edge Encryption Proxy für Java 17, bevor Sie versuchen, Yokohama oder höhere Versionen von zu installieren Edge Encryption Proxy.

Proxy-Server installieren

Das Installieren von Edge Encryption beinhaltet diese Schritte.

- Installieren Sie die Edge Encryption Proxy-Anwendung auf einem Server in Ihrem Netzwerk mithilfe des interaktiven oder des manuellen Installationsprogramms.
- Generieren Sie das RSA-Schlüsselpaar für die digitale Signatur von Verschlüsselungskonfigurationen und Verschlüsselungsregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Installieren Sie die Java Cryptography Extension (JCE), wenn Sie die AES 256-Verschlüsselung verwenden möchten.
- Wenn Sie eine sichere SSL-Verbindung verwenden, beziehen Sie ein Serverzertifikat und importieren Sie es in den Java KeyStore.
- Richten Sie Ihren Schlüsselspeicher und den Verschlüsselungsschlüssel ein.
- Wenn ordnungserhaltende Verschlüsselungstypen oder Verschlüsselungsmuster verwendet werden sollen, richten Sie eine MySQL-Datenbank auf einem Computer in Ihrem Netzwerk ein.
- Stellen Sie die gewünschten Eigenschaften ein. Eigenschaften befinden sich in der Konfigurationsdatei edgeencryption.properties.
- Geben Sie an, dass ein Proxy-Server eine vertrauenswürdige Quelle ist Edge Encryption Kann Anforderungen verarbeiten, die von diesem Proxy-Server stammen.

Zugriff auf den Proxy-Server

Verweisen Sie nach Abschluss der Installation den Browser jedes Benutzers auf den Edge Encryption Proxy mit dem URL-Format: <host>:<port>. Werte werden durch die Host- und Port-Eigenschaften in der Datei edgeencryption.properties bestimmt.

Ein Beispiel mit folgenden Werten:

Eigenschaft	Beispielwert
edgeencryption.proxy.host	hostname.mycompany.com
edgeencryption.proxy.http.port	8081

Ein Client greift unter der folgenden Adresse auf den Proxy-Server zu: http://hostname.mycompany.com:8081/.

Hinweis: DNS-Einstellungen und Routing-Regeln können verwendet werden. Host- und Portwerte werden von Ihrem Netzwerkadministrator festgelegt.

Edge Encryption anfordern

Die Edge Encryption Plugin (com.Glide.edgecryption) ist als separates Abonnement verfügbar.

Vorbereitungen

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

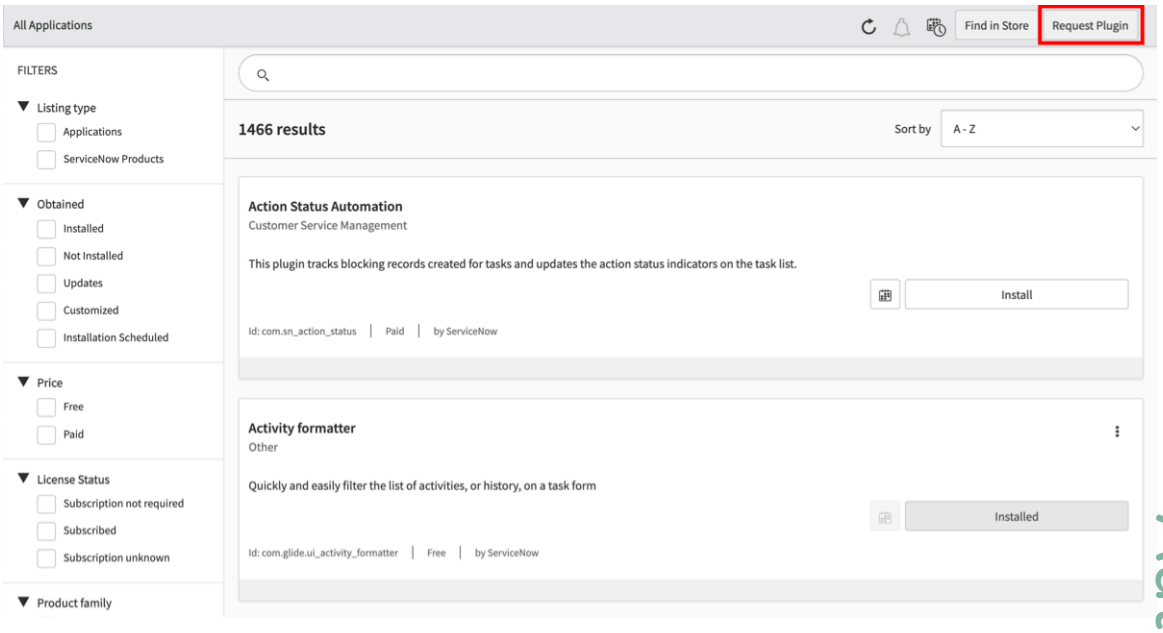
Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Erforderliche Rolle: keine

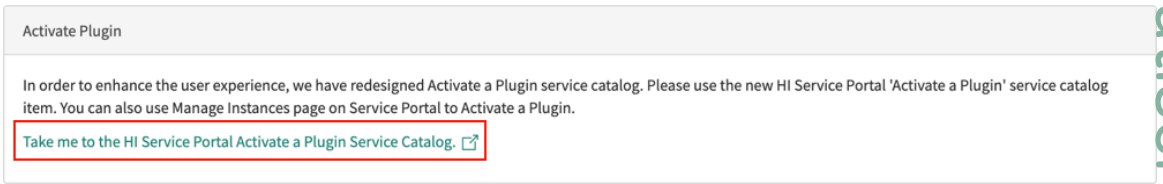
Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.

5. Wählen Sie **Aktionen > Plugin aktivieren** aus.

6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
	Datum und Uhrzeit zum Aktivieren des Plugins.

Automatische Übersetzung

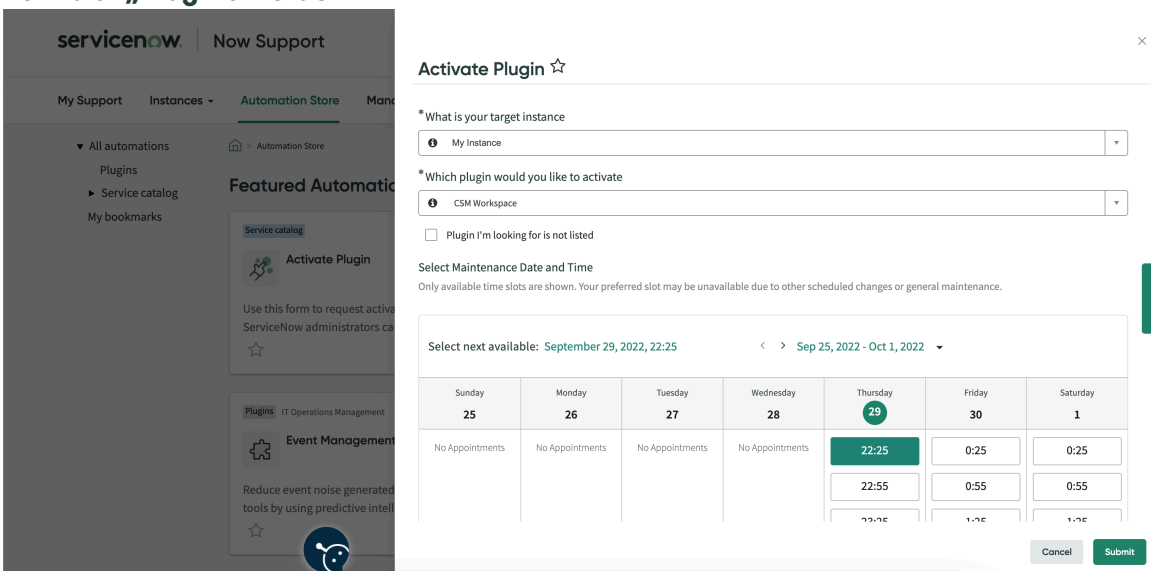
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	**Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Richten Sie einen Edge Encryption-Anwenderaccount ein

Die Edge Encryption Proxys stellen als Benutzer eine Verbindung mit der Instanz her, um Informationen zur Verschlüsselungskonfiguration zu erhalten und zu aktualisieren. Erstellen Sie zu diesem Zweck ein Benutzerkonto, und weisen Sie dem Benutzer die Edge Encryption-Rolle zu.

Vorbereitungen

Das Edge Encryption Plugin muss installiert sein, bevor Sie die Rolle zuweisen können.

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie auf Ihrer ServiceNow-Instanz ein Benutzerkonto, das von den Edge Encryption Proxy-Anwendung verwendet werden soll.
2. Weisen Sie dem Benutzer die Edge Encryption-Rolle zu.

Proxy-Server für die Edge Encryption herunterladen

Laden Sie die Edge Encryption Proxy-Server-Anwendung aus Ihrer Instanz herunter, und kopieren Sie die Datei auf jeden Computer, auf dem der Edge Encryption Proxy-Server ausgeführt werden soll.

Vorbereitungen

Bevor Sie dieses Verfahren starten, muss das Edge Encryption Plugin auf Ihrer Instanz installiert und aktiviert sein.

Hinweis: Die Edge EncryptionProxy wird offiziell nur in Oracle JRE unterstützt.

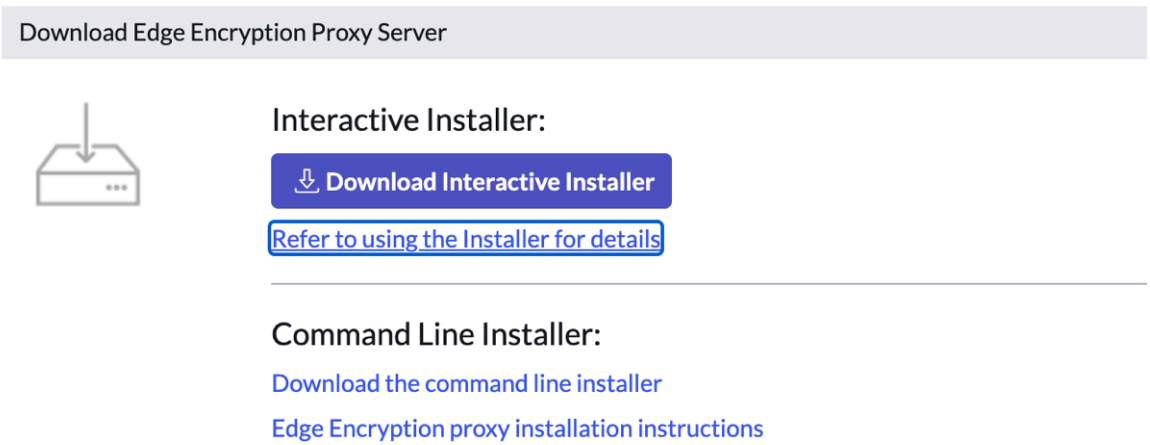
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**an.
2. Um das interaktive Installationsprogramm zu verwenden, klicken Sie auf **Laden Sie Das Interaktive Installationsprogramm Herunter** .

   Wenn Sie den Proxy-Server manuell installieren, wählen Sie die Betriebssystemversion für Ihren Proxy-Server aus.



   Hinweis: Da der Proxy-Server mindestens 4 GB Arbeitsspeicher benötigt, werden 32-Bit-JREs und 32-Bit-Betriebssysteme ab nicht mehr unterstützt Washington DC Release.

3. Kopieren Sie das Installationsprogramm auf jeden Computer, auf dem der Edge Encryption Proxy-Server ausgeführt werden soll.

   Hinweis: Wenn Sie manuell installieren Edge Encryption Proxy-Server, kopieren Sie die ZIP-Datei auf jeden Computer, auf dem ausgeführt werden soll Edge Encryption Proxy-Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Nach dem Herunterladen des Edge Encryption Installationsprogramms, Den Proxy-Server für die Edge Encryption mithilfe des interaktiven Installationsprogramms installieren. Bei manueller Installation, Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren.

Den Proxy-Server für die Edge Encryption mithilfe des interaktiven Installationsprogramms installieren

Installieren Sie den Edge Encryption Proxy-Server auf einem Windows- oder Linux-Computer mit dem interaktiven Installationsprogramm.

Vorbereitungen

Hinweis: SafeNet KeySecure-Keystore-Dateien werden vom Edge Encryption Installationsprogramm nicht unterstützt. So verwenden Sie einen SafeNet KeySecure-Keystore: Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren.

Das Edge Encryption Plugin muss in Ihrer Instanz installiert und aktiviert sein, bevor Sie dieses Verfahren starten. Stellen Sie sicher, dass Java-Version 11.0.6 oder höher auf dem Computer installiert ist, auf dem die ausgeführt wird Edge Encryption Installationsprogramm.

Erforderliche Rolle:

- security_admin auf Ihrer ServiceNow Instanz
- Lokaler oder Domänenadministrator auf einem Windows-Host
- Service-Benutzer mit vollem Dateisystemzugriff auf einem Linux-Host

Warum und wann dieser Vorgang ausgeführt wird

Nach der Installation eines neuen Proxy-Servers können Sie das Installationsprogramm erneut zur Durchführung von Tests ausführen, um Probleme bei der Installation zu erkennen oder die aktuellen Einstellungen zu ändern. Folgende Optionen stehen zur Verfügung:

- **Neu installieren**: Installieren Sie einen neuen Proxy-Server.
- **Installation überprüfen**: Führen Sie Tests durch, um Probleme bei einer früheren Installation zu erkennen und zu beheben.
- **Vorhandene neu installieren**: Führen Sie Tests durch, um Probleme in einer früheren Installation zu erkennen und zu beheben und vorhandene Einstellungen anzuzeigen oder zu ändern.

Hinweis: Wenn Sie den Proxy-Server auf einem Linux-Computer an einem privilegierten Port (Port 80 oder 443) installieren, müssen Sie das Installationsprogramm als Root-Benutzer mit vollem Dateisystemzugriff ausführen. Um den Dateisystemzugriff nach der Installation des Proxy-Servers einzuschränken, können Sie die SetUID-Funktion im Proxy-Installationsprogramm verwenden. Um diese Funktion zu aktivieren, starten Sie das Installationsprogramm als „Root“ oder „Sudo Root“. Wenn Sie vom Installationsprogramm dazu aufgefordert werden, geben Sie den Benutzernamen und die Benutzergruppe eines nicht privilegierten Benutzers an. Der Proxy-Server wird mit den Dateisystemberechtigungen des angegebenen Benutzers installiert. Sie können diesen Schritt überspringen, um die Standardinstallation mit Root-Berechtigungen fortzusetzen.

Prozedur

Verwenden Sie das Installationsprogramm, um mehrere Proxys für Ihre Instanz auf mehreren Computern zu installieren. Stellen Sie dabei sicher, dass die folgenden Kriterien zutreffen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alle Proxys müssen über dieselben Verschlüsselungsschlüssel und das gleiche RSA-Schlüsselpaar verfügen, mit dem Verschlüsselungskonfigurationen und -regeln digital signiert werden.
- Der Verschlüsselungsschlüssel muss der in der Instanz konfigurierte Standardschlüssel sein.
- Wenn eine Proxy-Datenbank als Teil der Installation eingerichtet wird, müssen alle Proxys dieselbe Proxy-Datenbank verwenden.

  Möglicherweise benötigen Sie eine Proxy-Datenbank für die gleichstellungserhaltende Verschlüsselung, die ordnungserhaltende Verschlüsselung oder Tokenisierung. Wenn keine dieser Funktionen verwendet wird, benötigen Sie keine Proxy-Datenbank.

Nächste Maßnahme

Informationen zur Verwendung von NVDA, einem Bildschirmleser für Assistive Technology, der zum Lesen von Java-Anwendungen mit Barrierefreiheit für Tastaturanwender entwickelt wurde, finden Sie unter Konfigurieren Sie einen Windows 64-Bit-Host für die Verwendung von 32-Bit-NVDA mit Java-Anwendungen .

Nach der Installation von Edge Encryption Proxy-Server, Legen Sie die anfängliche Arbeitsspeichergrenze des Proxy-Servers und die obere Arbeitsspeichergrenze fest .

Den Edge Encryption Proxy-Server (interaktives Installationsprogramm) installieren

Installieren Sie den Edge Encryption Proxy auf einem Windows- oder Linux-Computer.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Den Proxy-Server für die Edge Encryption herunterladen.
2. Öffnen Sie das Edge Encryption Proxy-Installationsprogramm.

   Hinweis: Bei der Installation auf einem Windows-Computer müssen Sie das Installationsprogramm als Administrator ausführen.

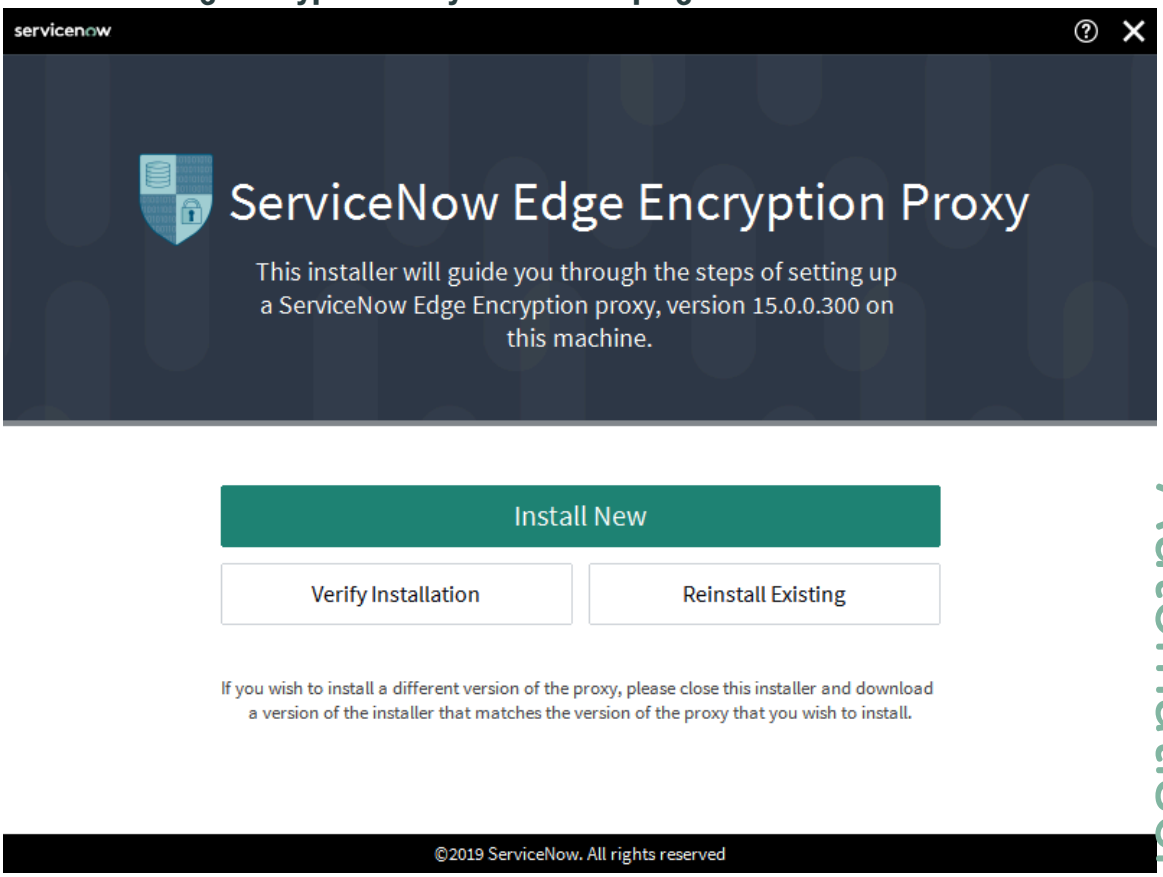
   a. Um das Installationsprogramm als Administrator auf einem Windows-Computer auszuführen, klicken Sie mit der rechten Maustaste auf die Eingabeaufforderung, und wählen Sie **Als Administrator ausführen**.

   b. Navigieren Sie in der Befehlszeile zu dem Verzeichnis, in dem sich die heruntergeladene JAR-Datei befindet.

   c. Führen Sie den folgenden Befehl aus: `java -jar <Dateiname>.jar`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Edge Encryption-Proxy-Installationsprogramm



Automatische Übersetzung

3. Um einen neuen Proxy-Server zu installieren, wählen Sie **Neu installieren**.
   Wenn bereits ein Proxy installiert ist, können Sie das Installationsprogramm folgendermaßen ausführen:
   - **Installation überprüfen**: Führen Sie Tests durch, um Probleme bei einer früheren Installation zu erkennen und zu beheben.
   - **Vorhandene neu installieren**: Führen Sie Tests durch, um Probleme in einer früheren Installation zu erkennen und zu beheben und vorhandene Einstellungen anzuzeigen oder zu ändern.
4. Konfigurieren Sie **Installationsort** und **ServiceNow-Zielinstanz**.

   a. Klicken Sie **Durchsuchen**, um einen Installationsort zu wählen, oder geben Sie manuell einen Installationspfad ein.

   b. Geben Sie die URL der ServiceNow Zielinstanz ein.
   Geben Sie das Protokoll und die Portnummer an.

   Example
   `https://example.servicenow.com:443`

   c. Geben Sie den Benutzernamen und das Passwort für einen Benutzer mit der Rolle „edge_encryption“ auf der ServiceNow Zielinstanz ein.

5. Klicken Sie auf **Weiter**.
6. Konfigurieren Sie die **Verbindungseinstellungen** und **Proxy-Einstellungen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellung	Beschreibung
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. **Hinweis:** Klicken Sie auf **FQDN erkennen**, um nach dem vollständig qualifizierten Domänennamen des Computers suchen und das Feld **Proxy-Host** automatisch auszufüllen. Zusammen mit dem Port definiert diese Eigenschaft die URL, die der Client für den Zugriff auf den Proxy-Server verwendet.
HTTP-Port	Port auf dem Proxy für die HTTP-Kommunikation.
HTTPS-Port	Port auf dem Proxy für die HTTPS-Kommunikation.
Proxy-Name	Proxy- und Service-Name. Der Proxy-Name muss eindeutig sein.
Proxy-Abrufintervall	Abrufintervall in Sekunden. Bei der Standardeinstellung dauert es 5 Sekunden, bis Änderungen der Verschlüsselungskonfiguration den Proxy-Server erreichen. Größere Werte führen dazu, dass die Instanz länger braucht, um Online-Proxys zu erkennen. **Hinweis:** Das Ändern der Standardeinstellung des Proxy-Abrufintervalls kann zu Erkennungsverzögerungen führen, wenn ein Proxy online geschaltet wird.
Proxy-Keep-Alive-Ping-Intervall	Zeit in Sekunden zwischen den vom Proxy an die Instanz ausgegebenen Pings. Pings werden regelmäßig ausgegeben, um die Verbindung zwischen dem Proxy und der Instanz zu überprüfen. Der Standardwert ist 10. Der Mindestwert ist 5.

7. Klicken Sie auf **Installieren**.
   Der Edge Encryption Proxy-Server installiert. Die Installation kann einige Minuten in Anspruch nehmen.

Konfigurieren Sie den Schutz von CyberArk-Eigenschaften

Konfigurieren Sie optional den Schutz von CyberArk-Eigenschaften, um sie sicher zu speichern Edge Encryption Passwörter in einem zentralen und sicheren digitalen Tresor.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Sie müssen CyberArk AIM (Application Identity Management) erwerben und konfigurieren, bevor Sie CyberArk-Verbindungsparameter und geschützte Anmeldeinformationen für einen Proxy-Server konfigurieren können. Im Rahmen der Installation des AIM-Clients wird die Datei JavaPasswordSDK.jar

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

im Installationsverzeichnis des AIM-Clients installiert. Der CyberArk-Tresor wird auf einem unabhängigen gehärteten Server installiert, und die AIM-Clients ermöglichen einen sicheren Zugriff auf diesen Server.

Hinweis: Sie müssen den CyberArk AIM-Client auf jedem Host-Computer installieren, auf dem ein Edge-Proxy installiert ist.

Im Edge-Installationsprogramm müssen Sie den Speicherort der Datei JavaPasswordSDK.jar angeben, um die CyberArk-Verbindung zum Edge-Proxy einzurichten. Sie müssen auch andere Werte eingeben, die Sie während der Installation des AIM-Clients definiert haben.

Das Einrichten des CyberArk-Passwortspeichers ist optional. Wenn Sie den CyberArk-Passwortspeicher nicht einrichten möchten, klicken Sie auf den CyberArk-Bildschirmen auf **Überspringen**.

Prozedur

1. Auf der CyberArk Connection-Seite des Edge Encryption-Installationsprogramms geben Sie die CyberArk-Verbindungsparameter ein.

CyberArk-Verbindungsparameter

Einstellung	Beschreibung
Pfad zu PasswordSDK.jar	Der Pfad zur Datei JavaPasswordSDK.jar, die während der CyberArk-Konfiguration auf dem Windows-Hostcomputer installiert wurde.
App-ID	Die bei der CyberArk-Konfiguration eingegebene **App-ID**.
Safe-Name	Der bei der CyberArk-Konfiguration eingegebene **Safe-Name**.

2. Klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite „CyberArk-geschützte Anmeldeinformationen“ des Installationsprogramms die Anmeldeinformationen ein, die von CyberArk geschützt werden sollen.
   - Um einen einzigen Anmeldeinformationsnamen für alle geschützten Passwörter zu verwenden, wählen Sie die Checkbox **Einen Anmeldeinformationsnamen für alle Anmeldeinformationen anwenden**, geben Sie den Anmeldeinformationsnamen ein, und klicken Sie auf **Übernehmen**.
   - Geben Sie den Anmeldeinformationsnamen für eines oder mehrere der folgenden Felder ein. Anmeldeinformationsnamen sind die Benutzernamen, die während der CyberArk-Konfiguration für die SSH-Schlüssel eingegeben wurden.

CyberArk-geschützte Anmeldeinformationen

Einstellung	Beschreibung
Edge Encryption-Benutzer	Der CyberArk-Anmeldeinformationsname für einen Edge Encryption-Benutzer.
Schlüsselspeicher des Signaturschlüssels	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher des Signaturschlüssels.
HTTPS Cert-Schlüsselspeicher	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher der HTTP-Zertifizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellung	Beschreibung
Schlüsselspeicher des Verschlüsselungsschlüssels	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher des Verschlüsselungsschlüssels.
Datenbank	Der CyberArk-Anmeldeiinformationsname für den Datenbankschlüsselspeicher.
SafeNet HTTPS Cert-Schlüsselspeicher	Der CyberArk-Anmeldeinformationsname für den Schlüsselspeicher der SafeNet HTTP-Zertifizierung.
SafeNet-Server	Der CyberArk-Anmeldeinformationsname für den SafeNet-Server.
Forward Proxy	Der CyberArk-Anmeldeinformationsname für den Forward Proxy.

4. Klicken Sie auf **Weiter**.

Den Signaturschlüssel konfigurieren

Konfigurieren Sie den Signaturschlüssel nach der Installation des Proxy-Servers über das Edge Encryption Proxy-Installationsprogramm.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Der Signaturschlüssel kennzeichnet Änderungen an Konfigurationen und Eigenschaften, die vom Proxy-Server vorgenommen werden. Der Signaturschlüssel muss ein asymmetrisches RSA-Schlüsselpaar in einem JCEKS KeyStore sein.

Hinweis: Bei der Installation mehrerer Proxys muss jeder Proxy denselben Signaturschlüssel verwenden.

Prozedur

1. Wählen Sie auf der Seite „Signaturschlüssel“ des Edge Encryption Installationsprogramms den Schlüsselspeicher auf dem Host-Computer aus, um den Signaturschlüssel zu speichern.
   - **Einen neuen Java KeyStore erstellen**: Geben Sie Verzeichnisspeicherort, Name und Passwort für den neuen Keystore ein.
   - **Vorhandenen Keystore verwenden**: Geben Sie den Speicherort und das Passwort der Keystore-Datei ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie einen Signaturschlüssel aus oder erstellen Sie ihn.
   - **Neuer Schlüssel**: Erstellen Sie einen Signaturschlüssel für diesen Proxy.
   - **Vorhandenen Schlüssel verwenden**: Verwenden Sie ein RSA-Schlüsselpaar aus dem ausgewählten Schlüsselspeicher.
   - **Vorhandenen Schlüssel importieren**: Importieren Sie ein RSA-Schlüsselpaar aus einem anderen Schlüsselspeicher. Navigieren Sie zur Keystore-Datei, geben Sie das Passwort für den Keystore ein und wählen Sie den Schlüsselalias aus. Geben Sie einen neuen Alias für den Schlüssel an.
4. Klicken Sie auf **Weiter**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das HTTPS-Zertifikat konfigurieren

Um Clients die Verbindung zum Edge Encryption Proxy-Server über eine sichere SSL-Verbindung zu ermöglichen, importieren Sie das HTTPS-Zertifikat in den Proxy-Server.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Der Edge Encryption Proxy stellt das HTTPS-Zertifikat für Clients bereit, die versuchen, eine Verbindung herzustellen.

Prozedur

1. Wählen Sie auf der Seite „HTTPS-Zertifikat“ des Edge Encryption Installationsprogramms den Schlüsselspeicher zum Speichern des Zertifikats aus.
   - **Einen neuen Java KeyStore erstellen**: Geben Sie Verzeichnisspeicherort, Name und Passwort für den neuen Keystore ein.
   - **Vorhandenen Keystore verwenden**: Geben Sie den Speicherort und das Passwort der Keystore-Datei ein.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie ein Zertifikat aus oder importieren Sie es.
   Der Schlüsselalias ist der angegebene Alias für das Zertifikat.
   - **Vorhandenes Zertifikat verwenden**: Verwenden Sie ein vorhandenes Zertifikat im ausgewählten Schlüsselspeicher.
   - **Aus Datei oder KeyStore importieren**: Importieren Sie ein Zertifikat aus einem anderen Schlüsselspeicher oder einer CER-Datei. Navigieren Sie zum Keystore oder zur .CER-Datei, geben Sie das Passwort ein und wählen Sie den Alias aus. Sie müssen einen neuen Alias für das Zertifikat angeben.
4. Klicken Sie auf **Weiter**.

Den AES 128-Bit-Verschlüsselungsschlüssel konfigurieren

Nachdem Sie das HTTPS-Zertifikat über konfiguriert haben Edge Encryption Proxy-Installationsprogramm: Konfigurieren Sie den 128-Bit-AES-Verschlüsselungsschlüssel, um Ihre Daten zu verschlüsseln.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Der Verschlüsselungsschlüssel ist entweder eine reine Textdatei im /Schlüssel-Verzeichnis oder ein geheimer Schlüssel in einem Schlüsselspeicher. Wenn Sie einen Keystore für Ihre AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel verwenden, müssen beide denselben Keystore verwenden.

Informationen zum Aktualisieren eines SSL-Zertifikats auf einem Edge-Proxy-Server finden Sie unter SSL-Zertifikat aktualisieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie den Ort des Verschlüsselungsschlüssels.

Option	Beschreibung
Dateispeicher	Verwenden Sie eine Datei, um einen einzelnen Verschlüsselungsschlüssel zu speichern. Sie können eine vorhandene Datei in verwenden /Keys Verzeichnis, oder Sie können eine neue Datei generieren. Um eine neue Datei zu erstellen, geben Sie einen Alias ein und klicken Sie auf **Generieren**. Es wird eine Datei mit einem Verschlüsselungsschlüssel erstellt. **Hinweis:** Diese Auswahl gibt sowohl den Speicherort als auch den Verschlüsselungsschlüssel an. Wenn Sie auswählen **Dateispeicher** , Klicken Sie auf **Als Nächstes** Und wechseln Sie zu Schritt 5 .
Erstellen Sie einen neuen Java-Schlüsselspeicher	Erstellen Sie einen Schlüsselspeicher, um den Verschlüsselungsschlüssel zu speichern.
Java-Schlüsselspeicherdatei	Speichern Sie den Verschlüsselungsschlüssel in einer vorhandenen Java-Schlüsselspeicherdatei.

2. Klicken Sie auf **Next (Weiter)**.
3. Wählen oder erstellen Sie den Verschlüsselungscode.

Option	Beschreibung
Neuer Schlüssel	Erstellen Sie einen Verschlüsselungsschlüssel und einen Alias. **Hinweis:** Sie müssen Kleinbuchstaben und Zahlen für den Aliasnamen (Schlüsselname, Schlüsselalias) gemäß Java-Schlüsselspeicheranforderungen verwenden. Weitere Informationen zum Keytool-Dienstprogramm finden Sie in der Java SE-Dokumentation .
Vorhandenen Schlüssel Verwenden	Verwenden Sie einen vorhandenen Verschlüsselungsschlüssel im ausgewählten Schlüsselspeicher.
Importieren Sie Den Vorhandenen Schlüssel	Importieren Sie einen Verschlüsselungsschlüssel aus einem anderen Schlüsselspeicher.

4. Klicken Sie auf **Next (Weiter)**.
5. Konfigurieren Sie den Schlüssel in der Instanz gemäß den in Ihrem Installationsprogramm definierten Anforderungen.
   Um den Schlüssel in der Instanz zu konfigurieren, navigieren Sie zur Instanz und definieren Sie einen Standardschlüssel. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren. Stellen Sie sicher, dass Schlüsselalias, Größe und Typ den im Installationsprogramm definierten Anforderungen entsprechen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardschlüsselanforderungen



6. Wenn der Schlüssel in der Instanz konfiguriert ist, kehren Sie zum Installationsprogramm zurück und klicken Sie auf **Nächster**.

Konfigurieren Sie den 256-Bit-AES-Verschlüsselungsschlüssel

Nachdem Sie den AES-128-Bit-Schlüssel über das Edge-Proxy-Installationsprogramm konfiguriert haben, können Sie optional einen AES-256-Bit-Verschlüsselungsschlüssel konfigurieren, um Ihre Daten zu verschlüsseln.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der Verschlüsselungsschlüssel ist entweder eine reine Textdatei im /Schlüssel-Verzeichnis oder ein geheimer Schlüssel in einem Schlüsselspeicher. Wenn Sie einen Schlüsselspeicher für Ihre AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel verwenden, müssen beide Schlüssel denselben Schlüsselspeicher verwenden. Wenn Sie keinen 256-Bit-AES-Verschlüsselungsschlüssel konfigurieren möchten, wählen Sie aus **Überspringen** Um mit der Installation des Proxy-Servers fortzufahren.

Informationen zum Aktualisieren eines SSL-Zertifikats auf einem Edge-Proxy-Server finden Sie unter SSL-Zertifikat aktualisieren .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie den Ort des Verschlüsselungsschlüssels.

Option	Beschreibung
Dateispeicher	Verwenden Sie eine Datei, um einen einzelnen Verschlüsselungsschlüssel zu speichern. Sie können eine vorhandene Datei in verwenden /Keys Verzeichnis, oder Sie können eine neue Datei generieren. Um eine neue Datei zu generieren, geben Sie einen Alias ein, und wählen Sie aus **Generieren** . Es wird eine Datei mit einem Verschlüsselungsschlüssel erstellt. **Hinweis:** Diese Auswahl gibt sowohl den Speicherort als auch den Verschlüsselungsschlüssel an. Wenn Sie auswählen **Dateispeicher** , Wählen Sie aus **Als Nächstes** Und wechseln Sie zu Schritt 5 .
Erstellen Sie einen neuen Java-Schlüsselspeicher	Erstellen Sie einen Schlüsselspeicher, um den Verschlüsselungsschlüssel zu speichern.
Java-Schlüsselspeicherdatei	Speichern Sie den Verschlüsselungsschlüssel in einer vorhandenen Java-Schlüsselspeicherdatei.

2. Wählen Sie **Weiter**.
3. Wählen oder erstellen Sie den Verschlüsselungscode.

Option	Beschreibung
Neuer Schlüssel	Erstellen Sie einen Verschlüsselungsschlüssel und einen Alias. **Hinweis:** Sie müssen Kleinbuchstaben und Zahlen für den Aliasnamen (Schlüsselname, Schlüsselalias) gemäß den Java-Schlüsselspeicheranforderungen verwenden. Weitere Informationen zum Keytool-Dienstprogramm finden Sie in der Java SE-Dokumentation .
Vorhandenen Schlüssel Verwenden	Verwenden Sie einen vorhandenen Verschlüsselungsschlüssel im ausgewählten Schlüsselspeicher.
Importieren Sie Den Vorhandenen Schlüssel	Importieren Sie einen Verschlüsselungsschlüssel aus einem anderen Schlüsselspeicher.

4. Wählen Sie **Weiter**.
5. **Wahlweise:** Informationen zur Verwendung der AES-256-Bit-Verschlüsselung finden Sie unter Konfigurieren Sie den 256-Bit-AES-Verschlüsselungsschlüssel.
6. Um die AES-256-Bit-Verschlüsselung zu verwenden, müssen Sie auch den AES-256-Bit-Standardverschlüsselungsschlüssel in der Instanz konfigurieren.

   Navigieren Sie dazu zur Instanz, und definieren Sie einen Standardschlüssel. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren. Stellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie sicher, dass Schlüsselalias, Größe und Typ den im Installationsprogramm definierten Anforderungen entsprechen.

7. Nachdem der Schlüssel in der Instanz konfiguriert wurde, kehren Sie zum Installationsprogramm zurück, und wählen Sie aus **Als Nächstes** .

SSL-Zertifikat aktualisieren

Wenn Sie ein SSL-Zertifikat auf einem Edge-Proxy-Server aktualisieren, müssen Sie das alte Zertifikat löschen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Beim Aktualisieren des SSL-Zertifikats auf dem Edge-Proxy-Server müssen Sie auch das alte Zertifikat löschen. Wenn nicht, wird das alte Zertifikat (in Form eines Alias in der Schlüsselspeicherdatei) weiterhin verwendet, auch wenn der Edge-Proxy-Server für die Verwendung des neuen Zertifikats konfiguriert ist.

Prozedur

1. Listen Sie auf dem Edge-Proxy-Server die Einträge im Java-Schlüsselspeicher auf:

```
keytool -list -keystore keystore.jceks -storetype jceks -storepass MY_SUPER_PASSWORD
```

2. Altes SSL-Zertifikat entfernen:

```
keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype jceks -storepass
 MY_SUPER_PASSWORD
```

3. Fügen Sie das neue SSL-Zertifikat dem Java-Schlüsselspeicher hinzu.

Konfigurieren Sie die Edge Encryption-Proxy-Datenbank

Wenn Sie Verschlüsselungstypen oder Verschlüsselungsmuster verwenden, die die Reihenfolge beibehalten, können Sie optional konfigurieren Edge Encryption Eigenschaften der Proxy-Datenbank.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Für die Verwendung von bestandserhaltenden Verschlüsselungstypen oder Verschlüsselungsmustern ist eine in Ihrem Netzwerk ausgeführte MySQL-Datenbank erforderlich. Diese Aufgabe verbindet den Proxy mit der Datenbank, die Datenbank wird jedoch nicht installiert oder konfiguriert.

Hinweis: Wenn Sie mehrere Proxy-Server verwenden, müssen alle Proxy-Server dieselbe Proxy-Datenbank verwenden. Die im Installationsprogramm eingegebenen Werte müssen für alle Proxy-Server gleich sein.

Prozedur

1. Bestätigen oder ändern Sie die Datenbank-URL, die der Speicherort der Proxy-Datenbank ist.
2. Geben Sie im Feld **Name** den Namen der Proxy-Datenbank ein.
   Der Standardwert ist *edgeencryption*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie den Benutzernamen und das Passwort für den Zugriff auf die Proxy-Datenbank ein.
4. Klicken Sie auf **Weiter**.

Den Proxy-Server der Edge Encryption starten

Nach dem Installieren und Konfigurieren eines Edge Encryption Proxys kann der Proxy aus dem Installationsprogramm gestartet werden.

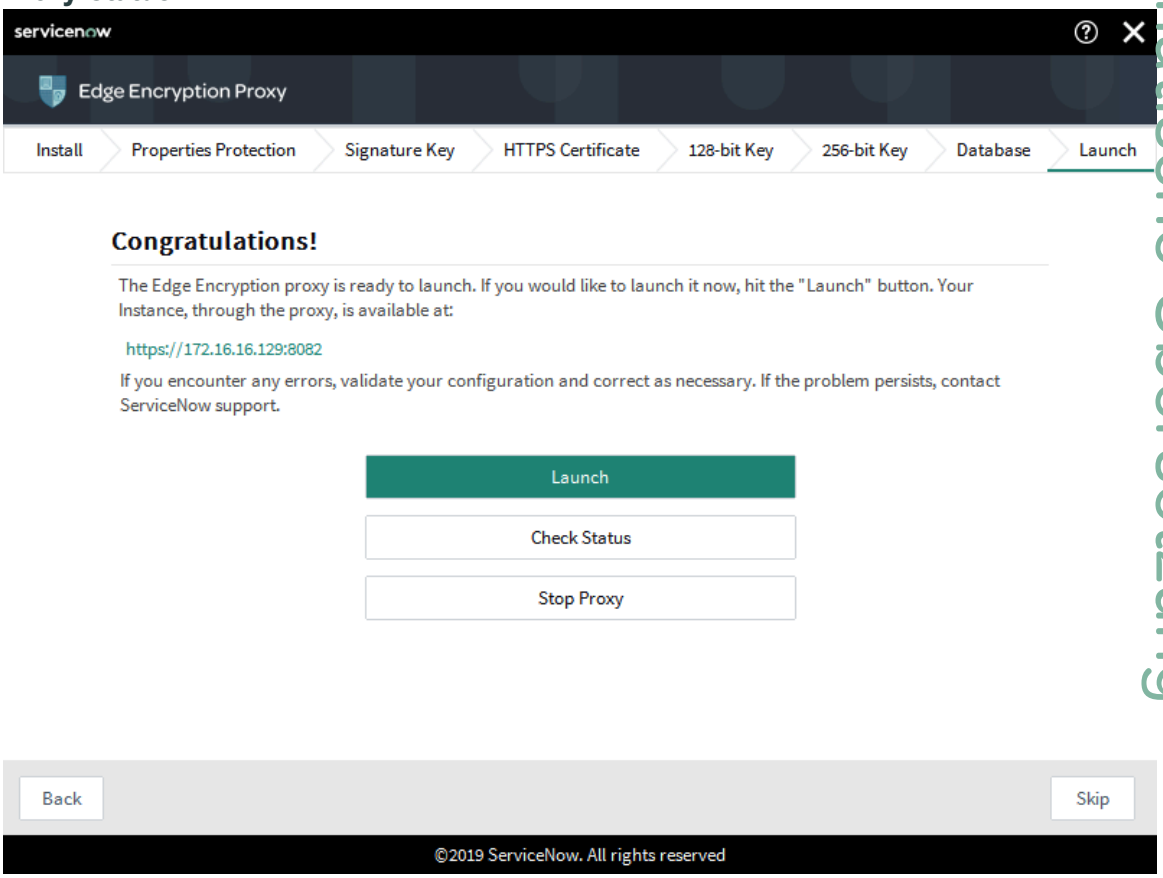
Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Kehren Sie nach der Konfiguration von Schlüsseln in der Instanz und der Konfiguration der Proxy-Datenbank zu zurück Edge Encryption Proxy-Installationsprogramm, und klicken Sie auf **Starten** .
2. Sie können bei Erkennen eines Problems oder zur Statusprüfung Ihres Proxy-Servers auf **Status prüfen**, um zu überprüfen, ob der Proxy ausgeführt wird.
   Eine Meldung zeigt den Proxy-Status an.

Proxy-Status



Automatische Übersetzung

Nächste Maßnahme

Nach erfolgreicher Installation des Edge Encryption Proxy-Servers, Legen Sie die anfängliche Arbeitsspeichergrenze des Proxy-Servers und die obere Arbeitsspeichergrenze fest.

Überprüfen und beheben Sie die Installation des Edge Encryption-Proxy-Servers

Nach dem Installieren des Edge Encryption Proxy können Sie die Installation überprüfen, um Probleme zu lokalisieren oder den Proxy zu starten und zu stoppen.

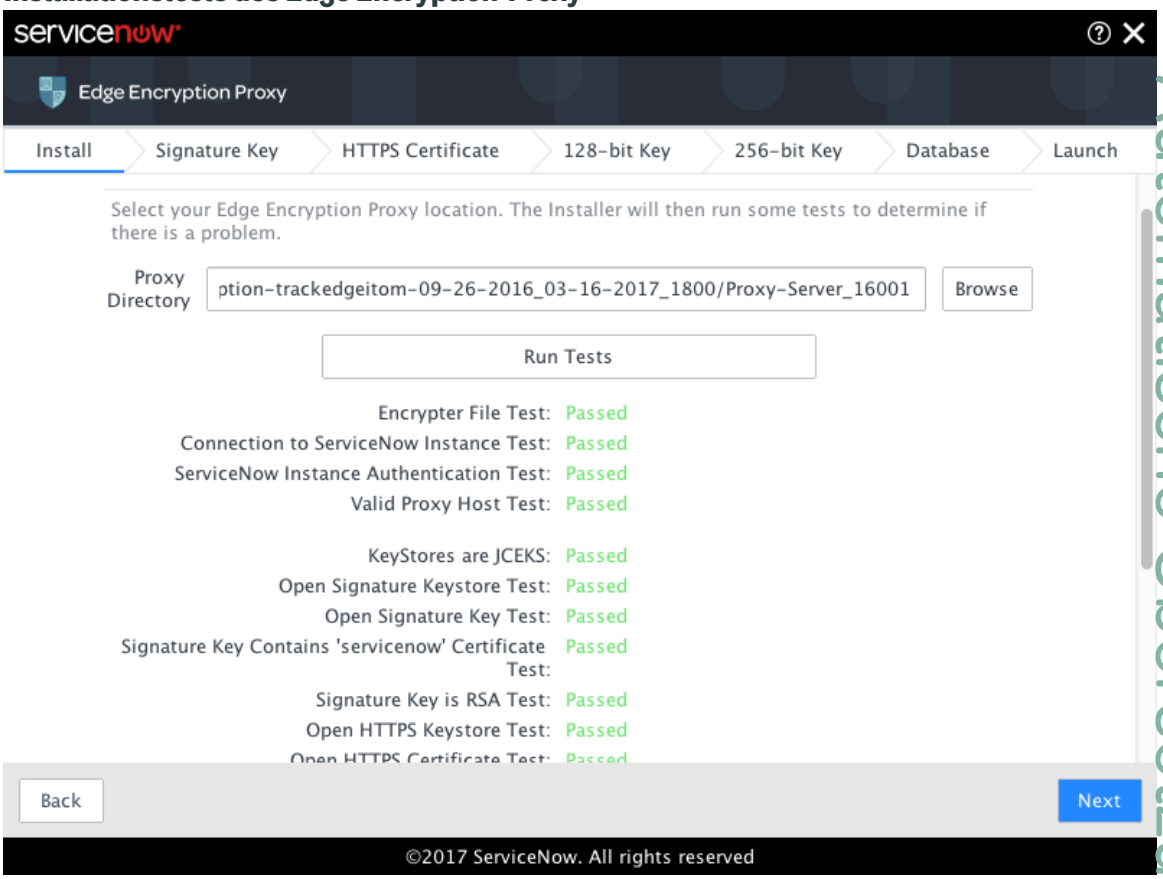
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie das Edge Encryption Proxy-Installationsprogramm.
2. Wählen Sie **Installation überprüfen**.
3. Klicken Sie auf **Proxy-Verzeichnis** und wählen Sie das Proxy-Verzeichnis.
4. Klicken Sie auf **Tests ausführen**.
   Testergebnisse werden angezeigt.

Installationstests des Edge Encryption-Proxy



5. Klicken Sie auf **Weiter**.
   Wenn ein Problem auftritt, können Sie das Installationsprogramm durchlaufen, um die Konfiguration zu korrigieren. Wenn keine Probleme auftreten, springt der Installer zur Seite **Starten**. Sie können den Proxy-Status überprüfen, den Proxy stoppen oder den Proxy aus der **Starten**-Seite starten.

Den Proxy-Server für die Edge Encryption mithilfe des Befehlszeilen-Installationsprogramms installieren

Installieren Sie manuell mehrere Edge Encryption Proxy-Server in Ihrem Netzwerk.

Vorbereitungen
Erforderliche Rollen: security_admin auf Ihrer ServiceNow-Instanz und lokaler Administrator auf dem Host-Computer.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ordnungserhaltende Verschlüsselungstypen oder Verschlüsselungsmuster verwendet werden sollen, richten Sie eine MySQL-Datenbank auf einem Computer in Ihrem Netzwerk ein, sofern noch nicht vorhanden.

Hinweis: Bei Verwendung der Unbound Technology-Verschlüsselungsschlüssel mit Edge Encryption installieren Sie den Proxy-Server mithilfe des Befehlszeileninstallationsprogramms auf dem Unbound-Client-Computer. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound Technology -Client ausgeführt werden.

Warum und wann dieser Vorgang ausgeführt wird

Richten Sie zuerst einen einzelnen Edge Encryption Proxy-Server ein. Nachdem Ihr erster Proxy-Server erfolgreich ausgeführt wurde, fügen Sie weitere Proxy-Server für eine Instanz hinzu, um eine optimale Umgebung zu gewährleisten. Siehe Umgebungsgröße Ihrer Edge Encryption anpassen, um die Anzahl zusätzlich erforderlicher Proxy-Server zu bestimmen.

Edge Encryption-Proxy-Server installieren (Befehlszeilen-Installationsprogramm)

Installieren Sie einen Edge Encryption Proxy auf einem 64-Bit-Windows- oder Linux-Computer.

Vorbereitungen

Erforderliche Rolle: Administrator

Java-Version 11.0.6 oder höher in der 11.x-Versionsreihe ist erforderlich, um das Installationsprogramm auszuführen.

Warum und wann dieser Vorgang ausgeführt wird

Installieren Sie den Edge Encryption Proxy-Server auf einem Computer in Ihrem Netzwerk mit dem entsprechenden Befehl für Ihren Zielcomputer. Bei der Installation des Edge Encryption Proxy-Servers auf einem Windows-Computer muss der Proxy-Server zusätzlich als Windows-Service installiert werden.

Wenn Sie den Proxy-Server der Edge Encryption aktualisieren, sichert das System den alten Proxy im Verzeichnis backup.dist-upgrade-<timestamp> unter dem aktuellen Installationsverzeichnis. Das Sicherungsverzeichnis wird während des Upgrade-Vorgangs erstellt und speichert die alten Proxy-Informationen.

Wenn Sie ein Upgrade über die Befehlszeile ausführen, kann eine dist-upgrade.log in dem Verzeichnis erstellt werden, in dem der Befehl ausgeführt wird. Das dist-upgrade.log enthält Protokolle für den Upgrade-Vorgang.

Bei einem fehlgeschlagenen Upgrade erstellt das System ein Verzeichnis failed-backup.dist-upgrade-<timestamp>. Zusätzlich kann logs/wrapper.log im ursprünglichen Proxy-Verzeichnis auch Fehlerinformationen enthalten.

Prozedur

1. Erstellen Sie das Installationsverzeichnis.
2. Laden Sie die Edge Encryption Proxy-Archivdatei in das Installationsverzeichnis herunter.
3. Öffnen Sie das Terminal und wechseln Sie in das Installationsverzeichnis.

   Hinweis: Bei der Installation auf einem Windows-Computer müssen Sie die Windows-Eingabeaufforderung mit Administratorrechten starten.

4. Führen Sie diesen Befehl für den Zielcomputer aus, und ändern Sie die Variablen entsprechend Ihrer Konfiguration: `java -jar edgeEncryption-<version>-all.jar -m install –n <proxy_name> --instancehost <host> -p <port> --Protocol https –s <install_path>`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Variable	Beschreibung
Keine	Version	Versionsnummer des Edge Encryption Proxy, der zur Ausführung der aktuellen Operation verwendet wird.
-m	Modus	Laufzeitmodus. Optionen sind „Installieren“ für einen neuen Edge-Proxy-Server oder „dist-Upgrade“ zum Upgrade eines vorhandenen Edge-Proxy-Servers.
-n	Proxy_Name	Name der installierten Edge Encryption Proxy-Server. Verwenden Sie einen eindeutigen Proxy_Name, um bestimmte Proxy-Instanzen identifizieren zu können.
--instancehost	host	Der Hostname Ihrer ServiceNow-Instanz (z. B. mycompany.service-now.com).
-p	port	Portieren Sie Ihren ServiceNow Instanz hört auf. Normalerweise horchen sichere HTTPS-Verbindungen auf dem Port **443** Und HTTP-Verbindungen horchen auf Port **80** .
--protocol	protocol	Protokoll, das der installierte Edge-Proxy verwendet, wenn eine Verbindung zum Back-End hergestellt wird ServiceNow Host. Dies ist normalerweise **HTTPS** (Bevorzugt für sichere TLS-Verbindungen) oder **HTTP** (Verbindungen ohne TLS) abhängig davon, welches Protokoll die Hostinstanz unterstützt.
-s	Install_path	Pfad zu dem Verzeichnis oder Ordner, in dem der neue Edge-Proxy installiert ist (Zielverzeichnis). Wenn das Verzeichnis noch nicht vorhanden ist, wird es von diesem Befehl erstellt. Wenn vorhanden, darf sie keine vorhandene Installation enthalten. Wenn diese Option übersprungen wird, wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Variable	Beschreibung
		der Standardordnername aus Proxy_Name und Port abgeleitet (z. B. EdgeProxy_443) Im aktuellen Verzeichnis.

Hinweis: Kopieren Sie keine Befehle aus dem Browser. Gelegentlich führen Kopier- / Einfügevorgänge dazu, dass unerwartete Zeichen auf dem Zielcomputer eingefügt werden und der Befehl falsch ausgeführt wird. Es ist am besten, den Befehl von Hand anhand der Dokumentation als Referenz einzugeben.

Um den Hilfebildschirm anzuzeigen, führen Sie diesen Befehl mit aus –Hilfe Option: java -jar edgeEncryption-<version>-all.jar --help

5. Beim Installieren auf einem Windows-Computer installieren Sie den Edge Encryption Proxy als Windows-Dienst.

   a. **Wahlweise:** Ändern Sie den Namen des Service, indem Sie öffnen Conf/Wrapper.conf Datei auf dem neuen Proxy und Festlegen der Eigenschaften in der folgenden Tabelle.

Eigenschaft	Beschreibung
wrapper.ntservice.name	Eindeutiger Name des Edge Encryption Proxy-Service.
wrapper.ntservice.displayname	Anzeigename des Edge Encryption Proxy-Service.
wrapper.ntservice.description (optional)	Beschreibung des Proxy-Server.

   Bei Nichtausführung dieses Schrittes wird der Edge Encryption Proxy-Service unter dem Namen **Edge Encryption** installiert.

   b. Speichern und schließen Sie die Datei.

   c. Öffnen Sie die Windows-Eingabeaufforderung und cd zu ServerName_port/bin.

   d. Führen Sie edgeencryption.bat installieren aus.

Ergebnis
Das Verzeichnis ProxyName_port wird im aktuellen Verzeichnis erstellt. Die Datei edgeencryption.properties wird mit den Host-, Port- und Protokollwerten über die Befehlszeile aktualisiert.

Das RSA-Schlüsselpaar für die digitale Signatur erstellen und konfigurieren

Erstellen Sie ein RSA-Schlüsselpaar, mit dem der Proxy-Server die digitale Signatur zum Signieren von Änderungen an den Verschlüsselungseigenschaften und der Konfiguration erstellen kann.

Vorbereitungen
Erforderliche Rolle: Administrator

Um die digitale Signatur zu erstellen und zu validieren, muss ein RSA-Schlüsselpaar generiert und im JCEKS Java KeyStore gespeichert werden, und jeder Proxy muss

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für die Verwendung dieses Schlüsselpaares konfiguriert sein. Generieren Sie ein Verschlüsselungsschlüsselpaar mit dem Befehl keytool.

Um das Keytool-Dienstprogramm mit einem auf SELinux (CentOS) installierten Proxy zu verwenden, müssen Sie das Laden von gemeinsam genutzten Bibliotheken aus dem Proxy-Java-Installationsverzeichnis aktivieren. Führen Sie dazu den folgenden Befehl als Root aus.

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter <proxy install dir>java/jre/bin/keytool.

Prozedur

1. Wechseln Sie in das KeyStore-Verzeichnis im Proxy-Download-Verzeichnis.
2. Ändern Sie das Standardpasswort.

   Das Standardpasswort lautet *changeme*.

   ```
   keytool -keystore keystore.jceks -storetype jceks -storepasswd -new <newpassword>
   ```

3. Erstellen Sie ein Verschlüsselungsschlüsselpaar.

   Hinweis: Geben Sie kein Passwort für den Schlüssel ein, wenn das keytool-Dienstprogramm zur Eingabe auffordert.

   Geben Sie diesen Befehl in einer einzigen Zeile ein.

   ```
   keytool -genkeypair -alias <key alias> -keyalg rsa -keystore keystore.jceks
   -storetype jceks -storepass <keystore password> -keysize 2048
   ```

4. Aktualisieren Sie die Eigenschaftsdatei des Verschlüsselungsproxys (edgeencryption.properties).

   a. Wechseln Sie in das Verzeichnis <installation directory>/conf/.

   b. Öffnen Sie die Datei edgeencryption.properties.

   c. Geben Sie die Eigenschaften für die Digitale Signatur ein.

      Diese Eigenschaften müssen für alle Proxys gleich sein.

5. Speichern und schließen Sie die Datei edgeencryption.properties.

Das Zertifikat für eine sichere SSL-Verbindung importieren und konfigurieren

Um eine sichere SSL-Verbindung zu verwenden, importieren Sie ein Serverzertifikat und fügen es zum Java KeyStore hinzu.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie müssen das Serverzertifikat und den übereinstimmenden privaten Schlüssel abrufen, bevor Sie ihn dem Java-Schlüsselspeicher hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Generieren Sie eine Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) mit `openssl` Befehl.

```
openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
```

2. Senden Sie Ihre CSR (MYCSR.csr im Beispiel oben) an Ihre Zertifizierungsstelle, damit sie signiert wird.
3. Erstellen Sie mit einen P12-Schlüsselspeicher für den Import `openssl` Befehl.

```
openssl pkcs12 -export -in MYSIGNEDCERT.pem -inkey PRIVATEKEY.key -name shared >
 MY_SERVER.p12
```

4. Speichern Sie Ihr Zertifikat und Ihren privaten Schlüssel in einer JCeks-Datei.

```
keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks -srckeystore
 MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
```

   Der Alias, der im Beispiel als angezeigt wird `MYALIAS` Kann ein beliebiger Wert sein. Sie verwenden diesen Alias in `edgeencryption.proxy.https.cert.alias` Eigenschaft in `edgeencryption.properties` Datei befindet sich in `<installation directory>/conf/` Ordner.

5. Beenden Sie den Edge-Proxy, und starten Sie ihn neu.

> **Hinweis:** Während eines Neustarts ist der Proxy-Server für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

Schlüsselspeicher und Verschlüsselungsschlüssel einrichten

Richten Sie den vom Edge Encryption Proxy Server verwendeten Schlüsselspeicher und die Verschlüsselungsschlüssel ein.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Bestimmen Sie sorgfältig den geeigneten Keystore-Typ entsprechend den Anforderungen Ihres Unternehmens.

Unterstützter Keystore	Beschreibung
Dateispeicher	Die Schlüssel werden in einer Datei in einem Dateisystem gespeichert, auf das der Edge Encryption Proxy-Server zugreift. In einer Datei gespeicherte Verschlüsselungsschlüssel werden nicht verschlüsselt. Der Schutz dieser Dateien liegt daher in Ihrer Verantwortung.
Java KeyStore	Ein Java KeyStore: ○ Speichert Schlüssel in einem Java JCEKS KeyStore. ○ Ist passwortgeschützt und sicherer als das Speichern von Schlüsseln in einer Datei im Dateisystem. ○ Kann mehrere Schlüssel speichern. Ein Schlüsselalias repräsentiert jeden Schlüssel, was die Verwaltung mehrerer Schlüssel erleichtert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützter Keystore	Beschreibung
	Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen keystore.jceks im Verzeichnis Schlüsselspeicher geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.
Enterprise Key Management (EKM)	**SafeNet KeySecure** Schlüssel werden mit der Schlüsselverwaltung von SafeNet KeySecure gespeichert und abgerufen. Sie müssen eine Lizenz von Gemalto erwerben, die Bibliotheken herunterladen und den SafeNet KeySecure-Schlüsselspeicher auf einem Host-Computer in Ihrem Netzwerk installieren, bevor Sie den Schlüsselspeicher auf dem Edge Encryption Proxy-Server konfigurieren. **Unbound Technology** Der base64-verschlüsselte Wrapped-Verschlüsselungsschlüssel wird als Textdatei auf dem Edge Encryption Proxy-Server gespeichert. Die Implementierung der Unbound Technology (zuvor Dyadic Security) behält die Kontrolle über den Wrapping-Schlüssel. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound-Technology-Client ausgeführt werden.

Hinweis: Wenn Sie einen anderen Schlüsselspeicher als das Basissystem Java JCEKS KeyStore verwenden, müssen Sie den öffentlichen Schlüssel ServiceNow in Ihren Schlüsselspeicher importieren. Der öffentliche Schlüssel-Alias ist `servicenow`.

2. Richten Sie den Schlüsselspeicher und die Verschlüsselungsschlüssel in Ihrem lokalen Netzwerk ein.

Einen Java KeyStore-Schlüsselspeicher einrichten

Sie können einen Java KeyStore-Schlüsselspeicher zum Speichern von Verschlüsselungsschlüsseln verwenden.

Vorbereitungen
Erforderliche Rolle: Administrator

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter <proxy install dir>/java/jre/bin/keytool.

Warum und wann dieser Vorgang ausgeführt wird
Der Edge Encryption Proxy wird mit der Java JCEKS KeyStore-Datei mit dem Namen keystore.jceks im Verzeichnis Schlüsselspeicher geliefert. Diese Schlüsselspeicherdatei enthält den öffentlichen Schlüssel ServiceNow, mit dem die von ServiceNow signierten Verschlüsselungsregeln überprüft werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Richten Sie die Keystore-Eigenschaften ein.
   a. Wechseln Sie in das Verzeichnis <installation directory>/conf/.
   b. Öffnen Sie die Datei edgeencryption.properties.
   c. Geben Sie die Eigenschaften für den Java KeyStore ein.
2. Speichern und schließen Sie die Datei edgeencryption.properties.

Nächste Maßnahme

Nach dem Einrichten des Java KeyStore, Erstellen Sie Verschlüsselungsschlüssel mit dem Java Keystore Keytool.

Erstellen Sie Verschlüsselungsschlüssel mit dem Java Keystore Keytool

Sie können das mit der Verschlüsselungsproxy-Distribution mitgelieferte Keytool verwenden, um AES 128-Bit- und AES 256-Bit-Verschlüsselungsschlüssel zu erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie müssen die Java 1.8-Version des Keytool-Dienstprogramms verwenden. Eine Kopie des Dienstprogramms finden Sie unter <proxy install dir>/java/jre/bin/keytool.

Weitere Informationen zum Keytool-Dienstprogramm finden Sie in der Java SE-Dokumentation .

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Der Java KeyStore erfordert, dass der Aliasname (Schlüsselname, Schlüsselalias) Kleinbuchstaben und Zahlen verwendet.

Prozedur

1. Wechseln Sie in das Verzeichnis <installation directory>/keystore/.
2. Führen Sie einen der folgenden Befehle aus, um den Verschlüsselungsschlüssel zu erstellen.

Hinweis: Wenn Sie diese Befehle aus einem anderen Verzeichnis als dem Keystore-Verzeichnis ausführen möchten, d. h. Sie haben den vorherigen Schritt übersprungen, müssen Sie die Option *-keystore* ändern, um den Pfad von Ihrem aktuellen Verzeichnis zum Keystore-Verzeichnis aufzunehmen. Zum Beispiel, wenn Sie sich im befunden haben <installation directory>\bin Verzeichnis, die Option wäre `-Schlüsselspeicher ../Schlüsselspeicher/Schlüsselspeicher.jceks` .

Option	Bezeichnung
AES 128	`keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks`
AES 256	`keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks`

Der Alias wird in der Instanz hinzugefügt, wenn Sie Standardschlüssel zuweisen.

Hinweis: Das Schlüsselpasswort muss mit dem Keystore-Passwort identisch sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einen SafeNet KeySecure-Schlüsselspeicher einrichten

Wenn Sie einen SafeNet-Schlüsselspeicher verwenden, kopieren Sie einen Satz Bibliotheken in das Proxy-Distributionsverzeichnis.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie müssen den SafeNet-Schlüsselspeicher installieren und einrichten, bevor Sie diesen Schritt ausführen. Sichern Sie eine Lizenz mit Thales Um die Bibliotheken herunterzuladen.

Hinweis: Für IngrianNAE Version 8,12 müssen Sie auch herunterladen commons-collections.jar Datei

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Unter Linux verwenden Dateipfade einen Schrägstrich (/).

Prozedur

1. Wechseln Sie in das Verzeichnis <installation directory>/conf/ directory, und öffnen Sie die Datei edgeencryption.properties.
2. Geben Sie die Eigenschaften für den SafeNet-Schlüsselspeicher ein.

   Hinweis: Sie können den SafeNet-Schlüsselspeicher mit mit Anwendername-/Passwortauthentifizierung oder Client-Zertifikatauthentifizierung konfigurieren, aber nicht mit einer Kombination aus beidem.

Example

Ein Beispiel für einen SafeNet-Schlüsselspeicher mit Authentifizierung mit Benutzername und Passwort.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_truststore
edgeencryption.nae.keystore.password = password
edgeencryption.nae.user = safenet_user
edgeencryption.nae.password = safenet_password
```

Example

Ein Beispiel für einen SafeNet-Schlüsselspeicher mit Client-Zertifikatsauthentifizierung. Durch diese Authentifizierungsmethode ist das Speichern von Benutzername und Passwort des SafeNet-Servers in der Eigenschaftendatei nicht erforderlich.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_clientcert
edgeencryption.nae.keystore.password = password
edgeencryption.nae.client.certificate = cert_name
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Hinzufügen oder Erstellen eines Schlüssels im SafeNet-Schlüsselspeicher.
   Der Schlüsselname (Alias) wird in der Instanz hinzugefügt, wenn Sie Standardschlüssel zuweisen.
4. Speichern und schließen Sie die Datei edgeencryption.properties.

Upgrade von Kingston oder niedriger auf London oder höher

Wenn Sie einen SafeNet-NAE-Server für Schlüsselspeicher mit Edge verwenden, bevor Sie den Proxy von aktualisieren Kingston Oder niedriger bis London Oder höher müssen Sie JAR-Dateien des Gemalto SafeNet-Client ProtectApp kopieren und neue Eigenschaften hinzufügen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Hinweis: Unter Linux verwenden Dateipfade einen Schrägstrich (/).

Prozedur
1. Kopieren Sie die folgenden Dateien aus <installation directory>/lib Zu <installation directory>/nae-Verzeichnis :
   - commons-collections<version>.jar
   - ingrianlog4j-api-<version>.jar
   - ingrianlog4j-core-<version>.jar
   - ingrianNAE-<version>.jar
2. Aktualisieren Sie auf der aktuellen Version (nicht aktualisiert) des Proxy <installation directory>/conf/edgeencryption.properties Datei durch Hinzufügen der folgenden zwei Eigenschaften:
   - *edgeencryption.ekm.provider.classname=* Com.snc.edgecryption.Encryption.CloudEdgeNaeKeyProvider
   - *edgeencryption.thirdparty.vendor.library.path=* <Verzeichnispfad zu dem Verzeichnis, in das Sie die JAR-Dateien in Schritt 1 kopiert haben>

     Hinweis: *edgeencryption.thirdparty.vendor.library.path* Für Java 11.
3. Speichern Sie die Änderungen.
4. Fahren Sie mit dem Upgrade auf fort London Oder höher.

Unbound Technology-Schlüssel einrichten

Verwenden Sie Schlüssel für Unbound Technology (zuvor dyadische Sicherheit) mit Edge Encryption Durch Speichern des base64-codierten umschlossenen Verschlüsselungsschlüssels als Textdatei auf dem Edge Encryption Proxy-Server und Bereitstellung des Wrapping-Schlüsselalias. Die Implementierung von Unbound Technology behält die Kontrolle über den Wrapping-Schlüssel.

Vorbereitungen
Erforderliche Rolle: security_admin

Identifizieren Sie in Ihrer Unbound Technology-Implementierung sowohl den Wrapping-Schlüssel als auch den Wrapped-Schlüssel. Verwenden Sie den RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING-Algorithmus für das Wrapping und das Auffüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Exportieren Sie den Wrapped-Schlüssel im base64-codierten Textformat. Speichern Sie die Datei mit dem Schlüsselalias als Namen ohne Dateierweiterung.

Hinweis: Bei Verwendung der Unbound Technology-Verschlüsselungsschlüssel mit Edge Encryption installieren Sie den Proxy-Server mithilfe des Befehlszeileninstallationsprogramms auf dem Unbound-Client-Computer. Der Edge Encryption Proxy-Server muss auf dem gleichen Computer wie der Unbound Technology -Client ausgeführt werden.

Prozedur

1. Fügen Sie den Wrapped-Verschlüsselungsschlüssel im base64-codierten Textformat zum Verzeichnis <proxy-installation-directory>/keys hinzu.
   Der Name der Datei muss der Schlüsselalias ohne Dateierweiterung sein.
2. Aktualisieren Sie die Datei edgeencryption.properties.
   a. Wechseln Sie in das Verzeichnis <proxy-installation-directory>/conf.
   b. Öffnen Sie die Datei edgeencryption.properties.
   c. Geben Sie die Dateispeichereigenschaften ein, und legen Sie den Wert von fest `edgeencryption.keyfile.directory`Bis Schlüssel .

      Diese Eigenschaft weist den Proxy-Server an, nach dem Verschlüsselungsschlüssel im Verzeichnis <Java-home-directory>/keys zu suchen.

      Weitere Informationen zu Edge Encryption Eigenschaften, siehe Eigenschaften des Proxy-Servers für die Edge Encryption.
   d. Heben Sie die Kommentare der Eigenschaften für die Konfiguration des dyadischen Anbieters auf, und legen Sie den Wert von fest `edgeencryption.ekm.provider.rsa.wrapping.key.alias`In den Alias des umschließenden Schlüssels in Ihrer ungebundenen Implementierung.
   e. Speichern und schließen Sie die Datei.

Nächste Maßnahme

Fügen Sie der Instanz den Aliasnamen der Verschlüsselung hinzu. Der Alias des Verschlüsselungsschlüssels ist der Dateiname des Wrapped-Verschlüsselungsschlüssels, der zum Verzeichnis <proxy-installation-directory>/keys hinzugefügt wurde. Wenn zum Beispiel die Datei im Verzeichnis myunboundkey heißt, fügen Sie diesen Namen zum Feld **Schlüsselalias** hinzu. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren.

Einen in einer Datei gespeicherten Verschlüsselungsschlüssel erstellen

Sie können eine einfache Textdatei als Schlüsselspeicher verwenden. Jede Datei enthält einen einzelnen Verschlüsselungsschlüssel.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Dieser Schritt erstellt sowohl den Schlüsselspeicher als auch den Verschlüsselungsschlüssel.

Hinweis: Der Name der Schlüsseldatei muss mit dem in der Tabelle der Verschlüsselungsschlüssel der Instanz angegebenen Schlüsselalias übereinstimmen. Weitere Informationen finden Sie unter Verschlüsselungsschlüssel für die Instanz konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie eine Datei im Ordner /keys des Installationsverzeichnisses des Proxy-Servers.
2. Fügen Sie den Verschlüsselungsschlüssel zur Datei hinzu.

Option	Bezeichnung
AES 128	Platzieren Sie den Verschlüsselungsschlüssel (genau 16 Byte) in der Datei.
AES 256	Platzieren Sie den Verschlüsselungsschlüssel (genau 32 Byte) in der Datei.

3. Aktualisieren Sie die Datei edgeencryption.properties.
   a. Wechseln Sie in das Verzeichnis <installation directory>/conf/.
   b. Öffnen Sie die Datei edgeencryption.properties.
   c. Geben Sie die Eigenschaften für den Dateispeicher ein.
   d. Speichern und schließen Sie die Datei.

Verschlüsselungsschlüssel für die Instanz konfigurieren

Edge Encryption bietet die Tools zum Verwalten von Verschlüsselungsschlüsseln, ohne den Proxy offline zu schalten.

Vorbereitungen

Erforderliche Rolle: security_admin

Vor dem Einrichten neuer Verschlüsselungsschlüssel für die Instanz:

1. Erstellen Sie den Verschlüsselungsschlüssel.
2. Stellen Sie den neuen Schlüssel allen Verschlüsselungsproxys zur Verfügung. Kopieren Sie entweder die Datei oder die Java-Schlüsselspeicherdatei auf jeden Proxy, oder stellen Sie sicher, dass jeder Proxy Zugriff auf den Java-Schlüsselspeicher oder das Enterprise Key Management (EKM)-Gerät hat.

Warum und wann dieser Vorgang ausgeführt wird

Schlüssel-Aliasse müssen eindeutig sein. Jeder Schlüsselalias muss auf jedem Proxy die gleiche Schlüsselgröße und den gleichen Typ haben, oder der Schlüssel kann nicht als Standard zugewiesen werden.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Schlüssel einrichten**an.
2. Führen Sie im Abschnitt „Neue Schlüssel hinzufügen“ des Formulars die folgenden Schritte aus, um einen neuen Schlüssel hinzuzufügen.

> **Wichtig:** Bei Verwendung von mit SafeNet versionierten Schlüsseln wird eine zusätzliche Spalte für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** kann nicht bearbeitet werden. Klicken Sie auf **Rufen Sie die neuesten Schlüsselversionen ab** Link in den zugehörigen Links, um die neueste Version jedes Schlüssels vom Edge-Proxy abzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeilen in der Liste mit einem **X** in der linken Spalte können gelöscht werden. Schlüssel, die als Standard verwendet wurden oder den **Status Verfügbar** haben, können nicht gelöscht werden.

a. Doppelklicken Sie auf die Zeile, die besagt **Fügen Sie eine neue Zeile ein.** .

b. Geben Sie im Bearbeitungsfeld einen Namen für den Schlüssel ein und klicken Sie dann auf das Häkchen.

Schlüsselaliasnamen bestehen aus Kleinbuchstaben und Zahlen. Großbuchstaben werden beim Klicken auf **Aktualisieren** in Kleinbuchstaben geändert. Schlüssel-Aliasse müssen eindeutig sein.

Hinweis: Wenn Sie Unbound Technology-Schlüssel verwenden, fügen Sie den Alias für den Verschlüsselungsschlüssel hinzu. Der Alias des Verschlüsselungsschlüssels ist der Dateiname des Wrapped-Verschlüsselungsschlüssels, der zum Verzeichnis <proxy-installation-directory>/keys hinzugefügt wurde. Wenn zum Beispiel die Datei im Verzeichnis myunboundkey heißt, fügen Sie diesen Namen zum Feld **Schlüsselalias** hinzu.

c. Doppelklicken Sie in derselben Zeile auf die Spalte **Schlüsselgröße**.

d. Wählen Sie im Auswahlfeld eine Schlüsselgröße, entweder **128 Bit** oder **256 Bits** aus und klicken Sie dann auf das Häkchen.

e. Doppelklicken Sie in derselben Zeile auf die Spalte **Typ**.

f. Wählen Sie im Auswahlfeld einen Schlüsseltyp, entweder **Datei**, **Keystore**, **SafeNet** oder **Unbound** aus und klicken Sie dann auf das Häkchen.

g. Wenn Sie mit dem Hinzufügen der Schlüssel fertig sind, klicken Sie auf **Nächster Schritt**.
Sie müssen für jeden Schlüssel einen Aliasnamen, eine Schlüsselgröße und einen Schlüsseltyp angeben, bevor Sie fortfahren.

3. Überprüfen Sie im Abschnitt „Schlüsselstatus“ des Formulars die Option **Status** des Schlüssels und stellen Sie sicher, dass **Verfügbar** eingestellt ist.
4. Wenn der Schlüssel **Verfügbar** ist, klicken Sie auf **Nächster Schritt**.
Dies kann einige Minuten dauern.

Hinweis: Bei Verwendung von mit SafeNet versionierten Schlüsseln wird eine zusätzliche Spalte für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** kann nicht bearbeitet werden.

Die Instanz verfolgt den Status jedes für jeden Proxy verfügbaren Verschlüsselungsschlüssels. Wenn ein Schlüssel für alle Proxys verfügbar ist, ändert sich dessen Status zu **Verfügbar**. Wenn sich der Status nach einigen Minuten nicht ändert, überprüfen Sie, ob der Schlüssel für alle Proxys verfügbar ist. Wenn der Zustand **Nicht verfügbar** bestehen bleibt, hat einer oder haben mehrere Proxys den Schlüssel nicht.

Zustände der Verschlüsselungsschlüssel

Status	Beschreibung
Verfügbar	Alle Online-Proxys haben den Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status	Beschreibung
Nicht verfügbar	Dies ist ein neuer Schlüssel, und die Proxys haben den Schlüssel noch nicht geladen, oder mindestens ein Proxy konnte den Schlüssel nicht laden.

5. Führen Sie im Abschnitt „Standardschlüssel ändern“ des Formulars einen der folgenden Schritte aus:
   - Geben Sie den Schlüsselalias ein.
   - Klicken Sie auf das Lupensymbol und wählen Sie einen Alias aus.

   Hinweis: Bei Verwendung von mit SafeNet versionierten Schlüsseln wird ein zusätzliches Feld für die **Schlüsselversion** angezeigt. Die **Schlüsselversion** ist ausgegraut und kann nicht bearbeitet werden. Wählen Sie nur die neueste Schlüsselversion aus. Wenn Sie eine frühere Version auswählen, wird die folgende Meldung angezeigt, wenn Sie auf klicken **Aktualisieren** Oder **Nächster Schritt** .

   > One of the default keys chosen is not the latest version available for the key. Please use the latest version.

   Wenn die Standardschlüssel nicht die neuesten Versionen der SafeNet-Schlüssel sind, ein **Aktualisieren Sie Standardschlüssel auf die neueste Version** Link wird in den zugehörigen Links angezeigt. Klicken Sie auf den Link, um die Standardschlüssel zu aktualisieren und die neueste Version zu verwenden.

6. Planen Sie im Abschnitt „Schlüsselrotation planen“ des Formulars einen Massenschlüssel-Rotationsauftrag oder einen Einzelschlüssel-Rotationsauftrag, um vorhandene Daten mit dem neuen Verschlüsselungsschlüssel zu verschlüsseln.

   Wenn Sie keinen Massenschlüssel-Rotationsauftrag oder Einzelschlüssel-Rotationsauftrag ausführen, bleiben vorhandene Daten mit dem alten Schlüssel verschlüsselt, bis auf die Daten erneut zugegriffen wird.

Konfigurieren Sie zusätzliche Eigenschaften in der Eigenschaftendatei „Edge Encryption“

Nach dem Installieren des Edge Encryption Proxy-Server in Ihrem Netzwerk und Einrichten des Schlüsselspeichers und der Schlüssel konfigurieren Sie die zusätzlichen Edge Encryption-Eigenschaften.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie <installation directory>/conf/edgeencryption.properties Datei und konfigurieren Sie Folgendes Edge Encryption Proxy-Server-Eigenschaften:
   - Zieleigenschaften (Instanz)
   - Benutzer-Account-Eigenschaften
   - Proxy-Eigenschaften
   - Wenn Sie die Reihenfolge verwenden, die Verschlüsselungstypen oder Verschlüsselungsmuster beibehält, konfigurieren Sie Eigenschaften der Proxy-Datenbank
   - Klartext und statische IV-Eigenschaften
2. Speichern und schließen Sie die Datei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen Web-Proxy

Wenn Ihr Netzwerk einen Web-Proxy verwendet, können Sie den Edge Encryption Proxy für die Verwendung für den Web-Proxy einrichten.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn Ihr Netzwerk keinen Web-Proxy verwendet, belassen Sie die Web-Proxy-Eigenschaften in der Konfigurationsdatei auskommentiert.

Der Edge Encryption Proxy-Server unterstützt die HTTP-Verbindung mit dem Web-Proxy und die Basisauthentifizierung.

Prozedur

1. Wechseln Sie in das Verzeichnis <installation directory>/conf/.
2. Öffnen Sie die Datei edgeencryption.properties.
3. Konfigurieren Sie die Web-Proxy-Eigenschaften.
4. Speichern und schließen Sie die Datei edgeencryption.properties.
5. Wenn der Web-Proxy ein kundenspezifisches Serverzertifikat verwendet, fügen Sie dieses Zertifikat zur JVM hinzu, die vom Edge Encryption Proxy-Server verwendet wird, um eine Vertrauensstellung zwischen dem Web-Proxy und dem Edge Encryption Proxy-Server zu erstellen.
   a. Verwenden Sie CD Befehl, zu dem navigiert werden soll <Java Home Directory>/JRE/lib/Security/cacerts
   b. Führen Sie den Befehl aus: `keytool -keystore cacerts -importcert -alias <chooseAlias> -file <certificateFile>`

Legen Sie die anfängliche Arbeitsspeichergrenze des Proxy-Servers und die obere Arbeitsspeichergrenze fest

Legen Sie das anfängliche und das obere Speichergrenze fest, um festzulegen, wie viel Speicher der Proxy-Server verbrauchen kann. Legen Sie diese Grenzwerte fest, um Leistungsprobleme in Ihrer Edge Encryption Implementierung zu vermeiden.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Legen Sie als Richtlinie sowohl die anfängliche Speichergrenze als auch die obere Speichergrenze auf denselben Wert fest. Weisen Sie dem Betriebssystem auf einem beliebigen Computer 2 GB des physischen Speichers zu. Weisen Sie dann den Rest des physischen Speichers dem Heap zu, indem Sie die Eigenschaften für die anfängliche Speichergrenze und die obere Speichergrenze verwenden. Weisen Sie beispielsweise auf einem Computer mit 8 GB Arbeitsspeicher dem Betriebssystem 2 GB zu, und weisen Sie die verbleibenden 6 GB (6144 MB) dem anfänglichen und dem oberen Speicher zu.

Wichtig: Wenn der Edge Encryption Proxy-Server ausgeführt wird, müssen Sie den Proxy-Server nach der Aktualisierung dieser Eigenschaften anhalten und neu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie in Ihrem Proxy-Server-Verzeichnis <install dir>/conf/wrapper.conf.
2. Fügen Sie am Ende der Datei die folgende Zeile hinzu, um die anfängliche Speichergrenze festzulegen:

   ```
   wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
   ```

   Legen Sie <number> auf die nächst verfügbare <number> in Reihenfolge der Eigenschaften von wrapper.java.additional.<number> fest, die in der Datei wrapper.conf definiert sind.

   Example
   Beispielsweise verfügen Sie über die folgende Liste von Eigenschaften wrapper.java.additional.<number>:

   ```
   wrapper.java.additional.1=
   wrapper.java.additional.2=
   ```

   Die höchste <number> in der obigen Liste ist **2**. Wenn Sie die Zeile wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m hinzufügen, setzen Sie <number> auf **3**, die nächst verfügbare Zahl.

   Wichtig: Lassen Sie keine Lücken in der Nummerierungsfolge.

   Setzen Sie <min_memory_in_MB> auf die Anzahl der verbleibenden Megabytes des Arbeitsspeichers, nachdem dem Betriebssystem 2 GB Arbeitsspeicher zugewiesen wurde.

3. Legen Sie die obere Speichergrenze fest.
   Da im Basissystem keine Obergrenze für den Arbeitsspeicher festgelegt ist, kann der Proxy-Server den gesamten verfügbaren Arbeitsspeicher verwenden. Wenn auf dem Server andere Dienste ausgeführt werden, können Sie die obere Speichergrenze festlegen.

   Fügen Sie am Ende der Datei die folgende Zeile hinzu:

   wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m

   Legen Sie <number> auf die nächst verfügbare <number> in Reihenfolge der Eigenschaften von wrapper.java.additional.<number> fest, die in der Datei wrapper.conf definiert sind.

   Example
   Beispielsweise verfügen Sie über die folgende Liste von Eigenschaften wrapper.java.additional.<number>:

   ```
   wrapper.java.additional.1=
   wrapper.java.additional.2=
   ```

   Die höchste <number> in der obigen Liste ist **2**. Wenn Sie die Zeile wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m hinzufügen, setzen Sie <number> auf **3**, die nächst verfügbare Zahl.

   Hinweis: Lassen Sie keine Lücken in der Nummerierungsfolge.

   Setzen Sie <max_memory_in_MB> auf die Anzahl der verbleibenden Megabytes des Arbeitsspeichers, nachdem dem Betriebssystem 2 GB Arbeitsspeicher zugewiesen wurde.

4. Speichern und schließen Sie die Datei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example: Beispiel: Festlegen der anfänglichen und oberen Speichergrenzen des Proxy-Servers

```
wrapper.java.additional.1 = -Djava.io.tmpdir=../tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

Nächste Maßnahme

Starten Sie den Edge Encryption-Proxy.

Starten Sie den Edge Encryption-Proxy

Nach dem Installieren und Konfigurieren eines Edge Encryption Proxys kann der Proxy aus der Befehlszeile gestartet werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Überprüfen Sie vor dem Starten des Verschlüsselungs-Proxys folgende Punkte:

- Das Plugin Edge Encryption ist in der Instanz aktiviert.
- Die Datei edgeencryption.properties wurde auf diesem Rechner konfiguriert.
- Bei Verwenden eines ordnungserhaltenden Verschlüsselungstyps oder Verschlüsselungsmusters wird die Proxy-Datenbank ausgeführt.

Hinweis: Beim erstmaligen Einrichten der Datei edgeencryption.properties oder Ändern der Eigenschaften können Sie bei Bedarf die Eigenschaft für die Passwortverschlüsselung nicht festlegen. Nachdem Sie überprüft haben, dass alles funktioniert, können Sie die Passwortverschlüsselungseigenschaft festlegen, den Proxy herunterfahren und den Proxy erneut starten.

Prozedur

1. Führen Sie den Proxy-Server aus.

Option	Bezeichnung
Auf einem Linux-Rechner	**a.** CD zu ServerName_port **b.** Ausführen von ./startup.sh
Auf einem Windows-Rechner	Führen Sie die folgenden Schritte aus der Befehlszeile als Administrator aus: **a.** CD zu ServerName_port/bin **b.** Ausführen von edgeencryption.bat starten

2. Überprüfen Sie das Protokoll auf dem Proxy-Server, um sicherzustellen, dass der Proxy ausgeführt wird.

Verschleiern Sie Passwörter in der Eigenschaftendatei

Verschleiern Sie Passwörter in edgeencryption.properties Datei, um die Eigenschaftendatei freigeben zu können, ohne Passwörter mit Klartext offenzulegen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Stellen Sie sicher, dass der Edge Encryption Proxy-Server eingerichtet ist und erfolgreich ausgeführt wird, bevor Sie diese Eigenschaft festlegen. Bevor Sie diese Eigenschaft festlegen, Den Edge Encryption Proxy stoppen.

Warum und wann dieser Vorgang ausgeführt wird
Das Festlegen dieser Eigenschaft kann das Debuggen von Verbindungs- und Zugriffsproblemen beim ersten Start schwierig machen. Legen Sie diese Eigenschaft nur in Produktionsumgebungen fest, nachdem der Proxy erfolgreich eingerichtet und getestet wurde.

Prozedur

1. Wechseln Sie in das Verzeichnis <installation directory>/conf/.
2. Erstellen Sie im Verzeichnis conf eine Textdatei, die eine komplexe Zeichenfolge oder einen Satz enthält, die als Passphrase verwendet werden kann, die der Proxy zum Verschleiern der Passwörter in der Datei edgeencryption.properties verwendet.
   Diese Passphrase sollte eine zufällige und komplexe Phrase sein, die sich nicht auf die Passwörter selbst bezieht.
3. Öffnen Sie die Datei edgeencryption.properties.
4. Legen Sie die Passwort-Verschlüsselungseigenschaft fest.
5. Speichern und schließen Sie die Datei edgeencryption.properties.

Nächste Maßnahme
Nachdem Sie diese Eigenschaft festgelegt haben, können Sie Starten Sie den Edge Encryption-Proxy.

Einen zusätzlichen Proxy manuell hinzufügen

Nachdem der erste Edge Encryption richtig konfiguriert und getestet wurde, können Sie zusätzliche Proxys auf einem Linux- oder Windows-Computer einrichten. Das Installieren mehrerer Proxys auf demselben Computer wird nicht empfohlen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Fügen Sie zusätzliche Proxy-Server auf zusätzlichen Computern hinzu, um eine optimale Umgebung sicherzustellen. Siehe Umgebungsgröße Ihrer Edge Encryption anpassen, um die Anzahl zusätzlich erforderlicher Proxys zu bestimmen.

Hinweis: Stellen Sie sicher, dass alle Proxys die gleichen Verschlüsselungsschlüssel und dasselbe RSA-Schlüsselpaar haben, das zum digitalen Signieren von Konfigurations- und Verschlüsselungsregeln für die Verschlüsselung verwendet wird. Wenn eine Proxy-Datenbank als Teil der Installation eingerichtet wurde, müssen alle Proxys dieselbe Proxy-Datenbank verwenden.

Prozedur

1. Installieren Sie den Proxy mit dem entsprechenden Befehl.
   Weitere Informationen finden Sie unter Den Edge Encryption Proxy-Server (interaktives Installationsprogramm) installieren.
2. Kopieren Sie alle Verschlüsselungsschlüssel und die Datei edgeencryption.properties vom ersten Proxy zum neuen Proxy.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verschlüsselungsschlüssel befinden sich möglicherweise im Proxy-Schlüsselspeicher im Verzeichnis /Keys oder in einem SafeNet KeySecure-Schlüsselspeicher.

3. Öffnen Sie die Datei edgeencryption.properties auf dem neuen Proxy.
4. Ändern Sie die folgenden Eigenschaften:

Eigenschaft	Beschreibung
edgeencryption.proxy.name	Eindeutiger Name des Proxy-Servers
edgeencryption.proxy.host	Der Servername, die IP-Adresse oder der vollständig qualifizierte Domänenname des Computers, auf dem der Proxy ausgeführt wird.
edgeencryption.proxy.http.port	Port auf dem Proxy für die HTTP-Kommunikation. Muss für alle Prozesse auf der Maschine eindeutig sein.
edgeencryption.proxy.https.port	Port auf dem Proxy für die HTTPS-Kommunikation. Muss für alle Prozesse auf der Maschine eindeutig sein.

5. Wenn Sie den Proxy-Server auf einem Windows-Computer installieren, müssen Sie den Namen des Service ändern. Indem Sie öffnen Conf/Wrapper.conf Datei auf dem neuen Proxy und Hinzufügen der in der folgenden Tabelle aufgeführten Eigenschaften.

   Hinweis: Sie müssen diesen Schritt ausführen, bevor Sie den Proxy-Server starten.

Eigenschaft	Beschreibung
wrapper.ntservice.name	Eindeutiger Name des Edge Encryption Proxy-Service.
wrapper.ntservice.displayname	Anzeigename des Edge Encryption Proxy-Service.
wrapper.ntservice.description (Optional)	Beschreibung des Proxy-Server.

6. Speichern und schließen Sie die Datei.
7. Starten Sie den Proxy mit dem entsprechenden Befehl.
   Weitere Informationen finden Sie unter Starten Sie den Edge Encryption-Proxy.

Authentifizieren Sie einen Edge Encryption Proxy-Server

Geben Sie an, dass ein Proxy-Server eine vertrauenswürdige Quelle ist Edge Encryption Kann Anforderungen verarbeiten, die von diesem Proxy-Server stammen.

Vorbereitungen

Wenn ein Proxy-Server nicht authentifiziert ist, enthält das Konsolenprotokoll die folgende Nachricht:

```
WARN This Edge Encryption proxy has not yet been authenticated by the instance.
Please navigate to the matching Proxy record on your ServiceNow instance and authenticate it.
```

Wenn Sie versuchen, auf den Proxy zuzugreifen, erhalten Sie die folgende Nachricht: Diese Website kann nicht erreicht werden .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um den Proxy während des Upgradeprozesses in einem Betriebsstatus zu halten, ist eine Authentifizierung erst erforderlich, nachdem die Proxy-Aktualisierung erfolgreich war.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Proxys**an.
2. Wählen Sie den Proxy aus, und klicken Sie auf **Authentifizieren** .

Ergebnis

Der Proxy wird von verschoben **Nicht Authentifiziert** Bis **Ausstehend** Bis **Authentifiziert** . Der Status ändert sich von **Nicht Authentifiziert** Bis **Ausstehend** Wenn Sie die Authentifizierung starten. Wenn die Authentifizierung abgeschlossen ist, ändert sich der Status von **Ausstehend** Bis **Authentifiziert** , Und Sie können auf den Proxy und zugreifen Edge Encryption Kann Anforderungen vom Proxy annehmen.

Hinweis: Wenn Sie den Proxy anhalten und neu starten, bleibt der Proxy erhalten **Authentifiziert** Und startet erfolgreich neu.

Den Edge Encryption Proxy stoppen

Sie können einen Edge Encryption Proxy aus der Befehlszeile stoppen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Den Proxy-Server stoppen.

Option	Bezeichnung
Auf einem Linux-Rechner	Ausführen von `./shutdown.sh`
Auf einem Windows-Rechner	Ausführen von `edgeencryption.bat stoppen` Um den Windows-Dienst zu entfernen, führen Sie `edgeencryption.bat entfernen` aus.

2. Überprüfen Sie das Protokoll auf dem Proxy-Server, um zu überprüfen, ob der Proxy angehalten wurde.

Den Edge Encryption Proxy unter Linux deinstallieren

Sie können den Edge Encryption Proxy deinstallieren. Wenn Sie den Proxy aktualisieren, ist es nicht notwendig, die aktuelle Version herunterzufahren und zu deinstallieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie müssen Zugriff auf den Computer haben, auf dem der Edge Encryption Proxy ausgeführt wird.

Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie vor dem Herunterfahren des Edge Encryption Proxy sicher, dass keine Benutzer über den Proxy mit der Instanz verbunden sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der unter Linux ausgeführte Verschlüsselungs-Proxy arbeitet als einzelner Prozess. Sie können diesen Prozess beenden, um Aufgaben wie das erneute Bereitstellen des Verschlüsselungsproxys auf einem anderen Host-Computer, das Aktualisieren der Proxyversion, das Aktualisieren der Java-Version oder das Ändern des eindeutigen Namens des Verschlüsselungsproxys bei der Bereitstellung des Verschlüsselungsproxys auf mehreren Proxy-Servern zu erledigen.

Prozedur

1. Sie können die Datei edgeencryption.properties speichern, bevor Sie das Verteilerverzeichnis löschen.
2. Führen Sie das Shell-Skript shutdown.sh aus.
3. Überprüfen Sie das Protokoll auf dem Proxy-Server, um sicherzustellen, dass der Proxy-Server heruntergefahren ist.
4. Löschen Sie die Dateien im Verteilerordner.

Den Edge Encryption Proxy unter Windows deinstallieren

Sie können den Edge Encryption Proxy deinstallieren. Wenn Sie den Proxy aktualisieren, ist es nicht notwendig, die aktuelle Version herunterzufahren und zu deinstallieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie müssen Zugriff auf den Computer haben, auf dem der Edge Encryption Proxy ausgeführt wird.

Stellen Sie vor dem Herunterfahren des Edge Encryption Proxy sicher, dass keine Benutzer über den Proxy mit der Instanz verbunden sind.

Prozedur

1. Sie können die Datei edgeencryption.properties speichern, bevor Sie das Verteilerverzeichnis löschen.
2. Ausführen von edgeencryption.bat stoppen
3. Ausführen edgeencryption.bat entfernen
4. Überprüfen Sie das Protokoll auf dem Proxy-Server, um zu überprüfen, ob der Proxy-Server heruntergefahren ist.
5. Löschen Sie die Dateien im Verteilerordner.

SSO für mehrere Anbieter mit Edge Encryption einrichten

Richten Sie SSO für mehrere Anbieter ein, um die Anmeldung über die Edge Encryption Proxy-Server-URL oder Instanz-URL zu ermöglichen. Wenn Sie Single Sign-on (SSO) für mehrere Anbieter mit implementieren Edge Encryption Wenn diese Option aktiviert ist, müssen sich einige Anwender möglicherweise über bei Ihrer Instanz anmelden Edge Encryption Proxy-Server, andere Anwender möglicherweise nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Aktivieren Sie das Plugin für die Installation des Single Sign-On-Installationsprogramms für mehrere Anbieter (com.snc.integration.sso.multi.installer).
- Aktivieren Sie das Plugin Edge Encryption (com.glide.edgeencryption) und stellen Sie sicher, dass ein oder mehrere Proxy-Server in Ihrem Netzwerk eingerichtet sind.
- Bestimmen Sie die URL für den Edge Encryption Proxy-Server, über den sich Benutzer mit SSO mehrerer Anbieter anmelden. So ermitteln Sie die URL eines Edge Encryption Proxy-Server, siehe Edge Encryption Wird Installiert.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der Anwender, der sich anmeldet, muss die entsprechende URL verwenden, um sich anzumelden, entweder mit dem Edge-Proxy oder nicht mit dem Edge-Proxy.

- Wenn alle Benutzer über den Edge Encryption Proxy-Server geleitet werden, richten Sie Ihren Anbieter-Identifizierungsdatensatz ein und definieren Sie die Proxy-Server-URL in den Feldern **ServiceNow Homepage**, **Entitäts-ID/Aussteller** und **URI der Zielgruppe**.
- Um einige Benutzer über den Proxy-Server und einige Benutzer an die Instanz weiterzuleiten, erstellen Sie zwei Anbieter-Identifizierungsdatensätze. Beide Datensätze verwenden den gleichen Wert im Feld **URL des Identitätsanbieters**. Einer der Datensätze wird jedoch über den Proxy-Server geleitet, während der andere zur Instanz führt.
  - Melden Sie sich über den Instanznamen an: https://<instance name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id Des IdP-Datensatzes für nicht-Edge-Proxy
  - Melden Sie sich über Edge-Proxy an: https://<edge hostname>:<port>/login_with_sso.do?Glide_sso_ID=<sys_ID Des IdP-Datensatzes für den Edge-Proxy

Prozedur

1. Aktivieren Sie die Duplizierung von Identitätsanbieter-URLs in Identitätsanbieter-Datensätzen.
   Eine eindeutige Einschränkung verhindert die Duplizierung der Identitätsanbieter-URL in zwei verschiedenen Identitätsanbieter-Datensätzen. Sie können die Duplizierung der URL des Identitätsanbieters in mehreren IdP-Datensätzen aktivieren, indem Sie ein Feld auf „Falsch“ setzen.
   a. Navigieren zu **Systemdefinition** > **Lexikon**an.
   b. Öffnen Sie Identitätsanbietertabelle [saml2_update1_properties] den Definitionsdatensatz für das Feld **idp**.
   c. Konfigurieren Sie das Formular, um das Feld **Eindeutig** hinzuzufügen.
   d. Stellen Sie sicher, dass der Wert im Feld **Eindeutig** auf **Falsch** gesetzt ist.
2. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an.
3. Erstellen Sie zwei Identitätsanbieter-Datensätze für denselben Identitätsanbieter: einen mit der Instanz-URL und einen mit der Edge Encryption Proxy-Server-URL.
   Informationen zum Erstellen eines Identitätsanbieterdatensatzes finden Sie unter Erstellen Sie einen externen Identitätsanbieter .
   a. Füllen Sie für die Edge Encryption Proxy-Server-URL das Formular mit diesen Werten aus.

Feld	Wert
URL des Identitätsanbieters	Importiert aus den IdP-Metadaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
ServiceNow Homepage	Die URL für Ihre Proxy-Server-Startseite. Zum Beispiel: https://<proxy hostname>:<port>/navpage.do
Entitäts-ID/Aussteller	https://<proxy hostname>:<port>
Zielgruppen-URI	https://<proxy hostname>:<port>

b. Klicken Sie auf **Absenden**.

c. Füllen Sie für die Instanz-URL das Formular mit diesen Werten aus.

Feld	Wert
URL des Identitätsanbieters	Importiert aus den IdP-Metadaten.
ServiceNow Homepage	https://<instance>.service-now.com/navpage.do
Entitäts-ID/Aussteller	https://<instance>.service-now.com/navpage.do
Zielgruppen-URI	https://<instance>.service-now.com/navpage.do

d. Klicken Sie auf **Absenden**.

4. Wahlweise: Wenn Sie mehrere Identitätsanbieter verwenden, ändern Sie den MultiSSO-Installations-Exit.

a. Navigieren zu **Systemdefinition** > **Installationsausgänge**an.
Das System zeigt die aktuelle Liste der Installations-Exits an.

b. Öffnen Sie **MultiSSO** Installations-Exit.

c. Lokalisieren Sie die folgende Anweisung im Feld **Skript**.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
   var idpRecord = this.getIdPRecord(request);
   if (idpRecord) {
      SSO_Helper.debug("IdP found based on SAML response: " +
 idpRecord.getUniqueValue());
      return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
   }
}
```

d. Ersetzen Sie die Anweisung durch den folgenden Code.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
   /* // You have two profiles that use the same IdP entity id it cannot use
   // the IdP issuer / entity id from the response otherwise it may result in the
   // wrong IdP profile. IdP initiated login will not work
   var idpRecord = this.getIdPRecord(request);
   if (idpRecord) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    SSO_Helper.debug("IdP found based on SAML response: " +
idpRecord.getUniqueValue());
    return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
    }*/
  return new SSO_Helper(null, true);
  }
```

Hinweis: Die durch IdP initiierte Anmeldung funktioniert in dieser Konfiguration nicht.

e. Klicken Sie auf **Aktualisieren**.

5. **Wahlweise:** Wenn Sie mehr als ein Unternehmen verwenden, konfigurieren Sie Anwender für SSO mit mehreren Anbietern, und aktualisieren Sie die sys_ID des Identitätsanbieterdatensatzes je nach Anwender.

   (Optional) Weitere Informationen finden Sie unter Konfigurieren Sie Anwender für Multi-Provider-SSO .

   - Um einen Benutzer für die Anmeldung über den Edge Encryption Proxy-Server zu konfigurieren, verwenden Sie die sys_id des Identitätsanbieter-Datensatzes, der die Edge Encryption Proxy-Server-URL verwendet.
   - Um einen Benutzer für die Anmeldung an der Instanz zu konfigurieren, verwenden Sie die sys_id des Identitätsanbieter-Datensatzes, der die Instanz-URL verwendet.

Login-URLs

URL	Login-Ziel
https://<proxy hostname>:<port>/login_with_sso.do?glide_sso_id=<sys_id of the IdP record for the proxy server URL>	Meldet sich über den Proxy-Server an.
https://<instance name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id of IdP record for the instance URL>	Meldet sich über die Instanz an.

Eigenschaften des Edge Encryption Proxy-Servers

Die Konfigurationsdatei edgeencryption.properties im Ordner <installation directory>/conf/ enthält Eigenschaften zum Konfigurieren Ihrer Umgebung.

Sie müssen den Proxy-Server neu starten, nachdem Sie Änderungen an den Eigenschaften des Proxy-Servers vorgenommen haben.

Klartext und statische IV-Eigenschaften

edgeencryption.customer.assigned.known.cleartext	Klartext, damit die Instanz überprüfen kann, ob alle Proxys die gleichen Schlüssel verwenden. Beim Start verschlüsselt der Proxy den Klartext und sendet den verschlüsselten Text an die Instanz. Die Instanz kennt weder den Klartext, noch werden an die Instanz Schlüssel gesendet. Diese Eigenschaft muss für alle Proxys gleich sein.
edgeencryption.encrypter.static.iv	Statischer IV (Initialisierungsvektor), der in der gleichstellungserhaltenden und ordnungserhaltenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Verschlüsselung verwendet wird. Diese Eigenschaft muss für alle Proxys identisch sein und genau 16 Byte (16 ASCII-Zeichen) betragen.

Eigenschaften der digitalen Signatur

edgeencryption.proxy.signature.keystore.path	Pfad und Name der Java KeyStore-Datei.
edgeencryption.proxy.signature.keystore.password	Passwort. Das Standardpasswort lautet <changeme>. Ändern Sie das Passwort nach der Installation des Java KeyStore.
edgeencryption.proxy.signature.keystore.keyalias	Das als Alias angegebene Argument -alias, wenn das RSA-Schlüsselpaar generiert wird.

Dateispeichereigenschaft

edgeencryption.keyfile.directory	Das Verzeichnis gibt an, wo Schlüsseldateien gespeichert werden. Wenn Sie den Java KeyStore oder einen SafeNet KeySecure-Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert. Beispiel: `edgeencryption.keyfile.directory=keys` Wenn Sie Schlüssel für Unbound Technology verwenden, deaktivieren Sie diese Eigenschaft und setzen Sie den Wert auf das Schlüsselverzeichnis.

Allgemeine Konfigurationseigenschaften

edgeencryption.config.poll.interval	Abrufintervall in Sekunden. Die Standardeinstellung bedeutet, dass es 5 Sekunden dauert, bis der Proxy von Änderungen der Verschlüsselungskonfiguration erfährt. Größere Werte führen dazu, dass die Instanz länger braucht, um einen Offline-Proxy zu erkennen. ⚠ **Warnung:** Diese Eigenschaft nicht ändern. Das Ändern der Standardeinstellung des Proxy-Abrufintervalls kann zu Erkennungsverzögerungen führen, wenn ein Proxy online geschaltet wird.
edgeencryption.rules.dir	Ordner, in dem die Verschlüsselungsregeln auf dem Proxy gespeichert sind.
edgeencryption.encryption.order_preserving.cache.enable	Die Einstellung bestimmt, ob Caching zur Unterstützung von ordnungserhaltenden Verschlüsselungstypen verwendet wird.
edgeencryption.encryption.order_preserving.cache.size	Maximale Cache-Größe, in Bytes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

edgeencryption.jobs.concurrency	Maximale Anzahl von Massenverschlüsselungsaufträgen, die gleichzeitig auf diesem Proxy ausgeführt werden können.
edgeencryption.jobs.requests_per_second	Anzahl der HTTP-Auftragsanforderungen pro Sekunde, die von diesem Proxy an die Instanz gesendet werden können.
edgeencryption.attachments.request.timeout.seconds	Zeitüberschreitung für das Hochladen von Anhängen in Sekunden.
edgeencryption.request.buffer.size	Größe einer Verschlüsselungsanforderung. Wenn eine Verschlüsselungsanforderung größer als diese Größe ist, wird der Überschuss auf der Festplatte gespeichert. ⚠ **Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.httpclient.request.buffer.size	Größe der Client-Anforderung. Wenn die Client-Anforderung größer als diese Größe ist, wird der Überschuss auf der Festplatte gespeichert. ⚠ **Warnung:** Diese Eigenschaft nicht ändern.
EdgeEncryption.httpclient.Header.size	Größe des Anforderungs-/Antwortheaders. • Mindestwert: 8K • Höchstwert: 32K ⚠ **Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.proxy.idle.timeout	Zeit in Sekunden, nach der eine Transaktion abläuft. Standardwert: 300 (Sekunden)
edgeencryption.proxy.keepalive.interval	Zeit in Sekunden zwischen den vom Proxy an die Instanz ausgegebenen Pings. Pings werden regelmäßig ausgegeben, um die Verbindung zwischen dem Proxy und der Instanz zu überprüfen. • Standardwert: 10 (Sekunden) • Mindestwert: 5 (Sekunden)
edgeencryption.register.retry.count	Maximale Anzahl, mit der der Proxy die Instanz anpingt, um zu versuchen, zu registrieren. Standardwert: 0 (kein Grenzwert)
edgeencryption.tokenization.exclusion.list	Verschlüsselungsmuster können in diesen Feldern gefundene Zeichenfolgen nicht tokenisieren.

Java KeyStore-Eigenschaften

edgeencryption.keystore.path	Pfad zum Java KeyStore. Wenn Sie einen Dateispeicher oder einen SafeNet KeySecure-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert. Beispiel: `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	Passwort, das der Proxy für die Verbindung zum Java KeyStore verwendet. Wenn Sie einen Dateispeicher oder einen SafeNet KeySecure-Schlüsselspeicher verwenden, lassen Sie diese Eigenschaft auskommentiert.

Protokollierungseigenschaften

Protokollierungseigenschaften befinden sich in der Datei lo4gj2.properties in <installation directory>/conf/ Verzeichnis. Diese Eigenschaften werden nur für die Problembehandlung oder auf Anweisung von geändert ServiceNow Support. Weitere Informationen finden Sie unter So erhöhen Sie die Debug-Protokollierung für den Edge Encryption-Proxy .

Schlüsselspeichereigenschaften des NAE-Geräts

edgeencryption.nae.retries	Anzahl der Wiederholungsversuche.
edgeencryption.nae.enabled	Die Einstellung zeigt an, ob ein NAE-Gerät verfügbar ist.
edgeencryption.nae.server	Name des NAE-Servers
edgeencryption.nae.port	Vom NAE-Server verwendeter Port.
edgeencryption.nae.protocol	Vom NAE-Server verwendetes Protokoll.
edgeencryption.nae.keystore.path	Pfad zum Keystore auf dem NAE-Server.
edgeencryption.nae.keystore.password	NAE-Schlüsselspeicherpasswort.
edgeencryption.nae.username	Benutzername, der zur Authentifizierung beim NAE-Gerät verwendet werden soll.
edgeencryption.nae.password	Passwort zur Authentifizierung beim NAE-Gerät.
edgeencryption.nae.client.certificate	Das Zertifikat, das sich im Keystore des NAE-Servers befindet. Legen Sie diese Eigenschaft für die Authentifizierung mithilfe eines Zertifikats anstelle von Benutzername und Passwort fest.

Passworteigenschaft

edgeencryption.encrypter.properties.password	Name der Datei im Ordner conf, der eine Zeichenfolge enthält, die innerhalb eines sicheren Prozesses zum Verschleiern von Passwörtern in der Datei edgeencryption.properties verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Hinweis: Name der Datei im Ordner conf, der eine Zeichenfolge enthält, die innerhalb eines sicheren Prozesses zum Verschleiern von Passwörtern in der Datei edgeencryption.properties verwendet wird.

Proxy-Eigenschaften

edgeencryption.proxy.host	Servername, IP-Adresse oder vollständig qualifizierter Domänenname des Computers, auf dem der Proxy ausgeführt wird. Zusammen mit dem Port definiert diese Eigenschaft die URL, die der Client für den Zugriff auf den Proxy-Server verwendet.
edgeencryption.proxy.name	Proxy-Name Muss für jeden Proxy eindeutig sein.
edgeencryption.proxy.http.port	Port auf dem Proxy für die HTTP-Kommunikation.
edgeencryption.proxy.https.port	Port auf dem Proxy für die HTTPS-Kommunikation.

Eigenschaft für gesperrte Proxy-Konfiguration

edgeencryption.proxy.locked	Bei „Wahr“ akzeptiert der Proxy keine Konfigurationsänderungen der Verschlüsselung oder Änderungen der Verschlüsselungsregel von der Instanz. Legen Sie diese Eigenschaft für die Produktionsinstanz fest, nachdem alle Verschlüsselungskonfigurationen und Regeln abgeschlossen sind.

Proxy-Datenbankeigenschaften

edgeencryption.db.url	Proxy-Datenbankspeicherort Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.user	Benutzername für den Zugriff auf die Proxy-Datenbank. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.password	Passwort für den Zugriff auf die Proxy-Datenbank. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen.
edgeencryption.db.name	Proxy-Datenbankname. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Der Standardwert für diese Eigenschaft ist Kantenverschlüsselung .
edgeencryption.db.bootstrap.file	Bootstrap-Datei für die Proxy-Datenbank. Die Datei ist relativ zum Verzeichnis sql/. Muss für alle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. ⚠ **Warnung:** Ändern Sie diesen Parameter unter normalen Umständen nicht.

Proxy-Server-Performance-Eigenschaften

Proxy-Server-Performance-Eigenschaften sind standardmäßig nicht in der Konfigurationsdatei vorhanden. Um die Standardwerte zu ändern, müssen Sie die Eigenschaften hinzufügen und den Proxy-Server neu starten. Weitere Informationen finden Sie unter Diagnose und Leistung von Edge Encryption.

edgeencryption.stat.collection.enabled	Aktiviert die Erfassung von Statistiken, die vom Edge Encryption Proxy-Server-Performance-Dashboard verwendet werden. Standardwert: true Fügen Sie diese Eigenschaft hinzu und setzen Sie den Wert auf „Falsch“, um die Sammlung von Statistiken zu deaktivieren, die vom Edge Encryption Proxy-Server-Performance-Dashboard verwendet werden.
edgeencryption.stat.collection.interval	Intervallzeit in Sekunden, in der der Edge Encryption Proxy-Server Statistiken erfasst. Der Wert darf nicht unter 30 Sekunden liegen. Standardwert: 30 (Sekunden)

SSL-Zertifikateigenschaften

Starten Sie Ihren Proxy neu, wenn Sie den Wert einer SSL-Zertifikateigenschaft ändern. Das System verwendet das HTTPS-Schlüsselpaar beim Start, um die Proxy-Serververbindung herzustellen und zu bestimmen, wie der Proxy Client-Anforderungen beantwortet.

edgeencryption.proxy.https.cert.alias	Alias des Zertifikats, das vom Proxy-Server für die Verbindung von Clients bereitgestellt wird.
edgeencryption.proxy.https.keystore.path	Pfad zum Schlüsselspeicher, der das HTTPS-Zertifikat enthält.
edgeencryption.proxy.https.keystore.password	Passwort für den Schlüsselspeicher, der das HTTPS-Zertifikat enthält.

Zieleigenschaften (Instanz)

edgeencryption.target.host	Hostname für die Instanz. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird. Zum Beispiel instancename.servicenow.com
edgeencryption.target.port	Instanzport. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird.
edgeencryption.target.protocol	Instanzprotokoll. Muss für alle Verschlüsselungs-Proxys identisch sein, die eine Verbindung mit derselben Instanz herstellen. Diese Eigenschaft wird festgelegt, wenn der Proxy installiert wird. Verfügbare Optionen: • http • https

Eigenschaften für nicht Unbound Technology-Anbieter

edgeencryption.ekm.provider.classname	Interner Klassenname für die Implementierung. ⚠ **Warnung:** Diese Eigenschaft nicht ändern.
edgeencryption.thirdparty.vendor.library.path	Pfad zur Unbound API-JAR-Datei auf dem Unbound-Client-Computer.
edgeencryption.ekm.provider.rsa.wrapping.key.alias	Wrapping-Schlüsselalias in der Implementierung der Unbound Technology. Muss für alle Proxys gleich sein.

Benutzer-Account-Eigenschaften

edgeencryption.target.username	Benutzername, mit dem sich der Proxy bei der Instanz anmeldet. Der Benutzer muss über die Rolle „edge_encryption“ verfügen. Weitere Informationen finden Sie unter Richten Sie einen Edge Encryption-Anwenderaccount ein.
edgeencryption.target.password	Passwort, mit dem sich der Proxy bei der Instanz anmeldet.

Web-Proxy-Eigenschaften

edgeencryption.webproxy.host	Webproxy-Name oder IP-Adresse
edgeencryption.webproxy.port	Port auf dem Web-Proxy.
edgeencryption.webproxy.user	Benutzername, der zum Herstellen einer Verbindung zum Web-Proxy verwendet wird. Wenn Ihr Web-Proxy keine Authentifizierung verwendet, lassen Sie diese Eigenschaft auskommentiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

edgeencryption.webproxy.password	Passwort für die Verbindung zum Web-Proxy. Wenn Ihr Web-Proxy keine Authentifizierung verwendet, lassen Sie diese Eigenschaft auskommentiert.

Veraltete Proxy-Verschlüsselungseigenschaften

edgeencryption.encrypter.default.key128

Gibt den Namen des aktuellen AES 128-Schlüssels an. Ein AES 128-Schlüssel muss verfügbar sein, auch wenn er nicht verwendet wird. Muss für alle Proxys gleich sein.

Führen Sie die Wartung dieser Schlüssel in der Instanz durch.

edgeencryption.encrypter.default.key256

Gibt den Namen des aktuellen AES 256-Schlüssels an. Muss für alle Proxys gleich sein.

Führen Sie die Wartung dieser Schlüssel in der Instanz durch.

edgeencryption.encrypter.key

Gibt den Schlüsselnamen für jeden Schlüssel an und wird verwendet, um die Standardschlüssel anzugeben. Dies ist der Schlüsselalias, der in die Metadaten integriert ist, die in jedem verschlüsselten Element enthalten sind und daher in der Instanz gespeichert werden. Der Schlüsselname muss aus Kleinbuchstaben bestehen.

edgeencryption.encrypter.type

Gibt den Typ des Verschlüsselungs-Schlüsselspeichersystems an.

edgeencryption.encrypter.file

Gibt den Pfad und den Dateinamen der dem Schlüssel zugeordneten Textdatei an.

edgeencryption.encrypter.password

Gibt das Passwort für den Zugriff auf den Schlüsselspeicher an.

CyberArk-Integration mit dem Edge-Proxy-Server

Verwenden Sie CyberArk, um Passwörter in einem zentralen und sicheren digitalen Tresor zu speichern, um Passwörter zu sichern, die zuvor im Klartext gespeichert und durch Dateizugriff gesichert wurden oder zuvor über eine zweite Datei verschlüsselt wurden.

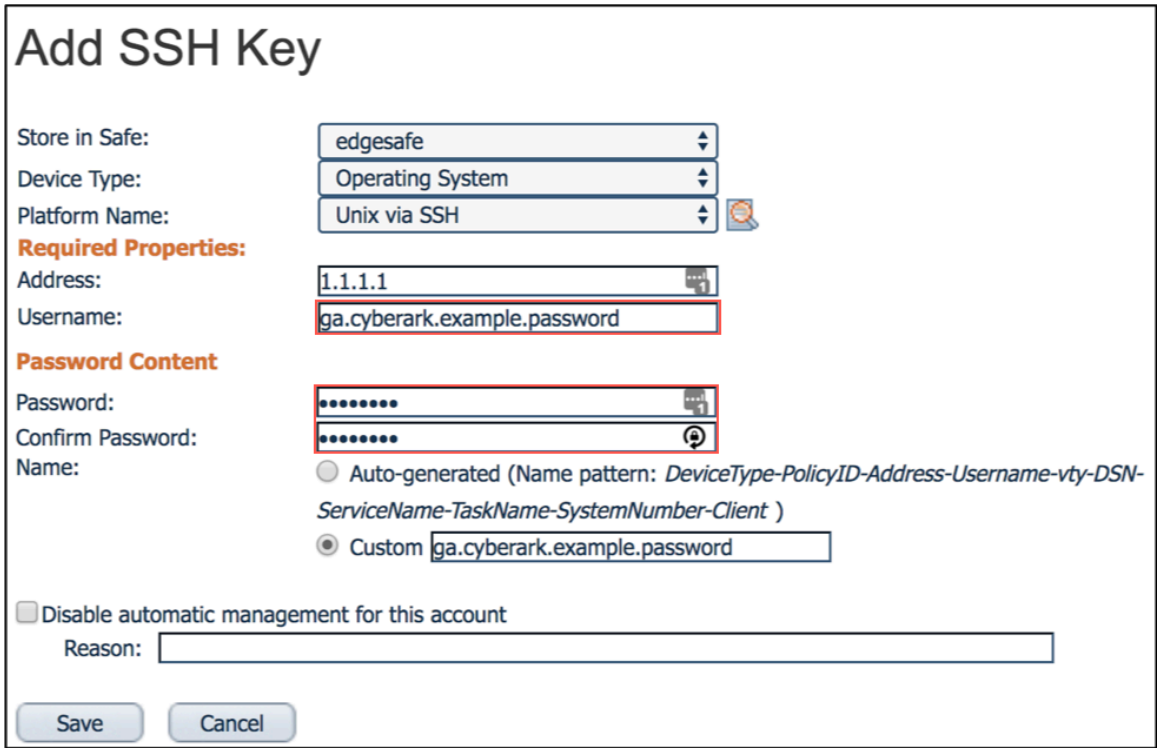
CyberArk AIM (Application Identity Management) verhindert unautorisierten Zugriff, indem hartcodierte und sichtbare Passwörter entfernt werden. AIM speichert Passwörter in einem digitalen Tresor auf einem unabhängigen gehärteten Server, wobei die Passwörter als digitale Anmeldeinformationen dargestellt werden. Die AIM-Clients (die Edge-Proxy-Server) verwenden die digitalen Anmeldeinformationen von CyberArk und greifen auf den unabhängigen Server zu, um die gesicherten Passwörter abzurufen. Auf den Edge-Proxy-Servern oder in der Instanz werden keine Passwörter gespeichert.

CyberArk-Anmeldeinformationen für digitale Tresore

Sie müssen CyberArk erwerben und konfigurieren, bevor Sie die CyberArk-Integration mit dem Edge-Proxy-Server einrichten können.

Legen Sie zum Hinzufügen eines Berechtigungsnachweises für CyberArk (der vom Edge-Proxy gelesen wird) den **Plattformnamen** der Anmeldeinformation auf **Unix über SSH** fest und stellen Sie sicher, dass Sie entweder einen **benutzerorientierten** Anmeldeinformations**namen** generieren oder den **Automatisch generierten** Ausweis**namen** notieren. Wenn Sie den Edge-Proxy für die Verwendung dieser Anmeldeinformation konfigurieren, stimmt der Proxy-Server mit dem **Namen** dieser Anmeldeinformation zur Einstellung im Proxy überein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



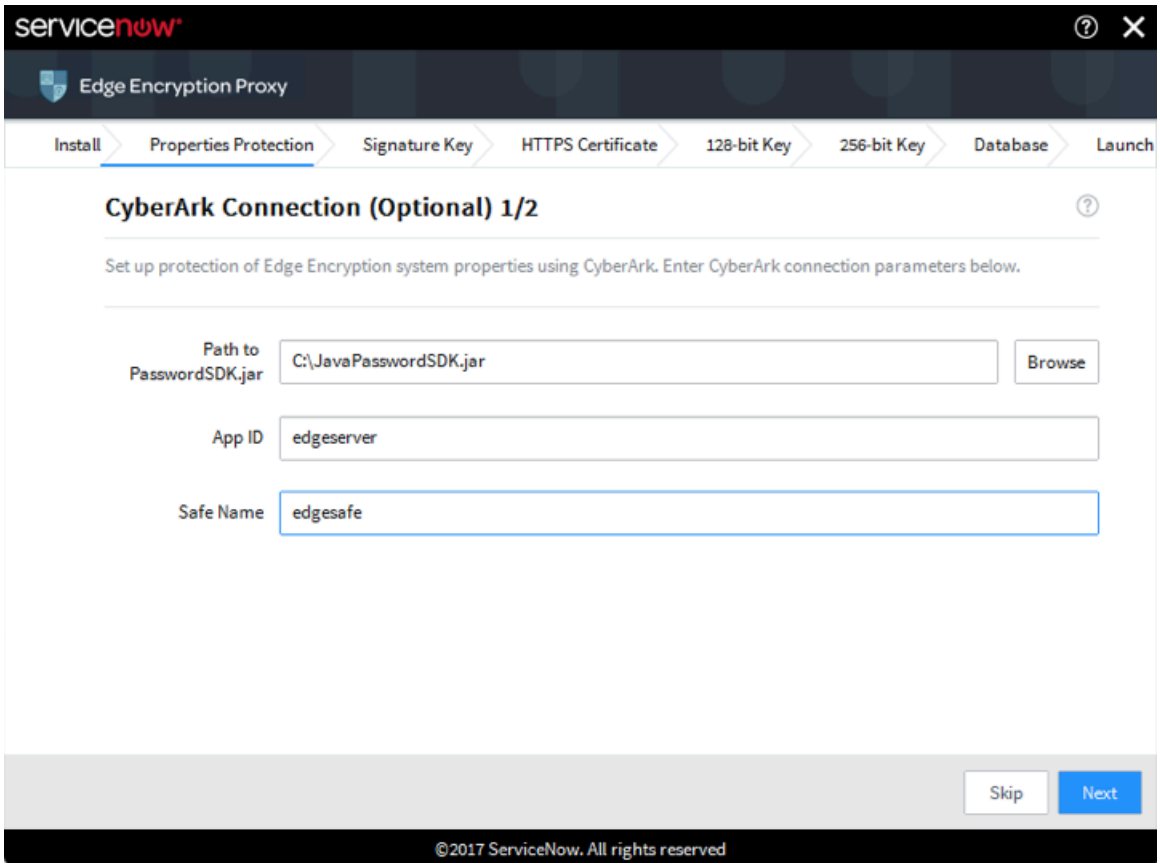
Jeder Anmeldeinformationseintrag enthält ein **Passwort**, das gespeichert wird, sowie einen **Namen** für die Anmeldeinformation, der von einer Anwendung für den Zugriff auf dieses Passwort verwendet wird.

Hinweis: CyberArk-Anmeldeinformationen sind keine Verschlüsselungsschlüssel.

Hinzufügen von CyberArk während der Installation eines Edge-Proxys

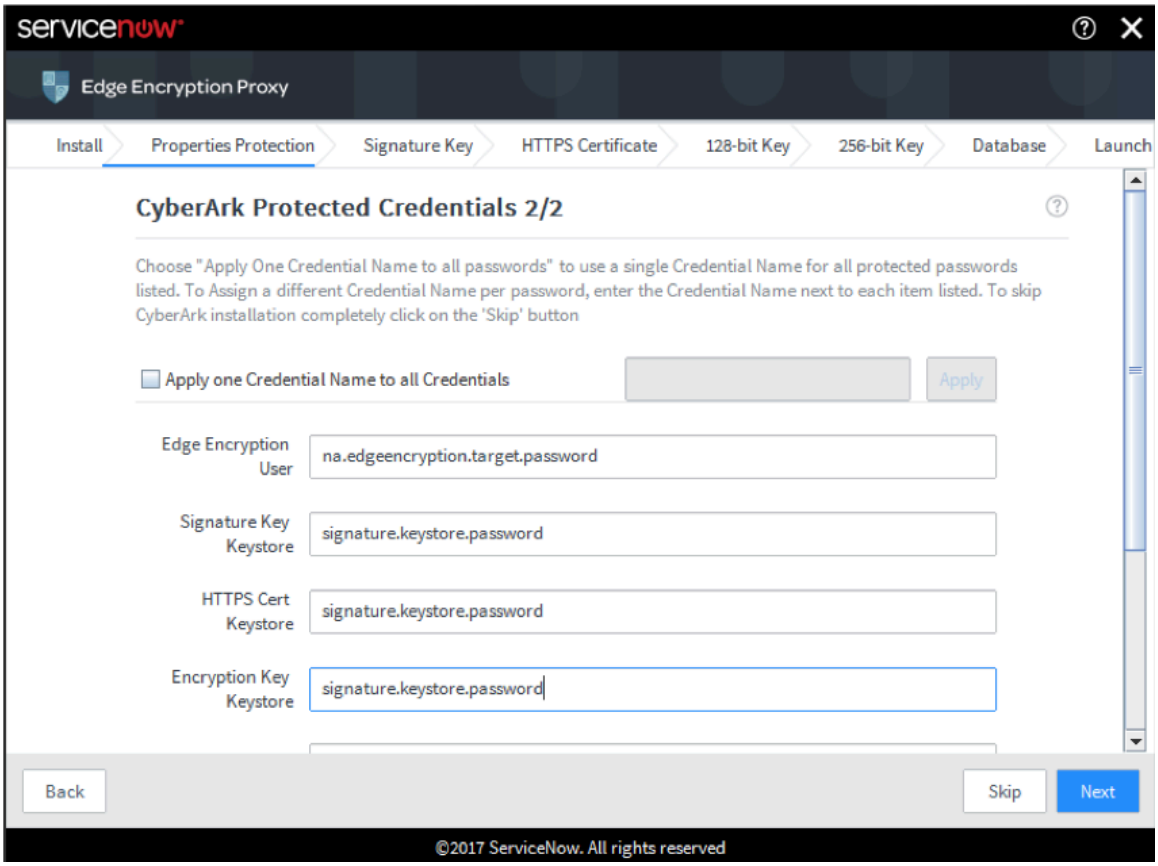
Das Proxy-Installationsprogramm enthält eine neue Konfigurationsseite für eine CyberArk-Integration. Diese Seite ist optional, wenn Sie CyberArk bei der Installation Ihres Proxy mit dem Proxy-Installationsprogramm nicht einschließen möchten. Sie können die CyberArk-Integration auch manuell in der Konfigurationsdatei einrichten und konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Proxy-Installationsprogramm enthält auch eine neue Seite für CyberArk-geschützte Anmeldeinformationen. Auf dieser Seite können verschiedene Eigenschaften mit einem oder mehreren Namen für die Anmeldeinformationen konfiguriert werden. Diese Seite ist optional, wenn Sie CyberArk bei der Installation Ihres Proxy mit dem Proxy-Installationsprogramm nicht einschließen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CyberArk-Passwortschutz

Jedes Passwortfeld im Edge-Proxy-Installationsprogramm, für das eine CyberArk-Anmeldeinformation im CyberArk-Tresor konfiguriert und auf der Seite mit den geschützten Anmeldeinformationen von CyberArk des Installationsprogramms angegeben ist, ist grau und enthält die Nachricht Von CyberArk geschützt.

Einen Load Balancer mit dem Edge-Proxy-Server verwenden

Sie können einen Load Balancer verwenden, um die Last auf den Proxy-Servern in Ihrem Edge Encryption Proxy-Setup auszugleichen. Wenn der Load Balancer und die Proxy-Server unterschiedliche Ports verwenden, geben Sie den Hostnamen und den HTTPS-Port des Load Balancer an, damit Benutzer die Antworten in ihrem Browser anzeigen können.

Wichtig: Alle Produktionsumgebungen sollten aus Gründen der Redundanz mindestens zwei Edge Encryption Proxy-Server enthalten.

Edge-Anforderungsverarbeitung ohne Load Balancer

Wenn Sie keinen Load Balancer verwenden, wird eine Anforderung wie im Folgenden beschrieben verarbeitet.

1. Der Benutzer gibt eine Anforderung von einem Browser aus.
2. Der Browser sendet die Anforderung an den Edge-Proxy-Server.
3. Der Proxy-Server sendet die Anforderung an die ServiceNow-Instanz.
4. Die ServiceNow-Instanz gibt die Antwort an den Proxy-Server zurück.
5. Der Proxy-Server fügt in der Antwortkopfzeile seine eigene Portnummer hinzu, bevor er die Antwort an den Browser des Benutzers zurücksendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anforderung wurde erfolgreich abgeschlossen, da der Benutzer die Antwort des Proxy-Servers unter der in der Antwortkopfzeile angegebenen Anschlussnummer anzeigen kann.

Edge-Anforderungsverarbeitung mit einem Load Balancer

Wenn Sie jedoch einen Load Balancer verwenden, kommuniziert der Browser des Benutzers direkt mit dem Load Balancer, nicht mit dem Proxy-Server. Eine Anforderung wird wie im Folgenden beschrieben verarbeitet.

Hinweis: Das folgende Beispiel verwendet 1025 als Portnummer des Proxy-Servers.

1. Der Benutzer gibt eine Anforderung von einem Browser aus.
2. Der Browser sendet die Anforderung an eine virtuelle IP (VIP) des Load Balancers, die auch als virtueller Server bezeichnet wird.
3. Der VIP ist so konfiguriert, dass er auf den Proxy-Server verweist (z. B. 10.2.200.148:1025). Somit leitet der Load Balancer die Anforderung an den Proxy-Server weiter.
4. Der Proxy-Server sendet die Anforderung an die ServiceNow-Instanz.
5. Die ServiceNow-Instanz gibt die Antwort an den Proxy-Server zurück.
6. Der Proxy-Server schreibt die Location-Kopfzeile in der Antwort mit Werten um, die in den Eigenschaften von risk-servicenow.dev.echonet:1025 konfiguriert sind.
   - **Host**: edgencryption.proxy.host
   - **HTTP-Port**: edgeencryption.proxy.http.port
   - **HTTPS-Port**: edgeencryption.proxy.https.port
7. Der Proxy-Server leitet die Antwort an den Load Balancer weiter, wobei die Location-Kopfzeile auf den Port des Proxy-Servers verweist.

Das Ergebnis hängt davon ab, ob Load Balancer und Proxy-Server denselben Port verwenden.

- Wenn Load Balancer und Proxy-Server denselben Port verwenden, ist die Anforderung erfolgreich, da der Benutzer die Antwort vom selben Port empfängt, der in der Antwort-Kopfzeile angegeben ist.
- Wenn Load Balancer und Proxy-Server unterschiedliche Ports verwenden, schlägt die Anforderung fehl, da der Browser des Benutzers nur mit dem Load Balancer kommuniziert, die Antwort sich jedoch auf dem Proxy-Server befindet.

Lösung

Sie können das Problem beheben, indem Sie einfach den Load Balancer und alle Edge-Proxy-Server am selben Port verwenden. Dies ist jedoch keine ideale Lösung. Eine bessere Lösung besteht darin, das System wissen zu lassen, welchen Port der Load Balancer verwendet.

Mit den folgenden Eigenschaften kann der Edge-Proxy-Server Antwortnachrichten an das Lastenausgleichsmodul umleiten, wenn der Proxy-Server und das Lastenausgleichsmodul unterschiedliche Ports verwenden.

- *edgeencryption.proxy.rewrite.location.host* Gibt den Hostnamen an, der für den Zugriff auf ServiceNow über den Lastenausgleichsmodul verwendet wird.
- *edgeencryption.proxy.rewrite.location.https.port* Gibt den HTTPS-Port an, der für den Zugriff auf ServiceNow über den Lastenausgleichsmodul verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Den Load Balancer konfigurieren

Wenn der Load Balancer und die Proxy-Server unterschiedliche Ports verwenden, geben Sie den Hostnamen und den HTTPS-Port des Load Balancer an, damit Benutzer die Antworten in ihrem Browser anzeigen können.

Vorbereitungen

Erforderliche Rollen:

- Lokaler oder Domänenadministrator auf einem Windows-Host
- Service-Benutzer mit vollem Dateisystemzugriff auf einem Linux-Host

Prozedur

1. Melden Sie sich als Administrator, Domänenadministrator oder Service-Benutzer beim Proxy-Server-Host an.
2. Navigieren Sie zum Installationsverzeichnis für den Edge-Proxy und wählen Sie `conf/edgeencryption.properties`.
3. Setzen Sie die folgenden Eigenschaften:

Eigenschaft	Beschreibung
edgeencryption.proxy.rewrite.location.host	Wenn Ihre Edge-Konfiguration einen Load Balancer enthält, um die Last zwischen Proxy-Servern auszugleichen, werden die Antworten auf den Load Balancer neu geschrieben, so dass Anfragen abgeschlossen werden können. ○ Wenn im Proxy-Setup ein Load Balancer vorhanden ist, geben Sie den Hostnamen an, mit dem Sie über den Load Balancer auf ServiceNow zugreifen. ○ Optional: Wenn das Proxy-Setup keinen Lastenausgleichsmodul enthält, können Sie diesen Wert auf den Hostnamen festlegen, der vom Proxy-Server verwendet wird.
edgeencryption.proxy.rewrite.location.https.port	Wenn Ihre Edge-Konfiguration einen Load Balancer zum Ausgleich der Last zwischen Proxy-Servern enthält, geben Sie den HTTPS-Port an, über den auf ServiceNow über den Load Balancer zugegriffen wird. ○ Wenn in der Konfiguration ein Load Balancer vorhanden ist, geben Sie den HTTPS-Port an, über den der Zugriff auf ServiceNow über den Load Balancer erfolgt. ○ Optional: Wenn in der Konfiguration kein Lastenausgleichsmodul vorhanden ist, können Sie diesen Wert auf den vom Proxy-Server verwendeten HTTPS-Port festlegen.

4. Speichern Sie die Datei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis
Anforderungen können abgeschlossen werden, da Benutzer jetzt Antworten in ihrem Browser anzeigen können.

Upgrade Von Edge Encryption

Sowohl Instanz-Upgrades als auch Proxy-Server-Upgrades erfordern in einer Edge Encryption-Umgebung eine besondere Berücksichtigung.

Instanz-Upgrades

Instanz-Upgrades in einer Edge-Encryption-Umgebung erfordern Vorsicht, um sicherzustellen, dass die Edge-Steuerelemente nach dem Instanz-Upgrade ordnungsgemäß funktionieren.

Während eines Instanz-Upgrades sollten Sie Folgendes nicht hinzufügen, bearbeiten oder löschen:

- Edge Encryption-Konfigurationen
- Edge Encryption-Regeln
- Edge Encryption-Tokenisierungsmuster
- Geplante Aufträge für die Edge Encryption
- Edge Encryption-Schlüsselkonfigurationen
- Geplante Upgrades für die Edge Encryption
- IP-Konfigurationen der Denylist für Edge Encryption

Ein geplanter Auftrag, der während des Instanz-Upgrades ausgeführt wird, wird nicht abgeschlossen. Um den unterbrochenen Auftrag abzuschließen, führen Sie den Auftrag nach dem Instanz-Upgrade erneut aus. Wenn Sie den Auftrag neu einplanen, geht die Verarbeitung, die vor dem Instanz-Upgrade stattgefunden hat, nicht verloren, und der Auftrag verarbeitet weiterhin nur die Daten, die noch nicht verarbeitet wurden.

Proxy-Server-Upgrades

Planen Sie ein Proxy-Upgrade, damit die Instanz den Edge Encryption Proxy-Server aktualisieren oder den Proxy-Server jederzeit manuell aktualisieren kann.

⚠ **Warnung:** Bei einem Upgrade unter Windows können Dateisperrungsprobleme auftreten, und das Upgrade kann fehlschlagen. Damit das Upgrade erfolgreich ist, sollten Sie im Installationsverzeichnis keine Dateien geöffnet haben. Außerdem sollte im Installationsverzeichnis keine Shell vorhanden sein. Insbesondere wenn Sie den Proxy über die Befehlszeile (über) starten `Bin\edgeencryption.bat –Installation/Start`) Im Installationsverzeichnis sollten Sie diese Shell schließen oder danach aus dem Installationsverzeichnis verschieben. Es dürfen keine Dateien im Installationsverzeichnis von einem Editor oder einer anderen Anwendung geöffnet werden.

Drittparteibibliotheken

Bibliotheken von Drittparteien, z. B. Gemalto, gehen bei Upgrades von Instanz- und Proxy-Servern verloren, wenn sie im selben Verzeichnis aufbewahrt werden. Sie können Folgendes ausführen, um den Verlust von Drittanbieterbibliotheken während Upgrades zu verhindern:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Fügen Sie die folgende Eigenschaft manuell zu edgeencryption.properties: hinzu

   `edgeencryption.ekm.provider.classname = com.snc.edgecryption.Encryption.CloudEdgeNaeKeyProvider`

2. Fügen Sie hinzu *`edgeencryption.thirdparty.vendor.library.path`*Standorteigenschaft der Lieferantenbibliothek und legen Sie sie auf fest `/Path/to/JAR` .

   Beispiel:

   `EdgeEncryption.Drittpartei.Vendor.Library.path = /App/servicenow/libs`

3. Kopieren Sie die SafeNet-JARs in diesen Pfad.

Nachdem Sie die Drittanbieterbibliotheken außerhalb von installiert haben Edge Encryption Bei der Installation gehen sie bei Upgrades nicht mehr verloren.

Geplante Upgrades

Wichtig: Während ServiceNow Instanz-Upgrades. Aktualisieren Sie auch Ihre Proxy-Serverversion, um sie an Ihre Instanzversion anzupassen und die Wahrscheinlichkeit von Kompatibilitätsproblemen zu reduzieren.

Planen Sie ein Upgrade, damit die Instanz den Proxy-Server zum geplanten Zeitpunkt aktualisieren kann. Diese Funktionalität ist nach dem Upgrade standardmäßig verfügbar. Ein geplantes Upgrade umfasst folgende Events:

1. Der Proxy-Server überprüft bei der Instanz, ob eine neue Version für das Upgrade verfügbar ist. Neue Versionen werden im Allgemeinen verfügbar, wenn die Instanz aktualisiert wird.
2. Der Administrator erhält beim Anmelden eine Benachrichtigung, wenn eine neue Version des Proxy-Servers verfügbar ist.
3. Der Administrator kann für jeden Proxy-Server Ein Upgrade des Edge Encryption Proxy-Servers planen.

   Hinweis: Nur Benutzer mit der Rolle „security_admin“ können einen Upgrade-Zeitplan über den Proxy-Server erstellen.

4. Sobald das Upgrade geplant ist, wird der Proxy-Server automatisch zum geplanten Zeitpunkt aktualisiert. Während des Upgrades ist der Proxy-Server nur für kurze Zeit offline.

   Hinweis: Da der Proxy-Server während des Upgrades neu startet, ist er für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

5. Während des geplanten Upgrades wird ein neues Proxy-Verzeichnis erstellt und Ihre Konfigurationsdateien werden in das neue Verzeichnis kopiert. Neue Eigenschaften werden in Ihre vorhandene Eigenschaftendatei geschrieben. Die folgenden Dateien oder Verzeichnisse in Ihrem alten Proxy-Verzeichnis werden in das neue Proxy-Verzeichnis kopiert.
   - Das Verzeichnis `/conf`
   - Das Verzeichnis `/keys`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Verzeichnis /keystore
- Die Datei java/jre/lib/security/cacerts

Dadurch bleiben Ihre Schlüssel, Schlüsselspeicher, Einstellungen und Zertifikate erhalten.

Hinweis: Nur die oben genannten Dateien werden in das neue Proxy-Verzeichnis kopiert. Andere angepasste Dateien im Proxy-Server-Verzeichnis werden während eines geplanten Upgrades nicht beibehalten. Die Upgrade-Protokolldatei befindet sich im ursprünglichen Proxy-Verzeichnis im folgenden Ordner: <original-proxy-directory>/tmp/upgrade-wrapper/bin.

Voraussetzungen für geplante Upgrades

Stellen Sie vor dem Planen eines Upgrades für einen Edge Encryption Proxy Folgendes sicher:

1. Die Umgebungsvariable *JAVA_HOME* verweist auf eine Java-Installation auf dem Computer, der sich außerhalb der Verzeichnisstruktur des Edge Encryption Proxys befindet.
2. Die Umgebungsvariable *JAVA_HOME* verweist auf eine Java-Installation mit Version 1.8_u144 oder höher.
3. Die *-Djava.io.tmpdir*Parameter in der Datei Wrapper.conf des Edge Encryption-Proxys verweist auf ein Verzeichnis, das sich AUSSERHALB der Verzeichnisstruktur des Edge Encryption-Proxys befindet, und der Proxy verfügt über Lese-/Schreib-/Ausführungsberechtigungen für das Verzeichnis. Optional können Sie den Parameter vollständig auskommentieren, so dass Java seinen Standard-TMP-Speicherort verwendet.

Manuelle Upgrades

Anstatt einen Aktualisierungszeitplan zu erstellen, können Sie jeden Proxy-Server über die Befehlszeile manuell aktualisieren. Siehe Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren oder Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren.

Proxy-Build-Status

Sie können einfach erkennen, ob ein Proxy-Server veraltet ist, indem Sie zu navigieren **Konfiguration der Edge Encryption** > **Proxys** > **Alle**an. Der Status Ihres Proxy-Builds wird in der Spalte **Proxy Build** mit den folgenden Farben dargestellt:

Grün

Ihr Proxy-Server ist auf dem neuesten Stand.

Gelb

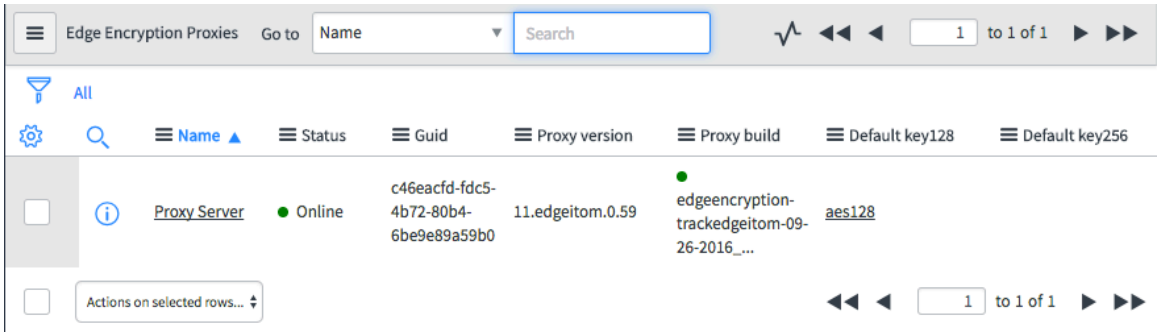
Ihr Proxy-Server ist veraltet und ein Upgrade ist erforderlich.

Orange

Upgrade fehlgeschlagen. Ihr Proxy-Server wird auf die alte Version zurückgesetzt, um sicherzustellen, dass keine Ausfallzeiten auftreten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Problembehandlung bei einem fehlgeschlagenen geplanten Proxy-Upgrade

Wenn ein geplantes Proxy-Upgrade fehlschlägt, wird der Proxy-Server auf die Version zurückgesetzt, von der Sie ein Upgrade durchführen. Alle Originaldaten, Schlüssel und Konfigurationsdateien bleiben erhalten. Dieser Vorgang kann mehrere Minuten dauern. Kontaktieren Sie Kundenservice und Support, um ein erfolgreiches Upgrade sicherzustellen.

Um den Grund für den Fehler zu ermitteln, können Sie **Fehlergrund** im Upgrade-Zeitplan überprüfen. Darüber hinaus wird das Installationsverzeichnis für das fehlgeschlagene Upgrade beibehalten, sodass Protokolldateien für die Problembehandlung verfügbar sind.

Hinweis: Überprüfen Sie vor dem Löschen zusätzlicher Proxy-Verzeichnisse immer, welches Verzeichnis aktuell ist, indem Sie die Protokolldateien überprüfen. Wenn die Protokolldateien eine aktuelle Aktivität aufweisen, ist der Proxy möglicherweise mit Ihrer Instanz verbunden.

Wenn ein geplantes Proxy-Upgrade wiederholt fehlschlägt, können Sie Ihren Proxy-Server manuell aktualisieren. Weitere Informationen finden Sie unter Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren und Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren.

Java-Mindestanforderungen

Der Hostcomputer, der installiert oder ausgeführt wird Edge Encryption Der Proxy-Server muss eine unterstützte Java-Version beibehalten. Aktuell unterstützte Versionen sind Java 17.0.3 oder höher in der 17.x-Versionsreihe.

Hinweis: Java 11 wird ab dem Yokohama-Release nicht mehr unterstützt. Aktualisieren Sie Ihre Umgebung mit Edge Encryption Proxy für Java 17, bevor Sie versuchen, Yokohama oder höhere Versionen von zu installieren Edge Encryption Proxy.

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner <Java-home-directory>/jre/lib/security hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zum Installieren der AES-256-Bit-Verschlüsselungsrichtliniendateien finden Sie unter Konfigurieren Sie den 256-Bit-AES-Verschlüsselungsschlüssel.

Umgebungen mit gemischten Proxy-Versionen

Obwohl eine Umgebung, in der alte Versionen des Proxy-Servers mit aktuellen Versionen des Proxy-Servers ausgeführt werden, nicht empfehlenswert ist, wird sie unterstützt, wenn sich alle Proxy-Server in der gleichen Versionsfamilie wie Ihre Instanz befinden. Wenn Sie beispielsweise eine Instanz im Zurich Release haben, unterstützt Ihre Umgebung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Proxy-Server von jedem Zurich Patch oder Hotfix. Es gelten jedoch die folgenden Einschränkungen.

- Wenn ein Proxy-Server Funktionen unterstützt, die ein anderer Proxy nicht unterstützt, tritt ein inkonsistentes Verhalten auf, je nachdem, welcher Proxy-Server verwendet wird.
- Wenn ein Proxy-Server nicht mehr aktuell ist, enthält er möglicherweise keine aktuellen Sicherheitsverbesserungen.

Wenn ein Proxy-Server aus einer früheren Version mit einer neueren Version der Instanz registriert wird, erhalten Sie regelmäßig Benachrichtigungen, dass der Proxy-Server nicht mehr aktuell ist. Um eine optimale und sichere Umgebung zu gewährleisten, empfiehlt ServiceNow, den Proxy-Server stets auf die neueste Version der von Ihrer Instanz unterstützten Software zu aktualisieren.

Ein Upgrade für den Edge Encryption Proxy-Server planen

Erstellen Sie einen Upgrade-Zeitplan, damit die Instanz einen veralteten Proxy-Server aktualisieren kann.

Vorbereitungen

Um ein Upgrade zu planen, müssen Sie über den Proxy-Server bei Ihrer Instanz angemeldet sein.
Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner <Java-home-directory>/jre/lib/security hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zum Installieren der AES-256-Bit-Verschlüsselungsrichtliniendateien finden Sie unter Konfigurieren Sie den 256-Bit-AES-Verschlüsselungsschlüssel.

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Sobald das Upgrade geplant ist, wird der Proxy-Server automatisch zum geplanten Zeitpunkt aktualisiert. Während des Upgrades ist der Proxy-Server nur für kurze Zeit offline.

Hinweis: Da der Proxy-Server während des Upgrades neu startet, ist er für kurze Zeit offline. Die Zeitdauer wird von Ihrer Umgebung bestimmt und wie lange es dauert, den Proxy-Dienst zu stoppen und erneut zu starten.

Während des geplanten Upgrades wird ein neues Proxy-Verzeichnis erstellt und Ihre Konfigurationsdateien werden in das neue Verzeichnis kopiert. Neue Eigenschaften werden in Ihre vorhandene Eigenschaftendatei geschrieben. Die folgenden Dateien oder Verzeichnisse in Ihrem alten Proxy-Verzeichnis werden in das neue Proxy-Verzeichnis kopiert.

- Das Verzeichnis /conf
- Das Verzeichnis /keys
- Das Verzeichnis /keystore
- Die Datei java/jre/lib/security/cacerts

Dadurch bleiben Ihre Schlüssel, Schlüsselspeicher, Einstellungen und Zertifikate erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Nur die oben genannten Dateien werden in das neue Proxy-Verzeichnis kopiert. Andere angepasste Dateien im Proxy-Server-Verzeichnis werden während eines geplanten Upgrades nicht beibehalten. Die Upgrade-Protokolldatei befindet sich im ursprünglichen Proxy-Verzeichnis im folgenden Ordner: <original-proxy-directory>/tmp/upgrade-wrapper/bin.

Wenn mehrere Proxy-Server nicht mehr aktuell sind, muss für jeden Proxy-Server ein Upgrade individuell geplant werden.

Hinweis: Vermeiden Sie das Hosten mehrerer Proxy-Server auf demselben Computer. Wenn Ihre Umgebung diese Konfiguration enthält, sollten Sie jedoch nicht gleichzeitig Upgrades auf mehrere Proxys auf demselben Computer planen.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Proxys** > **Upgrade-Zeitpläne**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus.

Formular für den Zeitplan für die Aktualisierung des Edge Encryption Proxy

Feld	Beschreibung
Proxy-Server	Proxy-Server wird aktualisiert.
Zielversion	Version, auf die Sie Ihren Proxy-Server aktualisieren. Dieser Wert ist schreibgeschützt und auf die aktuellste für Ihre Instanz verfügbare Proxy-Version festgelegt.
Geplante Startzeit	Datum und Uhrzeit, zu der das Upgrade gestartet werden soll.
Aktiv	Gibt an, ob das geplante Upgrade aktiv ist. Wenn dieses Feld nicht ausgewählt ist, wird das Upgrade nicht zum geplanten Datum und zur geplanten Uhrzeit ausgeführt.
Status	Der Upgrade-Status. Dieser Wert ist schreibgeschützt. Mögliche Status sind: ○ Ausstehend ○ Wird ausgeführt ○ Abgeschlossen ○ Fehlgeschlagen

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Die typische Zeit für ein Upgrade beträgt weniger als 15 Minuten. Nachdem ein Upgrade ausgeführt wurde, können Sie die Upgrade-Details überprüfen, um mehr darüber zu erfahren. Wenn Ihr Upgrade fehlgeschlagen ist, überprüfen Sie **Fehlergrund**, um die nächsten Schritte festzulegen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade-Details

Feld	Beschreibung
Ab Version	Die Version, von der der Server aktualisiert wurde.
Zur Version	Die Version, auf die der Server aktualisiert wurde.
Tatsächliche Startzeit	Zeit, zu der das Upgrade begann.
Endzeit	Uhrzeit, zu der das Upgrade beendet wurde.
Fehlergrund	Grund für das Fehlschlagen des Upgrades.

Einen unter Linux laufenden Edge Encryption Proxy-Server manuell aktualisieren

Einen Proxy aktualisieren, der unter Linux ausgeführt wird.

Vorbereitungen

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner <Java-home-directory>/jre/lib/security hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zum Installieren der AES-256-Bit-Verschlüsselungsrichtliniendateien finden Sie unter Konfigurieren Sie den 256-Bit-AES-Verschlüsselungsschlüssel.

Erforderliche Rolle: Security_admin oder lokaler Administrator auf dem Hostcomputer

Prozedur

1. Laden Sie die Edge Encryption Proxy-Update-Archivdatei in das Installationsverzeichnis herunter.
   a. Navigieren zu **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**
   b. Wählen Sie aus **Laden Sie das Befehlszeilen-Installationsprogramm herunter** Link.
   c. Wenn der Download beginnt, wählen Sie Ihr Installationsverzeichnis als Download-Speicherort aus.
2. Wechseln Sie in das Installationsverzeichnis.
3. Führen Sie den folgenden Befehl aus:

```
java -jar edgeencryption-dist-<version>-linux-x86-64.jar -m dist-upgrade -c <proxy directory>
```

Option	Beschreibung
Proxy-Verzeichnis	Das Verzeichnis im Installationsverzeichnis, in dem der Proxy ursprünglich installiert wurde. Dieses Verzeichnis wird von der Installation erstellt.

Wenn Sie den Hilfebildschirm anzeigen möchten, führen Sie diesen Befehl ohne Argumente aus: `java -jar edgeencryption-dist-<version>-linux-x86-64.jar`

Ein neues Proxy-Verzeichnis wird mit dem aktuellen Zeitstempel erstellt. Eine Sicherung des alten Proxy-Verzeichnisses wird als Backup.dist-Upgrade_timestamp im neuen Proxy-Installationsverzeichnis

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwaltet. Der alte Proxy wird heruntergefahren und der neue Proxy gestartet. Alle offenen Verbindungen/Transaktionen auf dem alten Proxy-Server werden beendet.

4. Überprüfen Sie das Proxy-Protokoll im neuen Verzeichnis und in der Instanz, um sicherzustellen, dass der neue Proxy ausgeführt wird.

Einen unter Windows laufenden Edge Encryption Proxy-Server manuell aktualisieren

Einen Proxy aktualisieren, der unter Windows ausgeführt wird.

Vorbereitungen

Wenn Sie die AES 256-Bit-Verschlüsselung mit Java 8 Update 141 (8u141) oder niedriger verwenden, müssen Sie die Java Cryptography Extension (JCE) Jurisdiction Policy Files installieren, indem Sie sie in das Java-Stammverzeichnis des Systems des jeweiligen Edge Encryption Proxy-Server-Host kopieren. Fügen Sie diese Dateien dem Ordner <Java-home-directory>/jre/lib/security hinzu, bevor Sie ein geplantes oder manuelles Upgrade durchführen. Informationen zum Installieren der AES-256-Bit-Verschlüsselungsrichtliniendateien finden Sie unter Konfigurieren Sie den 256-Bit-AES-Verschlüsselungsschlüssel.

Erforderliche Rolle: Security_admin oder lokaler Administrator auf dem Hostcomputer

Prozedur

1. Laden Sie die Edge Encryption Proxy-Update-Archivdatei in das Installationsverzeichnis herunter.
   a. Navigieren zu **Konfiguration der Edge Encryption** > **Installation und Downloads** > **Downloads**
   b. Wählen Sie aus **Laden Sie das Befehlszeilen-Installationsprogramm herunter** Link.
   c. Wenn der Download beginnt, wählen Sie Ihr Installationsverzeichnis als Download-Speicherort aus.
2. Starten Sie das Windows-CMD-Terminalprogramm mit Administratorrechten.
3. Wechseln Sie in das Installationsverzeichnis.
4. Führen Sie den folgenden Befehl aus:

```
java -JAR edgeEncryption-dist-<version>-all.jar -m dist-Upgrade -c <proxy directory>
```

Option	Beschreibung
Proxy-Verzeichnis	Das Verzeichnis im Installationsverzeichnis, in dem der Proxy ursprünglich installiert wurde. Dieses Verzeichnis wird von der Installation erstellt.

Wenn Sie den Hilfebildschirm sehen möchten, führen Sie diesen Befehl ohne Argumente aus: java -JAR edgeEncryption-dist-<version>-all.jar

Ein neues Proxy-Verzeichnis wird mit dem aktuellen Zeitstempel erstellt. Eine Sicherung des alten Proxy-Verzeichnisses wird als Backup.dist-Upgrade_timestamp im neuen Proxy-Installationsverzeichnis verwaltet. Der alte Proxy wird heruntergefahren und der neue Proxy gestartet. Alle offenen Verbindungen/Transaktionen auf dem alten Proxy-Server werden beendet.

5. Überprüfen Sie das Proxy-Protokoll im neuen Verzeichnis und in der Instanz, um zu überprüfen, ob der Proxy aktualisiert wurde und ausgeführt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Upgrade des Edge Encryption Proxy-Servers rückgängig machen

Wenn ein Proxy-Upgrade nicht erfolgreich ist, können Sie zur vorherigen Version zurückkehren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Upgrade bei Verwendung der geplanten Upgrade-Funktion in der Version Zurich fehlschlägt, wird der Proxy-Server automatisch auf die alte Version zurückgesetzt. Der alte Proxy-Server wird unverändert in einem Sicherungsverzeichnis gespeichert.

Wenn Sie ein manuelles Upgrade rückgängig machen möchten, können Sie diese Schritte ausführen.

Prozedur

1. Fahren Sie den Proxy herunter.
2. Löschen Sie das neue Proxy-Verzeichnis.
3. Benennen Sie das Sicherungsverzeichnis in den Proxy-Namen um.
   Das Sicherungsverzeichnis befindet sich im Proxy-Installationsverzeichnis mit dem Namen `<proxy name>_backup`
4. Starten Sie den Proxy.
5. Überprüfen Sie das Proxy-Protokoll und die Instanz, um sicherzustellen, dass der Proxy online ist.

Konfiguration Von Edge Encryption

Nachdem der Edge Encryption Proxy-Server installiert ist und ausgeführt wird, verwalten Sie Edge Encryption über den Proxy-Server.

Sie müssen alle Schritte unter Edge Encryption Wird Installiert ausführen, bevor Sie Verschlüsselungskonfigurationen und Verschlüsselungsmuster auf der Instanz erstellen.

Hinweis: Um auf die Konfiguration von Edge Encryption zugreifen zu können, müssen Sie sich über den Proxy-Server anmelden und zur Rolle security_admin wechseln.

Rotation von Verschlüsselungsschlüsseln

Führen Sie die Rotation von Verschlüsselungsschlüsseln aus der Instanz aus. Fügen Sie einen neuen Schlüssel hinzu, ändern Sie die Standardschlüsselzuweisung, und planen Sie dann eine Massenschlüsselrotation oder eine einzelne Schlüsselrotation.

Bevor Sie einen Verschlüsselungsschlüssel als Standardschlüssel festlegen, stellen Sie den Schlüssel für jeden Proxy zur Verfügung. Dadurch wird sichergestellt, dass die Proxys den Schlüssel zur Verschlüsselung von Daten haben, wenn der Schlüssel als Standardschlüssel zugewiesen wird. Alle Proxys müssen Zugriff auf einen Schlüssel haben, bevor dieser Schlüssel als Standardschlüssel zugewiesen werden kann.

Warnung: Richten Sie vor dem Löschen eines Schlüssels aus dem Proxy einen Massenschlüssel-Rotationsauftrag ein, und führen Sie ihn aus, um sicherzustellen, dass der Schlüssel nicht von Daten in der Instanz verwendet wird. Wenn Informationen noch mit diesem Schlüssel verschlüsselt sind, können Sie die Informationen nach dem Löschen des Schlüssels nicht entschlüsseln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verhalten von Edge-Filterung und -Sortierung

Wenn Sie Standardschlüssel ändern, achten Sie darauf, eine Schlüsselrotation durchzuführen (entweder Massen- oder Einzelschlüsselrotation). Andernfalls erhalten Sie beim Sortieren und Filtern von Datensätzen möglicherweise unerwartete Ergebnisse. Stellen Sie sich zum Beispiel das folgende Szenario vor:

1. Sie erstellen verschlüsselte Datensätze mit einem Verschlüsselungsschlüssel.
2. Sie erstellen einen neuen Schlüssel und legen ihn als Standard fest.
3. Sie erstellen einen neuen Satz verschlüsselter Datensätze mit dem neuen Verschlüsselungsschlüssel.

Wenn Sie bei der Verbindung über den Edge-Proxy nach einem verschlüsselten Feld filtern, werden möglicherweise nicht alle Datensätze korrekt herausgefiltert, oder Datensätze werden unerwartet angezeigt. Der Filter funktioniert nur für Datensätze, die mit dem aktuellen Standardschlüssel verschlüsselt wurden. Die mit dem vorherigen Standardschlüssel verschlüsselten Datensätze werden weiterhin in der Listenansicht angezeigt.

Wenn Sie bei der Verbindung über den Edge-Proxy nach einem verschlüsselten Feld sortieren, werden im verschlüsselten Feld zwei Gruppen von Datensätzen mit demselben visuell lesbaren Text angezeigt.

Planen Sie einen einzelnen Schlüsselrotationsauftrag

Planen Sie einen Auftrag, um Daten zu finden, die mit einem bestimmten Schlüsselalias verschlüsselt sind, und verschlüsseln Sie die Daten dann erneut mit dem aktuellen Standardverschlüsselungsschlüssel. Die Daten werden entschlüsselt, bevor sie mit dem Standardschlüssel erneut verschlüsselt werden.

Vorbereitungen

Erforderliche Rolle: security_admin

Aktualisieren Sie den Standardschlüssel in, bevor Sie diesen Auftrag planen **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Standardschlüssel festlegen**an.

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Reserviert** > **Einzelschlüsselrotation planen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Einzelschlüsselrotation**.
Schlüssel	Geben Sie den Schlüssel ein, der stillgelegt werden soll. Stellen Sie sicher, dass dieser Schlüssel nicht mehr der Standardschlüssel in ist **Konfiguration der Edge Encryption** > **Konfiguration des Verschlüsselungsschlüssels** > **Standardschlüssel festlegen**an.
Schätzen Sie die Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Nicht verfügbar, wenn eine Einzelschlüsselrotation ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Dieses Feld ist schreibgeschützt und aktiv. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl der Audit-Datensätze, die verarbeitet werden sollen. Nicht verfügbar, wenn eine Einzelschlüsselrotation ausgeführt wird.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
Anzahl der Datensätze schätzen wird bei der Verarbeitung geprüfter Felder nicht unterstützt.

Einen Massenschlüssel-Rotationsauftrag planen

Planen Sie einen Auftrag, um nach mit einem vorherigen Schlüssel verschlüsselten Daten zu suchen, und verschlüsseln Sie die Daten anschließend erneut mit den aktuellen Standard-Verschlüsselungsschlüsseln. Die Daten werden entschlüsselt, bevor sie mit dem aktuellen Standardschlüssel erneut verschlüsselt werden.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Schlüsselmassenrotation planen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Massenschlüsselrotation**.
Schätzen Sie die Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Nicht verfügbar, wenn eine Massenrotation ausgeführt wird.
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Dieses Feld ist schreibgeschützt und aktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl der Audit-Datensätze, die verarbeitet werden sollen. Nicht verfügbar, wenn eine Massenrotation ausgeführt wird.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, um diesen Auftrag zu deaktivieren.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
Anzahl der Datensätze schätzen wird bei der Verarbeitung geprüfter Felder nicht unterstützt.

Einen Rotationsauftrag für einen Anhangsschlüssel planen

Planen Sie einen Auftrag, um mit einem bestimmten Schlüsselalias verschlüsselte Anhänge zu finden, und verschlüsseln Sie die Anhänge dann erneut mit dem aktuellen Standardverschlüsselungsschlüssel. Der Anhang wird entschlüsselt, bevor er mit dem Standardschlüssel erneut verschlüsselt wird.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Anhangsschlüsselrotation planen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Anhangsschlüsselrotation**.
Aktiv	Deaktivieren Sie das Häkchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Geschätzte Datensatzanzahl**.
5. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder mit Verschlüsselungskonfigurationen verschlüsseln

Verschlüsseln Sie Felder, indem Sie Verschlüsselungskonfigurationen erstellen.

Um Edge Encryption zu konfigurieren, müssen Sie über den Proxy mit der Instanz verbunden sein. Testen Sie alle Änderungen auf einer Instanz außerhalb der Produktion, bevor Sie sie auf die Produktionsinstanz anwenden.

Verschlüsselungsschlüssel definieren

Nachdem ein oder mehrere Proxys eingerichtet und ein Standardverschlüsselungsschlüssel konfiguriert wurde, überprüft die Instanz, ob die Schlüssel für alle Proxys verfügbar sind. Sie können einen Verschlüsselungsschlüssel nicht als Standardschlüssel festlegen, es sei denn, alle Proxys haben den Schlüssel. Nachdem ein Standardschlüssel definiert wurde, können Sie Verschlüsselungskonfigurationen erstellen.

Zu verschlüsselnde Felder und Anlagen zuweisen

Die Zuweisung von zu verschlüsselnden Feldern und Anhängen bedeutet, dem Feld oder der Anlage einen Verschlüsselungstyp zuzuordnen. Bevor Sie ein Feld als verschlüsselt markieren, bewerten Sie diese Vorfälle.

- Bestimmen Sie, welche Systemfunktionen betroffen sein könnten.
- Überprüfen Sie alle Skripts auf die Verwendung des Felds.
- Nehmen Sie die gewünschten Anpassungen an der Feldgröße vor. Nachdem ein Feld für die Verschlüsselung konfiguriert wurde, kann die Feldgröße nicht geändert werden.

Durch das Markieren eines zu verschlüsselnden Felds wird die Feldgröße erweitert, um die verschlüsselten Daten zu speichern. Der Prozess zum erweitern der Feldgröße kann je nach Anzahl der Datensätze in der Tabelle lange dauern.

API-Support

Feldverschlüsselung Aktualisiert `SetDisplayValue()` Und `SetValue()` APIs, damit sie verschlüsselte Daten für verschlüsselte Felder einfügen können. Es wird auch aktiviert `GetDisplayValue()` Und `GetValue()` Um Klartextwerte zurückzugeben.

Das folgende Skript veranschaulicht diese API-Änderungen, wenn die Kurzbeschreibung des Incidents verschlüsselt wird:

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

Bei Verwendung von `GetValue()` Um verschlüsselten Text zu erhalten, gibt Ihr Skript den verschlüsselten Text nicht mehr zurück. Ihr Skript gibt den nur-Text zurück, vorausgesetzt, der Anwender hat Zugriff auf das kryptografische Modul. `GetValue()` Gibt den verschlüsselten Text zurück, wenn der Anwender keinen Zugriff auf das kryptografische Modul hat.

Erstellen Sie eine Feldverschlüsselungskonfiguration

Wählen Sie die zu verschlüsselnden Felder aus und geben Sie den Verschlüsselungstyp an.

Vorbereitungen
Erforderliche Rolle: security_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Neu erstellen**an.
2. Füllen Sie das Formular aus.

Feld	Beschreibung
Tabelle	Die Tabelle, die das zu verschlüsselnde Feld enthält.
Typ	Ob eine Tabellenspalte oder Anhänge für die Tabelle verschlüsselt werden sollen. Wählen Sie **Spalte**.
Spalte	Das zu verschlüsselnde Feld. Wird nur angezeigt, wenn **Typ** Ist **Spalte** . Nur Zeichenfolge, Datum, Datum/Uhrzeit, Journal, Journaleingabe, und URL-Felder werden unterstützt. ○ **Zeichenfolgen- und URL-Felder** : Sie können einer übergeordneten Tabelle oder einer untergeordneten Tabelle eine Verschlüsselungskonfiguration hinzufügen. ○ **Datums- und Datums-/Uhrzeitfelder** : Sie können nur einer übergeordneten Tabelle eine Verschlüsselungskonfiguration hinzufügen. Sie können eine neue Verschlüsselungskonfiguration nicht einer untergeordneten Tabelle hinzufügen. **Hinweis:** Abhängig von der Anzahl der Datensätze, die von den Feldern „Datum“ und „Datum/Uhrzeit“ betroffen sind, kann es einige Minuten dauern, bis die Verschlüsselungskonfiguration erstellt wird. Stellen Sie sicher, dass Sie die Verschlüsselungskonfiguration für die Felder „Datum“ und „Datum/Uhrzeit“ erstellen, wenn das Transaktionsvolumen in der Instanz niedrig ist.
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp.

Hinweis: Eine bestimmte Kombination aus Tabelle und Feld kann jeweils nur eine aktive Konfiguration haben.

3. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Nachdem Sie den Verschlüsselungskonfigurationsdatensatz hinzugefügt haben, können Sie einen Verschlüsselungsauftrag erstellen, um vorhandene Daten zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag ausführen, verschlüsselt Edge die vorhandenen Daten bei der nächsten Änderung der Daten. Details finden Sie unter Einen Verschlüsselungsauftrag planen.

Erstellen Sie eine Variablenverschlüsselungskonfiguration

Wählen Sie Servicekatalog-Variablen aus, die verschlüsselt werden sollen, und identifizieren Sie den Verschlüsselungstyp.

Vorbereitungen

Erforderliche Rolle: security_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung**an.
2. In **Konfigurationen Der Edge Encryption-Variablen** Liste, klicken Sie auf **Neu** .
3. Füllen Sie das Formular aus.

Feld	Beschreibung
Variable	Die zu verschlüsselnde Variable.
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Nachdem Sie den Verschlüsselungskonfigurationsdatensatz hinzugefügt haben, können Sie einen Verschlüsselungsauftrag erstellen, um vorhandene Daten zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag ausführen, verschlüsselt Edge die vorhandenen Daten bei der nächsten Änderung der Daten. Details finden Sie unter Einen Verschlüsselungsauftrag planen.

Eine Verschlüsselungskonfiguration deaktivieren

Nachdem Sie ein Feld oder die Anhänge einer Tabelle für die Verschlüsselung konfiguriert haben, können Sie die Verschlüsselung beenden, indem Sie die Verschlüsselungskonfiguration deaktivieren. Nach dem Deaktivieren der Verschlüsselung können Sie einen Entschlüsselungsauftrag für Felder oder einen Entschlüsselungsauftrag für Anhänge ausführen, um die verschlüsselten Daten aus der Instanz zu entfernen.

Vorbereitungen

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

⚠ **Warnung:** Durch das Deaktivieren einer Verschlüsselungskonfiguration wird der Verschlüsselungsdatensatz nicht gelöscht, und der Verschlüsselungstyp kann nicht geändert werden.

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Konfigurationen der Edge Encryption** > **Alle**an.
   Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.
2. Klicken Sie auf die zu deaktivierende Verschlüsselungskonfiguration.
   Das Formular **Edge Encryption-Konfiguration** wird angezeigt.
3. Klicken Sie auf das Feld **Aktiv**.
   Das Feld **Aktiv** ist leer.
4. Klicken Sie auf **Aktualisieren**.
   Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.

Nächste Maßnahme

Sie können einen Entschlüsselungs- oder Anlagenentschlüsselungsauftrag ausführen, um Daten in der Instanz zu entschlüsseln. Wenn Sie keinen Auftrag ausführen, werden die verschlüsselten Daten bei der nächsten Änderung entschlüsselt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einen Verschlüsselungsauftrag planen

Sie können einen Auftrag zum Auffinden und Verschlüsseln aller unverschlüsselten Daten in einem bestimmten Feld mit dem für das Feld konfigurierten Standardverschlüsselungsschlüssel planen. Wenn Sie nach dem Konfigurieren eines Felds für die Verschlüsselung keinen Verschlüsselungsauftrag erstellen, werden nur neue Werte verschlüsselt.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**
   Um einen Auftrag für ein Feld oder zu erstellen **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung** Dient zum Erstellen eines Auftrags für eine Variable.
2. Klicken Sie auf das Feld, für das Sie einen Verschlüsselungsauftrag planen möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenverschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für alle vorherigen Auftragsausführungen angezeigt.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Auftragsart	Wählen Sie **Verschlüsselung**.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Geschätzte Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt.
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt. Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl geprüfter Datensätze, die verarbeitet werden sollen. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt. Dieses Feld ist nur sichtbar wenn **Historische Aufzeichnungen verarbeiten** ausgewählt ist. **Hinweis:** Die Schätzung kann größer sein als die tatsächliche Anzahl der verarbeiteten Datensätze.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Einen Entschlüsselungsauftrag planen

Sie können einen Auftrag zum Entschlüsseln von Daten in einem verschlüsselten Feld einplanen, um klare Daten in der Instanz zu speichern.

Vorbereitungen

Hinweis: Sie müssen den Verschlüsselungsdatensatz für das Feld als inaktiv markieren (deaktivieren Sie das Feld **Aktiv**), um den Entschlüsselungsauftrag auszuführen.

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle** Um einen Auftrag für ein Feld oder zu erstellen **Konfiguration der Edge Encryption** > **Konfiguration der Variablenverschlüsselung** Dient zum Erstellen eines Auftrags für eine Variable.
2. Klicken Sie auf das Feld, das Sie entschlüsseln möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenentschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Entschlüsselung**.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Geschätzte Anzahl der Datensätze	Geschätzte Gesamtzahl der zu verarbeitenden Datensätze. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt.
Historische Datensätze verarbeiten	Wählen Sie diese Option aus, um historische Datensätze in der Audit-Tabelle zu verarbeiten, wenn das Feld geprüft wird. Wenn Sie historische Datensätze für ein Feld in der Audit-Tabelle verschlüsseln, werden sowohl neue als auch alte Werte verschlüsselt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Weitere Informationen zu geprüften Feldern finden Sie unter Auditing.
Schätzen Sie die maximale Anzahl der Audit-Datensätze	Geschätzte maximale Anzahl geprüfter Datensätze, die verarbeitet werden sollen. Wird nach Auswahl von **Geschätzte Anzahl der Datensätze** ausgefüllt. Dieses Feld ist nur sichtbar wenn **Historische Aufzeichnungen verarbeiten** ausgewählt ist. **Hinweis:** Die Schätzung kann größer sein als die tatsächliche Anzahl der verarbeiteten Datensätze.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Anhänge mithilfe der Standardverschlüsselung verschlüsseln

Sie können Anhänge für bestimmte Tabellen verschlüsseln.

Alle Anhänge für eine Tabelle verwenden denselben Verschlüsselungstyp. Verschlüsselte Anhänge werden bei der Textsuche nicht durchsucht. Für Anhänge sind nur die Standardverschlüsselungstypen zulässig. Die ordnungs- und gleichstellungserhaltenden Verschlüsselungstypen sind nicht zulässig.

Für eine Sitzung unter Umgehung des Edge Encryption Proxy:

- Auf einem Datensatz mit aktivierter Anhangsverschlüsselung:
  - Der Benutzer kann Anhänge und die Namen der Anhänge sehen.
  - Der Benutzer kann keine neuen Anhänge hinzufügen.
- Auf einem Datensatz ohne aktivierte Anhangsverschlüsselung:
  - Der Benutzer kann vorhandene Anhänge öffnen und herunterladen.
  - Der Benutzer kann neue Anhänge hinzufügen.

Für eine Sitzung, die den Verschlüsselungsproxy verwendet, kann der Benutzer bestehende Anhänge öffnen und herunterladen sowie neue Anhänge hinzufügen.

Die Anhangsverschlüsselung konfigurieren

Wählen Sie die Tabellen aus, deren Anhänge verschlüsselt werden sollen, und geben Sie den Verschlüsselungstyp an.

Vorbereitungen
Erforderliche Rolle: security_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Konfigurationen der Edge Encryption** > **Neu erstellen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Konfiguration der Edge Encryption

Feld	Beschreibung
Tabelle	Wählen Sie eine Tabelle aus, deren Anhänge verschlüsselt werden sollen.
Typ	Ob eine Tabellenspalte oder Anhänge für die Tabelle verschlüsselt werden sollen. Wählen Sie **Anhang**.
Spalte	Das zu verschlüsselnde Tabellenfeld. Dieses Feld wird angezeigt, wenn der **Typ Spalte** und nicht **Typ Anhang** ist.
Verschlüsselungstyp	Der zu verwendende Verschlüsselungstyp. Für Anhänge sind nur Standard AES128 und Standard AES256 zulässig.

3. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Nachdem der Verschlüsselungsdatensatz hinzugefügt wurde, können Sie einen Anhangsverschlüsselungsauftrag erstellen, um vorhandene Anhänge zu verschlüsseln. Wenn Sie keinen Verschlüsselungsauftrag für Anhänge ausführen, verschlüsselt das System neue Anhänge, wenn Sie sie anhängen.

Hinweis: Wenn Sie markieren *`Attribut „Edge_Encryption_Clear_attachment_allowed“`* Als **Wahr** Im Eintrag „Sammlungswörterbuch“ der Tabelle werden mit Edge Encryption unverschlüsselte Anhänge zu einer Tabelle hinzugefügt, um Anhänge zu verschlüsseln. Wenn Sie dieses Attribut aktivieren, sollten Sie einen „Anhangsverschlüsselungsauftrag“ einrichten, damit alle hinzugefügten unverschlüsselten Anhänge verschlüsselt werden.

Einen Anhangsverschlüsselungsauftrag planen

Sie können einen Auftrag so planen, um unverschlüsselte Anhänge für eine angegebene Tabelle zu suchen und zu verschlüsseln. Verwenden Sie dazu den für die Tabelle konfigurierten Standard-Verschlüsselungsschlüssel.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**an.
2. Klicken Sie auf die Tabelle, für die Sie einen Verschlüsselungsauftrag planen möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Massenverschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.

4. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Auftragsart	Wählen Sie **Anhangsverschlüsselung**.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Einen Anhangsentschlüsselungsauftrag planen

Sie können einen Auftrag planen, um alle verschlüsselten Anhänge für eine bestimmte Tabelle zu entschlüsseln und klare Anhänge in der Instanz zu speichern.

Vorbereitungen

Hinweis: Sie müssen den Verschlüsselungsdatensatz für die Tabelle als inaktiv markieren (deaktivieren Sie das Feld **Aktiv**), um den Entschlüsselungsauftrag auszuführen, da ansonsten nichts passieren wird.

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**an.
2. Klicken Sie auf die Tabelle mit den Anlagen, die Sie entschlüsseln möchten.
3. Klicken Sie unter **Zugehörige Links** auf **Anhangsmassenentschlüsselungsauftrag planen**.

   Das Formular **Geplanter Verschlüsselungsauftrag** wird mit allen Feldern angezeigt. Am unteren Rand des Formulars werden Datensätze für vorherige Auftragsausführungen angezeigt.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Anhangsentschlüsselung**.
Aktiv	Deaktivieren Sie das Häkchen, wenn Sie diesen Auftrag deaktivieren möchten.
Tabelle	Wählen Sie eine Tabelle.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

5. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
6. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.
7. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

Den Verschlüsselungstyp eines Felds oder Anhangs ändern

Sie können den Verschlüsselungstyp eines Felds oder eines Anhangs ändern, indem Sie im vorhandenen Verschlüsselungskonfigurationssatz einen neuen Verschlüsselungstyp auswählen. Eine bestimmte Tabellen- und Feldkombination kann jeweils nur eine aktive Konfiguration haben.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Konfiguration der Edge Encryption** > **Verschlüsselungskonfigurationen** > **Alle**an. Die Liste **Edge Encryption-Konfigurationen** wird angezeigt.
2. Öffnen Sie den Datensatz für die zu ändernde Verschlüsselungskonfiguration.
3. Klicken Sie auf die Dropdown-Liste **Verschlüsselungstyp** und wählen Sie einen neuen Verschlüsselungstyp.

   Hinweis: Für Anhänge sind nur Standard AES128 und Standard AES256 zulässig.

4. Führen Sie, falls erforderlich, einen Auftrag zur Verschlüsselung oder Anhangsverschlüsselung aus.
   Es ist nicht notwendig, einen Verschlüsselungsauftrag auszuführen. Wenn Sie keinen Verschlüsselungsauftrag ausführen, wird das Feld oder der Anhang bei der nächsten Änderung des Felds oder des Anhangs mit dem neuen Verschlüsselungstyp verschlüsselt.

Zeichenketten mithilfe von Verschlüsselungsmustern tokenisieren

Sie können Zeichenkettenmuster durch Token ersetzen, bevor sie an die Instanz gesendet und dort gespeichert werden.

Vorbereitungen

Um Verschlüsselungsmuster verwenden zu können, müssen Sie eine MySQL-Datenbank in Ihrem Netzwerk installieren und einrichten. Dies ist die gleiche Datenbank, die für die ordnungserhaltende Verschlüsselung verwendet wird. Um Verschlüsselungsmuster erstellen oder bearbeiten zu können, müssen Sie über den Proxy mit der Instanz verbunden sein.

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Basissystemmuster verwenden oder eigene Muster erstellen. Basissystemmuster sind erweiterte Muster. Verschlüsselungsmuster enthalten die folgenden Einschränkungen.

- Ein Muster aller Alpha-Zeichen ist nicht zulässig.
- Die minimale Mustergröße beträgt fünf Zeichen. Sie können diese Einstellung mithilfe einer Systemeigenschaft ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Quantifizierer * und + sind in Verschlüsselungsmustern nicht zulässig.
- Verschlüsselungsmuster stimmen mit vollständigen Wörtern überein, nicht mit Teilen von Zeichenfolgen, die in eine größere Zeichenfolge eingebettet sind. Wörter werden durch Leerzeichen und Zeichen definiert, die nicht in ein Muster eingefügt werden können.
- Wenn dieselbe Zeichenfolge mehrmals an die Instanz gesendet wird, wird sie durch das gleiche Token ersetzt.
- Die Textsuche nach exakten Übereinstimmungen wird unterstützt. Die Abfragezeichenfolge wird mit einem Token ausgetauscht, wenn sie an die Instanz gesendet wird, die Suche nach Token durchgeführt wird und wenn die Suchergebnisse an den Proxy-Server zurückgegeben werden, werden die Token durch den Klartext ersetzt. Features wie Stemming werden nicht unterstützt.

Bei der Verwendung von Mustern verlässt der Klartext niemals Ihr Netzwerk. Wenn der Proxy-Server mit einem Muster in einer Anforderung übereinstimmt, die an die Instanz gerichtet ist, ersetzt der Proxy die Zeichenfolge durch ein Token derselben Größe. Das Token wird anstelle der Klartextzeichenfolge an die Instanz gesendet. Wenn die Antwort von der Instanz an den Proxy-Server gesendet wird, ersetzt der Proxy das Token durch die Zeichenfolge. Bei Anzeige über den Proxy-Server wird die Zeichenfolge als Klartext angezeigt.

Hinweis: Verschlüsselte Felder werden nicht auf Verschlüsselungsmuster geprüft.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Verschlüsselungsmuster** > **Neu erstellen**an.
   Alternativ können Sie zu **Erweiterte Muster** navigieren, um ein vorkonfiguriertes Muster zu aktivieren oder zu bearbeiten.
2. Geben Sie den Musternamen ein.
3. Definieren Sie den **Eingabetyp für Edge-Muster**.

Option	Bezeichnung
Basis	Eine Reihe von Zeichentypen. Klicken Sie in der Registerkarte **Eingabe Basismuster** auf die Registerkarte **Hinzufügen** und wählen Sie einen Zeichentyp. Das **Beispielmuster** zeigt das Muster an, wenn Zeichen hinzugefügt werden. Klicken Sie auf **Neuer Block**, um das nächste Zeichen in die nächste Zeile zu verschieben. Auf diese Weise können Sie Zeichen in einem langen Muster gruppieren. Klicken Sie auf **X**, um das letzte Zeichen im Muster zu löschen.
Erweitert	Ein Java-RegEx-Ausdruck. Wenn „Erweitert“ ausgewählt ist, können Sie den Eingabetyp nicht wieder in „Basis“ ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Geben Sie im Feld **Beispielmuster** ein Muster ein, um den RegEx-Ausdruck zu testen. Geben Sie im Feld **Muster** einen Java-RegEx-Ausdruck ein. Klicken Sie auf **Bestätigen**, um zu überprüfen, ob der Ausdruck mit dem Muster übereinstimmt.

Der Eingabetyp legt fest, wie Sie das Muster eingeben. Die Verwendung des Musters wird dadurch nicht beeinflusst.

4. Klicken Sie auf **Absenden**.

Reparieren oder stellen Sie die Bestellung wieder her, wobei verschlüsselte Daten aufbewahrt werden

Wenn Sie die Rolle Security-Admin haben, können Sie vom Edge Encryption Proxy ausgeführte Aufträge planen, um Felder zu reparieren oder wiederherzustellen, die ordnungserhaltende Verschlüsselung verwenden.

Aufgaben planen, um:

- Auftragstoken zu reparieren
- Die Proxy-Datenbank neu zu erstellen.

Die Ausführung dieser Aufträge kann ein zeitaufwändiger Vorgang sein, der sich auf die Leistung von auswirken kann Edge Encryption Proxy. Planen Sie diese Jobs zu einem Zeitpunkt ein, zu dem keine Benutzer oder eine Mindestanzahl von Benutzern das System nutzen, z. B. am Wochenende um Mitternacht.

Einen Reparaturauftrag für ein Auftragstoken planen

Sie können einen Auftrag planen, um Felder zu finden und zu reparieren, in denen das Auftragstoken fehlt.

Vorbereitungen
Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie diese Aufträge, um einzelne Felder in einer Tabelle zu reparieren oder um alle Felder unter Verwendung der ordnungserhaltenden Verschlüsselung zu reparieren. Führen Sie diesen Auftrag aus, wenn die Proxy-Datenbank während der Ausführung der Instanz offline war. Dies führt zu ordnungserhaltenden Feldern, deren Auftragstoken fehlen.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Plantafel Tokenreparatur**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein.
Auftragsart	Wählen Sie **Reparatur von Reihenfolge-Token**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Alle Felder	Aktivieren Sie dieses Kontrollkästchen, um alle Tabellen zu reparieren.
Tabelle	Wählen Sie eine Tabelle.
Spalte	Wählen Sie eine Spalte.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der der Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Geschätzte Datensatzanzahl**.

Einen Proxy-Datenbank-Wiederherstellungsauftrag planen

Führen Sie diesen Auftrag aus, wenn die Proxy-Datenbank Daten verloren hat. Dieser Auftrag findet alle Datensätze, die mit einem Token verschlüsselt wurden (ordnungserhaltender Verschlüsselungstyp), und sendet sie an den Proxy, damit die Proxy-Datenbank neu erstellt werden kann.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Reserviert** > **Datenbankwiederherstellung planen**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen für diesen Auftrag ein.
Auftragsart	Wählen Sie **Datenbankwiederherstellung**.
Aktiv	Deaktivieren Sie dieses Kontrollkästchen, wenn Sie diesen Auftrag deaktivieren möchten.
Ausführen	Wählen Sie den Zeitraum zwischen den Auftragsausführungen.
Wird gestartet	Geben Sie das Datum und die Uhrzeit ein, zu der dieser Auftrag zum ersten Mal ausgeführt werden soll.

3. Klicken Sie auf das Menüsymbol in der Formular-Kopfzeile und wählen Sie **Speichern**.
4. Um eine geschätzte Anzahl von Datensätzen anzuzeigen, die aktualisiert werden sollen, klicken Sie auf **Die Anzahl der Datensätze schätzen**.

Konfigurieren Sie die Liste „IP-Adressen ablehnen“

Verhindern Sie, dass eine IP-Adresse in Ihrem Netzwerk Anforderungen an Ihre Instanz sendet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: security_admin

Da sich der Edge Encryption Proxy-Server in Ihrem Netzwerk befindet, kann er Schwachstellen-Scans durch Ihre Netzwerksoftware unterzogen werden. Um zu verhindern, dass IP-Scanner oder andere Anforderungen an Ihren weitergeleitet werden ServiceNow Instanz können Sie einer Deny-Liste IP-Adressen, IP-Bereiche oder Netzwerkmasken hinzufügen. Jede Verbindung mit dem Proxy-Server über eine Deny-Adresse wird beendet und nicht an Ihre Instanz weitergeleitet.

Um eine IP-Adresse auf eine Deny-Liste zu setzen, müssen Sie über den Proxy-Server bei Ihrer Instanz angemeldet sein.

Wichtig: Stellen Sie sicher, dass Sie Ihre Netzwerktopologie verstehen, bevor Sie IP-Adressen in Ihrem Netzwerk einer Deny-Liste hinzufügen. Wenn der Deny-Liste eine IP-Adresse hinzugefügt wird, wird jeder Anwender mit dieser IP-Adresse vom Zugriff auf gesperrt Edge Encryption Proxy-Server.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Wartung** > **IP-Adressen auf Deny-Liste**an.
   Die Listenansicht „Verschlüsselungs-Proxy-IP-Denylists“ [Edge_Encryption_ip_Blacklist] wird geöffnet.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus.

Feld	Beschreibung
Proxy-Server	Die Edge Encryption Proxy-Server, der an der Weiterleitung von Anforderungen von Adressen in der Deny-Liste gehindert wird.
IP, IP-Bereich oder Netzwerkmaske	Anfragen von dieser IP-Adresse, diesem Bereich oder dieser Netzwerkmaske werden nicht an Ihre ServiceNow-Instanz weitergeleitet. Beispielwerte sind: ○ IP-Adresse: 10.10.10.5 ○ IP-Bereich: 10.10.10.1-15 ○ Netzwerkmaske: 10.10.10.0/24 **Hinweis:** Sie können entweder IPv4- oder IPv6-Adressen verwenden
Aktiv	Ob der Datensatz aktiv ist Nur IP-Adressen aus aktiven Datensätzen können keine Anfragen an die Instanz senden.
Beschreibung	Beschreibung des Datensatzes der Deny-Liste.

4. Klicken Sie auf **Absenden**.
5. Wiederholen Sie diese Schritte für alle anderen Proxys, für die eine IP-Adresse verweigert werden soll.

Ergebnis

Die Edge Encryption Der Proxy-Server beendet eine Verbindung von IP-Adressen, Bereichen oder Netzwerkmasken in der Deny-Liste und kann die Anforderung nicht an die Instanz weiterleiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten von einem Datensatzersteller verschlüsseln

Konfigurieren Sie Ihren Edge Encryption Proxy-Server, um Einfügungen von einem Datensatzersteller zuzulassen, indem Verschlüsselungsregeln aus dem Datensatzersteller-Datensatz erstellt werden.

Vorbereitungen

Erforderliche Rolle: security_admin

Datensatzersteller ermöglichen Endbenutzern das Erstellen von aufgabenbasierten Datensätzen, z. B. Servicekatalog und Serviceportal. Wenn ein Datensatzersteller versucht, Daten in ein für die Verschlüsselung markiertes Feld einzufügen, wird eine ungültige Einfügemeldung angezeigt und die Daten werden nicht im Feld gespeichert.

Das Verschlüsseln von Daten von einem Datensatzersteller erfordert eine für das Zielfeld definierte Verschlüsselungskonfiguration. Stellen Sie sicher, dass Sie eine Verschlüsselungskonfiguration für das Zielfeld und die Zieltabelle erstellt haben, bevor Sie eine Verschlüsselungsregel von einem Datensatzersteller erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Feldverschlüsselungskonfiguration. Um Anhänge eines Datensatzerstellers zu verschlüsseln, Die Anhangsverschlüsselung konfigurieren.

Prozedur

1. Melden Sie sich über den Edge Encryption Proxy-Server bei der Instanz an.
2. Navigieren zu **Servicekatalog** > **Katalogdefinitionen** > **Datensatzersteller**an.
3. Erstellen Sie einen Datensatzersteller Erfassen oder öffnen Sie einen vorhandenen Datensatzersteller-Datensatz.
4. Wählen Sie unter **Zugehörige Links Eine Edge Encryption-Regel erstellen**.
   Es werden automatisch zwei inaktive Verschlüsselungsregeln erstellt, um Daten zu verschlüsseln, die vom Datensatzersteller an das für die Verschlüsselung markierte Feld gesendet werden.

Verschlüsselungsregel	Beschreibung
<RecordProducerName>	Regel erstellt, um POST-Parameter von Servicekatalog zu verarbeiten und Variablen den Feldern in der Instanz zuzuordnen.
<RecordProducerName>Json	Regel, die erstellt wurde, um eine JSON-Nutzlast von Serviceportal zu verarbeiten und Variablen den Feldern in der Instanz zuzuordnen.

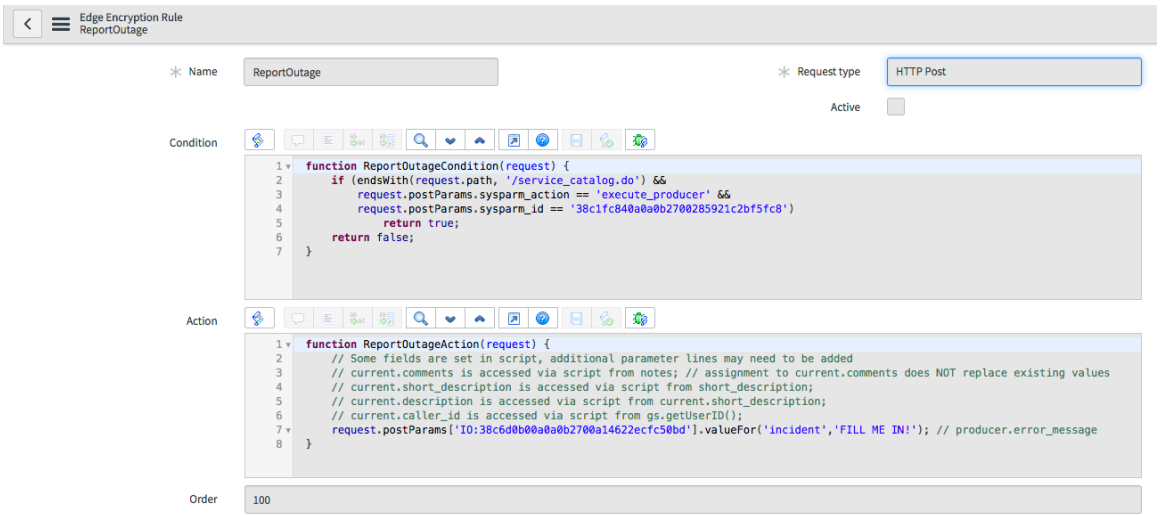
5. Aktivieren Sie die erforderlichen Verschlüsselungsregeln, die vom Datensatzersteller erstellt wurden.
   a. Navigieren zu **Konfiguration der Edge Encryption** > **Regeln** > **Alle**an.
   b. Öffnen Sie je nach Verwendungsort des Datensatzerstellers die zugehörige vom Datensatzersteller erstellte Verschlüsselungsregel und wählen Sie die Option **Aktiv**.
   Bei Verwendung des Datensatzerstellers im Servicekatalog aktivieren Sie die Verschlüsselungsregel <RecordProducerName>. Bei Verwendung des Datensatzerstellers im Serviceportal aktivieren Sie die Verschlüsselungsregel <RecordProducerName>Json.
6. **Wahlweise:** Untersuchen Sie das **Aktion** der Verschlüsselungsregel und fügen Sie die erforderlichen Feldnamen oder Anweisungen hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

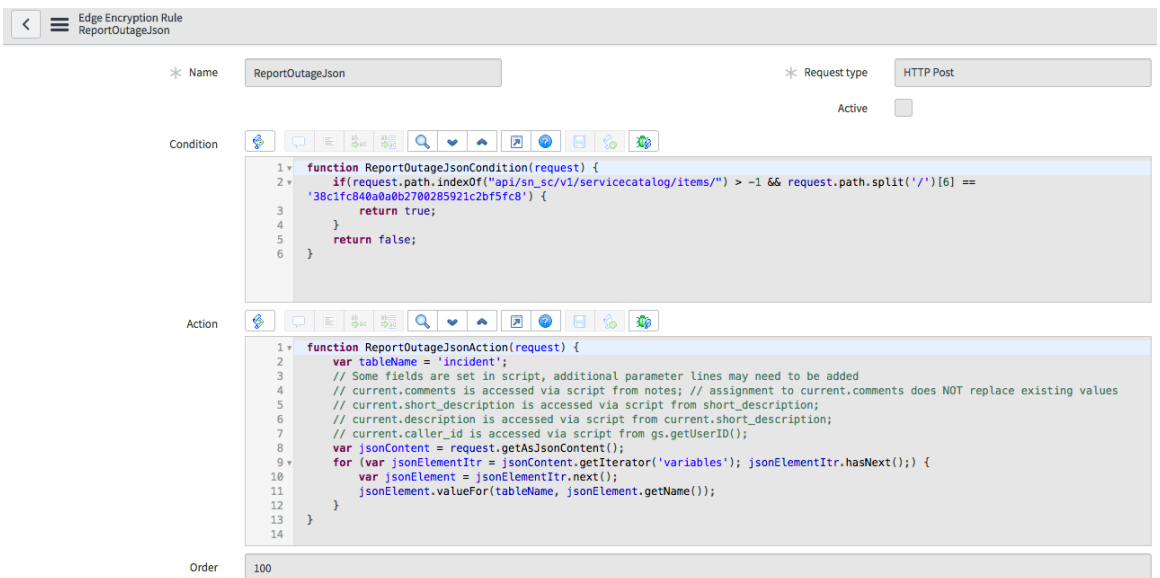
(Optional) Wenn ein Datensatzersteller eine Variable direkt einem Feld in einer Tabelle zuordnet, ordnet die Verschlüsselungsregel die Variable automatisch dem richtigen Feld zu. Wenn eine Variable jedoch indirekt durch verschiedene Skripts auf der Plattform zugeordnet wird, müssen Sie möglicherweise die Regeln aktualisieren, um jede Variable dem richtigen Feld zuzuordnen.

Example

(Optional) Die folgende Verschlüsselungsregel wurde aus dem Datensatzersteller „Report Outage“ erstellt und verarbeitet die POST-Parameter von Servicekatalog, um Variablen den Feldern in der Instanz zuzuordnen. Ersetzen Sie „FÜLL MICH AUS“ mit dem Zielfeld.



Die folgende Verschlüsselungsregel wurde aus dem Datensatzersteller „Report Outage“ erstellt und verarbeitet die JSON-Payload von Serviceportal, um Variablen den Feldern in der Instanz zuzuordnen. Fügen Sie zusätzliche Anweisungen hinzu, um alle Skriptvariablen den Zielfeldern zuzuordnen.



Wenn die Nutzdaten des Datensatzerstellers geprüft werden, enthält das Element error_message den Wert für das Feld short_description. Durch Hinzufügen der folgenden Anweisung können Sie die Skriptvariable error_message dem Feld short_description zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
if (jsonElement.getName() == 'error_message')
      jsonElement.valueFor(tableName, 'short_description');
```

Der Wert des Feldes **Aktion** ändert sich zu:

```
function ReportOutageJsonAction(request) {
 var tableName = 'incident';
 // Some fields are set in script, additional parameter lines may need to be added
 // current.comments is accessed via script from notes; // assignment to current.comments
 does NOT replace existing values
 // current.short_description is accessed via script from short_description;
 // current.description is accessed via script from current.short_description;
 // current.caller_id is accessed via script from gs.getUserID();
 var jsonContent = request.getAsJsonContent();
 for (var jsonElementItr = jsonContent.getIterator('variables'); jsonElementItr.hasNext();) {
  var jsonElement = jsonElementItr.next();
  if (jsonElement.getName() == 'error_message')
   jsonElement.valueFor(tableName, 'short_description');
            } else {
         jsonElement.valueFor(tableName, jsonElement.getName());
 }
}
```

Ergebnis
Die beiden Verschlüsselungsregeln ermöglichen es dem Datensatzersteller, Werte in Felder einzufügen, die für die Verschlüsselung von entweder markiert sind Servicekatalog Oder Serviceportal.

Eine benutzerdefinierte Verschlüsselungsregel definieren

Es kann notwendig sein, sensible Informationen in HTTP-Anforderungen auf dem Weg zu Ihrer Instanz zu identifizieren und zu verschlüsseln. Sie können Verschlüsselungsregeln schreiben, um Daten in solchen Anforderungen zu identifizieren, zu interpretieren und zu verschlüsseln, und Felder in der Anforderung zu Tabellenfeldnamen in Ihrer Instanz zuordnen.

Was ist eine Verschlüsselungsregel?

Verschlüsselungsregeln sind Skripts, die auf dem Edge Encryption Proxy-Server ausgeführt werden, um Felder in einer Anforderung Feldern in einer Tabelle in Ihrer ServiceNow-Instanz zuzuordnen. Eine Verschlüsselungsregel weist den Edge Encryption Proxy-Server an, wie Daten in benutzerdefinierten Payloads verschlüsselt werden.

Hinweis: Verschlüsselungsregeln unterstützen nur ECMAScript 3 und niedriger.

Wann werden benutzerdefinierte Regeln verwendet?

Ein Satz von Verschlüsselungsregeln ist im Edge Encryption Plugin enthalten. Diese Regeln behandeln viele Anwendungsfälle der Core-Plattform, z. B.:

- Bearbeiten eines Felds über das Listenbearbeitungsformular
- Aktualisieren eines Datensatzes aus dem Datensatzformular
- Direkter Webservice verwalten
- Daten aus der REST Application Program Interface (API) werden verarbeitet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen, die mit Standardformularen und -listen erstellt wurden, sollten ohne benutzerdefinierte Verschlüsselungsregeln funktionieren.

Wenn Sie Skripts entwickeln, die Daten enthalten, die verschlüsselt werden sollen, erstellen Sie Verschlüsselungsregeln, um diese Daten zu finden und Glide-Tabellenfeldnamen zuzuordnen. Zum Beispiel:

- Geskriptete Prozessoren
- Geskriptete Webservices
- Geskriptete REST-APIs, UIs oder Ajax-Skripts

Format einer Verschlüsselungsregel

Regeln bestehen aus drei Teilen:

- **Bedingung**: Gibt die Art der Anforderung an.
- **Aktion**: Ordnet Felder in der Anforderung Feldern in einer Tabelle zu und verschlüsselt Werte, die Feldern mit definierten Verschlüsselungskonfigurationen zugeordnet sind.
- **Reihenfolge**: Priorität der Regel. Die Regel mit der niedrigsten Priorität mit einer erfüllten Bedingung ist die einzige ausgeführte Regel. Wie Business Rules laufen die Regeln vom niedrigsten zum höchsten.

Mit Ausnahme von Anhangsanforderungen werden HTTP-Anforderungen von ausgewertet Edge Encryption Proxy-Server. Die Edge Encryption Der Proxy-Server wertet alle Verschlüsselungsregelbedingungen in Prioritätsreihenfolge aus, bis entweder alle Bedingungen „falsch“ oder eine Bedingung „wahr“ zurückgibt. Wenn eine Bedingung „wahr“ zurückgibt, wird die Aktion für die Anforderung ausgeführt, und das Ergebnis wird an die Instanz weitergeleitet. Andere Bedingungen werden nicht bewertet. Daher sollten die Bedingungen für die Verschlüsselungsregeln so genau wie möglich sein. Eine generische Regel kann für eine Anforderung, die von einer anderen Regel verarbeitet werden soll, als „Wahr“ bewertet werden, was dazu führt, dass die Anforderung durch die falsche Aktion verarbeitet wird. Wenn eine generische Bedingung unvermeidbar ist, sollte die Regel mit einem Wert höherer Ordnung markiert werden, damit spezifischere Regeln zuerst ausgewertet werden.

Richtlinien zum Erstellen von Verschlüsselungsregeln

Durch das Erstellen effizienter, optimierter Verschlüsselungsregeln kann die Verarbeitungszeit für die Skriptvalidierung reduziert werden.

Allgemeine Leitlinie : Wenn Regeln lang werden, versuchen Sie, die Anzahl der Blöcke zu minimieren und die Regeln nach Möglichkeit auseinanderzubrechen. Im Idealfall sollten benutzerdefinierte Regeln für bestimmte Anwendungsfälle gelten, anstatt mehrere Fälle zu umfassen, mit den Anweisungen Falls oder „Switch“ im Aktionsskript.

1. Teilen Sie die Regeln, wann immer möglich. Beispiel:
   - Erstellen Sie unterschiedliche Regeln für verschiedene Tabellen und stellen Sie sicher, dass jede Regel nur für die jeweilige Tabelle ausgeführt wird.
   - Erstellen Sie verschiedene Regeln für jeden Datensatzersteller, den Sie anvisieren, oder zumindest für jede Teilmenge der Datensatzersteller. Anstelle einer Regel, die auf Dutzende von sys_ids abzielt, können Sie mehrere verschiedene Regeln erstellen, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf kleinere Teilmengen von Datensatzerstellern abzielen, oder sogar eine Regel pro sys_id erstellen.

Hinweis: Das Erstellen mehrerer Regeln erfordert mehr Wartung. Der Nachteil ist, dass mehrere, einfachere Regeln effizienter validiert werden können als längere, komplexere Regeln.

2. Minimieren Sie die Anzahl der Blöcke. Da das Verarbeitungsmodul jeden Block während der Auswertung von Skripts durchsucht, führt eine große Anzahl von Blöcken zu Verzögerungen bei der Validierung. Beispiel:
   - Ersetzen Sie alle Falls-Blöcke durch ein Array-Lookup, und ersetzen Sie alle Blöcke im Array-Lookup durch nur einen Falls-Block.
   - Kombinieren Wenn Sperrt, wann immer sie gruppiert werden können.

Verschlüsselungsregel-APIs

Verschlüsselungsregeln werden in JavaScript geschrieben und verwenden Edge Encryption APIs zum Auffinden und Verschlüsseln sensibler Informationen im Hauptteil einer Anforderung. Die API verwendet ähnliche Ausdrücke wie xPath, um durch JSON- und XML-Inhalte zu navigieren.

Edge Encryption APIs verarbeiten die Anforderung aus dem Stream, während sie in den Ausgabestream geschrieben wird. Durch die Stream-Analyse können Verschlüsselungsregeln netzwerkfähig sein. Das mehrmalige Abrufen und Analysieren von Inhalten aus dem Körper kann jedoch zu unerwarteten Ergebnissen führen. Um dieses potenzielle Problem aufzuheben, sollten Anforderungen von der Aktion in einem einzigen Durchgang verarbeitet werden.

Beim Erstellen von Verschlüsselungsregeln können Sie keine Glide-APIs, Skripteinbindungen, Geschäftsregeln oder globale Parameter wie verwenden `Aktuell` . Da die Regeln für HTTP-Objekte erstellt werden, ist ein globales Objekt `Anforderung` verfügbar.

Beim Erstellen von Verschlüsselungsregeln können Sie keine APIs aus dem Allow-Listenmanager oder bereichsbezogene Anwendungen verwenden.

Fehlerbehandlung

Wenn eine Bedingung oder Aktion einer Verschlüsselungsregel eine Ausnahmebedingung auslöst, überprüfen Sie das Proxy-Protokoll auf Informationen zur Problembehandlung.

Die Client-Anforderung überprüfen

Bevor Sie eine benutzerdefinierte Verschlüsselungsregel erstellen, müssen Sie das Format der Client-Anforderung festlegen, die auf dem Edge Encryption Proxy-Server eingegeben wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Da Verschlüsselungsregeln Client-Anforderungen durchlaufen und bestimmen, was ggf. verschlüsselt werden muss, müssen Sie den Typ der Anforderung kennen, für die Sie eine Regel erstellen. Das Format der Client-Anforderung bestimmt die Struktur Ihrer Verschlüsselungsregel und die zur Verwendung in der Regel verfügbaren APIs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

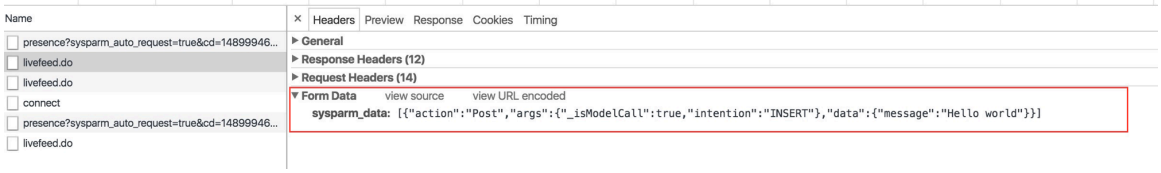
1. Überprüfen Sie die Client-Anforderung.

   Abhängig von der Quelle der Anforderung stehen die folgenden Tools zur Verfügung, um die Anforderung zu überprüfen und das Format zu bestimmen.

Quelle der Anforderung	Verfügbare Tools
Client-Browser	Verwenden Sie die Entwicklerkonsole in Ihrem Browser, um die Client-Anforderung zu überprüfen. Zu den nützlichen Tools gehören: ○ Firefox Netzwerkmonitor ○ Chrome Netzwerkbereich
Drittanbieter/externe Quelle	Verwenden Sie ein HTTP-Protokollanalysegerät, um die Anforderung zu überprüfen. Zu den nützlichen Tools gehören: ○ Wireshark ○ HTTP Scoop Alternativ können Sie häufig Dokumentation für die externe Quelle verwenden, um das Format der Anforderung zu bestimmen.

2. Überprüfen Sie das Paket in der Client-Anforderung und stellen Sie Folgendes fest:
   - Die Methode der Client-Anforderung
   - Der URL-Pfad der Anforderung
   - Die URL-Parameter
   - Die POST-Parameter, falls vorhanden
   - Das Format des Anforderungstextes, falls vorhanden

Example



Ergebnis

Durch Überprüfen der Anforderung erhalten Sie Informationen zu den Feldern, die Sie in Ihrer Verschlüsselungsregel filtern und iterieren müssen. Hinweise zum besseren Verständnis der Felder im Objekt `Anforderung` finden Sie unter Anforderung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Verschlüsselungsregel erstellen

Der Proxy verwendet Verschlüsselungsregeln, um Inhalte in HTTP-Anforderungen zu finden, die verschlüsselt werden sollen.

Vorbereitungen

Erforderliche Rolle: security_admin

Bevor Sie eine Verschlüsselungsregel erstellen, müssen Sie Die Client-Anforderung überprüfen, um das Format zu bestimmen.

Warum und wann dieser Vorgang ausgeführt wird

Um Verschlüsselungsregeln erstellen oder bearbeiten zu können, müssen Sie über einen Verschlüsselungs-Proxy mit der Instanz verbunden sein.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration der Edge Encryption** > **Regeln** > **Neu erstellen**an.
2. Geben Sie im Feld **Name** einen Namen ein.
3. Wählen Sie unter **Anfragetyp** eine HTTP-Methode aus.
   - **HTTP Post**
   - **HTTP Get**
   - **HTTP Put**
   - **HTTP Patch**
   - **HTTP Delete**

   Hinweis: Vor- Jakarta Nur Instanzen zulassen **HTTP-Abrufen** Und **HTTP-Post** Methoden.
4. Geben Sie im Feld **Bedingung** eine JavaScript-Anweisung ein, die festlegt, wann die Regel ausgeführt werden soll.
5. Geben Sie im Feld **Aktion** eine JavaScript-Funktion ein, die ausgeführt werden soll, wenn die Bedingung erfüllt ist.
6. Geben Sie im Feld **Auftrag** die relative Priorität der Regel ein.
7. Klicken Sie auf **Absenden** oder speichern Sie das Formular.

Bedingungen für Verschlüsselungsregeln

Die Bedingungen für die Verschlüsselungsregeln bestimmen, ob die Regel ausgeführt werden soll.

Eine Bedingung für eine Verschlüsselungsregel muss „Wahr“ zurückgeben, wenn die Regel die HTTP-Anfrage behandeln soll; andernfalls muss sie „Falsch“ zurückgeben.

Beachten Sie beim Erstellen Ihrer Bedingung, dass pro Anforderung nur eine Regel ausgeführt wird. Daher muss die Bedingung so allgemein oder spezifisch sein, dass sie unter den vorgesehenen Umständen ausgeführt werden kann.

Hinweis: Seien Sie vorsichtig, wenn Sie Überprüfungen des Inhalts in der Bedingung durchführen. Übermäßige Überprüfungen können für den Proxy-Server teuer sein und zu einer erhöhten Latenzzeit bei der Bearbeitung komplexer Anfragen führen.

Die Bedingung kann den Methodentyp, den Inhaltstyp, den URL-Pfad oder beliebige URL-Abfragezeichenfolgeparameter verwenden, um zu bestimmen, ob die Regel die Anforderung verarbeiten soll. Die Bedingung hat auf diese Felder über das Objekt Anforderung Zugriff.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass Sie vor dem Erstellen einer Verschlüsselungsregel die Client-Anforderung überprüft haben und die für das Auslösen der Regel erforderlichen Bedingungen kennen.

Hinweis: Um effiziente Regeln zu erstellen, sollten Sie einfache Möglichkeiten berücksichtigen, Anforderungen auszuschließen, die nicht von einer Regel ausgewertet werden sollen. Erstellen Sie Ihre Bedingung, um zuerst für diese Anforderungen „Falsch“ zurückzugeben. Diese Methode erhöht die Leistung und leitet die Anforderung schneller an die richtige Regel weiter.

Verschlüsselungsregelobjekte und APIs sind für Verschlüsselungsregelbedingungen verfügbar.

Beispiel mit Pfad und Postparametern

```
/*This condition checks if the request coming in has a path ending in
"/sample_processor.do" and if a post parameter exists in that request called myPostParam */

function SampleCondition(request) {
  if (endsWith(request.path, "/sample_processor.do") && request.postParams.myPostParam) {
     return true;
  }
  return false;
}
```

Beispiel mit urlParams und contentType

```
/* This condition checks if a url parameter exists in the query called
myUrlParam and if the content type contains 'xml'
(if so, you can expect the body to be an XML payload).
Then, it checks if the xml payload contains myXmlTag */

function SampleCondition2(request) {
  if (request.urlParams.myUrlParam && request.contentType.indexOf('xml') > -1 &&
 request.xmlContains('myXmlTag')) {
     return true;
  }
 return false;
}
```

Aktionen für Verschlüsselungsregeln

Eine Verschlüsselungsregel ordnet Felder in einer Client-Anforderung Feldern in einer Tabelle in Ihrer Instanz zu und identifiziert Felder, die für die Verschlüsselung markiert sind.

Eine Verschlüsselungsregelaktion wird nur ausgeführt, wenn die Bedingung der Verschlüsselungsregel „Wahr“ zurückgibt. Eine Verschlüsselungsregel gibt die Daten an, die in Ihrer Anforderungs-Payload verschlüsselt werden sollen. Da die Regel über den Inhalt im Anforderungsobjekt iteriert, müssen Sie die Form und Struktur Ihres Anforderungstexts verstehen und festlegen, was in der Anforderung verschlüsselt werden muss. Die zu verschlüsselnden Daten befinden sich möglicherweise in:

- einem POST- oder URL-Parameter,
- einem JSON- oder XML-Inhalt in einem POST- oder URL-Parameter,
- einer JSON-Payload,
- einer XML-Payload.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie vor dem Schreiben einer Verschlüsselungsregelaktion Folgendes sicher:

- Die Client-Anforderung überprüfen.
- Stellen Sie fest, wo sich die sensiblen Daten im Objekt Anforderung befinden.
- Bestimmen Sie das Feld und den Tabellennamen, in das Daten eingefügt werden sollen, oder verstehen Sie, wie man dies dynamisch aus der Anforderung entnimmt.

Verschlüsselungsregelobjekte und APIs stehen für Verschlüsselungsregelaktionen und -bedingungen zur Verfügung.

Verschlüsselungsregelobjekte und APIs

Verwenden Sie Verschlüsselungsregel-APIs, um Werte in Anforderungen zu analysieren und zu verschlüsseln, die sich durch den Edge Encryption Proxy-Server zur Instanz bewegen.

Die für Ihre Verschlüsselungsregel verfügbaren APIs hängen vom Format des Anforderungsobjekts ab. Wenn der contentType-Parameter des Anforderungsobjekts beispielsweise XML ist, können Sie XML-APIs verwenden, um Werte in der Payload zu analysieren und zu verschlüsseln. Nachdem Sie den Objekttyp in Ihrer Anforderung ermittelt haben, können Sie eine Verschlüsselungsregel mit den verfügbaren APIs erstellen.

Verschlüsselungsregel-APIs sind sowohl in den Bedingungen für Verschlüsselungsregeln als auch in Aktionsskripts verfügbar.

Anforderung

Das Objekt *`Anforderung`* ist ein globales Objekt, das in Edge Encryption Regelaktionen und Bedingungsskripts verfügbar ist.

Das Objekt *`Anforderung`* ist ein JavaScript-Objekt, das die Client-Anforderung darstellt, die an den Edge Encryption Proxy-Server gesendet wird. Sie müssen Ihre Verschlüsselungsregel erstellen, um das Objekt *`Anforderung`* zu analysieren, die Objektwerte *`Anforderung`* Feldern in einer Tabelle in der Instanz zuordnen und alle sensiblen Daten im Objekt *`Anforderung`* verschlüsseln.

Das Objekt *`Anforderung`* enthält die folgenden Attribute und Daten aus der Client-Anforderung:

Anforderungsobjektfelder

Feld	Beschreibung
Pfad	Der Pfadbestandteil der URL.
requestMethod	GET, POST, PUT, PATCH, DELETE.
contentType	Das Kopfzeilenfeld „Content-Type“.
urlParams	Die Parameter in der Abfragezeichenfolge. Dies kann auch als String ausgewertet werden.
postParams	Wenn es sich um einen Formular-Post handelt, enthält dieser die Post-Parameter.

Anforderung – getAsJsonContent()

Gibt die Anforderung als iterierbares Objekt vom Typ *`JsonNode`* zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige JSON-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt *`Anforderung`*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald die Anforderung als `JsonNode`-Objekt zurückgegeben wird, können Sie mit Hilfe von JSON-APIs über das Objekt iterieren und Felder verschlüsseln.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Die Anforderung als iterierbarer `JsonNode`.

Anforderung – getAsXmlContent()

Gibt den Anforderungsinhalt als iterierbares Objekt vom Typ `XMLContent` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige XML-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt `Anforderung`.

Sobald die Anfrage als `XMLContent`-Objekt zurückgegeben wird, können Sie mit Hilfe von XML-APIs über die Objekt- und Verschlüsselungsfelder iterieren.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLContent	Die Anforderung als iterierbares Objekt vom Typ `XMLContent`.

Anforderung – XMLContains (Zeichenfolgenpfad)

Gibt „Wahr“ zurück, wenn der angegebene Pfad im XML DOM vorhanden ist.

Diese Methode ist nur verfügbar, wenn der Anforderungstext eine gültige XML-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt `Anforderung`.

Parameter

Name	Typ	Beschreibung
Pfad	Zeichenfolge	XPath-Anweisung, nach der Sie suchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
Boolean	Gibt an, ob der angegebene Pfad im XML DOM vorhanden ist.

POST- und URL-Parameter-APIs

POST- und URL-Parameter können als Eigenschaften des Objekts *Anforderung* über request.postParams und request.urlParams aufgerufen werden.

Auf jeden einzelnen Parameter kann als Eigenschaft der übergeordneten Objekte *postParams* und *urlParams* durch Aufrufen von request.postParams.myParam zugegriffen werden. Jeder Parameter, auf den auf diese Weise zugegriffen wird, ist ein Objekt der zugrunde liegenden Klasse *ParameterValue*. Alle APIs in dieser Klasse können für jeden Parameter aufgerufen werden.

Nach dem Überprüfen der Client-Anforderung kann es notwendig sein, auf Parameterwerte aus dem Objekt *Anforderung* zuzugreifen und diese zu verschlüsseln. Abhängig von den Daten in der Clientanforderung können Sie Werte auf mehrere Arten verschlüsseln und sie Feldern in der Instanz zuordnen.

Den Wert einer bekannten Tabelle und eines Felds verschlüsseln

Wenn Sie den Namen der Instanztabelle und des Felds kennen, in dem die verschlüsselten Daten gespeichert werden sollen, können Sie sie explizit in der Verschlüsselungsregel definieren. Möglicherweise wissen Sie beispielsweise, dass die Anforderung in der Instanz verarbeitet wird, um einen Incident zu erstellen, und Sie möchten den Parameter **Text** im Beschreibungsfeld verschlüsseln. In diesem Fall können Sie die folgende Aktion erstellen.

```
function SampleAction1() {
   request.postParams.text.valueFor('incident', 'description');
}
```

Den Wert einer dynamisch definierten Tabelle und eines Felds verschlüsseln

Wenn Sie andererseits den Namen des Feldes nicht kennen, das die verschlüsselten Daten füllen sollen, können Sie sie mit **tableName** und **fieldName** dynamisch definieren.

Im folgenden Beispiel wird eine generische Anforderung verarbeitet, in der möglicherweise Daten in verschiedenen Aufgabentabellen (z. B. Incident, Problem und Change_request) in der Instanz gespeichert werden.

```
function SampleAction2() {
   var tableName = request.urlParams.table;
   for (var parameter in request.postParams) {
      var currentParam = request.postParams[parameter];
      var fieldName = currentParam.toString();
      if (fieldName == 'text') {
         currentParam.valueFor(tableName, 'description')
      } else {
         currentParam.valueFor(tableName, fieldName);
      }
   }
}
```

Diese Aktion:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ruft die Zieltabelle aus den URL-Parametern ab.
- Iteriert über die URL-Parameter.
- Fordert den Edge Encryption Proxy-Server auf, jeden URL-Parameter mit einem Namen zu verschlüsseln, der einem für die Verschlüsselung markierten Feld entspricht.
- Sucht nach einem bestimmten Parameter namens *Text* und fordert den Edge Encryption Proxy auf, den Wert basierend auf der Verschlüsselungskonfiguration für das Beschreibungsfeld in der Incident-Tabelle zu verschlüsseln.

In diesem Beispiel führt die Methode valueFor() eigentlich keine Verschlüsselung durch. Vielmehr fordert das Verfahren den Edge Encryption Proxy-Server auf, zu prüfen, ob das Tabellen-/Feldpaar im Anforderungsobjekt mit einer Verschlüsselungskonfiguration zur Verschlüsselung vorgemerkt ist, und gegebenenfalls zu verschlüsseln.

JSON oder XML innerhalb eines Parameters verschlüsseln

Ein POST- oder URL-Parameter kann JSON- oder XML-Inhalte enthalten. In diesem Fall können Sie den Inhalt innerhalb des Parameters verarbeiten, die Werte durchlaufen und die erforderlichen Felder verschlüsseln. In diesem Beispiel wird weiterhin über einen POST-Parameter auf **tableName** zugegriffen, aber der Wert des Feldes ist das JSON-Objekt **Daten**.

```
function SampleAction3() {
   var tableName = request.postParams.table;
   var data = request.postParams.data;
   var dataIterator = data.getAsJsonContent().iterator();
   while (dataIterator.hasNext()) {
      var jsonElement = dataIterator.next();
      var fieldName = jsonElement.getName();
      if (fieldName == 'text') {
         jsonElement.valueFor(tableName, 'description');
      } else {
         jsonElement.valueFor(tableName, fieldName);
      }
   }
}
```

Ein Beispiel für eine Verschlüsselungsregelaktion, die XML innerhalb eines POST-Parameters verarbeitet.

```
function SampleAction4() {
   var tableName = request.postParams.table;
   var data = request.postParams.data;
   var dataIterator = data.getAsXmlContent().getIteratorOverAllChildren();
   while (dataIterator.hasNext()) {
      var jsonElement = dataIterator.next();
      var fieldName = jsonElement.getName();
      if (fieldName == 'text') {
         jsonElement.valueFor(tableName, 'description');
      } else {
         jsonElement.valueFor(tableName, fieldName);
      }
   }
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Anforderung verschlüsseln

In einer Client-Anforderung, die vertrauliche Daten enthält, tritt möglicherweise eine verschlüsselte Abfrage in einem Parameter auf. Um ein Feld in einer Abfrage einem verschlüsselten Wert in der Instanzdatenbank zuzuordnen, müssen Sie eine Verschlüsselungsregel erstellen, die den Proxy-Server auffordert, zu prüfen, ob ein Feld in der Abfrage für die Verschlüsselung markiert ist. Die Methode encodedQueryFor() analysiert eine verschlüsselte Abfrage für eine bestimmte Tabelle und prüft, ob Felder in der Abfrage Verschlüsselungskonfigurationen enthalten.

In diesem Beispiel durchläuft die Regel die Parameter und sucht den Parameter **Filter**, der voraussichtlich eine Glide-codierte Abfrage ist.

```
function SampleAction5() {
   var tableName = request.urlParams.table;
   for (var parameter in request.postParams) {
      var currentParam = request.postParams[parameter];
      var fieldName = currentParam.toString();
      if (fieldName == 'filter') {
         currentParam.encodedQueryFor(tableName);
      } else {
         currentParam.valueFor(tableName, fieldName);
      }
   }
}
```

Wenn beispielsweise der Wert von **Filter** `short_description=My sensitive information^number=INC000056^category=Outage` ist, würde die Abfrage in der Instanz zu `short_description=<Encrypted(My sensitive information)>^number=INC000056^category=Outage` werden.

ParameterValue - toString()

Konvertiert den POST- oder URL-Parameterwert in eine Zeichenfolge.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Parameterwert als Zeichenfolge.

ParameterValue - getAsJsonContent()

Gibt die Anforderung als iterierbares Objekt vom Typ *`JsonNode`* zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar, wenn der Anforderungstext eine gültige JSON-Payload ist. Wenn Sie nicht sicher sind, in welchem Format der Anforderungstext enthalten ist, überprüfen Sie das Feld „contentType“ im Objekt *`Anforderung`*.

Sobald die Anforderung als *`JsonNode`*-Objekt zurückgegeben wird, können Sie mit Hilfe von JSON-APIs über das Objekt iterieren und Felder verschlüsseln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Die Anforderung als iterierbarer `JsonNode`.

ParameterValue - getAsXmlContent()

Gibt den Anforderungsinhalt als iterierbares Objekt vom Typ `XMLContent` zurück.

Diese Methode ist nur in einer Edge Encryption-Regel verfügbar Diese Methode setzt voraus, dass der Anforderungstext eine gültige XML-Payload ist. Sie können den contentType überprüfen, um sicherzustellen, dass dies der Fall ist.

Sobald die Anfrage als `XMLContent`-Objekt zurückgegeben wird, können Sie mit Hilfe von XML-APIs über die Objekt- und Verschlüsselungsfelder iterieren.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLContent	Die Anforderung als iterierbares Objekt vom Typ `XMLContent`.

ParameterValue - encodedQueryFor(String tableName)

Gibt an, dass der Wert des Elements eine codierte Abfrage für die angegebene Tabelle ist.

Das Aufrufen dieser Funktion für einen Parameter teilt dem Proxy mit, dass der Wert des Parameters ein ist Codierte Abfragezeichenfolgen Für die angegebene Tabelle. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

Ergebnisse

Typ	Beschreibung
void	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ParameterValue - valueFor(String tableName, String fieldName)

Gibt an, dass der Wert des Elements dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

Durch Aufrufen dieser Methode für einen Elementwert wird dem Proxy mitgeteilt, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

XML-APIs

XML-APIs können nach dem Aufrufen von `getAsXmlContent()` entweder über das Objekt `Anforderung` oder eine Eigenschaft `ParameterValue` verwendet werden.

Wenn Sie XML-APIs zum Schreiben Ihrer Verschlüsselungsregel verwenden, können Sie ein allgemeines Format verwenden:

1. Aufrufen von `getAsXmlContent()` über das Objekt `Anforderung` oder die Eigenschaft `ParameterValue`. Dies gibt ein iterierbares Objekt der zugrunde liegenden Klasse `XMLContent` zurück.
2. Aufrufen von `getIterator()` oder `getIterator(String xPath)` im Objekt `XMLContent`. Dies gibt ein Objekt `XMLElementIterator` zurück, das zum Iterieren von XML-Elementen verwendet werden kann.
3. Aufrufen der Methode `hasNext()` im Objekt `XMLElementIterator`, um zu bestimmen, ob ein anderes Element verfügbar ist.
4. Aufrufen von `next()` im Objekt `XMLElementIterator`, um das nächste XML-Element zurückzugeben. Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.
5. Aufruf von `valueFor(String tableName, String fieldName)` auf dem XML-Element. Diese Methode teilt dem Proxy mit, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

> **Hinweis:** Um festzustellen, ob Sie `valueFor(String tableName, String fieldName)` auf einem XML-Element aufrufen möchten, können Sie die Methode `getName()` verwenden, um den Namen des Elements zurückzugeben.

Zu einem bekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die XML-Payload auf der Instanz verarbeitet, um Datensätze in die Incident-Tabelle einzufügen. Das Beschreibungsfeld füllt den Incident mit short_description aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
<data>
   <record>
      <name>'Test Record 1'</name>
      <description>'Test Record 1 Description'</description>
      <tag>critical</tag>
   </record>
   <record>
      <name>'Test Record 2'</name>
      <description>'Test Record 2 Description'</description>
      <tag>security</tag>
   </record>
</data>
```

Die folgende Verschlüsselungsregelaktion kann angewendet werden:

```
function sampleXmlAction1() {
   var xmlContent = request.getAsXmlContent();
   // This loop iterates over all description tags that match the given path
   var xmlElementIterator = xmlContent.getIterator('data/record/description');
   while (xmlElementIterator.hasNext()) {
      var xmlElement = xmlElementIterator.next();
      xmlElement.valueFor('incident', 'short_decription');
   }
}
```

Diese Aktion iteriert das Tag **Beschreibung** und fordert den Proxy-Server auf, die Werte zu verschlüsseln und sie in der Instanz in instance.short_description einzufügen.

Hinweis: Diese Regel findet alle Tags **Beschreibung** in allen Tags **Datensatz** in der XML-Payload. Wenn es nur ein einziges Vorkommen eines zu verschlüsselnden Tags gibt, verwendet die Regel weiterhin die xPath- und Iteratorstruktur. Es iteriert jedoch nur einmal in der Schleife.

Zu einem unbekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel iteriert die Regel die Tags **Datensatz**, weiß jedoch nicht, welche Tags innerhalb des Tags **Datensatz** zu erwarten sind. Es ist nur bekannt, dass die Tags innerhalb der Tags **Datensatz** mit den Namen der in der Tabelle „URL-Parameter“ angegebenen Spalten übereinstimmen.

Die Regel legt außerdem fest, dass bei Vorliegen einer Incident-Tabelle, die Daten im Tag **Beschreibung** verschlüsselt und im Feld short_description der Instanz gespeichert werden sollen.

```
function sampleXmlAction2() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
      encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //Then, iterate over all tags representing fields in the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
   while (fieldIterator.hasNext()) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      var field = fieldIterator.next();
      var fieldName = childElement.getName();
      //if table is incident, then description is encrypted for the short_description field
      if (tableName == 'incident' && fieldName == 'description') {
         field.valueFor(tableName, 'short_description');
      } else {
         //if table is not incident, ask the proxy to check if the given field is encrypted for the
 given table
         field.valueFor(tableName, fieldName);
      }
   }
}
```

In der Funktion *`encryptFieldsInRecord()`* wird die Methode *`valueFor()`* für eine Tabelle und ein Feld aufgerufen, die aufgrund der Anforderung dynamisch zugewiesen werden. Obwohl sich die Tabellen- und Feldnamen ändern können, fordert die Regel den Proxy auf, zu prüfen, ob das Feld in der Tabelle aufgrund der definierten Verschlüsselungskonfigurationen verschlüsselt werden muss.

Wenn das Feld nicht für die Verschlüsselung konfiguriert ist oder das Tag nicht mit einem Feld in der Tabelle übereinstimmt, überspringt der Proxy dieses Tag. Wenn das Tag mit einem für die Verschlüsselung markierten Feld übereinstimmt, verschlüsselt der Edge Encryption Proxy-Server den Wert.

Eine verschlüsselte Abfrage verwenden

In diesem Beispiel haben alle Tags das Attribut **Filter**, das angibt, ob das Tag eine verschlüsselte Abfrage enthält.

```
<data>
   <record>
      <name filter="false">'Test Record 1'</name>
      <description filter="false">'Test Record 1 Description'</description>
      <query filter="true">category=1^name=edge</query>
   </record>
   <record>
      <name filter="false">'Test Record 2'</name>
      <description filter="false">'Test Record 2 Description'</description>
      <query filter="true">category=2^severity=3</query>
  </record>
</data>
```

Die folgende Verschlüsselungsregelaktion kann angewendet werden:

```
function sampleXmlAction3() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
      encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //this time we want to iterate over all tags representing fields in the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
   while (fieldIterator.hasNext()) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    var field = fieldIterator.next();
    var fieldname = childElement.getName();
    //let's look at the filter attribute, if true, then encrypt as encoded query
    if (field.getAttributeValue('filter') == 'true') {
       field.encodedQueryFor(tableName);
    } else {
       //if it is false then check if the field should be encrypted
       field.valueFor(tableName, fieldName);
    }
  }
}
```

Wenn das Attribut **Filter** „Wahr“ ist, fordert die Regel den Proxy-Server auf, die Werte in der verschlüsselten Abfrage zu verschlüsseln. Bei „falsch“ fordert die Regel den Proxy auf, zu überprüfen, ob das Feld verschlüsselt werden soll.

XMLContent

Ein globales Objekt, das Methoden zum Iterieren des XML-Inhalts bereitstellt.

Sie können auf ein Objekt `XMLContent` zugreifen, indem Sie getAsXmlContent() auf einem Objekt `Anforderung` aufrufen.

Sie greifen auf XML-Daten in einem POST- oder URL-Parameter zu, indem Sie request.postParams.<parameter name>.getAsXmlContent() oder request.urlParams.<parameter name>.getAsXmlContent() aufrufen.

XMLContent - getIterator()

Gibt ein Objekt `XMLElementIterator` für den XML-Inhalt zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, das zum Iterieren von Elementen im Objekt `XMLContent` verwendet werden kann.

XMLContent - getIterator(String xPath)

Gibt ein Objekt `XMLElementIterator` für den XML-Inhalt basierend auf dem angegebenen Parameter zurück.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-ähnlicher Ausdruck, der angibt, wo im Objekt `XMLContent` begonnen werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, das zum Iterieren von Elementen im Objekt `XMLContent` verwendet werden kann.

XMLElementIterator

Stellt Methoden zum Iterieren von XML-Elementen bereit.

Sie erhalten ein Objekt `XMLElementIterator`, indem Sie die Methode `getIterator()` in der Klasse `XMLContent` aufrufen.

XMLElementIterator - hasNext()

Bestimmt, ob ein anderes Element verfügbar ist.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Boolean	„Wahr“, wenn ein anderes Element verfügbar ist.

XMLElementIterator - next()

Gibt das nächste Element im Iterator zurück.

Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElement	Das nächste XML-Element

XMLElement

Stellt Methoden zum Iterieren von XML-Elementen und zum Zuordnen von Werten zu Feldern in einer Tabelle bereit.

Sie erhalten ein Objekt `XMLElement`, indem Sie die Methode `next()` eines Objekts `XMLElementIterator` aufrufen.

XMLElement - getIterator(String xPath)

Gibt ein Objekt `XMLElementIterator` für das XML-Element basierend auf dem angegebenen Parameter zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-ähnlicher Ausdruck, der angibt, wo im Objekt `XMLElement` begonnen werden soll.

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, mit dem über Elemente im Objekt `XMLElement` iteriert werden kann.

XMLElement - getIteratorOverAllChildren()

Gibt ein Objekt `XMLElementIterator` zurück, das alle Unterelemente des XML-Elements basierend auf dem angegebenen Parameter enthält.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
XMLElementIterator	Ein Objekt, mit dem über Elemente im Objekt `XMLElement` iteriert werden kann.

XMLElement - valueFor(String tableName, String fieldName)

Gibt an, dass der Wert des Elements dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

Durch Aufrufen dieser Methode für einen Elementwert wird dem Proxy mitgeteilt, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss. Wenn die Tabellen- und Feldnamen unbekannt sind, können Sie die Methode `valueFor()` auf einer Tabelle und einem Feld mit der Bezeichnung Dynamisch zugeordnet basierend auf der Anfrage aufrufen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

XMLElement - encodedQueryFor(String tableName)

Gibt an, dass der Wert des Elements eine codierte Abfrage für die angegebene Tabelle ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Aufrufen dieser Funktion für ein Element teilt dem Proxy mit, dass der Wert des Elements ein ist Codierte Abfragezeichenfolgen Für die angegebene Tabelle. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

Ergebnisse

Typ	Beschreibung
void	

XMLElement - getName()

Gibt den Elementnamen zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Elementname.

XMLElement - getAttributeValue(String attribute)

Gibt den Wert des angegebenen Attributs zurück.

Parameter

Name	Typ	Beschreibung
Attribut	Zeichenfolge	Der Attributname.

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Attributwert.

JSON-APIs

JSON-APIs können nach dem Aufrufen von `getAsJsonContent()` entweder über das Objekt `Anforderung` oder eine Eigenschaft `ParameterValue` verwendet werden.

Wenn Sie JSON-APIs zum Schreiben Ihrer Verschlüsselungsregel verwenden, können Sie ein allgemeines Format verwenden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aufrufen von `getAsJsonContent()` im Objekt `Anforderung`. Dies gibt ein iterierbares Objekt der zugrunde liegende Klasse `JsonNode` zurück.
2. Rufen Sie An `Iterator()` Oder `GetIterator (Zeichenfolge XPath)` Auf der `JsonNode` Objekt. Dies gibt ein Objekt `JsonNodeIterator` zurück, das zum Iterieren von Knoten im JSON-Objekt verwendet werden kann.
3. Aufrufen der Methode `hasNext()` im Objekt `JsonNodeIterator`, um zu bestimmen, ob ein anderes Element verfügbar ist.
4. Aufrufen von `next()` im Objekt `JsonNodeIterator`, um das nächste JSON-Element zurückzugeben. Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.
5. Aufrufen von `valueFor(String tableName, String Feldname)` auf dem JSON-Element. Diese Methode teilt dem Proxy mit, dass der Wert für dieses Element dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy prüft dann, ob das Feld verschlüsselt werden muss.

Hinweis: Um festzustellen, ob Sie `valueFor(String tableName, String fieldName)` auf einem JSON-Element aufrufen möchten, können Sie die Methode `getName()` verwenden, um den Namen des Elements zurückzugeben.

Zu einem bekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die JSON-Payload auf der Instanz verarbeitet, um Datensätze in die Incident-Tabelle einzufügen. Das Beschreibungsfeld füllt den Incident mit short_description aus.

```
{
   data: {
      records: [
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         },
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         }],
      "query": "assigned_to=3D4860165813e63a00d00abd322244b092^category=vulnerability"
   },
   "source": "10.11.13.14"
}
```

Die folgende Regel kann gelten:

```
function sampleJsonAction1() {
   var jsonContent = request.getAsJsonContent();
   // This loop iterates over all description elements in the records array
   var jsonNodeIterator = jsonContent.getIterator('/data/records/description');
   while (jsonNodeIterator.hasNext()) {
      var jsonNode = jsonNodeIterator.next();
      jsonNode.valueFor('incident', 'short_decription');
   }
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Aktion iteriert die Knoten **Beschreibung** und fordert den Proxy-Server auf, die Werte zu verschlüsseln und sie in instance.short_description auf der Instanz einzufügen.

Hinweis: Diese Regel findet alle Knoten **Beschreibung** innerhalb der JSON-Payload. Wenn nur ein Knoten zu verschlüsseln ist, verwendet die Regel weiterhin die xPath- und Iterator-Struktur. Es iteriert jedoch nur einmal in der Schleife.

Zu einem unbekannten Tabellenfeld in der Instanz zuordnen

In diesem Beispiel wird die Regel **Datensätze** iteriert. Es ist jedoch nicht bekannt, welche Knoten zu erwarten sind. Es ist nur bekannt, dass für jedes Objekt innerhalb von **Datensätze** die Knoten mit den Namen der im URL-Parameter der Tabelle angegebenen Spalten übereinstimmen.

Die Regel legt außerdem fest, dass bei Vorliegen einer Incident-Tabelle, die Daten im Knoten **Beschreibung** verschlüsselt und im Feld short_description der Instanz gespeichert werden sollen.

```
function sampleJsonAction2() {
   var jsonContent = request.getAsJsonContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var jsonNodeIterator = jsonContent.getIterator('data/records');
   while (jsonNodeIterator.hasNext()) {
         encryptFieldsInRecord(jsonNodeIterator.next());
   }
}
function encryptFieldsInRecord(jsonNode) {
   //this time we want to iterate over all nodes
   var fieldIterator = jsonNode.iterator();
   while (fieldIterator.hasNext()) {
         var field = fieldIterator.next();
         var fieldname = childElement.getName();
         if (fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
         } else {
            field.valueFor(tableName, fieldName);
         }
   }
}
```

In der Funktion *`encryptFieldsInRecord()`* wird die Methode *`valueFor()`* für eine Tabelle und ein Feld aufgerufen, die aufgrund der Anforderung dynamisch zugewiesen werden. Obwohl sich die Tabellen- und Feldnamen ändern können, fordert die Regel den Proxy auf, zu prüfen, ob das Feld in der Tabelle aufgrund der definierten Verschlüsselungskonfigurationen verschlüsselt werden muss.

Wenn das Feld nicht für die Verschlüsselung konfiguriert ist oder der Knotenname nicht mit einem Feld in der Tabelle übereinstimmt, überspringt der Proxy diesen Knoten. Wenn der Knotenname mit einem für die Verschlüsselung markierten Feld übereinstimmt, verschlüsselt der Proxy den Wert.

Eine verschlüsselte Abfrage verwenden

```
function sampleJsonAction3() {
   var jsonContent = request.getAsJsonContent();
   var tableName = request.urlParam.table;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        if (jsonNode.getName() == 'records')
            encryptRecors(jsonNodeIterator.next());
        else if (jsonNode.getName() == 'query')
            jsonNode.encodedQueryFor(tableName);
    }
}
function encryptRecords(jsonNode) {
    //we iterate over all fields in the node
    var recordIterator = jsonNode.iterator();
    while (recordIterator.hasNext()) {
        encryptFieldsInRecord(recordIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            field.valueFor(tableName, fieldName);
    }
}
```

In diesem Beispiel wird die Regel **Daten** iteriert. Mit Auffinden von **Datensätzen** wird die gleiche Logik wie im zweiten Beispiel ausgeführt, wobei die Felder in jedem Knoten iteriert werden. Nach Auffinden des Knotens **Abfrage** wird *`encodedQueryFor()`* aufgerufen, um Werte verschlüsseln, die in der Abfrage verschlüsselt werden sollen.

JsonNode

Ein globales Objekt, das Methoden zum Durchlaufen des JSON-Inhalts bereitstellt.

Sie können auf ein Objekt *`JsonNode`* zugreifen, indem Sie getAsJsonContent() in einem Objekt *`Anforderung`* aufrufen.

Sie haben Zugriff auf JSON-Inhalte von einem POST- oder URL-Parameter, indem Sie request.postParms.<parameter name>.getAsJsonContent() oder request.urlParms.<parameter name>.getAsJsonContent() aufrufen.

JsonNode - getIterator(String xPath)

Gibt ein Objekt *`JsonNodeIterator`* für den JSON-Inhalt zurück.

Diese Methode kann nur für den Stammknoten verwendet werden, kann jedoch auch verwendet werden, um tief in das JSON-Objekt zu gelangen. Nachfolgende Traversen müssen die Methode *`Iterator()`* verwenden.

Parameter

Name	Typ	Beschreibung
xPath	Zeichenfolge	Ein xPath-Ausdruck.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
JsonNodeIterator	Ein Objekt, das Knoten im JSON-Objekt iterieren kann.

JsonNode - iterator()

Gibt ein Objekt `JsonNodeIterator` zurück, das alle untergeordneten Knoten des aktuellen Knotens iteriert.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNodeIterator	Ein Objekt, das Knoten im JSON-Objekt iterieren kann.

JsonNode - getAsString()

Gibt den aktuellen Knotenwert als Zeichenfolge zurück.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der aktuelle Knotenwert.

JsonNode - getAsString(String propertyName)

Gibt den Zeichenfolgenwert der angegebenen Eigenschaft zurück.

Parameter

Name	Typ	Beschreibung
propertyName	Zeichenfolge	Der Name der Eigenschaft.

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Der Eigenschaftswert.

JsonNode - getName()

Gibt den Namen des aktuellen JSON-Knotens zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Zeichenfolge	Name des aktuellen JSON-Knotens.

JsonNode - valueFor(String tableName, String fieldName)

Gibt an, dass die JSON-Eigenschaft dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist.

Durch Aufrufen dieser Methode für eine JSON-Eigenschaft wird dem Proxy mitgeteilt, dass der Wert für diese Eigenschaft dem angegebenen Feld in der angegebenen Tabelle zugeordnet ist. Der Proxy entscheidet dann, ob das Feld verschlüsselt werden muss. Wenn die Tabellen- und Feldnamen unbekannt sind, können Sie die Methode `valueFor()` auf einer Tabelle und einem Feld mit der Bezeichnung Dynamisch zugeordnet basierend auf der Anfrage aufrufen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Der Tabellenname.
fieldName	Zeichenfolge	Der Feldname.

Ergebnisse

Typ	Beschreibung
void	

JsonNode - encodedQueryFor(String tableName)

Gibt an, dass der Wert der JSON-Eigenschaft eine codierte Abfrage für die angegebene Tabelle ist.

Durch das Aufrufen dieser Funktion auf einem JSON-Knoten wird dem Proxy mitgeteilt, dass der Wert ein ist Codierte Abfragezeichenfolgen Für die angegebene Tabelle. Der Proxy analysiert die verschlüsselte Abfrage und verschlüsselt die Werte für Felder in der verschlüsselten Abfrage, die verschlüsselt werden müssen.

Parameter

Name	Typ	Beschreibung
tableName	Zeichenfolge	Die Tabelle, auf der die Abfrage ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
void	

JsonNodeIterator

Sie erhalten ein Objekt `JsonNodeIterator`, indem Sie die Methoden `getIterator()` oder `iterator()` der Klasse `JsonNode` aufrufen.

JsonNodeIterator - hasNext()

Bestimmt, ob eine andere Eigenschaft verfügbar ist.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
Boolean	„Wahr“, wenn eine andere Eigenschaft verfügbar ist.

JsonNodeIterator - next()

Gibt die nächste Eigenschaft im Iterator zurück.

Sie können `next()` erst nach Aufrufen von `hasNext()` aufrufen.

Parameter

Name	Typ	Beschreibung
Keine		

Ergebnisse

Typ	Beschreibung
JsonNode	Der nächste `JsonNode`.

print(String message)

Gibt eine Nachricht an die Wrapper-Protokolldatei aus: <proxy server directory>/logs/wrapper_<date>.log.

Diese Methode ist nur in einem Edge Encryption-Regelaktionsskript verfügbar

Parameter

Name	Typ	Beschreibung
Nachricht	Zeichenfolge	Die Nachricht, die in die Wrapper-Protokolldatei geschrieben werden soll.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
void	

Nicht zulässige Schlüsselwörter

Der Edge Encryption Proxy überprüft Verschlüsselungsregelskripts, bevor die Regel gespeichert wird. Viele JavaScript-Stichwörter sind in Verschlüsselungsregelskripts nicht zulässig.

Nicht zulässige Schlüsselwörter

Stichwort
__DIR__
__FILE__
__LINE__
__parent__
__proto__
Fehler
Ausw
getClass
getPrototypeOf
Java
javax
javafx
JavaImporter
laden
loadWithNewGlobal
neu
Pakete
Objekt
Prototyp
RegExp
setPrototypeOf
diese
werfen

Attribute für das Edge-Encryption-Dictionary

Fügen Sie Tabellen und Feldern Wörterbuchattribute hinzu, um zu steuern, wie sie mit Edge Encryption funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um ein Wörterbuchattribut auf „wahr“ festzulegen, müssen Sie eingeben `Attribut=wahr` In **Attribute** Feld. Informationen zum Hinzufügen eines Dictionary-Attributs zu einem Datensatz finden Sie unter Tabellen und Felder werden mithilfe von Wörterbuchattributen geändert .

Edge Encryption ausgeschlossen [edge_encryption_excluded]

Bestimmt, ob das Feld von der Verschlüsselung ausgeschlossen ist.

Wenn auf festgelegt `Wahr`, Das Feld oder die Tabelle kann nicht verschlüsselt werden. Wenn auf festgelegt `Falsch`, Das Feld kann verschlüsselt werden.

- Wert: Wahr/falsch
- Zielelement: Feld oder Tabelle
- Standardwert: false

Edge Encryption aktiviert [edge_encryption_enabled]

Bestimmt, ob das Feld für die Verschlüsselung durch eine Verschlüsselungskonfiguration geeignet ist.

Wenn auf festgelegt `Wahr`, Das Feld ist für die Verschlüsselung geeignet. Wenn auf festgelegt `Falsch`, Das Feld ist nicht für die Verschlüsselung geeignet. Da dieses Attribut vom System verwendet wird und nicht geändert werden kann, wird es dem Anwender nicht angezeigt.

Hinweis: Dieses Attribut gibt weder an, dass ein Feld verschlüsselt ist, noch löst es eine Verschlüsselungslogik für das Feld aus. Das Attribut bestimmt vielmehr die Möglichkeit, dass das Feld von einem Benutzer verschlüsselt wird.

- Wert: Wahr/falsch
- Zielelement: Feld
- Standardwert: „Wahr“ für Zeichenfolgenfelder

Klartext für die Edge Encryption zulässig [edge_encryption_clear_text_allowed]

Bestimmt, ob serverseitige Skripts unverschlüsselte Daten an eine verschlüsselte Zeichenfolge im Feld für Anwenderaktionen, die über den Proxy-Server ausgeführt werden, oder an serverseitige automatisierte Skripts, z. B. geplante Aufgaben, anhängen können.

Wenn auf festgelegt `Wahr`, Anhängende Daten sind zulässig. Wenn auf festgelegt `Falsch`, Anhängen von Daten ist nicht zulässig.

- Wert: Wahr/falsch
- Zielelement: Feld
- Standardwert: falsch

Domain Separation und Edge Encryption

Domänentrennung wird unter bestimmten Umständen mit unterstützt Edge Encryption. Edge Encryption Bietet die Möglichkeit, Daten aus der Umgebung des Kunden mithilfe bestimmter Konfigurationen, Regeln und Schlüssel zu verschlüsseln, die auf definiert sind Edge Encryption Proxy. Die Edge Encryption Proxy ist nicht domänenbewusst und kann domänenspezifische Einstellungen nicht unterstützen. Mit der Domain Separation können Sie Daten, Prozesse und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung.

Funktionsweise der Domänentrennung in der Edge Encryption

Die Edge Encryption kann verwendet werden, wenn keine domänenspezifischen Schlüssel, Konfigurationen und Regeln erforderlich sind.

Zugehörige Informationen

Domänentrennung für Service Provider

Datenintegration mit Edge Encryption

Um Daten von Drittanbietern mit einer Instanz über Edge Encryption zu integrieren, müssen Sie die Daten über den Edge Encryption Proxy-Server mit unterstützten Integrationen weiterleiten. Unterstützte Integrationen verwenden Verschlüsselungsregeln des Basissystems, die Daten in jeder Payload auf Felder in einer Tabelle abbilden.

Daten in für die Verschlüsselung markierte Felder hochladen

Edge Encryption unterstützt nicht den Import von Daten aus oder den Export von Daten nach Excel, CSV, XML oder anderen Dateitypen in oder aus Feldern mit definierten Verschlüsselungskonfigurationen.

ODBC-Treiber

Verschlüsseln Sie Anforderungen und Datenabfragen über den Edge Encryption Proxy-Server mit dem ODBC-Treiber.

Weitere Informationen: Edge Encryption ODBC-Treiberintegration

MID-Server

Sie können MID-Server so konfigurieren, dass Daten über einen Edge Encryption Proxy-Server geleitet werden. Es gelten jedoch einige Einschränkungen.

Weitere Informationen: Edge Encryption MID-Server-Integration

REST/SOAP Web Services

Verwenden Sie REST/SOAP Web Services zum Aktualisieren oder Abrufen von Datensatzdaten über den Edge Encryption Proxy-Server.

Weitere Informationen: Webservices

JSONv2-Webservice

Verwenden Sie JSONv2-Webservice-APIs zum Aktualisieren oder Abrufen von Datensatzdaten über den Edge Encryption Proxy-Server. Verschlüsselungsregeln des Basissystems unterstützen APIs zum Abrufen und Ändern von Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um einen einzelnen Datensatz über die Datenänderungs-API einzufügen, verwenden Sie die Methoden `insert()` oder `insertMutiple()`.
- Um mehrere Datensätze über die Datenänderungs-API einzufügen, verwenden Sie die Methode `insertMultiple()`.

Weitere Informationen: JSONv2-Webservice

Um Daten von benutzerdefinierten Drittanbieter-Integrationen zu verschlüsseln, die oben nicht aufgeführt sind, erstellen Sie benutzerdefinierte Verschlüsselungsregeln. Weitere Informationen finden Sie unter Eine benutzerdefinierte Verschlüsselungsregel definieren.

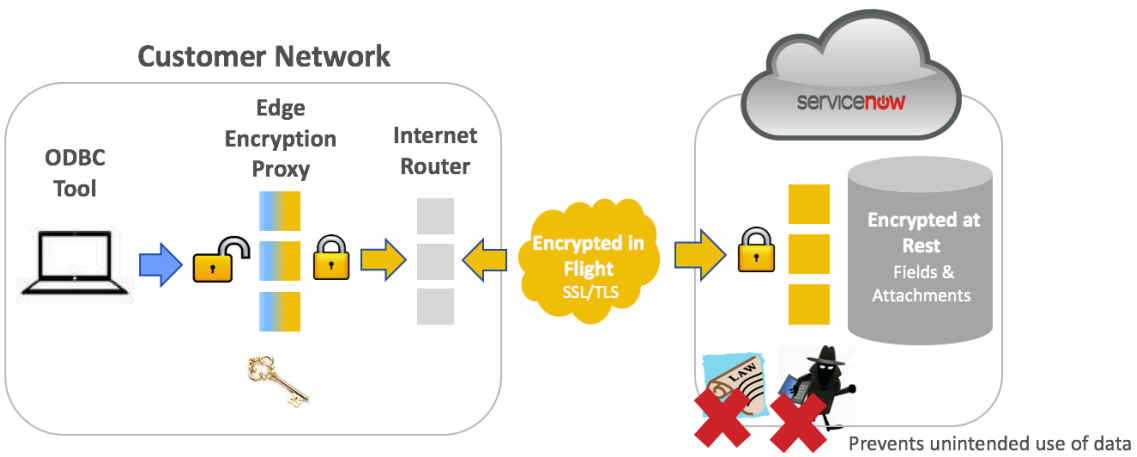
Anhänge zu zur Verschlüsselung markierten Datensätzen hochladen

Anhänge können in Tabellen hochgeladen werden, wobei die Anhangsverschlüsselung mithilfe von REST- und SOAP Web Services konfiguriert wird.

Edge Encryption ODBC-Treiberintegration

Konfigurieren Sie Ihren ODBC-Treiber für die Abfrage von Daten, die mit Edge Encryption verschlüsselt sind. Der Edge Encryption Proxy-Server verschlüsselt ODBC-Treiberanfragen an die ServiceNow-Instanz, wenn Edge Encryption mit dem ODBC-Treiber integriert ist.

Verschlüsselte Antworten von der Instanz werden über den Edge Encryption Proxy-Server entschlüsselt, bevor sie an den ODBC-Treiber in Ihrem Netzwerk weitergeleitet werden.



Für eine erfolgreiche Integration muss der ODBC-Treiber dem Zertifikat des Edge Encryption Proxy-Servers vertrauen. Wenn das Zertifikat des Edge Encryption Proxy-Servers von einer Zertifizierungsstelle signiert wird, die vom ODBC-Treiber vertraut wird, wird dem Proxy-Server Edge Encryption automatisch vertraut. Wenn jedoch eine Zertifizierungsstelle, der der ODBC-Treiber vertraut, das Edge Encryption Proxy-Server-Zertifikat nicht signiert hat, müssen Sie das selbst signierte Zertifikat in den ODBC-Truststore importieren.

Ein selbstsigniertes Zertifikat in den ODBC-Truststore importieren

Wenn eine Zertifizierungsstelle, der der ODBC-Treiber vertraut, das Edge Encryption Proxy-Server-Zertifikat nicht signiert hat, müssen Sie ein selbst signiertes Zertifikat in den ODBC-Truststore importieren. Sie können das Zertifikat vom Edge Encryption Proxy-Server exportieren und in den ODBC-Truststore importieren.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um festzustellen, ob eine vom ODBC-Treiber vertrauenswürdige Zertifizierungsstelle das Zertifikat des Edge Encryption Proxy-Servers signiert hat, führen Sie den folgenden Befehl im Schlüsselspeicherverzeichnis im Stammverzeichnis des Proxys aus, um eine Liste der vom ODBC-Treiber vertrauenswürdigen Zertifizierungsstellen anzuzeigen:

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts" -list
```

Hinweis:

In den meisten Fällen stellt der Client eine Verbindung mit her Edge Encryption Proxys über ein Lastenausgleichsmodul, sodass das Zertifikat das im Lastenausgleichsmodul konfigurierte Zertifikat ist.

Wenn kein Lastenausgleichsmodul zwischen dem Client und dem Edge-Proxy-Server vorhanden ist, ist das Zertifikat das vom Edge-Proxy präsentierte Zertifikat und wird in konfiguriert *edgeencryption.properties*Datei.

```
edgeencryption.proxy.https.port = 9090
edgeencryption.proxy.https.keystore.path = keystore/keystore
edgeencryption.proxy.https.keystore.password = password
edgeencryption.proxy.https.cert.alias = jetty
```

Weitere Informationen zum Bearbeiten von Eigenschaften finden Sie unter Konfigurieren Sie zusätzliche Eigenschaften in der Eigenschaftendatei „Edge Encryption“

Prozedur

1. Wechseln Sie in das Schlüsselspeicherverzeichnis im Proxy-Stammverzeichnis.
2. Überprüfen Sie den Schlüsselspeicher auf das selbstsignierte Zertifikat.
   a. Um den Schlüsselspeicher für das Zertifikat zu überprüfen, können Sie den folgenden Befehl ausführen, um alle Elemente im Schlüsselspeicher aufzulisten.

      ```
      keytool -list -keystore keystore.jceks -storetype jceks -v
      ```

   b. Suchen Sie den Schlüsselalias in der Liste der Elemente.
3. Exportieren Sie das Zertifikat mithilfe des Schlüsselalias in eine CER-Datei.

   ```
   keytool -export -alias <key alias> -keystore keystore.jceks -storetype jceks -rfc -file <file name>.cer
   ```
4. Wechseln Sie in Ihr ODBC-Truststore-Verzeichnis: ODBC\ip\Java\jre\lib\security\cacerts.
5. Importieren Sie das Zertifikat in Ihren ODBC-Truststore.

   ```
   keytool -keystore cacerts -importcert -alias $<key alias> -file <file name>.cer
   ```

Die ODBC-Treibereigenschaften festlegen

Legen Sie die ODBC-Treibereigenschaften so fest, dass Anforderungen über den Edge Encryption Proxy-Server geleitet werden.

Vorbereitungen

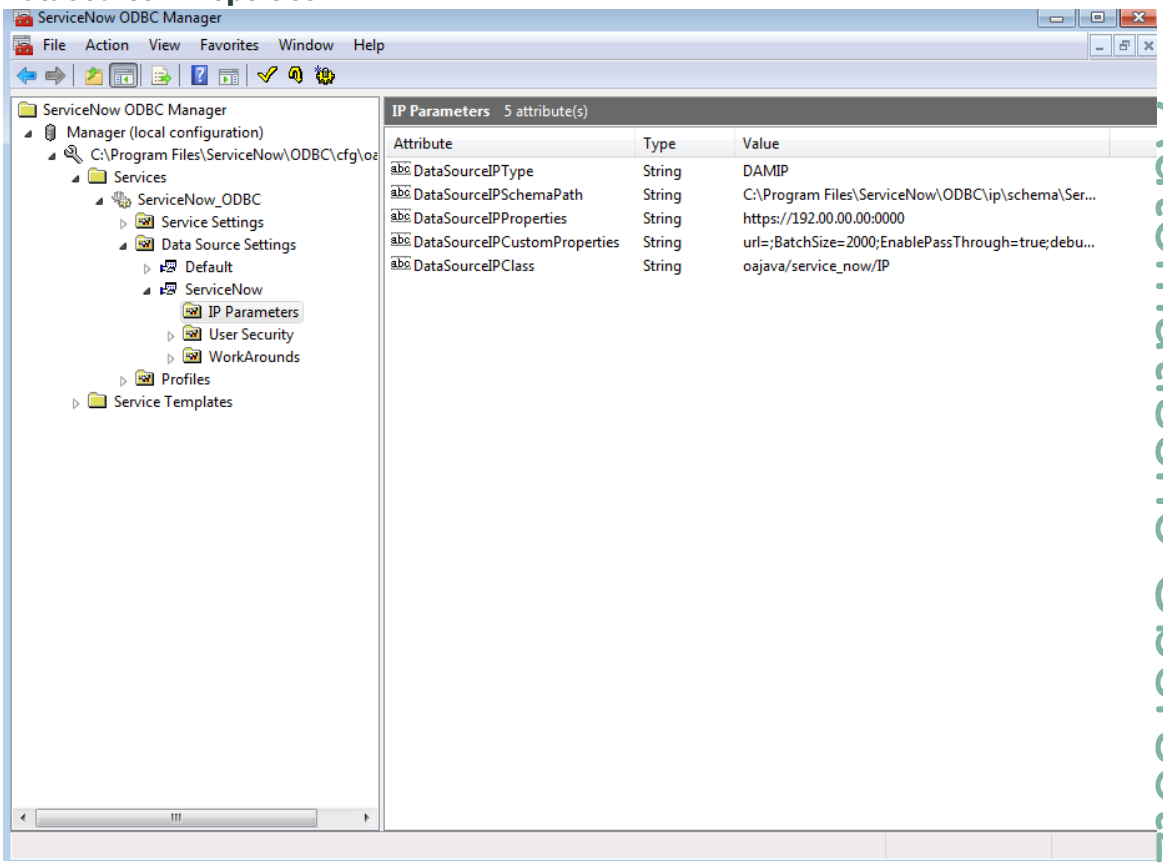
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie in Windows zu **Start** > **Programme** > **ServiceNow ODBC-Verwaltungskonsole**an.
2. Erweitern Sie das Stammverzeichnis der Konsolenstruktur um: ServiceNow ODBC Manager\Manager \<installation location>\Services\ServiceNow_ODBC\Data Source Settings\ServiceNow\IP Parameters.
3. Doppelklicken Sie auf das Attribut **DataSourceIPProperties**.
4. Ändern Sie den **Wert** auf die URL Ihres Edge Encryption Proxy-Servers, wie z. B. https://<IP address>:<port>

DataSourceIPProperties



5. Klicken Sie auf **OK**.

Nächste Maßnahme

Der ODBC-Treiber ist jetzt so konfiguriert, dass Anforderungen an die Instanz über den Edge Encryption Proxy-Server weitergeleitet werden.

Edge Encryption MID-Server-Integration

Konfigurieren Sie MID-Server so, dass Daten über den Edge Encryption Proxy-Server geleitet werden.

Bei der Integration mit MID-Server fungiert der Edge Encryption Proxy-Server als Endpunkt des MID-Server. Der Edge Encryption Proxy-Server verschlüsselt und entschlüsselt dann die zwischen der ServiceNow-Instanz und dem MID-Server übertragenen Daten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einschränkungen bei der Integration mit dem MID-Server

Wenn die Daten von MID-Server so konfiguriert sind, dass sie den Edge Encryption Proxy-Server durchlaufen, gelten die folgenden Einschränkungen:

- Die Verschlüsselung der ECC-Warteschlangenfelder wird nicht unterstützt.
- Verschlüsselte Daten können nicht mit Discovery oder Service-Mapping verwendet werden.

Den MID-Server auf den Edge Encryption Proxy-Server verweisen

Bis Übergeben Sie Daten von MID-ServerÜber Edge Encryption Proxy-Server, aktualisieren Sie MID-Server Konfigurationsdatei, auf die verwiesen werden soll MID-Server Zu Edge Encryption Proxy-Server.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn MID-Server so konfiguriert ist, das der Edge Encryption Proxy-Server durchlaufen wird, können Sie die Web-Proxy-Eigenschaften in der MID-Server-Konfigurationsdatei nicht verwenden, um den Datenverkehr über den Edge Encryption Proxy-Server zu Ihrer Instanz zu leiten. Stattdessen müssen Sie den Edge Encryption Proxy-Server als den Endpunkt von MID-Server einstellen.

Prozedur

1. Navigieren Sie zum lokalen MID-Server-Verzeichnis und öffnen Sie die Datei config.xml.
2. Suchen Sie das Element `<parameter name="url" value="https://YOUR_INSTANCE.service-now.com" />` und ändern Sie die Eigenschaft „Wert“ auf die URL Ihres Edge Encryption Proxy-Servers.
   Beispiel: `http://hostname.mycompany.com:8081`
   Mit diesem Schritt wird MID-Server angewiesen, den Datenverkehr an den Edge Encryption Proxy-Server und nicht an die Instanz zu leiten. Der Edge Encryption Proxy-Server wiederum verschlüsselt alle erforderlichen Felder und leitet die Nutzdaten an die Instanz weiter.
3. Speichern und schließen Sie die Datei.
4. Starten Sie MID-Server neu, wenn schon in Ausführung.

Diagnose und Leistung von Edge Encryption

Überwachen sie Performance-Trends des Edge Encryption Proxy-Servers und untersuchen Sie die vom Edge Encryption Proxy-Server generierten Fehler.

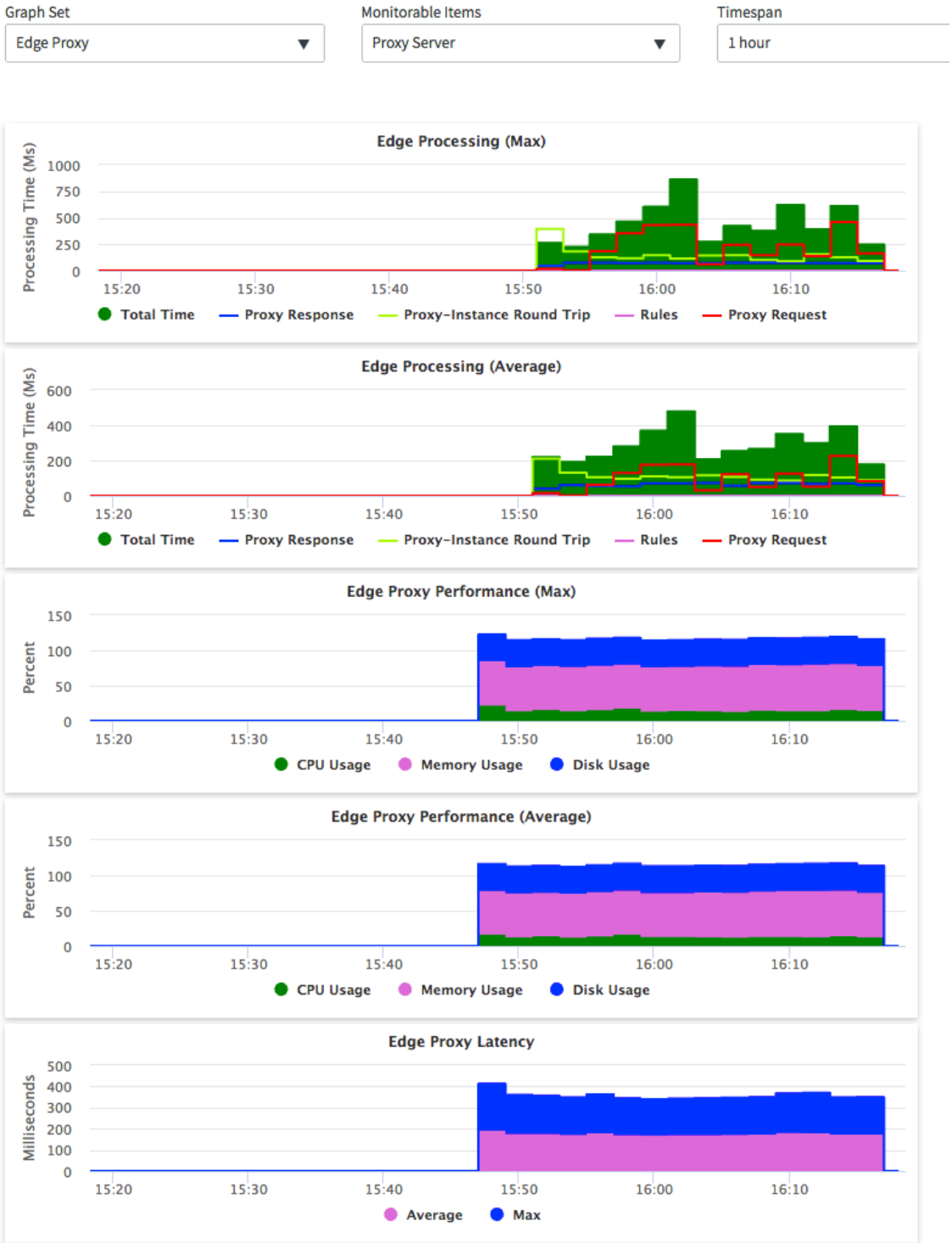
Edge-Proxy-Performance

Sehen Sie sich die wichtigsten Performance-Trends des Edge Encryption Proxy-Servers mithilfe des Edge-Proxy-Diagramms auf der ServiceNow Performance-Homepage an. Überwachte Trends umfassen:

- Maximale und durchschnittliche Antwortzeit zwischen Client, Proxy-Server und Instanz.
- CPU, Speicherplatz und Speicherplatz des Host-Computers.
- Maximale und durchschnittliche Netzwerklatenz zwischen dem Proxy-Server und der ServiceNow-Instanz.

Hinweis: Edge Encryption Proxy-Server mit doppelten Namen melden keine Performance-Trends.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Edge-Verarbeitung (Maximum und Durchschnitt)

Maximale und durchschnittliche Zeit in Millisekunden für die Verarbeitung einer Anforderung. Diese Datenpunkte sind allgemeine Trends im Zeitablauf.

- **Gesamtzeit**: Zeit, in der der Proxy-Server eine Anforderung von einem Client erhält und eine Antwort sendet. Dieser Datenpunkt ist die Summe der nachfolgenden Datenpunkte.
- **Proxy-Antwort**: Zeit, in der der Proxy-Server eine Antwort der Instanz verarbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

- **Proxy-Instanz-Rundlauf**: Zeit, in der der Proxy-Server eine Anforderung an die Instanz sendet und eine Antwort erhält. Enthält die Netzwerklatenz zwischen dem Proxy-Server und der Instanz sowie die Zeit, die die Instanz für die Verarbeitung der Anforderung benötigt.
- **Regeln**: Zeit, die der Proxy-Server benötigt, um eine Anforderung anhand definierter Verschlüsselungsregeln auszuwerten.
- **Proxy-Anforderung**: Zeit, in der der Proxy-Server eine Client-Anforderung verarbeitet und an die Instanz weiterleitet.

Edge Proxy-Performance (Maximum und Durchschnitt)

Maximaler und durchschnittlicher Prozentsatz der auf dem Host-Computer verwendeten Ressourcen.

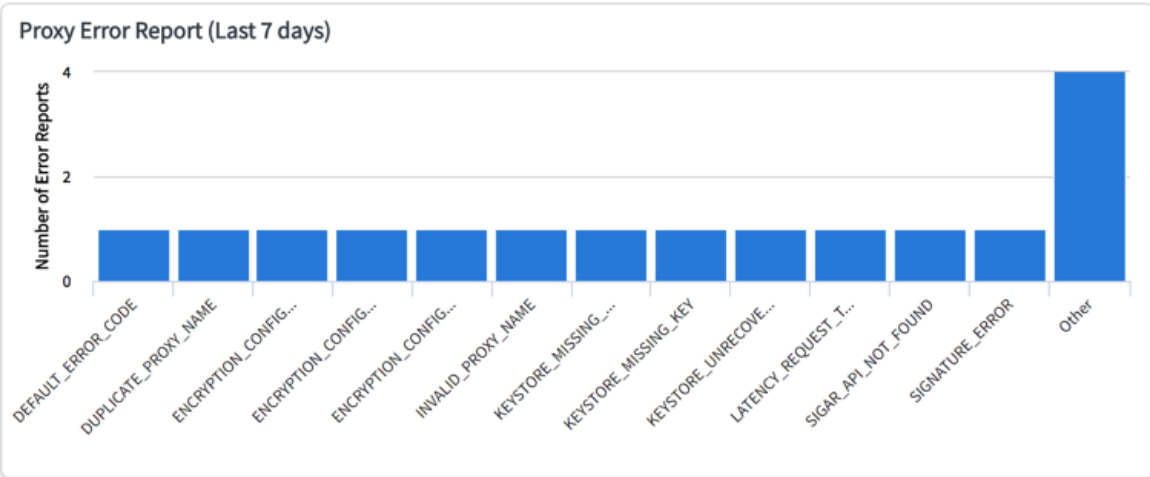
- CPU-Auslastung
- Speicherauslastung
- Festplattenauslastung

Edge-Proxy-Latenzzeit

Maximale und durchschnittliche Netzwerklatenz in Millisekunden zu einem bestimmten Zeitpunkt. Die Latenz wird durch die Rundlaufzeit bestimmt, die ein Proxy-Server benötigt, um einen einfachen Ping an die Instanz zu senden und eine Antwort zu empfangen.

Proxy-Fehlerberichte

Navigieren zu **Konfiguration der Edge Encryption** > **Diagnose und Fehlerbehebung** > **Proxy-Fehlerberichte** Zum Anzeigen aller in den letzten sieben Tagen erfassten Proxy-Serverfehler.



Fehler werden über einen Zeitraum von einer Minute erfasst. Jede Minute wird ein Fehlerbericht generiert. Die vertikale Achse zeigt die Anzahl der Fehlerberichte der letzten sieben Tage an, die jeden Fehler enthalten. Selbst wenn beispielsweise der Fehler DEFAULT_ERROR_CODE über einen Zeitraum von einer Minute mehrmals ausgelöst wird, erreicht die Leiste DEFAULT_ERROR_CODE nur einen Fehler auf der Achse **Anzahl der Fehlerberichte**.

In dieser Ansicht können Sie:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Auf die einzelnen Proxy-Fehlercodeleisten klicken, um den Bericht über einen einzelnen Fehler für jeden Proxy-Server anzuzeigen. In dieser Ansicht können Sie erneut auf die Leiste klicken, um den Fehlertext in der Edge Encryption Proxy-Statistiktabelle [edge_encryption_stat] anzuzeigen. Folgen Sie den Links im Fehlertext, um weitere Informationen und mögliche Schritte zur Fehlerbehebung anzuzeigen.
- Klicken Sie auf **Andere**, um die zweite Seite des Fehlerberichts zu sehen.

Hinweis: Wenn Sie mehr als einen Proxy-Server mit demselben Namen haben, wird im Proxy-Fehlerbericht ein einzelner Fehler DUPLICATE_PROXY_NAME angezeigt. Für Proxy-Server mit doppelten Namen werden keine anderen Fehler gemeldet. Wenn dieser Fehler auftritt, stellen Sie sicher, dass alle Proxy-Server eindeutige Namen haben.

Zusätzlich Überwachungsressourcen

Die Instanz verfolgt alle Verschlüsselungsproxys. Jeder Edge Encryption Proxy-Server registriert sich beim Start. Die Instanz wird benachrichtigt, wenn:

- Ein neuer Edge Encryption Proxy-Server gestartet wird.
- Ein Edge Encryption Proxy-Server absichtlich heruntergefahren wird.

Wenn ein Edge Encryption Proxy-Server versucht, sich bei einer Instanz zu registrieren, die Edge Encryption nicht installiert hat, wird der Proxy nicht gestartet.

Alle Verschlüsselungskonfigurationsdateien werden geprüft. Gelöschte Datensätze werden für alle Verschlüsselungskonfigurationsdateien geprüft. Audit-Datensätze werden in der Tabelle sys_audit abgelegt. Um den Verlauf eines bestimmten Konfigurationsdatensatzes anzuzeigen, zeigen Sie den Datensatz an, und klicken Sie auf **Verlauf** > **Liste** Im Menü. Der Massenverschlüsselungsauftrag wird keinem Audit unterzogen.

Verwenden Sie die folgenden zusätzlichen Ressourcen, um Ihre Proxy-Server zu überwachen.

Tabelle	Beschreibung
Ungültige Einfügeversuche [sys_edge_encryption_invalid_insert_log]	Liste der Versuche, die folgenden Daten in verschlüsselten Feldern zu speichern: • Nicht verschlüsselte Daten. • Daten, die nicht von einem Edge Encryption Proxy stammen. Die Instanz lehnt alle Versuche ab, diese Daten zu speichern, und protokolliert sie anschließend. Wenn Sie die Rolle Security-Admin haben, können Sie die Protokolle in der Liste „Ungültige Einfügeversuche“ anzeigen.
Auftragsfehler [sys_encryption_job_execution]	Eine Liste der Aufträge, die nicht erfolgreich ausgeführt wurden.
Systemprotokolle	Die Instanz sucht regelmäßig nach Nachrichten von jedem registrierten Proxy-Server. Wenn ein Proxy-Server im erforderlichen Zeitraum keine Nachricht gesendet hat, wird ein Fehler protokolliert. Die Protokollnachricht enthält Informationen zum Verschlüsselungs-Proxy und den letzten Zeitpunkt, zu dem der Proxy die Instanz gepingt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	Wenn die Instanz feststellt, dass keiner der Verschlüsselungsproxys online ist, protokolliert sie eine Nachricht. Diese Meldungen werden zum Systemprotokoll hinzugefügt.

Die Edge Proxy-Statistikerfassung deaktivieren oder reduzieren

Verhindern Sie, dass der Edge Encryption Proxy-Server Edge Proxy Diagrammsatz-Statistiken an die ServiceNow Performance-Homepage sendet, oder reduzieren Sie die Häufigkeit der statistischen Erfassung.

Vorbereitungen

Erforderliche Rolle: admin oder security_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch das Hinzufügen von Eigenschaften in der Konfigurationsdatei edgeencryption.properties können Sie:

- Den Edge Proxy-Diagrammsatz deaktivieren.
- Das Intervall ändern, in dem die Statistiken vom Edge Encryption Proxy-Server erfasst werden. Standardmäßig werden Statistiken alle 30 Sekunden erfasst.

Prozedur

1. Öffnen Sie in Ihrem Installationsverzeichnis des Proxy-Servers die Konfigurationsdatei edgeencryption.properties im Ordner <installation directory>/conf/.
2. Fügen Sie einen der hinzu Eigenschaften des Edge Encryption Proxy-Servers.
3. Starten Sie den Proxy-Server neu.

Erhöhen Sie die Debug-Protokollierung für Edge Encryption Proxy

Erhöhen Sie die Protokollierungsstufe, um die Protokolle zu interpretieren und Probleme mit dem Proxy zu debuggen.

Es gibt derzeit drei Optionen zum Erhöhen der Debug-Protokollierung in Edge Encryption Proxy. Erhöhen Sie die Protokollierungsstufe, um Probleme zu debuggen. Stellen Sie technischen Support mit Informationen bereit, um das Problem mit ausführlicheren Protokollanweisungen zu untersuchen.

Richten Sie die Debug-Protokollierung je nach Problem auf eine von drei Arten ein:

- Debugging-Probleme mit Ausnahme der SSL-Konnektivität
- Protokollierung von Zeitmetriken für Anforderungen über den Proxy
- Debugging von Problemen mit der SSL-Konnektivität zwischen dem Edge Encryption-Proxy und der Instanz

Für alle Debug-Fälle können Sie die Protokolle in Ihren eigenen Protokollen anzeigen und interpretieren oder einen Incident öffnen, um eine Interpretation von zu erhalten ServiceNow Technischer Support, der die Beschreibung des Problems und seine Reproduktion bereitstellt.

Debugging-Probleme mit Edge Encryption Andere Anwendung als SSL-Konnektivität

Verwenden Sie diese Methode, um Probleme mit zu debuggen Edge Encryption Anwendung, ohne den Proxy anzuhalten und neu zu starten. Diese Schritte erhöhen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Protokollierungsstufe und helfen bei der Behebung der Ursache mit ausführlicheren Protokollanweisungen.

Vorbereitungen
Erforderliche Rolle: Administrator

Hinweis: Änderungen an vorgenommen $Proxy_Installation_location/conf/log4j2.properties Dateien werden vom Proxy innerhalb von etwa 60 Sekunden nach dem Vornehmen der Änderungen verwendet. Sie müssen die Proxys nicht neu starten.

Prozedur

1. In $Proxy_Installation_location/conf/log4j2.properties Datei Suchen Sie die folgende Zeile.

```
logger.edge.level=info
```

2. Ändern Sie die obige Zeile wie folgt:

```
logger.edge.level=debug
```

3. Speichern Sie die Änderung.
   Es kann bis zu 60 Sekunden dauern, bis der Change wirksam wird, dies erfordert jedoch keinen Proxy-Neustart.
4. Reproduzieren Sie Ihr Problem.
5. Überprüfen Sie auf Debug-Protokollanweisungen im Zusammenhang mit der Anwendung in $Proxy_Installation_location/logs/edgeencryption.log Datei.

Ergebnis
Nach der Änderung der Eigenschaft können Sie zusätzliche Details in anzeigen $Proxy_Installation_location/logs/edgeencryption.log Datei. Wenn Sie das Debugging abgeschlossen haben, setzen Sie die an vorgenommene Änderung zurück $Proxy_Installation_location/conf/log4j2.properties Datei.

Protokollierung von Zeitmetriken für Anforderungen über den Proxy

Aktivieren Sie die Protokollierung der Zeitmetrik, um eine Metrikanweisung für jede Anforderung hinzuzufügen, die von bearbeitet wird Edge Encryption Proxy. Jede dieser Protokollanweisungen für Zeitmetriken enthält nützliche Informationen zur Anforderung, z. B. Verarbeitungszeiten und welche Verschlüsselungsregel verwendet wurde.

Vorbereitungen
Erforderliche Rolle: Administrator

Hinweis:

Die zusätzlichen Protokollierungseinstellungen werden dem hinzugefügt $Proxy_Installation_location/conf/log4j2.properties Datei. Vorgenommene Änderungen werden vom Proxy innerhalb von etwa einer Minute nach den Änderungen an der Datei dynamisch übernommen, sodass Sie die Proxys nicht neu starten müssen.

Prozedur

1. Ändern Sie $Proxy_Installation_location/conf/log4j2.properties Datei durch Hinzufügen der folgenden Zeilen am Ende der Datei

```
appender.timinglog.type=RollingFile
appender.timinglog.name=TimingLog
appender.timinglog.fileName=../logs/edgenetwork.log
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
appender.timinglog.filePattern=../logs/$${date:yyyy-MM}/edgenetwork-%d{yyyy-MM-dd-HH}-%i.log.gz
appender.timinglog.layout.type=PatternLayout
appender.timinglog.layout.pattern=%d [%t] %-5p %m%n
appender.timinglog.policies.type=Policies
appender.timinglog.policies.size.type=SizeBasedTriggeringPolicy
appender.timinglog.policies.size.size=500MB
appender.timinglog.strategy.type=DefaultRolloverStrategy
appender.timinglog.strategy.max=4

logger.timing.name=com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache
logger.timing.level=debug
logger.timing.additivity=false
logger.timing.appenderRef.rolling.ref=TimingLog
```

2. Speichern Sie die Datei.

Ergebnis

Nach log4j.properties Die Datei wird gespeichert, die folgenden Nachrichtentypen werden in angezeigt $Proxy_Installation_location/logs/edgenetwork.log Protokolldatei für Netzwerkzeiten.

```
2022-07-21 12:56:15,783 [qtp1971991758-7700] DEBUG
 com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache -
 request_uri=/api/now/ui/presencesysparm_auto_request=true&cd=1658433375754
 request_method=POST client_request_received="2022-07-21 12:56:15,015"
 proxy_request_processing_time=6 all_rules_processing_time=0
 rule_executed="REST JSON" rule_execution_time=1 proxy_instance_round_trip=14
 proxy_response_processing_time=1 total_time_from_proxy=21 reponse_code=201
 glide_user=SCv3_1:BAz1ZK7ee9XoroG2nvMlixHpgTvsT4fY2bwQvnH2WdU=:y5HGsTTqo3Pjq6
G0xk4LoazCwCiWRJk4/6SpbXuBzqg=:6816f79cc0a8016401c5a33be04be441
 jsessionid_suffix=037A66
```

Die Werte in den Protokollnachrichten lauten wie folgt:

```
request_uri: The URI being requested

request_method: The HTTP method being used, for example, GET, POST, PUT, PATCH,
 DELETE

client_request_received: The timestamp noting when the HTTP client request arrived at the
 Edge proxy

proxy_request_processing_time: How long the Edge proxy took to process the request in
 milliseconds

all_rules_processing_time: Total time it took to execute all of the Edge Encryption rules for the
 request in milliseconds

rule_executed: The name of the encryption rule that was executed

rule_execution_time: How long it took to execute listed rule_executed in milliseconds

proxy_instance_round_trip: The time from when the Edge proxy sent the request to the instance
 until the instance sent the response and was received by the edge proxy in milliseconds
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

proxy_response_processing_time: How long the Edge proxy took to process the response in milliseconds

total_time_from_proxy: The total time from when the Edge proxy received the request from the client and returned the response to the client in milliseconds

response_code: HTTP response code

glide_user: The glide_user cookie value

jsessionid_suffix: The JSession cookie suffix associated with the request

Debuggen von Problemen mit SSL-Konnektivität zwischen Edge Encryption Proxy und die Instanz

Verwenden Sie diese Methode, um Probleme mit der SSL-Konnektivität zwischen zu debuggen Edge Encryption Proxy und Ihre Instanz, z. B. der Zugriff auf die Instanz schlägt über den Proxy fehl. Diese Schritte erhöhen die Protokollierung und helfen bei der Suche nach ausführlichen Protokollanweisungen.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: Das Debugging der SSL-Konnektivität ist nur bei der Behebung von Problemen mit dem TLS-Konnektivitätstyp relevant. In der Praxis ist dies nicht üblich und wird selten benötigt.

Prozedur

1. Den Proxy-Server stoppen.
2. Fügen Sie der Datei die folgende Zeile hinzu $Proxy_Installation_location/conf/Wrapper.conf , Was eine Java-Starteigenschaft ist:

   ```
   wrapper.java.additional.<next available number in sequence> = -Djavax.net.debug=all
   ```

   Zum Beispiel:

   ```
   For example: wrapper.java.additional.4 = -Djavax.net.debug=all
   ```

3. Speichern Sie die Änderung, und starten Sie den Proxy-Server neu.
4. Reproduzieren Sie Ihr Konnektivitätsproblem.

Ergebnis

Nach der Reproduktion des Problems können Debug-Protokollanweisungen im Zusammenhang mit dem SSL-Austausch in gefunden werden $Proxy_Installation_location/logs/Wrapper_<current date>.log Datei. Wenn Sie das Debugging abgeschlossen haben. Sie können die zusätzliche Protokollierung Remote durchführen, indem Sie die in den vorherigen Schritten erstellte Zeile entfernen oder kommentieren.

Datenbankverschlüsselung

ServiceNow® Bietet Datenbankverschlüsselungsmethoden (Database Encryption, DBE) und Volldatenträger-Verschlüsselungsmethoden für Kunden mit gesetzlichen Verpflichtungen zum Datenschutz, die möglicherweise Schutz im Ruhezustand für alle Daten erfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Beginnend mit Washington DC Release, Datenbankverschlüsselung wird für zukünftige Veraltet vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter Cloud-Verschlüsselung Mit Schlüsselverwaltung

Untersuchen	Anforderung	Referenz
		
Erfahren Sie mehr über die wichtigsten Funktionen und den Geschäftsnutzen der Datenbankverschlüsselung.	Erfahren Sie mehr darüber, wie Sie die Rotation des Datenbankschlüssels anfordern.	Datenbankverschlüsselung mit kundengesteuertem Switch (DBE-CCS) ist eine Verschlüsselungslösung, die alle Daten im Ruhezustand verschlüsselt, wenn sie nicht in der Datenbank verwendet werden.

Datenbankverschlüsselung Erkunden

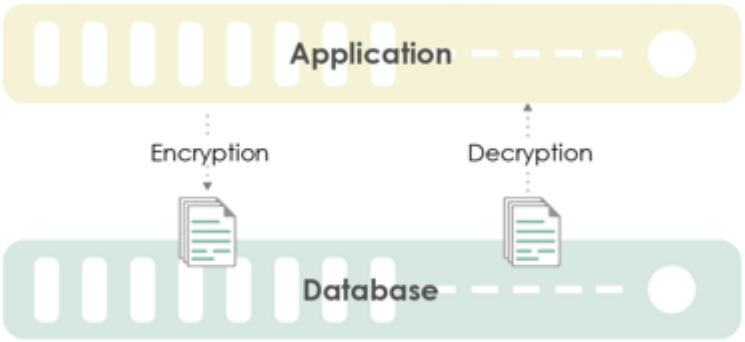
ServiceNow® Bietet Datenbankverschlüsselungsmethoden (Database Encryption, DBE) und Volldatenträger-Verschlüsselungsmethoden für Kunden mit gesetzlichen Verpflichtungen zum Datenschutz, die möglicherweise Schutz im Ruhezustand für alle Daten erfordern.

Wichtig: Beginnend mit Washington DC Release, Datenbankverschlüsselung wird für zukünftige Veraltet vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter Cloud-Verschlüsselung Mit Schlüsselverwaltung

Mit der Datenbankverschlüsselung können alle Daten mit der symmetrischen AES-256-Verschlüsselung geschützt werden, unabhängig davon, ob die Datenbank online oder offline ist. Von ServiceNow AI Platform Perspektive, alle Daten-Flows in entschlüsselt.

- Die Datenbankverschlüsselung unterstützt die Verschlüsselung aller gespeicherten Daten in Echtzeit und bietet Schutz für Daten online und offline ohne Verlust der Funktionalität.
- Die vollständige Datenträgerverschlüsselung schützt Offline-Daten, wenn ein Datenträgerverlust oder -Diebstahl auftritt.

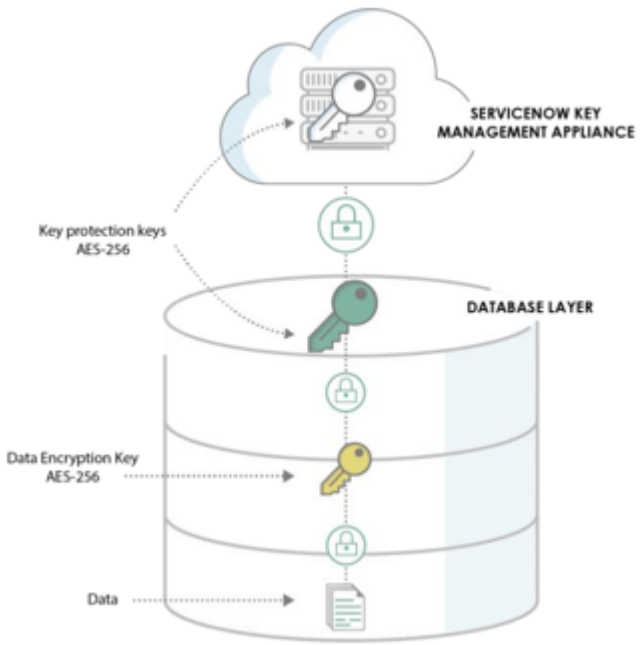
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit der Datenbankverschlüsselung werden alle gespeicherten Daten verschlüsselt, und einzelne Datensätze oder Tabellen werden während des Zugriffs im Arbeitsspeicher entschlüsselt. Neue oder geänderte Daten werden verschlüsselt, wenn sie in eine Tabelle eingegeben werden, und zugehörige Aktivitätsprotokolldateien (bin, Wiederholen, Rückgängig machen und Fehler) werden ebenfalls verschlüsselt.

Die Datenbankverschlüsselung ist für Anwender transparent, ohne dass die Funktionalität verloren geht. Bei Verwendung dieser Funktion werden alle Instanzen zusammen mit Replikationsdatenverkehr und Sicherungen verschlüsselt. Das Klonen von Instanzen ist weiterhin mit geringfügigen Leistungsauswirkungen für die Verwendung der Datenbankverschlüsselung von bis zu 5 % verfügbar. Sowohl neue als auch vorhandene Instanzen in unterstützten Releases von ServiceNow AI Platform Kann die Datenbankverschlüsselung nutzen.

Wie dargestellt, ServiceNow Speichert und verwaltet Schlüssel mithilfe einer Schlüsselhierarchie auf drei Ebenen:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Ein kundenspezifischer AES-256-Schlüssel wird von der Datenbank-Engine erstellt und zum Verschlüsseln der Daten verwendet.
2. Ein zweiter kundenspezifischer AES-256-Schlüssel wird von der Datenbank-Engine erstellt und zum Schutz des Schlüssels der ersten Ebene verwendet.
3. Ein dritter AES-256-Schlüssel wird von erstellt und in FIPS 140 validierten Schlüsselverwaltungsgeräten in gespeichert ServiceNow Rechenzentren. Dieser Schlüssel schützt den Schlüssel der zweiten Ebene und ist für jede Kundeninstanz eindeutig.

Die ServiceNow AI Platform Unterstützt auch die Datenbankverschlüsselung mit einem vom Kunden bereitgestellten Switch, DBE mit CCS. Dies ist eine Verschlüsselungslösung, die alle Daten im Ruhezustand verschlüsselt, wenn sie nicht in der Datenbank verwendet werden. Es verwendet AES-Verschlüsselung nach Industriestandard ohne Auswirkungen auf die Funktionalität. Die Datenbank verschlüsselt Daten, während sie auf den Datenträger geschrieben werden, und entschlüsselt Daten, wenn sie vom Datenträger gelesen werden. Das bedeutet, dass Anwendungen die Daten immer unverschlüsselt haben, um die erforderliche Logik und Funktionen ohne Auswirkungen auszuführen.

Hinweis: Datenbankverschlüsselung wird für lokale Instanzen nicht unterstützt.

Wenn Sie eigene Schlüssel für die Datenbankverschlüsselung verwenden, finden Sie unter Datenbankverschlüsselung mit vom Kunden gesteuertem Switch.

Datenbankschlüsselrotation wird angefordert

Rotieren Sie den Datenbankschlüssel jährlich oder nach Bedarf, indem Sie eine Support-Anforderung senden.

Vorbereitungen

Erforderliche Rolle: Administrator

Wichtig: Beginnend mit Washington DC Release, Datenbankverschlüsselung wird für zukünftige Veraltet vorbereitet. Cloud Encryption ist die Ersatzlösung für die Verschlüsselung von Daten im Ruhezustand. Weitere Informationen finden Sie unter Cloud-Verschlüsselung Mit Schlüsselverwaltung

Warum und wann dieser Vorgang ausgeführt wird

Die Schlüsselrotation erfolgt nachts innerhalb von 24 Stunden vor dem Ablaufdatum und unterbricht den Service für die Instanz nicht.

Hinweis: Derzeit ist die Schlüsselrotation nur in verfügbar ServiceNow Commercial, Government Community Cloud (GCC), Frankreich und Singapur Umgebungen.

Prozedur

Kontakt Kundenservice und Support So fordern Sie eine der folgenden Schlüsselrotationsaktionen an:

- Registrieren Sie sich, um eine jährliche Schlüsselrotation für alle festgelegten Instanzen durchzuführen.
- Rufen Sie einen Verlaufsbericht der letzten drei Schlüsselrotationen ab, der Folgendes enthält:
  - Instanzname.
  - Schlüsselname und -Version.
  - Daten und Uhrzeiten der Rotation.
- Planen Sie eine frühzeitige Schlüsselrotation außerhalb der jährlichen geplanten Rotation.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenbankverschlüsselung mit vom Kunden gesteuertem Switch

Datenbankverschlüsselung mit kundengesteuertem Switch (DBE-CCS) ist eine Verschlüsselungslösung, die alle Daten im Ruhezustand verschlüsselt, wenn sie nicht in der Datenbank verwendet werden.

Wichtig:

Die Datenbankverschlüsselung mit vom Kunden gesteuertem Switch hat den Prozess zum Ende der Lebensdauer begonnen und hat die Meilensteine für das Ende des Verkaufs und das Ende der Verlängerung ab dem Yokohama-Release erreicht. Informationen zur Unterstützung der Verschlüsselung von Daten im Ruhezustand finden Sie unter Cloud-Verschlüsselung Mit Schlüsselverwaltung.

Übersicht

Die Datenbankverschlüsselung mit vom Kunden gesteuertem Switch verwendet AES-Verschlüsselung nach Branchenstandard, ohne Auswirkungen auf die Funktionalität. Die Datenbank verschlüsselt Daten, wenn sie auf den Datenträger geschrieben und von der Datenbank entschlüsselt werden, wenn sie vom Datenträger gelesen werden. Anwendungen haben die Daten immer in einem unverschlüsselten Status, um die erforderliche Logik und Funktionen auszuführen.

DBE-CCS verwendet eine in der Datenbank native Technologie, häufig als Tablespace Encryption oder transparente Datenverschlüsselung bezeichnet. Weitere Informationen zur Technologie finden Sie unter MariaDB-Website Unter „Tablespace-Verschlüsselung“.

DBE-CCS erfordert, dass Sie einen HTTPS-REST-Service-Endpunkt einrichten, der regelmäßig den geheimen Schlüssel für bereitstellt ServiceNow Instanz. Der CCS-Endpunkt gibt dann den geheimen Kundenschlüssel zurück, der mit dem öffentlichen Schlüssel der Datenbankinstanz verschlüsselt ist.

Kundenendpunkt

Wichtig: Ihre Organisation ist allein für die Einrichtung und Wartung Ihres CCS-Endpunkts verantwortlich. Die Endpunktspezifikation des Kunden wird in bereitgestellt KB0789788 .

A ServiceNow Der Technologiepartner Fortanix ist verfügbar, um Ihren Kundenendpunkt für Sie zu implementieren. Wenden Sie sich direkt an den Technologiepartner, um Details zur Integration zu erhalten. Weitere Informationen finden Sie unter Verwendung von Fortanix Data Security Manager mit ServiceNow .

Mehrere ServiceNow Versionsunterstützung

Wichtig: Datenbankverschlüsselung ist ein bezahltes Infrastrukturangebot, das Releaseunabhängig ist. Sie kann auf jedes unterstützte Release und auf neue oder vorhandene Instanzen angewendet werden.

Andere Referenzen

Weitere Informationen zu DBE mit CCS finden Sie in diesen Referenzen:

Referenz	Beschreibung
KB0993681	Architektur des kundengesteuerten Switches für Datenbankverschlüsselung
KB0789788	Implementierungsleitfaden für DBE mit CCS

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Um auf KB-Artikel zuzugreifen, müssen Sie sich zuerst bei authentifizieren Now Support.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

servicenow

Zugriffsverwaltung

Mit Zugriffsmanagement können Sie Zugriff auf haben ServiceNow® Instanz sicher.

Zero Trust-Zugriff



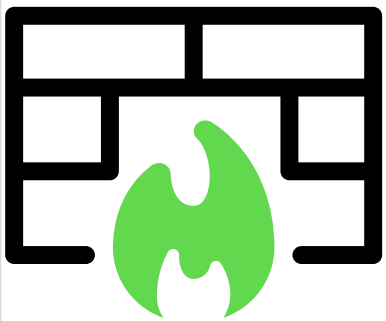
Zero Trust Access stellt sicher, dass der gesamte Zugriff auf Anwendungen und Daten nur nach der Identitätsverifizierung und Risikobewertung des Anwenders mit den geringsten Berechtigungen gewährt wird.

Domain Separation



Mit ServiceNow AI Platform, Service Provider (SPS) können ihren Kunden ein schnelleres Onboarding bieten, Compliance einhalten und ihre Daten mithilfe von Domänentrennung schützen.

Authentifizierung

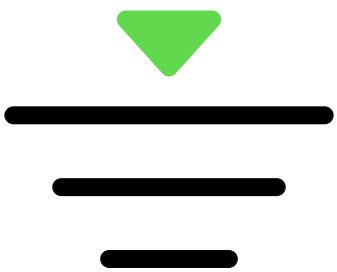


Die Authentifizierung von ServiceNow validiert die Identität eines Anwenders, der auf eine Instanz zugreift, und autorisiert den Anwender dann für Funktionen, die der Rolle oder Auftragsfunktion des Anwenders entsprechen.

ACL



Datenfilterung



Verwenden Sie die Datenfilterung, um bei Leseabfragen den Zugriff auf Tabellen und Datensätze basierend auf Themenattributen zu steuern.

Sicherheitsrollen



Sicherheitsrollen bieten zusätzliche Sicherheit. Jeder Anwender muss mindestens eine Rolle haben, damit die Instanz zwischen internen und externen Anwendern unterscheiden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Verbindung und Anmeldeinformationen



Anmelde- und Verbindungsinformationen sind erforderlich, um auf einen Computer oder ein Netzwerkgerät für Discovery, Service-Mapping und Cloud-Management zuzugreifen oder um mit Orchestration zu arbeiten.

ServiceNow-Zugriffssteuerung



Mit dem Plugin „SNC-Zugriffssteuerung“ können Sie steuern, welche Kundenservice- und Supportmitarbeiter wann auf Ihre Instanz zugreifen können.

Zero Trust Access (ZTA)

Zero Trust Access (ZTA) ist ein Sicherheitsmodell, das davon ausgeht, dass kein Anwender oder Gerät standardmäßig vertrauenswürdig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von Zero Trust Access.

Aktivieren



Erfahren Sie, wie Sie Zero Trust Access aktivieren.

Konfigurieren



Konfigurieren Sie Zero Trust-Zugriff.

Referenz: Eigenschaften



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zero Trust-Zugriff Erkunden

Zero Trust Access (ZTA) ist ein Sicherheitsmodell, das davon ausgeht, dass kein Anwender oder Gerät standardmäßig vertrauenswürdig ist.

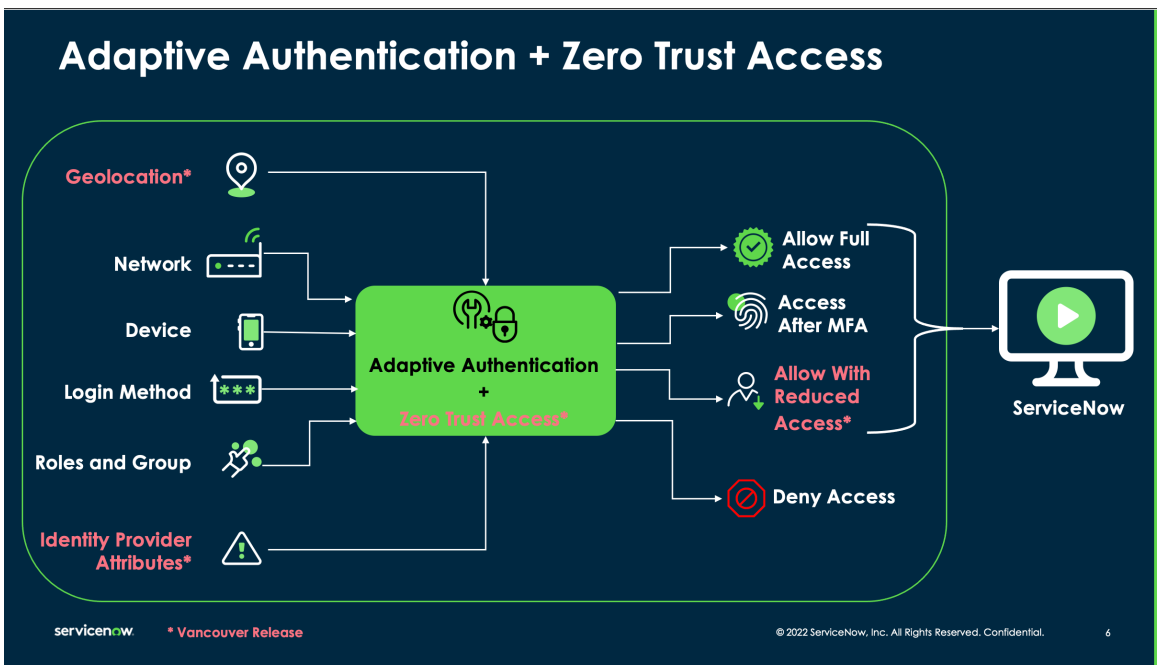
ZTA stellt sicher, dass jeder Zugriff auf Anwendungen und Daten nur nach der Identitätsverifizierung und Risikobewertung des Anwenders mit geringsten Berechtigungen gewährt wird.

Zero Trust: Richtlinienbasierter Sitzungszugriff

ServiceNow Zero Trust: Richtlinienbasierter Sitzungszugriff (Sitzungszugriff) ermöglicht Unternehmen die dynamische Reduzierung von Anwenderberechtigungen in einer Websitzung basierend auf einer Vielzahl von Faktoren, einschließlich IP-Adresse, Standort, Authentifizierungsmethode, Anwenderrolle, Gruppe, Anwender mit MFA und Attributen, die vom Identitätsanbieter (IDP) gemeinsam genutzt werden. Dies kann dazu beitragen, Organisationen vor nicht autorisiertem Zugriff und Datenschutzverletzungen zu schützen, auch wenn Anwender mit hohen Berechtigungen von nicht vertrauenswürdigen Geräten oder Standorten aus auf Anwendungen zugreifen.

Zero Trust: Richtlinienbasierter Sitzungszugriff

Mit dieser Option können Sicherheitsadministratoren den Anwenderzugriff in einer Sitzung basierend auf IP-Adresse, Standort, Attributen des Identitätsanbieters und Anwenderattributen mithilfe von Richtlinien für adaptive Authentifizierung reduzieren oder einschränken.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Sitzungszugriffskonfigurationen können nur mit ausgeführt werden `Security_admin` Rolle. Sie müssen Ihre Rolle auf erhöhen `Security_admin` .
- Der Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Anwender zugewiesen ist. In diesem Fall gibt es keine Änderungen an der angemeldeten Sitzung. Der Anwender greift weiterhin mit den zugewiesenen Berechtigungen auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, während der Anwender bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Anwender muss sich von der Sitzung abmelden, damit die Richtlinie wirksam ist.
- Der Sitzungszugriff hat keine Auswirkungen, wenn sich der Anwender in einem vertrauenswürdigen Netzwerk befindet und später innerhalb einer Sitzung zu einem VPN wechselt (Änderung des Standorts oder Netzwerks).
- Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu eingeschränktem Zugriff. Beispielsweise führt ein Anwender, der nach dem Einrichten der Sitzung vom Unternehmensnetzwerk zu einem nicht vertrauenswürdigen Netzwerk wechselt, nicht zu eingeschränktem Zugriff, es sei denn, der Anwender meldet sich ab und meldet sich erneut an.
- Funktion „Sitzungszugriff“ (Zero Trust Access – ZTA), Rollen wie `snc_internal` Und `snc_external` Kann nicht entfernt werden.
- Durch die Funktion „Sitzungszugriff“ (Zero Trust Access – ZTA) wird keine Rolle aus entfernt `sys_user_has_role` Oder die Tabelle der Anwendergruppenmitgliedschaft. Basierend auf der ZTA-Richtlinie wird die Anwendersitzung mit eingeschränkten oder eingeschränkten Rollen eingerichtet.
- Die im Systemkontext ausgeführten Skripts berücksichtigen die ZTA-Sitzungsrollen nicht.

Anwendungsfall

Im Folgenden finden Sie einige der Anwendungsfälle von Zero Trust Access:

- Reduzieren Sie Berechtigungen basierend auf dem mit der Sitzung verbundenen Risiko. Beispielsweise kann ein Erfüller-Rollenanwender, der sich außerhalb des vertrauenswürdigen Netzwerks anmeldet, so konfiguriert werden, dass nur die Rolle der anfordernden Person für die Sitzung verwendet wird.
- Reduzieren Sie den Zugriff basierend auf der IDP-Antwort für eine Anwendersitzung, wenn der Anwender ein nicht vertrauenswürdiges Gerät verwendet. Weitere Informationen finden Sie unter Konfigurieren Sie das Attribut „Identitätsanbieter“ für den Sitzungszugriff.

Diese Rollenverschiebung stellt sicher, dass der Anwender keine anderen vorhandenen Berechtigungen in einer Sitzung hat. Wenn sich der Anwender über ein vertrauenswürdiges Netzwerk anmeldet, werden alle vorhandenen Berechtigungen für eine Sitzung zugewiesen.

Mehrere IP-Bedingungen und mehrere Rollen- oder Gruppenzuweisungen können als Teil der Richtlinie definiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zero Trust-Zugriff: Mobil

Sie können die Richtlinie Zero Trust-Zugriff – Sitzungszugriff innerhalb der Richtlinie „Adaptive Authentication“ verwenden, um die Rollen oder Berechtigungen der jeweiligen Sitzung auf Mobilgeräten zu reduzieren.

Zero Trust-Zugriff: Der mobile Sitzungszugriff kann durch Aktivieren von aktiviert werden **glide.authenticate.session_access.mobile.enabled** Aus der Tabelle mit den Systemeigenschaften.

Zur Verwendung von Zero Trust Access – Sitzungszugriff mobil mit den IDP-Attributen können Sie konfigurieren **glide.authenticate.session_access.mobile.refresh_token_interval** Feld. Dadurch können Administratoren den Sitzungszugriff basierend auf dem Aktualisierungstoken effektiv steuern.

Weitere Informationen finden Sie unter Konfigurieren Sie Zero Trust Access für Mobilgeräte .

Zero Trust-Zugriff Wird Aktiviert

Aktivieren Sie **Zero Trust: Richtlinienbasierter Sitzungszugriff** Com.snc.Zero_Trust_Session_Access Plugin, mit dem Sicherheitsadministratoren den Anwenderzugriff in einer Sitzung basierend auf IP-Adresse, Standort, Attributen des Identitätsanbieters und Anwenderattributen mithilfe adaptiver Authentifizierungsrichtlinien reduzieren oder einschränken können.

Vorbereitungen
Erforderliche Rolle: Administrator

Plugin-Typ: Bezahlt und Lizenz erforderlich.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach **Zero Trust: Richtlinienbasierter Sitzungszugriff** (Com.snc.Zero_Trust_Session_Access) Plugin mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

   Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Sitzungszugriffsrolle wird konfiguriert

Konfigurieren Sie den Sitzungszugriff, um den Anwenderzugriff in einer Sitzung basierend auf IP, Standort, Attributen des Identitätsanbieters und Anwenderattributen mithilfe von Richtlinien für adaptive Authentifizierung zu reduzieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: security_admin

Hinweis:

- Sitzungszugriffskonfigurationen können nur mit ausgeführt werden `Security_admin` Rolle. Sie müssen Ihre Rolle auf erhöhen `Security_admin` .
- Der Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Anwender zugewiesen ist. In diesem Fall gibt es keine Änderungen an der angemeldeten Sitzung. Der Anwender greift weiterhin mit seinen zugewiesenen Berechtigungen auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, während der Anwender bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Anwender muss sich von der Sitzung abmelden, damit die Richtlinie wirksam ist.
- Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu eingeschränktem Zugriff. Beispielsweise führt ein Anwender, der nach dem Einrichten der Sitzung vom Unternehmensnetzwerk zu einem nicht vertrauenswürdigen Netzwerk wechselt, nicht zu eingeschränktem Zugriff, es sei denn, der Anwender meldet sich ab und meldet sich erneut an.
- Funktion „Sitzungszugriff“ (Zero Trust Access – ZTA), Rollen wie `snc_internal` Und `snc_external` Kann nicht entfernt werden.
- Durch die Funktion „Sitzungszugriff“ (Zero Trust Access – ZTA) wird keine Rolle aus entfernt `sys_user_has_role` Oder die Tabelle der Anwendergruppenmitgliedschaft. Basierend auf der ZTA-Richtlinie wird die Anwendersitzung mit eingeschränkten oder eingeschränkten Rollen eingerichtet.
- Die im Systemkontext ausgeführten Skripts berücksichtigen die ZTA-Sitzungsrollen nicht.

Prozedur

1. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.
2. Um eine Konfiguration der Sitzungszugriffsrolle zu erstellen, wählen Sie aus **Neu** .
3. Füllen Sie im Formular die folgenden Felder aus:

Konfiguration der Sitzungszugriffsrolle

Feld	Beschreibung
Name	Name der Konfiguration
Beschreibung	Kurzbeschreibung der Konfiguration.
Richtlinie	Wählen Sie die Richtlinie für die adaptive Authentifizierung aus. Verwenden Sie das Suchsymbol, um die Liste der Richtlinien anzuzeigen.
Aktion	**Entfernen Sie Rollen** Oder **Auf Rollen beschränken** . ○ **Entfernen Sie Rollen** : Wenn sich der konfigurierte Anwender anmeldet, wird die Liste der Rollen, die in der Rollen-

Automatische Übersetzung

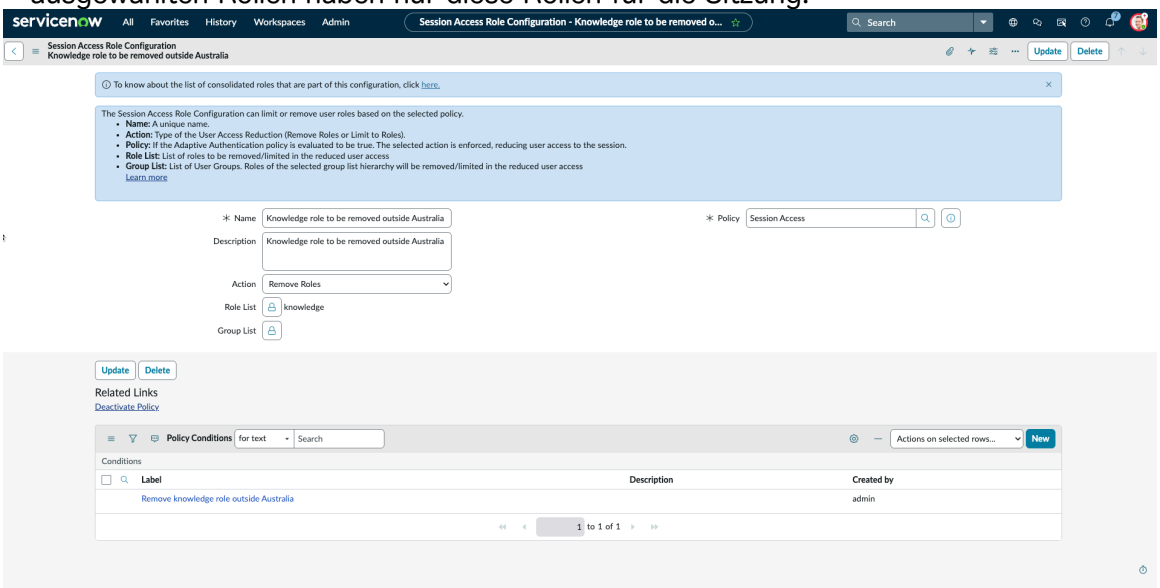
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	oder Gruppenliste angegeben sind, für die Sitzung entfernt. ○ **Auf Rollen Beschränken** : Wenn sich der konfigurierte Anwender anmeldet, werden dem Anwender nur die ausgewählten Rollen bereitgestellt, und alle anderen Rollen werden für die Sitzung entfernt.
Rollenliste	Wählen Sie Rollen aus der Rollenliste aus.
Gruppenliste	Wählen Sie die Rollen aus der Gruppenliste aus, die Sie entfernen oder auf den Anwender beschränken möchten.

4. Auswählen, **Übermitteln** .

Die Anmeldung für Anwender basierend auf den konfigurierten Ländern lautet wie folgt:

- In **Entfernen Sie Rollen** , Die Anwender aus den konfigurierten Ländern mit den ausgewählten Rollen verfügen nicht mehr über diese Rollen für die Sitzung.
- In **Auf Rollen Beschränken** , Die Anwender aus den konfigurierten Ländern mit den ausgewählten Rollen haben nur diese Rollen für die Sitzung.



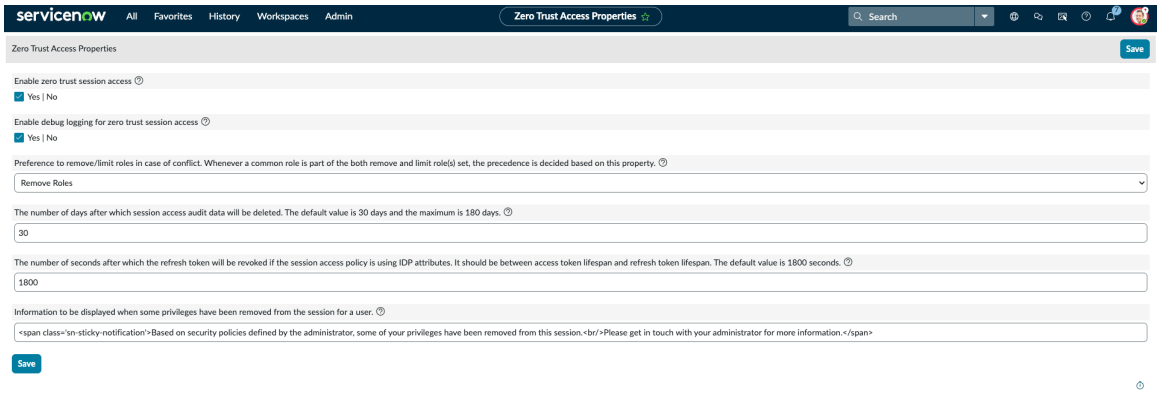
Weitere Informationen zum Entfernen oder Einschränken von Rollen für eine Sitzung, erklärt anhand eines Beispielanwendungsfalls, finden Sie unter Tutorial: Zero Trust-Zugriff Verwenden.

Zero Trust Access-Systemeigenschaften

Verwenden Sie Systemeigenschaften, um Zero Trust-Zugriff zu aktivieren und anzupassen, um Ihre Sicherheitsanforderungen zu erfüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften



Zero Trust Access-Systemeigenschaften

Eigenschaft	Beschreibung
Aktivieren Sie Zero Trust-Sitzungszugriff	Option, mit der Administratoren die Zero Trust-Sitzungszugriffsfunktion verwenden können. Standardmäßig ist der Wert Falsch .
Debug-Protokollierung für Zero Trust-Sitzungszugriff aktivieren	Option zum Aktivieren der Debug-Protokollierung für Zero Trust-Sitzungszugriff.
Einstellung zum Entfernen/Einschränken von Rollen im Konfliktfall. Immer wenn eine allgemeine Rolle Teil der festgelegten Rolle(n) zum Entfernen und zum Einschränken von Rollen ist, wird der Vorrang basierend auf dieser Eigenschaft festgelegt.	**Entfernen Sie Rollen** Oder **Rollen Begrenzen**
Die Anzahl der Tage, nach denen Audit-Daten des Sitzungszugriffs gelöscht werden. Der Standardwert ist 30 Tage, der Höchstwert 180 Tage.	Standardmäßig beträgt dies 30 Tage.
Die Anzahl der Sekunden, nach denen das Aktualisierungstoken widerrufen wird, wenn die Sitzungszugriffsrichtlinie IDP-Attribute verwendet. Er muss zwischen der Lebensdauer des Zugriffstokens und der Lebensdauer des Aktualisierungstokens liegen. Der Standardwert ist 1800 Sekunden.	Standardmäßig sind es 1800 Sekunden.
Informationen, die angezeigt werden sollen, wenn für einen Anwender einige Berechtigungen aus der Sitzung entfernt wurden.	Beschreibung, die Sie Ihren Anwendern hinsichtlich der Einschränkung oder Entfernung von Berechtigungen anzeigen möchten. Beispielbeschreibung: Basierend auf den vom Administrator definierten Sicherheitsrichtlinien wurden einige Ihrer Rollen aus dieser Sitzung entfernt. Wenden Sie sich an Ihren Administrator, um weitere Informationen zu erhalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

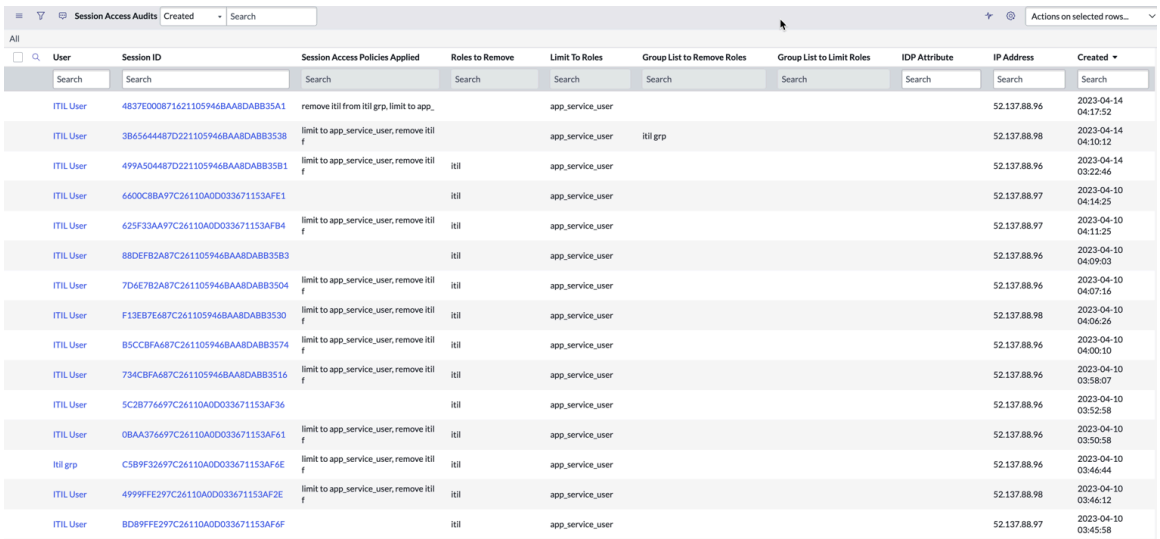
Audits des Sitzungszugriffs

Die Sitzungszugriffs-Audits zeigen Sitzungszugriffsprotokolle und Informationen im Zusammenhang mit der Sitzung eines Anwenders an.

Audits

Das Audit „Sitzungszugriff“ zeigt Audit-Informationen wie folgt an:

Hinweis: Verwenden Sie glide.authenticate.session_access.log_audit_event Eigenschaft zum Ausfüllen der Audit-Informationen.



Audits des Sitzungszugriffs

Feld	Beschreibung
Anwender	Details des Anwenders.
Sitzungs-ID	Details zur Sitzung, die als eindeutige ID angezeigt werden.
Mobile-Client	Die Details des mobilen Clients. **ServiceNow-Agent** (Now Agent) und **ServiceNow-Anforderung** (Now Mobile).
Sitzungszugriffsrichtlinien angewendet	Die angewendete Sitzungszugriffsrichtlinie.
Zu entfernende Rollen	Rollen, die während der Protokollierung vom Anwender entfernt wurden.
Auf Rollen beschränken	Rollen, die während der Protokollierung auf den Anwender beschränkt waren.
Gruppenliste zur Entfernung von Rollen	Informationen zur Gruppe, die Rollen für den Anwender entfernt hat.
Gruppenliste zur Beschränkung von Rollen	Informationen zur Gruppe, die eingeschränkte Rollen für den Anwender hat.
Mobile-Client	Details des Anwenders, der sich über Mobilgeräte mit eingeschränktem oder entferntem Zugriff angemeldet hat.
IDP-Attribut	Der IDP, der für diese Sitzung verwendet wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audits des Sitzungszugriffs (Fortsetzung)

Feld	Beschreibung
IP-Adresse	Details der IP-Adresse, die der Anwender zum Anmelden verwendet.
Erstellt	Details zum Datum und zur Uhrzeit des erstellten Anwenderdatensatzes.

Tutorial: Zero Trust-Zugriff Verwenden

Verfahren zur Verwendung der Zero Trust-Zugriffsfunktion mit einem End-to-End-Anwendungsfall.

Vorbereitungen
Erforderliche Rolle: security_admin

Aktivieren Sie **Aktivieren Sie die Eigenschaft „Sitzungszugriff“** .

Hinweis:

- Sitzungszugriffskonfigurationen können nur mit ausgeführt werden `Security_admin` Rolle. Sie müssen Ihre Rolle auf erhöhen `Security_admin` .
- Der Sitzungszugriff unterstützt keine Integrationen.
- Der Sitzungszugriff hat keine Auswirkungen, wenn die reduzierte oder eingeschränkte Rolle keinem Anwender zugewiesen ist. In diesem Fall gibt es keine Änderungen an der angemeldeten Sitzung. Der Anwender greift weiterhin mit seinen zugewiesenen Berechtigungen auf die Instanz zu.
- Der Sitzungszugriff hat keine Auswirkungen, während der Anwender bereits bei der Instanz angemeldet ist und gleichzeitig der Administrator die Richtlinie konfiguriert. Der Anwender muss sich von der Sitzung abmelden, damit die Richtlinie wirksam ist.
- Sitzungszugriff wird zum Zeitpunkt der Anmeldung erzwungen. Jede Änderung der Risikoparameter während der Sitzung führt nicht zu eingeschränktem Zugriff. Beispielsweise führt ein Anwender, der nach dem Einrichten der Sitzung vom Unternehmensnetzwerk zu einem nicht vertrauenswürdigen Netzwerk wechselt, nicht zu eingeschränktem Zugriff, es sei denn, der Anwender meldet sich ab und meldet sich erneut an.
- Funktion „Sitzungszugriff“ (Zero Trust Access – ZTA), Rollen wie `snc_internal` Und `snc_external` Kann nicht entfernt werden.
- Durch die Funktion „Sitzungszugriff“ (Zero Trust Access – ZTA) wird keine Rolle aus entfernt `sys_user_has_role` Oder die Tabelle der Anwendergruppenmitgliedschaft. Basierend auf der ZTA-Richtlinie wird die Anwendersitzung mit eingeschränkten oder eingeschränkten Rollen eingerichtet.
- Die im Systemkontext ausgeführten Skripts berücksichtigen die ZTA-Sitzungsrollen nicht.

Sitzungszugriff ist eine Funktion, mit der Administratoren eine Reihe von Rollen dynamisch reduzieren oder auf den Anwender beschränken können, wenn der Anwender versucht, sich aus verschiedenen Umgebungen bei der Instanz anzumelden, z. B. sich über das nicht vertrauenswürdige Netzwerk anmelden, sich über ein anderes Gerät anmelden usw.

Der Sitzungszugriff kann durch die erstellte Richtlinie und die ausgewählte Aktion beim Ausführen der Konfiguration gesteuert werden. Einige der Szenarien lauten wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Richtlinie auf „wahr“ festgelegt ist und die Rollenaktion auf festgelegt ist **Entfernen Sie Rollen** , Dann werden die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Anwender entfernt, wenn er versucht, sich bei der Instanz anzumelden.
- Wenn die Richtlinie auf „wahr“ festgelegt ist und die Rollenaktion auf festgelegt ist **Auf Rollen Beschränken** , Dann werden dem Anwender nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen zugewiesen, wenn versucht wird, sich bei der Instanz anzumelden.

Das folgende Verfahren erläutert eine End-to-End-Konfiguration der Sitzungszugriffskonfiguration, basierend darauf, dass die Rolle auf den Anwender beschränkt ist, der sich bei der Instanz anmeldet. Ebenso können Sie Rollen entfernen, indem Sie auswählen **Entfernen Sie Rollen** Option während der Konfiguration.

Prozedur

1. Navigieren zu **Alle** > **Sitzungszugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.
2. Wählen Sie auf der Seite Sitzungszugriffsrollenkonfigurationen die Option aus **Neu** .
3. Um eine Rolle für den Anwender einzuschränken, füllen Sie im Formular die Felder aus:
   - Name
   - Beschreibung
   - Richtlinie
   - Aktion
   - Rollenliste
   - Gruppenliste

   a. Wählen Sie Aus **Auf Rollen Beschränken** Zum Einschränken von Rollen für den Anwender. Beispiel: **itil** .

   b. Wählen Sie Aus **Wissen** Rolle aus der Rollenliste.

   c. Wählen Sie aus **Richtlinie** .

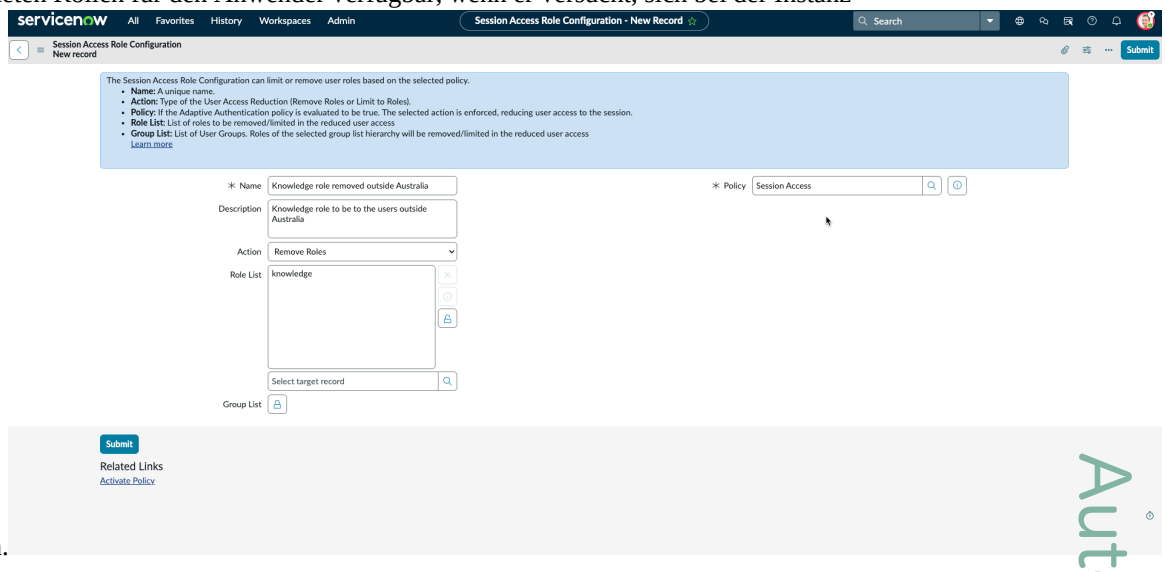
   Sie können die Sitzungszugriffsrichtlinie mithilfe von Authentifizierungsrichtlinien und Filterkriterien (Rolle, Gruppe, IP, Standort) mit Richtlinieneingaben und -Bedingungen erstellen.

   Verwenden Sie die Richtlinie in der Konfiguration „Sitzungszugriff“. Sie möchten beispielsweise die Rolle (Wissen) auf den Anwender beschränken, der sich außerhalb des Standorts (Australien) anmeldet.

   d. Wählen Sie Aktion als aus **Auf Rollen Beschränken** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Richtlinie auf „wahr“ festgelegt ist, sind nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Anwender verfügbar, wenn er versucht, sich bei der Instanz



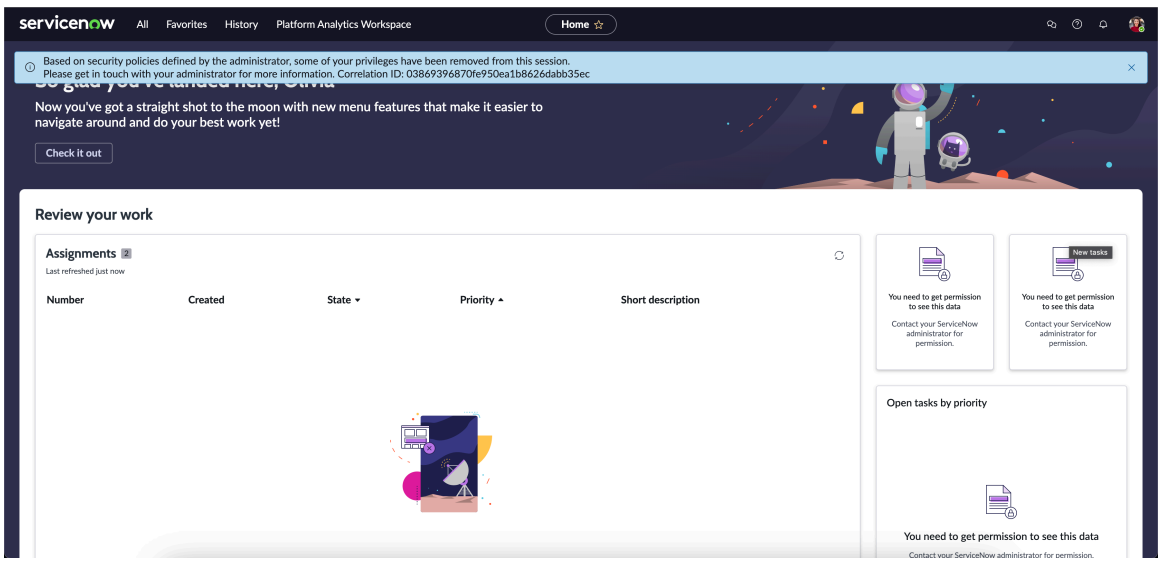
anzumelden.

e. Wählen Sie **Absenden**.

Ebenso können Sie die Gruppe aus der Gruppenliste auswählen, um Rollen für die Anwender innerhalb der Gruppe einzuschränken oder zu entfernen.

Wenn sich der Anwender bei der Instanz außerhalb Australiens anmeldet, wird nur der verwendet **Wissen** Die Rolle und die zugehörigen untergeordneten Rollen werden für die protokollierte Sitzung zugewiesen, und andere Rollen sind dem Anwender eingeschränkt.

Nach der Anmeldung wird der Anwender mit der folgenden Fehlermeldung auf der Plattform im Profilabschnitt angezeigt:



Der Anwender kann sich an die Administratoren wenden und die Korrelations-ID für die Untersuchung angeben.

Hinweis: Die Korrelations-ID ist die sys_ID des entsprechenden Audit-Datensatzes in der Audit-Tabelle für den Sitzungszugriff.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie das Attribut „Identitätsanbieter“ für den Sitzungszugriff

Verwenden Sie das aus der SAML-Antwort (Security Assertion Markup Language) und OpenID Connect (OIDC) erstellte Attribut „Identity Provider“ (IDP), um den Zugriff von Anwendersitzungen auf die Instanz zu entfernen oder zu beschränken.

Vorbereitungen

Erforderliche Rolle: security_admin

Aktivieren Sie **Aktivieren Sie die Eigenschaft „Sitzungszugriff“** .

Hinweis: Um die Konfiguration der Sitzungszugriffsrolle zu verwenden, müssen Sie Ihre Rolle auf erhöhen `Security_admin` .

Der Sitzungszugriff kann durch die erstellte Richtlinie und die ausgewählte Aktion beim Ausführen der Konfiguration gesteuert werden. Einige der Szenarien lauten wie folgt:

- Wenn die Richtlinie auf „wahr“ festgelegt ist und die Rollenaktion auf festgelegt ist **Entfernen Sie Rollen** Zusammen mit der Eingabe und Bedingung des IDP-Attributs werden die ausgewählten Rollen und die zugehörigen untergeordneten Rollen für den Anwender entfernt, wenn er versucht, sich bei der Instanz anzumelden.
- Wenn die Richtlinie auf „wahr“ festgelegt ist und die Rollenaktion auf festgelegt ist **Auf Rollen Beschränken** Zusammen mit der Eingabe und Bedingung des IDP-Attributs werden dem Anwender beim Versuch, sich bei der Instanz anzumelden, nur die ausgewählten Rollen und die zugehörigen untergeordneten Rollen zugewiesen.

Das folgende Verfahren zeigt die Schritte zum Konfigurieren des IDP-Attributs aus der SAML-Antwort A-Richtlinieneingabe, um den Sitzungszugriff zu steuern.

Prozedur

1. Navigieren zu **Alle** > **Sitzungszugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.
2. Wählen Sie auf der Seite Sitzungszugriffsrollenkonfigurationen die Option aus **Neu** .
3. Um eine Rolle für den Anwender zu entfernen, füllen Sie im Formular die Felder aus:
   - Name
   - Beschreibung
   - Richtlinie
   - Aktion
   - Rollenliste
   - Gruppenliste

   a. Wählen Sie Aus **Entfernen Sie Rollen** Zum Entfernen von Rollen für den Anwender.
   Beispiel: **itil** .

   b. Wählen Sie Aus **itil** Rolle aus der Rollenliste.

   c. Wählen Sie aus **Richtlinie** .
   Weitere Informationen zum Erstellen von Richtlinien mithilfe verschiedener Filterkriterien mit der Richtlinienerstellung der adaptiven Authentifizierung finden Sie unter Filterkriterien.

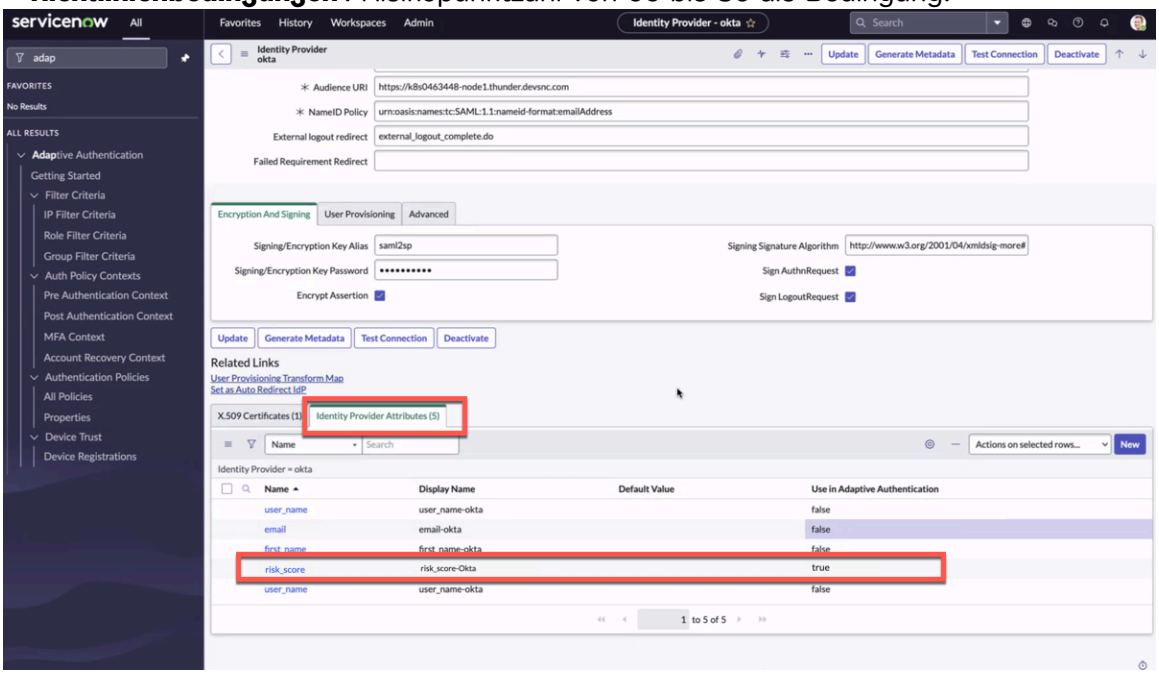
   d. Wählen Sie Aktion als Rollen entfernen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Richtlinie auf „wahr“ festgelegt ist und die Rollenaktion auf festgelegt ist **Entfernen Sie Rollen** , Dann werden die ausgewählten Rollen für den Anwender entfernt, wenn er versucht, sich bei der Instanz anzumelden.

e. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und Richtlinienbedingung. Zum Beispiel:

- **Richtlinieneingabe** : Risikopunktzahlattribut aus Okta (IDP).
- **Richtlinienbedingungen** : Risikopunktzahl von 60 bis 80 als Bedingung.



Basierend auf dieser Konfiguration wird der Anwender nicht mit den Rollen authentifiziert, wenn der Attributwert der Risikopunktzahl aus Okta (IDP) über 80 hinausgeht **Mitarbeiter**) Und den untergeordneten Rollen, die in die Instanz entfernt wurden, wird der Anwender nur mit anderen zugewiesenen Rollen authentifiziert. Wenn die Risikopunktzahl zwischen 60 und 80 liegt, wird der Anwender mit allen Rollen bei der Instanz authentifiziert.

Weitere Informationen zum Erstellen der Richtlinie für den Kontext nach der Authentifizierung mit Richtlinieneingaben und -Bedingungen finden Sie unter Kontext nach der Authentifizierung.

Hinweis: Wenn **Aktivieren Sie Den Sitzungszugriff** Eigenschaft ist inaktiv, dann schränkt die Konfiguration für Sitzungszugriff die Rollen des Anwenders nicht ein oder entfernt sie nicht.

f. Wählen Sie **Absenden**.

Zero Trust-Zugriff für Mobilgeräte

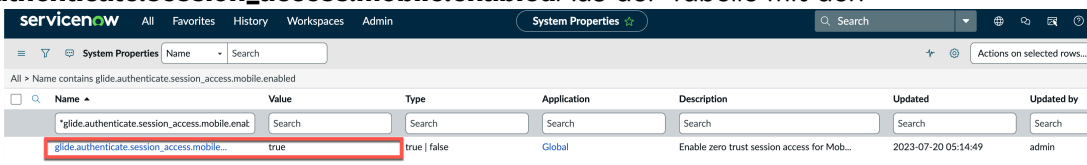
Zero Trust Access (ZTA) ist ein Sicherheitsmodell, das davon ausgeht, dass kein Anwender oder Gerät standardmäßig vertrauenswürdig ist.

Sie können die Richtlinie Zero Trust-Zugriff – Sitzungszugriff innerhalb der Richtlinie „Adaptive Authentication“ verwenden, um die Rollen oder Berechtigungen der jeweiligen Sitzung in Mobile für Anwender zu reduzieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

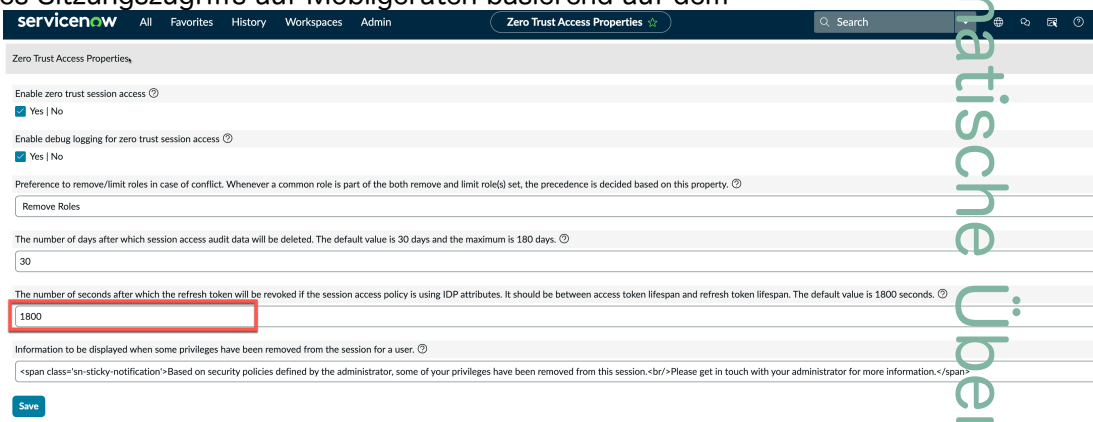
Um Zero Trust-Zugriff auf Mobilgeräten zu aktivieren, müssen Sie die folgenden Aufgaben ausführen:

- Sitzungszugriffskonfigurationen können nur mit ausgeführt werden `Security_admin` Rolle. Sie müssen Ihre Rolle auf erhöhen `Security_admin` .
- Aktivieren Sie **Zero Trust: Richtlinienbasierter Sitzungszugriff** `Com.snc.Zero_Trust_Session_Access` Richtlinie.
- Aktivieren Sie **glide.authenticate.session_access.mobile.enabled**Aus der Tabelle mit den



Systemeigenschaften.

- Konfigurieren Sie **glide.authenticate.session_access.mobile.refresh_token_interval** Feld zur Steuerung des Sitzungszugriffs auf Mobilgeräten basierend auf dem



Aktualisierungstoken.

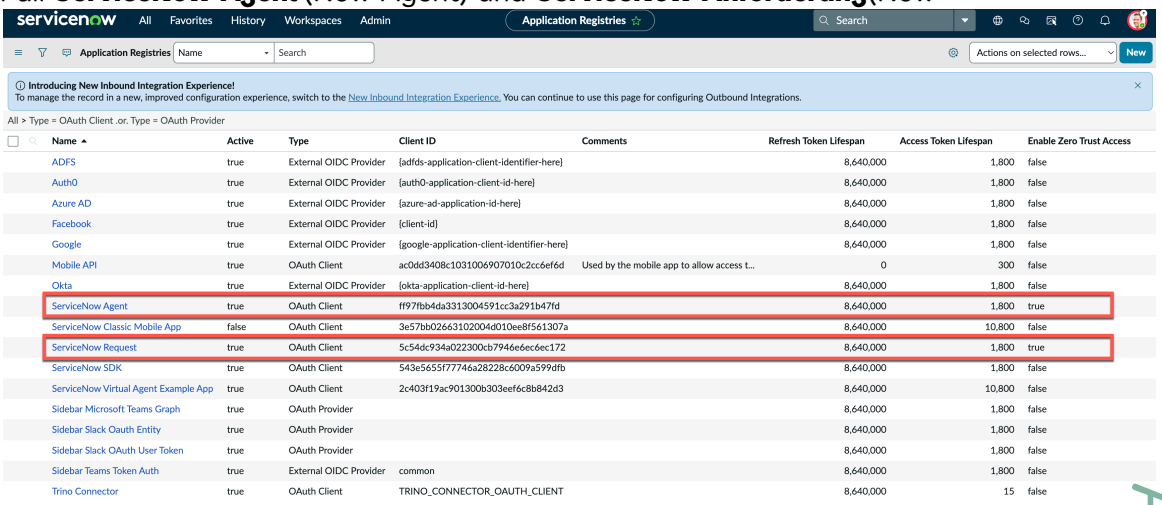
> **Hinweis:** Sie müssen die Aktualisierungstoken-Sekunden konfigurieren, wenn Sie einen IDP für Mobile-App-Anmeldungen verwenden. Standardmäßig werden Anwender nach 1800 Sekunden (30 Minuten) von den mobilen Apps abgemeldet.

- Legen Sie „Zero Trust-Zugriff aktivieren“ unter auf „wahr“ fest **Anwendungsregistrierungen** Für die mobile Client-Anwendung (OAuth-Client). In

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diesem Fall **ServiceNow-Agent** (Now Agent) und **ServiceNow-Anforderung**(Now



Name	Active	Type	Client ID	Comments	Refresh Token Lifespan	Access Token Lifespan	Enable Zero Trust Access
ADFS	true	External OIDC Provider	{adfds-application-client-identifier-here}		8,640,000	1,800	false
Auth0	true	External OIDC Provider	{auth0-application-client-id-here}		8,640,000	1,800	false
Azure AD	true	External OIDC Provider	{azure-ad-application-id-here}		8,640,000	1,800	false
Facebook	true	External OIDC Provider	{client-id}		8,640,000	1,800	false
Google	true	External OIDC Provider	{google-application-client-identifier-here}		8,640,000	1,800	false
Mobile API	true	OAuth Client	ac0dd3408c1031006907010c2cc6ef6d	Used by the mobile app to allow access t...	0	300	false
Okta	true	External OIDC Provider	{okta-application-client-id-here}		8,640,000	1,800	false
ServiceNow Agent	true	OAuth Client	ff97fbb4da33130045 91cc3a291b47fd		8,640,000	1,800	true
ServiceNow Classic Mobile App	false	OAuth Client	3e57bb02663102004d010ee8f561307a		8,640,000	10,800	false
ServiceNow Request	true	OAuth Client	5c54dc934a022300cb7946e6ec6ec172		8,640,000	1,800	true
ServiceNow SDK	true	OAuth Client	543e5655f77746a28228c6009a599dfb		8,640,000	1,800	false
ServiceNow Virtual Agent Example App	true	OAuth Client	2c403f19ac901300b303eef6c8b842d3		8,640,000	10,800	false
Sidebar Microsoft Teams Graph	true	OAuth Provider			8,640,000	1,800	false
Sidebar Slack Oauth Entity	true	OAuth Provider			8,640,000	1,800	false
Sidebar Slack OAuth User Token	true	OAuth Provider			8,640,000	1,800	false
Sidebar Teams Token Auth	true	External OIDC Provider	common		8,640,000	1,800	false
Trino Connector	true	OAuth Client	TRINO_CONNECTOR_OAUTH_CLIENT		8,640,000	15	false

Mobile).

- Konfigurieren Sie die Sitzungszugriffsrolle, um Rollen für die Anwenderprotokollierung basierend auf den Richtlinieneingaben und -Bedingungen zu reduzieren oder zu entfernen. Weitere Informationen zur Konfiguration finden Sie unter Sitzungszugriffsrolle wird konfiguriert.

Die Konfiguration wertet die Anmeldung aus, um die Rollen der Anwender zu reduzieren oder zu entfernen, die auf zugreifen ServiceNow® Instanz basierend auf den Richtlinienfiltern und -Bedingungen. Weitere Informationen finden Sie unter Konfigurieren Sie Zero Trust Access für Mobilgeräte .

Kontinuierliche Authentifizierung (CA)

ServiceNow Mit der kontinuierlichen Authentifizierung von können Sie Anwender erneut verifizieren und authentifizieren, wenn sie auf von Ihnen geschützte Ressourcen zugreifen.

Untersuchen	Aktivieren
	

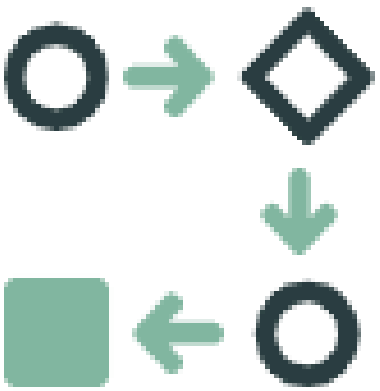
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen der kontinuierlichen Authentifizierung.

Erfahren Sie, wie Sie die kontinuierliche Authentifizierung aktivieren.

Konfigurieren



Konfigurieren Sie Die Kontinuierliche Authentifizierung.

Referenz: Eigenschaften



Informieren Sie sich über die Eigenschaften in der kontinuierlichen Authentifizierung.

Kontinuierliche Authentifizierung Erkunden

ServiceNow Mit können Sie Anwender erneut verifizieren und authentifizieren, wenn sie auf von Ihnen geschützte Ressourcen zugreifen.

ServiceNow Die kontinuierliche Authentifizierung von ist ein Sicherheitsmechanismus, der die Identität eines Anwenders nicht nur bei der ersten Anmeldung, sondern während der gesamten Sitzung des Anwenders verifiziert. CA ist auf erstellt ServiceNow Die Sicherheitsarchitektur von Zero Trust-Zugriff, die die Sicherheit verbessern soll, indem sichergestellt wird, dass der Anwender auch nach dem ersten Authentifizierungsprozess den von ihm behaupteten bleibt.

CA arbeitet nach den folgenden Zero Trust-Zugriffsprinzipien:

- **Explizit verifizieren** : Kein implizites Vertrauen für Anwender, Geräte oder Systeme in einem Netzwerk, unabhängig vom Standort. Jeder Anwender und jedes Gerät muss explizit authentifiziert und autorisiert werden, unabhängig vom Standort oder früheren Zugriff.
- **Verwenden Sie den Zugriff mit den geringsten Berechtigungen** : Gewähren Sie nur den Mindestzugriff oder die Mindestberechtigungen, die für die Ausführung bestimmter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgaben erforderlich sind, und begrenzen Sie potenzielle Schäden durch gefährdete Accounts oder Systeme.“

- **Verstoß annehmen** : Anstatt sich nur auf Prävention zu verlassen, gehen Sie von einem Verstoß aus, und konzentrieren Sie sich auf proaktive Erkennung, Eindämmung und Reaktion.

CA bietet die Möglichkeit, die Step-up-Authentifizierung oder erneute Authentifizierung basierend auf den Daten zu erzwingen, auf die Anwender zugreifen, und den Aktivitäten, die sie ausführen. Administratoren entscheiden sich für die Erstellung von Sicherheitsrichtlinien auf Tabellen- oder Datenklassenebene.

Sie können die Step-up-Authentifizierung (MFA) oder die erneute Authentifizierung (SSO – SAML oder OIDC) innerhalb einer angemeldeten Sitzung erzwingen, wenn der Anwender versucht, auf personenbezogene Daten (PII) und vertrauliche Daten zuzugreifen.

Hinweis: Sie müssen installieren **Zero Trust: Kontinuierliche Authentifizierung** (`Com.snc.Zero_Trust_Continuous_authentication`) Für die Auswahl EINER CA, die eine Lizenz erfordert.

Vorteile

Im Folgenden finden Sie einige der Vorteile der Verwendung VON CA:

- **Verbesserte Sicherheit** : Durch die kontinuierliche Überprüfung der Identität des Anwenders kann das System potenzielle Sicherheitsbedrohungen schneller erkennen und darauf reagieren.
- **Reduziertes Risiko der Kontoübernahme** : Selbst wenn ein Angreifer Zugriff auf die Sitzung eines Anwenders erhält, kann die kontinuierliche Authentifizierung verhindern, dass er auf vertrauliche Daten zugreifen kann.

Anwendungsfälle

Im Folgenden finden Sie einige der Anwendungsfälle für die Verwendung VON CA:

- Erzwingen Sie die erneute Authentifizierung, bevor Sie mithilfe verschiedener Richtlinien Zugriff auf vertrauliche Daten zulassen.
- Erzwingen Sie regelmäßige erneute Authentifizierung oder Step-up-Authentifizierung mit verschiedenen Richtlinien:
  - Verwenden Sie eine erneute Authentifizierung, die MFA des IdP und SSO des IdP enthalten kann.
  - Verwenden Sie die Step-up-Authentifizierung mit ServiceNow MFA von .

Rollen in CA

CA hat die folgenden Rollen:

- CA-Administrator (ca_admin): Möglichkeit zum Erstellen, Bearbeiten und Anzeigen von CA-Richtlinien. Konfigurieren Sie CA-Eigenschaften, und zeigen Sie Dashboards (Metriken) von CA an.
- Richtlinienadministrator (ca_Policy_admin): Möglichkeit, CA-Richtlinien zu erstellen, zu bearbeiten und anzuzeigen.
- Auditor (ca_Auditor): Möglichkeit, Dashboards (Metriken) von CA anzuzeigen. Und Richtlinien und Protokolle von CA.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um CA zu konfigurieren, müssen Sie Ihre Rolle auf erhöhen **CA_admin** Und führen Sie die Richtlinienkonfigurationen aus.

Hinweis: Alle diese 3 Rollen sind erhöhte Rollen.

Module in CA

Im Folgenden finden Sie die verschiedenen Module innerhalb der CA:

- Richtlinien : Zeigen Sie die verschiedenen erstellten Richtlinien für die kontinuierliche Authentifizierung an.
- Metriken : Zeigen Sie die verschiedenen Metriken für die kontinuierliche Authentifizierung zu KPI-Zwecken an, und verstehen Sie die Verwendung von CA in Ihrer Organisation.
- Systemeigenschaften : Verwenden Sie Systemeigenschaften, um die kontinuierliche Authentifizierung (CA) zu aktivieren und anzupassen, um Ihre Sicherheitsanforderungen für Zero Trust-Zugriff zu erfüllen.

Zugehörige Informationen

Richtlinien

Metriken

Systemeigenschaften

Vorarbeit für kontinuierliche Authentifizierung

Kontinuierliche Authentifizierung Wird Aktiviert

Kontinuierliche Authentifizierung Wird Konfiguriert

Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung

Richtlinien

Zeigen Sie die verschiedenen erstellten Richtlinien für die kontinuierliche Authentifizierung an.

Das Formular „CA-Richtlinien“ enthält die Details der CA-Richtlinien, die für die Tabelle oder Datenklasse erstellt werden. Sie können Richtliniendatensätze über die anwenderdefinierten Richtlinien verwalten.

Um auf die Seite „Richtlinien“ zuzugreifen, navigieren Sie zu **Alle** > **Kontinuierliche Authentifizierung**, Wählen Sie aus **Richtlinien** Registerkarte. Im Folgenden finden Sie die Richtliniendetails, die auf der Seite angezeigt werden:

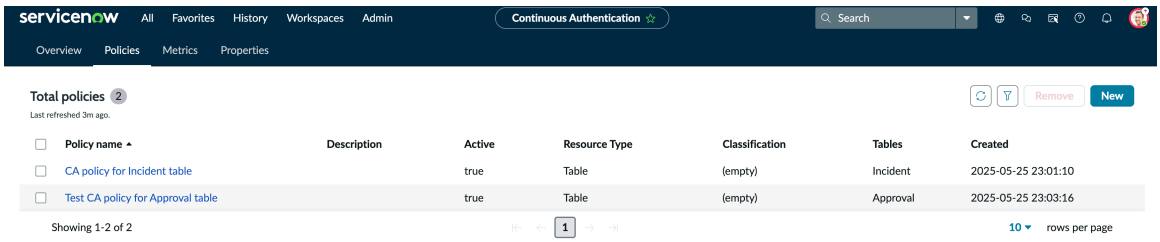
Seite „Richtlinien“

Feld	Beschreibung
Richtlinienname	Richtlinienname
Beschreibung	Richtlinienbeschreibung
Aktiv	Richtlinienstatus
Ressourcentyp	Ausgewählter Ressourcentyp, der für die Richtlinie verwendet wird
Klassifizierung	Für die Richtlinie ausgewählte Datenklassifizierung
Tabellen	Für die Richtlinie ausgewählte Tabellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Richtlinien“ (Fortsetzung)

Feld	Beschreibung
Erstellt	Richtlinienerstellungsdetails



Zugehörige Informationen

Metriken

Systemeigenschaften

Kontinuierliche Authentifizierung Erkunden

Metriken

Zeigen Sie die verschiedenen Metriken für die kontinuierliche Authentifizierung an.

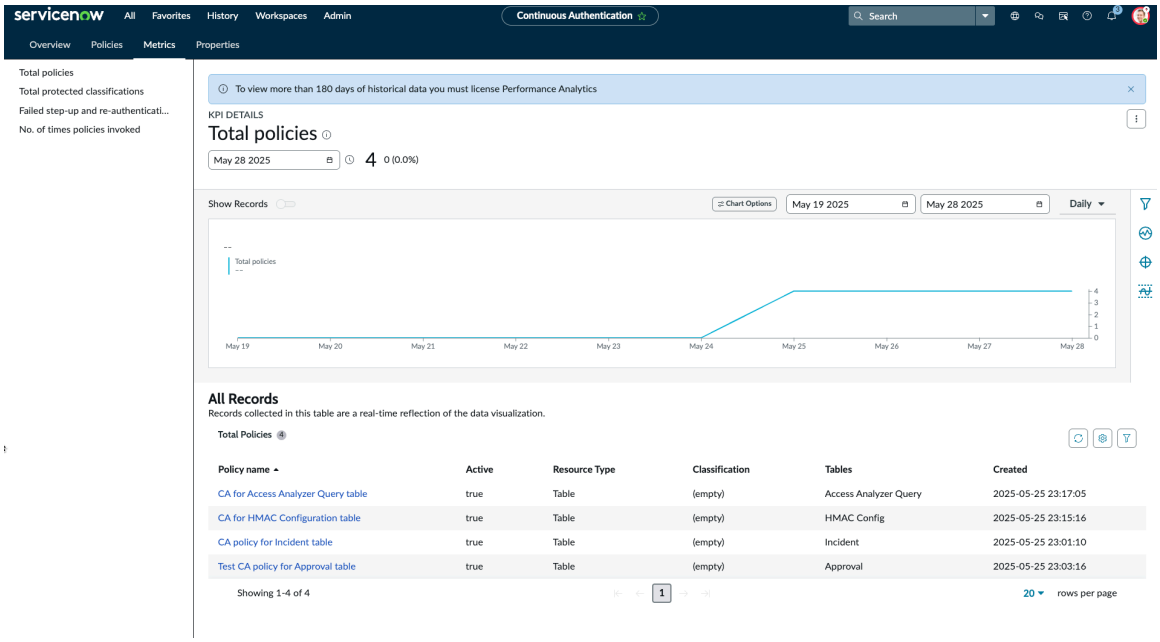
Um auf die Seite „Metriken“ zuzugreifen, navigieren Sie zu **Alle** > **Kontinuierliche Authentifizierung**, Wählen Sie aus **Metriken** Registerkarte.

Im Folgenden finden Sie die verschiedenen KPI-Details, die Sie für die kontinuierliche Authentifizierung anzeigen können:

Metriken

Metriken	Beschreibung
Richtlinien insgesamt	KPI für die Anzahl der Richtlinien für die kontinuierliche Authentifizierung, die für die Anwender erstellt werden.
Gesamtzahl der geschützten Klassifikationen	KPI für die Anzahl der Klassifizierungen, die aufgrund der Erstellung DER CA-Richtlinie geschützt sind.
Fehler beim Step-up oder erneuten Authentifizieren	KPI für die Anzahl der fehlgeschlagenen Step-up (MFA) oder erneuten Authentifizierung (SSO).
Anzahl der Aufrufe von Richtlinien	KPI für die Gesamtzahl der Aufrufe von CA-Richtlinien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Die KPI-Details werden 180 Tage lang angezeigt. Um Verlaufsdaten von mehr als 180 Tagen anzuzeigen, müssen Sie lizenzieren **Performance Analytics** .

Zugehörige Informationen

- Richtlinien
- Metriken
- Systemeigenschaften
- Kontinuierliche Authentifizierung Erkunden

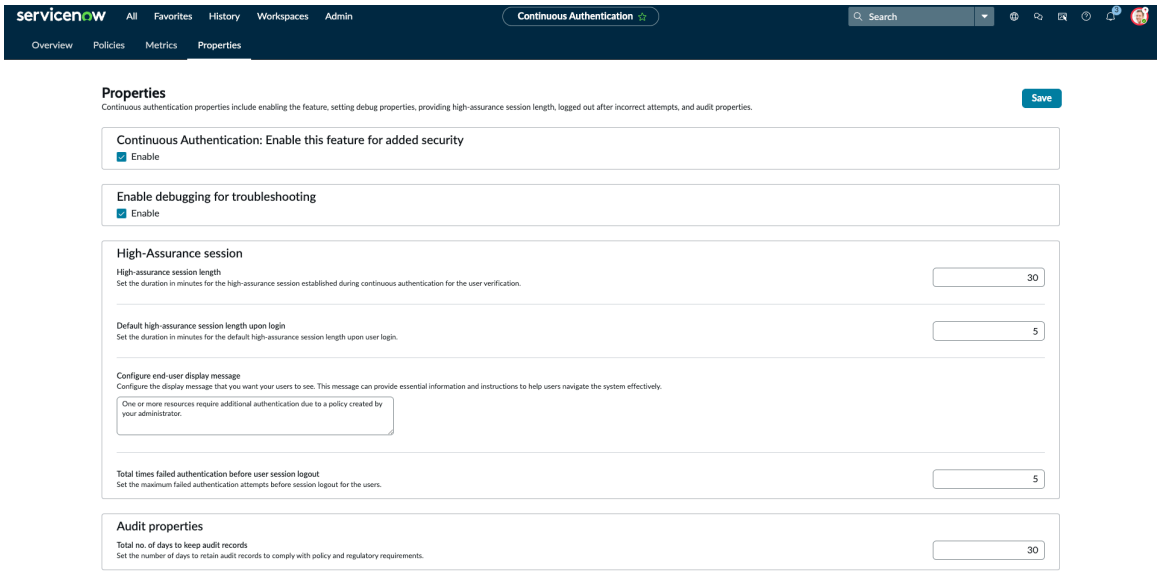
Systemeigenschaften

Verwenden Sie Systemeigenschaften, um die kontinuierliche Authentifizierung (CA) zu aktivieren und anzupassen, um Ihre Sicherheitsanforderungen für Zero Trust-Zugriff zu erfüllen.

Eigenschaften

Um auf die Eigenschaftenseite zuzugreifen, navigieren Sie zu **Alle** > **Kontinuierliche Authentifizierung**, Wählen Sie aus **Eigenschaften** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Folgenden finden Sie die verschiedenen Systemeigenschaften für CA:

Systemeigenschaften der kontinuierlichen Authentifizierung

Eigenschaft	Beschreibung
Allgemeine Eigenschaften	
Kontinuierliche Authentifizierung (*glide.zta.continuous_authentication.enabled*)	Aktivieren Sie diese Option, um die Funktion für die kontinuierliche Authentifizierung zu verwenden
Debugging Aktivieren (*glide.zta.continuous_authentication.debug.enabled*)	Aktivieren Sie diese Option, um die Debugging-Informationen im Zusammenhang mit der kontinuierlichen Authentifizierung anzuzeigen.
Hohe Sicherheit	
Länge der Sitzung mit hoher Sicherheit (*glide.zta.high_assurance.session.timeout*)	Geben Sie die hohe Länge der Assurance-Sitzung an, nach der sich die Endanwender erneut authentifizieren sollen. Standard: 10 Minuten. **Hinweis:** Der Wert muss zwischen 1 und 480 liegen.
Standardmäßige Länge der Sitzung mit hoher Sicherheit bei der Anmeldung (*glide.zta.default.high_assurance.session.lifespan*)	Geben Sie die Dauer in Minuten für die standardmäßige Sitzungslänge mit hoher Sicherheit bei der Anmeldung an. Standardwert: **5** Minuten. **Hinweis:** Die Eigenschaft gilt nur für die lokale Anmeldung.
Anzeigenachricht für Endanwender konfigurieren (*glide.zta.high_assurance.session.message*)	Geben Sie die Nachricht an, die dem Endanwender zur erneuten Authentifizierung angezeigt wird. Standardnachricht: Eine oder mehrere Ressourcen erfordern aufgrund einer von Ihrem Administrator erstellten Richtlinie zusätzliche Authentifizierung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften der kontinuierlichen Authentifizierung (Fortsetzung)

Eigenschaft	Beschreibung
Gesamtzahl der fehlgeschlagenen Authentifizierungen vor Sperre des Anwenderaccounts (*glide.zta.high_assurance.session.max.login.failed.attempts*)	Legen Sie die maximale Anzahl fehlgeschlagener Authentifizierungsversuche fest, bevor die Anwender abgemeldet werden. **Hinweis:** Der Wert muss zwischen 3 und 10 liegen.
Audit-Eigenschaften	
Gesamtzahl der Tage für die Aufbewahrung von Audit-Datensätzen (*glide.zta.continuous_authentication.audit.lifespan*)	Geben Sie die Anzahl der Tage an, die Sie die Audit-Datensätze für CA speichern möchten. **Hinweis:** Der Wert muss zwischen 1 und 180 liegen.
Gesamtzahl Von Tagen, nach denen Richtlinien gelöscht werden, nachdem sie deaktiviert wurden (*glide.zta.continuous_authentication.policy.lifespan*)	Geben Sie die Anzahl der Tage an, nach denen die CA-Richtlinien gelöscht werden.

Wichtig:

- Standardmäßig sind Sitzungen mit hoher Sicherheit für mobile App-Sitzungen nicht erforderlich, auch wenn eine Richtlinie für kontinuierliche Authentifizierung in der Quelle aktiv ist. Um dieses Verhalten zu ändern und den Zugriff aus mobilen App-Sitzungen zu blockieren, aktualisieren Sie **glide.zta.high_assurance.mobile.session.allowed** Eigenschaftswert bis Falsch .
- Die **sys_properties** , **sys_Continuous_auth_Policy** , **sys_user** Tabellen sind für CA ausgeschlossen und können der CA-Richtlinienkonfiguration nicht hinzugefügt werden.

Zugehörige Informationen

Kontinuierliche Authentifizierung Erkunden

Richtlinien

Metriken

Vorarbeit für kontinuierliche Authentifizierung

Vorarbeit für kontinuierliche Authentifizierung

Stellen Sie sicher, dass Sie die folgenden Vorarbeiten durchführen, bevor Sie die kontinuierliche Authentifizierung (CA) verwenden.

CA ist auf erstellt ServiceNow Die Sicherheitsarchitektur von Zero Trust-Zugriff, die die Sicherheit verbessern soll, indem sichergestellt wird, dass der Anwender auch nach dem ersten Authentifizierungsprozess den von ihm behaupteten bleibt.

Hinweis: Sie müssen installieren **Zero Trust: Kontinuierliche Authentifizierung** (Com.snc.Zero_Trust_Continuous_authentication) Für die Auswahl EINER CA, die eine Lizenz erfordert.

Die CA-Konfiguration kann basierend auf den folgenden Faktoren durchgeführt werden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- LDAP oder lokale Anmeldung (Anwendername und Passwort)
- SSO-Anmeldung (SAML oder OIDC) .

CA für lokale Anmeldung

Wenn sich die Anwender lokal anmelden und die Identität der Anwender überprüfen, wird MFA als Authentifizierungsmechanismus verwendet. Wenn die Anwender MFA nicht eingerichtet haben, ist es obligatorisch, das Setup abzuschließen.

Hinweis:

- In Yokohama wird MFA für Anwender für jede Anmeldung bei erzwungen ServiceNow Lokale Anmeldung wird ausgeführt.
- Stellen Sie sicher, dass die MFA-Eigenschaften aktiv und entsprechend Ihren Anforderungen konfiguriert sind. Weitere Informationen zu MFA-Eigenschaften finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

Weitere Informationen finden Sie unter Sitzung mit hoher Sicherheit für nicht-SSO-Anmeldung.

CA für SSO-Anmeldung

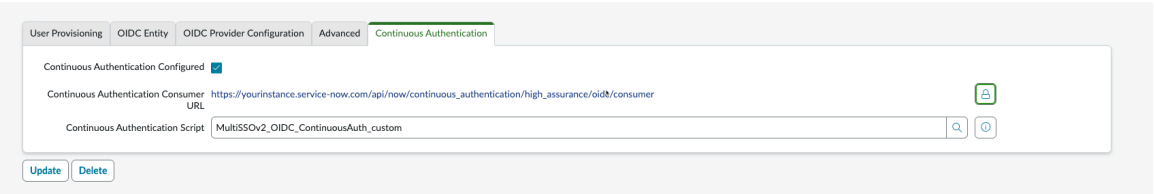
Wenn die Anwender eine SSO-basierte Anmeldung durchführen (SAML oder OIDC). Um die Identität der Anwender zu überprüfen, wird dasselbe SSO, das bei der ersten Anmeldung verwendet wurde, als erneute Verifizierung mit erneuter Authentifizierung oder als MFA des IdP angezeigt.

Hinweis:

- Sie müssen installieren **Zero Trust: Kontinuierliche Authentifizierung** (Com.snc.Zero_Trust_Continuous_authentication) Für die Auswahl EINER CA, die eine Lizenz erfordert.
- Aktivieren Sie das Single Sign-on-Installationsprogramm für Integration – mehrere Anbieter (*com.snc.integration.sso.multi.installer*)-Plugin.

Sie müssen den IDP für CA wie folgt konfigurieren:

- Aktivieren Sie das Kontrollkästchen, das für einen bestimmten Multi-SSO-Datensatz festgelegt werden muss, um zu validieren, dass dieser Satz für die Verwendung von CA bereit ist.



- Für OIDC basiert DIE CA auf der Umleitung zurück zu api/now/Continuous_authentication/High_Assurance/oidc/Consumer Endpunkt, der im IDP konfiguriert werden muss. Sowohl die erneute Authentifizierung als auch die MFA-Optionen von IdP sind verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für SAML verwenden die SSO-Datensätze das standardmäßige Wiederholungsskript für alle Identitätsanbieter (IdP), um die erneute Authentifizierung zu unterstützen.

Hinweis:

  - Dient zum Konfigurieren von STEP-up für **Okta** Sie können verwenden **ContinuousAuth_Okta_StepUp_Script** Im IdP-Datensatz. Weitere Informationen finden Sie hier Dokumentation .
  - Dient zum Konfigurieren von STEP-up für **Entra-ID** Oder **Azure** Sie können verwenden **ContinuousAuth_Azure_StepUp_Script** Und fügen Sie den erforderlichen Anspruch hinzu. Weitere Informationen finden Sie hier Dokumentation .

Weitere Informationen finden Sie unter Hohe Sicherheit für SSO-Anmeldung.

Zugehörige Informationen

Kontinuierliche Authentifizierung Erkunden

Kontinuierliche Authentifizierung Wird Aktiviert

Kontinuierliche Authentifizierung Wird Konfiguriert

Kontinuierliche Authentifizierung Wird Aktiviert

Installieren Sie zum Aktivieren der Funktion „kontinuierliche Authentifizierung“ in Ihrer -Instanz **Zero Trust: Kontinuierliche Authentifizierung** (`Com.snc.Zero_Trust_Continuous_authentication`)-Plugin.

Vorbereitungen

Erforderliche Rolle: Administrator

Mit diesem Plugin können Sicherheitsadministratoren Sicherheitsrichtlinien definieren, die eine Step-up-Authentifizierung (MFA) oder erneute Authentifizierung (SSO) innerhalb einer angemeldeten Sitzung erfordern, basierend auf den Daten, auf die der Anwender zugreift, und den von ihm ausgeführten Aktivitäten.

Sie müssen installieren **Zero Trust: Kontinuierliche Authentifizierung** (`Com.snc.Zero_Trust_Continuous_authentication`) Für die Auswahl EINER CA, die eine Lizenz erfordert.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach **Zero Trust: Kontinuierliche Authentifizierung** (`Com.snc.Zero_Trust_Continuous_authentication`) Plugin mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Zugehörige Informationen

Vorarbeit für kontinuierliche Authentifizierung

Kontinuierliche Authentifizierung Wird Konfiguriert

Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung

Kontinuierliche Authentifizierung Wird Konfiguriert

Konfigurieren Sie Richtlinien für kontinuierliche Authentifizierung (CA), um die Anwender erneut zu authentifizieren, wenn versucht wird, auf von Ihnen geschützte Ressourcen zuzugreifen.

Vorbereitungen

- Erforderliche Rolle: Admin (ca_admin)

Hinweis: Sie müssen Ihre Rolle auf erhöhen **CA_admin** .

- Sie müssen installieren **Zero Trust: Kontinuierliche Authentifizierung** (Com.snc.Zero_Trust_Continuous_authentication) Für die Auswahl EINER CA, die eine Lizenz erfordert.
- Aktivieren Sie die kontinuierliche Authentifizierung (*glide.zta.continuous_authentication.enabled*) Systemeigenschaft. Weitere Informationen finden Sie unter Systemeigenschaften.
- Aktivieren Sie das Single Sign-on-Installationsprogramm für Integration – mehrere Anbieter (*com.snc.integration.sso.multi.installer*)-Plugin.
- Machen Sie sich mit den Vorarbeiten vertraut, die vor der Konfiguration DER CA für die Instanz erforderlich sind. Weitere Informationen finden Sie unter Vorarbeit für kontinuierliche Authentifizierung.
- CA-Richtlinien können für Datenklasse oder Tabelle konfiguriert werden.

Prozedur

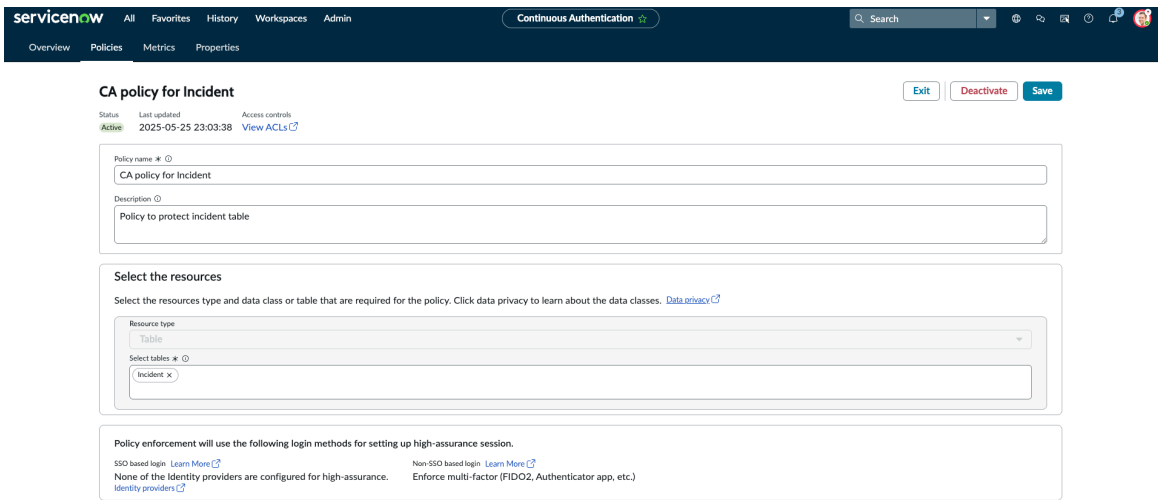
1. Navigieren zu **Alle** > **Kontinuierliche Authentifizierung**an.
2. Wählen Sie Aus **Richtlinien** Registerkarte.
3. Wählen Sie **Neu**.
4. Füllen Sie im Formular die folgenden Felder aus:

Kontinuierliche Authentifizierung

Feld	Beschreibung
Richtlinienname	Name der Richtlinie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

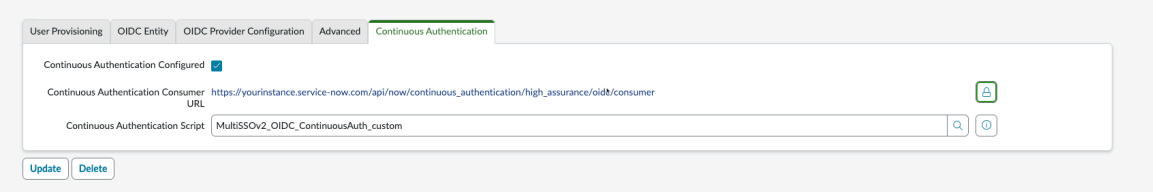
Feld	Beschreibung
Beschreibung	Generische Beschreibung der Richtlinie
Ressourcen auswählen	Optionen: ○ **Datenklasse** . Sie können eine Datenklasse erstellen und für die CA-Richtlinienkonfiguration verwenden. **Hinweis:** Weitere Informationen zum Erstellen einer Datenklasse finden Sie unter Datenklassifizierung. ○ **Tabelle** **Hinweis:** ○ Die mit Metadaten ausgewählte Tabelle zeigt einen Fehler an. ○ Sie müssen überprüfen, ob Sie den Zugriff auf die Metadatentabelle tatsächlich einschränken möchten, da dies den Konfigurationszugriff für Ihre Anwender beeinträchtigen kann. ○ Die **sys_properties** , **sys_Continuous_auth_Policy** , **sys_user** Tabellen sind für CA ausgeschlossen und können der CA-Richtlinienkonfiguration nicht hinzugefügt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können eine der Anmeldemethoden für die CA-Richtlinie verwenden:

- **SSO-basierte Anmeldung** : Geben Sie die Felder in an **Kontinuierliche Authentifizierung** Registerkarte im Identitätsanbieter-Datensatz, und legen Sie den Identitätsanbieter-Datensatz als fest **Aktiv** .



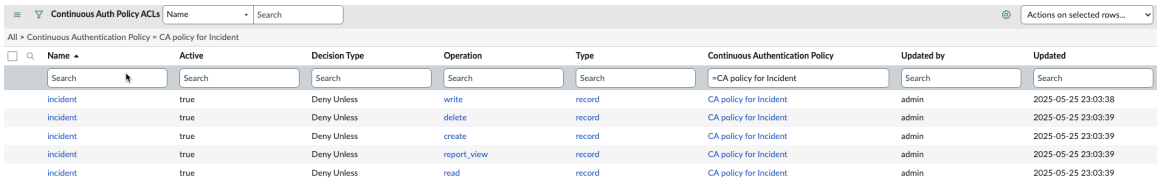
Weitere Informationen zur Konfiguration von Identitätsanbietern finden Sie unter OIDC Und SAML .

- **Nicht-SSO-basierte Anmeldung** : Wenn kein Identitätsanbieter mit Konfiguration für kontinuierliche Authentifizierung vorhanden ist, wird Multifaktor-Authentifizierung (MFA) standardmäßig als Anmeldemethode verwendet. Stellen Sie sicher, dass die MFA-Eigenschaften aktiv und entsprechend Ihren Anforderungen konfiguriert sind. Weitere Informationen zu MFA-Eigenschaften finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

5. Wählen Sie Aus **Speichern Und Aktivieren** .

Ergebnis

Basierend auf den für die Konfiguration bereitgestellten Details wird DIE CA-Richtlinie mit der Zugriffssteuerungsliste (ACLs) für die ausgewählte Tabelle oder Datenklasse erstellt. Sie können die Details der erstellten ACLs anzeigen, indem Sie auswählen **Zeigen Sie ACLs an** Auf der Richtlinienseite.

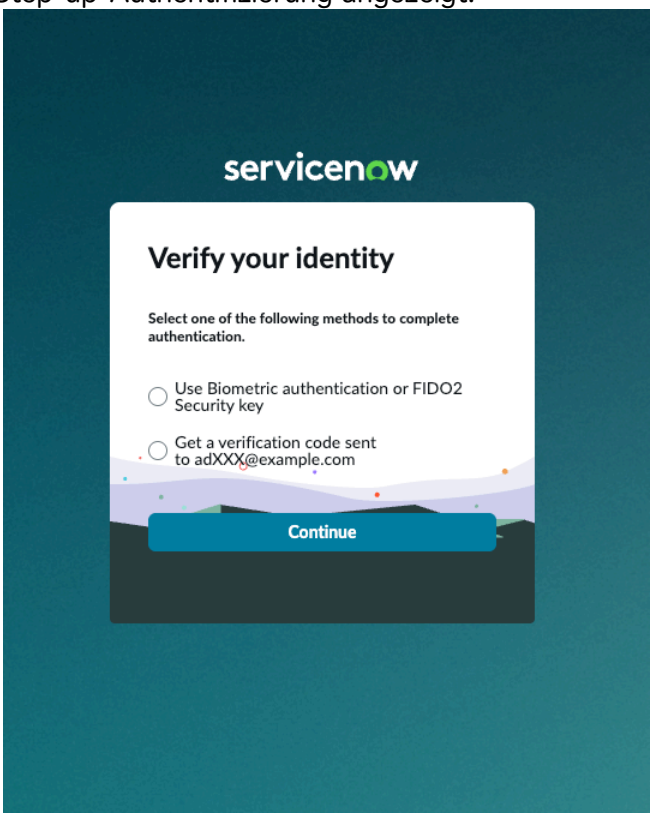


Name	Active	Decision Type	Operation	Type	Continuous Authentication Policy	Updated by	Updated
incident	true	Deny Unless	write	record	CA policy for Incident	admin	2025-05-25 23:03:38
incident	true	Deny Unless	delete	record	CA policy for Incident	admin	2025-05-25 23:03:39
incident	true	Deny Unless	create	record	CA policy for Incident	admin	2025-05-25 23:03:39
incident	true	Deny Unless	report_view	record	CA policy for Incident	admin	2025-05-25 23:03:39
incident	true	Deny Unless	read	record	CA policy for Incident	admin	2025-05-25 23:03:39

Die erstellte CA-Richtlinie fordert den Anwender basierend auf den folgenden Szenarien zur Authentifizierung auf, auf die Tabelle oder Datenklasse zuzugreifen, die Sie mit der Richtlinie geschützt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

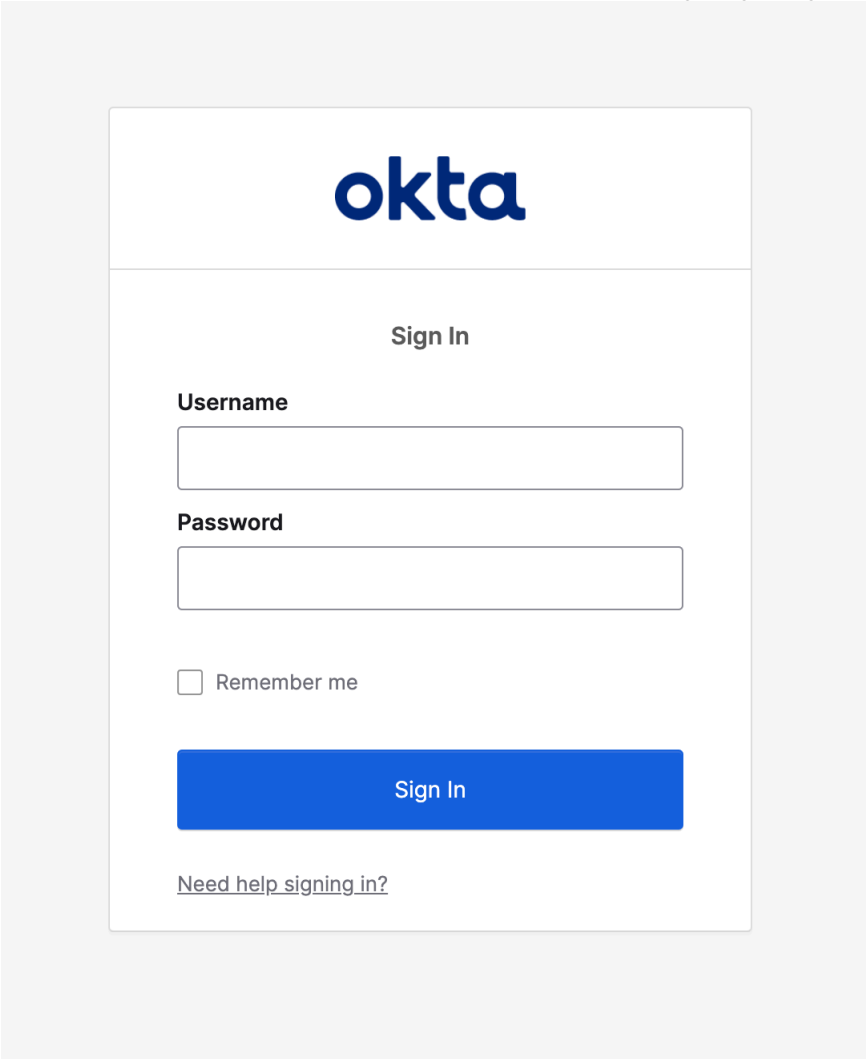
- Anwender, der sich lokal angemeldet hat, um sich bei der Instanz anzumelden, wird mit Plattform-MFA zur Step-up-Authentifizierung angezeigt.



Hinweis: Der zuletzt verwendete MFA-Faktor von Anwendern wird zur Authentifizierung angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwender, der SSO-Anmeldung (OIDC oder SAML) durchgeführt hat, um sich bei der Instanz anzumelden, wird mit SSO zur erneuten Authentifizierung angezeigt.



Für den Anwender wird jetzt eine Sitzung mit hoher Sicherheit eingerichtet. Sitzung mit hoher Sicherheit ist auf die Länge der Sitzung mit hoher Sicherheit (`glide.zta.high_assurance.session.timeout`) Systemeigenschaft. Wenn die Sitzungszeit mit hoher Sicherheit die Eigenschaftslänge überschreitet, wird der Anwender zur erneuten Authentifizierung oder zur Verstärkung der Authentifizierung aufgefordert.

Weitere Informationen zur End-to-End-Konfiguration der kontinuierlichen Authentifizierung für Tabellen oder Daten finden Sie unter:

- Tutorial: Kontinuierliche Authentifizierung für eine Tabelle konfigurieren.
- Tutorial: Kontinuierliche Authentifizierung für eine Datenklasse konfigurieren.

Zugehörige Informationen

Kontinuierliche Authentifizierung Erkunden

Vorarbeit für kontinuierliche Authentifizierung

Kontinuierliche Authentifizierung Wird Aktiviert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tutorial: Kontinuierliche Authentifizierung für eine Tabelle konfigurieren

Verfahren, das die End-to-End-Konfiguration der Richtlinie für die kontinuierliche Authentifizierung für eine Tabelle und die Auswirkungen auf die Anwender aufgrund der Konfigurationsänderungen beschreibt.

Vorbereitungen

- Erforderliche Rolle: Admin (ca_admin)

  Hinweis: Sie müssen Ihre Rolle auf erhöhen **CA_admin** .

- Sie müssen installieren **Zero Trust: Kontinuierliche Authentifizierung** (`Com.snc.Zero_Trust_Continuous_authentication`) Für die Auswahl EINER CA, die eine Lizenz erfordert.
- Aktivieren Sie die kontinuierliche Authentifizierung (*`glide.zta.continuous_authentication.enabled`*) Systemeigenschaft. Weitere Informationen finden Sie unter Systemeigenschaften.
- Aktivieren Sie das Single Sign-on-Installationsprogramm für Integration – mehrere Anbieter (*`com.snc.integration.sso.multi.installer`*)-Plugin.
- Machen Sie sich mit den Vorarbeiten vertraut, die vor der Konfiguration DER CA für die Instanz erforderlich sind. Weitere Informationen finden Sie unter Vorarbeit für kontinuierliche Authentifizierung.

Prozedur

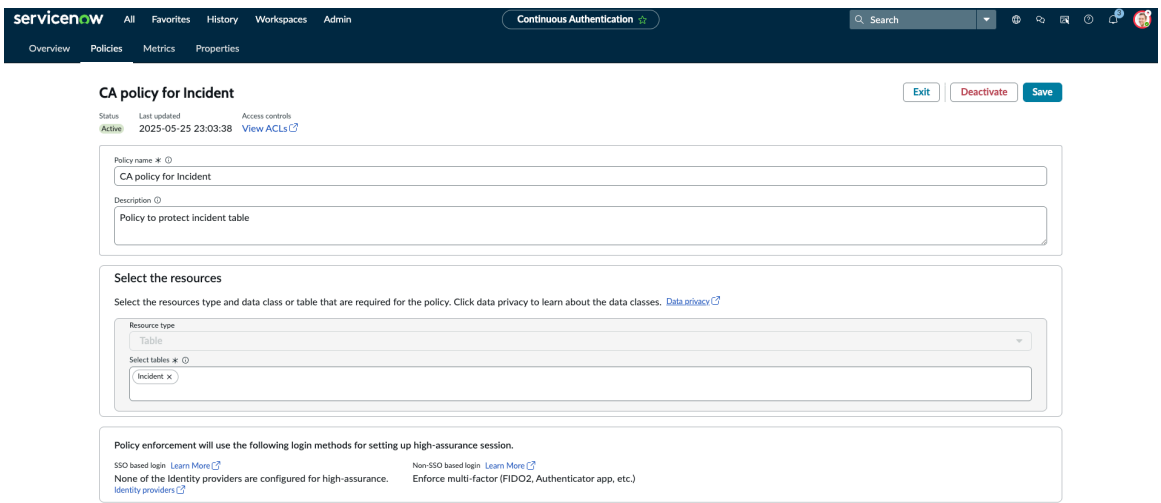
1. Navigieren zu **Alle** > **Kontinuierliche Authentifizierung**an.
2. Wählen Sie Aus **Richtlinien** Registerkarte.
3. Wählen Sie **Neu**.
4. Füllen Sie im Formular die folgenden Felder aus:

Kontinuierliche Authentifizierung

Feld	Beschreibung
Richtlinienname	Name der Richtlinie
Beschreibung	Generische Beschreibung der Richtlinie
Ressourcen auswählen	Wählen Sie aus **Tabelle** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

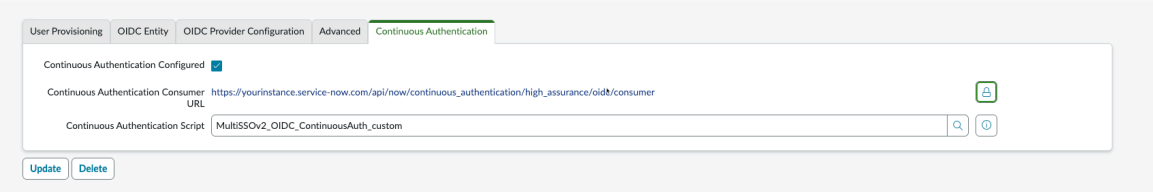
Feld	Beschreibung
	Hinweis: ○ In diesem Beispiel **Incident** Tabelle ist ausgewählt. Sie können je nach Anforderung beliebig viele Tabellen auswählen. ○ Die mit Metadaten ausgewählte Tabelle zeigt einen Fehler an. Sie müssen überprüfen, ob Sie den Zugriff auf die Metadatentabelle tatsächlich einschränken möchten, da dies den Konfigurationszugriff für Ihre Anwender beeinträchtigen kann. ○ Die **sys_properties** , **sys_Continuous_auth_Policy** , **sys_user** Tabellen sind für CA ausgeschlossen und können der CA-Richtlinienkonfiguration nicht hinzugefügt werden.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können eine der Anmeldemethoden für die CA-Richtlinie verwenden:

- **SSO-basierte Anmeldung** : Geben Sie die Felder in an **Kontinuierliche Authentifizierung** Registerkarte im Identitätsanbieter-Datensatz, und legen Sie den Identitätsanbieter-Datensatz als fest **Aktiv** .



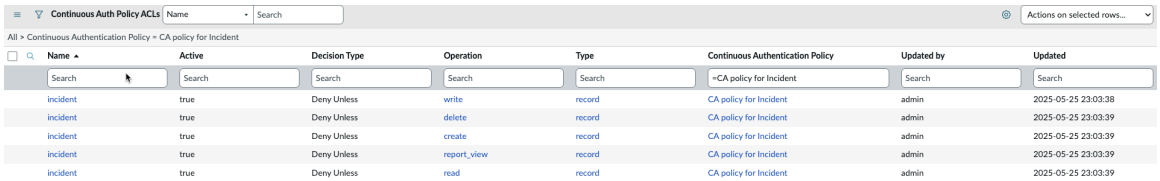
Weitere Informationen zur Konfiguration von Identitätsanbietern finden Sie unter OIDC Und SAML .

- **Nicht-SSO-basierte Anmeldung** : Wenn kein Identitätsanbieter mit Konfiguration für kontinuierliche Authentifizierung vorhanden ist, wird Multifaktor-Authentifizierung (MFA) standardmäßig als Anmeldemethode verwendet. Stellen Sie sicher, dass die MFA-Eigenschaften aktiv und entsprechend Ihren Anforderungen konfiguriert sind. Weitere Informationen zu MFA-Eigenschaften finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

5. Wählen Sie Aus **Speichern Und Aktivieren** .

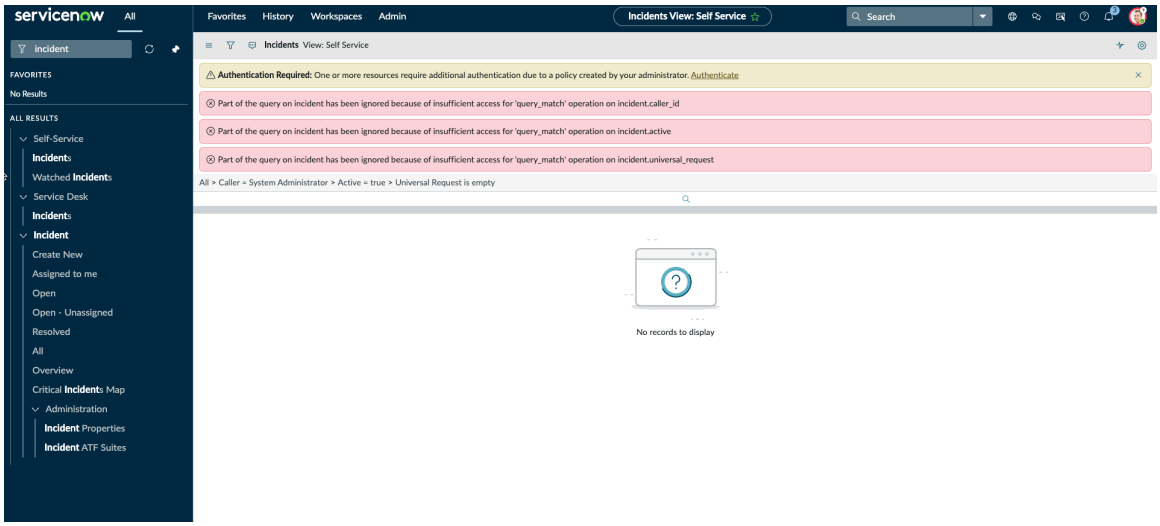
Ergebnis

Basierend auf den für die Konfiguration bereitgestellten Details wird DIE CA-Richtlinie mit der Zugriffssteuerungsliste (ACLs) für die ausgewählte Tabelle oder Datenklasse erstellt. Sie können die Details der erstellten ACLs anzeigen, indem Sie auswählen **Zeigen Sie ACLs an** Auf der Richtlinienseite.



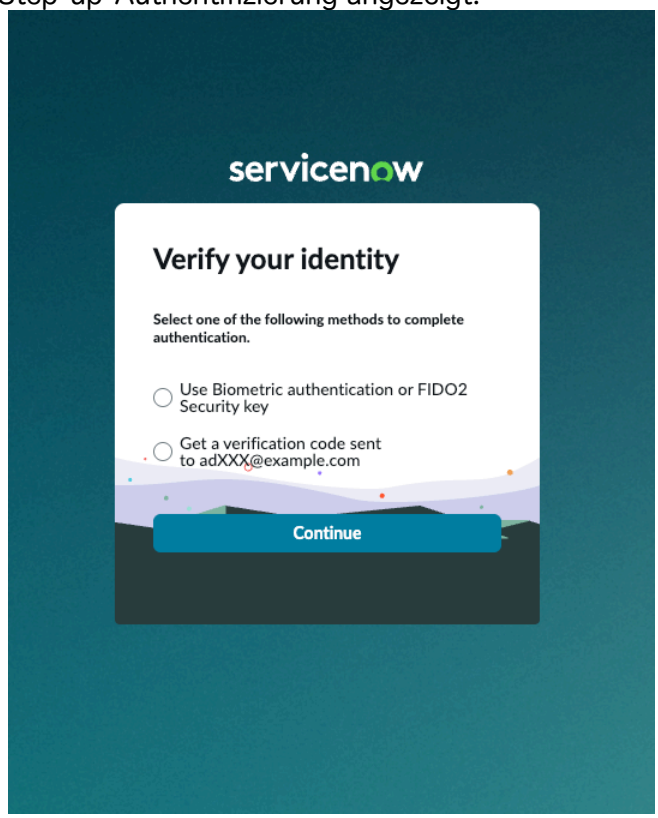
Die erstellte CA-Richtlinie fordert den Anwender zur Authentifizierung für den Zugriff auf die Tabelle auf (in diesem Fall **Incident** Tabelle), die Sie mit der Richtlinie geschützt haben. Die Anwender können auswählen **Authentifizieren** Option.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



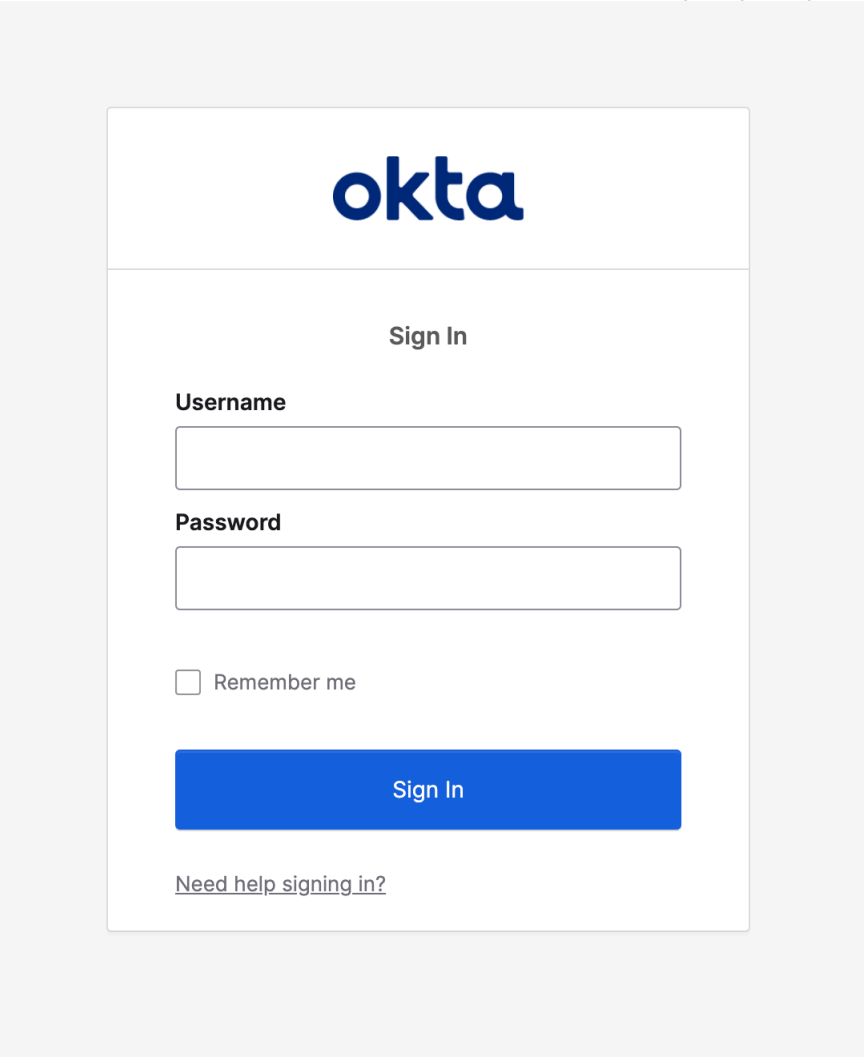
Führen Sie die Authentifizierung basierend auf den folgenden Schritten durch:

- Anwender, der sich lokal angemeldet hat, um sich bei der Instanz anzumelden, wird mit Plattform-MFA zur Step-up-Authentifizierung angezeigt.

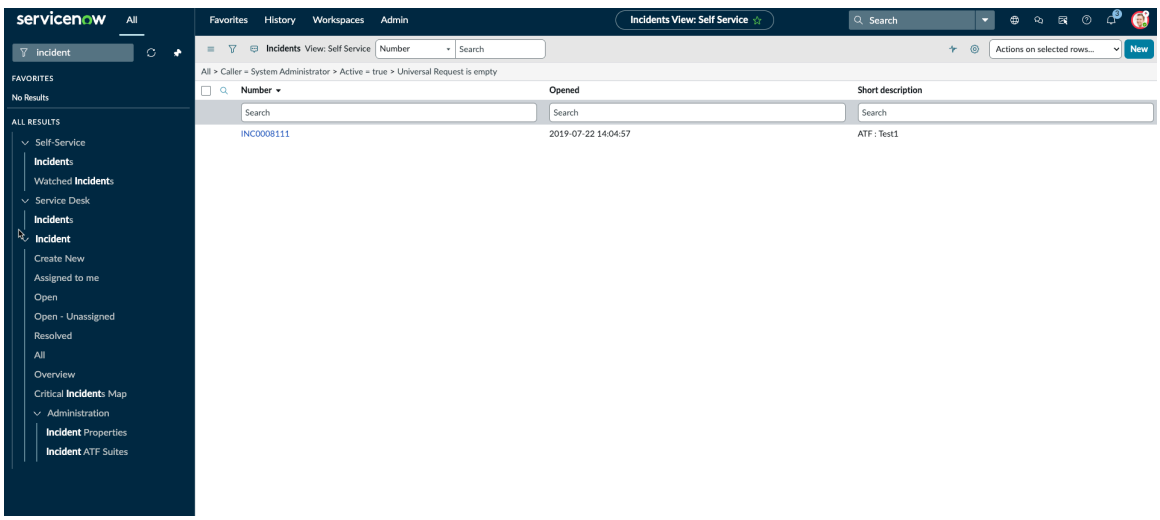


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwender, der SSO-Anmeldung (OIDC oder SAML) durchgeführt hat, um sich bei der Instanz anzumelden, wird mit SSO zur erneuten Authentifizierung angezeigt.



Nach erfolgreicher Authentifizierung wird die Tabelle angezeigt.



Für den Anwender wird jetzt eine Sitzung mit hoher Sicherheit eingerichtet. Sitzung mit hoher Sicherheit ist auf die Länge der Sitzung mit hoher Sicherheit (`glide.zta.high_assurance.session.timeout`) Systemeigenschaft. Wenn die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sitzungszeit mit hoher Sicherheit die Eigenschaftslänge überschreitet, wird der Anwender zur erneuten Authentifizierung oder zur Verstärkung der Authentifizierung aufgefordert.

Zugehörige Informationen

Kontinuierliche Authentifizierung Wird Konfiguriert

Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung

Kontinuierliche Authentifizierung Erkunden

Tutorial: Kontinuierliche Authentifizierung für eine Datenklasse konfigurieren

Verfahren, das die End-to-End-Konfiguration der Richtlinie für die kontinuierliche Authentifizierung für eine Datenklasse und die Auswirkungen auf die Anwender aufgrund der Konfigurationsänderungen beschreibt.

Vorbereitungen

- Erforderliche Rolle: Admin (ca_admin)

  Hinweis: Sie müssen Ihre Rolle auf erhöhen **CA_admin** .

- Sie müssen installieren **Zero Trust: Kontinuierliche Authentifizierung** (Com.snc.Zero_Trust_Continuous_authentication) Für die Auswahl EINER CA, die eine Lizenz erfordert.
- Aktivieren Sie die kontinuierliche Authentifizierung (*glide.zta.continuous_authentication.enabled*) Systemeigenschaft. Weitere Informationen finden Sie unter Systemeigenschaften.
- Aktivieren Sie das Single Sign-on-Installationsprogramm für Integration – mehrere Anbieter (*com.snc.integration.sso.multi.installer*)-Plugin.
- Machen Sie sich mit den Vorarbeiten vertraut, die vor der Konfiguration DER CA für die Instanz erforderlich sind. Weitere Informationen finden Sie unter Vorarbeit für kontinuierliche Authentifizierung.

Prozedur

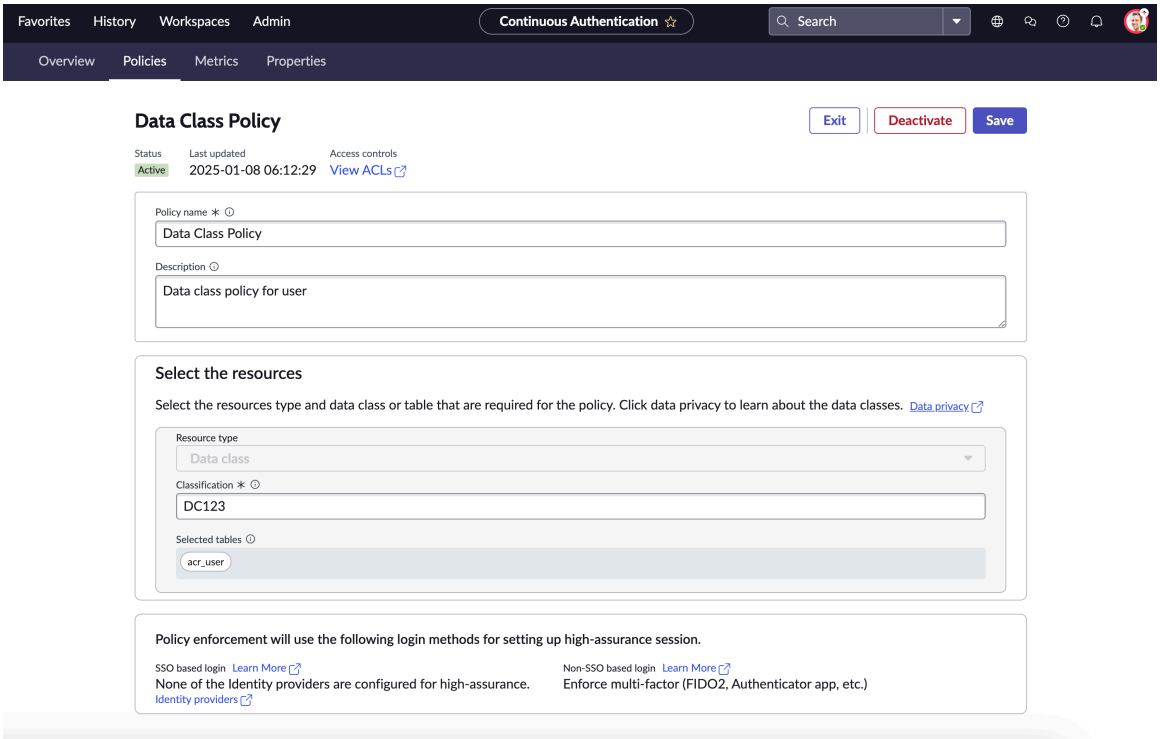
1. Navigieren zu **Alle** > **Kontinuierliche Authentifizierung**an.
2. Wählen Sie Aus **Richtlinien** Registerkarte.
3. Wählen Sie **Neu**.
4. Füllen Sie im Formular die folgenden Felder aus:

Kontinuierliche Authentifizierung

Feld	Beschreibung
Richtlinienname	Name der Richtlinie
Beschreibung	Generische Beschreibung der Richtlinie
Ressourcen auswählen	Wählen Sie aus **Datenklasse** . Sie können eine Datenklasse erstellen und für die CA-Richtlinienkonfiguration verwenden.

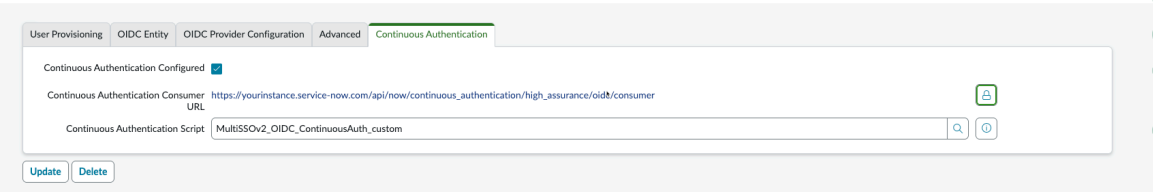
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Weitere Informationen zum Erstellen einer Datenklasse finden Sie unter Datenklassifizierung.



Hinweis: Sie können eine der Anmeldemethoden für die CA-Richtlinie verwenden:

- **SSO-basierte Anmeldung** : Geben Sie die Felder in an **Kontinuierliche Authentifizierung** Registerkarte im Identitätsanbieter-Datensatz, und legen Sie den Identitätsanbieter-Datensatz als fest **Aktiv** .



Weitere Informationen zur Konfiguration von Identitätsanbietern finden Sie unter OIDC Und SAML .

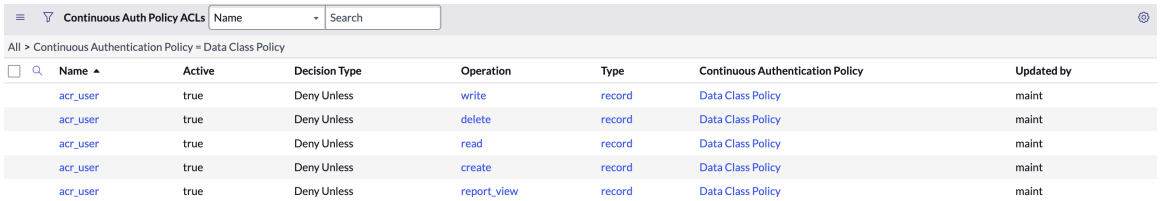
- **Nicht-SSO-basierte Anmeldung** : Wenn kein Identitätsanbieter mit Konfiguration für kontinuierliche Authentifizierung vorhanden ist, wird Multifaktor-Authentifizierung (MFA) standardmäßig als Anmeldemethode verwendet. Stellen Sie sicher, dass die MFA-Eigenschaften aktiv und entsprechend Ihren Anforderungen konfiguriert sind. Weitere Informationen zu MFA-Eigenschaften finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

5. Wählen Sie Aus **Speichern Und Aktivieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

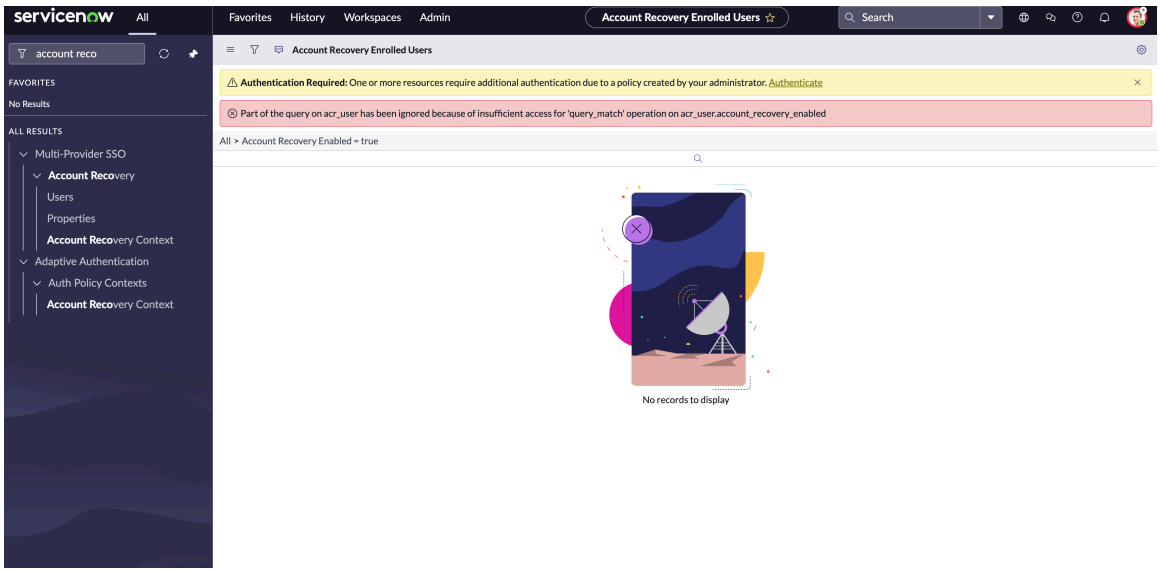
Ergebnis

Basierend auf den für die Konfiguration bereitgestellten Details wird DIE CA-Richtlinie mit der Zugriffssteuerungsliste (ACLs) für die ausgewählte Tabelle oder Datenklasse erstellt. Sie können die Details der erstellten ACLs anzeigen, indem Sie auswählen **Zeigen Sie ACLs an** Auf der Richtlinienseite.



Name	Active	Decision Type	Operation	Type	Continuous Authentication Policy	Updated by
acr_user	true	Deny Unless	write	record	Data Class Policy	maint
acr_user	true	Deny Unless	delete	record	Data Class Policy	maint
acr_user	true	Deny Unless	read	record	Data Class Policy	maint
acr_user	true	Deny Unless	create	record	Data Class Policy	maint
acr_user	true	Deny Unless	report_view	record	Data Class Policy	maint

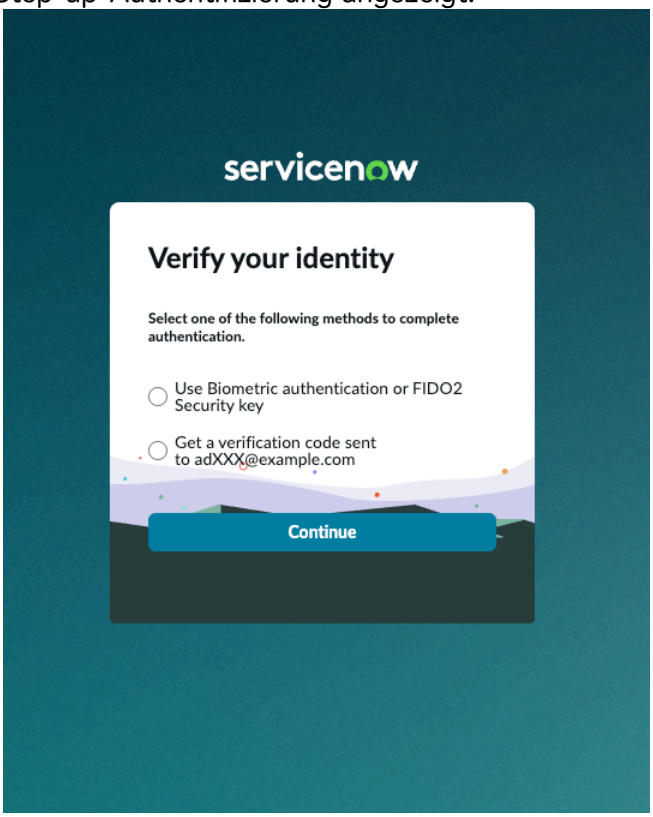
Die erstellte CA-Richtlinie fordert den Anwender zur Authentifizierung bei der Datenklasse (in diesem Fall Datenklassensatz für die Tabelle) auf **Accountwiederherstellung**), die Sie mit der Richtlinie geschützt haben. Die Anwender können auswählen **Authentifizieren** Option.



Führen Sie die Authentifizierung basierend auf den folgenden Schritten durch:

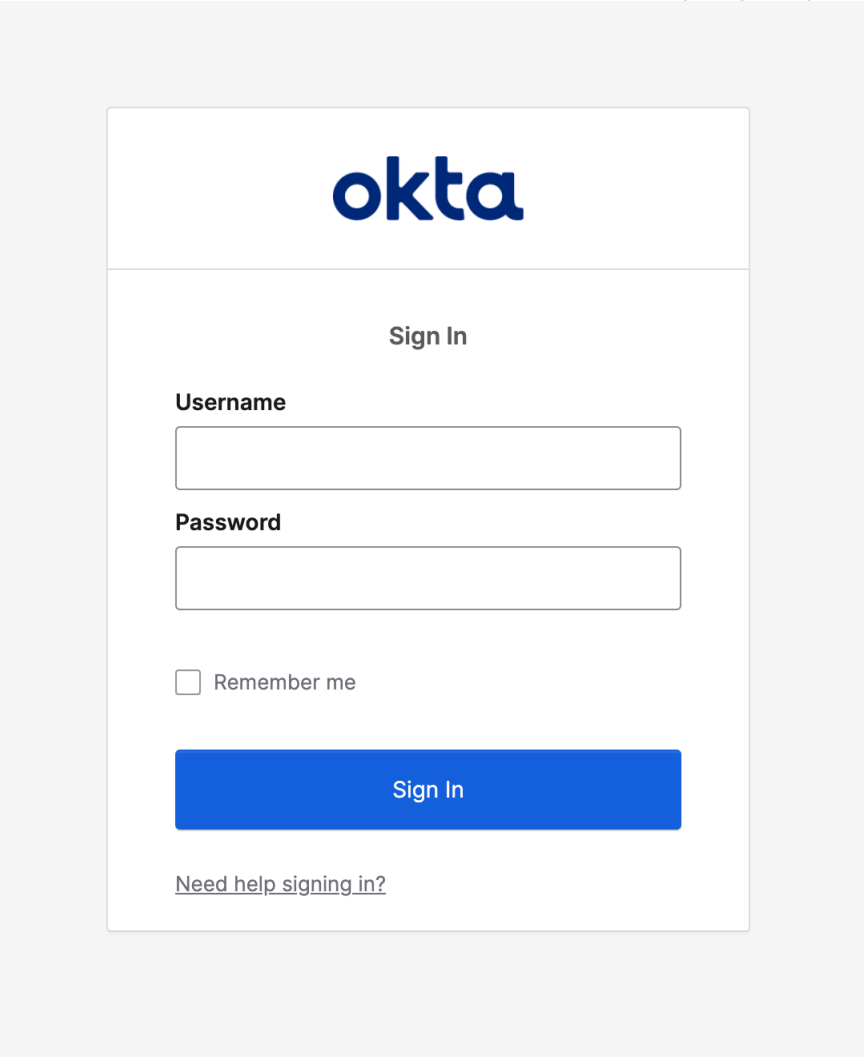
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwender, der sich lokal angemeldet hat, um sich bei der Instanz anzumelden, wird mit Plattform-MFA zur Step-up-Authentifizierung angezeigt.

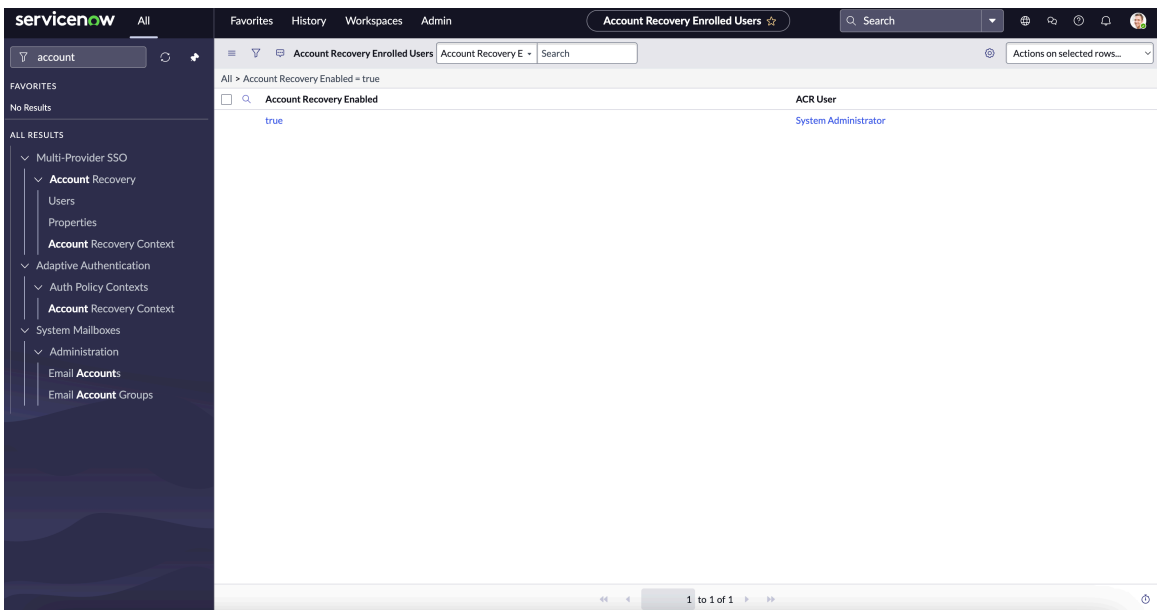


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwender, der SSO-Anmeldung (OIDC oder SAML) durchgeführt hat, um sich bei der Instanz anzumelden, wird mit SSO zur erneuten Authentifizierung angezeigt.



Nach erfolgreicher Authentifizierung wird die Tabelle mit der Datenklasse angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für den Anwender wird jetzt eine Sitzung mit hoher Sicherheit eingerichtet. Sitzung mit hoher Sicherheit ist auf die Länge der Sitzung mit hoher Sicherheit (`glide.zta.high_assurance.session.timeout`) Systemeigenschaft. Wenn die Sitzungszeit mit hoher Sicherheit die Eigenschaftslänge überschreitet, wird der Anwender zur erneuten Authentifizierung oder zur Verstärkung der Authentifizierung aufgefordert.

Zugehörige Informationen

Kontinuierliche Authentifizierung Wird Konfiguriert

Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung

Kontinuierliche Authentifizierung Erkunden

Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung

Richten Sie eine Sitzung mit hoher Sicherheit für mit ein ServiceNow Kontinuierliche Authentifizierung von .

Eine Sitzung mit hoher Sicherheit ist eine Sicherheitsmaßnahme zum Herstellen einer sicheren und vertrauenswürdigen Verbindung mit den Identitäten (Anwendern), die auf Daten zugreifen und mit einem hohen Maß an Vertrauen verifiziert werden.

ServiceNow Hohe Sicherheit von wird durch robuste Authentifizierungsmethoden erreicht, die eine erneute Authentifizierung mit Methoden wie Multifaktor-Authentifizierung (MFA) und Single Sign-on (SSO) erzwingen, während die Anwender versuchen, auf vertrauliche Daten zuzugreifen.

Wenn sich der Anwender erneut authentifiziert oder eine Step-up-Authentifizierung (MFA) durchführt, wird eine Sitzung mit hoher Sicherheit eingerichtet, die den Anwendern die Möglichkeit bietet, auf die vom CA-Administrator geschützten Daten basierend auf der CA-Richtlinienkonfiguration zuzugreifen.

Im Folgenden finden Sie die Methoden zur erneuten Authentifizierung, die verwendet werden, um eine hohe Sicherheit basierend auf der Art der Anmeldung einzurichten:

- Hohe Sicherheit für SSO-Anmeldung
- Hohe Sicherheit für nicht-SSO-Anmeldung

Vom Anwender erstellte Sitzung mit hoher Sicherheit ist basierend auf der Länge der Sitzung mit hoher Sicherheit (`glide.zta.high_assurance.session.timeout`) Vom CA-Administrator festgelegt.

Die Sitzung mit hoher Sicherheit kann basierend auf Ihren Anforderungen angepasst werden, indem Sie festlegen **Hohe Sicherheit** Systemeigenschaften:

Systemeigenschaften mit hoher Sicherheit

Feld	Beschreibung
Länge der Sitzung mit hoher Sicherheit (`glide.zta.high_assurance.session.timeout`)	Geben Sie die hohe Länge der Assurance-Sitzung an, nach der sich die Endanwender erneut authentifizieren sollen. Standard: 30 Minuten. **Hinweis:** Der Wert muss zwischen 1 und 480 liegen.
Standardmäßige Länge einer Sitzung mit hoher Sicherheit bei der Anmeldung	Geben Sie die Dauer in Minuten für die standardmäßige Sitzungslänge mit hoher Sicherheit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

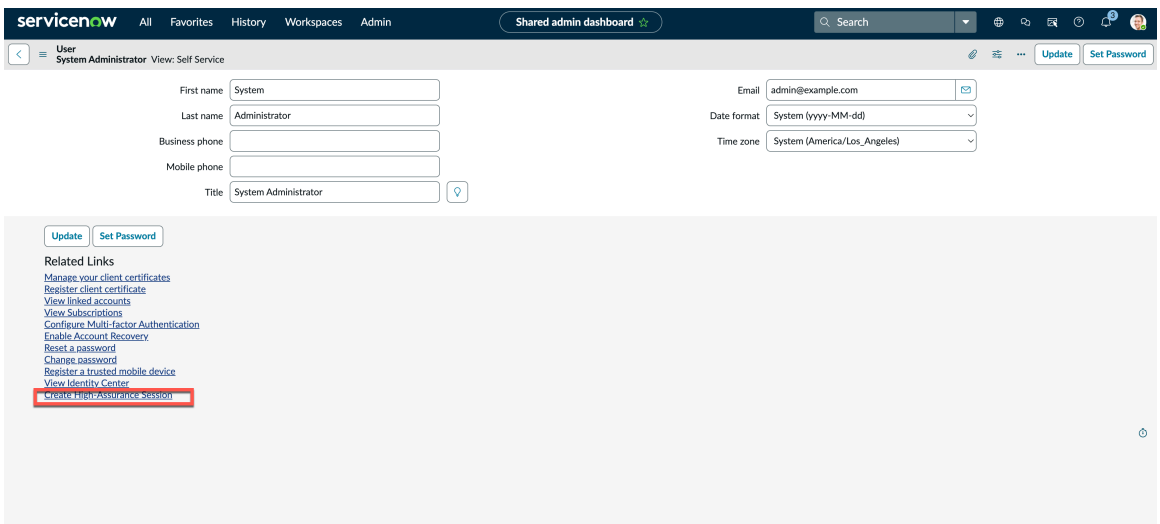
Systemeigenschaften mit hoher Sicherheit (Fortsetzung)

Feld	Beschreibung
	bei der Anwenderanmeldung an. Standardwert: **5** Minuten. **Hinweis:** Diese Eigenschaft gilt nur für nicht-sso-Anmeldungen.
Anzeigenachricht für Endanwender konfigurieren (*glide.zta.high_assurance.session.message*)	Geben Sie die Nachricht an, die dem Endanwender bei erneuten Authentifizierung angezeigt wird. Standardnachricht: Eine oder mehrere Ressourcen erfordern aufgrund einer von Ihrem Administrator erstellten Richtlinie zusätzliche Authentifizierung .
Gesamtzahl der fehlgeschlagenen Authentifizierungen vor Sperre des Anwenderaccounts (*glide.zta.high_assurance.session.max.login.failed.attempts*)	Legen Sie die maximale Anzahl fehlgeschlagener Authentifizierungsversuche fest, bevor die Anwender abgemeldet werden. **Hinweis:** Der Wert muss zwischen 3 und 10 liegen.

Sitzung mit hoher Sicherheit als Präventivmaßnahme

Anwender, die mit Daten mit hohen Berechtigungen arbeiten, z. B. Finanztransaktionen, Behördeninformationen, personenbezogene Daten, können eine Sitzung mit hoher Sicherheit als Präventivmaßnahme einrichten, um häufige Authentifizierungsbenachrichtigungen während ihrer angemeldeten Sitzung zu vermeiden.

Sitzung mit hoher Sicherheit kann von selbst erstellt werden. Um eine Sitzung mit hoher Sicherheit zu erstellen, wählen Sie aus **Anwenderprofil** > **Profil**an. In **Zugehörige Links** Abschnitt auswählen **Sitzung Mit Hoher Sicherheit Erstellen** . Verifizieren Sie Ihre Identität, um eine Sitzung mit hoher Sicherheit zu erstellen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Kontinuierliche Authentifizierung Erkunden

Vorarbeit für kontinuierliche Authentifizierung

Kontinuierliche Authentifizierung Wird Konfiguriert

Hohe Sicherheit für SSO-Anmeldung

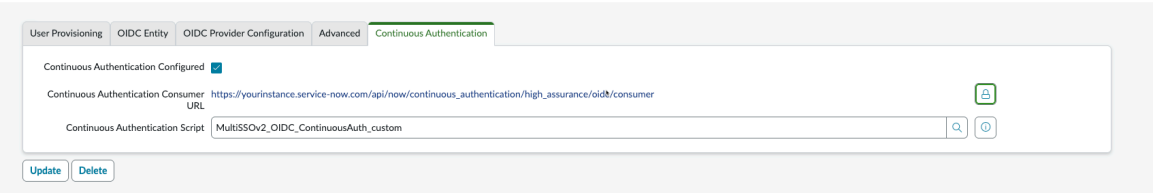
Richten Sie eine Sitzung mit hoher Sicherheit für die SSO-Anmeldung mit ein ServiceNow Kontinuierliche Authentifizierung von .

Eine Sitzung mit hoher Sicherheit ist eine Sitzung, bei der ein Anwender seine Identität verifizieren und sich für einen bestimmten Zeitraum bei einem bestimmten Identitäts- oder Identitätsanbieter authentifizieren muss.

ServiceNow Mit der Funktion „kontinuierliche Authentifizierung (CA)“ können Sie Richtlinien erstellen, die eine Sitzung mit hoher Sicherheit für Anwender erstellen, die auf personenbezogene Daten (Personally Identifiable Information, PII) oder vertrauliche Daten zugreifen, oder den Zugriff auf explizite Daten beschränken, die Sie schützen möchten.

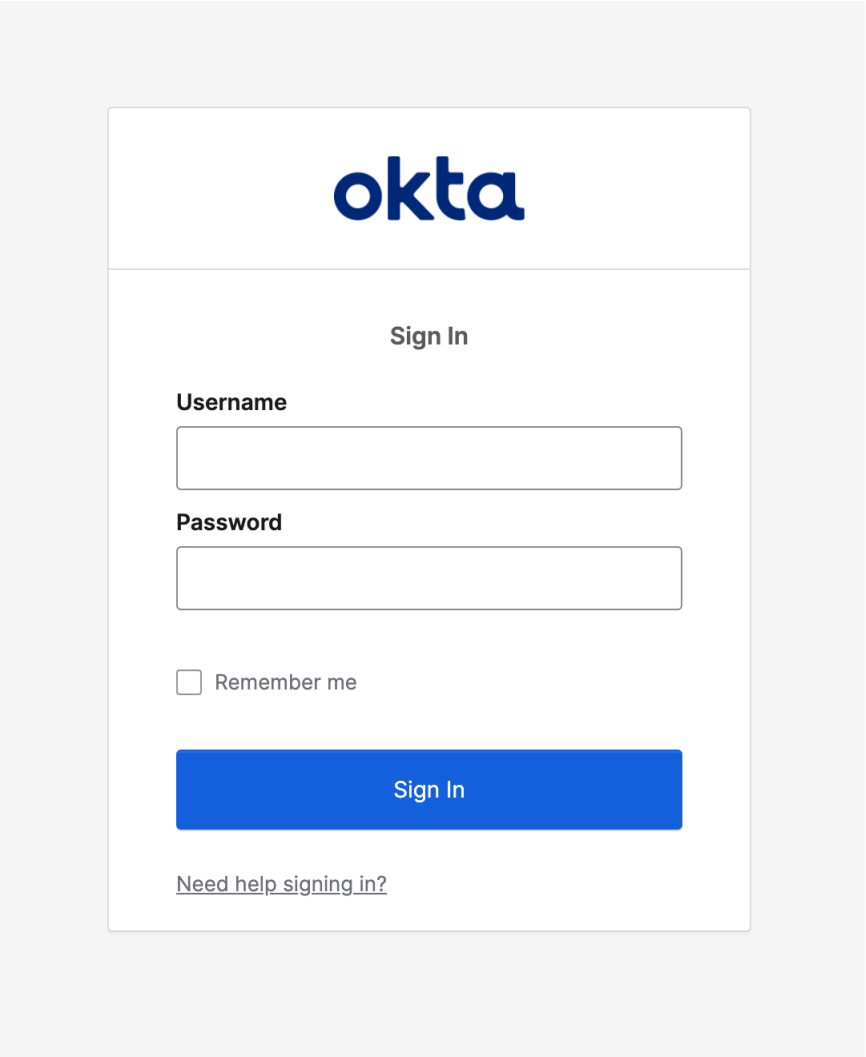
Wenn sich der Anwender erneut authentifiziert, wird eine Sitzung mit hoher Sicherheit eingerichtet, die den Anwendern die Möglichkeit bietet, basierend auf der CA-Richtlinienkonfiguration auf die vom CA-Administrator geschützten Daten zuzugreifen.

Sie können CA-Richtlinien erstellen, um die Identität der Anwender zu überprüfen und die Anwender für den Zugriff auf die von Ihnen geschützten Daten zu authentifizieren. Sie können die CA-Richtlinie konfigurieren und die Details zum Identitätsanbieter im Identitätsanbieter-Datensatz angeben, um eine Sitzung mit hoher Sicherheit einzurichten.



Die Anwender, die eine SSO-basierte Anmeldung durchführen (SAML oder OIDC), und wenn versucht wird, auf die geschützten Daten zuzugreifen, wird der Bildschirm zur erneuten Authentifizierung mit demselben SSO aufgefordert, das der Anwender bei der ersten Anmeldung verwendet hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nach erfolgreicher SSO-Authentifizierung werden den Anwendern für einen bestimmten Zeitraum die geschützten Daten angezeigt. Sie können die Eigenschaften konfigurieren, um die Zeitgrenze basierend auf Ihren Anforderungen zu ändern. Weitere Informationen finden Sie unter Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung.

Durch die erneute Authentifizierung mit SSO-Anmeldung (SAML oder OIDC) wird eine Sitzung mit hoher Sicherheit erstellt, die eine sichere und vertrauenswürdige Verbindung mit den Identitäten (Anwendern) herstellt, die auf die geschützten Daten zugreifen.

Eine für den Anwender eingerichtete Sitzung mit hoher Sicherheit ist auf die Länge der Sitzung mit hoher Sicherheit (`glide.zta.high_assurance.session.timeout`) Systemeigenschaft. Wenn die Sitzungszeit mit hoher Sicherheit die Eigenschaftslänge überschreitet, wird der Anwender zur erneuten Authentifizierung oder zur Verstärkung der Authentifizierung aufgefordert.

Zugehörige Informationen

- Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung
- Vorarbeit für kontinuierliche Authentifizierung
- Kontinuierliche Authentifizierung Wird Konfiguriert

Sitzung mit hoher Sicherheit für nicht-SSO-Anmeldung

Richten Sie eine Sitzung mit hoher Sicherheit für nicht-SSO-Anmeldungen (lokal oder LDAP) mit ein ServiceNow Kontinuierliche Authentifizierung von .

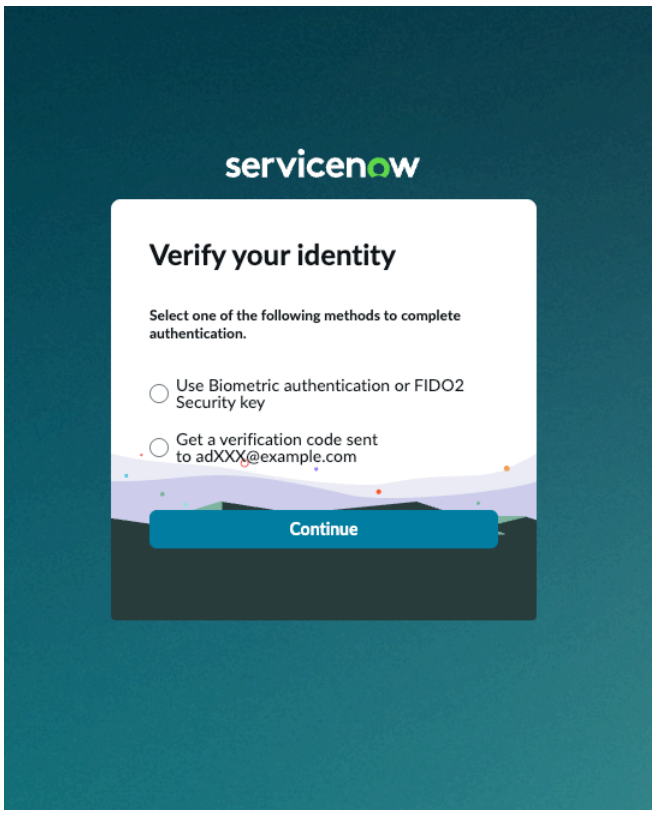
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Sitzung mit hoher Sicherheit ist eine Sitzung, bei der ein Anwender seine Identität verifizieren und sich für einen bestimmten Zeitraum bei einem bestimmten Identitäts- oder Identitätsanbieter authentifizieren muss.

ServiceNow Mit der Funktion „kontinuierliche Authentifizierung (CA)“ können Sie Richtlinien erstellen, die eine Sitzung mit hoher Sicherheit für Anwender erstellen, die auf personenbezogene Daten (Personally Identifiable Information, PII) oder vertrauliche Daten zugreifen, oder den Zugriff auf explizite Daten beschränken, die Sie schützen möchten.

Wenn der Anwender eine Step-up-Authentifizierung (MFA) durchführt, wird eine Sitzung mit hoher Sicherheit eingerichtet, die den Anwendern die Möglichkeit bietet, auf die vom CA-Administrator geschützten Daten basierend auf der CA-Richtlinienkonfiguration zuzugreifen.

Sie können CA-Richtlinien erstellen, um die Identität der Anwender zu überprüfen und die Anwender für den Zugriff auf die von Ihnen geschützten Daten zu authentifizieren. Die Anwender, die nicht-SSO-basierte Anmeldungen durchführen (lokal oder LDAP), und wenn versucht wird, auf die geschützten Daten zuzugreifen, wird der Bildschirm „Step-up Authentication“ (MFA) zu den Anwendern aufgefordert.



Nach erfolgreicher Authentifizierung werden den Anwendern die geschützten Daten für einen bestimmten Zeitraum angezeigt. Sie können die Eigenschaften konfigurieren, um die Zeitgrenze basierend auf Ihren Anforderungen zu ändern. Weitere Informationen finden Sie unter Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung.

Hinweis: Wenn die Anwender MFA nicht eingerichtet haben, ist es obligatorisch, das Setup abzuschließen.

Durch die Durchführung der Step-up-Authentifizierung (MFA) wird eine Sitzung mit hoher Sicherheit erstellt, die eine sichere und vertrauenswürdige Verbindung mit den Identitäten (Anwendern) herstellt, die auf die geschützten Daten zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine für den Anwender eingerichtete Sitzung mit hoher Sicherheit ist auf die Länge der Sitzung mit hoher Sicherheit (`glide.zta.high_assurance.session.timeout`) Systemeigenschaft. Wenn die Sitzungszeit mit hoher Sicherheit die Eigenschaftslänge überschreitet, wird der Anwender zur erneuten Authentifizierung oder zur Verstärkung der Authentifizierung aufgefordert.

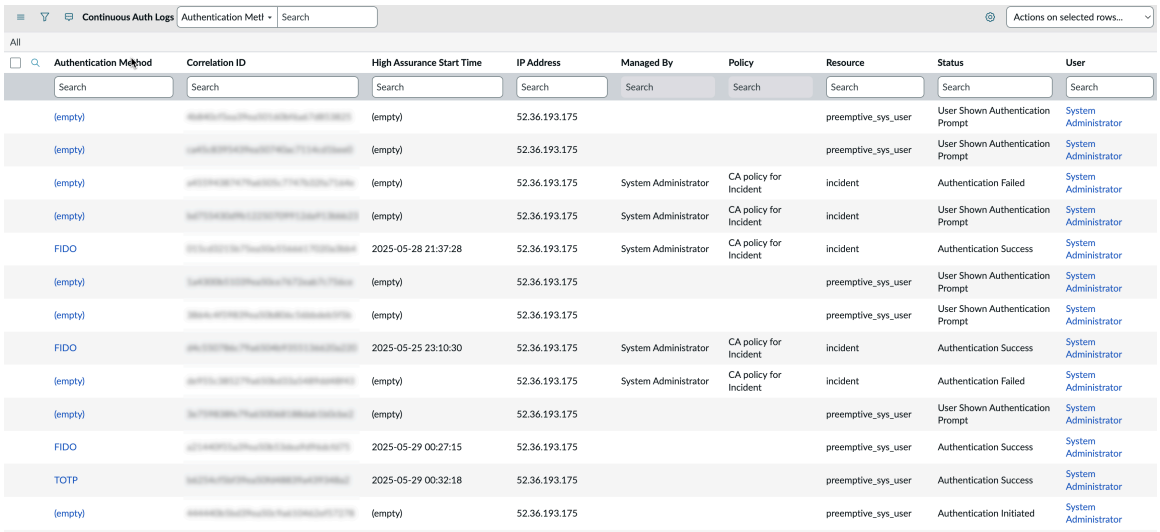
Zugehörige Informationen

- Sitzung mit hoher Sicherheit mit kontinuierlicher Authentifizierung
- Vorarbeit für kontinuierliche Authentifizierung
- Kontinuierliche Authentifizierung Wird Konfiguriert

Audit-Protokolle für kontinuierliche Authentifizierung

Beschreibt die Details zu Protokollen der kontinuierlichen Authentifizierung (Continuous Authentication, CA). In den CA-Protokollen werden alle Authentifizierungsversuche der Anwender angezeigt.

Die Audit-Informationen für das CA-Protokoll sind in verfügbar **Continuous_auth_log.LIST** Seite. Sie können eingeben **Continuous_auth_log.LIST** In der Navigation zum Anzeigen der CA-Protokolle.



Auf der Protokollseite werden Informationen zur Authentifizierungsmethode, zur Korrelations-ID und andere Details im Zusammenhang mit der Sitzung des Anwenders angezeigt.

Domänentrennung für Service Provider

Mit der ServiceNow Platform können Service Provider (SPs) ihren Kunden ein schnelleres Onboarding bieten, die Compliance erfüllen und ihre Daten durch Domänentrennung schützen. Sie können Client-Daten, Prozesse und Berichte in logische Gruppierungen unterteilen, die als Domänen bezeichnet werden. SPs steuern, wer welche Inhalte sieht und darauf zugreifen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über die Domänentrennung.

Konfigurieren



Konfigurieren Sie Die Domänentrennung.

Referenz



Ruft Details zur Domänentrennung ab.

Analysieren



Erfahren Sie mehr über die Analyse der Domänentrennung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung erkunden

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logisch definierte Domänen trennen.

Die Domänentrennung ist am besten geeignet für Kunden, die:

- absolute Datentrennung zwischen Business-Entitäten (Datentrennung) benötigen.
- Geschäftsprozessdefinitionen und Benutzerschnittstellen für jede Domäne anpassen möchten (delegierte Verwaltung).
- einige globale Prozesse und globale Berichte in einer einzigen Instanz verwalten.
- Trennen Sie Daten zwischen Service Providern, Kunden, Partnern oder Unterorganisationen.
- Haben geringfügige oder moderate Prozessunterschiede zwischen Kunden.

Domänentrennung im Vergleich zu separaten Instanzen

Die Domänentrennung bietet zwar Unterstützung für mehrere Mandanten, die Mehrmandantenfähigkeit ist jedoch auch weiterhin in einer einzelnen Instanz enthalten. Einige globale Eigenschaften, Daten und Prozesse werden über alle Domänen hinweg gemeinsam genutzt. Zum Beispiel mit dem System *Merken Sie sich* Auf der Anmeldeseite des Systems ist global und kann nicht pro Domäne angegeben werden.

Wenn Sie eine vollständige und vollständige Trennung aller Systemeigenschaften benötigen und keine globalen Berichterstellungen oder globalen Prozesse erfordern, sind separate Instanzen die beste Option.

Datentrennung

Mitglieder einer Domäne sehen nur die Daten, die in ihrer Domäne enthalten sind, oder die untergeordneten Domänen, die in der Domänenhierarchie niedriger sind. Standardmäßig sind alle Anwender und alle Datensätze Mitglieder der globalen Domäne, es sei denn, ein Administrator weist sie einer bestimmten Domäne zu. Sobald Sie einer Domäne einen Benutzer oder einen Datensatz zugewiesen haben, vergleicht die Instanz die Domäne des Benutzers mit der Domäne des Datensatzes, um zu bestimmen, ob der Benutzer den Datensatz aufrufen kann.

ServiceNow-Anwendungen sind mit den folgenden inkrementellen Supportstufen definiert. Diese Ebenen basieren auf der Perspektive tatsächlicher Anwendungsfälle und Personas.

Datentrennung : Mandanten sehen nur Daten, für die sie Berechtigungen haben. Mandanten können Zugriff auf andere Mandantendaten gewährt werden, können jedoch keine Mandantendaten abfragen, wenn sie keinen Zugriff haben.

UI-Trennung : Unterstützt eine mandantenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.

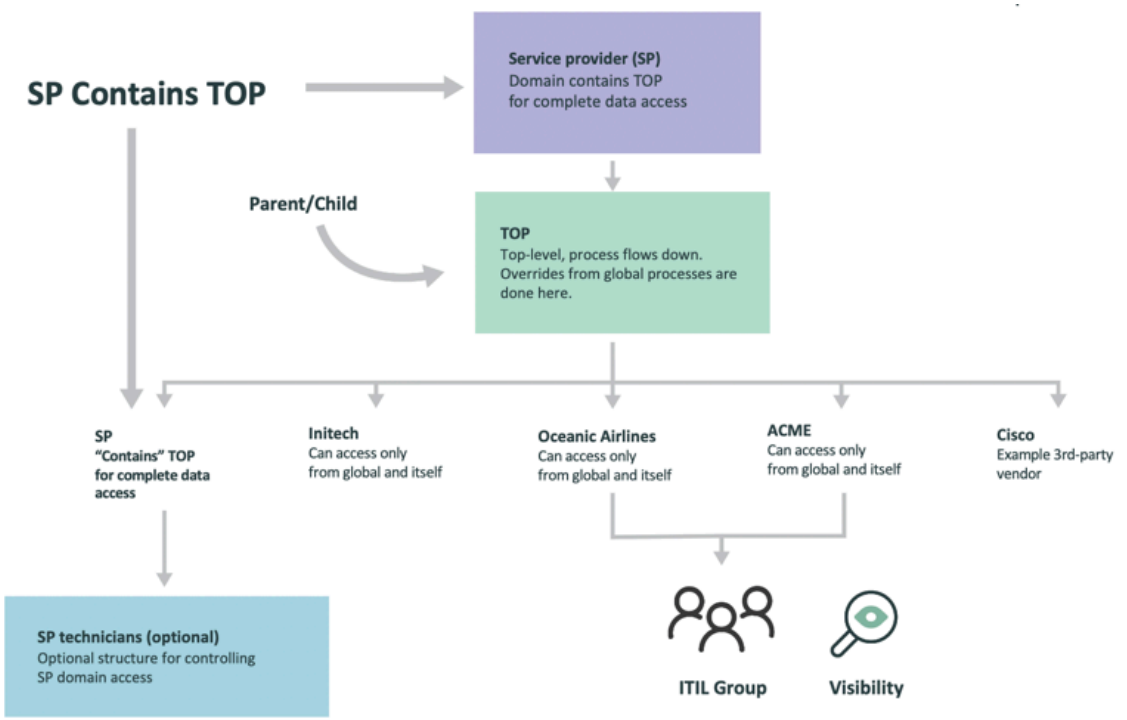
Geschäftslogik-Trennung : Sie können mandantenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Geschäftsregeln, Clientskripts, UI-Richtlinie und UI-Aktionen erstellen.

Hierarchische Modellierung : Nested-Multi-Tenancy, damit übergeordnete Mandanten auf untergeordnete Mandantenressourcen zugreifen können. Die Geschäftslogik für übergeordnete Mandanten wird automatisch für untergeordnete Mandanten ausgeführt und kann auf jeder Ebene überschrieben werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mandantenübergreifende Intelligenz (Domänenbereich) : Verarbeitet automatisch die Daten, Metadaten, Geschäftslogik und Verarbeitungskontext für Mandanten, die Zugriff auf zusätzliche Mandantendaten haben.

Im Allgemeinen sind Daten, die auf einer höheren Ebene in der Domänenhierarchie definiert sind, auf niedrigeren Ebenen in der Hierarchie nicht sichtbar.

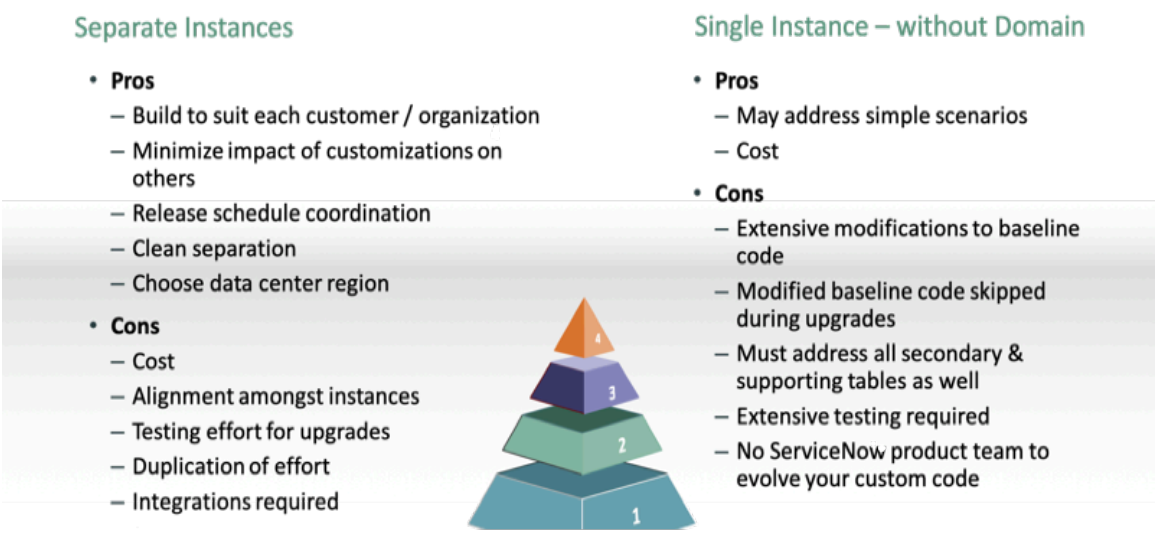


Domänenpfadmigration

Domänenpfade werden für alle Kunden verwendet. Domänennummerierung wird nicht verwendet. Kundenservice und Support Kann beim Upgrade helfen.

Alternativen zur Domänentrennung

Separate Instanzen sind eine häufige Alternative zur Domänentrennung. Dies bietet ein hohes Maß an Flexibilität bei der Erfüllung der Anforderungen für Kunden und Stakeholder mit geringen bis keinen Auswirkungen auf andere.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Bevor Sie die Domänentrennung aktivieren, wenden Sie sich an Ihren Vertreter, um sicherzustellen, dass sie für Ihre Umgebung geeignet ist. Die Domänentrennung fügt einen Verwaltungsaufwand hinzu. Obwohl sie deaktiviert werden kann, kann sie nicht aus einer Instanz entfernt werden.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Plugin „Domänentrennung“

Konfiguration, die an interne oder externe Kunden delegiert werden kann

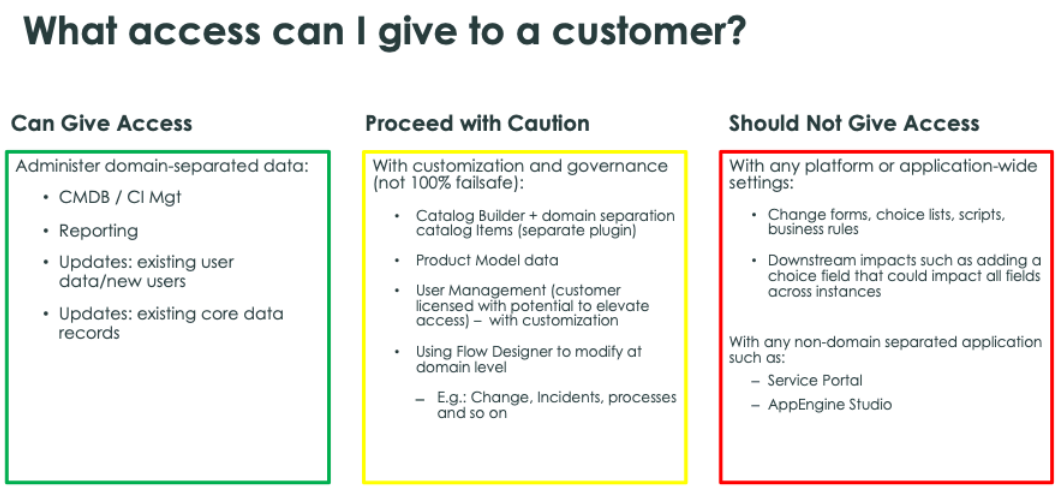
Domänentrennung Ist so konzipiert, dass sie geben ServiceNow® Service Provider (SPS) die Möglichkeit, die Services zu konfigurieren, die sie ihren Kunden anbieten. Es ist nicht so konzipiert, dass Kunden diese Services selbst verwalten können, mit Ausnahme einiger Bereiche, die in diesem Thema beschrieben werden.

Übersicht

Es ist für SP-Kunden sicher, allein Daten in ihrer Domäne zu verwalten, die sich nicht auf die Lizenzierung oder andere Kunden auswirken. Zum Beispiel ist es für einen Kunden sicher, neue Berichte zu erstellen oder Konfigurationselemente zu verwalten, aber es ist nicht sicher, dass er Felder, Auswahlmöglichkeiten, Geschäftsregeln und andere Prozesse anpassen kann, bei denen sie sich auf andere Kunden in derselben Instanz auswirken können.

Die ServiceNow Administratorrollen des Basissystems und ihre Zugriffssteuerungen auf dem ServiceNow Die Plattform ist für ein einzelnes Administratorteam pro Instanz konzipiert. Beispielsweise wird einer der Ressourcen des SP die Rolle „Domain_admin“ gewährt, um alle Domäneneinstellungen für die Instanz zu verwalten und neue Domänen zu erstellen. Für alle domänenspezifischen Administratoraufgaben sollte der SP nach Bedarf neue „Kundenadministrator“-Rollen und Zugriffssteuerungen erstellen, um seinen Kunden bestimmten Zugriff zu gewähren.

Die folgende Abbildung zeigt eine Übersicht über allgemeine Administratorfunktionen in verschiedenen Kategorien, was für einen Kunden sicher ist.



Kann Zugriff gewähren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele:

- CI-Datenverwaltung in der CMDB
- Berichterstellung
- Updates für vorhandene Anwenderdaten oder neue Anwender ohne Rollen
- Updates für vorhandene Kerndatensätze wie Abteilung, Gruppe, Standort, Kostenstelle oder neue Gruppen ohne Rollen und neue Abteilungen/Kostenstellen/Standort.

Fahren Sie mit Vorsicht fort

Beispiele:

- Katalogelemente: Um kundenspezifische Katalogelemente zu erstellen, die vom Kunden aktualisiert werden können, können zwei Funktionen zusammen verwendet werden: Domänentrennung für Katalogelemente (Domänentrennung und Servicekatalog) Ermöglicht es dem Instanzbesitzer, Elemente in der Domäne des Kunden zu erstellen. Der Instanzbesitzer kann eine Rolle erstellen, mit der Kunden Safe-Felder wie Preis, Beschreibung und Bilder aktualisieren können. Die Katalog-Generator (Neu im Quebec-Release), gibt dem SP-Administratorteam die Möglichkeit, Elementvorlagen zu erstellen, die sicher an Kunden verteilt werden können, um neue Elemente innerhalb ihrer Domäne aus einer verbindlichen UI-Experience zu erstellen.
- Anwender-/Gruppenverwaltung: Es ist sicher, eine „Kundenadministrator“-Rolle zu erstellen, die Anwenderdatensätze erstellen und ändern kann. Das Hinzufügen und Entfernen von Rollen kann sich jedoch auf Sicherheit und Lizenzierung auswirken. Im Basissystem gibt es keine Möglichkeit, Rollen zu unterteilen, die für einen Kunden sicher sind, ihnen zu gewähren. Das Gleiche gilt für die Erstellung und Änderung von Gruppen. Die Gruppe selbst kann zwar geändert werden, das Hinzufügen oder Subtraktion von Rollen sollte jedoch gesteuert werden.
- Flow Designer : ServiceNow Flow Designer Ist das Erstellungstool, das zum Erstellen eines Prozesses (Workflows) für Tabellen verwendet wird. Die Rolle „Flow_Designer“ bietet Kunden skriptfreien Zugriff zum Erstellen von Flows. Sie können jeden Flow in Domänen darüber in der Hierarchie lesen und klonen. Sie können Flows in ihrer Domäne erstellen und ändern. Dies kann jedoch nicht in einem Silo geschehen. Jeder, der sich auf den Prozess auswirken kann, muss dem globalen Administratorteam für Governance hinzugefügt werden, damit Prozesse einander nicht abbrechen oder andere Konflikte verursachen.

Gewähren Sie keinen Zugriff

Das Verständnis der Funktionsweise von Auswahlfeldern ist hilfreich, um zu verstehen, warum sie nur vom SP-Administratorteam verwaltet werden sollten.

- Struktur eines Auswahlfelds: Auswahlfeldwerte werden in der Tabelle „sys_choice“ gespeichert und gruppiert nach: Tabelle, Domäne und Sprache.

  Zum Beispiel die **Status** Das Feld in einer Aufgabe ist für jede Tabelle verfügbar, die eine Aufgabe erweitert. Das bedeutet, dass jede Tabelle eigene Werte haben kann, diese Werte mit der Domäne multipliziert werden können, und die Domänenwerte können mit der Sprache multipliziert werden.

  Alle Werte für **Status** In allen Tabellen werden Domänen und Sprachen als Werte für betrachtet **Status** Feld.

- Funktionsweise von Änderungen an Auswahlfeldern: Wenn ein Auswahlfeld aktualisiert wird, wird eine Nutzlast mit allen Werten für dieses Feld (Tabellen, Domänen, Sprachen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erstellt. Wenn Sie diese Nutzlast auf einer Instanz installieren, werden alle vorhandenen Werte für das Feld gelöscht, und die neuen Werte werden geladen. Dadurch wird sichergestellt, dass keine doppelten Einträge oder verbleibenden Werte vorhanden sind, die nicht mehr gültig sind.

Aus diesem Grund ist es nicht möglich, einem Kunden in einer domänengetrennten Instanz die Möglichkeit zu geben, Auswahlfelder direkt zu aktualisieren, da dies sich auf die gesamte Instanz auswirken würde. Darüber hinaus können Sie Auswahlmöglichkeiten nicht direkt in einer Produktionsinstanz aktualisieren, da alle importierten Update-Sätze, die sich auf dieses Feld auswirken, die vorhandenen Auswahlmöglichkeiten überschreiben würden. In einigen Fällen können Auswahlfelder Prozesse selbst steuern, was zum Bruch führen würde, wenn ein Kunde diese Felder ändern würde.

Weitere Informationen finden Sie unter:

- Anwenderverwaltung erkunden
- Eine ACL-Regel erstellen
- Lernpfad für Service Provider an der ServiceNow University
- Domänentrennung für Service Provider
- Service Provider-Konzepte
- Anwendungsunterstützung für Domänentrennung
- Release-Hinweise zur Domänentrennung

Domänenzuweisung

Standardmäßig fügt die Domänentrennung Tabellen und ihren Erweiterungen ein Domänenfeld hinzu.

Sie können die Domänentrennung auch auf alle neuen Tabellen erweitern, die Sie erstellen, indem Sie eine hinzufügen **sys_Domain** Feld zur Wörterbuchdefinition der Tabelle. Standardmäßig trennt das System nur Plattform- und Baselineanwendungstabellen nach Domäne, sofern angemessen.

⚠ **Warnung:** ServiceNow Empfiehlt keine Domänentrennungstabellen (beliebige Tabellen mit dem Präfix „sys_“ wie die Tabellen „Wörterbucheintrag“ [sys_dictionary] und „Wörterbucheintrag überschreiben“ [sys_dictionary_override]), da dies zu unerwarteten Ergebnissen führen kann.

Jedem Datensatz ist eine einzelne Domäne zugewiesen. Diese Domäne wird in gespeichert **sys_Domain** Feld. Mehrere Tabellen haben standardmäßig die **sys_Domain** Spalten und sind bereits domänengetrennt.

Der Wert von **sys_Domain** Das Feld enthält die Domäne, die dem Datensatz von einer der folgenden Elemente zugewiesen ist:

- Unternehmen, zu dem der Anwender gehört
- Business-Regel beim Erstellen des Datensatzes
- Modul, das beim Erstellen des Datensatzes verwendet wird
- Formularvorlage, die beim Erstellen des Datensatzes verwendet wird
- Domäne des übergeordneten Datensatzes
- Dem Anwenderdatensatz zugewiesene Domäne
- Domäne des Anwenders, der sie erstellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das System verhindert, dass die folgenden Tabellen domänengetrennt werden:

- Zugriffssteuerung [sys_Security_acl]
- Skripteinbindung [sys_script_include]
- Systemeigenschaft [sys_properties]
- Entitäten Der Sicherheitsausschluss-/Aufnahmeliste [sys_Security_Restricted_list]
- Wörterbucheintrag [sys_dictionary]
- Wörterbucheintrag Überschreiben [sys_dictionary_override]

Zuweisen von Anwendern zu Unternehmen

Administratoren können Anwender schnell einer Domäne zuweisen, indem sie sie einem Unternehmen zuweisen. Nachdem Anwender einer Domäne zugewiesen wurden, erben Datensätze automatisch die Domäne des Anwenders.

Wenn Bow Ruggeri beispielsweise dem ACME-Unternehmen zugewiesen wird, wird er automatisch der ACME-Domäne zugewiesen. Wenn Don Goodliffe dem Initech-Unternehmen zugewiesen wird, wird er automatisch der Initech-Domäne zugewiesen. Alle von ihnen erstellten Datensätze werden automatisch der entsprechenden Domäne hinzugefügt.

Verwenden von Business-Regeln zum Zuweisen von Domänen

Administratoren können eine Business-Regel verwenden, um beim Erstellen eines Datensatzes automatisch einen Domänenwert festzulegen. Die Business-Regel muss einen Wert in festlegen **sys_Domain** Feld. Administratoren müssen sicherstellen, dass ein vorhanden ist **sys_Domain** Spalte, die für die Tabelle des Datensatzes verfügbar ist. Siehe Empfohlene Domain Separation-Verfahren für Service Provider für weitere Informationen.

Verwenden von Modulen zum Zuweisen von Domänen

-Administratoren können verwenden **Sysparm_Domain** URL-Parameter zum automatischen Zuweisen neuer Datensätze zu einer bestimmten Domäne aus einem Modul. Administratoren müssen ein Modul mit erstellen **Argument** Wert von: Sysparm_Domain=sys_ID der Domäne .

Verwenden von Formularvorlagen zum Zuweisen von Domänen

Administratoren können eine Formularvorlage verwenden, um einer bestimmten Domäne automatisch neue Datensätze zuzuweisen. -Administratoren müssen hinzufügen **sys_Domain** Feld zum Formular, und wählen Sie einen Domänenwert aus. Beispiel: Legen Sie fest **sys_Domain** Feld bis **TOP-/ACME-Domäne** Weist automatisch alle Datensätze aus dieser Vorlage der TOP-/ACME-Domäne zu.

Domänenvererbung für Tabellen

Standardmäßig erben zugehörige Datensätze die Domäne des übergeordneten Datensatzes. Zum Beispiel:

- Ein Change-Aufgabendatensatz erbt die Domäne des übergeordneten Change-Anforderungsdatensatzes.
- Ein Problemdatensatz erbt die Domäne des übergeordneten Incident-Datensatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Domänenzuweisung basierend auf Anwenderdomänen

Wenn keine anderen Domänenbedingungen gelten, erbt ein Datensatz automatisch die Domäne des Anwenders, der ihn erstellt hat.

Sichtbarkeitsdomänen und enthält Domänen

Sichtbarkeitsdomänen steuern, was ein bestimmter Anwender oder eine bestimmte Gruppe von Anwendern sehen kann. „Enthält“-Domänen steuern, was eine gesamte Anwenderdomäne sehen kann.

Sichtbarkeitsdomänen

Das Element „Sichtbarkeitsdomänen“ bestimmt, ob Anwender aus einer Domäne auf Datensätze aus einer anderen Domäne zugreifen können. Ordnen Sie dieses Element den Datensätzen „Anwender“ [sys_user] und „Gruppe“ [sys_user_Group] in zugehörigen Listen in diesen Datensätzen zu. Gruppen gewähren ihren Mitgliedern die Sichtbarkeitsdomänen der Gruppe. Wenn ein Anwender eine Gruppe verlässt, verliert er die Sichtbarkeitsdomänen der Gruppe. Wenn Anwendern eine Sichtbarkeitsdomäne gewährt wird, werden alle Rechte für die Datensätze in dieser Domäne basierend auf ACL-Regeln (Access Control List) gewährt.

Eine Sichtbarkeitsdomäne:

- Ist eine Anwender-zu-Domäne-Beziehung und wird explizit gewährt.
- Ist keine untergeordnete Domäne.
- Wird nicht von der Auswahl in der Domänenauswahl gesteuert. Anwender mit Zugriff auf eine Sichtbarkeitsdomäne sehen immer Daten in dieser Domäne und ihren untergeordneten Domänen.

Hinweis: Die übermäßige Verwendung von Sichtbarkeitsdomänen wird nicht empfohlen. Obwohl Transparenz eine Methode ist, mit der Anwender auf Datensätze zugreifen können, ist es am besten, enthält-Domänen für eine robustere Steuerung zu verwenden.

Enthält Domänen

Normalerweise definieren über- und untergeordnete Beziehungen die Domänenhierarchie. Eine enthält Domäne ermöglicht es Ihnen, Domänen nach Bedarf unabhängig von über- und untergeordneten Beziehungen zu verknüpfen. Enthält jedoch Domänen, die nur Domänendaten Sichtbarkeit gewähren. Prozesse bleiben von enthält-Beziehungen nicht betroffen.

Enthält Domäne:

- Ist eine viele-zu-viele-Domäne-Beziehung.
- Kann untergeordnete Domänen haben. Wenn eine Domäne ausgewählt ist, können Sie die Daten aus dieser Domäne und ihren untergeordneten Elementen anzeigen.
- Wird durch die Auswahl in der Domänenauswahl gesteuert.

Hinweis: Wenn Sie den Domänendatensatz öffnen, wird der Bereich auf die Domäne dieses Datensatzes festgelegt, sodass nur untergeordnete Domänen angezeigt werden können. Wählen Sie Aus **Domänenbereich Ein/Aus** Aus dem Menü, um die zugehörige Liste auszufüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enthält Domänenbeispiel

Wenn die Home-Domäne eines Anwenders A ist und die A-Domäne die Domänen B und C enthält, werden sie alle zu Peer-Domänen. Das bedeutet, dass der Anwender Daten aus den Domänen A, B und C sieht, während er sich in seiner Heimatdomäne A befindet. Wenn Anwender Domänen mit der Domänenauswahl in Domäne B ändern, werden nur Daten in Domäne B angezeigt. Wenn Anwender direkt mit einem Datensatz aus Domäne B oder Domäne C interagieren, werden nur Daten für diese Domäne angezeigt.

Beispiel für Sichtbarkeitsdomäne

Wenn sich Don Goodliffe in der Datenbankdomäne befindet und sich Bow Ruggeri in der Netzwerkdomäne befindet und sich keine Incidents in der globalen Domäne befinden, kann Don aufgrund der Datentrennung nicht auf Bow-Incidents zugreifen.

Sichtbarkeitsdomänen werden basierend auf der Gruppenmitgliedschaft geerbt

Wenn Sie die Domänentabelle auf die Tabelle „Gruppe“ [sys_user_Group] festlegen, können Anwender Sichtbarkeitsdomänen basierend auf ihrer Gruppenmitgliedschaft erben.

Zugehörige Informationen

Enthält Abfragen und Domänenzugriff

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenbereich

Der Domänenbereich definiert, auf was Anwender zugreifen können und was nicht.

Jeder Anwender hat zwei Domänenbereiche, wenn eine Sitzung in einer domänengetrennten Instanz eingerichtet wird.

- *Sitzungsumfang* Wird bei Einrichtung der Sitzung auf die im Anwenderdatensatz des Anwenders aufgeführte Domäne festgelegt. Anwender können ihren Sitzungsdomänenbereich manuell über die Domänenauswahl ändern.
- *Datensatzumfang* Verwendet die Domäne des Datensatzes und ist aktiv, wenn das Formular eines Datensatzes angezeigt wird.

Standardmäßig hat der Datensatzumfang Vorrang vor dem Sitzungsumfang, sodass Anwender in Domänen höherer Ebenen die Daten- und Prozessbeschränkungen jedes Datensatzes einhalten. Diese Benutzer können jedoch den Domänenumfang erweitern oder einklappen, um Daten aus anderen Domänen anzuzeigen oder auszublenden. Beispielsweise hat ein Anwender in der Domäne Service Provider (SP) auch Einblick in untergeordnete Domänen wie die ACME-Domäne. Bei der Betrachtung eines Incident-Datensatzes aus der ACME-Domäne kann der Anwender den Domänenbereich erweitern, um Werte aus der SP-Domäne anzuzeigen, oder den Domänenbereich reduzieren, um nur Datensatzwerte anzuzeigen, die der ACME-Domäne des Datensatzes entsprechen.

Hinweis: Benutzer haben immer Zugriff auf Daten aus Domänen, die ihnen durch die Domänensichtbarkeit explizit gewährt wurden.

Anwender mit der Anwenderrolle „Domain_expand_scope“ können den Domänenbereich aus auswählen **Domänenbereich Ein/Aus** UI-Aktion im Formular. Wenn der Datensatzumfang aktiv ist, klicken Sie auf die UI-Aktion, um den Sitzungsumfang zu erweitern und alle verfügbaren Daten basierend auf der Domäne des Anwenders und den untergeordneten Domänen anzuzeigen. Wenn der Sitzungsumfang in Kraft ist, klicken Sie auf die UI-Aktion,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um den Datensatzumfang zu reduzieren und nur Daten anzuzeigen, die der Domäne des aktuellen Datensatzes entsprechen.

Hinweis: In einem Datensatz wird die UI-Aktion zum Umschalten des Domänenbereichs nicht angezeigt, wenn sich der Datensatz in der globalen Domäne befindet oder wenn die Domäne des Anwenders mit der Domäne des Datensatzes übereinstimmt.

Datensatzwertauswahl aus anderen Domänen

Anwender, die mehrere Domänen sehen können, haben die Möglichkeit, Datensatzwerte aus einer Domäne auszuwählen, die sich von der Domäne des Datensatzes unterscheidet.

Beispielsweise möchten Service Desk-Mitarbeiter, die für einen Service Provider arbeiten, sich bestimmte Incidents zuweisen, um Probleme im Namen ihrer Kunden zu lösen. Wenn dies geschieht, der Incident **Zugewiesen an** Das Feld kann einen Anwender aus der SP-Domäne enthalten, auch wenn der Incident-Datensatz selbst einer untergeordneten Domäne wie ACME zugeordnet ist.

Wenn Sie einen Datensatzwert aus einer anderen Domäne auswählen, ändert sich die Domäne des Datensatzes nicht. Der Datensatz behält seine ursprüngliche Domäne bei. Wenn ein Anwender einen Datensatz mit Werten aus mehreren Domänen anzeigt, bestimmt die Domänentransparenz des Anwenders, was er sieht.

Datensatzwertauswahl

Wenn diese Bedingungen erfüllt sind	Der Anwender hat Zugriff auf diese UI-Elemente
Der Anwender hat Zugriff auf die Domäne des aktuellen Datensatzes, auf den in einem Feld verwiesen wird.	Der Anwender kann: • Siehe Anzeigewert des Referenzfelds. Beispielsweise wird der Anwendername in angezeigt **Zugewiesen an** Feld. • Sehen Sie sich das zugehörige Datensatz aus dem Referenzsymbol an. Beispielsweise wird der Anwenderdatensatz für den Anwender in angezeigt **Zugewiesen an** Feld. • Wählen Sie Werte aus einer beliebigen sichtbaren Domäne aus. Beispielsweise können Anwender aus der SP- und ACME-Domäne ausgewählt werden.
Der Anwender hat keinen Zugriff auf die Domäne des aktuellen Datensatzes, auf den in einem Feld verwiesen wird.	Der Anwender kann: • Anzeigewerte des Referenzfelds werden nicht angezeigt. (Dies ist der Fall, wenn die Domänentrennung in Madrid oder späteren Releases aktiviert wurde und der Anwender keinen Zugriff auf die Domäne dieses Datensatzes hat.) • Wählen Sie nur Werte aus der Domäne des Datensatzes aus. Beispielsweise kann nur Anwender aus der ACME-Domäne ausgewählt werden.

Domänen und zugehörige Unternehmen

Mit der Domänentrennung können Sie Änderungen, die Sie an einem Unternehmensdatensatz vornehmen, in die Domäne und andere Datensätze kaskadieren, die dem Unternehmen zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig weist das System Anwender automatisch derselben Domäne wie ihr Unternehmen zu. Beispielsweise werden alle Anwender des ACME-Unternehmens automatisch Mitglieder der TOP-/ACME-Domäne.

Hinweis: Anwender mit der Administratorrolle können ihre eigenen Anwenderdatensätze ändern und somit Domänen ändern. Service Provider möchten möglicherweise entweder die delegierte Verwaltung deaktivieren oder einen Genehmigungsprozess einrichten, um sicherzustellen, dass der Anwender die Administratorrolle benötigt.

Wenn Sie die Domäne eines Unternehmens ändern, ändert die Instanz automatisch die Domäne der folgenden zugehörigen Datensätze, um sie der neuen Domäne des Unternehmens anzupassen.

- Standorte
- Abteilungen
- Gruppen
- Anwender

Hinweis: Die Instanz ändert die Domäne eines Datensatzes, in dem Sie ausgewählt haben, nicht automatisch **Verwaltete Domäne** Kontrollkästchen.

Domänendeaktivierung und zugehörige Unternehmen

Wenn Sie eine Domäne deaktivieren, schließt die Instanz automatisch die folgenden Aktionen ab.

- Deaktiviert alle Unternehmen in der Domäne.
- Verhindert, dass sich alle Anwender anmelden, die dem inaktiven Unternehmen zugewiesen sind.

Hinweis: Wenn ein Anwender aus einem inaktiven Unternehmen versucht, sich anzumelden, wird dem Anwender eine Fehlermeldung ähnlich wie angezeigt Unternehmen inaktiv: Ihr Zugriff auf diese Instanz ist nicht autorisiert .

Wenn Sie beispielsweise die ACME-Domäne aus den Beispieldaten deaktivieren, deaktiviert die Instanz auch das ACME-Unternehmen, und die drei Beispielanwender sind gesperrt.

Konzepte für Service Provider

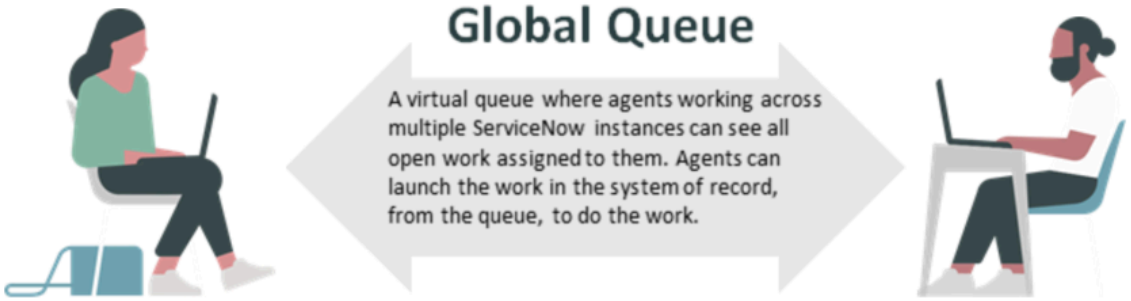
Diese Konzepte funktionieren mit vorhandenen ServiceNow Plattformfähigkeiten, mit denen Sie häufige Anwendungsfälle lösen können.

Globale Warteschlange v.2

Das globale Warteschlangenkonzept bietet eine einzige virtuelle Ansicht von Aufgaben, die sich in mehreren Instanzen befinden. Das Konzept erstellt eine anwenderdefinierte Anwendung, um eine Erfüller-Ansicht der Arbeit bereitzustellen, die sich in mehreren Instanzen befindet, ohne Aufgaben oder Daten replizieren zu müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht



Service Provider mit Service Desk-Mitarbeitern, die Aufgaben aus mehreren Systemen bearbeiten, integrieren die Daten in eine zentrale Instanz oder einen „Schwenkstuhl“ zwischen Instanzen. Diese Methode kann in einigen Fällen angemessen sein, die Erstellung und Wartung kann jedoch teuer und zeitaufwändig sein. Diese Methode eröffnet dem Anbieter auch die Möglichkeit, potenzielle Audits und Datenanforderungen wie die Datenschutz-Grundverordnung (DSGVO) in allen Instanzen zu berücksichtigen, in denen sich die Daten jetzt befinden.

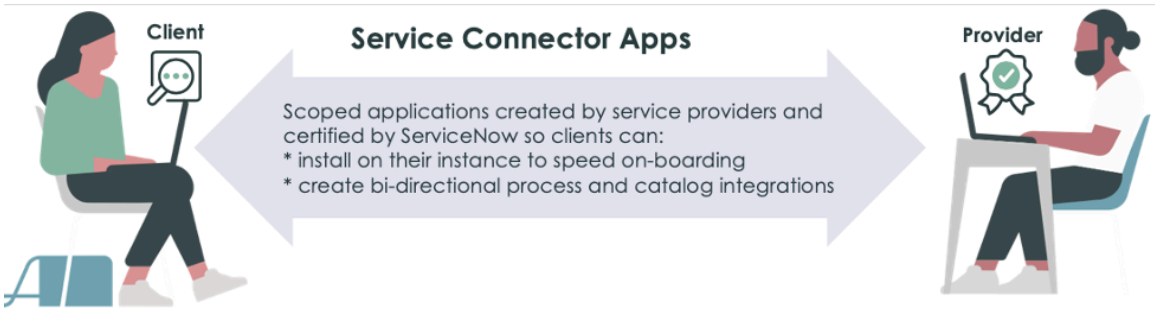
Die globale Warteschlange v.2 ist eine Alternative: Mit dieser Methode können Service Desk-Mitarbeiter die ihnen zugewiesenen Daten aus einer einzelnen Instanz anzeigen, ohne dass souveräne Daten auf der Instanz gespeichert werden, bei der sie angemeldet sind. Beispiel: In Fällen, in denen Kunden Anforderungen an den Datenstandort haben, aber Service Desk-Mitarbeitern aus anderen Ländern Zugriff gewähren, kann der Anbieter einen Helpdesk „Follow-the-Sun“ mithilfe der globalen Warteschlange v.2 verwenden.

Erfahren Sie mehr über Globale Warteschlange v.2 Proof of Concept Auf der ServiceNow Wissenswebsite.

Hinweis: Im Quebec-Release wurde der Proof of of Concept für globale Warteschlange auf globale Warteschlange V 2 aktualisiert.

Service Provider-Connector

Die Connector-Anwendung des Service Providers ist ein Referenzdesign zum Erstellen von ServiceNow Store-Anwendung für Ihre Kunden zur Integration in Ihre Systeme. Service Provider-Anwendungen helfen Ihnen, das Onboarding zu beschleunigen und standardisierte Integrationen zu erstellen.

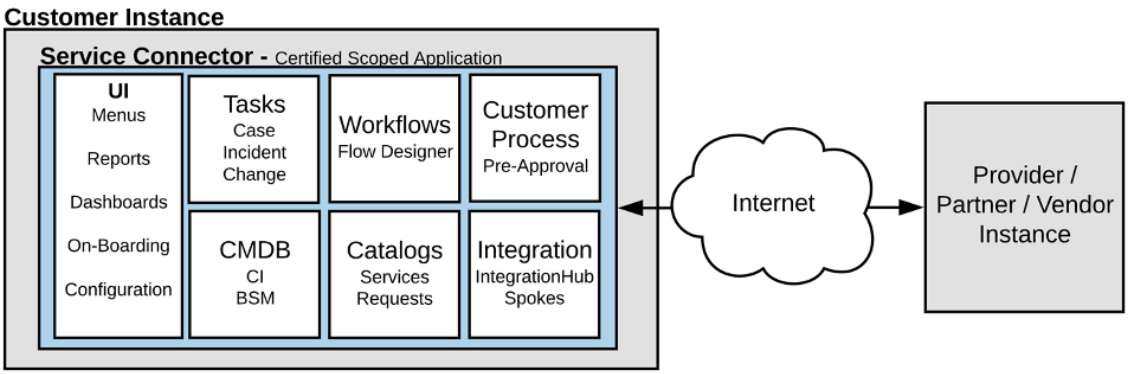


Vorteile von Service Connectors

Wenn Service Provider (Lieferanten, Lieferanten, Partner) Connectors veröffentlichen, ist das Kunden-Onboarding schneller, was eine schnellere Abrechnung bedeutet. Integrierte Instanzen erhöhen die Produktivität und die Transparenz in ServiceNow Vorteile des Ökosystems und des Partnerprogramms. Spezifische Vorteile sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eliminiert anwenderdefinierte Integrationen, einschließlich der Kosten für Services, die für die Bereitstellung und Wartung erforderlich sind.
- Services sind in ihren vom Anbieter definiert ServiceNow Instanzen und beseitigen Sie die Komplexität und Kosten anwenderdefinierter Integrationen.
- Workflows und Kataloganforderungen können mit den Prozessen und Genehmigungen des Kunden vor den Prozessen des Anbieters synchronisiert werden, sodass Kunden ihre eigenen Prozesse verfolgen können.
- Alle Daten, die für den Kunden in der Instanz des Anbieters erstellt oder geändert wurden (z. B. CIs), können zur Sichtbarkeit und Verwendung in Prozessen wieder in der Instanz des Kunden synchronisiert werden.



Schlüsselfunktionen

Funktion	Beschreibung
Anwenderoberfläche	Ein Service-Connector sollte mindestens die folgenden UI-Komponenten enthalten: • Berichte/Dashboards: Berichte und Dashboards, die von der Persona-Hilfe mit Sichtbarkeit vordefiniert sind. • Menü und Module: Der Kunde sollte die Anwendung über das beschreibende Menü finden können **XYZ-Services des Anbieters** . • Rollen: Jeder Connector erfordert Anwender- und Administratorrollen, um sicherzustellen, dass der Zugriff vom Kunden gesteuert werden kann. Beispiel: „X_snc_XYZ_user“ oder „x_snc_XYZ_admin“. • Onboarding: Schnelles Onboarding ist für eine gute Kunden-Experience von entscheidender Bedeutung und sollte über Playbook, geführtes Setup oder Katalogelement so einbezogen werden, dass für den Kunden keine professionellen Services erforderlich sind, um live zu gehen. (Professionelle Services sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung
	verfügbar, das Onboarding kann jedoch ohne IT erfolgen.) • Konfiguration: Datenpunkte sollten in Prozesse integriert werden, um die meisten normalen Prozesskonfigurationen zu berücksichtigen, die ein Kunde erreichen muss. Dadurch werden professionelle Services so weit wie möglich eliminiert. • Dokumentation: Eine gründliche Dokumentation erhöht die Kundenzufriedenheit und die Anwenderfreundlichkeit. • Support-Integration oder Kontaktinformationen: Der Kunde benötigt eine einfache Möglichkeit, bei Problemen, Fragen oder Anforderungen mit dem Service Provider in Kontakt zu bleiben.
Aufgaben	Verwenden Sie Anwendung für Aufgaben wie Incidents, Fall, Changes, Probleme usw. sollte im Connector vordefiniert sein. Diese Integrationen werden mit erstellt Flow Designer Und IntegrationHub Um ein Höchstmaß an Resilienz und Leistung sicherzustellen.
CMDB	Die Synchronisierung von Kerndaten, z. B. die für ordnungsgemäße ITIL-Prozesse erforderlichen CIs, sollte zwischen Anbieter- und Kundeninstanzen synchronisiert werden.
Workflows	Alle Workflows müssen in entworfen werden Flow Designer Um Resilienz und Leistung sicherzustellen.
Kataloge	Der Katalog des Anbieters, von dem der Kunde anfordert, sollte als datensatzproduzierender Katalog in die Anwendung aufgenommen werden. Die vom Element in der Instanz des Kunden generierte Anforderung muss eBonded mit den Instanzen des Anbieters durchgeführt werden. Die Workflows des Anbieters halten die Anforderung auf dem neuesten Stand und werden mit der Instanz des Kunden synchronisiert.
Kundenprozesse	Alle Mechanismen zum Synchronisieren von Anforderungen mit der Instanz des Anbieters sollten es Kundenprozessen ermöglichen, mit den Anforderungen zu interagieren, bevor sie an die Instanz des Anbieters gesendet werden. Während der Anbieterverarbeitung können Genehmigungen nach Bedarf an die Instanz des Kunden gesendet werden.
Integration	Integrationen sollten mit erstellt werden Flow Designer Und IntegrationHub Um ein Höchstmaß an Resilienz und Leistung sicherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mögliche Komponenten, die Sie in einen Service Connector aufnehmen können

Komponente	Beschreibung
Instanzdatenreplikation (IDR)	Wenn Replikation das Ziel ist: • Kann für die Prozessintegration verwendet werden, kann jedoch abhängig von der Komplexitätsintegrationslogik basierend auf dem Statusübergang zu starr sein • Weitere Informationen finden Sie unter Instanzdatenreplikation
IntegrationHub	Wenn Prozessintegration das Ziel ist: • Einfacher, mitten in einem Prozess als Teil eines komplexen oder bedingten Schritts mitten in einem Flow einzufügen • Weitere Informationen finden Sie unter IntegrationHub
Globale Arbeitswarteschlange (Virtuell)	Wenn der Aufgabenverbund das Ziel ist und die externe Speicherung von Daten nicht zulässig ist: • Wird verwendet, wenn Service Desk-Mitarbeiter über mehrere hinweg arbeiten ServiceNow Instanzen und müssen alle ihnen zugewiesenen offenen Arbeiten anzeigen • Zurückgegebene Zeilen müssen auf weniger als 1000 beschränkt sein • Weitere Informationen finden Sie unter Globale Arbeitswarteschlange
Remotetabellen	Wenn die externe Datennutzung ohne Speicher das Ziel ist: • Wird verwendet, um eine Instanz mit Drittparteiquellen oder mit einer anderen Instanz zu verbinden, um externe Daten abzurufen und optional im Arbeitsspeicher zu zwischenspeichern. Die Daten werden zu schreibgeschützten Zwecken wie Gruppieren, Sortieren, Zusammenfassen und Filtern als Tabelle in der Instanz behandelt. • Weitere Informationen finden Sie unter Externe Daten werden mithilfe von Remote-Tabellen und -Skripts abgerufen
Flow Designer	Wenn Prozessdesign das Ziel ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
	• Wird zur Automatisierung von Prozessen in einer einzigen Designumgebung verwendet. Prozessbesitzer können natürliche Sprache verwenden, um Genehmigungen, Aufgaben, Benachrichtigungen und Datensatzvorgänge ohne Codierung zu automatisieren. • Weitere Informationen finden Sie unter Flow Designer .

Erfahren Sie mehr über Service Connector – Proof of Concept Auf der ServiceNow Wissenswebsite.

Mit Domänentrennung installiert

Mehrere Plattformkomponenten werden mit Domänentrennung hinzugefügt oder geändert.

Rollen

Rolle	Beschreibung
Domain_admin	Kann Domänen erstellen, bearbeiten und löschen.

Ergänzungen zu [sys_Domain]-Feldern

Das Feld sys_Domain wird den folgenden Tabellen hinzugefügt:

Tabellen mit dem Feld „sys_Domain“

Tabellen
sys_attachment
sys_user_has_role
sys_Group_has_role
sys_email
sys_user_group
core_company
cmn_location
cmn_Department
sys_Gauge
sys_Report
kb_Feedback
Sysapproval_Approver
sys_user_grmember

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld für die Aufgabentabelle

MSP-Erweiterungen fügen der Aufgabentabelle ein Feld „Task_for“ hinzu. Dieses Referenzfeld bezieht sich auf die Anwendertabelle.

Optionen für den Gruppentyp

MSP-Erweiterungen fügen dem Feld Typ der Gruppentabelle mehrere neue Standardoptionen hinzu. Fügen Sie diesen Typen nach Bedarf hinzu, oder aktualisieren Sie sie, um Ihre Domänen zu unterstützen.

Tabellen
Sicherheit
Support
Sichtbarkeit

Business-Regeln

Name	Tabelle	Beschreibung
Domäne – Aktivieren/ Deaktivieren	core_company	Aktiviert die zugehörige Domäne, wenn mindestens eines ihrer Unternehmen aktiv ist. Deaktiviert die zugehörige Domäne, wenn alle zugehörigen Unternehmen inaktiv sind.
Domäne: Kaskadierendes Unternehmen	core_company	Hält die Domäne eines Unternehmens mit seinen Anwendern, Gruppen, Abteilungen und Standorten synchronisiert.
Domäne – Domäne Kaskadieren – E-Mail	sys_email	Synchronisiert die Domäne einer E-Mail mit ihren Anhängen.
Domäne – Domäne Kaskadieren – Gruppe	sys_user_group	Hält die Domäne einer Gruppe mit ihren geerbten Rollen (sys_Group_has_role-Datensätze) synchronisiert.
Domäne – Domäne Kaskadieren – Wissen	kb_knowledge	Synchronisiert die Domäne eines wissensartikels mit dem zugehörigen Feedback.
Domäne – Domäne Kaskadieren – Aufgabe	Aufgabe	Hält die Domäne mit zugehörigen Aufgaben für wf_context, wf_Executing, wf_history, Anhänge, E-Mails, Task_sla und sein Workflow, sysApprover_Approver und sein Workflow sowie sysApproval_Group und sein Workflow.
Domäne: Domäne Kaskadieren: Anwender	sys_user	Hält die Domäne eines Anwenders mit den Datensätzen „Gruppenmitgliedschaft“ (sys_user_grmember) und „Rolle“ (sys_user_has_role) synchronisiert.
Domäne – Domäne Kaskadieren – Version	wf_Workflow_Version	Hält Domänen mit zugehörigen Workflow-Versionen für wf_activity und wf_Transition synchronisiert.
Domäne: Deaktivieren Sie Unternehmen	Domäne	Deaktiviert zugehörige Unternehmen, wenn eine Domäne deaktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Tabelle	Beschreibung
Domäne – Standard – Aufgabe	Aufgabe	Legt die Aufgabendomäne basierend auf der Aufgabe für die Domäne des Anwenders fest. Wenn diese Domäne global ist, legt sie stattdessen die Domäne auf Standard fest.
Domäne – Standard – Anwender	sys_user	Legt die Domäne eines Anwenders auf Standard fest, wenn die Domäne andernfalls global gewesen wäre.
Domäne: Datensatz Der Globalen Domäne Nicht Zulassen	Domäne	Verhindert die Erstellung einer Domäne mit dem Namen global.
Domäne: Kopie Überschreiben	sys_App_Application	Wenn eine Anwendung für eine Domäne überschrieben wird, erstellt eine Kopie ihrer Module für die neue Anwendung.
Domäne: Kopie Überschreiben	sys_Data_policy2	Wenn eine Datenrichtlinie für eine Domäne überschrieben wird, erstellt eine Kopie ihrer Datenrichtlinienregeln für die neue Datenrichtlinie.
Domäne: Kopie Überschreiben	sys_Gauge	Wenn eine Anzeige für eine Domäne überschrieben wird, erstellt eine Kopie ihrer Anzeigeanzahlen für die neue Anzeige.
Domäne: Kopie Überschreiben	sys_ui_action	Wenn eine UI-Aktion für eine Domäne überschrieben wird, erstellt eine Kopie ihrer UI-Aktionsansichten für die neue UI-Aktion.
Domäne: Kopie Überschreiben	sys_ui_list_Control_Embedded	Wenn ein Steuerelement für eingebettete Listen für eine Domäne überschrieben wird, erstellt eine Kopie seiner Client- und Serverskripts für das neue Steuerelement für eingebettete Listen.
Domäne: Kopie Überschreiben	sys_ui_Policy	Wenn eine UI-Richtlinie für eine Domäne überschrieben wird, erstellt eine Kopie ihrer UI-Richtlinienaktionen für die neue UI-Richtlinie.
Domäne – Domäne Festlegen – Genehmigungen	Sysapproval_Approver	Legt die Domäne basierend auf der Domäne des genehmigten Datensatzes fest.
Domäne – Domäne Festlegen – Anhang	sys_attachment	Legt die Domäne basierend auf der Domäne des übergeordneten Datensatzes fest.
Domäne – Domäne festlegen – CMDB_CI	cmdb_ci	Legt die Domäne eines CI auf die des Unternehmens fest.
Domäne – Domäne Festlegen – Abteilung	cmn_Department	Legt die Domäne einer Abteilung auf die des Unternehmens fest.
Domäne – Domäne Festlegen – Domäne	Domäne	Legt die Domäne einer Domäne für sich selbst fest.
Domäne – Domäne Festlegen – E-Mail	sys_email	Legt die Domäne basierend auf der Domäne des übergeordneten Datensatzes fest. Der übergeordnete Datensatz einer E-Mail ist der im Instanzfeld angegebene Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Tabelle	Beschreibung
Domäne – Domäne Festlegen – Feedback	kb_Feedback	Legt die Domäne eines Wissensfeedbacks auf die Domäne seines wissensartikels fest.
Domäne – Domäne Festlegen – Gruppe	sys_user_group	Legt die Domäne einer Gruppe auf die des Unternehmens fest.
Domäne – Domäne Festlegen – Gruppengenehmigungen	SysApproval_Group	Legt die Domäne basierend auf der Domäne des genehmigten Datensatzes fest.
Domäne – Domäne Festlegen – Gruppenrolle	sys_Group_has_role	Legt die Domäne einer Gruppenrolle auf die der Gruppe fest.
Domäne – Domäne Festlegen – Standort	cmn_location	Legt die Domäne eines Standorts auf die des Unternehmens fest.
Domäne – Domäne festlegen – Aufgaben-SLA	Task_sla	Legt die Domäne eines Aufgaben-SLAs auf die Domäne seiner Aufgabe fest.
Domäne – Domäne Festlegen – Anwender	sys_user	Legt die Domäne eines Anwenders auf die des Unternehmens fest.
Domäne – Domäne Festlegen – Anwenderrolle	sys_user_has_role	Legt die Domäne einer Anwenderrolle auf die Domäne ihres Anwenders fest.
Domäne – Domäne festlegen – WF-Aktivitätsthist	wf_History	Legt die Workflow-Aktivitätsverlaufsdomäne basierend auf der Domäne des übergeordneten Workflow-Kontexts fest.
Domäne – Domäne festlegen – WF-Kontext	wf_context	Legt die Workflow-Kontextdomäne basierend auf der Domäne des referenzierten Datensatzes fest, falls vorhanden.
Domäne – Domäne festlegen – WF-Ausführungsaktivität	wf_Executing	Legt die Aktivitätsdomäne des Workflows basierend auf der Domäne des übergeordneten Workflow-Kontexts fest.
Domäne – Aufgabe festlegen für – Change	Change-Anforderung	Beim Konvertieren eines Tickets in eine Change-Anforderung legt das Feld angefordert von auf den Wert „Aufgabe für“ des Tickets fest.
Domäne – Aufgabe festlegen für – Incident	Incident	Beim Konvertieren eines Tickets in einen Incident legt das Feld Anrufer auf den Wert „Aufgabe für“ des Tickets fest.
Domäne: Validierungsstandard	Domäne	Stellt sicher, dass nur für eine Domäne das Kontrollkästchen Standard aktiviert ist.
Domäne: Primäre Domäne Validieren	Domäne	Stellt sicher, dass nur für eine Domäne das Kontrollkästchen Primär aktiviert ist.
Mit Domänen-Support-Plugin installierte Business-Regeln		
Ändern Sie Den Domänensatz	sys_dictionary	Legt den Domänensatz auf die aktuelle Domäne fest.
Eigenschaften der Domänenunterstützung	sys_properties	Legt die Systemeigenschaften so fest, dass sie der Domänenabfragemethode (Domänenpfade oder Domänennummerierung) entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client-Skripts

Client-Skript	Beschreibung
Domäne – Unternehmen und Standort festlegen (sys_script)	Überwacht das Feld „Incident-Anrufer“ auf Changes. Wenn die Felder „Unternehmen“ und „Standort“ noch keinen Wert haben, fügt das Skript diese Informationen aus dem Anruferdatensatz hinzu. Wenn die Felder „Unternehmen“ und „Standort“ bereits einen Wert haben, behält das Skript die vorhandenen Werte bei.
Deaktiviertes Skript	
(BP) Stellen Sie Standort auf Anwender fest	Überwacht das Feld „Incident-Standort“ und legt das Feld „Standort“ auf den Standort des Anrufers fest.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Anwendungssupport für die Domänentrennung

Viele ServiceNow Anwendungen unterstützen Domänentrennung im Basissystem, aber nicht alle. Einige unterstützte Anwendungen enthalten Einschränkungen für die Daten und administrativen Einstellungen, die domänengetrennt werden können. Diese Definitionen beschreiben die Supportstufen der Domänentrennung aus der Perspektive tatsächlicher Anwendungsfälle und der Personen, die sie verwenden.

Support-Ebenen für Domänentrennung

ServiceNow Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und die Datenweiterleitung, verfügen über erweiterte Geschäftslogik-Trennung oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kunden). ServiceNow Anwendungen werden mit den folgenden inkrementellen Supportstufen definiert.

Basic	Standard	Enhanced
• Data is domain-separated • Logic exists to ensure proper data routing, caching, rollups, and aggregations • Global configuration operational for multiple tenants	• Application properties are domain-aware as needed • Business logic can be domain-separated by the instance owner per tenant	• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic

Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Logik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Basis

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- In der Anwendung berücksichtigen die Benutzeroberfläche, Cache-Schlüssel, Berichterstellung, Rollups, Zusammenfassungen usw. Domänen zur Produktionslaufzeit.
- Der Besitzer der Instanz muss in der Lage sein, die Anwendung so einzurichten, dass sie mandantenübergreifend funktioniert.

Beispiel-Anwendungsfall: Wenn ein SP den Chat verwendet, um auf die Nachricht eines Mandanten zu antworten, muss der Client die Antwort des SP sehen können.

Standard

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Prozesse können vom Service Provider (SP) pro Kunde erstellt oder geändert werden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss in der Lage sein, die Business-Logik- und Datenparameter für das Minimum der lebensfähigen Produkte (MVP) pro Mandant wie für die spezifische Anwendung erwartet zu konfigurieren.

Beispielanwendungsfall: Ein Administrator muss Kommentare obligatorisch machen können, wenn ein Datensatz für einen Mandanten geschlossen wird, aber nicht für einen anderen.

Verbessert

- Umfasst die Stufen **Basis** und **Standard**.
- Ein datengesteuerter Prozess ermöglicht es Service Provider-Kunden, die Geschäftslogik basierend auf definierten Anwendungsfällen zu ändern. Diese Konfigurationen sind UI-basiert und ausfallsicher, sodass Konfigurationen von einem Kunden sich nicht auf einen anderen auswirken können.
- Mandanten der Instanz müssen die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter für sich selbst konfigurieren können. Diese Logik und diese Parameter würden für die normale Funktion der Anwendung erwartet.

Beispiel-Anwendungsfall: Mandanten-Kunden einer gemeinsam genutzten Umgebung müssen in der Lage sein, die Impact-, Dringlichkeits- oder Prioritätsmatrix zu ändern, um die Priorität in ihrer Domäne festzulegen.

Hinweis: Effektive Domäne (*)

Manchmal unterstützt eine Plattformfunktion oder -Anwendung SP-Anwendungsfälle auch ohne das Domänen-Framework effektiv. Wenn ja, müssen die Anwendungsfälle die Unterstützung der Domänentrennung beschreiben. Ein Sternchen (*), nachdem die Supportstufe diese Art von Konfiguration anzeigt.

Unterstützte Funktion	Standard	Standard	Erweitert
Domänenspalte ist für Basistabellen der -Anwendung vorhanden.			

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Funktion	Standard	Standard	Erweitert
Die domänenspezifische Konfiguration wird vom Instanzbesitzer verwaltet.	●	●	●
Mandantendomänen können ihre eigenen Anwendungsdaten verwalten.		●	●
Anwendungseigenschaften sind bei Bedarf domänenbewusst.		●	●
Geschäftslogik und Prozesse können vom Instanzbesitzer domänengetrennt werden.		●	●
Geschäftslogik und -Prozesse können von der Mandantendomäne verwaltet werden.			●

Supportstufen nach Anwendung

Produkt-Suite	Anwendung	Supportstufe
App-Entwicklung und Low-Code	App Engine Studio	Kein Support
	Automatisierungszentrale	Standard
	Robotic Process Automation (RPA)-Hub	Standard
	ServiceNow Studio	Kein Support
	Tabellen-Generator	Standard
	App Engine Management Center	Kein Support
	Entscheidungstabellen Erkunden	Standard
	Enterprise Resource Planning-Integration	Kein Support
	Enterprise Resource Planning Customization Mining	Kein Support
	Next Experience UI Builder	Standard
Kundenservice-Management	Communities	Kein Support
	Kundenservice-Management	Standard
	Releasemanagement	Standard*
	Order Management für Customer Service Management	Standard
	Support Nach Dem Verkauf	Standard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Supportstufe
	Domain Separation in Personaloptimierung für den Kundenservice	Standard
DevOps	Domain Separation und DevOps Change-Geschwindigkeit	Kein Support
	Domain Separation und DevOps Config	
Employee Service Management	HR Service Delivery	Standard*
	Arbeitsschutz	Kein Support
	Vertragsmanagement Pro	Standard
	Legal Service Delivery	Standard
	Procurement Service Management (PSM)	Kein Support
	Safe Workplace-Suite	Auf der Anwendungswebsite finden Sie Informationen zu den einzelnen Support-Stufen für Anwendungen
	Connector für SharePoint Online-Suchen	Standard
	Universelle Anforderung	Standard
	UR-Aufgabe	Standard
	Personaloptimierung für HR	Standard
Management von Environmental, Social und Governance	Management von Environmental, Social und Governance	Standard
Außendienst-Management	Field Service Management	Standard
Governance, Risk und Compliance	Business Continuity Management	Standard
	Governance, Risk and Compliance (GRC)	Standard
	Operational Resilience	Standard
Branchenprodukte		
•Financial Services	Financial Services Card Operations	Standard
	Financial Services Deposit Operations	
	Financial Services Payment Operations	
	Intelligente Services für Betrug	
	Sachwert- und Unfallversicherung Servicing	
	Lebensversicherungsservices	
	Versicherungsansprüche	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Supportstufe
	Financial Services Know Your Customer	
	Kreditvorgang Für Finanzdienstleistungen	
	Dokumentverarbeiter Für Finanzdienstleistungen	
• Gesundheitswesen und Biowissenschaften	EMR Help	Standard
	Healthcare and Life Sciences Service Management Core	Standard
	Pre-Visit Management	Standard
	Patient Support Services	Standard
	Vaccine Administration Management	Standard
Commercial Operations für die Produktion	Commercial Operations für die Produktion	Standard
	Einzelhandels-Core	Standard
	Verwaltung Von Einzelhandelsaufgaben	Standard
• Fertigungsindustrie	Industrial Process Manager	Standard
	Operational Technology Manager	Standard
	Operational Technology Vulnerability Response	Standard
	Operational Technology Manager	Standard
Telekommunikation, Medien und Technologie (TMT)	Kundenerfolgsmanagement	Standard
	Problem-Management des Kundenservice	Standard
	Now Assist für Telekommunikation, Medien und Technologie (TMT)	Standard (geerbt von Domänentrennung in Now Assist-Administrator Konsole).
	Proaktive Service-Experience-Workflows	Standard
	Service Bridge	Standard
	Fallanwendung für Technologie-Produktsupport	Standard (geerbt von Kundenservice-Management).
	Telecommunications Network Inventory	Standard
IT Asset Management	Cloud Insights	Kein Support
	Hardware Asset Management	Erweitert
	Software Asset Management	Erweitert
	Enterprise Asset Management	Standard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Supportstufe
Strategisches Portfoliomanagement	Agile Development	Standard*
	Alignment Planner Workspace	Standard
	Application Portfolio Management	Standard
	Cost Management	Kein Support
	Demand-Management	Standard
	Finanzmanagement	Kein Support
	Investment Funding	Standard
	Projektportfoliomanagement	Standard*
	Releasemanagement	Standard*
	Scaled Agile Framework (SAFe)	Standard*
	Test Management	Standard*
	Ziel-Framework	Standard
IT Operations Management	Cloud Provisioning and Governance	Standard
	Agent Client Collector	Standard
	Discovery	Standard
	Ereignismanagement	Standard
	Service Operations-Arbeitsbereich für ITOM	Standard
	Health Log Analytics	Standard
	Metric Intelligence	Standard
	Service-Zuordnung	Standard
	Bewertung Der Cloud-Migration	Standard
	Aktionsbibliothek	Kein Support
	Governance für Cloud-Konfigurationen	Kein Support
	Tag Governance	Standard
	Abrechnung für Cloud-Einblicke	Kein Support
	Cloud-Bereitstellung und -Governance: Google Cloud	Standard
	Cloud-Bereitstellung und -Governance-Terraform	Standard
	Cloud-Vorgangsarbeitsbereich	Standard
	Cloud-Discovery	Standard
IT Service Management	Benchmarks	Kein Support
	Change-Management	Standard
	Coaching	Standard

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Supportstufe
	Management kontinuierlicher Verbesserungen	Standard
	Vertragsmanagement	Kein Support
	Domain Separation und Release-Management von Digitalprodukten	Standard
	Kostenzeile	Kein Support
	Incident Communications Management	Standard
	Incident-Management	Standard
	Facilities Service Management	Standard
	Incident-Management	Standard
	Bereitschaftsplanung	Standard
	Asset-Management	Standard
	Problem-Management	Standard
	Beschaffung	Standard*
	Produktkatalog	Standard
	Anforderungsmanagement	Standard
	Servicekatalog	Standard
	Service-Level-Management	Standard
	Service Portfoliomanagement	Standard*
	Site Reliability Operations	Standard*
	Nichtverfügbarkeit von Aufgaben	Standard
	Domain Separation und Vendor Management-Arbeitsbereich	Kein Support
	Walk-up Experience	Standard
Konfiguration und Navigation für Mobile	Mobil	Standard
Now Intelligence	Dashboards	Standard
	Leistungsanalysen	Erweitert
	Process Optimization	Standard
	Berichterstellung	Standard
	User Experience Analytics	Standard
Die zugehörigen Listen namens ServiceNow AI Platform	Administration	
	Domänentrennung und Mitarbeiterchat	Standard
	ServiceNow AI Platform Fähigkeiten	
	Anwenderoberfläche	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Supportstufe
	Advanced Work Assignment	Standard
	AI Search	Durchsucht die Einhaltung von Domänenbeschränkungen aus indizierten Datensätzen
	App Engine Studio	Kein Support
	Application Management	Kein Support
	Bewertungen	Standard
	Automated Test Framework	Standard*
	ServiceNow Voice	
	Codesignatur	Grundlegender Support
	Contextual Search	Standard
	Configuration Management (CMDB)	Standard
	Content-Management-System	Kein Support
	Anmeldeinformationen und Verbindungen	Standard
	Datenzertifizierung	Standard*
	Data Classification	Erweitert
	Datenschutz	Kein Support
	Datenverwaltung	Standard*
	Delegierte App-Entwicklung	Kein Support
	Dependency Views	Standard
	Dokumentenservices	Kein Support
	Dynamische Übersetzung	Standard
	Edge Encryption	Grundlegender Support
	Connectors für externe Inhalte	Kein Support*
	Feldverschlüsselung	Kein Support
	Verschlüsselung	Kein Support
	Cloud-Verschlüsselung mit Schlüsselverwaltung	Grundlegender Support
	Feldnormalisierung	Kein Support
	Flow Designer	Standard*
	Geführtes Setup	Kein Support
	Domänentrennung und IntegrationHub	Standard*
	Integrationen mit Anwendungen und Datenquellen von Drittparteien	Standard+Standard
	Knowledge Management	Standard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Supportstufe
	Hermes Messaging Service	Kein Support
	Verwaltete Dokumente	Kein Support
	MetricBase	Standard
	Verständnis Für Natürliche Laungage	Standard+Standard
	Benachrichtigungen	Standard
	ODBC-Treiber	Standard*
	Orchestration	Standard*
	Password Reset	Standard
	Platform-Sicherheit	Zielseite der Domänentrennung
	Datenschutz	Kein Support
	Predictive Intelligence	Standard
	Proaktive Auslöser	Standard
	Process Automation Designer	Standard
	Remotetabellen	Kein Support
	Zeitpläne	Standard
	Skript-Debugger	Standard
	Suchvorschläge	Kein Support
	Service Portal	Kein Support
	Service Graph Connectors	Kein Support
	Domänentrennung und Sidebar	Standard
	Status-Flows	Kein Support
	Subscription Management	Standard*
	Umfragemanagement	Standard*
	Task Intelligence	Kein Support
	Domänentrennung und Zeitkarten	Standard*
	UI Builder	Standard
	Virtual Agent	Standard
	Visual Task Boards	Standard
	Webservices	Standard*
	Workflow	Standard*
	Arbeitsbereich	Standard
Security Operations	Configuration Compliance	Standard
	Configuration Data Management	Standard
	IBM QRadar Offense Ingestion	Standard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkt-Suite	Anwendung	Supportstufe
	Integration der Microsoft Graph-Sicherheits-API-Warnungserfassung	Standard
	Security Incident Response	Standard
	Threat Intelligence	Standard
	Vulnerability Response	Standard
Service Management	Facilities Service Management	Standard
	Geplante Wartung	Standard*
	Proaktive Auslöser	Standard
	NOW-Code-Editor	Kein Support
	Personaloptimierung für ITSM	Standard
	Vendor Management-Arbeitsbereich	Standard

Empfohlene Domain Separation-Verfahren für Service Provider

Sie können Domänentrennung für Ihre Anwendungen und Services erstellen, implementieren und verwalten.

Domänengrundlagen

Mit Domänentrennung (auch bekannt als ServiceNow Multimandant-Plattformarchitektur) können Sie Anwendungsdaten, Anwenderoberfläche und Geschäftslogik in einer einzigen Kundeninstanz trennen, die hierarchische Modellierung mit mandantenübergreifender Intelligenz unterstützt. Die Geschäftslogik beschreibt, wie die Domänentrennung konfiguriert wird und welche Regeln sich auf die Konfiguration auswirken.

Bevor Sie mit der Domain Separation Journey beginnen, finden Sie hier einige bewährte Praktiken. Wählen Sie Themen nach Belieben aus, oder folgen Sie ihnen in der Reihenfolge, indem Sie auf die Links unter dem Bild klicken.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung erklärt

Mit der Domänentrennung können Sie Anwendungsdaten, UI und Geschäftslogik, z. B. Regeln oder Workflows, in einer einzigen Kundeninstanz trennen. Die Trennung dieser Elemente in logisch definierte Domänen unterstützt bestimmte Hierarchien für alle Kunden, die Ihre Anwendungen verwenden.

Domänengrundlagen

Domänentrennung, auch bekannt als ServiceNow Die Architektur der Multimandantenplattform, erhöht die Verwaltung einer Instanz erheblich. Wenn Sie die Domänentrennung jedoch richtig verwenden, kann dies die Effizienz verbessern, die Sicherheit erhöhen und die Leistung der Instanzen Ihrer Kunden steigern.

Sie können einige globale Standards und Eigenschaften, z. B. Systemeigenschaften und Tabellenschema, nicht pro Mandant trennen.

Lesen Sie die folgenden Richtlinien, bevor Sie mit der Trennung von Domänen beginnen.

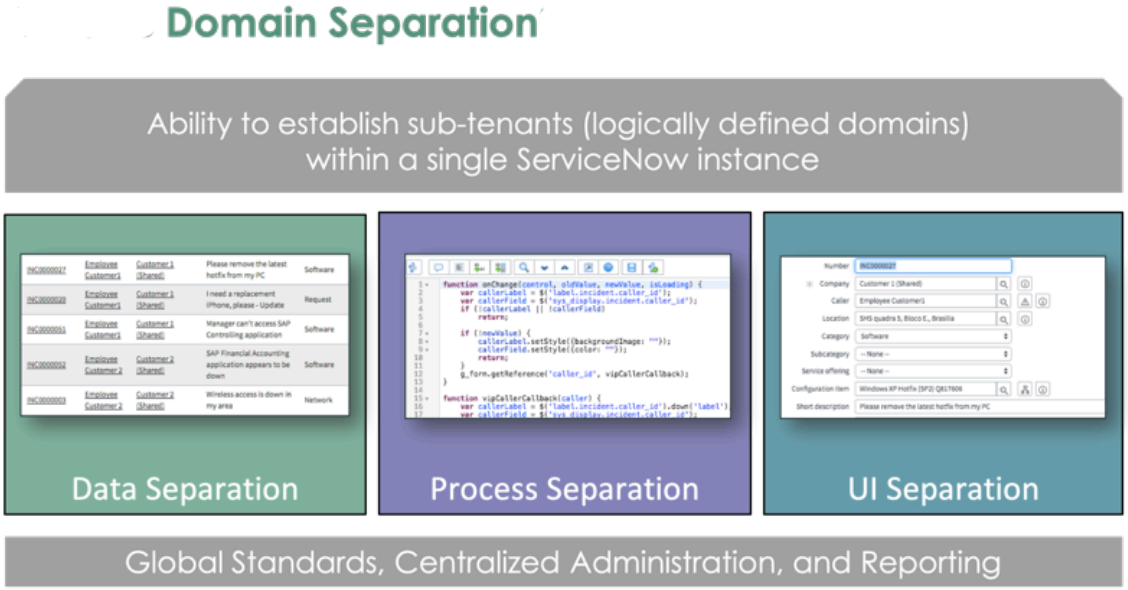
Was Sie mit der Domänentrennung tun können

- Datentrennung: Ermöglicht Mandanten der Domäne, nur Daten anzuzeigen, für die sie Berechtigungen haben. Mandanten können Zugriff auf andere Mandantendaten gewährt werden, können jedoch keine Mandantendaten abfragen, auf die sie keinen Zugriff haben.
  - Wenn Sie Datensätze aktualisieren, werden keine Update-Satz-Datensätze generiert.
  - Anwender, einschließlich der Kundenaccounts, die für Integrationen verwendet werden, sehen nur die Daten in den Domänen, für die sie Zugriffsberechtigung haben.
  - Kunden, Service Desk-Mitarbeiter und Erfüller sehen Daten, die sich auf die von ihnen unterstützten Kunden und Organisationen beziehen.
- UI-Trennung: Unterstützt eine mandantenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.
  - Sie können die browserbasierte Anwenderoberfläche überschreiben, einschließlich Anwendungsmenüs, Listen, Formularen und Dashboards. Sie können sie auch für eine bestimmte Domäne oder einen Satz von Domänen anpassen, während Sie Ihre grundlegende Prozesslogik beibehalten.
  - Service Provider können die angezeigten Branding- und UI-Elemente ändern, um die individuellen Kundenanforderungen zu erfüllen.
- Geschäftslogik-Trennung: Erstellt mandantenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Geschäftsregeln, Clientskripts, UI-Richtlinie und UI-Aktionen.
- Hierarchische Modellierung: Verschachtelt mehrere Mandanten, damit übergeordnete Mandanten auf untergeordnete Mandantenressourcen zugreifen können. Die Geschäftslogik für übergeordnete Mandanten wird automatisch für untergeordnete Mandanten ausgeführt, die Sie auf jeder Ebene überschreiben können.
- Mandantenübergreifende Intelligenz: Verarbeitet automatisch Daten, Metadaten, Geschäftslogik und Verarbeitungskontext für Mandanten mit Zugriff auf zusätzliche Mandantendaten.

Domänentrennung auf einen Blick

Die folgende Grafik zeigt die Aufteilung von Daten-, Prozess- und UI-Trennung. Diese Konzepte werden im Abschnitt empfohlene Praktiken ausführlich besprochen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

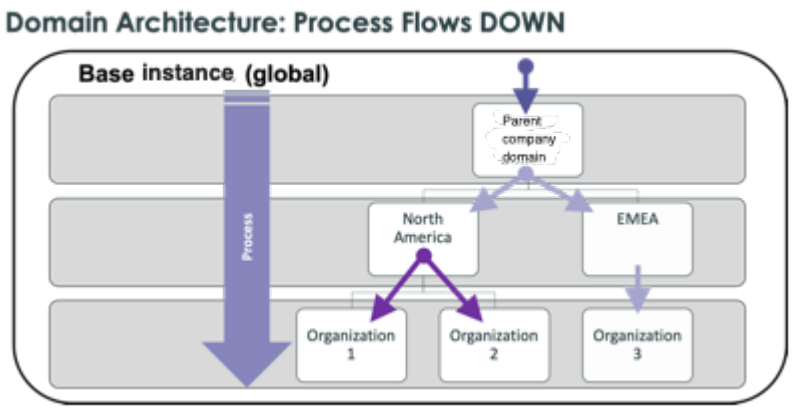


Domänenarchitektur

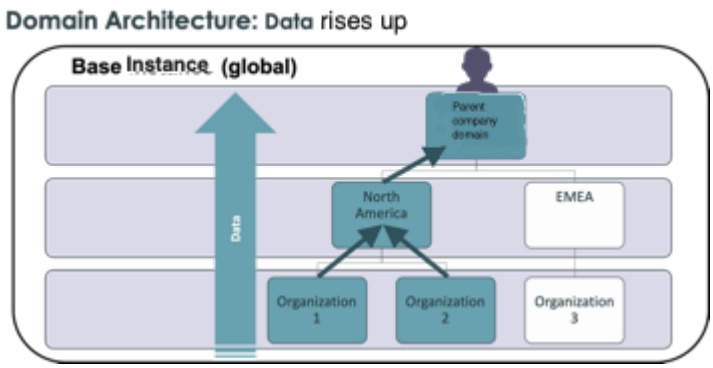
Anwenderdatensätzen wird ein Domänenwert zugewiesen, der die Startdomäne des Anwenders darstellt. Anwender haben keinen Zugriff auf Daten in übergeordneten Domänen, Peer-Domänen oder Domänen in anderen Verzweigungen der Hierarchie.

Siehe Enthält Abfragen und Domänenzugriff Für erweiterte Optionen, um zusätzliche Domänentransparenz zu gewähren.

Das folgende Diagramm zeigt, wie der Architekturprozess in die untergeordneten



Domänen abfließt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wertversprechen für Domänentrennung

Mit der Domänentrennung können Service Provider über eine Architektur mit mehreren Mandanten verfügen, die ihren Kunden Angebote effizient und sicher bereitstellt. Starke universelle Prozessstandards, datengesteuertes Prozessdesign, strikte Governance und zentralisierte Administration tragen dazu bei, diese Vorteile zu maximieren.

Vorteile der Domänentrennung

Die Mandanten einer Domäne profitieren von einer schnellen Rentabilität, einem geringeren Verwaltungsaufwand und der Nutzung der von Instanzbesitzern bereitgestellten Business-Services.

Hier ist eine Schnellansicht dieser Vorteile.

Instanzbesitzer	Domänenmandanten
Mitarbeiterproduktivität des Service Providers	Erhöhte Sicherheit
Nur Prozess-Deltas verwaltet	Vorgefertigte Prozesse und Funktionen
Verwaltungseffizienz	Reduziertes Personal erforderlich
Weniger Client-Integrationen	Schnelleres Onboarding
Upgradefähigkeit und Skalierbarkeit	Nutzen Sie die neuesten Releases
Datentrennung	Vom Instanzbesitzer bereitgestellte Services
Globale Berichterstellung	

Definition der Domänentrennung

Mit Domänentrennung (auch bekannt als ServiceNow® Multimandant-Plattformarchitektur) können Sie Anwendungsdaten, UI und Geschäftslogik in einer einzigen Kundeninstanz trennen, die hierarchische Modellierung mit mandantenübergreifender Intelligenz (Kunden) unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Domänentrennung

Domänengetrennt ServiceNow Anwendungen werden mit den folgenden Eigenschaften definiert:

Datentrennung

Ermöglicht Kunden, nur die Daten anzuzeigen, für die sie Berechtigungen haben. Kunden können Zugriff auf andere Kundendaten gewährt werden, aber keine Kundendaten abfragen, wenn sie keinen Zugriff haben.

UI-Trennung

Unterstützt eine kundenspezifische Experience für UI-Elemente wie Ansichten, Listen, Bezeichnungen usw.

Geschäftslogik-Trennung

Unterstützt kundenspezifische Systemrichtlinien wie E-Mail-Benachrichtigungen, Geschäftsregeln, Client-Skripts, UI-Richtlinie und UI-Aktionen.

Hierarchische Modellierung

Unterstützt geschachtelte Mehrmandantenfähigkeit, damit übergeordnete Mandanten (Kunden) auf untergeordnete Kundenressourcen zugreifen können. Die Geschäftslogik für übergeordnete Kunden wird automatisch für untergeordnete Kunden ausgeführt und kann auf jeder Ebene überschrieben werden.

Kundenübergreifende Intelligenz (Domänenbereich)

Verarbeitet automatisch die Daten, Metadaten, Geschäftslogik und Verarbeitungskontext für Mandanten, die Zugriff auf zusätzliche Mandantendaten haben.

Domain Separation-Hierarchien

Erstellen Sie beim Definieren einer Domänenarchitektur eine Hierarchie, um Ihre Prozesse und Workflows zu nachzuverfolgen.

Beispiele für Domain Separation-Hierarchien

Das folgende Diagramm ist ein guter Ausgangspunkt für die Definition der Domänenarchitektur. Es zeigt die Beziehung zwischen den TOP- und den untergeordneten Domänen und wie sich der Prozess, die Daten und die Geschäftsregeln auf die übergeordneten und untergeordneten Domänen auswirken.

- Im folgenden Beispiel ist TOP eine Prozessdomäne. Sie darf keine Benutzer enthalten. Eigentlich sollte TOP die neuen Prozesse enthalten, die die Eigentümer der Instanzen entwickeln, sowie die Überschreibungen zu diesen Prozessen aus der globalen Domäne.
- Nur der Service Provider (SP) hat Zugriff auf die Standarddomäne. Diese Domäne enthält keine aktiven Benutzer. Die Domäne enthält nur die „verlorenen“ Daten, die Sie der richtigen Domäne neu zuweisen müssen.

  Hinweis: Wenn Daten keiner bestimmten Domäne zugewiesen sind, werden sie in die Standarddomäne verschoben. Sie gehen vorübergehend „verloren“ und müssen der richtigen Domäne zugewiesen werden.

- Aufgaben und Benutzer ohne Domäne werden beim Erstellen oder Aktualisieren von Domänen automatisch in der Standarddomäne eingefügt. Sie können diese Aktion überschreiben, indem Sie entweder die Option **Standard** für diesen Datensatz deaktivieren oder die Option **Standard** für einen anderen Domänendatensatz auswählen. Wenn Sie noch keine Standarddomäne festgelegt haben, werden Aufgaben und Benutzer ohne Domäne in die globale Domäne verschoben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verschieben Sie keine Daten zwischen Domänen, während Sie die Instanz verwenden.
- Wenn Daten in der Standarddomäne landen, bedeutet dies, dass Sie ein Konfigurations- oder Verfahrensproblem haben.

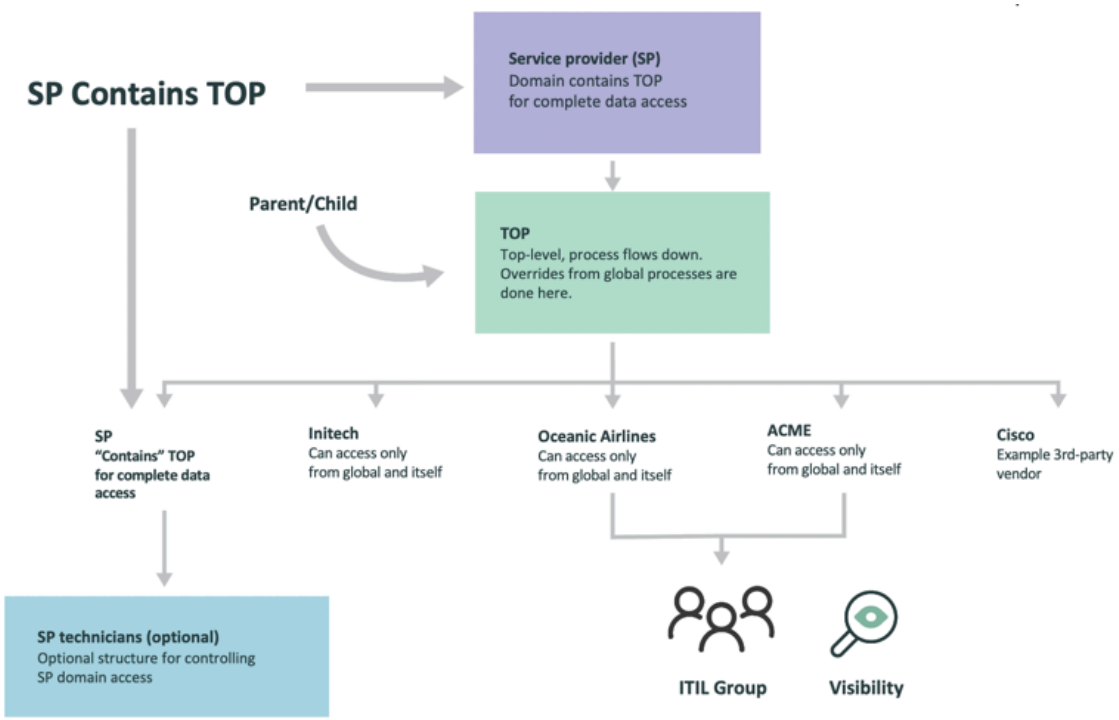
Das Wort „Global“ wird in diesem Diagramm nicht angezeigt, da keine globale Domäne vorhanden ist. Denken Sie daran, dass „global“ das Fehlen einer Domäne in einem Datensatz bezeichnet.

Eine Tabelle ohne Domänenfeld bedeutet beispielsweise, dass die Tabelle alle globalen Datensätze enthält. Eine Tabelle mit einem Domänenfeld bedeutet, dass jeder Datensatz ohne Domäne eine globale Domäne ist.

Das Wort „global“ befindet sich im Domänenfeld. Es wird automatisch dort platziert, wenn der Datensatz keine Domäne hat.

Globale Datensätze sind für alle Benutzer der Instanz verfügbar, sofern sie nicht durch Sicherheitskonfigurationen eingeschränkt werden.

- Verwenden Sie die Standarddomäne, um sicherzustellen, dass Datensätze nicht in der globalen Domäne in Tabellen landen, die niemals globale Datensätze enthalten dürfen.
- Die Besitzer eine Instanz müssen dann die Datensätze in der Standarddomäne selektieren und in die richtige Domäne verschieben.



Domänenhierarchien

- Über-/untergeordnet: betroffener Prozess und betroffene Daten
  - Design, das auf einem Prozess-Flow basiert.
  - Denken Sie daran, dass die übergeordneten Domänen auf alle Daten in den untergeordneten Domänen zugreifen können.
- Domäne „Enthält“: Nur Daten sind betroffen. Beispiel: Wenn SP im Diagramm „TOP“ enthält, werden Prozesse in SP nicht in der Domäne „TOP“ und abwärts ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Gewährt Personen in Gruppen Datenzugriffsrechte, die dedizierten Zugriff auf bestimmte Domänen erfordern.
- Enthält Ursachen oder Bedingungen, die Datenbankabfragen hinzugefügt werden sollen, die Leistungsprobleme bei großen Domänen und Datensätzen verursachen können

- Sichtbarkeit: Hierarchie, die für Benutzer immer sichtbar ist, sobald Sie Zugriff gewähren. Nur die Daten sind betroffen, nicht die Prozesse.
  - Gewährt einer anderen Domäne, die beim Erstellen der über- und untergeordneten Hierarchie keinen Zugriff hatte, Datenzugriff auf eine Domäne
  - Ermöglicht es Benutzern, alle Daten in den Domänen zu sehen, für die sie Sichtbarkeitszugriff haben, und zwar jederzeit, unabhängig von dem Datensatz, an dem sie gerade arbeiten

> **Hinweis:** Gehen Sie sparsam damit um, da mit „Sichtbarkeit“ vollständiger Zugriff gewähren werden kann, was Sie möglicherweise nicht beabsichtigen.

Grundprinzipien der Definition einer Domänenhierarchie

Uneingeschränkte und eingeschränkte Anwendungsfälle für Domänentrennung.

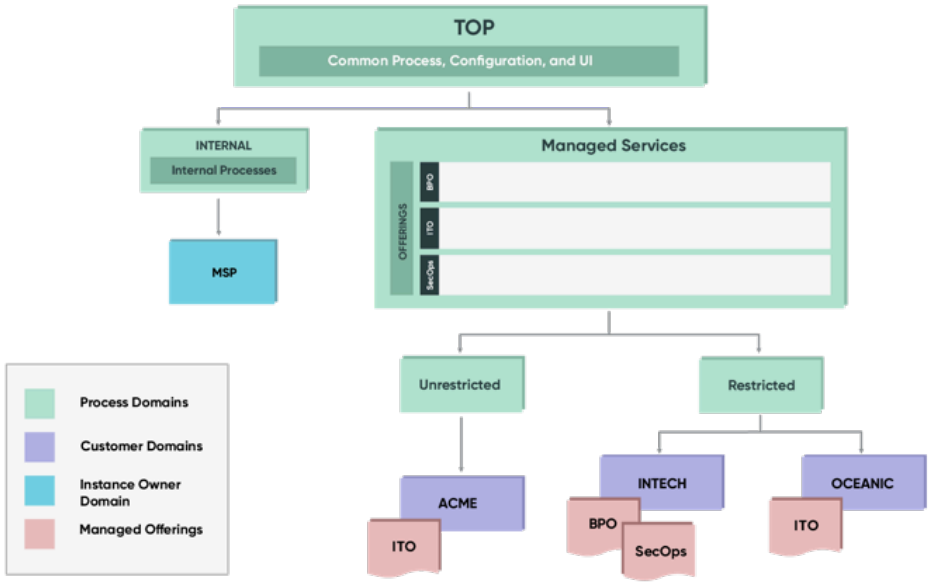
Viele SPs haben Kunden, die implizit angeben, dass der Zugriff auf ihre Domänen streng reguliert werden muss, was die Verwendung der Funktion „Enthält“ in der TOP-Domäne einschränkt. Das folgende Diagramm erläutert, wie diese Regelung durch die Unterteilung der Domänen in eingeschränkte und unbeschränkte Domänen abgeschwächt werden kann.

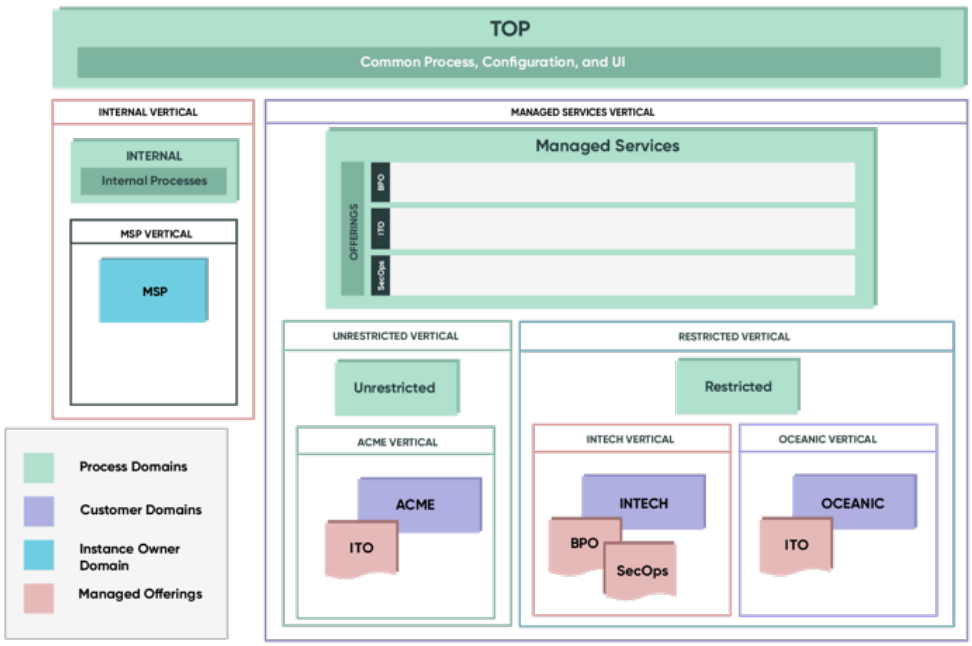
1. Kunden befinden sich in einer bestimmten „Vertikalen“ der Hierarchie der Domänentrennung. Dies bedeutet, dass sie nur Prozesse nutzen, die in ihrer Domäne und allen übergeordneten Domänen in der Hierarchie definiert sind. Alle Prozesse, die in Domänen definiert sind, die sich nicht in ihrer linearen Übergeordnet-Untergeordnet-Hierarchie befinden, gelten nicht.

> **Hinweis:** Kunden oder „Mandanten“ sind Entitäten, die vollständig voneinander getrennt sind, nicht wie Abteilungen oder Geschäftsbereiche, die Ressourcen gemeinsam nutzen.

2. Strikt vertikale Einheiten (beschränkt, Managerservices usw.) sind zulässig, solange die Kunden nur zu einer von ihnen gehören.
3. Services, Produkte oder Angebote, die für alle Kunden horizontal verfügbar sein müssen, werden nicht in separaten Domänenhierarchien definiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





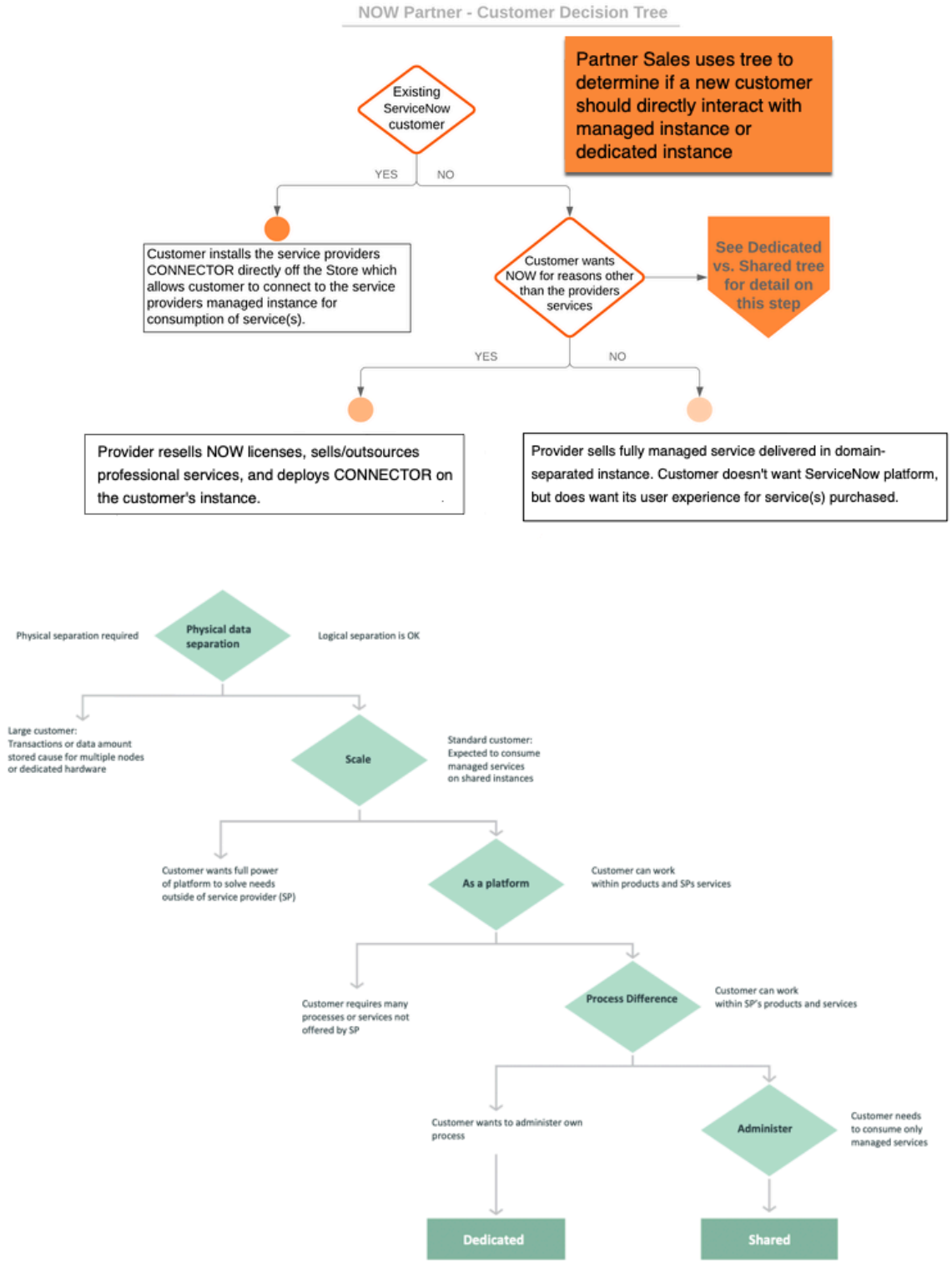
Hier sind einige beispielhafte Anwendungsfälle:

- Sie können beispielsweise unter TOP zwei Domänen erstellen: *Nicht beschränkt* und *Beschränkt*.
  - Platzieren Sie Kunden, die keine SP-Sichtbarkeitsbeschränkungen haben, zusammen mit ihren Domänen unter „Nicht beschränkt“.
  - Platzieren Sie Kunden, die diese Anforderung haben, zusammen mit ihren Domänen unter „Beschränkt“.
- Systemadministratoren können dann die Funktionen „Enthält“ und „Sichtbarkeit“ effizient und gezielt verwenden.
  - Wenden Sie „Enthält“ auf „Nicht beschränkt“ an, sodass ein einziges „Enthält“ den meisten Kunden Sichtbarkeit gewähren kann.
  - Wenden Sie die Domänensichtbarkeit bei Bedarf mithilfe von „Domänensichtbarkeitsgruppen“ auf bestimmte Domänen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kundenentscheidungsbäume

Das folgende Diagramm zeigt, wie Sie das richtige Hierarchiemodell auswählen. Sie können separate Hierarchien, Hybrid-Hierarchien oder freigegebene Hierarchien auswählen, je nachdem, welche Prozesse und Funktionen Sie in Ihren Domänenstrukturen benötigen.



Weitere Informationen zur Hierarchiearchitektur finden Sie unter Referenzarchitektur des Service Providers.

Automatische Übersetzung

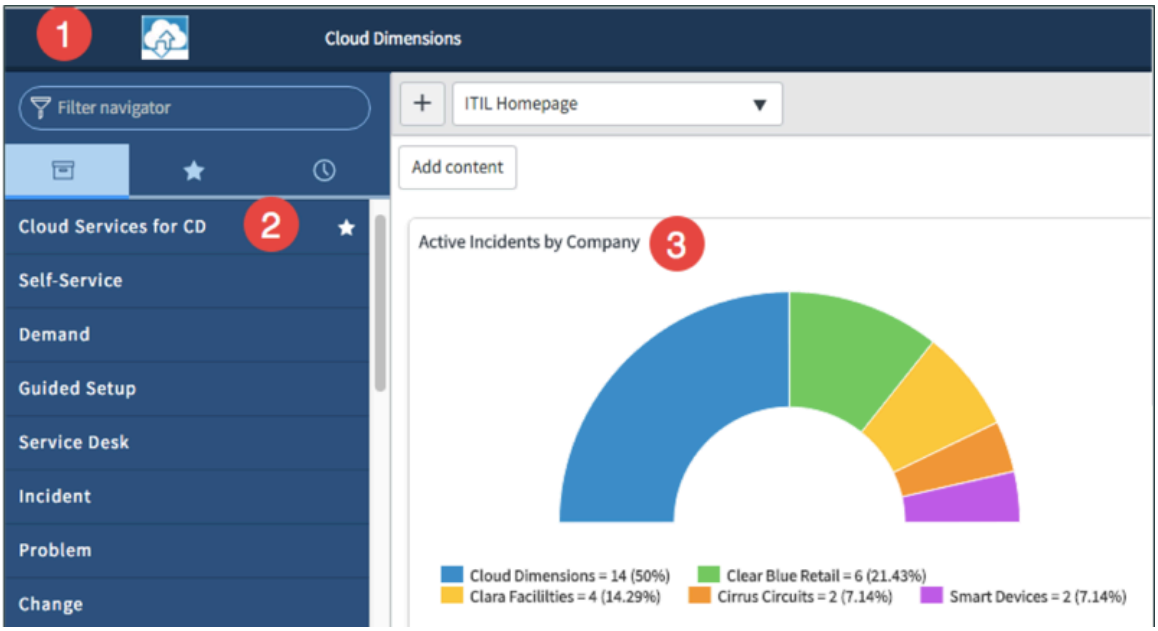
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontext- und Domänentrennung

Der Kontext der Sitzung eines Anwenders bestimmt die Prozesse, Daten und Anwenderoberfläche (UI), während der Anwender Listenansichten, Homepages, Berichte und Wissensartikel durchsucht. Der Kontext wird durch die von Ihnen erstellten Prozesse, die von Ihnen festgelegten Business-Regeln, Ihre Workflows und andere Faktoren bestimmt.

Kontext der Anwendersitzung

Viele Faktoren bestimmen den Kontext einer Anwendersitzung, z. B. Anwenderprofile, Gruppen, Unternehmenskriterien usw. Im folgenden Diagramm sehen Sie, dass die Incidents, die ein Unternehmen erstellt hat, Teil des Kontexts sind.



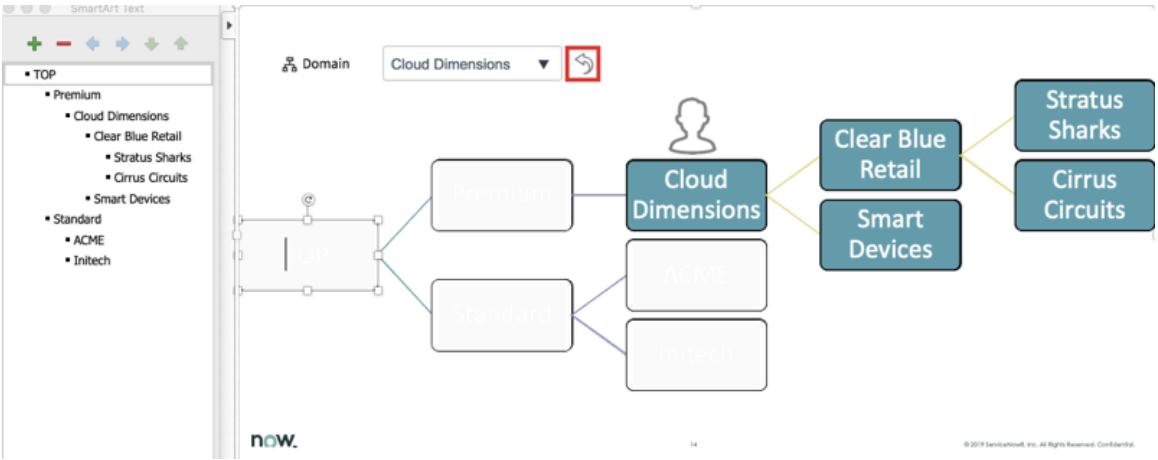
Der Anwender in diesem Beispiel hat eine Startdomäne von Cloud Dimensions.

1. Das Branding spiegelt die Einstellungen in der Domäne „Cloud-Dimensionen“ und im Unternehmensdatensatz wider.
2. Der Anwendungsnavigator zeigt die Elemente an, die von Domänen höherer Ebenen geerbt werden, sowie die Module, die in der Cloud Dimensions-Domäne definiert sind.
3. Die Homepages und Listendaten spiegeln die Daten wider, die für den Anwender sichtbar sind. Diese Daten basieren auf dem Sitzungskontext des Anwenders. In diesem Fall kann der Anwender in der Cloud-Dimensionsdomäne die Daten in Cloud-Dimensionen, untergeordneten Domänen und der globalen Domäne anzeigen.

Der Anwendersitzungskontext startet in der Startdomäne

Im folgenden Diagramm werden die Elemente des Kontexts angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Systemadministrator legt die Home-Domänen von Anwendern in ihren Anwenderdatensätzen fest. Normalerweise ist die Startdomäne eines Anwenders auf dieselbe Domäne wie die Domäne seines Unternehmens festgelegt. Wenn sich der Anwender anmeldet, wird die Domänenauswahl automatisch auf die Heimatdomäne des Anwenders festgelegt. Anwender können jederzeit zu ihrer Heimatdomäne zurückkehren, indem Sie auf das Pfeilsymbol in der Domänenauswahl klicken.

Die Liste der Domänenauswahl enthält Domänen im Sitzungskontext des Anwenders. Anwender können ihren Sitzungskontext weiter einschränken, indem sie untergeordnete Domänen mit der Auswahl auswählen.

Der Kontext der Anwendersitzung enthält die Startdomäne des Anwenders und alle untergeordneten Domänen. Dieser Satz von Domänen im Sitzungskontext des Anwenders wird automatisch an jede Abfrage angehängt, die an die Datenbank gesendet wird. Auf diese Weise sind die Ergebnisse auf die Daten in diesen Domänen und globale Daten beschränkt. Dieser Prozess ist in den kompilierten Code eingebettet, der nicht zugänglich ist.

Service-Accounts, die für Integrationen verwendet werden, verfügen auch über Anwendersitzungskontext. Es gibt Anwenderkontext und Datensatzkontext mit jeweils eigenen Daten in einer eigenen Domäne. Diese Kontexte wirken sich auf die Integrationen aus. Datenbankabfragen (Datensätze) sind auf die gleiche Weise wie interaktive Anwender (Anwender) beschränkt, was bedeutet, dass sie normal funktionieren, aber durch die vom Entwickler konfigurierten Einschränkungen eingeschränkt sind.

Sie können in weitere Möglichkeiten zum Hinzufügen von Domänen zum Sitzungskontext eines Anwenders erfahren Referenzarchitektur des Service Providers.

Datensatzkontext

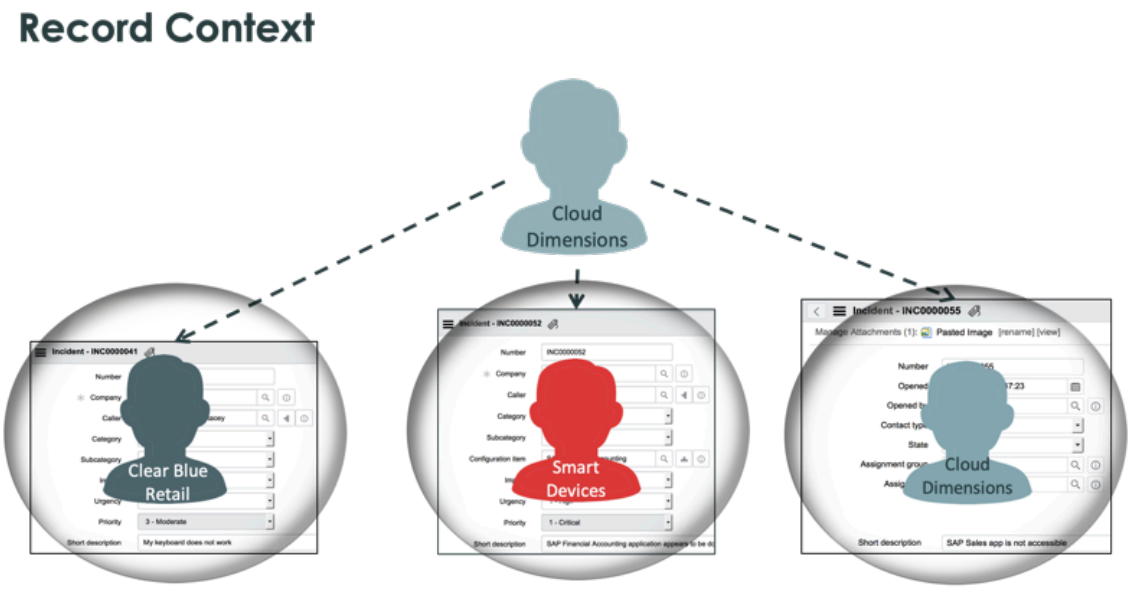
Wenn ein Anwender Drilldown zu einzelnen Datensätzen durchführt, wird der Datensatzkontext aktiviert. Der Datensatzkontext bestimmt die UI-Elemente und Prozesse, die auf den Datensatz angewendet werden sollen.

Die Domäne eines Datensatzes bestimmt den Prozess, die Daten und die Verfügbarkeit von UI-Elementen im Datensatz.

Hinweis:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Datensatzkontext bleibt auch dann bestehen, wenn sich die Domäne des Anwenders ändert.
- Anwender können Datensätze gleichzeitig auf mehreren Browserregisterkarten anzeigen und gleichzeitig ihren eigenen Datensatzkontext beibehalten.

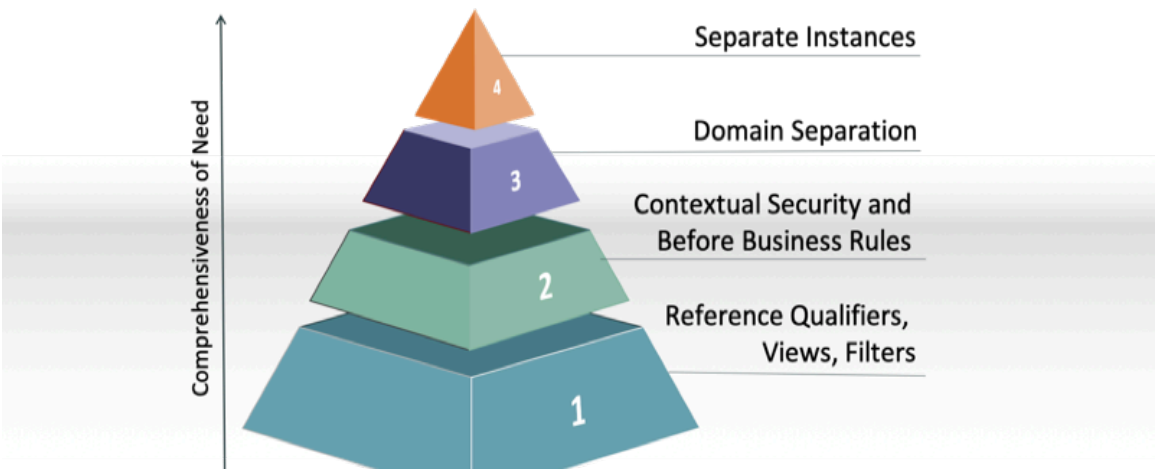


Trennen und Sichern von Daten mit Domänentrennung

Sie können Daten in trennen und sichern ServiceNow Plattform auf verschiedene Arten, je nach den Anforderungen Ihres Kunden.

Trennen von Daten auf mehrere Arten

Das folgende Diagramm zeigt vier Möglichkeiten, wie Sie Daten trennen können. Sie können separate Instanzen, Domänentrennung, kontextbezogene Sicherheits- und Geschäftsregeln und die Referenzarchitektur selbst verwenden, um Daten zu trennen.



Sie können Daten auf folgende vier Arten trennen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Anpassen von Referenzarchitektur Mit Qualifizierern und Filtern, damit Abteilungen und Gruppen innerhalb eines Unternehmens sich auf ihre eigene Arbeit konzentrieren können. Durch die Trennung der Daten zwischen diesen Abteilungen oder Gruppen kann eine Abteilung oder Gruppe die Datensätze einer anderen Abteilung oder Gruppe nicht sehen.
2. Hinzufügen von Business-Regeln für kontextbezogene Sicherheit und vor Abfragen als zusätzliche Sicherheitsebenen zum Schutz vor Datenschutzverletzungen. Siehe Kontext- und Domänentrennung Und Business-Regeln vor Abfrage Um mehr über Domänentrennung und Business-Regeln zu erfahren.
3. Hinzufügen einer weiteren Sicherheitsstufe in einem Unternehmen mithilfe der Domänentrennung. Die Daten aus jeder Datenbankabfrage sind auf die Daten beschränkt, die in einer Domäne sichtbar sind, bevor kontextbezogene Sicherheits- und Business-Regeln ausgeführt werden.
4. Verwenden Sie separate Instanzen, um die Daten auf Datenbank- und Anwendungsebene zu trennen.

Separate Instanzen, Domänentrennung, kontextbezogene Sicherheits- und Geschäftsregeln und die Referenzarchitektur sind Möglichkeiten zur Trennung von Daten. Diese vier Möglichkeiten beziehen sich zueinander, wie durch die Verständlichkeit des Bedarfspfeils im Diagramm angezeigt. Wie jede Ebene mit den anderen Ebenen interagiert, hängt davon ab, wie Sie Ihre Domänentrennungskonfiguration einrichten.

Nicht alle Organisationen erfordern Domänentrennung. Möglicherweise finden Sie andere Alternativen, z. B. separate Instanzen oder eine einzelne Instanz ohne Domäne. Weitere Informationen zu diesen Alternativen finden Sie unter Bewertung der Notwendigkeit für Domänentrennung.

Mandantenübergreifende Intelligenz

In einer Architektur mit mehreren Mandanten haben Sie eine einzelne Instanz, die mehrere Mandanten bedient. Daten, Metadaten, Geschäftslogik und Verarbeitungskontext für Mandanten werden automatisch mit Zugriff auf zusätzliche Mandantendaten verarbeitet.

Einzelne im Vergleich zu mehreren Mandanten

Einzelmandanteninstanz

Sie sind ein ServiceNow Kunde, Sie haben die Lizenzen gekauft, und es liegt an Ihnen, zu entscheiden, welche Services Sie möchten. Sie können bei Bedarf ein Upgrade durchführen, Vorschauen aller großartigen neuen Funktionen anzeigen und Ihre Instanz sofort konfigurieren. Ein einzelner Mandant hat diese Vorteile und Einschränkungen:

- Sie haben höhere Vorlaufkosten und Verwaltungsaufwand, aber Sie haben mehr Freiheit beim Umbauen und erweitern.
- Sie haben höhere Kosten für die Beschaffung und Wartung der Instanz- und Lieferverwaltungspersonal. Obwohl Sie die Umgebung nach Bedarf erstellen können, müssen Sie die Anforderungen einhalten ServiceNow Empfohlene Praktiken und Standards.

Instanz mit mehreren Mandanten

Eine andere Person besitzt die Instanz, möglicherweise ein Service Provider mit mehreren Kunden. Sie führen ein Upgrade durch, wenn sie möchten, und setzen neue Services auf die Instanz, wenn sie möchten. Wenn Sie Kunde eines Service Providers sind, sind Sie höchstwahrscheinlich in seiner Instanz, da

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie das wollten, was er bietet. Mehrere Mandanten haben diese Vorteile und Einschränkungen:

- Ein zentralisiertes Personal verwaltet Konfigurationen, Integrationen und Upgrades.
- Der Instanzbesitzer stellt hinzugefügte Services bereit.
- Domänenmandanten haben niedrigere Vorlaufkosten für die Verwendung von ServiceNow Plattform hat niedrigere monatliche Kosten, da sie sie für viele Mandanten freigeben und keine Mitarbeiter für die Verwaltung der Umgebung beschäftigen müssen.
- Vorteile, die aus Anforderungen oder Changes geteilt werden, die von anderen Mandanten initiiert wurden.

Alternativen zur Domänentrennung

Sie können eine separate Instanz als Alternative zur Domänentrennung für Ihre Kunden verwenden. Eine separate Instanz ermöglicht Ihnen die Flexibilität, die Anforderungen für die Datentrennung innerhalb der Gruppen und Abteilungen in einer Organisation zu erfüllen, ohne dass dies Auswirkungen auf andere hat.

Separate Instanzen

Vor- und Nachteile separater Instanzen

Separate Instanz	Einzelinstanz – ohne Domäne
Vorteile	**Vorteile**
Für jeden Kunden/jede Organisation konzipiert	Kann einfache Szenarien behandeln
Minimieren Sie die Auswirkungen der Anpassung auf andere	Kosten
Abstimmung des Release-Zeitplans	**Nachteile**
Trennung bereinigen	Umfangreiche Änderungen am Baseline-Code
Wählen Sie die RECHENZENTRUMSREGION aus	Geänderter Basissystemcode während Upgrades übersprungen
Nachteile	Muss auch alle sekundären und unterstützenden Tabellen berücksichtigen
Kosten	Umfangreiche Tests erforderlich
Ausrichtung von Instanzen	Nein ServiceNow Produktteam zur Entwicklung Ihres anwenderdefinierten Codes
Testaufwand für Upgrades	
Doppelter Aufwand	
Integrationen erforderlich	

Sie können Upgrades und Releases für jede Instanz separat zeitlich festlegen. Wenn Sie jedoch separate Instanzen verwenden möchten, müssen Sie eine Menge Koordination mit anderen Personen durchführen, die Instanzen verwalten. Indem Sie eine Instanz mit kontextbezogener Sicherheit, Formularansichten, Referenzqualifizierern, Filtern und robusten Bedingungen konfigurieren, Sie müssen in Ihrem Unternehmen keine Domänentrennung verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit einer separaten Instanz können Sie Daten- und Prozesstrennung behandeln, aber Ihre Instanzbesitzer müssen die umfangreichen Anpassungen, die für separate Instanzen erforderlich sind, verwalten und mit ihnen Schritt halten.

Zugehörige Informationen

Kontext- und Domänentrennung

Referenzarchitektur des Service Providers

Bewertung der Notwendigkeit für Domänentrennung

Möglicherweise funktioniert die Domänentrennung nicht immer für die Organisationen Ihrer Kunden. Es ist am besten, wenn Sie Ihre Entscheidung für die Domänentrennung anhand der Anforderungen Ihrer Kunden treffen.

Bewertung der Notwendigkeit für Domänentrennung

Gründe für Domänentrennung

Diese Faktoren können Ihnen helfen, die Domänentrennung für die Organisationen Ihrer Kunden zu wählen:

- Ihre Kunden haben eine moderate Ausrichtung der Prozesse und allgemeinen Plattformanforderungen.
- Ihre Kunden planen, Aufgaben als Erfüller und nicht als anfordernde Personen zu bearbeiten.
- Ihre Kunden haben eine vertragliche Vereinbarung, die die Isolierung von Datensätzen erfordert, aber Ihr Instanzbesitzer hat festgestellt, dass die Anforderung an anderer Stelle in der Konfiguration erfüllt werden kann.
- Die Instanzbesitzer Ihres Unternehmens verfügen über ganze Entitäten, die als physisch getrennte Organisationen arbeiten und keine Daten freigeben, aber eine vollständige Berichterstellung ist weiterhin erforderlich. Separate Domänen ermöglichen Datensichtbarkeit, wenn sie richtig konfiguriert sind.

Gründe für keine Domänentrennung

Diese Faktoren können auf Gründe hinweisen, warum die Organisationen Ihrer Kunden möglicherweise nicht die Domänentrennung einrichten möchten:

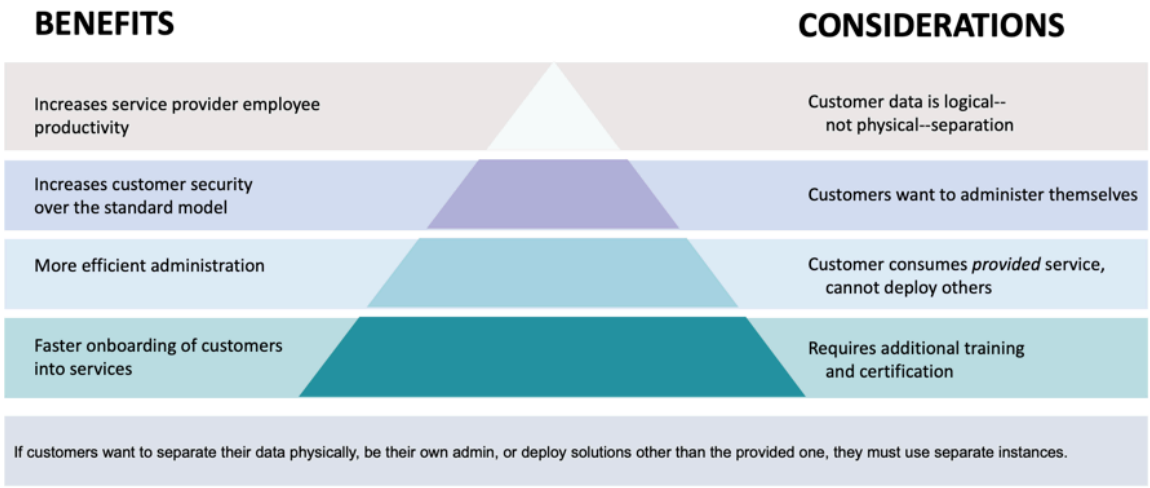
- Ihre Kunden möchten ihre Umgebung verwalten, die Umgebung vollständig besitzen und die Roadmap für die Erweiterung festlegen.
- Ihre Kunden verlangen, dass die Daten und Prozesse auf physischer Ebene oder auf Datenbankebene vollständig isoliert sind.

Hinweis:

Domänengetrennte Instanzen enthalten eine gemeinsam genutzte Datenbank, sodass die Isolationsanforderung untergraben wird.

- Abteilungen in der Organisation Ihrer Kunden möchten Datensätze isolieren. (Zugriffssteuerungen reichen möglicherweise aus.)
- Ihre Kunden wünschen sich alle ihre eigenen Prozesse, Geschäftsregeln und Workflows.
- Die Unternehmenskultur ist eine der nicht-Zusammenarbeit zwischen den Organisationen Ihrer Kunden.
- Ihre Kunden interagieren nur als Endanwender mit der Plattform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

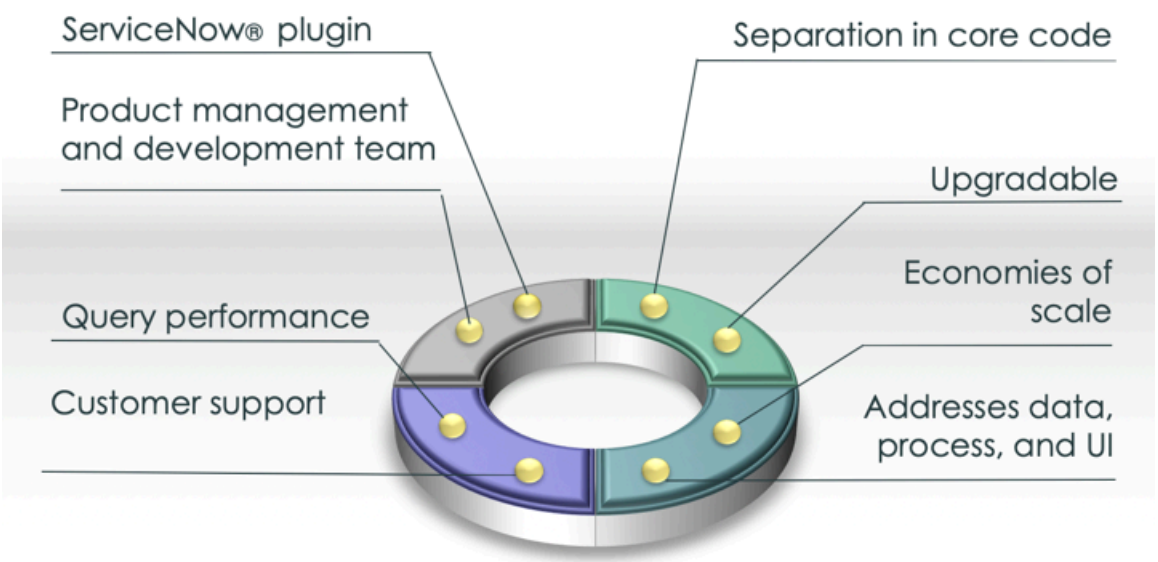


Vorteile der Domänentrennung

Domänentrennung kann für die Organisationen Ihrer Kunden besser funktionieren als jede andere Methode zum Trennen der Daten zwischen Gruppen und Abteilungen.

Vorteile der Domänentrennung auf einen Blick

Sie können die Domänentrennung mit aktivieren ServiceNow Plugin mit Funktionen, die in die Kernplattform integriert sind. Die Konfiguration separater Domänen wird von einem Produktmanager verwaltet, der von einem Entwicklungsteam unterstützt wird. Erweiterungen und Korrekturen für die Domänentrennungsfunktion sind in enthalten ServiceNow Releases und bereit für die Verwendung durch Kunden. Für Unterstützung bei der Domänentrennung können Ihre Instanzbesitzer verwenden Kundenservice und Support Ressourcen, z. B. Serviceportal .



Funktionsweise einer Datenbankabfrage mit Domänentrennung

Die Verwendung von Datenbankabfragen mit Domänentrennung in den Anwendungen Ihrer Kunden hilft ihnen, ihre Daten zu schützen. Diese Abfragen beschleunigen dann die Konfigurations- und Build-Prozesse.

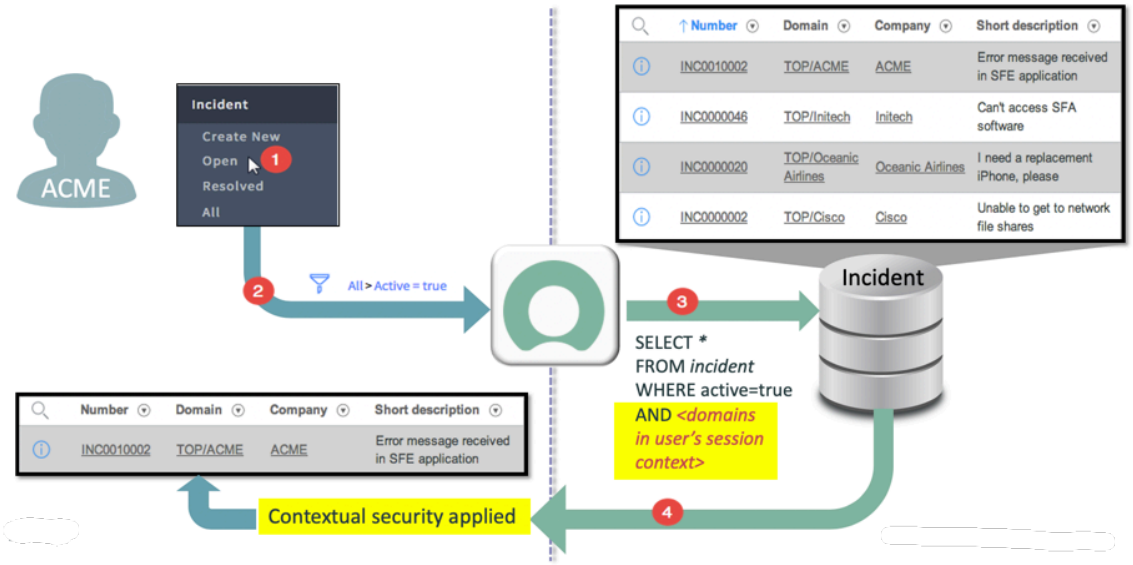
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie die Domänentrennung Daten schützt

In der folgenden Abbildung enthält die Incident-Tabelle [Incident] ein Domänenfeld, das von der Aufgabe des Incident übernommen wird. Wenn Sie dieses Domänenfeld sehen, wissen Sie, dass die Datensätze in der Tabelle Domänenzuweisungen haben können.

Wenn sich Anwender anmelden, wird ihre Startdomäne mit den Domänen angezeigt, auf die sie zugreifen können. Dies wird als Sitzungskontext des Anwenders bezeichnet. Weitere Informationen zu Sitzungskontexten finden Sie unter Kontext- und Domänentrennung.

Datenbankabfrage mit Domänentrennung



1. In einem Browser wählt der Anwender aus einem der Unternehmen, Acme, das Modul offene Incidents aus, um alle Incidents anzuzeigen, bei denen Active=wahr ist.
2. Der Filter Active=true wird an die Anwendung übermittelt.
3. Die Anwendung sendet dann eine Abfrage an die Datenbank, indem eine WHERE-Klausel an Active=true angehängt wird. Die WHERE-Klausel schränkt die Incident-Datensätze ein, die auf die Datensätze zurückgegeben werden, die sich in der Domäne des Anwenders befinden oder auf die der Anwender zugreifen kann. Nur die Datensätze in diesen Domänen werden zur Verarbeitung an die Anwendung zurückgegeben.
4. Kontextbezogene Sicherheit wird angewendet, wodurch die Daten, die an den Anwender zurückgegeben werden, weiter eingeschränkt werden. Die Incident-Datensätze werden in der Liste offene Incidents angezeigt.

Hinweis:

Wenn Sie kontextbezogene Sicherheit anwenden, erstellen Sie Grenzwerte für die Daten, die an den Anwender zurückgegeben werden. Diese Grenzwerte schützen andere Inhalte, die Anwender möglicherweise nicht sehen sollen.

Weitere Informationen zur kontextbezogenen Sicherheit finden Sie unter Kontext- und Domänentrennung.

Hinweis: Diese Verarbeitungslogik gilt für alle Abfragen für die Datenbank, einschließlich der Abfragen, die mithilfe von Integrationen ausgelöst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufen für Domänentrennung

Wählen Sie aus drei Kategorien für die Domänentrennung einer Anwendung für die Organisationen Ihrer Kunden aus.

Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und die Datenweiterleitung, verfügen über erweiterte Geschäftslogik-Trennung oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kunden). Diese Definitionen beschreiben die Supportstufen aus der Perspektive tatsächlicher Anwendungsfälle und der Personen, die sie implementieren.

Inkrementell ServiceNow Supportstufen



Ebene	Typ	Zusammenfassung
Kein Support		• Das Domänenfeld kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden. • Diese Ebene wird nicht als domänengetrennt betrachtet.
Standard	Kundendatenverwaltung	• Geschäftslogik: Stellt sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Service Providers der Anwendung gelangen. • In der Anwendung, Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups, Zusammenfassungen usw. berücksichtigen alle die Eigenschaften der Domäne zur Laufzeit. • Ihre Instanzbesitzer müssen die Anwendung so einrichten können, dass sie normal über mehrere Mandanten hinweg funktioniert. Anwendungsfall: Wenn ein Service Provider Chat verwendet, um auf die Nachricht eines Kunden zu antworten,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ebene	Typ	Zusammenfassung
		muss der Client die Antwort sehen können.
Standard	Kundenprozessmanagement	• Enthält die Basisebene • Geschäftslogik: Prozesse können pro Kunde vom Service Provider erstellt oder geändert werden. Die Anwendungsfälle spiegeln wider, wie die Anwendung von mehreren Service Provider-Kunden in einer einzigen Instanz verwendet wird. • Ihre Instanzbesitzer müssen in der Lage sein, die Geschäftslogik und Datenparameter für ein Minimum praktikables Produkt (MVP) pro Kunde für die spezifische Anwendung zu konfigurieren. Anwendungsfall: Der Administrator muss in der Lage sein, Kommentare erforderlich zu machen, wenn ein Datensatz für einen Kunden geschlossen wird, aber nicht für einen anderen Kunden.
Erweitert	Vom Kunden selbst verwaltete Konfiguration	• Enthält Basis- und Standard-Ebenen • Ermöglicht Service Provider-Kunden das Ändern der Geschäftslogik, die auf definierten Anwendungsfällen basiert. Diese Konfigurationen sind UI-basiert und fehlersicher, sodass Konfigurationen eines Kunden keinen anderen Kunden betreffen können. • Die Instanzkunden müssen in der Lage sein, die MVP-Geschäftslogik und Datenparameter selbst zu konfigurieren. Anwendungsfall: Der Kunde einer gemeinsam genutzten Umgebung muss in der Lage sein, Änderungen gemäß Auswirkung, Dringlichkeit oder Priorität innerhalb einer Domäne vorzunehmen.
Effektive Domäne*		In einigen Fällen unterstützt eine Plattformfunktion oder -Anwendung Serviceanbieter-Anwendungsfälle, auch wenn das Domänen-Framework nicht verwendet wird. Die Anwendungsfälle müssen detailliert sein, um die Domänentrennung zu unterstützen. Ein Sternchen (*) nach der Supportstufe gibt diese Art von Konfiguration an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ebene	Typ	Zusammenfassung
		Anwendungsfall: Vor New York, Servicekatalog Hatte keine Domänenunterstützung, aber die Instanzbesitzer konnten separate Kataloge und Elemente für jeden Mandanten in einer domänengetrennten Instanz mithilfe von Anwenderkriterien konfigurieren. Das Ergebnis war, dass jeder Mandant Servicekatalog auf Standardebene verwenden konnte.

Informationen zum Anzeigen aller Anwendungen, die nach ihrer Supportstufe aufgelistet sind, finden Sie unter Anwendungssupport für die Domänentrennung.

Zusammenfassung

Domänentrennung ist ein Framework, das Sie verwenden müssen, um Ihre Anwendungen auf ihre Kunden aufmerksam zu machen.

Berücksichtigen Sie die Fähigkeiten des Domänen-Frameworks, die Geschäftsanwendungsfälle Ihrer Anwendungen, die Personas und die Verwendung der Anwendung, bevor Sie das Framework verwenden können, um Ihre Anwendung unterstützbar zu machen.

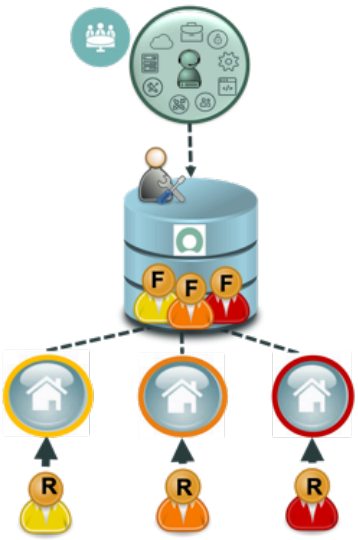
Referenzarchitektur des Service Providers

Ihre Kunden können über ein Portal auf Service Provider-Services (SP) zugreifen, das für sie konzipiert ist, um ihre domänengetrennte Instanz zu erreichen.

Grundlegende Attribute der Referenzarchitektur des Service Providers

- Sie weisen einer Domäne keine Erfüller zu. Stattdessen teilen Sie sie domänenübergreifend. Dies macht es schwieriger, zu auditieren, wie viele Erfüller Sie pro Domäne haben.
- Sie können die Domänenverwaltung freigeben und nutzen. Dies bedeutet, dass kein Overhead besteht und Sie Lizenzen optimieren können.
- Die Anzahl der Anwender in der Instanz kann sich ändern, wenn Sie einen neuen Kunden erhalten. Ein neuer Kunde kann zu Zehntausenden oder sogar Hunderttausenden neuer Anwender im System führen. Die Gesamtzahl der Anwender ist in einer gemeinsam genutzten Umgebung praktisch unbegrenzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- SP customers access SP services via a portal to the SP Domain Separated instance
- SP uses ServiceNow shared instance(s) to manage their service delivery
- SP could have a shared instance per region to support data sovereignty requirements

Legend:

Centralized governance at the SP

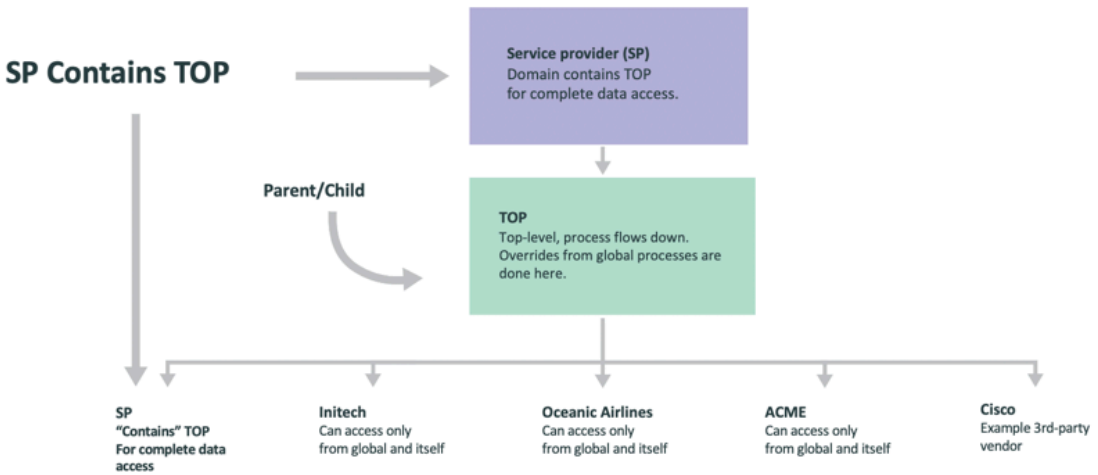
Centralized administration at the SP. Shared business requirements and configurations

Both SP and customer fulfillers on one instance

Customer requesters on each instance

Das Portal für SP-Services ist für die gemeinsam genutzte SP-Instanz dediziert oder freigegeben. Service Provider verwenden ServiceNow Freigegebene Instanzen zur Verwaltung ihrer Servicebereitstellung.

Referenzhierarchie für domänengetrennte Instanzen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der SP-Referenzarchitektur

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

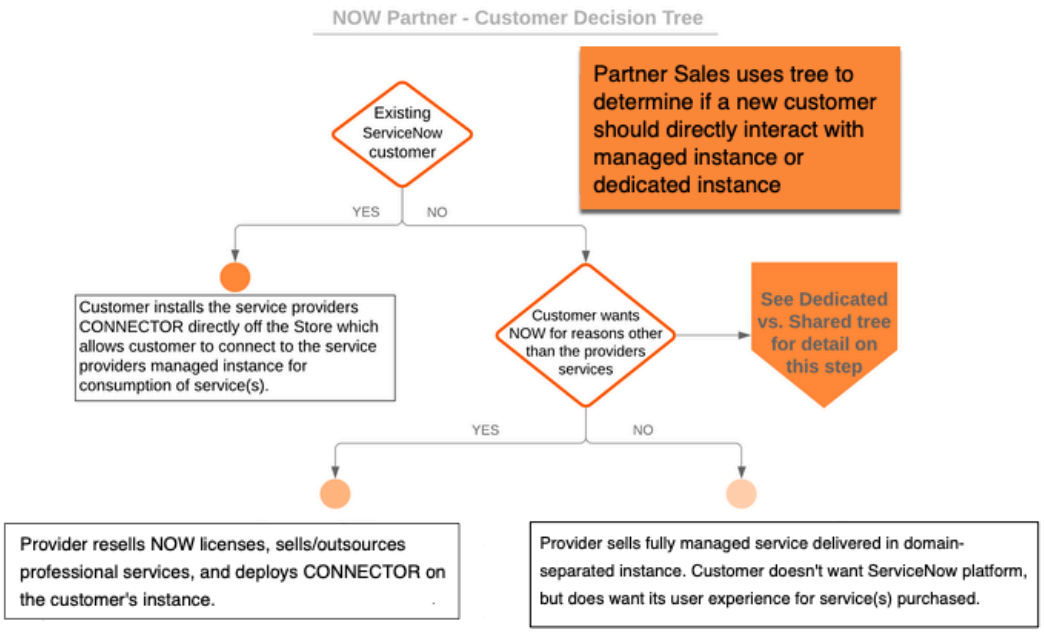
Entscheidungsstrukturen der Referenzarchitektur des Service Providers

Sie können Entscheidungsstrukturen und ein Vergleichsdiagramm verwenden, um zu bestimmen, ob ein neuer Kunde einer gemeinsam genutzten Instanz oder ihrer eigenen dedizierten Instanz hinzugefügt werden soll.

Entscheidungsstrukturen

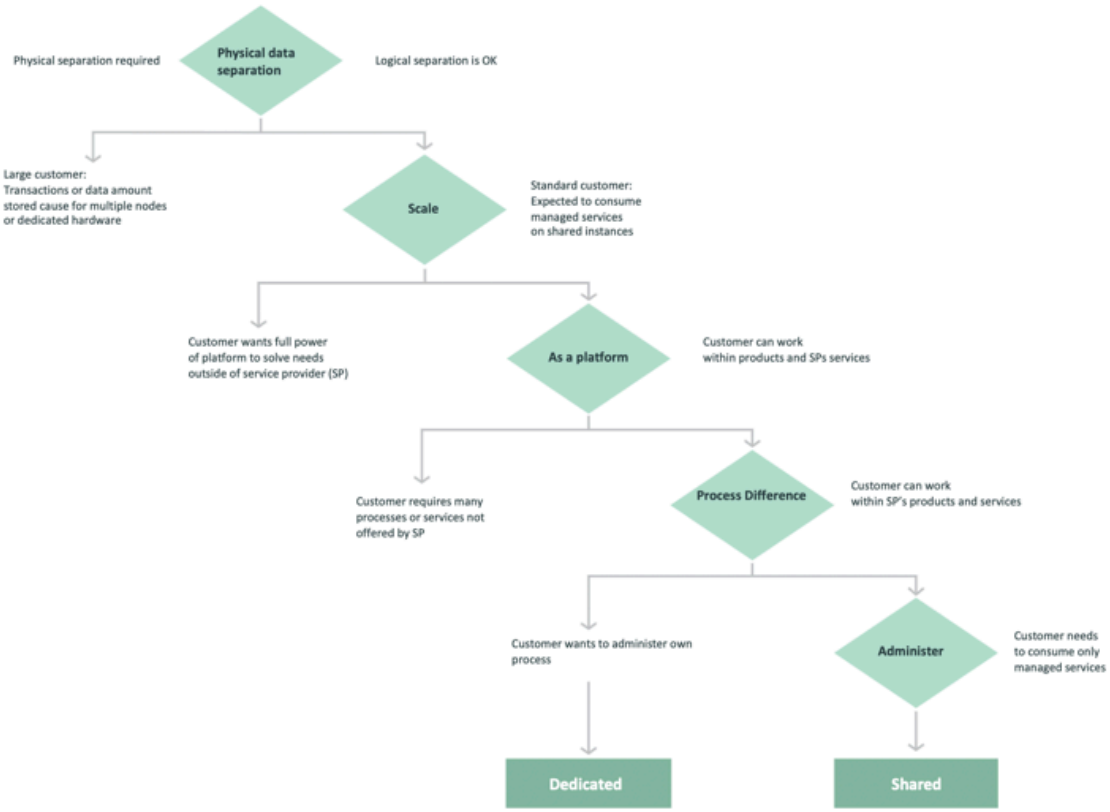
Verwenden Sie diese Entscheidungsstrukturen, um Ihren Kunden zu helfen, zu entscheiden, ob eine verwaltete oder dedizierte Instanz verwendet werden soll.

Kundenentscheidungsstruktur



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Vergleich der SP-Referenzarchitektur

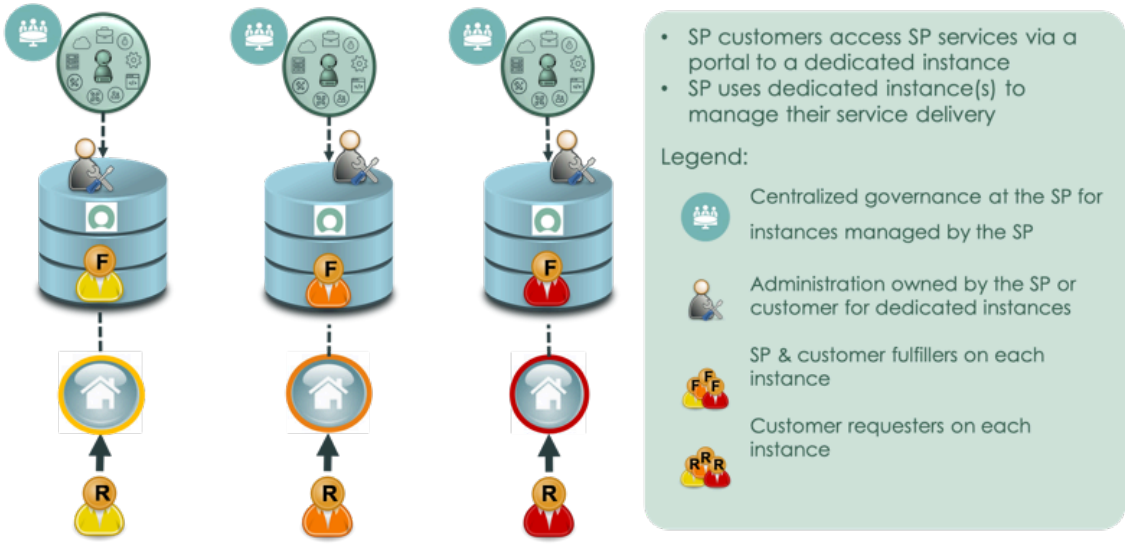
Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Referenzarchitektur des Service Providers für dedizierte Instanzen

Service Provider-Kunden (SP) können über ein Portal zu einer dedizierten Instanz auf SP-Services zugreifen. SPS verwenden diese dedizierten Instanzen, um ihre Servicebereitstellung zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dedizierte Instanzen



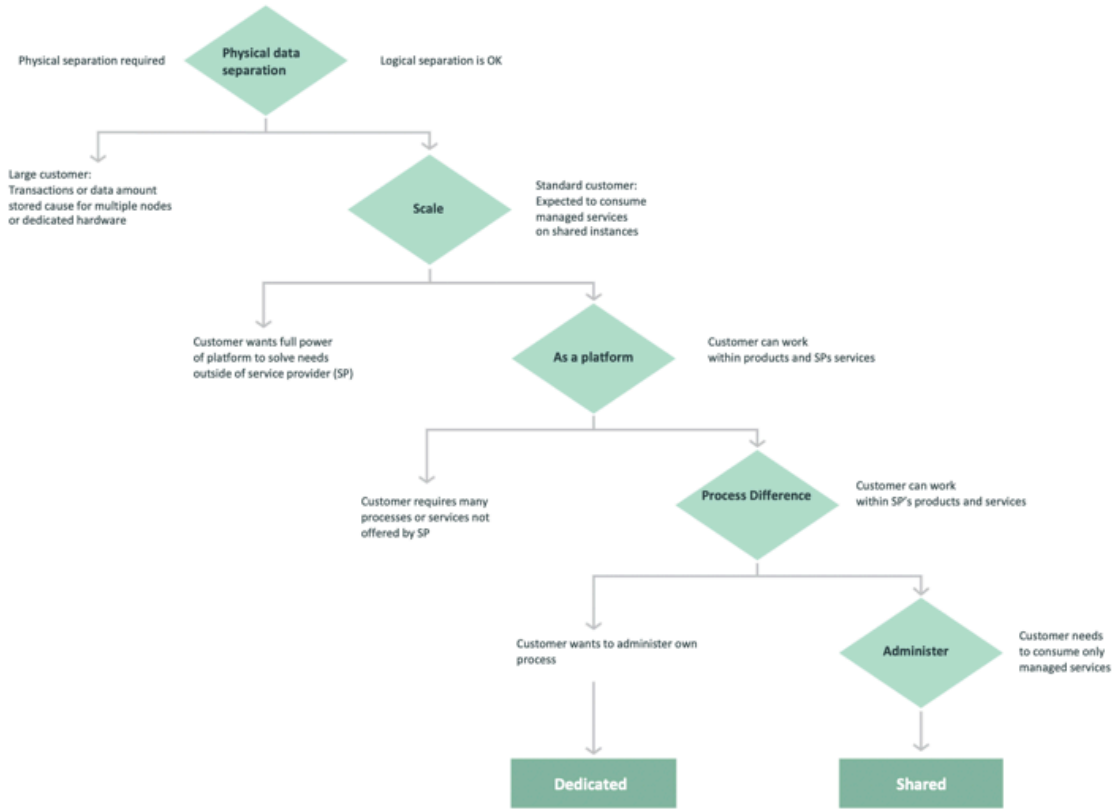
Attribute

- Dedizierte Instanzen erfordern eine separate Verwaltung und dedizierte Teams. Sie benötigen mehrere Lizenzen für die Administratoren und Entwickler, die sich bei mehreren Instanzen anmelden.
- Jede Instanz hat eine begrenzte Anzahl von anfordernden Personen und Erfüller. Wenn Sie einen neuen Kunden erhalten, müssen Sie eine Instanz beschaffen, die auf der Größe und dem Umfang des Unternehmens Ihres Kunden basiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Freigegebene Instanz

Dedizierte vs. Freigegebene Instanz



Vergleich der SP-Referenzarchitektur

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Service Provider-Referenzarchitektur für Hybrid

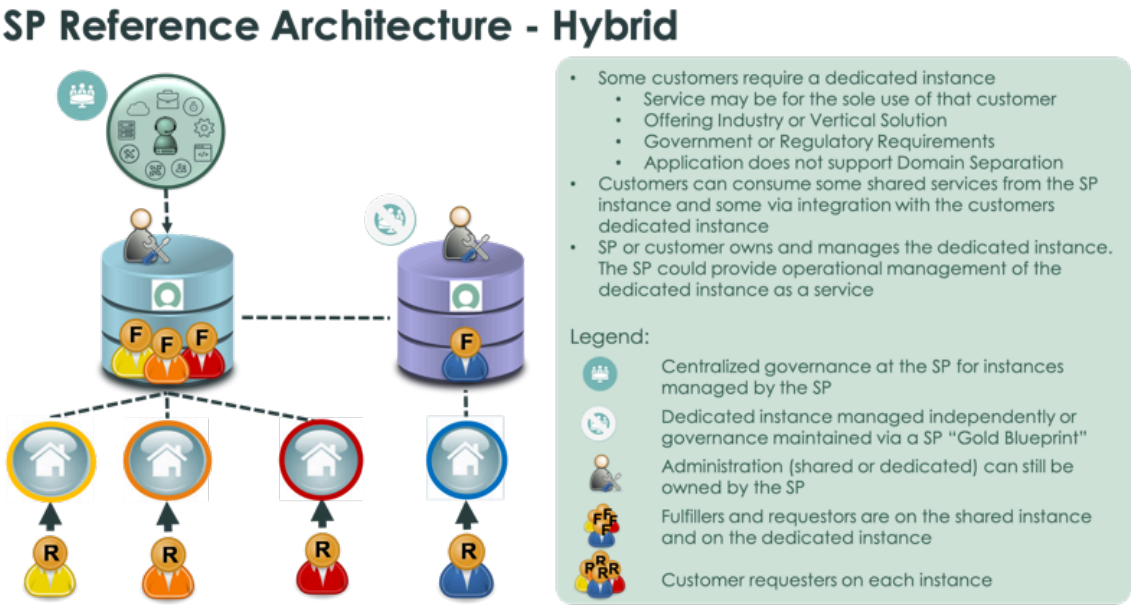
Verwenden Sie die Referenzarchitektur des Hybrid Service Providers (SP) für eine anwenderdefinierte Lösung. Ihre Kunden benötigen eine dedizierte Instanz für einen bestimmten Service. Sie können die gemeinsam genutzte SP-Instanz weiterhin für andere Services verwenden, erfordern jedoch die Integration jeder Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hybridarchitektur

Ihr Kunde kann für die direkte Bereitstellung dieses zusätzlichen Service verantwortlich sein. Sie müssen eine Hybridlösung mit mehreren Attributen erstellen, die Ihr Kunde bereitstellen kann.



Attribute

- Sie können die Verwaltung der Instanz freigeben und nutzen. Dies bedeutet, dass kein Overhead besteht und Sie Lizenzen optimieren können.
- Wenn eine neue Instanz für eine dezentrale Umgebung vorhanden ist, ist das Programmteam verantwortlich und entsprechend als dedizierte Administratoranwender für diese Instanz finanziert. In einer zentralen Umgebung, in der alle Instanzen aus einem Blueprint stammen, benötigen Sie doppelte Administrationslizenzen.
- Sie weisen einer Domäne keine Erfüller zu. Stattdessen können Sie sie domänenübergreifend freigeben.
- Wenn ein Kunde sowohl eine gemeinsam genutzte Umgebung als auch eine dedizierte Umgebung freigibt, benötigt er in beiden Umgebungen einen Erfüller. Dies bedeutet mehr Arbeit für jedes Team, da die Prozesse für freigegebene und dedizierte Instanzen unterschiedliche Arbeit für jede Instanz erfordern.
- Die Anzahl der Anwender in der Instanz kann sich ändern, wenn Sie einen neuen Kunden erhalten. Ein neuer Kunde kann zu Zehntausenden oder sogar Hunderttausenden neuer Anwender im System führen. Die Gesamtzahl der Anwender ist in einer gemeinsam genutzten Umgebung praktisch unbegrenzt.
- Jede Instanz hat eine begrenzte Anzahl von anfordernden Personen und Erfüller. Wenn Sie einen neuen Kunden erhalten, müssen Sie eine Instanz beschaffen, die auf der Größe und dem Umfang des Unternehmens Ihres Kunden basiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der SP-Referenzarchitektur

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

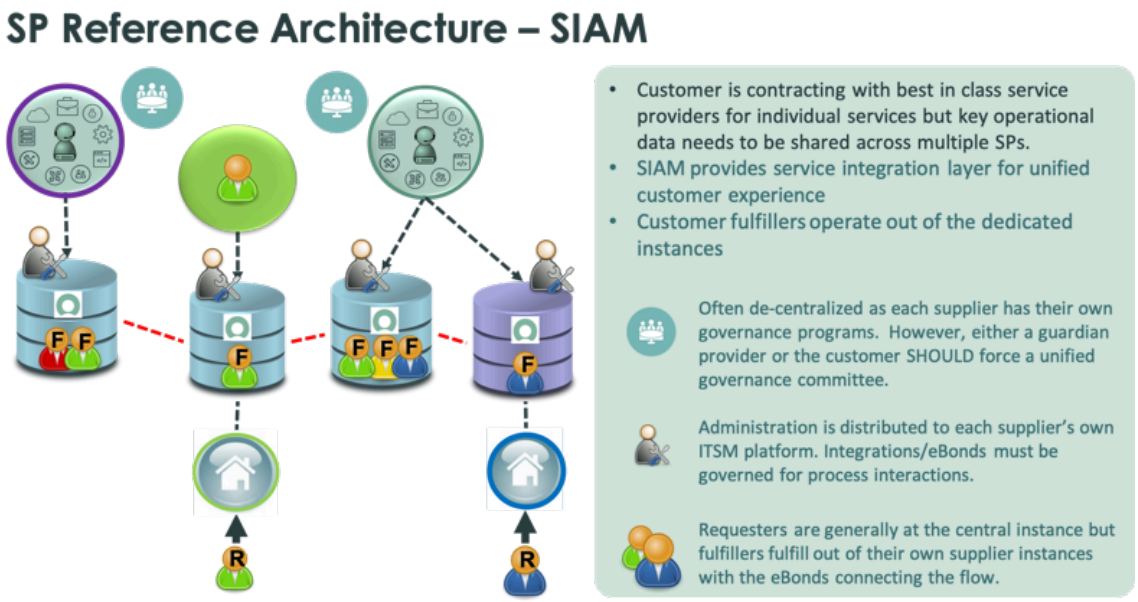
Referenzarchitektur des Service Providers für Verwaltung von Serviceintegrationen(SIAM)

Die Verwaltung von Serviceintegrationen Die Architektur von Service Integration and Management (SIAM) für Service Provider (SP) integriert Services für eine einheitliche Kunden-Experience.

Attribute der SIAM-Architektur

- Kunden greifen auf SP-Services über ein dediziertes oder freigegebenes Portal auf die freigegebene SP-Instanz zu.
- SPS-Verwendung ServiceNow Freigegebene Instanzen zur Verwaltung ihrer Servicebereitstellung.

SIAM-Architektur auf einen Blick



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der SP-Referenzarchitektur

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

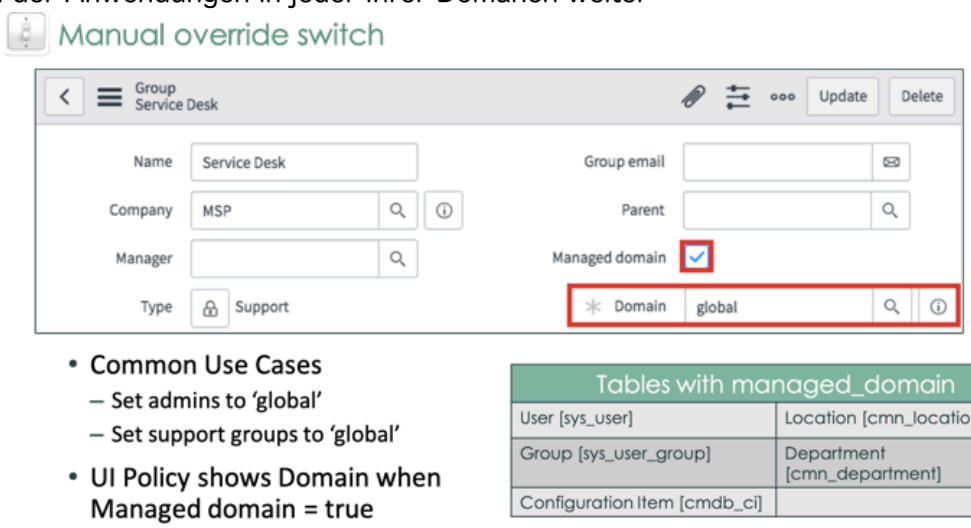
Domänentrennungsbegriffe

Mit ServiceNow Instanz können Sie die Effizienz verbessern, die Sicherheit erhöhen und die Leistung Ihrer Kundenorganisationen steigern. Es ist hilfreich, einige der häufigsten Begriffe beim Erstellen Ihrer Konfigurationen zu verstehen.

Verwaltete Domäne

In einer verwalteten Domäne die **Verwaltete Domäne** Mit dem Feld können Domänenadministratoren manuell eine Domäne für den Anwender, die Gruppe, die Abteilung, den Standort oder den CI-Datensatz auswählen. anstatt die Domäne zu verwenden, die automatisch aus dem Unternehmensdatensatz zugewiesen wird.

Wenn Sie diese Eigenschaften ändern möchten, können Sie sie überschreiben, um die Funktionen der Anwendungen in jeder Ihrer Domänen weiter



anzupassen.

Prozesstabellen

Wenn in Prozesstabellen ein Wert in angezeigt wird **Überschreibungen [sys_overrides]** Feld ist ein Prozessüberschreibungsdatensatz vorhanden. Das bedeutet, dass die delegierte Verwaltung in Kraft ist, mit der Administratoren domänenspezifische Richtlinien festlegen

Automatische Übersetzung

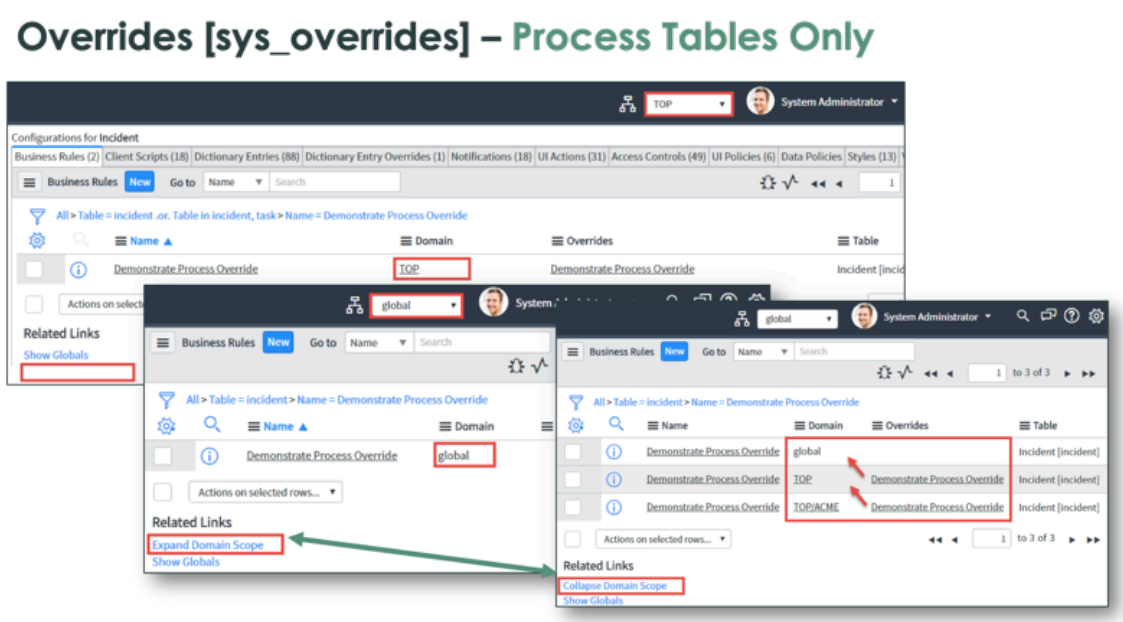
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können. Administratoren in der globalen Domäne können verwenden **Erweitern/Reduzieren Sie Den Domänenbereich** Zugehöriger Link zum Anzeigen von Überschreibungsdatensätzen.

Hinweis: Berichte sind in Domänen getrennt und enthalten einen **Überschreibungen** Feld. Um alle Berichte aus der globalen Domäne anzuzeigen, verwenden Sie die **Erweitern Sie Den Domänenbereich** Zugehöriger Link.

Wenn Sie Prozesstabellen aus einer Domäne anzeigen, werden nur die relevanten Prozessdatensätze für die ausgewählte Domäne angezeigt. Wenn Sie eine Prozesstabelle aus der globalen Domäne anzeigen, wird die angezeigt **Erweitern Sie Den Domänenbereich** Der zugehörige Link wird angezeigt, damit Sie alle Prozessdatensätze anzeigen können, einschließlich Überschreibungen. Um nur die relevanten Prozessdatensätze für global erneut anzuzeigen, verwenden Sie die **Domänenbereich Reduzieren** Zugehöriger Link.

Die Domänenbereichsfunktion wird nur für Prozesstabellen verwendet und bewirkt, dass die Sichtbarkeit von Daten in der Tabelle in die entgegengesetzte Richtung verschoben wird. Beispielsweise kann ein Datensatz in der übergeordneten Domäne im untergeordneten Element angezeigt werden, ein übergeordnetes Element kann keinen untergeordneten Datensatz sehen. Dadurch kann der Prozess zu untergeordneten Domänen abgeleitet werden.



Typen von Domänen

Verschiedene Arten von Domänen können Ihnen helfen, Ihre Prozesse und Daten und ihre Funktionsweise in der Anwendung oder Funktion zu organisieren.

Kundendomäne

In der Domäne des Kunden befinden sich die Anwenderoberfläche sowie der Prozess, der steuert, wie die Daten verwendet werden.

Die ACME-Domäne im folgenden Bild ist eine Kundendomäne.

Prozessdomäne

Sie erstellen Prozesse dafür, wie die Daten verwendet werden und was sie in der Domäne tun. Diese Prozesse müssen diese Attribute haben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bestimmte Prozesse und UI-Einstellungen für eine Reihe von Domänen
- Keine Kerndaten jeglicher Art (z. B. bestimmte Anwenderdaten).
- Die OBERSTE Domäne im folgenden Bild ist eine Prozessdomäne.

Datendomäne

Die Datendomäne enthält Daten, die für mehrere Kunden relevant sind. Diese Daten können freigegeben werden, ohne die tatsächlichen Kundendomänen freizugeben. Jeder Kunde hat eine eigene Datendomäne und kann darauf zugreifen.

Hinweis:

Diese Art von Domäne ist nicht häufig und kann bei Übernutzung zu Leistungsproblemen führen. Wenden Sie sich vor der Verwendung an einen SP-Architekten.

Beispiel: Die Domäne kann Aufgaben enthalten, mit denen ACME, Cisco und der SP interagieren müssen.

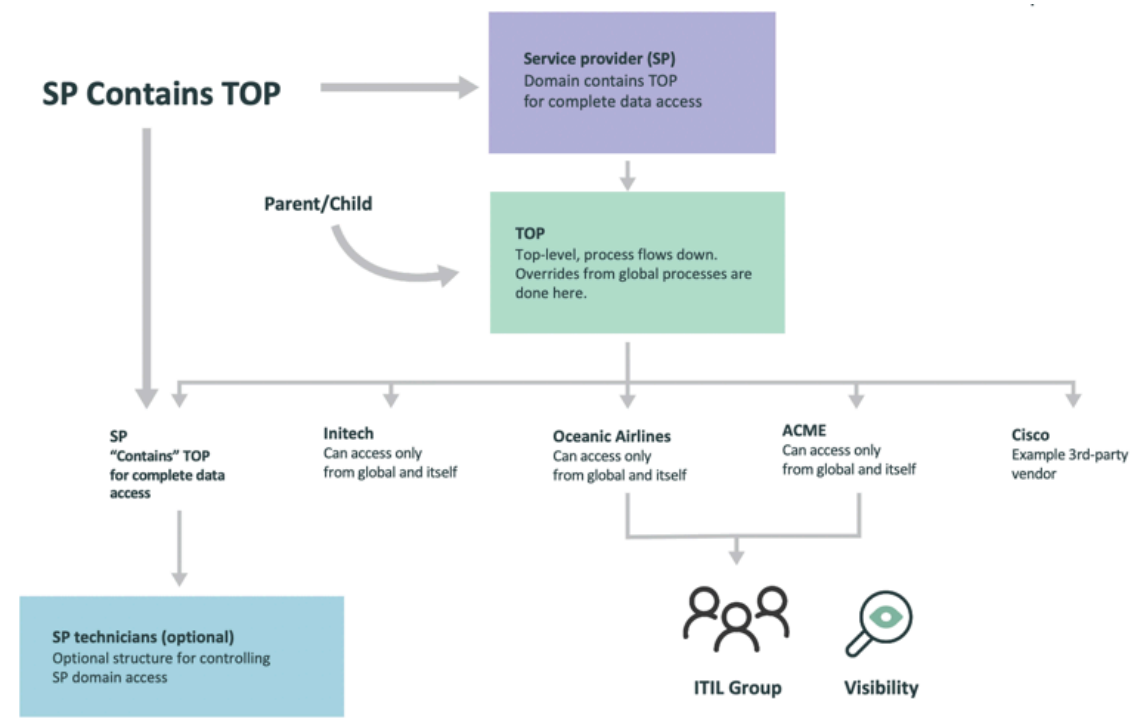
Die Standarddomäne im folgenden Bild ist eine Datendomäne.

Anwenderdaten

Anwenderdatensatzdaten gehören nie in die globale Domäne oder eine der Prozessdomänen. Anwender werden hauptsächlich in Kundendomänen erstellt und können gelegentlich in Datendomänen erstellt werden.

Administratoraccounts sind speziell, da sie nicht als tägliche Anwender der Instanz verwendet werden sollten und sich in der globalen Domäne befinden sollten, um administrative Funktionen zu erleichtern.

Domänenhierarchie



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen, Administrator, globaler Prozess

Listen

Wenn Sie in der globalen Domäne mit der rechten Maustaste auf die Bezeichnung eines Auswahlfelds klicken, wählen Sie aus **Konfigurieren Sie Auswahlmöglichkeiten** , Und fügen Sie dann eine neue Auswahl hinzu. Die Auswahl wird automatisch in alle domänenspezifischen Listen für dieses Feld verschoben. Wenn die neue Option als markiert ist **Ausgewählt** , Wird als aktiv hinzugefügt. Wenn die neue Option als markiert ist **Verfügbar** , Wird als inaktiv hinzugefügt.

Instanzenverwaltung

Die Administratoren des Instanzbesitzers müssen alle normalen Prozesse in einer domänengetrennten Instanz erstellen, ändern und warten. Einzelne Domänenmanager können einige Teile datengesteuerter Prozesse verwalten. Die Typen von Domänenmanagern verwalten die Anwenderverwaltung, Support-Gruppenmitgliedschaften und Standorte oder verwalten Anwendungen, die auf die Mandantenverwaltung ausgerichtet sind.

Globaler Prozess/globale Parameter

Sie können den Prozess erstellen und verwalten, der sich auf die globale Domäne auswirkt, sowie die Parameter festlegen. Diese Eigenschaften sind für alle Anwender einer domänengetrennten Instanz gemeinsam.

Beispiele: Systemeigenschaften, Wörterbuchüberschreibungen, `sys_documentation` (Feldbezeichnungen), das Datenmodell (Klassen, CI-Typen usw.), Tabellen und Felder `[sys_dictionary]` (Zugriff kann eingeschränkt werden), Indizierung (Textindizes sowie Datenbank), ACLs, Installationsausgänge, eingehende Aktionen, öffentliche Seiten, und Interceptors.

Domäne: Trennen Sie eine anwenderdefinierte Tabelle

Möglicherweise müssen Sie anwenderdefinierte Tabellen in separaten Domänen erstellen. Dieses Thema behandelt sowohl das Verfahren als auch das Konzept hinter der Domänentrennung einer anwenderdefinierten Tabelle.

1. Erstellen Sie ein sys_Domain-Feld

Hinweis: Wenn eine Systemtabelle oder eine Tabelle nicht vom Plugin „Domänentrennung“ domänengetrennt wurde, sollte sie nicht domänengetrennt werden.

Verwenden Sie diese Punkte als Leitfaden zum Erstellen eines Felds „sys_Domain“.

- Erstellen Sie ein neues Feld als *`domain_id`*Typ.
  - Spaltenname: sys_Domain
  - Andere Attribute: Automatisch definiert
- Der SYS_Domain_path wird automatisch erstellt.

Der Spaltenname **sys_Domain** Ist in reserviert ServiceNow AI Platform, Das bedeutet, dass das System ihn erkennt und automatisch den entsprechenden Feldtyp und die entsprechenden Attribute für Sie anwendet. Diese automatische Konfiguration erstellt auch einen entsprechenden **sys_Domain_path** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie den Spaltennamen auf fest `sys_Domain` Anstatt die Bezeichnung zu verwenden.
- Domänentrennung ist nicht für jede Tabelle geeignet. Im Allgemeinen, wenn eine Tabelle Teil der Basisinstanz ist und diese Tabelle keinen hat **sys_Domain** Feld, sollten Sie es so lassen.

A **sys_Domain** Das Feld wird automatisch erstellt, wenn Sie ein Feld vom Typ „Domain_ID“ mit dem Namen „sys_Domain“ erstellen.

2. Fügen Sie eine Business-Regel hinzu, um die Domäne festzulegen

Ohne Business-Regeln

Die Domäne wird auf die aktuelle Domäne des Anwenders festgelegt, der den Datensatz erstellt.

Mit Business-Regeln

Die Domäne wird mit geskripteter Logik zugewiesen, normalerweise basierend auf dem Feld „Unternehmen“.

Zusätzlich zu `Feld „sys_Domain“` , Anwenderdefinierte Tabellen benötigen eine Business-Regel ähnlich wie **Domäne – Domäne Festlegen – Aufgabe** Zum Festlegen des Werts des Domänenfelds. Darüber hinaus benötigen Sie **Domäne – Standard – Aufgabe** , Wodurch Datensätze ohne Domäne in die Standarddomäne verschoben werden, wenn die erste Regel keine Domäne zuweisen kann.

Überprüfen Sie in der Aufgabentabelle die Geschäftsregeln für Domäne. Achten Sie besonders auf das Feld Reihenfolge. Die Priorität der Ausführung wird durch das Feld Reihenfolge von niedrig nach hoch gegeben.

Die erste Regel, die ausgeführt wird, **Domäne – Domäne Festlegen – Aufgabe** , Versucht, die Domäne des Datensatzes basierend auf der Domäne des Unternehmens des Datensatzes festzulegen.

Wenn die erste Regel keine entsprechende Domäne findet, wird die zweite Regel **Domäne – Standard – Aufgabe** , Wird ausgeführt. Diese Regel legt die Domäne des Datensatzes auf die Standarddomäne fest.

Wenn sich die Domäne eines Aufgabendatensatzes ändert, wird schließlich der **Domäne – Domäne Kaskadieren – Aufgabe** Die Business-Regel ändert die Domäne in allen Datensätzen im Zusammenhang mit der Aufgabe, z. B. Workflows, Metriken, SLAs und Anhänge.

3. Fügen Sie eine Business-Regel hinzu, wenn Schritt 2 fehlgeschlagen ist

Wenn die anfängliche Business-Regel keine Domäne festlegt und die Domäne noch leer oder global ist, wird eine zweite Business-Regel ausgeführt. Diese Regel untersucht `Aufgabe_für` Feld, das auf dem Anrufer oder basiert `Angefordert_für` Feld. Diese Regel überprüft, ob Sie die Domäne des Datensatzes basierend auf der Domäne des Anwenders festlegen können. Wenn nicht, legt die Business-Regel die Domäne auf die Standarddomäne fest.

Im Folgenden finden Sie ein Beispielskript für die Business-Regel:

```
/* essentially
If (task_for is set)
  set the domain to the user's domain
ELSE
  set the domain to the default domain
*/
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Domäne – kaskadierende Domäne – Aufgabe

Aufgaben können viele zugehörige Tabellen haben, die für Geschäftsziele zusammenarbeiten. Diese zugehörigen Datensätze umfassen Workflow, SLA, Genehmigungen, Anhänge und E-Mail. Wenn sich die Domäne einer Aufgabe ändert, muss sich auch die Domäne der zugehörigen Datensätze ändern, damit sie für Anwender in der neuen Domäne sichtbar bleiben.

Diese Kaskadierungsregel wird häufig ausgelöst, wenn Sie Datensätze aus der Standarddomäne löschen.

Die zugehörigen Datensätze für eine kaskadierende Domäne, die im Skript enthalten ist, werden ähnlich dem Beispiel angezeigt:

```
/*
* Keep domains in sync w/related records for:
* workflow context
* workflow history
* approver tables and related workflows
* attachments
* emails
*/
```

Domäneneigenschaften und -Designs anpassen

Sie können die Unternehmenseigenschaften und -Designs Ihrer Kunden innerhalb der von Ihnen konfigurierten Domänen anpassen. Durch die Anpassung werden ihre Instanzen in das Gesamtbild des Unternehmens angepasst.

Anpassen von Unternehmensdesigns und -Logos

Im Unternehmensdatensatz können Sie bestimmte Designdesigns und Logos für jedes Unternehmen anpassen.

Passen Sie die Domäne an

Wenn Sie das Service Provider-Plugin installiert haben, bewirken die in den Kerntabellen enthaltenen Standard-Business-Regeln standardmäßig, dass die Domäne des Datensatzes auf die Domäne des Unternehmens festgelegt wird, das dem Datensatz zugeordnet ist. Das Unternehmen kann die Tabellen wie Aufgabe, Anwender, Gruppe, Standort, Abteilung, steuern. und so weiter.

Mit allen diesen Tabellen mit Ausnahme der Aufgabentabelle können Sie die Domäne überschreiben, in der ein Datensatz erstellt wird. Dadurch erhalten Sie weitere Anpassungsoptionen.

Verwalten der Domänentrennung für bestimmte Verwendungen

Sie können separate Domänen für E-Mail-Benachrichtigungen einrichten und die Eigenschaften von Katalog, Tabellen, Anwendern, Gruppen und Ansichten anpassen. Dadurch können Sie spezifischeres Verhalten in jeder Domäne bereitstellen, was Ihren Kunden mehr Flexibilität verleiht.

E-Mails

Sie können separate Domänen für E-Mail-Benachrichtigungen und Überschreibungen verwenden. Wenn Sie separate Domänen für Benachrichtigungen verwenden, können Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Überschreibung durchführen, die auf der Domäne nur des angehängten Datensatzes basiert, nicht auf der gesamten Domäne des Anwenders.

Servicekatalog

Der Servicekatalog ist jetzt domänengetrennt, damit Ihre Kunden den Katalog sehen und darauf zugreifen können. Elemente werden als ODER-Bedingungen verarbeitet, wenn mehrere Elemente verwendet werden. Service Provider sollten die Kategorien und Elemente selbst verwalten, damit sie speziell ihren eigenen Kriterien entsprechen.

Anwender und Gruppen

Verwenden Sie nur Administratorkonten in der globalen Domäne, da Administratoren Zugriff auf alle Domänen benötigen. Führen Sie alle Ihre Anwendungstests von einer tatsächlichen Domäne aus, nicht in der globalen Domäne. Überschreibungen werden in der globalen Domäne nicht ordnungsgemäß verarbeitet. Administratoren sollten auch Anwenderaccounts in der Produktion zugewiesen werden, wenn sie die Anwendung verwenden sollen.

Arbeiten mit Feldern

Bei der Arbeit mit Feldern sind mehrere Punkte zu berücksichtigen. Achten Sie besonders auf diese Felder, da sie viele Variationen haben können, die sich auf Ihre Konfigurationen auswirken.

Listen

Es gibt persönliche, globale und Domänenlisten sowie mehrere Ansichten von jeder.

Formulare

Es gibt globale Listen und Domänenlisten sowie mehrere Ansichten von jeder.

Eine Datenbank

Alle von Ihnen erstellten Felder sind für alle Anwender in einer Datenbank vorhanden. Berücksichtigen Sie die globalen Auswirkungen, bevor Sie eine erstellen.

Hinweis: ACL-Skripts können nicht verhindern, dass ein Feld in einer Liste angezeigt wird, da sie nicht ausgeführt werden. Sie können eine LESE-ACL hinzufügen, um ein Feld vor Anwendern auszublenden, wenn die ACL nur rollenbasiert ist.

Tabellen werden erstellt

Wenn Sie eine Tabelle erstellen, sollten Sie eine hinzufügen `sys_Domain` Oder `sys_overrides` Feld. Jede Tabelle, die Daten enthält, auf die Ihre Instanzanwender zugreifen müssen, benötigt `sys_Domain` Feld. Tabellen, die Prozesse erweitern oder unterstützen und in untergeordnete Domänen fließen müssen, benötigen ebenfalls `sys_Domain` Feld.

Domänentrennung mit der Domänenauswahl konfigurieren

Verwenden Sie die Domänenauswahl klug, und erinnern Sie sich an den 80/15/5-Ansatz, damit Sie nicht zu viel anpassen und die Leistung Ihrer Instanz beeinträchtigen.

Überprüfen Sie Ihre Domäne, bevor Sie Änderungen vornehmen

Die Domänenauswahl sammelt alle Domänen in einer Liste, aus der Sie auswählen können.

Wenn Ihre Sitzung eine Zeitüberschreitung hat und Sie nicht abgemeldet werden, fällt Ihre Sitzung auf die Domäne in Ihrem Anwenderdatensatz zurück. Sie verlieren gleichzeitig auch alle erhöhten Rollen. In diesem Fall kann Ihre Domänenauswahl weiterhin die zuletzt ausgewählte Domäne anzeigen, wenn der obere Frame der Liste nicht neu geladen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aus diesem Grund sollten Sie Ihre Liste vollständig neu laden, wenn Sie die Instanz irgendwann nicht verlassen haben.

Konfiguration in der OBERSTEN Domäne oder der globalen Domäne

Domänentrennung funktioniert am besten, wenn Sie Kunden Services bereitstellen, die in ihrer Konfiguration und Anwender- und Gruppendefinition größtenteils Standard sind. Je mehr Sie „einmalige“ Lösungen anpassen und erstellen, desto mehr schaffen Sie einen Fehlerspielraum. Wenn Sie Ihre Prozesse und Geschäftslogik erstellen, sollten alle Variationen in Eigenschaften enthalten sein, die für jeden Kunden automatisch funktionieren. Prozesse können zwar noch nach Bedarf angepasst werden. Seien Sie jedoch sehr vorsichtig, wenn Sie entscheiden, wann und in welchem Umfang eine eindeutige Konfiguration für einen einzelnen Kunden erstellt werden soll.

Sie müssen bei der Konfiguration Ihrer Domänen einen Ansatz von „80-15-5“ verwenden, um zu große Margen für die Anpassung und somit Fehler zu vermeiden.

- Empfohlener Ansatz für Konfiguration:
  - **80 %** Oder mehr **Standard**
  - **15 %** Oder mehr **Parametrisch**
  - Kleiner als **5 %** **Konfiguration**
- Legen Sie fest, ob ein vorgeschlagener Change eine globale oder eine konfigurierbare Eigenschaft sein soll.
- Überbauen Sie nicht, indem Sie immer mehr Anpassungen hinzufügen, die verwaltet werden müssen. Gehen Sie stattdessen wie folgt vor:
  - Beginnen Sie mit den Basissystemfunktionen, und überprüfen Sie alle Lücken, bevor Sie Änderungen vornehmen.
  - Suchen Sie nach Lösungen ohne Code.
  - Verwenden Sie serverseitige Skripts, erstellen Sie modulare APIs, und erstellen Sie domänengetrennte Eigenschaften.
  - Wenn Sie Client-Skripting verwenden müssen, verwenden Sie nur ServiceNow APIs. Beschränken Sie „synchrone“ Aufrufe (Aufrufe, die vom Client zum Server hin- und hergehen, auch AJAX genannt).
  - Schreiben Sie alle Skripts logisch, um sie einfach und effektiv zu halten. Erzwingen Sie Peer-Überprüfungen von Codeänderungen, und stellen Sie sicher, dass jeder dem folgt Empfohlene Domain Separation-Verfahren für Service Provider In diesem Abschnitt.

Überlegungen zur Leistung der Domänentrennung

Achten Sie beim Konfigurieren der Domänentrennung in Ihren Anwendungen und Services darauf, die Anzahl und die Eigenschaften der von Ihnen erstellten Domänen zu berücksichtigen. Zu viele Domänen mit hohen Eigenschaften können sich auf die Leistung Ihrer Instanz auswirken.

Einschränkende eigenschaftsschwere Domänen

Sie können beliebig viele Domänen erstellen, stellen Sie jedoch sicher, dass Sie keine unnötigen Domänen auf der Instanz erstellen. Die Gewichtung zu vieler Domänen in der Instanz mit vielen Eigenschaften kann sich auf die Leistung Ihrer Instanz auswirken.

Die Anzahl der Domänen wirkt sich nicht auf die Leistung aus, sondern vielmehr auf die darin enthaltenen Domänen. Zu viele Eigenschaften können verlangsamen Domänenauswahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

, Was dann die allgemeine Anwender-Experience Ihrer Kunden verlangsamt. Wenn Sie die Domänenauswahl laden und bereits eine große Anzahl von Domänen mit vielen Eigenschaften haben, muss die Domänenauswahl alle Domänen laden, bevor Sie in der Sitzung die Kontrolle erhalten. Dieser Prozess kann zu einem Ausfall führen, bei dem Sie erst dann auf etwas in der Instanz zugreifen können, wenn die Domänenauswahl abgeschlossen ist. Bevor Sie neue Domänen erstellen, navigieren Sie unter zur Domänenhierarchie **Domänenadministrator** > **Domänenzuordnung** Und stellen Sie sicher, dass Sie tatsächlich eine neue Domäne oder eine vorhandene erstellen müssen Domänenhierarchie Kann funktionieren.

Verwenden Core-UI Domänenauswahl

Die Domänenreferenzauswahl ist in verfügbar Core-UI. Mit der Referenzauswahl laden Sie nicht alle Domänen gleichzeitig, sondern die Domäne wird durchsucht, wenn Sie mit der Eingabe des Namens Ihrer Domäne in die Domänenauswahl beginnen.

Aktivieren Sie die Domänenreferenzauswahl in Core-UI Führen Sie die folgenden Schritte aus:

1. Geben Sie im Anwendungsnavigator `sys_properties.list` ein.
2. Legen Sie die Eigenschaft *`glide.ui.domain_reference_picker.enabled`* auf „Wahr“ fest.
3. Aktualisieren Sie den Browser.

Hinweis: Laden Sie keine große Anzahl von Domänen (über 30) über Integrations- oder Importsätze hoch, ohne zuerst einige Tests durchzuführen, da Sie sonst Ihre Instanz herunterfahren könnten.

Domänenhierarchien werden eingerichtet

Sie können Verlangsamungen und Leistungsauswirkungen in Ihrer Instanz vermeiden, indem Sie wissen, wie Domänenhierarchien funktionieren, und sie ordnungsgemäß einrichten.

Basierend auf der Domänenhierarchie haben Anwender Zugriff auf die Daten in ihrer Heimatdomäne und allen untergeordneten Domänen. Der Prozess fließt hinunter zu den untergeordneten Domänen, und die Daten werden hochgestuft.

Nehmen Sie Änderungen an der vorhandenen Domänenhierarchie nur bei Bedarf vor. Wenn Sie das übergeordnete Element einer Domäne aktualisieren, richtet das System die übergeordnete Domäne mit allen untergeordneten Domänen, die die Domänenhierarchie ändern, neu ein. Wenn die Domänenhierarchie aktualisiert wird, löst das System eine kaskadierende Aktualisierung für alle Tabellen aus, die sich auf Domänen beziehen, für die Datensätze, die in dieser Domäne erstellt werden. Daher muss auch eine große Anzahl unterstützender Tabellen aktualisiert werden.

Aus den gleichen Gründen sollten Sie niemals Massenaktualisierungen durchführen, auch wenn Sie die Domänenhierarchie ändern müssen. Stellen Sie sich die Anzahl der Abfragen vor, die das System ausführen muss, um die Domänenhierarchie zu ändern. Führen Sie immer ein Update in kleinen Batches durch. Bevor Sie mit dem nächsten Update-Batch beginnen, stellen Sie sicher, dass DWR-Datensätze (Domain Work Request) verarbeitet werden. DWRs sind Berichte, die anzeigen, ob Fehler auftreten, nachdem Sie die Domänenhierarchie geändert haben.

Nachverfolgung von DWR-Datensätzen

Suchen Sie in der Tabelle „syslog_Domain“ in der Spalte Nachricht für nach einem Informationseintrag **DWR-Ausführung abgeschlossen.** Um zu bestätigen, dass DWR abgeschlossen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Domänenprotokolle werden auf Fehler und Warnungen überprüft

Überprüfen Sie die Domänenprotokolle, um Fehler oder Warnungen in Ihren Domänenpfadprozessen und Hierarchiekonfigurationen zu finden.

Sie finden die Domänenprotokolle in der Tabelle Domänenprotokoll [syslog_Domain]. Wenn die Domänenhierarchie aktualisiert wird, löst das System eine geplante Aufgabe aus, um die Domänenpfade neu zu berechnen. Die Tabelle „Domänenprotokolle“ erfasst die Ergebnisse.

Suchen Sie in dieser Tabelle nach Fehlern und Warnungen. Nach der Überprüfung dieser Tabelle müssen Sie diese Fehler beheben und die Domänenpfadvalidierung erneut ausführen.

In diesem Beispiel eines Protokolls hat das System zehn verwaiste Datensätze in der Tabelle „sys_ui_list“ erkannt. Die Fehler in diesen Datensätzen müssen behoben werden, bevor der Domänenpfad erfolgreich ausgeführt werden kann.

Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again.	com.glide.domain.validator
Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again. Entries causing the error are as follows:sys_id:1d13ae40470002007f47563dbb9a7170, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:22e34b23470002007f47563dbb9a718c, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:4c85fa809f233100fc6cd4b4232e706b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:94648b23470002007f47563dbb9a711b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a0844b23470002007f47563dbb9a71ef, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a95ff2c09f233100fc6cd4b4232e7096, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:bd25f4719f233100fc6cd4b4232e70da, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:c1263e809f233100fc6cd4b4232e70f6, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:d8a72c45475002007f47563dbb9a71bb, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:e4c3ce39eb10020045e1a5115206fea0, sys_domain:60e014f69f013100fbf01f80a57fcf00	com.glide.domain.validator

Weitere Informationen zu Domänentrennungsfehlern finden Sie unter Beheben Sie Domänentrennungsfehler.

Wichtigkeit der Standarddomäne

Die Organisation Ihrer Domänen ist ein wichtiger Teil des Domänentrennungsprozesses. Wenn Sie keine Standarddomäne festlegen, gehen neue Aufgaben und Anwenderdatensätze an die globale Domäne. Jeder kann die Datensätze in der globalen Domäne sehen, was bedeutet, dass Daten angezeigt werden können, wenn sie nicht angezeigt werden sollen.

Wenn Sie die Standarddomäne festlegen, sind ihre Datensätze für keinen anderen Anwender als einen Administrator sichtbar.

Hinweis: Der Standardzugriff kann geändert werden, indem Anwendern Sichtbarkeit für die Standarddomäne oder die übergeordnete Domäne gewährt wird.

Sie sollten immer eine Standarddomäne für die Domänendatensätze in Ihrer Instanz festlegen. In der Standarddomäne weist das System automatisch Aufgaben- und Anwenderdatensätze zu, die noch keiner Domäne zugewiesen sind.

Wenn Sie eine Standarddomäne über den Bildschirm Domänenverwaltung erstellen, fügen Sie den Namen Standard in hinzu **Name** Feld, um es von anderen Domänen zu unterscheiden. Überprüfen Sie **Standard** Kontrollkästchen für den Datensatz.

Verwalten Sie regelmäßig die Datensätze, die Sie in der Standarddomäne erstellen, und verschieben Sie sie in die richtigen Domänen. Wenn Datensätze häufig in der Standarddomäne angezeigt werden, müssen Sie möglicherweise untersuchen, warum. Idealerweise sollten Sie sicherstellen, dass alle Datensätze in den entsprechenden Domänen erstellt werden (nicht in globalen Domänen oder Standarddomänen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enthält Abfragen und Domänenzugriff

Verwenden Sie eine Abfrage „enthält“ nur in speziellen Fällen, z. B. wenn Anwender oder Gruppen Daten aus einer Domäne anzeigen müssen, auf die sie keinen Zugriff haben, Sie diese Anwender jedoch nicht in eine Domäne verschieben möchten. Das Erstellen der Domäne „enthält“ und des Anwender- oder Gruppenzugriffs für eine Domäne sollte nur dann eine Ausnahme sein, wenn dies unbedingt erforderlich ist.

„Enthält“ ist eine Domäne-zu-Domäne-Beziehung, die viele-zu-viele ist und keine Auswirkungen auf den Prozessfluss hat. Wenn Sie eine große Anzahl von Domänen-„enthält“-Beziehungen erstellen oder einen breiten Zugriff gewähren, generieren Sie Abfragen mit zu vielen ODER-Bedingungen. ODER-Bedingungen sind langsam und wirken sich auf die Leistung Ihrer Instanz aus. Anstatt zu viele „enthält“-Beziehungen zu verwenden, richten Sie Ihre Domänenhierarchie wie folgt ein:

Beispielabfrage

```
SELECT ... FROM task task0 ignore index(number) WHERE task0.`sys_class_name`
= 'incident' AND (task0.`sys_domain_path` = '/' OR task0.`sys_domain_path` LI
KE '!!$/!!(/%' OR task0.`sys_domain_path` LIKE '!!$/!!$/!!&/%') ORDER BY task
0.`number` DESC limit 0,20
```

Bevor Sie Anwender in eine Domäne verschieben, stellen Sie sicher, dass sie wirklich Zugriff auf diese Domäne haben sollten. Wiegen Sie die Vorteile und Einschränkungen ab. Die obige Abfrage bezieht sich auf nur eine enthält Beziehung. Wenn Sie eine Domäne haben, die eine andere Domäne enthält und diese Domäne einer Reihe anderer Domänen übergeordnet ist, haben Sie viele weitere ODER Bedingungen. Seien Sie vorsichtig, wenn Sie eine Domänenzuordnung erstellen, damit Sie sich nicht auf die Leistung Ihrer Instanz auswirken.

Abfragemethode für Domänenpfade

Sie können effektive Abfragen mit Domänenpfaden erstellen.

Domänenpfade anstelle von Domänenspooling verwenden (`sys_Domain`) Oder Domänennummerierung. Abfragen, die Domänenpfade verwenden, sind viel schneller als Spooling oder Nummerierung.

Domänenpfade ist die Standardabfragemethode für Instanzen, die Domänentrennung aktiviert haben.

Wenn Sie die Abfragemethode in Ihrer Instanz überprüfen möchten, suchen Sie im Administrator-Dashboard nach den folgenden Systemeigenschaften:

- *`If domain path is enabled`*: In der Tabelle „Systemeigenschaften“ wird angezeigt `glide.sys.domain.provider=domain_paths` Und `glide.sys.domain.paths.installed=true` .
- *`If domain path is not enabled`*: In der Tabelle „Systemeigenschaften“ wird angezeigt glide.sys.domain.provider != Domain_Pfade,glide.sys.domain.paths.installed=false

Langsame Abfragen und SQL-Debugging

Das Debugging von SQL und langsamen Abfragen kann Ihnen helfen, Probleme mit der langsamen Geschwindigkeit in einer Instanz zu lösen.

Wenn Sie eine Instanz debuggen, können Sie entweder SQL-Debugging aktivieren, um nach langsamen Abfragen zu suchen, oder Sie können nach langsamen Abfragen suchen, indem Sie die Tabelle „langsame Abfragen“ [sys_query_pattern] überprüfen, indem Sie zu navigieren **Systemdiagnose > Statistiken > Langsame Abfragen** . Diese Tabelle speichert alle langsamen Abfragen in der Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie die Tabelle durchsuchen, suchen Sie nach Abfragen, die enthalten `Domain_path` Um festzustellen, ob langsame Abfragen auf den Domänenpfad in Ihrer Instanz zurückzuführen sind.

Wenn Sie langsame Abfragen finden, versuchen Sie zu analysieren, warum sie langsam sind.

Häufige Gründe für langsame Abfragen

- Eine Abfrage hat zu viele ODER-Bedingungen (weitere Informationen finden Sie unter Enthält Abfragen und Domänenzugriff). Platzieren Sie in der Domänenhierarchie den Anwender oder eine Domäne auf einer Hierarchieebene, auf der „enthält“ oder „Sichtbarkeit“ nicht erforderlich ist.
- Die Abfragemethode ist nicht die Abfragemethode des Domänenpfads (weitere Informationen finden Sie unter Abfragemethode für Domänenpfade): Wenn Sie die Abfragemethode des Domänenpfads nicht verwenden, wenden Sie sich an Kundenservice und Support.
- Für eine Abfrage muss eine Datenbank indiziert werden, damit Sie schnell sehen können, was sich in der Datenbank befindet. Wenn Sie die langsame Abfrage identifizieren können, führen Sie den „Erklärungsplan“ aus, um zu sehen, ob Optionen für die Indizierung verfügbar sind. Der „Plan erklären“ ist eine Funktion von SQL, die die Abfrage und ihre Vorgänge anzeigt.

Business-Regeln vor Abfrage

Sie können eine Business-Regel vor der Abfrage verwenden, um die Datentrennung in einer Instanz zu unterstützen. ServiceNow Anwendungen, die die Domänentrennung unterstützen, unterstützen möglicherweise nur die Trennung von Daten und die Datenweiterleitung, verfügen über erweiterte Geschäftslogik-Trennung oder unterstützen die Verwaltung der Anwendung auf Mandantenebene (Kunden).

Eine Business-Regel vor Abfrage ist ein zusätzlicher Code, den Sie zur Unterstützung der Datentrennung in domänengetrennten Umgebungen verwenden.

Warnung: Verwenden Sie nicht die Business-Regel vor Abfrage anstelle des Plugins „Domänentrennung“. Diese Geschäftsregel verhindert Datenverluste nicht so sicher wie das Plugin.

Verwenden der Business-Regel vor Abfrage für die Datentrennung

In diesen Situationen können Sie die Business-Regel „vor Abfrage“ mit Datentrennung verwenden:

- Wenn Domänentrennung von nicht unterstützt wird ServiceNow Anwendung und Sie müssen einem oder mehreren nicht internen Kunden außerhalb der Service Provider-Organisation Tabellen- oder Zeilenzugriff gewähren oder einschränken.

  Hinweis: Bevor Sie mit der Entwicklung beginnen, wenden Sie sich an ServiceNow Kundensupport über die Anwendungs-Roadmap für dieses Produkt; Verbesserungen des Domänensupports sind möglicherweise für bevorstehende Releases geplant.

- Wenn eine Tabelle domänengetrennt ist, der Zugriff auf ihre Zeilen jedoch basierend auf bestimmten Bedingungen gewährt oder eingeschränkt werden muss, die nur für eine Reihe von Domänen im System gelten.

  Hinweis: Beispielsweise hat ein Kunde in der X-Domäne mehrere Lieferanten, die diese Domäne unterstützen, und diesen Lieferanten wird Zugriff gewährt, nur die Datensätze anzuzeigen, die ihnen zugewiesen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Punkte, die vor der Erstellung von Business-Regeln für die Abfrage berücksichtigt werden sollen

Sie können vor AbfrageBusiness-Regeln ein Skript ausführen, um den Zugriff auf übergeordnete und untergeordnete Tabellen basierend auf einer Kombination aus Anwenderinformationen, Gruppenmitgliedschaften, Unternehmen, Rollen oder datensatzspezifischen Feldbedingungen zu verhindern. Vor der Abfrage werden Business-Regeln in separate Domänen eingefügt und erstellt, um sie global auf eine bestimmte Verzweigung einer Domänenhierarchie anzuwenden.

- Wo Sie können, erstellen Sie Business-Regeln vor der Abfrage am niedrigsten möglichen Teil der Domänenhierarchie, damit die Regel nur für Anwender ausgeführt wird, für die sie gilt.
- Wissen Sie, dass es Szenarien im System gibt, in denen Business-Regeln möglicherweise nicht ausgeführt werden oder in denen eine vom Anwender ausgelöste Interaktion die Ausführung einer Business-Regel nicht auslösen kann. Beispielsweise wird eine Business-Regel nicht ausgeführt, wenn Sie Transformationszuordnungen mit deaktivierten Business-Regeln ausführen haben, oder wenn Sie Skripts mit deaktiviertem Workflow haben.
- Füllen Sie immer das Bedingungsfeld aus, um anzugeben, wann die Regel ausgeführt wird. Sie können beispielsweise angeben, ob die Business-Regel nur für bestimmte Lieferanten in einer Domäne gilt.

> ⚠ **Warnung:** Beim Entwerfen und Codieren von Business-Regeln (insbesondere Business-Regeln abfragen), beschränken ODER Klauseln und Suchen in nicht indizierten Feldern. Zu viele ODER -Klauseln und -Suchen in nicht indizierten Feldern können Abfragen verlangsamen oder die Leistung Ihrer Instanz beeinträchtigen.

- Verwenden Sie Business-Regeln vor Abfrage nur, wenn erforderlich. Zu viele vor-Abfrageregeln können sich auf die Leistung Ihrer Instanz auswirken.

Vor der Abfrage werden Business-Regeln vor Zugriffssteuerungslisten (ACLs) ausgeführt und funktionieren im Allgemeinen besser. Dies gilt insbesondere, wenn Sie die zurückgegebenen Ergebnisse auf die Anwender in Service Provider-Umgebungen (SP) beschränken, die Zugriff auf mehrere Domänen im System haben.

> ℹ **Hinweis:** Das Filtern der Daten ist für Anwender transparent (im Gegensatz zu ACLs), die die Nachricht nicht sehen Datensicherheit schränkt… ein. Bei der Interaktion mit Daten.

Wann nicht vor Abfrage-Business-Regeln und ACLs verwendet werden sollen

Seien Sie vorsichtig, wenn Sie Geschäftsregeln und ACLs vor Abfrage verwenden, um Kundendaten zu trennen. Indem Sie sowohl Business-Regeln als auch ACLs verwenden, erstellen Sie Anpassungen, die Sie dann beibehalten müssen. Anpassungen können potenziell Leistungsprobleme verursachen. Ihre Entwicklungsteams sollten Prozesse erstellen, um sicherzustellen, dass sie das System nicht beschädigen.

Domänentrennung bietet Skalierbarkeit und Governance mit der aktuellen Domänenpfad-Abfragemethode (v3), einem weit unterstützten Framework. Die ServiceNow Plattform- und App-Teams sind für die Wartung des Frameworks verantwortlich, wodurch der Kunde entlastet wird.

Bei Unternehmen mit vielen Kunden in vielen Instanzen kann eine übermäßige Verwendung von vor-Abfragen und ACLs dazu führen, dass die Datenbankabfragen nicht gut funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie Domänentrennung aktiviert ist

Sie können die Domänentrennung mit aktivieren ServiceNow Plugin. Ein Produktmanager, der von einem Entwicklungsteam unterstützt wird, verwaltet die Funktionalität. Erweiterungen und Korrekturen für die Domänentrennungsfunktion sind in enthalten ServiceNow Releases. Instanzbesitzer können konsultieren Kundenservice und Support Ressourcen, z. B. Serviceportal, Um https://support.servicenow.com Für Unterstützung bei der Domänentrennung.

Domänenpfad in Skripts wird vermieden

Domänenpfade können dazu führen, dass sich die Werte Ihres Skripts ändern oder sogar unterbrechen. Verwenden Sie sie daher nicht in Skripts.

Ihr Skript darf nicht vom Domänenpfad abhängen, da wenn Sie die Domänenhierarchie jemals ändern, der Domänenpfad neu berechnet und sein Wert geändert wird. Wenn dies geschieht, sind Ihre Skripts nutzlos oder können Fehler auslösen oder brechen. Die beste Strategie besteht darin, Ihre Skripts nicht basierend auf Domänenpfaden zu schreiben.

Verwenden Sie **sys_Domain** Feld in Ihren Skripts anstatt abhängig vom Domänenpfad. Wenn Sie die Domänenhierarchie jemals ändern, wird der Domänenpfad neu berechnet, und sein Wert ändert sich, was dazu führen kann, dass Ihre Skripts nutzlos sind, Fehler auslösen oder brechen. Suchen Sie nach Geschäftsregeln des Basissystems, die verwenden **sys_Domain** Feld, um einige Ideen zu erhalten, bevor Sie eigene Skripts erstellen.

Die ServiceNow Die Plattform erfasst nicht die sys_Domain_path-Werte in einem Update-Satz, um Probleme mit Unterschieden in der Domänenhierarchie für jede Instanz zu vermeiden. Daher sollten Sie die Domänenhierarchie validieren, nachdem Sie einen Update-Satz importiert haben, um sicherzustellen, dass die Domänenpfadwerte für Ihre Datensätze korrekt sind.

Weitere Informationen zum Domänenpfad finden Sie unter Domänentrennung anfordern Und Domain Separation Center.

Domänenzuweisungen

Wie Sie eine Domäne zuweisen, wirkt sich auf den Wert des Felds „sys_Domain“ aus. Die Zuweisungen enthalten Designs und Geschäftseigenschaften, die sich auf die Funktionsweise der Anwendung in jeder Domäne auswirken.

Wert des Felds „sys_Domain“

Der Wert von **sys_Domain** Das Feld enthält die Domäne, die dem Datensatz von einer der folgenden Personen zugewiesen wird:

- Unternehmen, zu dem der Anwender gehört
- Business-Regel, die beim Erstellen des Datensatzes verwendet wird
- Modul, das beim Erstellen des Datensatzes verwendet wird
- Formularvorlage, die beim Erstellen des Datensatzes verwendet wird
- Domäne des übergeordneten Datensatzes
- Domäne, die dem Anwenderdatensatz zugewiesen ist
- Domäne des Anwenders, der sie erstellt

Stellen Sie sicher, dass Ihre Domänenzuweisungsstrategien und -Designs gut dokumentiert und getestet sind, damit Sie Datensätze erstellen, während diese Strategien und Designs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in die richtige Domäne eingefügt werden. Auf diese Weise können Sie sehen, dass die Eigenschaften jeder Domäne dupliziert oder geändert werden müssen.

Domänentrennung und Kundenservice-Management (CSM) Plugin

Um das beste Ergebnis zu erzielen, beachten Sie, wie die Eigenschaften in der CSM Plugin-Arbeit. Wenn das Plugin aktiviert ist, können Sie den Status Ihrer Datensätze in Ihren Domänen anzeigen.

Instanzbesitzer müssen sich an wenden Kundenservice und Support Zum Aktivieren von *csm_auto_account_domain_generation*Eigenschaft.

Hinweis: Diese Basissystemeigenschaft befindet sich in der Tabelle „Systemeigenschaften“ und ist verfügbar, nachdem CSM-Plugins aktiviert wurden.

Was die Eigenschaft bewirkt

Jedes Mal, wenn ein neuer Account in der Kundenserviceanwendung erstellt wird, wird eine Domäne erstellt und unter der OBERSTEN Domäne platziert. Wenn das übergeordnete Feld im Account-Formular ausgefüllt wird und ein neuer Datensatz eingefügt wird, wird dieser Account als Unterdomäne des übergeordneten Elements erstellt.

Was passiert, wenn diese Eigenschaft nicht „wahr“ ist und die Domäne aktiviert ist

Neue Account-Datensätze in einer domänengetrennten Umgebung werden automatisch in der Standarddomäne platziert.

In der Header-Leiste können Sie den Status der Datensätze mit aktiviertem Plugin anzeigen.

Hilfe Zur Domänentrennung

Zusätzliche Unterstützung bei der Domänentrennung

Videoübersicht zur Domänentrennung

Erkunden, Lernen, Entwickeln



Empfohlene Vorgehensweisen

Tipps und Tricks für die kluge Erstellung und Entwicklung Ihrer Domänenstruktur

Konzepte für Service Provider

Konzepte, die mit funktionieren ServiceNow Plattform, die Ihnen bei der Lösung gängiger Anwendungsfälle hilft



Supportstufen nach Anwendung

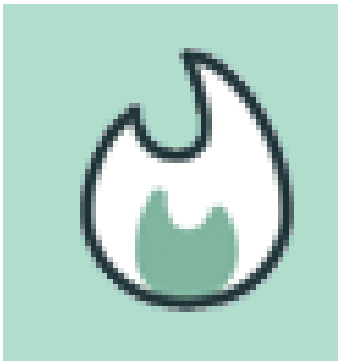
Wird Ihre Anwendung für die Domänentrennung unterstützt? Siehe Supportstufen und Anwendungsfälle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klassen

- Für Entwickler: ServiceNow Domänentrennung Der Entwickler-Site
- Für Service Provider: Domänentrennung für Service Provider (Anmeldung an der ServiceNow University erforderlich)



Safe Workplace-Suite und Domänentrennung

ServiceNow Safe Workplace-Anwendungen helfen Ihnen, Ihre Arbeitsplätze wieder zu öffnen und den Arbeitsschutz Ihrer Mitarbeiter nach Notfällen und Pandemien wie COVID-19 zu unterstützen. Die Suite verfügt über viele Anwendungen, mit denen Ihre Organisation mobilisieren, wiederherstellen und neu erstellen kann.



Setup und Verwaltung

- Upgrades
- Domänentrennung anfordern
- Erstellen Sie eine Domäne
- Konfiguration, die an interne oder externe Kunden delegiert werden kann



Problembehandlung

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support
- In der Community Fragen stellen oder beantworten

Setup und Verwaltung der Domänentrennung

Das Einrichten der Domänentrennung umfasst die Anforderung der Aktivierung eines Plugins, das Festlegen von Optionen und das Zuweisen von Anwendern und Datensätzen zu Domänen.

Gehen Sie wie folgt vor, um die Domänentrennung einzurichten:

1. Domänentrennung anfordern
2. Erstellen Sie eine Domäne
3. Fügen Sie einer Tabelle ein Domänenfeld hinzu

Sie können diese grundlegenden administrativen Aufgaben auch für Domänen ausführen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivieren oder deaktivieren Sie eine Domäne
- Zeigen Sie Domänenbeziehungen an
- Domänenbereich erweitern
- Erstellen Sie eine domänenspezifische Auswahlliste

Siehe Erweiterte Verwaltung der Domänentrennung Für eine Liste der Aufgaben, die ausgeführt werden sollen, nachdem Sie die Domänentrennung eingerichtet und die grundlegende Verwaltung durchgeführt haben.

Domänentrennung anfordern

Alle Domänenunterstützungsfunktionen werden mit einem Plugin namens aktiviert **Domänensupport: Installationsprogramm Für Domänenerweiterungen** . Administratoren können die Aktivierung dieses Plugins anfordern.

Vorbereitungen

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account-Manager kann die Bereitstellung von veranlassen `com.glide.domain.msp_extensions.installer`Plugin wurde in den Produktions- und Unterproduktionsinstanzen Ihrer Organisation im Allgemeinen innerhalb weniger Tage aktiviert.

Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn das Plugin „Domänensupport – Domänenerweiterungs-Installationsprogramm“ bereits aktiv ist, werden Inhalte im Plugin „Domänensupport – Domänenerweiterungs-Installationsprogramm“ nicht installiert, um potenzielle Konflikte mit einer vorhandenen Implementierung zu vermeiden.

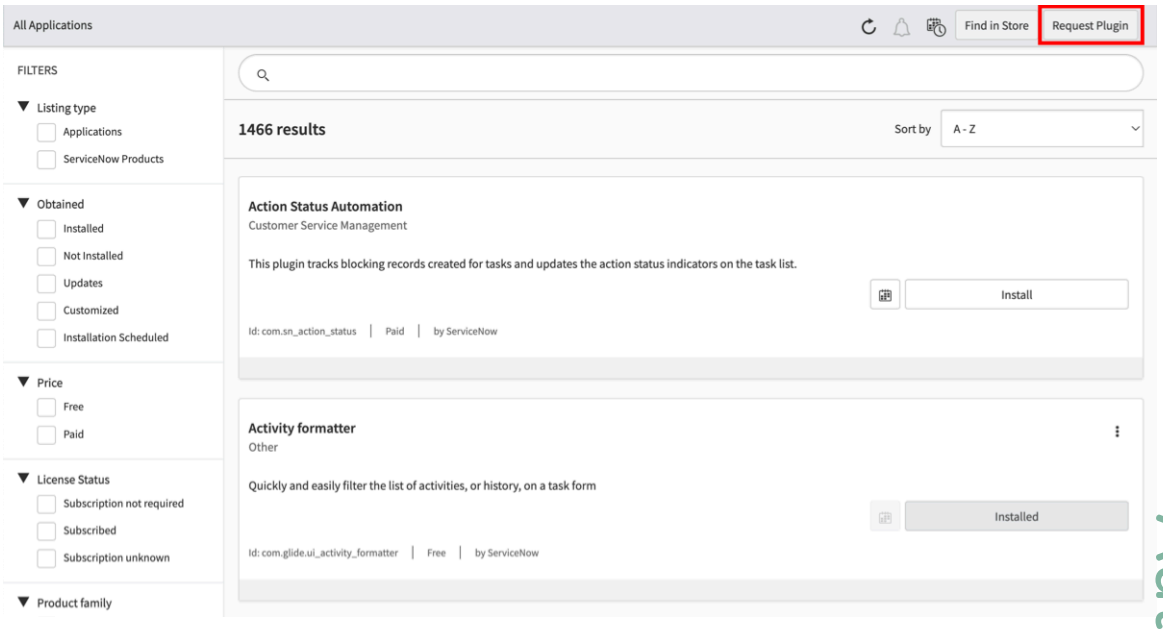
Domänentrennung ersetzt Unternehmenstrennung. Ab Helsinki-Release kann das Plugin „Unternehmenstrennung“ nicht mehr aktiviert werden. Wenn die Unternehmenstrennung jedoch bereits aktiv ist, wenn Sie die Domänentrennung aktivieren, sind beide Plugins gleichzeitig aktiv. Sie können den Aktivierungsstatus der Unternehmenstrennung mit steuern `glide.db.separation.field`Eigenschaft.

Hinweis: Domänenpfade werden für alle Kunden ab Helsinki verwendet. Domänennummerierung wird nicht mehr verwendet. Kundenservice und Support Kann beim Upgrade helfen.

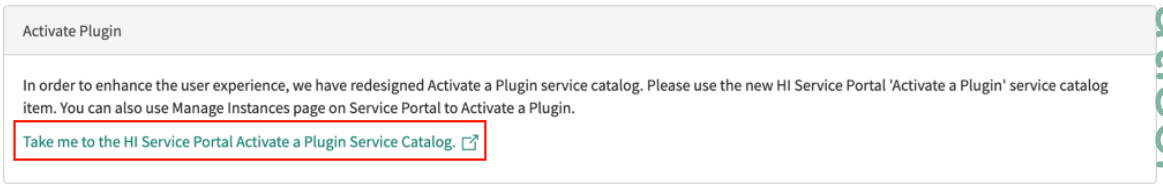
Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.

5. Wählen Sie **Aktionen > Plugin aktivieren** aus.

6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
	Datum und Uhrzeit zum Aktivieren des Plugins.

Automatische Übersetzung

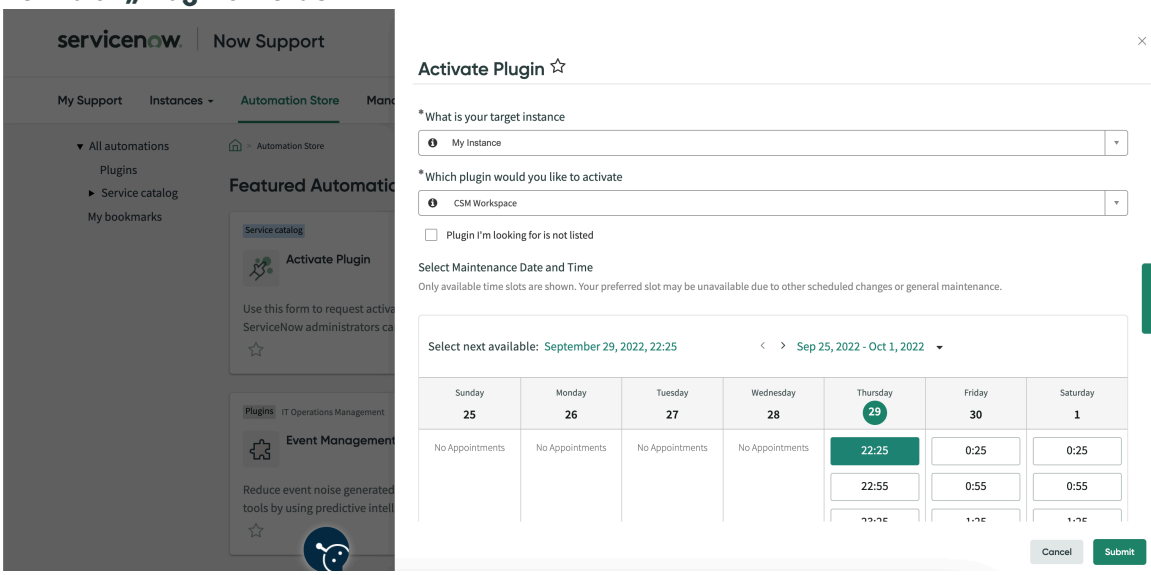
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	**Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Ergebnis

Durch die Aktivierung des Plugins „Domänenerweiterungs-Installationsprogramm“ werden diese Funktionen aktiviert:

- Domänentrennung basiert auf der Domäne [sys_Domain] Tabelle.
- Durch die delegierte Verwaltung kann jede Domäne über eine separate Richtlinie verfügen.
- Alle Datensätze sind Teil der globalen Domäne.
- Die Domäne des aktuellen Anwenders bestimmt die Domäne, die verwendet werden soll, wenn ein Datensatz in einer anderen Domäne angezeigt oder bearbeitet wird.

Zugehörige Informationen

Plugin „Domänentrennung“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin „Domänentrennung“

Das Plugin „Domänenunterstützung – Domänenerweiterungs-Installationsprogramm“ aktiviert mehrere Domänentrennungsfunktionen und -Eigenschaften gleichzeitig. Dieses Plugin wird normalerweise als Plugin „Domänentrennung“ bezeichnet.

Empfohlene Praxis für die Aktivierung des Plugins „Domänentrennung“

Im Rahmen der Entwicklung der Domänentrennung müssen Administratoren Aktivierung anfordern Dieses Plugins. Um die besten Ergebnisse zu erzielen, aktivieren Sie das Plugin „Domänentrennung“ zu Beginn des Entwicklungsprozesses, vorzugsweise bevor ein anderes Plugin aktiviert wird.

Wichtig: Fordern Sie die Aktivierung des Plugins „Domänenerweiterungs-Installationsprogramm“ (com.glide.domain.msp_extensions.installer) an, bevor Sie die Domänentrennung aktivieren (Plugin com.snc.PA.Domain_Support).

Wenn Sie Domänentrennung gegen Ende von aktivieren ServiceNow Implementierung oder sobald eine Instanz live gegangen ist, ist Ihre Anwendung sowohl in Bezug auf Leistung als auch im Prozess gefährdet. In etablierten Instanzen könnten je nachdem, wie die Dinge in der Entwicklung strukturiert waren, das Risiko für die Plattform und ihre Nutzbarkeit hoch sein. Weitere Informationen zum Domänentrennungsprozess finden Sie unter Domänentrennung erkunden.

Wenn beispielsweise das Plugin „Domänentrennung“ aktiviert ist, wird der **Domäne** Die Spalte (sys_Domain) wird der Aufgabentabelle hinzugefügt, und jeder vorhandene Datensatz wird automatisch in platziert **Global** . Zur Verwendung eines Skripts, um alle Datensätze den richtigen Domänen zuzuweisen, ist eine etablierte übergeordnete/untergeordnete Hierarchie erforderlich. Diese Arten von geskripteten Aktionen riskieren Datenbeschädigung oder -Verlust und mögliche Produktionsausfallzeiten, wenn große Datenmengen verschoben werden. Ein Großteil des Plattformcodes wird auch in platziert **Global** , Z. B. Geschäftsregeln, Clientskripts, Formularansichten und Workflows.

Wenn ein Kunde Code erstellt oder ändert ServiceNow Code, es besteht ein Risiko für die Plattformleistung und -Verwendbarkeit. Instanzbesitzer können ihre Implementierung erheblich verzögern oder lange Ausfallzeiten mit dieser Art von Ansatz erleben.

Funktionen des Plugins „Domänentrennung“

Diese Funktionen sind aktiviert, wenn Sie das Plugin aktivieren:

- Domänentrennung basiert auf der Domäne [sys_Domain] Tabelle.
- Durch die delegierte Verwaltung kann jede Domäne über eine separate Richtlinie verfügen.
- Alle Datensätze sind Teil der globalen Domäne.
- Die Domäne des aktuellen Anwenders bestimmt die Domäne, die verwendet werden soll, wenn ein Datensatz in einer anderen Domäne angezeigt oder bearbeitet wird.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänensystemeigenschaften und Anwendereinstellungen

Administratoren haben Zugriff auf Eigenschaften und Anwendereinstellungen, die den Domänenbereich steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften

Neue Aktivierungen der Domänentrennung beschränken den Domänenbereich automatisch auf die Domäne des Datensatzes für alle zugehörigen Daten oder Prozesse. Wenn der Anwender einen Datensatz in einem Formular anzeigt, sind die zugehörigen Daten des Datensatzes (z. B. Referenzauswahl und zugehörige Listendaten) und angewendete Prozesse (z. B. Geschäftsregeln und Client-Skripts) auf den Domänenbereich des Datensatzes beschränkt. Wenn sich Datensätze auf mehreren Registerkarten befinden, hat jede Registerkarte ihren eigenen Domänenbereich basierend auf dem auf dieser Registerkarte geöffneten Datensatz. Die folgenden Eigenschaften beschränken den Domänenbereich entweder auf die Domäne des Datensatzes und die aktuelle Sitzungsdomäne des Anwenders.

Domänensystemeigenschaften

Eigenschaft	Details
glide.sys.domain.use_record_domain_for_processes	Beschränkt den Domänenbereich für alle Prozesse auf die Domäne des Datensatzes. Diese Eigenschaft gilt nicht für Business-Regeln. Geschäftsregeln werden immer aus dem Domänendatensatz verarbeitet. • *Typ*: true | false • *Standardwert*: true • *Speicherort*: Tabelle „Systemeigenschaft“ [sys_properties]
glide.sys.domain.use_record_domain_for_data	Beschränkt den Domänenbereich für alle Daten auf die Domäne des Datensatzes. • *Typ*: true | false • *Standardwert* : „Wahr“ in neuen Domänenaktivierungen ab Fuji (Upgrades von Instanzen, die älter als Fuji sind, haben diese Eigenschaft nicht in der Tabelle) • *Speicherort*: Tabelle „Systemeigenschaft“ [sys_properties]

Wenn entweder `glide.sys.domain.use_record_domain_for_processes`Oder `glide.sys.domain.use_record_domain_for_data`Eigenschaft ist auf festgelegt **Wahr** , Die folgenden Eigenschaften werden unabhängig von ihrer Einstellung nicht verwendet:

- `glide.sys.domain.use_record_domain`
- `glide.sys.domain.use_record_domain_for_client_scripts`
- `glide.sys.domain.domain_change_notify`
- `glide.sys.domain.no_change_roles`

Eine vollständige Liste der Eigenschaften finden Sie unter Verfügbare Systemeigenschaften .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Bei neuen Aktivierungen der Domänentrennung ab dem Jakarta-Release bestimmt die Sitzungsdomäne die Geschäftsregeln, die in der Domänentabelle ausgeführt werden. In früheren Versionen wurden für die Domänentabelle ausgeführte Geschäftsregeln basierend auf der Hierarchie der neu erstellten Domäne festgelegt. Dieses Verhalten wird von geändert `glide.sys.domain.skip_domain_insert_businessrules`Eigenschaft. Wenn Sie diese Eigenschaft auf „wahr“ festlegen, wird die Leistung beim Einfügen der Domäne erheblich verbessert.

Domänenbereichseigenschaften für Business-Regeln, die in der Domänentabelle ausgeführt werden

Eigenschaft	Details
Glide.sys.Domain.Skip_Domain_insert_businessrules	Gibt den Domänenbereich für Business-Regeln an, die in der Domänentabelle ausgeführt werden. Bei neuen Aktivierungen der Domänentrennung ist die Eigenschaft standardmäßig „wahr“, und Geschäftsregeln werden von der Sitzungsdomäne bestimmt. In vorhandenen Implementierungen ist die Eigenschaft „falsch“, und die Geschäftsregeln werden durch die Hierarchie der neu erstellten Domäne bestimmt. • *Typ*: true | false • *Standardwert* : „Wahr“ in neuen Domänenaktivierungen ab Jakarta. Falsch in vorhandenen Implementierungen.
Glide.sys.Domain.Skip_non_global_businessrule_if_nodomain	Stellt sicher, dass nur bus.rules aus der globalen Domäne ausgeführt werden, wenn queryNoDomain() verwendet wird oder wenn die Tabelle nicht domänengetrennt ist, sodass Sie alle anderen Business-Regeln überspringen können • *Typ*: true | false • Wenn Sie die Eigenschaft auf „falsch“ festlegen, wird das alte Verhalten wiederhergestellt und nicht an ausgerichtet ServiceNow® Empfohlene Praktiken. • Empfohlen: Trennen Sie Ihre Tabellen von Domänen. Versuchen Sie immer, die Domäne des Datensatzes anstelle der Sitzungsdomäne zu verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendereinstellungen

Darüber hinaus können Anwenderadministratoren die folgenden Anwendereinstellungen global oder pro Anwender festlegen:

Anwendereinstellungen des Domänenbereichs

Einstellung	Kategorie	Aktualisiert von	Details
glide.domain.session_scope	Domäne	Nur Administrator	Bei „wahr“ wird der Standardbereich auf die Sitzungsdomäne des Anwenders und nicht auf die Domäne des Datensatzes festgelegt. Bei „falsch“ ist der Standardbereich die Domäne des Datensatzes. Anwender mit der Anwenderrolle „Domain_expand_scope“ können den Domänenbereich weiterhin nach Bedarf ändern. • **Typ**: true | false • **Standardwert**: false
glide.domain.session_scope_notification	Domäne	Nur Administrator	Bei „wahr“ wird ein visueller Hinweis angezeigt, dass Datensatzwerte einen erweiterten Domänenbereich enthalten. Bei „falsch“ wird die Benachrichtigung ausgeblendet. • **Typ**: true | false • **Standardwert**: true

Zugehörige Informationen

Eigenschaften der Anwendung „Domänentrennung“

Erstellen Sie eine Domäne

Sie können eine Domäne erstellen, indem Sie einen Datensatz in der Tabelle [Domäne] erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Beachten Sie beim Erstellen einer neuen Domäne Folgendes:

- Nur eine Domäne kann die Standarddomäne sein.
- Nur eine Domäne kann die primäre Domäne sein.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**an.
2. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die erforderlichen Felder aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.

Domänenformularfelder

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Domäne ein.
Typ	Wählen Sie einen Domänentyp aus, der die Domäne beschreibt. Standardmäßig sind die Domänentypen *Lieferant* , *Kunde* , Und *MSP* . Sie können auch eigene Auswahlmöglichkeiten hinzufügen.
Primär	Aktivieren Sie das Kontrollkästchen, wenn diese Domäne die Domäne der obersten Ebene in der Hierarchie sein soll. Die Domäne der obersten Ebene hat nur untergeordnete Domänen und keine übergeordneten Domänen.
Standard	Wählen Sie aus, ob diese Domäne die Standarddomäne für Ihre Hierarchie sein soll.
Übergeordnet	Wählen Sie den Namen der Domäne höher in der Hierarchie aus, die diese Domäne enthält. Dieses Feld muss einen Wert haben, damit die Domäne in der Domänenzuordnung angezeigt wird.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die Domäne zur Verwendung verfügbar zu machen. Sie müssen diese Option auswählen, damit diese Domäne in der Domänenzuordnung angezeigt wird.
Beschreibung	Geben Sie eine Beschreibung für die Domäne ein.

Jeder Domänendatensatz kann auch mehrere zugehörige Datensätze haben:

- Unternehmen
- Enthält Domänen
- Enthalten in

Nächste Maßnahme

Um die Domänenhierarchie zu ändern, wechseln Sie zur zugehörigen Liste enthält Domänen, und wählen Sie die Domänendatensätze aus, die die untergeordneten (enthaltenen) Domänen der Beziehung enthält.

Legen Sie eine Domäne als Standard fest

Hat eine Domäne zur Standarddomäne gemacht, der das System automatisch Aufgaben- und Anwenderdatensätze zuweist, die noch keiner Domäne zugewiesen sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Wenn Sie keine Standarddomäne festlegen, werden neue Aufgaben und Anwenderdatensätze in der globalen Domäne platziert.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**an.
2. Öffnen Sie die Domäne, die die Standarddomäne sein soll, z. B. Haupt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Konfigurieren Sie das Formularlayout, um hinzuzufügen **Standard** Feld.
4. Aktivieren Sie das Kontrollkästchen **Default (Standard)**.
5. Klicken Sie auf **Aktualisieren**.

Verwalten Sie die Domäne für bestimmte Datensätze manuell

Standardmäßig weist das System automatisch eine Domäne basierend auf dem Unternehmensdatensatz des Anwenders zu. In einigen Fällen möchten Domänenadministratoren jedoch manuell verwalten, welcher Domäne ein bestimmter Datensatz angehört.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die **Verwaltete Domäne** Mit dem Feld können Domänenadministratoren manuell eine Domäne für den Anwender, die Gruppe, die Abteilung, den Standort oder den CI-Datensatz auswählen. anstatt die automatisch aus dem Unternehmensdatensatz zugewiesene Domäne zu verwenden. Die **Verwaltete Domäne** Das Feld ist für diese Datensatztypen verfügbar.

- Benutzerdatensätze
- Gruppendatensätze
- Abteilungsdatensätze
- Standortdatensätze
- CI-Datensätze

Prozedur

1. Navigieren Sie zu dem Datensatz, den Sie manuell verwalten möchten.
2. Wählen Sie aus **Verwaltet** Kontrollkästchen „Domäne“.
3. Von **Domäne** Feld die Domäne für den Datensatz auswählen.
4. Klicken Sie auf **Aktualisieren**.

Wird gelöscht **Verwaltete Domäne** Kontrollkästchen blendet aus **Domäne** Feld und der Datensatz verwendet den Domänenwert aus dem Unternehmen des Datensatzes.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänengetrennte Tabellen

Mit der Funktion „Domänengetrennte Tabellen“ können Sie auf einen Blick sehen, welche Tabellen in Ihrer Instanz domänengetrennt sind.

Übersicht

Verwenden Sie die Funktion „domänengetrennte Tabellen“, um zu sehen, welche Tabellen domänengetrennt sind. Beginnen Sie mit der Eingabe von „Domäne“ in **Alle** Filter für Zugriff **Domänengetrennte Tabellen** Im linken Navigationsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können diese Ansicht filtern, um Spaltennamen anzuzeigen oder zu entfernen, um nach bestimmten Eigenschaften oder Attributen zu suchen, die in Ihren Tabellen enthalten sind. In der Liste werden zwei Tabellentypen angezeigt:

- Tabellen, die explizit enthalten *sys_domain*Spalte vorhanden, wobei **Spalte** Name wird angezeigt *sys_domain*Wert in der Liste.
- Tabellen, die verwenden *domain_master*Attribut zum Ableiten der Domänentrennung aus einem referenzierten Datensatz, wobei **Attribute** Spalte enthält *domain_master=ref-field-value*Wert.

Wenn Sie die Auswahl „Übereinstimmung anzeigen“ oder „Ausfiltern“ im Menü „Spaltenname“ verwenden, können Sie diese beiden Tabellentypen anzeigen.

Domänenüberschreibungsbetrachter

Mit der Domänenüberschreibungsanzeige können Sie alle Ihre Prozessüberschreibungen gleichzeitig in der gesamten Instanz anzeigen und verwalten.

Übersicht

Anstatt eine aufwendige Suche nach Überschreibungen in Ihren Skripts zu erstellen, können Sie die Domänenüberschreibungsanzeige verwenden, um sie schnell zu finden. Beginnen Sie mit der Eingabe von „Domäne“ in **Alle** Filter für Zugriff **Viewer Für Domänenüberschreibung** Im linken Navigationsbereich.

Die Tabellenauswahl im Domänenüberschreibungsanzeige zeigt eine Liste nur der Tabellen an, die Datensatzüberschreibungen enthalten, zusammen mit einer Anzahl von Überschreibungen in dieser Tabelle. Nachdem Sie eine Tabelle ausgewählt haben, wird eine Liste aller übergeordneten Datensätze mit Überschreibungen zurückgegeben. Sie können alle schnell anzeigen **Übergeordnete Datensätze** , **Domäne** Des übergeordneten Datensatzes und eines **Anzahl** Von Überschreibungen für jeden Datensatz.

Auswählen **Überschreibungen Anzeigen** Lädt eine neue Registerkarte, auf der alle Überschreibungen, einschließlich des übergeordneten Datensatzes, in der Standardlistenansicht angezeigt werden. Wählen Sie eine Tabelle aus der Dropdown-Liste aus, um alle Datensätze und Überschreibungen anzuzeigen. Wählen Sie Aus **Überschreibungen Anzeigen** In einem Datensatz, um alle datensatzspezifischen Überschreibungen anzuzeigen.

Hinweis: Nur Tabellen mit Überschreibungen werden aufgelistet.

Weitere Informationen finden Sie unter Erstellen Sie domänengetrennte Eigenschaftsüberschreibungen .

Aktivieren oder deaktivieren Sie eine Domäne

Wenn Sie eine Domäne aktivieren oder deaktivieren, wird der Aktivierungsstatus an Unternehmen innerhalb der Domäne weitergegeben.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Unternehmensdatensatz aktivieren, aktiviert die Domänentrennung automatisch die dem Unternehmen zugeordnete Domäne. Wenn Sie beispielsweise das ACME-Unternehmen aktivieren, aktivieren Sie auch die TOP-/ACME-Domäne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zum Domänendatensatz.
2. Löschen oder wählen Sie aus **Aktiv** Kontrollkästchen.
3. Klicken Sie auf **Aktualisieren**.

> ⚠ **Warnung:** Löschen Sie keine Domänen. Deaktivieren Sie Domänen, die Sie nicht mehr benötigen, anstatt sie zu löschen.

Fügen Sie einer Tabelle ein Domänenfeld hinzu

Trennen Sie als Administrator eine anwenderdefinierte Tabelle, indem Sie ihr ein sys_Domain-Feld hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

> ℹ **Hinweis:**
>
> Fügen Sie den Basissystemtabellen keine Domänen hinzu.

Prozedur

1. Navigieren Sie zur Listenansicht der Tabelle.
   Geben Sie beispielsweise ein <table name>.Liste Im Navigationsfilter.
2. Klicken Sie mit der rechten Maustaste auf den Listenheader, und wählen Sie aus **Konfigurieren** > **Listenlayout**an.
3. In **Erstellen Sie ein neues Feld** Abschnitt eingeben sys_Domain Als **Name** Und Domänen-ID Als **Typ** .
4. Klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Speichern**.

> ℹ **Hinweis:**
>
> Jede andere Methode zum Erstellen eines Felds fügt einen hinzu **u_** Präfix für den Spaltennamen. Aber mit dem Domänenfeld erstellt das System das Feld automatisch ohne **u_** Präfix. Sie können die folgende Funktionalität als Verknüpfung verwenden: Immer dann, wenn Sie eine erstellen **sys_Domain** Feld, benennen Sie es **sys_Domain** Und lassen Sie den Feldtyp unverändert. Das System legt den Feldtyp automatisch auf fest **Domänen-ID** Und die Feldbezeichnung bis **Domäne** , Mit wenigen Klicks.
>
> Das Hinzufügen von Domänen zu Basissystemtabellen erfordert prohibitiv gründliche Tests, Updates und das Hinzufügen neuer Logik. Darüber hinaus ist der Quellcode in vielen Fällen für den Kunden nicht zugänglich.

Zeigen Sie Domänenbeziehungen an

Die Domänenzuordnung bietet Domänenadministratoren eine schreibgeschützte Darstellung der aktiven Domänen in der Instanz und ihrer Beziehung zueinander.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Für alle Domänenzuordnungen muss eine Domäne als primäre Domäne festgelegt sein. Darüber hinaus muss jede Domäne in der Domänenzuordnung diese Kriterien erfüllen:

- Die **Übergeordnet** Feld muss ausgefüllt werden (die primäre Domäne ist die einzige Ausnahme).
- Die **Aktiv** Das Kontrollkästchen muss aktiviert sein.

Die Domänenzuordnung zeichnet keine Domänenbeziehungen für Domänen, die die Zuordnungskriterien nicht erfüllen.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänenzuordnung**an.
2. Klicken Sie auf das Plus (**+**) Oder minus (**–**) Symbole in den Domänenheadern zum ein- oder Ausblenden von Unterdomänen.

Wählen Sie eine primäre Domäne aus

Die primäre Domäne gibt die Domäne der obersten Ebene in der Domänenzuordnung an.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

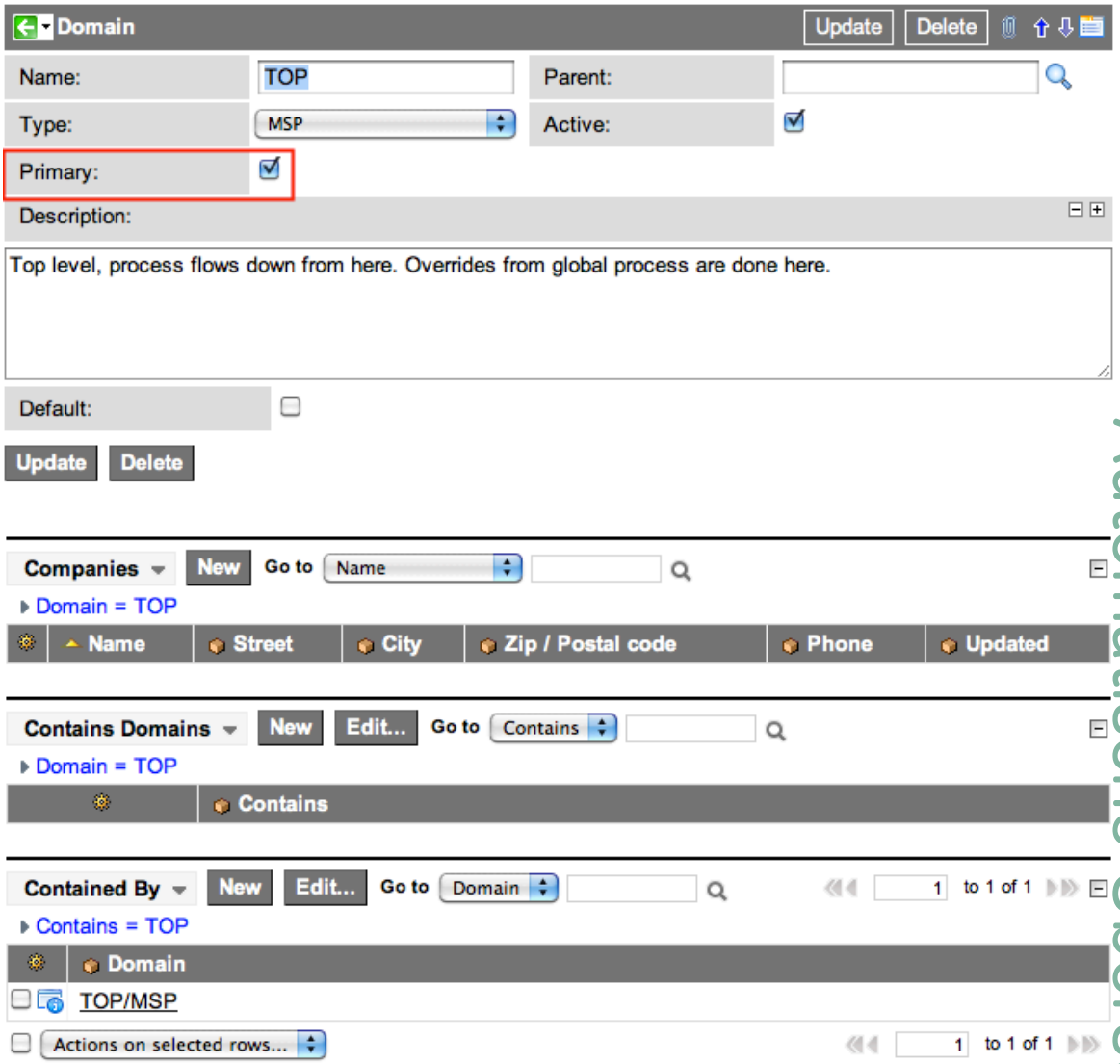
Die primäre Domäne kann keine übergeordnete Domäne haben und muss mindestens eine untergeordnete Domäne haben. Es kann jeweils nur eine primäre Domäne vorhanden sein. Wenn Sie eine andere Domäne als primäre Domäne auswählen, wird die vorherige primäre Domäne überschrieben.

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**an.
2. Wählen Sie die Domäne aus, die die primäre Domäne sein soll, z. B. TOP.
3. Wählen Sie aus **Primär** Kontrollkästchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Aktualisieren**.



Automatische Übersetzung

„Erstellen“ enthält Beziehungen zwischen Domänen

Erstellen Sie eine „enthält“-Beziehung zwischen Domänen, um die Domänenhierarchie zu ändern.

Vorbereitungen

Erforderliche Rolle: Administrator

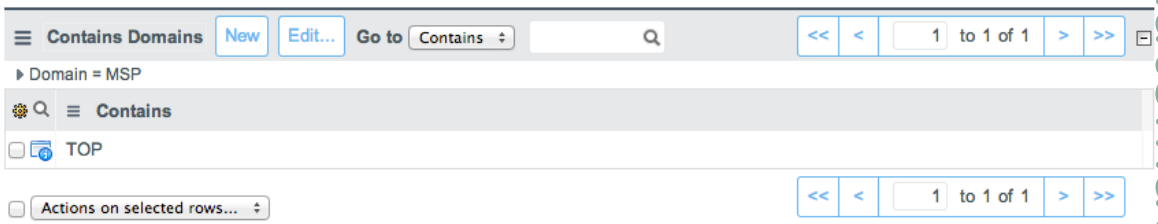
Warum und wann dieser Vorgang ausgeführt wird

Domänen in einer enthält-Beziehung erben die Einstellungen der enthaltenden Domäne. Mit der enthaltenden Domäne können Anwender Daten in der enthaltenen Domäne sowie alle untergeordneten Elemente anzeigen. Prozesse sind von einer enthält-Beziehung nicht betroffen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zur Domänentabelle.
2. Wählen Sie den Domänendatensatz aus, der die übergeordnete Domäne (Container) der neuen enthält-Beziehung ist.
3. Schalten Sie den Domänenbereich ein/aus Um bei Bedarf zwischen Sitzungsumfang und Datensatzumfang zu wechseln.
4. Klicken Sie in der zugehörigen Liste enthält Domänen auf **Bearbeiten** .
5. Wählen Sie die Domänendatensätze aus, die die untergeordneten (enthaltenen) Domänen der enthält-Beziehung sind.
   Standardmäßig werden nur untergeordnete Domänen angezeigt, wenn die Domänenauswahl auf Global festgelegt ist. Schalten Sie den Domänenbereich ein/aus, um alle Domänen anzuzeigen.
6. Klicken Sie Auf **Speichern** , Und klicken Sie dann auf **Aktualisieren** .



Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenbereich erweitern

Standardmäßig, wenn ein Anwender in der globalen Domäne eine Tabelle mit anzeigt **sys_overrides** Spalte, sieht der Anwender Datensätze nur aus der globalen Domäne. Wenn ein Administrator in der globalen Domäne eine Prozesstabelle anzeigt, sieht dieser Administrator nur Datensätze, die sich in dieser Prozesstabelle befinden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Ändern Sie `glide.sys.restrict_global_domain_processes`Eigenschaft bis **Wahr** .
2. Klicken Sie auf , um Datensätze aus allen Domänen anzuzeigen **Erweitern Sie Den Domänenbereich** Unter zugehörige Links.
3. Um zur Anzeige von Datensätzen nur aus der globalen Domäne zurückzukehren, klicken Sie auf **Domänenbereich Reduzieren** .

Fügen Sie einer Liste der Sichtbarkeitsdomänen Domänen Domänen Domänen hinzu

Durch das Hinzufügen einer Sichtbarkeitsdomäne kann ein Anwender oder eine Gruppe Datensätze aus einer anderen Domäne anzeigen und potenziell bearbeiten, unabhängig von der normalen Domänenmitgliedschaft des Anwenders oder der Gruppe.

Vorbereitungen

Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

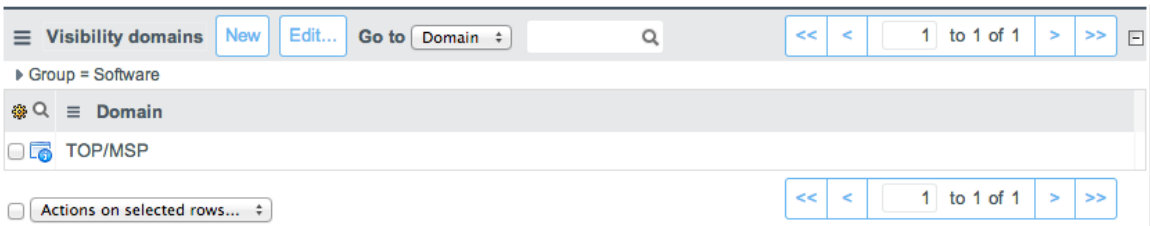
Warum und wann dieser Vorgang ausgeführt wird

Das Zuweisen von Sichtbarkeitsdomänen an alle Mitglieder einer Gruppe ist dem Zuweisen an einzelne Anwender vorzuziehen.

Hinweis: Durch das Hinzufügen einer Sichtbarkeitsdomäne werden die Zugriffssteuerungsregelanforderungen einer Tabelle oder eines Datensatzes nicht geändert.

Prozedur

1. Navigieren Sie zur Gruppentabelle.
2. Wählen Sie die Gruppe aus, die Sie mit Sichtbarkeitsdomänen bereitstellen möchten.
3. Fügen Sie hinzu **Sichtbarkeitsdomänen** Zugehörige Liste zum Formular.
4. Von **Sichtbarkeitsdomänen** Zugehörige Liste, klicken Sie auf **Bearbeiten** .
5. Wählen Sie die Domänendatensätze aus, die die Gruppe oder Domäne anzeigen soll.
6. Klicken Sie Auf **Speichern** , Und klicken Sie dann auf **Aktualisieren** .



Gewähren Sie einem einzelnen Anwender Sichtbarkeitsdomänen

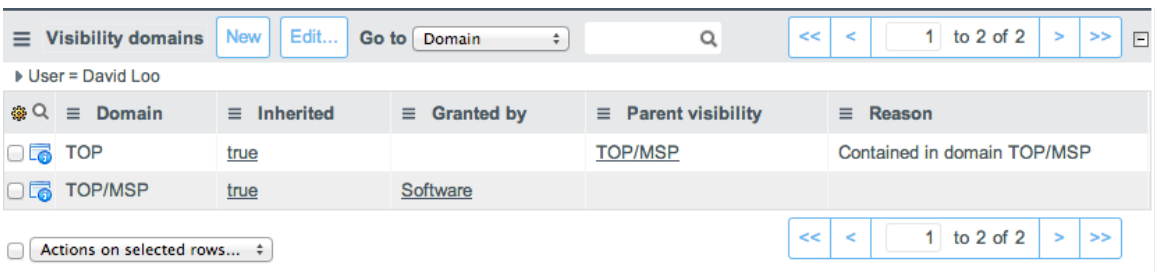
Es ist zwar möglich, Sichtbarkeitsdomänen für bestimmte Anwender im Anwenderformular hinzuzufügen, es ist jedoch am besten, sie nur über Gruppen hinzuzufügen. Dies steuert Berechtigungen und Zugriff, wenn Einzelpersonen Abteilungen wechseln oder das Unternehmen verlassen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.
2. Wählen Sie den Anwender aus, den Sie Sichtbarkeitsdomänen bereitstellen möchten.
3. Fügen Sie hinzu **Sichtbarkeitsdomänen** Zugehörige Liste zum Formular.
4. Klicken Sie in der zugehörigen Liste Sichtbarkeitsdomänen auf **Bearbeiten** .
5. Wählen Sie die Domänen aus, deren Datensätze der Anwender sehen soll.
6. Klicken Sie Auf **Speichern** , Und klicken Sie dann auf **Aktualisieren** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die eingebettete Liste der Sichtbarkeitsdomäne enthält die folgenden Felder.

Feld	Beschreibung
Domäne	Domäne, die für die Gruppe oder den Anwender sichtbar ist.
Geerbt	Domäne wird von Domänensichtbarkeit oder einer übergeordneten Domäne geerbt.
Gewährt Von	Name der Gruppe, die Domänensichtbarkeit gewährt hat.
Übergeordnete Sichtbarkeit	Name der übergeordneten Domäne, der zum Gruppieren von Datensätzen verwendet wird. Wenn der übergeordnete Datensatz gelöscht wird, werden auch alle Datensätze mit demselben übergeordneten Element gelöscht.

Erstellen Sie eine domänenspezifische Auswahlliste

Administratoren können Auswahllisten so konfigurieren, dass sie Einträge enthalten, die für eine bestimmte Domäne spezifisch sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Wählen Sie die Domäne aus der Domänenauswahl aus, in der die Auswahl hinzugefügt werden soll.
2. Klicken Sie mit der rechten Maustaste auf das Auswahlfeld, das Sie anpassen und auswählen möchten **Konfigurieren Sie Auswahlmöglichkeiten** .
3. Aktualisieren oder fügen Sie Auswahlmöglichkeiten hinzu.
4. Übertragen Sie Changes über den normalen Change-Prozess, z. B. Update-Sätze.

> **Hinweis:** Administratoren sollten sicherstellen, dass die Auswahlmöglichkeiten domänenübergreifend eindeutig sind, um administrative Verwirrung in der globalen Domäne zu verhindern.

Wenn ein Administrator eine neue Auswahl aus der globalen Domäne hinzufügt, sehen Anwender aus Domänen unterhalb der Hierarchie die neue Auswahl am Ende ihrer aktuellen Auswahllisten. Wenn die neue Auswahl auf globaler Ebene nicht aktiv ist, ist sie für Domänenanwender über verfügbar **Konfigurieren Sie Auswahlmöglichkeiten** Wird jedoch nicht als aktive Auswahl angezeigt.

Erweiterte Verwaltung der Domänentrennung

Administratoren können Informationen zur Domänentrennung anzeigen, potenzielle Probleme identifizieren und Konfigurationseinstellungen ändern.

Sie können diese erweiterten administrativen Aufgaben für Domänen ausführen:

- Verwenden Sie Domänenauswahlmenüs
- Zeigen Sie Domänenbeziehungen an

Verwenden Sie Domänenauswahlmenüs

Die Instanz bietet die Domänenauswahl über zwei Menüformate.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Domänenauswahl: Bietet eine einfache Dropdown-Liste der verfügbaren Domänen.
- Domänenreferenzauswahl: Aktiviert ein Referenzfeld, das Filterung und eine automatische Vervollständigung bietet, Vorauseintragsfunktion. Verwenden Sie dieses Format für längere Listen.

Die Platzierung dieser Auswahlmöglichkeiten und das Verfahren zum ein- oder Ausblenden unterscheiden sich je nach Version der Anwenderoberfläche.

Aktivieren Sie Domänenauswahlmenüs in Core-UI

Domänenauswahl in wird angezeigt Core-UI Aktiviert standardmäßig die Domänenauswahl. Nach dem Aktivieren der Domänenauswahl können Sie eine Systemeigenschaft hinzufügen, um die Domänenreferenzauswahl zu aktivieren.

Vorbereitungen

Hinweis: Die Domänentrennung (Plugin com.snc.PA.Domain_Support) ist erforderlich, um die Domänenreferenzauswahl zu aktivieren.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Klicken Sie im Header auf das Zahnradsymbol.
2. Klicken Sie auf der Registerkarte Allgemein auf **Domänenauswahl im Header anzeigen** Wechseln.
   Die Domänenauswahl wird in angezeigt Core-UI Header.
3. **Wahlweise:** Aktivieren Sie die Domänenreferenzauswahl.

   Hinweis: Durch Aktivieren der Domänenreferenzauswahl wird die globale Option aus der Liste entfernt. Um zu Ihrer Startdomäne zurückzukehren, klicken Sie auf den Rückgabeteil neben dem Referenzfeld. Admin-Anwender können auf den Rückgabepfeile klicken, um zur globalen Domäne zurückzukehren.

   a. Geben Sie `sys_properties.list` im Anwendungsnavigator ein.

   b. Wenn nicht bereits vorhanden, fügen Sie hinzu `Glide.ui.Domain_reference_Picker.enabled` Eigenschaft und legen Sie den Wert auf fest **Wahr** .

   c. Aktualisieren Sie den Browser.
   Die Domänenreferenzauswahl wird in angezeigt Core-UI Header.

Beschränken Sie den Zugriff auf die Domänenauswahl

Verwenden Sie eine Systemeigenschaft, um den Zugriff auf die Domänenauswahl in einzuschränken Core-UI Und Next Experience.

Vorbereitungen

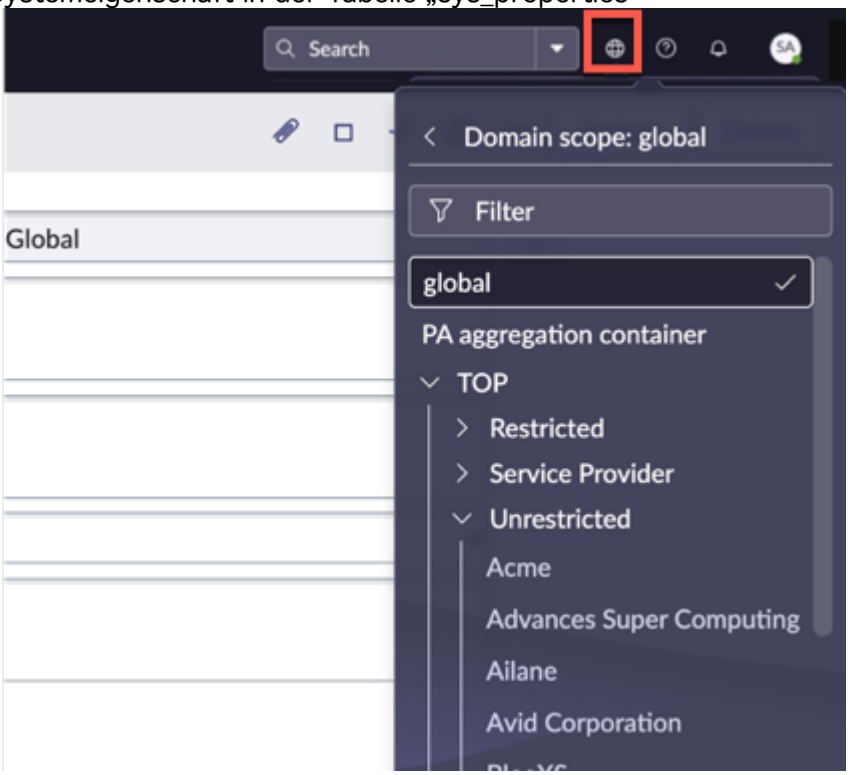
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig können Anwender mit der Rolle ITIL und Rollen, die die Rolle ITIL enthalten (z. B. Administrator), auf die Domänenauswahl in zugreifen Next Experience. Sie können anderen Rollen Zugriff gewähren, indem Sie sie der Eigenschaft hinzufügen, oder Rollen einschränken, indem Sie sie entfernen. Es wird empfohlen, die Rolle nur auf Administratoren zu beschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administratoren können Anwendern Zugriff gewähren, indem sie eine Systemeigenschaft in der Tabelle „sys_properties“ erstellen.



Prozedur

1. Öffnen Sie die Tabelle „Systemeigenschaften“ [sys_properties].
2. Diese Eigenschaft hinzufügen: `Glide.ui.polaris.Domain_Picker.role`
3. Konfigurieren Sie den Eigenschaftswert als kommagetrennte Liste von Rollen: **administrator, itil** .
   Weitere Informationen finden Sie unter Konfigurieren Sie Next Experience-Auswahlmöglichkeiten

Eigenschaften der Anwendung „Domänentrennung“

Das Plugin „Domänentrennung“ verfügt über zwei neue Tabellen, um Service Providern mehr Flexibilität bei der Anpassung ihrer Anwendungen zu geben, die Domänentrennung verwenden. Diese Tabellen sind die Tabelle „Systemanwendungseigenschaft“ [sys_Application_property] und die Tabelle „Systemanwendungseigenschaftswert“ [sys_Application_property_value].

Neue Tabellen bieten weitere Optionen

Bei Service Provider-Anwendungen (SP) können bestimmte Aktionen je nach Domäne variieren. Jedoch ist ServiceNow® Die Tabelle „Systemeigenschaften des Basissystems“ [sys_properties] ist nicht domänengetrennt und erfüllt daher nicht die Anforderungen für Anwendungen, die Domänentrennung verwenden.

Jeder SP-Kunde möchte seine Anwendungen möglicherweise anders anpassen. Zuvor wurden Funktionen, die angepasst werden konnten, nur als ein globaler Wert definiert. Anwendungsentwickler benötigen eine flexiblere Tabelle. Jetzt können Sie Ihre Anwendung ändern, ohne jedes Mal Code erstellen zu müssen, wenn Sie die Funktionalität hinzufügen oder ändern möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsweise von Überschreibungen in den neuen Tabellen

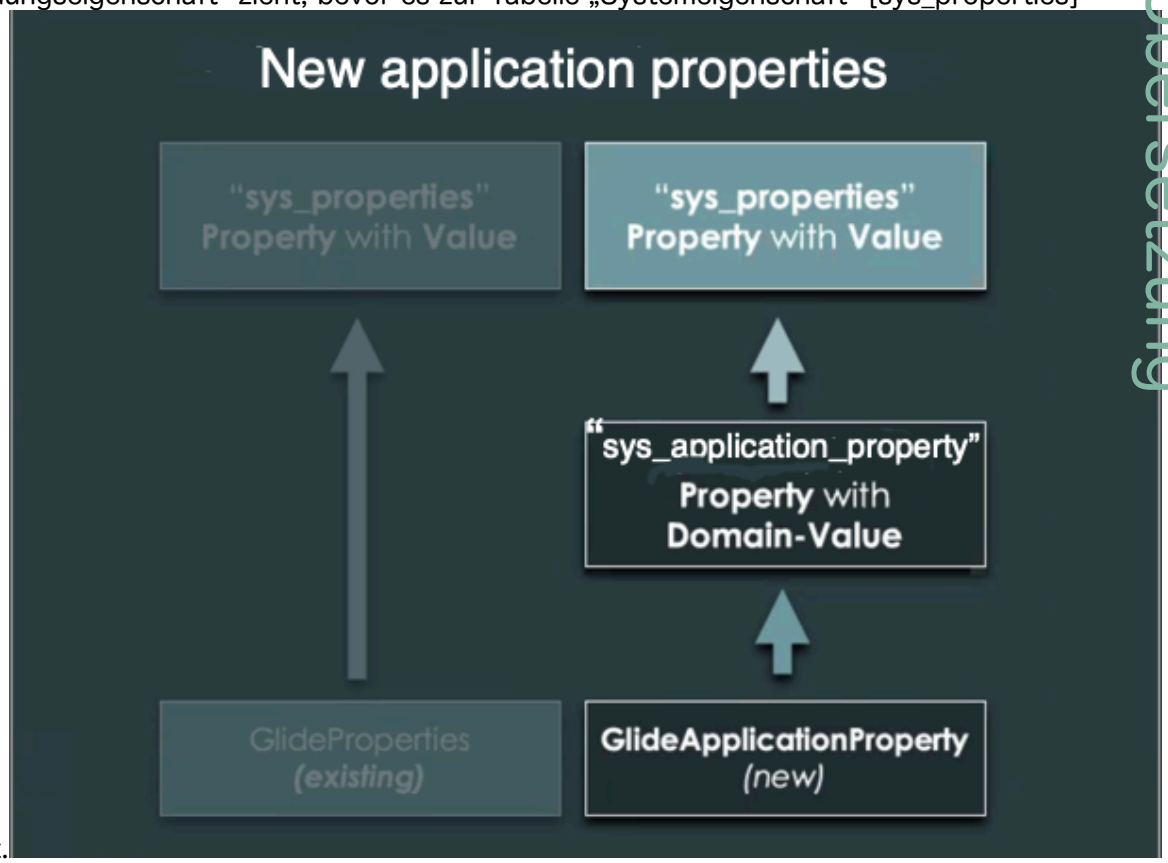
Entwickler verwenden normalerweise ServiceNow Tabelle „Systemeigenschaft“ [sys_properties] zum Erstellen verschiedener Funktionen in Anwendungen. Wenn Sie eine Anwendung so entwickeln möchten, dass sie sich in verschiedenen Domänen unterschiedlich verhält, müssen Sie sie selbst anpassen.

Im Release Paris vereinfacht die neue Tabelle „Anwendungseigenschaft“ [sys_Application_property] diese Anpassung. Anstatt für einen Wert direkt zur Systemeigenschaftstabelle zu wechseln, wird die Anwendungseigenschaftstabelle zuerst in die Systemanwendungstabelle geleitet. Diese neue Tabelle speichert jetzt die Logik, die Sie zum Konfigurieren Ihrer Anwendung benötigen. Wenn eine Eigenschaft in der neuen Tabelle gefunden wird, wird dieser Inhalt verwendet. Wenn diese Tabelle keine Informationen enthält, wird die Tabelle mit den Eigenschaften des Basissystems angezeigt.

Wenn Sie die Unterstützung für die Domänentrennung konfigurieren, können Sie dieser neuen Tabelle „Anwendungseigenschaften“ Domänenlogik hinzufügen. Diese Tabelle kann Eigenschaften enthalten, die in der Tabelle „Systemeigenschaften“ nicht vorhanden sind. Oder Sie können der Konfigurationstabelle Eigenschaften hinzufügen, die jede Eigenschaft überschreiben können, die Sie in der Tabelle „Systemeigenschaften“ auswählen.

Angenommen, Sie möchten eine Anwendung mit der Funktion „erster Wochentag“ konfigurieren. Manchmal möchten Sie, dass der erste Tag der Woche Sonntag ist. In anderen Fällen möchten Sie möglicherweise, dass der erste Wochentag Montag ist. In der Basissystemtabelle gibt es möglicherweise nur die Option „One Day 1“ (Sonntag). Mit der neuen Tabelle können Sie eine weitere Eigenschaft speichern, d. h. Tag 1, Sonntag und eine untergeordnete Domäne Montag.

Diese Abbildung zeigt, wie das System Eigenschaften aus der Tabelle „Anwendungseigenschaft“ zieht, bevor es zur Tabelle „Systemeigenschaft“ [sys_properties] wechselt.

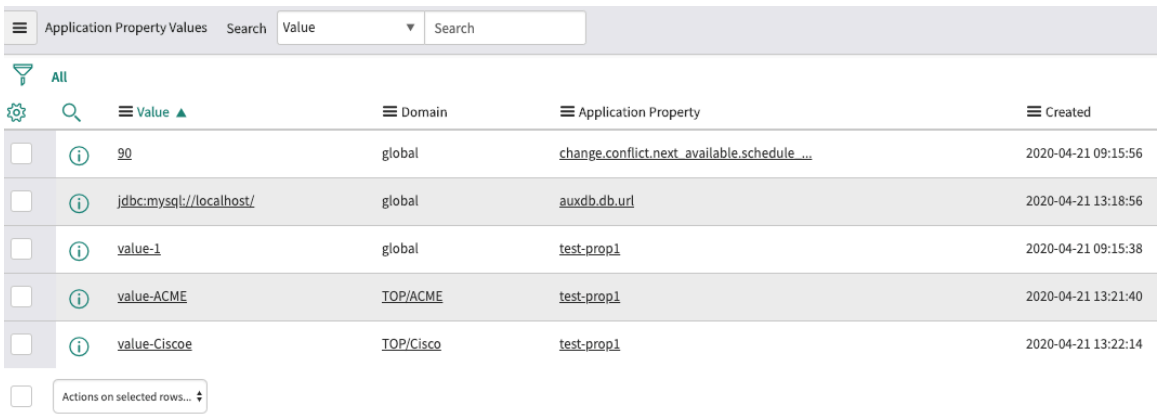


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie bereichsbezogene Apps in der neuen Tabelle funktionieren

Die neue Tabelle „Anwendungseigenschaften“ wird von bereichsbezogenen Anwendungen unterstützt. Der Name der Anwendungseigenschaft ist ähnlich wie der Systemeigenschaftsname eindeutig. Dies bedeutet, dass ihm der Bereichsname vorangestellt wird, wenn er nicht global ist. Der Umfang einer Anwendung wirkt sich auf Ihre Konfiguration aus. Der Umfang kann bestimmen, welcher Tag 1 als Sonntag und welcher als Montag definiert ist. Sie können dieselbe Eigenschaft verwenden, sie jedoch so anpassen, dass Tag 1, Sonntag die übergeordnete Domäne und Tag 1, Montag die untergeordnete Domäne ist. In der neuen Tabelle gibt es sowohl eine Domänenspalte als auch eine Bereichsspalte, sodass Sie diese Eigenschaften für jede festlegen können.

Sie können die Ansicht „Domänenbereich erweitern“ in der Tabelle „sys_Application_property_value“ verwenden, um alle Überschreibungen anzuzeigen, wie in der folgenden Abbildung gezeigt.



Hinweis:

Wenn diese Tabellen nicht verfügbar sind, stellen Sie sicher, dass Sie das Plugin „Domänenerweiterungs-Installationsprogramm“ (com.glide.domain.msp_extensions.installer) aktiviert haben.

Neue Anwendungseigenschaftstabellen

Die neue Tabelle „Systemanwendungseigenschaft“ [sys_Application_property] enthält diese Felder:

- name
- Beschreibung
- Typ (Auswahl von Zeichenfolge, wahr|falsch, Ganzzahl, Zeitzone, Farbe, und so weiter)
- default_value
- Eigenschaft (Verweis auf sys_properties)
- Usage_Notes
- Read_roles
- Write_roles
- Eindeutiger Schlüssel: (Name)

Die neue Tabelle „Eigenschaftswert der Systemanwendung“ [sys_Application_property_value] enthält diese Felder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sys_Application_property (Verweis auf sys_Application_property)
- sys_domain
- sys_overrides
- Wert
- Eindeutiger Schlüssel: (sys_Application_property, sys_Domain)

Neue APIs

Die neuen APIs werden auch in bereichsbezogenen Apps unterstützt. Domänengetrennte Anwendungseigenschaften haben eindeutige APIs. Die GlideApplicationProperty-API verfügt über zwei neue skriptfähige Methoden, die sowohl in globalen als auch in bereichsbezogenen Anwendungen verfügbar sind. Siehe GlideApplicationProperty: Bereichsbezogen, Global Um mehr über diese neuen APIs zu erfahren.

Zugehörige Informationen

Empfohlene Domain Separation-Verfahren für Service Provider

Domänenmigrationstool

Verwenden Sie das Domänenmigrationstool, um einen Kunden aus einer domänengetrennten Umgebung in seine eigene dedizierte Instanz zu verschieben.

Plugin „Domänenmigrationstool“

Das Plugin „Domain Migration Tool“ (com.Glide.Domain.Migration_Tool) vereinfacht die Aufgabe, einen Kunden aus einer domänengetrennten Umgebung in eine flexiblere dedizierte Instanz zu verschieben. Kunden möchten möglicherweise zu einer separaten Instanz migrieren, um die Vorteile von besser nutzen zu können ServiceNow AI Platform Fähigkeiten. Obwohl das Plugin „Domänentrennung“ installiert ist, sind die Eigenschaften der Daten- und Prozesstrennung deaktiviert.

Hinweis: Sie müssen eine geklonte Instanz anfordern und die Aktivierung des Plugins „Domain Migration Tool“ anfordern, bevor Sie es verwenden können.

Das Domänenmigrationstool wird nur ausgeführt, wenn sowohl Daten- als auch Prozesstrennung in der domänengetrennten Instanz aktiviert sind:

- Die *glide.sys.domain.partitioning*Dateneigenschaft muss auf festgelegt werden **Wahr** .
- Die *glide.sys.domain.delegated_administration*Prozesseigenschaft muss auf festgelegt sein **Wahr** .

Was das Migrationstool tut

- Automatisiert einen Großteil des Migrationsprozesses, insbesondere das Bereinigen von Daten.
- Migriert die domänengetrennte Instanz zu einer neuen dedizierten Instanz.
- Löscht Daten aus der dedizierten Instanz.

Hinweis: Das Tool löscht keine Daten, die global sind, sich in der Zieldomäne oder in zusätzlichen Datendomänen (falls angegeben) befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Reduziert Prozessdaten oder löscht Prozessdaten, wenn sie nicht reduziert werden können
- Speichert Prozessdatensätze, die für die Zieldomäne sichtbar sind
- Aktualisiert die speziellen Tabellen „sys_choice“, „sys_ui_list“ und „sys_ui_related_list“
- Bereinigt Datensätze, die von Domänentrennungs-Plugins hinzugefügt wurden:
  - Business-Regeln
  - UI-Aktionen
  - Geplante Aufgaben
  - Installationsausgänge
  - Navigationsmodule
- Deaktiviert die Domänentrennung und entfernt Domänen aus der geklonten Instanz:
  - Legt diese Eigenschaften auf fest **Falsch** In der geklonten Instanz:
    - *`glide.sys.domain.partitioning`*
    - *`glide.sys.domain.delegated_administration`*
    - *`glide.sys.domain.enabled`*
  - Löscht alle Domänen mit Ausnahme der Zieldomäne und aller zusätzlichen angegebenen Datendomänen.
- Aktualisiert **Status** Feld in der Tabelle „Domain_Migration_Tool_Status“.

Individueller Status der Tabellen

Status	Beschreibung
Ausstehend	Standardstatus von domänengetrennten Tabellen während der Migration. Die Migration der Tabellen ist geplant, die Migration wurde jedoch noch nicht gestartet.
Fehler	Fehler auf Tabellenebene. Wenn der Migrationsprozess mit Fehlern abgeschlossen wurde, gibt dieser Status an, welche Tabellen Fehler aufweisen.
Wird ausgeführt	Der Status der Tabelle, die derzeit migriert wird. Nur eine Tabelle kann diesen Status haben und wird derzeit migriert.
Erfolgreich	Der Status der Tabellen, die erfolgreich migriert wurden.
Erfolgreich beendet	Der Migrationsprozess wurde ohne Fehler abgeschlossen.
Mit Fehlern abgeschlossen	Der Migrationsprozess wurde mit Fehlern abgeschlossen.

- Protokolliert Fortschritt und Status in „syslog_Domain“

  Die Quelle ist **MigrationTool** Für alle Protokolleinträge, die der Migration zugeordnet sind.

  - Protokolliert jede Datentabelle und wie viele Datentabellen verbleiben
  - Protokolliert jede Prozesstabelle und welche Datensätze der Domäne derzeit deaktiviert oder gelöscht werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Was das Migrationstool nicht tut

- Klonen Sie die Instanz
- Erstellen Sie eine weitere domänengetrennte Instanz
- Migrieren Sie Datensätze (Daten oder Prozess), wenn entweder Daten- oder Prozesstrennungseigenschaften deaktiviert sind, bevor Sie das Tool ausführen
- Ändern Sie alle Daten in der Quellinstanz
- Daten löschen, die global sind, sich in der Zieldomäne oder in zusätzlichen Datendomänen befinden (falls angegeben)

Was Sie nach der Ausführung des Tools tun müssen

Das Domänenmigrationstool automatisiert die Entfernung von Daten außerhalb der gewünschten Domänen (Zieldomäne, zusätzliche Datendomänen und globale Domäne). Sie müssen alle verbleibenden Konfigurationen auswerten, um sicherzustellen, dass sie für Ihre dedizierte Instanz geeignet sind und funktionieren. Wenn Sie beispielsweise eine Business-Regel hatten, die das Domänenfeld in Datensätzen festlegt, sollten Sie diese Business-Regel deaktivieren, da sie nicht mehr einem Zweck dient.

Migrieren Sie eine domänengetrennte Instanz zu einer dedizierten Instanz

Verschieben Sie einen Kunden aus einer domänengetrennten Umgebung in seine eigene dedizierte Instanzumgebung.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

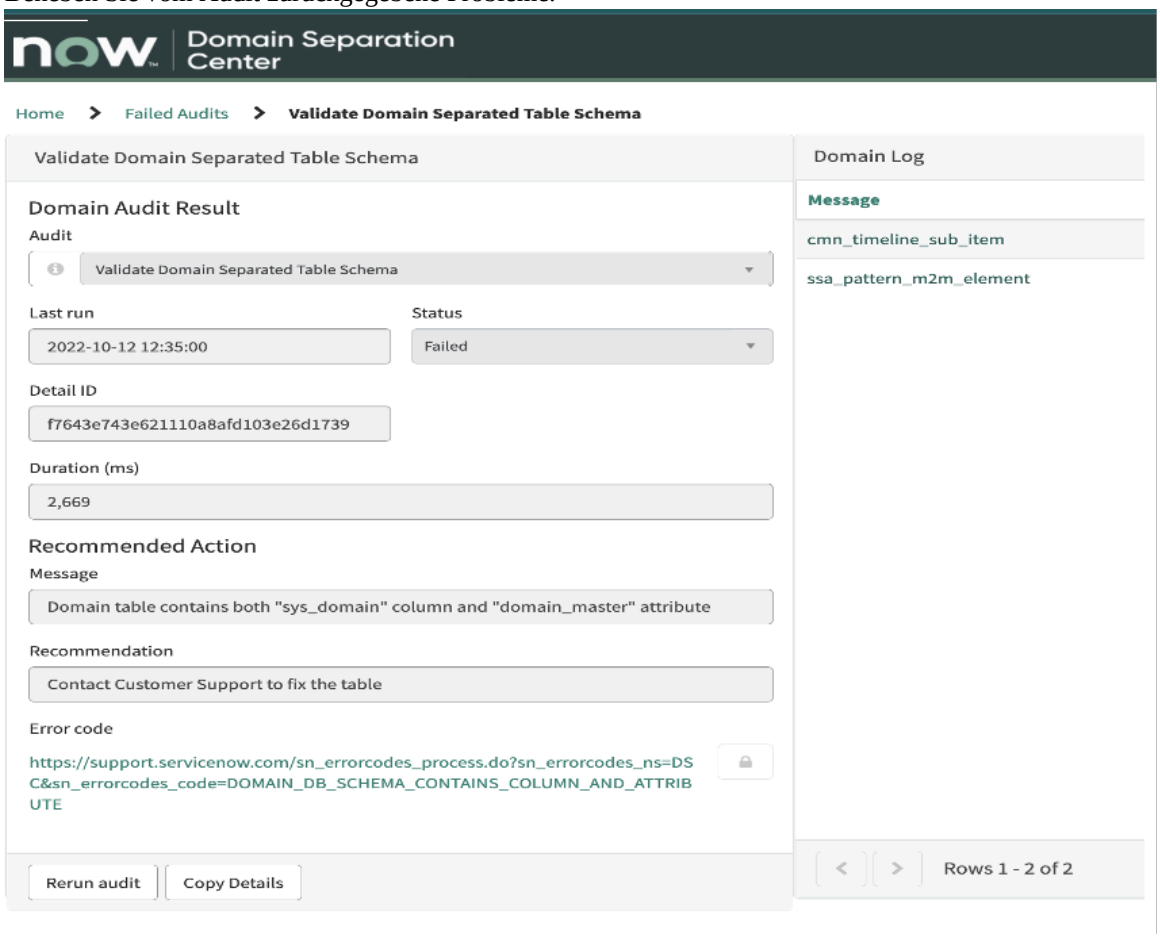
1. Erhöhen Sie die Berechtigungen auf die Rolle security_admin.
   Details siehe Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Alle** > **Domänenadministrator** > **Domänenmigrationstool**an.
   Greifen Sie auch mit zu **Domain_Migration_Tool_Status.list** .
3. Klicken Sie auf **Neu**.
4. Füllen Sie das Formular aus.

Feld	Beschreibung
Zieldomäne	Geben Sie die Domäne an, die sowohl für den Prozess als auch für die Daten verwendet wird, die Sie migrieren möchten. Nur die Zieldomäne wird beibehalten, keine ihrer untergeordneten Elemente, es sei denn, dies ist in angegeben **Zusätzliche Datendomänen** Feld.
Zusätzliche Datendomänen	Geben Sie optional zusätzliche Datendomänen an, die Sie migrieren möchten. Wenn Sie die Zieldomäne und alle ihre untergeordneten Elemente migrieren möchten, müssen Sie alle untergeordneten Elemente angeben.

5. Wählen Sie **Absenden**.
6. Öffnen Sie das gerade übermittelte Formular.
7. Navigieren zu **Alle** > **Domain Separation Center** > **Audits konfigurieren** .
   Weitere Informationen finden Sie unter Domain Separation Center.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

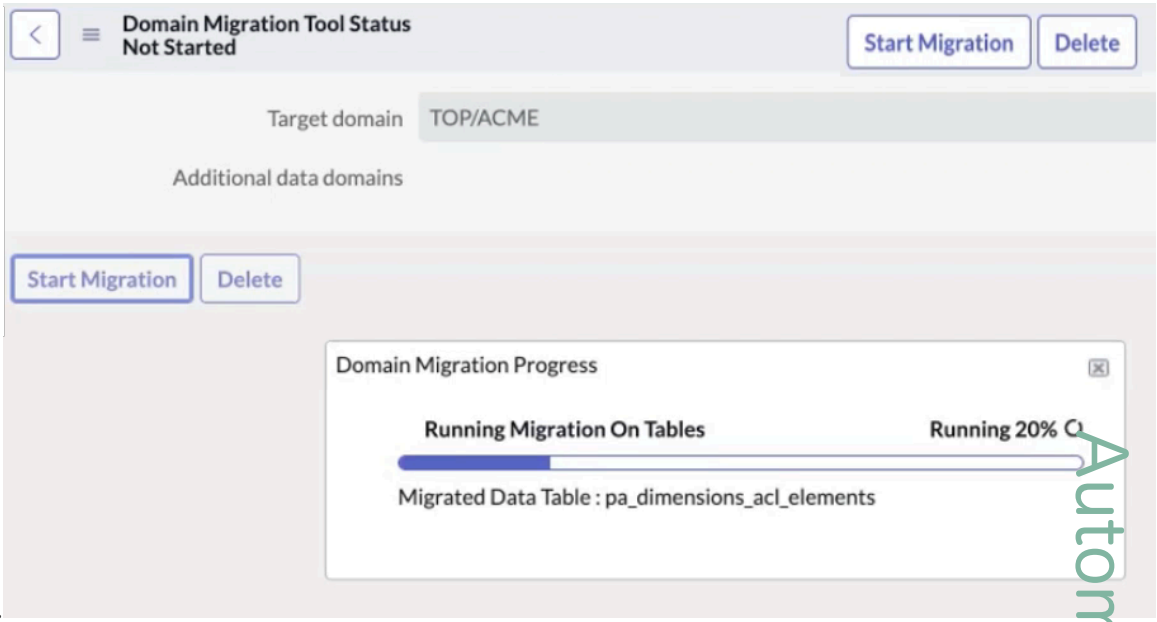
8. Legen Sie fest **Validieren Sie Das Schema Der Domänengetrennten Tabelle** Audit bis **Aktiv** Und weisen Sie einen Zeitplan zu.
   Dies ist ein vorsichtiges Domänenaudit, um das Schema auf die Integrität von domänengetrennten Tabellen vorab zu überprüfen. Auf diese Weise können Sie Fehler beheben, bevor Sie die Migration ausführen.
9. Führen Sie aus **Audit-Zeitplan** Das das Schema enthält.
   Details siehe Führen Sie Audits sofort aus.
10. Beheben Sie vom Audit zurückgegebene Probleme.



11. Wählen Sie Aus **Starten Sie Die Migration** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Fortschrittsbalken des Ausführungstrackers und das Domänenmigrationstool werden



ausgelöst.

- Die aktuell fortschreitende Migrationstabelle wird zusammen mit dem Gesamtprozentsatz der erfolgreich migrierten Tabellen angezeigt.
- Die Tabelle, in der alle domänengetrennten Tabellen mit dem Migrationsstatus, der Gesamtzahl der Datensätze in jeder Tabelle und der Anzahl der migrierten Datensätze aufgezeichnet werden.
- Die Anzahl der Tabellen, in denen die Migration fehlgeschlagen ist, wird ebenfalls aufgezeichnet.
- Die **Status** Wird aktualisiert, wenn das Tool seine Funktionen ausführt.
- Die Domänenmigration wird weiterhin im Hintergrund ausgeführt, wenn Sie den Fortschrittsbalken schließen. Greifen Sie auf zu `sys_Execution_Tracker` Tabelle und suchen nach **Migration für Tabellen wird ausgeführt** Dient zum Überprüfen des Migrationsprozesses, der im Hintergrund ausgeführt wird.

Der Status des Domänenmigrationstools zeigt die folgenden Felder an:

Statusfelder des Domänenmigrationstools

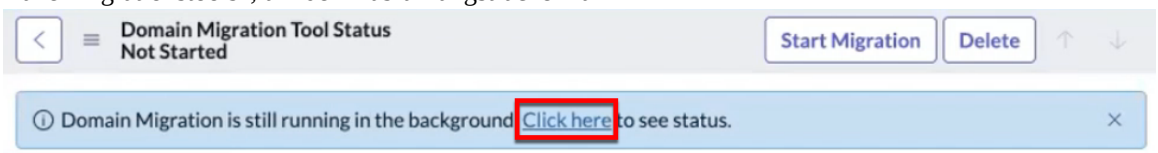
Feld	Beschreibung
Status	Zeigt den Migrationsstatus an. ○ **Datentabellen werden migriert...** : Status „in Bearbeitung“. ○ **Migration erfolgreich** : Der aktualisierte Status nach einer erfolgreichen Migration. ○ **Eine falsche Konfiguration wird in einer der domänengetrennten Tabellen beobachtet** : Gibt einen Fehler bei der Datenmigration an. Ein Schemafehler wurde gefunden. Die Migration wird nicht gestartet. Führen Sie das Audit aus **Validieren Sie das Schema der domänengetrennten Tabelle** . Das Audit schlägt fehl und zeigt die Tabellen an, die nicht dem Schemastandard entsprechen. ○ **Abgeschlossen mit Fehlern in Überprüfungstabellen** : Die Anzahl der Tabellen zur Behandlung der Schemamigration wird aufgelistet. Suchen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie die Fehler in der Anzahl der Überprüfungstabellen, und beheben Sie Schemaprobleme. ○ **Domänenmigration für Tabellen fehlgeschlagen...** : Nicht-Zieldatensätze sollten manuell aus fehlgeschlagenen Tabellen gelöscht werden. ○ **Erfolgreich Abgeschlossen** : Wenn alle Tabellen migriert wurden.
Zieldomäne	Die ausgewählte Zieldomäne für die Migration.
Zusätzliche Datendomänen	Wird ausgefüllt, wenn mehrere Migrationsdomänen ausgewählt wurden.
Anzahl der erneut verarbeiteten Tabellen	Dieses Feld wird nur ausgefüllt, wenn eine Tabelle nicht migriert werden kann. Wenn keine Fehler auftreten, ist diese Anzahl null. In diesem Fall werden die Tabellen überprüft, um die Migration erneut zu versuchen. Wenn keine Fehler auftreten, müssen Sie die Tabellen nicht erneut überprüfen oder die Migration erneut versuchen.
Aktuell verarbeitete Tabelle	Zeigt den Namen der Tabelle an, die derzeit migriert wird. Nach erfolgreicher Migration ist dieses Feld leer.

12. Wählen Sie aus **Klicken Sie hier**Link auf der Seite „Status des Domänenmigrationstools“, um den Ausführungstracker zu öffnen.

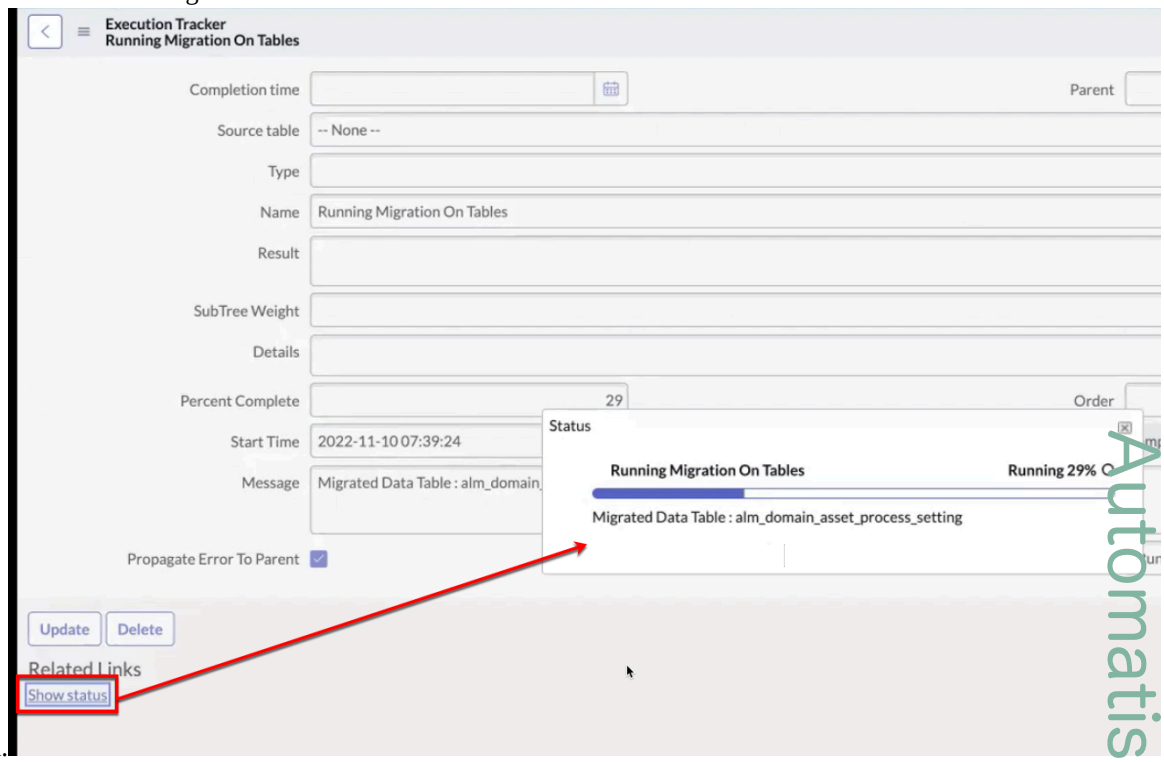


Sie können auch auf zugreifen `sys_Execution_Tracker` Tabelle und suchen nach **Migration für Tabellen wird ausgeführt** Dient zum Überprüfen des Migrationsprozesses, der im Hintergrund ausgeführt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

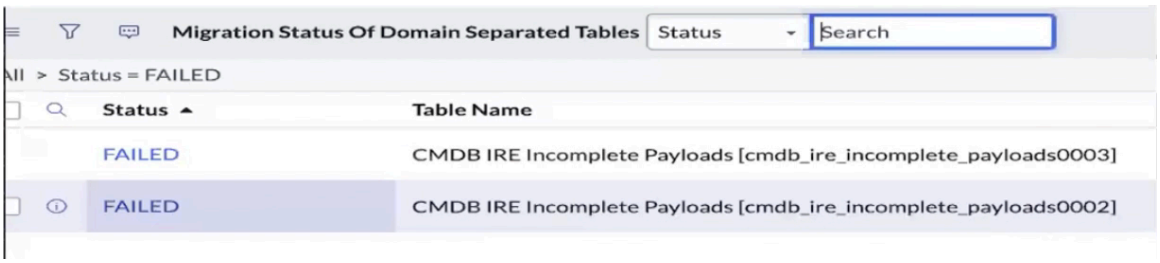
13. Wählen Sie Aus **Status anzeigen**Im Abschnitt „zugehörige Links“, um jederzeit während der Migration auf den Fortschrittsbalken zuzugreifen.



Wenn eine Tabelle die Schemaprüfung nicht bestanden hat, wird der Gesamtstatus der domänengetrennten Tabellen auf festgelegt **Fehlgeschlagen**.



Es wird geben **Fehlgeschlagen** Einträge für jede entsprechende Tabelle.

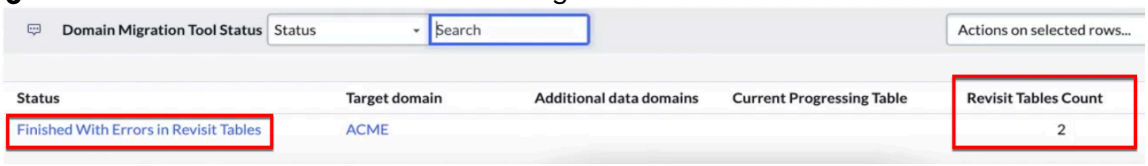


Der Rest der Migration wird fortgesetzt, und eine Zusammenfassung aller fehlgeschlagenen Tabellen und der Gesamtzahl von **Anzahl Der**

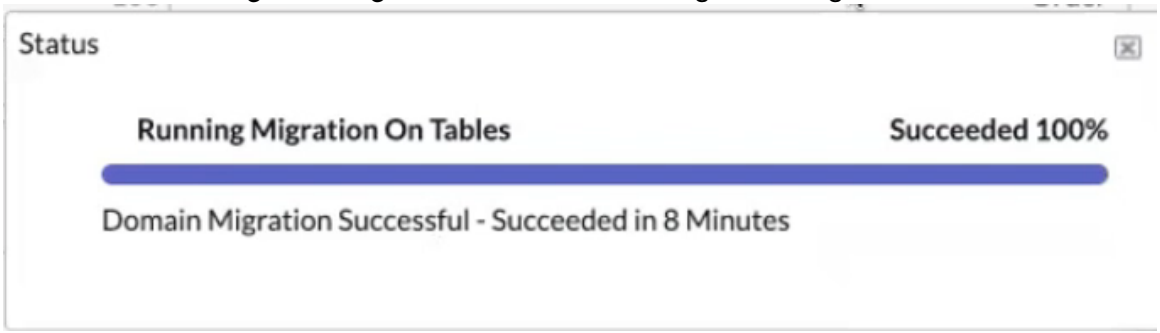
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ÜberprüfungstabellenWird im Status des Domänenmigrationstools ausgefüllt.



Die **Status** Ist **Erfolgreich Abgeschlossen**Wenn die Migration abgeschlossen ist.



Prozessverwaltung

Mit der Prozessverwaltung können Administratoren domänenspezifische Richtlinien festlegen.

Die in der Domänenhierarchie unten festgelegten Richtlinien überschreiben Richtlinien, die höher in der Domänenhierarchie festgelegt sind. In einer Domäne können Administratoren domänenspezifische Versionen dieser globalen Richtlinien und Einstellungen festlegen:

- Client-Skripts
- Systemrichtlinien
- Anwendungs- und Modulnamen
- Anwendungsrollen
- Modulfilter

⚠ **Warnung:** Alle Anwender mit der Administratorrolle haben besonderen Zugriff auf alle Systemfunktionen, -Funktionen und -Daten, da Administratoren ACL-Regeln überschreiben und alle Rollenprüfungen bestehen können. Gewähren Sie diese Berechtigung sorgfältig.

Wenn Anwender haben **Administrator** Rolle, dann sind alle Richtlinien in der Instanz für sie verfügbar, unabhängig von der zugewiesenen Domäne. Sie können eine bestimmte Domäne eingeben, und dann sind nur Richtlinien in dieser Domäne oder höher sichtbar und während einer relevanten Transaktion verarbeitet. Wenn ein Administrator eine Richtlinie ändert, die sich in einer höheren Domäne oder der globalen Domäne befindet, erstellt das System automatisch einen neuen Datensatz für die aktuelle Domäne dieses Administrators. Der ursprüngliche Richtlinien-, Anwendungs- oder Moduldatensatz wird dadurch nicht geändert. Dieser neue Datensatz überschreibt den ursprünglichen.

Um Änderungen an einer Richtlinie in einer Domäne auf untergeordneter Ebene vorzunehmen, wechseln Sie zu dieser Domäne, und ändern Sie die Richtlinie. Dieser Ansatz erstellt den Richtliniendatensatz in Ihrer Domäne, der den ursprünglichen, übergeordneten Richtliniendatensatz überschreibt.

Ändern Sie nicht die Richtlinie auf höherer Ebene, und ändern Sie dann die **Domäne** Feld in dieser Richtlinie. Dieser Ansatz erstellt keinen Richtliniendatensatz in Ihrer Domäne auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

untergeordneter Ebene, und der Richtliniendatensatz für die Domäne auf höherer Ebene wird nicht gespeichert.

Die **sys_overrides** Das Feld gibt an, dass eine Richtlinie, Anwendung oder ein Modul auf einer niedrigeren Ebene in der Hierarchie einen Datensatz auf einer höheren Ebene überschreibt. Das System legt dieses Feld automatisch fest, wenn ein Administrator versucht, eine Richtlinie, Anwendung oder ein Modul zu ändern, die zu einer anderen Domäne höher in der Hierarchie gehört.

Anstatt den Datensatz auf höherer Ebene zu ändern, wird das versuchte Update in eine Einfügung und geändert **sys_overrides** Das Feld ist festgelegt, um die Richtlinie, Anwendung oder das Modul auf höherer Ebene anzugeben, die bzw. das überschrieben wird. Wenn später die Datensätze für eine relevante Transaktion geladen werden, wird anstelle des Originals die überschreibende domänenspezifische Richtlinie, Anwendung oder Modul verwendet.

Domänen für die Prozessverwaltung

Standardmäßig verwendet die Prozessverwaltung immer die Domäne des Datensatzes, um zu bestimmen, welche Richtlinien angewendet werden sollen.

Die Domäne des Datensatzes hat Vorrang vor der Domäne des Anwenders. Wenn in der Domäne des Datensatzes keine Richtlinien vorhanden sind, überprüft die delegierte Administration nach Richtlinien auf der nächsthöhen Ebene der Domänenhierarchie. Die Suche nach Domänenrichtlinien wird in der Domänenhierarchie fortgesetzt, bis die globale Domäne erreicht wird. Wenn in der Domänenhierarchie keine Domänenrichtlinien niedriger sind, verwendet die Prozessverwaltung die Richtlinien für die globale Domäne.

Fred Luddy ist beispielsweise ein Anwender in der Acme-Domäne, der Datensätze in den untergeordneten Domänen Acme: Atlanta, Acme: San Diego und Acme: NY anzeigen kann. Wenn dieser Anwender einen Datensatz in der Acme: San Diego-Domäne öffnet, sucht die Prozessverwaltung zuerst nach Richtlinien in der Acme: San Diego-Domäne. Wenn auf dieser Ebene der Domänenhierarchie keine Richtlinien vorhanden sind, überprüft die Prozessverwaltung nach Richtlinien aus der Acme-Domäne. Wenn in der Acme-Domäne keine Richtlinien vorhanden sind, verwendet die Prozessverwaltung die globalen Domänenrichtlinien, da es keine anderen Domänen höher in der Domänenhierarchie gibt.

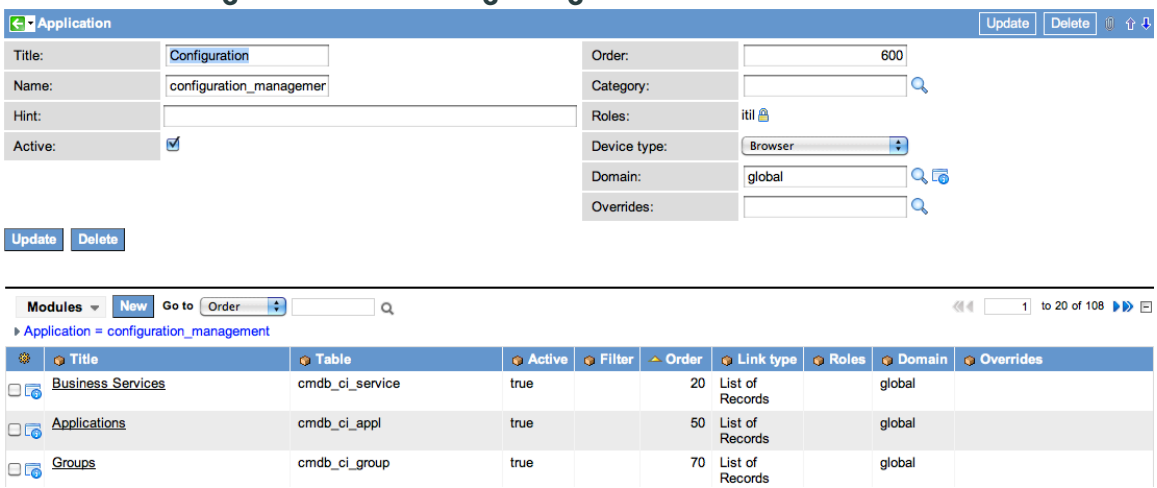
Beispiel für die Prozessverwaltung mit domänenspezifischen Anwendungen

Das folgende Beispiel veranschaulicht die Prozessverwaltung mit domänenspezifischen Anwendungen und Modulen.

Als Administrator der Oceanic-Domäne entscheidet sich David Loo, die Konfigurationsanwendung anzupassen. Zunächst überprüft David die im Anwendungsmodul „Konfiguration“ verfügbaren Module.

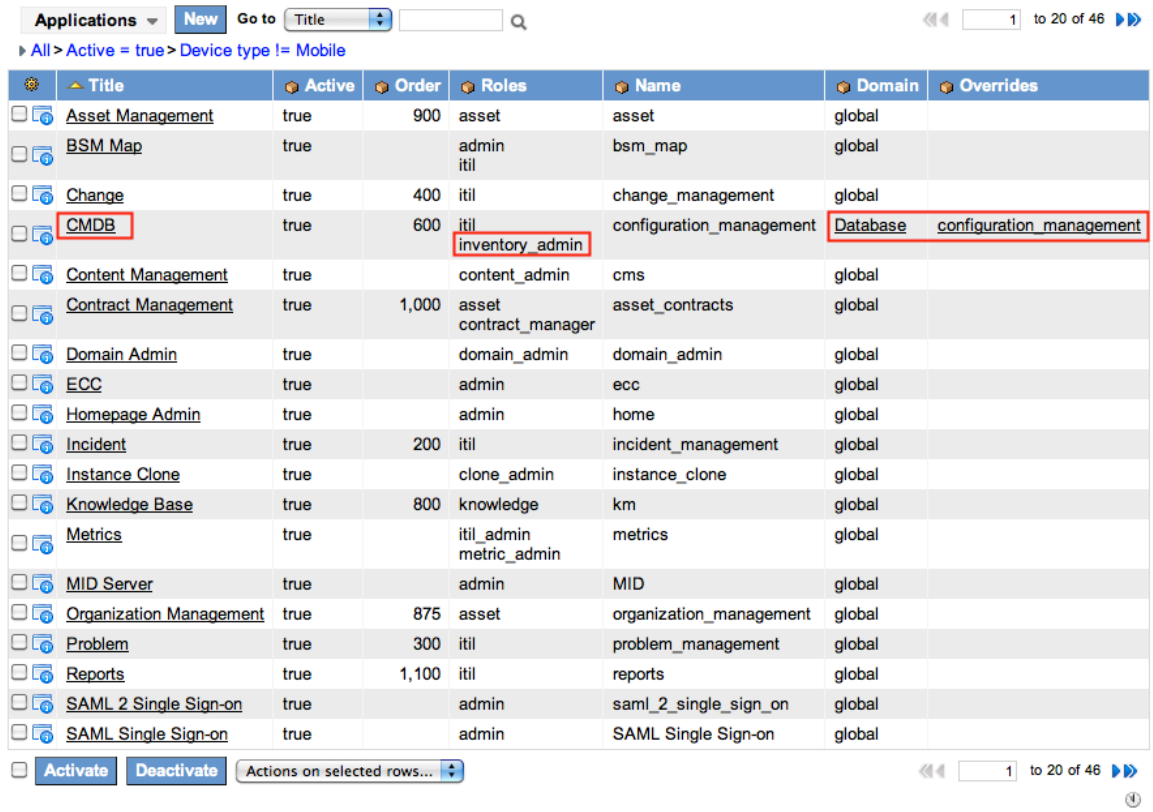
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht der Konfigurationsanwendung wird gestartet



David beschließt, die Konfigurationsanwendung in CMDB umzubenennen und der Rolle „Inventory_admin“ zu erlauben, die Anwendung anzuzeigen.

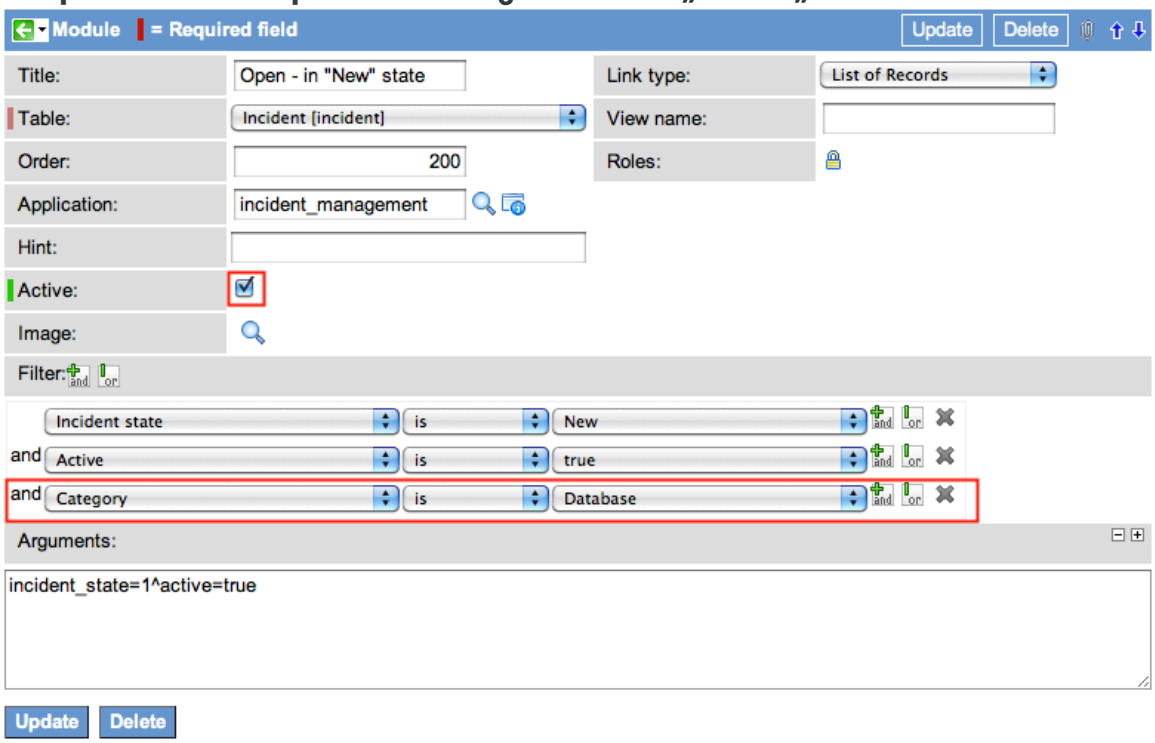
Beispiel für domänenspezifische Changes an der Konfigurationsanwendung



Als Nächstes entscheidet David, die Incident-Anwendung zu ändern, indem er aktiviert **Offen – im Status „Neu“** Modul und Hinzufügen eines neuen Filterelements, um offene Incidents in der Kategorie „Ozeane“ anzuzeigen.

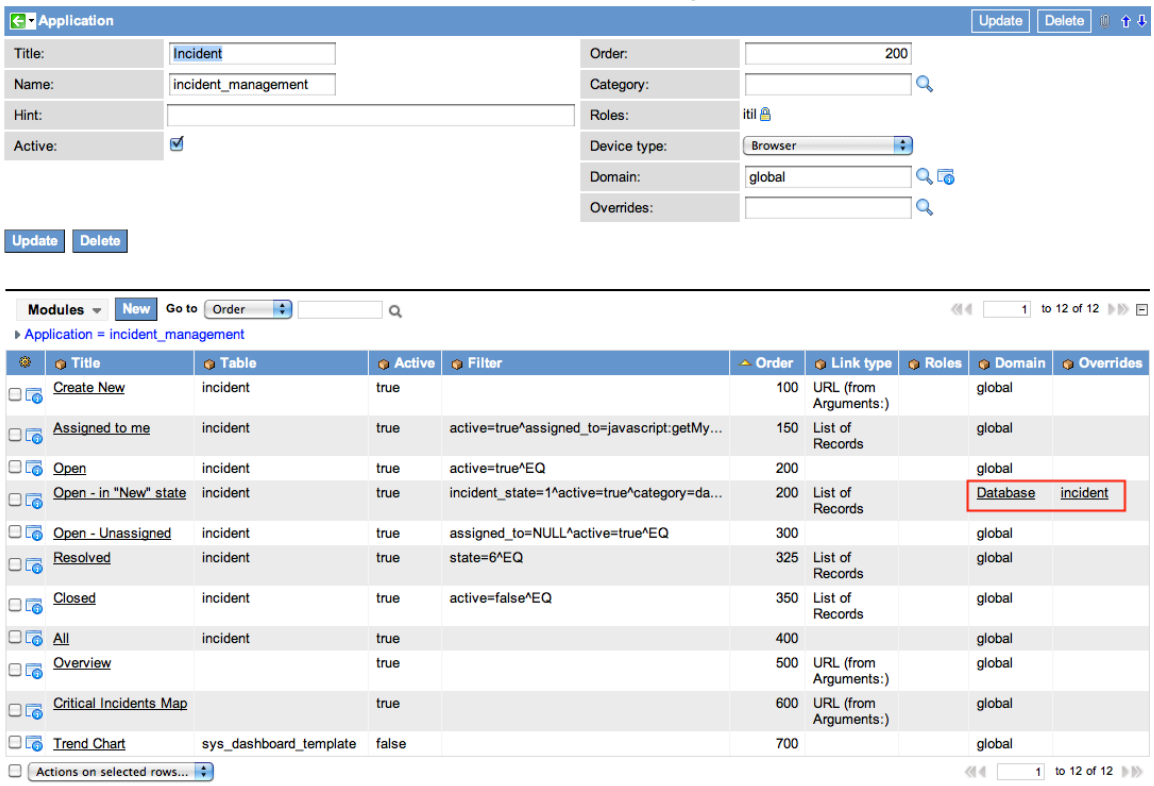
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für domänenspezifische Changes am Modul „Offen – „Neu“ – Status“



Dadurch wird ein neuer Moduleintrag in der Anwendung erstellt, anstatt das vorhandene Modul in der globalen Domäne zu überschreiben.

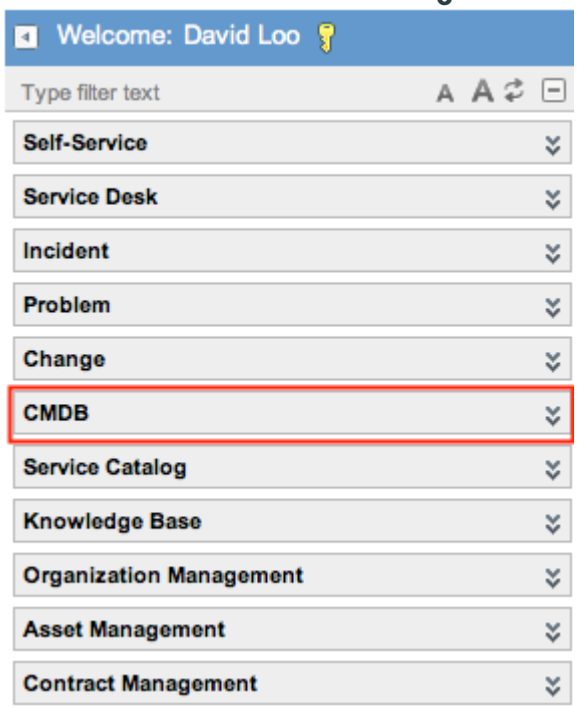
Domänenspezifische Ansicht der Incident-Anwendung



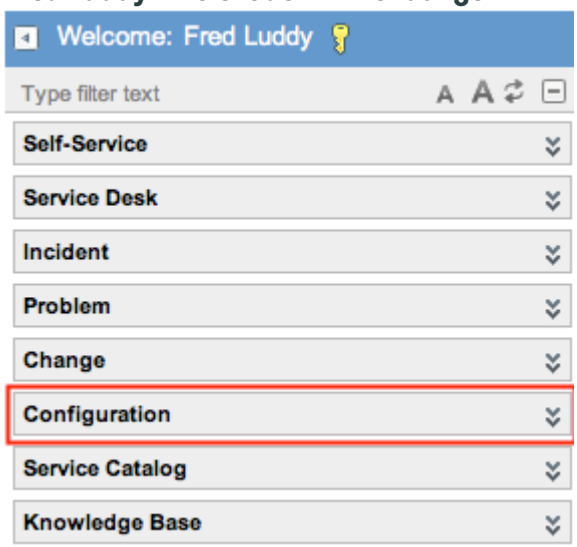
Wenn sich ein anderer Administrator aus einer anderen Domäne, z. B. Fred Luddy, anmeldet und sich die Konfigurationsanwendung ansieht, werden die Einstellungen aus der globalen Domäne angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

David Loo-Ansicht der Anwendungen



Fred Luddy-Ansicht der Anwendungen



Aktivieren Sie die ausführliche Domänenprotokollierung und Debug-Nachrichten

Domänenprotokoll und Debug-Nachrichten ermöglichen Ihnen die Behebung von Domänenkonfigurationsfehlern.

Vorbereitungen

Erforderliche Rolle: Administrator

Stellen Sie sicher, dass Sie die neueste Instanz sind, um die beste Leistung zu erzielen.

Prozedur

1. Navigieren Sie im Domain Separation Center zu **Domänenadministrator** .
2. Klicken Sie Auf **Konfigurieren Sie Das Domänenzentrum** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Für **Aktivieren Sie die ausführliche Domänenprotokollierung** , Wählen Sie aus **Ja** Kontrollkästchen.
4. Klicken Sie auf **Aktualisieren**.

Zeigen Sie eine Echtzeitdomänennachricht an

Sie können Echtzeitdomänennachrichten aus den Systemprotokollen anzeigen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Ausführliche Domänenprotokollierung aktivieren: Navigieren Sie zu **Alle** > **Domänenadministrator** > **Domain Separation Center** > **Domänencenter konfigurieren** > **Aktiviert die Detaildomänenprotokollierung** > **Ja** (Oder legen Sie die Eigenschaft fest Glide.sys.Domain.ausführlich Bis **Wahr**).
2. Navigieren zu **Systemdiagnostik** > **Sitzung debuggen** > **Alle aktivieren**an.
   Da dies eine Echtzeitüberprüfung ist, muss die Debug-Sitzung nicht ausgeführt werden, bevor die Protokolldateien überprüft werden.
3. Navigieren Sie zur Sitzungs-Debug-Konsole, um die detaillierten Systemdomänenprotokolle anzuzeigen.
4. Suchen Sie nach der Textabfrage für die Tabelle.

   Diese Abfrage findet Protokollnachrichten in diesem Format:

   ```
   08:36:43.974: [Domain Paths] Query against table incident restricted by domain values
    [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b],
   Database[287ee6fea9fe198100ada7950d0b1b73],
   Database San Diego[db53a9290a0a0a650091abebccf833c6], global, NY
    DB[5f74727dc0a8010e01efe33a251993f9]]
   ```

   In diesem Beispiel hat der Anwender, der die Incident-Tabelle anzeigt, nur Datensätze gesehen, die den DB-Domänen Database Atlanta, Database, Database San Diego, Global und NY entsprechen.

Zeigen Sie eine historische Domänennachricht an

Zeigen Sie historische Domänennachrichten in der Protokolldatei an, um Probleme mit der Domänentrennung zu beheben.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Ausführliche Domänenprotokollierung aktivieren: Navigieren Sie zu **Alle** > **Domänenadministrator** > **Domain Separation Center** > **Domänencenter konfigurieren** > **Aktiviert die Detaildomänenprotokollierung** > **Ja** (Oder legen Sie die Eigenschaft fest Glide.sys.Domain.ausführlich Bis **Wahr**).
2. Navigieren zu **Systemdiagnostik** > **Sitzung debuggen** > **Alle aktivieren**an.
3. Lassen Sie die Debug-Sitzung für einen Zeitraum, z. B. einen Tag, ausführen, bevor Sie die Protokolldateien überprüfen.
4. Navigieren zu **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Öffnen Sie den Datensatz für den Tag, den Sie anzeigen möchten.
   Protokolldateien verwenden das Namensformat `Localhost_log.<yyyy-mm-dd>.txt` .
6. Klicken Sie auf **Herunterladen** Zugehörigen Link zum Protokoll.
7. Öffnen Sie die heruntergeladene Protokolldatei in einem Texteditor, und suchen Sie nach Protokollnachrichten im folgenden Format:

   Abfrage für Tabellen-Incident, eingeschränkt durch Domänenwerte `[Global, Software[8a4dde73c6112278017a6a4baf547a7]]`

   In diesem Beispiel hat ein Anwender nur Datensätze aus der Incident-Tabelle gesehen, die den globalen Domänen und der Softwaredomäne entsprechen.

Beheben Sie Domänentrennungsfehler

Wenn Probleme bei der Domänentrennung auftreten, überprüfen Sie diese Liste der Lösungen.

Fehler oder Symptom	Lösung
Eine sys_ID der Domäne verweist auf eine nicht vorhandene Domäne	Dieser Fehler tritt auf, wenn ein Datensatz, z. B. ein Anwender- oder Aufgabendatensatz, einen hat `sys_Domain` Spaltenwert, dessen `sys_ID` Ist in der aktuellen Domänentabelle nicht vorhanden. Die Domäne `sys_ID` Könnte versehentlich gelöscht worden sein, oder es könnte auf eine vorherige Domänentabelle verweisen, wenn Sie die Domänentabelle geändert haben. Um den Fehler zu beheben, öffnen Sie eine Liste für die Tabelle, die den Fehler enthält, und filtern Sie nach dem ungültigen `sys_Domain` Wert. Geben Sie dann entweder manuell die richtige ein `sys_Domain` Werten Sie sie aus, oder entfernen Sie sie. **Hinweis:** Sie können eine ungültige Domäne haben `sys_IDs` In einer beliebigen Tabelle, die auf die Domänentabelle verweist. Beispielsweise können ungültige Domänen-IDs in der Anwendersichtbarkeitsdomäne auftreten `[sys_user_Visibility]` , Gruppensichtbarkeitsdomäne `[sys_user_Group_Visibility]` , Und enthaltene Domäne `[Domain_contains]` Tabellen.
Ein Domänenpfad oder eine Domänennummer sys_ID verweist auf die falsche Domäne	Dieser Fehler tritt auf, wenn eine Domänennummer- oder Domänenpfadabfrage nicht mit dem tatsächlichen Domänennamen synchronisiert ist. Dieser Fehler kann bei Domänennummern auftreten, wenn das Hinzufügen von Domänen eine Umnummerierung erfordert oder während der Konvertierung von Domänennummern in Domänenpfade. Um den Fehler zu beheben, überprüfen Sie die Ergebnisse in Domain Separation Center. Wenn der Fehler weiterhin besteht, können Sie den Wert für manuell bearbeiten `sys_Domain_path` Oder `sys_Domain_number` Spalten, die auf die richtige Domäne verweisen.
Die Domänenstrukturstruktur ist beschädigt	Dieser Fehler tritt auf, wenn eine Reihe von Domänen Beziehungen enthält, die eine Endlosschleife zwischen Domänen erstellen. Um den Fehler zu beheben, öffnen Sie eine Liste für die Domänentabelle, und bearbeiten Sie die Domäne mit Werten manuell, um keine Schleife zu bilden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivierungsdienstprogramm zur Domänentrennung nach der Produktion

Das Aktivierungsdienstprogramm für Domänentrennung nach der Produktion unterstützt die Aktivierung der Domänentrennung in einer Live-Umgebung.

Plugin „Domänentrennung aktivieren“ nach der Produktion

Das Plugin „Aktivierungsdienstprogramm für Domain Separation nach der Produktion“ (com.Glide.Domain.activation_Utility) vereinfacht die Erstellung einer domänengetrennten Umgebung in einer Live-Umgebung nach der Produktion. Kunden möchten möglicherweise die Domänentrennung in Nachproduktionsumgebungen aktivieren, um die Vorteile von besser nutzen zu können ServiceNow AI Platform Fähigkeiten. Das Dienstprogramm bietet ein schrittweises geführtes Setup zum Erstellen von Domänen.

Hinweis: Das Ausfüllen von Domänendatensätzen in domänengetrennten Tabellen erfordert Ausfallzeiten oder eingeschränkten Zugriff auf die Instanz.

Was das Aktivierungsdienstprogramm tut

- Bietet ein schrittweises geführtes Setup zum Erstellen von Domänen.
- Führt einen Hintergrundauftrag aus, um die Installation der Domänentrennung zu verarbeiten, wobei sowohl die Eigenschaften „Prozess“ als auch „Datentrennung“ deaktiviert sind.
- Behält Prozessdatensätze bei, die für die Zieldomäne (erste) sichtbar sind
- Erkennt, identifiziert und protokolliert Fehler während des Domänenerstellungsprozesses
- Zeigt Lösungen für häufige Fehler an
- Protokolliert alle während des Setup-Prozesses ausgeführten Aktionen zu Audit-Zwecken
- Generiert eine detaillierte Zusammenfassung, einschließlich aller durchgeführten Aktionen, erstellten Domänen und Änderungen am System

Verwaltung Von Domänenaufträgen

Warteschlange mehrere Domänentrennungen werden sequenziell in einem einzelnen Hintergrundauftrag mithilfe des Domänenauftrags-Managers aktualisiert.

Wenn ein Domänendatensatz geändert wird, z. B. Reparenting oder eine Änderung der Hierarchie, wird standardmäßig ein Auftrag ausgeführt, um alle Datensätze in domänengetrennten Tabellen zu korrigieren. Sie können steuern, wann dieses Verhalten mit auftritt **Domänenauftragsmanager** Und überwachen Sie den laufenden Auftragsfortschritt mit **Zeigen Sie Den Auftragsfortschritt An** Schaltfläche.

Verwenden Sie **Domänenauftragsmanager** Um Domänenaufträge anzuhalten, stellen Sie mehrere Domänentabellenänderungen in die Warteschlange, und lösen Sie den Auftrag in der Warteschlange aus, wenn er mit allen Änderungen bereit ist.

Fortschritt des Domänenauftrags

Bezeichnung	Beschreibung
Auftragsart	Der aktuelle Auftragstyp
Status	Der Status des Auftrags, siehe **Auftragsstatus** Im Auftragsmanager für weitere Informationen.
Fortschritt	Laufender Auftragsfortschritt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänenauftragsmanager

Feld	Beschreibung
Auftragsart	Supportauftragstypen: Hierarchieänderung
Auftragsstatus	• Aktiv • Angehalten **Hinweis:** Standardmäßig werden angehaltene Aufträge in 1 Stunde automatisch fortgesetzt. Aktivieren Sie diese Option, um dies zu deaktivieren und den Auftrag später manuell zu aktivieren

Nach Domäne löschen

Bereinigen Sie inaktive Domänen auf Blattebene in der Domänenhierarchie mit einem kontrollierten und automatisierten Tool.

Vorbereitungen

Erforderliche Rolle: Domänentrennungsadministrator

Prozedur

1. **Alle** > **Domänenadministrator** > **Bereinigungswarteschlange**
2. Wählen Sie aus **Bereiten Sie Sich Auf Die Bereinigung Vor** Schaltfläche.
3. Wählen Sie die Domänen aus, die in die Warteschlange zum Löschen gestellt werden sollen.
   Die Liste zeigt alle verfügbaren inaktiven Domänen auf Blattebene, die zum Löschen ausgewählt werden können.
4. Wählen Sie **Speichern**.
   Ausgewählte Domänen spiegeln jetzt ein wider **Bereit für Bereitstellung** status in der Tabelle. Domänen müssen bereitgestellt werden, bevor sie in die Warteschlange zum Löschen gestellt werden.
5. Wählen Sie aus **Wechseln Sie zu Bereitstellung** Schaltfläche.
6. Geben Sie die Anzahl der Tage ein, die die bereitgestellte Domäne vor dem Löschen beibehalten soll.

   Hinweis: Sobald die Domäne in verschoben wird **Bereitgestellt und Löschung geplant** status, kann nicht aus der Bereinigungswarteschlange entfernt werden.

Bevor eine Domäne gelöscht wird, können Domänenadministratoren auf den Datenabdruck der Domäne zugreifen.

7. Wählen Sie aus **Vorschau Der Domänendaten Anzeigen** Schaltfläche.
   Ein Auftrag wird in die Warteschlange gestellt, um die inaktiven Domänen nach Metadaten zu durchsuchen.
8. Nachdem der Auftrag ausgeführt wurde, wählen Sie einen Domänendatensatz aus, um seine Metadaten anzuzeigen.

Domain Separation Center

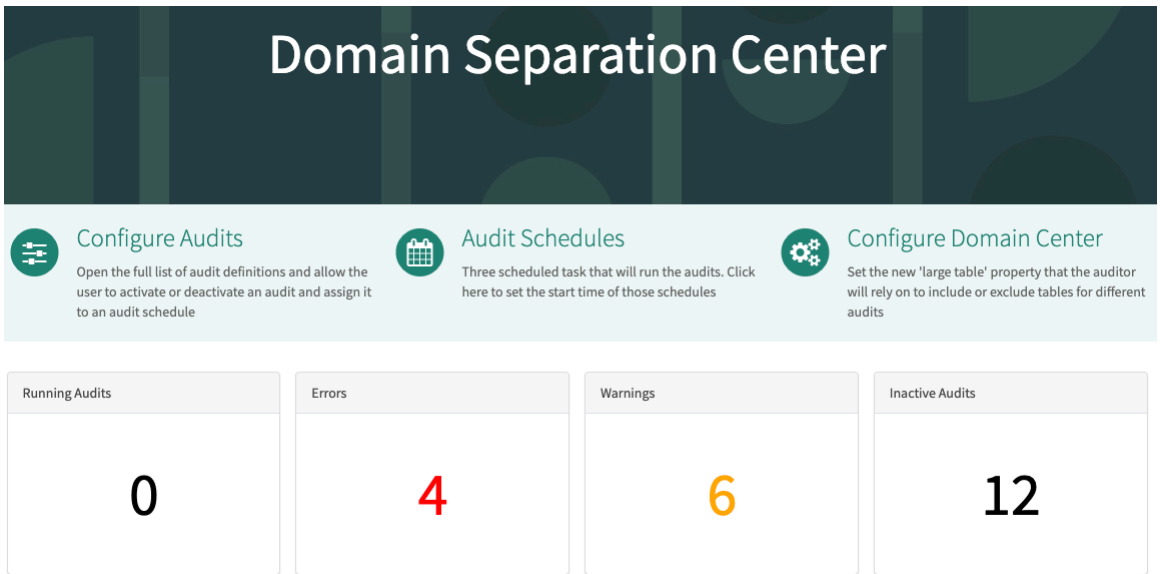
Auditieren Sie Ihre Domänen regelmäßig, um Probleme aufzudecken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht

Das Domain Separation Center ist ein Dashboard, in dem Sie Audits für alle in Ihrer Tabelle „Domain_Audit_Definition“ gespeicherten Domänen planen und konfigurieren können. Mit dem Dashboard können Sie Audit-Ergebnisse überprüfen und sich näher mit Domänenfehlern und Warnungen befassen. Das Domain Separation Center-Dashboard finden Sie unter <ServiceNow-instance-name>/Domaincenter .

Das Domain Separation Center bietet viele Audits. Sie können keine eigenen erstellen. Sie können jedoch konfigurieren, wie oft sie ausgeführt werden. Audits werden für alle Domänen ausgeführt, die in der Tabelle „Domain_Audit_Definition“ gespeichert sind.



Konfigurieren Sie Audits

Sie können konfigurieren, ob ein Audit aktiv ist und wie häufig es ausgeführt wird.

1. Wählen Sie im Domain Separation Center die Option aus **Konfigurieren Sie Audits** .

   Die **Konfigurieren Sie Audits** Seite wird angezeigt.

2. Konfigurieren Sie jedes Audit, das Sie aktiv sein möchten. Audits sind standardmäßig inaktiv.
   a. Wählen Sie ein Audit aus.
   b. Wählen Sie aus **Aktiv** Feld zum Aktivieren des Audits.
   c. Geben Sie an, wie oft das Audit in ausgeführt wird **Häufigkeit** Feld.

      Das Domain Separation Center führt alle Audits mit derselben Häufigkeit gleichzeitig aus. Nicht auswählen **Täglich** Für Audits werden in großen Tabellen ausgeführt.

   d. Wiederholen Sie diese Schritte für jedes Audit, das Sie aktivieren möchten.
3. Wählen Sie **Speichern**.

Zeitpläne für Audit

Konfigurieren Sie ein oder mehrere Audits für die tägliche, wöchentliche oder monatliche Ausführung. Der Planer gibt an, an welchen Tagen und zu welchen Zeiten diese Audits ausgeführt werden sollen. Alle Audits mit derselben Zeitplanungshäufigkeit werden beim Konfigurieren sequenziell gestartet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

1. Wählen Sie im Domain Separation Center die Option aus **Audit-Zeitpläne** .

   Die **Audit-Zeitplan** Seite wird angezeigt.

2. Konfigurieren Sie die Audit-Zeitpläne.
   a. Wählen Sie einen Zeitplannamen aus.
   b. Geben Sie die Tageszeit für die Ausführung des Audits an.

      Zeiteinheiten werden mit der 24-Stunden-Uhr gemessen, d. h. 14 entspricht 14 14 Uhr.

   c. Wählen Sie für wöchentliche Zeitpläne den Wochentag aus, an dem das Audit ausgeführt werden soll, wobei 1 Sonntag ist.
   d. Wählen Sie für monatliche Zeitpläne den Tag des Monats aus, an dem das Audit ausgeführt werden soll.
   e. Wiederholen Sie den Vorgang für die anderen Zeitpläne.
3. Wählen Sie Aus **Speichern** Zum Speichern der Konfigurationsänderungen.
4. Wählen Sie Aus **Jetzt Ausführen** Um alle Audits auszuführen, die für die Ausführung geplant sind, mit der oben im rechten Bereich angezeigten Häufigkeit, z. B. wenn der Bereichstitel lautet, **Domänenaudit-Zeitplan: Täglich** , Alle täglich ausgeführten Audits werden ausgeführt.

Um den Status eines laufenden Audits anzuzeigen, wählen Sie im Domain Separation Center die Zahl aus **Audits Werden Ausgeführt** Feld.

Führen Sie Audits sofort aus

Audits werden normalerweise wie geplant ausgeführt. Sie können jedoch alle Audits für den Befehl ausführen.

1. Wählen Sie im Domain Separation Center die Option aus **Audit-Zeitpläne** .

   Die **Audit-Zeitplan** Seite wird angezeigt.

2. Wählen Sie den Namen des Audit-Zeitplans aus, den Sie ausführen möchten, z. B. täglich, wöchentlich oder monatlich.
3. Wählen Sie **Jetzt ausführen**.

Um den Status eines laufenden Audits anzuzeigen, wählen Sie im Domain Separation Center die Zahl aus **Audits Werden Ausgeführt** Feld.

Konfigurieren Sie das Domain Separation Center

1. Wählen Sie im Domain Separation Center die Option aus **Konfigurieren Sie Das Domänenzentrum** .
2. Auf der **Konfigurieren Sie Das Domänenzentrum** Seite, für **Aktiviert die Detaildomänenprotokollierung** , Wählen Sie aus **Ja** Zum Speichern detaillierter Protokolle, die bei der Diagnose domänenbezogener Probleme helfen. Detaillierte Protokollierung kann zu Leistungsproblemen führen.

   Diese Protokolle beziehen sich auf serverseitige Protokolle in der Tabelle „syslog_Domain“. Informationen zum Anzeigen der Protokolle finden Sie unter Audits mit Warnungen und Fehlern anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie im Slushbucket alle Ihre großen Tabellen aus, und verschieben Sie sie in **Ausgewählt** Spalte.

   Tägliche Audits sollten nicht für große Tabellen ausgeführt werden. Ausgegraute Tabellennamen in **Ausgewählt** Spalte ist groß und kann nicht in verschoben werden **Verfügbar** Spalte.

4. Wählen Sie **Aktualisieren**.

Zeigen Sie Audits mit Warnungen und Fehlern an

Im Dashboard **Fehler** Und **Warnungen** Geben Sie detaillierte Informationen zu Audits an, bei denen Probleme aufgetreten sind. Protokolle im Zusammenhang mit der Domänentrennung befinden sich auf Ihrem Server in der Tabelle „syslog_Domain“.

1. Wählen Sie im Domain Separation Center die Nummer aus **Fehler** Oder **Warnungen** Feld.

   Die **Fehler** Oder **Warnungen** Seitenanzeigen bzw.

2. Wählen Sie eines der Audits in der Liste aus.

   Auf der Seite werden detaillierte Informationen zu Problemen mit dem von Ihnen ausgewählten Audit angezeigt. Die Nachrichten in **Audit-Ergebnisdetails** Informationen zu Tabellen-Audits, bei denen Fehler oder Warnungen festgestellt wurden, finden Sie in den Werten in der Tabelle „syslog_Domain“.

3. So zeigen Sie die Protokolle auf dem Server an, die Informationen zu Warnungs- oder Fehler-Audits enthalten:
   a. Kopieren Sie **Detail-ID** Wert im linken Bereich einer Warnung oder eines Fehlers.
   b. Geben Sie im Filternavigator von HI ein *`Syslog_Domain.do`* .

      Die Seite Domänenprotokoll wird angezeigt.

   c. In **Quelle** Suchfeld eingeben `=<Detail-ID>` (Kein Leerzeichen nach dem Gleichheitszeichen), z. B. =f6a00fd29a85b300a9503a81b9169678.

      Auf der Seite „Domänenprotokoll“ werden nur die Protokolle angezeigt, die sich auf das Audit mit der von Ihnen angegebenen Detail-ID beziehen. Jede Zeile in der Tabelle gibt einen anderen Datensatz an, in dem das Audit Probleme gefunden hat. Beachten Sie, dass **Nachricht** Das Feld auf dieser Seite stimmt mit den Werten überein, die im Domain Service Center angezeigt werden **Nachricht** Spalte. Das Format der Nachricht stimmt mit dem Audit-Typ überein.

4. Wählen Sie Folgendes aus:
   - **Audit Erneut Ausführen** – Führen Sie ein Audit erneut aus, um festzustellen, ob noch eine Warnung oder ein Fehler auftritt.
   - **Deaktivieren Sie Audit** – Deaktivieren Sie ein Audit.
   - **Details Kopieren** – Kopiert Audit-Details in die Zwischenablage.

Zeigen Sie laufende und ausstehende Audits an

Aktive Audits werden regelmäßig ausgeführt oder in der Warteschlange ausgeführt, wie geplant. Sie können ihren Status während der Ausführung anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wählen Sie die Nummer im aus **Audits Werden Ausgeführt** Feld zum Anzeigen von Audits, die derzeit ausgeführt werden oder deren Ausführung aussteht.

   Die **Audits Werden Ausgeführt** Seite wird angezeigt.

2. Wählen Sie ein Audit aus, um weitere Informationen zu erhalten.

Zeigen Sie inaktive Audits an

1. Wählen Sie die Nummer im aus **Inaktive Audits** Feld.

   Die **Inaktive Audits** Auf der Seite werden alle Audits angezeigt, die derzeit deaktiviert sind.

2. Wählen Sie eines der Audits aus, um weitere Informationen anzuzeigen.
3. Um ein Audit zu aktivieren, wählen Sie aus **Aktiv** Und verwenden Sie **Häufigkeit** Feld, um anzugeben, wie oft das Audit ausgeführt wird.
4. Wählen Sie **Aktualisieren**.

Konfigurieren Sie das Domain Separation Center

Geben Sie an, welche Tabellen in Domänen groß sind und ob Sie eine detaillierte Protokollierung wünschen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können Audits so planen, dass sie täglich, wöchentlich oder monatlich ausgeführt werden. Audits, die für große Tabellen ausgeführt werden, können eine beträchtliche Zeit in Anspruch nehmen. Aus diesem Grund sollten Sie vermeiden, tägliche Audits für große Tabellen auszuführen. Das Starten eines neuen Audits an einem Audit, dessen Ausführung länger als einen Tag dauert, kann negative Konsequenzen haben.

Eine detaillierte Protokollierung kann bessere Einblicke in die während Audits gefundenen Probleme bieten, kann jedoch zu Leistungsproblemen führen.

Prozedur

1. Wählen Sie im Domain Separation Center die Option aus **Konfigurieren Sie Das Domänenzentrum** . Die Seite Domain Center konfigurieren wird angezeigt.
2. Wählen Sie Aus **Ja** Für **Aktiviert die Detaildomänenprotokollierung** , Um detaillierte Protokolle zu speichern, die bei der Diagnose domänenbezogener Probleme helfen.
   Diese Protokolle beziehen sich auf serverseitige Protokolle in der Tabelle „Domänenprotokoll“ [syslog_Domain]. Informationen zum Anzeigen der Protokolle finden Sie im Abschnitt Audits mit Warnungen und Fehlern anzeigen.
3. Verschieben Sie in der Liste alle Ihre großen Tabellen in **Ausgewählt** Spalte.
   Tägliche Audits sollten nicht für große Tabellen ausgeführt werden. Ausgegraute Tabellennamen in **Ausgewählt** Spalte ist groß und kann nicht in verschoben werden **Verfügbar** Spalte.
4. Wählen Sie **Aktualisieren**.
5. Wenn Sie große Tabellen haben, die nie geprüft werden sollen, legen Sie fest `com.glide.domain.audit.big_tables.additional`Systemeigenschaft für eine kommagetrennte Liste dieser Tabellennamen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Audits

Konfigurieren Sie, ob ein Audit aktiv ist und wie häufig es ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Klicken Sie im Domain Separation Center auf **Konfigurieren Sie Audits** .
   T wird angezeigt.
2. Konfigurieren Sie auf der Seite Audits konfigurieren jedes Audit, das Sie aktiv sein möchten.
   Audits sind standardmäßig inaktiv.
   a. Klicken Sie auf ein Audit.
   b. Klicken Sie auf **Aktiv** Kontrollkästchen zum Aktivieren des Audits.
   c. Geben Sie an, wie oft das Audit in ausgeführt wird **Häufigkeit** Feld.
   Das Domain Separation Center führt alle Audits mit derselben Häufigkeit gleichzeitig aus. Nicht auswählen **Täglich** Für Audits werden in großen Tabellen ausgeführt.
   d. Wiederholen Sie die Schritte a–c für jedes Audit, das Sie aktivieren möchten.
3. Klicken Sie auf **Speichern**.

Audits planen

Geben Sie die Uhrzeit und den Tag an, an dem Audits ausgeführt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie Mindestens ein Audit wurde konfiguriert Zur täglichen, wöchentlichen oder monatlichen Ausführung. Der Planer gibt an, an welchen Tagen und zu welchen Zeiten diese Audits ausgeführt werden sollen. Alle Audits mit derselben Zeitplanungshäufigkeit werden sequenziell ab dem Zeitpunkt der Konfiguration ausgeführt.

Prozedur

1. Klicken Sie im Domain Separation Center auf **Audit-Zeitpläne** .
   Die Seite Audit Schedule (Audit-Zeitplan) wird angezeigt.
2. Konfigurieren Sie die Audit-Zeitpläne.
   a. Klicken Sie auf einen Zeitplannamen.
   b. Geben Sie die Tageszeit für die Ausführung des Audits an.
   Zeiteinheiten verwenden die 24-Stunden-Uhr (d. h. 14 entspricht 14 Uhr).
   c. Wählen Sie für wöchentliche Zeitpläne den Wochentag aus, an dem das Audit ausgeführt werden soll, wobei 1 Sonntag ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie für monatliche Zeitpläne den Tag des Monats aus, an dem das Audit ausgeführt werden soll.

e. Wiederholen Sie den Vorgang für die anderen Zeitpläne.

3. Klicken Sie Auf **Speichern** Zum Speichern der Konfigurationsänderungen.
4. **Wahlweise:** Klicken Sie Auf **Jetzt Ausführen** Zum Ausführen aller Audits, die für die Ausführung geplant sind, mit der Häufigkeit, die oben im rechten Bereich angezeigt wird.
   Beispiel: Wenn der Bereichstitel lautet **Domänenaudit-Zeitplan: Täglich** , **Jetzt Ausführen** Führt sofort alle Audits aus, deren tägliche Ausführung geplant ist.

Nächste Maßnahme
Um den Status eines laufenden Audits anzuzeigen, klicken Sie im Domain Separation Center auf die Zahl im **Audits Werden Ausgeführt** Feld.

Führen Sie Audits sofort aus

Audits werden normalerweise wie geplant ausgeführt. Sie können jedoch alle Audits auf Befehl ausführen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Sie können einzelne Audits nicht manuell ausführen. Sie können jedoch alle Audits ausführen, die mit derselben Zeitplanungshäufigkeit konfiguriert sind. Sie können beispielsweise alle Audits ausführen, die so konfiguriert sind, dass sie täglich ausgeführt werden.

Prozedur

1. Klicken Sie im Domain Separation Center auf **Audit-Zeitpläne** .
2. Klicken Sie auf den Namen des Audit-Zeitplans, den Sie ausführen möchten (z. B. täglich, wöchentlich oder monatlich).
3. Klicken Sie auf **Jetzt ausführen**.

Nächste Maßnahme
Um den Status eines laufenden Audits anzuzeigen, klicken Sie im Domain Separation Center auf die Zahl im **Audits Werden Ausgeführt** Feld.

Zeigen Sie Audits mit Warnungen und Fehlern an

Das Domain Separation Center bietet Details zu Audit-Fehlern und -Warnungen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Im Domain Separation Center-Dashboard **Fehler** Und **Warnungen** Geben Sie detaillierte Informationen zu Audits an, bei denen Probleme aufgetreten sind. Protokolle im Zusammenhang mit der Domänentrennung befinden sich auf Ihrem Server in der Tabelle „syslog_Domain“. Fehler sind Probleme, die sofortige Aufmerksamkeit erfordern. Warnungen führen nicht zu Fehlern, enthalten aber Best Practices, z. B. dass der Domänenname nicht zu lang wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie im Domain Separation Center auf die Zahl im **Fehler** Oder **Warnungen** Feld.
   Die **Fehler** Oder **Warnungen** Seite wird angezeigt.
2. Klicken Sie auf eines der Audits in der Liste.
   Auf der Seite werden detaillierte Informationen zu Problemen mit dem von Ihnen ausgewählten Audit angezeigt. Die Nachrichten in **Audit-Ergebnisdetails** Informationen zu Tabellen-Audits, bei denen Fehler oder Warnungen festgestellt wurden, finden Sie in den Werten in der Tabelle „syslog_Domain“ auf dem Server.
3. So zeigen Sie die Protokolle auf dem Server an, die Informationen zu Warnungs- oder Fehler-Audits enthalten:

   a. Kopieren Sie **Detail-ID** Wert im linken Bereich einer Warnung oder eines Fehlers.

   b. In der Instanz, die das Domain Separation Center ausführt, in **Filternavigator** , Eingabetaste `Syslog_Domain.list` .
   Die Seite Domänenprotokoll wird angezeigt.

   c. Im Suchfeld von **Quelle** Spalte eingeben `=<Detail-ID>` (Kein Leerzeichen nach dem Gleichheitszeichen), z. B. `=f6a00fd29a85b300a9503a81b9169678` .
   Auf der Seite „Domänenprotokoll“ werden nur die Protokolle angezeigt, die sich auf das Audit mit der von Ihnen angegebenen Detail-ID beziehen. Jede Zeile in der Tabelle gibt einen anderen Datensatz an, in dem das Audit Probleme gefunden hat. Beachten Sie, dass **Nachricht** Das Feld auf dieser Seite stimmt mit den in angezeigten Werten überein **Nachricht** Spalte des Domänen-Service Centers. Die in der Nachricht enthaltenen Informationen stimmen mit dem Audit-Typ überein.

4. **Wahlweise:** Wählen Sie eine der folgenden Optionen aus:
   - **Audit Erneut Ausführen** – Führen Sie ein Audit erneut aus, um festzustellen, ob noch eine Warnung oder ein Fehler auftritt.
   - **Deaktivieren Sie Audit** – Deaktivieren Sie ein Audit.
   - **Details Kopieren** – Audit-Details in die Zwischenablage kopieren.

Zeigen Sie laufende und ausstehende Ergebnisse an

Sie können laufende und ausstehende Audits anzeigen, um ihren Status anzuzeigen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Aktive Audits werden regelmäßig ausgeführt oder in der Warteschlange ausgeführt, wie geplant. Sie können ihren Status während der Ausführung anzeigen.

Prozedur

1. Klicken Sie auf die Zahl im **Audits Werden Ausgeführt** Feld zum Anzeigen von Audits, die derzeit ausgeführt werden oder deren Ausführung aussteht.
   Die Seite „laufende Audits“ wird angezeigt.
2. Klicken Sie auf ein laufendes oder ausstehendes Audit, um Informationen dazu anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie inaktive Audits an

Sie können alle inaktiven Audits an einem Ort anzeigen und optional aktivieren.

Vorbereitungen
Erforderliche Rolle: Administrator

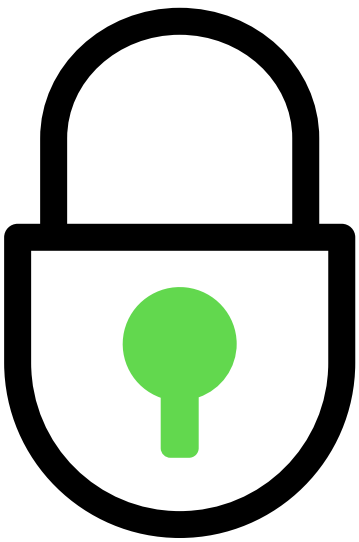
Prozedur

1. Klicken Sie auf die Zahl im **Inaktive Audits** Feld.
   Auf der Seite „inaktive Audits“ werden alle Audits angezeigt, die derzeit deaktiviert sind.
2. Klicken Sie auf eines der Audits, um weitere Informationen anzuzeigen.
3. **Wahlweise:** Aktivieren Sie ein Audit, indem Sie auf klicken **Aktiv** Feld und gibt an, wie oft das Audit in ausgeführt wird **Häufigkeit** Feld.
4. Klicken Sie auf **Aktualisieren**.

Authentifizierung

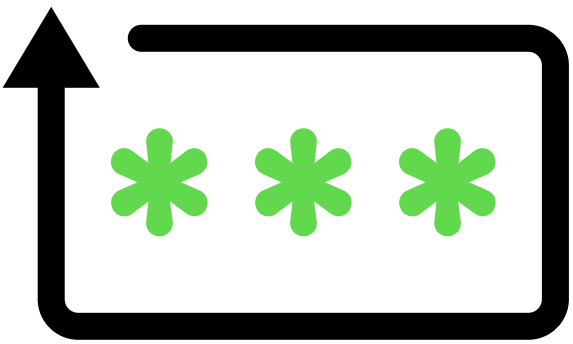
ServiceNow Die Authentifizierung von validiert die Identität eines Anwenders, der auf eine Instanz zugreift, und autorisiert den Anwender dann für Funktionen, die der Rolle oder Auftragsfunktion des Anwenders entsprechen.

Erste Schritte



Single Sign-on (SSO) für mehrere Anbieter

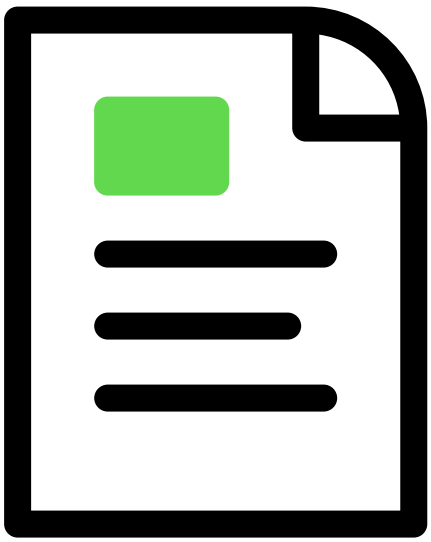
Anwendername und Passwort, die in Identitätsanbietern konfiguriert sind, die über einen übereinstimmenden Anwenderaccount in der Datenbank verfügen.



OAuth eingehend und ausgehend

Die OAuth-basierte Authentifizierung validiert die Identität des Clients, der versucht, mithilfe eines Authentifizierungsprotokolls eine Vertrauensbasis für das System herzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



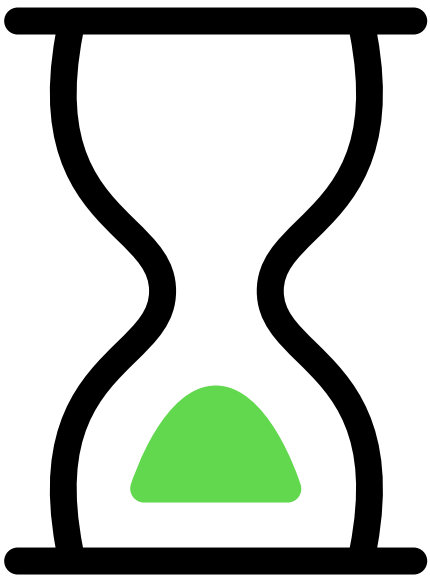
API-Zugriffsrichtlinie

Die API-Zugriffsrichtlinie definiert die Berechtigungen und den Zugriff auf eine API, die über eine Richtlinie gesteuert werden können.



Digest-Token-Authentifizierung

Anwendername und Geheimnis in der Tabelle führen Sie einen anwenderspezifischen Hash-Vorgang aus, z. B. SHA1, SHA 256 oder MD5. Dieser Wert muss als Teil des URL-Suffixes angehängt werden, das für den Abfrageparameter funktioniert.



Zeitlich begrenzte Authentifizierung



Multifaktor-Authentifizierung (MFA)

Mit MFA können Sie die zweite Authentifizierungsebene bereitstellen, die die Verwendung von Passcode aus einer Authentifizierungs-App, einem Hardwareschlüssel, einem biometrischen Authentifikator, einer SMS oder einer E-Mail umfasst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die linkbasierte Authentifizierung auf dem

ServiceNow

Instanz. Der konfigurierte Link kann für den Anwender per E-Mail oder SMS freigegeben werden, und der Anwender kann diese Links verwenden, um sich bei der Instanz anzumelden.



Zertifikatbasierte Authentifizierung

Eindeutige PEM-codierte Zertifikate, die Anwendern anstelle von Anwendername und Passwort für die zertifikatbasierte Authentifizierung zugeordnet sind.



Selbstregistrierung

Verwenden Sie die Selbstregistrierung externer Anwender, um ein großes Volumen externer Anwender in Ihrer Instanz zu integrieren.



LDAP

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können mehrere verschiedene Methoden zur Authentifizierung von Anwendern verwenden. Anwenderanmeldeinformationen werden mit verschiedenen gespeicherten Anmeldeinformationen für jede Methode abgeglichen.

Hinweis:

- Die Okta SSO-Plugin ist veraltet.
- Weitere Informationen zu den Sicherheitseigenschaften, die sich auf die Autorisierungsverarbeitung auswirken, finden Sie unter Zugriffssteuerung In Instanzsicherheitshärtungseinstellungen.
- Sie können die SAML- und Digest-Authentifizierung über die SSO-Anwendung mehrerer Anbieter verwenden.

Adaptive Authentifizierung

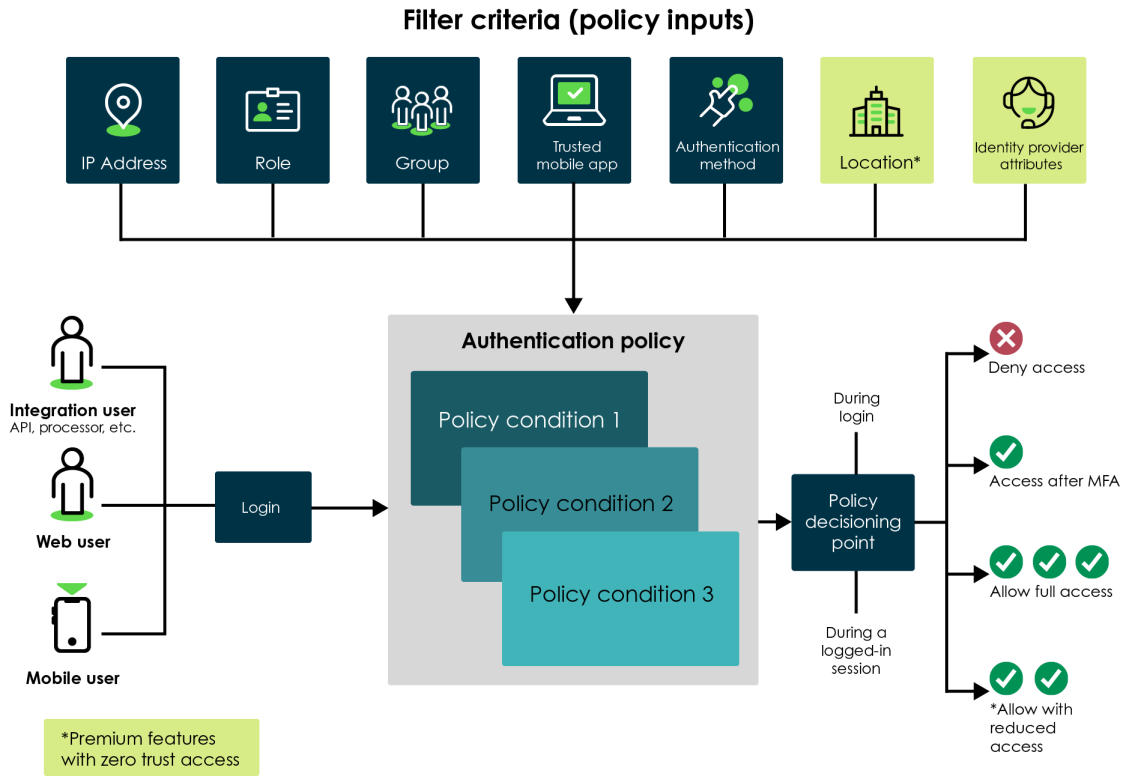
Verwenden Sie das Richtlinien-Framework für adaptive Authentifizierung, um kontextbezogene Authentifizierungssteuerungen für die richtigen Anwender zur richtigen Zeit durchzusetzen. Die adaptive Authentifizierung verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten und dann den Zugriff auf Ihre Instanz basierend auf den angegebenen Richtlinienbedingungen zu verweigern oder zu erlauben.

Verwenden Sie Richtlinien und Kontexte für die adaptive Authentifizierung, um den Zugriff auf Ihre Instanz für Anwender und APIs basierend auf Kriterien wie IP-Adresse, Anwenderrolle und Anwendergruppe zu beschränken. Sie können die integrierten Authentifizierungsrichtlinien entsprechend Ihren Sicherheitsanforderungen konfigurieren.

Beispielsweise kann ein -Administrator konfigurieren *`Allow Access Policy`*Erlaubt Anmeldungen nur von Anwendern innerhalb eines vertrauenswürdigen Bereichs von IP-Adressen, die Mitglieder einer bestimmten Rolle sind. Wenn zugewiesen an *`Post-authentication context`*, Die Zugriffsrichtlinie verweigert den Zugriff von nicht vertrauenswürdigen IP-Adressen.

Um eine anwenderdefinierte Nachricht in der Sprache Ihrer Instanz festzulegen, müssen Sie das Schlüssel-Wert-Paar in hinzufügen sys_ui_message.list Und aktualisieren sys_ui_message Datensatz. Wenn Sie sich mit einem falschen Passwort anmelden, wird die anwenderdefinierte Nachricht in der bevorzugten Sprache angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Komponenten der adaptiven Authentifizierung

Authentifizierungsrichtlinien

Authentifizierungsrichtlinien bewerten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen und erlauben oder verweigern den Zugriff je nach Ausgabe der Auswertung der Richtlinienbedingungen. Beispielsweise ist der Zugriff nur zulässig, wenn alle Richtlinienbedingungen in angegeben sind **Zugriffsrichtlinie Zulassen** Auswertung auf „wahr“.

Authentifizierungsrichtlinien verwenden Informationen, die durch Filterkriterien bereitgestellt werden, um sie mit den Bedingungen der Richtlinie zu vergleichen, um zu bestimmen, ob Zugriff auf die Instanz gewährt werden soll. Beispielsweise stellt ein Filterkriterium die IP-Adresse eines Anwenders bereit, und eine Richtlinienbedingung bestimmt, ob diese Adresse innerhalb des spezifischen Bereichs liegt, bevor Zugriff gewährt wird. Weitere Informationen zu Authentifizierungsrichtlinien finden Sie in Authentifizierungsrichtlinien.

Kontexte der Authentifizierungsrichtlinie

Authentifizierungsrichtlinienkontexte definieren, wie und wann Richtlinien während des Anmeldevorgangs durchgesetzt werden. Der Kontext vor der Authentifizierung wird ausgeführt, bevor dem Anwender ein Anmeldebildschirm angezeigt wird. Der Kontext nach der Authentifizierung wird ausgeführt, nachdem der Anwender seine Anmeldeinformationen eingegeben hat. Um eine Richtlinie zu verwenden, muss sie einem Richtlinienkontext zugewiesen werden. Weitere Informationen zu diesen Kontexten finden Sie unter Kontexte der Authentifizierungsrichtlinie.

Filterkriterien

Filterkriterien (auch als Richtlinieneingaben bezeichnet) werden als Eingaben für Richtlinienbedingungen verwendet. Richtlinienbedingungen verwenden diese Eingaben, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Anforderungen von Authentifizierungsanforderungen zu verifizieren und zu erfüllen. Diese Eingaben enthalten Informationen wie Anwenderrolle, IP-Bereich und Identitätsanbieter. Weitere Informationen zu Filterkriterien finden Sie unter Filterkriterien.

Authentifizierungseigenschaften

Verwenden Sie Authentifizierungseigenschaften, um zu steuern, ob die adaptive Authentifizierung in Ihrer Instanz aktiv ist. Sie können auch Eigenschaften verwenden, um das Debugging zu aktivieren und zu definieren, welche Messaging-Anwender sehen, wenn der Zugriff blockiert wird. Weitere Informationen zu diesen Eigenschaften finden Sie unter Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung.

REST API-Zugriffsrichtlinien

Sie können die Filterkriterien des adaptiven Authentifizierungs-Frameworks verwenden, um den Zugriff auf eingehend zu beschränken ServiceNow REST-APIs. Weitere Informationen finden Sie unter REST API-Zugriffsrichtlinien.

Domänentrennung und adaptive Authentifizierung

Die adaptive Authentifizierung wird auf domänengetrennten Instanzen auf der Bedingungsebene der Authentifizierungsrichtlinie unterstützt. Richtlinienbedingungen wirken sich auf die Domäne in den Datensätzen aus **Domäne** Feld [sys_Domain]. Richtlinienbedingungen in der globalen Domäne wirken sich auf alle Domänen aus.

Adaptive Authentifizierungsereignisse

Sie können die Tabelle „Ereignisse der adaptiven Authentifizierung“ verwenden, um über die Ereignisse zu erfahren, die spezifisch für die Funktion der adaptiven Authentifizierung aufgetreten sind. Weitere Informationen finden Sie unter Adaptive Authentifizierungsereignisse.

Aktivieren Adaptive Authentifizierung

Sie können aktivieren Adaptive Authentifizierung Plugin (Com.snc.adaptive_authentication) Für Adaptive Authentifizierung Wenn Sie die Administratorrolle innehaben.

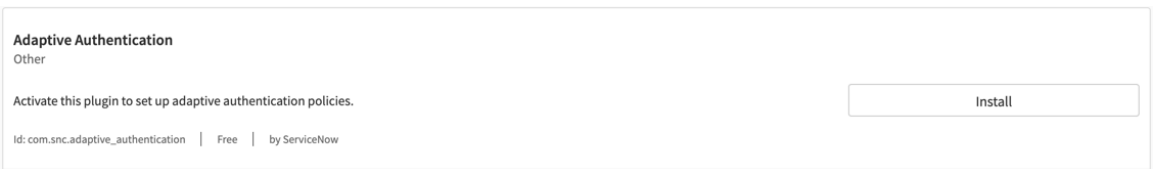
Vorbereitungen

Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach **Adaptive Authentifizierung** (Com.snc.adaptive_authentication) Plugin mithilfe der Filterkriterien und der Suchleiste.



   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Nächste Maßnahme

Konfigurieren Sie Ihre Authentifizierungsrichtlinien, um kontextbezogene Authentifizierungssteuerungen für Ihre Instanz zu erzwingen.

Sobald Ihre Richtlinien konfiguriert sind. Aktivieren Sie die adaptive Authentifizierung mit **Aktivieren Sie Die Authentifizierungsrichtlinie** Richtlinie. Weitere Informationen zu den Eigenschaften der adaptiven Authentifizierung finden Sie unter Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung.

Filterkriterien

Filterkriterien (auch als Richtlinieneingaben bezeichnet) werden als Eingaben für Richtlinienbedingungen verwendet, um die Anforderungen einer Authentifizierungsanforderung zu verifizieren und zu erfüllen.

Verwenden Sie Filterkriterien, um Richtlinien zur Informationsauthentifizierung bereitzustellen, z. B. die IP-Adresse, Rollen oder Gruppen eines Anwenders. Fügen Sie diese Kriterien in hinzu **Richtlinienbedingungen** Abschnitt Ihrer Richtlinien.

Bei der adaptiven Authentifizierung werden sieben Arten von Filterkriterien verwendet. Ihre Authentifizierungsrichtlinien können eines oder mehrere dieser Kriterien verwenden, um Authentifizierungsanforderungen auszuwerten.

Hinweis: Standortfilter und Identitätsanbieter-Filter sind mit der Zero Trust-Zugriffsfunktion verfügbar. Weitere Informationen finden Sie unter Zero Trust Access (ZTA).

Filterkriterientypen

Typ	Beschreibung
IP-Filterkriterien	Verwenden Sie IP-Filterkriterien, um Anwender basierend auf den IP-Adressen des Anwenders zu filtern. Sowohl IPv4 als auch IPv6 werden unterstützt.
Rollenfilterkriterien	Verwenden Sie Rollenfilterkriterien, um Anwender basierend auf ihren Rollen zu filtern.
Gruppenfilterkriterien	Verwenden Sie Gruppenfilterkriterien, um Anwender basierend auf der Anwendergruppe zu filtern, zu der der Anwender gehört.
Standortfilterkriterien	Verwenden Sie Standortfilterkriterien, um Anwender basierend auf dem Anwenderstandort zu filtern.
Filterkriterien für Attribut des Identitätsanbieters	Verwenden Sie die Attribute des Identitätsanbieters, die von der SAML-Antwort vom IdP empfangen werden, als Filterkriterien für die Authentifizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Generische Kriterien

Zusätzlich zu den zuvor aufgeführten Typen gibt es vier generische Filterkriterien. Diese Kriterien werden nicht in Ihrem Filternavigator angezeigt, Sie können sie jedoch auswählen, wenn Sie Ihren Authentifizierungsrichtlinien Richtlinieneingaben hinzufügen.

Generische Filterkriterientypen

Typ	Beschreibung
Authentifizierungsschema	Verwenden Sie , um basierend auf dem Authentifizierungsschema des Anwenders zu filtern. Dieses Kriterium ist ein Auswahltyp mit zwei Optionen: • Anwendername und Passwort, die eine lokale Anmeldung angeben • SSO, das eine Multi-SSO-basierte Anmeldung (SAML, OIDC oder Digest) angibt. **Hinweis:** Dieses Filterkriterium ist nur verfügbar, wenn **Integration: Single Sign-On-Installationsprogramm Für Mehrere Anbieter** [Plugin com.snc.integration.sso.multi.installer] ist installiert.
Identitätsanbieter	Verwenden Sie , um basierend auf dem Identitätsanbieter des Anwenders zu filtern. Verwenden Sie zusammen mit den Kriterien für das Authentifizierungsschema, um eine granulare Kontrolle über den Anmeldeprozess zu haben. Dieses Kriterium ist ein Verweis auf **Identitätsanbieter** Tabelle [sso_properties]. **Hinweis:** Dieses Filterkriterium ist nur verfügbar, wenn **Integration: Single Sign-On-Installationsprogramm Für Mehrere Anbieter** [Plugin com.snc.integration.sso.multi.installer] ist installiert.
Rollenbasierte MFA	Verwenden Sie , um basierend auf der rollenbasierten MFA-Funktion zu filtern. Dieses Kriterium ist ein boolesches Filterkriterium, das angibt, ob rollenbasierte MFA für den Anwender aktiviert ist.
Anwenderbasierte MFA	Verwenden Sie , um basierend auf der anwenderbasierten MFA-Funktion zu filtern. Dieses Kriterium ist ein boolesches Filterkriterium, das angibt, ob anwenderbasierte MFA für den Anwender aktiviert ist.
Vertrauenswürdige mobile App	Vertrauenswürdiger Filter für mobile Apps zum Aktivieren des Instanzzugriffs über die mobile App.

IP-Filter

Verwenden Sie IP-Filterkriterien, um die Anwender basierend auf den IP-Adressen des Anwenders zu filtern. Sowohl IPv4 als auch IPv6 werden unterstützt.

Mit IP-Filterkriterien können Sie Anwender basierend auf den IP-Adressen des Anwenders filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich zuzulassen oder zu verweigern.

Erstellen Sie IP-Filterkriterien

Mit IP-Filterkriterien können Sie Anwender basierend auf den IP-Adressen des Anwenders filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich zuzulassen oder zu verweigern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

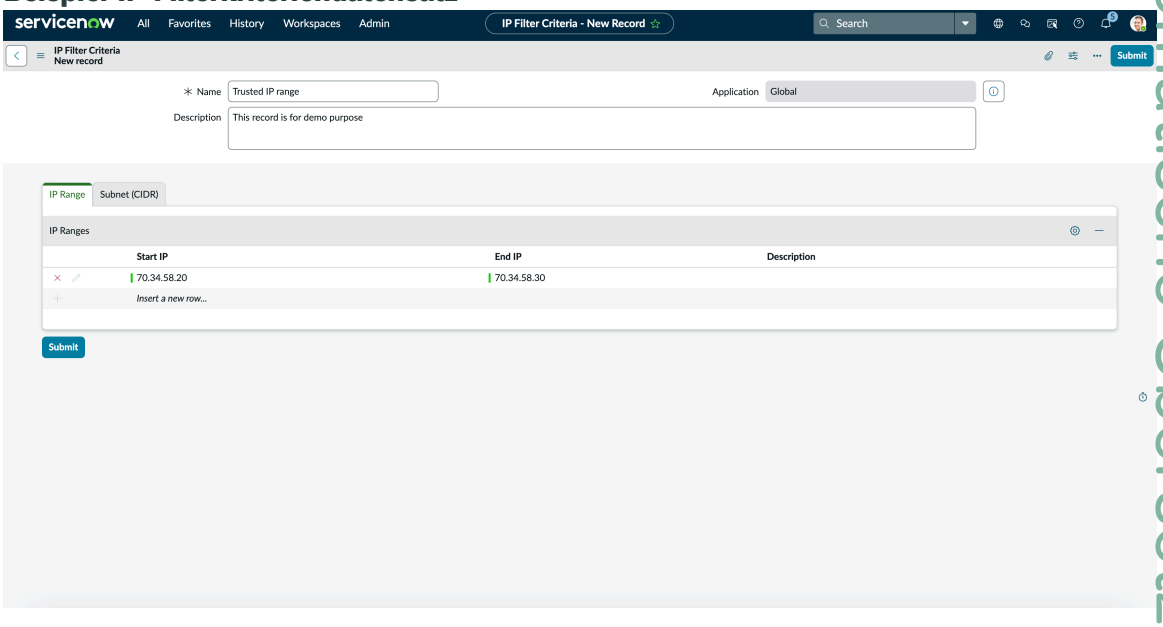
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **IP-Filterkriterien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „IP-Filterkriterien“

Feld	Beschreibung
Name	Name zur Identifizierung des IP-Netzwerks.
Beschreibung	Kurzbeschreibung des IP-Netzwerks.
Anwendung	Umfang der Anwendung.

Beispiel-IP-Filterkriteriendatensatz



4. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.
5. Von **IP-Bereich** Registerkarte, doppelklicken Sie auf **Fügen Sie eine neue Zeile ein** .
   Sie können eine einzelne IP-Adresse oder mehrere IP-Adressbereiche eingeben. Geben Sie beispielsweise für einen Bereich von IP-Adressen ein 192.0.2.0 In **Start-IP** Spalte und 192.0.2.255 In **End-IP** Spalte.

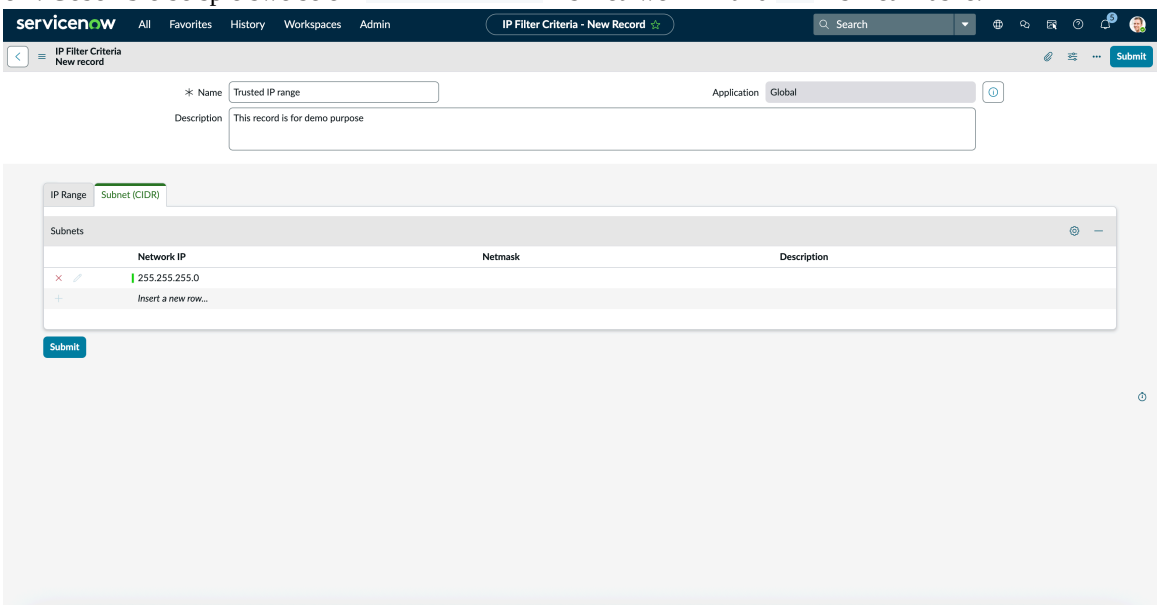
   Hinweis: Stellen Sie für eine einzelne IP-Adresse sicher, dass Sie dieselbe IP-Adresse in eingeben **Start-IP** Adresse und **End-IP** Spalten. Wenn Sie eine IP-Adresse in eingeben **Start-IP** Verlassen Sie die Spalte **End-IP** Spalte leer, und speichern Sie dann den Datensatz. Die **End-IP** Die Spalte wird automatisch mit demselben ausgefüllt **Start-IP** Adresse.

6. Von **Subnetz (CIDR)** Registerkarte, doppelklicken Sie auf **Fügen Sie eine neue Zeile ein** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geben Sie die Netzwerk-IP-Adresse und die Netzmaske im Format Classless Inter-Domain Routing (CIDR) ein. Geben Sie beispielsweise ein 255.255.255.0 Als Netzwerk-IP und 25 Als Netzmaske.



Rollenfilter

Verwenden Sie Rollenfilterkriterien, um Anwender basierend auf ihren Rollen zu filtern.

Mit Rollenfilterkriterien können Sie Anwender basierend auf den Rollen filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine Liste von Anwenderrollen zuzulassen oder zu verweigern.

Erstellen Sie Rollenfilterkriterien

Mit Rollenfilterkriterien können Sie Anwender basierend auf den Rollen filtern. Sie können eine Authentifizierungsrichtlinie konfigurieren, um den Zugriff auf eine Liste von Anwenderrollen zuzulassen oder zu verweigern.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

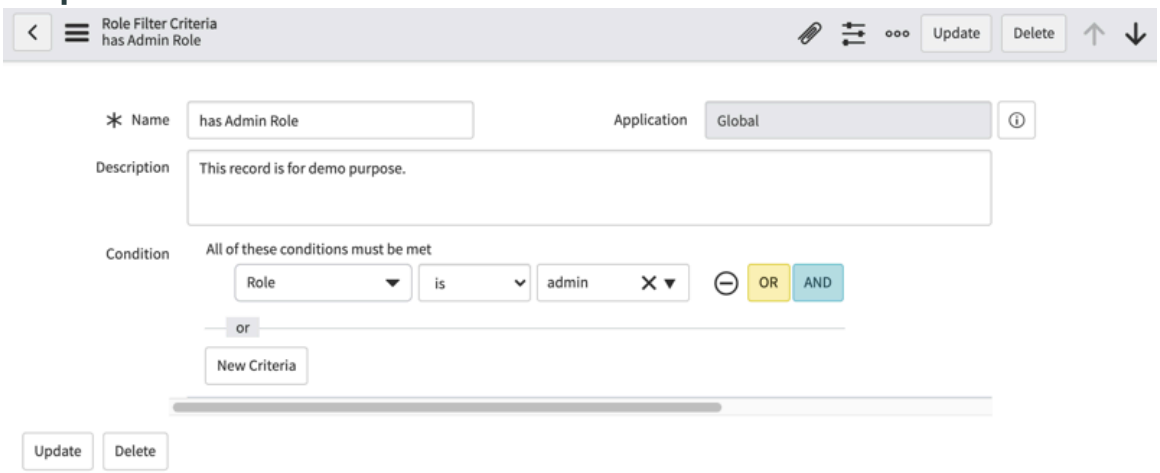
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Rollen-Filterkriterien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Formular „Rollenfilterkriterien“

Feld	Beschreibung
Name	Name zur Identifizierung der Rolle.
Anwendung	Umfang der Anwendung.
Beschreibung	Kurzbeschreibung der Rolle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Rollenfilterkriteriendatensatz

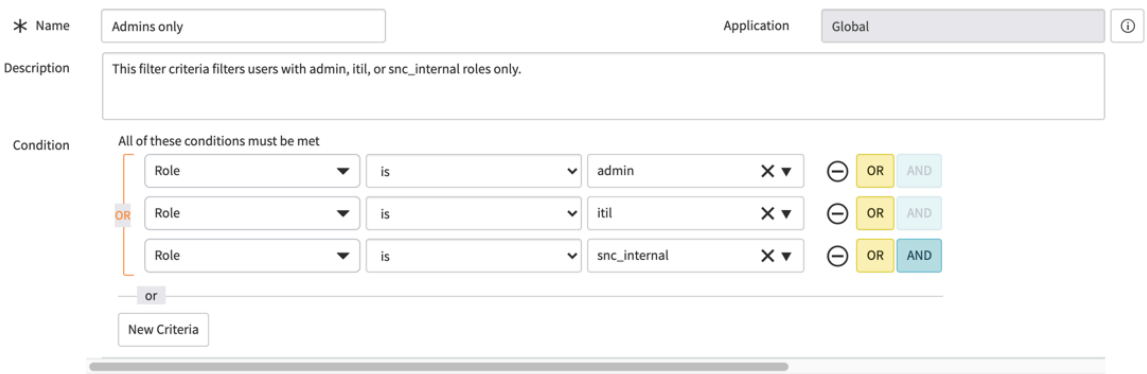


4. Von **Rollen für Kriterien** , Doppelklicken Sie auf **Fügen Sie eine neue Zeile ein** .
5. Erstellen Sie mit dem Bedingungsgenerator eine Bedingung für eine bestimmte Rolle.

   Sie können beispielsweise eine Bedingung erstellen, die nur Anwender mit den Rollen admin, itil oder snc_internal zulässt. Weitere Informationen zum Bedingungsgenerator finden Sie unter Erstellen Sie eine Bedingungsanweisung mit dem Bedingungsgenerator .

   Hinweis:

   - Derzeit wird Dot-Walking in Rollenfilterkriterien nicht unterstützt.
   - Folgende Operatoren werden für Rollenfilterkriterien nicht unterstützt:
     - Ist nicht
     - Enthält nicht
     - Unterscheidet sich von
     - Ist leer
     - Ist identisch mit
     - Ist nicht leer
     - Ist leere Zeichenfolge



Gruppenfilter

Verwenden Sie Gruppenfilterkriterien, um Anwender basierend auf der Anwendergruppe zu filtern, zu der der Anwender gehört.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppenfilterkriterien ermöglichen oder verweigern Anwenderzugriff basierend auf der Anwendergruppe, zu der der Anwender gehört.

Erstellen Sie Gruppenfilterkriterien

Gruppenfilterkriterien ermöglichen oder verweigern Anwenderzugriff basierend auf der Anwendergruppe, zu der der Anwender gehört.

Vorbereitungen
Erforderliche Rolle: Administrator

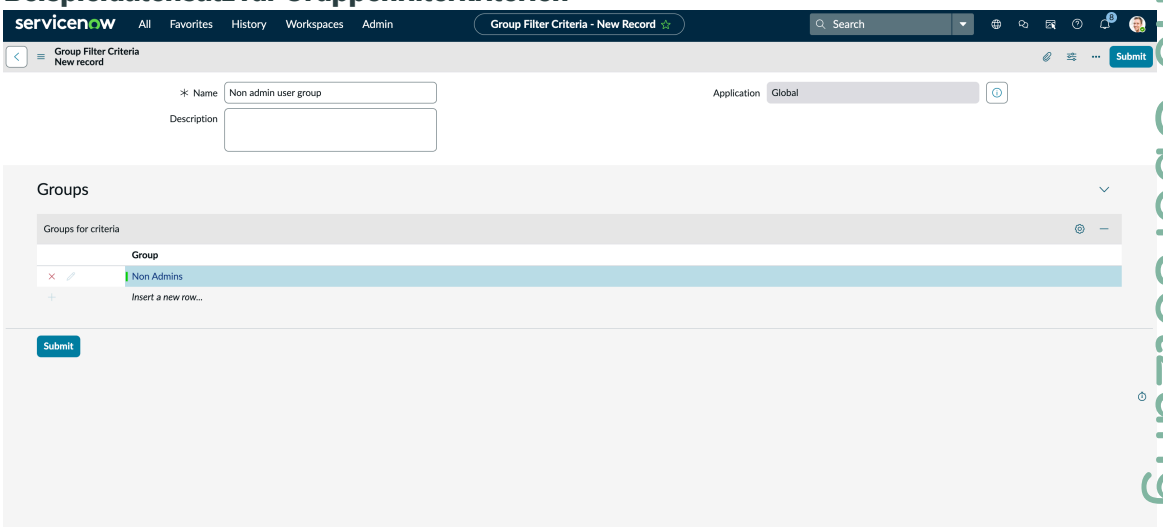
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Gruppenfilterkriterien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Gruppenfilterkriterien

Feld	Beschreibung
Name	Name zur Identifizierung der Gruppe.
Beschreibung	Kurzbeschreibung der Gruppe.
Anwendung	Umfang der Anwendung.

Beispieldatensatz für Gruppenfilterkriterien



4. Von **Gruppen für Kriterien** Registerkarte, doppelklicken Sie auf **Fügen Sie eine neue Zeile ein** .
5. Klicken Sie auf das Suchsymbol , Suchen und wählen Sie eine Anwendergruppe aus.
6. Klicken Sie auf das Speichersymbol.

Standortfilter

Standortfilterkriterien können als Filtereingabe für Anwender basierend auf dem Anwenderstandort verwendet werden.

Standortfilter ist ein Filterkriterium, das Administratoren beim Erstellen der Authentifizierungsrichtlinien basierend auf dem physischen Standort des Geräts verwenden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Der Standortfilter ist mit der Zero Trust-Zugriffsfunktion verfügbar. Weitere Informationen finden Sie unter Zero Trust Access (ZTA).
- Die Instanz muss sich in ADCv2 befinden. Wenn sich die Instanz nicht in ADCv2 befindet, sind die Informationen zum Anwenderstandort nicht verfügbar.

Mit den Standortfilterkriterien können Sie Folgendes ausführen:

- Fungieren Sie als Richtlinieneingabe für Richtlinienbedingungen, um die Anforderungen für die Authentifizierung zu verifizieren und zu erfüllen.
- Bieten Sie die Möglichkeit, Richtlinien für adaptive Authentifizierung basierend auf zu erstellen **Land** .
- Instanzzugriff auf eine bestimmte Geografie zulassen oder nicht zulassen.
- Verwenden Sie die standortbasierte vor- oder Nachauthentifizierungsrichtlinie, um:
  - Verhindern Sie den Zugriff aus sanktionierten Ländern außerhalb einer engen, vom Datenschutz kontrollierten Region nach Ermessen des Unternehmens.
  - Gewähren Sie Zugriff auf Bereiche nur innerhalb der geltenden Datenschutzregion und des Ermessens des Unternehmens.
  - Konfigurieren Sie die landesbasierte Allow-Liste für die Authentifizierung.

Anwendungsfälle

Im Folgenden finden Sie einige der Anwendungsfälle für die Verwendung von Standortfilterkriterien für die adaptive Authentifizierung:

- Blockieren Sie den Zugriff auf die Instanz aus einem Land.
- Zugriff auf die Instanz nur aus einem bestimmten Land zulassen.
- Erzwingen Sie die Step-up-Authentifizierung oder MFA, um sich basierend auf dem Land anzumelden.
- Reduzieren oder beschränken Sie Rollen für den Anwender basierend auf dem Land.
- Standortfilterkriterien können für MFA, Zero Trust Access (ZTA), Kontext vor der Authentifizierung und Kontext nach der Authentifizierung verwendet werden.

Standortidentifizierung

Die Standortservices zur Identifizierung des Standorts des Anwenders werden von einem Drittanbieterservice bereitgestellt – MaxMind.

Der Standort des Anwenders wird über das VPN aus dem Header „x-Forward-for“ identifiziert. Wenn der Service keinen Header ausfüllt, wird nur die VPN-IP (Standort) als Anwenderstandort angezeigt.

Hinweis: Wenn nach der Konfiguration des Standortfilters falsche Standorte angezeigt werden, finden Sie unter KB-artikel Zur Problembehandlung.

Aktivieren Sie Standortbasierten Zugriff

Aktivieren Sie **Zero Trust: Standortbasierter Zugriff** (`Com.snc.Zero_Trust_location_Access`), damit Administratoren adaptive Authentifizierungsrichtlinien basierend auf dem Standort des Anwenders konfigurieren können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

- Abhängiges Plugin: Adaptive Authentifizierung
- Plugin-Typ: Bezahlt und Lizenz erforderlich.
- Die Instanz muss sich in ADCv2 befinden. Wenn sich die Instanz nicht in ADCv2 befindet, sind die Informationen zum Anwenderstandort nicht verfügbar.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach **Zero Trust: Standortbasierter Zugriff** (`Com.snc.Zero_Trust_location_Access`) Plugin mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Erstellen Sie Standortfilterkriterien

Verwenden Sie Standortfilterkriterien, um Eingaben für die Anwenderauthentifizierung basierend auf dem Anwenderstandort zu filtern.

Vorbereitungen

Erforderliche Rolle: Administrator

Plugin erforderlich: **Zero Trust: Standortbasierter Zugriff** (`Com.snc.Zero_Trust_location_Access`).

Eigenschaft: Aktivieren Sie die Eigenschaft „Adaptive Authentifizierung“.

Hinweis: Administratoren können die Richtlinie nur basierend auf Standortfiltern erstellen, wenn der Standort für die aktuelle Anwendersitzung verfügbar ist.

Prozedur

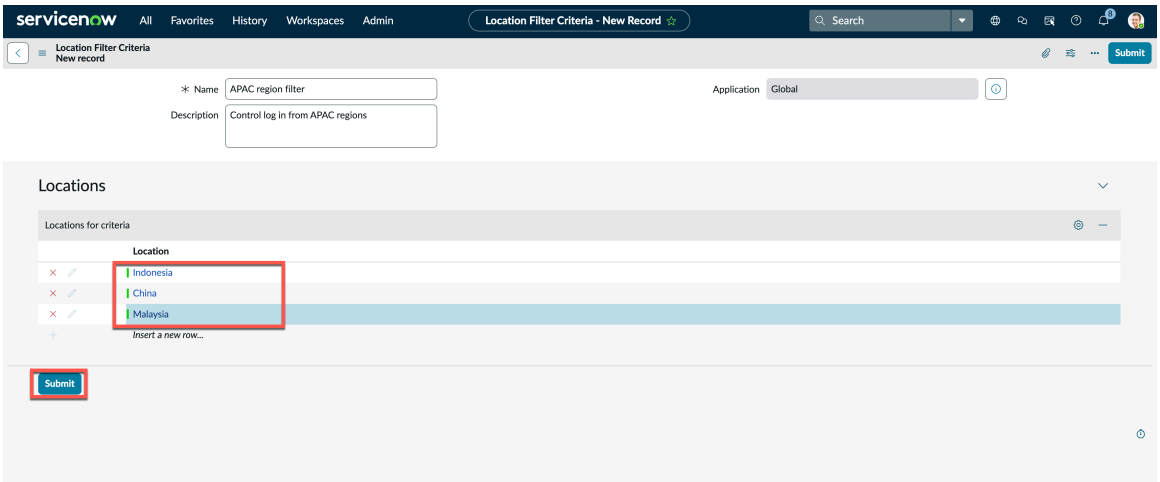
1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Standortfilterkriterien**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standortfilterkriterien“

Feld	Beschreibung
Name	Name zur Identifizierung der Kriterien.
Beschreibung	Kurzbeschreibung der Kriterien.
Anwendung	Umfang der Anwendung.

4. In **Standorte** Doppelklicken Sie auf der Registerkarte Standorte für Kriterien auf Abschnitte **Fügen Sie eine neue Zeile ein** .
5. Geben Sie die Standorte an.



6. Wählen Sie **Absenden**.

Tutorial: Standortfilterkriterien verwenden

Beschreibt die Schritte zur Verwendung von Standortfilterkriterien in der Authentifizierungsrichtlinie und zur Beschränkung des Zugriffs auf die Anwender basierend auf dem Standort.

Vorbereitungen

Erforderliche Rolle: Administrator

Plugin erforderlich: **Zero Trust: Standortbasierter Zugriff** (`Com.snc.Zero_Trust_location_Access`).

Eigenschaft: Aktivieren Sie die Eigenschaft „Adaptive Authentifizierung“.

> **Hinweis:** Administratoren können die Richtlinie nur basierend auf Standortfiltern erstellen, wenn der Standort für die aktuelle Anwendersitzung verfügbar ist.

Im folgenden Verfahren wird beschrieben, wie Standortfilterkriterien in einer Authentifizierungsrichtlinie erstellt und verwendet werden.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Standortfilter**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Automatische Übersetzung

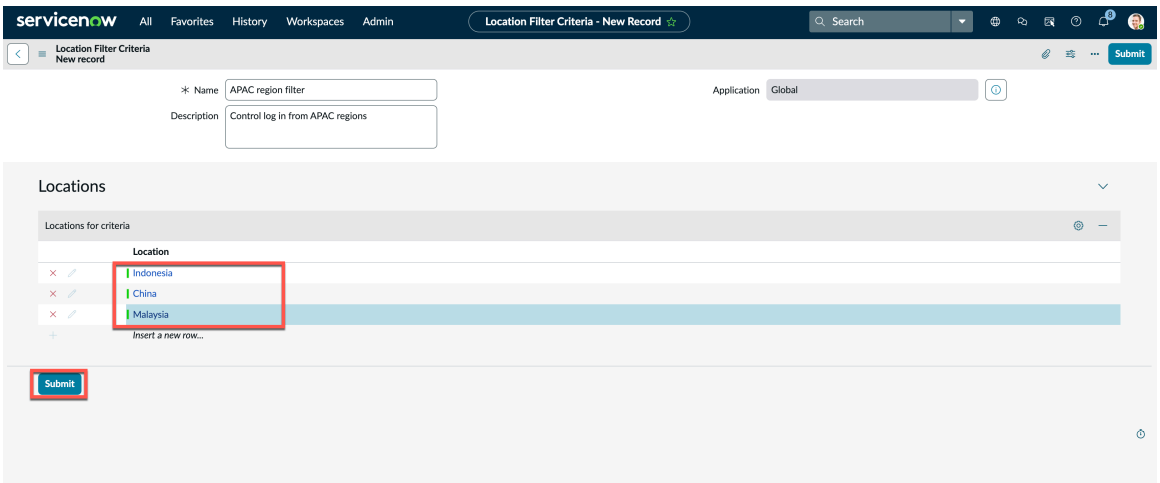
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standortfilterkriterien“

Feld	Beschreibung
Name	Name zur Identifizierung der Kriterien.
Beschreibung	Kurzbeschreibung der Kriterien.
Anwendung	Umfang der Anwendung.

4. In **Standorte** Doppelklicken Sie auf der Registerkarte Standorte für Kriterien auf Abschnitte **Fügen Sie eine neue Zeile ein** .
5. Geben Sie die Standorte an.

   Verwenden Sie beispielsweise einige der APAC-Regionen, um die Anmeldungen der Anwender zu steuern, die aus APAC kommen.



   Basierend auf den im Beispiel festgelegten Kriterien können Sie Anmeldungen von steuern Indonesien , China , Und Malaysia Für Ihre Instanz.

6. Wählen Sie **Absenden**.
7. Verwenden Sie die Filterkriterien, die in einem beliebigen Authentifizierungskontext (vor, nach, MFA) und Sitzungszugriff erstellt wurden.

   Weitere Informationen zur Konfiguration basierend auf Authentifizierungskontext und Sitzungszugriff finden Sie unter:

   - Standortfilter im Kontext vor der Authentifizierung
   - Standortfilter im Kontext nach der Authentifizierung
   - Standortfilter im MFA-Kontext
   - Standortfilter für Sitzungszugriff

   Sie können die Eigenschafts-ID – Fehlermeldung verwenden, die dem Anwender angezeigt wird, wenn die Anmeldung aufgrund eines Fehlers der Authentifizierungsrichtlinie (glide.auth.policy.ui.error.message), um die Fehlermeldung anzupassen.

Verwenden Sie den Standortfilter im Kontext vor der Authentifizierung

Verwenden Sie die Standortfilterkriterien, die im Kontext vor der Authentifizierung erstellt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Plugin erforderlich: **Zero Trust: Standortbasierter Zugriff** (`Com.snc.Zero_Trust_location_Access`).

Erstellen Sie einen Standortfilter mit den Ländern, in denen Sie den Zugriff auf die Anwender basierend auf dem Standort beschränken möchten. Weitere Informationen finden Sie unter Erstellen Sie Standortfilterkriterien.

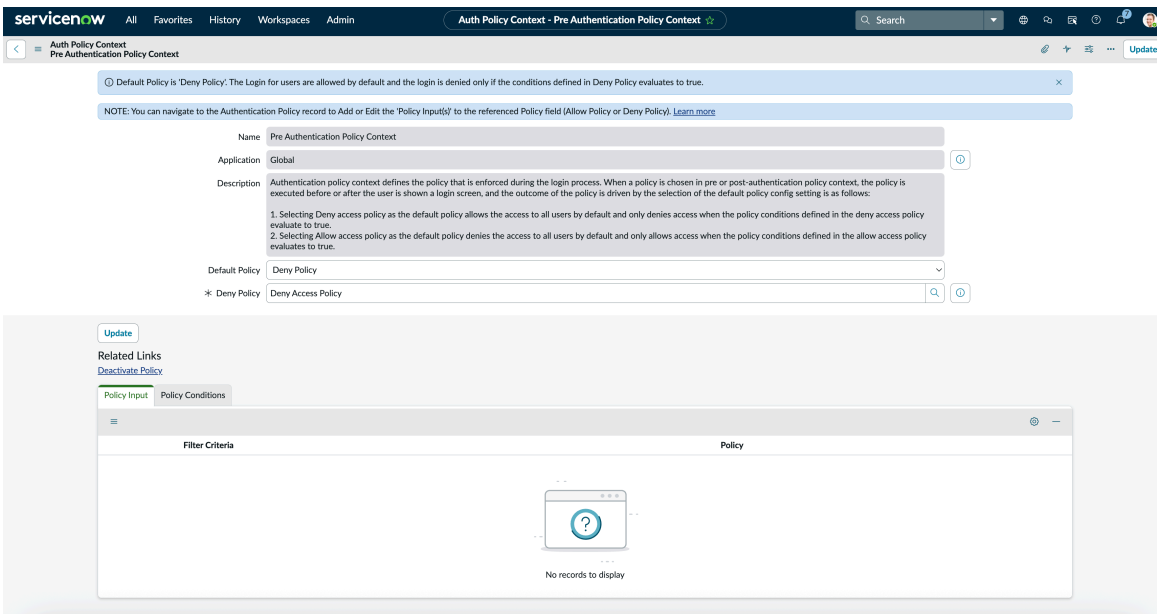
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **Kontext vor der Authentifizierung**an.

   Wenn im Kontext der Richtlinie vor der Authentifizierung eine Richtlinie ausgewählt wird:

   - Wenn Sie die Richtlinie „Zugriff verweigern“ als Standardrichtlinie auswählen, ist der Zugriff standardmäßig für alle Anwender zulässig. Der Zugriff wird nur verweigert, wenn die in der Richtlinie „Zugriff verweigern“ definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.
   - Wenn Sie die Richtlinie „Zugriff zulassen“ als Standardrichtlinie auswählen, wird standardmäßig allen Anwendern der Zugriff verweigert, und der Zugriff ist nur zulässig, wenn die in der Richtlinie „Zugriff zulassen“ definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

   Das Beispiel zeigt, wie Sie die Anmeldungen von den angegebenen Standorten aus beschränken können. Sie können Zugriff verweigern und die zugehörige Richtlinie (Zugriff verweigern) als Richtlinie vor der Authentifizierung auswählen und die Richtlinieneingaben und -Bedingungen angeben.

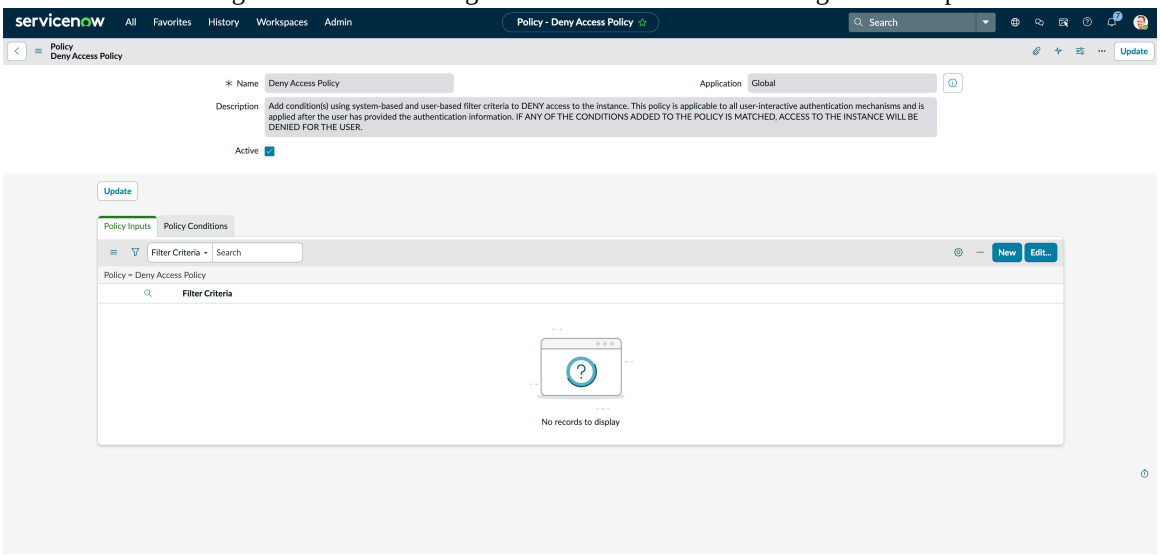


2. Wählen Sie das Informationssymbol und dann aus **Öffnen Sie Den Datensatz** Um zu öffnen **Richtlinie Ablehnen** Datensatz.

   Hinweis: Das in dieser Aufgabe beschriebene Beispiel ist **Richtlinie Ablehnen** . Sie können auch verwenden **Richtlinie Zulassen** Und legen Sie die Bedingungen entsprechend fest, um die Anmeldungen zu steuern.

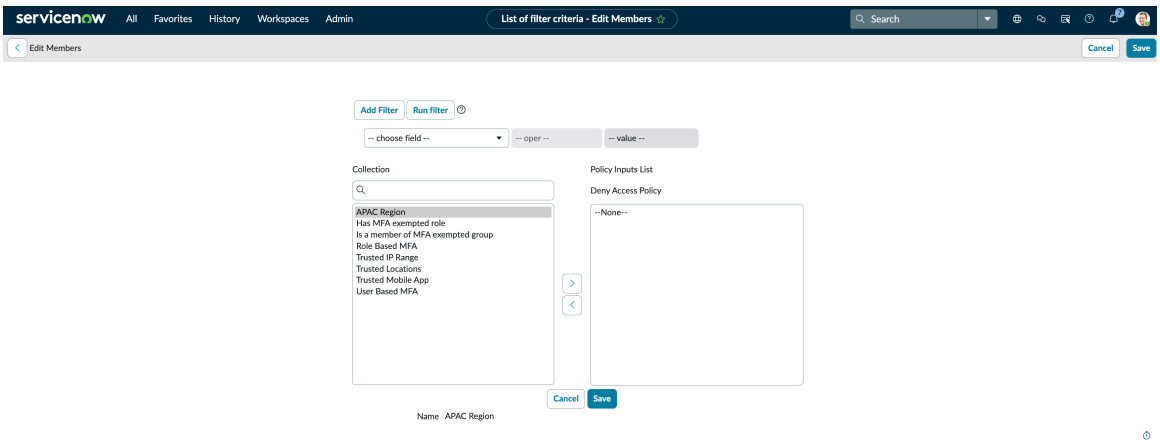
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie in der Zugriffsrichtlinie verweigern im Abschnitt Richtlinieneingaben die Option aus **Neu** .



4. Fügen Sie die Eingabe Standortfilter und hinzu **Speichern** .

   Beispiel: APAC-Region.

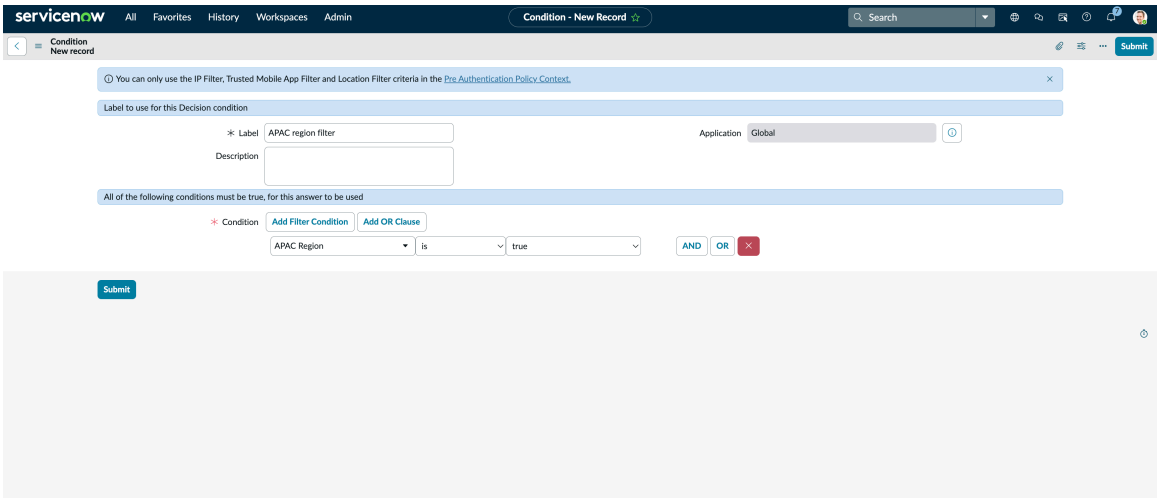


   Der Filter wird als hinzugefügt **Richtlinieneingaben** .

5. Wählen Sie die Registerkarte Richtlinienbedingungen aus, und wählen Sie aus **Neu** .
6. Geben Sie auf der Seite „Bedingungen“ die Bezeichnung und die Bedingungen an, und legen Sie sie auf „wahr“ fest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- In diesem Beispiel bedeutet die Auswahl von „wahr“ als Bedingung, dass der Anwender, der sich aus den konfigurierten Regionen anmeldet, sich nicht bei der Instanz anmelden kann.
- Wenn die Bedingung auf „falsch“ festgelegt ist, können sich nur Anwender aus konfigurierten Regionen bei der Instanz anmelden, und die anderen Anwender können sich nicht bei der Instanz anmelden.

7. Wählen Sie **Absenden**.
   Den Anwendern, die den Instanzlink auswählen und aus den konfigurierten Ländern protokollieren, wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt (Fehlermeldung, die von ihren Administratoren auf der Seite mit den Richtlinieneigenschaften konfiguriert wurde).

Verwenden Sie Den Kontext Für Standortfilter Nach Der Authentifizierung

Verwenden Sie die Standortfilterkriterien, die im Kontext nach der Authentifizierung erstellt wurden.

Vorbereitungen

Erforderliche Rolle: Administrator

Plugin erforderlich: **Zero Trust: Standortbasierter Zugriff** (`Com.snc.Zero_Trust_location_Access`).

Erstellen Sie einen Standortfilter mit den Ländern, in denen Sie den Zugriff auf die Anwender basierend auf dem Standort beschränken möchten. Weitere Informationen finden Sie unter Erstellen Sie Standortfilterkriterien.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **Kontext nach der Authentifizierung**an.

   Wenn im Kontext der Richtlinie nach der Authentifizierung eine Richtlinie ausgewählt wird:

   - Wenn Sie die Richtlinie „Zugriff verweigern“ als Standardrichtlinie auswählen, ist der Zugriff standardmäßig für alle Anwender zulässig. Der Zugriff wird nur verweigert, wenn die in der Richtlinie „Zugriff verweigern“ definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie die Richtlinie „Zugriff zulassen“ als Standardrichtlinie auswählen, wird standardmäßig allen Anwendern der Zugriff verweigert, und der Zugriff ist nur zulässig, wenn die in der Richtlinie „Zugriff zulassen“ definierten Richtlinienbedingungen als „wahr“ ausgewertet werden.

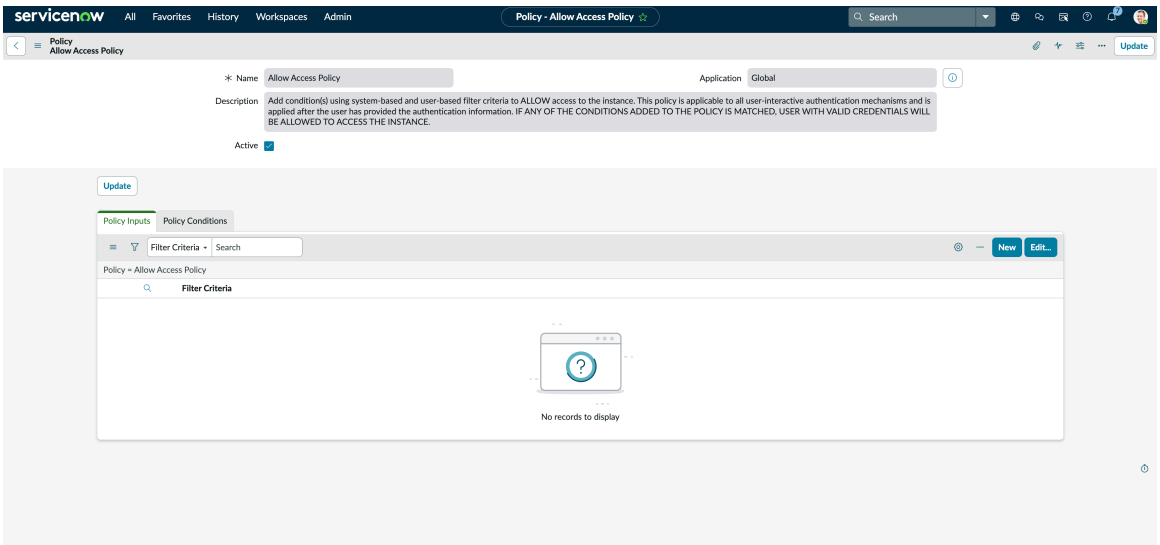
Das Beispiel zeigt, wie Sie einen konfigurieren können itil Anwender mit der Bedingung, dass nur vom angegebenen Standort (USA) auf die Instanz zugegriffen werden kann. Und itil Anwender können sich nicht aus anderen Ländern anmelden.

Nachdem Anwender ihre Anmeldeinformationen auf der Anmeldeseite angegeben haben. Sie können Zugriff zulassen und die zugehörige Richtlinie (Zugriff zulassen) als Richtlinie nach der Authentifizierung auswählen und die Richtlinieneingaben und -Bedingungen angeben.

2. Wählen Sie das Informationssymbol und dann aus **Öffnen Sie Den Datensatz** Um zu öffnen **Richtlinie Zulassen** Datensatz.

> **Hinweis:** Das in dieser Aufgabe beschriebene Beispiel ist **Richtlinie Zulassen** . Sie können auch verwenden **Richtlinie Ablehnen** Und legen Sie die Bedingungen entsprechend fest, um die Anmeldung zu steuern.

3. Wählen Sie im Abschnitt „Zugriffsrichtlinie zulassen“ im Abschnitt „Richtlinieneingaben“ die Option aus **Neu** .

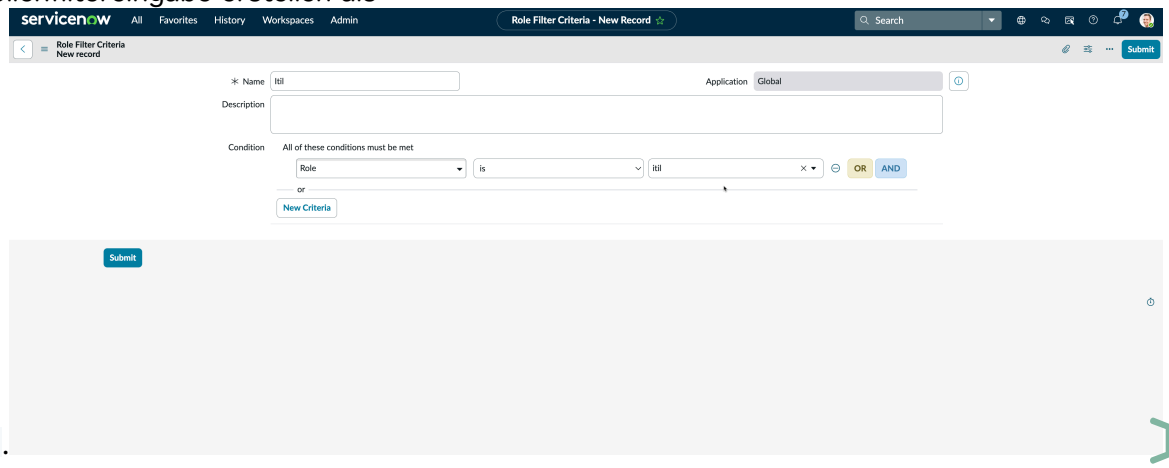


4. Fügen Sie die Rollenfilterkriterien und Standortfilterkriterien hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

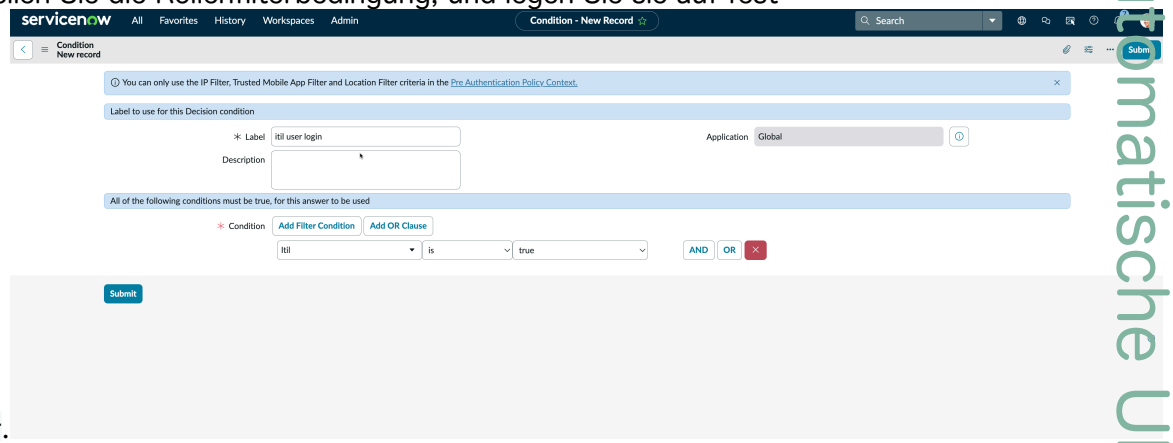
a. Rollenfilterkriterien werden hinzugefügt:

- Rollenfiltereingabe erstellen als



itil.

- Erstellen Sie die Rollenfilterbedingung, und legen Sie sie auf fest



Wahr.

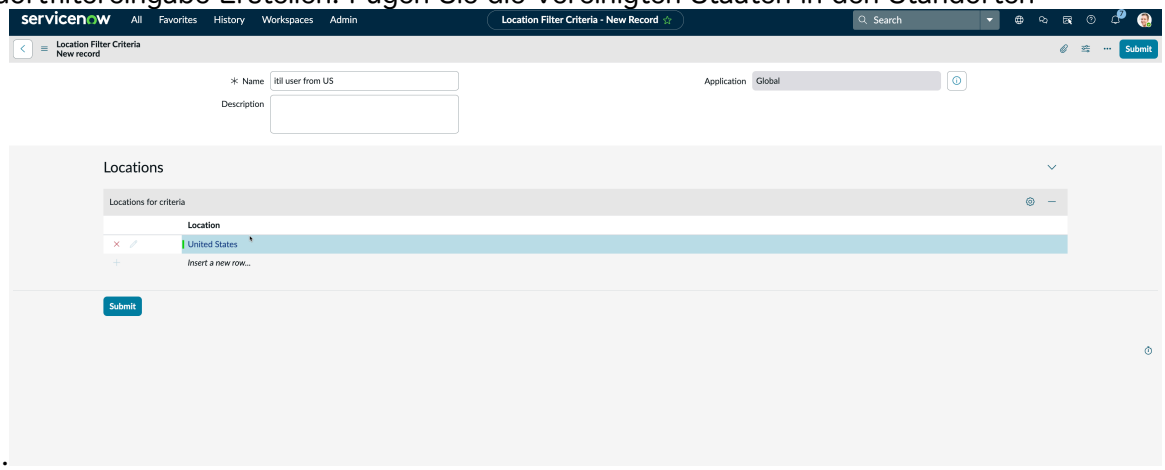
Weitere Informationen zum Erstellen von Rollenfilterkriterien finden Sie unter Erstellen Sie Rollenfilterkriterien.

b. Standortfilterkriterien werden hinzugefügt:

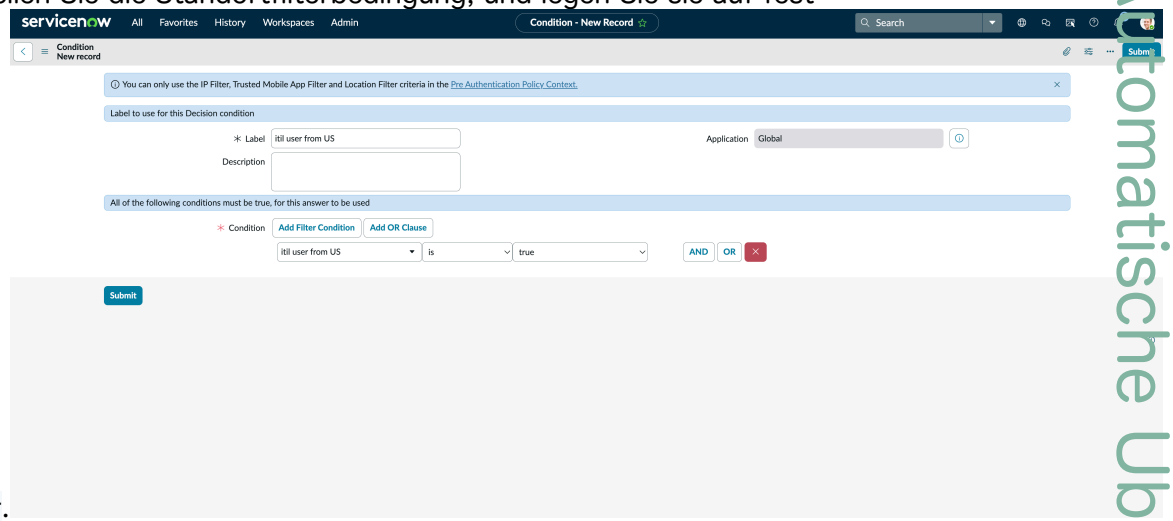
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Standortfiltereingabe Erstellen. Fügen Sie die Vereinigten Staaten in den Standorten hinzu.



- Erstellen Sie die Standortfilterbedingung, und legen Sie sie auf fest Wahr.



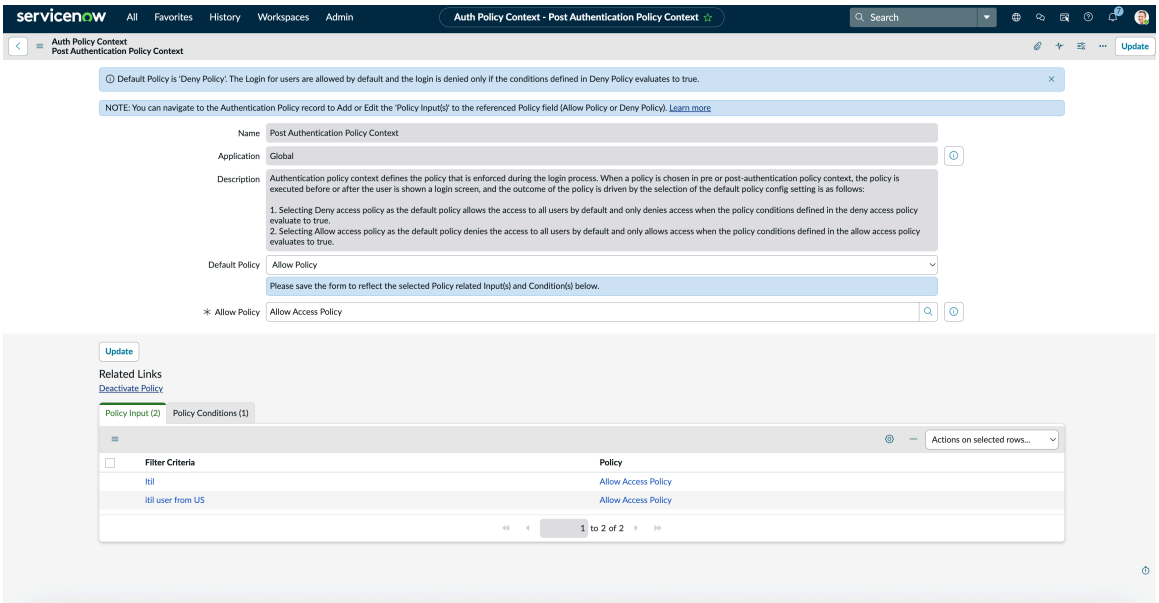
Weitere Informationen zum Erstellen von Rollenfilterkriterien finden Sie unter Erstellen Sie Standortfilterkriterien.

Die Richtlinie „Zugriff zulassen“ zeigt die Richtlinieneingaben und -Bedingungen an, die in den vorherigen Schritten erstellt wurden:

- Richtlinieneingaben: itil, itil-Anwender aus den USA
- Richtlinienbedingungen: itil-Anwenderanmeldung, itil-Anwender aus US-Bedingung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- In diesem Beispiel bedeutet die Auswahl von „wahr“ als Bedingung, dass itil Anwender, die sich aus dem konfigurierten Land (USA) anmelden, können sich bei der Instanz anmelden.
- Wenn die Bedingung auf „falsch“ festgelegt ist, wird die verwendet itil Anwender aus dem konfigurierten Land (USA) können sich nicht bei der Instanz anmelden, und die anderen Anwender können sich nicht bei der Instanz anmelden.

5. Wählen Sie Aus **Übermitteln** Oder **Aktualisieren** Dient zum Aktualisieren des Kontexts nach der Authentifizierung.
   Die itil Anwender, die den Instanzlink auswählen, ihre Anmeldeinformationen angeben und sich dann außerhalb des konfigurierten Landes (USA) anmelden, werden eine Fehlermeldung zur Zugriffsverweigerung angezeigt (Fehlermeldung, die von ihren Administratoren auf der Seite mit den Richtlinieneigenschaften konfiguriert wurde).

Verwenden Sie Standortfilter im MFA-Kontext

Verwenden Sie die im MFA-Kontext erstellten Standortfilterkriterien.

Vorbereitungen

Erforderliche Rolle: Administrator

Plugin erforderlich: **Zero Trust: Standortbasierter Zugriff** (Com.snc.Zero_Trust_location_Access).

Im folgenden Verfahren wird beschrieben, wie Sie einen Standortfilter mit den Ländern erstellen, für die Sie MFA als zweiten Faktor für die Authentifizierung bei Anwendern basierend auf dem Standort konfigurieren möchten.

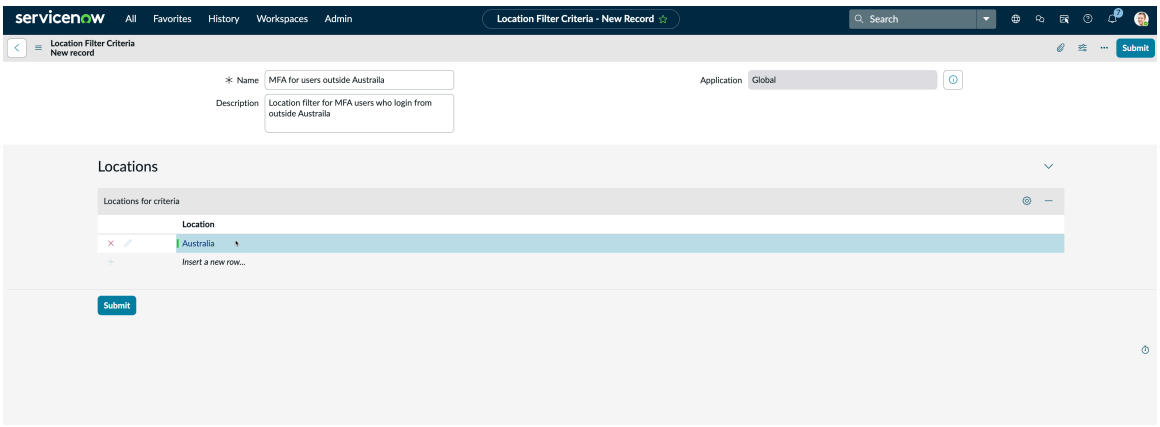
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontext der Authentifizierungsrichtlinie** > **MFA-Kontext**an.
2. Wählen Sie aus **STEP-up-MFA-Richtlinie** Informationssymbol, und wählen Sie dann aus **Öffnen Sie Den Datensatz** Um zu öffnen **MFA-Kontext** .

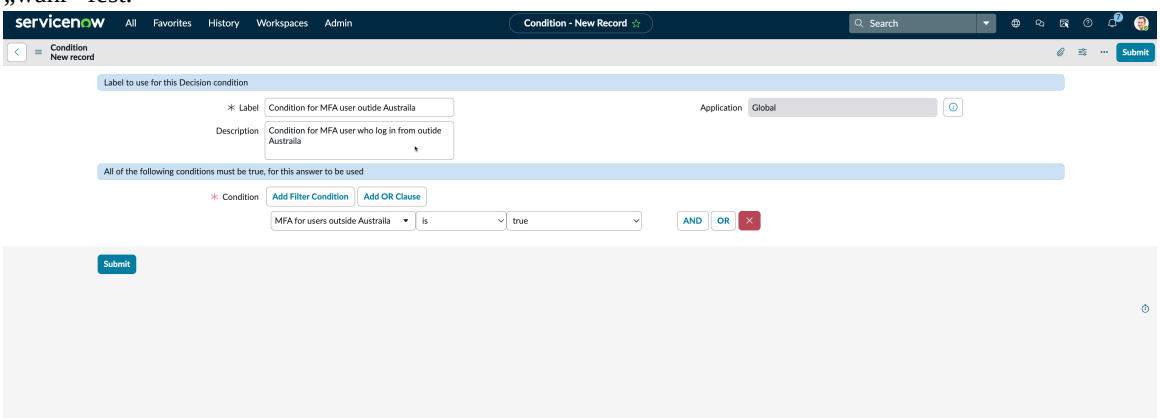
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie auf der Seite Step-up-MFA-Richtlinie auf der Registerkarte Richtlinieneingaben die Option aus **Neu** .
4. Fügen Sie die Eingabe Standortfilter und hinzu **Übermitteln** .

   Sie möchten beispielsweise MFA für Anwender anzeigen, die sich außerhalb Australiens bei der Instanz anmelden.



5. Wählen Sie auf der Seite Step-up MFA-Richtlinie die Registerkarte Richtlinienbedingungen aus, und wählen Sie aus **Neu** .
6. Geben Sie auf der Seite „Bedingungen“ die Bezeichnung und die Bedingungen an, und legen Sie sie auf „wahr“ fest.



7. Wählen Sie **Absenden**.
8. Aktivieren Sie auf der Seite „Step-up-MFA-Richtlinie“ die MFA-Richtlinie, falls dies der Fall ist **Deaktiviert** .
9. Wählen Sie Aus **Aktualisieren** Um die Konfiguration zu aktualisieren.

   Die Anwender außerhalb des konfigurierten Landes (Australien), die den Instanzlink auswählen und ihre Anmeldeinformationen angeben; werden auf dem MFA-Bildschirm angezeigt, um die Anmeldeinformationen des zweiten Faktors für die Anmeldung bei der Instanz bereitzustellen.

Verwenden Sie den Standortfilter für den Sitzungszugriff

Verwenden Sie die in Sitzungszugriff erstellten Standortfilterkriterien, um Rollen basierend auf dem Standort des Anwenders zu reduzieren.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin erforderlich: **Zero Trust: Standortbasierter Zugriff** (Com.snc.Zero_Trust_location_Access).

Im folgenden Verfahren wird beschrieben, wie Sie einen Standortfilter mit den Ländern erstellen, die Sie entfernen oder Rollen basierend auf dem Standort auf die Anwender beschränken möchten.

Prozedur

1. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.
2. Um eine Konfiguration der Sitzungszugriffsrolle zu erstellen, wählen Sie aus **Neu** .
3. Füllen Sie im Formular die folgenden Felder aus:

Konfiguration der Sitzungszugriffsrolle

Feld	Beschreibung
Name	Name der Konfiguration
Beschreibung	Kurzbeschreibung der Konfiguration.
Richtlinie	Wählen Sie die Zugriffsrichtlinie aus. Verwenden Sie das Suchsymbol, um die Liste der Richtlinien anzuzeigen. **Hinweis:** Sie müssen die Standortfiltereingabe und -Bedingungen hinzufügen, indem Sie den Richtliniendatensatz öffnen.
Aktion	**Entfernen Sie Rollen** Oder **Auf Rollen beschränken** . ○ **Entfernen Sie Rollen** : Wenn sich der konfigurierte Anwender anmeldet, wird die Liste der Rollen, die in der Rollen- oder Gruppenliste bereitgestellt werden, für die angemeldete Sitzung entfernt. ○ **Auf Rollen Beschränken** : Wenn sich der konfigurierte Anwender angemeldet hat, werden dem Anwender nur die ausgewählten Rollen bereitgestellt, und alle anderen Rollen werden für die angemeldete Sitzung entfernt.
Rollenliste	Wählen Sie die Rolle aus der Rollenliste aus.
Gruppenliste	Wählen Sie die Rolle aus der Gruppenliste aus.

4. Auswählen, **Übermitteln** .

Die Anmeldung für Anwender basierend auf den konfigurierten Ländern lautet wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn **Entfernen Sie Rollen** , Die Anwender aus den konfigurierten Ländern im Standortfilter werden mit den für die Sitzung konfigurierten Rollen entfernt.
- Wenn **Auf Rollen Beschränken** , Die Anwender aus den konfigurierten Ländern im Standortfilter haben nur die Rollen, die für die Sitzung konfiguriert sind.

Weitere Informationen zum Entfernen oder Einschränken von Rollen für eine Sitzung finden Sie unter Tutorial: Zero Trust-Zugriff Verwenden.

Attributfilter Des Identitätsanbieters

Verwenden Sie die Attribute des Identitätsanbieters, die von der SAML-Antwort (Security Assertion Markup Language) und OpenID Connect (OIDC) vom Identitätsanbieter (IdP) empfangen werden, als Filterkriterien für die Authentifizierung.

Um alle Attribute von einem IdP über die SAML- und OIDC-Antwort abzurufen, sollten Sie eine Testverbindung mit dem IdP durchführen. Nach einer erfolgreichen Testverbindung werden die Attribute auf einer neuen Registerkarte auf der Konfigurationsseite des Identitätsanbieters hinzugefügt.

Weitere Informationen finden Sie in den folgenden Themen:

- Identitätsanbieter-Attribute für Markup-Sprache für SicherheitsAssertion
- Identitätsanbieter-Attribute für OpenID Connect

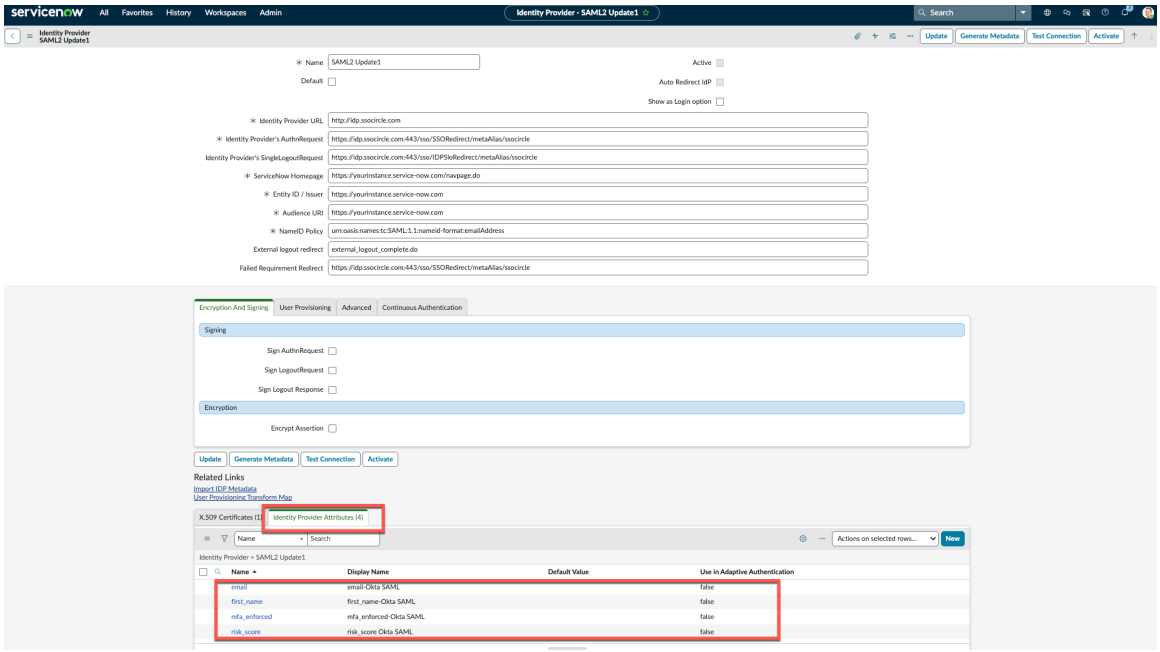
Identitätsanbieter-Attribute für Markup-Sprache für SicherheitsAssertion

Verwenden Sie die Attribute des Identitätsanbieters, die von der SAML-Antwort (Security Assertion Markup Language) und OpenID Connect (OIDC) vom Identitätsanbieter (IdP) empfangen werden, als Filterkriterien für die Authentifizierung.

Um alle Attribute von einem IdP über die SAML-Antwort abzurufen, sollten Sie eine Testverbindung mit dem IdP durchführen. Nach einer erfolgreichen Testverbindung werden die Attribute auf einer neuen Registerkarte auf der Konfigurationsseite des Identitätsanbieters hinzugefügt.

- Der Identitätsanbieter-Filter ist mit der Zero Trust-Zugriffsfunktion verfügbar. Weitere Informationen finden Sie unter Zero Trust Access (ZTA).
- IdP-Attributfilterkriterien können in verwendet werden Kontext nach der Authentifizierung, Zero Trust Access (ZTA) Sitzungsabbruch, und Multifaktor-Authentifizierungskontext.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können Attribute auch hinzufügen, indem Sie auswählen **Neu** Aus dem Abschnitt „Attribute des Identitätsanbieters“ und verwenden Sie diese Attribute für die adaptive Authentifizierung, indem Sie sie auf festlegen Wahr .

Die **Attribute Des Identitätsanbieters** Werden mit den folgenden Details angezeigt:

Formular „Standortfilterkriterien“

Feld	Beschreibung
Name	Attributname, der vom Identitätsanbieter bereitgestellt wird.
Anzeigename	Anzeigename ist der detaillierte Name, der für die Filterkriterien verwendet wird. **Hinweis:** Sie können einen lesbaren Namen als Anzeigenamen angeben. In einigen Fällen ist der von den Identitätsanbietern bereitgestellte Anzeigename lang und nicht lesbar.
Standardwert	Der Standardwert wird für die Auswertung der Filterkriterien verwendet, falls das Attribut in der SAML-Antwort fehlt.
In adaptiver Authentifizierung verwenden	Option zur Verwendung des Attributs in der adaptiven Authentifizierung.

Hinweis: Attribute, die aus Azure IdP ausgefüllt werden, haben aufgrund der Namenslänge des Attributs Namen und Anzeigenamen, die auf Zeichen beschränkt sind.

Sie können auch neue Attribute hinzufügen, indem Sie auswählen **Neu** In **Attribute Des Identitätsanbieters** Abschnitt.

Wenn die Option „in adaptiver Authentifizierung verwenden“ auf „wahr“ festgelegt ist, wird das ausgewählte Attribut als Filterkriterien in den generischen Filterkriterien hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: **Risk_Score** Auf festlegen `Wahr` . Auf der Seite „Allgemeine Filterkriterien“ wurde ein neuer Filter erstellt.

Verwenden Sie das Attribut des Identitätsanbieters als Filterkriterien für SAML

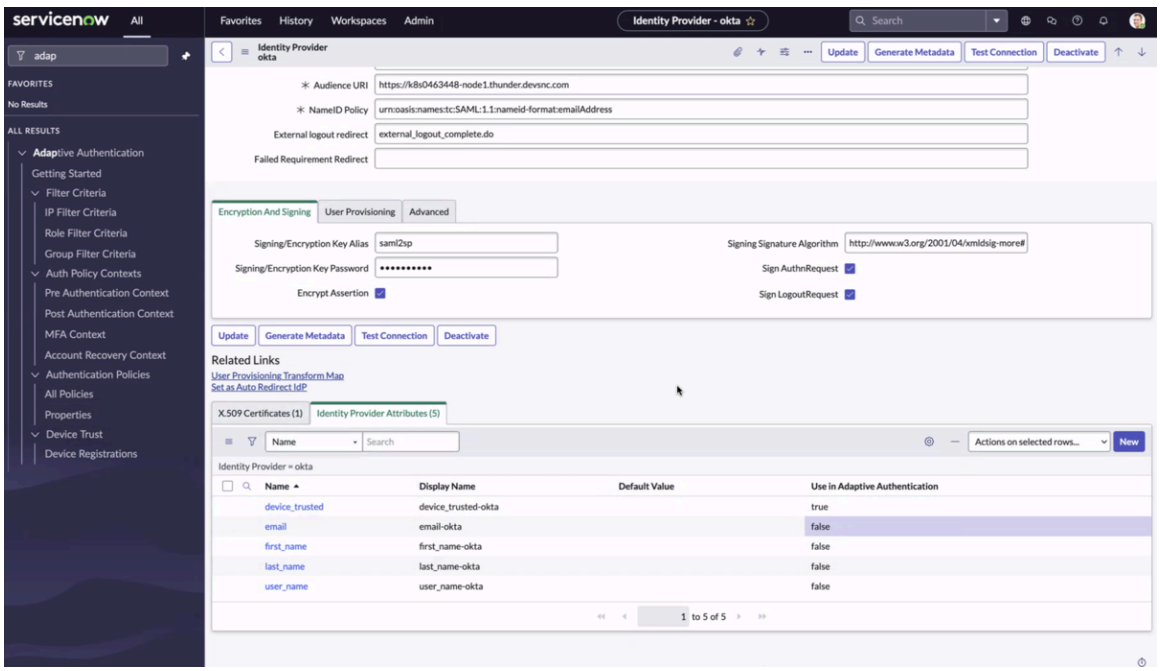
Verwenden Sie das Attribut Identitätsanbieter (IDP) aus der SAML-Antwort (Security Assertion Markup Language) als Filterkriterien für die Authentifizierungsrichtlinie.

Vorbereitungen
Erforderliche Rolle: Administrator

Sie können eine Sitzungszugriffsrichtlinie mithilfe des Richtlinienkontexts (Vorauthentifizierung, Nachauthentifizierung, Multifaktor-Authentifizierung) und Filterkriterien (Rolle, Gruppe, IP, Standort) mit Richtlinieneingaben und -Bedingungen erstellen.

Das folgende Verfahren zeigt die Schritte zum Konfigurieren des IdP-Attributs aus der SAML-Antwort als Richtlinieneingabe zur Steuerung der Authentifizierung in **Kontext Nach Der Authentifizierung** , **Kontext der Multifaktor-Authentifizierung (MFA)** , Und **Zero Trust: Richtlinienbasierter Sitzungszugriff** .

Die Okta-IDP-Attribute werden im folgenden Screenshot angezeigt. Sie sollten die Verwendung in adaptiver Authentifizierung auf „wahr“ festlegen, um sie in zu verwenden **Kontext Nach Der Authentifizierung** , **Kontext der Multifaktor-Authentifizierung (MFA)** , Und **Zero Trust: Richtlinienbasierter Sitzungszugriff** Richtlinien.



Hinweis: Richtlinien in den Abschnitten nach der Autorisierung, MFA, Zero Trust – richtlinienbasierter Sitzungszugriff werden ausgeführt, nachdem die Anwender die Anmeldeinformationen oder SSO-Antwort eingegeben haben.

Prozedur

1. Verwendung des IDP-Attributs im Kontext der Richtlinie nach der Authentifizierung.
   Beispiel: Konfigurieren, um Anmeldungen über die Okta-IDP-Attribute zu aktivieren, wenn das Gerät vertrauenswürdig ist.

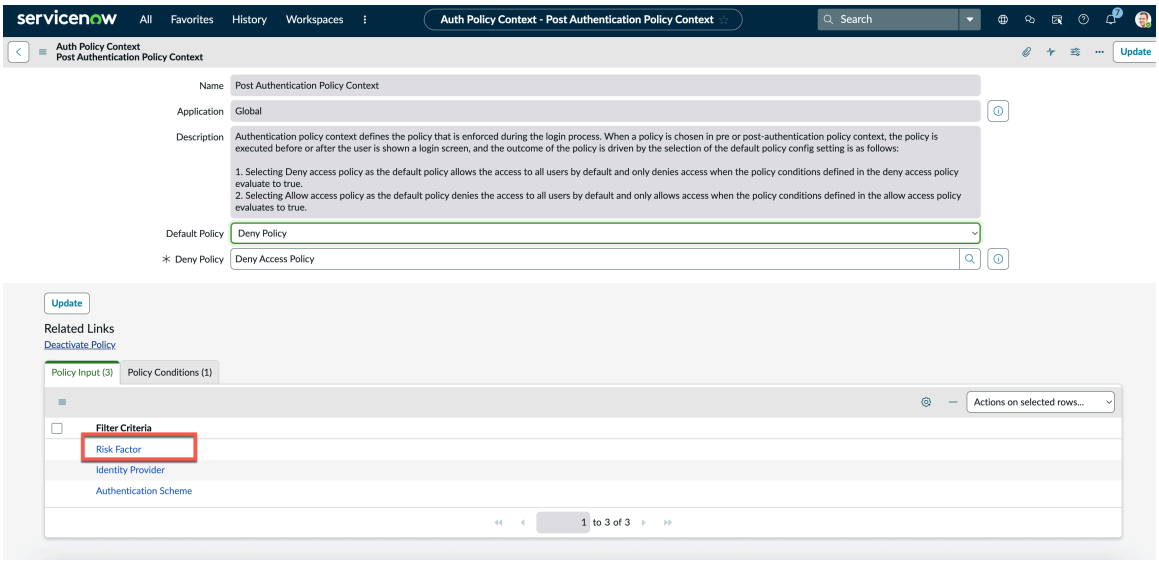
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext Der Post-Authentifizierungsrichtlinie.**an.

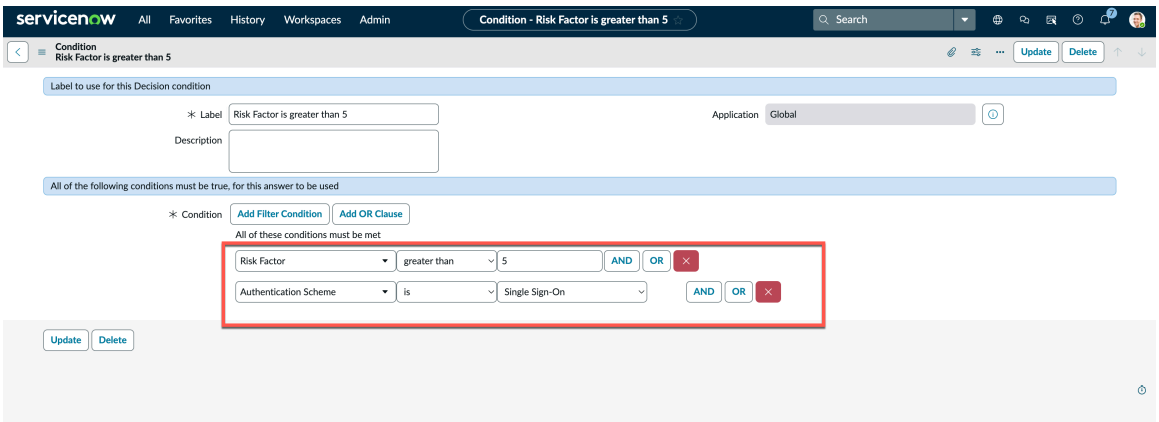
b. Wählen Sie Aus **Richtlinie Zulassen** Und öffnen Sie den Richtliniendatensatz.

c. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und Richtlinienbedingung.

- **Richtlinieneingabe** : Hinzufügen **Device_Trusted-okta** .



- **Richtlinienbedingungen** : **Device_Trusted-okta** Ist Vertrauenswürdig Und **Identitätsanbieter** Ist Okta .



Basierend auf dieser Konfiguration wird der Anwender bei der Instanz authentifiziert, wenn das Gerät von Okta (IdP) vertrauenswürdig ist.

Weitere Informationen zum Erstellen des Kontexts nach der Authentifizierung mit Richtlinie und Bedingung finden Sie unter Kontext nach der Authentifizierung.

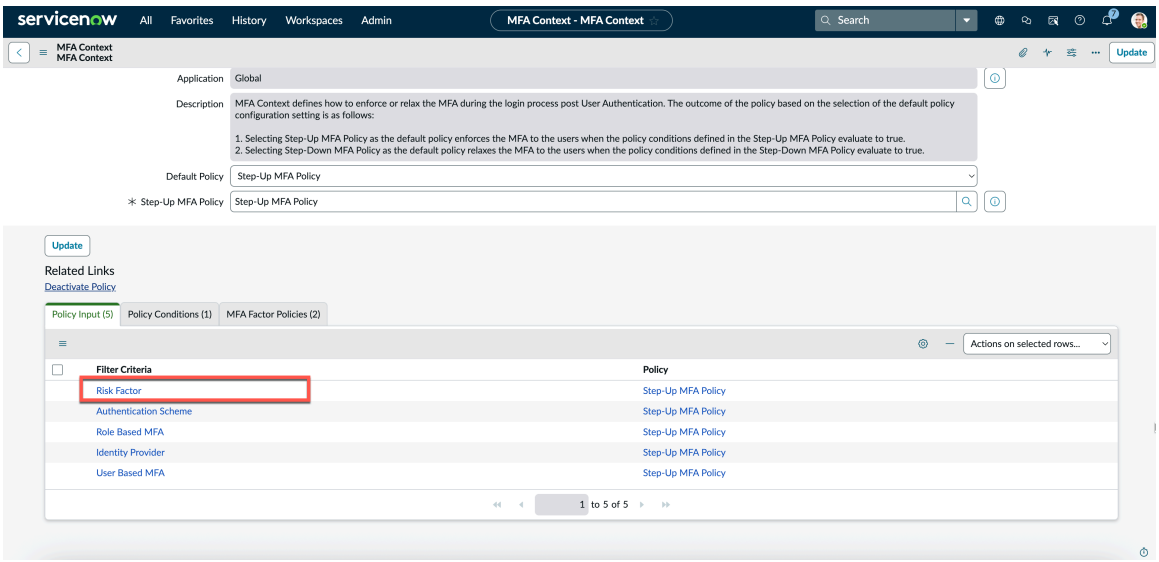
2. Verwendung des IDP-Attributs im MFA-Richtlinienkontext.
Beispiel: Konfigurieren, um MFA über die Okta-IDP-Attribute zu aktivieren, wenn das Gerät nicht vertrauenswürdig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

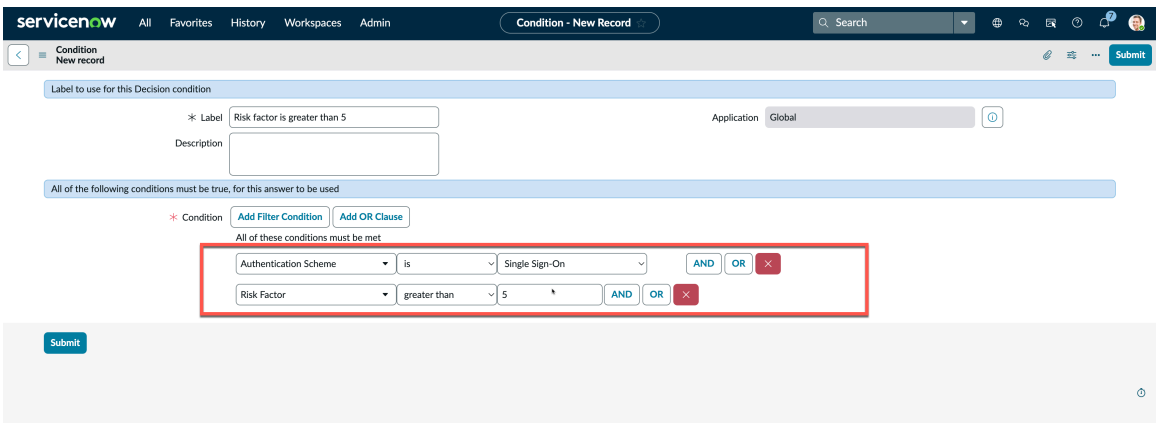
a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext der MFA-Authentifizierungsrichtlinie.**an.

b. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und Richtlinienbedingung.

- **Richtlinieneingabe** : Hinzufügen **Device_Trusted-okta** .



- **Richtlinienbedingungen** : **Device_Trusted-okta** Ist Not_Trusted Und **Identitätsanbieter** Ist Okta .



Wenn das Gerät basierend auf dieser Konfiguration nicht von Okta (IdP) vertrauenswürdig ist, zeigte der Anwender eine Authentifizierung mit einem zweiten Faktor an, um sich bei der Instanz anzumelden.

Weitere Informationen zum Erstellen eines MFA-Kontexts mit Richtlinie und Bedingung finden Sie unter Multifaktor-Authentifizierungskontext.

3. Verwendung des IDP-Attributs in Zero Trust – richtlinienbasierter Sitzungszugriff.
Beispiel: Konfigurieren, um die Berechtigung von zu reduzieren Itil Rolle aus Okta-IDP-Attributen, wenn das Gerät nicht vertrauenswürdig ist.

Automatische Übersetzung

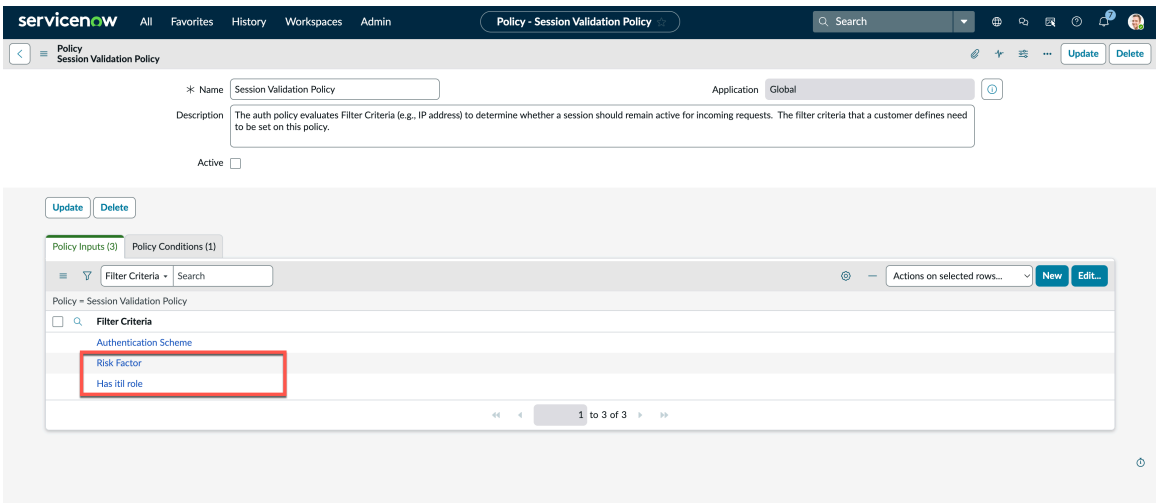
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.

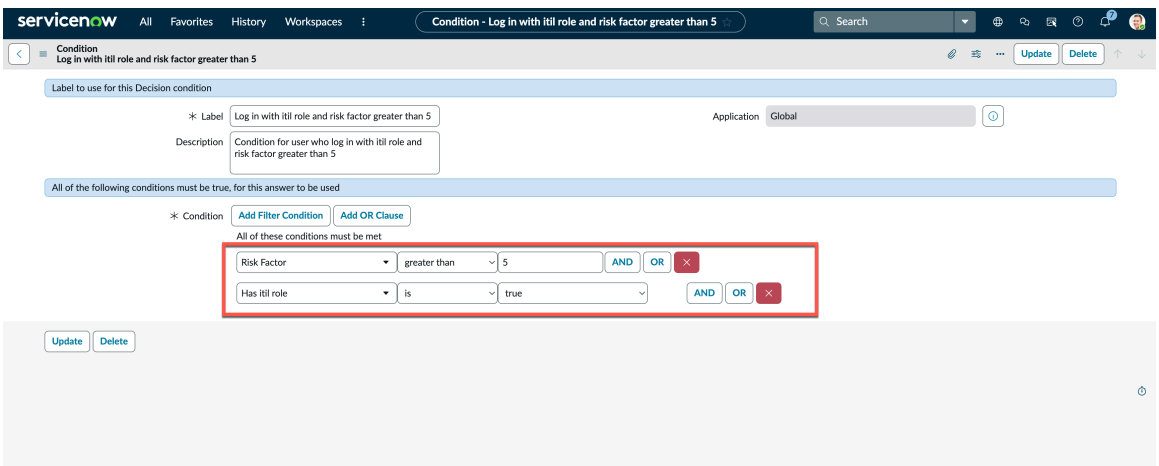
b. Erstellen Sie eine Konfiguration der Sitzungszugriffsrolle.

c. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und Richtlinienbedingung.

- **Richtlinieneingabe** : Hinzufügen **Device_Trusted-okta** Und **Hat itil-Rolle** .



- **Richtlinienbedingungen** : **Device_Trusted-okta** Ist `Not_Trusted` , **Identitätsanbieter** Ist `Okta` , Und **Hat itil-Rolle** Ist `Wahr` .



Basierend auf dieser Konfiguration, wenn `itil` Anwender, die ein Gerät verwenden, das von Okta (IdP) nicht vertrauenswürdig ist, dann werden die Berechtigungen des Anwenders für die angemeldete Sitzung eingeschränkt.

Weitere Informationen zum Erstellen des Zero Trust – richtlinienbasierten Sitzungszugriffs mit Richtlinie und Bedingung finden Sie unter Zero Trust Access (ZTA).

Identitätsanbieter-Attribute für OpenID Connect

Verwenden Sie die Attribute des Identitätsanbieters, die von OpenID Connect (OIDC) vom Identitätsanbieter (IdP) empfangen werden, als Filterkriterien für die Authentifizierung.

Sie können die IdP-Attribute manuell basierend auf den Ansprüchen erstellen, die als Teil des ID-Tokens erhalten wurden.

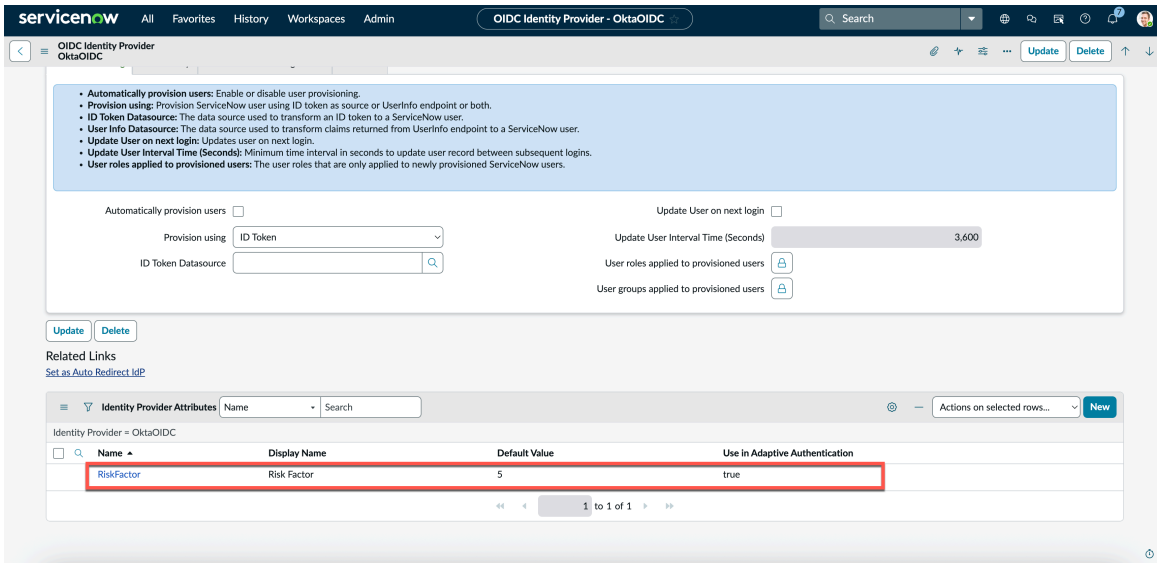
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Der Identitätsanbieter-Filter ist mit der Zero Trust-Zugriffsfunktion verfügbar. Weitere Informationen finden Sie unter Zero Trust Access (ZTA).
- IdP-Attributfilterkriterien können in verwendet werden Kontext nach der Authentifizierung, Zero Trust Access (ZTA) Sitzungsabbruch, und Multifaktor-Authentifizierungskontext.

Starten Sie die Konfiguration, indem Sie die IdP-Attribute hinzufügen, indem Sie auswählen **Neu** Aus dem Abschnitt „Attribute des Identitätsanbieters“ und verwenden Sie diese Attribute für die adaptive Authentifizierung, indem Sie sie auf festlegen `Wahr` .



Die **Risikofaktor** Definiert in der OIDC-Konfiguration in den Identitätsanbieterattributen stammt aus den ID-Token-Ansprüchen. Dieser Wert kann ein vorhandener Anspruch oder ein anwenderdefinierter Anspruch sein, wie auf der IdP-Seite konfiguriert. Verwenden Sie diesen Anspruch in verschiedenen Authentifizierungskontexten, um das Anmeldeverhalten des Anwenders anzupassen und zu steuern.

Die **Attribute Des Identitätsanbieters** Werden mit den folgenden Details angezeigt:

Formular „Standortfilterkriterien“

Feld	Beschreibung
Name	Attributname, der vom Identitätsanbieter bereitgestellt wird.
Anzeigename	Anzeigename ist der detaillierte Name, der für die Filterkriterien verwendet wird. **Hinweis:** Sie können einen lesbaren Namen als Anzeigenamen angeben. In einigen Fällen ist der von den Identitätsanbietern bereitgestellte Anzeigename lang und nicht lesbar.
Standardwert	Der Standardwert wird für die Auswertung der Filterkriterien verwendet, falls das Attribut in der SAML-Antwort fehlt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standortfilterkriterien“ (Fortsetzung)

Feld	Beschreibung
In adaptiver Authentifizierung verwenden	Option zur Verwendung des Attributs in der adaptiven Authentifizierung.

Hinweis: Attribute, die aus Azure IdP ausgefüllt werden, haben aufgrund der Namenslänge des Attributs Namen und Anzeigenamen, die auf Zeichen beschränkt sind.

Sie können auch neue Attribute hinzufügen, indem Sie auswählen **Neu** In **Attribute Des Identitätsanbieters** Abschnitt.

Wenn die Option „in adaptiver Authentifizierung verwenden“ auf „wahr“ festgelegt ist, wird das ausgewählte Attribut als Filterkriterien in den generischen Filterkriterien hinzugefügt. Beispiel: **Risk_Score** Auf festlegen `Wahr` . Auf der Seite „Allgemeine Filterkriterien“ wurde ein neuer Filter erstellt.

Verwenden Sie das Attribut des Identitätsanbieters als Filterkriterien für OIDC

Verwenden Sie das Attribut Identitätsanbieter (IDP) aus der OpenID Connect-Antwort (OIDC) als Filterkriterien für die Authentifizierungsrichtlinie.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie können eine Sitzungszugriffsrichtlinie mithilfe des Richtlinienkontexts (Vorauthentifizierung, Nachauthentifizierung, Multifaktor-Authentifizierung) und Filterkriterien (Rolle, Gruppe, IP, Standort) mit Richtlinieneingaben und -Bedingungen erstellen.

Das folgende Verfahren zeigt die Schritte zum Konfigurieren des IdP-Attributs aus der SAML-Antwort als Richtlinieneingabe zur Steuerung der Authentifizierung in **Kontext Nach Der Authentifizierung** , **Kontext der Multifaktor-Authentifizierung (MFA)** , Und **Zero Trust: Richtlinienbasierter Sitzungszugriff** .

Die Okta-IDP-Attribute werden im folgenden Screenshot angezeigt. Sie sollten die Verwendung in adaptiver Authentifizierung auf „wahr“ festlegen, um sie in zu verwenden **Kontext Nach Der Authentifizierung** , **Kontext der Multifaktor-Authentifizierung (MFA)** , Und **Zero Trust: Richtlinienbasierter Sitzungszugriff** Richtlinien.

Hinweis: Richtlinien in den Abschnitten nach der Autorisierung, MFA, Zero Trust – richtlinienbasierter Sitzungszugriff werden ausgeführt, nachdem die Anwender die Anmeldeinformationen oder SSO-Antwort eingegeben haben.

Prozedur

1. Verwendung des IDP-Attributs im Kontext der Richtlinie nach der Authentifizierung.
   Beispiel: Konfigurieren, um die Anmeldung über die Okta-IDP-Attribute zu aktivieren, wenn das Gerät vertrauenswürdig ist.

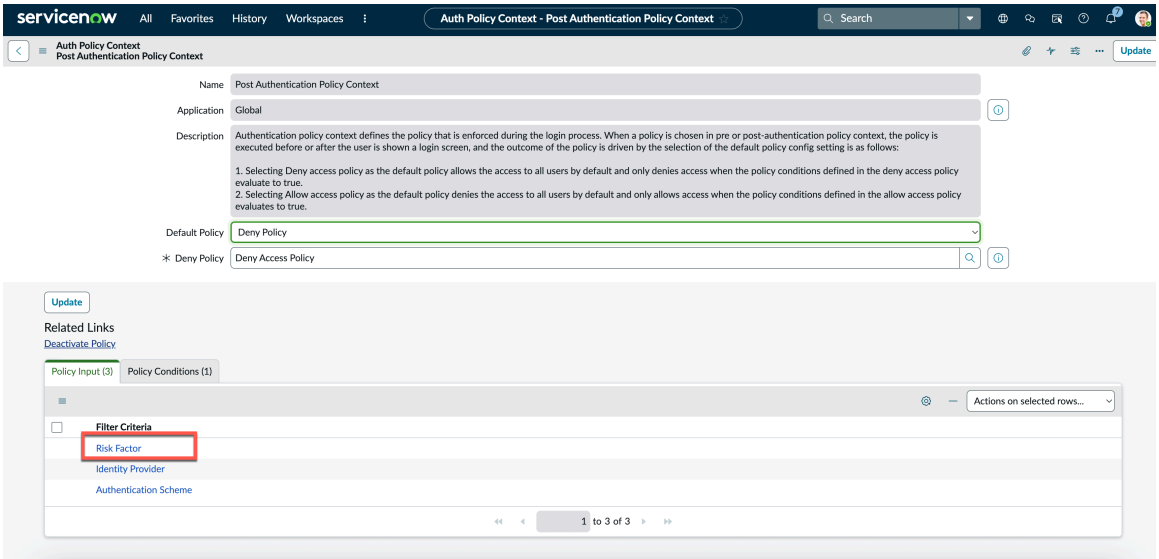
   a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext Der Post-Authentifizierungsrichtlinie.**an.

   b. Wählen Sie Aus **Richtlinie Zulassen** Und öffnen Sie den Richtliniendatensatz.

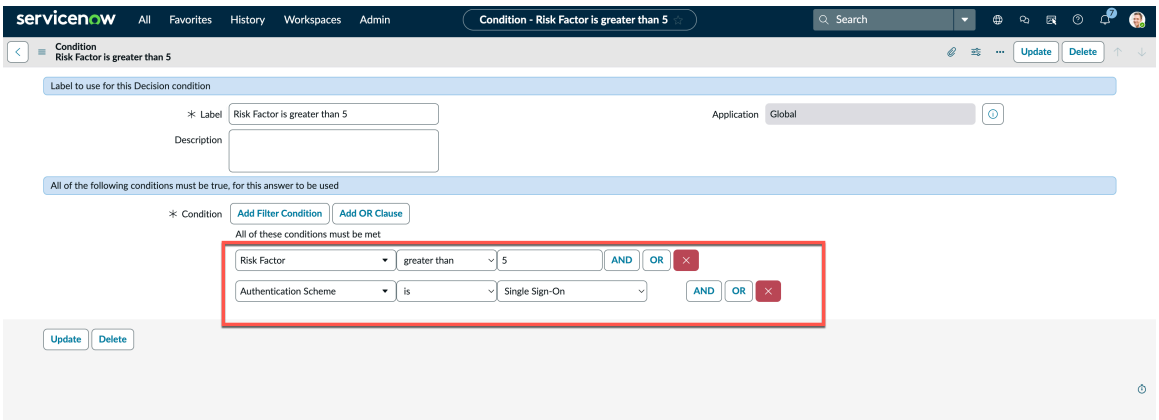
   c. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und Richtlinienbedingung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe** : Hinzufügen **Risikofaktor** .



- **Richtlinienbedingungen** : **Risikofaktor** Größer als 5 Und **Authentifizierungsschema** Ist Single Sing-On .



Basierend auf dieser Konfiguration wird der Anwender bei der Instanz authentifiziert, wenn das Gerät von Okta (IdP) vertrauenswürdig ist.

Weitere Informationen zum Erstellen des Kontexts nach der Authentifizierung mit Richtlinie und Bedingung finden Sie unter Kontext nach der Authentifizierung.

2. Verwendung des IDP-Attributs im MFA-Richtlinienkontext.
Beispiel: Konfigurieren, um MFA über die Okta-IDP-Attribute zu aktivieren, wenn das Gerät nicht vertrauenswürdig ist.

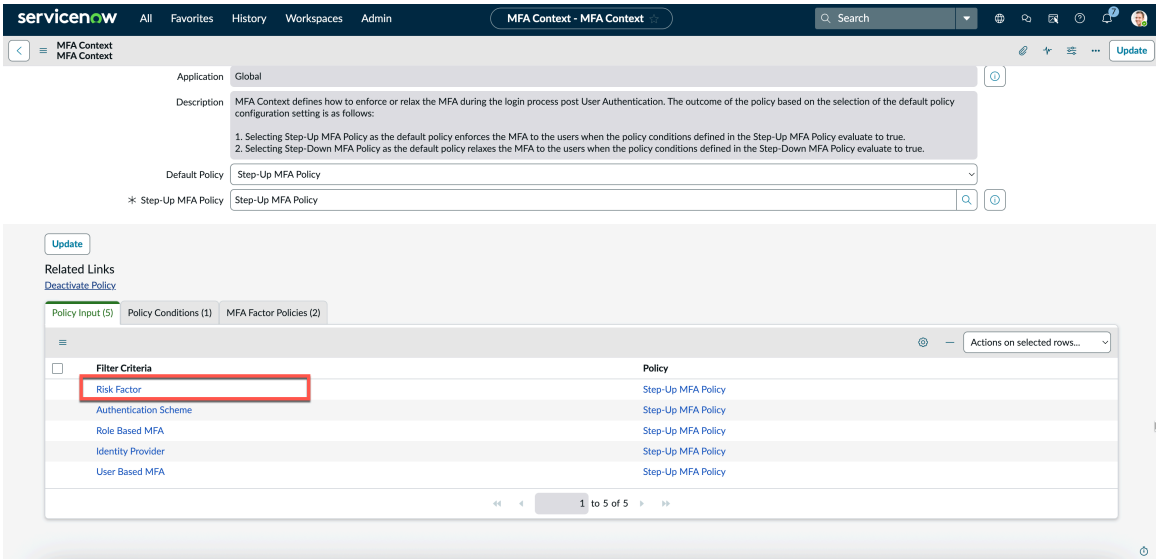
a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext der MFA-Authentifizierungsrichtlinie.**an.

b. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und Richtlinienbedingung.

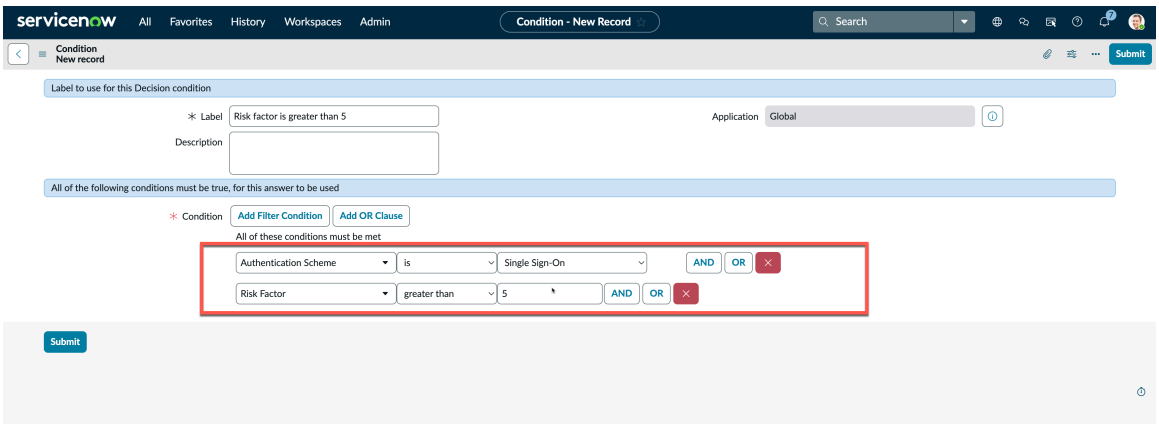
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe** : Hinzufügen **Risikofaktor** .



- **Richtlinienbedingungen** : **Risikofaktor** Größer als 5 Und **Authentifizierungsschema** Ist Single Sing-On .



Wenn das Gerät basierend auf dieser Konfiguration nicht von Okta (IdP) vertrauenswürdig ist, zeigte der Anwender eine Authentifizierung mit einem zweiten Faktor an, um sich bei der Instanz anzumelden.

Weitere Informationen zum Erstellen eines MFA-Kontexts mit Richtlinie und Bedingung finden Sie unter Multifaktor-Authentifizierungskontext.

3. Verwendung des IDP-Attributs in Zero Trust – richtlinienbasierter Sitzungszugriff.
Beispiel: Konfigurieren, um die Berechtigung von zu reduzieren Itil Rolle aus Okta-IDP-Attributen, wenn das Gerät nicht vertrauenswürdig ist.

a. Navigieren zu **Alle** > **Zero Trust-Zugriff** > **Konfigurationen der Sitzungszugriffsrolle**an.

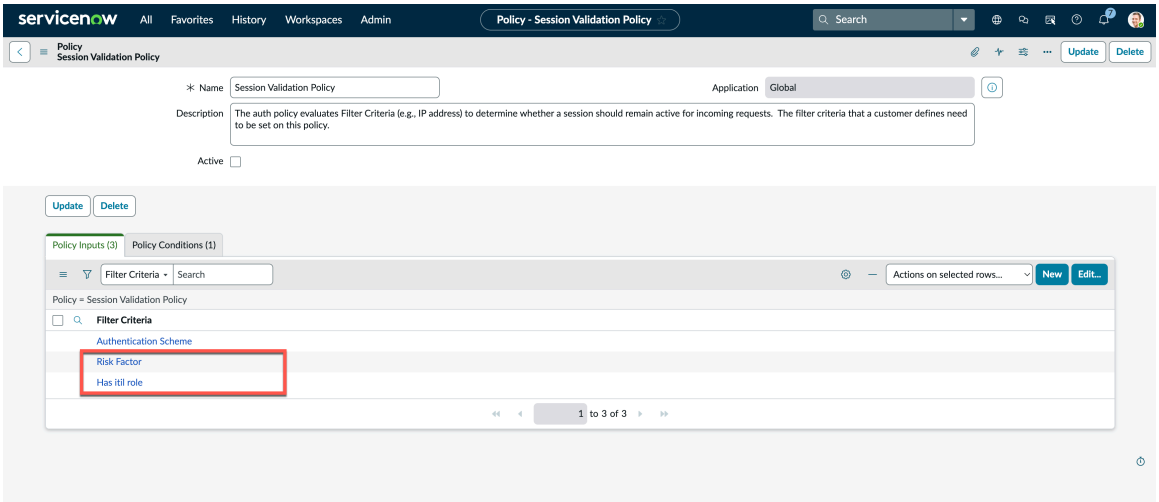
b. Erstellen Sie eine Konfiguration der Sitzungszugriffsrolle.

c. Erstellen Sie in der Richtlinieneingabe die Richtlinieneingabe und Richtlinienbedingung.

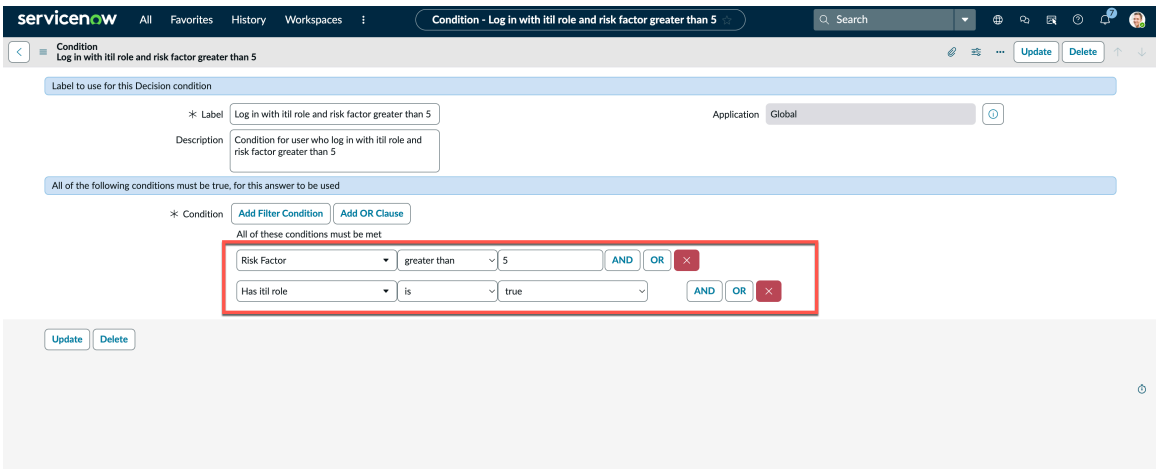
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinieneingabe** : Hinzufügen **Risikofaktor** Und **Hat itil-Rolle** .



- **Richtlinienbedingungen** : **Risikofaktor** Größer als 5 Und **Authentifizierungsschema** Ist Single Sing-On .



Basierend auf dieser Konfiguration, wenn itil Anwender, die ein Gerät verwenden, das von Okta (IdP) nicht vertrauenswürdig ist, dann werden die Berechtigungen des Anwenders für die angemeldete Sitzung eingeschränkt.

Weitere Informationen zum Erstellen des Zero Trust – richtlinienbasierten Sitzungszugriffs mit Richtlinie und Bedingung finden Sie unter Zero Trust Access (ZTA).

Kontexte der Authentifizierungsrichtlinie

Verwenden Sie Authentifizierungsrichtlinienkontexte, um zu bestimmen, wie und wann Ihre Instanz Authentifizierungsrichtlinien durchsetzt.

Authentifizierungskontexte definieren, wie und wann eine Richtlinie während des Anmeldevorgangs durchgesetzt wird. Weisen Sie einem Richtlinienkontext eine Richtlinie zu, um Eingaben und Bedingungen für die Verarbeitung der Authentifizierung durch Ihre Instanz zu definieren.

Kontext vor der Authentifizierung

Richtlinien im Vorautorisierungskontext werden ausgeführt, wenn ein Anwender zum ersten Mal auf die Instanz zugreift, bevor ein Anmeldebildschirm angezeigt wird. Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können den Vorautorisierungskontext verwenden, um den Zugriff zuzulassen oder zu verweigern, bevor Ihre Anwender basierend auf Ihrer ausgewählten Richtlinie zur Eingabe der Anmeldeinformationen aufgefordert werden. Da diese Richtlinien ausgewertet werden, bevor ein Anwender Informationen eingibt, können diese Richtlinien Kriterien wie die Rollen oder Gruppen eines Anwenders nicht berücksichtigen.

Weitere Informationen zu diesem Kontext finden Sie unter Kontext vor der Authentifizierung.

Kontext nach der Authentifizierung

Richtlinien im Kontext nach der Autorisierung werden ausgeführt, nachdem Ihre Anwender ihre Anmeldeinformationen oder SSO-Antwort eingegeben haben. Ihre Instanz ermöglicht oder verweigert den Zugriff basierend auf Ihrer ausgewählten Richtlinie. Da sich Ihre Anwender anhand ihrer Anmeldeinformationen identifiziert haben, kann die Richtlinie Anwenderinformationen verwenden, um zu bestimmen, ob Zugriff gewährt werden soll.

Weitere Informationen zu diesem Kontext finden Sie unter Kontext nach der Authentifizierung.

MFA-Kontext (Multifaktor-Authentifizierung)

Richtlinien, die dem MFA-Kontext zugewiesen sind, definieren, ob MFA während des Anmeldevorgangs erzwungen werden soll. Ob Ihre Instanz MFA erzwingt, wird durch die Konfiguration von Richtlinien in diesem Kontext bestimmt. Weitere Informationen zu diesem Kontext finden Sie unter Multifaktor-Authentifizierungskontext.

Account-Wiederherstellungskontext

Administratoren können die Accountwiederherstellung (ACR) konfigurieren, um Wiederherstellungsaktivitäten durchzuführen, z. B. die Behebung von SSO-Fehlkonfigurationen oder abgelaufenen Zertifikaten. Um die Accountwiederherstellung zu verwenden, müssen Sie mindestens einen Administratoraccount als Accountwiederherstellungsanwender registrieren. Single Sign-on kann in Ihrer Instanz erst aktiviert werden, wenn mindestens ein Account konfiguriert ist. Weitere Informationen zum Kontext, der festgelegt werden kann, finden Sie unter Account-Wiederherstellungskontext.

Kontext der Sitzungsvalidierung

Der Sitzungsvalidierungskontext kann mit dem Richtlinien-Framework für adaptive Authentifizierung verwendet werden. Das Framework verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen (Sitzung) auszuwerten und dann den Zugriff basierend auf Richtlinienbedingungen zu verweigern oder zuzulassen. Weitere Informationen finden Sie unter Sitzungsvalidierungskontext.

Standardrichtlinie

Im Richtlinienkontext können Sie eine Standardrichtlinie in definieren **Standardrichtlinie** Feld. Dieser Standard definiert, wie Ihre Instanz auf das Ergebnis Ihrer Richtlinie reagiert. Die verfügbaren Standardrichtlinienoptionen werden durch den verwendeten Kontext bestimmt. Details zu diesen Optionen finden Sie in den Dokumenten, die diese einzelnen Kontexte beschreiben.

Kontext vor der Authentifizierung

Der Richtlinienkontext vor der Authentifizierung definiert, wie und wann eine Richtlinie während des Anmeldevorgangs durchgesetzt wird. Die in diesem Kontext verwendete Richtlinie wird ausgeführt, bevor Ihre Anwender einen Anmeldebildschirm sehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatz für Kontext vor der Authentifizierung

Richtlinien im Kontext vor der Authentifizierung werden ausgeführt, wenn ein Anwender zum ersten Mal auf die Instanz zugreift, bevor er einen Anmeldebildschirm sieht.

Sie können den Kontext vor der Authentifizierung verwenden, um den Zugriff zuzulassen oder zu verweigern, bevor Ihre Anwender basierend auf Ihrer ausgewählten Richtlinie zur Eingabe der Anmeldeinformationen aufgefordert werden. Da diese Richtlinien ausgewertet werden, bevor ein Anwender Informationen eingibt, können diese Richtlinien keine Kriterien wie die Rollen oder Gruppen eines Anwenders berücksichtigen.

Verwenden Sie die Felder in **Richtlinienkontext vor der Authentifizierung** Datensatz, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Formular „Kontext vor der Authentifizierung“

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Bewertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Zulassungsrichtlinie** Verweigert standardmäßig allen Anwendern den Zugriff und lässt den Zugriff nur zu, wenn die in der ausgewählten Richtlinie Bedingungen erfüllt sind **Richtlinie Zulassen** Feld wird als „wahr“ ausgewertet. **Verweigerungsrichtlinie** Ermöglicht standardmäßig den Zugriff für alle Anwender und verweigert den Zugriff nur, wenn die Bedingungen erfüllt sind, die die Richtlinie in ausgewählt hat **Richtlinie Ablehnen** Feld wird als „wahr“ ausgewertet.
Zulassungsrichtlinie	Die Richtlinie, die für diesen Kontext verwendet wird. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **Richtlinie Zulassen** .
Verweigerungsrichtlinie	Die Richtlinie, die für diesen Kontext verwendet wird. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **Richtlinie Ablehnen** .

Hinweis:

Sie können die Kriterien IP-Filter, Trusted Mobile App-Filter und Standortfilter nur im Kontext der Richtlinie vor der Authentifizierung verwenden.

Richtlinieneingaben und -Bedingungen

Die **Richtlinieneingabe** Und **Richtlinienbedingungen** Registerkarten zeigen die Eingaben und Bedingungen der in ausgewählten Richtlinie an **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -Bedingungen verwendet werden. Um Ihre Richtlinie zu ändern, navigieren Sie über das Referenzsymbol (zur Richtlinie) Neben **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld.

Dieses Beispiel zeigt einen Richtlinienkontextdatensatz vor der Authentifizierung, der standardmäßig so konfiguriert ist, dass der Zugriff verweigert wird. Der Kontext verwendet eine Richtlinie namens **Zugriffsrichtlinie verweigern** . Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die in angezeigt werden **Richtlinieneingabe** Und **Richtlinienbedingung** Registerkarten.

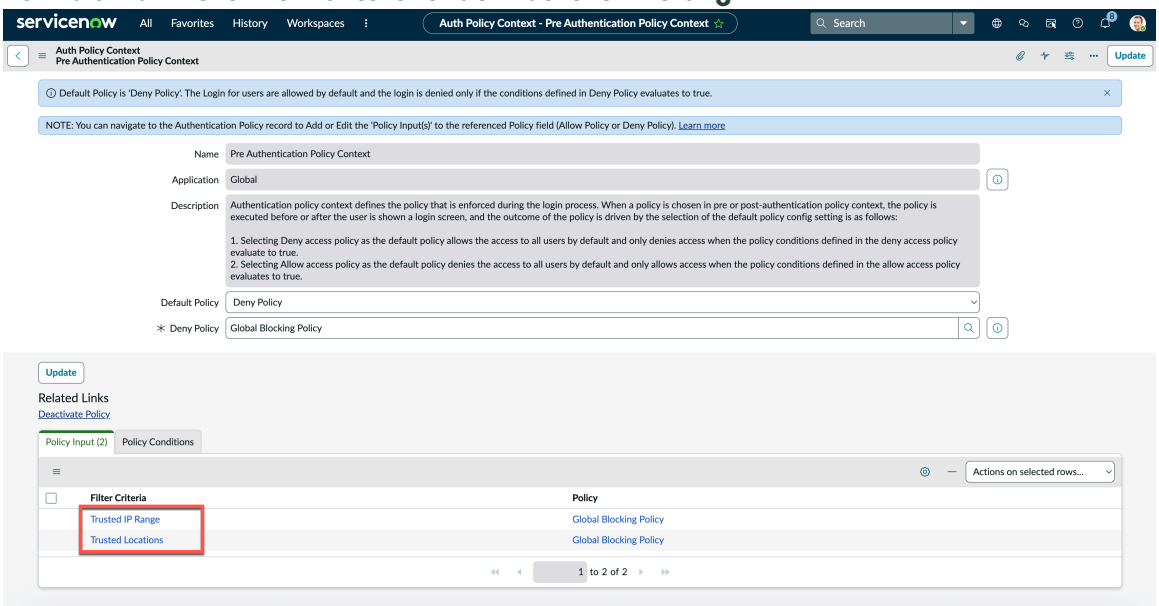
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Im Richtlinienkontext vor der Authentifizierung können nur IP-basierte Filter, standortbasierte Filter oder vertrauenswürdige Mobile-App-Filter verwendet werden.
- Immer wenn ein Vorauthentifizierungssatz mit nicht absoluten Bedingungen oder Filterkriterien vorhanden ist, wird eine Fehlermeldung angezeigt, die angibt, dass die Richtlinie oder der Kontext nicht konfiguriert werden kann. Es wird empfohlen, alle Eingaben für den Kontext vor der Authentifizierung zu validieren, bevor er in der Instanz ausgeführt wird.

  Beispiel: Wenn sich der Administrator außerhalb des vertrauenswürdigen Netzwerks befindet und den Kontext vor der Authentifizierung mit IP-Bereichen konfiguriert und die IP-Bereiche nicht mit der aktuellen Sitzung des Administrators übereinstimmen, wird der Administrator blockiert.

Formular für Richtlinienkontext vor der Authentifizierung



Kontext nach der Authentifizierung

Der Richtlinienkontext nach der Authentifizierung definiert, wie und wann eine Richtlinie während des Anmeldevorgangs durchgesetzt wird. Die in diesem Kontext verwendete Richtlinie wird ausgeführt, nachdem Ihre Anwender einen Anmeldebildschirm sehen.

Kontextdatensatz nach der Authentifizierung

Richtlinien im Kontext nach der Autorisierung werden ausgeführt, nachdem Ihre Anwender ihre Anmeldeinformationen oder SSO-Antwort eingegeben haben. Ihre Instanz ermöglicht oder verweigert den Zugriff basierend auf Ihrer ausgewählten Richtlinie. Da sich Ihre Anwender anhand ihrer Anmeldeinformationen identifiziert haben, kann die Richtlinie Anwenderinformationen wie Rolle oder Gruppe verwenden, um zu bestimmen, ob Zugriff gewährt werden soll.

Verwenden Sie die Felder im Richtlinienkontextdatensatz nach der Authentifizierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Kontext nach der Authentifizierung

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Bewertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Zulassungsrichtlinie** Verweigert standardmäßig allen Anwendern den Zugriff und lässt den Zugriff nur zu, wenn die in der ausgewählten Richtlinie Bedingungen erfüllt sind **Richtlinie Zulassen** Feld wird als „wahr“ ausgewertet. **Verweigerungsrichtlinie** Ermöglicht standardmäßig den Zugriff für alle Anwender und verweigert den Zugriff nur, wenn die Bedingungen erfüllt sind, die die Richtlinie in ausgewählt hat **Richtlinie Ablehnen** Feld wird als „wahr“ ausgewertet.
Zulassungsrichtlinie	Die Richtlinie, die für diesen Kontext verwendet wird. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **Richtlinie Zulassen** .
Verweigerungsrichtlinie	Die Richtlinie, die für diesen Kontext verwendet wird. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **Richtlinie Ablehnen** .

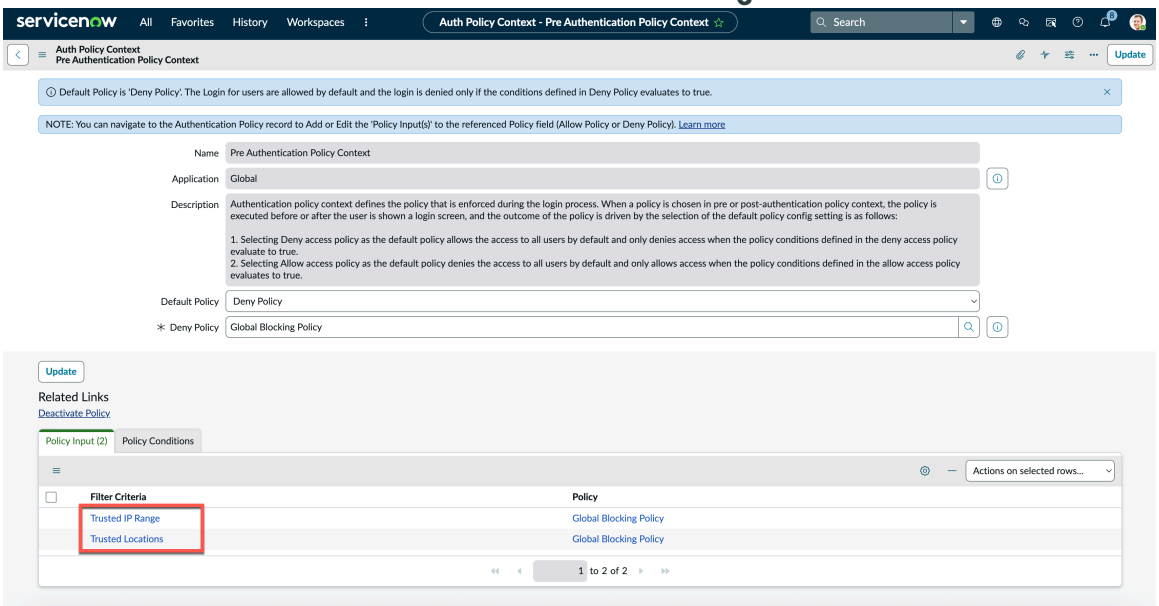
Richtlinieneingaben und -Bedingungen

Die **Richtlinieneingabe** Und **Richtlinienbedingungen** Registerkarten zeigen die Eingaben und Bedingungen der in ausgewählten Richtlinie an **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -Bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie über das Referenzsymbol (zur Richtlinie) Neben **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld.

Dieses Beispiel zeigt einen Richtlinienkontextdatensatz nach der Authentifizierung, der standardmäßig so konfiguriert ist, dass der Zugriff verweigert wird. Der Kontext verwendet eine Richtlinie namens **Zugriffsrichtlinie verweigern** . Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die in angezeigt werden **Richtlinieneingabe** Und **Richtlinienbedingung** Registerkarten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Richtlinienkontext nach der Authentifizierung



Multifaktor-Authentifizierungskontext

Der Richtlinienkontext für Multifaktor-Authentifizierung (MFA) verwendet eine Richtlinie, um zu definieren, wie und wann MFA während des Anmeldevorgangs erzwungen wird.

MFA-Kontextdatensatz

Der MFA-Richtlinienkontext definiert, ob Ihre Anwender bei der Anmeldung eine zweite Form der Authentifizierung bereitstellen müssen. Dieser Kontext verweigert nicht den Zugriff auf Ihre Instanz als Richtlinien nach der Authentifizierung und vor der Authentifizierung. Die in diesem Kontext ausgewählte Richtlinie hat Vorrang vor Anwender- oder rollenbasierten Konfigurationen für die Multifaktor-Authentifizierung.

Um auf den MFA-Kontext zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.

Verwenden Sie die Felder im Richtlinienkontextdatensatz nach der Authentifizierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

Hinweis:

- Wenn die Standardrichtlinie ist **STEP-up-MFA-Richtlinie** , Anwender werden mit Multifaktor-Authentifizierung angezeigt, wenn die Richtlinie in konfiguriert ist **STEP-up-MFA-Richtlinie** Wird als „wahr“ ausgewertet. Richtlinie hat Vorrang vor der Anwender- oder rollenbasierten Konfiguration.
- MFA mit SSO-Anmeldung ist nur verfügbar, wenn `glide.authenticate.mfa.with.multisso.enabled` Eigenschaft ist auf „wahr“ festgelegt.
- Sie können zum Datensatz der Authentifizierungsrichtlinie navigieren, um „Richtlinieneingabe(en)“ zum Feld „Referenzierte Richtlinie“ hinzuzufügen oder zu bearbeiten (**STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie**).
- Die MFA-Kontextrichtlinie gilt nur für Anwenderanmeldungen. Sie gilt nicht für die API-Authentifizierung, die Standardauthentifizierung und die Erteilung von Anmeldeinformationen für das Passwort des OAuth-Ressourcenbesitzers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA-Kontextformular

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Bewertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Step-Up-MFA-Richtlinie** Erzwingt MFA für Anwender, wenn die Richtlinienbedingungen in definiert sind **STEP-up-MFA-Richtlinie** Feld wird als „wahr“ ausgewertet. **Step-Down-MFA-Richtlinie** Erzwingt standardmäßig MFA. MFA wird nur dann erzwungen, wenn die Richtlinienbedingungen in definiert sind **STEP-Down-MFA-Richtlinie** Feld wird als „wahr“ ausgewertet.
Step-Up-MFA-Richtlinie	Die Richtlinie, die für diesen Kontext verwendet wird. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **STEP-up-MFA-Richtlinie** .
Step-Down-MFA-Richtlinie	Die Richtlinie, die für diesen Kontext verwendet wird. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **STEP-Down-MFA-Richtlinie** .

Richtlinieneingaben und -Bedingungen

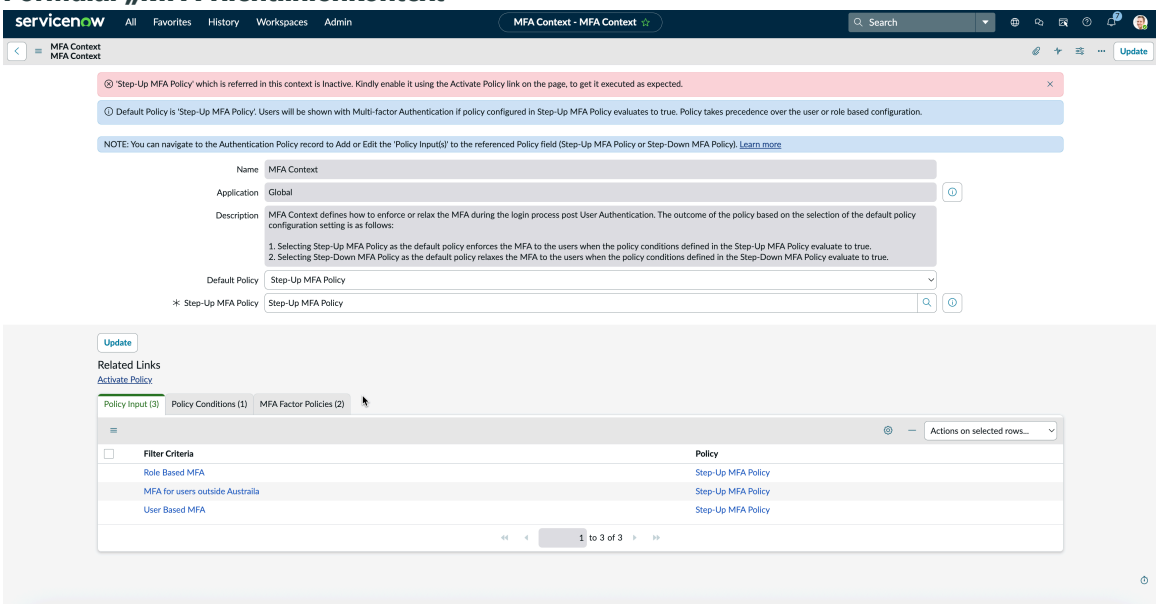
Die **Richtlinieneingabe** Und **Richtlinienbedingungen** Registerkarten zeigen die Eingaben und Bedingungen der in ausgewählten Richtlinie an **STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie** Feld. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -Bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie über das Referenzsymbol (zur Richtlinie ⓘ) Neben **STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie** Feld.

Hinweis: Richtlinienbedingungen können von hier aus erstellt werden, es wird jedoch empfohlen, neue Richtlinienbedingungen auf der Richtlinienseite hinzuzufügen.

Dieses Beispiel zeigt einen MFA-Kontextdatensatz, der mit einer Step-up-MFA-Richtlinie konfiguriert wurde. Diese Standardrichtlinie bedeutet, dass MFA nur erzwungen wird, wenn die in der Richtlinie definierten Bedingungen als „wahr“ ausgewertet werden. Der Kontext verwendet eine Richtlinie namens **STEP-up-MFA-Richtlinie** . Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die in angezeigt werden **Richtlinieneingabe** Und **Richtlinienbedingung** Registerkarten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „MFA-Richtlinienkontext“



MFA-Faktorrichtlinien

MFA-Faktorrichtlinien sind eine kritische Komponente der Sicherheitslage einer Organisation, sodass Sie zusätzliche Verifizierungsschritte über Passwörter hinaus erzwingen können. Diese Richtlinien definieren die Authentifizierungsmethoden, die Anwender für den Zugriff verwenden müssen, und bieten einen flexiblen und anpassbaren Ansatz für die Authentifizierung. Weitere Informationen finden Sie unter Richtlinien für Multifaktor-Authentifizierungsfaktor.

Account-Wiederherstellungskontext

Der Account-Wiederherstellungskontext verwendet eine Richtlinie, um zu definieren, wie und wann die Account-Wiederherstellung eingerichtet werden kann.

Administratoren können diesen Kontext und die zugehörige Richtlinie anzeigen und ändern, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Kontext der Accountwiederherstellung**an.

Hinweis: Standardmäßig lautet die Richtlinie **Richtlinie Zulassen** . Die Anmeldung für Anwender ist standardmäßig eingeschränkt, und die Anmeldung ist nur zulässig, wenn die Bedingungen in definiert sind **Richtlinie Zulassen** Wird als „wahr“ ausgewertet.

Verwenden Sie die Felder im Kontext der Accountwiederherstellung, um zu definieren, wie Ihre Instanz die Richtlinie verwendet.

Kontenwiederherstellungskontextformular

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Bewertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

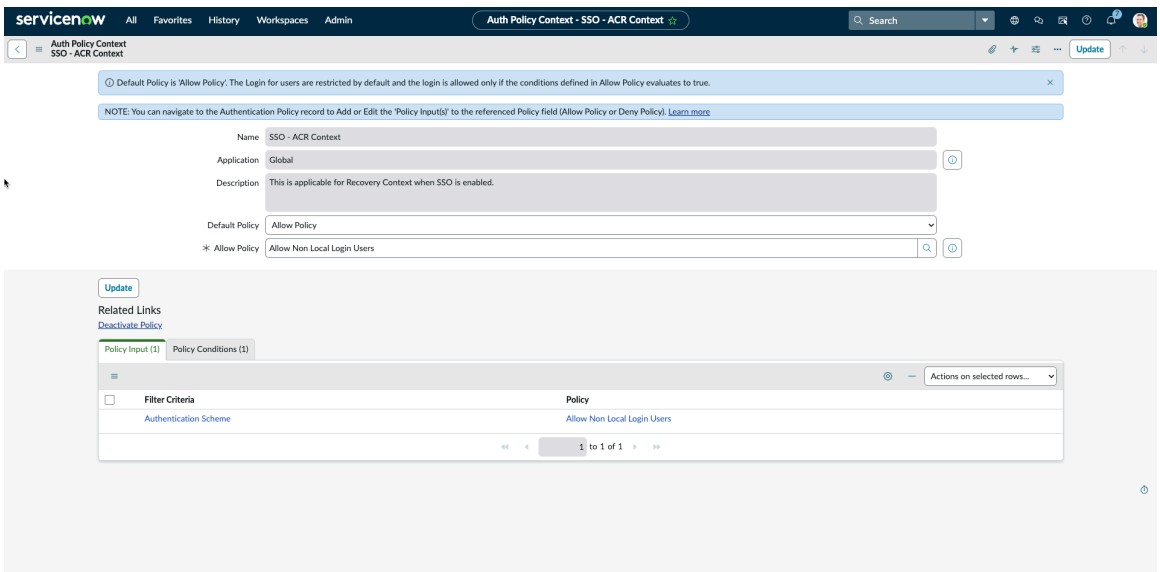
Kontenwiederherstellungskontextformular (Fortsetzung)

Feld	Beschreibung
	• Zulassungsrichtlinie • Verweigerungsrichtlinie
Zulassungsrichtlinie	Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **Richtlinie Zulassen** .
Verweigerungsrichtlinie	Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **Richtlinie Ablehnen** .

Richtlinieneingaben und -Bedingungen

Die **Richtlinieneingabe** Und **Richtlinienbedingungen** Registerkarten zeigen die Eingaben und Bedingungen der in ausgewählten Richtlinie an **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -Bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie über das Informationssymbol neben zur Richtlinie **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld.

Hinweis: Richtlinienbedingungen können von hier aus erstellt werden, es wird jedoch empfohlen, neue Richtlinienbedingungen auf der Richtlinienseite hinzuzufügen.



Sitzungsvalidierungskontext

Verwenden Sie den Sitzungsvalidierungskontext als zusätzliche Schutzebene gegen Sitzungs- oder Cookie-Hijacking.

Sie können den Sitzungsvalidierungskontext mit verwenden Adaptive Authentifizierung Richtlinien-Framework. Das Framework verwendet Authentifizierungsrichtlinien, um Authentifizierungsanforderungen auszuwerten, und verweigert dann entweder den Zugriff oder lässt ihn basierend auf Richtlinieneingaben und -Bedingungen zu.

Die Kontextrichtlinie für Sitzungsvalidierung kann in Verbindung mit der Richtlinie nach der Authentifizierung verwendet werden, bei der ein Administrator während der angemeldeten Sitzung IP-Einschränkungen für bestimmte oder alle Anwender erzwingen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Funktion „Sitzungsvalidierungskontext“ wertet die IP-Adressen basierend auf den von Ihnen festgelegten Bedingungen aus und ermöglicht den Zugriff auf die Instanz innerhalb einer Sitzung. Die Ergebnisse des Sitzungsvalidierungskontexts lauten wie folgt:

- Richtlinie verweigern: Wenn Sie die Richtlinie „Zugriff verweigern“ als Standardrichtlinie auswählen, können Anwender die Sitzung standardmäßig fortsetzen. Die Sitzung wird nur beendet, wenn eine der in der Richtlinie „Zugriff verweigern“ definierten Richtlinienbedingungen als „wahr“ ausgewertet wird.
- Allow-Richtlinie: Wenn Sie als Standardrichtlinie Zugriffsrichtlinie zulassen auswählen, wird die Anwendersitzung sofort beendet, es sei denn, eine der in der Richtlinie „Allow Access“ definierten Richtlinienbedingungen wird als „wahr“ ausgewertet.

Hinweis:

- Der Sitzungsvalidierungskontext für eine Authentifizierungsrichtlinie ist auf festgelegt **Richtlinie Zulassen** Standardmäßig.
- Der Kontext der Sitzungsvalidierung wird über die Allow-Richtlinie implementiert. Es wird nicht empfohlen, den Kontext auf „Richtlinie ablehnen“ festzulegen.

Der Kontext der Sitzungsvalidierung basiert auf dem folgenden Mechanismus:

- Erfasst die IP-Adresse des Anwenders bei der Sitzungserstellung aus einer Anwenderanforderung und speichert sie in der Sitzung und Datenbank.
- Lehnt eine Anforderung ab, wenn ihre IP-Adresse von der in der Sitzung oder außerhalb der vom Kunden definierten gültigen IP-Bereiche abweicht, die Sie definiert haben.

Hinweis: Der Sitzungsvalidierungskontext ist:

- Nur für authentifizierte Anwender verfügbar.
- Gilt nicht für Gastanwendersitzungen oder native mobile Apps.
- Optional und basierend auf der Anforderung, dass es konfiguriert werden kann.
- Wird nur für die Anforderungen nach der Anmeldung ausgeführt.

Vorteile der Sitzungsvalidierung

Der Sitzungsvalidierungskontext bietet die folgenden Vorteile:

- Beschränkt den Zugriff auf ServiceNow® Wenn Hijacker die Sitzungscookies eines Anwenders von einem Gerät auf ein anderes kopieren, um die Identität der Sitzung anzunehmen.
- Schränkt den Sitzungszugriff des Anwenders ein, wenn er ein unsicheres Netzwerk verwendet.
- Konfiguriert die verschiedenen Regeln und IP-Bereiche nach Anwendergruppe oder Rolle für Anwenderanmeldungen.

Datensatz für Sitzungsvalidierungskontext

Richtlinien im Kontext der Sitzungsvalidierung führen Anforderungen nach der Anmeldung aus.

Verwenden Sie die Felder im Datensatz für den Richtlinienkontext der Sitzungsvalidierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Sitzungsvalidierungskontext

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts.
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Bewertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Zulassungsrichtlinie** Verweigert standardmäßig allen Anwendern den Zugriff und lässt nur dann Zugriff zu, wenn die Bedingungen in der festgelegt sind **Richtlinie Zulassen** Feld wird als „wahr“ ausgewertet. **Verweigerungsrichtlinie** Ermöglicht standardmäßig den Zugriff für alle Anwender und verweigert den Zugriff nur, wenn die Bedingungen in der festgelegt sind **Richtlinie Ablehnen** Feld wird als „wahr“ ausgewertet.
Zulassungsrichtlinie	Die für diesen Kontext verwendete Richtlinie. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **Richtlinie Zulassen** .
Verweigerungsrichtlinie	Die für diesen Kontext verwendete Richtlinie. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **Richtlinie Ablehnen** .

Sie können auswählen **Richtlinie Zur Sitzungsvalidierung** Als Richtlinie zulassen oder Richtlinie ablehnen basierend auf der Richtlinieneingabe und den Richtlinienbedingungen.

Hinweis:

Sie können nur die Filterkriterien IP, Rolle und Gruppe für die Richtlinie „Sitzungsvalidierung“ verwenden.

Richtlinieneingaben und -Bedingungen

Die **Richtlinieneingabe** Und **Richtlinienbedingungen** Registerkarten zeigen die Eingaben und Bedingungen der in ausgewählten Richtlinie an **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -Bedingungen verwendet werden. Um Ihre Richtlinie zu ändern, navigieren Sie über das Referenzsymbol (zur Richtlinie ⓘ) Neben **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld.

Aktivieren Sie Den Sitzungsvalidierungskontext

Verwenden Sie den Sitzungsvalidierungskontext, um den Zugriff auf einzuschränken ServiceNow® Wenn Hijacker die Sitzungscookies eines Anwenders von einem Gerät auf ein anderes kopieren, um die Identität der Sitzung anzunehmen, oder den Sitzungszugriff des Anwenders einschränken, wenn sie ein unsicheres Netzwerk verwenden.

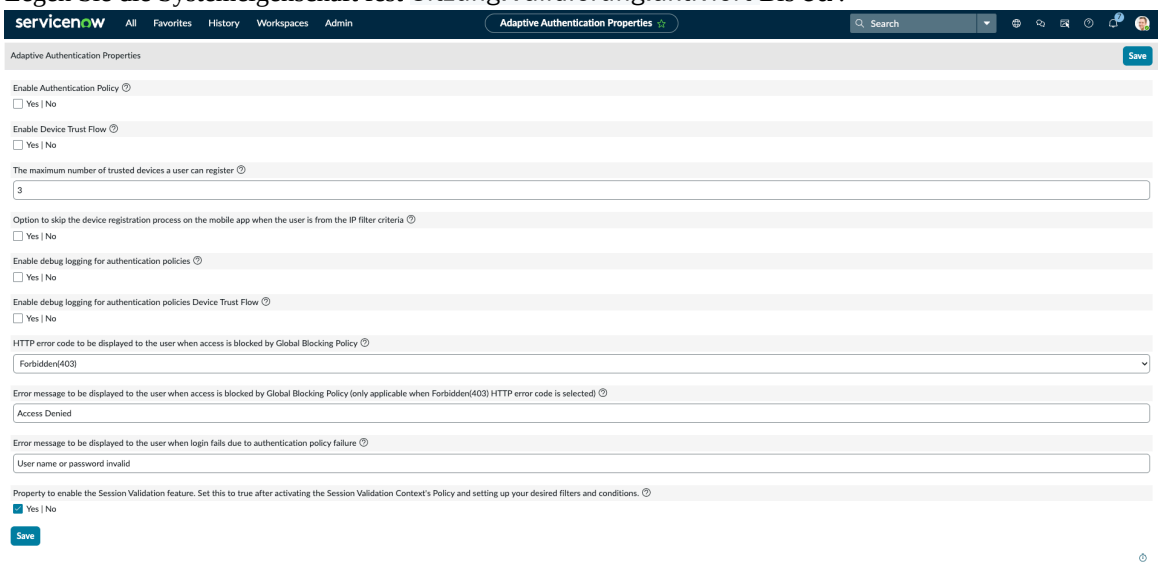
Vorbereitungen
Erforderliche Rolle: Administrator

Um die Sitzungsvalidierung zu verwenden, müssen Sie die folgenden Schritte ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.
2. Wählen Sie aus **Richtlinie Zur Sitzungsvalidierung** In den Richtlinien (sys_Authentication_Policy_list.do) Seite.
3. Geben Sie an **Richtlinieneingaben** Und **Richtlinienbedingungen** .
4. Legen Sie die Bedingungen auf fest **Wahr** Oder **Falsch** Für die Filter, die Sie hinzugefügt haben.
5. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der Richtlinie, nachdem Sie die Sitzungsvalidierungsrichtlinie mit Richtlinieneingaben und -Bedingungen eingerichtet haben.
6. Wählen Sie ein aus **AuthnRequest erzwingen** Kontrollkästchen für den Standard-Identitätsanbieter in der Tabelle „sso_properties“, wenn für die Instanz SSO konfiguriert ist.
7. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**an.
8. Legen Sie die Systemeigenschaft fest `Sitzung.Validierung.aktiviert` Bis **Ja** .



Ergebnis

Die Sitzungsvalidierungsfunktion ist aktiviert. Sie können die Richtlinieneingaben und -Bedingungen für die Richtlinie konfigurieren, um die Funktion zu verwenden. Weitere Informationen finden Sie unter Tutorial: Sitzungsvalidierung Konfigurieren.

Tutorial: Sitzungsvalidierung Konfigurieren

Konfigurieren Sie die Sitzungsvalidierung im Framework für adaptive Authentifizierung, um als zusätzliche Schutzebene für Sitzungs- oder Cookie-Hijacking bereitzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

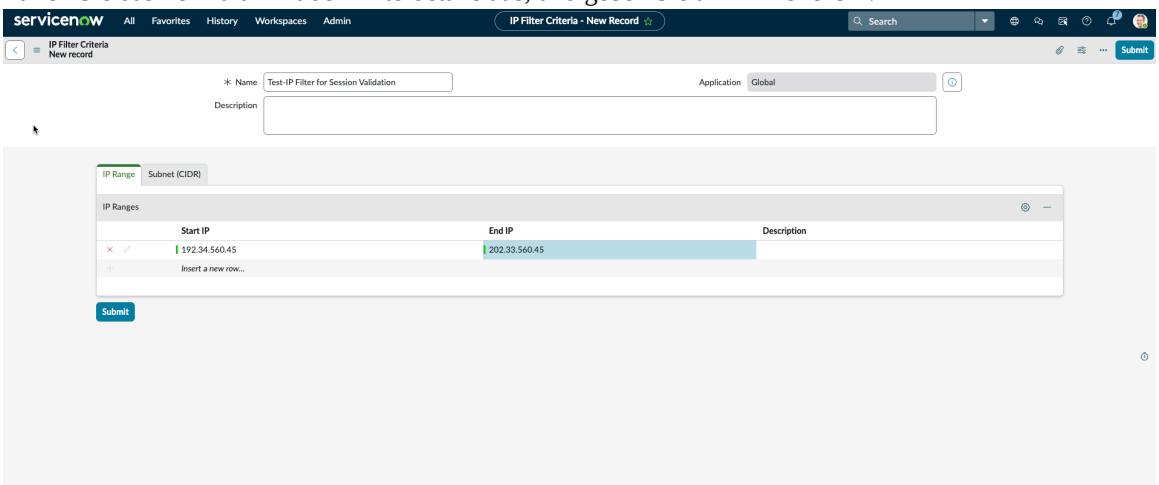
Plugin erforderlich: **Adaptive Authentifizierung** (Com.snc.adaptive_authentication)

Um die Sitzungsvalidierung zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.
2. Wählen Sie aus **Richtlinie Zur Sitzungsvalidierung** In den Richtlinien (sys_Authentication_Policy_list.do) Seite.
3. Wählen Sie Aus **Richtlinieneingaben** .
   a. Wählen Sie Aus **Neu** Oder **Bearbeiten** .
   b. Wählen Sie die Art der Richtlinieneingabe (Filterkriterien) aus, die Sie erstellen möchten. Verfügbare Optionen sind IP-, Rollen- und Gruppenfilterkriterien. Wählen wir aus **IP-Filterkriterien** .
   c. Füllen Sie das Formular mit den Filterdetails aus, und geben Sie an **IP-Bereich** .



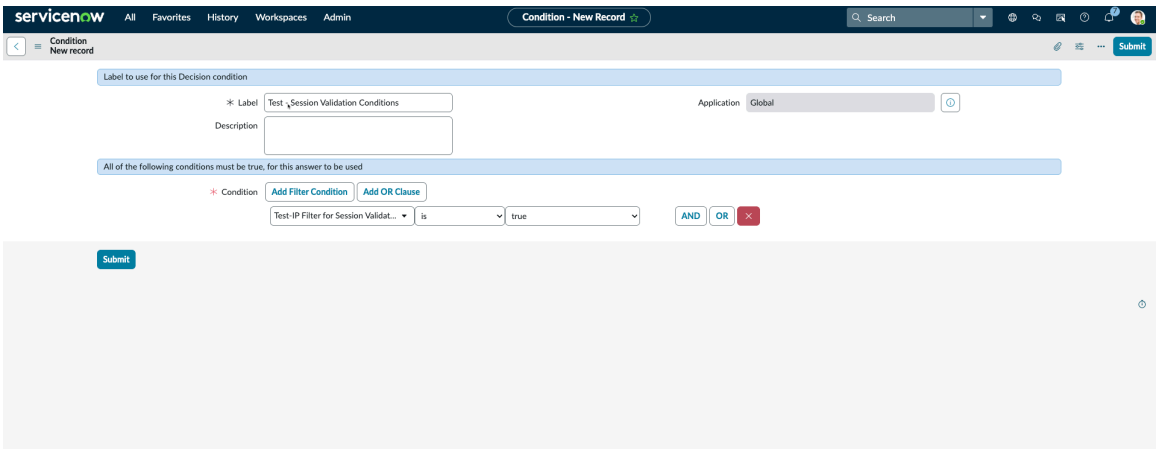
Weitere Informationen zum Erstellen eines IP-Filters finden Sie unter Erstellen Sie IP-Filterkriterien.

   d. Wählen Sie **Absenden**.
4. Wählen Sie Aus **Richtlinienbedingungen** Auf der Seite „Sitzungsvalidierungsrichtlinie“.
   a. Wählen Sie **Neu**.
   b. Füllen Sie das Formular aus, und legen Sie die Bedingung für die Richtlinieneingabe fest.

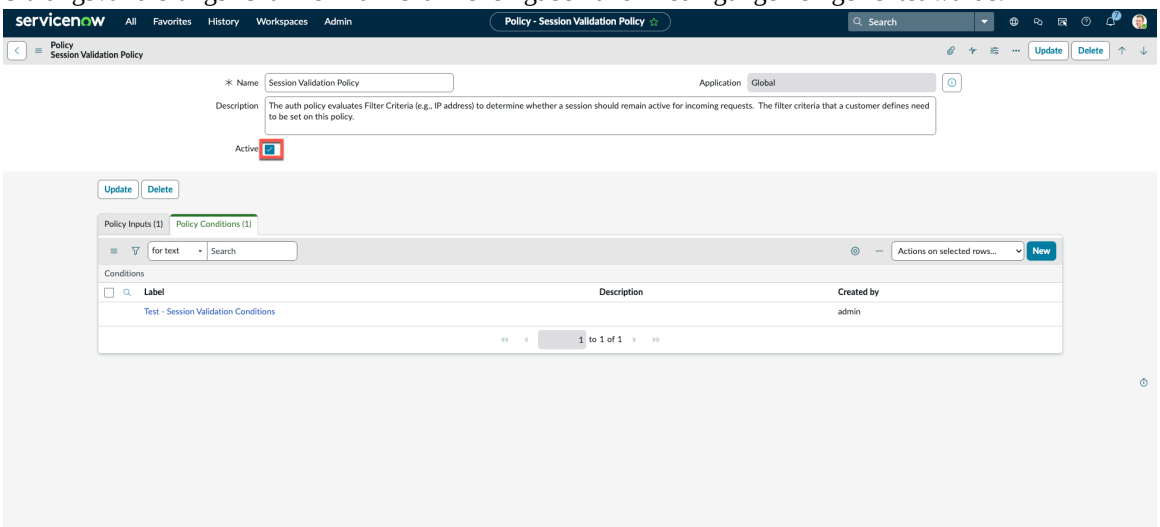
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können die Bedingungen auf festlegen `Wahr` Oder `Falsch` Basierend auf der Konfiguration der Richtlinieneingabe. In diesem Beispiel ist er auf festgelegt `Wahr` . Wenn Sie die Bedingung in diesem Fall auf „wahr“ festlegen, kann sich nur der Anwender mit der konfigurierten IP-Adresse anmelden.

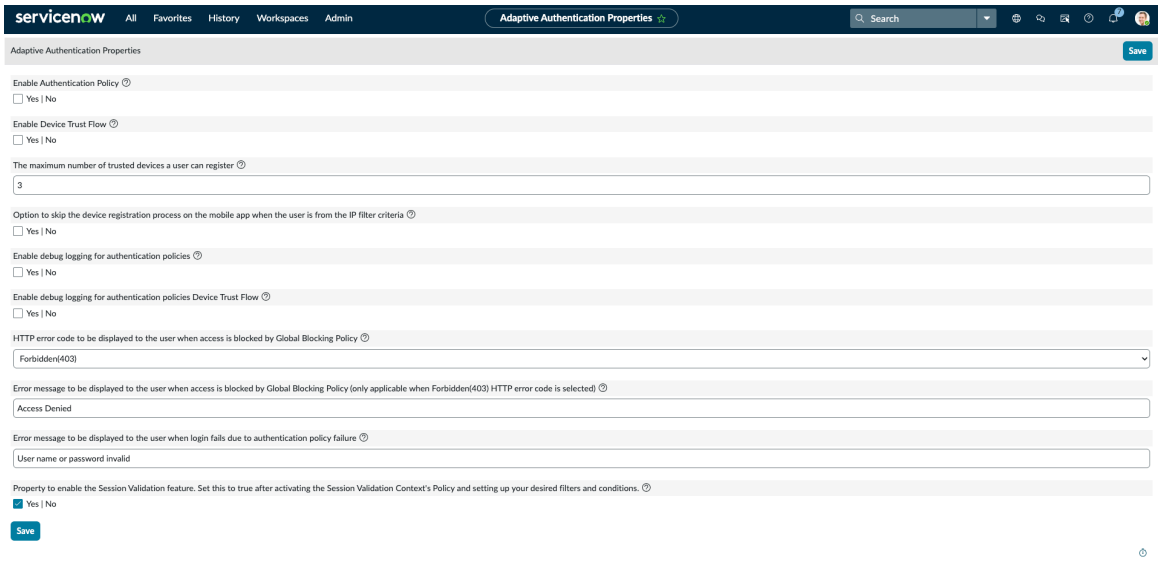


5. Wählen Sie aus `Aktiv` Kontrollkästchen zum Aktivieren der Richtlinie, nachdem die Sitzungsvalidierungsrichtlinie mit Richtlinieneingaben und -Bedingungen eingerichtet wurde.



6. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften** Und aktivieren Sie die Eigenschaft Sitzungsvalidierung.

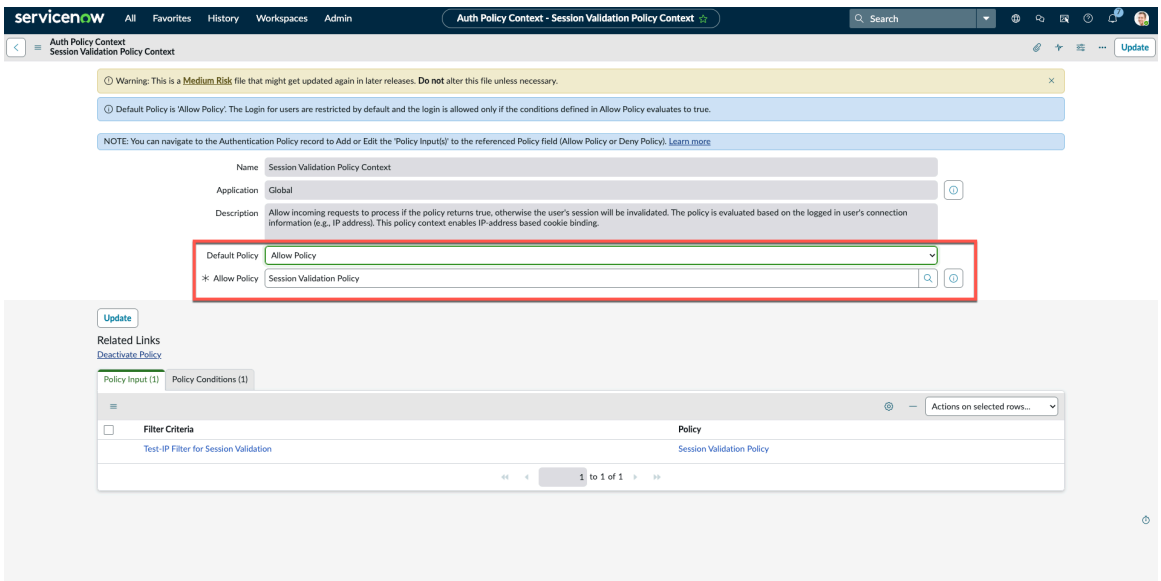
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Sitzungsvalidierungskontext**an.
8. Legen Sie die Standardrichtlinie auf fest **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Legt den Kontext der Sitzungsvalidierung gemäß der Richtlinieneingabe und den Richtlinienbedingungen fest.

   Hinweis: Standardmäßig gilt:

   - Der Sitzungsvalidierungskontext ist auf festgelegt **Richtlinie Zulassen** .
   - „Richtlinie zulassen“ ist als ausgewählt **Richtlinie Zur Sitzungsvalidierung** .



Ergebnis

Die Konfiguration wertet die Anmeldesitzung basierend auf den folgenden Faktoren aus:

- Schränkt den Zugriff auf ein ServiceNow® Instanz, wenn Hijacker die Sitzungscookies eines Anwenders von einem Gerät auf ein anderes kopieren, um die Identität einer Sitzung anzunehmen.
- Schränkt den Sitzungszugriff des Anwenders ein, wenn er ein unsicheres Netzwerk verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Authentifizierungsrichtlinien

Authentifizierungsrichtlinien bewerten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen und erlauben oder verweigern den Zugriff je nach Ausgabe der Auswertung der Richtlinienbedingungen. Beispielsweise ist der Zugriff nur zulässig, wenn alle Richtlinienbedingungen in angegeben sind **Zugriffsrichtlinie Zulassen** Auswertung auf „wahr“.

Verwenden Sie die integrierten Authentifizierungsrichtlinien, oder erstellen Sie eine Authentifizierungsrichtlinie entsprechend Ihren Sicherheitsanforderungen. Sie können die Richtlinien in Ihrer Instanz finden, indem Sie zu navigieren **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.

Hinweis: Zu jedem Zeitpunkt kann entweder die Zugriffsrichtlinie zulassen oder die Zugriffsrichtlinie verweigern ausgeführt werden, aber nicht beides.

Richtlinie	Beschreibung
Zugriffsrichtlinie zulassen	Lehnt standardmäßig alle Authentifizierungsanforderungen ab. Lässt nur die Authentifizierungsanforderungen zu, die den angegebenen Richtlinienbedingungen entsprechen.
Vorauthentifizierungsrichtlinie für Zugriffsgenehmigung	Vorauth-Richtlinie für Zugriff zulassen.
Nicht lokale Anmeldungsanwender zulassen	Wählen Sie diese Richtlinie aus, um nicht lokale Anmeldungsanwender zuzulassen. Wird im Kontext von SSO-Wiederherstellungs-Flows verwendet.
Zugriffsrichtlinie verweigern	Ermöglicht standardmäßig Authentifizierungsanforderungen. Verweigert nur die Authentifizierungsanforderungen, die den angegebenen Richtlinienbedingungen entsprechen.
Globale Sperrrichtlinie	Verweigert die Zugriffsanforderungen von Anwendern und APIs vor der Authentifizierung. Diese Richtlinie kann als Alternative zu verwendet werden Zugriffssteuerung für IP-Adressen .
Richtlinie Zur Sitzungsvalidierung	Die Authentifizierungsrichtlinie wertet Filterkriterien (z. B. IP-Adresse) aus, um zu bestimmen, ob eine Sitzung für eingehende Anforderungen aktiv bleiben soll. Sie müssen die Filterkriterien für diese Richtlinie festlegen.
Lokale Anmeldeverweigerungsrichtlinie	Wählen Sie diese Richtlinie aus, um alle lokalen Anmeldungen zu blockieren. Wird im Kontext von SSO-Wiederherstellungs-Flows verwendet.
STEP-Down-MFA-Richtlinie	Wählen Sie Aus **STEP-Down-MFA-Richtlinie** Als Standardrichtlinie in Situationen, in denen Anwender keine MFA-Authentifizierung benötigen. Wenn die in der Step-up-MFA-Richtlinie definierten Richtlinienbedingungen als „wahr“ ausgewertet werden, müssen sich Anwender nicht mit MFA anmelden.
STEP-up-MFA-Richtlinie	Wählen Sie Aus **STEP-up-MFA-Richtlinie** Als Standardrichtlinie, die MFA-Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie	Beschreibung
	erfordert, wenn die Richtlinienbedingungen, die in der Step-up-MFA-Richtlinie definiert sind, als wahr ausgewertet werden.

Konfigurieren Sie eine Authentifizierungsrichtlinie

Konfigurieren Sie eine Authentifizierungsrichtlinie, um Eingaben und Bedingungen zu definieren, die verwendet werden sollen, um Zugriff auf eine Instanz zu gewähren oder die Multifaktor-Authentifizierung zu erzwingen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.

   Hinweis: Um Beispiele für abgeschlossene Richtlinien anzuzeigen, können Sie diese Richtlinien in Ihrer Instanz überprüfen:

   - DEMORICHTLINIE: Lokale Anmeldung nur für Administratoren aus dem vertrauenswürdigen IP-Bereich zulassen
   - DEMORICHTLINIE: Lokale Anmeldung nur für Administratoren zulassen
   - DEMORICHTLINIE – Anwendername- und passwortbasierte Authentifizierung für bestimmte Anwender einschränken

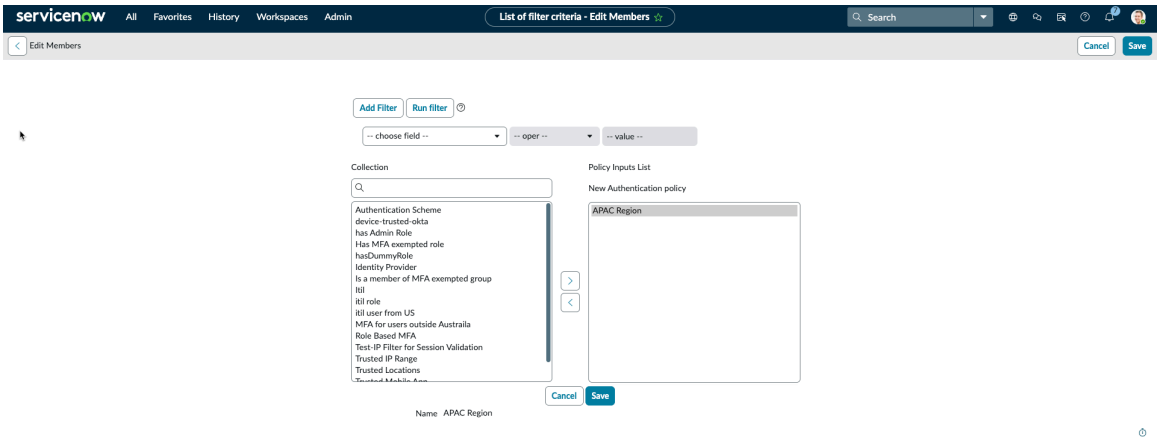
2. Klicken Sie auf **Neu** Schaltfläche zum Erstellen eines neuen Richtliniendatensatzes.
3. In **Richtlinie** Füllen Sie die Felder aus.

   Richtlinienformular

Feld	Beschreibung
Name	Name Ihrer Richtlinie.
Anwendung	Die bereichsbezogene Anwendung für die Richtlinie. Dieses Feld wird automatisch mit der aktuellen Anwendung ausgefüllt.
Beschreibung	Beschreibung der Richtlinie
Aktiv	Gibt an, ob die Richtlinie aktiv ist.

4. Von **Richtlinieneingaben** Klicken Sie auf die Registerkarte **Bearbeiten** .
5. Wählen Sie mindestens ein Filterkriterium aus **Sammlung** Listen Sie sie auf, und verschieben Sie sie in **Richtlinieneingabeliste** Von **Zugriffsrichtlinie Zulassen** Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Informationen zum Erstellen eigener Filterkriterien zur Verwendung in diesem Abschnitt finden Sie unter Filterkriterien.

6. Von **Richtlinienbedingungen** Klicken Sie auf die Registerkarte **Neu** .
7. Füllen Sie die Felder des Formulars aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Sie können beispielsweise Bedingungen erstellen, die nur Auftragnehmer aus einer Liste vertrauenswürdiger IP-Adressen zulassen.

8. **Wahlweise:** Wiederholen Sie Schritt 7, um zusätzliche Richtlinienbedingungen zu erstellen.

Hinweis: Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen ODER der Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als „wahr“ ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

9. Klicken Sie auf **Speichern**.

Fügen Sie einem Authentifizierungsrichtlinienkontext eine Authentifizierungsrichtlinie hinzu

Fügen Sie einem der Kontexte der Authentifizierungsrichtlinie eine Authentifizierungsrichtlinie hinzu. Der Authentifizierungskontext verwendet die Richtlinieneingaben und -Bedingungen, um zu bestimmen, ob Nutzungen Zugriff auf die Instanz gewährt wird oder ob MFA für Ihre Anwender erzwungen wird.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie**, Und wählen Sie je nach Bedarf einen der Einträge aus.

   Kontext vor der Authentifizierung

   Verwenden Sie den Vorautorisierungskontext, um Ihre Richtlinie auszuwerten, bevor der Anwender den Anmeldebildschirm sieht. Benutzern wird basierend auf dieser Auswertung Zugriff gewährt oder verweigert.

   Kontext nach der Authentifizierung

   Verwenden Sie den Kontext nach der Autorisierung, um Ihre Richtlinie auszuwerten, nachdem der Anwender seine Anmeldeinformationen eingegeben hat. Benutzern wird basierend auf dieser Auswertung Zugriff gewährt oder verweigert. Da diese Auswertung erfolgt, nachdem die Instanz den Anwender identifiziert hat, können Richtlinien in diesem Kontext ihre Bewertung basierend auf Anwenderdaten wie ihrer Rolle oder Gruppe vornehmen.

   MFA-Kontext

   Verwenden Sie den MFA-Kontext, um zu bestimmen, ob ein Anwender bei der Anmeldung die Multifaktor-Authentifizierung verwenden muss.

   Sitzungsvalidierungskontext

   Verwenden Sie den Sitzungsvalidierungskontext, um die IP-Adresse zu bewerten, die basierend auf den als Filter definierten Bedingungen festgelegt wird und den Zugriff auf die Instanz innerhalb einer Sitzung ermöglicht.

2. In **Standardrichtlinie** Feld einen Wert auswählen.
   Der Wert in diesem Feld bestimmt, wie der Kontext das Ergebnis der Bedingungen Ihrer Richtlinie verwendet.

   Die in diesem Feld verfügbaren Optionen hängen vom ausgewählten Kontext ab. Weitere Informationen zu diesen Kontexten finden Sie unter Kontexte der Authentifizierungsrichtlinie.

3. Weisen Sie dem Kontext eine Richtlinie zu.
   Der Name des Felds hängt davon ab, welchen Kontext Sie ausgewählt haben.

   Kontext vor und nach der Authentifizierung

   Diese Kontexte haben einen **Richtlinie Ablehnen** Oder **Richtlinie Zulassen** Feld, abhängig von der Auswahl in **Standardrichtlinie** Feld.

   MFA-Kontext

   Dieser Kontext hat einen **STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie** Feld, abhängig von der Auswahl in **Standardrichtlinie** Feld.

   Kontext der Sitzungsvalidierung

   Dieser Kontext hat einen **Richtlinie Zulassen** Oder **Richtlinie Ablehnen** Feld, abhängig von der Auswahl in **Standardrichtlinie** Feld.

4. Klicken Sie auf **Aktualisieren**.
   Nach dem Aktualisieren des Datensatzes können Sie die Eingaben und Bedingungen Ihrer Richtlinie in anzeigen **Richtlinieneingabe** Und **Richtlinienbedingungen** Registerkarten.

Adaptive Authentifizierungsereignisse

Sie können die Tabelle „Ereignisse der adaptiven Authentifizierung“ verwenden, um mehr über die Ereignisse zu erfahren.

Im Folgenden finden Sie einige der Protokolle, die in der Tabelle „Ereignisse der adaptiven Authentifizierung“ nachverfolgt werden können:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- glide.adaptive.auth.log.success.event : Um zu erfahren Erfolg Ereignisse für API-Anmeldungen nach der Authentifizierung.
- glide.adaptive.auth.log.mfa.relax.event : Um zu erfahren mfa_Relax Ereignisse für MFA-Kontext.

Hinweis:

- Für den Kontext vor der Authentifizierung Rest API-Zugriffsrichtlinien vom Typ „ Pre_auth „: Standardmäßig Fehler Ereignisse werden protokolliert. Erfolg Ereignisse Kann nicht Protokolliert werden.
- Für den Kontext nach der Authentifizierung Rest API-Zugriffsrichtlinien vom Typ anderer als „ Pre_auth „: Standardmäßig Fehler Ereignisse oder protokolliert. Für Erfolg Zu protokollierende Ereignisse müssen Sie aktivieren glide.adaptive.auth.log.success.event Eigenschaft.
- Für MFA: Standardmäßig MFA-Durchsetzung Ereignisse werden protokolliert.
- Damit MFA-Relaxationsereignisse protokolliert werden können, müssen Sie aktivieren glide.adaptive.auth.log.mfa.relax.event Eigenschaft. MFA-Entspannung Würde dasselbe Ereignis protokollieren als MFA-Durchsetzung , Aber mit Ergebnis Feld mit ausgefüllt Falsch .

Konfigurieren Sie die Eigenschaften der adaptiven Authentifizierung

Konfigurieren Sie nach der Aktivierung der adaptiven Authentifizierung die Eigenschaften der adaptiven Authentifizierung entsprechend Ihren Sicherheitsanforderungen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**an.
2. Konfigurieren Sie diese Eigenschaften:

Adaptive Authentifizierung – Eigenschaften

Eigenschaft	Beschreibung	Wert
Authentifizierungsrichtlinie aktivieren (glide.authenticate.auth.policy.enabled)	Option zum Aktivieren der Authentifizierungsrichtlinie.	Ja | Nein
Debug-Protokollierung für Authentifizierungsrichtlinien aktivieren (glide.authenticate.policy.debug)	Option zum Aktivieren der Debug-Protokollierung für die Authentifizierungsrichtlinien.	Ja | Nein
HTTP-Fehlercode, der dem Anwender angezeigt werden soll, wenn der Zugriff durch die globale Sperrrichtlinie (glide.authenticate.global.blocking_policy.error_code) blockiert wird	HTTP-Fehlercode, der während der Anmeldung angezeigt wird, wenn die globale Blockierungsrichtlinie eine Anwenderanmeldung blockiert.	Wählen Sie aus: ○ Unzulässig (403) ○ Nicht Gefunden (404)
Fehlermeldung, die dem Anwender angezeigt werden soll, wenn der Zugriff durch die globale Sperrrichtlinie blockiert wird (gilt nur, wenn der HTTP-Fehlercode	Fehlermeldung, die angezeigt wird, wenn die globale Sperrrichtlinie den Zugriff blockiert.	Textfeld

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Wert
„Forbidden(403)“ ausgewählt ist) (glide.authenticate.global.blocking_policy.error_message)		
Flow für Gerätevertrauen aktivieren (glide.authenticate.preauth.allow.trusted.device)	Option zum Aktivieren des vertrauenswürdigen Geräte-Flows.	Ja | Nein
Maximale Anzahl vertrauenswürdiger Geräte, die ein Anwender registrieren kann (glide.trusted.device.max.count)	Dies ist die maximale Anzahl vertrauenswürdiger Geräte, die ein Anwender registrieren kann.	Textfeld
Geräteregistrierung für Gerätevertrauensfluss überspringen, wenn der Anwender aus dem vertrauenswürdigen Netzwerk stammt (glide.authenticate.preauth.skip.user.registration)	Option zum Überspringen der Registrierung, wenn der Anwender versucht, sich über das vertrauenswürdige Netzwerk zu registrieren	Ja | Nein
Eigenschaft zum Aktivieren der Sitzungsvalidierungsfunktion. Legen Sie diese Option auf „wahr“ fest, nachdem Sie die Richtlinie des Sitzungsvalidierungskontexts aktiviert und die gewünschten Filter und Bedingungen eingerichtet haben (Session.validation.enabled).	Option zum Aktivieren der Sitzungsvalidierungsfunktion. Legen Sie diese Option auf „wahr“ fest, nachdem Sie die Richtlinie des Sitzungsvalidierungskontexts aktiviert und die gewünschten Filter und Bedingungen eingerichtet haben.	Ja | Nein

Tutorial: Konfigurieren Sie die adaptive Authentifizierung

Verwenden Sie diese Beispielschritte, um die adaptive Authentifizierung für eine Instanz zu konfigurieren.

Zur Verwendung dieses Tutorials benötigen Sie eine Instanz mit Adaptive Authentifizierung Aktiviert. Details zu diesem Vorgang finden Sie unter Aktivieren Adaptive Authentifizierung.

Das Beispiel führt Sie durch die Erstellung einer neuen Richtlinie und deren Anwendung auf eine Instanz. In diesem Tutorial werden Sie:

Erstellen Sie einen Filterkriteriendatensatz

Erstellen Sie einen Gruppenfilterkriteriendatensatz, der als Eingabe für Ihre Richtlinie verwendet werden soll. Mit diesem Datensatz kann Ihre Richtlinie den Zugriff basierend auf der Gruppe eines Anwenders bestimmen. In diesen Schritten definieren Sie die Gruppe oder Gruppen, die die Richtlinie zum Bestimmen des Zugriffs verwendet.

Erstellen Sie eine Richtlinie

Erstellen Sie eine Richtlinie, die bestimmt, ob ein Anwender auf die Instanz zugreifen kann. Diese Richtlinie verwendet den von Ihnen erstellten Gruppenfilterkriteriendatensatz als Eingabe. In diesen Schritten definieren Sie auch Richtlinienbedingungen, die definieren, wie die Richtlinie die Richtlinieneingabe verwendet, um den Anwenderzugriff zu bestimmen.

Konfigurieren Sie einen Richtlinienkontext

Konfigurieren Sie **Kontext Der Post-Authentifizierungsrichtlinie** Um Ihre neue Richtlinie zu verwenden. Wenn diese Konfiguration aktiviert ist, verweigert Ihre Instanz Anwendern innerhalb der im Filterkriteriendatensatz definierten Gruppe den Zugriff.

Erstellen Sie einen Filterkriteriendatensatz

Erfahren Sie, wie Sie einen Kriteriendatensatz erstellen, der als Richtlinieneingabe für Ihre Richtlinie zur adaptiven Authentifizierung verwendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

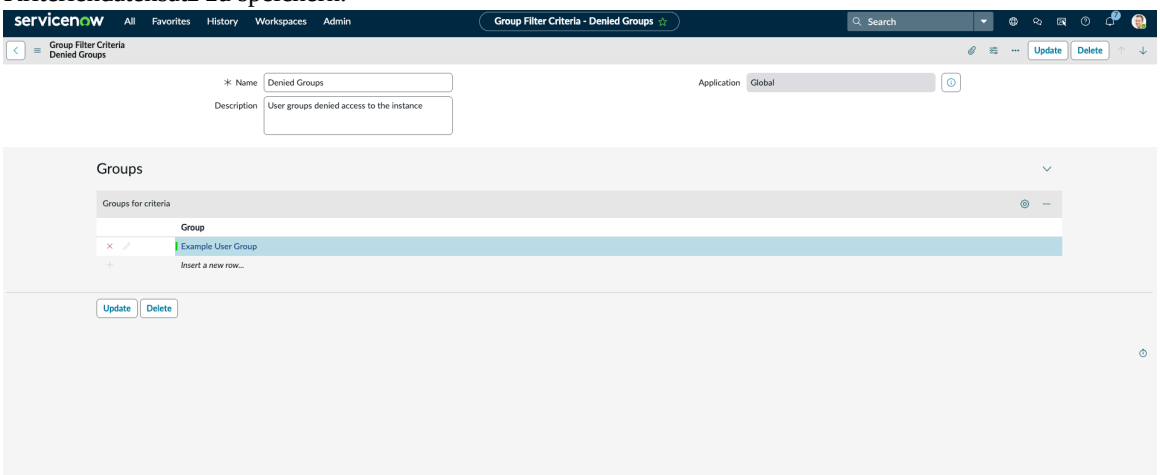
Erforderliche Rolle: Administrator

Um den Zugriff auf Ihre Instanz basierend auf Anwendergruppen zu verweigern, müssen Sie einen Gruppenfilterkriteriendatensatz erstellen. Dieser Datensatz definiert eine Anwendergruppe oder eine Reihe von Anwendergruppen, die Ihre Richtlinie Zugriff gewähren oder verweigern kann. In diesem Beispiel erstellen Sie einen Gruppenfilterkriteriendatensatz für eine einzelne Anwendergruppe.

Weitere Informationen zu Anwendergruppen und ihrer Verwendung in Ihrer Instanz finden Sie unter Anwenderverwaltung erkunden .

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Filterkriterien** > **Gruppenkriterien**an.
2. Klicken Sie auf **Neu**, um einen neuen Datensatz zu erstellen.
3. In **Name** Geben Sie einen Namen für Ihren Datensatz ein.
   Beispiel: Abgelehnte Gruppen .
4. In **Beschreibung** Geben Sie eine kurze Beschreibung ein.
   Beispiel: Anwendergruppen haben Zugriff auf die Instanz verweigert .
5. In **Gruppen für Kriterien** Liste, doppelklicken Sie auf **Neue Zeile einfügen...** .
6. Geben Sie den Namen einer Anwendergruppe ein, oder klicken Sie auf das Referenzsymbol ( ), um eine Gruppe aus einer Liste auszuwählen.
   Wenn Sie eine neue Anwendergruppe für Ihre Filterkriterien erstellen möchten, klicken Sie auf das Referenzsymbol ( ), und klicken Sie dann auf **Neu** Schaltfläche. Weitere Informationen zum Erstellen von Anwendergruppen finden Sie unter Erstellen Sie eine Anwendergruppe .
7. Nachdem Sie Ihre Anwendergruppe hinzugefügt haben, klicken Sie auf **Übermitteln** Um Ihren Kriteriendatensatz zu speichern.



Erstellen Sie eine Richtlinie

Erfahren Sie, wie Sie eine Richtlinie erstellen, um den Zugriff auf Anwendergruppen zu verweigern, die in Ihren Gruppenfilterkriterien definiert sind.

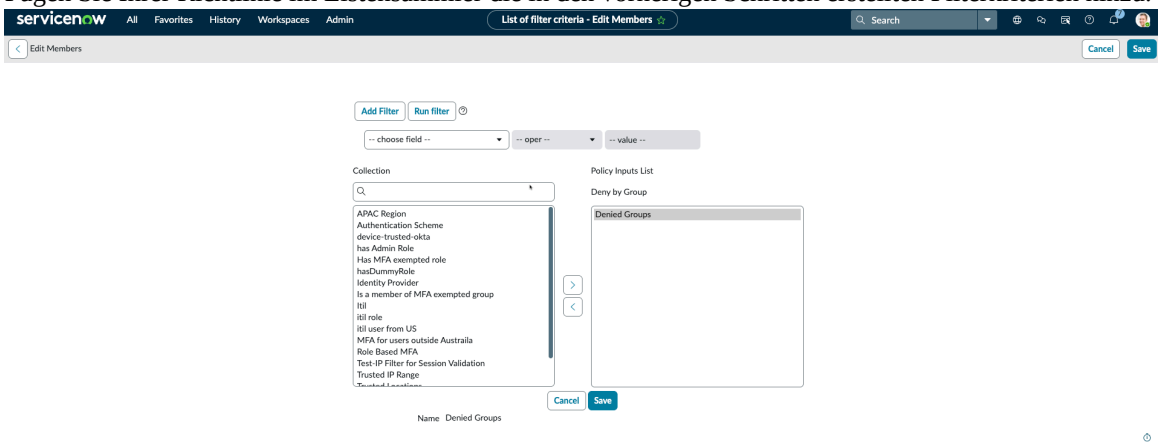
Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

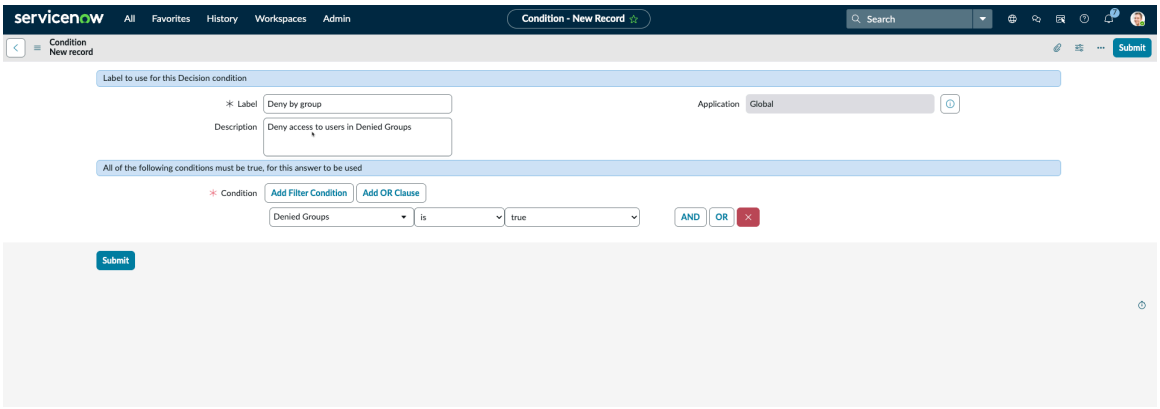
Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Alle Richtlinien**an.
2. In **Richtlinien** Liste, klicken Sie auf **Neu** .
3. In **Name** Geben Sie einen Namen für Ihren Datensatz ein.
   Beispiel: Ablehnen nach Gruppe .
4. In **Beschreibung** Geben Sie eine kurze Beschreibung ein.
   Beispiel: Anwendergruppen haben Zugriff auf die Instanz verweigert .
5. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.
   Nach dem Speichern wird die **Richtlinieneingaben** Und **Richtlinienbedingungen** Listen werden im Formular angezeigt.
6. In **Richtlinieneingaben** Liste, klicken Sie auf **Bearbeiten** .
7. Fügen Sie Ihrer Richtlinie im Listensammler die in den vorherigen Schritten erstellten Filterkriterien hinzu.



8. Klicken Sie auf **Speichern**.
   Die Instanz speichert die Richtlinieneingabe und zeigt die Anzeige des Richtliniendatensatzes erneut an.
9. In **Richtlinienbedingungen** Liste, klicken Sie auf **Neu** .
10. In **Bezeichnung** Feld erstellen Sie beispielsweise eine Bezeichnung für diese Bedingung Ablehnen nach Gruppe .
11. In **Beschreibung** Geben Sie eine kurze Beschreibung ein.
    Beispiel: Verweigern Sie Anwendern in abgelehnten Gruppen den Zugriff .
12. In **Bedingung** Wählen Sie die Filterkriterien aus, die Sie in den vorherigen Schritten erstellt haben, und wählen Sie dann aus **Ist** , Und **Wahr** Um die Bedingung abzuschließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



13. Klicken Sie auf **Speichern**.

Konfigurieren Sie einen Richtlinienkontext

Konfigurieren Sie den Kontext der Richtlinie nach der Authentifizierung, um Ihre neue Richtlinie zu verwenden. Wenn diese Konfiguration aktiviert ist, verweigert Ihre Instanz Anwendern innerhalb der im Filterkriteriendatensatz definierten Gruppe den Zugriff.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext nach der Authentifizierung**an.
   Sie müssen verwenden **Kontext Nach Der Authentifizierung** Da die in diesem Tutorial verwendete Richtlinie bewerten muss, in welcher Gruppe sich ein Anwender befindet. Diese Informationen sind erst verfügbar, nachdem ihre Anmeldeinformationen eingegeben wurden.
2. In **Standardrichtlinie** Feld auswählen Richtlinie Ablehnen .
   Diese Auswahl gewährt Anwendern standardmäßig Zugriff und verweigert den Zugriff nur, wenn die Richtlinienbedingungen als „wahr“ ausgewertet werden.
3. In **Richtlinie Ablehnen** Wählen Sie die Richtlinie aus, die Sie in den vorherigen Schritten erstellt haben.
4. Klicken Sie Auf **Aktualisieren** Zum Speichern des Richtlinienkontextdatensatzes.

Adaptive Authentifizierung für vertrauenswürdige Mobile-Apps

Greifen Sie auf zu ServiceNow Aus nicht vertrauenswürdigen Netzwerken mithilfe von Now Mobile-App.

Adaptive Authentifizierung für vertrauenswürdige Mobile-Apps

Mit der adaptiven Authentifizierung für vertrauenswürdige Mobile-Apps können Anwender auf zugreifen ServiceNow Instanz, die verwendet Now Mobile-App. Die Instanz ist hinter einer vertrauenswürdigen IP-Netzwerkgrenze geschützt.

Im Folgenden finden Sie einige der Szenarien, in denen Sie Zugriff auf die Instanz benötigen, während Sie sich außerhalb Ihres Netzwerks befinden.

Als Mitarbeiter benötigen Sie Zugriff auf Now Mobile-App Und Mitarbeiter-Service Center (Portal) von außerhalb des Netzwerks. Mit dem Filter Trusted Mobile App können Sie die eingehende Anforderung identifizieren, die von einer vertrauenswürdigen Person stammt Now Mobile-App Das mit einem Anwenderaccount verknüpft ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Administrator können Sie die Richtlinie konfigurieren. Mit der Richtlinie können Anwender ihre Mobilgeräte registrieren und auf die Instanz in einem vertrauenswürdigen Netzwerk zugreifen.

Als Benutzer können Sie Ihr Mobilgerät registrieren, indem Sie die in der Instanz angezeigte QR scannen. Nach der Registrierung können Sie sich über bei Ihrer -Instanz anmelden Now Mobile-App, Mit Ihren Anmeldeinformationen.

Hinweis: Um das Mobilgerät zu registrieren, müssen Sie sich in einem vertrauenswürdigen Netzwerk befinden. Nach der Registrierung können Sie sich auch über andere Netzwerke bei der Instanz anmelden.

Features

Als Administrator können Sie die folgenden Funktionen verwenden:

- Konfigurieren Sie Richtlinien mithilfe vertrauenswürdiger App-Filterkriterien.
- Erstellen Sie Richtlinienbedingungen mit neuen Filterkriterien für vertrauenswürdige mobile Apps.
- Unterstützt alle Anmeldemethoden in der vertrauenswürdigen mobilen App für die Anwender (lokale Anmeldung, SAML, OIDC und MFA).
- Widerrufen Sie ein vertrauenswürdiges Gerät.
- Fügen Sie Sicherheitsereignisse für alle Aktionen zur Geräteregistrierung oder zum Widerruf hinzu. Die Ereignisse können verwendet werden, um den Anwender zu benachrichtigen.
- Unterstützen Sie Sicherheitsereignisse für Signaturfehler, Cookie-Validierungsfehler, ungültige Token, ungültige Header oder Abfrageparameter.
- Steuern Sie die maximale Anzahl registrierter Geräte.
- Verhindern Sie die Registrierung eines neuen Geräts, es sei denn, der Anwender entfernt ein vorhandenes gekoppeltes Gerät.
- Erfassen Sie, wann ein Gerät zuletzt verwendet wurde.

Aktivieren Sie Trusted Mobile App

Aktivieren Sie die adaptive Authentifizierung mit der Trusted Mobile-App, indem Sie die Authentifizierungsrichtlinie und Filterbedingungen verwenden.

Vorbereitungen

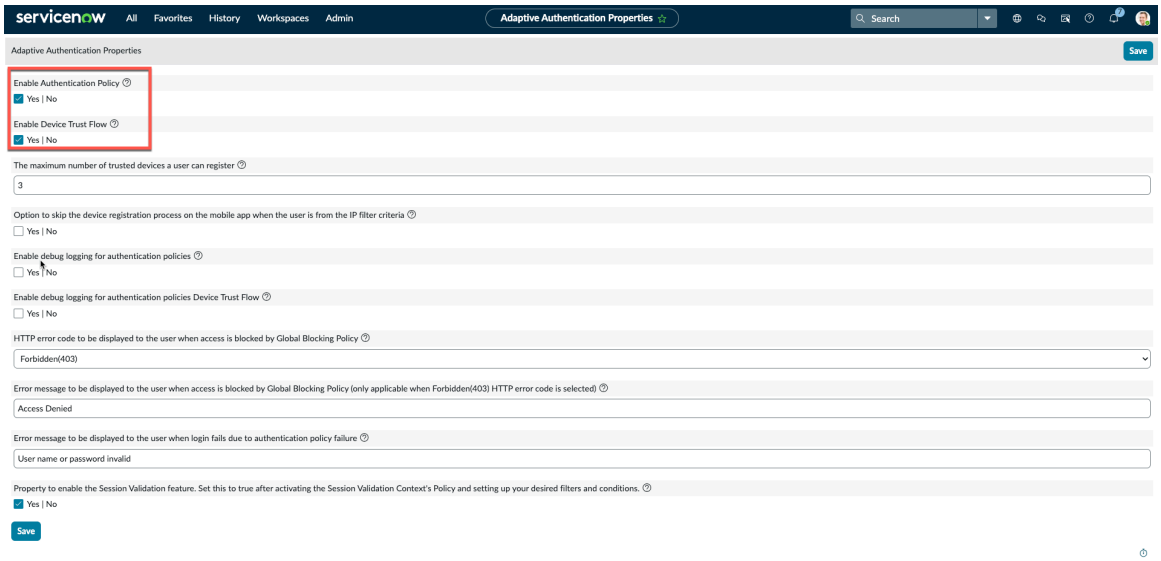
Stellen Sie sicher, dass die adaptive Authentifizierung (`com.snc.adaptive_authentication`) Plugin ist installiert.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**an.
2. Aktivieren Sie auf der Seite „Eigenschaften der adaptiven Authentifizierung“ die folgenden Eigenschaften:
   - Aktivieren Sie die Authentifizierungsrichtlinie (`glide.authenticate.auth.policy.enabled`)
   - Flow Für Gerätevertrauen Aktivieren (`glide.authenticate.preauth.allow.trusted.device`)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Um die Flow-Eigenschaft „Gerätetuenswürdigkeit“ zu deaktivieren, müssen Sie die Bedingungen mit dem vertrauenswürdigen mobilen Filter entfernen. Andernfalls wird eine Fehlermeldung angezeigt, um die Bedingungen zu entfernen.

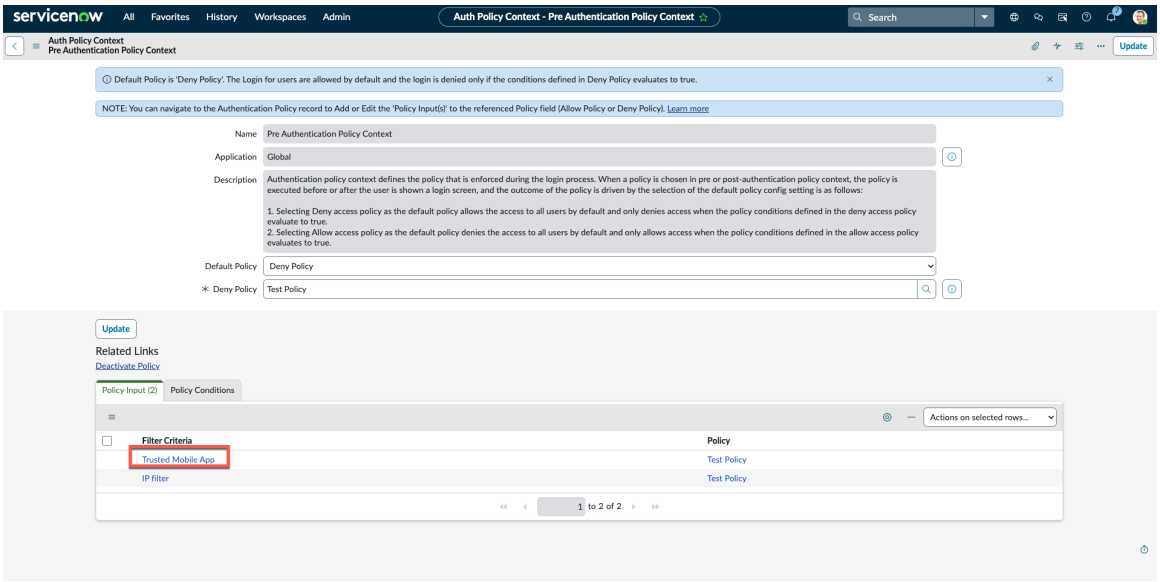
3. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **Kontext vor der Authentifizierung**an.
4. Definieren Sie die Bedingungen im Kontext vor der Authentifizierung.
   Weitere Informationen finden Sie unter Kontext vor der Authentifizierung.

   Hinweis: Standardmäßig lautet die Richtlinienbedingung **Richtlinie Ablehnen** . Sie können in ändern **Richtlinie Zulassen** . Diese Richtlinien sind direkte Gegensätze.

   - Mit **Richtlinie Zulassen** , Allen Anwendern wird standardmäßig der Zugriff verweigert, und der Zugriff ist nur zulässig, wenn die Bedingungen der Zugriffsrichtlinie „wahr“ sind.
   - Mit **Richtlinie Ablehnen** , Alle Anwender haben standardmäßig Zugriff, und der Zugriff wird nur verweigert, wenn die Bedingungen der Zugriffsverweigerungsrichtlinie „wahr“ sind.

   In der Richtlinieneingabe die Richtlinieneingabe **Vertrauenswürdige Mobile-App** Ist eine Richtlinieneingabe für die vertrauenswürdige mobile App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

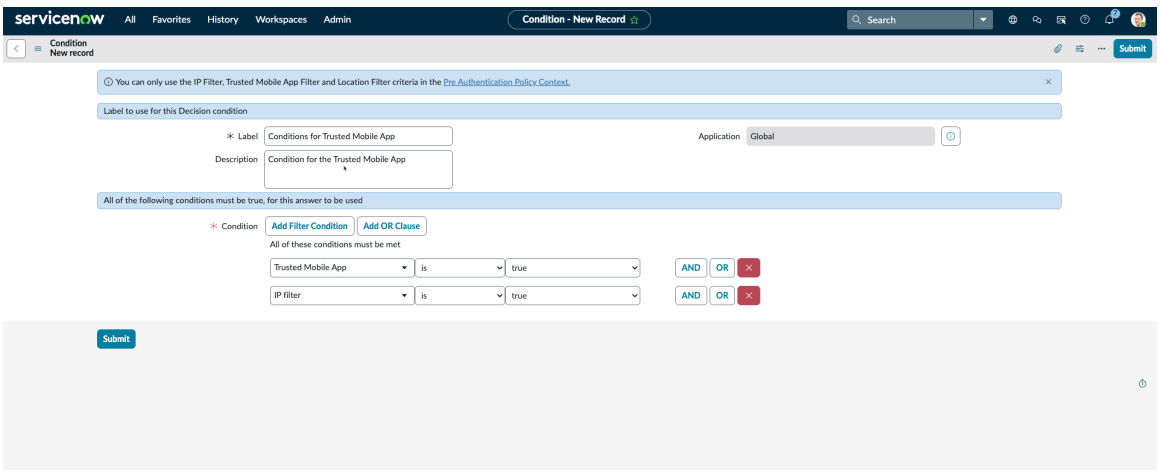


5. Erstellen Sie in den Richtlinienbedingungen die Bedingung, indem Sie auf klicken **Neu** .

6. Füllen Sie die Felder im Formular aus.

Formular „Filterbedingung“

Feld	Beschreibung
Bezeichnung	Name der Bedingung
Beschreibung	Beschreibung der Bedingung
Anwendung	Anwendungsbereich für diesen Datensatz
Bedingung	Bedingungen basierend auf UND UND ODER. Da die Authentifizierungsrichtlinie ist **Richtlinie Zulassen** , Die Bedingung für die vertrauenswürdige Mobile-App ist im auf dem Bild angezeigten Beispiel auf „wahr“ festgelegt.



7. Klicken Sie auf **Absenden**.

Ergebnis

Die Richtlinieneingabe- und Filterbedingungen werden für die Funktion „vertrauenswürdiges Gerät“ erstellt. Benutzer können mit der Funktion „vertrauenswürdiges Gerät“ fortfahren, um auf zuzugreifen ServiceNow

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanz aus nicht vertrauenswürdigen Netzwerken mithilfe von Now Mobile-App. Weitere Informationen finden Sie unter Registrieren Sie ein vertrauenswürdiges Gerät.

Registrieren Sie ein vertrauenswürdiges Gerät

Registrieren Sie ein vertrauenswürdiges Gerät, um auf zuzugreifen ServiceNow Instanz außerhalb des Netzwerks.

Vorbereitungen

Sie müssen sich im vertrauenswürdigen Netzwerk befinden, um die Registrierung vertrauenswürdiger Geräte durchzuführen.

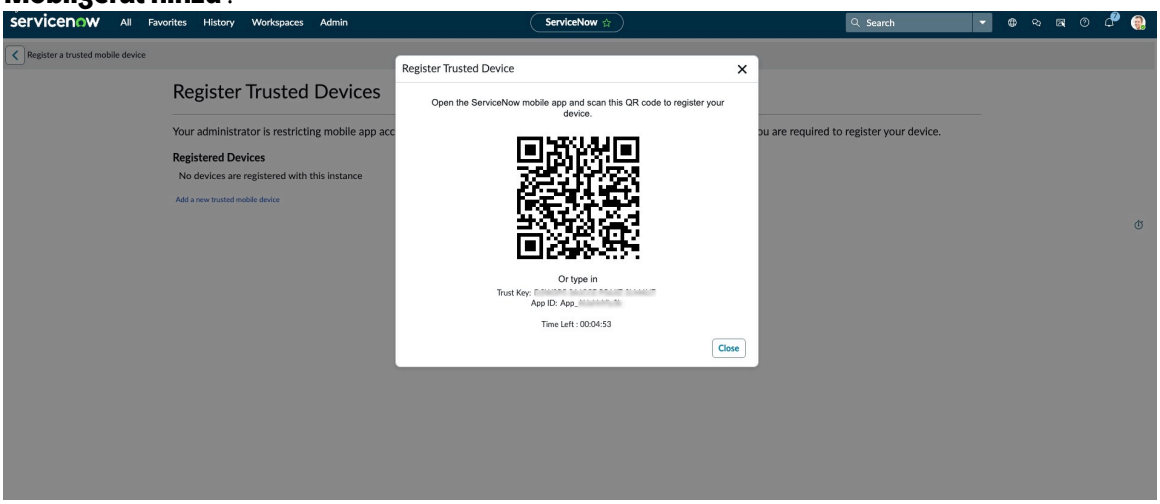
Erforderliche Rolle: keine

Prozedur

1. Navigieren Sie zu einer der folgenden Menüoptionen:
   - Auf der ServiceNow AI Platform, Navigieren Sie zu **Alle** > **Self-Service** > **Mein Profil**an.

     Hinweis: Sie können auch auf Ihr Profil zugreifen, indem Sie im Instanzheader auf Ihren Anwendernamen klicken.

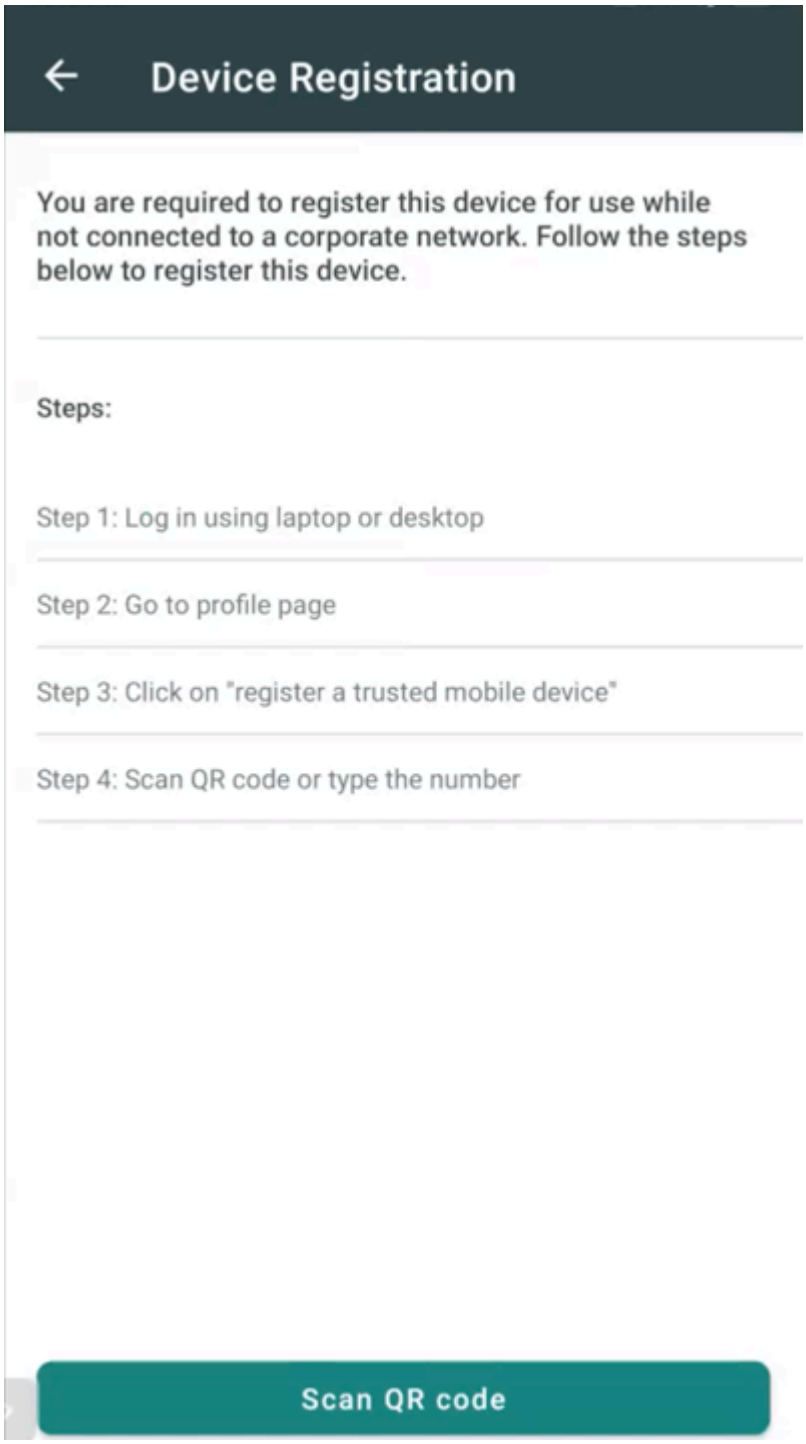
   - Auf der Now Support Klicken Sie auf das Profil, und wählen Sie aus **Vertrauenswürdiges Gerät** .
2. Klicken Sie in Ihrem Anwenderprofil auf **Registrieren Sie ein vertrauenswürdiges Mobilgerät** Im Abschnitt zugehörige Links.
   Die Seite Vertrauenswürdige Geräte registrieren wird angezeigt.
3. Registrieren Sie ein neues Gerät, indem Sie auf klicken **Fügen Sie ein neues vertrauenswürdiges Mobilgerät hinzu** .



4. Im Bildschirm Geräteregistrierung auf Ihrem ServiceNow Tippen Sie auf die Mobile-App **QR-Code scannen** Schaltfläche und scannen Sie den QR-Code, der auf Ihrem Laptop oder Desktop angezeigt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

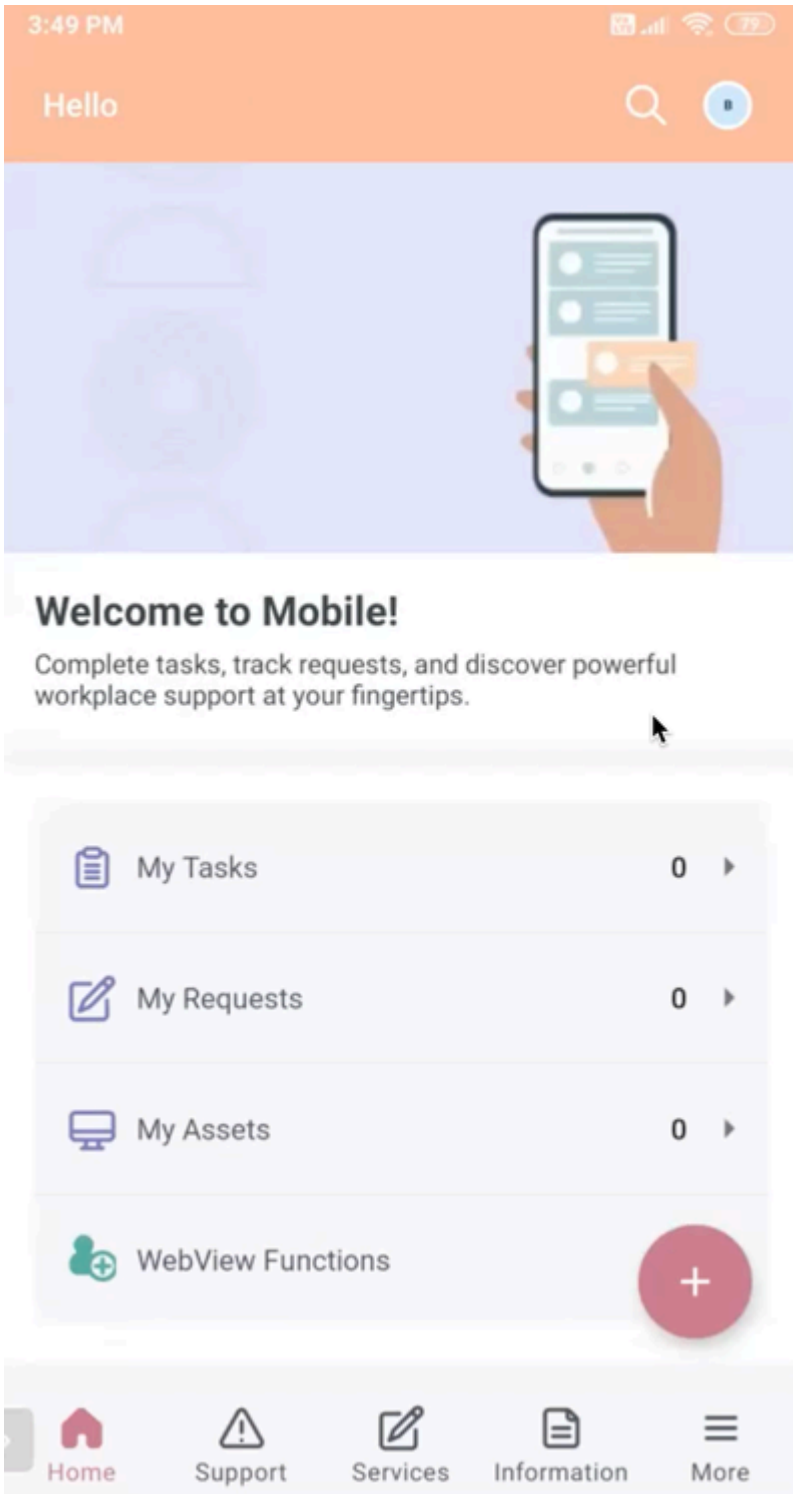


Der Registrierungsprozess wird abgeschlossen, und Sie werden zu Ihrer Anmeldeseite aufgefordert, um Ihre Authentifizierung abzuschließen.

5. Geben Sie Ihre Anmeldeinformationen an, und melden Sie sich bei an Now Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der mobile Startbildschirm wird angezeigt.



Automatische Übersetzung

Ergebnis

Auf der Seite „Vertrauenswürdige Geräte registrieren“ auf Ihrem Laptop oder Desktop wird das registrierte Gerät angezeigt. Sie können verwenden Symbol, wenn Sie das registrierte Gerät von der Seite entfernen möchten.

Nächste Maßnahme

Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Gerätevertrauen** > **Geräteregistrierung** Um alle Details des registrierten Geräts anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie Ihr vertrauenswürdiges Gerät

Verwalten Sie Ihr vertrauenswürdiges Gerät über die Registrierungsseite für vertrauenswürdiges Gerät.

Vorbereitungen
Erforderliche Rolle: keine

Prozedur

1. Navigieren Sie zu einer der folgenden Menüoptionen:
   - Auf der ServiceNow AI Platform, Navigieren Sie zu **Alle** > **Self-Service** > **Mein Profil**an.

     Hinweis: Sie können auch auf Ihr Profil zugreifen, indem Sie im Instanzheader auf Ihren Anwendernamen klicken.

   - Auf der Now Support Klicken Sie auf das Profil, und wählen Sie aus **Vertrauenswürdiges Gerät** .
2. Klicken Sie in Ihrem Anwenderprofil auf **Registrieren Sie Das Vertrauenswürdige Gerät** Im Abschnitt zugehörige Links.
   Die Seite Vertrauenswürdige Geräte registrieren wird angezeigt.
3. Entfernen Sie auf der Seite „Vertrauenswürdige Geräte registrieren“ das Gerät, indem Sie auf klicken

   Symbol.

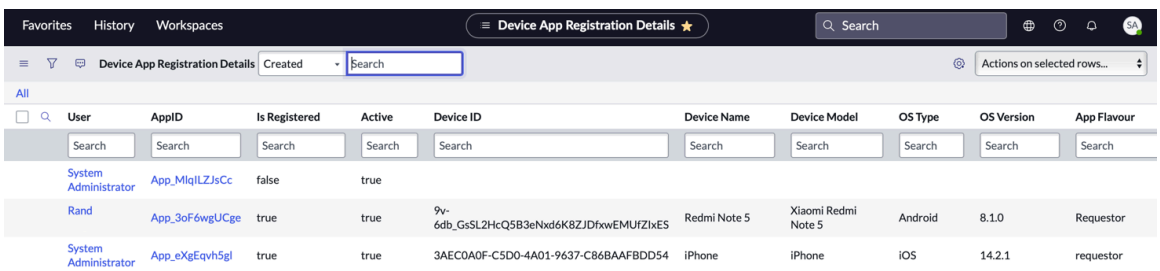
   Hinweis: Das gelöschte Mobilgerät muss erneut registriert werden, um auf die Instanz zuzugreifen.

Registrierungsdetails der registrierten Geräte

Zeigen Sie die Details der Geräte an, die bei Ihrem registriert sind ServiceNow Instanz.

Um alle Details des bei der Instanz registrierten Geräts anzuzeigen, navigieren Sie zu **Alle** > **Adaptive Authentifizierung** > **Gerätevertrauen** > **Geräteregistrierung**an.

Verwenden Sie den Filter, um das Gerät zu identifizieren. Klicken Sie auf **AppId** Feld, um mehr über das registrierte Gerät zu erfahren.



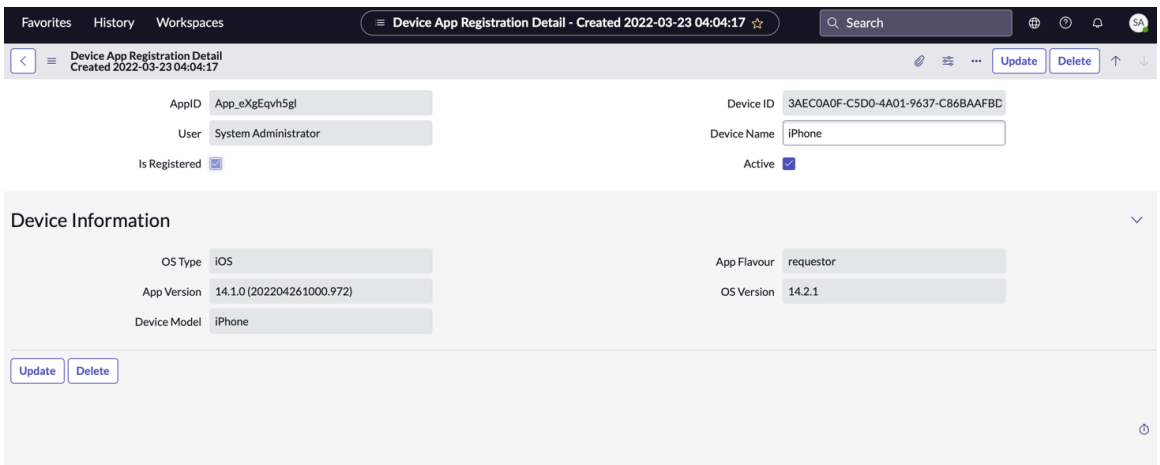
Die folgenden Details werden für das Gerät angezeigt:

- AppID
- Geräte-ID

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwender
- Gerätename
- Geräteinformationen wie:
  - BS-Typ
  - App-Variante
  - App-Version
  - BS-Version
  - Gerätemodell



Fehlerbehebung für vertrauenswürdige Mobile-App

Überprüfen Sie diese Problembehebungsszenarien, um Probleme mit der Trusted Mobile App zu beheben.

In den folgenden Abschnitten werden einige Problembehandlungsszenarien und Möglichkeiten zur Problembehandlung beschrieben.

Zeitdifferenz zwischen Instanz und Mobilgerät (Clock-Skew)

Wenn ein Taktversatz vorhanden ist, können Sie die Uhr auf Ihrem Mobilgerät für die Verwendung des vertrauenswürdigen Geräts anpassen oder zurücksetzen.

Ablauf des QR-Codes innerhalb von fünf Minuten

Der QR-Code für die Funktion „vertrauenswürdiges Gerät“ läuft innerhalb von fünf Minuten ab. In einem solchen Fall können Sie klicken, um einen neuen QR-Code anzuzeigen.

Hinweis: Der Ablauf des QR-Codes kann erweitert werden. Um den Code-Ablauf zu verlängern, wenden Sie sich an Ihren Administrator.

Systemeigenschaft hat sich geändert

Wenn sich die Systemeigenschaft geändert hat, überprüfen Sie die Registrierung basierend auf der Systemeigenschaft für die gültigen Anmeldeinformationen, die für die Anmeldung verwendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Maximale Anzahl registrierter Geräte

Wenn die maximale Anzahl von Geräteregistrierungen erreicht ist, entfernen Sie das vorhandene Gerät, oder wenden Sie sich an Ihren Administrator, um die maximale Geräteregistrierung zu ändern.

API-Authentifizierung

Authentifizierungskonfigurationen für API.

API-basierte Authentifizierung in ServiceNow® Validiert die Identität eines Anwenders, der auf eine Instanz zugreift, und autorisiert den Anwender dann für Funktionen, die der Rolle oder Auftragsfunktion des Anwenders entsprechen, während er einen API-Aufruf von ausführt ServiceNow® Instanz.

Im Folgenden sind die Typen der API-Authentifizierung in aufgeführt ServiceNow®:

- Zertifikatbasierte Authentifizierung
- OAuth
- Tokenbasierte Authentifizierung

Zertifikatbasierte Authentifizierung

Mit der zertifikatbasierten Authentifizierung können Sie eingehende API-Anforderungen mithilfe von Zertifikaten einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) gegenseitig authentifizieren.

Zertifikatbasierte Authentifizierung für eingehende Webservices

Authentifizieren Sie eingehende Anforderungen an ServiceNow SOAP- und REST-APIs. Informationen zum Einrichten der gegenseitigen Authentifizierung für eingehende Webservices finden Sie unter Richten Sie die zertifikatbasierte Authentifizierung ein.

OAuth

Die OAuth-basierte Authentifizierung validiert die Identität des Clients, der versucht, mithilfe eines Authentifizierungsprotokolls eine Vertrauensbasis für das System herzustellen.

OAuth 2,0 – offene Autorisierung ist das branchenübliche Autorisierungsprotokoll, das die Einfachheit von Cliententwicklern berücksichtigt und gleichzeitig spezifische Autorisierungs-Flows für Webanwendungen, Desktop-Anwendungen und Mobilgeräte bereitstellt.

Eingang

Erstellen Sie einen Endpunkt für externe Clients, die auf Ihre Instanz zugreifen möchten. Dadurch wird ein OAuth-Client-Anwendungsdatensatz erstellt und eine Client-ID und ein geheimer Client generiert, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt. Weitere Informationen finden Sie unter OAuth eingehend.

Tokenbasierte Authentifizierung

Token-basierte Authentifizierung für die Konfiguration eingehender REST APIs mit API-Schlüssel oder HMAC.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützen Sie API-Token für REST-API-Endpunkte, damit die ServiceNow® Für die Anwenderauthentifizierung.

Die tokenbasierte Authentifizierung für die Konfiguration eingehender REST-APIs kann auf durchgeführt werden ServiceNow® Instanz mit API-Schlüssel oder HMAC-Token .

API-Schlüssel und HMAC-Authentifizierung für eingehende REST-APIs

Unterstützen Sie API-Token für REST API-Endpunkte, damit ServiceNow® Anwendername und Passwort sind in der Webhook-URL nicht sichtbar.

Aktivieren Sie die API-schlüsselbasierte Authentifizierung, um die eingehende Webhook-URL sicher zu authentifizieren.

Um den API-Schlüssel und die HMAC-Authentifizierung zu verwenden, müssen Sie (Plugin: `Com.Glide.tokenbased_auth`) In ServiceNow® Instanz.

⚠ **Warnung:** Verwenden **VERÖFFENTLICHEN** Anforderung, wenn vertrauliche Informationen an den Server übermittelt werden.

Die Installation des API-Schlüssels und der HMAC-Authentifizierung hängt von den folgenden Plugins ab:

- Plugin für REST API-Authentifizierungsbereich (`com.glide.rest.auth.scope`)
- REST API-Zugriffsrichtlinien-Plugin (`Com.Glide.Rest.Policy`)
- Authentifizierungsbereich (`com.glide.auth.scope`)

Vorteile

API-Schlüssel und HMAC-Authentifizierung für eingehende REST-APIs aktivieren:

- Möglichkeit, einen API-Schlüssel oder ein HMAC-Token für die REST API-Authentifizierung anzugeben.
- Fähigkeit, einen Anwenderaccount dem API-Schlüssel oder HMAC-Token zuzuordnen.
- Möglichkeit, ein Token als Abfrageparameter oder Header innerhalb des REST-API-Aufrufs anzugeben.
- Fähigkeit, den Authentifizierungsbereich API-Schlüssel- oder HMAC-Token-Konfigurationen zuzuordnen, sodass API-Schlüssel nur zum Aufrufen von APIs verwendet werden können, die einem bestimmten Bereich zugeordnet sind.
- Fähigkeit, eine API-Schlüssel- oder HMAC-Token-Konfiguration einem Authentifizierungsprofil zuzuordnen, das in API-Zugriffsrichtlinien verwendet werden kann.

Aktivieren Sie API-Schlüssel und HMAC-Authentifizierung

Sie können den Plugin-API-Schlüssel und die HMAC-Authentifizierung aktivieren (`Com.Glide.tokenbased_auth`) In Ihrem ServiceNow® Instanz.

Vorbereitungen
Erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach API-Schlüssel und HMAC-Authentifizierung Plugin (`Com.Glide.tokenbased_auth`) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

API-Schlüssel konfigurieren – Token-basierte Authentifizierung

Konfigurieren Sie einen API-Schlüssel, um die Authentifizierung für REST API-Endpunkte zu unterstützen.

Vorbereitungen

Erforderliche Rolle: Administrator

Erforderliches Plugin: API-Schlüssel und HMAC-Authentifizierung (`Com.Glide.tokenbased_auth`)

Prozedur

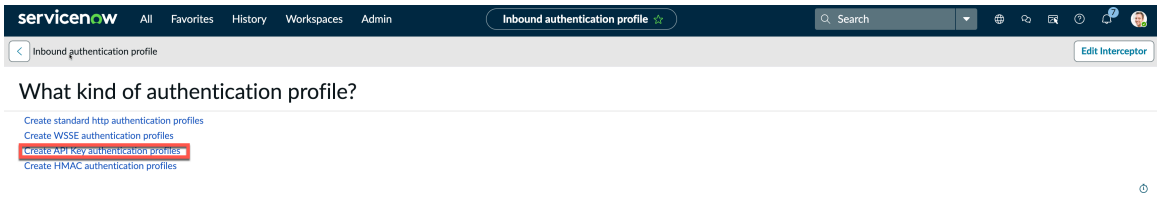
1. Erstellen Sie ein eingehendes Authentifizierungsprofil.

   a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**an.

   b. Wählen Sie **Neu**.
   Das System zeigt die Meldung an Welche Art von Authentifizierungsprofil?

   c. Wählen Sie Aus **Erstellen Sie API-Schlüssel-Authentifizierungsprofile** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

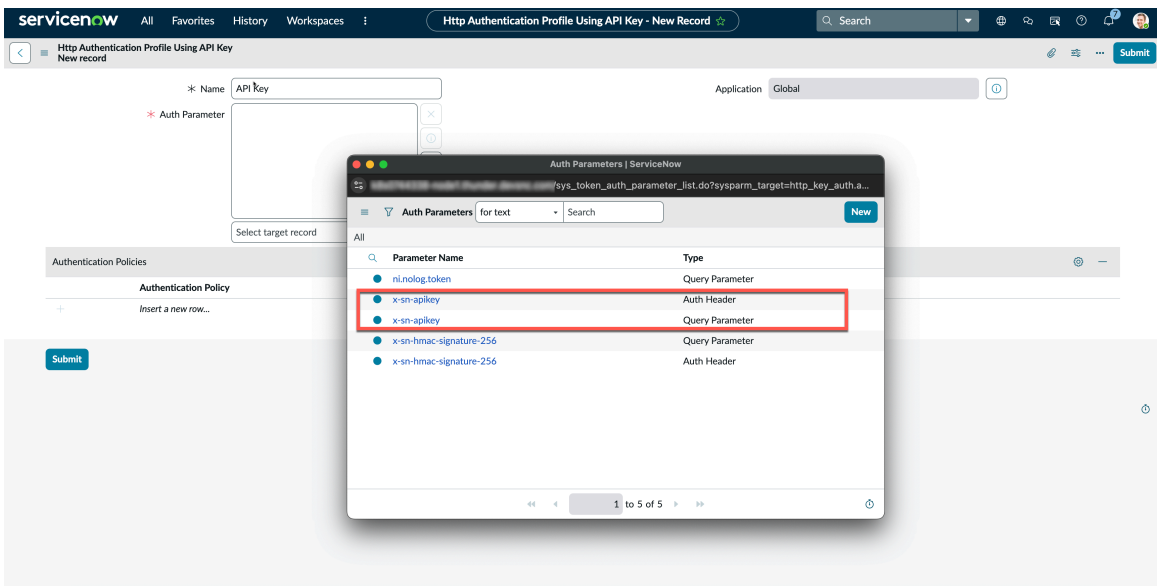


d. Füllen Sie im Formular die Felder aus.

API-Schlüssel-Authentifizierungsprofile

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Anwendung	Umfang der Authentifizierungsrichtlinie.
Auth-Parameter	Wählen Sie den Authentifizierungsparameter für die Authentifizierungsanforderung aus. Sie können die Standardoptionen auswählen oder einen neuen Authentifizierungsparameter erstellen: ▪ X-sn-apikey: Authentifizierungsheader ▪ X-sn-apikey: Header des Abfrageparameters

Hinweis: Die ausgewählte Option muss im REST-Aufruf im Authentifizierungs-Header oder Abfrageparameter definiert werden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie ein Präfix für den API-Schlüssel hinzufügen möchten, öffnen Sie die von Ihnen ausgewählte Authentifizierungsparameterdatei, und geben Sie an **Präfix** Feld.

e. Bestätigen Sie das Formular.

2. Erstellen Sie einen REST-API-Schlüssel.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**an.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die folgenden Felder aus:

API-Schlüssel

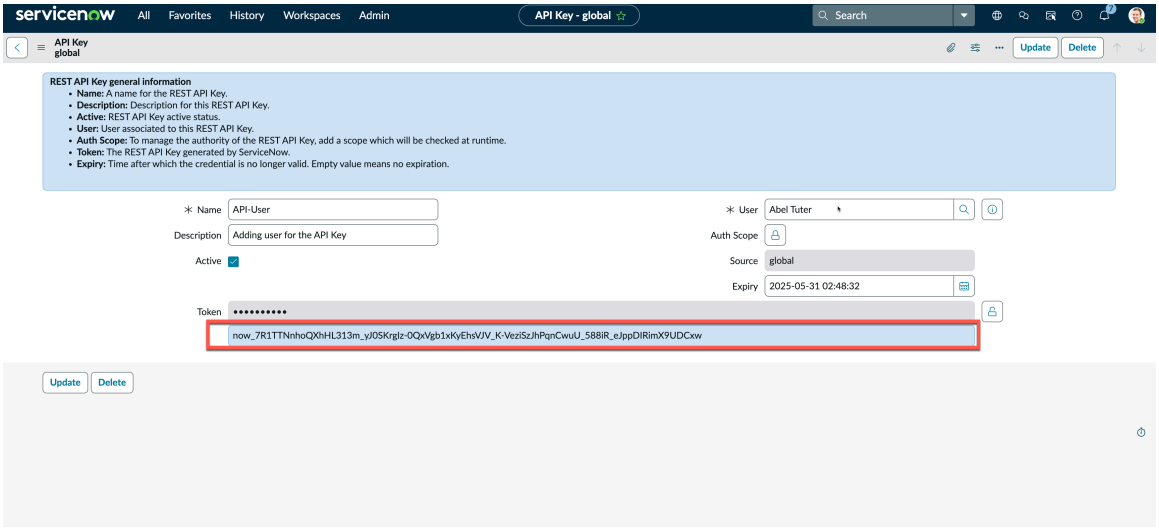
Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST API-Schlüssels zu verwalten.
Token	Der von generierte REST-API-Schlüssel ServiceNow AI Platform. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeit, nach der die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf. **Hinweis:** Weitere Informationen zum Ablauf des Tokens finden Sie unter Token-Ablauf wird bereinigt.

d. Bestätigen Sie das Formular.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Öffnen Sie den Datensatz, der erstellt wurde, um das von generierte Token anzuzeigen ServiceNow AI Platform Für den Anwender.



3. Erstellen Sie eine REST API-Zugriffsrichtlinie.

a. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**an.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die Felder aus.

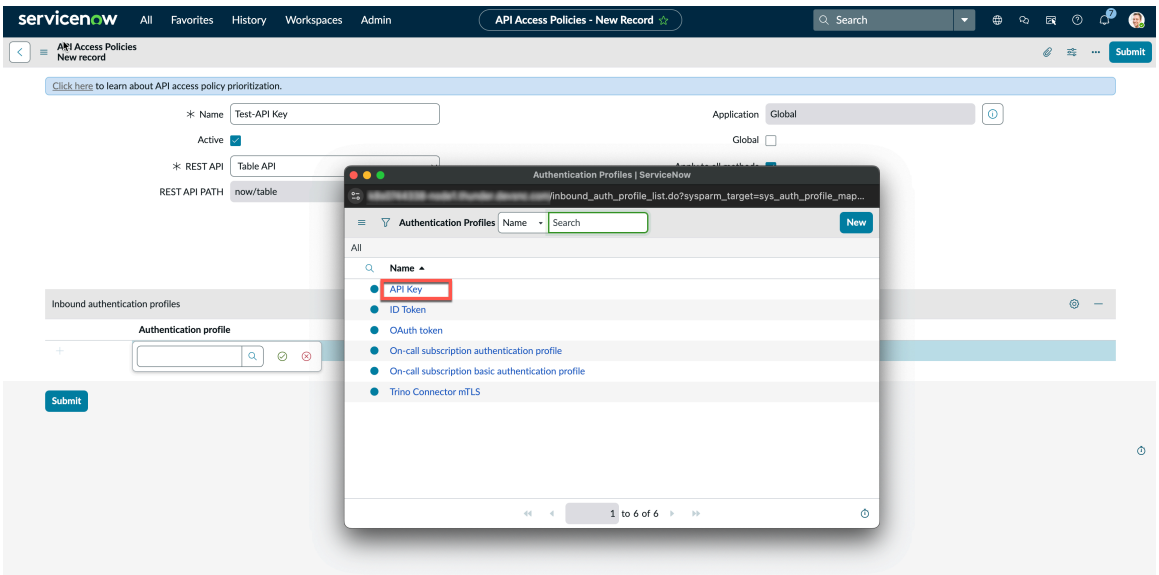
API-Zugriffsrichtlinien

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
REST-API	Die REST-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API** .
REST-API-PFAD	API-Pfad der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **Now/Anhang** .
HTTP-Methode	Für die Interaktion mit der API verwendete Methode. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1** . Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST-API erstellen möchten, müssen Sie für jede Version einzelne Richtlinien erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ressource	Untergeordnete Ressource der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **/Now/attachment**
Anwendung	Umfang der Anwendung.
Global	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie auf alle Methoden, Versionen und Ressourcen für die API anzuwenden. **Hinweis:** Token-basierte Authentifizierung ist in der globalen REST API-Richtlinie nicht zulässig.
Auf alle Methoden anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Ressourcen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Versionen anzuwenden.
Auf alle Versionen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Ressourcen anzuwenden.



d. Fügen Sie das erstellte API-Authentifizierungsprofil hinzu.

e. Bestätigen Sie das Formular.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können den REST-API-Aufruf mit dem x-sn-apikey (Token) senden, der von generiert wurde ServiceNow AI Platform Während der API-Schlüsselerstellung innerhalb des Headerparameters oder des Abfrageparameters basierend auf der Konfiguration für die Authentifizierung.

Warnung: Verwenden **VERÖFFENTLICHEN** Anforderung, wenn vertrauliche Informationen an den Server übermittelt werden.

Konfigurieren Sie HMAC – Token-basierte Authentifizierung

Konfigurieren Sie HMAC, um die Authentifizierung für REST API-Endpunkte zu unterstützen.

Vorbereitungen

Erforderliche Rolle: Administrator

Erforderliches Plugin: API-Schlüssel und HMAC-Authentifizierung (Com.Glide.tokenbased_auth)

Prozedur

1. Erstellen Sie eine HMAC-Konfiguration.

   a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **HMAC-Konfiguration**an.

   b. Wählen Sie **Neu**.

   Hinweis: Sie können auch verwenden **Standard-HMAC SHA256 Base64-Codierung** Wird bei der Installation des Plugins erstellt.

   c. Füllen Sie im Formular die folgenden Felder aus:

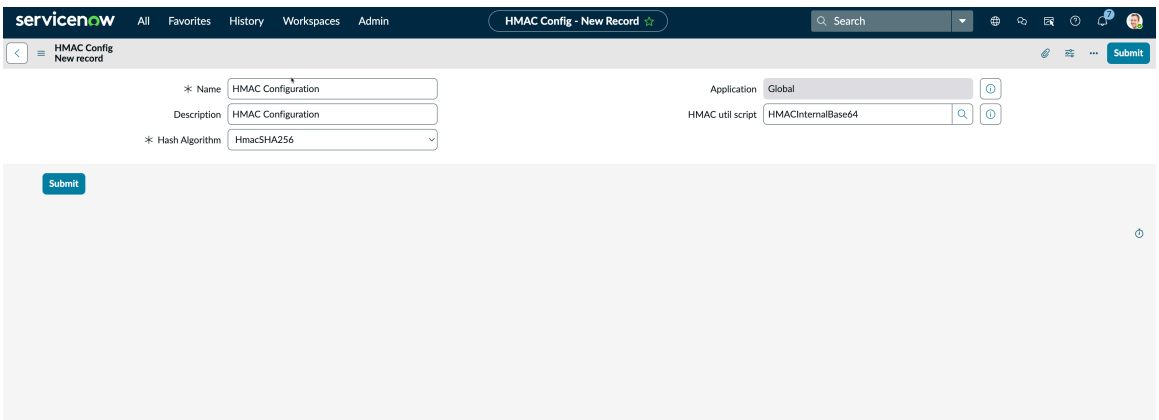
HMAC-Konfiguration

Feld	Beschreibung
Name	Name für die HMAC-Konfiguration.
Anwendung	Umfang der Konfiguration.
Beschreibung	Detaillierte Beschreibung der Konfiguration.
Hash-Algorithmus	Wählen Sie den Hash-Algorithmus aus. Verfügbare Optionen: ▪ HmacSHA256 ▪ HmacSHA384 ▪ HmacSHA512
HMAC-Hilfsskript	Dienstprogrammskript für HMAC.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn Sie die HMAC-Authentifizierung mit Anforderungstext, Zeitstempel und Geheimnis ohne Schlüssel-ID validieren, gehen Sie wie folgt vor: ▪ Erstellen Sie eine anwenderdefinierte Skripteinbindung als HMAC-Util-Skript ▪ Verwenden Sie diese Skripteinbindung, um den eingegebenen Zeitstempel und den Anforderungstext zu interpretieren. Für jedes freigegebene Geheimnis, das in erstellt wurde ServiceNow® Instanz ist eine Schlüssel-ID vorhanden. Sie müssen die Schlüssel-ID als Standardschlüssel-ID im HMAC-Authentifizierungsprofil konfigurieren.



d. Senden Sie den Datensatz ab.

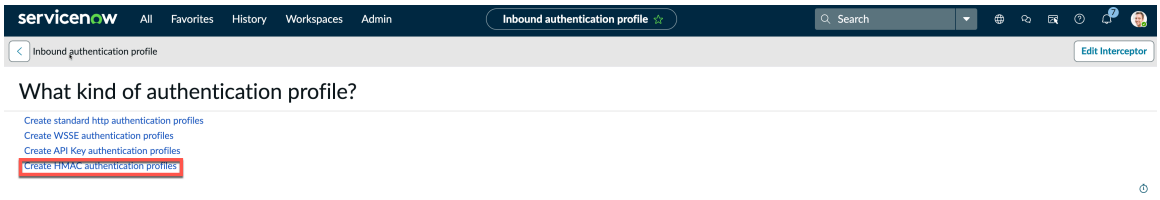
2. Erstellen Sie ein eingehendes Authentifizierungsprofil.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**an.

b. Wählen Sie **Neu**.
Das System zeigt die Meldung an Welche Art von Authentifizierungsprofil?

c. Wählen Sie Aus **Erstellen Sie HMAC-Authentifizierungsprofile** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



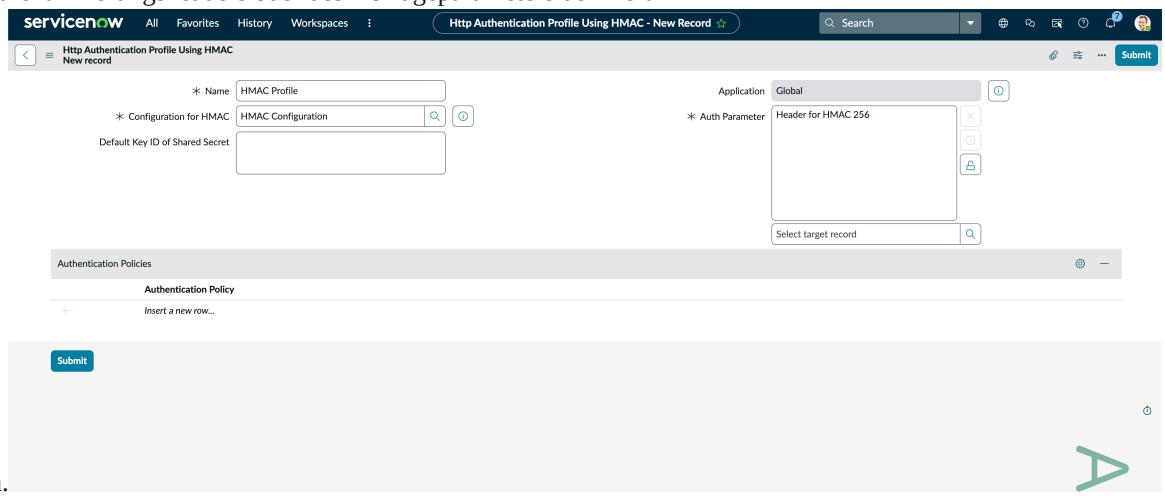
d. Füllen Sie im Formular die Felder aus.

HMAC-Authentifizierungsprofile

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Anwendung	Umfang der Authentifizierungsrichtlinie.
Konfiguration für HMAC	Wählen Sie die erstellte HMAC-Konfiguration aus.
Auth-Parameter	Wählen Sie den Authentifizierungsparameter für die Authentifizierungsanforderung aus. Sie können die Standardoptionen auswählen oder einen neuen Authentifizierungsparameter erstellen: ▪ X-sn-hmac-Signature-256: Authentifizierungsheader ▪ X-sn-hmac-Signature-256: Abfrageparameter
Standardschlüssel-ID des gemeinsamen Geheimnisses	Die Tokeninformationen, die in diesem Feld für die Verwendung von HMAC aktualisiert werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die ausgewählte Option muss im REST-Aufruf als Teil des Authentifizierungsheaders oder des Abfrageparameters definiert werden.



e. Bestätigen Sie das Formular.

3. Erstellen Sie ein HMAC-Geheimnis.

a. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-HMAC-Geheimnis**an.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die folgenden Felder aus:

REST-API-HMAC-Geheimnis

Feld	Beschreibung
Name	Name zur Identifizierung des geheimen HMAC-Geheimnisses der REST API.
Beschreibung	Beschreibung für das REST API-HMAC-Geheimnis.
Aktiv	Status des REST API-HMAC-Geheimnisses.
Anwender	Anwender, der dem REST API-HMAC-Geheimnis zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Schlüssel-ID	Schlüssel-ID, die als Teil des REST-Aufrufs gesendet werden muss. Schlüssel-ID wird nach dem Senden des Formulars generiert.
Gemeinsames Geheimnis	Freigegebene Geheimnisse des Anwenders. Zum Beispiel das Passwort.
Quelle	Quelle des Datensatzes.
Ablauf	Zeit, nach der die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

Automatische Übersetzung

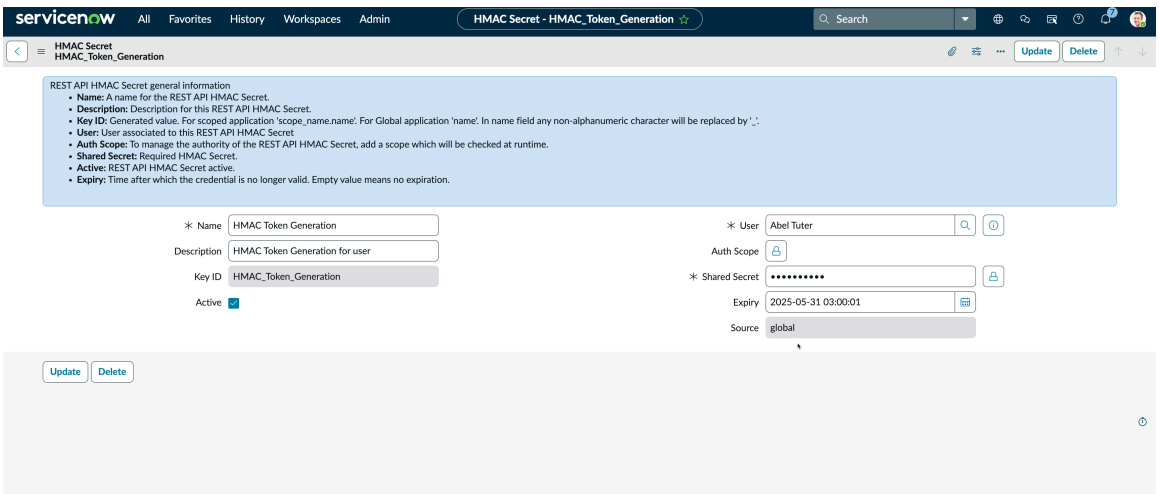
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Weitere Informationen zum Ablauf des Tokens finden Sie unter Token-Ablauf wird bereinigt.

d. Bestätigen Sie das Formular.

e. Öffnen Sie den erstellten Datensatz.

Suchen Sie die von generierte Schlüssel-ID ServiceNow AI Platform Für den Anwender.



Hinweis: Sie können die Schlüssel-ID, die während der Schlüssel-ID generiert wurde, dem Authentifizierungsprofil hinzufügen, das für HMAC erstellt wurde, wenn Sie den Authentifizierungs- oder Abfrageparameter für den API-Aufruf nicht angeben möchten.

4. Erstellen Sie eine REST API-Zugriffsrichtlinie.

a. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**an.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die Felder aus.

API-Zugriffsrichtlinien

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
REST-API	Die REST-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API** .
REST-API-PFAD	API-Pfad der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **Now/Anhang** .

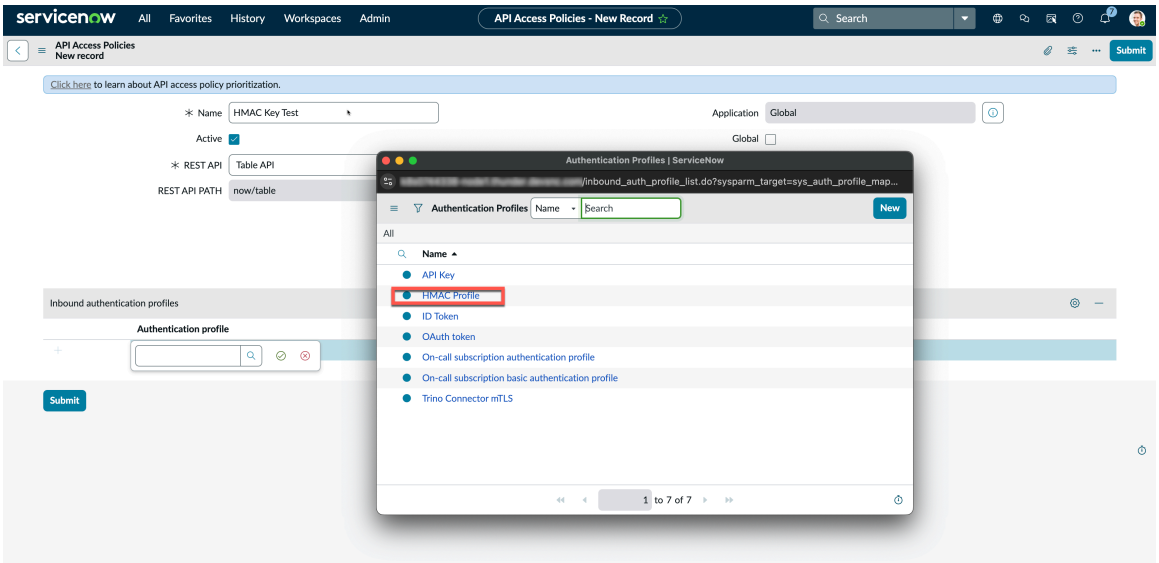
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
HTTP-Methode	Für die Interaktion mit der API verwendete Methode. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1** . Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST-API erstellen möchten, müssen Sie für jede Version einzelne Richtlinien erstellen.
Ressource	Untergeordnete Ressource der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **/Now/attachment**
Anwendung	Umfang der Anwendung.
Global	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie auf alle Methoden, Versionen und Ressourcen für die API anzuwenden. **Hinweis:** Token-basierte Authentifizierung ist in der globalen REST API-Richtlinie nicht zulässig.
Auf alle Methoden anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Methoden, Versionen und Ressourcen für die API anzuwenden.
Auf alle Ressourcen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Versionen anzuwenden.
Auf alle Versionen anwenden	Aktivieren Sie dieses Feld, um die Authentifizierungsrichtlinie für die API auf alle Ressourcen anzuwenden.

d. Fügen Sie das erstellte API-Authentifizierungsprofil hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Bestätigen Sie das Formular.
Sie können den REST API-Aufruf senden:

- Mit der x-sn-hmac-Signature-256, die von generiert wurde ServiceNow®
  Während der API-Schlüsselerstellung innerhalb des Headerparameters oder des Abfrageparameters basierend auf der Konfiguration für die Authentifizierung.
- Mit Pre-Request-Skript mit gemeinsam verwendetem Geheimnis als Teil der Anforderung.

> ⚠ **Warnung:** Verwenden **VERÖFFENTLICHEN** Anforderung, wenn vertrauliche Informationen an den Server übermittelt werden.

Token-Ablauf wird bereinigt

Details zum Bereinigen des Tokenablaufs mithilfe verschiedener Systemeigenschaften.

Sobald der API-Schlüssel oder das HMAC-Geheimnis abläuft, werden die Details 7 Tage lang aufbewahrt. Eine geplante Aufgabe `Abgelaufene Anmeldeinformationen für Token-Authentifizierung bereinigen` Löscht danach die abgelaufenen API-Schlüssel oder HMAC-Geheimnisse. Sie können dieses Verhalten konfigurieren und das Löschen mit den folgenden Eigenschaften steuern:

- **com.snc.platform.security.token.auth.cleanup** : Verwenden Sie diese Eigenschaft, wenn Sie abgelaufene API-Schlüssel und HMAC-Token löschen möchten. Standardmäßig `Wahr` .
- **com.snc.platfrom.security.token.auth.days.expired.api_key.is.kept** : Legen Sie den Wert basierend auf Ihrer Anforderung fest, um die Anzahl der Tage zu bestimmen, die abgelaufen bleiben sollen `API` Token im System. Standardmäßig 7.
- **com.snc.platfrom.security.token.auth.days.expired.hmac_key.is.kept** : Legen Sie den Wert basierend auf Ihrer Anforderung fest, um die Anzahl der Tage zu bestimmen, die abgelaufen bleiben sollen `HMAC` Token im System. Standardmäßig 7.

Um zur Tokenablaufeigenschaft zu navigieren, geben Sie ein `sys_properties.list` Suchen Sie in der Navigationsleiste nach den folgenden Eigenschaften. Ändern Sie den Ablauf basierend auf Ihren Anforderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API-Zugriffsrichtlinie

Die API-Zugriffsrichtlinie definiert die Berechtigungen und die Dauer des Zugriffs auf eine API.

Mit der API-Zugriffsrichtlinie können Sie den Zugriff auf eingehend beschränken ServiceNow® APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie.

Im Folgenden finden Sie die Unterstützung der dreistufigen Authentifizierungsrichtlinie für die nicht interaktiven Sitzungen:

- **REST-API** : Der Administrator kann eine globale API-Authentifizierungsrichtlinie oder eine API-spezifische Authentifizierungsrichtlinie definieren.
- **SOAP-API** : Der Administrator kann eine globale API-Authentifizierungsrichtlinie oder eine API-spezifische Authentifizierungsrichtlinie definieren.
- **System-/Exportprozessor** : Der Administrator kann fünf Basissystemauthentifizierungsprofile definieren, die verwendet werden können, um das Authentifizierungsprofil auf die API-Authentifizierungsrichtlinie für Prozessoren oder die prozessorspezifische Authentifizierungsrichtlinie anzuwenden.

Hinweis: Wenn Sie eine globale Authentifizierungsrichtlinie hinzufügen, gilt die Richtlinie für alle REST APIs, SOAP APIs oder System-/Exportprozessoren.

Im Folgenden finden Sie die automatisch installierten Plugins für API-Richtlinien und Authentifizierungsbereich:

- Com.Glide.Rest.Policy
- Com.Glide.SOAP.Policy
- com.glide.processor.policy
- com.glide.rest.auth.scope

Sie können die standardmäßige globale Sperrrichtlinie konfigurieren oder eine anwenderdefinierte API-Zugriffsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Und wenden Sie Filterkriterien an, die Filterbedingungen oder Abfragen enthalten, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden.

Die folgenden API-Zugriffsrichtlinien werden in unterstützt ServiceNow®:

- REST API-Zugriffsrichtlinien
- Zugriffsrichtlinien für SOAP-API

Informationen zu Richtlinien im Zusammenhang mit Exportprozessoren finden Sie unter Zugriffsrichtlinie für System- oder Exportprozessoren.

REST API-Zugriffsrichtlinien

Mit REST API-Zugriffsrichtlinien können Sie den Zugriff auf eingehende REST APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie beschränken.

Eine REST-API, auch als RESTful-API bezeichnet, ist eine Art von Anwendungsprogrammierschnittstelle (API), die den Richtlinien des REST-Architekturstils

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

entspricht. REST APIs bieten ein hohes Maß an Flexibilität, wodurch sie im gesamten Web verbreitet ist.

Filterkriterien enthalten Filterbedingungen oder Abfragen, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden.

Sie können die standardmäßige globale Sperrrichtlinie konfigurieren oder eine anwenderdefinierte API-Zugriffsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Sie können beispielsweise eine anwenderdefinierte API-Zugriffsrichtlinie erstellen, die nur den OAuth 2,0-Authentifizierungstyp aus einem angegebenen IP-Adressbereich zulässt. Authentifizierungsanforderungen anderer Authentifizierungstypen und Zugriffsanforderungen von anderen IP-Adressen als den angegebenen IP-Adressen werden abgelehnt.

Aktivieren REST API-Zugriffsrichtlinie

Sie können aktivieren REST API-Zugriffsrichtlinie Plugin (Com.Glide.Rest.Policy), wenn Sie die Administratorrolle innehaben. Die Anwendung enthält Demodaten und installiert zugehörige ServiceNow® Store-Anwendungen und Plugins, sofern sie nicht bereits installiert sind.

Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit installiert REST API-Zugriffsrichtlinie :

- Plugins: com.gilde.auth.profile, com.snc.adaptive_authentication, com.snc.platform.security.oauth
- Tabellen: sys_api_Access_Policy, sys_auth_Profile_Mapping, auth_Policy_Mapping, inbound_auth_Profile, std_http_auth.

Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach REST API-Zugriffsrichtlinie Plugin (Com.Glide.Rest.Policy) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

   Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Authentifizierungsprofil

Erstellen Sie ein Authentifizierungsprofil, und fügen Sie dem Profil eine oder mehrere Authentifizierungsrichtlinien hinzu. Sie können auch konfigurieren **ID-Token** Und **OAuth-Token** Standardmäßig verfügbare Authentifizierungsprofile.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: Sie können Authentifizierungsrichtlinien, IP-Bereich, rollenbasiert, anwenderbasiert usw. mit gegenseitiger Authentifizierung und anwenderdefinierter Authentifizierung anwenden.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**an.
2. Wählen Sie **Neu**.
   Das System zeigt die Meldung an. Welche Art von Authentifizierungsprofil?
3. Wählen Sie Aus **Erstellen Sie Standard-HTTP-Authentifizierungsprofile** .
4. Füllen Sie im Formular die Felder aus.

Formular „Standardauthentifizierungsprofil“

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Beschreibung	Beschreibung der Authentifizierungsrichtlinie.
Aktiv	Option zum Aktivieren der Authentifizierungsrichtlinie.
Anwendung	Umfang der Authentifizierungsrichtlinie.
Typ	Typ der verfügbaren Authentifizierung. Sie können auswählen **Standardauthentifizierung** , **ID-Token** , **Zertifikatbasierte Authentifizierung** , Oder **OAuth** .
OAuth-Entität	OAuth-Entitätsprofil. Dieses Feld wird nur angezeigt, wenn **ID-Token** Oder **OAuth** Ist aus ausgewählt **Typ** .

5. Doppelklicken Sie auf **Neue Zeile einfügen**.
6. Wählen Sie eine Authentifizierungsrichtlinie aus der Liste aus, und wählen Sie das Speichern-Symbol .

Hinweis: Wählen Sie nicht Zugriffsrichtlinie zulassen oder Zugriffsrichtlinie verweigern. Diese Richtlinien sind nur für Anwenderanmeldungen vorgesehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können eine oder mehrere Authentifizierungsrichtlinien für ein Authentifizierungsprofil hinzufügen.

Hinweis:

Header authentifizieren [WWW-Authenticate].

Wenn die REST-API-Zugriffsrichtlinie aktiv ist, wird das zuletzt zugeordnete Authentifizierungsprofil im Authentifizierungs-Header zurückgegeben. Wenn der Server alle Authentifizierungsschemata zurückgeben soll, verwenden Sie glide.security.response.authenticate.header.auth_profile.first_scheme_only Eigenschaft und legen Sie sie auf fest **Falsch** . Die Antwort wird mit mehreren Headern zurückgegeben. Zum Beispiel:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Erstellen Sie EINE REST-API-Zugriffsrichtlinie

Erstellen Sie eine API-Zugriffsrichtlinie, und ordnen Sie ein Authentifizierungsprofil zu, um den Authentifizierungstyp für eine REST-API einzuschränken. Sie können beispielsweise eine API-Zugriffsrichtlinie erstellen, die nur die ID-Token-Authentifizierung für eine REST-API zulässt.

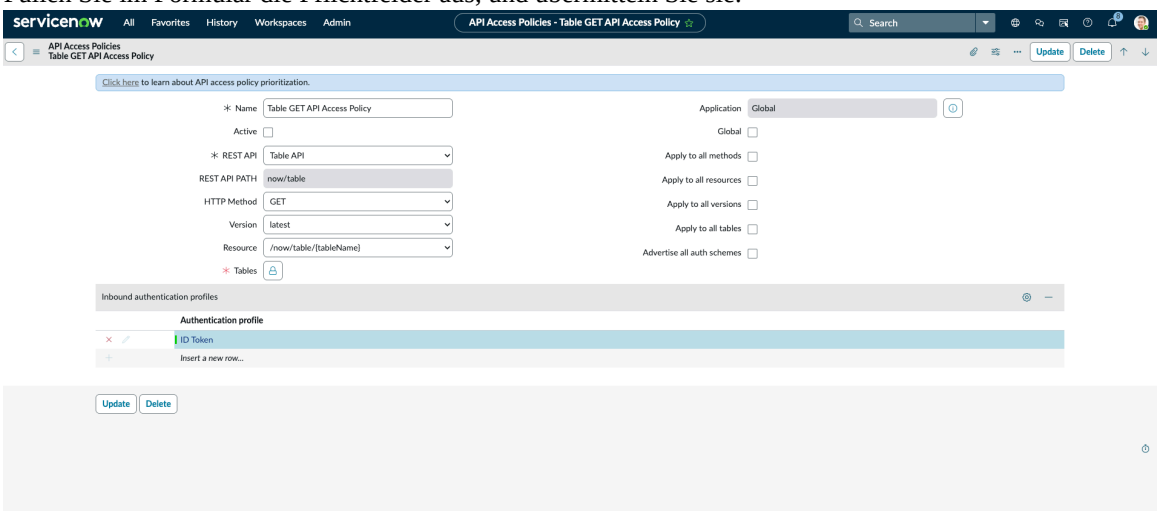
Vorbereitungen

Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Erstellen Sie ein Authentifizierungsprofil .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien**an.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Pflichtfelder aus, und übermitteln Sie sie.



Hinweis: Sie müssen das übermittelte Formular erneut öffnen, um zusätzliche Felder auszufüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API-Zugriffsrichtlinien

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
REST-API	Die REST-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **Anhang-API** .
REST-API-PFAD	API-Pfad der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **Now/Anhang** .
HTTP-Methode	Für die Interaktion mit der API verwendete Methode. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt.
Version	Version der API. Beispiel: **v1** . Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. **Hinweis:** Wenn Sie eine Authentifizierungsrichtlinie für alle Versionen einer REST-API erstellen möchten, müssen Sie für jede Version einzelne Richtlinien erstellen.
Ressource	Untergeordnete Ressource der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: **/Now/attachment**
Tabelle	Die Tabellen, für die die API-Zugriffsrichtlinie gilt. Diese Option gilt nur für Richtlinien für *Tabelle* API.
Anwendung	Umfang der Anwendung.
Global	Option zum Anwenden der Richtlinie auf alle Methoden, Versionen und Ressourcen für die API.
Auf alle Methoden anwenden	Option zum Anwenden der Richtlinie auf alle Methoden, Versionen und Ressourcen für die API.
Auf alle Ressourcen anwenden	Option zum Anwenden der Richtlinie auf alle oder die API-Ressourcen.
Auf alle Versionen anwenden	Option zum Anwenden der Richtlinie auf alle oder die API-Versionen.
Auf alle Tabellen anwenden	Option zum Anwenden der Richtlinie auf alle Tabellen. Diese Option gilt nur für Richtlinien für *Tabelle* API.
A Veröffentlichen Sie alle Authentifizierungsschemata	Bestimmt, ob WWW-Authentifizierung Der Header enthält alle konfigurierten Authentifizierungsschemas. Wenn auf festgelegt Falsch (Standard) enthält der Header nur das zuletzt konfigurierte Authentifizierungsprofil in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

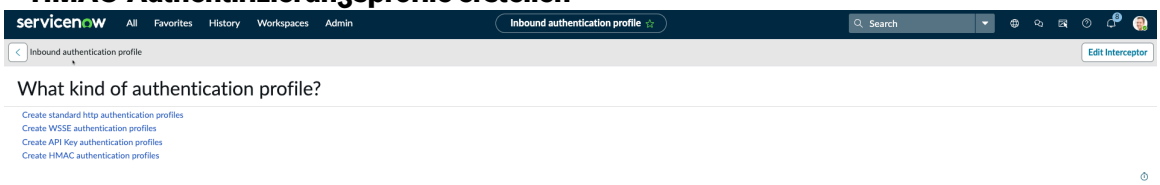
Feld	Beschreibung
	Richtlinie. Wenn auf festgelegt Wahr , Der Header listet alle konfigurierten Authentifizierungsschemata auf.

Hinweis: Weitere Informationen zur Priorisierung der API-Zugriffsrichtlinie finden Sie unter Priorisierung der API-Zugriffsrichtlinie.

4. Doppelklicken Sie auf **Neue Zeile einfügen**.
5. Wählen Sie ein eingehendes Authentifizierungsprofil aus der Liste aus, und wählen Sie das Speichern-Symbol .
   Sie können beispielsweise hinzufügen **Standardauthentifizierung** , **ID-Token** , **Zertifikatbasierte Authentifizierung** , **OAuth** Oder **WSSE-Authentifizierung** .

   a. Um ein oder mehrere eingehende Authentifizierungsprofile hinzuzufügen, wählen Sie aus **Neu** Um ein neues Profil zu erstellen.

   b. Wählen Sie Aus **Welche Art von Authentifizierungsprofilen?** .
      - **Standardmäßiges http-Authentifizierungsprofil erstellen**
      - **WSSE-Authentifizierungsprofile erstellen**
      - **Authentifizierungsprofile für API-Schlüssel erstellen**
      - **HMAC-Authentifizierungsprofile erstellen**



   c. Speichern Sie den Datensatz nach dem Erstellen des Authentifizierungsprofils.

6. Wählen Sie Aus **Übermitteln** Zum übermitteln der REST API-Zugriffsrichtlinie.

Priorisierung der API-Zugriffsrichtlinie

Erfahren Sie mehr über die Logik der Richtlinienpriorisierung, wenn mehrere API-Zugriffsrichtlinien für konfiguriert sind ServiceNow® Instanz.

API-Zugriffsrichtlinien werden basierend auf dem Typ der auf Ihrem festgelegten REST API-Richtlinie priorisiert ServiceNow® Instanz.

Der Ansatz definiert unterschiedliche Gewichtungen für jeden Teil der API, z. B. Methode, Ressource und Version.

Die API-Richtlinie wird zuerst für „nicht global“ und dann für „global“ priorisiert. Mit anderen Worten: Eine nicht globale Zugriffsrichtlinie überschreibt immer eine globale API-Zugriffsrichtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Priorisierungslogik lautet wie folgt:

Priorisierung

Felder	Priorität	Priorisierungslogik
Methode, Ressource und Version	1	Wenn die 3 Felder mit der Richtlinie übereinstimmen, hat diese Richtlinie die erste Priorität.
Methode+-Ressource	2	Wenn die 2 Felder mit der Richtlinie übereinstimmen, hat diese Richtlinie die erste Priorität.
Ressource + Version	3	Wenn die 2 Felder zusammen mit dem Feld **Auf alle Methoden anwenden** Stimmt mit der Richtlinie überein, dann hat diese Richtlinie die dritte Priorität.
Ressource	4	Wenn das Feld zusammen mit dem Feld **Auf alle Methoden anwenden** Stimmt mit der Richtlinie überein, dann hat diese Richtlinie die 4. Priorität.
Methode + Version	5	Wenn die 2 Felder zusammen mit dem Feld **Auf alle Ressourcen anwenden** Stimmt mit der Richtlinie überein, dann hat diese Richtlinie die 5. Priorität.
Methode	6	Wenn das Feld zusammen mit dem Feld **Auf alle Ressourcen anwenden** Stimmt mit der Richtlinie überein, dann hat diese Richtlinie die 5. Priorität.
Version	7	Wenn das Feld zusammen mit den Feldern **Auf alle Methoden anwenden** Und **Auf alle Versionen anwenden** Stimmt mit der Richtlinie überein, dann hat diese Richtlinie die 7. Priorität.
Global und auf alle Methoden anwenden	8	Wenn die Felder **Global** Ist Wahr Und **Auf alle Methoden anwenden** Ist Falsch Dann hat diese Richtlinie die 8. Priorität.
Global und auf alle Methoden anwenden	9	Wenn die Felder **Global** Ist Wahr Und **Auf alle Methoden anwenden** Ist Wahr Dann hat diese Richtlinie die 9. Priorität.

REST-API-Authentifizierungsbereich

Verwenden Sie den REST API-Authentifizierungsbereich, um Zugriff auf eine bestimmte REST API bereitzustellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Früher ist jedes Zugriffstoken oder OIDC-Token mit verknüpft Anwenderaccount Bereich, der vollen Zugriff auf die REST-APIs des Anwenders hat. Von Zurich Release, um nur Zugriff auf die bestimmten REST-APIs zu gewähren, den **REST API-Authentifizierungsbereich** Wird eingeführt.

Nach dem Erstellen des Datensatzes für den REST-API-Authentifizierungsbereich müssen Sie für den Zugriff auf diese REST-API denselben Authentifizierungsbereich der OAuth-Entität zuordnen, die Zugriff auf diese REST-API haben soll. Für eine neue OAuth-Entität ist der Standardauthentifizierungsbereich leer.

Hinweis: Sofern Sie keinen Datensatz für den REST API-Authentifizierungsbereich haben, kann auf die REST API von allen gültigen OAuth-Entitäten zugegriffen werden.

Sie müssen den Authentifizierungsbereich innerhalb der OAuth-Entität manuell verknüpfen. Die Anwenderaccount Ist ein spezieller Bereich. Wenn er einer OAuth-Entität zugeordnet ist, kann er auf jede API zugreifen, auch wenn Sie einen REST API-Authentifizierungsbereichsdatensatz mit einem anderen Authentifizierungsbereich erstellt haben.

Weitere Informationen zur Verwendung des API-Authentifizierungsbereichs in der neuen Experience für eingehende Integrationen finden Sie unter Eingehende Integrationen.

Hinweis:

- Nachdem der REST-API-Authentifizierungsbereich aktiviert und dem Authentifizierungsbereich für die REST-API hinzugefügt wurde, kann das vorhandene OAuth-Token nicht mehr auf diese API zugreifen, es sei denn, der Administrator fügt diesen Authentifizierungsbereich der entsprechenden OAuth-Entität hinzu
- Der Administrator ist dafür verantwortlich, sicherzustellen, dass oauth_Entity über den richtigen Authentifizierungsbereich verfügt, nachdem der Authentifizierungsbereich mit der REST-API verknüpft wird.
- Von ausgestellte OAuth-Zugriffstoken ServiceNow Unterstützt den Authentifizierungsbereich.
- OIDC-Token, das nicht von ausgegeben wird ServiceNow Wird von validiert ServiceNow.
- Das OIDC-Token hat seinen Bereich aus IDP, wenn Sie ein ID-Token benötigen. Hier ist der Authentifizierungsbereich für ServiceNow Anstelle von Drittpartei (IdP).

Konfigurationen für REST API-Bereich

Führen Sie die folgenden Aufgaben aus, um den REST API-Bereich zu konfigurieren:

- Erstellen Sie einen Authentifizierungsbereich
- Verknüpfen Sie den Authentifizierungsbereich mit der REST-API
- Authentifizierungsbereich mit OAuth-Entität verknüpfen
- Führen Sie einen OAuth-Flow aus, um das OAuth-Zugriffstoken abzurufen
- Verwenden Sie das OAuth-Zugriffstoken, um den API-Aufruf durchzuführen

Aktivieren Sie den REST API-Authentifizierungsbereich

Sie können das Plugin „REST API-Authentifizierungsbereich“ (com.glide.rest.auth.scope) aktivieren, um die OAuth-Entität mit Authentifizierungsbereichen zu verknüpfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Installieren Sie die folgenden Plugins:

- OAuth 2.0
- REST API-Provider
- Authentifizierungsbereich
- REST-API-Bereich

Hinweis: Die *REST API Scope*Plugin wird als Teil von hinzugefügt Tokyo Release.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie den REST API-Authentifizierungsbereich (`com.glide.rest.auth.scope`) Plugin mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

   Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Eigenschaften und Tabellen des REST API-Authentifizierungsbereichs

Das Plugin „REST API-Authentifizierungsbereich“ (com.glide.rest.auth.scope) enthält die folgenden Systemeigenschaften, Tabellen und Skripts.

Eigenschaften des REST API-Authentifizierungsbereichs

Der REST API-Authentifizierungsbereich fügt die folgenden Systemeigenschaften hinzu.

Eigenschaften

Name	Beschreibung
`com.glide.rest.api.auth.scope.check.enable`	Diese Eigenschaft wird verwendet, um die Prüfung des Authentifizierungsbereichs auf Plattformebene zu deaktivieren. Bei „falsch“ wird während der Laufzeit die Überprüfung des Authentifizierungsbereichs übersprungen, unabhängig davon, ob sie mit der REST-API verknüpft ist oder nicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften (Fortsetzung)

Name	Beschreibung
	Standardmäßig ist diese Eigenschaft auf „wahr“ festgelegt. Diese Eigenschaften werden verwendet, wenn Sie das vorherige Release-Verhalten wiederherstellen möchten.
`com.glide.oauth.token.scope.useraccount`	Diese Eigenschaft wird nur verwendet, wenn `useraccount` Der Authentifizierungsbereich wird gelöscht und vom Endanwender manuell wieder hinzugefügt. In diesem Fall die SYS-ID für `useraccount` Ist geändert. Diese Eigenschaft muss auf die neue sys_ID aktualisiert werden Während der Laufzeit wird anstelle des Namens des Authentifizierungsbereichs die SYS-ID des Authentifizierungsbereichs verwendet.

REST API-Authentifizierungsbereichstabellen

REST API-Authentifizierungsbereich: Die folgenden Tabellen.

Tabellen

Name	Beschreibung
Authentifizierungsbereich (sys_auth_scope)	Diese Tabelle definiert den Authentifizierungsbereich, der mit der REST API und der OAuth-Entität verknüpft werden kann. Der Name des Authentifizierungsbereichs muss eindeutig und global sein.
REST API-Authentifizierungsbereich (sys_api_Access_scope)	Diese Tabelle verknüpft die REST-API mit dem Authentifizierungsbereich.

Konfigurieren Sie den REST API-Authentifizierungsbereich

Verknüpfen Sie die OAuth-Entität mit einem Authentifizierungsbereich, um das Token für den Zugriff auf die REST-APIs zu verwalten, die mit dem Authentifizierungsbereich verknüpft sind.

Vorbereitungen
Installieren Sie die folgenden Plugins:

- OAuth 2.0
- REST API-Provider
- Authentifizierungsbereich
- REST-API-Authentifizierungsbereich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die *REST API Auth Scope*Plugin wird als Teil von hinzugefügt Tokyo Release.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **API-Authentifizierungsbereiche** > **REST-API-Authentifizierungsbereich**an.
   Die Seite REST API-Authentifizierungsbereiche wird angezeigt.
2. Um einen neuen REST API-Authentifizierungsbereich zu konfigurieren, klicken Sie auf **Neu** .
3. Füllen Sie im Formular die Felder aus.

REST-API-Authentifizierungsbereich

Name	Ein eindeutiger Name, der den REST API-Authentifizierungsbereich identifiziert.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die Konfiguration zu aktivieren.
Anwendung	Schreibgeschützter Anwendungsbereich.
REST-API	Die REST-API, auf die der Authentifizierungsbereich angewendet wird. Zum Beispiel die Tabellen-API.
Authentifizierungsbereich	Wählen Sie den Authentifizierungsbereich über das Suchsymbol aus.
REST-API-PFAD	API-Pfad der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: Now/table.
HTTP-Methode	Für die Interaktion mit der API verwendete Methode. Wählen Sie die Methode aus der Dropdown-Liste aus. Sie können deaktivieren **Wenden Sie den Authentifizierungsbereich auf alle HTTP-Methoden in dieser API an** Feld im Formular manuell, um die Methode auszuwählen.
REST API-Version	Version der API. Beispiel: V1. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Sie können deaktivieren **Wenden Sie den Authentifizierungsbereich auf alle Versionen in dieser API an** Feld im Formular manuell, um die Version auszuwählen.
Ressource	Untergeordnete Ressource der REST-API. Dieses Feld wird basierend auf der ausgewählten REST-API automatisch ausgefüllt. Beispiel: /Now/table. Sie können deaktivieren **Wenden Sie den Authentifizierungsbereich auf alle Ressourcen in dieser API an** Feld im

Automatische Übersetzung

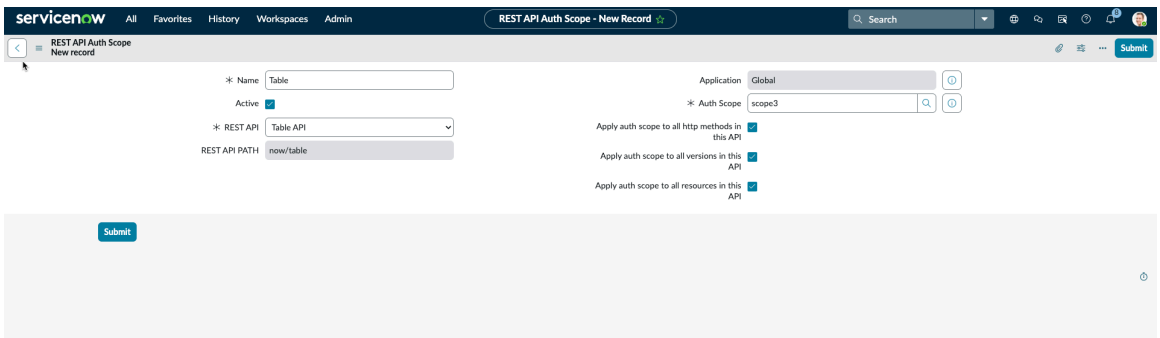
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Formular manuell, um die Ressourcen auszuwählen.
Authentifizierungsbereich auf alle HTTP-Methoden in dieser API anwenden	Wenn diese Option aktiviert ist, wird der Authentifizierungsbereich auf alle HTTP-Methoden in der API angewendet.
Authentifizierungsbereich auf alle Versionen in dieser API anwenden	Wenn aktiviert, wird der Authentifizierungsbereich auf alle Versionen in der API angewendet.
Authentifizierungsbereich auf alle Ressourcen in dieser API anwenden	Wenn diese Option aktiviert ist, wird der Authentifizierungsbereich auf alle Ressourcen in der API angewendet

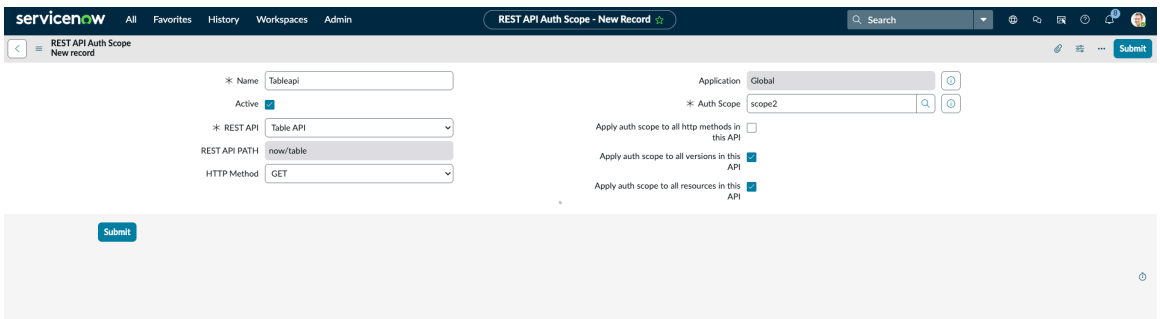
4. Klicken Sie auf **Absenden**.
   Basierend auf der ausgewählten REST-API und dem Authentifizierungsbereich ruft die APIs Informationen ab, die für den Bereich spezifisch sind.

Example: Erwägen Sie die Erstellung von drei REST API-Authentifizierungsbereichen für die Tabellen-API

Der erste Authentifizierungsbereich wird dem zugeordnet **Tabellen-API** Wenn alle HTTP-Methoden, Versionen und Ressourcen aktiviert sind.

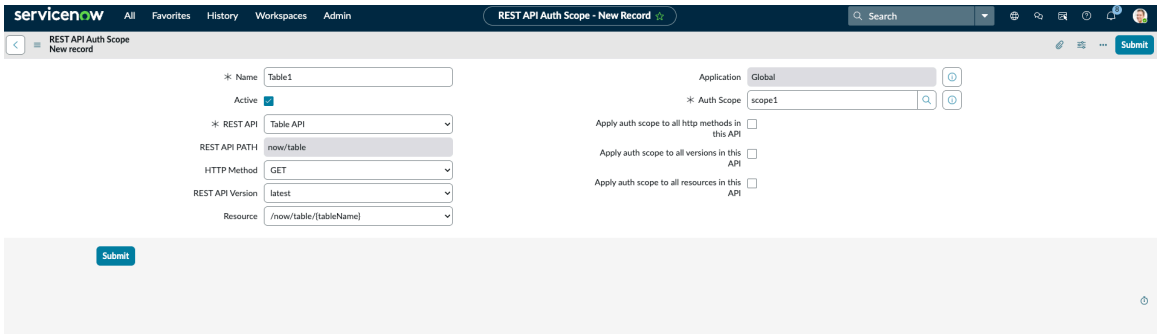


Der zweite Authentifizierungsbereich wird dem zugeordnet **Tabellen-API** Mit allen Versionen und Ressourcen aktiviert. Sie wählen jedoch die HTTP-Methode aus, in diesem Beispiel die **ABRUFEN** Methode.



Der dritte Authentifizierungsbereich wird dem zugeordnet **Tabellen-API** Ohne aktivierte HTTP-Methoden, -Versionen und -Ressourcen. Sie wählen die HTTP-Methode, die Version und die Ressource jedoch manuell aus. In diesem Beispiel lautet die HTTP-Methode **ABRUFEN** , REST API-Version ist **Aktuell** , Und Ressource ist `/Now/table/{tableName}` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn alle diese Authentifizierungsbereiche erstellt wurden, können Sie verwenden **ABRUFEN** Methode mit allen drei Bereichen, aber für **VERÖFFENTLICHEN** , **PLATZIEREN** , **LÖSCHEN** , Oder **PATCH** Nur Methoden **Umfang3** Kann verwendet werden.

REST-API-Bereich – Fehlerbehebung

Problembehebungsaktionen können bei der Lösung gängiger Probleme beim Einrichten oder Ausführen des REST API-Bereichs helfen.

Problembehandlung

Problem	Aktion
DIE REST-API ist mit dem Authentifizierungsbereich verknüpft. Zur Laufzeit wird jedoch keine Überprüfung des Authentifizierungsbereichs durchgeführt, auch wenn die Bearer-Token-Authentifizierung verwendet wird.	• Stellen Sie sicher, dass der Datensatz „sys_api_Access_Policy“ aktiv ist. Zur Laufzeit werden inaktive Datensätze ignoriert. • Überprüfen Sie, ob die Eigenschaft vorhanden ist `com.glide.rest.api.auth.scope.check.enable`ist auf „falsch“ festgelegt. • Überprüfen Sie, ob das OAuth-Token hat Anwenderaccount Authentifizierungsbereich.
REST-API ist mit verknüpft `auth_scope1`, Jedoch das Zugriffstoken, das hat `auth_scope2`Kann auch darauf zugreifen.	• Überprüfen Sie, ob dieser Datensatz aktiv ist. • Überprüfen Sie auf diesen REST, und überprüfen Sie, ob andere Datensätze die gleichen APIs, aber verschiedene Anwendungsmethoden, Versionen oder Ressourcen haben.
DIE REST-API ist mit dem Authentifizierungsbereich verknüpft, zur Laufzeit wird jedoch keine Überprüfung des Authentifizierungsbereichs für durchgeführt `basicAuth`Und `mutualAuth`.	Dies wird erwartet, da der REST-API-Authentifizierungsbereich nur für das OAuth-Zugriffstoken oder OIDC-Token gilt. BasicAuth, Sitzungs-Cookie und zertifikatbasierte Authentifizierung werden nicht angewendet.
REST-API-Aufruf gibt 403 zurück, wenn das OAuth-Zugriffstoken verwendet wird.	Überprüfen Sie, ob die Fehlermeldung „erforderlicher api-Zugriffsbereich fehlt“ angezeigt wird. Wenn gefunden, schlägt die Überprüfung des Authentifizierungsbereichs für diese REST API fehl

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung (Fortsetzung)

Problem	Aktion
Vordefiniert Anwenderaccount Wurde gelöscht und kann nicht sicher wiederhergestellt werden.	Exportieren Anwenderaccount Als xml Aus der anderen Instanz importieren oder erstellen Anwenderaccount Und ändern Sie die Systemeigenschaft *glide.oauth.token.scope.useraccount*Zum neu erstellten sys_ID-Datensatz.

Häufige Fragen

Im Folgenden finden Sie einige der häufig gestellten Fragen bei der Verwendung des REST API-Authentifizierungsbereichs:

Kann ein OAuth-Token mit mehreren Authentifizierungsbereichen verknüpft werden?

Ja, eins oauth_Entität Kann mit mehreren Authentifizierungsbereichen verknüpft werden, jedes von diesem ausgestellte OAuth-Token oauth_Entität Hat dieselben Authentifizierungsbereiche.

Können verschiedene OAuth-Token mit verschiedenen Authentifizierungsbereichen auf dieselbe REST-API zugreifen?

Ja, für dieselbe REST-API kann sie von verschiedenen Authentifizierungsbereichen aufgerufen werden. Solange ein Authentifizierungsbereich übereinstimmt, gibt der Authentifizierungsbereich die Ergebnisse zurück.

Kann OAuth-Zugriffstoken mit aufrufen Anwenderaccount **Zugriff auf REST APIs des Authentifizierungsbereichs?**

Ja, die Anwenderaccount Hat vollständigen Zugriff auf den Authentifizierungsbereich.

Kann der OAuth-Zugriffstoken-OAuth-Bereich dynamisch geändert werden?

Ja, der Geltungsbereich der Authentifizierung ist nicht mit dem Zugriffstoken in hartcodiert oauth_credential Tabelle. Stattdessen wird der Authentifizierungsbereich von verknüpft abgerufen oauth_Entität Während der Laufzeit.

Kann das OAuth-Token nach der Aktualisierung dieselben Authentifizierungsbereiche beibehalten?

Ja, der Authentifizierungsbereich ändert sich nach der Token-Aktualisierung nicht, es sei denn oauth_admin Ändern Sie den Authentifizierungsbereich, der mit verknüpft ist oauth_Entität .

Vordefiniert Anwenderaccount **Der Datensatz des Authentifizierungsbereichs wird gelöscht. Kann ein neuer Authentifizierungsbereich mit dem Namen sein** Anwenderaccount **Erstellt werden?**

Erstellen eines neuen Authentifizierungsbereichs mit demselben Anwenderaccount Funktioniert nicht. In der Laufzeit wird verwendet sys_ID Ändern Sie anstelle des Namens für die Überprüfung des Authentifizierungsbereichs die Systemeigenschaft *glide.oauth.token.scope.useraccount*Zu neu erstellt sys_ID Datensatz.

Wenn Administrator, ändern Sie den Authentifizierungsbereich, der mit verknüpft ist oauth_Entität **, Werden alle vorhandenen OAuth-Zugriffstoken, die von dieser OAuth-Entität ausgegeben werden, ebenfalls geändert?**

Ja, der Authentifizierungsbereich ist nicht direkt mit dem OAuth-Zugriffstoken verknüpft, sondern wird von abgerufen oauth_Entität Während der Laufzeit.

Kann verschiedene OAuth-Zugriffstoken desselben ausgegeben werden oauth_Entität **Haben Sie unterschiedliche Authentifizierungsbereiche?**

Nein, der gesamte Zugriff auf das Token wird von demselben erteilt oauth_Entität Und haben immer die gleichen Authentifizierungsbereiche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kann ein Anwender verschiedene Authentifizierungsbereiche für einen bestimmten Endpunkt definieren?

Nein, es gibt eine eindeutige Einschränkungsprüfung für einen bestimmten REST API-Endpunkt. Für denselben REST-API-Endpunkt kann es jedoch mehr als einen übereinstimmenden Authentifizierungsbereich haben.

Wird die Überprüfung des Authentifizierungsumfangs auch für BasicAuth verwendet?

Nein, die Überprüfung des Authentifizierungsbereichs ist nur das OAuth-Zugriffstoken und das OIDC-Token, sie wird nicht angewendet `basicAuth`Und `mutualAuth`

Zugriffsrichtlinien für SOAP-API

Mit den Zugriffsrichtlinien der SOAP-API können Sie den Zugriff auf eingehende SOAP-APIs basierend auf dem Authentifizierungstyp und den angegebenen Filterkriterien der Zugriffsrichtlinie einschränken.

Mit den SOAP-API-Zugriffsrichtlinien können Sie das eingehende Authentifizierungsprofil und die API-Zugriffsrichtlinien auf eingehende SOAP- und geskriptete SOAP-APIs anwenden.

Sie können nutzen ServiceNow API-Zugriffsrichtlinien wie IP-Bereich und rollenbasierte Einschränkungen, um eingehende SOAP-API-Aufrufe basierend auf der Authentifizierung zuzulassen oder zu untersagen.

Als Administrator können Sie die folgenden Aktionen ausführen, um die Richtlinien anzuwenden.

- Aktivieren Sie die Plugins SOAP-API-Zugriffsrichtlinie und Authentifizierungsprofil. Weitere Informationen finden Sie unter Aktivieren Sie die SOAP-API-Zugriffsrichtlinie.
- Erstellen Sie SOAP-API-Zugriffsrichtlinien, und ordnen Sie diese Richtlinien einem Authentifizierungsprofil zu. Weitere Informationen finden Sie unter Erstellen Sie eine SOAP-API-Zugriffsrichtlinie und Erstellen Sie ein Authentifizierungsprofil.

  Hinweis: Die Richtlinien gelten für die SOAP-Tabellen-API oder die geskriptete SOAP-API. Neben dem Standard `http` Und `WSSE` Authentifizierungsprofil.

- Erstellen Sie Authentifizierungsrichtlinien wie IP-Bereich und rollenbasierte Einschränkungen, und ordnen Sie diese Richtlinie dem Authentifizierungsprofil zu. Weitere Informationen finden Sie unter Erstellen Sie eine API-Authentifizierungsrichtlinie.

Aktivieren Sie die SOAP-API-Zugriffsrichtlinie

Installieren Sie für die SOAP-API-Zugriffsrichtlinie die SOAP-API-Zugriffsrichtlinie (`Com.Glide.SOAP.Policy`)-Plugin.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Das folgende Element wird mit dem SOAP-API-Zugriffsrichtlinien-Plugin installiert: Prozessorzugriffsrichtlinie (`com.glide.processor.policy`)

Abhängiges Plugin: Authentifizierungsprofil (`com.glide.auth.profile`)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie das SOAP-API-Zugriffsrichtlinien-Plugin (`Com.Glide.SOAP.Policy`) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

   Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Erstellen Sie ein Authentifizierungsprofil

Erstellen Sie ein Authentifizierungsprofil, und fügen Sie dem Profil eine oder mehrere Authentifizierungsrichtlinien hinzu. Sie können auch konfigurieren **ID-Token** Und **OAuth-Token** Standardmäßig verfügbare Authentifizierungsprofile.

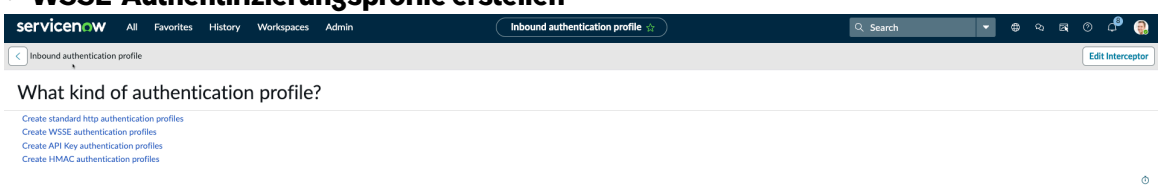
Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: Sie können Authentifizierungsrichtlinien, IP-Bereich, rollenbasiert, anwenderbasiert usw. mit gegenseitiger Authentifizierung und anwenderdefinierter Authentifizierung anwenden.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Eingehende Authentifizierungsprofile**an.
2. Wählen Sie **Neu**.
   Das System zeigt die Meldung an. Welche Art von Authentifizierungsprofil?
3. Wählen Sie Aus **Welche Art von Authentifizierungsprofilen?** .
   - **Standardmäßiges http-Authentifizierungsprofil erstellen**
   - **WSSE-Authentifizierungsprofile erstellen**



4. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Standardauthentifizierungsprofil“

Feld	Beschreibung
Name	Name zur Identifizierung der Authentifizierungsrichtlinie.
Beschreibung	Beschreibung der Authentifizierungsrichtlinie.
Aktiv	Option zum Aktivieren der Authentifizierungsrichtlinie.
Anwendung	Umfang der Authentifizierungsrichtlinie.
Typ	Typ der verfügbaren Authentifizierung. Sie können auswählen **Standardauthentifizierung** , **ID-Token** , **Zertifikatbasierte Authentifizierung** , **OAuth** , Oder **WSSE** (Im Falle eines WSSE-Authentifizierungsprofils).
OAuth-Entität	OAuth-Entitätsprofil. Dieses Feld wird nur angezeigt, wenn **ID-Token** Oder **OAuth** Ist aus ausgewählt **Typ** .

5. Doppelklicken Sie auf **Neue Zeile einfügen**.
6. Wählen Sie eine Authentifizierungsrichtlinie aus der Liste aus, und wählen Sie das Speichern-Symbol .

Hinweis: Nicht auswählen **Zugriffsrichtlinie Zulassen** Oder **Zugriffsrichtlinie Verweigern** . Diese Richtlinien sind nur für Anwenderanmeldungen vorgesehen.

Sie können eine oder mehrere Authentifizierungsrichtlinien für ein Authentifizierungsprofil hinzufügen.

Wenn sich das Authentifizierungsprofil ändert, gibt der Autorisierungs-Header einen Wert zurück, der für die zu diesem Zeitpunkt vorgenommenen Änderungen spezifisch ist. Um alle im Header „WWW-Authenticate“ zurückgegebenen Authentifizierungsschemata abrufen zu können, müssen Sie aktivieren glide.security.response.authenticate.header.auth_profile.first_scheme_only Bis **Falsch** . Die Antwort wird mit mehreren Headern zurückgegeben. Zum Beispiel:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Erstellen Sie eine SOAP-API-Zugriffsrichtlinie

Erstellen Sie eine API-Zugriffsrichtlinie, und ordnen Sie ein Authentifizierungsprofil zu, um den Authentifizierungstyp für eine SOAP-API einzuschränken. Sie können beispielsweise eine API-Zugriffsrichtlinie erstellen, die nur die ID-Token-Authentifizierung für eine SOAP-API zulässt.

Vorbereitungen

- Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Erstellen Sie ein Authentifizierungsprofil .
- Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

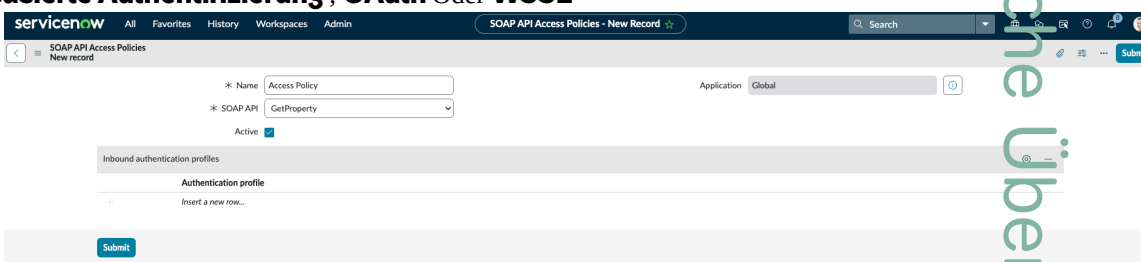
Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Zugriffsrichtlinien für SOAP-API**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „API-Zugriffsrichtlinien“

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
SOAP-API	SOAP-API, auf die die Zugriffsrichtlinie angewendet wird. Beispiel: **GetProperty-API** .
Anwendung	Umfang der Anwendung.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.

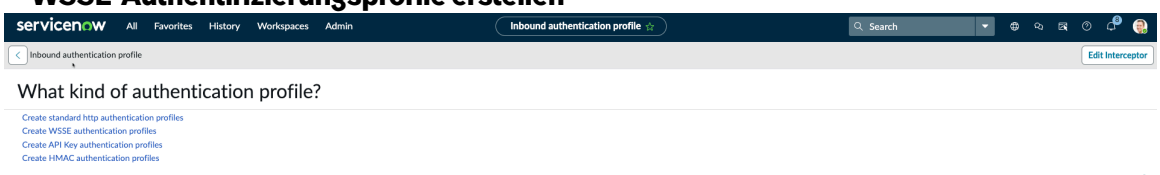
4. Doppelklicken Sie im Abschnitt „eingehende Authentifizierung“ auf **Fügen Sie eine neue Zeile ein** .
5. Wählen Sie ein eingehendes Authentifizierungsprofil aus der Liste aus, und klicken Sie auf das Speichern-Symbol .
   Sie können beispielsweise hinzufügen **Standardauthentifizierung** , **ID-Token** , **Zertifikatbasierte Authentifizierung** , **OAuth** Oder **WSSE-Authentifizierung**.



   a. Um ein oder mehrere eingehende Authentifizierungsprofile hinzuzufügen, klicken Sie auf **Neu** Um ein neues Profil zu erstellen.

   b. Wählen Sie Aus **Welche Art von Authentifizierungsprofilen?** .

   - **Standardmäßiges http-Authentifizierungsprofil erstellen**
   - **WSSE-Authentifizierungsprofile erstellen**



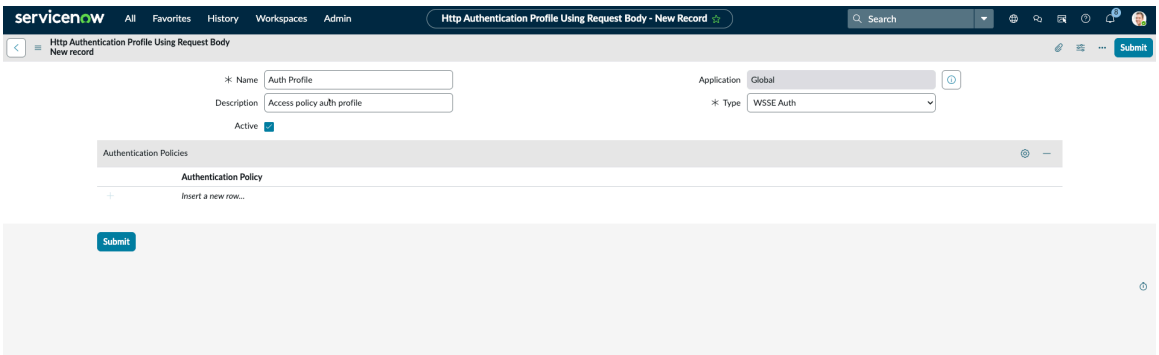
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Um ein WSSE-Authentifizierungsprofil zu erstellen, füllen Sie die Felder im Formular aus.

WSSE-Authentifizierungsprofil

Feld	Beschreibung
Name	Eindeutiger Name der API-Zugriffsrichtlinie.
Beschreibung	Beschreibung des Authentifizierungsprofils.
Anwendung	Umfang der Anwendung.
Aktiv	Option zum Aktivieren der API-Zugriffsrichtlinie.
Typ	WSSE-Authentifizierung als Authentifizierungsprofil WSSE (Websicherheit).



d. Speichern Sie den Datensatz nach dem Erstellen des Authentifizierungsprofils.

6. Klicken Sie Auf **Übermitteln** Zum übermitteln der SOAP-API-Zugriffsrichtlinie.

Erstellen Sie eine globale API-Zugriffsrichtlinie, um SOAP-APIs zu schützen

Erstellen Sie eine einzige globale API-Zugriffsrichtlinie, um alle SOAP-APIs zu schützen.

Vorbereitungen

- Erforderliche Rolle: Administrator
- Installieren Sie **Prozessorzugriffsrichtlinie** (`com.glide.processor.policy`)-Plugin
- Stellen Sie sicher, dass ein Authentifizierungsprofil erstellt wird. Weitere Informationen finden Sie unter Erstellen Sie ein Authentifizierungsprofil .

In den folgenden Schritten wird beschrieben, wie Sie eine einzige globale Zugriffsrichtlinie zum Schutz aller SOAP-APIs erstellen.

Hinweis: Die auf den einzelnen SOAP-API-Ebenen definierten Richtlinien überschreiben den **SOAPProcessor** Globale Zugriffsrichtlinie auf Ebene.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Prozesszugriffsrichtlinien**an.

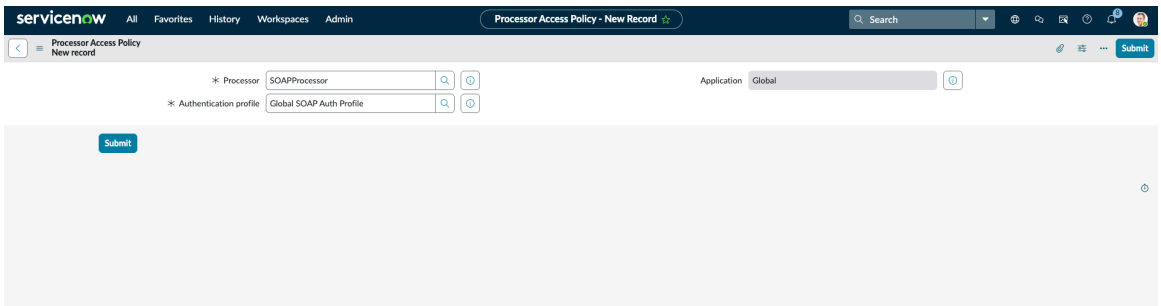
2. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Zugriffsrichtlinie verarbeiten“

Feld	Beschreibung
Prozessor	Name zur Identifizierung der Authentifizierungsrichtlinie. Wählen Sie zum Beispiel aus, **SOAPProcessor** (Authentifizierungsprofil).
Anwendung	Umfang der Authentifizierungsrichtlinie. Standard: Global
Authentifizierungsprofil	Typ des Authentifizierungsprofils. Auswählen, **Globales SOAP-Authentifizierungsprofil** .



3. Wählen Sie **Absenden**.

Filterkriterien für APIs

Filterkriterien enthalten Filterbedingungen oder Abfragen, die als Richtlinieneingaben für eine Authentifizierungsrichtlinie verwendet werden. Richtlinieneingaben werden verwendet, um ein oder mehrere Filterkriterien zu gruppieren und die Richtlinienbedingungen einer Authentifizierungsrichtlinie zu definieren. Beispielsweise definieren IP-Filterkriterien eine IP-Adresse im CIDR-Format (Classless Inter-Domain Routing) oder einen Bereich von IP-Adressen.

Sie können Filterkriterien basierend auf der IP-Adresse, Rolle und der Anwendergruppe des Anwenders erstellen, zu der er gehört.

Hinweis: Sie verwenden auch die Filterkriterien, die aus erstellt wurden **Adaptive Authentifizierung** Modul. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Sie können Filterkriterien für APIs mit demselben Prozess wie Filterkriterien für die adaptive Authentifizierung erstellen. Nähere Informationen hierzu finden Sie unter Filterkriterien.

Zugehörige Informationen

Erstellen Sie IP-Filterkriterien

Erstellen Sie Rollenfilterkriterien

Erstellen Sie Gruppenfilterkriterien

API-Authentifizierungsrichtlinien

Authentifizierungsrichtlinien bewerten Authentifizierungsanforderungen basierend auf den angegebenen Richtlinienbedingungen und erlauben oder verweigern den Zugriff je nach übereinstimmenden Kriterien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die integrierte globale Blockierungsrichtlinie verwenden oder eine Authentifizierungsrichtlinie gemäß Ihren Sicherheitsanforderungen erstellen. Die globale Blockierungsrichtlinie lehnt die Authentifizierungsanforderungen von Anwendern und APIs basierend auf den angegebenen Filterkriterien ab.

Hinweis: Verwenden oder ändern Sie keine Zugriffsrichtlinie zulassen und Zugriffsverweigerungsrichtlinie. Diese Richtlinien sind nur für Anwenderanmeldungen vorgesehen.

Erstellen Sie eine API-Authentifizierungsrichtlinie

Mit Authentifizierungsrichtlinien können Sie Zugriffsbeschränkungen für die APIs basierend auf den angegebenen Filterkriterien erzwingen.

Vorbereitungen
Erforderliche Rolle: Administrator

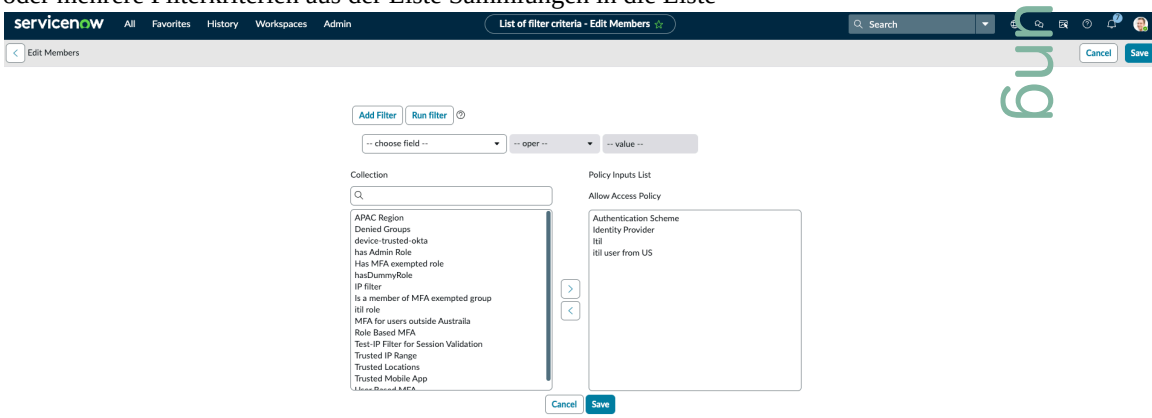
Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Authentifizierungsrichtlinie**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Richtlinienformular

Feld	Beschreibung
Name	Name zur Identifizierung der Richtlinie.
Beschreibung	Kurzbeschreibung der Richtlinie.
Anwendung	Umfang der Anwendung.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Wählen Sie auf der Registerkarte Richtlinieneingaben die Option aus **Bearbeiten** Um die vorhandenen Filterkriterien hinzuzufügen.
   Sie können auch eine neue Richtlinieneingabe erstellen. Weitere Informationen finden Sie unter Erstellen Sie Richtlinieneingaben .
6. Verschieben Sie ein oder mehrere Filterkriterien aus der Liste Sammlungen in die Liste



   Richtlinieneingaben.
7. Wählen Sie **Speichern**.
8. Wählen Sie auf der Registerkarte Richtlinienbedingungen die Option aus **Neu** .

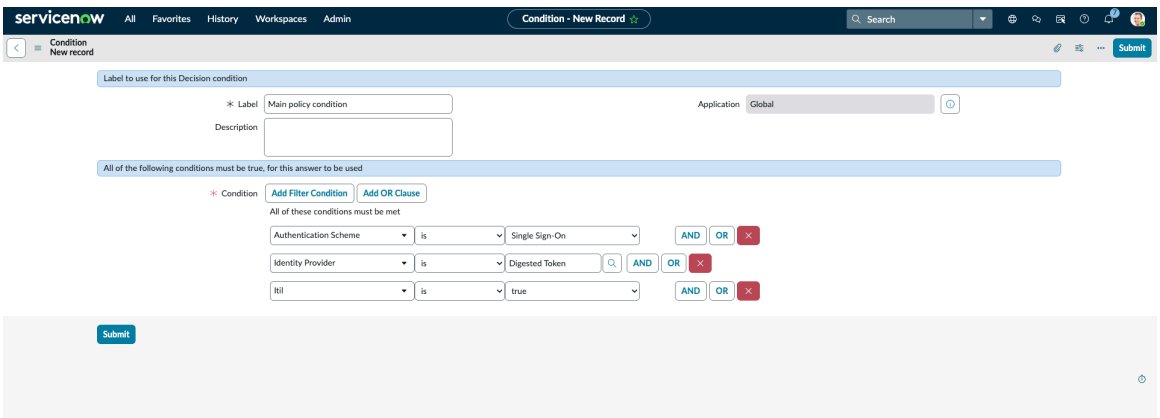
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name der Richtlinienbedingung.
Beschreibung	Kurzbeschreibung der Richtlinienbedingung.
Anwendung	Umfang der Anwendung.
Bedingung	Mindestens eine Bedingung, die mit kombiniert wird **ODER** Filter.



10. Wählen Sie **Absenden**.

Konfigurieren Sie die globale Sperrrichtlinie für APIs

Die globale Blockierungsrichtlinie verweigert die Authentifizierungsanforderungen von Anwendern und APIs basierend auf den angegebenen Richtlinienbedingungen. Diese Richtlinie kann als Alternative zur Zugriffssteuerung für IP-Adressen verwendet werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **Globale Sperrrichtlinie**an.
2. Von **Richtlinieneingaben** Klicken Sie auf die Registerkarte **Bearbeiten** .
3. Wählen Sie mindestens ein Filterkriterium aus **Sammlung** Listen Sie sie auf, und verschieben Sie sie in **Globale Sperrrichtlinie** Liste.
   Sie können auch zusätzliche Filter hinzufügen.
4. Von **Richtlinienbedingungen** Klicken Sie auf die Registerkarte **Neu** .
5. Füllen Sie im Formular diese Felder aus:

Bedingungsformular

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Sie können beispielsweise Bedingungen erstellen, die nur Auftragnehmer aus einer Liste vertrauenswürdiger IP-Adressen zulassen.

Zugriffsrichtlinie für System- oder Exportprozessoren

Möglichkeit für System- oder Exportprozessoren, die Prozessorzugriffsrichtlinie zu nutzen, um alle Exportendpunkte zu sichern.

Fähigkeit, alle Exportendpunkte zu sichern und das eingehende Authentifizierungsprofil und die Prozessorzugriffsrichtlinien auf globaler Ebene oder Instanzebene anzuwenden.

Hinweis:

- Nicht öffentliche Prozessoren, einschließlich Exportprozessoren wie CSV, PDF usw., werden für Zugriffsrichtlinien unterstützt.
- Skriptprozessoren werden auch für Zugriffsrichtlinien unterstützt.

Beispielanwendungsfälle

- Der Administrator kann den RSS-Prozessor blockieren, wenn er nicht beabsichtigt wird, ihn zu verwenden, indem er die API-Zugriffsrichtlinie nutzt.
- Der Administrator kann ein Authentifizierungsprofil mit Standardauthentifizierung erstellen und eine Authentifizierungsrichtlinie zuordnen, die immer als „falsch“ ausgewertet wird.

  Beispiel: Erstellen Sie IP-Kriterien mit einem Bereich von `0.0.0.0` Bis `255.255.255.255` (Fügen Sie auch IPv6-Adressraum hinzu) und fügen Sie dann die Richtlinienbedingung mit dem Operator „falsch“ hinzu. Auf diese Weise werden Richtlinienbedingungen immer als „falsch“ bewertet, und die API-Zugriffsrichtlinie blockiert den Zugriff unabhängig davon, woher die Anforderung stammt.

- Zugriff auf den Prozessor nur über ein vertrauenswürdiges Netzwerk zulassen.

Aktivieren Sie die Prozessorzugriffsrichtlinie

Installieren Sie für Prozessor die Prozessorzugriffsrichtlinie (`com.glide.processor.policy`)-Plugin.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Elemente werden mit der Prozessorzugriffsrichtlinie installiert:

- Systemeigenschaft: com.glide.auth.profile.supported.processor.list
- Modul in der Navigation: Prozessorzugriffsrichtlinien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie die Prozessorzugriffsrichtlinie (`com.glide.processor.policy`) Plugin mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Nächste Maßnahme

an.

Konfigurieren Sie das Authentifizierungsprofil für die Prozessoren. Weitere Informationen finden Sie unter . Konfigurieren Sie das Authentifizierungsprofil für den Prozessor.

Konfigurieren Sie das Authentifizierungsprofil für den Prozessor

Wenden Sie das Authentifizierungsprofil für die Exportprozessoren an.

Vorbereitungen

Erforderliche Rolle: Administrator

Plugin erforderlich: Prozessorzugriffsrichtlinie (`com.glide.processor.policy`)

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffsrichtlinien für Prozessor**an.
2. Um dem Prozessor ein Authentifizierungsprofil hinzuzufügen, klicken Sie auf **Neu** .
3. Füllen Sie im Formular die Felder aus.

Formular „Zugriffsrichtlinie verarbeiten“

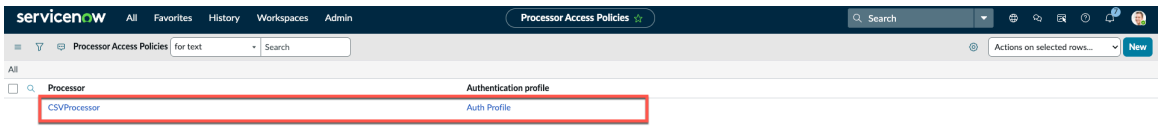
Feld	Beschreibung
Prozessor	Name zur Identifizierung der Authentifizierungsrichtlinie. **Hinweis:** Öffentliche Prozessoren werden nicht unterstützt. Wenn ein nicht unterstützter Prozessor ausgewählt wird, wird während der Übermittlung des Prozessors ein Fehler angezeigt.
Anwendung	Umfang der Authentifizierungsrichtlinie. Standard: Global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Authentifizierungsprofil	Typ des Authentifizierungsprofils. Sie können auswählen **ID-Token** Oder **OAuth-Token** .

4. Klicken Sie auf **Absenden**.
   Das Authentifizierungsprofil wird auf den Prozessor angewendet.

   Beispielsweise ist das OAuth-Authentifizierungsprofil für den CSV-Prozessor konfiguriert. In diesem Fall müssen Sie das OAuth-Zugriffstoken für den Export mit CSV als Exportoption verwenden.



Zertifikatbasierte Authentifizierung

Mit der zertifikatbasierten Authentifizierung können Sie Anwenderanmeldungen oder eingehende API-Anforderungen mithilfe von Zertifikaten von einer vertrauenswürdigen Zertifizierungsstelle (CA) gegenseitig authentifizieren.

Hinweis: Die zertifikatbasierte Authentifizierung wird auf der Instanz mit aktivierter lokaler Verschlüsselung und Edge Encryption nicht unterstützt.

Zertifikatbasierte Authentifizierung für Anwenderoberflächenanmeldungen

Ermöglichen Sie Endanwendern die Verwendung von PIV-Karten (persönliche Identitätsverifizierung) oder CAC-Karten (Common Access Card), um sich bei anzumelden ServiceNow AI Platform Oder Serviceportal Anstatt einen Anwendernamen und ein Passwort zu verwenden. Informationen zum Einrichten der gegenseitigen Authentifizierung für Anwenderoberflächenanmeldungen finden Sie unter Richten Sie die zertifikatbasierte Authentifizierung ein.

Nachdem die zertifikatbasierte Authentifizierung eingerichtet wurde, können Endanwender ihre Einrichtung abschließen und sich anmelden. Weitere Informationen finden Sie unter Melden Sie sich mit zertifikatbasierter Authentifizierung an.

Zertifikatbasierte Authentifizierung für eingehende Webservices

Authentifizieren Sie eingehende Anforderungen an ServiceNow SOAP- und REST-APIs. Informationen zum Einrichten der gegenseitigen Authentifizierung für eingehende Webservices finden Sie unter Richten Sie die zertifikatbasierte Authentifizierung ein.

Richten Sie die zertifikatbasierte Authentifizierung ein

Richten Sie die gegenseitige Authentifizierung für anwenderoberflächenbasierte Anmeldungen oder eingehende Webservices ein.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie, ob Ihre Instanz einen ADCv2-Lastenausgleichsmodul verwendet. Weitere Informationen finden Sie unter wissensartikel zur ADCv2-Migration . Wenn Ihre Instanz den ADCv2-Lastenausgleichsmodul nicht verwendet, wenden Sie sich an Now Support.

Prozedur

Richten Sie die zertifikatbasierte Authentifizierung ein, um:

- Ermöglichen Sie Endanwendern, sich sicher bei anzumelden ServiceNow AI Platform Oder Serviceportal Mit PIV- oder CAC-Karten. Nachdem die zertifikatbasierte Authentifizierung aktiviert ist, können Sie das PEM-Zertifikat selbst registrieren, oder ein Administrator kann das Zertifikat für Sie zuordnen. Weitere Informationen finden Sie unter Melden Sie sich mit zertifikatbasierter Authentifizierung an.
- Aktivieren Sie die gegenseitige Authentifizierung für eingehende Webservices. Sobald die zertifikatbasierte Authentifizierung eingerichtet ist, verwendet das System die bereitgestellten Zertifikate, um Anforderungen für den Zugriff gegenseitig zu authentifizieren ServiceNow REST- und SOAP-APIs.

Aktivieren Sie die zertifikatbasierte Authentifizierung

Sie können das Plugin für die zertifikatbasierte Authentifizierung aktivieren (com.glide.auth.mutual) Für ServiceNow AI Platform Wenn Sie die Administratorrolle innehaben.

Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Tabellen werden mit installiert Zertifikatbasierte Authentifizierung :

- sys_user_certificate
- sys_CA_certificate
- sys_CA_certificate_api_Track

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach Zertifikatbasierte Authentifizierung Plugin (com.glide.auth.mutual) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

   Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrieren Sie das CA-Zertifikat

Registrieren Sie Stammzertifikate oder Zwischenzertifikate, um sie für die Authentifizierung verfügbar zu machen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **CA-Zertifikatkette**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „CA-Zertifikat für gegenseitige Authentifizierung“

Feld	Beschreibung
Name	Name zur Identifizierung des Zertifikats.
Ablaufbenachrichtigung	Option zum Warnen von Anwendern, wenn ein Zertifikat abläuft.
Benachrichtigung bei Ablauf	Liste der Anwender, die benachrichtigt werden sollen, wenn das Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Anzahl der Tage, in denen eine Benachrichtigung an Anwender gesendet wird, bevor ein Zertifikat abläuft.
Aktiv	Option zum Aktivieren des Clientzertifikats.
Format	PEM
Typ	Typ des Zertifikats. Verfügbare Optionen: ○ **CA-Zertifikat** : Das Stamm-CA-Zertifikat. Kann auch Zwischenzertifikate in die Kette einschließen. CA-Zertifikate werden automatisch mit dem Lastenausgleichsmodul synchronisiert. Verwenden Sie diese Option, wenn möglich, um zu vermeiden, dass ein erforderliches Zertifikat in der Kette fehlt. ○ **Zwischenzertifikat** : Ein Zwischenzertifikat in der Zertifikatkette. Dieses Zertifikat verbleibt nur in der Instanz und wird nicht mit dem Lastenausgleichsmodul synchronisiert. Verwenden Sie diese Option nur, wenn Sie einer vorhandenen Kette ein Zwischenzertifikat hinzufügen müssen.
Kurzbeschreibung	Kurzbeschreibung des Anwender-Client-Zertifikats.

Hinweis: Während des Zertifikathochladens werden die schreibgeschützten Felder, **Gültig ab** , **Läuft Ab** , **Läuft in Tagen ab** , **Aussteller** , Und **Betreff** , **Zertifikatkette** , Und **PEM-Zertifikat** Werden extrahiert und automatisch ausgefüllt.

4. Klicken Sie auf **Absenden**.
5. **Wahlweise:** Klicken Sie Auf **Validiert Speicher/Zertifikate** Dient zum Validieren des Zertifikats.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PEM-Zertifikat dem Anwender zuordnen

Ordnen Sie Anwendern PEM-Zertifikate zu, damit sie sich mit PIV- oder CAC-Karten anmelden oder eingehende Anforderungen authentifizieren können. Sie können einem Anwender mehrere PEM-Zertifikate zuordnen.

Vorbereitungen

- Erforderliche Rolle: Administrator
- Stellen Sie sicher, dass Sie über das PEM-Zertifikat (Privacy Enhanced Mail) des Anwenders verfügen.

Hinweis: Nach der Konfiguration „PEM-Zertifikat zu Anwender zuordnen“ schlägt die Option „Zertifikat verifizieren“ fehl. Dies liegt daran, dass das PEM-Zertifikat nicht gespeichert ist.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **Anwender-zu-Zertifikat-Zuordnung** Und klicken Sie auf **Neu** .
2. Füllen Sie diese Felder im Formular aus:

Formular „Anwenderclient-Zertifikat“

Feld	Beschreibung
Name	Name des Anwenderclientzertifikats.
Ablaufbenachrichtigung	Option zum Warnen von Anwendern, wenn ein Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Anzahl der Tage, in denen eine Benachrichtigung an Anwender gesendet wird, bevor ein Zertifikat abläuft.
Benachrichtigung bei Ablauf	Liste der Anwender, die benachrichtigt werden sollen, wenn das Zertifikat abläuft.
Aktiv	Option zum Aktivieren des Clientzertifikats.
Anwender	Anwender, der dem Clientzertifikat zugeordnet ist. Das System empfängt das Clientzertifikat entweder von der eingehenden Anforderung oder Zertifikatregistrierung , Und verwendet dann den in diesem Feld angegebenen Anwender, um eine Sitzung zum Ausführen der Anforderung zu initiieren.
Kurzbeschreibung	Kurzbeschreibung des Anwender-Client-Zertifikats.
Format	Das PEM-Format (Privacy Enhanced Mail) ist ein Base-64-codiertes Zertifikat für Distinguished Encoding Rules (DER).
Typ	Client-Zertifikat Dieses Feld ist schreibgeschützt.

Hinweis: Während des Zertifikathochladens werden die schreibgeschützten Felder, **Gültig ab** , **Läuft Ab** , **Läuft in Tagen ab** , **Aussteller** , Und **Betreff** Werden extrahiert und automatisch ausgefüllt.

3. Klicken Sie auf das Anhangssymbol, und laden Sie das Zertifikat hoch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
   Das Zertifikat wird validiert und dem angegebenen Anwender zugeordnet, wenn das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) stammt.

Konfigurieren Sie zertifikatbasierte Authentifizierungseigenschaften

Verwenden Sie Systemeigenschaften, um zertifikatbasierte Authentifizierungsfunktionen zu aktivieren oder zu deaktivieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Zertifikatsbasierte Authentifizierung** > **Eigenschaften**an.
2. Füllen Sie die Felder des Formulars aus.

Formular „Eigenschaften der zertifikatbasierten Authentifizierung“

Eigenschaft	Beschreibung
Zertifikatbasierte Authentifizierung aktivieren	Option zum Aktivieren der zertifikatbasierten Authentifizierung für Anwenderoberflächenanmeldungen und eingehende Webservices. Standardwert: wahr
Zeigen Sie die Option „mit PIV/CAC anmelden“ im Anmeldebildschirm an	Zeigt an **Melden Sie sich mit der PIV/CAC-Karte an** Option auf dem Anmeldebildschirm. Ermöglicht Anwendern die Anmeldung mit zertifikatbasierter Authentifizierung über die Anwenderoberfläche. Standardwert: false
Automatische Weiterleitung für die zertifikatbasierte Anmeldung aktivieren	Bestimmt, ob der Anwender auf klicken muss **Melden Sie sich mit der PIV/CAC-Karte an** Nachdem Sie ein registriertes Zertifikat ausgewählt und die PIN eingegeben haben. Aktivieren Sie diese Option, um sich automatisch beim Anwender anzumelden, nachdem er ein registriertes Clientzertifikat ausgewählt und seine PIN eingegeben hat. Deaktivieren Sie diese Option, um zu erfordern, dass der Anwender auf klickt **Melden Sie sich mit der PIV/CAC-Karte an** Nachdem sie ein registriertes Clientzertifikat ausgewählt und ihre PIN eingegeben haben. Standardwert: false

Melden Sie sich mit zertifikatbasierter Authentifizierung an

Nachdem Ihr Administrator die zertifikatbasierte Authentifizierung eingerichtet hat, können Sie das Clientzertifikat registrieren und sich mit Ihrer PIV-Karte (persönliche Identitätsverifizierung) oder CAC-Karte (Common Access Card) anmelden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrieren Sie das Clientzertifikat für Ihre PIV- oder CAC-Karte

Bevor Sie sich bei anmelden ServiceNow AI Platform Mit Ihrer PIV- oder CAC-Karte müssen Sie das Clientzertifikat Ihrer PIV- oder CAC-Karte registrieren. Wenn Sie das Clientzertifikat nicht registrieren können, wenden Sie sich an Ihren Administrator. Ihr Administrator kann auch das Clientzertifikat Ihrer PIV- oder CAC-Karte registrieren.

Vorbereitungen

- Stellen Sie sicher, dass die zertifikatbasierte Authentifizierung aktiviert ist.
- Stellen Sie sicher, dass ein Kartenleser an Ihren Computer angeschlossen und Ihre PIV- oder CAC-Karte eingesetzt ist.
- Erforderliche Rolle: keine

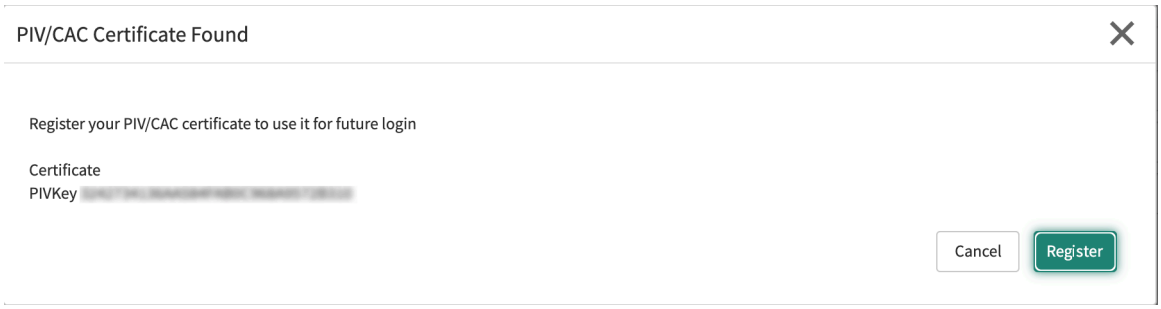
Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Administrator benötigen, um Ihr Clientzertifikat zu registrieren, finden Sie unter PEM-Zertifikat dem Anwender zuordnen.

Prozedur

1. Melden Sie sich bei an ServiceNow AI Platform Verwenden Sie Ihren Anwendernamen und Ihr Passwort.
2. Klicken Sie im auf Ihren Namen **Anwendermenü** Und wählen Sie aus **Profil** .
3. Von **Zugehörige Links** , Klicken Sie auf **Client-Zertifikat registrieren** .

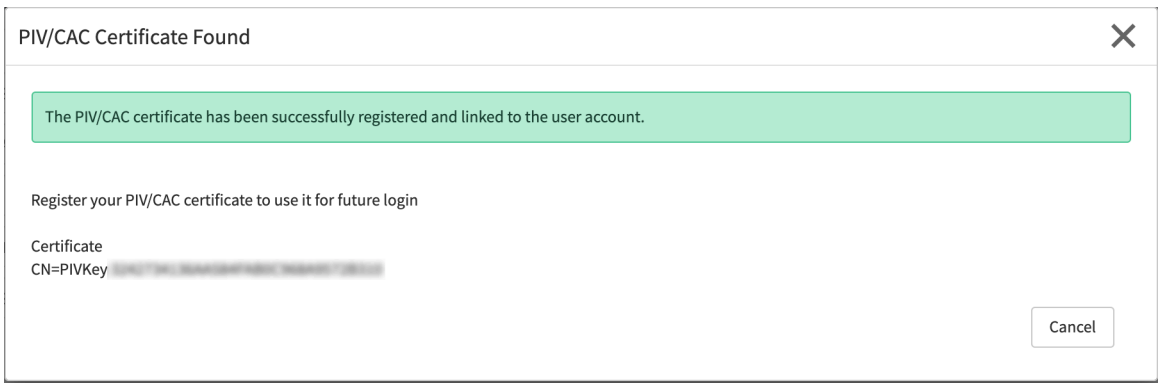
   Wenn ein gültiges ist-Zertifikat verfügbar ist, wird die folgende Meldung angezeigt:



4. Klicken Sie auf **registrieren**.

   Nach erfolgreicher Registrierung wird die folgende Meldung angezeigt:

   Das PIV/CAC-Zertifikat wurde registriert und mit dem Anwenderaccount verknüpft.



Wenn Sie sich das nächste Mal bei anmelden ServiceNow AI Platform, Sie können sich mit Ihrer PIV- oder CAC-Karte anmelden. Weitere Informationen finden Sie unter Melden Sie sich bei an ServiceNow AI Platform Mit PIV- oder CAC-Karte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Melden Sie sich bei an ServiceNow AI Platform Mit PIV- oder CAC-Karte

Sie können sich mit Ihrer PIV- oder CAC-Karte anstelle von Anwendername und Passwort anmelden, wenn die zertifikatbasierte Authentifizierung auf aktiviert ist ServiceNow AI Platform.

Vorbereitungen

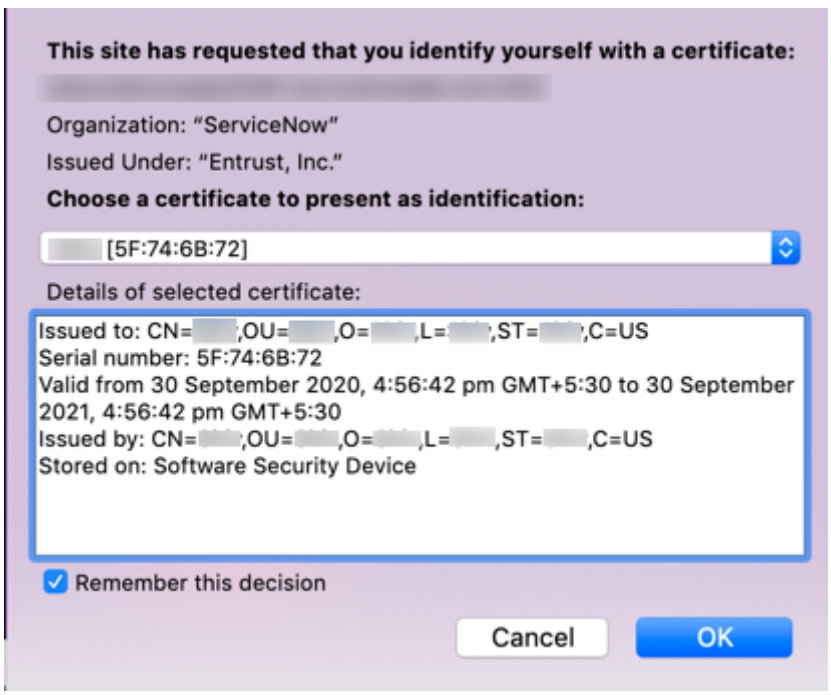
- Erforderliche Rolle: keine
- Stellen Sie sicher, dass die zertifikatbasierte Authentifizierung aktiviert ist.
- Stellen Sie sicher, dass ein PIV- oder CAC-Kartenleser an Ihren Computer angeschlossen ist.
- Stellen Sie sicher, dass Ihnen ein Clientzertifikat Ihrer PIV- oder CAC-Karte zugeordnet ist. Weitere Informationen finden Sie unter Registrieren Sie das CA-Zertifikat.

Prozedur

1. Legen Sie Ihre PIV- oder CAC-Karte in den Kartenleser ein.
2. Navigieren Sie in einem Browser zu Ihrer Instanz.
   Der Browser fordert zur Eingabe einer PIN für Ihre PIV- oder CAC-Karte auf.
3. Geben Sie die PIN Ihrer PIV- oder CAC-Karte in die Browseraufforderung ein.

   Hinweis: Wenn Sie Ihre PIN vergessen haben, wenden Sie sich an Ihren Administrator.

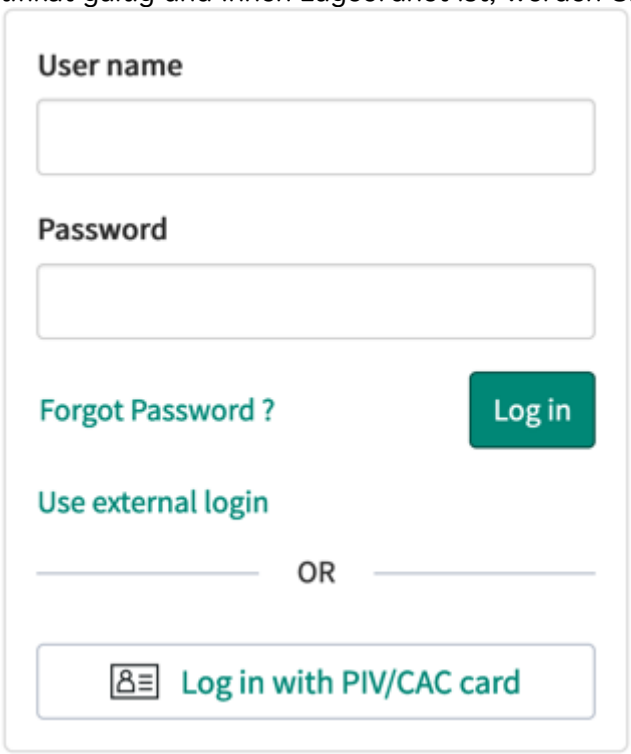
4. Wenn Sie eine richtige PIN eingeben, zeigt der Browser eine Aufforderung zur Auswahl eines Zertifikats an.



5. Wählen Sie ein Zertifikat in der Browser-Eingabeaufforderung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Zertifikat gültig und Ihnen zugeordnet ist, werden Sie zur Anmeldeseite



weitergeleitet.

6. Klicken Sie Auf **Melden Sie sich mit der PIV/CAC-Karte an** Schaltfläche.

   Um sich von abzumelden ServiceNow AI Platform, Sie müssen PIV oder CAC aus dem Kartenleser entfernen und dann den Browser schließen.

Ihre Client-Zertifikate verwalten

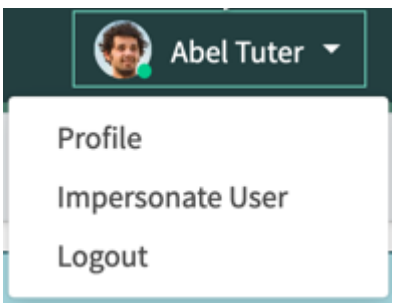
Zeigen Sie Client-Zertifikate an, die Ihrem Account zugeordnet sind, und löschen Sie sie.

Vorbereitungen

- Stellen Sie sicher, dass die zertifikatbasierte Authentifizierung aktiviert ist.
- Erforderliche Rolle: keine

Prozedur

1. Melden Sie sich bei an ServiceNow AI Platform Verwenden Sie Ihren Anwendernamen und Ihr Passwort.
2. Klicken Sie im auf Ihren Namen **Anwendermenü** Und wählen Sie aus **Profil** .



3. Von **Zugehörige Links** , Klicken Sie auf **Verwalten Sie Ihre Clientzertifikate** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Tabelle „Anwenderclientzertifikate“ [sys_user_certificate] wird geöffnet und zeigt Zertifikate an, die Ihrem Account zugeordnet sind.

4. Zeigen Sie Ihrem Account zugeordnete Zertifikate an, oder löschen Sie sie.

Anwenderdefinierte Instanz-URLs

Sie können Ihren aktivieren ServiceNow Instanz, auf die über eine firmengebrandete oder anwenderdefinierte URL zugegriffen werden soll.

Übersicht über anwenderdefinierte URL

Sie können anwenderdefinierte URL verwenden, um zu aktivieren ServiceNow Instanz, auf die über eine oder mehrere unternehmenseigene oder anwenderdefinierte URLs zugegriffen werden soll.

Anwenderdefinierte URLs können einem bestimmten Portal zugeordnet werden. Zum Beispiel kann der Administrator definieren http://support.acme.com Für CSM-Portal und http://hr.acme.com Für HR-Portal. In einer solchen Situation müssen Anwender zur Authentifizierung auf Grundlage der anwenderdefinierten URL, auf die Anwender zugreifen, an verschiedene IDPs weitergeleitet werden.

Wichtig:

- Erstellen Sie keine anwenderdefinierte URL mit mehr als 100 Domänen pro Instanz.
- Sie müssen den anwenderdefinierten URL-Datensatz aus löschen ServiceNow Instanz zuerst und löscht dann alle DNS-Einträge (Domain Name Server) vom DNS-Server.
- Jede Löschung des DNS-Eintrags vom DNS-Server vor dem Löschen des anwenderdefinierten URL-Datensatzes aus ServiceNow Instanz würde dazu führen, dass das Löschen anderer entsprechender anwenderdefinierter URL-Datensätze aus blockiert wird ServiceNow.

Von Tokyo, Sie können Anwendern die automatische Umleitung zu den angegebenen IDPs ermöglichen, die im anwenderdefinierten URL-Datensatz definiert sind.

Hinweis: Anwenderdefinierte URLs sind für lokale Kunden oder Entwicklerinstanzen nicht verfügbar. Außerdem muss die URL öffentlich sein.

Nur der Besitzer der Domäne der obersten Ebene (Top-Level Domain, TLD) oder einer beliebigen Unterdomäne kann die anwenderdefinierte URL für eine DNS-Subdomäne konfigurieren. Beispielsweise kann Ihre Instanz die folgende festgelegte URL und zusätzliche anwenderdefinierte URLs haben:

Beispiel für anwenderdefinierte URL

Beispiel-URLs	Monatlich
https://acme.service-now.com	Der anfängliche Domänenname für Acme, der im Lieferumfang enthalten war ServiceNow Instanz.
https://support.acme.com	Eine anwenderdefinierte URL, die Ihrem zugeordnet ist ServiceNow Instanz. Diese URL wird als Alias (CNAME) des anfänglichen Domänennamens bezeichnet.
https://US-support.acme.com	Eine sekundäre anwenderdefinierte URL, die einem Serviceportal in Ihrer Instanz zugeordnet wird. Ihre

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für anwenderdefinierte URL (Fortsetzung)

Beispiel-URLs	Monatlich
	Instanz kann mehrere anwenderdefinierte URLs für dasselbe Serviceportal unterstützen.

Überlegungen zu anwenderdefinierten URL außerhalb Ihrer Instanz

Bevor Sie eine anwenderdefinierte URL zuordnen können, müssen Sie eine URL über einen Domänenanbieter besitzen (oder erwerben). Es sind auch bestimmte Konfigurationen erforderlich, bevor Sie eine anwenderdefinierte URL in Ihrer Instanz erstellen und zuordnen können.

Anwenderdefinierte URL-Konfigurationen

Konfigurationselemente	Beschreibung
Legen Sie den CNAME mit dem Anbieter fest	Der CNAME-Datensatz muss als festgelegt werden ServiceNow Instanz-URL.
Bestimmen Sie Ihren dedizierten VIP-Status	Der Status des VIP.

Hinweis: Beim Löschen oder Aktualisieren von CNAME-Datensätzen, die auf Ihre Instanz verweisen, müssen Sie diese Sequenz befolgen, um zu vermeiden, dass Datensätze in der Instanz freistehen. Löschen Sie zuerst die CNAME-Datensätze aus Ihrer Instanz, und entfernen oder aktualisieren Sie dann die CNAME-Einstellung bei Ihrem DNS-Provider.

Aktivieren Sie anwenderdefinierte URLs

Aktivieren Sie die Einrichtung anwenderdefinierter URLs auf Ihrem ServiceNow Instanz. Sie können das Plugin „Anwenderdefinierte URL“ (com.snc.customurl) aktivieren, wenn Sie die Administratorrolle innehaben.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.
2. Suchen und klicken Sie auf **Anwenderdefinierte URL** Plugin.

   Hinweis: Wählen Sie nicht aus **Anwenderdefinierte URL: Intern** Plugin, das eine interne Komponente für geskriptete anwenderdefinierte URL-APIs ist.

3. Klicken Sie im Datensatz „Anwenderdefinierte URL“ auf **Aktivieren/Reparieren** Zugehöriger Link.
4. Klicken Sie im Fenster Plugin-Aktivierung auf **Aktivieren** .
   Wenn das Fenster „Plugin-Aktivierung“ erneut geöffnet wird und die Meldung angezeigt wird, dass das Plugin aktiviert ist, klicken Sie auf **Formular Schließen Und Neu Laden** Um in diesem Formular zu bleiben.
5. Suchen Sie in der zugehörigen Liste Plugin-Dateien nach der folgenden Eigenschaft, und ändern Sie den Einstellungswert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Glide.Customurl.aktiviert	Um anwenderdefinierte URLs zu aktivieren, legen Sie den Wert auf fest **Wahr** . Standardmäßig ist diese Eigenschaft auf festgelegt **Falsch** , D. h. Sie können keine anwenderdefinierte URL zuordnen. **Hinweis:** Um diese Funktion zu deaktivieren, legen Sie diese Eigenschaft wieder auf fest **Falsch** .

6. Klicken Sie auf **Aktualisieren**.

Legen Sie eine anwenderdefinierte URL als Instanz-URL fest

Fügen Sie Ihrer Instanzkonfiguration eine anwenderdefinierte URL hinzu, die anstelle von verwendet werden soll ServiceNow URL.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie müssen das Plugin „anwenderdefinierte URL“ aktivieren und eine URL erworben oder registriert haben, bevor Sie die anwenderdefinierte URL zu Ihrer Instanz hinzufügen.

Prozedur

1. Navigieren zu **Alle** > **Anwenderdefinierte URL** > **Anwenderdefinierte URL**an.
2. Sie sollten entweder:
   - Klicken Sie Auf **Neu** Um Ihrer Instanz einen neuen Domänennamen zuzuordnen.
   - Wählen Sie eine anwenderdefinierte URL aus, die bereits als Instanz-URL festgelegt werden soll.
3. Füllen Sie die entsprechenden Felder aus:

Anwenderdefinierte URL-Felder

Feld	Beschreibung
Domänenname	Vollqualifizierter Domänenname (FQDN) der anwenderdefinierten URL. Der FQDN ist eine CNAME-Umleitung, die im Namensserver-Datensatz für die anwenderdefinierte Domäne erstellt wurde. **Hinweis:** Beispielsweise können Sie im Namensserver für acme.com einen Eintrag erstellen: `support.acme.com 300 IN CNAME acme.servicenow.com`
Ist Instanz-URL	Kontrollkästchen, um diese anwenderdefinierte URL für alle ausgehenden URLs zu aktivieren. Nur eine aktive anwenderdefinierte URL kann die Instanz-URL sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Um diese Einstellung für eine anwenderdefinierte URL zu aktivieren, klicken Sie auf **Als Instanz-URL festlegen** Im URL-Datensatz. Alle vorherigen anwenderdefinierten URLs werden dann entfernt.
Status	Status des anwenderdefinierten URL-Datensatzes. Wenn der Status lautet **Aktiv** , Die anwenderdefinierte URL ist bereitgestellt und einsatzbereit.
Serviceportal	Serviceportal, das Sie verwenden möchten, wenn Sie Anwender über die anwenderdefinierte URL zu Ihrer Instanz umleiten.
Identitätsanbieter	Mit dem Identitätsanbieter für die anwenderdefinierte URL können Sie Anwendern die automatische Umleitung zu den angegebenen IDPs ermöglichen, die im anwenderdefinierten URL-Datensatz definiert sind.

Eine anwenderdefinierte URL sollte innerhalb von sechs Stunden in Ihrer Instanz aktiviert werden.

Hinweis:

- Sie müssen den anwenderdefinierten URL-Datensatz aus löschen ServiceNow Instanz zuerst und löscht dann alle DNS-Einträge (Domain Name Server) vom DNS-Server.
- Jede Löschung des DNS-Eintrags vom DNS-Server vor dem Löschen des anwenderdefinierten URL-Datensatzes aus ServiceNow Instanz würde dazu führen, dass das Löschen anderer entsprechender anwenderdefinierter URL-Datensätze aus blockiert wird ServiceNow.

Anwenderdefinierte URL mit Identitätsanbieter

Legen Sie Ihre anwenderdefinierte URL mit dem Identitätsanbieter fest, damit der Anwender sich mit seinen IdPs anmelden kann

Vorbereitungen

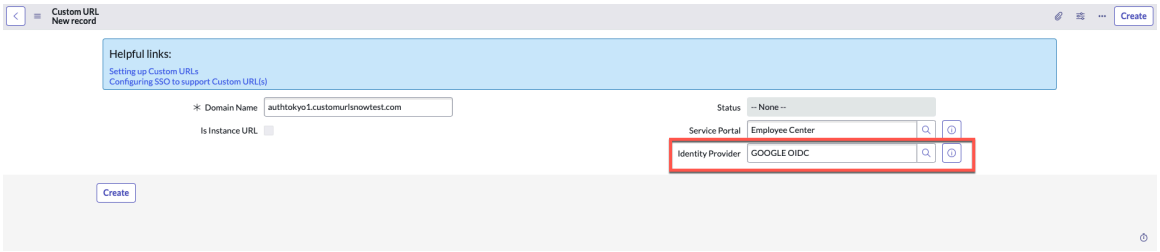
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderdefinierte URL** > **Anwenderdefinierte URL**an.
2. Klicken Sie auf **Neu**.
3. Geben Sie die Details des IdP in an **Identitätsanbieter** Feld.

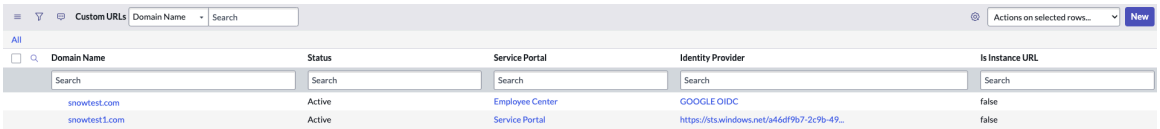
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zu anderen Feldern finden Sie unter Legen Sie eine anwenderdefinierte URL als Instanz-URL fest.



4. Klicken Sie auf **Erstellen**.

Der Datensatz wird erstellt und auf der Seite „Anwenderdefinierte URL“ angezeigt.



Wenn auf die anwenderdefinierte URL zugegriffen wird, wird der Anwender zum konfigurierten Identitätsanbieter weitergeleitet. In diesem Fall greifen Sie auf zu snowtest.com , Der Anwender wird zu navigiert **Mitarbeiter-Center** , Und dann zu umgeleitet Google Identitätsanbieter.

Hinweis:

- Wenn Serviceportal Feld ist leer, und das Feld Identitätsanbieter ist definiert. Wenn der Anwender auf die anwenderdefinierte URL zugreift, wird der Anwender direkt zum konfigurierten Identitätsanbieter navigiert.
- Wenn beides Serviceportal Das Feld „Identitätsanbieter“ ist definiert, wenn der Anwender mit auf die anwenderdefinierte URL zugreift Serviceportal Wenn definiert ist, wird der Anwender zum konfigurierten Identitätsanbieter navigiert.
- Wenn beides Serviceportal Und das Feld „Identitätsanbieter“ ist definiert. Wenn der Anwender mit dem anderen nicht definierten Portal auf die anwenderdefinierte URL zugreift, wird der Anwender zum automatischen Umleiten des Identitätsanbieters navigiert, wenn er in der Instanz konfiguriert ist.

5. Verwenden Sie die Anmeldeinformationen, um sich bei der Anwendung anzumelden.

Anwenderdefinierte URL-Datencenter-Auftragsinformationen

Jede anwenderdefinierte URL, die ist Zugeordnet Ihre Instanz verfügt über einen entsprechenden ServiceNow-Rechenzentrumsauftrag, der ausgeführt wird und URL-Informationen anzeigt, die für Ihre Instanz relevant sind, wie in der Tabelle beschrieben.

Stellenfeld	Beschreibung
Auftrags-ID	Eindeutige ID des Auftrags, der die Domäne der anwenderdefinierten URL überprüft.
Letzte Ausführung um	Datum und Uhrzeit der letzten Ausführung des Auftrags.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellenfeld	Beschreibung
Nutzlast	Liste der Domänen oder anwenderdefinierten URLs, die zur CERT-Bereitstellung an das Rechenzentrum gesendet wurden.
Abrufanzahl	Gibt an, wie oft die Ergebnisse für diesen Auftrag abgefragt wurden.
Ergebnis	Überprüft und validiert jede Domäne oder anwenderdefinierte URL, die in einer Nutzlast gesendet wird.
Status	Status des Rechenzentrumsauftrags.

Generieren Sie SP-Metadaten für anwenderdefinierte SAML/SSO-URL-Installationen

Für eine SAML- oder SSO-Installation sind die SP-Metadaten erforderlich, die für den IdP generiert wurden, bevor die anwenderdefinierte URL-Instanz generiert wird.

Vorbereitungen

Erforderliche Rolle: Administrator

Der IdP benötigt SP-Metadaten für die Instanz, um Anforderungen zu authentifizieren und weiterzuleiten.

Hinweis: Das Hinzufügen der Assertion Consumer Service-URL (SP-Anmelde-URL) kann für jeden IdP (Azure, ADFS oder Okta) unterschiedlich sein.

Prozedur

1. Wählen Sie Ihr installiertes SSO-Plugin aus:

Option	Bezeichnung
Mehrfachanbieter-SSO	Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an. Wählen Sie einen IdP aus, und klicken Sie auf **Generieren Sie Metadaten** Schaltfläche. Die Integration generiert automatisch die SP-Metadaten der Instanz aus den Systemeigenschaftseinstellungen.
SAML 2 SSO	Navigieren zu **SAML 2 Single Sign-on** > **Metadaten**an. Die Integration generiert automatisch die SP-Metadaten der Instanz aus den Systemeigenschaftseinstellungen.

2. Kopieren Sie die SP-Metadaten in das Textfeld.

Zum Beispiel:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
 <AssertionConsumerService isDefault="true" index="0"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://yourinstance.service-now.com/navpage.do" />
 <AssertionConsumerService index="1"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://yourinstance.service-now.com/consumer.do"/>
</SPSSODescriptor>
</EntityDescriptor>
```

3. Geben Sie die Instanz-SP-Metadaten für den IdP an.
   Beispielsweise ermöglicht SSOCircle einem Anwender, die SP-Metadaten online bereitzustellen.
4. **Wahlweise:** So richten Sie anwenderdefinierte URLs in Azure ein:
   a. Wechseln Sie zu **App-Registrierungen** .
   b. Wählen Sie Aus **Alle Apps** Aus dem Menü.
   c. Wählen Sie aus **ServiceNow-App** .
   d. Klicken Sie auf Einstellungen, um die URL zu konfigurieren.
5. **Wahlweise:** So richten Sie anwenderdefinierte URLs in Okta ein:
   a. Erstellen Sie zwei ServiceNow UD Okta-Anwendungen.
   b. Eine Okta-Anwendung für die Instanz-URL „service-now.com“.
   c. Eine Okta-Anwendung für die anwenderdefinierte URL.

   Hinweis:
   - Deaktivieren Sie **Deaktivieren Sie „Authentifizierung Erzwingen“** Innerhalb der Okta-Konfiguration für **Verbindung Testen** Um erfolgreich auszuführen.
   - Wenn Sie den Identitätsanbieter-Datensatz testen, der der Basis-URL zugeordnet ist, müssen Sie sich mit der Basis-URL bei der Instanz anmelden.
   - Wenn Sie den Identitätsanbieter testen, der der anwenderdefinierten URL zugeordnet ist, müssen Sie sich mit der anwenderdefinierten URL bei der Instanz anmelden.
6. **Wahlweise:** Um die OAuth-Authentifizierung zu verwenden, richten Sie die Umleitungs-URL als alle registrierten anwenderdefinierten URLs in der OAuth-Anwendungsendpunktkonfiguration für die externen Client-Anwendungen ein.
   Die Umleitungs-URL ist synonym mit der Rückruf-URL, zu der der Autorisierungsserver umleitet.
7. **Wahlweise:** So verwenden Sie den Google reCAPTCHA-Service: Richten Sie ein API-Schlüsselpaar ein.

Anwenderdefinierte URL-Fehler und Korrekturen

Eine Liste allgemeiner Fehler und zugehöriger Korrekturen für ein anwenderdefiniertes URL-Setup und eine Konfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Setup

Fehlermeldung	Beheben
Anwenderdefinierte URL kann nicht erstellt werden. Versuchen Sie es später erneut.	Möglicherweise liegt ein Problem außerhalb Ihrer Kontrolle vor, das die Erstellung der anwenderdefinierten URL beeinträchtigt. Führen Sie die Ausführung zu einem anderen Zeitpunkt aus, bevor Sie sich an den Support wenden. **Hinweis:** Es dauert normalerweise 30 Minuten, um eine anwenderdefinierte URL zu erstellen. Wenn es länger dauert, wenden Sie sich an https://support.servicenow.com/now?draw=case.
Die Anforderung für eine neue anwenderdefinierte URL kann nicht gesendet werden, da eine andere Anforderung für eine anwenderdefinierte URL für Ihre Instanz noch ausgeführt wird.	Überprüfen Sie den Status Ihrer anwenderdefinierten URL-Aufträge, bevor Sie eine neue Anforderung übermitteln.
Sie müssen die folgenden Eigenschaften löschen, bevor die Instanz-URL festgelegt werden kann: Glide-Proxy, Glide-Servlet.	
Die Bereitstellung von <custom_domain> wird noch ausgeführt. Dieser Prozess kann bis zu X Stunden dauern. Ihr Instanzadministrator erhält eine Benachrichtigung, wenn dieser Prozess abgeschlossen ist.	Nachdem die Bereitstellung in einer Instanz für eine anwenderdefinierte URL gestartet wurde, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor sich der Status ändert.
<custom_domain> ist jetzt als neue Instanz-URL festgelegt. <base.service-now.com> ist noch in Betrieb, aber alle neuen URLs, z. B. in Benachrichtigungen, verwenden <custom_domain>.	Nur eine URL kann als Instanz-URL festgelegt werden. Die anderen URLs, die Ihrer Instanz zugeordnet sind, können aktiv sein, aber nur die Instanz-URL kann Benachrichtigungen verwenden.
Der anwenderdefinierte URL-<custom_domain> wird so festgelegt, dass er sofort aus der Instanzkonfiguration entfernt und auf <base.service-now.com> zurückgesetzt wird. <custom_domain> setzt eine Zuordnung zu dieser Instanz fort, solange der CNAME-Datensatz in Ihrem DNS festgelegt ist.	Diese Nachricht bestätigt, dass Sie Ihre anwenderdefinierte URL ändern möchten. Durch Akzeptieren dieser Bestätigung initiieren Sie die Änderung der URL an Ihrer Instanz. Jede URL, die sich in Ihrer Domänennamenliste als anwenderdefinierte URL befindet, kann aktiv sein, es sei denn, Sie entfernen sie aus dem CNAME-Datensatz Ihres Anbieters.
Sie können glide.servlet.uri nicht ändern. Diese Eigenschaft wird durch die anwenderdefinierte URL festgelegt.	
Sie können glide.proxy.host nicht ändern. Diese Eigenschaft wird durch die anwenderdefinierte URL festgelegt.	
Der CNAME-Datensatz für <custom_domain> verweist nicht auf <base.service-now.com>.	Die Konfiguration auf der URL-Anbieterseite ist nicht korrekt. Überprüfen Sie Ihre Konfiguration im CNAME-Datensatz.
CNAME-Datensatz für <custom_domain> fehlt.	Der CNAME-Datensatz muss von Ihrem URL-Provider konfiguriert werden, bevor die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlermeldung	Beheben
	anwenderdefinierte URL für Ihre Instanz festgelegt werden kann.

Installationsausgänge

Installationsausgänge sind Anpassungen, die Java verlassen, um ein Skript aufzurufen, bevor sie zu Java zurückkehren.

Hinweis: Die hier beschriebene Funktionalität erfordert die **Admin**-Rolle.

Verfügbare Installationsausgänge

Navigieren zu **Systemdefinition** > **Installationsausgänge**an. Einige Installationsausgangsnamen (Login, Logout, ValidatePassword, ExternalAuthentication) sind reserviert und können nicht geändert werden. Andere Installationsausgänge können diese mit einem anwenderdefinierten Skript überschreiben, das das Skript im Standardinstallationsausgang ersetzt.

Die folgenden Installationsausgänge sind im Basissystem verfügbar:

Installationsausgang	Beschreibung
Anmelden	Verwendet ein Anwendername- und Passwortpaar und authentifiziert sich beim Anwenderobjekt
Abmelden	Führt den Anwender nach der Abmeldung zur Willkommensseite; kann von LogoutRedirect überschrieben werden
LogoutUmleitung	Führt den Anwender nach der Abmeldung zu einer angegebenen URL
ExternalAuthentication	Authentifiziert sich mithilfe von Header, Parameter oder Cookie; kann von DigestSingleSignOn und PGPSingleSignOn überschrieben werden
DigestSingleSignOn	Authentifiziert sich mithilfe von Header, Parameter oder Cookie und entschlüsselt die Digest-Verschlüsselung
PGPSingleSignOn	Authentifiziert sich mithilfe von Header, Parameter oder Cookie und entschlüsselt die PGP-Verschlüsselung
ValidatePassword	Standardmäßig aktiv, beginnend mit Helsinki Release; ermöglicht Kunden, ihre eigene Passwortvalidierung zu definieren; kann von ValidatePasswordStronger überschrieben werden
ValidierenPasswordStronger	Passwörter müssen mindestens 8 Zeichen lang sein und eine Ziffer, einen Großbuchstaben und einen Kleinbuchstaben enthalten
GetIntegrationSessionTimeout	Implementiert das standardmäßige Timeout-Verhalten für Integrationssitzungen.

Anmeldungsänderungen

Die folgende Änderung an **Melden Sie Sich An** Beim Installationsausgang wird der Sitzungszeitüberschreitungswert jedes Anwenders festgelegt, während sich der Anwender anmeldet. In diesem Beispiel, wenn der Anwendername lautet *Administrator* , Die Sitzung wird auf eine Zeitüberschreitung in 30 Sekunden festgelegt.

```
gs.include("PrototypeServer");
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

      process : function() {
        // the request is passed in as a global
        var userName = request.getParameter("user_name");
        var userPassword = request.getParameter("user_password");

        var authed = GlideUser.authenticate(userName, userPassword);
        if (authed) {
          // ************************************************************
          // customization - if the userName == admin, set the session
          // timeout to be 30 seconds. You can implement your own
          // session timeout algorithm here by checking to see if a user
          // belongs to a certain group or has a certain role.
          // Values of setMaxInactiveInterval exceeding 1440 minutes are
          // treated as one day (1440 minutes).

         if (userName == "admin") {
            request.getSession().setMaxInactiveInterval(30);
          }
          // ************************************************************
          return GlideUser.getUser(userName);
        }

        this.loginFailed();

        return "login.failed";
      },

      loginFailed : function() {
        var message = GlideSysMessage.format("login_invalid");
        var gSession = GlideSession.get();
        gSession.addErrorMessage(message);

        var userName = request.getParameter("user_name");
        EventManager.queue("login.failed", "", userName, "");
      }

}
```

Sitzungszeitüberschreitung kann auch gemäß IP-Adresse festgelegt werden.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

      process : function() {
        // the request is passed in as a global
        var userName = request.getParameter("user_name");
        var userPassword = request.getParameter("user_password");
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        var authed = GlideUser.authenticate(userName, userPassword);
        if (authed) {

        // ************************************************************
        // customization - if the user is logging in from a particular IP
        // range starting with XXX.XXX you can implement your own
        // session timeout algorithm here by checking the login IP
        //
        // Values of setMaxInactiveInterval exceeding 1440 minutes are
        // treated as one day (1440 minutes).

        var clientIP = gs.getSession().getClientIP().toString();

        // if client IP starts with specified range
        if (clientIP.indexOf('XXX.XXX') == 0) {
          // set to 10 hours
          request.getSession().setMaxInactiveInterval(60 * 60 * 10);
        }
        // ************************************************************

          return GlideUser.getUser(userName);
        }

        this.loginFailed();

        return "login.failed";
      },

      loginFailed : function() {
        var message = GlideSysMessage.format("login_invalid");
        var gSession = GlideSession.get();
        gSession.addErrorMessage(message);

        var userName = request.getParameter("user_name");
        EventManager.queue("login.failed", "", userName, "");
      }

}
```

Zugehörige Informationen

IP-bereichsbasierte Authentifizierung

Eine Möglichkeit zum Sichern einer webbasierten Anwendung besteht darin, den Zugriff basierend auf der IP-Adresse zu beschränken.

Sie können den Zugriff auf eine bestimmte Adresse oder einen bestimmten Adressbereich blockieren, von der Sie vermuten, dass sie böswilligen Personen angehören. Mit der Instanz können Sie den Zugriff nach IP-Adresse steuern.

Hinweis: Verwenden Sie die Vorauthentifizierungskontextrichtlinie für Adaptive Authentication (AA), um IP-basierte Authentifizierungen und Einschränkungen für zusätzliche Funktionen zu erzwingen. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Hinweise und Einschränkungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das System lässt Sie nicht zu, sich selbst zu sperren. Wenn Sie also versuchen, eine Regel hinzuzufügen, die Ihre aktuelle Adresse gesperrt würde, warnt das System Sie und lehnt Ihre Einfügung ab.
- Wenn Sie sich in einem Unternehmens-Intranet befinden, seien Sie bei der Einrichtung Ihrer IP-Regeln sehr vorsichtig. Die IP-Adresse, die Sie auf Ihrem eigenen Computer sehen (z. B. 10.10.10.25), hat im Allgemeinen keine Beziehung zur IP-Adresse, die Sie tatsächlich im Internet angezeigt werden. Ihr Unternehmen gibt Ihre Adresse wahrscheinlich Proxys und/oder NATs in einen vorhersehbaren Satz ausgehender Adressen, zu denen Sie Ihr Netzwerkteam wahrscheinlich fragen müssen.
- Ein Anwender, dessen Zugriff basierend auf einer Zugriffsregel eingeschränkt ist, erhält in seinem Browser den Fehler 403.
- Eingeschränkte Anwender verwenden keine Transaktionen, Semaphore oder zählen nicht für die Anzahl der Serverressourcen an.
- Diese Funktion ersetzt oder überschreibt Ihre vorhandenen Zugriffssteuerungsregeln nicht, wenn Sie beispielsweise ein VPN in unserem Rechenzentrum ausführen. Dies ist eine zusätzliche Prüfung, die zusätzlich zu allen Zugriffssteuerungen erfüllt werden muss, die wir möglicherweise für Ihr PIX eingerichtet haben.
- Allow-Regeln ersetzen immer Deny-Regeln. Wenn also eine Adresse sowohl zulässig (durch eine Regel) als auch verweigert (durch eine zweite Regel) ist, ist sie tatsächlich zulässig.
- Sternchen und CIDR-Blöcke werden derzeit nicht unterstützt.
- Bei weitergeleiteten Proxy-Adressen werden die Allow-Regeln auf jede Adresse in der Kette angewendet, und dann werden die Deny-Regeln auf jede Adresse in der Kette angewendet, wenn keine der Allow-Regeln übereinstimmt.
- Die IP-bereichsbasierte Authentifizierung kann sich auf die Übertragung von Update-Sätzen auswirken. Wenn die Zugriffssteuerung für IP-Adressen in der Quellinstanz aktiviert ist, fügen Sie die IP-Adressen aller Anwendungsknoten, die Ihre Instanz unterstützen, als Ausnahmen hinzu.

Hinweis: Um Informationen zu Ihren Instanz-IP zu finden, melden Sie sich bei an ServiceNow – NOW-Support , Und suchen Sie nach **Meine IP-Informationen** Servicekatalogelement.

Hinweis: Um mehr über zu erfahren `com.snc.ipauthenticator`Und `glide.ip.authenticate.strict`Eigenschaften, die den Instanzzugriff auf bestimmte IP-Bereiche beschränken, finden Sie in den folgenden Themen unter Instanzsicherheits-Härtungseinstellungen:

Plugin „Zugriff auf bestimmte IP-Bereiche einschränken“ [aktualisiert in Security Center 1,3]

Zugriffssteuerung für IP-Adressen

Wenden Sie eine IP-Zugriffssteuerung auf ausgehenden Datenverkehr, eingehenden Datenverkehr oder bidirektionalen Datenverkehr an. Das System blockiert eine IP-Adresse nur, wenn eine übereinstimmende Deny-Regel vorhanden ist und keine übereinstimmende Allow-Regel vorhanden ist. Standardmäßig gibt es keine Einschränkungen für den Zugriff auf Ihre Instanz.

Vorbereitungen

Hinweis: Verwenden Sie die Vorauthentifizierungskontextrichtlinie für Adaptive Authentication (AA), um IP-basierte Authentifizierungen und Einschränkungen für zusätzliche Funktionen zu erzwingen. Weitere Informationen finden Sie unter Adaptive Authentifizierung.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Die IP-Adresssteuerung ist nur für externe IPs konfiguriert und blockiert keine internen IP-Adressen von ServiceNow.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **IP-Adressen-Zugriffssteuerung** Um eine Liste Ihrer IP-Zugriffssteuerungen anzuzeigen.
   Möglicherweise müssen Sie das Plugin „IP-bereichsbasierte Authentifizierung“ [com.snc.ipauthenticator] aktivieren.
2. Füllen Sie das Formular aus.

   Hinweis: Um Informationen zu Ihren Instanz-IP zu finden, melden Sie sich bei an ServiceNow – NOW-Support , Und suchen Sie nach **Meine IP-Informationen** Servicekatalogelement.

Feld	Beschreibung
Typ	Typ der einzubeziehenden Zugriffssteuerungsregel. ○ *Zulassen* : Jede IP-Adresse in diesem Bereich kann mit dieser Instanz interagieren. ○ *Ablehnen* : Jede IP-Adresse in diesem Bereich kann nicht mit dieser Instanz interagieren, es sei denn, sie ist in einer Allow-Regel aufgeführt. Außerdem können Sie beim Hinzufügen von Deny-Regeln Ihre eigene öffentliche IP-Adresse nicht verweigern, oder Ihre Instanz aktualisiert keine Deny-Regel. **Hinweis:** Zur Unterstützung von Wartung, Upgrades und Kundenservice und Support, Einige ServiceNow Interne IPs können nicht durch Deny-Regeln blockiert werden.
Wegbeschreibung	Richtung der IP-Zugriffssteuerungsregel. ○ **Eingehend** : Lässt eingehende Transaktionen zu oder lehnt sie ab. Dies sind Transaktionen, die von außerhalb Ihrer Instanz initiiert wurden. ○ **Ausgehend** : Lässt ausgehende Transaktionen zu oder lehnt sie ab. Dies sind Transaktionen, die von innerhalb Ihrer Instanz initiiert wurden. ○ **Bidirektional** : Erlaubt oder lehnt sowohl eingehende als auch ausgehende Transaktionen ab.
Aktiv	Wenn diese Option ausgewählt ist, ist das Formular aktiv.
Beschreibung	Beschreibung der Zugriffssteuerung.
Bereichsstart	Startbereich von IP-Adressen, die zugelassen oder abgelehnt werden sollen. **Hinweis:** Diese Regeln wirken sich auch auf die Übertragung von Update-Sätzen aus. Um sicherzustellen, dass die Zugriffssteuerung für IP-Adressen nicht dazu führt, dass Update-Sätze fehlschlagen, fügen Sie die Zielinstanz als Ausnahme hinzu.
Bereichsende	Endbereich von IP-Adressen, die zugelassen oder abgelehnt werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Um den Zugriff nur auf bestimmte VPN-Adressen zu beschränken, geben Sie einen Sperrbereich von ein **0.0.0.0** Bis **255.255.255.255** In **Ablehnen** Und geben Sie nur die spezifischen zulässigen VPN-Bereiche ein.

3. Klicken Sie auf **Absenden**.

Abgelehnte IP-Adressen suchen

Suchen Sie abgelehnte IP-Adressen in den Knotenprotokolldateien der Instanz.

Vorbereitungen
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird
Protokolleinträge für blockierte IP-Adresse werden wie folgt angezeigt: `2018-10-21 18:37:43 (175) http-30 WARNUNG *** WARNUNG *** Sicherheit eingeschränkt: Zugriff eingeschränkt (xx.xx.xxx.xxx nicht autorisiert 2015)` .

Hinweis: Abgelehnte IP-Adressen sind die Knotenprotokolldateien der anzeigbaren Instanz, die nicht in den Systemprotokollen angezeigt werden können.

Prozedur

1. Navigieren zu **Alle** > **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Browser.**an.
2. Durchsuchen Sie die Protokolle nach Kriterien, z. B. Zeitraum und Nachricht.
3. Sie können Protokolldateien auch herunterladen, wenn Sie wissen, nach welchem Protokoll Sie suchen, indem Sie zu navigieren **Systemprotokolle** > **Dienstprogramme** > **Knotenprotokolldatei-Download**an.

Integration von Lightweight Directory Access Protocol

Mit einer LDAP-Integration kann Ihre Instanz Ihren vorhandenen LDAP-Server als primäre Quelle von Anwenderdaten verwenden.

Administratoren integrieren ein LDAP-Verzeichnis (Lightweight Directory Access Protocol), um den Anwenderanmeldeprozess zu optimieren und administrative Aufgaben wie das Erstellen von Anwendern und das Zuweisen von Rollen zu automatisieren. Eine LDAP-Integration ermöglicht es dem System, Ihren vorhandenen LDAP-Server als primäre Quelle von Anwenderdaten zu verwenden. Normalerweise ist eine LDAP-Integration auch Teil einer Single Sign-on-Implementierung.

Die Integration verwendet die Anmeldeinformationen des LDAP-Service-Accounts, um den eindeutigen Anwendernamen (DN) vom LDAP-Server abzurufen. Bei Angabe des DN-Werts für den Anwender wird die Integration dann mit LDAP mit dem DN und dem Passwort des Anwenders erneut gebunden. Das vom Anwender eingegebene Passwort ist vollständig in der HTTPS-Sitzung enthalten. Die Integration speichert nie LDAP-Passwörter.

Die Integration verwendet eine schreibgeschützte Verbindung, die nie in das LDAP-Verzeichnis schreibt. Die Integration fragt nur Informationen ab und aktualisiert dann die interne Datenbank entsprechend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Ausführliche Informationen zum Einrichten der Integration finden Sie unter Setup der LDAP-Integration.

Hinweis: Wenn Ihre Instanz eine LDAP-Integration verwendet und die Active Directory-Einstellungen erfordern, dass Anwender ihr Passwort bei der Anmeldung zurücksetzen, können sich Ihre Anwender nicht bei der Instanz anmelden. Die Instanz kann das Active Directory-Passwort eines Anwenders nicht ändern.

Funktionen der LDAP-Integration

Die LDAP-Integrationsfunktionen umfassen Folgendes.

Geplante LDAP-Aktualisierung

Ein geplanter Scan Ihres LDAP-Servers wird normalerweise einmal pro Nacht ausgeführt. Es fragt die Attribute aller anwendbaren Anwenderdatensätze ab und vergleicht sie mit dem Account auf unseren Servern. Wenn ein Unterschied besteht, ändern wir unseren Anwenderdatensatz mit dem geänderten Attribut. Die Last, die während der Aktualisierung auf den LDAP-Server gesetzt wird, hängt davon ab, wie viele Datensätze abgefragt werden und wie viele Attribute verglichen werden. Wir empfehlen, die Aktualisierung außerhalb der Spitzenzeiten zu planen. Ein großer Aktualisierungsvorgang kann sich auf andere geplante Vorgänge auswirken, z. B. das Ausführen von Berichten, und sollte geplant werden, um Konflikte zu minimieren.

LDAP-Listener

LDAP-Listener ist unsere Version einer persistenten Abfrage (oder persistenten Suche). Wir stellen eine Dauerabfrage für Änderungen an Ihrem LDAP-Server aus und warten ständig auf eine Antwort. Vorausgesetzt, Ihr Server unterstützt eine persistente Suche, werden alle Änderungen, die an einem Ihrer anwendbaren LDAP-Accounts vorgenommen wurden, an den LDAP-Listener zurückgegeben und innerhalb von etwa 10 Sekunden an Ihre Instanz gesendet. Dies ist ein äußerst nützliches Tool, mit dem wir nahezu in Echtzeit die Accountdetails Ihrer Anwender abrufen können, ohne auf die nächste geplante Aktualisierung warten zu müssen.

LDAP-Anmeldung bei Bedarf

Nachdem eine LDAP-Integration eingerichtet wurde, kann die Instanz neuen Anwendern ermöglichen, sich beim System anzumelden, auch wenn sie noch keinen Account in der Instanz haben. Wenn ein neuer Anwender versucht, sich bei der Instanz anzumelden, überprüft die Integration, ob dieser Anwender über einen Account in der Instanz verfügt. Wenn die Integration keinen vorhandenen Anwenderaccount findet, fragt sie den LDAP-Server automatisch nach dem eingegebenen Anwendernamen ab. Wenn ein übereinstimmender LDAP-Account gefunden wird, versucht die Integration, sich mit dem vom Anwender eingegebenen Passwort zu authentifizieren. Wenn das Passwort gültig ist, erstellt die Instanz einen Account für den Anwender, füllt den Account mit allen anwendbaren LDAP-Informationen aus und meldet den Anwender bei der Instanz an.

Bei der Anmeldung bei Bedarf wird die Transformationszuordnung „LDAP-Anwenderimport“ verwendet. Weitere Informationen zu Transformationszuordnungsanforderungen finden Sie unter LDAP-Transformationszuordnungen.

LDAP-Datenauffüllung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die in dieser Integration beschriebene Funktionalität ist standardmäßig nicht verfügbar. Diese Integration umfasst eine Anpassung nach der Bereitstellung, die von einem erfahrenen Administrator oder von durchgeführt wird ServiceNow Berater für professionelle Services.

Eine Integration in die LDAP-Server ermöglicht es Ihnen, die Datenbank der Instanz schnell und einfach mit Anwenderdatensätzen aus der vorhandenen LDAP-Datenbank zu füllen. Um Dateninkonsistenzen zu verhindern, können Sie eingehende LDAP-Datensätze erstellen, ignorieren oder überspringen.

Sie können auch die Daten einschränken, die die Integration importiert, indem Sie LDAP-Attribute angeben und dadurch nur die Daten importieren, die Sie für eine Instanz bereitstellen möchten. Normalerweise werden die von Ihnen angegebenen LDAP-Attribute Teil der Integration Transformationszuordnung . Wenn Sie keine LDAP-Attribute angeben, importiert die Integration alle verfügbaren Objektattribute vom LDAP-Server. Die Instanz speichert importierte LDAP-Daten in temporären Importsatztabellen. Je mehr Attribute Sie importieren, desto länger ist die Importzeit. Weitere Informationen finden Sie unter Geben Sie die LDAP-Attribute an.

LDAP-Authentifizierung

Verwenden Sie die LDAP-Authentifizierung für den Zugriff mit LDAP-Anmeldeinformationen.

Wenn ein Anwender auf der Anmeldeseite Netzwerkanmeldeinformationen eingibt:

1. Die Instanz übergibt die Anmeldeinformationen an einen LDAP-Server, um die Instanz zu finden.
2. Mit RDNs wird die DN-Zeichenfolge des Anwenders validiert. Wird nur validiert, wenn mindestens eine der LDAP-OU-Konfigurationen mit verwendet wird Tabelle=sys_user Hat einen RDN konfiguriert.
3. Der LDAP-Server antwortet mit einer autorisierten oder nicht autorisierten Nachricht, die das System verwendet, um zu bestimmen, ob Zugriff gewährt werden soll.

Durch die Authentifizierung bei Ihrem LDAP-Server greifen Anwender mit denselben Anmeldeinformationen auf die Plattform zu, die sie für andere interne Ressourcen in Ihrer Netzwerkdomäne verwenden. Außerdem können Sie alle vorhandenen Passwörter und Sicherheitsrichtlinien wiederverwenden, die bereits vorhanden sind. Beispielsweise verfügt der LDAP-Server möglicherweise bereits über Richtlinien zum Sperren von Accounts und zum Ablauf von Passwörtern.

Wenn Sie LDAP aktivieren, aktualisiert das System Anwenderdatensätze mit diesen Feldern.

Aktualisierungen des LDAP-Anwenderdatensatzes

Feld	Beschreibung
Quelle	Gibt an, ob LDAP zur Validierung eines Anwenders verwendet wird. Wenn die Quelle mit ldap beginnt, wird der Anwender über LDAP validiert. Wenn die Quelle nicht mit ldap beginnt, wird das Passwort im Anwenderdatensatz verwendet, um den Anwender bei der Anmeldung zu validieren.
LDAP-Server	Gibt an, welcher LDAP-Server den Anwender authentifiziert, wenn mehrere LDAP-Server vorhanden sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Das System unterstützt keine LDAP-Passwortauthentifizierung über einen MID-Server. Eine Instanz muss eine direkte Verbindung mit einem LDAP-Server herstellen können, um die Passwortauthentifizierung zu unterstützen.

LDAP-Integration verstehen

Mit einer LDAP-Integration kann Ihre Instanz Ihren vorhandenen LDAP-Server als primäre Quelle von Anwenderdaten verwenden.

LDAP-Integrationsvoraussetzungen

- Der Verzeichnisservices-Server muss LDAP v3-konform sein
- Eingehender Netzwerkzugriff über die Firewall muss zulässig sein (auf den LDAP-Server)
- Externe IP oder Name des LDAP-Servers
- Anwenderanmeldeinformationen mit schreibgeschütztem Zugriff
- Für LDAPS ein PKI-Zertifikat

LDAP-Integrationszeitpunkt

LDAP-Integrationen werden normalerweise vor dem Go-Live der Instanz durchgeführt, können jedoch jederzeit integriert werden.

LDAP-Serverdatenintegrität

Einige Anwender haben Bedenken, dass eine Drittpartei (in diesem Fall die Instanz) Änderungen an Ihrem LDAP-Server vornimmt (schreibt). In einer LDAP-Integration schreibt Ihre Instanz nicht in das interne LDAP-Verzeichnis. Die Instanz fragt Informationen ab und aktualisiert ihre Datenbank entsprechend.

Die Instanz nimmt keine Änderungen am internen LDAP-Server vor. Der Service-Account ist schreibgeschützt.

Die meisten Änderungen (einschließlich Ergänzungen) an Ihrem LDAP-Server sind der Instanz innerhalb von Sekunden verfügbar, je nachdem, wie viele Komponenten der vollständigen LDAP-Integration vorhanden sind.

Um die Synchronisierung von LDAP-Datensätzen zu gewährleisten, planen Sie einen regelmäßigen Scan des LDAP-Servers, um Änderungen zu erfassen.

Die Instanz synchronisiert keine Abteilungsdatensätze. Anwender und Gruppenmitgliedschaften werden durch den LDAP-Listener-Mechanismus und eine tägliche vollständige LDAP-Suche auf dem neuesten Stand gehalten, aber die Instanz löscht keine dieser Einträge, sobald sie aus LDAP entfernt wurden.

Wenn ein Eintrag gelöscht werden soll, wird auch der gesamte Verlauf gelöscht, und alle Verweise darauf werden gelöscht oder gelöscht. Konfigurationselemente (CIs), SLA-Vereinbarungen, Softwarelizenzen, Bestellungen und Servicekatalog-Einträge haben alle einen Verweis auf Abteilung. Wenn Abteilung gelöscht wird, werden diese Verweise gelöscht. Es gibt viele Verweise auf Anwender, daher würde das Löschen eines Anwenders den gesamten Verlauf dessen verlieren, was dieser Anwender getan hat. Derzeit treffen unsere Kunden die Entscheidung, zu löschen oder nicht zu löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheit

Die Verbindung wird von einem einzelnen Computer über eine feste IP-Adresse über einen bestimmten Port in Ihrer Firewall hergestellt. Die Authentifizierung erfolgt mit einem schreibgeschützten LDAP-Account Ihrer Wahl. Sie können Standard-LDAP verwenden oder die öffentliche Seite eines laden SSL-Zertifikat in Ihrem Verzeichnis installiert , In diesem Fall können wir LDAPS verwenden. Um eine weitere Sicherheitsebene hinzuzufügen, bieten wir auch die Option eines Punkt-zu-Punkt-IPSEC-VPN-Tunnels an. Wenden Sie sich an Ihren Account Manager, um Details und Preise zu erhalten.

Sichere LDAP-Verbindungen

Verbindung	Beschreibung
MID-Server	Um Ihren LDAP-Server vor externem Netzwerkverkehr zu schützen, installieren Sie einen MID-Server im lokalen Netzwerk, und konfigurieren Sie das System so, dass es über einen sicheren Kanal mit dem MID-Server kommuniziert.
LDAPS	Um eine verschlüsselte LDAPS-Verbindung herzustellen, laden Sie die öffentliche Seite des SSL-Zertifikats Ihres LDAP-Servers. Die Integration verwendet das Zertifikat, um die gesamte Kommunikation zwischen dem LDAP-Server und der Instanz zu verschlüsseln.
VPN	Um den LDAP-Server mit einem verschlüsselten Punkt-zu-Punkt-IPSEC-VPN-Tunnel zu sichern, wenden Sie sich an Ihren Account Manager, um Details und Preise zu erhalten.

Ein weiterer zu berücksichtigender Sicherheitsaspekt sind die in einer LDAP-Integration freigegebenen Daten. Um die für Ihre Instanz verfügbaren Daten zu begrenzen, geben Sie Attribute in Ihrer Transformationszuordnung an. Weitere Informationen finden Sie unter LDAP-Transformationszuordnungen.

LDAP-Daten werden in die Instanz importiert

Es wird empfohlen, Attribute so zu definieren, dass nur erforderliche Daten importiert werden. Definierte Attribute werden der Instanzanwenderdatenbank zugeordnet.

Wir können die Frage nicht beantworten, welche spezifischen Attribute erforderlich sind, da dies durch den Umfang des Projekts und die Geschäftsanforderungen bestimmt wird.

Unterstützte Typen von LDAP-Servern

Die Instanz wurde erfolgreich in Microsoft Active Directory, Novell, Domino (Lotus Notes) und Open LDAP integriert. Wir verwenden JNDI, um eine Schnittstelle mit dem LDAP-Server herzustellen. Solange Ihr LDAP-Server LDAP v3-konform ist, ist die Integration erfolgreich.

LDAP-Single-Sign-on

Zusammen mit der Datenauffüllungsfunktion, die mit dem LDAP-Import bereitgestellt wird, können Sie die von der Anwendung unterstützte externe Authentifizierungsfunktion verwenden, um zu verhindern, dass sich Ihre Anwender jedes Mal anmelden müssen.

Mehrere LDAP-Domänen

Die empfohlene Methode für die Verarbeitung mehrerer Domänen besteht darin, einen separaten LDAP-Serverdatensatz für jede Domäne zu erstellen. Jeder LDAP-Serverdatensatz muss auf einen Domänencontroller für diese Domäne verweisen. Dies bedeutet, dass das lokale Netzwerk Verbindungen zu jedem der Domänencontroller zulassen muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Erweiterung auf mehr als eine Netzwerkdomäne ist es wichtig, dass Sie eindeutige LDAP-Attribute für die Anwendungsanwendernamen identifizieren und Zusammenfügungswerte importieren. Ein gemeinsames eindeutiges Zusammenfügungsattribut für Active Directory ist ObjektSid . Eindeutige Anwendernamen können je nach LDAP-Datendesign variieren. Allgemeine Attribute sind E-Mail Oder UserPrincipalName .

Verarbeitung von Abfragegrenzwerten

Standardmäßig hat Active Directory 2000/2003 einen LDAP-Abfragegrenzwert (MaxPageSize) Von 1000 Objekten, um übermäßige Lasten und Denial-of-Service-Angriffe zu verhindern. Wir haben zwei Methoden, um mit diesem Grenzwert umzugehen.

Die Standardmethode besteht darin, die Abfrage so aufzuteilen, dass weniger als 1000 Objekte gleichzeitig zurückgegeben werden. Beispielsweise fragen Sie nur ein Objekt ab, das mit dem Buchstaben „a“ beginnt, und fragen Sie dann nach „b“-Objekten ab. Die effizientere Methode für große Umgebungen besteht in der Aktivierung von Paging. Paging wird standardmäßig auf allen Microsoft Active Directory-Servern unterstützt. Die Ergebnisse werden automatisch in mehrere Ergebnissätze aufgeteilt, sodass wir die Abfrage nicht in mehrere Anforderungen aufteilen müssen.

LDAP-Abfragetyp

Wenn ein LDAP-Passwort angegeben wird, wird eine „einfache Bindung“ durchgeführt. Wenn kein LDAP-Passwort angegeben wird, wird „keines“ verwendet. In diesem Fall muss der LDAP-Server eine anonyme Anmeldung zulassen.

LDAP-Authentifizierung

Wir verwenden bereitgestellte Service-Account-Anmeldeinformationen für LDAP, um den Anwender-DN vom LDAP-Server abzurufen. Bei Angabe des DN-Werts für den Anwender wird dann anhand des Anwenders-DN und des angegebenen Passworts eine erneute Bindung mit LDAP durchgeführt.

Passwortspeicher

Das vom Anwender eingegebene Passwort ist vollständig in seiner HTTPS-Sitzung enthalten. Wir speichern dieses Passwort nirgendwo.

LDAP-Authentifizierung wird eingerichtet

Diese Felder im Anwenderdatensatz beziehen sich auf LDAP:

- **Quelle** : Das Feld Quelle gibt an, ob ein Anwender mit LDAP validiert wird. Wenn das Quellfeld mit „ldap“ beginnt, wird der Anwender über LDAP validiert. Wenn das Feld „Quelle“ nicht mit „ldap“ beginnt, wird das Passwort im Anwenderdatensatz verwendet, um den Anwender bei der Anmeldung zu validieren.
- **LDAP-Server** : Die Instanz unterstützt mehrere LDAP-Server, daher bestimmt das Feld LDAP-Server, welcher Server zur Authentifizierung des Anwenders verwendet werden soll.

LDAP-Integrationsanforderungen

Überprüfen Sie die Anforderungen für die LDAP-Integration, die ein PKI-Zertifikat einen LDAP-konformen Verzeichnisserviceserver umfassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Integration erfordert:

- Ein LDAP v3-konformer Verzeichnisserviceserver
  - Ermöglicht eingehenden Netzwerkzugriff über die Firewall (auf den LDAP-Server)
  - (Optional) akzeptiert die anonyme Anmeldung
  - (Optional) unterstützt Paging für große LDAP-Abfragen
- Die externe IP-Adresse oder der vollqualifizierte Domänenname des LDAP-Servers. Sie können auch verwenden MID-Server .
- Ein schreibgeschützter LDAP-Account Ihrer Wahl
- Für mehrere Domänen Netzwerkzugriff für jeden Domänencontroller
- Für LDAPS ein PKI-Zertifikat
- Für LDAP-Listener ein Microsoft Active Directory-Server, der persistente Abfragen unterstützt (ADNotify)

Unterstützte LDAP-Server

Verwenden *JNDI* Für die Schnittstelle mit dem LDAP-Server wurde die Instanz erfolgreich in die folgenden Server integriert:

- Microsoft Active Directory
- Novell
- Domino (Lotus Notes)
- Öffnen Sie LDAP

LDAP-Abfragegrenzwerte

Standardmäßig hat Active Directory 2000/2003 einen LDAP-Abfragegrenzwert (MaxPageSize) Von 1000 Objekten, um übermäßige Lasten und Denial-of-Service-Angriffe zu verhindern. Das System verfügt über zwei Methoden zur Handhabung dieses Grenzwerts.

- Die Standardmethode besteht darin, die Abfrage so aufzuteilen, dass weniger als 1000 Objekte gleichzeitig zurückgegeben werden. Beispielsweise fragen Sie nur Objekte ab, die mit dem Buchstaben a beginnen, und fragen Sie dann nach b-Objekten ab.
- Die effizientere Methode für große Umgebungen besteht in der Aktivierung von Paging, das standardmäßig auf allen Microsoft Active Directory-Servern unterstützt wird. Paging teilt die Ergebnisse automatisch in mehrere Ergebnissätze auf, damit die Integration die Abfrage nicht in mehrere Anforderungen aufteilen muss.

Setup der LDAP-Integration

Administratoren können die LDAP-Integration aktivieren, um die Anmeldung von Anwendern über das LDAP-Verzeichnis des Unternehmens zu ermöglichen.

LDAP verwendet normalerweise einen dieser Arten von Kommunikationskanälen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Kommunikationskanäle

Verbindung	Beschreibung	LDAP-Importunterstützung?	Unterstützung der LDAP-Authentifizierung?
MID-Server-Verbindung	Kommuniziert standardmäßig über HTTP auf Port 80. Für diesen Kommunikationskanal ist kein Zertifikat erforderlich. Die Verbindung zwischen dem MID-Server und der Instanz erfolgt über HTTPS (Port 443). Sie können den MID-Server verwenden, um Daten über LDAP zu importieren, aber Sie können den MID-Server nicht für die LDAP-Authentifizierung verwenden. Fahren Sie mit fort Definieren Sie den LDAP-Server .	Ja	Nein
Standard-LDAP-Integration	Kommuniziert standardmäßig über TCP auf Port 389. Für diesen Kommunikationskanal ist kein Zertifikat erforderlich. Fahren Sie mit fort Definieren Sie den LDAP-Server .	Ja	Ja
SSL-verschlüsselte LDAP-Integration (LDAPS)	Kommuniziert standardmäßig über TCP auf Port 636. Dieser Kommunikationskanal erfordert ein Zertifikat. Fahren Sie mit fort Installieren Sie das LDAP X.509 SSL-Zertifikat Zum Abrufen und Hochladen des Zertifikats.	Ja	Ja
VPN-Verbindung	Kommuniziert über einen IPSEC-Tunnel. Kaufen oder erstellen Sie einen IPSEC-Tunnel in Ihrem lokalen Netzwerk. Fahren Sie mit fort Definieren Sie den LDAP-Server .	Ja	Ja

Bei Verwendung eines MID-Servers stellt der MID-Server eine Verbindung zur Instanz her, und der MID-Server stellt auch eine Verbindung zum LDAP-Server her. In beiden Fällen initiiert der MID-Server die Verbindung:

1. Zuerst stellt der MID-Server eine Verbindung zum LDAP-Server über LDAP auf Port 389 her.
2. Dann initiiert der MID-Server eine HTTPS-verschlüsselte Verbindung mit der Instanz auf Port 443, um die Daten an die Instanz zu übertragen.

Weitere Informationen zu VPNs, MID-Servern und LDAP finden Sie unter Sie benötigen kein VPN-Teil II In der Community.

Installieren Sie das LDAP X.509 SSL-Zertifikat

Sie können ein X.509-Zertifikat für Ihre LDAP-Integration installieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Kaufen oder generieren Sie ein SSL-Zertifikat auf Ihrem LDAP-Server.
2. Navigieren zu **LDAP** > **Zertifikat** Und klicken Sie auf **Neu** .
3. Füllen Sie die Formularfelder aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Der Zertifikatname.
Ablaufbenachrichtigung	Wählen Sie diese Option aus, um eine Benachrichtigung an die in ausgewählten Anwender zu senden **Benachrichtigen Sie bei Ablauf** Feld. Standardmäßig ist dies aktiviert.
Benachrichtigung bei Ablauf	Wählen Sie die Anwender aus, um die Benachrichtigung über den Ablauf des Zertifikats zu überarbeiten. Wenn keine Anwender ausgewählt sind, wird standardmäßig der angemeldete Anwender zusammen mit den letzten beiden angemeldeten Anwendern mit der Administratorrolle hinzugefügt.
Tage vor Ablauf benachrichtigen	Die Anzahl der Tage vor Ablauf, die die Instanz die Benachrichtigung sendet. Geben Sie einen Wert von mindestens 20 ein. Für Instanzen, die auf Istanbul und spätere Releases aktualisiert wurden, ist dieser Wert auf 20 festgelegt, es sei denn, ein größerer Wert ist angegeben.
Aktiv	Ein Kontrollkästchen, das angibt, dass dieses Zertifikat aktiv ist.
Format	Das Format des Zertifikats.
Typ	Der Zertifikatcontainer. Die Instanz erkennt Zertifikate aus Truststores, Java-Schlüsselspeicher und PKCS#12-Schlüsselspeicher.
Gültig ab	Die Instanz fügt diesem Feld automatisch das Zertifikat „gültig ab“ hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft ab	Die Instanz fügt diesem Feld automatisch das Ablaufdatum des Zertifikats hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft in Tagen ab	Die berechnete Anzahl von Tagen bis zum Ablauf.
Kurzbeschreibung	Eine Beschreibung für das Zertifikat.
Bearbeiter	Die Instanz fügt diesem Feld automatisch den Zertifikataussteller hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Betreff	Die Instanz fügt diesem Feld automatisch den Zertifikatbetreff hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
PEM-Zertifikat	Geben Sie den Wert des X509-Zertifikats ein.

Hinweis: Die Integration signiert das Zertifikat derzeit in der Kommunikation zwischen der Instanz und dem IdP nicht.

4. Klicken Sie auf **Speichern**.

Nächste Maßnahme
Klicken Sie Auf **Validiert Speicher/Zertifikate** Zum Testen des Truststores und des Zertifikats.

Definieren Sie einen LDAP-Server

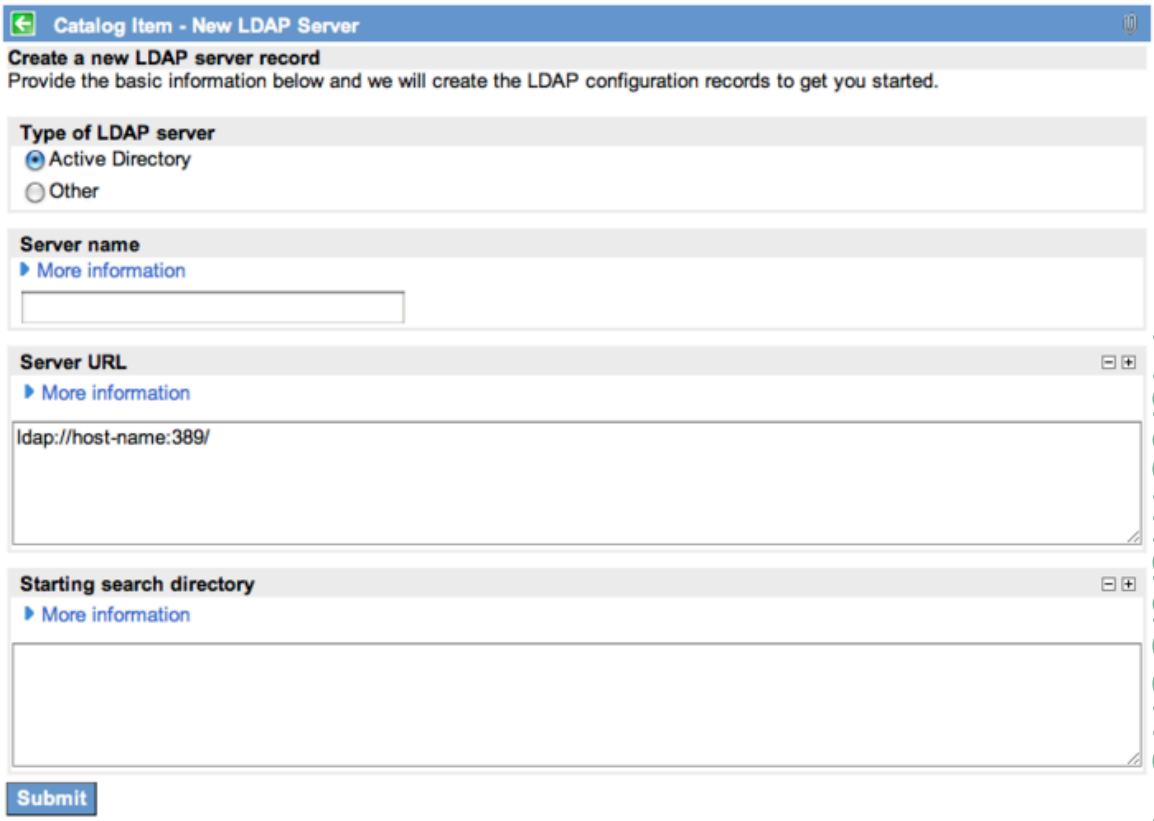
Erstellen Sie einen neuen LDAP-Serverdatensatz in der Instanz.

Vorbereitungen
Erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **Neuen Server erstellen**an.
2. Füllen Sie die Formularfelder aus.



In **Server-URL** Feld werden die gültigen URLs aller Server durch ein Leerzeichen getrennt angezeigt. Server werden zuerst nach Betriebsstatus sortiert, mit Servern, die sind **Aktiv** Zuerst aufgeführt, dann sortiert nach **Reihenfolge** Von Ihnen angegebener Wert. Der erste aufgeführte Server ist der primäre LDAP-Server. Die anderen sind redundante Server.

Hinweis: Zwischen der Änderung des tatsächlichen Betriebsstatus und der Anzeige gibt es eine leichte Verzögerung.

Alternativ können Sie einen redundanten LDAP-Server hinzufügen, indem Sie zu einem vorhandenen LDAP-Server-Datensatz navigieren und eine Zeile in die eingebettete Liste der LDAP-Server-URLs einfügen.

3. Klicken Sie auf **Absenden**.

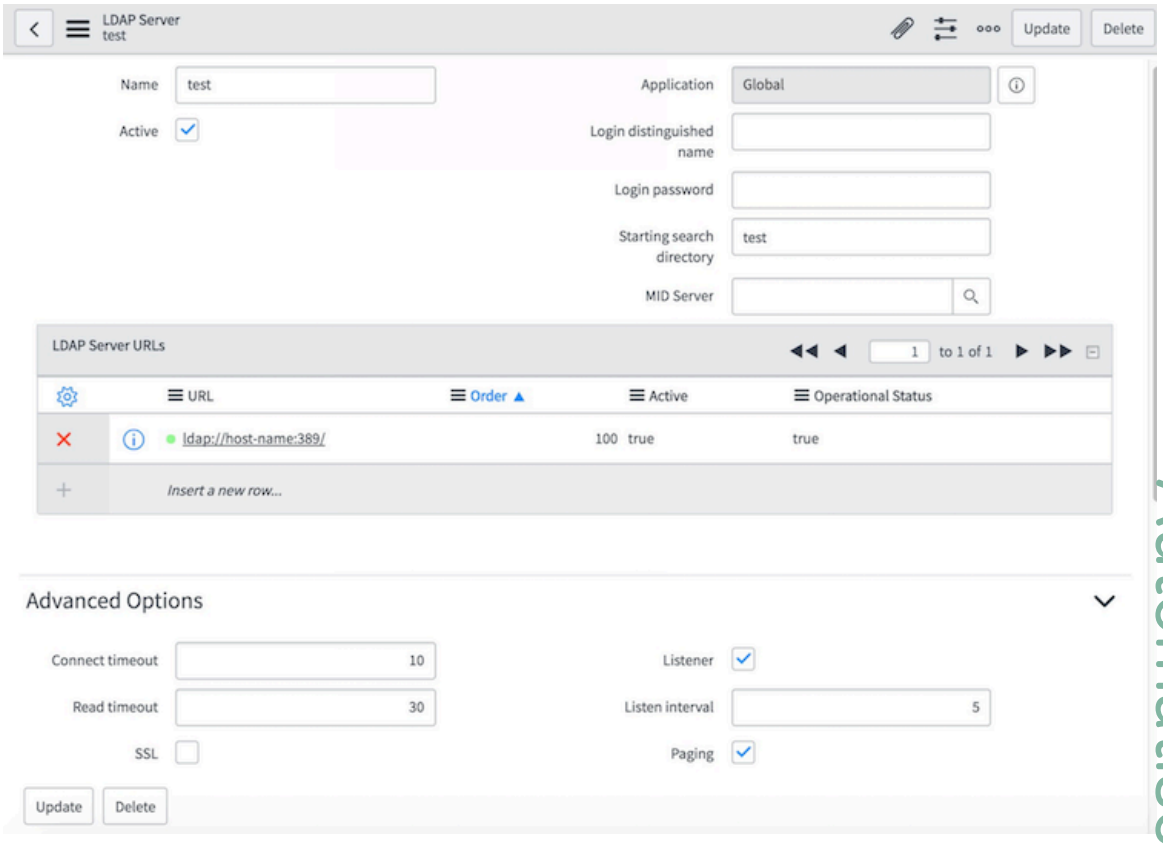
Hinweis: Sie können auch einen vorhandenen LDAP-Server-Datensatz ändern, indem Sie zu navigieren **System-LDAP** > **LDAP-Server** Und nehmen die erforderlichen Änderungen vor.

4. Nehmen Sie bei Bedarf Änderungen an den Feldern vor.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Serverformular



Feld	Beschreibung
Name	Geben Sie den Namen des Servers ein.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, wenn der Server aktiv ist.
LDAP-Server-URLs	Geben Sie die URLs der primären und Sicherungsserver für LDAP ein. Server werden zuerst nach Betriebsstatus sortiert, wobei Server, die zuerst auf der Liste hochgefahren sind, und dann nach dem von Ihnen angegebenen Reihenfolgewert sortiert werden. Der erste aufgeführte Server ist der primäre LDAP-Server. Die anderen sind redundante Server.
Server-URL	Geben Sie die URL des Servers ein. Konfigurieren Sie das Formular, um dieses Feld bei Bedarf hinzuzufügen. Es handelt sich um ein berechnetes schreibgeschütztes Feld, das die Liste der LDAP-Server anzeigt, die Sie auch in anzeigen können **LDAP-Server-URLs** Feld, durch ein Leerzeichen getrennt und nach Betriebsstatus und den Reihenfolgenwerten der URLs sortiert.
Eindeutiger Anmeldename	Geben Sie den eindeutigen Namen (DN) des Anwenders ein, der die LDAP-Verbindung authentifiziert. Für den Zugriff auf einen LDAP-Verzeichnisserver muss der Anwendername das vollständige Format für eindeutige Namen aufweisen: servicenow@service-now.com
Anmeldepasswort	Geben Sie das Passwort des Servers ein.
Suche im Verzeichnis wird gestartet	Geben Sie den relativen Distinguished Name (RDN) des Standardsuchverzeichnisses ein. Alle Abfragen an diesen LDAP-Server beginnen mit diesem RDN.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server	Wählen Sie den MID-Server aus, den Sie für die Verbindung mit dem LDAP-Server verwenden möchten. Wenn Sie einen MID-Server zum Herstellen einer LDAP-Verbindung verwenden, müssen Sie den LDAP-Server nicht für externen Netzwerkverkehr freigeben. Außerdem muss kein VPN-Tunnel zwischen Ihrem LDAP-Server und eingerichtet werden ServiceNow Rechenzentren. **Hinweis:** ◦ Der MID-Server-Anwender muss über die Rolle user_admin verfügen, um LDAP-Serverkonfigurationsdatensätze lesen zu können. ◦ Folgendes ist für den MID-Server nicht verfügbar: ▪ LDAP-Authentifizierung ▪ SSL-Verbindung
Connect-Zeitüberschreitung	Wenn ein MID-Server konfiguriert ist, läuft die Verbindung unabhängig von dieser Einstellung nach 10 Sekunden ab. Diese Einstellung ist hartcodiert und kann nicht geändert werden.
Zeitüberschreitung beim Lesen	Geben Sie die Anzahl der Sekunden an, die die Integration zum Lesen von LDAP-Daten benötigt. Die Integration stoppt das Lesen von LDAP-Daten, nachdem die Verbindung die Lesezeitüberschreitung überschritten hat. Wenn Sie eine SSL-Verbindung aktivieren, können Sie auch einen Wert für die Lesezeitüberschreitung mit festlegen `com.glide.ssl.read.timeout`Systemeigenschaft. Wenn Sie sowohl für dieses Feld als auch für die Systemeigenschaft Zeitüberschreitungswerte eingeben, hat der niedrigste Zeitüberschreitungswert Vorrang.
SSL	Aktivieren Sie dieses Kontrollkästchen, damit der LDAP-Server eine SSL-verschlüsselte Verbindung herstellt. Wenn Sie einen MID-Server ausgewählt haben, ist dieses Feld nicht verfügbar. Wenn Sie eine LDAPS-Integration verwenden und der Standard-SSL-Port 636 ist, ist keine weitere Konfiguration erforderlich; SSL wird automatisch aktiviert. Wenn die LDAPS-Integration einen anderen SSL-Port verwendet, definieren Sie die alternativen SSL-Verbindungseigenschaften. **Hinweis:** Stellen Sie sicher, dass ein Netzwerkadministrator die lokale Firewall so konfiguriert, dass der Anwendungsserver auf den LDAP-Server zugreifen kann. Wenn sich der LDAP-Server in einem internen Netzwerk befindet, leitet die Firewall die IP-Adresse (oder NATs) des Anwendungsservers über die Firewall am richtigen Port weiter.
Listener	Aktivieren Sie dieses Kontrollkästchen, damit die Integration regelmäßig abfragt Microsoft Active Directory-Server oder LDAP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Server, die die Steuerung von persistenten Suchanforderungen unterstützen. Wenn Sie einen MID-Server ausgewählt haben, ist die Listener-Funktionalität für diesen MID-Server verfügbar. Weitere Informationen finden Sie unter Aktivieren Sie einen LDAP-Listener, und legen Sie Systemeigenschaften fest.
Abhörintervall (Zeitüberschreitungswert)	Geben Sie den Listener-Zeitüberschreitungswert in der Anzahl der Minuten an, die die Integration bei jeder Verbindung auf LDAP-Daten hört. Die Integration hört nicht mehr auf LDAP-Daten, nachdem die Verbindung das Abhörintervall überschritten hat.
Paging	Aktivieren Sie dieses Kontrollkästchen, damit der LDAP-Server LDAP-Attributdaten in mehrere Ergebnissätze aufteilt, anstatt mehrere Abfragen zu übermitteln.

Hinweis: Wenn Sie ein LDAP-Passwort angeben, führt die Integration einen einfachen Bindungsvorgang durch. Wenn Sie kein LDAP-Passwort angeben, muss der LDAP-Server eine anonyme Anmeldung zulassen, andernfalls kann die Integration nicht an den LDAP-Server gebunden werden.

Ergebnis

Wenn ein LDAP-Server-Datensatz auf „aktiv“ festgelegt ist, testet das System automatisch jede Verbindung, um sie zu validieren.
Validierungen umfassen:

- Der LDAP-Server ist über die angegebene URL und den angegebenen Port zugänglich
- Die LDAP-Server-URL ist ordnungsgemäß formatiert
- Die Anmeldeinformationen sind gültig

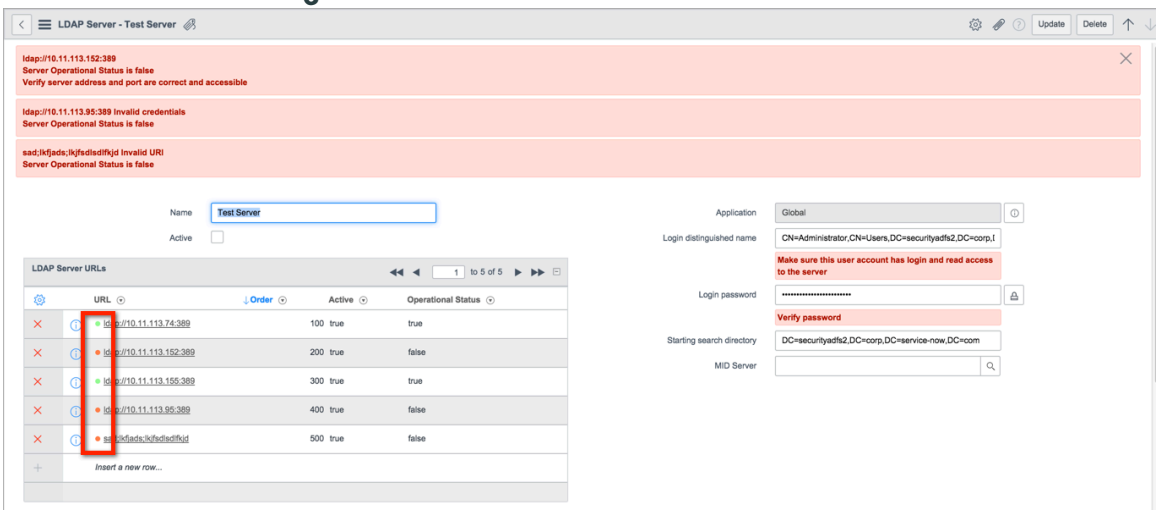
Ab dem Fuji-Release zeigt das System farbige Punkte neben jeder Server-URL an:

Symbole für LDAP-Serververbindung

Farbe	Beschreibung
Grün	Der Server, falls aktiv und funktionsfähig.
Grau	Der Server ist weder aktiv noch funktionsfähig.
Rot	Der Server ist aktiv, aber nicht funktionsfähig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Serververbindungsstatus



Aktivieren Sie einen LDAP-Listener, und legen Sie Systemeigenschaften fest

Das Aktivieren eines Listeners ist optional. Wenn diese Option aktiviert ist, benachrichtigt ein Listener das System, LDAP-Datensätze kurz nach einem Update auf dem LDAP-Server zu verarbeiten.

Vorbereitungen

Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

A *Listener* Ist ein dedizierter Prozess, der regelmäßig nach Änderungen auf dem LDAP-Server sucht.

Der Listener kann auf einem Microsoft Active Directory-Server bereitgestellt werden, der persistente Abfragen (ADNotify) unterstützt, oder auf einem LDAP-Server, der die Steuerung von persistenten Suchanforderungen unterstützt (mit OID 2.16.840.1.113730.3,4.3).

Wenn der LDAP-Server eine persistente Suche unterstützt, erkennt der LDAP-Listener alle Benutzer- und Gruppenänderungen, die an einem der entsprechenden LDAP-Accounts vorgenommen wurden, und leitet sie innerhalb von etwa 10 Sekunden an Ihre Instanz weiter. Dadurch kann die Instanz nahezu in Echtzeit die Account-Details Ihrer Anwender kopieren, ohne auf die nächste geplante Aktualisierung warten zu müssen. Der LDAP-Listener kann nur Objekte synchronisieren, die den Tabellen „Anwender“ [sys_users] und „Gruppe“ [sys_user_Group] zugeordnet sind.

Hinweis: Wenn ein Anwender über den Listener hinzugefügt wird, der Anwender jedoch die vom OU-Filter definierten Anforderungen nicht erfüllt, ignoriert die Instanz den Datensatz auf dem LDAP-Server. Wenn die Kriterien erfüllt sind, wird der Anwender der Instanz hinzugefügt.

So aktivieren Sie einen Listener:

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**an.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.
3. Wählen Sie aus **Listener** Kontrollkästchen.
4. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Das System importiert nur Anwenderdatensätze, die dem LDAP-OU-Filter entsprechen. Eingehende Anwenderdatensätze, die die Filteranforderungen nicht erfüllen, werden als ungültig gekennzeichnet und vom Import ignoriert. Administratoren können ausführliche LDAP-Protokollierung aktivieren, um festzustellen, ob eingehende Datensätze nicht mit dem LDAP-OU-Filter übereinstimmen.

5. **Wahlweise:** Navigieren Sie zur Tabelle „Systemeigenschaften“ [sys_properties], und legen Sie die Systemeigenschaften des LDAP-Listeners fest.

LDAP-Listener-Eigenschaften

Eigenschaft	Beschreibung
glide.ldap.listener.use_background_transaction	Bei „wahr“ wird der LDAP-Listener als Hintergrundtransaktion gestartet. Indem der LDAP-Listener als Hintergrundtransaktion ausgeführt wird, ka Kontingentregel „LDAP-Listener-Transaktion starten/stoppen“ die Transa abbrechen, nachdem die maximale Dauer erreicht ist (standardmäßig 5 Minuten). Dieses Verhalten verhindert, dass ein LDAP-Listener unbegren wartet. **Hinweis:** Diese Eigenschaft gilt nur für LDAP-Verbindungen, die keinen MID-Server verwenden. Verwenden `glide.ldap.listener.mid.use_background_transac` zur Steuerung des Verhaltens von LDAP-Verbindungen, die über ein MID-Server laufen. ○ Typ: Wahr | Falsch ○ Standardwert: false ○ Speicherort: zu Tabelle „Systemeigenschaften“ [sys_prope hinzufügen
glide.ldap.listener.mid.use_background_transaction	Bei „wahr“ wird der LDAP-Listener als Hintergrundtransaktion gestartet. Indem der LDAP-Listener als Hintergrundtransaktion ausgeführt wird, kann die Kontingentregel „LDAP-Listener – MID-Transaktion starten/ stoppen“ die Transaktion abbrechen, nachdem die maximale Dauer erreic ist (standardmäßig 5 Minuten). Dieses Verhalten verhindert, dass ein LDA Listener unbegrenzt wartet. **Hinweis:** Diese Eigenschaft gilt nur für LDAP-Verbindungen, die einen MID-Server verwenden. Verwenden `glide.ldap.listener.use_background_transaction` zur Steuerung des Verhaltens von LDAP-Verbindungen, die keinen M Server durchlaufen. ○ Typ: Wahr | Falsch ○ Standardwert: false ○ Speicherort: zu Tabelle „Systemeigenschaften“ [sys_prope hinzufügen
Glide.ldap.Listener.Mid.one_listener	Bei „wahr“ wird nur eine einzelne ECC-Warteschlangennachricht erstellt, den LDAP-Listener über einen MID-Server zu starten oder zu stoppen. Be

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	„falsch“ können mehrere ECC-Warteschlangennachrichten erstellt werden zur Erstellung mehrerer Threads führt, um den LDAP-Listener zu starten stoppen. ○ Typ: Wahr | Falsch ○ Standardwert: true ○ Speicherort: zu Tabelle „Systemeigenschaften“ [sys_prope hinzufügen

Geben Sie die LDAP-Attribute an

Geben Sie die Attribute an, die in LDAP-Serverabfragen enthalten sind, indem Sie den LDAP-Server verwenden **Attribute** Feld. Dies kann die Leistung und die Sicherheit verbessern.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig lädt das System alle Attribute für jedes Objekt, für das es über die Berechtigung zum Lesen von Ihrem LDAP-Server verfügt. Mit **Attribute** Feld können Sie die Attribute angeben und dadurch einschränken, die die LDAP-Abfrage zurückgibt. Die Verwendung dieses Ansatzes für große LDAP-Importe kann die Geschwindigkeit dieser Importe erheblich verbessern.

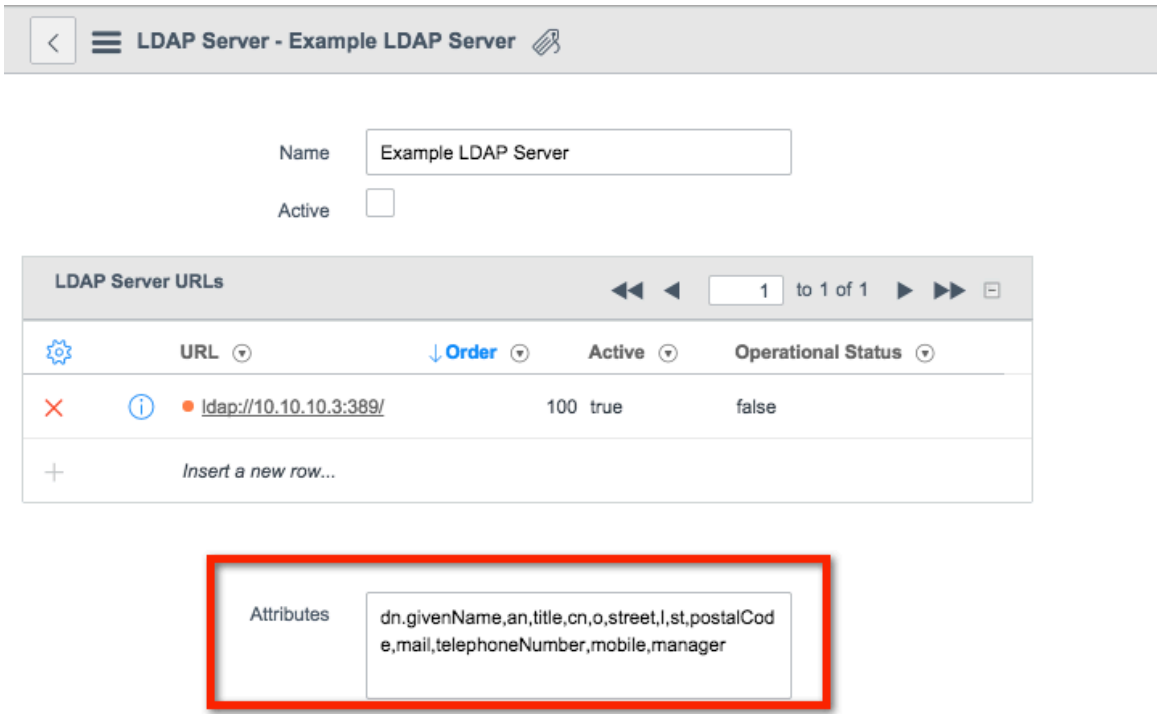
Prozedur

Definieren Sie nach Möglichkeit Attribute explizit.

Wenn Informationen vorhanden sind, die der Instanz nicht zugänglich gemacht werden sollen, schließen Sie das Attribut aus. Wenn Sie keine LDAP-Serverattribute angeben, können Anwendertransaktionen für längere Zeiträume einfrieren, wenn einem LDAP-Serverobjekt neue Attribute hinzugefügt werden, da das System damit beschäftigt ist, Daten aus den neuen Attributen zu laden.

Hinweis: Um die Manager-Suchskripts zu verwenden, die unter Transformationszuordnung für LDAP-Daten auswählen oder erstellen beschrieben werden, geben Sie an **Manager** Und **dn** (Eindeutiger Name) in **Attribute** Feld. Keines der Attribute ist erforderlich, um Teil einer Transformationszuordnung zu sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Testen Sie eine LDAP-Verbindung

Die Instanz testet die Verbindung automatisch jedes Mal, wenn ein Anwender das LDAP-Server-Formular öffnet. Alternativ können Sie die Verbindung zum LDAP-Server manuell über das LDAP-Serverformular testen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden Fehlermeldungen im LDAP-Serverformular angezeigt, wenn Probleme beim Herstellen der Verbindung mit dem LDAP-Server auftreten.

Hinweis: Mitarbeiter können auch die Konnektivität zwischen der Instanz und dem LDAP-Server überprüfen. Wenden Sie sich an den technischen Support, um Unterstützung beim Überprüfen der LDAP-Konnektivität zu erhalten

So testen Sie eine Verbindung manuell:

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**an.
2. Wählen Sie den zu testenden LDAP-Server aus.
3. Unter **Zugehörige Links** , Klicken Sie auf **Verbindung testen** .
4. Unter **Zugehörige Links** , Klicken Sie auf **Durchsuchen** Um sicherzustellen, dass die entsprechende LDAP-Verzeichnisstruktur für das System sichtbar ist.
5. **Wahlweise:** Wenn die Verbindung erfolgreich war, klicken Sie auf **Durchsuchen** Dient zum Anzeigen der LDAP-Quellverzeichnisstruktur, die für die Instanz sichtbar ist.

Hinweis: Die **Filter** Und **RDN** Felder auf der linken Seite des Fensters „Durchsuchen“ werden ignoriert, wenn Sie das Suchfeld auf der rechten Seite verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Die Instanz ändert den Betriebsstatus von LDAP-Servern abhängig vom Ergebnis des Verbindungstests.

- Wenn Ihre Instanz eine Verbindung zu einem Server herstellt, der über einen verfügt **Betriebsstatus** Wert von **Ausgefallen** , **Betriebsstatus** Wert wird automatisch in geändert **Aktiv** . Diese Funktionalität wird sowohl für automatische als auch für manuelle Verbindungstests unterstützt.
- Wenn keine Verbindung zu einem Server hergestellt werden kann, der über einen verfügt **Betriebsstatus** Wert von **Aktiv** , **Betriebsstatus** Wert wird automatisch in geändert **Ausgefallen** . Diese Funktionalität wird nur für automatische Verbindungstests unterstützt, nicht für manuelle Tests.

Definieren von LDAP-Organisationseinheiten

Eine Definition der Organisationseinheit (OU) gibt die LDAP-Quellverzeichnisse an, die für die Integration verfügbar sind.

Vorbereitungen

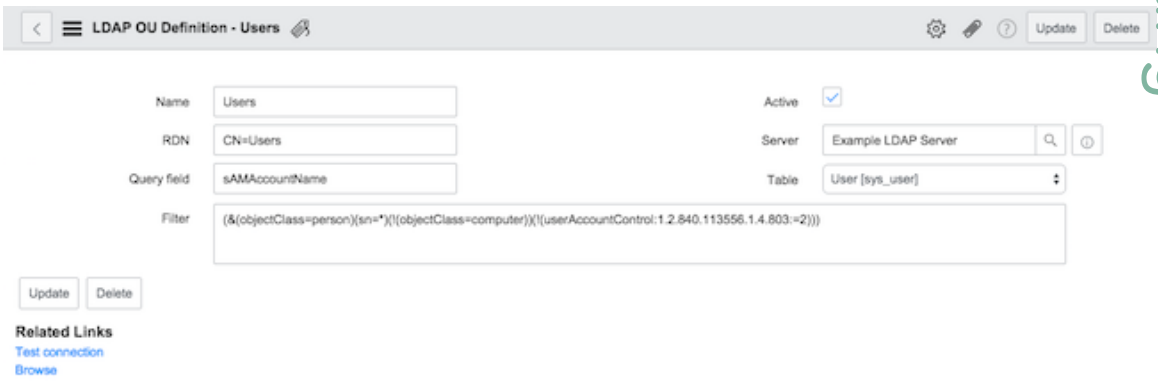
Erforderliche Rolle: admin.

Warum und wann dieser Vorgang ausgeführt wird

OE-Definitionen können Standorte, Personen oder Anwendergruppen enthalten. Jede LDAP-Serverdefinition enthält zwei Beispiel-OU-Definitionen: Eine zum Importieren von Gruppen in das System und die andere für Anwender.

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**an.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.
3. In **LDAP-OU-Definitionen** Zugehörige Liste wählen Sie entweder aus **Gruppen** Oder **Anwender** Beispiel-OU-Definition.
4. Füllen Sie das Formular „LDAP-OU-Definition“ aus (siehe Tabelle).
5. Klicken Sie auf **Aktualisieren**.
   Das System testet die Verbindung zum LDAP-Server automatisch.
6. Unter **Zugehörige Links** , Klicken Sie auf **Durchsuchen** Zum Anzeigen der LDAP-Verzeichnisdatensätze, die die OU-Definition zurückgibt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „OE-Definition“

Feld	Beschreibung
Name	Geben Sie den Namen an, den die Integration beim Verweis auf diese OE verwendet. Der hier eingegebene Name wird zu einem LDAP-Ziel im Datenquellendatensatz.
RDN	Geben Sie den relativen eindeutigen Namen des Unterverzeichnisses an, das Sie durchsuchen möchten. Dieser RDN wird mit dem Suchverzeichnis aus der LDAP-Serverdefinition kombiniert, um das Unterverzeichnis zu identifizieren, das Informationen für diese Organisationseinheit enthält. Beispielsweise verwendet die Beispiel-OU-Definition den RDN-Wert von `CN=Anwender` Zum Durchsuchen des LDAP-Verzeichnisses `CN=Anwender,DC=Service-now,DC=com` Und ein beliebiges Verzeichnis unterhalb dieses Punkts. Dieses Feld muss mit einem Unterverzeichnis in Ihrem LDAP-System übereinstimmen.
Abfragefeld	Geben Sie den Namen des Attributs auf dem LDAP-Server an, das nach Datensätzen abgefragt werden soll. Das Abfragefeld muss sowohl in einzelnen als auch in mehreren Domäneninstanzen eindeutig sein. Verwenden Sie für beste Ergebnisse E-Mail-Adressen oder andere Anmeldeinformationen, die den Anwender in einer Instanz mit mehreren Domänen eindeutig identifizieren. Active Directory verwendet **SAMAccountName** Attribut. Andere LDAP-Server verwenden tendenziell **cn** Attribut. **Hinweis:** Die **Abfragefeld** Muss dem zugeordnet werden **Anwender-ID** Feld in der Anwendertabelle [sys_user]. Beispiel: Wenn sich ein Active Directory-Anwender als anmeldet `joe.Beispiel` , Es muss ein Anwenderdatensatz mit vorhanden sein **Anwender-ID** Wert von **joe.Beispiel** Und ein LDAP-Datensatz mit **SAMAccountName** Wert von **joe.Beispiel** .
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die OU-Definition zu aktivieren und Administratoren das Testen des Datenimports zu ermöglichen. Die Integration kann jedoch nur Daten aus aktiven OU-Definitionen in das System übernehmen.
Tabelle	Geben Sie die Tabelle an, die die zugeordneten Daten von Ihrem LDAP-Server empfängt. Wählen Sie für Anwender aus **Anwender (sys_user)** , Und wählen Sie für Gruppen aus **Gruppe (sys_Group)** .
Filter	Geben Sie eine LDAP-Filterzeichenfolge ein, um bestimmte Datensätze auszuwählen, die aus der OU importiert werden sollen. Je spezifischer die LDAP-Filterabfrage ist, desto effizienter ist die Abfrage. Beispielsweise verwendet die OU-Definition „Anwender LDAP“ den folgenden Filter, um Datensätze auszuwählen, die als Person klassifiziert sind, eine haben **sn** Attributwert, sind keine Computer und sind nicht als inaktiv gekennzeichnet: `(&(objectClass=Person)(sn=*)(!(objectClass=Computer)) (!(userAccountControl:1,2.840.113556.1,4.803:=2)))` Sie können eine Beschreibung der LDAP-Filtersyntax finden, indem Sie im Internet nach suchen `LDAP-Filter-RFC` .

Example: Beispiel für Definitionen von Organisationseinheiten

Angenommen, Sie haben einen LDAP-Server mit der folgenden Verzeichnisstruktur:

dc=meine-Domäne,dc=com

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ou=Gruppen
  - cn=Entwicklung
  - cn=HR
  - cn=Vertrieb
- Ou=Anwender
  - Ou = Entwicklung
  - Ou=HR
  - Ou=Vertrieb

Angenommen, Sie möchten die HR-Gruppe und HR-Anwender aus der Anwendung ausschließen. Gehen Sie wie folgt vor:

1. Erstellen Sie einen LDAP-Serverdatensatz mit einem Startsuchverzeichnis von dc=my-Domain,dc=com.
2. Erstellen Sie einen OU-Definitionsdatensatz für ou=Gruppen mit einem Filter zum Ausschließen von cn=HR.
3. Erstellen Sie einen OU-Definitionsdatensatz für ou=Anwender mit einem Filter zum Ausschließen von ou=HR.

Wenn Sie keine zusätzlichen Attribute oder Filter mit einer OU-Definition angeben, gibt die LDAP-Abfrage die gesamte Unterstruktur aus dem Startverzeichnis und dem RDN zurück.

In diesen Beispielen hätte eine OU-Definition mit dem RDN-Wert ou=Groups und keinem Filter alle Gruppen zurückgegeben. Ebenso hätte eine OU-Definition mit dem RDN-Wert ou=Users und keinem Filter alle Anwender und untergeordneten Organisationseinheiten zurückgegeben.

Erstellen Sie eine Datenquelle für LDAP

Jede Definition der LDAP-Organisationseinheit (OU) verfügt über eine eigene zugehörige Liste von Datenquellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Beide **LDAP-Server** Und **LDAP-OU-Definition** Muss aktiv sein, damit die Testladeaktion ordnungsgemäß funktioniert. Wenn die Testlast zum ersten Mal aktiviert wird, nimmt das System bis zu 20 Datensätze ab, um die Länge der Importsatzfelder zu bestimmen. Wenn die Stichprobendatensätze keine Werte für enthalten **Anwender-ID** Feld, legt das System die Feldlänge für alle nachfolgenden Importe auf die Standardlänge von 40 fest. Durch den Import werden alle importierten Daten gekürzt, die die Länge des Tabellenfelds „Importsatz“ überschreiten. Darüber hinaus die **Anwender-ID** Feld wird auf maximal 40 Zeichen gekürzt. Beachten Sie, dass die 20 geladenen Datensätze nicht umgewandelt werden können und nur zu Testzwecken dienen. Wenn die Testdatensätze Werte für enthalten **Anwender-ID** Feld wird die Feldlänge basierend auf der Feldlänge der längsten Anwender-ID in den Testdatensätzen festgelegt.

So erstellen Sie eine neue Datenquelle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-LDAP** > **LDAP-Server**an.
2. Wählen Sie den zu konfigurierenden LDAP-Server aus.
3. In **LDAP-OU-Definitionen** Zugehörige Liste: Wählen Sie ein Element aus, z. B. **Gruppen** Oder **Anwender** .
4. In **Datenquellen** Zugehörige Liste, klicken Sie auf **Neu** .
5. Füllen Sie das Formular „Datenquelle“ aus (siehe Tabelle).
6. Klicken Sie auf **Absenden**.
7. Unter **Zugehörige Links** , Klicken Sie auf **Laden Sie 20 Datensätze Im Test** Um zu testen, ob die Datenquelle LDAP-Daten in die Importtabelle übernehmen kann.

Formular „Datenquellen“

Feld	Beschreibung
Name	Geben Sie den Namen an, den die Integration beim Verweis auf diese Datenquelle verwendet.
Tabellenname für Importsatz	Geben Sie den Namen der Bereitstellungstabelle ein, in der das System die importierten LDAP-Datensätze und -Attribute vorübergehend platziert. Überprüfen Sie diese Tabelle, um importierte LDAP-Datensätze anzuzeigen. Sie können denselben Namen der Importsatztabelle für alle LDAP-Datenquellen verwenden.
Typ	Wählen Sie Aus **LDAP** Gibt an, dass es sich bei den importierten Daten um LDAP-Daten handelt. Nachdem Sie den Typ ausgewählt haben **LDAP** , Im Formular wird angezeigt **LDAP-Ziel** Feld.
LDAP-Ziel	Wählen Sie die LDAP-OU-Definition aus, die dieser Datenquelle zugeordnet ist.

LDAP-Anwender automatisch bereitstellen

Sie stellen automatisch Anwender bereit, die sich auf dem LDAP-Server, aber noch nicht in Ihrer Instanz befinden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

Erstellen Sie die folgenden Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties]:

LDAP-Eigenschaften

LDAP-Eigenschaft	Beschreibung
glide.ldap.authentication	Aktiviert die LDAP-Authentifizierung mithilfe von LDAP zur Authentifizierung von Anwendern. Legen Sie diese Eigenschaft auf fest **Wahr** (Der Standardwert).
glide.ldap.user.autoprovision	Aktiviert LDAP, dass das System automatisch Anwender in der Anwendertabelle [sys_user] erstellt, wenn der Anwender in LDAP vorhanden ist, sich aber noch nicht in der Instanz befindet. Legen Sie diese Eigenschaft auf fest **Wahr** (Der Standardwert).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beide Eigenschaften müssen auf festgelegt werden **Wahr** Damit die automatische Bereitstellung funktioniert.

LDAP-Integration über MID-Server

Administratoren können mithilfe einer LDAP-Datenquelle über einen MID-Server (Management, Instrumentation und Discovery) integrieren.

Der MID-Server ermöglicht die Kommunikation und das Verschieben von Daten zwischen ServiceNow AI Platform Und externe Anwendungen, Datenquellen und Services. Weitere Informationen zur Installation eines MID-Servers finden Sie unter MID-Server-Installation .

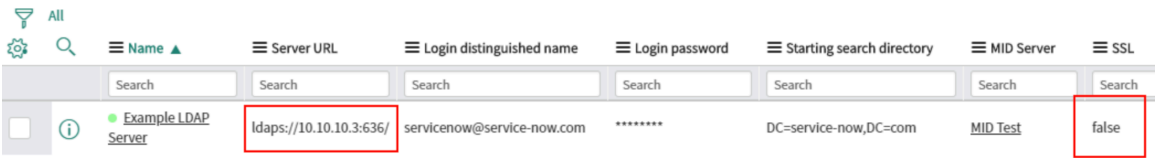
Wenn Sie einen MID-Server zum Herstellen einer LDAP-Verbindung verwenden, müssen Sie den LDAP-Server nicht für externen Netzwerkverkehr freigeben. Es ist nicht mehr erforderlich, einen VPN-Tunnel zwischen Ihrem LDAP-Server und Rechenzentren einzurichten. Der MID-Server-Anwender muss über die Rolle user_admin verfügen, um LDAP-Serverkonfigurationsdatensätze lesen zu können.

Hinweis: Der MID-Server lässt die Verwendung der UI-Aktion nicht zu `<instance>/sys_ui_action.do?sys_ID=1b4f7ef30a0001060058e223c9a5744c` Zum Aktualisieren von Anwender- und Gruppendatensätzen aus LDAP.

Eine MID-Server-Verbindung kommuniziert standardmäßig über HTTP auf Port 80. Für diesen Kommunikationskanal ist kein Zertifikat erforderlich. Die Verbindung zwischen dem MID-Server und der Instanz erfolgt über HTTPS (Port 443). Die Instanz stellt über LDAP oder LDAPS eine direkte Verbindung zum LDAP-Server her. Diese Verbindung kann entweder über das Internet oder über einen VPN-Tunnel erfolgen.

Hinweis: LDAP kann nicht über den MID-Server mit Passwortauthentifizierung kommunizieren.

Für eine sichere Kommunikation über SSL müssen Sie dies tun Fügen Sie ein SSL-Zertifikat für den MID-Server hinzu . Ändern Sie die LDAP-Server-URL von LDAP in LDAPS und ändern Sie sie in Port 636.



Hinweis: Wenn Sie einen neuen LDAP-Server erstellen, wird die SSL-Kennzeichnung des MID-Servers standardmäßig auf „falsch“ festgelegt. Sie können dieses Verhalten ignorieren.

Informationen zum Festlegen von Verbindungseigenschaften für einen bestimmten LDAP-Server finden Sie unter Definieren Sie einen LDAP-Server.

Konfigurieren Sie die LDAP-Verbindungsüberwachung

Ändern oder deaktivieren Sie die LDAP-Verbindungsüberwachung und -Benachrichtigungen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Instanz sendet automatisch eine E-Mail an Anwender, die in der Gruppe „LDAP-Administratoren“ konfiguriert sind, wenn eine LDAP-Serververbindung fehlschlägt. Dies verwendet E-Mail-Benachrichtigung, die von gestartet wird **LDAP-Verbindungstest** Geplante Aufgabe. Diese E-Mail-Benachrichtigung ist standardmäßig aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Instanz sendet die E-Mail-Benachrichtigung nur, wenn mindestens ein Mitglied in der LDAP-Administratorgruppe vorhanden ist. Stellen Sie sicher, dass Sie diese Gruppe mit den Anwendern ausfüllen, die Sie die E-Mail erhalten möchten.

Standardmäßig testet die geplante Aufgabe die Verbindung alle 15 Minuten. So ändern Sie dieses Intervall oder deaktivieren die Überwachung:

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
2. Öffnen **LDAP-Verbindungstest** .
3. Führen Sie einen der folgenden Schritte aus:
   - Ändern Sie das Intervall in **Wiederholungsintervall** Feld.
   - Deaktivieren Sie die Überwachung, indem Sie löschen **Aktiv** Kontrollkästchen.

Importieren Sie Binärdaten über einen MID-Server

Als Administrator können Sie BLOB-Daten (BLOB) mit einer LDAP-Integration über den MID-Server importieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Fügen Sie der Systemeigenschaft den Namen der LDAP-Spalte hinzu, aus der Sie Binärdaten importieren möchten `Glide.ldap.binary_attributes` .
2. Fügen Sie eine MID-Server-Eigenschaft mit dem Namen hinzu `Glide.ldap.binary_attributes` Und derselbe Wert, den Sie für die Systemeigenschaft festgelegt haben.

Fehlerbehebung bei LDAP-Integration über MID-Server

Bei der Integration von LDAP über MID-Server können Probleme in den folgenden Bereichen auftreten.

Sie können diese Probleme beheben, indem Sie die Ausgaben in der ECC-Warteschlange (External Communication Channel) (anzeigen**Discovery** > **Ausgabe und Artefakte** > **ECC-Warteschlange**) an.

Verbindungsprobleme Testen

Beim Definieren von OUs auf dem Server gibt es eine **Verbindung testen** Zugehörige Liste, die zum Überprüfen der LDAP-Verbindung verwendet wird. Wenn Sie auf diesen Link klicken, sollte in der ECC-Warteschlange eine einzelne Ausgabenachricht mit dem Themennamen angezeigt werden **LDAPConnectionTesterProbe** . Nachdem der Test auf dem MID-Server abgeschlossen wurde, sollte in der ECC-Warteschlange eine Eingabenachricht mit demselben Themennamen angezeigt werden. Wenn **Name** Spalte für die angezeigte Eingabenachricht **Wahr** , Der Test war erfolgreich. Führen Sie einen Drilldown zum Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testverbindung

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:24:17	mid.server.local_mid	LDAPConnectionTesterProbe	true	04a952038f21010036bf21ca47e79a30	input	processed	2013-07-29 13:24:19
2013-07-29 13:24:04	mid.server.local_mid	LDAPConnectionTesterProbe		04a952038f21010036bf21ca47e79a30	output	processed	2013-07-29 13:24:17

Probleme Durchsuchen

Beim Definieren von OUs auf dem Server gibt es eine **Durchsuchen** Zugehörige Liste, die zum Anzeigen der LDAP-Verzeichnisdatensätze verwendet wird, die die OU-Definition zurückgibt. Wenn Sie auf diesen Link klicken, sollte in der ECC-Warteschlange eine einzelne Ausgabenachricht mit dem Themennamen angezeigt werden **LDAPBrowseProbe** . Nachdem Daten vom MID-Server zurückgegeben wurden, sollte in der ECC-Warteschlange eine Eingabenachricht mit demselben Themennamen angezeigt werden. Wenn **Name** Spalte für die angezeigte Eingabenachricht **Wahr** , Der Test war erfolgreich. Führen Sie einen Drilldown zum Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

Importprobleme Laden

Beim Hochladen von Daten (z. B. mit der Funktion „Testladen von 20 Datensätzen“) sollte die ECC-Warteschlange eine einzelne Ausgabenachricht mit dem Themennamen anzeigen **LDAPProbe** .

Nachdem Daten vom MID-Server zurückgegeben wurden, sollte in der ECC-Warteschlange eine weitere Eingabenachricht namens angezeigt werden **LDAPProbeabgeschlossen** . Die **Name** Die Spalte für diese Eingabenachricht zeigt die Gesamtzahl der zurückgegebenen Datensätze an.

Zusätzliche Eingabenachrichten, auch genannt **LDAPProbe** , Wird angezeigt. Die **Name** Die Spalte für diese Eingabenachricht zeigt die höchste Datensatznummer im Batch an. Wenn die Gesamtzahl der zurückgegebenen Datensätze 258 beträgt und die Batchgröße 200 beträgt (Standard), werden zwei eingehende LDAPProbe-Nachrichten (200, 258) und eine eingehende LDAPProbeCompleted-Nachricht (258) empfangen.

Führen Sie einen Drilldown zum Datensatz durch, um die Nutzlast anzuzeigen und sicherzustellen, dass sie keine Fehlermeldungen enthält.

Importlast

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:09:48	mid.server.local_mid	LDAPProbeCompleted	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:48	LDAPProbeResult	LDAPProbe	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:36	mid.server.local_mid	LDAPProbe		ed0a0d7a8f32010036bf21ca47e79a56	output	processed	2013-07-29 13:09:46

Halten Sie auch nach einer Ausgabenachricht mit dem Namen Ausschau **LDAPProbeError** .

Fehlermeldung

All > Created on Today > Topic = LDAPProbeError

Created	Agent	Topic	Source	Queue	State	Processed	Error string
2014-02-20 14:52:55	mid.server.localdublinmid	LDAPProbeError	MID Server reported error: java.lang.Exc...	output	error	2014-02-20 14:53:02	No message handler for this message.

Klicken Sie auf den Link in **Name** Spalte zum Anzeigen der Details des Fehlers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Paging

LDAP-Paging funktioniert nicht, wenn die Paging-Größe auf dem LDAP-Server kleiner als 1000 ist. Legen Sie die MID-Server-Eigenschaft fest *glide.ldap.max_results*Auf einen Wert kleiner oder gleich der Paging-Größe des LDAP-Servers.

LDAP kann Binärdaten nicht importieren

Um Binärdaten über LDAP zu importieren, z. B. ein Anwenderfoto, müssen Sie das Binärattribut in die MID-Server-Eigenschaft aufnehmen *glide.ldap.binary_attributes*. Für das Anwenderfotobeispiel kann das Attribut sein `JpegPhoto` .

Daten importieren und zuordnen

LDAP-Importzuordnungen stimmen Felder in Ihrer LDAP-Datenbank mit Feldern in Ihrer Instanz überein.

Hinweis: LDAP-Zuordnung wirkt sich auf die Leistung aus, daher wird empfohlen, sie außerhalb der Spitzenzeiten zu planen oder einige Datensätze gleichzeitig zu verarbeiten, um die Systemverfügbarkeit aufrechtzuerhalten.

Definieren Sie eine Transformationszuordnung, die nur die erforderlichen oder erforderlichen Attribute importiert. Je nach Version der Instanz, die Sie verwenden, variiert die Methode zum Festlegen von LDAP-Zuordnungsbeziehungen.

Die einfachste Möglichkeit, zu wissen, ob Sie eine Version ausführen, die die System-LDAP-Anwendung für die LDAP-Integration verwendet, besteht darin, die Anwendung über den Anwendungsnavigator zu finden.

Die **Führen Sie Business-Regeln Aus** Option wird nur für die Zieltabelle angewendet. Nur Transformationszuordnungen, die der Zieltabelle zugeordnet sind, führen die Business-Regeln aus, die verschiedenen Tabellen zugeordnet sind. Wenn Sie eine Anwendergruppe aktualisieren und Business-Regeln in einer Anwendergruppentabelle ausgeführt werden, müssen für die Gruppe Rollen definiert sein.

Zuordnungsoptionen für LDAP-Import

System-LDAP-Anwendung?	Karte
Ja	Verwenden Sie einen *Transformationszuordnung* Um Ihre Zuordnung anzugeben.
Nein	Verwenden Sie ein LDAP *Legacy-Importzuordnung* Um Ihre Zuordnung oder die standardmäßige LDAP-Transformation anzugeben, die in Baseline-Instanzen enthalten ist. Denken Sie daran, den anzupassen **Zusammenfügen** Feld, das mit den richtigen Feldern abgeglichen werden soll.

Geplante Importe

Mit einem geplanten Import können Administratoren LDAP-Daten regelmäßig importieren. Standardmäßig enthält die LDAP-Integration zwei Beispiele für geplante Importe:

- Example LDAP User Import (LDAP-Anwenderimportbeispiel)
- Example LDAP Group Import (LDAP-Gruppenimportbeispiel)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Keines der Beispiele ist standardmäßig aktiv. Ändern Sie diese geplanten Importe, um die Geschäftsanforderungen Ihres Unternehmens zu erfüllen.

LDAP-Transformationszuordnungen

Die Transformationszuordnung verschiebt Daten aus der Importsatztabelle in die Zieltabelle (Anwender oder Gruppe).

Die LDAP-Integration verwendet Standard-Importsätze und Transformationszuordnungen. Sie können auch anwenderdefinierte LDAP-Transformationszuordnungen erstellen.

Wichtig: Unabhängig davon, ob Sie anwenderdefinierte LDAP-Transformationszuordnungen auswählen oder erstellen, muss eine aktive Transformationszuordnung für eine Reihe von Quell- und Zieltabellen vorhanden sein. Wenn Sie mehrere Transformationszuordnungen für dieselbe Quell- und Zieltabelle aktivieren, können doppelte Einträge in der Zieltabelle entstehen, es sei denn, Sie fügen sich mit den übereinstimmenden Feldern zusammen.

Standard-LDAP-Transformationszuordnungen

Standardmäßig stellt das System zwei Transformationszuordnungen für LDAP-Daten bereit.

Standard-LDAP-Transformationszuordnungen

Transform Map	Quelltabelle	Zieltabelle	Beschreibung
LDAP-Anwenderimport	[ldap_Import]	[sys_user]	Standardmäßige Transformationszuordnung zum Erstellen von Anwenderdatensätzen aus LDAP-Anmeldeinformationen als Teil der LDAP-Anmeldung bei Bedarf. Enthält Zuordnungen für einen Active Directory LDAP-Server.
LDAP-Gruppenimport	[ldap_Group_Import]	[sys_user_group]	Standard-Transformationszuordnung zum Erstellen von Gruppendatensätzen aus LDAP-OUs. Enthält Zuordnungen für einen Active Directory LDAP-Server.

Hinweis: Standardmäßig verfügt das System über keine Transformationszuordnung für LDAP-Abteilungsdatensätze.

Anforderungen für anwenderdefinierte LDAP-Transformationszuordnungen

Wenn Sie eine anwenderdefinierte Transformationszuordnung erstellen möchten, muss die Transformationszuordnung die folgenden Zuordnungsanforderungen erfüllen.

Anforderungen für anwenderdefinierte LDAP-Transformationszuordnungen

Quelltabelle	Quellfeld	Zieltabelle	Zielfeld	Zusammenfügen	Beschreibung
ldap_Import	u_Quelle	sys_user	Quelle	falsch	Die **u_Quelle** Feld gibt den LDAP-DN des importierten Anwenders oder der importierten Gruppe an. Das System verwendet dieses Feld, um zu bestimmen, ob ein Anwender eine LDAP-Authentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen für anwenderdefinierte LDAP-Transformationszuordnungen (Fortsetzung)

Quelltabelle	Quellfeld	Zieltabelle	Zielfeld	Zusammenfügen	Beschreibung
					benötigt, um den Manager eines Anwenders zu finden und Anwender in Gruppen einzuordnen.
ldap_Import	Wählen Sie eines der folgenden Felder aus: • u_samaccountname • u_DN • u_cn	sys_user	user_name	wahr	Wenn LDAP in Active Directory integriert ist, wählen Sie aus **u_samaccountname** Als Quellfeld. Wenn andere LDAP-Verzeichnisse verwendet werden, wählen Sie aus **u_DN** Oder **u_cn** Als Quellfeld.

Unterschiede zwischen LDAP-Transformationszuordnungen und Legacy-Importzuordnungen

Wenn Sie LDAP-Zuordnungsbeziehungen mithilfe von Transformationszuordnungen angeben, besteht ein großer Unterschied darin, wie Referenzfelder für Manager und Abteilung festgelegt werden.

Bei Verwendung von *Transformationszuordnung* , Es ist erforderlich, einen zu verwenden *Transformationsskript* Zum Erstellen von Referenzen. Dies liegt daran, dass der Wert, der einem LDAP-Attribut wie „Manager“ zugeordnet ist, der Distinguished Name (DN) des Managers ist.

Ohne zusätzliche Logik wird ein Anwenderdatensatz mit einem Managernamen erstellt, der der eindeutige Name dieses Anwenders in LDAP ist. Die Integration enthält ein Transformationsskript, um die Erstellung dieser Referenzen zu erleichtern. Die standardmäßige Transformationszuordnung „LDAP-Anwenderimport“ enthält Transformationsskripts für diese Referenzen.

Vorhandene Zuordnungsbeziehungen

Wenn Sie Legacy-Importzuordnungen aktualisieren, um Zuordnungen zu transformieren, können Sie die LDAP-Zuordnungsbeziehungen beibehalten, die vor dem Hinzufügen der System-LDAP-Anwendung vorhanden waren. Der LDAP-Server verfügt über einen **Zuordnung** Feld, das einen Verweis auf die Legacy-Importzuordnung darstellt.

Hinweis: Standardmäßig ist dieses Feld ausgeblendet, daher müssen Sie das Formular konfigurieren, um es anzuzeigen.

Wenn Sie zur Verwendung einer Transformationszuordnung wechseln möchten, löschen Sie den Verweis auf die Legacy-Importzuordnung.

Einstellungen für LDAP-Importzuordnung

Überprüfen und verwenden Sie Attribute, um die Felder einzuschränken, die die Integration aus der LDAP-Quelle importiert. Darüber hinaus ist es

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wichtig, das Feld user_Name dem LDAP-Attribut zuzuordnen, das die Anmelde-ID des Anwenders enthält. Für Active Directory ist dies normalerweise das Attribut sAMAccountName. Wenn Sie ein binäres Attribut importieren und zusammenfügen möchten (z. B. objectSid oder ObjectGUID), müssen Sie ein anwenderdefiniertes Transformationsskript erstellen.

Hinweis: Jeder Wert, der dem Feld user_Name zugeordnet ist, muss eindeutig sein.

Wenn Sie keine Transformationszuordnung angeben (z. B. LDAP-Anwenderimport), verwendet die Integration die folgenden Standardzuordnungen:

Standardzuordnung für LDAP-Import

Anwenderfeld oder Variable	LDAP-Attribut
user_name	SAMAccountName
E-Mail	mail
Telefon	Telefonnummerierung
home_phone	Festnetztelefon
mobile_phone	Mobile
first_name	Givname
last_name	sn
Titel	Titel
department	department
Manager	Manager
Zweiter_Name	Initialen
u_member	groups
u_member	Mitglieder
u_Manager	Manager

LDAP-Datentransformation

Wenn ein LDAP-Attribut einfache Daten enthält, verknüpft die Transformationszuordnung ein importiertes LDAP-Attribut mit einem entsprechenden Feld in der Zieltabelle (Anwender oder Gruppe). Beispiel: Beispieldaten im Attribut „sAMAccountName“ sind dem zugeordnet **Anwender-ID** Feld in der Anwendertabelle.

Wenn die importierten LDAP-Daten einem Referenzfeld zugeordnet sind, sucht die Instanz nach einem vorhandenen übereinstimmenden Datensatz. Wenn kein übereinstimmender Datensatz vorhanden ist, erstellt die Instanz einen neuen Datensatz für das Referenzfeld, sofern die Feldzuordnung nichts anderes angibt.

Angenommen, das LDAP-Attribut l ist dem zugeordnet **Standort** Referenzfeld in der Anwendertabelle. Immer wenn der Import einen Attributwert einführt, der keinem vorhandenen Standortdatensatzwert entspricht, erstellt die Transformationszuordnung einen neuen Standortdatensatz. Der neue Standortdatensatz hat denselben Wert wie das importierte Attribut, und der importierte Anwenderdatensatz hat jetzt einen Link zum neuen Standortdatensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt jedoch Fälle, in denen das LDAP-Attribut einen Distinguished Name (DN) zurückgibt, der im Wesentlichen ein Verweis auf einen anderen Datensatz im LDAP-Verzeichnis ist. Beispielsweise enthält das Manager-Attribut normalerweise den eindeutigen Namen für den Manager des aktuellen LDAP-Verzeichniseintrags. Ein importierter DN verwendet normalerweise eine lange Textzeichenfolge, z. B. cn=Beth Anglin,ou=Users,dc=my-Domain,dc=com.

Warnung: Stellen Sie sicher, dass Ihre Zielfelder lang genug sind, um einen DN zu enthalten. Viele Textfelder verwenden die Standardlänge 40, die für einige DN-Werte möglicherweise nicht lang genug ist. Die ServiceNow Das System kürzt jeden Wert, der die Feldlänge überschreitet.

Administratoren möchten normalerweise nicht, dass das System neue Anwender aus dem DN-Wert erstellt, da der neue Anwender nicht mit einem vorhandenen Anwender verknüpft ist. Stattdessen möchten Administratoren, dass der Import den vorhandenen Anwenderdatensatz des Managers sucht und dem neu importierten Anwender zuordnen soll. Die LDAPUtils Skripteinbindung enthält SetManager Und ProcessManager Funktionen, die einen DN analysieren und nach einem vorhandenen Anwender suchen können. Um die besten Ergebnisse zu erzielen, verwenden Sie diese Funktionen, um eine anwenderdefinierte Transformationszuordnung zu erstellen.

Zum Beispiel die LDAP-Anwenderimport Das Transformationszuordnungsskript ruft auf SetManager Funktion:

```
//
// The manager coming in from LDAP is the DN value for the manager.
// The line of code below will locate the manager that matches the
// DN value and set it into the target record.  If you are not
// interested in getting the manager from LDAP then remove or
// comment out the line below
ldapUtils. setManager (source , target ) ;
```

In einigen Fällen importiert die Integration den Datensatz eines Anwenders, bevor der Anwenderdatensatz des zugehörigen Managers importiert wird. Um solche Fälle zu bearbeiten, können Sie anrufen ProcessManager Funktion nach Abschluss der Transformation. Zum Beispiel die **LDAP-Anwenderimport** Transformationszuordnung verwendet einen OnComplete Transformationsskript zum Aufrufen von ProcessManager Funktion.

```
// It is possible that the manager for a user did not exist in the database when // the
 user was processed and therefore we could not locate and set the manager field. // The
 processManagers call below will find all those records for which a manager could  // not be
 found and attempt to locate the manager again. This happens at the end of the  // import and
 therefore all users should have been created and we should be able to  // locate the manager
 at this point
ldapUtils. processManagers ( ) ;
```

Entfernen oder kommentieren Sie SetManager Und ProcessManager Funktionsaufrufe, wenn Ihre LDAP-Integration das Manager-Attribut nicht verwendet.

LDAP-Skripting

Erstellen Sie anwenderdefinierte Transformationszuordnungen, Skripts und Business-Regeln, um Anforderungen beim Importieren von Daten anzugeben.

Anwenderdefinierte Transformationszuordnungen sollten enthalten Beim Start Und OnAfter Transformationsskripts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Beim Start Das Skript muss aufrufen LDAPUtils Skripteinbindung und Protokollierung starten. Zum Beispiel die **LDAP-Anwenderimport** Transformationszuordnung hat einen Beim Start Skript, das diesen Code verwendet:

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

Die OnAfter Das Skript muss aufrufen AddMembers Funktion. Zum Beispiel:

```
ldapUtils.addMembers (source , target ) ;
```

Legen Sie deaktivierte Active Directory-Anwender auf inaktiv fest

Verwenden Sie das folgende Skript, um Anwender automatisch zu deaktivieren, wenn der zugehörige AD-Anwender deaktiviert ist.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können deaktivierte Active Directory-Anwender identifizieren, indem Sie den Wert von überprüfen UserAccountControl Attribut. Diese Regel wird immer ausgeführt, wenn UserAccountControl Der Wert ändert und deaktiviert Anwenderaccounts, wenn dies der Fall ist **Anwender-Account-Steuerung** Kennzeichnet einen deaktivierten AD-Account.

Verwenden Sie das folgende Skript, um Anwender automatisch zu deaktivieren, wenn der zugehörige AD-Anwender deaktiviert ist.

Prozedur

1. Konfigurieren Sie das Anwenderformular, und erstellen Sie ein neues Ganzzahlfeld namens **Anwender-Account-Steuerung** .
2. Fügen Sie dem neuen Feld eine Zuordnung für userAccountControl (extern) hinzu.
3. Erstellen Sie eine neue Business-Regel mit den folgenden Eigenschaften:

Deaktivieren Sie die Business-Regel „AD-Anwender“

Business-Regel-Feld	Wert
Name	Deaktivieren Sie AD-Anwender
Tabelle	Benutzer [sys_user]
Wann	Vor
Bedingung	current.u_user_account_control.changes()

Das Feld Skript muss Folgendes enthalten:

```
var disabledFlag = 2;
//perform a bitwise comparison on userAccountControl to see if the 2 bit flag is enabled
if (current.u_user_account_control & disabledFlag) {
  gs.log('Disabling user: ' + current.user_name + 'userAccountControl=' +
 current.u_user_account_control);
  current.active='false';
  current.locked_out='true';
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weisen Sie LDAP-Feldwerte zu

Sie können ein Skript verwenden, um jedem Feld, für das eine Feldzuordnung vorhanden ist, einen Wert zuzuweisen.

Um beispielsweise dem Feld sys_user.company einen Wert zuzuweisen, erstellen Sie eine Feldzuordnung für das Feld „Unternehmen“, und fügen Sie ein Transformationsskript hinzu:

```
company = "Don's Sporting Goods";
```

Schließen Sie bestimmte LDAP-Anwender aus

Wenn Sie die LDAP-Anwenderliste nicht vollständig mithilfe von LDAP-Filtereigenschaften filtern können, können Sie Anwender mit einem Zuordnungsskript ausschließen.

Nachdem Sie die Logik ausgeführt haben, um einen Anwender zu identifizieren, der nicht importiert werden soll, legen Sie das Feld user_Name auf eine leere Zeichenfolge fest, und dieser Anwender wird nicht importiert.

```
user_name='';
```

Eine Möglichkeit, Anwender zu identifizieren, die herausgefiltert werden sollen, besteht darin, nach einer Zeichenfolge in zu suchen DistinguishedName Attribut. Dieses Skript schließt beispielsweise Accounts aus, die sich nicht in einer Anwender-OU befinden. Sie können dieses Skript verwenden, wenn Sie zu viele Anwender-OE haben, die in die LDAP-Option der Ziel-OU aufgenommen werden können.

```
//vdn is a variable mapped to distinguishedName
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
if (vdn.indexOf('OU=Users')<0) {
  user_name='';
  gs.log('LDAP Import Skipping User: ' + vdn);
}
```

Eine komplexere Methode zum Filtern besteht in der Verwendung regulärer Ausdrücke.

```
//vcn is a variable mapped to cn
//vdn is a variable mapped to distinguishedName
//c is the regular expression string
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
var vcn = source.getElement(this.cn);
var c = /^[a-z][a-z][a-z][0-9][0-9][0-9]$/;
var nvcn = vcn.toLowerCase();
//test to see if the cn is in the form of 3 letters followed by 3 numbers, only import these
if (c.test(nvcn)) {
 user_name = nvcn;
} else {
 gs.log("LDAP import rejected username: " + vcn + " for DN: " + vdn);
 user_name = "";
}
```

Legen Sie die Auswahlaktion für Referenzfeldimporte fest

Die LDAP-Transformationszuordnung bestimmt, wie Felder in der Importsatz-Tabelle Feldern in vorhandenen Tabellen wie Incident oder Anwender zugeordnet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn die LDAP-Transformationszuordnung ein Feld in der Importsatztabelle aktualisiert, erstellt die Integration automatisch einen neuen Datensatz, wenn in den LDAP-Daten ein neuer Datensatz vorhanden ist. Wenn die LDAP-Transformationszuordnung ein Referenzfeld aktualisiert, in dem Daten aus einer anderen Tabelle gespeichert werden, kann der Administrator neue LDAP-Datensätze erstellen, ignorieren oder ablehnen. Wenn die Integration beispielsweise einen neuen Abteilungsdatensatz erhält, der keiner vorhandenen Abteilung entspricht, können Sie alle anderen LDAP-Datensatzfelder aktualisieren, ohne einen neuen Abteilungsdatensatz in der Instanz zu erstellen. Mit der Transformationszuordnung können Sie die Datensatzerstellungsoptionen für jedes Referenzfeld festlegen.

Prozedur
1. Navigieren zu **Alle** > **System-LDAP** > **Transformationszuordnungen**an.
2. Wählen Sie in der zugehörigen Liste Feldzuordnungen eine der folgenden Aktionen aus **Auswahlaktion** Feld:
   - **Erstellen** – Erstellt einen neuen Referenzfelddatensatz, wenn kein übereinstimmender Datensatz vorhanden ist.
   - **Ignorieren** – Ignoriert neue Datensätze im Referenzfeld und schließt die Verarbeitung aller anderen Felder in der Transformationszuordnung ab.
   - **Ablehnen** – Stoppt die Transformation für den gesamten Datensatz.

   Hinweis: In der Feldzuordnung wird nur angezeigt **Auswahlaktion** Feld für Referenzfelder.

Überprüfen Sie die LDAP-Zuordnung
Aktualisieren Sie nach dem Erstellen einer LDAP-Transformationszuordnung die LDAP-Daten, um sicherzustellen, dass die Transformationszuordnung wie erwartet funktioniert.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur
1. Navigieren zu **Alle** > **System-LDAP** > **Geplante Lasten**an.
2. Klicken Sie auf Ihren LDAP-Importauftrag.
3. Klicken Sie auf **Jetzt ausführen**.

Fehlerbehebung bei LDAP-Integration
Wenn Sie Ihren LDAP-Server integrieren und Fragen haben, können diese Elemente Ihnen bei der Behebung des Problems helfen.

Vorläufige Prüfungen
- Wenn LDAP nicht verfügbar ist, können sich Anwender nicht bei der Instanz anmelden. Eine gute Praxis ist es, lokale Accounts für Administratoren zu haben, damit Administratoren bei ausgefallenem LDAP weiterhin auf die Instanz zugreifen können.
- Überprüfen Sie den Service-Account, um sicherzustellen, dass er nicht abgelaufen oder gesperrt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie das Format des Anwendernamens. Anstatt nur den Anwendernamen zu verwenden, versuchen Sie, die Domäne mit dem Anwendernamen oder username@Domain zu verwenden.
- Überprüfen Sie, ob Sie geändert haben System_ID Eintrag in ldap_Server_config Datensatz. Wenn Sie ändern System_ID Unbeabsichtigt mit einem Update-Satz System_ID Verweist auf den falschen Knoten für die Zielinstanz und funktioniert nicht.

Fehlercodes

Die LDAP-Protokolldatei listet Branchenstandard-Fehlercodes für LDAP und Active Directory (AD) auf. Die LDAP-Protokolldatei ist in der Wrapper-Datei enthalten. Die LDAP-Fehlercodes sind zweistellige Nummern, während die Active Directory-Fehlercodes dreistellige Zahlen sind. Eine Liste der häufigsten Fehlercodes finden Sie unter LDAP-Fehlercodes .

Integration mehrerer Domänen

Sie können mehrere Domänen innerhalb derselben Gesamtstruktur oder in vollständig nicht vertrauenswürdige Domänen integrieren. Es wird empfohlen, eine separate zu erstellen LDAP-Serverdatensatz Für jede Domäne. Jeder LDAP-Serverdatensatz muss auf einen Domänencontroller für die angegebene Domäne verweisen. Dies bedeutet, dass Sie Verbindungen zu jedem der Domänencontroller zulassen müssen. Mehrere AD-Gesamtstrukturen über LDAP mit einem LDAP-Account werden nicht unterstützt.

Wenn Sie auf mehr als eine Domäne erweitern, ist es wichtig, dass Sie eindeutige LDAP-Attribute für die Anwendungsanwendernamen identifizieren und Zusammenfügungswerte importieren. Ein gemeinsames eindeutiges Zusammenfügungsattribut für Active Directory ist ObjektSid . Eindeutige Anwendernamen variieren je nach LDAP-Datendesign. Allgemeine eindeutige Attribute sind E-Mail Oder UserPrincipalName .

Eingehende Datensätze

Siehe LDAP-Transformationszuordnungen Legt fest, wie die Integration eingehende LDAP-Datensätze verarbeitet, denen in Referenzfeldern keine übereinstimmenden Werte fehlen.

Allgemeine Authentifizierungsfehler

- Anwender kann sich nicht anmelden (ungültiger DN)
- Ungültige CN
- Ungültige Verbindung

Automatische LDAP-Verbindungstests

Sie können Verbindungen zu LDAP-Servern manuell testen oder zulassen ServiceNow Um die Verbindungen automatisch zu testen.

Das System testet die Verbindung automatisch:

- Jedes Mal, wenn ein Anwender das LDAP-Server-Formular öffnet.
- Über die geplante LDAP-Verbindungstest-Aufgabe, die standardmäßig alle 15 Minuten ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können ändern, wie oft diese geplante Aufgabe ausgeführt wird. Wenn mit dieser geplanten Aufgabe keine Verbindung hergestellt werden kann, wird der Verbindungstest nach fünf Minuten oder der Hälfte wiederholt **Wiederholungsintervall** Wert in der geplanten Aufgabe, je nachdem, was zuerst eintritt.

Fehlermeldungen werden im Formular angezeigt, wenn Probleme beim Herstellen der Verbindung mit dem LDAP-Server auftreten. Ebenfalls unterstützt werden Testverbindungen für Server hinter einem MID-Server.

Zeigen Sie den LDAP-Monitor an

Sie können aktuelle Informationen zu LDAP-Servern und -Listenern mithilfe der LDAP-Überwachung anzeigen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die verfügbaren status sind:

- Aktiv
- Inaktiv
- Fehler
- Aktiv (wird beendet...)
- Fehler (wird heruntergefahren...)

Neben dem aktuellen Status zeigt der Monitor auch Folgendes an:

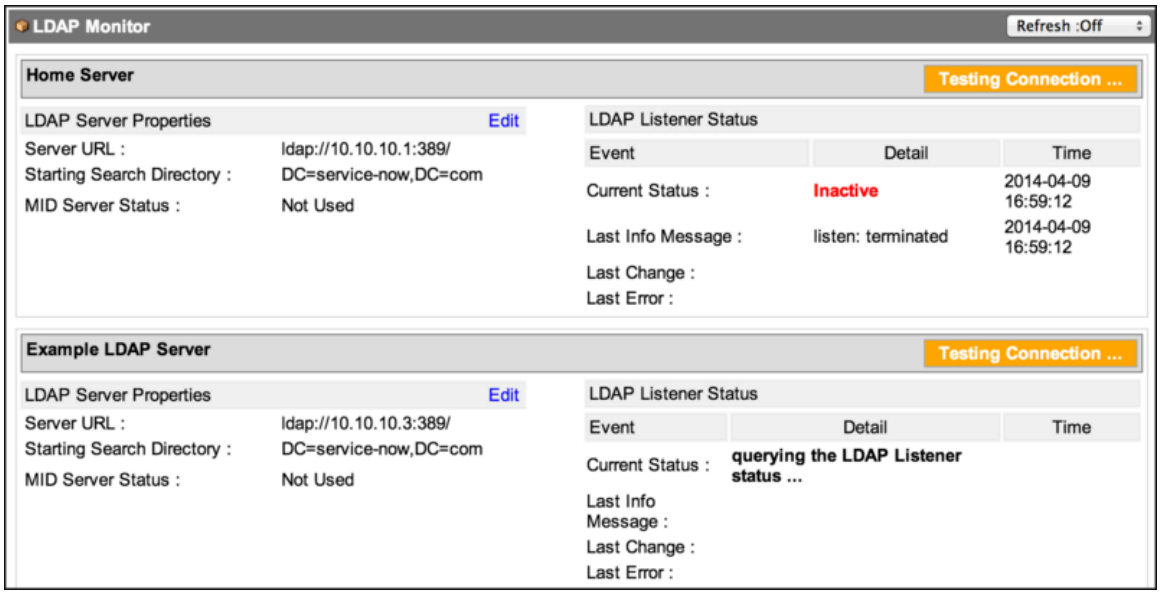
- Die letzte vom Listener erkannte Nachricht, z. B. Warten auf LDAP-Änderungen, Fehler beim Herstellen der Verbindung usw.
- Die letzte LDAP-Anwenderänderung, z. B. neuer Anwender, aktualisierter Anwender usw.
- Der letzte Fehler, der aufgetreten ist.

So zeigen Sie die LDAP-Überwachung an:

Prozedur

Navigieren zu **Alle** > **LDAP** > **System-LDAP** > **LDAP-Überwachung**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beschreibungen der Eigenschaften und Felder im Bildschirm finden Sie in der Tabelle.

LDAP-Überwachung

Feld	Beschreibung
Neu laden	Sie können die Aktualisierungsrate konfigurieren, indem Sie auf klicken **Aktualisieren** Feld in der Header-Leiste „LDAP Server Monitor“ und Auswahl der Anzahl der Sekunden zwischen jeder Datenaktualisierung. Sie können auch auswählen **Keine** Zum Unterdrücken der Aktualisierung.
Verbindungsstatus	Der Serververbindungsindikator befindet sich auf der rechten Seite über den Statusfeldern des LDAP-Listeners. Wenn der Server verbunden ist, ist das Feld grün und wird angezeigt *Verbunden* . Wenn der Server nicht verbunden ist, wird das Feld rot und angezeigt *Nicht Verbunden* . Wenn die Serververbindung getestet wird, ist das Feld gelb und wird angezeigt *Verbindung Wird Getestet* .
LDAP-Servereigenschaften	
Bearbeiten	Während Sie LDAP-Server überwachen, können Sie dies Nehmen Sie Änderungen an den Eigenschaften vor Durch Klicken **Bearbeiten** Im Bildschirm LDAP-Serverüberwachung.
Server-URL	Die Kombination aus Servername und Serverport, an dem der LDAP-Server abhört. Häufig ist der Port auf einen der folgenden Werte festgelegt: • 389: Der Standardanschluss für die Verbindung mit LDAP in Klartext • 636: Der Standardanschluss für die Verbindung mit LDAP über eine SSL-Verbindung Beispielwert: ldap://10.10.10.3:389/ Ihr LDAP-Server kann mehr als eine URL-Adresse haben. Dadurch werden NICHT mehrere Verzeichnisstrukturen eingerichtet, aus denen Sie Daten importieren können. Dies geschieht durch die Erstellung eines weiteren LDAP-Servereintrags. Es wird jedoch Redundanz geschaffen, wenn Sie mehrere LDAP-Server haben, um einen einzelnen Fehlerpunkt zu vermeiden. Die LDAP-URL-Adressen werden durch ein Leerzeichen getrennt, und das System versucht automatisch jede Serveradresse nacheinander, bis eine gültige Verbindung hergestellt werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suche im Verzeichnis wird gestartet	Das Startverzeichnis oder RDN (relative Distinguished Name), in dem das System mit der Suche nach Anwendern oder Gruppen beginnt. Beispielwert: DC=Service-now,DC=com Es sind keine Daten ÜBER diesem Punkt für den Import verfügbar. Die Instanz hat Einblick in das angegebene Verzeichnis und die DARUNTER LIEGENDEN Verzeichnisse in der LDAP-Hierarchie.
MID-Serverstatus	Der aktuelle Verbindungsstatus des MID-Servers.
Status des LDAP-Listeners	
Aktueller Status	Dies gibt an, ob der Listener aktiv ist.
Letzte Infonachricht	Dies zeigt die letzte Nachricht, die der LDAP-Server im Zusammenhang mit Anwender- und Gruppenänderungen erhalten hat, sowie die Uhrzeit des Empfangs der Nachricht.
Letzter Change	Dies zeigt die letzte Änderung am LDAP-Server und den Zeitpunkt der Durchführung.
Letzter Fehler	Dies zeigt den letzten Fehler, der auf dem LDAP-Server aufgetreten ist, und den Zeitpunkt des Auftretens.

LDAP-Fehlercodes

Die LDAP-Protokolldatei listet Branchenstandard-Fehlercodes für LDAP und Active Directory (AD) auf.

Standardfehlercodes

Standard-LDAP-Fehler

Fehler/ Datencode	Text	Beschreibung
0	LDAP_SUCCESS	Gibt an, dass der angeforderte Client-Vorgang erfolgreich abgeschlossen wurde.
2	LDAP_PROTOCOL_ERROR	Gibt an, dass der Server eine ungültige oder falsch formatierte Anforderung vom Client erhalten hat.
3	LDAP_TIMELIMIT_ÜBERSCHRITTEN	Gibt an, dass die vom Client oder Server angegebene Zeitgrenze des Vorgangs überschritten wurde. Bei Suchvorgängen werden unvollständige Ergebnisse zurückgegeben.
4	LDAP_SIZELIMIT_ÜBERSCHRITTEN	Gibt an, dass bei einem Suchvorgang die vom Client oder Server angegebene Größenbeschränkung überschritten wurde. Unvollständige Ergebnisse werden zurückgegeben.
5	LDAP_COMPARE_FALSE	Gibt keine Fehlerbedingung an. Gibt an, dass die Ergebnisse eines Vergleichsvorgangs falsch sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
6	LDAP_COMPARE_TRUE	Gibt keine Fehlerbedingung an. Gibt an, dass die Ergebnisse eines Vergleichsvorgangs „wahr“ sind.
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	Gibt an, dass der Client während eines Bindungsvorgangs eine Authentifizierungsmethode angefordert hat, die vom LDAP-Server nicht unterstützt wird.
8	LDAP_STRONG_AUTH_REQUIRED	Gibt einen der folgenden an: In Bindungsanforderungen akzeptiert der LDAP-Server nur eine starke Authentifizierung. In einer Client-Anforderung hat der Client einen Vorgang wie „Löschen“ angefordert, der eine starke Authentifizierung erfordert. In einer unverlangten Benachrichtigung über die Trennung der Verbindung erkennt der LDAP-Server, dass die Sicherheit zum Schutz der Kommunikation zwischen Client und Server unerwartet fehlgeschlagen ist oder gefährdet wurde.
9		Reserviert.
10	LDAP_REFERRAL	Gibt keine Fehlerbedingung an. In LDAPv3 gibt an, dass der Server nicht den Zieleintrag der Anforderung enthält, aber dass die Server im Feld „Referral“ dies tun können.
11	LDAP_ADMINLIMIT_EXCEEDED	Gibt an, dass ein von einer Administratorbehörde festgelegtes LDAP-Serverlimit überschritten wurde.
12	LDAP_NICHT AVAILABLE_CRITICAL_EXTENSION	Gibt an, dass der LDAP-Server eine Anforderung nicht erfüllen konnte, da mindestens eine kritische Erweiterung nicht verfügbar war. Entweder unterstützt der Server die Steuerung nicht, oder die Steuerung ist für den Vorgangstyp nicht geeignet.
13	LDAP_VERTRAULICHKEIT_ERFORDERLICH	Gibt an, dass die Sitzung nicht durch ein Protokoll wie Transport Layer Security (TLS) geschützt ist, das die Vertraulichkeit der Sitzung bietet.
14	LDAP_SASL_BIND_IN_PROGRESS	Gibt keine Fehlerbedingung an, gibt jedoch an, dass der Server für den nächsten Prozessschritt bereit ist. Der Client muss dem Server denselben SASL-Mechanismus senden, um den Prozess fortzusetzen.
15		Nicht verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
16	LDAP_NO_SUCH_ATTRIBUTE	Gibt an, dass das im Änderungs- oder Vergleichsvorgang angegebene Attribut im Eintrag nicht vorhanden ist.
17	LDAP_UNDEFINED_TYPE	Gibt an, dass das im Änderungsvorgang oder beim Hinzufügen angegebene Attribut im Schema des LDAP-Servers nicht vorhanden ist.
18	LDAP_INAPPROPRIATE_MATCHING	Gibt an, dass die im Suchfilter angegebene Übereinstimmungsregel keiner für die Syntax des Attributs definierten Regel entspricht.
19	LDAP_CONSTRAINT_VIOLATION	Gibt an, dass der in einem DN-Vorgang zum Ändern, Hinzufügen oder Ändern angegebene Attributwert gegen Einschränkungen verstößt, die für das Attribut festgelegt sind. Die Einschränkung kann eine Größe oder einen Inhalt haben (nur Zeichenfolge, kein Binär).
20	LDAP_TYPE_OR_VALUE_EXISTS	Gibt an, dass der in einem Modify- oder Add-Vorgang angegebene Attributwert bereits als Wert für dieses Attribut vorhanden ist.
21	LDAP_INVALID_SYNTAX	Gibt an, dass der in einem Add-, Compare- oder Modify-Vorgang angegebene Attributwert eine nicht erkannte oder ungültige Syntax für das Attribut ist.
22-31		Nicht verwendet.
32	LDAP_NO_SUCH_OBJECT	Gibt an, dass das Zielobjekt nicht gefunden wurde. Dieser Code wird für folgende Vorgänge nicht zurückgegeben: Suchvorgänge, die die Suchbasis finden, aber keine Einträge finden, die dem Suchfilter entsprechen. Bindungsvorgänge.
33	LDAP_ALIAS_PROBLEM	Gibt an, dass ein Fehler aufgetreten ist, wenn ein Alias zurückgestellt wurde.
34	LDAP_INVALID_DN_SYNTAX	Gibt an, dass die Syntax des DN falsch ist. (Wenn die DN-Syntax korrekt ist, die Strukturregeln des LDAP-Servers den Vorgang jedoch nicht zulassen, gibt der Server den Code 53 zurück: LDAP_UNWILLING_TO_PERFORM.)
35	LDAP_IS_LEAF	Gibt an, dass der angegebene Vorgang für einen Blatteintrag nicht ausgeführt werden kann. (Dieser Code befindet sich derzeit nicht in den LDAP-Spezifikationen, ist jedoch für diese Konstante reserviert.)
36	LDAP_ALIAS_DEREF_PROBLEM	Gibt an, dass der Client während eines Suchvorgangs entweder keine Zugriffsrechte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
		zum Lesen des Namens des Aliase-Objekts hat, oder das Aufheben der Referenzierung ist nicht zulässig.
37-47		Nicht verwendet.
48	LDAP_INAPPROPRIATE_AUTH	Gibt an, dass der Client während eines Bindungsvorgangs versucht, eine Authentifizierungsmethode zu verwenden, die der Client nicht richtig verwenden kann. Beispiel: Eine der folgenden Ursachen für diesen Fehler: Der Client gibt einfache Anmeldeinformationen zurück, wenn starke Anmeldeinformationen erforderlich sind...ODER...der Client gibt einen DN und ein Passwort für eine einfache Bindung zurück, wenn für den Eintrag kein Passwort definiert ist.
49	LDAP_INVALID_CREDENTIALS	Gibt an, dass während eines Bindungsvorgangs eine der folgenden Ereignisse aufgetreten ist: Der Client hat entweder einen falschen DN oder ein falsches Passwort übergeben, oder das Passwort ist falsch, da es abgelaufen ist, die Angriffserkennung den Account gesperrt hat, oder ein anderer ähnlicher Grund. Weitere Informationen finden Sie im Datencode.
49 / 52e	AD_INVALID-ANMELDEINFORMATIONEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Fehler an, der zurückgegeben wird, wenn der Anwendername gültig ist, die Kombination aus Passwort und Anwenderanmeldeinformationen jedoch ungültig ist. Dies ist das AD-Äquivalent des LDAP-Fehlercodes 49.
49 / 525	ANWENDER NICHT GEFUNDEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, der zurückgegeben wird, wenn der Anwendername ungültig ist.
49 / 530	NOT_ALLOWED_TO_LOGON_AT_THIS_TIME	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, der einen Anmeldefehler darstellt, der verursacht wurde, da der Anwender sich derzeit nicht anmelden darf. Gibt nur zurück, wenn ein gültiger Anwendername und gültige Passwortanmeldeinformationen angezeigt werden.
49 / 531	RESTRICTED_TO_SPECIFIC_MACHINES	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, der einen Anmeldefehler darstellt, der verursacht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
		wurde, da der Anwender sich nicht von diesem Computer aus anmelden darf. Gibt nur zurück, wenn ein gültiger Anwendername und gültige Passwortanmeldeinformationen angezeigt werden.
49 / 532	PASSWORD_EXPIRED	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, bei dem es sich um einen Anmeldefehler handelt. Das angegebene Account-Passwort ist abgelaufen. Gibt nur zurück, wenn gültige Anmeldeinformationen für Anwendername und Passwort vorhanden sind.
49 / 533	ACCOUNT_DISABLED	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, bei dem es sich um einen Anmeldefehler handelt. Der Account ist derzeit deaktiviert. Gibt nur zurück, wenn gültige Anmeldeinformationen für Anwendername und Passwort vorhanden sind.
49 / 568	ERROR_TOO_MANY_CONTEXT_IDS	Gibt an, dass während eines Anmeldeversuchs der Sicherheitskontext des Anwenders zu viele Sicherheits-IDs angesammelt hat. Dies ist ein Problem mit dem spezifischen LDAP-Anwenderobjekt/Account, das vom LDAP-Administrator untersucht werden sollte.
49 / 701	ACCOUNT_EXPIRED	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an, bei dem es sich um einen Anmeldefehler handelt. Der Account des Anwenders ist abgelaufen. Gibt nur zurück, wenn gültige Anmeldeinformationen für Anwendername und Passwort vorhanden sind.
49 / 773	ANWENDER MUSS PASSWORT ZURÜCKSETZEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Datenfehler an. Das Passwort des Anwenders muss vor der ersten Anmeldung geändert werden. Gibt nur zurück, wenn gültige Anmeldeinformationen für Anwendername und Passwort vorhanden sind.
50	LDAP_INSUFFICIENT_ACCESS	Gibt an, dass der Anrufer nicht über ausreichende Rechte verfügt, um den angeforderten Vorgang auszuführen.
51	LDAP_BUSY	Gibt an, dass der LDAP-Server zu beschäftigt ist, um die Clientanforderung zu verarbeiten. Wenn der Client jedoch wartet und die Anforderung erneut übermittelt, kann der Server sie dann möglicherweise verarbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
52	LDAP_NICHT VERFÜGBAR	Gibt an, dass der LDAP-Server die Bindungsanforderung des Clients nicht verarbeiten kann, normalerweise weil er heruntergefahren wird.
52e	AD_INVALID-ANMELDEINFORMATIONEN	Gibt einen Active Directory (AD) AcceptSecurityContext-Fehler an, der zurückgegeben wird, wenn der Anwendername gültig ist, die Kombination aus Passwort und Anwenderanmeldeinformationen jedoch ungültig ist. Dies ist das AD-Äquivalent des LDAP-Fehlercodes 49: LDAP_INVALID_CREDENTIALS.
53	LDAP_UNWILLENS_TO_PERFORMING	Gibt an, dass der LDAP-Server die Anforderung aufgrund von serverdefinierten Einschränkungen nicht verarbeiten kann. Dieser Fehler wird aus den folgenden Gründen zurückgegeben: Die Anforderung zum Hinzufügen von Einträgen verstößt gegen die Strukturregeln des Servers...ODER...die Anforderung zum Ändern von Attributen gibt Attribute an, die Anwender nicht ändern können...ODER...Passwortbeschränkungen verhindern die Aktion...ODER...Verbindungsbeschränkungen verhindern die Aktion.
54	LDAP_LOOP_DETECT	Gibt an, dass der Client einen Alias oder eine Referral-Schleife erkannt hat und diese Anforderung daher nicht abschließen kann.
55-63		Nicht verwendet.
64	LDAP_NAMING_VIOLATION	Gibt an, dass der Vorgang „DN hinzufügen oder ändern“ gegen die Strukturregeln des Schemas verstößt. Beispielsweise platziert die Anforderung den Eintrag einem Alias untergeordnet. Die Anforderung platziert den Eintrag einem Container untergeordnet, der durch die Containment-Regeln verboten ist. Der RDN für den Eintrag verwendet einen unzulässigen Attributtyp.
65	LDAP_OBJECT_CLASS_VIOLATION	Gibt an, dass der Vorgang „DN hinzufügen, ändern oder ändern“ gegen die Objektklassen-Regeln für den Eintrag verstößt. Beispielsweise geben die folgenden Anforderungstypen diesen Fehler zurück: Der Vorgang „Hinzufügen“ oder „Ändern“ versucht, einen Eintrag ohne Wert für ein erforderliches Attribut

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-LDAP-Fehler (Fortsetzung)

Fehler/ Datencode	Text	Beschreibung
		hinzuzufügen. Der Vorgang „Hinzufügen“ oder „Ändern“ versucht, einen Eintrag mit einem Wert für ein Attribut hinzuzufügen, das die Klassendefinition nicht enthält. Der Änderungsvorgang versucht, ein erforderliches Attribut zu entfernen, ohne die zusätzliche Klasse zu entfernen, die das Attribut als erforderlich definiert.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	Gibt an, dass der angeforderte Vorgang nur für Blatteinträge zulässig ist. Beispielsweise geben die folgenden Anforderungstypen diesen Fehler zurück: Der Client fordert einen Löschvorgang für einen übergeordneten Eintrag an. Der Client fordert einen DN-Änderungsvorgang für einen übergeordneten Eintrag an.
67	LDAP_NOT_ALLOWED_ON_RDN	Gibt an, dass der Änderungsvorgang versucht hat, einen Attributwert zu entfernen, der den relativen eindeutigen Namen des Eintrags bildet.
68	LDAP_BEREITS_VORHANDEN	Gibt an, dass beim Hinzufügen-Vorgang versucht wurde, einen bereits vorhandenen Eintrag hinzuzufügen, oder dass beim Änderungsvorgang versucht wurde, einen Eintrag in den Namen eines bereits vorhandenen Eintrags umzubenennen.
69	LDAP_NO_OBJECT_CLASS_MODS	Gibt an, dass der Änderungsvorgang versucht hat, die Strukturregeln einer Objektklasse zu ändern.
70	LDAP_RESULTS_TOO_LARGE	Reserviert für CLDAP.
71	LDAP_AFFECTS_MULTIPLE_DSAS	Gibt an, dass der Vorgang „DN ändern“ den Eintrag von einem LDAP-Server auf einen anderen verschiebt und mehr als einen LDAP-Server erfordert.
72-79		Nicht verwendet.
80	LDAP_OTHER	Gibt eine unbekannte Fehlerbedingung an. Dies ist der Standardwert für NDS-Fehlercodes, die nicht anderen LDAP-Fehlercodes zugeordnet sind.
775	USER_ACCOUNT_LOCKED	Gibt an, dass Anwender sich nicht anmelden können, da der Anwenderaccount gesperrt ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderdefinierte Fehlercodes

Anwenderdefinierte LDAP-Fehlercodes

Fehler/Datencode	Text
10000	LDAP_ERROR_GENEREL
10001	LDAP_ERROR_MAL_FORMED_URL
10002	LDAP_ERROR_UNAUTHENTICATED_BIND
10300	LDAP_ERROR_COMMUNICATION_EXCEPTION
10301	LDAP_ERROR_SOCKET_TIMEOUT
10302	LDAP_ERROR_CONNECTION_REJECTED
10303	LDAP_ERROR_CONNECTION_RESET
10304	LDAP_ERROR_NO_ROUTE
10305	LDAP_ERROR_UNKNOW_HOST
10400	LDAP_ERROR_SSL_EXCEPTION
10401	LDAP_ERROR_SSL_EMPTY_CERT_STORE
10402	LDAP_ERROR_SSL_CERT_NOT_FOUND
10403	LDAP_ERROR_SSL_CERT_EXPIRED
10500	LDAP_ERROR_INVALID_SEARCH_FILTER_EXCEPTION

Senden Sie ein einmaliges Passwort, wenn der LDAP-Server ausgefallen ist

Eine LDAP-Eigenschaft ist verfügbar, um ein einmaliges Passwort an einen Anwender zu senden, wenn sich der Anwender nicht anmelden kann, da der LDAP-Server ausgefallen ist. Sie können auch eine andere Eigenschaft konfigurieren, um zu steuern, wie lange das Passwort gültig ist.

Vorbereitungen

Erforderliche Rolle: Administrator

Um ein einmaliges Passwort zu erhalten, müssen dem Anwender Benachrichtigungen in seinem Anwenderprofil aktiviert sein. Die Benachrichtigung ist nur eine E-Mail-Nachricht. SMS-Nachrichten werden nicht unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Beide Eigenschaften sind standardmäßig aktiviert. Der Standardwert für die Eigenschaft, die die Passwortgültigkeit steuert, beträgt 10 Minuten.

Prozedur

1. Öffnen Sie die Liste der Systemeigenschaften, indem Sie eingeben `sys_properties.list` Im Filter des Anwendungsnavigators.
2. Suchen Sie nach *`glide.ldap.onetime.password.enabled`*Eigenschaft.
3. Legen Sie die Eigenschaft auf fest `Wahr` .
4. Um die Passwortgültigkeitszeit für einen Anwender zu ändern, legen Sie die folgende Eigenschaft auf eine ganze Anzahl von Minuten fest: *`glide.authenticate.onetime.password.validity`*.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LDAP-Datensatzsynchronisierung

Administratoren können inaktive, deaktivierte oder gelöschte LDAP-Datensätze mit ihren LDAP-Datensätzen synchronisieren.

Bei der LDAP-Datensatzsynchronisierung werden inaktive Datensätze auf dem LDAP-Server erkannt und die entsprechenden LDAP-Datensätze aktualisiert. Die Erkennung inaktiver LDAP-Datensätze umfasst die Definition konsistenter Datenindikatoren für jedes Anwenderobjekt, den Import von LDAP-Daten und die Auswertung der Datenindikatoren.

Ein Datenindikator kann sein:

- Ein Datumsfeld
- Mitgliedschaft in einer bestimmten OE (Identifizieren Sie durch Analysieren von *dn*Attribut), mit *useraccountcontrol*Attribut
- Eine Kombination dieser Indikatoren

Importierte Daten gelangen über Importsatztabellen in die Instanz, in denen die Daten ausgewertet und verarbeitet werden können.

Der Importprozess kann verwenden LDAP-Aktualisierungsfilter Bei mehreren Importaufträgen zur Aufteilung verschiedener Arten von Anwenderdatensätzen und zur separaten Verarbeitung von Datensätzen.

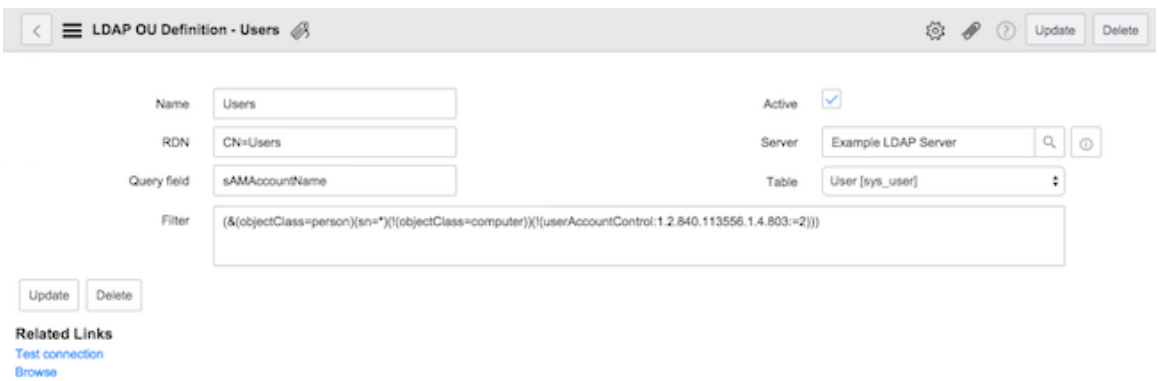
LDAP-Aktualisierungsfilter

Filter für den LDAP-Aktualisierungsprozess können verwendet werden, um die Verarbeitung anzugeben, bei der Einfügungen deaktivierter Anwender ignoriert werden.

Sie können den LDAP-OU-Filter lösen, um alle Daten in Ihre Importsatztabelle (einschließlich inaktiver Anwender) aufzunehmen, und dann eine Verarbeitung angeben, bei der das Einfügen deaktivierter Anwender ignoriert wird. Die Beispiel-OU-Definition „Anwender“, die die Instanz in ihrem sofort einsatzbereiten LDAP-Beispiel bereitstellt, enthält einen Filter.

Dieser Filter ist wichtig, da er definiert, welche Anwenderdatensätze in die zu bewertende Importsatztabelle aufgenommen werden. Eine Einschränkung dieses Filters besteht zwar darin, dass inaktive Anwender herausgefiltert werden, sodass die inaktiven Anwenderdatensätze nicht in die temporären Tabellen des Importsatzes importiert werden. Da die inaktiven Anwenderdatensätze nicht sichtbar sind, können die Datensatzindikatoren nicht bewertet werden.

LDAP-OU-Filter



Um die Filterung innerhalb des Haupt-LDAP-Aktualisierungsprozesses zu verwenden, ändern Sie den Filter so, dass alle Anwenderdatensätze berücksichtigt werden. Das

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis ist, dass alle Datensätze in die temporäre Tabelle des Importsatzes geladen werden, wo sie ausgewertet und umgewandelt werden können.

Hinweis: Hier gibt es eine Vorsichtsmaßnahme: Da die Filterung alle Datensätze einbezieht, können Sie eine große Anzahl älterer inaktiver LDAP-Accounts haben, die nicht in die Instanz eingefügt werden sollten. Für einen deaktivierten Anwender darf niemals ein Anwenderdatensatz erstellt werden.

LDAP-Extraktion

Ein LDAP-Extraktionsprozess kann implementiert werden, um deaktivierte Anwender zu erkennen.

Ein Extrakt aus Ihrer LDAP-Quelle kann mithilfe einer aktiven Kennzeichnung, die für jeden Datensatz im Import auf „falsch“ festgelegt werden kann, nach deaktivierten Anwendern gefiltert werden. Geben Sie („target.Active=false“) an, und kopieren Sie sie in **Skript** Feld direkt im Datensatz der Tabellentransformationszuordnung.

Vorteile

Zu den Vorteilen dieser Methode gehören:

- Einfaches Skripting
- Vorhandene Anwenderdatensätze sind nicht an der Verarbeitung beteiligt
- Inaktive Anwender werden nicht in eine temporäre Importtabelle geladen
- Keine Auswirkung auf die Leistung

Nachteile

Zu den Nachteilen dieser Methode gehören:

- Ein zusätzlicher Prozess wird erstellt
- Der Extraktsatz muss an einem Ort platziert werden, an dem Ihre Datenquelle darauf zugreifen kann

Alternative Methode

LDAP-Aktualisierungsfilter Verwenden Sie mehrere Importaufträge, um verschiedene Arten von Anwenderdatensätzen aufzuteilen und Datensätze für eine separate Verarbeitung zu trennen.

Inaktive LDAP-Anwenderaccounts

Erkennen Sie, dass ein vorhandener, aktueller Anwenderaccount inaktiv ist oder deaktiviert oder aus einem Active Directory (AD) LDAP gelöscht wurde.

Ein häufiges LDAP-Integrationsproblem besteht darin, deaktivierte oder gelöschte Anwender in einem Active Directory (AD) zu erkennen und dann in der Instanz zu deaktivieren. In einem Active Directory-LDAP ist normalerweise ein Filter so festgelegt, dass inaktive Anwender beim Aktualisieren ausgeschlossen werden. Die Instanz erkennt also keine Anwender, die in AD deaktiviert oder gelöscht wurden. Das Problem besteht darin, zu erkennen, dass ein vorhandener, aktueller Anwender inaktiv ist oder aus AD gelöscht wurde.

Weitere Informationen zum Suchen inaktiver Accounts finden Sie unter Suchen Sie inaktive LDAP-Accounts mithilfe des Felds userAccountControl .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der empfohlene Ansatz ist bis *Deaktivieren* Anwenderdatensätze und alle anderen Arten von Datensätzen, nicht löschen. Jeder Datensatz ist mit anderen Datensätzen verknüpft, und durch das Löschen eines Datensatzes werden alle Beziehungen zu diesen anderen Datensätzen zerstört. Durch das Deaktivieren von Datensätzen werden diese Beziehungen aufrechterhalten.

Suchen Sie inaktive LDAP-Accounts mithilfe des Felds userAccountControl

Identifizieren Sie, wann ein Active Directory-Anwender (AD) gelöscht (oder deaktiviert) wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Eine Methode besteht darin, den aktiven Status von AD-Anwendern nachzuverfolgen und eine Business-Regel zu erstellen, um entsprechende Accounts zu aktualisieren, wenn ein AD-Account inaktiv ist.

Prozedur

1. Erstellen Sie ein neues Zeichenfolgenfeld in der Anwendertabelle [sys_user], um den Wert des AD nachzuverfolgen **UserAccountControl** Feld.
   Beispiel: `u_ad_user_Account` .
2. Erstellen Sie ein LDAP-Transformationsskript, um den Feldwert festzulegen.

   Example

   ```
   target.u_ad_user_account = source.userAccountControl
   ```

3. Aktualisieren Sie den LDAP-Filter, um deaktivierte AD-Accounts anzuzeigen.

   Example
   Hier ist ein Beispiel für einen Filter.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer))(!
   (userAccountControl:1.2.840.113556.1.4.803:=2)))
   ```

   Hier ist ein Beispiel für einen Ersatzfilter, den Sie verwenden können.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer)))
   ```

4. Erstellen Sie eine onChange-Geschäftsregel, um das aktive Feld auf „falsch“ festzulegen, wenn das Feld u_ad_user_Account den Wert 514 hat.
   „514“ gibt einen inaktiven Account an.

LDAP-Skriptbeispiele

Die folgenden Skriptbeispiele gehen davon aus, dass Sie ein Active Directory (AD) für Ihren LDAP-Server verwenden.

Skript „userAccountControl-Attributwerte“
Dieses Beispiel testet die Quelle für die userAccountControl-Attributwerte, die einem deaktivierten Anwender zugeordnet sind (514 oder 546).

```
//Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol == '546'){
  target.active=false;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  target.locked_out=true;
}
```

Hier ist ein Beispiel mit einer bitweisen Prüfung:

```
if(source.u_useraccountcontrol & 2){
  active = false;
}
```

UserAccountControl-Attributskript

In diesem Beispiel wird das Attribut userAccountControl untersucht, aber nicht auf bestimmte Werte getestet. Es enthält auch die Option zum erneuten Aktivieren von LDAP-Anwenderaccounts.

```
/*
* Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
* Convert the userAccountControl attribute back to a hex value
*/
var ctrl = parseInt(source.u_useraccountcontrol, 10);
ctrl = ctrl.toString(16);

/*
* The only digit we care about is the final one
* A final hex digit value of '2' in 'ctrl' means disabled
*/
if(ctrl.substr(-1) == "2"){

  //Deactivate and lock the user account
  target.active = false;
  target.locked_out = true;

  //Ignore any insert of a disabled record
  if(action == 'insert'){
    ignore = true;
  }
}
/* Optional: Uncomment else block to reactivate and unlock the user account
else {
  target.active = true;
  target.locked_out = ctrl.substr(-2, 1) == "1";
}
*/
```

OnBefore-Transformationszuordnungsskript

Hier ist ein Beispiel für ein onBefore-Transformationszuordnungsskript. Das Skript identifiziert deaktivierte Datensätze und Datensätze, die eingefügt werden. Wenn ein deaktivierter Anwender eingefügt wird, ignoriert die Vorgangstransformation den Datensatz.

```
//Ignore any insert of a disabled record as defined by the 'userAccountControl' attribute
var uc = source.u_useraccountcontrol;
if((uc == '514' || uc == '546') && action == 'insert'){
  ignore = true;
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DN-Mitgliedsskript

Dieses Skriptbeispiel führt Flexibilität ein, indem es sich nicht auf die Werte 546 und 514 userAccountControl stützt, sondern stattdessen überprüft, ob der Anwender Mitglied eines bestimmten Distinguished Name (DN) ist. Sie können dieses Skript entweder in verwenden **Skript** Feld des Datensatzes „Tabelle-Transformationszuordnung“ oder in einem onBefore-Transformationszuordnungsskript.

```
//Deactivate LDAP-disabled users during transform based on OU membership in 'dn'
if(source.u_dn.indexOf('OU=Disabled Accounts') > -1){
  target.active = false;
  target.locked_out = true;
}
```

Active Directory-Anwendungsmodus (ADAM)

Active Directory Application Mode (ADAM) ist ein LDAP-konformer Verzeichnisservice (Lightweight Directory Access Protocol).

Hinweis: Eine grundlegende Ebene des Verständnisses mit Microsoft Windows Server und Active Directory sind erforderlich, um dieses Thema zu verstehen. Sie müssen auch über Administratorberechtigungen auf dem Server verfügen, den Sie für ADAM konfigurieren.

Dies sind Beispielverfahren. Aufgrund von Installations- und Umgebungsvariationen können wir keinen direkten Support anbieten. Wir empfehlen, mit zu arbeiten Microsoft Berater.

ADAM verfügt über eine einfache Installation und wird als Service auf ausgeführt Windows Betriebssysteme. Es kann vollständig angepasst und als Anwendungskomponente verteilt oder als eigenständiges LDAP-Verzeichnis verwendet werden. ADAM verwendet die gleichen Technologien wie Active Directory-Domänencontroller (einschließlich Replikations- und Delegierungsfunktionen) und verfügt über eigene Verwaltungs- und Anpassungsfunktionen. Kann als ausgeführt werden Windows Service. ADAM kann auf installiert werden Windows Betriebssysteme XP, 2000, 2003 und 2008. ADAM ist Teil von enthalten Windows Server 2003 R2 und Windows Server 2008. Ein Download ist unter verfügbar http://www.microsoft.com/downloads http://www.microsoft.com/downloads für frühere Betriebssysteme.

Sicherheit

Einige Sicherheitsrichtlinien des Unternehmens verbieten externen Lieferanten und Partnern, eine direkte Verbindung zu einem Active Directory (AD)-Domänencontroller herzustellen. Wenn die Offenlegung bestimmter AD-Objekte oder -Attribute für einen externen Lieferanten oder Partner untersagt ist, kann der Zugriff auf Objekte und Attribute mithilfe von AD Security Access Control-Einträgen (ACE oder ACL) blockiert werden. Je nach Sicherheitsanforderungen kann diese Methode Komplexität in der Integration verursachen. Es wird empfohlen, mehrere Domänen und Gesamtstrukturen zu konsolidieren. Wenn alle LDAP-Importe und -Authentifizierungen über eine einzige Quelle kanalisiert werden müssen, kann ADAM als konsolidierte Quelle verwendet werden. Mit Release von Windows2008 diese Funktionalität wurde in Light-Weight-Directory Service, LDS umbenannt. Installation und Konfiguration ähneln Windows Server 2003 R2.

Empfohlenes Wissen

Für diese Aufgabe müssen Sie AD, Objektklassen und Attribute verstehen. Um eine erfolgreiche Integration zu erzielen, müssen Sie über die aktuelle AD-Objektstruktur informiert sein, mit Active Directory-Delegierungen vertraut sein und eine Strategie für die Verwendung VON ADAM und für welche Zwecke haben. Wenn Sie mit AD oder ADAM nicht vertraut sind, konfigurieren Sie mit Ihrem AD-Administrator eine neue ADAM-Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Treuhänder

Wenn `UserProxy` Objekte werden verwendet. Der Computer, der ADAM hostet, muss Mitglied der Domäne sein, die über die AD-Accounts verfügt, oder Mitglied einer vertrauenswürdigen Domäne.

Interne Konnektivität

Wenn `UserProxy` Objekte werden verwendet. Der ADAM-Computer muss eine Verbindung zu den zugehörigen Domänencontrollern herstellen können, um die Proxy-Authentifizierung durchzuführen.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Konfigurieren einer Instanz mit ADAM

Bei der ersten Installation werden die ADAM-Dateien auf Ihren Computer kopiert, erfordert Komponenten registriert und die Anwendungsverknüpfungen erstellt.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden alle Anwendungsdateien in installiert %Systemroot%\ADAM .

- Windows Server 2003 R2: ADAM kann mit installiert werden **Systemsteuerung > Programme hinzufügen und entfernen > Manager für optionale Komponenten**an.
- Windows Server 2000 Und Windows XP: Heruntergeladen http://www.microsoft.com/downloads Von Microsoft.

Erstellen Sie den ersten Instanzservice, der als erster von ADAM gehosteter Verzeichnisservice fungiert. Führen Sie einen der folgenden Schritte aus:

Prozedur

- Ausführen `adaminstall.exe` Aus dem ADAM-Ordner.
- Verwenden Sie **Erstellen Sie eine ADAM-Instanz** Verknüpfung von **Startmenü > Programme > ADAM** Ordner.

1. Wählen Sie aus **Eine eindeutige Instanz** Installationsoption.

   Hinweis: Sie können diese Option verwenden, um ein Instanzreplikat auf einem zweiten Server zu installieren, um ein fehlertolerantes System bereitzustellen.

2. Füllen Sie die Felder aus.

ADAM-Instanz

Feld	Beschreibung
Instanzname	Wird hauptsächlich verwendet, um zu identifizieren Windows Servicename und Anzeigename
Ports	Legt die Portnummern fest, die für LDAP- und LDAPS-Listener verwendet werden sollen. Der Standard-LDAP-Port ist 389, LDAPS

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ist 636. Wenn diese Ports auf dem Server verwendet werden, wählt der Setup-Assistent neue Ports aus. Arbeiten Sie mit Ihrem Netzwerkadministrator zusammen, um die besten Ports für die Verwendung zu ermitteln
Anwendungsverzeichnispartition	Erstellt eine Anwendungsverzeichnispartition. In diesem Schritt nicht erforderlich, empfehlen wir, die neue Partition jetzt zu erstellen. Eine gute Praxis besteht darin, denselben eindeutigen Namen wie Ihre Gesamtstruktur oder Domäne zu verwenden, aber die Domäne der höchsten Ebene durch adam anstelle von com oder local zu ersetzen. Beispiel: Wenn Ihre Gesamtstrukturpartition lautet *dc=myCompany,dc=com*, Sie könnten die ADAM-Partition als erstellen *dc=myCompany,dc=adam*
Dateispeicherorte	Wählt die Speicherorte für die ADAM-Partitionsdaten aus.
Service-Account-Auswahl	Wählt einen Service-Account aus, als den die Instanz ausgeführt wird. Für eigenständige Services können Sie den standardmäßigen Netzwerkservice-Account verwenden. Wenn Sie Replikate verwenden möchten, müssen Sie einen Account verwenden, der Zugriff auf alle ADAM-Instanzen hat.
ADAM-Administratoren	Die Delegierung im ADAM-Verzeichnis, die die integrierte Windows-Authentifizierung nutzt. So wird der anfängliche Zugriff für die Administration gewährt. Sobald dem ursprünglichen Account Rechte gewährt wurden, delegiert dieser Anwender oder diese Gruppe Rechte an andere Windows-Anwender oder ADAM-Anwender. Sie können den Standard auswählen, um nur dem aktuellen Anwender Administratorzugriff zu gewähren, oder einem anderen Anwender oder einer anderen Gruppe basierend auf Ihren Anforderungen Zugriff zu gewähren.
Importieren Sie LDIF-Dateien	Die zu importierenden Dateien. Ms-UserProxy ist die wichtigste zu importierende Datei, aber es lohnt sich, alle verfügbaren Dateien hinzuzufügen, da das Schema wenig Overhead verursacht und Sie sich keine Gedanken darüber machen müssen, es später zu erweitern, wenn Ihre Anforderungen erweitert werden. Bestätigen Sie die Details, und schließen Sie die Konfiguration ab.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Richten Sie die ADAM-Konsole ein

Richten Sie die ADAM-Konsole ein. Auch wenn es viele Ähnlichkeiten zwischen ADAM und Active Directory gibt, kann die Verwaltung sehr unterschiedlich sein, da es keine gibt **Anwender und Computer** Verwaltungskonsole.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der Großteil der allgemeinen Administration wird mit der ADAM ADSI MMC-Konsole ausgeführt, die über verfügbar ist **ADAM** Startmenü. Wenn Sie die ADAM ADSI-Konsole zum ersten Mal ausführen, müssen Sie eine Verbindung zu der von Ihnen erstellten Partition herstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie mit der rechten Maustaste auf **ADAM-ADSI-Bearbeitung** Element im linken Rahmen.
2. Geben Sie der neuen Verbindung einen Namen, und aktualisieren Sie die Felder „Servername“ und „Port“ mit den Informationen, die Sie beim Erstellen der Instanz verwendet haben.
3. Wählen Sie Aus **Eindeutiger Name** Oder **Benennungskontext** Und geben Sie den eindeutigen Namen der Anwendungspartition an, die Sie zuvor erstellt haben.
   Sie können eine Verbindung mit herstellen `Konfiguration und Schema` Partitionen für erweiterte Konfigurationsoptionen.
   Sie sollten jetzt in der Partition und in den Standardcontainern für LostAndFound, NTDS-Quoten und Rollen sehen können. Der Rollencontainer wurde noch nicht konfiguriert.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Erstellen Sie Container und Organisationseinheiten für ADAM

Gruppieren Sie Objekte, die in ADAM gespeichert sind, logisch in Container und Organisationseinheiten (OU), genau wie in Active Directory.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Klicken Sie mit der rechten Maustaste auf die Stammpartition, und navigieren Sie zu **Neu** > **Objekt** > **OrganizationalUnit**an.

   Hinweis: Sie können auch die Liste anderer Objekte anzeigen, die verfügbar sind. Diese Liste variiert je nach den Schemaerweiterungen, die beim Importieren der LDF-Dateien installiert wurden.

2. Wenn Sie zur Eingabe eines Werts aufgefordert werden, geben Sie den Namen der OE ein, z. B. `Anwender` .
   Auf dem Bildschirm wird ein angezeigt **Weitere Attribute** Schaltfläche.
3. Verwenden Sie die Schaltfläche, um zusätzlichen Attributen Werte zuzuweisen.
   Für die OE und Container sind keine zusätzlichen Werte erforderlich.
   Nach dem Erstellen der OE werden die neuen OE als untergeordnetes Element des Stammobjekts aufgelistet.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Delegierung mit ADAM

Sobald die OU-Struktur erstellt wurde, definieren Sie die Berechtigungsdelegierungen, um die Objekte für eingeschränkte Anwender ordnungsgemäß zu sichern.

Wie bei Active Directory gibt es zwei allgemeine Möglichkeiten, Berechtigungen zu gewähren:

- Fügen Sie einer Gruppe Anwender hinzu, denen bereits die entsprechenden Berechtigungen zugewiesen sind.
- Definieren Sie neue Berechtigungen für die ADAM-Objekte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für diese Aufgabe besprechen wir Berechtigungen auf Objektebene. Informationen zu Gruppenmitgliedschaften finden Sie im Abschnitt Gruppenverwaltung.

Da wir keine Anwender- und Computerkonsole für ADAM haben, werden alle Berechtigungen auf Objektebene mit dem Active Directory-Dienstprogramm definiert `DSACLS.exe` . Diese Datei befindet sich im ADAM-Programmverzeichnis. Beim Ausführen von ADAM-Dienstprogrammen empfiehlt es sich, die ADAM Tools-Befehlsaufforderung zu starten. Dadurch werden die richtigen Versionen der Tools sichergestellt. DSALCS wird verwendet, um Objektzugriffsrechte anzuzeigen und festzulegen.

Beispiel: „ `Dsacls \\localhost:50010\dc=mycompany,dc=adam` „ Zeigt die Berechtigungen an, die dem Stamm der Partition zugewiesen sind `dc=myCompany,dc=adam`Wird auf dem localhost ausgeführt, Port 50010. DSACLS ist ein komplexes Tool, das zum Erstellen komplexer Delegierungen verwendet wird. Ausführen `„DSACLS /?“` Für Nutzungshinweise.

Zugehörige Informationen

Erstellen Sie Container und Organisationseinheiten für ADAM

Verwenden Sie ADAMSync, um ADAM auszufüllen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM-Objekte werden ausgefüllt

ADAM-Objekte umfassen Anwenderobjekte, UserProxy-Objekt und Gruppenobjekte.

Anwenderobjekte

Anwender können mit der ADAM ADSI-Bearbeitungskonsole genauso erstellt werden wie bei der OU-Erstellung. Anwender können auch mit AD-Befehlszeilen-Tools verwaltet werden, was den Umfang dieses Dokuments überschreitet. Das einzige obligatorische Attribut für neue Anwenderobjekte ist *cn*, Bei dem es sich um einen Kurznamen oder den vollständigen Namen des Anwenders handelt. Es gibt auch eine breite Palette optionaler Attribute, die den Active Directory-Anwenderattributen ähneln. Sie können auf die vollständige Liste der Attribute zugreifen, indem Sie Eigenschaften aus dem Anwenderobjekt auswählen.

UserProxy-Objekte

Für ServiceNow LDAP-Integration wird empfohlen `AnwenderProxy` Objekte in ADAM, die einen Proxy-Account erstellen, der mit dem zugehörigen AD-Anwenderaccount verknüpft ist. Dadurch können Sie zulassen, dass ADAM Anmeldeinformationen mit AD-Anwendernamen und Passwörtern aus der Domäne ohne authentifiziert ServiceNow Direkte Verbindung zum Domänencontroller. `AnwenderProxy` Objekte ähneln AD- und ADAM-Anwenderobjekten sehr, mit Ausnahme von, die keine Passwörter speichern und einen haben `ObjektSid` Attribut, das die SID aus dem verknüpften AD-Anwenderobjekt enthält. So funktioniert der Proxy. `AnwenderProxy` Objekte werden mit erstellt `ADSIEdit` Konsolen- oder Befehlszeilen-Tools, dies kann jedoch langwierig sein. Es wird empfohlen, einen automatisierten Prozess wie unten definiert zu verwenden.

Gruppenobjekte

Gruppen werden mit der ADSIEdit-Konsole und AD-Befehlszeilen-Tools erstellt. Gruppenkonzepte ähneln AD und werden verwendet, um Gruppen und Mitglieder in zu integrieren ServiceNow. Der größte Unterschied besteht darin, dass ADAM-Gruppen Mitglieder von ADAM oder vertrauenswürdige AD-Domänen enthalten können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ADAM-Objekterstellung wird automatisiert

Wenn Sie daran interessiert sind, Active Directory-Accounts mit ADAM ZU synchronisieren, empfehlen wir Ihnen die Verwendung Microsoft *ADAMSync* Tool. Dies ist die häufigste Verwendung von ADAM für ServiceNow LDAP-Integration.

Über Berechtigungsdelegierung

ADAM enthält einige integrierte Gruppen mit Standardberechtigungen. Diese Gruppen befinden sich im Container `cn=roles,dc=myCompany,dc=adam` . Diese ähneln Domänenebenengruppen und haben Rechte für Objekte in der aktuellen Partition. Ähnlich wie AD-Gesamtstrukturen können Sie auch eine höhere Berechtigungsstufe mit den Standardgruppen in festlegen `cn=role,cn=Configuration,dc=myCompany,dc=adam` . Sie müssen eine Verbindung zur Konfigurationspartion in herstellen `ADSIEdit` . Die Gruppe „Administratoren“ enthält standardmäßig den beim Setup angegebenen Account. Dieses Mitglied ist nicht immer sichtbar, da es über die Konfigurationsgruppen geerbt wird. Administratoren haben die volle Kontrolle über alle Partitionsobjekte. Die Lesergruppe enthält standardmäßig keine Mitglieder und hat Lesezugriff auf alle Objekte in der Partition. Die Gruppe „Anwender“ ist eine dynamische Gruppe, genau wie in Active Directory. Vorübergehend werden alle ADAM-Anwender eingeschlossen, die in der Partition erstellt wurden.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM-Setup wird getestet und behoben

Das primäre Tool zum Testen ist LDP. Auf diese Weise können Sie die Anwenderauthentifizierung vollständig testen.

Der Großteil der Objektverwaltung kann mit der ADAM ADSI-Bearbeitungskonsole abgeschlossen werden, die Zugriff auf die gesamte Sammlung von Objekten und Attributen bietet. Die höchste Ebene für Steuerung und Fehlerbehebung von ADAM-Services verwenden Windows Service, der während des Instanz-Setups erstellt wurde. Der Servicename variiert und hängt vom Namen der erstellten Instanz ab. Dieser Service muss ausgeführt werden, damit der ADAM-Service ausgeführt werden kann. Wenn Verbindungsprobleme auftreten, sollten Sie die Netzwerkkonfigurationen überprüfen, um sicherzustellen, dass Sie über den entsprechenden Netzwerkzugriff verfügen, um eine Verbindung zum Server und ADAM-Port herzustellen. Für jede installierte ADAM-Instanz wird ein Windows-Ereignisprotokoll erstellt. Dies ist auch ein großartiges Tool für die Fehlerbehebung bei ADAM-Services.

Die Windows Das Sicherheitsereignisprotokoll ist auch bei der Fehlerbehebung hilfreich `UserProxy` Authentifizierungen. Alle `UserProxy` Anmeldeversuche werden im Sicherheitsprotokoll protokolliert und verweisen auf die Adresse des Remote-Client-Geräts, den eindeutigen Namen des Anwenders, der sich anmelden möchte, und den Ergebnis- oder Statuscode.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Sicherung und Wiederherstellung mit ADAM

Alle ADAM-Daten können mit standardmäßigen Dateisystemsicherungsmethoden gesichert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Redundanz

ADAM verfügt über integrierte Replikationsdienstprogramme, die auf derselben Technologie wie AD basieren. Ein vollständiges Lese- und Schreibreplikat einer ADAM-Partition kann auf demselben oder einem anderen Computer vorhanden sein. Sie können dieses Replikat auf verschiedene Arten verwenden, um eine fehlertolerante LDAP-Integration mit der Instanz bereitzustellen. Eine Option besteht darin, der Instanz beide Partitionen über die Firewall zugänglich zu machen und beide Server im Feld LDAP-Eigenschaften-Server zu definieren.

Zugehörige Informationen

Active Directory-Anwendungsmodus (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Verwenden Sie LDAPS mit ADAM

Die Standardkonfiguration für `UserProxy` Die Objektauthentifizierung dient der Erzwingung der LDAPS-Kommunikation (Secure LDAP). LDAPS erfordert SSL-Zertifikate, um den Netzwerkverkehr zu sichern.

Um diese Anforderung zu entfernen, nehmen Sie die folgende Änderung mit vor `ADSIEdit` Konsole, die mit der Konfigurationspartition verbunden ist.

```
Object: CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration
Attribute: msDS-Other-Setings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

Starten Sie den ADAM-Service neu, um die neue Einstellung zu verwenden.

Um sichere Bindungen zu unterstützen und die übertragenen Anwender- und Passwortinformationen zu verschlüsseln, muss auf dem Server und einem beliebigen LDAP-Client ein SSL-Zertifikat installiert werden. Da der ADAM-Service eingeschränkt und kontrolliert genutzt wird, ist es möglich, ein selbst signiertes Zertifikat zu verwenden, das die Anforderungen erfüllt, ohne dass Zertifikatkosten anfallen oder eine Zertifizierungsstelle (Certificate Authority, CA) aufgebaut wird. Wenn Sie bereits eine ZERTIFIZIERUNGSSTELLE haben, können Sie ein Zertifikat ausstellen. Erstellen Sie andernfalls ein selbstsigniertes Zertifikat.

Selbstsigniertes Zertifikat wird erstellt

Zur Verwendung von `selfssl` Dienstprogramm, Internetinformationsservices (IIS) müssen installiert sein. Dieser Service kann entfernt werden, nachdem Sie das Zertifikat generiert haben. Sie können das Dienstprogramm selfssl.exe aus dem IIS-Ressourcenkit abrufen. Wenn IIS bereits installiert ist, erstellen Sie eine neue Website, damit die aktuellen Sites während der Zertifikatgenerierung nicht betroffen sind. SelfSSL muss das neue selbst ausgestellte Zertifikat vorübergehend an eine gültige Website anhängen.

SelfSSL ist ein Befehlszeilentool mit den folgenden allgemeinen Parametern.

Selfssl-Parameterbeschreibungen

Parameter	Beschreibung
/T	Fügt das Zertifikat „vertrauenswürdige Zertifikate“ auf dem lokalen Computer hinzu
/N:cn	Legen Sie den allgemeinen Namen des Zertifikats fest. Dies muss mit dem vollqualifizierten Domänennamen des Servers übereinstimmen, der den Webservice mit dem Zertifikat ausführt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Selfssl-Parameterbeschreibungen (Fortsetzung)

Parameter	Beschreibung
/K	Legt die Stärke der Schlüsselgröße in Bits fest
/V	Anzahl der Tage, die das Zertifikat gültig ist
/S	Website-ID, an die das Zertifikat angehängt werden soll
/P	IP-Port des Webservice

Das allgemeine Namensattribut muss mit dem externen Namen oder der externen Adresse übereinstimmen, die die Instanz für die Verbindung mit Ihrem ADAM-Computer verwendet. Sie müssen die ID der IIS-Website abrufen, es sei denn, Sie verwenden die Standardwebsite 1, die nicht im Befehl „selfssl“ definiert werden muss. Ein Beispielbefehl zum Generieren eines Zertifikats für mein Unternehmen wäre:

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /P:50001 /T
```

Mit dieser Anweisung wird ein Zertifikat erstellt, das 10 Jahre gültig ist. Legen Sie den Wert auf eine beliebige Dauer fest, beachten Sie jedoch, dass das neue Zertifikat generiert und an die Instanz übermittelt werden muss, bevor das alte abläuft. Wir empfehlen, das Ablaufdatum auf dem Zertifikat zu notieren.

Sobald das Zertifikat generiert wurde, können Sie es von der Website entfernen oder die gesamte Website löschen, wenn Sie eine temporäre Website erstellt haben.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Weisen Sie das Zertifikat ADAM zu

Installieren Sie ein SSL-Zertifikat auf dem Server und einem beliebigen LDAP-Client, um sichere Bindungen zu unterstützen und die übertragenen Anwender- und Passwortinformationen zu verschlüsseln.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Da der ADAM-Service eingeschränkt und kontrolliert genutzt wird, ist es möglich, ein selbst signiertes Zertifikat zu verwenden, um Ihre Anforderungen zu erfüllen, ohne dass Zertifikatkosten anfallen oder eine Zertifizierungsstelle (Certificate Authority, CA) aufgebaut werden muss.

Prozedur

1. Öffnen Sie die MMC-Konsole für Zertifikate, und erstellen Sie zwei Konsolenverbindungen, eine für lokale Computerzertifikate und die andere für lokale Computerservicezertifikate im neuen ADAM-Service. Das neue Zertifikat finden Sie unter Zertifikate (Lokaler Computer)\Persönlich\Zertifikate .
2. Kopieren Sie das Zertifikat in den Container für den ADAM-Service Zertifikate: Service (ADAM-Servicename)\ADAM_Servicename\Vertrauenswürdige Stammzertifikate\Zertifikate Und kopieren Sie das Zertifikat nach Zertifikate: Service (ADAM-Servicename)\ADAM_ADAM-Servicename\persönlich\Zertifikate .
3. Öffnen Sie die Registerkarte „Details“ des von Ihnen kopierten Zertifikats, notieren Sie sich den Datumsstempel „gültig ab“, und weisen Sie der Zertifikatschlüsseldatei Lesezugriff zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wechseln Sie zu C:\Dokumente und Einstellungen\alle Anwender\Anwendungsdaten\Microsoft\Crypto\RSA\MachineKeys Und identifizieren Sie das Zertifikat mit dem übereinstimmenden Zeitstempel. Weisen Sie dem Service-Account, der ADAM ausführt, Lese- und Ausführungsrechte zu. Standardmäßig ist dies **Netzwerkservice** .

4. Starten Sie den ADAM-Service neu, um das neue Zertifikat zu aktivieren.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Exportieren Sie das öffentliche Schlüsselzertifikat

LDAPS-Clients, einschließlich der Instanz, benötigen das öffentliche Schlüsselzertifikat, um eine sichere Verbindung mit ADAM herzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Exportieren Sie aus den oben verwendeten Serverzertifikatkonsolen einen öffentlichen Schlüssel, der von den Clients verwendet werden soll.

Prozedur

1. Wählen Sie das Zertifikat aus, klicken Sie mit der rechten Maustaste, und wählen Sie aus **Alle Aufgaben/ Export** .
   Exportieren Sie den privaten Schlüssel nicht. Wählen Sie das standardmäßige DER-codierte binäre X.509-Format aus, und geben Sie den Namen der Exportdatei an.
2. Installieren Sie das öffentliche Zertifikat auf den LDAP-Clients, die über LDAPS eine Verbindung zum Server herstellen.
   Wenn Sie dazu aufgefordert werden, fügen Sie das Zertifikat zu hinzu `Vertrauenswürdige Stammzertifikatstellen` Speichern.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Zugriffskonto für Active Directory-Anwendungsmodus (ADAM)

Das System erfordert einen Anwenderaccount, um die Objektinformationen des Active Directory-Anwendungsmodus (ADAM) zu lesen, die in die Anwendungsinstanz importiert werden.

Erstellen Sie den Account mit einer der folgenden Methoden:

- Erstellen Sie einen lokalen ADAM-Anwenderaccount, weisen Sie ihm ein Passwort zu, und weisen Sie Berechtigungen zu.
- Weisen Sie einer Berechtigung zu Windows Domänenaccount auf der ADAM-Partition.
- Verwenden Sie einen `UserProxy` Account.

Wenn Sie ADAM als LDAP-Quelle verwenden, müssen Sie den vollqualifizierten Distinguished Name (FQDN) des ADAM-Accounts auf den LDAP-Servern der Instanz angeben **Eindeutiger Anmeldename** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Active Directory-Anwendungsmodus (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Testen Sie die LDAPS-Verbindungen

Testen Sie die LDAPS-Verbindungen. Es gibt zwei Konsolenverbindungen, eine für lokale Computerzertifikate und die andere für lokale Computerservicezertifikate im neuen ADAM-Service.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Ausführen `LDP.exe` Aus dem ADAM-Installationsordner c:\Windows\adam .
   Stellen Sie sicher, dass die ADAM-Version ausgewählt ist, da dies nicht der Standard ist Windows LDP-Client.
2. Öffnen Sie eine neue Verbindung mit **Verbindung/Verbindung** Menü.
   Der Servername muss mit der CN übereinstimmen, die dem Zertifikat zugewiesen ist.
3. Geben Sie ein **LDAPS-Port** Und wählen Sie aus **SSL** Kontrollkästchen.
   Die Ergebnisse einer erfolgreichen Verbindung sind einige allgemeine Serverinformationen und keine Fehler.
4. Binden (anmelden) Sie an den Service.
   Um typische LDAP-Clientverbindungen zu replizieren, wählen Sie die Option einfache Bindung aus. Geben Sie einen gültigen ADAM-Anwender oder ein `UserProxy` Eindeutiger Name im Anwenderfeld und das zugehörige Passwort.
   Wenn Sie eine Rückgabemeldung mit der Angabe „authentifiziert als:….“ sehen Dann haben Sie erfolgreich eine Verbindung mit LDAPS hergestellt.

Zugehörige Informationen

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Verwenden Sie ADAMSync, um ADAM auszufüllen

Administratoren verwenden MS ADAMSync, um LDAP-Verzeichnisse auszufüllen, die MS ADAM verwenden.

Hinweis:

In diesem Dokument wird davon ausgegangen, dass Sie mindestens ein grundlegendes Verständnis von Microsoft Windows Server, Active Directory und ADAM haben und bereits über eine funktionsfähige verfügen Active Directory-Anwendungsmodus (ADAM) Instanz mit einer Partition.

Dies sind Beispielverfahren. Aufgrund der Komplexität und der Tatsache, dass sie in Ihrer Umgebung ausgeführt wird, können wir keinen direkten Support anbieten. Wir empfehlen Ihnen, mit zu arbeiten Microsoft Oder ein Microsoft Berater, wenn Sie auf Probleme stoßen.

Sobald ADAM installiert und die erste Partition erstellt wurde, können Sie sie mit Objekten ausfüllen.

Die folgenden Optionen sind verfügbar:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Manuelle Objekterstellung mit GUI oder Skripts. Diese Option ist ineffizient und langsam.
- Integrieren Sie mit Active Directory Microsoft Integrationsinformationsserver. Diese Option bietet letztendlich die meiste Flexibilität und Funktionalität, erfordert jedoch einige erweiterte Konfigurationen. Es ist eine kostenlose Version von MIIS verfügbar, die mit Active Directory, ADAM und kompatibel ist Microsoft Globale Adresslisten von Exchange. Sofern Sie nicht bereits Erfahrung mit MIIS haben, empfehlen wir Ihnen, nicht zu versuchen, eine neue Umgebung nur für die LDAP-Integration zu implementieren.
- Verwenden Sie ADAMSync, ein Synchronisierungstool, das Microsoft Stellt mit ADAM bereit. Dies ist die Option, die hier erläutert wird.

Definieren Sie ADAM-Anwenderaccounts

Definieren Sie Anwenderaccounts in ADAM. Ein Anwenderaccount wird für die Instanz verwendet, mit der eine Verbindung hergestellt werden soll, und der andere Anwenderaccount für ADAMSync.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Diese Accounts können lokale ADAM-Anwenderobjekte, UserProxy-Objekte oder ein Windows-Account aus einer vertrauenswürdigen Domäne sein.

Die *ADAM User*Account erfordert schreibgeschützten Zugriff auf die Verzeichnisstruktur, die Sie in Ihre Instanz importieren. Die beste Möglichkeit, dies zu erreichen, besteht darin, den Account dem Mitgliederattribut in der Lesergruppe hinzuzufügen, die in cn=roles,dc=mycompany,dc=adam gefunden wird.

Neue ADAM-Anwenderaccounts sind standardmäßig deaktiviert. Sie müssen die neuen Accounts aktivieren und ein Passwort festlegen.

Prozedur

1. Aktivieren Sie Anwender, indem Sie das Attribut „MSDS-UserAccountDisabled“ in „FALSCH“ ändern.
2. Klicken Sie mit der rechten Maustaste auf das Anwenderobjekt, und setzen Sie das Passwort zurück.
3. Testen Sie die neuen Accounts mithilfe von LDP, wie in definiert Active Directory-Anwendungsmodus (ADAM) Um sicherzustellen, dass eine Verbindung hergestellt werden kann.
   Verwenden Sie den **LDAP** > **Ansicht/Struktur** Option, bei der der Basis-DN leer gelassen wird, um sicherzustellen, dass Sie die Objekte im Verzeichnis mithilfe der neuen Accounts anzeigen können. Die Konfiguration, das Schema und die Domänenpartition müssen im linken Bereich sichtbar sein. Durchlaufen Sie die Domänenpartition. Wenn Sie einen neuen lokalen ADAM-Account verwenden, wird „keine untergeordneten Elemente“ angezeigt, was bedeutet, dass Sie keinen Lesezugriff auf die Objekte haben. Überprüfen Sie die Setup-Gruppenmitgliedschaften, und testen Sie sie erneut.

   ADAMSync verwendet *ADAMSync User*Account zum Verwalten von Objekten in der ADAM-Partition. Dieser Account erfordert Administratorrechte, da er ADAM-Objekte erstellt, aktualisiert und löscht.

   ADAMSync verwendet *ADAMSync AD*Account zum Lesen der AD-Objekte, die mit ADAM synchronisiert werden.

Richten Sie ADAMSync ein

ADAMSync ist in enthalten Windows Server 2003 R2. Laden Sie ADAMSync herunter, und installieren Sie sie, wenn Sie ein anderes Betriebssystem verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweitern des Schemas

Das ADAM-Schema muss erweitert werden, um ADAMSync zu unterstützen.

1. Führen Sie den folgenden Befehl unter c:\Windows\adam aus, um die ADAMSync-Schemaerweiterungen zu importieren. Möglicherweise müssen Sie Server:Port ändern und Anmeldeinformationen hinzufügen, wenn der aktuelle Anwender keinen Zugriff hat. Weitere Informationen finden Sie in der Datei AdamSyncMetadata.ldf.

```
ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
#configurationNamingContext
```

2. Führen Sie dasselbe mit MS-AdamSchemaW2k3.ldf aus, um Windows 2003-Attribute zu unterstützen.

```
ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
#configurationNamingContext
```

Empfohlene Schemaänderungen

Hier sind einige zusätzliche Schemaänderungen, die wir empfehlen.

1. Öffnen Sie eine neue MMC-Konsole, und fügen Sie das ADAM-Schema-Snap-in hinzu.
2. Stellen Sie eine Verbindung zur ADAM-Instanz her.
3. Erweitern Sie den Ordner Klassen, und suchen Sie die userProxy-Klasse, öffnen **Eigenschaften** .
4. Überprüfen Sie die folgenden optionalen Attribute auf der Registerkarte Attribute, und fügen Sie alle hinzu, die noch nicht vorhanden sind.
   - Unternehmen
   - department
   - GivenNane
   - mail
   - PhysikalDeliveryOfficeName
   - SAMAccountName
   - sn
   - Telefonnummerierung
   - Titel
   - UserAccountControl
   - userPrincipalName
5. Starten Sie den ADAM-Service neu, um die neuen Einstellungen zu aktivieren.

Installieren Sie die ADAM-Konfigurationsdatei

Installieren Sie die ADAM-Konfigurationsdatei über die Windows-Befehlszeile.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Installieren Sie die Konfigurationsdatei.

```
C:\WINDOWS\adam>adamsync /install localhost:50000 MS-AdamSyncConf-SNC.XML
```

2. Führen Sie die Synchronisierungsdatei aus, um sich bei der Konsole anzumelden.

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```

3. Überprüfen Sie die Ergebnisse mithilfe der ADSIEdit-Konsole.
   Sie sollten die neuen Objekte und Attribute anzeigen, die von ADAMSync erstellt wurden.
4. Führen Sie ldap aus, um die UserProxy-Authentifizierung zu testen.
   Der Synchronisierungsprozess wird automatisiert

   Richten Sie den Synchronisierungsprozess als ein Windows Geplante Aufgabe. Sie müssen entweder die Anmeldeinformationen in der Konfigurationsdatei oder in der Befehlszeile angeben oder die geplante Aufgabe mit einem Account ausführen, der Zugriff hat.

   Spezielle Hinweise

   - Sie können mehrere Konfigurationsdateien und geplante Aufgaben erstellen, um ADAM aus mehreren Quellen zu synchronisieren.

     In diesem Beispiel wird das Attribut „sAMAccountName“ importiert, das als Anwendungsanmeldung verwendet werden kann. Wenn Sie die Quelle synchronisieren, müssen Sie sicherstellen, dass Sie über einen eindeutigen Attributwert verfügen, der für die Anmeldeinformationen verwendet werden kann. „SAMAccountName“ ist garantiert innerhalb einer Domäne eindeutig, aber nicht für mehrere Domänen.

   - Wenn Sie verwenden Microsoft Exchange, wir empfehlen, cn=SystemMailbox*-Objekte als Teil der Object-Filter-Konfiguration auszuschließen.

Beispiel für ADAM-Konfigurationsdateien

Alle Konfigurationen für ADAMSync werden in XML-Dateien gespeichert.

Standardkonfigurationsdatei mit Kommentaren

In der ADAMSync-Installation ist eine Standardkonfigurationsdatei namens MS-AdamSyncConf.xml enthalten. Erstellen Sie eine Kopie dieser Datei, damit Sie ein Basisbeispiel haben, auf das Sie in Zukunft verweisen können. Dieses Beispiel ist die Standardkonfigurationsdatei mit hinzugefügten Kommentaren.

```
<?xml version="1.0"?>
<doc>
 <configuration>
<!-- Sync File Description -->
<description>MyCompany ADAMSync Configuration</description>
  <security-mode>object</security-mode>;
<!-- source-ad-name = fqdn of the domain controller -->;
  <source-ad-name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
<!-- source-ad-partition = root AD domain partition -->;
  <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
<!-- source-ad-account = use this to specify an account to connect to AD -->;
<!-- if not used, the current user will be used  -->;
  <source-ad-account>;</source-ad-account>;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 <account-domain>;</account-domain>;
<!-- target-dn = target ADAM OU -->;
 <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
 <query>;
<!-- base-dn = should be the root AD partition if you want all users -->;
  <base-dn>;dc=myCompany,dc=com</base-dn>;
<!-- object-filter = standard ldap query format, this will grab all users -->;
<!-- need to review results to see if you should modify this filter -->;
  <object-filter>;(objectCategory=person)</object-filter>;
  <attributes>;
<!-- include=userproxy requires objectSID to link back to the AD account -->;
   <include>;objectSID</include>;
   <include>;givenName</include>;
   <include>;sn</include>;
   <include>;description</include>;
   <include>;title</include>;
   <include>;company</include>;
   <include>;department</include>;
   <include>;mail</include>;
   <include>;physicalDeliveryOfficeName</include>;
   <include>;telephoneNumber</include>;
   <include>;sAMAccountName</include>;
  </attributes>;
 </query>;
<!-- map for user-to-userproxy object types -->;
 <user-proxy>;
  <source-object-class>;user</source-object-class>;
  <target-object-class>;userProxy</target-object-class>;
 </user-proxy>;
 <schedule>;
  <aging>;
   <frequency>;0</frequency>;
   <num-objects>;0</num-objects>;
  </aging>;
  <schtasks-cmd>;</schtasks-cmd>;
 </schedule>;
</configuration>;
<synchronizer-state>;
 <dirsync-cookie>;</dirsync-cookie>;
 <status>;</status>;
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
</synchronizer-state>;
</doc>;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdatei für LDAP-Filter

Sie können eine beliebige Filterebene im Wert „object-Filter“ in der Konfigurationsdatei angeben. Verwenden Sie die standardmäßige LDAP-Abfragesyntax mit den folgenden XML-Escape-Zeichen anstelle der Standardoperatoren.

- UND = „&“ ersetzen durch &
- ODER = „|“ (vertikale Linie) durch | ersetzen
- NICHT = „!“ Ersetzen durch !

Referenzkonfigurationsdatei

Hier ist eine tatsächliche Konfigurationsdatei, auf die als Beispiel verwiesen werden kann.

```
<?xml version="1.0"?>;
<doc>;
 <configuration>;
<description>;SNCTest ADAMSync Configuration</description>;
  <security-mode>;object</security-mode>;
  <source-ad-name>;domaincontroller.service-now.com</source-ad-name>;
  <source-ad-partition>;dc=service-now,dc=com</source-ad-partition>;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
  <target-dn>;ou=servicenow users,dc=service-now,dc=adam</target-dn>;
  <query>;
   <base-dn>;dc=service-now,dc=com</base-dn>;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;userAccountControl</include>;
   </attributes>;
  </query>;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
  </user-proxy>;
  <schedule>;
   <aging>;
    <frequency>;0</frequency>;
    <num-objects>;0</num-objects>;
   </aging>;
   <schtasks-cmd>;</schtasks-cmd>;
  </schedule>;
 </configuration>;
 <synchronizer-state>;
  <dirsync-cookie>;</dirsync-cookie>;
  <status>;</status>;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
</synchronizer-state>;
</doc>;
```

Konfigurieren Sie Microsoft Active Directory für sichere LDAPS-Kommunikation

Verwenden Sie Zertifikatpaare, um die Microsoft Active Directory (AD) LDAPS-Kommunikation zu aktivieren.

Hinweis: Diese Verfahren wurden mit Windows 2003 R2 Standard Edition entworfen und getestet und funktionieren mit allen Versionen von Windows 2003.

Die sichere LDAP-Kommunikation (LDAPS) ähnelt der SSL-Kommunikation (HTTPS), da beide die Daten zwischen Servern und Clients verschlüsseln. Zu diesem Zweck geben der Server und die Clients gemeinsame Informationen mithilfe von Zertifikatpaaren frei. Der Server enthält das private Schlüsselzertifikat, und die Clients halten das öffentliche Schlüsselzertifikat. Diese Zertifikate sind erforderlich, um die Microsoft Active Directory (AD) LDAPS-Kommunikation zu aktivieren.

Um LDAPS für Active Directory zu konfigurieren, müssen Sie:

- Stellen Sie sicher, dass die Active Directory-Domäne eingerichtet ist und dass die Instanz über die Firewall eine Verbindung zum Active Directory-Server herstellen kann.
- Verifiziert, ob eine Zertifizierungsstelle (Certificate Authority, CA) vorhanden ist, die ein Zertifikat für den Domänencontroller (DC) ausstellen kann. Wenn Sie noch keine CA-Infrastruktur haben, gibt es zwei Optionen.
  - Richten Sie eine eigenständige CA ein, um das Zertifikat auszustellen
  - Fordern Sie ein Drittparteizertifikat an
- Wenn Sie bereits eine ZERTIFIZIERUNGSSTELLE haben, können Sie ein Zertifikat von einer internen ZERTIFIZIERUNGSSTELLE generieren.

Alle Zertifikate haben ein definiertes Ablaufdatum, das in den Zertifikateigenschaften angezeigt werden kann. Wenn das Zertifikat abläuft, schlägt der gesamte LDAPS-Datenverkehr fehl, und Ihre Anwender können sich nicht mehr bei der Instanz anmelden. Um dies zu beheben, muss ein neues Zertifikat ausgestellt und auf Ihrer Instanz installiert werden.

Der standardmäßige Ablauf für Microsoft CA-Zertifikate beträgt ein Jahr. Externe CA-Zertifikate werden normalerweise in Schritten von einem Jahr erworben. Beachten Sie, wann Ihr Zertifikat abläuft, oder verwenden Sie die Funktion „Ablaufbenachrichtigung“ der Anwendung (befindet sich in **System-LDAP** > **Zertifikate**) an. Stellen Sie sicher, dass Sie ein neues Zertifikat bereit haben, bevor das alte abläuft. Dies gibt Ihnen Zeit, das neue Zertifikat zu installieren und zu testen, bevor das alte abläuft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie eine eigenständige Zertifizierungsstelle für Active Directory ein

Der erste Schritt zur Konfiguration von Microsoft Active Directory für SSL-Zugriff besteht in der Einrichtung einer eigenständigen Zertifizierungsstelle (CA).

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Machen Sie sich keine Sorgen über die Ressourcennutzung, da beide erforderlichen Services (IIS und CA) nach der Ausgabe der Zertifikate deaktiviert werden können.

Prozedur

1. Installieren Sie Internet Information Server (IIS).
2. Installieren Sie Zertifizierungsstellenservices im eigenständigen Modus.
3. Überprüfen Sie, ob die Webanwendung „Zertifikatservices“ installiert und aktiv ist.

Nächste Maßnahme
Erweitern Sie mit der IIS-Manager-Konsole den lokalen Computer, und wählen Sie aus *Websites* . Der Status von **Standard-Website** Muss sein *Wird Ausgeführt* . Sie sollten auch einen sehen *CertSrv* Anwendung, die unter aufgeführt ist **Standard-Website** . Wenn die Website nicht ausgeführt wird oder die Anwendung fehlt, müssen Sie das Problem beheben, bevor Sie fortfahren.

Generieren Sie ein Zertifikat von einer internen Zertifizierungsstelle

Wenn Sie Microsoft Active Directory für SSL-Zugriff konfigurieren, müssen Sie ein internes Zertifikat generieren und das externe Zertifikat anfordern.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Diese Schritte gelten für Microsoft CA-Services. Wenn Sie eine andere interne CA-Plattform haben, wenden Sie sich an Ihren lokalen CA-Administrator.

Prozedur

1. Navigieren Sie auf dem Domänencontroller (DC), für den Sie ein Zertifikat erstellen möchten, zu `http://localhost/certsrv` Oder geben Sie den Namen des CA-Servers an, wenn er sich auf einem Remote-Server befindet.
2. Klicken Sie auf der Willkommensseite auf **Fordern Sie ein Zertifikat an** Und wählen Sie aus *Erweiterte Zertifikatanforderung* .
3. Wählen Sie auf der Seite Erweiterte Zertifikatanforderung die Option aus **Erstellen** Und senden Sie eine Anforderung an diese CA.
4. Schließen Sie die erweiterte Zertifikatanforderung wie folgt ab:

Felder für erweiterte Zertifikatanforderung

Feld	Eintrag
Name	Der vollqualifizierte Domänenname (FQDN) des DC, der das Zertifikat anfordert.
E-Mail	Die E-Mail-Adresse der Person, die für das Zertifikat verantwortlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eintrag
Unternehmen	Ihr Unternehmensname.
Einstellungen für Schlüsseloptionen	
Erstellen Sie einen neuen Schlüsselsatz	Wählen Sie es aus.
CSR	Microsoft RSA SChannel Kryptografieanbieter.
Schlüsselnutzung	Austausch.
Schlüsselgröße	1024 wird empfohlen. Die Instanz unterstützt bis zu 2048.
Name des automatischen Schlüsselcontainers	Wählen Sie es aus.
Speichern Sie das Zertifikat im lokalen Computerzertifikatspeicher	Wählen Sie es aus.

5. Klicken Sie auf **Absenden**.
   Sie werden zu einer Seite weitergeleitet, die Ihren bereitstellt **Anforderungs-ID** , Notieren Sie sich diese ID.
6. Um die ausstehende Anforderung zu verarbeiten, gehen Sie wie folgt vor:
   a. Öffnen Sie die Verwaltungskonsole der Zertifizierungsstelle.
   b. Erweitern Sie den Serverknoten, und wählen Sie aus **Ausstehende Anforderungen** .
   c. Suchen Sie die Anforderungs-ID für die soeben übermittelte Anforderung, klicken Sie mit der rechten Maustaste, und wählen Sie sie aus *Alle Aufgaben/Probleme, um die Anforderung zu genehmigen und das Zertifikat auszustellen* .
7. Um das ausgestellte Zertifikat abzurufen, gehen Sie wie folgt vor:
   a. Navigieren Sie im DC, in dem Sie die Anforderung von gestellt haben, zu `http://localhost/certsrv` , Oder geben Sie den Namen des CA-Servers an, wenn er sich auf einem Remote-Server befindet.
   b. Wählen Sie Aus `Zeigen Sie den Status einer ausstehenden Zertifikatanforderung an` .
   c. Wählen Sie den Link zum neuen Zertifikat aus.
   d. Wählen Sie den Link zu aus **Installieren Sie dieses Zertifikat** .

Nächste Maßnahme

Sie müssen ein Drittparteizertifikat anfordern. Zertifikate von externen CAS können für nur 30 USD pro Jahr erworben werden. Detaillierte Verfahren zum anfordern eines Zertifikats von einer externen ZERTIFIZIERUNGSSTELLE finden Sie im Microsoft-artikel 321051 . Befolgen Sie das Exportverfahren, nachdem es empfangen, installiert und getestet wurde.

Testen Sie die LDAPS-Konnektivität lokal

Testen Sie die LDAPS-Konnektivität nach der Installation der internen Zertifikate und Drittparteizertifikate, wenn Sie Microsoft Active Directory für SSL-Zugriff konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Stellen Sie sicher, dass Windows Support Tools auf dem Domänencontroller (DC) installiert sind.
   Das Support-Tools-Setup (suptools.msi) finden Sie im `\Support\Tools` Verzeichnis auf Ihrer Windows Server-CD.
2. Navigieren zu **Start** > **Alle Programme** > **Windows-Support-Tools** > **Befehlszeile**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geben Sie in der Befehlszeile ein `ldp` Um das Tool zu starten.

3. Von *ldp* Fenster auswählen **Verbindung** > **Connect** Und geben Sie den lokalen FQDN und die Portnummer (636) an.
   Wählen Sie auch aus *SSL* .
   Wenn erfolgreich, werden in einem Fenster Informationen zur Active Directory-SSL-Verbindung angezeigt und aufgelistet. Wenn die Verbindung nicht erfolgreich ist, versuchen Sie, Ihr System neu zu starten, und wiederholen Sie diesen Vorgang.

Exportieren Sie das öffentliche Schlüsselzertifikat, um dem LDAP-Zertifikat zu vertrauen

Exportieren Sie das Zertifikat des öffentlichen Schlüssels, und importieren Sie es in die Anwendung, wenn Sie Microsoft Active Directory für SSL-Zugriff konfigurieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn Ihre Zertifizierungsstelle kein vertrauenswürdiger Drittparteilieferant ist, müssen Sie das Zertifikat für die ausstellende CA exportieren, damit wir ihr vertrauen können, und durch Zuordnung dem LDAP-Serverzertifikat vertrauen können. Für Anwender von MS Certificate Services können Sie den Zertifikatpfad anzeigen, indem Sie das Zertifikat in der Konsole anzeigen, die zum Exportieren verwendet wird. Wählen Sie aus **Zertifikatpfad** Registerkarte. Sie müssen alle Zertifikate in der Kette exportieren. Sie können das CA-Zertifikat im selben Ordner wie das LDAP-Zertifikat finden, indem Sie im Zertifikatpfad nach dem Namen suchen. Übermitteln Sie alle Zertifikate zum Importieren in Ihre Instanz.

Prozedur

1. Fügen Sie in einer aktuellen oder neuen MMC-Konsole das Snap-in Zertifikat (lokaler Computer) hinzu.
2. Öffnen Sie `Persönlich/Zertifikate` Ordner.
3. Suchen Sie das neue Zertifikat.
   Die Spalte „ausgestellt an“ zeigt den FQDN des Domänencontrollers an.
4. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie aus *Alle Aufgaben/Export* .
5. Exportieren Sie im DER- oder Base-64-Format.
   Benennen Sie die Datei im Format `Mycompany.cer` . Dies ist das öffentliche Schlüsselzertifikat, das auf der Instanz verwendet werden muss, um sicher mit Ihrem Domänencontroller zu kommunizieren.
6. Testen Sie LDAPS lokal, bevor Sie das Zertifikat an die Instanz übermitteln.

Nächste Maßnahme
Importieren Sie nach Abschluss dieses Verfahrens das Zertifikat des öffentlichen Schlüssels in die Anwendung.
Siehe Installieren Sie das LDAP X.509 SSL-Zertifikat Zum Hochladen des Zertifikats in die Anwendung.

Globale LDAP-Katalognutzung

Einem DC kann die Rolle Global Catalog (GC) gewährt werden. Die Rolle „globaler Katalog“ (GC) ist ein LDAP-konformes Verzeichnis, das aus einer Teildarstellung jedes Objekts aus jeder Domäne innerhalb einer Gesamtstruktur besteht.

Administratoren konfigurieren Active Directory, um Lightweight Directory Access Protocol (LDAP)-Verzeichnisinformationen mithilfe einer der folgenden Hosting-Methoden zu hosten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die gängige Methode zum Hosting von LDAP-Verzeichnisinformationen besteht darin, das standardmäßige LDAP oder LDAPS (sicheres LDAP) auf den Ports 389 oder 636 zu verwenden. Diese Standard-LDAP-Ports sind immer auf einem Domänencontroller (DC) vorhanden und werden selten geändert. Der Zugriff auf diese Verzeichnispartition bietet Zugriff auf alle Objekte innerhalb der Domäne, die auf dem DC gehostet wird. Es gibt keine Möglichkeit, mit dieser Methode auf Objekte aus anderen Domänen zuzugreifen.
- Einem DC kann auch die Rolle Global Catalog (GC) gewährt werden. Die Rolle „globaler Katalog“ (GC) ist ein LDAP-konformes Verzeichnis, das aus einer Teildarstellung jedes Objekts aus jeder Domäne innerhalb der Gesamtstruktur besteht. Auf dieses LDAP-Verzeichnis kann über Port 3268 zugegriffen werden, mit LDAPS auf Port 3269. Die Zertifikatanforderungen für LDAPS und LDAP-Standard-Ports sind identisch.

LDAP-Abhängigkeiten des globalen Katalogs

- Für den Domänencontroller, mit dem Ihre Instanz eine Verbindung herstellt, muss die Rolle „globaler Katalog“ aktiviert sein.
- Firewall-Regeln müssen eingehenden Datenverkehr an den Domänencontroller an Port 3268 (LDAP) oder 3269 (LDAPS) zulassen.

Spezielle Hinweise

- Nicht alle Attribute werden auf die GC-Partition repliziert. Allgemeine Attribute wie Vorname, Nachname, E-Mail, Telefonnummer, Beschreibung, und Adresse sind enthalten. Zusätzliche Attribute können dem GC hinzugefügt werden, sollten jedoch beschränkt werden, um die Auswirkungen auf den Datenverkehr der Gesamtstruktur-Replikation zu minimieren.
- Standardmäßige LDAP-Integrationen verwenden „sAMAccountName“ normalerweise als UserID der Instanz und als Zusammenfügungsschlüssel in der LDAP-Importzuordnung, da dies garantiert innerhalb einer Domäne eindeutig ist. Dieses Attribut ist nicht mehr eindeutig, wenn eine gesamte Gesamtstruktur von Domänen angezeigt wird. Ein neues eindeutiges Attribut muss identifiziert werden und als Anwender-ID und Zusammenfügungsschlüssel. Diese müssen nicht das gleiche Attribut sein und können je nach Walddesign variieren. Wenden Sie sich an Ihren Active Directory-Administrator. Normalerweise ist der userPrinicpalName ein eindeutiges Attribut für alle Domänen, aber dies ist möglicherweise kein anwenderfreundlicher Name für die Anmeldung, kann jedoch für den eindeutigen Bezeichner bei Importen verwendet werden. Ein allgemeines Attribut, das für die Anwender-ID verwendet wird, ist die E-Mail-Adresse. Diese Entscheidungen wirken sich auf die LDAP-Eigenschaften und die LDAP-Zuordnung aus.
- Der für den Zusammenfügungsschlüssel in der LDAP-Importzuordnung verwendete Wert muss eindeutig sein und für jedes importierte Objekt vorhanden sein. Wenn er nicht eindeutig ist oder nicht vorhanden ist, werden falsche Datensätze mit Änderungen aktualisiert.
- Wenn Sie bereits über eine LDAP-Integration verfügen und diese in eine GC ändern möchten, ändern Sie den Importzusammenfügungsschlüssel. Die neuen Schlüsselwerte müssen importiert werden, bevor Sie den Zusammenfügungsschlüssel ändern können.
- Wenn Sie Änderungen an Ihrer LDAP-Integration vornehmen, die Ihre Integration beeinträchtigen, sollten Sie diese Änderungen als ersten Schritt rückgängig machen. Danach wenden Sie sich an Kundenservice und Support Mit vollständigen Informationen darüber, was Sie versuchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geringfügige OpenLDAP-Schemaänderung

In OpenLDAP 2,3-Systemen, die das Back-bdb (Berkley-Back-End) verwenden, nehmen Administratoren geringfügige Änderungen an ihrem Schema vor, um die Integration zu erleichtern.

Warnung: Die hier beschriebene Anpassung wurde für die Verwendung in bestimmten Fällen entwickelt und wird von Now Support nicht unterstützt. Diese Methode wird wie sie ist zur Verfügung gestellt und sollte vor der Implementierung gründlich getestet werden. Veröffentlichen Sie alle Fragen und Kommentare zu dieser Anpassung in unserem Community-Forum .

In OpenLDAP 2,3 bietet Back-bdb eingeschränkte Unterstützung für die Indexierung von Ungleichheiten (Sortierung). Sie wird nur für die Syntax generalizedTime und ChangeSequenceNumber implementiert. Sie kann für Syntax, die Teilzeichenfolgen unterstützt, nicht unterstützt werden. Suchfilter, die Ungleichheiten enthalten, werden mit dem Anwesenheitsindex verarbeitet.

Wir empfehlen, ein anwenderdefiniertes Attribut zu diesem Zweck zu erstellen, anstatt zu ändern, was bereits indiziert oder im Schema vorhanden ist (z. B. *servnowid*).

Ändern Sie das OpenLDAP-Schema

Ändern Sie das OpenLDAP-Schema. In diesen Schritten wird eine Schemaänderung von OpenLDAP 2,3 beschrieben, die von einem unserer Kunden bereitgestellt wurde, der ihm bei der Integration in seine Instanz geholfen hat.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Warnung: Die hier beschriebene Anpassung wurde für die Verwendung in bestimmten Fällen entwickelt und wird von Now Support nicht unterstützt. Diese Methode wird wie sie ist zur Verfügung gestellt und sollte vor der Implementierung gründlich getestet werden. Veröffentlichen Sie alle Fragen und Kommentare zu dieser Anpassung in unserem Community-Forum .

So ändern Sie das OpenLDAP-Schema für die Integration mit der Instanz:

Prozedur

1. Erstellen Sie ein anwenderdefiniertes Attribut.

Example

```
attribute ( 1.3.6.1.4.1.3403000.2.1.8

    NAME 'servnowid'
 ORDERING caseIgnoreOrderingMatch
 EQUALITY caseIgnoreMatch
 SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

2. Fügen Sie das Attribut in die ausgewählte objectclass-OID ein.

Example

```
objectclass ( 1.3.6.1.4.1.3403000.2.2.1
    NAME 'BcfUserIdentifiers' SUP top AUXILIARY
 MAY ( uniqid $ unixid $ servnowid ) )
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In OpenLDAP 2,3 können Sie die Serverkonfigurationen dynamisch ändern, Sie können jedoch nur das Schema erweitern. Sie können das vorhandene Schema nicht ändern oder löschen. Anstatt eine weitere Objektklasse für dieses Attribut in der dynamischen Konfiguration zu erstellen, verwenden Sie die statische Konfigurationsdatei slapd.conf.

3. Fügen Sie in slapd.conf die Indizierung für das neue Attribut im Abschnitt bdb Ihres Hauptdatenbank-Back-Ends ein.

Example

```
database bdb (configs here) ....

index servnowid pres

(other indexes here) .....
```

4. Führen Sie als Stamm Slapindex aus, um dieses Attribut zu indizieren, um es in Suchfiltern verfügbar zu machen.
Stellen Sie sicher, dass der OpenLDAP-Daemon nicht ausgeführt wird oder sich im schreibgeschützten Modus befindet, bevor Sie slapindex starten.

Datensatz-LDAP-Löschungen

Standardmäßig löscht die Instanz keine Einträge, nachdem sie aus LDAP entfernt wurden.

Löschen eines Eintrags, auch als bezeichnet *Datensatz* , Löscht auch den gesamten Verlauf und Verweise auf den gelöschten Eintrag.

Zum Beispiel Konfigurationselemente (CIs), SLA-Vereinbarungen, Softwarelizenzen, Bestellungen, und Servicekatalog-Einträge haben alle einen Verweis auf Abteilung. wenn eine Abteilung gelöscht wird, löscht die Integration alle Verweise auf die Abteilung. Außerdem führt das Löschen eines Anwenders dazu, dass der gesamte Verlauf dessen verloren geht, was dieser Anwender getan hat.

Entscheiden Sie, ob oder beibehalten werden sollen Löschen Sie alle Datensätze aus einer Tabelle Entsprechend den Anforderungen Ihrer Organisation.

Gleichzeitige Sitzungen begrenzen

Sie können die Anzahl gleichzeitiger interaktiver Sitzungen für einen Anwender oder eine Rolle in einer Instanz auf allen Knoten beschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von gleichzeitigen Sitzungen begrenzen.

Aktivieren



Erfahren Sie, wie Sie gleichzeitige Sitzungen begrenzen.

Satz



Legen Sie die Begrenzung gleichzeitiger Sitzungen für einen Anwender oder eine Rolle fest.

Deaktivieren



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden – Begrenzung gleichzeitiger Sitzungen

Sie können die Anzahl gleichzeitiger interaktiver Sitzungen für einen Anwender oder eine Rolle in einer Instanz auf allen Knoten beschränken.

Gleichzeitige interaktive Sitzungen beziehen sich auf die Anzahl der Sitzungen, die ein Anwender pro haben kann ServiceNow Instanz. Eine aktive Instanzsitzung findet bei jeder neuen Anmeldung bei einem bestimmten statt ServiceNow Instanz. Standardmäßig gibt es keine Einschränkungen für die Anzahl der aktiven Instanzsitzungen, die ein Anwender haben kann.

Mit dem Jakarta-Release können Sie die Anzahl der aktiven gleichzeitigen Sitzungen pro Benutzer beschränken. Wenn sich der Anwender anmeldet, nachdem die maximale Anzahl aktiver Sitzungen erreicht wurde, wird die älteste aktive Sitzung beendet, und eine neue interaktive Sitzung wird aktiv. Wenn ein Anwender versucht, über einen Browser auf eine geschlossene Sitzung zuzugreifen, wird er zur Anmeldeseite weitergeleitet.

Hinweis: Die **Gleichzeitige Sitzungen begrenzen** Das Plugin muss aktiv sein, um ein maximales Sitzungslimit zu aktivieren. Grenzwerte werden über die Eigenschaft glide.authenticate.max.concurrent.interactive.sessions festgelegt. Ein Höchstgrenzwert gilt für jeden Anwender oder jede Rolle, für den die Grenzwerteigenschaft aktiv ist. Für einen Anwender oder eine mit dem Anwender verbundene Rolle muss der Wert limit_concurrent_Sessions auf „wahr“ festgelegt sein, damit der Grenzwert für Sitzungen initiiert werden kann. Für das Jakarta-Release unterstützt diese Funktion keine Sitzungen, die über die native mobile App oder nicht interaktive Mechanismen erstellt wurden.

Ein typischer Anwendungsfall, wenn eine maximale gleichzeitige Sitzung von 1 festgelegt ist:

1. Der Anwender greift auf den ersten zu ServiceNow Instanz über Chrome.
2. Nachdem sich der Anwender erfolgreich angemeldet hat, ServiceNow Erstellt Sitzung 1 (S1) für den Anwender.
3. Der Anwender entscheidet, einen weiteren Zugriff auf zu initiieren ServiceNow Instanz über Firefox.
4. Nachdem sich der Anwender erfolgreich angemeldet hat, ServiceNow Erstellt Sitzung 2 (S2) für den Anwender.
5. Da der Anwender eine maximale Anzahl gleichzeitiger Sitzungen von 1 hat, wird die S1-Sitzung ungültig, wenn S2 erstellt wird.
6. Wenn der Anwender durch Chrome zurückkehrt, um auf S1 zuzugreifen ServiceNow Instanz wird der Anwender zur Anmeldeseite weitergeleitet, da S1 ungültig ist.

Gleichzeitige Sitzungen schränken die Arbeit mit allen ein ServiceNow Authentifizierungsmechanismen: SAML, LDAP und lokale Datenbankauthentifizierung. Es funktioniert auch mit Multifaktor-Authentifizierung und allen interaktiven Elementen ServiceNow Authentifizierungsmechanismen. Die Quelle der Sitzung kann über angezeigt werden **sys_user_Session** Tabelle unter der Spalte **Typ** . Die Werte können sein:

- Webbrowser
- Mobiler Browser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ServiceNow Mobile-App
- Nicht interaktiv (SOAP, WSDL, OAuth)

Aktivieren und konfigurieren Sie das Plugin „gleichzeitige Sitzungen begrenzen“

Sie können das Plugin „gleichzeitige Sitzungen begrenzen“ (com.glide.limit.concurrent.sessions) aktivieren, wenn Sie die Administratorrolle innehaben.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.
2. Suchen und klicken Sie auf das Plugin „gleichzeitige Sitzungen begrenzen“.
3. Überprüfen Sie im System-Plugin-Formular die Plugin-Details, und klicken Sie dann auf den zugehörigen Link **Aktivieren/Aktualisieren**.
4. Klicken Sie auf **Aktivieren**.
5. Um diese Funktion zu aktivieren und eine maximale Anzahl gleichzeitiger Sitzungen festzulegen, wechseln Sie zu **Plugin-Dateien** Suchen Sie nach den folgenden Eigenschaften, und ändern Sie die Einstellungswerte.

Option	Bezeichnung
glide.authenticate.limit.concurrent.interactive-.sessions	Sie können die Möglichkeit aktivieren, gleichzeitige Sitzungen zu begrenzen, indem Sie den Wert auf festlegen **Wahr** . Standardmäßig ist diese Eigenschaft auf festgelegt **Falsch** , D. h. es gibt keine Beschränkung für die Anzahl der interaktiven Sitzungen, die ein Anwender aktiv haben kann. **Hinweis:** Um diese Funktion zu deaktivieren, legen Sie diese Eigenschaft wieder auf fest **Falsch** .
glide.authenticate.max.concurrent.interactive-.sessions	Sie können die maximale Anzahl gleichzeitiger aktiver interaktiver Sitzungen festlegen, die ein Anwender auf der Instanz auf allen Knoten haben kann.

6. **Wahlweise:** Sie können bei Bedarf auch die folgenden Eigenschaften ändern.

Option	Bezeichnung
glide.authenticate.session.types.to.limit.concurrency	Diese Eigenschaft begrenzt Sitzungstypen. Standardmäßig haben nur die Webbrowsersitzungen einen Grenzwert. Zu den Sitzungstypen gehören: ○ Webbrowser (1) ○ Mobiler Browser (2)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	○ ServiceNow Mobile-App (3) ○ Nicht interaktiv (10) Sie können den Wert für den Webbrowser auf „1“, für den mobilen Browser auf „2“ oder für beide auf „1,2“ festlegen. **Hinweis:** Nur Web- und mobile Browsersitzungen können einen Grenzwert haben. Es gibt keine Grenzwerte für Sitzungen, die aus stammen ServiceNow Mobile App oder nicht interaktive Sitzungen.
glide.authenticate.limit.concurrent.sessions.across.all.nodes	Diese Eigenschaft schränkt den Grenzwert gleichzeitiger Sitzungen pro Knoten ein, anstatt sie auf alle Knoten von einzuschränken ServiceNow Instanz. Standardmäßig ist der Wert auf „wahr“ festgelegt, wodurch Anwendersitzungen auf allen Knoten beschränkt werden. Wenn die Eigenschaft auf „falsch“ festgelegt ist, unterliegen nur die Sitzungen auf diesem Knoten und nicht die auf den anderen Knoten dem Grenzwert.

7. Klicken Sie Auf **Aktualisieren** Damit die Einstellungen wirksam werden.

Nächste Maßnahme

Legen Sie ein Limit für gleichzeitige Sitzungen nach Anwender oder Rolle fest.

Zugehörige Informationen

Liste der Plugins (Zurich)

Legen Sie ein Limit für gleichzeitige Sitzungen nach Anwender oder Rolle fest

Sie können ein Limit für gleichzeitige Sitzungen für einen bestimmten Anwender oder eine bestimmte Rolle festlegen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender** oder **Anwenderadministration** > **Rollen**an.
2. Wählen Sie einen Anwender oder eine Rolle aus, für den Sie ein Limit für gleichzeitige Sitzungen festlegen möchten, und überprüfen Sie die **Begrenzen Sie Gleichzeitige Sitzungen** Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Aktualisieren** .
   Für den Anwender oder die Rolle ist ein Grenzwert festgelegt, wie viele gleichzeitige Sitzungen gleichzeitig geöffnet sein können.

Deaktivieren Sie ein Limit für gleichzeitige Sitzungen nach Anwender oder Rolle

Sie können ein Limit für gleichzeitige Sitzungen für einen bestimmten Anwender oder eine bestimmte Rolle deaktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender** oder **Anwenderadministration** > **Rollen**an.
2. Wählen Sie einen Anwender oder eine Rolle aus, für den Sie ein Limit für gleichzeitige Sitzungen deaktivieren möchten, und deaktivieren Sie die Option **Begrenzen Sie Gleichzeitige Sitzungen** Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Aktualisieren** .
   Für den Anwender oder die Rolle gilt keine Beschränkung, wie viele gleichzeitige Sitzungen gleichzeitig geöffnet sein können.

Lokale Authentifizierung

Verwenden ServiceNow® Lokale Authentifizierung, um sicherzustellen, dass sich die Anwender auf einem lokalen Gerät anmelden.

Die lokale Authentifizierung ist eine Methode zur Verifizierung der Identität eines Anwenders auf einem lokalen Gerät. Es verwendet eindeutige Merkmale oder Anmeldeinformationen des Anwenders, um die Anmeldung des Anwenders zu validieren.

Verwenden ServiceNow® Lokale Authentifizierungsfunktionen von für sicheren Zugriff auf ServiceNow® Instanz auf Ihren lokalen Geräten.

Anmelde- und Authentifizierungssicherheit

Konfigurieren Sie die Sicherheitsoptionen für die Anmeldung, um den Zugriff auf Ihre Instanz zu steuern.

Konfigurieren Sie Ihre Anmeldesicherheit



Erfahren Sie, wie Sie die Anmeldesicherheit konfigurieren.

Definieren Sie Anmeldeszenarien



Definieren Sie Anmeldeszenarien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Passwortzurücksetzung



Erfahren Sie mehr über das Zurücksetzen des Anmeldepassworts.

Erkunden Sie die Anmelde- und Authentifizierungssicherheit

Konfigurieren Sie die Sicherheitsoptionen für die Anmeldung, um den Zugriff auf Ihre Instanz zu steuern.

Sicherheitsoptionen

Sie können mehrere Aspekte der Sicherheit der Anwenderanmeldung und -Authentifizierung steuern:

Funktion	Beschreibung	Verwandte Themen
Steuerungen für das an- und Abmelden	Steuern Sie mehrere Dimensionen des an- und Abmeldeprozesses für Anwender, z. B. die Angabe einer Zielseite, die der Anwender bei der Anmeldung sieht, und steuern Sie, wie sich Anwender abmelden.	• Definieren Sie Anmeldeszenarien • Konfigurieren Sie die Eingabeaufforderung zur Bestätigung der Abmeldung • Installationsausgänge • Sperrung für fehlgeschlagene Anmeldeversuche angeben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung	Verwandte Themen
Authentifizierungssicherheit	Steuern Sie den Prozess zum Zurücksetzen des Passworts und Funktionen wie die Option „mich speichern“. Sie können auch IP-adressbasierte Steuerungen für den Zugriff auf die Instanz verwenden und eine Nonce für die Single Sign-on-Digest-Authentifizierung implementieren.	• Konfigurieren Sie Ihre Passwortrichtlinie • Passwortzurücksetzung • Anwendernamen speichern • IP-bereichsbasierte Authentifizierung • Implementieren Sie eine Nonce

Definieren Sie Anmeldeszenarien

Sie können alle Anwender nach der Anmeldung zu derselben Seite weiterleiten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn sich Anwender direkt bei einer Instanz anmelden, z. B. bei http://{instance_name}.service-now.com/, führt das System Folgendes aus:

1. Greift auf den Wert in der Eigenschaft zu `glide.entry.page.script`. Der Standardwert der Eigenschaft wird von einer Skripteinbindung mit dem Namen abgeleitet *CMSEintragsseite* .
2. Leitet den Anwender zur Instanzanmeldeseite weiter, wenn die Eintragsseite eine Anmeldung erfordert.
3. Wendet ggf. Anmelderegeln auf den Anwender an.

So erzwingen Sie das System, alle Anwender nach der Anmeldung zu derselben Seite zu leiten:

Prozedur

1. Navigieren zu **Alle** > **Inhaltsmanagement** > **Konfiguration** > **Konfigurationsseite**an.
2. Wählen Sie einen Wert für aus *Anmeldeseite* Oder erstellen Sie nach Bedarf eine neue Seite.

   Wenn diese Seite nicht die Standardseite der Site ist, wird sie immer hierher umgeleitet. Wenn es sich um eine Website-Standardseite handelt, werden Anmelderegeln angewendet. Wenn dieser Wert null ist, verwendet das System navpage.do als Eintragsseite. Geben Sie hier keine Anmeldeseite ein. Andernfalls müssen sich Anwender zweimal anmelden.

   Anmeldung bei einer Instanz, um auf einen Datensatz zuzugreifen:

   Wenn sich Anwender bei einer Instanz anmelden, um anhand ihres global eindeutigen Bezeichners (sys_ID) auf einen Datensatz zuzugreifen, z. B. http://{instance}.service-now.com/incident.do?sys_id={sys_id}, führt das System Folgendes aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Leitet den Anwender zu einer Anmeldeseite weiter, wenn er sich noch nicht angemeldet hat.

b. Leitet den Anwender zum entsprechenden Datensatz weiter, wenn er darauf zugreifen darf. Wenn der Anwender keine Zugriffsrechte für den Datensatz hat, wird eine Meldung über Zugriffsverweigerung angezeigt.

Anmeldung beim Serviceportal oder einer CMS-Website:

Wenn sich Anwender beim Serviceportal oder auf einer CMS-Website anmelden, z. B. http://<instance>.service-now.com/site-name/page.do, führt das System Folgendes aus:

- Wenn ein Wert in vorhanden ist *Anmeldeseite* Feld im Serviceportal oder im CMS-Websiteformular wird der Anwender zu dieser Anmeldeseite geleitet und gegebenenfalls Anmeldungsregeln auf den Anwender angewendet.
- Wenn keine Anmeldeseite angegeben ist, wird der Anwender zum Wert in weitergeleitet *Homepage* Feld im Serviceportal oder im CMS-Site-Formular.

Anmeldung beim Serviceportal oder einer CMS-Website, um auf einen Datensatz zuzugreifen:

Wenn sich Anwender beim Serviceportal oder einer CMS-Website anmelden, um auf einen Datensatz wie http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident,{sys_id} zuzugreifen, folgt das System dem gleichen Verfahren und leitet den Anwender schließlich zum Datensatz weiter. Wenn der Anwender keine Zugriffsrechte für den Datensatz hat, wird eine Meldung über Zugriffsverweigerung angezeigt.

Anmeldungen und das Mitarbeiter-Selfserviceportal

Das System verfolgt die erste Startseite, auf die ein Anwender zugreifen möchte, auch wenn er sich beim Mitarbeiter-Selfserviceportal anmelden möchte.

Berücksichtigen Sie die folgenden Szenarien.

Beispiel 1:

1. Ein Anwender ist nicht angemeldet und versucht dann, mithilfe einer bestimmten SYS-ID in der URL auf einen Datensatz zuzugreifen.
2. Das System leitet den Anwender zur Anmeldeseite weiter.
3. Anstatt sich anzumelden, versucht der Anwender, auf eine andere Website zuzugreifen, z. B. das Mitarbeiter-Selfservice-Portal (/ess).
4. Das System leitet den Anwender erneut zur Anmeldeseite weiter.
5. Der Anwender meldet sich an und wird zu dem Datensatz weitergeleitet, auf den der Anwender zuerst anstatt zum Mitarbeiter-Selfserviceportal zugreifen wollte.

Beispiel 2:

1. Ein Anwender ist nicht angemeldet und versucht dann, mithilfe einer bestimmten SYS-ID in der URL über das Mitarbeiter-Selfservice-Portal (/ess) auf einen Datensatz zuzugreifen.
2. Das System leitet den Anwender zur Anmeldeseite weiter.
3. Anstatt sich anzumelden, versucht der Anwender, über das Mitarbeiter-Selfserviceportal auf einen anderen Datensatz zuzugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Das System leitet den Anwender erneut zur Anmeldeseite weiter.
5. Der Anwender meldet sich an und wird zum ersten Datensatz und nicht zum zweiten weitergeleitet.

Geben Sie eine Anmelde-Zielseite an

Standardmäßig sehen Anwender ihre Homepage bei der Anmeldung. Sie können eine andere Anmelde-Zielseite angeben, indem Sie eine Systemeigenschaft oder das Inhaltsverwaltungssystem verwenden.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Um eine Anmelde-Zielseite für alle Anwender anzugeben, ändern Sie den Eigenschaftswert in der Tabelle „sys_properties“.

Prozedur

1. Typ sys_properties.list Im Navigationsfilter.
2. Suchen Sie nach **Glide.Login.Startseite** Systemeigenschaft.
3. In **Wert** Feld den Namen der Seite eingeben, die alle Anwender bei der Anmeldung sehen.

   Verwenden <page name>.do ; Sie können auslassen http://"instance".service-now.com/ Teil der URL. Um den Seitennamen oder die URL einer Seite im System zu bestimmen, können Sie auf einen Link verweisen. Einige mögliche Seiten sind Willkommen.do Und Incident.tun .

   Um eine Dashboard-Zielseite anzugeben, legen Sie die Eigenschaft auf fest $Dashboards.do?Dashboard=<SYS_ID> . Ersetzen Sie <SYS_ID> durch die sys_ID des Dashboards.

   Um Anwender zum Serviceportal zu leiten, legen Sie die Eigenschaft auf fest /Sp

   Hinweis: Diese Eigenschaft ist systemweit, daher wirkt sich die Einstellung auf alle Anwender aus. Um eine Anmeldung speziell für Anwender ohne Rollen festzulegen, können Sie die gleichen Schritte ausführen und verwenden **Glide.entry.loggedin.page_ess** Eigenschaft.

   Sie können auch eine Anmelde-Zielseite mit dem Inhaltsverwaltungssystem angeben.

Sperrung für fehlgeschlagene Anmeldeversuche angeben

Das System bietet inaktive Skriptaktionen, mit denen Sie die Anzahl der fehlgeschlagenen Anmeldeversuche angeben können, bevor ein Benutzeraccount gesperrt wird, und mit denen die Anzahl nach einer erfolgreichen Anmeldung zurückgesetzt wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

Navigieren zu **Alle** > **Systemrichtlinie** > **Skriptaktionen** Zum Anzeigen oder Aktivieren der Skripts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Ab der Kingston-Release werden die Skriptaktionen **SNC-Benutzersperrprüfung mit automatischer Entsperrung** und **SNC-Benutzerlöschung** nach einem zBoot aktiviert.

Weitere Informationen zu Eigenschaften, die sich auf fehlgeschlagene Anmeldeversuche auswirken, finden Sie unter Verwalten fehlgeschlagener Anmeldeversuche (Instanzsicherheitshärtung) In den Instanzsicherheitshärtungseinstellungen.

Skriptaktion	Beschreibung
SNC-Benutzersperrprüfung mit automatischer Entsperrung	• Verwendet den Wert der Eigenschaft `glide.user.max_unlock_attempts`, um den Grenzwert für fehlgeschlagene Anmeldeversuche festzulegen. • Entsperrt den Benutzeraccount nach dem für die Eigenschaft `glide.user.unlock_timeout_in_mins` angegebenen Zeitraum. Wenn kein Wert angegeben ist, entsperrt das System den Benutzeraccount nach dem Standardzeitraum von 15 Minuten.
SNC-Benutzersperrprüfung	Verfolgt die Anzahl der fehlgeschlagenen Anmeldeversuche und sperrt den Benutzeraccount nach einer angegebenen Anzahl von fehlgeschlagenen Anmeldeversuchen (Standard: 5).
SNC-Benutzerlöschung	Aktualisiert den Benutzerdatensatz nach einer erfolgreichen Anmeldung: Setzt die Anzahl der fehlgeschlagenen Anmeldeversuche zurück und aktualisiert das Datum der letzten Anmeldung.

Nächste Maßnahme

Jedes Mal, wenn ein Benutzer versucht, sich anzumelden, wird die Aktion in einem Ereignisprotokoll aufgezeichnet. Sie können ein Protokoll der fehlgeschlagenen Anmeldeversuche anzeigen.

1. Navigieren zu **Systemrichtlinie** > **Ereignisprotokolle**an.
2. Filtern Sie im Feld **Name** nach **login.failed**. Sie können den versuchten Anmeldenamen, das Datum und die IP-Adresse anzeigen, die für den Versuch protokolliert wurden.

UI-Seiten öffentlich oder privat machen

Sie können Seiten öffentlich machen, wenn Sie möchten, dass Ihre Anwender die Seiten sehen, ohne sich anzumelden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die meisten Seiten können nur von angemeldeten Anwendern angezeigt werden. Eine begrenzte Anzahl von Seiten ist öffentlich, sodass sich Anwender nicht anmelden müssen, um sie anzuzeigen, z. B. die Willkommensseite, die Vorderseite sowie die Anmelde- und Abmeldeseiten.

Warnung: Mehrere öffentliche Seiten des Basissystems sind für die Funktionalität vieler Funktionen erforderlich. Deaktivieren Sie öffentliche Seiten des Basissystems nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Anwendungsnavigator-Filter ein `sys_public.list` .
2. Klicken Sie auf **Neu**.
3. Erstellen Sie in der Tabelle „sys_public“ einen Datensatz mit den folgenden Werten.

Feld	Beschreibung
Seite	Der Name der Seite. Beispiel: $sp
Aktiv	Wenn diese Option ausgewählt ist, ist die Seite öffentlich zugänglich. Deaktivieren Sie die Option aktiv, wenn die Seite privat sein soll.

4. Klicken Sie auf **Speichern**.
   Wenn „aktiv“ auf „wahr“ festgelegt wird, ist die Seite öffentlich, also jeder, der besucht `<instance_name>/sp` Oder `<instance_name>/$sp.do` Kann auf die Seite zugreifen.

Anforderungen an die Passwortkomplexität

Passwörter in Ihrem ServiceNow® Instanz muss Komplexitätsanforderungen erfüllen.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von Passwortkomplexitätsanforderungen.

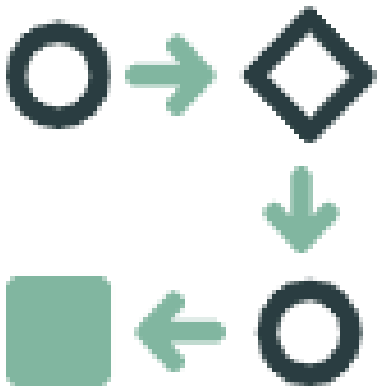
Aktivieren



Erfahren Sie, wie Sie Passwortkomplexitätsanforderungen aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren



Konfigurieren Sie die Anforderungen für die Passwortkomplexität.

Referenz: Nicht unterstützte Passwortzeichen



Informieren Sie sich über die nicht unterstützten Passwortzeichen.

Erkunden Sie die Anforderungen an die Passwortkomplexität

Passwörter in Ihrem ServiceNow® Instanz muss Komplexitätsanforderungen erfüllen.

Die Richtlinieneinstellung für die Komplexitätsanforderungen für Passwörter bestimmt, ob Passwörter eine Reihe von Richtlinien für sichere Passwörter erfüllen müssen.

Anforderungen an die Passwortkomplexität werden erzwungen, wenn ein Passwort geändert oder erstellt wird.

Die Anforderungen an die Passwortkomplexität gelten und funktionieren basierend auf den folgenden Faktoren:

- Wenn `glide.apply.password_policy.on_login`Eigenschaft ist aktiviert, die Überprüfung der Passwortrichtlinie wird für den Anwender während der Anmeldung erzwungen. Während der Anmeldung muss der Anwender die Passwortrichtlinie einhalten und das Passwort für die Instanz ändern.
- Die Anforderungen der Passwortrichtlinie basieren auf der Basic Multilingual Plane (BMP), die Zeichen für alle modernen Sprachen enthält. ServiceNow Instanzen werden mit BMPs von etwa 10.000 Zeichen geliefert.
- Passwörter innerhalb der zulässigen BMPs können für Ihre Instanz festgelegt werden. Passwörter, die innerhalb dieser BMPs nicht eingehalten werden, sind nicht zulässig.

Bei Bedarf können Sie vorschreiben, dass Passwörter regelmäßig geändert werden, mindestens alle 90 Tage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen und gesperrte Zeichen

Um eine sichere Netzwerkumgebung zu ermöglichen, müssen Anwender starke Passwörter verwenden, die eine Kombination aus Buchstaben, Zahlen und Symbolen enthalten. Diese Kombinationen helfen, nicht autorisierte Anwender zu verhindern, die normalerweise manuelle oder automatisierte Methoden verwenden, um schwache Passwörter zu erraten.

Das Passwort für Ihre Instanz muss die folgenden Anforderungen erfüllen:

- Mindestens 8 Zeichen.
- Maximal 100 Zeichen.
- Enthält Kleinbuchstaben und Großbuchstaben
- Enthält Sonderzeichen.
- Enthält Ziffern.

Sie können eine Liste gängiger fehlerhafter Passwörter sperren, z. B.:

- Vorhersagbare und sich wiederholende Sequenzen wie „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw.
- Mitarbeitername oder Anwendernamen.
- Relevante Marken- oder Produktnamen.
- Standorte, z. B. Hauptsitz des Unternehmens, Stadt, Land usw.
- Unternehmensspezifische interne Begriffe oder Abkürzungen.
- Emojis.

Hinweis: Anwender-, Marken- oder unternehmensspezifische Zeichen, die nicht im Passwort verwendet werden können, können auf der Seite „Passwortrichtlinie“ oder „Passwort ausschließen“ konfiguriert werden.

Aktivieren Sie Passwortrichtlinien in Ihrer Instanz

Implementieren Sie Passwortrichtliniensteuerungen bei der Anmeldung. Zwingt Anwender, ihr Passwort zu ändern, wenn das Passwort die Kriterien der Passwortrichtlinie nicht erfüllt.

Vorbereitungen

Erforderliche Rolle: Administrator

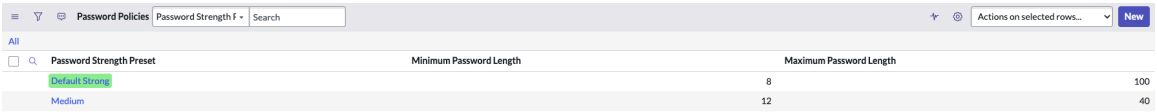
Warum und wann dieser Vorgang ausgeführt wird

Das Plugin „Passwortrichtlinie“ (com.Glide.password_Policy) ist standardmäßig aktiviert. Die Richtlinie tritt in Kraft, wenn ein Anwender das Passwort ändert oder zurücksetzt.
Die **Voreinstellung Für Passwortstärke** Feld wird automatisch auf festgelegt **Standardmäßig Stark** . Wenn Sie neue Kriterien hinzufügen möchten, können Sie das folgende Verfahren ausführen.

Wenn Sie Ihre Instanz über angepasst haben `ValidatePasswordStronger`Installationsausgang oder Anmeldeinformationsspeicher für Passwortzurücksetzung `pwd_cred_store`Eigenschaft, dann siehe Eigenschaften der Passwortrichtlinie Um zu erfahren, wie eine Passwortrichtlinie für Ihre Instanz implementiert wird.

Hinweis: Die aktive Passwortrichtlinie wird für die Instanz wie gezeigt hervorgehoben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Um die Passwortrichtlinie zu ändern, navigieren Sie zu **Alle** > **Passwortzurücksetzung** > **Anmeldeinformationsspeicher**, Wählen Sie die Anmeldeinformationen aus, und ändern Sie **Passwortrichtlinie** Feld für die erforderliche Richtlinieneingabe.

Prozedur

1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Passwortrichtlinien**an.
2. Klicken Sie auf **Neu**.
   Das Formular „Passwortrichtlinie“ wird angezeigt.
3. Geben Sie an **Name** Für Ihre Passwortrichtlinie.
4. Wählen Sie im Abschnitt Passwortrichtlinienkriterien eine der folgenden Voreinstellungen aus **Voreinstellung Für Passwortstärke** Feld.

Vorgegebene Passwortstärke	Beschreibung
Standard	Füllt die Felder für erforderliche Passwortzeichen wie folgt automatisch aus: ○ Legt Fest **Mindestanzahl der Großbuchstaben** Bis 1. ○ Legt Fest **Mindestanzahl Kleinbuchstaben** Bis 1. ○ Legt Fest **Mindestanzahl numerischer Zeichen** Bis 1. ○ Legt Fest **Mindestanzahl der Sonderzeichen** Bis 0. Die Mindestlänge des Passworts beträgt 8 Zeichen und die Höchstzahl 100 Zeichen.
Mittel	Füllt die Felder für erforderliche Passwortzeichen wie folgt automatisch aus: ○ Legt Fest **Mindestanzahl der Großbuchstaben** Bis 1. ○ Legt Fest **Mindestanzahl Kleinbuchstaben** Bis 1. ○ Legt Fest **Mindestanzahl numerischer Zeichen** Bis 1. ○ Legt Fest **Mindestanzahl der Sonderzeichen** Bis 1. Die Mindestlänge des Passworts beträgt 12 Zeichen und die Höchstzahl 40 Zeichen.
Hoch	Füllt die Felder für erforderliche Passwortzeichen wie folgt automatisch aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgegebene Passwortstärke	Beschreibung
	◦ Legt Fest **Mindestanzahl der Großbuchstaben** Bis 1. ◦ Legt Fest **Mindestanzahl Kleinbuchstaben** Bis 2. ◦ Legt Fest **Mindestanzahl numerischer Zeichen** Bis 1. ◦ Legt Fest **Mindestanzahl der Sonderzeichen** Bis 3. Die Mindestlänge des Passworts beträgt 8 Zeichen und die Höchstzahl 100 Zeichen.
Standardmäßig stark	Füllt die Felder für erforderliche Passwortzeichen wie folgt automatisch aus: ◦ Legt Fest **Mindestanzahl der Großbuchstaben** Bis 1. ◦ Legt Fest **Mindestanzahl Kleinbuchstaben** Bis 1. ◦ Legt Fest **Mindestanzahl numerischer Zeichen** Bis 1. ◦ Legt Fest **Mindestanzahl der Sonderzeichen** Bis 1. Die Mindestlänge des Passworts beträgt 8 Zeichen und die Höchstzahl 100 Zeichen.
Anwenderdefiniert	Füllt die Felder für erforderliche Passwortzeichen wie folgt automatisch aus: ◦ Legt Fest **Mindestanzahl der Großbuchstaben** Bis 1. ◦ Legt Fest **Mindestanzahl Kleinbuchstaben** Bis 1. ◦ Legt Fest **Mindestanzahl numerischer Zeichen** Bis 1. ◦ Legt Fest **Mindestanzahl der Sonderzeichen** Bis 1. Die Mindestlänge des Passworts beträgt 8 Zeichen und die Höchstzahl 100 Zeichen. Sie können auch anpassen **Passwort-Richtlinienskript** Wird angezeigt.
Erweitert	Auswählen **Erweitert** Wird angezeigt **Passwort-Regelskript** Und **Passwort-Stärkeskript** . Je nach Anforderung können Sie diese Skripts anpassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Passwortrichtlinie wird basierend auf der ausgewählten Voreinstellung angewendet.

5. Füllen Sie die verbleibenden Felder im Formular aus.

Formular „Passwortrichtlinie“

Feld	Beschreibung
Mindestlänge von Passwörtern	Mindestlänge des Passworts. Diese Option wird für alle Voreinstellungen mit Ausnahme von angezeigt **Erweitert** . Legen Sie dieses Feld auf mindestens 8 bis 10 Zeichen fest.
Maximale Passwortlänge	Maximale Länge des Passworts. Diese Option wird für alle Voreinstellungen außer angezeigt **Erweitert** . Legen Sie dieses Feld auf maximal 100 Zeichen fest.
Mindestanzahl der Großbuchstaben	Mindestanzahl von Großbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der Kleinbuchstaben	Mindestanzahl von Kleinbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der numerischen Zeichen	Mindestanzahl von Zeichen im Passwort, von 0 bis 10.
Mindestanzahl der Sonderzeichen	Mindestanzahl von Sonderzeichen im Passwort, von 0 bis 10.
Eingeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Beispiel: Wenn Sie eingeben `$,!` , Dann können Anwender nur „$“ und „!“ verwenden. Als Sonderzeichen im Passwort. Es können keine anderen Sonderzeichen verwendet werden. Ein Passwort mit anderen Sonderzeichen ist nicht zulässig.
Ausgeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Beispiel: Wenn Sie eingeben `@$!` , Dann können Anwender „@“, „$“ und „!“ nicht verwenden. Als Sonderzeichen in ihren Passwörtern. **Hinweis:** Diese Option ist verfügbar, wenn `glide.password_policy.use_excluded_special_ch` ist aktiviert.
Anwenderdaten nicht zulassen	Option zum Nichtzulassen von Anwenderdaten, die authentifizierungsbezogen sind.
Schwellenwert für Sequenzlänge	Die Sequenzlänge Ihres Passworts.
Schwellenwert für Wiederholungslänge	Die Wiederholungslänge Ihres Passworts.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ○ Sowohl der Schwellenwert für die Sequenzlänge als auch der Schwellenwert für die Wiederholungslänge können maximal acht Zeichen lang sein. Mit diesen Feldern können Sie schwache Kombinationen von Passwörtern mit vorhersagbaren und sich wiederholenden Sequenzen wie „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw. einschränken. ○ Wenn **Voreinstellung Für Passwortstärke** Ist auf festgelegt **Standardmäßig Stark** , Dann wird die Länge für den Schwellenwert für die Sequenzlänge und den Schwellenwert für die Wiederholungslänge auf vier Zeichen festgelegt.
Passwort testen	Geben Sie in diesem Feld Ihr tatsächliches Passwort an.

6. Klicken Sie Auf **Testen Sie Ihr Passwort** .
7. Nachdem das Passwort als gültig getestet wurde, klicken Sie auf **Übermitteln** Um das Passwort zu übermitteln.

Hinweis: Testen Sie Ihr Passwort immer vor dem Senden.

Eigenschaften der Passwortrichtlinie

Mit den Eigenschaften der Passwortrichtlinie können Sie Passwortrichtlinien verwalten, Passwörter auflisten und während der Anmeldung eine Passwortrichtlinie anwenden.

Navigieren zu **Passwortrichtlinie** > **Eigenschaften** Zum Anzeigen und Bearbeiten der Eigenschaften der Passwortrichtlinie.

Eigenschaft	Beschreibung
Glide.enable.password_Policy	Aktiviert eine Passwortrichtlinie für Ihre Instanz. Die Richtlinie tritt in Kraft, wenn ein Anwender ein Passwort ändert oder zurücksetzt. Diese Eigenschaft wird automatisch auf festgelegt **Wahr** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Hinweis: • Wenn Ihre Instanz angepasst wird, über `ValidatePasswordStronger`Installation beenden oder Ihren Anmeldeinformationsspeicher für Passwortzurücksetzung [pwd_cred_Store], dann müssen Sie diese Eigenschaft erstellen und Ihren Systemeigenschaften hinzufügen. • Vor Orlando Release, wenn Ihre Instanz mit angepasst wurde `ValidatePasswordStronger`Installation beenden, dann mussten Sie die Eigenschaft „Passwortrichtlinie“ erstellen, damit die Passwortrichtlinie funktioniert. • Beginnend mit Orlando Release, es gibt keine Anpassung des Installationsabschlusses. Die Eigenschaften der Passwortrichtlinie funktionieren standardmäßig. Diese Eigenschaften können manuell deaktiviert werden.
Glide.enable.Blacklist_password	Verbietet die Verwendung bestimmter Passwörter. Der Administrator kann Passwörter in die Tabelle „Ausgeschlossenes Passwort“ einfügen. Diese Eigenschaft wird automatisch auf festgelegt **Wahr** .
Glide.Apply.password_Policy.on_login	Zwingt Anwender, die Passwörter bei ihrer nächsten Anmeldung zu ändern, wenn die vorhandenen Passwörter nicht der aktuellen Passwortrichtlinie entsprechen. Diese Eigenschaft wird automatisch auf festgelegt **Falsch** . Wert wird auf festgelegt **Wahr** Erzwingt während der Anmeldung eine Passwortrichtlinie. **Hinweis:** Das Aktivieren dieser Eigenschaft kann dazu führen, dass eine beträchtliche Anzahl von Anwendern, die nicht der neuen Passwortrichtlinie entsprechen, ihre Passwörter ändern muss.
glide.password_policy.user_excluded_special_char	Ermöglicht Anwendern die Verwendung der Option „ausgeschlossenes Sonderzeichen“ im Formular „Passwortrichtlinie“.
Glide.validieren.sys_user.password.field	Aktiviert die Validierung des Anwenderpassworts anhand der Passwortrichtlinie, wenn ein Administrator das Formular „sys_user“ oder die Listenansicht bearbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Glide.Passwort.Richtlinie.generieren.Passwort.Feld.deaktiviert	Deaktiviert **Passwort** Feld im Popup-Fenster „Passwort festlegen“ im Formular „sys_user“.
glide.user.show.password.field	Aktiviert **Passwort** Feld im Formular „sys_user“.
glide.password_policy.debug	Aktiviert die Debug-Protokollierung für die Passwortrichtlinie.

Konfigurieren Sie Ihre Passwortrichtlinie

Mit Passwortrichtlinienkriterien können Sie Ihr Passwort sichern und die Mindestanforderungen an die Passwortkomplexität einhalten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Das Plugin „Passwortrichtlinie“ [com.Glide.password_Policy] ist standardmäßig aktiviert. Sie tritt in Kraft, wenn ein Anwender das Passwort ändert oder zurücksetzt. Wenn Sie Ihre Instanz über den Installationsausgang ValidatePasswordStronger oder Ihren Anmeldeinformationsspeicher für die Passwortzurücksetzung [pwd_cred_Store] angepasst haben, finden Sie weitere Informationen unter Eigenschaften der Passwortrichtlinie .

Prozedur

1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Passwortrichtlinien**an.

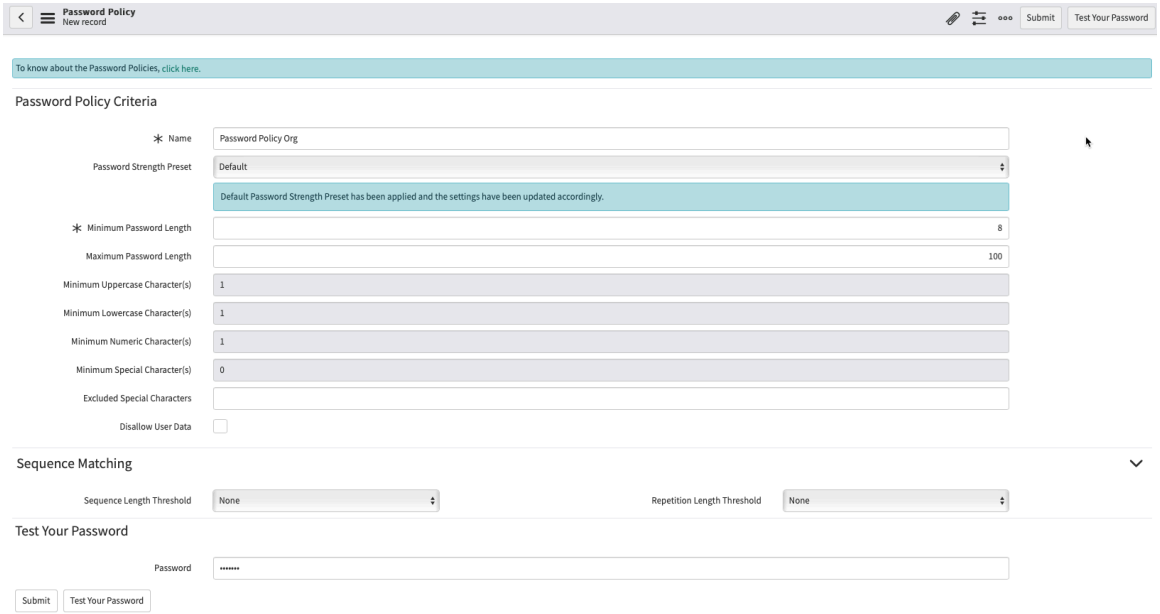
   Hinweis: **Standardmäßig Stark** Voreinstellung in aktiviert als Standardkriterien für die Passwortakzeptanz. Wenn Sie neue Kriterien hinzufügen möchten, können Sie die folgenden Schritte ausführen.

2. Klicken Sie auf **Neu**.

   Die Seite „neuer Datensatz für Passwortrichtlinie“ enthält die folgenden Abschnitte, die Sie zum Festlegen Ihres Passworts angeben müssen:

   - **Passwortrichtlinienkriterien**
   - **Sequenzabgleich**
   - **Passwort testen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Geben Sie an **Name** Für Ihre Passwortrichtlinie.
4. In **Kriterien Für Passwortrichtlinie** Wählen Sie im Abschnitt die Voreinstellung aus **Voreinstellung Für Passwortstärke** . Folgende Voreinstellungen sind verfügbar:

Voreinstellung für Passwortstärke und zugehörige Beschreibung

Vorgegebene Passwortstärke	Beschreibung
Standard	Auswählen **Standard** Füllt die erforderlichen Passwortzeichen wie folgt automatisch aus: ○ Mindestens ein Großbuchstabe ○ Mindestens ein Kleinbuchstabe ○ Mindestens ein numerisches Zeichen
Mittel	Auswählen **Mittel** Füllt die erforderlichen Passwortzeichen basierend auf folgenden Zeichen automatisch aus: ○ Mindestens ein Großbuchstabe ○ Mindestens ein Kleinbuchstabe ○ Mindestens ein numerisches Zeichen ○ Mindestens ein Sonderzeichen
Hoch	Auswählen **Hoch** Füllt die Passwortzeichen automatisch wie folgt aus: ○ Mindestens ein Großbuchstabe ○ Mindestens zwei Großbuchstaben ○ Mindestens ein numerisches Zeichen ○ Mindestens drei Sonderzeichen
Standardmäßig stark	Auswählen **Standardmäßig Stark** Füllt die erforderlichen Passwortzeichen basierend auf folgenden Zeichen automatisch aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgegebene Passwortstärke	Beschreibung
	○ Mindestens ein Großbuchstabe ○ Mindestens ein Kleinbuchstabe ○ Mindestens ein numerisches Zeichen ○ Mindestens ein Sonderzeichen
Anwenderdefiniert	Auswählen **Anwenderdefiniert** Füllt die erforderlichen Passwortzeichen basierend auf folgenden Zeichen automatisch aus: ○ Mindestens ein Großbuchstabe ○ Mindestens ein Kleinbuchstabe ○ Mindestens ein numerisches Zeichen ○ Mindestens ein Sonderzeichen Sie können auch anpassen **Passwort-Richtlinienskript** Wird angezeigt.
Erweitert	Auswählen **Erweitert** Wird angezeigt **Passwort-Regelskript** Und **Passwort-Stärkeskript** . Je nach Anforderung können Sie diese Skripts anpassen.

Hinweis: Die Passwortrichtlinie wird basierend auf der ausgewählten Voreinstellung angewendet.

5. Geben Sie die in der Tabelle beschriebenen Felder an:

Formular „Passwortrichtlinie“

Feld	Beschreibung
Mindestlänge von Passwörtern	Mindestlänge des Passworts. Diese Option wird für alle Voreinstellungen außer angezeigt **Erweitert** . **Hinweis: Mindestlänge Des Passworts** Ist ein Pflichtfeld und es wird empfohlen, es auf mindestens 8 bis 10 Zeichen festzulegen.
Maximale Passwortlänge	Maximale Länge des Passworts. Diese Option wird für alle Voreinstellungen außer angezeigt **Erweitert** . **Hinweis: Maximale Passwortlänge** Ist ein optionales Feld und wird empfohlen, es auf maximal 100 Zeichen festzulegen.
Mindestanzahl der Großbuchstaben	Mindestanzahl von Großbuchstaben im Passwort, von 0 bis 10.
Mindestanzahl der Kleinbuchstaben	Mindestanzahl von Kleinbuchstaben im Passwort, von 0 bis 10.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Mindestanzahl der numerischen Zeichen	Mindestanzahl von Zeichen im Passwort, von 0 bis 10.
Mindestanzahl der Sonderzeichen	Mindestanzahl von Sonderzeichen im Passwort, von 0 bis 10.
Eingeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Wenn Sie beispielsweise „$,!“ eingeben Anwender können nur „$“ und „!“ verwenden. Als Sonderzeichen im Passwort. Es können keine anderen Sonderzeichen verwendet werden, und ein Passwort mit anderen Sonderzeichen ist nicht zulässig.
Ausgeschlossene Sonderzeichen	Lassen Sie einen eingeschränkten Satz von Sonderzeichen ohne Trennzeichen zu. Beispiel: Wenn „@$!“ Ist eingegeben, Anwender dürfen „@“, „$“ und „!“ nicht verwenden können. Als Sonderzeichen in ihren Passwörtern. **Hinweis:** Diese Option ist verfügbar, wenn die Eigenschaft glide.password_policy.use_excluded_special_char aktiviert ist.
Anwenderdaten nicht zulassen	Sie ist aktiviert, um die Anwenderdaten nicht zuzulassen.

6. Geben Sie im Abschnitt Sequenzabgleich an **Schwellenwert Für Sequenzlänge** Und **Schwellenwert Für Wiederholungslänge** .

   Hinweis:

   - Sowohl der Schwellenwert für die Sequenzlänge als auch der Schwellenwert für die Wiederholungslänge können maximal acht Zeichen lang sein. Mit diesen Feldern können Sie schwache Kombinationen von Passwörtern mit vorhersagbaren und sich wiederholenden Sequenzen wie „123456“, „qwerty“, „!@#$%^“, „aaaaa“ usw. einschränken.
   - Für **Standardmäßig Stark** , Die Länge für den Schwellenwert für die Sequenzlänge und den Schwellenwert für die Wiederholungslänge wird als vier Zeichen ausgewählt.

7. In **Testen Sie Ihr Passwort** Geben Sie Ihr Passwort an.
8. Klicken Sie Auf **Testen Sie Ihr Passwort** .
9. Sobald das Passwort gültig ist, klicken Sie auf **Übermitteln** Um das Passwort zu übermitteln.

   Hinweis: Testen Sie Ihr Passwort immer vor dem Senden.

Konfigurieren Sie das Passwort für einen Anwender

Legen Sie das Passwort Ihres Anwenders für die Instanz basierend auf der konfigurierten Passwortrichtlinie fest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Anwender, die zum Festlegen des Passworts für ihre erste Anmeldung erstellt wurden. Weitere Informationen finden Sie unter Erstellen Sie einen Anwender .

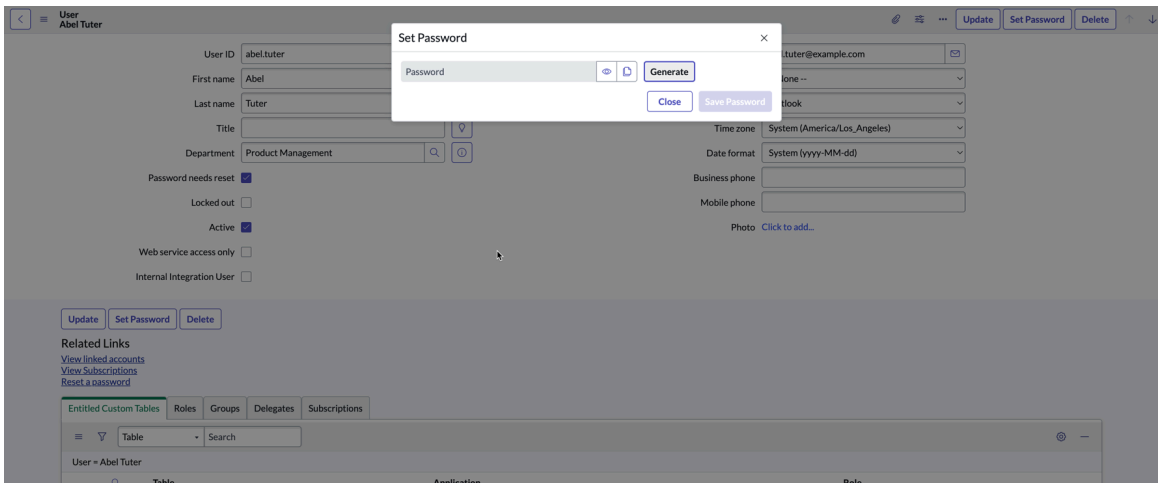
Zum Ausfüllen von **Passwort** Feld direkt im Anwenderformular aktivieren **Aktivieren Sie diese Option, um das Passwortfeld im Formular „sys_user“ anzuzeigen** (glide.user.show.password.field). Weitere Informationen zu den Eigenschaften finden Sie unter Eigenschaften der Passwortrichtlinie.

Erforderliche Rolle: Administrator

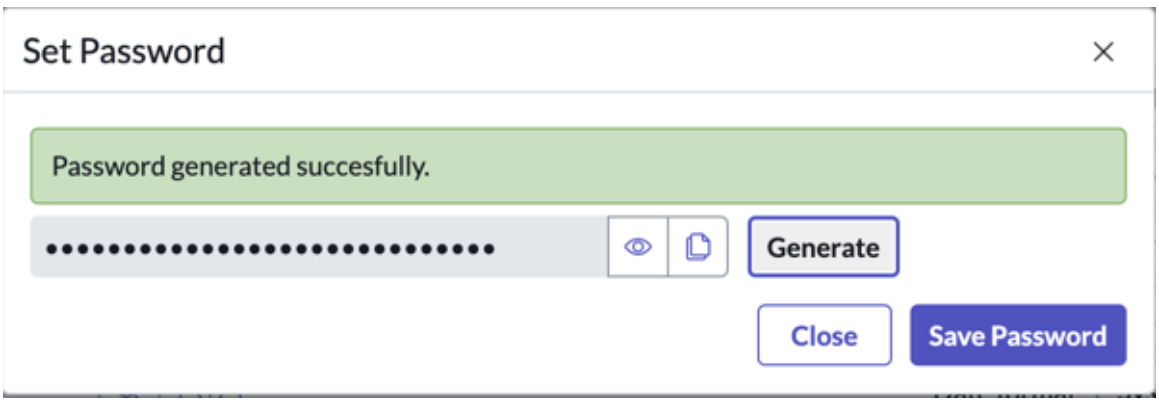
Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.
2. Wählen Sie den Anwender aus der Liste auf der Seite Anwender aus.
3. Um das Passwort basierend auf der Passwortrichtlinie festzulegen, klicken Sie auf **Passwort Festlegen** .

   Das Popup-Fenster Passwort festlegen wird angezeigt.



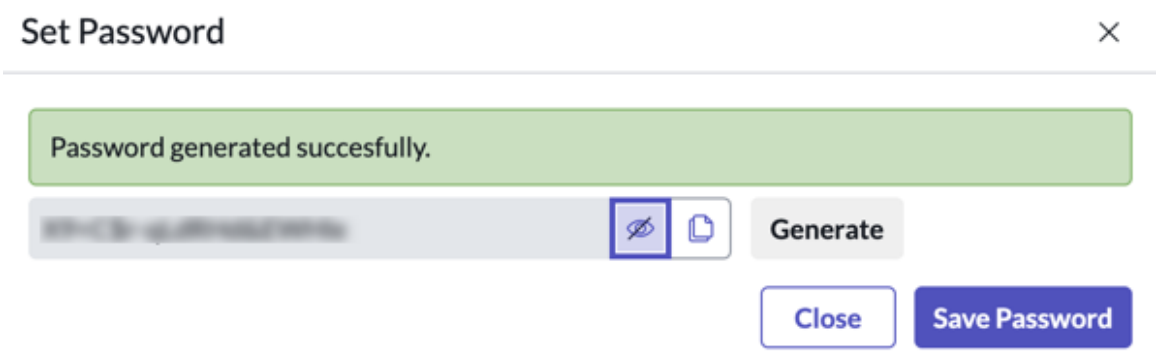
4. Führen Sie im Feld Passwort festlegen die folgenden Schritte aus.
   a. Klicken Sie Auf **Generieren** Zum Generieren des Passworts.



   b. Klicken Sie auf **Anzeigen** Symbol zum Anzeigen des Passworts.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Klicken Sie auf **Kopieren** Symbol zum Kopieren des Passworts, das für den Anwender freigegeben werden soll.



5. Klicken Sie Auf **Passwort Speichern** .

Das Passwort ist für den Anwender festgelegt. Außerdem ist das Kontrollkästchen Passwort benötigt Rest automatisch aktiviert.

Der Anwender muss während der ersten Anmeldung dasselbe Passwort für die Anmeldung verwenden und das Passwort bei der Anmeldung ändern, wobei er die von den Administratoren konfigurierte Passwortrichtlinie einhalten muss.

Schließen Sie Passwörter über Passwortrichtlinien in Ihrer Instanz aus

Fügen Sie der Tabelle „Ausgeschlossenes Passwort“ Passwörter hinzu, um zu verhindern, dass bestimmte Passwörter von Anwendern in Ihrer Instanz verwendet werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können beliebig viele Passwörter sperren. Einige der Beispiele sind:

- Vorhersagbare und sich wiederholende Sequenzen, z. B. „123456“, „qwerty“, „!@#$%^“, „aaaaa“, und so weiter.
- Mitarbeitername oder Anwendernamen.
- Relevante Marken- oder Produktnamen.
- Standorte, z. B. Hauptsitz des Unternehmens, Stadt, Land usw.
- Unternehmensspezifische interne Begriffe oder Abkürzungen.
- Emojis.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Passwortrichtlinie** > **Ausgeschlossene Passwörter**an.
2. Um Ihrer Ausschlussliste ein Passwort hinzuzufügen, klicken Sie auf **Neu** Und geben Sie das Passwort ein.
3. Navigieren zu **Passwortrichtlinie** > **Ausschlusslistenverwaltung** Um das Passwort Ihrer Anwender zu steuern und zu verhindern, dass Anwender ein ungültiges Passwort für die Instanz verwenden.

   Die **Ausschlusslistenverwaltung** Hat etwa 5000 häufig verwendete Passwörter.

Nicht unterstützte Passwortzeichen

Es gibt Passwortzeichen, die nicht unterstützt werden. Anwender können diese Zeichen nicht verwenden, basierend auf ServiceNow Anforderungen an die Passwortkomplexität.

Um eine sichere Netzwerkumgebung zu ermöglichen, müssen Anwender starke Passwörter verwenden, die eine Kombination aus Buchstaben, Zahlen und Symbolen enthalten. Diese Kombinationen helfen, nicht autorisierte Anwender zu verhindern, die normalerweise manuelle oder automatisierte Methoden verwenden, um schwache Passwörter zu erraten.

- Die Anforderungen der Passwortrichtlinie basieren auf der Basic Multilingual Plane (BMP), die Zeichen für alle modernen Sprachen enthält. ServiceNow Die Instanz wird mit BMPs von etwa 10000 Zeichen geliefert.
- Passwortzeichen innerhalb dieser zulässigen BMPs können für Ihre Instanz festgelegt werden. Passwortzeichen, die nicht innerhalb dieser BMPs enthalten, sind nicht zulässig.

Hinweis: Anwender- oder unternehmensspezifische Zeichen, die nicht im Passwort verwendet werden können, können in der Liste „Passwörter ausschließen“ konfiguriert werden.

Weitere Informationen zu den Eigenschaften der Passwortrichtlinie finden Sie unter Eigenschaften der Passwortrichtlinie .

Passwortzurücksetzung

Der standardmäßige Self-Service-Passwortzurücksetzung-Prozess ermöglicht es einem Benutzer, das Passwort ohne Hilfe von Service-Desk-Mitarbeitern zurückzusetzen.

Example: Der standardmäßige Self-Service-Ablauf für das Zurücksetzen des Passworts

1. Wenn sich ein Benutzer nicht an das Passwort erinnert, kann er auf den Link **Passwort vergessen?** auf dem Anmeldebildschirm klicken.
2. Die Anwendung Passwortzurücksetzung wird gestartet. Auf der Seite **Identität** identifiziert sich der Benutzer durch Eingabe eines **Benutzernamens**.
3. Auf der Seite **Überprüfen** weist der Benutzer nach, dass er die Person ist, die mit dem Benutzernamen verknüpft ist. In diesem Beispiel gibt der Benutzer die E-Mail-Adresse ein, die dem Benutzerprofil zugeordnet ist. Der Administrator kann eine andere Überprüfungsmethode konfigurieren oder zusätzliche Überprüfungen erfordern, z. B. eine persönliche Frage, die nur der Benutzer beantworten kann.
4. Auf der Seite **Zurücksetzen** wird der Benutzer angewiesen, die E-Mail auf Anweisungen zu überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Der Benutzer öffnet die E-Mail und klickt auf den Link **Hier**, um das Passwort zurückzusetzen. Der Link ist für einen von Ihnen angegebenen Zeitraum gültig (verwenden Sie **Password_Reset.Request.expiry** Eigenschaft).
6. Die Seite **Passwort zurücksetzen** führt den Benutzer durch den Prozess zum Zurücksetzen des Passworts.

Der standardmäßige Self-Service-Passwortzurücksetzung-Prozess (com.glideapp.password_reset) definiert:

- Den URI, der angibt, wohin Benutzer beim Klicken auf **Passwort vergessen?** umgeleitet werden. Standardmäßig ist dieser Wert **/$pwd_Reset.do?sysparm_url=ss_default** , Der derselbe Wert ist, der in verwendet wird *glide.security.password_reset.uri*Eigenschaft. In früheren Releases wurde dieser Wert auf **/reset_password.do** festgelegt.
- Die Option **URL zum Zurücksetzen des Passworts aktivieren**, die angibt, dass der Benutzer nach dem Klicken auf **Passwort vergessen?** eine E-Mail mit einem Link zum Zurücksetzen des Passworts erhalten sollte.
- Der Überprüfungsablauf „Persönliche Daten – E-Mail-Adresse eingeben“, der den dreischrittigen Prozess für die Passwortzurücksetzung angibt.

Siehe Konfigurieren Sie Ihren Prozess zur Passwortzurücksetzung Anweisungen zum Zugriff auf dieses Formular und zum Konfigurieren der Felder.

Hinweis:

- Diese Funktion steht für lokal authentifizierte Benutzer zur Verfügung, die den in ihrem Benutzerdatensatz angegebenen Benutzernamen und das entsprechende Passwort eingeben. Anwender, die sich über eine SSO-Lösung oder eine LDAP-Integration bei der Instanz anmelden, können Passwörter nicht mithilfe des BeispielSelf-Service zurücksetzen Passwortzurücksetzung Prozess.
- Der Endbenutzer muss die Benachrichtigungseinstellungen aktivieren und konfigurieren. Siehe Abonnementbasierte Benachrichtigungen . Administratoren können x Ändern Sie die E-Mail, die an den Endanwender gesendet wird .

Ändern Sie Passwortzurücksetzung Benachrichtigungs-E-Mail-Text

Anwender des Selfservice Passwortzurücksetzung Prozess erhält eine E-Mail-Benachrichtigung, wenn er die Passwortzurücksetzung anfordert. Sie können den Text der E-Mail und andere Aspekte der Benachrichtigung ändern.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Dieser Prozess ist nur relevant, wenn Anwender dies sind Abonnementbasierte Benachrichtigungen .

Prozedur

1. Navigieren zu **Alle** > **Systembenachrichtigung** > **Benachrichtigungen**an.
2. Wählen Sie aus **URL zur Passwortzurücksetzung** Benachrichtigung.
3. Ändern Sie den Text der E-Mail in **Inhalt** Abschnitt.
   Informationen zum Konfigurieren anderer Aspekte der Benachrichtigung finden Sie unter Erstellen Sie eine E-Mail-Benachrichtigung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Passwortzurücksetzung-Eigenschaften konfigurieren

Sie können Eigenschaften angeben, die die Passwortzurücksetzung-Erfahrung für Endbenutzer konfigurieren.

Vorbereitungen
Erforderliche Rolle: password_reset_admin

Warum und wann dieser Vorgang ausgeführt wird
Es gibt zwar keine Bereichsgrenzen für die Werte, die Sie für Eigenschaften eingeben können, es sollten jedoch nur positive Ganzzahlwerte ab 1 verwendet werden. Wenn Sie den Grenzwert für den oberen Bereich einer Eigenschaft festlegen, müssen Sie die vom Benutzer ausgeführte Aufgabe berücksichtigen.

Sie werden beispielsweise nicht zulassen wollen, dass Benutzer 100 Versuche haben, um ihre Identität zu bestätigen. Ein üblicherer Wert sind 3 Versuche. Ebenso wenig werden Sie wollen, dass Benutzer während des Registrierungsprozesses 30 Sicherheitsfragen auswählen und beantworten müssen. Eine häufiger verwendete Anzahl von Sicherheitsfragen liegt zwischen 5 und 7.

Prozedur

1. Navigieren zu **Alle** > **Passwortzurücksetzung** > **Eigenschaften**an.
   Für Informationen zum Passwortzurücksetzung Eigenschaften, siehe Passwortzurücksetzung Globale Eigenschaften an.
2. Aktualisieren Sie die Einstellungen nach Bedarf, und klicken Sie dann auf **Speichern**.

Anwendernamen speichern

Wenn **Merken Sie sich** Das Kontrollkästchen ist bei der Anmeldung aktiviert, ein Cookie wird auf dem Computer des Anwenders gespeichert. Dieses Cookie authentifiziert den Anwender bei nachfolgenden Besuchen automatisch.

Wenn sich der Anwender abmeldet, wird das Cookie gelöscht. Der Standardwert von **Merken Sie sich** Das Kontrollkästchen wird von einer Eigenschaft gesteuert, und ob das Kontrollkästchen auf der Anmeldeseite angezeigt wird oder nicht, wird durch eine andere Eigenschaft gesteuert.

Zwei Eigenschaften, `glide.ui.user_cookie.life_span_in_days`Und `glide.ui.user_cookie.max_life_span_in_days`Steuern Sie den vom System „Glide_user“ generierten Cookie-Ablaufwert. Wenn ein Benutzer auf eine Instanz mit aktiviertem „Benutzernamen speichern“ zugreift, wird der Ablaufzeitraum für Cookies durch den Zugriff zurückgesetzt, bis der maximale (glide.ui.user_cookie.max_life_span_in_days) Grenzwert für die Lebensdauer erreicht ist.

Hinweis: Weitere Informationen zu diesen Eigenschaften finden Sie in den folgenden Themen in Instanzsicherheitshärtungseinstellungen:

- Absolute Sitzungszeitüberschreitungsdauer minimieren [aktualisiert in Security Center 1,3]
- Zeitüberschreitungsdauer des Sitzungsfensters minimieren [aktualisiert in Security Center 1,3]

Standardwert des Kontrollkästchens „Anwendernamen speichern“ ändern

Sie können den Standardwert von ändern **Merken Sie sich** Kontrollkästchen.

Vorbereitungen
Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **UI-Eigenschaften**an.
2. Suchen Sie nach *Default value of "Remember me" checkbox on login page*Eigenschaft (*glide.ui.remember.me.default*).
3. Zum Festlegen des Standardwerts von **Merken Sie sich** Kontrollkästchen für **Nein** , Deaktivieren Sie das Kontrollkästchen für die Eigenschaft.
4. Um den Standardwert von wiederherzustellen **Merken Sie sich** Kontrollkästchen für **Ja** , Aktivieren Sie das Kontrollkästchen Eigenschaft.

Kontrollkästchen „Anwendernamen speichern“ entfernen

Sie können entfernen **Merken Sie sich** Kontrollkästchen, damit Anwender keinen Zugriff auf diese Funktion haben.

Vorbereitungen

Erforderliche Rolle: security_admin

Hinweis: Weitere Informationen zu dieser Eigenschaft finden Sie unter Entfernen Sie „mich speichern“ In Instanzsicherheitshärtungseinstellungen.

Prozedur

1. Erhöhen Sie Ihre Rolle auf Security_admin.
2. Navigieren zu **Systemeigenschaften** > **UI-Eigenschaften**an.
3. Suchen Sie nach *Remove "Remember me" checkbox from login page*Eigenschaft (*glide.ui.forgetme*).
4. Aktivieren Sie das Kontrollkästchen für die Eigenschaften.
   Mit dieser Einstellung wird entfernt **Merken Sie sich** Kontrollkästchen, löscht vorhandene Cookies für ungültig und deaktiviert die Funktion „mich speichern“ vollständig.
5. Um wiederherzustellen **Merken Sie sich** Kontrollkästchen zur Anmeldeseite deaktivieren Sie das Kontrollkästchen für die Eigenschaft.

Konfigurieren Sie die Eingabeaufforderung zur Bestätigung der Abmeldung

Sie können eine Eingabeaufforderung zur Bestätigung der Abmeldung aktivieren, um zu verhindern, dass sich Anwender versehentlich abmelden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Das folgende Verfahren funktioniert nur in UI-Versionen vor Core-UI, Das ist die neueste und am häufigsten verwendete.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **System**an.
2. Suchen Sie nach **Fordern Sie den Anwender auf, eine Abmeldeanforderung zu bestätigen** Eigenschaft, und aktivieren Sie das Kontrollkästchen.
3. Wenn der Anwender auf klickt **Melden Sie Sich Ab** Schaltfläche, wird ein Bestätigungsdialogfeld angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Implementieren Sie eine Nonce

Sie können eine Nonce für die Single Sign-on-Digest-Authentifizierung implementieren.

Um eine Nonce mit den unverschlüsselten Token- oder verschlüsselten Tokenmethoden von Single Sign-on zu verwenden, gelten diese Schritte mit nur wenigen geringfügigen Änderungen.

Hinweis: Die Nonce wird nur für Anmeldeanforderungen verwendet, nicht für andere Anforderungstypen. Wenn das System nach der Anmeldung einen Nonce-Wert erhält, wird der Nonce-Wert nicht verbraucht.

Vorteile

Die Verwendung einer Nonce verhindert, dass ein böswilliger Anwender einen Wiedergabeangriff ausführt, um sich bei Ihrem System anzumelden.

Nonce-Prozess-Flow

Wenn ein Kunde das verarbeitete Token Single Sign-on implementiert hat und die Sicherheit einer Nonce hinzufügen möchte, folgt er einem bestimmten Prozess-Flow.

1. Ein Anwender meldet sich beim Portal des Kunden an.
2. Der Kunde generiert die erforderlichen SSO-Parameter und fügt eine zufällige Nonce an das Ende an Wenn der Kunde beispielsweise die Authentifizierungsantwort über die Abfragezeichenfolge weiterleitete, kann dies wie folgt aussehen:

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

Die Instanz empfängt diese Anforderung und ruft die Authentifizierungsvariablen ab. Bevor versucht wird, die Integrität der Authentifizierungsantwort zu überprüfen, überprüft die Instanz die Nonce anhand einer internen Tabelle (u_authentication_nonce), um sicherzustellen, dass sie noch nicht vorhanden ist. Wenn die Nonce in dieser Tabelle nicht vorhanden ist, wird die Nonce der Tabelle hinzugefügt, und der Authentifizierungsprozess kann fortgesetzt werden. Wenn dieser Nonce-Wert jedoch bereits in der Tabelle vorhanden ist, wird der Authentifizierungsversuch abgebrochen und ein Fehlercode wird angezeigt `Failed_missing_Request` Wird zurückgegeben, wodurch der Anwender normalerweise zur Anmeldeseite zurückkehrt.

Implementieren Sie eine Nonce

Fügen Sie dem Authentifizierungsheader eine kryptografische Nonce hinzu, um sicherzustellen, dass sie nur einmal verwendet werden kann.

- Erstellen Sie eine Systemeigenschaft namens *`glide.authenticate.header.nonce_key`*Und legen Sie den Wert auf den Variablennamen fest, den Sie für die Nonce verwenden, z. B. NONCE oder NCE.
- Erstellen Sie eine neue Tabelle mit dem Namen `u_authentication_nonce` . Fügen Sie der Tabelle mit dem Namen ein Feld hinzu `u_nonce` .
- Gehe zu **Systemeigenschaften** > **Installationsausgänge** Und erstellen Sie ein Element mit dem Namen `DigestSingleSignOnNonce` Welche ExternalAuthentication überschreibt (*`glide.authenticate.external_property`*).
- Fügen Sie dem Skriptteil des neu erstellten DigestSingleSignOnNonce den folgenden Code hinzu.

```
gs.include("PrototypeServer");
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {

 process : function() {

  var headerKey = GlideProperties.get("glide.authenticate.header.key", "SM_USER");
  var headerDigestKey = GlideProperties.get("glide.authenticate.header.encrypted_key",
 "DIGEST");
  var headerNonceKey = GlideProperties.get("glide.authenticate.header.nonce_key", "NCE");
  var fieldName = GlideProperties.get("glide.authenticate.header.value", "user_name");
  var fkey = GlideProperties.get("glide.authenticate.secret_key");

  // Look in the Headers
  var data = request.getHeader(headerKey);
  var encdata = request.getHeader(headerDigestKey);
  var nonce = request.getHeader(headerNonceKey);

  // If not, then check the URL Parameters
  if (data == null || encdata == null || nonce == null) {
   data = request.getParameter(headerKey);
   encdata = request.getParameter(headerDigestKey);
   nonce = request.getParameter(headerNonceKey);
  }

  // then maybe its a cookie
  if (data == null || encdata == null || nonce == null) {
   var cookies = request.getCookies();
   data = GlideCookieMan.getCookieValue(cookies, headerKey);
   encdata = GlideCookieMan.getCookieValue(cookies, headerDigestKey);
   nonce = GlideCookieMan.getCookieValue(cookies, headerNonceKey);
  }

  // if found run encryption
  if (data != null && encdata != null && nonce != null) {
   try {

    // Replace all spaces with plus(+)'s, converted in url
    encdata = encdata.replaceAll(' ', '+');

    // ----- Encrypt the username|nonce
    var key = this.getDigest( data + "|" + nonce, fkey);

    // Check for match of received encoded data
    // and your encoding of user name
    if (encdata == key) {
     var ugr = new GlideRecord("sys_user");
     ugr.initialize();
     if (!ugr.isValidField(fieldName)) {
      GlideLog.warn("External authorization is set to use field: '"+ fieldName + "' which doesn't
 exist");
      return "failed_missing_requirement";
     }
     ugr.addQuery(fieldName, data);
     ugr.query();
     if (!ugr.next()) {
      var userLoad = GlideUser.getUser(data);
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    if (userLoad == null)
     return "failed_authentication";

    ugr.initialize();
    ugr.addQuery(fieldName, data);
    ugr.query();
    if (!ugr.next())
     return "failed_authentication";

   }

   if (this.processNonce(nonce)){
    var userName = ugr.getValue("user_name");
    return userName;
   }
   else return "failed_missing_requirement";
   }
  else {

   return "failed_authentication";
  }
 } catch(e) {
  gs.log(e);
  return "failed_authentication";
 }
 // Encoded data didn't match recieved Encoded data
} else {

 return "failed_missing_requirement";
}
},

getDigest : function( data, fkey ) {
 try {
  // default to something JDK 1.4 has
  var MAC_ALG = "HmacSHA1";
  return SncAuthentication.encode(data, fkey, MAC_ALG);

 } catch (e) {
  gs.log(e.toString());
  throw 'failed_missing_requirement';
 }
} ,

processNonce : function( sentNonce ) {
 var ngr = new GlideRecord("u_authentication_nonce");

 ngr.addQuery("u_nonce", sentNonce);
 ngr.query();
 if (ngr.next()) {
  gs.log("This SSO entry has already been processed! (Nonce: " + sentNonce + ")");
  return false;
 }
 var ngrNew = new GlideRecord("u_authentication_nonce");
 ngrNew.initialize();
 ngrNew.u_nonce = sentNonce;
 ngrNew.insert();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 gs.log("Inserted new nonce: " + sentNonce);
 return true;
 }
};
```

- Sobald Sie Ihren neuen Installationsausgang gespeichert haben, wechseln Sie zum Installationsausgang von DigestSingleSignOn, und stellen Sie sicher, dass aktiv = falsch festgelegt ist.

Ihre Instanz sollte jetzt so konfiguriert werden, dass eine Nonce implementiert wird.

Multi-Faktor-Authentifizierung

Erfahren Sie, wie Sie die Multifaktor-Authentifizierung (MFA) aktivieren, verwenden und konfigurieren.

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von MFA.	Erfahren Sie, wie MFA aktiviert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden



MFA verwenden.

MFA mit Single Sign-on (SSO)



Erfahren Sie, wie MFA mit Single Sign-on (SSO) konfiguriert wird.

Durchsetzung der Multifaktor-Authentifizierung

Durchsetzung von MFA für nicht-SSO-Anmeldungen bei ServiceNow Aus dem Yokohama-Release.

MFA erhöht die Sicherheit, indem Anwender während der Anmeldung zwei oder mehr Nachweise zum Nachweis ihrer Identität vorlegen müssen. MFA schützt Accounts vor Bedrohungen wie Phishing und Kontoübernahmen.

MFA ist ein kritisches Sicherheitstool gegen verschiedene Angriffe im Zusammenhang mit Identitätsübernahmen. ServiceNow Erzwingt MFA standardmäßig nach dem Yokohama-Upgrade und macht sie für nicht-SSO-Anmeldungen obligatorisch (Anwender, die sich nur mit Anwendernamen und Passwort oder LDAP-basierter Authentifizierung anmelden), um eine bessere Sicherheitslage zu gewährleisten und das Risiko von Verstößen zu reduzieren.

Die MFA-Durchsetzung erfolgt über eine MFA-Richtlinie, die standardmäßig von Yokohama oder einem Upgrade auf Yokohama aktiviert ist.

Hinweis:

- Die Richtlinie ist für alle aktiviert **Nicht-snc_external** Benutzer, die eine lokale (Anwendername und Passwort) oder LDAP-basierte Authentifizierung durchführen.
- Der Instanzadministrator kann den Durchsetzungsumfang ändern, indem er die MFA-Kontextrichtlinie, Richtlinienkriterien oder Richtlinienbedingungen ändert.

Hier sind weitere Details zur MFA-Durchsetzung:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für alle Produktions- und nicht-Produktionsinstanzen erzwungen.
- Wird für alle erzwungen **Nicht-snc_external** Anwender und **Nicht-SSO** Melden Sie sich an.
- Für die Integration mit Standardauthentifizierung und Anmeldeinformationen für das Passwort des OAuth-Ressourcenbesitzers ist keine MFA von Yokohama erforderlich.

Weitere Informationen zu den Changes aufgrund der Durchsetzung finden Sie unter Änderungen aufgrund der Multifaktor-Authentifizierung.

Weitere Informationen zu MFA finden Sie unter Multifaktor-Authentifizierung erkunden.

Zugehörige Informationen

Multifaktor-Authentifizierung wird konfiguriert

Multifaktor-Authentifizierung wird verwendet

Eigenschaften der Durchsetzung der Multifaktor-Authentifizierung

Fehlerbehebung bei der Durchsetzung der Multifaktor-Authentifizierung

Häufig gestellte Fragen – Durchsetzung der Multifaktor-Authentifizierung

Änderungen aufgrund der Multifaktor-Authentifizierung

Informationen zu den Changes, die aufgrund der MFA-Durchsetzung erwartet werden.

MFA-Durchsetzungsänderungen, die wie folgt erwartet werden:

- Keine Auswirkung auf die Integration.
- Anwender, die MFA bereits registriert haben, werden während der lokalen Anmeldung weiterhin mit MFA herausgefordert.
- Wenn ein Anwender MFA noch nicht eingerichtet hat, wird er nach dem Yokohama-Upgrade zunächst für einen bestimmten Zeitraum von der MFA befreit, in dem er MFA registrieren kann.
- Wenn der Anwender sich nicht selbst registrieren kann, wird nach Abschluss des Befreiungszeitraums (Standard: 30 Tage) MFA erzwungen und muss MFA einrichten.
- Nach 90 Tagen wird MFA standardmäßig erzwungen. Für Erstanmeldungen nach 90 gibt es keinen Zeitraum für die Selbstregistrierung. Administratoren können diesen Zeitraum konfigurieren.

Als Administrator können Sie sich auf die MFA-Durchsetzung vorbereiten, indem Sie Folgendes ausführen:

- Überprüfen Sie die Konfiguration der MFA-Kontextrichtlinie, und passen Sie die Richtlinienbedingungen an Ihre Geschäftsanforderungen an.
- Fügen Sie die standardmäßig bereitgestellte ausgenommene Gruppe hinzu, wenn andere Anwender befreit werden müssen.
- Überprüfen Sie die MFA-Durchsetzungseigenschaften, und passen Sie sie entsprechend Ihren Anforderungen an. Weitere Informationen finden Sie unter Eigenschaften der Durchsetzung der Multifaktor-Authentifizierung.

Example: MFA-Durchsetzungsszenario nach 30 Tagen der MFA-Durchsetzung

- **Szenario 1 für Acme Corp** : In der Instanz, wenn der Anwender keine aktive MFA-Richtlinie hat. Stellen Sie sich vor, dass Sarah lokale Authentifizierung verwendet, um auf eine Instanz zuzugreifen. Beim Upgrade auf das Yokohama-Release während der Anmeldung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird eine Meldung zur Registrierung bei MFA angezeigt. Es gibt 30 Tage, um dieses Setup abzuschließen. Wenn Sarah das Setup nach 30 Tagen nicht abschließt, erfordert das Konto die Anmeldung von MFA und kann erst dann darauf zugreifen, wenn MFA eingerichtet wurde.

- **Szenario 2 für Acme Corp** : In der Instanz war Anita bereits MFA zusammen mit lokaler Authentifizierung. Anita erfordert weiterhin MFA ohne das 30-tägige Selbstregistrierungsfenster.
- **Szenario 3 für Acme Corp** : In der Instanz verwendet Olivia Single Sign-on (SSO) für die Authentifizierung. Es gibt keine Auswirkungen auf die Anmelde-Experience, und Olivia wird für MFA nicht erzwungen.
- **Szenario 4 für Globex Corp** : In der Instanz, wenn ein Anwender bereits über eine MFA-Richtlinie verfügt, die MFA für alle lokalen Anmeldeversuche außerhalb des vertrauenswürdigen Netzwerks des Unternehmens vorschreibt. Beim Upgrade auf Yokohama oder ein späteres Release bleibt das MFA-Durchsetzungsverhalten für Anwenderanmeldungen unverändert.

Eigenschaften der Durchsetzung der Multifaktor-Authentifizierung

Konfigurieren Sie die Eigenschaften für die MFA-Durchsetzung von Yokohama, und führen Sie ein Upgrade auf Yokohama durch.

Um die MFA-Durchsetzungseigenschaften festzulegen, navigieren Sie zu **sys_properties.list** Dient zum Validieren oder Ändern der MFA-Durchsetzungseigenschaften.

MFA-Durchsetzungseigenschaften

Feld	Beschreibung
glide.authenticate.multifactor.setup.bypass.count	Anzahl der Fälle, in denen ein Anwender das Einrichten der Multifaktor-Authentifizierung umgehen kann (maximal können 3 umgangen werden, danach wird die Anzahl als 3 behandelt).
glide.authenticate.multifactor.self_enrollment.period	Gibt die Anzahl der Tage an, an denen ein Anwender die Möglichkeit erhält, sich selbst für MFA zu registrieren, nach der der Anwender automatisch mit MFA herausgefordert wird. Jeder Wert, der 90 überschreitet, wird nur als 90 Tage behandelt.
glide.authenticate.multifactor.enforcement.max_validation_period	Gibt die maximale Anzahl von Tagen an, für die ein neuer Anwender die Option zur Selbstregistrierung für MFA erhält. Nach dieser Option werden alle Anmeldungen neuer Anwender, die nicht-SSO-Anmeldungen ausführen, automatisch mit MFA abgefragt. Jeder Wert, der 270 überschreitet, wird nur als 270 Tage behandelt.
glide.authenticate.multifactor.enforcement.debug	Debug-Protokollierung für MFA-Durchsetzung. Hilft beim Debugging der Flows für MFA-Anmeldungen. **Hinweis:** Diese Eigenschaft ist in der Instanz nicht vorhanden. Sie müssen die Eigenschaft bei Bedarf erstellen und aktivieren.
glide.authenticate.hybrid_user_tracking.enabled	Eigenschaft für die Nachverfolgung von Hybridanwendern. Die Anwenderaccounts, die im entsprechenden sys_user-Datensatz nicht als

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA-Durchsetzungseigenschaften (Fortsetzung)

Feld	Beschreibung
	„nur Webservice-Zugriff“ markiert sind, aber dennoch Integrationen (z. B. API-Anmeldungen) mit Anwendername und Passwort durchführen, werden in der Tabelle „Anwenderanmeldeinformationen“ nachverfolgt, wenn diese Eigenschaft aktiviert ist. **Hinweis:** Diese Eigenschaft ist in der Instanz nicht vorhanden. Sie müssen die Eigenschaft bei Bedarf erstellen und aktivieren.
`glide.authenticate.hybrid_user_tracking.debug`	Ein Debug-Protokollierungsprotokoll für die Nachverfolgung von Hybrid-Anwender-API-Anmeldungen.Side **Hinweis:** Diese Eigenschaft ist in der Instanz nicht vorhanden. Sie müssen die Eigenschaft bei Bedarf erstellen und aktivieren.

Fehlerbehebung bei der Durchsetzung der Multifaktor-Authentifizierung

Informationen zur Fehlerbehebung aufgrund der MFA-Durchsetzung.

ServiceNow Erzwingt MFA standardmäßig nach dem Yokohama-Upgrade und macht sie für nicht-SSO-Anmeldungen obligatorisch (Anwender, die sich nur mit Anwendernamen und Passwort oder LDAP-basierter Authentifizierung anmelden), um eine bessere Sicherheitslage zu gewährleisten und das Risiko von Verstößen zu reduzieren.

Die MFA-Durchsetzung erfolgt über eine MFA-Richtlinie, die standardmäßig von Yokohama oder einem Upgrade auf Yokohama aktiviert ist. Im Folgenden finden Sie einige der Problembehandlungsaufgaben, die Sie ausführen können, wenn sich das MFA-Verhalten ändert:

- Debuggen Sie mit den Tools zur Fehlerbehebung
- Navigieren Sie zu den Eigenschaften Protokollspeicherort und Debugging
- Verstehen Sie die MFA-Szenarien basierend auf Ihrer Anwender-Experience bei der Verwendung von MFA
- Machen Sie sich mit dem MFA-Problem vertraut, das aufgrund eines Upgrades von einem vorherigen Release aufgetreten ist

MFA debuggen

Verwenden Sie eines der folgenden Tools oder eine Kombination, um die Debug-Informationen zu verstehen:

- **Splunk** – Zum Anzeigen der Debug-Protokolle.
- Systemprotokolle oder Knotenprotokolle.
- **HAR** Protokolle zum Analysieren der Debug-Protokolle für die MFA.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollspeicherort und Debugging-Eigenschaften

Navigieren Sie zum folgenden Speicherort, um mehr über Protokolle zu erfahren:

- Navigieren Sie zu für Systemprotokolle **Alle** > **Systemprotokoll** > **Systemprotokolle**an.
- Navigieren Sie für Knotenprotokolle zu **Alle** > **Systemprotokolle** > **Dienstprogramme** > **Knoten-Protokolldateibrowser**an.

Die System-Debug-Protokolle und Instanzknotenprotokolle sind für den Debug-Zweck erforderlich. Im Folgenden sind die Debug-Eigenschaften aufgeführt, die aktiviert werden müssen:

- glide.webauthn.debug.enabled
- glide.log.default_log_debug
- glide.authenticate.policy.debug
- glide.authenticate.hybrid_user_tracking.debug

MFA-Problem basierend auf Szenarien

Szenario 1: Der Anwender kann sich mit keinem seiner zweiten Faktoren anmelden

Setzen Sie die MFA für Ihre Anwender zurück, und löschen Sie die alten Anwenderdatensätze aus den folgenden Tabellen:

- User_Multifactor_auth
- sys_user_public_credential
- sys_user_Multi_factor_Setup

Szenario 2: Der Administrator kann sich mit keinem seiner zweiten Faktoren anmelden

Ein anderer Anwender mit Administratorzugriff kann die MFA für jeden blockierten Administratoranwender zurücksetzen. Wenn das Problem weiterhin besteht, wenden Sie sich an ServiceNow Support.

Scenario3: Fehler, der während des MFA-Setups oder der Validierung beobachtet wurde

Überprüfen Sie die Warnung „zugeordnete Fehlercodes/Warnung: Ihr sechsstelliger Verifizierungscode ist falsch. Versuchen Sie es erneut mit dem richtigen Code.“

Führen Sie die nachfolgenden Schritte durch:

- Wenn bei der TOTP-Authentifikator-App Datum und Uhrzeit des Authentifikator-MFA-Geräts und der Instanz nicht synchronisiert sind (±30 Sek.), wird der TOTP-Code nicht akzeptiert. Überprüfen Sie das Datum und die Uhrzeit des Geräts und der Instanz.
- Konfigurieren Sie im Fall von E-Mails die Benachrichtigung auf Anwenderebene, die Konfiguration ausgehender E-Mails und den Anwender richtig in der sys_user Tabelle.
- Konfigurieren Sie im Falle von SMS die Integration von Twillio oder einem anderen SMS-Service Provider ordnungsgemäß, und legen Sie sie auf „aktiv“ fest. Überprüfen Sie, ob die Mobiltelefonnummer des Anwenders in korrekt konfiguriert ist sys_user Tabelle.

Häufig gestellte Fragen – Durchsetzung der Multifaktor-Authentifizierung

Details zu einigen der FAQs, die aufgrund der MFA-Durchsetzung durchgeführt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA ist ein kritisches Sicherheitstool gegen verschiedene Angriffe im Zusammenhang mit Identitätsübernahmen. ServiceNow Erzwingt MFA standardmäßig nach dem Yokohama-Upgrade und macht es für nicht-SSO-Anmeldungen obligatorisch (Anwender, die sich nur mit Anwendername und Passwort oder LDAP-basierter Authentifizierung anmelden).

Die MFA-Durchsetzung erfolgt über eine MFA-Richtlinie, die standardmäßig von Yokohama oder einem Upgrade auf Yokohama aktiviert ist. Sie können die folgenden Links überprüfen, um mehr über Fragen zur MFA-Durchsetzung zu erfahren:

- MFA-Durchsetzungsausnahme
- MFA-Durchsetzungsanforderungen – Was und warum
- MFA-Durchsetzungsumfang
- Zeitleiste für MFA-Durchsetzung
- MFA-Metriken
- MFA-Typen
- MFA-Zurücksetzung

MFA-Durchsetzungsanforderungen – Was und warum

Häufig gestellte Fragen zur MFA-Durchsetzung und warum dies wichtig ist.

1. Was ist die MFA?

   Multifaktor-Authentifizierung (MFA) ist ein Sicherheitsprozess, bei dem Sie mindestens zwei Verifizierungsarten bereitstellen müssen, bevor sie auf ein Konto oder System zugreifen können. Weitere Informationen finden Sie unter Multifaktor-Authentifizierung erkunden.

2. Warum ist das MFA-Durchsetzungsmandat?

   MFA ist zum Schutz Ihrer Account- und Datensicherheit erforderlich. Cyberbedrohungen ändern sich ständig, und Passwörter allein bieten keinen ausreichenden Schutz vor nicht autorisiertem Zugriff mehr.

   - Wenn MFA aktiviert ist, benötigen die Angreifer auch dann, wenn sie über Ihr Passwort verfügen, noch eine zweite Form der Verifizierung. Diese zusätzliche Ebene blockiert die meisten nicht autorisierten Versuche erheblich, sodass Ihre Informationen sicherer bleiben.
   - Wenn Sie MFA als Standard festlegen, minimieren Sie das Risiko von Sicherheitsverletzungen, und schützen Sie Ihr Konto automatisch. Dies bedeutet, dass Sie mehr Sicherheit erhalten, ohne zusätzliche Sicherheitsentscheidungen treffen zu müssen.

3. Warum ist es wichtig, MFA zu aktivieren?

   Das Aktivieren von MFA erhöht die Sicherheit Ihres Accounts. Passwörter allein reichen nicht aus, da Passwörter bei Datenschutzverletzungen offengelegt werden können. Mit MFA kann jemand ohne einen zweiten Verifizierungsschritt nicht auf Ihren Account zugreifen, auch wenn jemand Ihr Passwort kennt.

4. Warum ServiceNow MFA benötigen?

   ServiceNow Verpflichtet MFA, Sie vor diesen Bedrohungen zu schützen. Dies ist eine einfache, aber effektive Möglichkeit, nicht autorisierte Zugriffe zu reduzieren. Durch die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderung von MFA gibt es für jeden Account eine starke Schutzebene, wodurch die Sicherheitsrisiken für Sie und alle Anwender reduziert werden.

5. Was ist die MFA-Anforderung für Bestandskunden?

   Für Bestandskunden, die ihre Instanz auf Yokohama oder ein späteres Release aktualisieren:

   - Wenn die Instanz nicht bereits über verfügt **Adaptive Authentifizierung** – Multifaktor-Authentifizierungskontext Wenn diese Option aktiviert ist, wird sie automatisch als Standard-MFA-Richtlinie aktiviert.
   - Alle internen Anwender (Anwender, die nicht über die Rolle „snc_external“ verfügen), die sich mit lokaler oder LDAP-Authentifizierung anmelden, müssen MFA innerhalb von 30 Tagen nach ihrer ersten erfolgreichen Anmeldung einrichten. Während dieser Zeit können Sie sich normal anmelden, aber zum Zeitpunkt der Anmeldung wird eine Meldung angezeigt, um sich bei MFA zu registrieren.
   - Nach 30 Tagen ist MFA standardmäßig erforderlich, und Anwender können sich nicht anmelden, ohne das MFA-Setup abzuschließen.

6. Was ist die MFA-Anforderung für neue Kunden?

   Für alle Instanzen, die das Yokohama-Release oder höher verwenden, ist MFA standardmäßig für alle internen Anwender aktiviert. Dies gilt auch für Anwender, die nicht über verfügen `snc_external` Rollen und melden sich mit lokaler oder LDAP-Authentifizierung an. Ab der ersten Anmeldung müssen die Anwender MFA einrichten und verwenden.

MFA-Durchsetzungsumfang

Häufig gestellte Fragen zum MFA-Durchsetzungsumfang und warum dies wichtig ist.

1. Welche Anwender-, Anmelde- und Umgebungstypen erfordern MFA?

   Ab dem Yokohama-Release mit der neuen standardmäßigen sicheren MFA-Richtlinie MFA für die folgenden Szenarien erzwungen:

   - Alle Anwender außer den Anwendern haben **snc_external** Rolle.
   - Alle Anwender, die eine lokale Authentifizierung oder LDAP-Authentifizierung (Lightweight Directory Access Protocol) mit Anwendernamen und Passwort durchführen.
   - Alle Kundeninstanzen, einschließlich Produktions-, Subprod- und Testinstanzen, die vor dem Upgrade noch keine aktive MFA-Richtlinie hatten.

   Der Instanzadministrator kann den Durchsetzungsumfang ändern, indem er die MFA-Kontextrichtlinie, Richtlinienkriterien oder Richtlinienbedingungen ändert.

2. Ist MFA für Single-Sign-on (SSO)-Anmeldungen erforderlich?

   Nein Mit der standardmäßigen sicheren MFA-Richtlinie ist MFA für die SSO-Anmeldung (SAML, OIDC, zertifikatbasierte Authentifizierung) nicht erforderlich.

   Kunden können mit ihrem Single Sign-on (SSO)-Anbieter (Identitätsanbieter oder IdP) zusammenarbeiten, um Multifaktor-Authentifizierung (MFA) auf der IdP-Seite zu erzwingen. Wenn die Durchsetzung von MFA auf der IdP-Seite nicht möglich ist, haben Kunden auch die Möglichkeit, zu aktivieren ServiceNow MFA der Plattform für SSO-Anmeldungen, indem Sie die Anweisungen in befolgen Multifaktor-Authentifizierung mit Single Sign-on.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ist MFA für externe Anwender erforderlich?

   Nein Mit der standardmäßigen sicheren MFA-Richtlinie ist MFA für Anwender mit der Rolle „snc_external“ nicht erforderlich.

   - Administratoren können dieses Verhalten ändern und MFA für externe Anwender erzwingen, indem sie die MFA-Richtlinienbedingungen aktualisieren.
   - Externe Anwender, die vor dem Upgrade auf Yokohama oder höher bereits eine MFA durchlaufen haben, haben weiterhin MFA.
   - Externe Anwender können ihr Profil aufrufen und sich selbst für MFA registrieren.

4. Ist MFA für die Anmeldung bei der Mobile-App erforderlich?

   Ja. Die MFA-Richtlinie wird auf die Anmeldung in der Web- und Mobile-App mit Anwendernamen und passwortbasierter nicht-SSO-Anmeldung angewendet.

5. Ist MFA für nicht-Produktions- und Testumgebungen erforderlich?

   Ja. MFA wird für alle Kundeninstanzen erzwungen, einschließlich Produktions-, nicht-Produktions-, Entwicklungs- und Testumgebungen. wenn auf der Instanz keine aktive MFA-Richtlinie vorhanden war, bevor ein Upgrade auf Yokohama oder höher durchgeführt wurde.

6. Ist MFA für Entwicklerinstanzen erforderlich?

   Ja. MFA wird für alle Entwicklerinstanzen erzwungen, die sich in Yokohama oder höher befinden.

7. Ist MFA für die API-Authentifizierung erforderlich?

   Nein Ab Yokohama oder einem späteren Release ist MFA nur für Anwendernamen- und passwortbasierte interaktive Anwenderanmeldungen erforderlich. Dies bedeutet API-Authentifizierung mit Standardauthentifizierung mit Arbeit ohne MFA. Kunden werden empfohlen, alternative sichere API-Authentifizierungsmethoden wie OAuth oder mTLS zu verwenden. Weitere Details finden Sie hier.

   a. Klon

   b. Update-Satz-Abruf

   c. RPA

8. Gibt es Auswirkungen auf den Klon-Setup-Prozess aufgrund von MFA?

   Nein, der Klon-Setup-Prozess funktioniert weiterhin mit Anwendername und Passwort und erfordert keine MFA.

9. Gibt es Auswirkungen auf den Abruf des Update-Satzes aufgrund von MFA?

   Nein, der Update-Satz-Abruf funktioniert weiterhin mit Anwendername und Passwort und erfordert keine MFA.

10. Gibt es Auswirkungen auf RPA-Bots, auf die zugegriffen wird ServiceNow Instanzen?

    Ja, wenn der RPA-Bot den interaktiven Anwendernamen und die Passwortanmeldung für den Zugriff auf verwendet ServiceNow Instanz, muss MFA ausgeführt werden. Administratoren können RPA-Bot-Accounts zu hinzufügen **Von MFA befreite Anwendergruppe** Wenn sie MFA für RPA-Bot-Accounts lockern möchten.

11. Ist MFA für die OAuth-basierten Integrationen erforderlich?

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die OAuth-Ressourcenbesitzer-Passwortanmeldeinformationen (ROPC) funktionieren mit Anwendername und Passwort, ohne MFA zu erfordern. Für Autorisierungscode ist der Gewährungstyp MFA als Teil des Anwenderanmelde-Flows erforderlich, bevor die OAuth-Zustimmung erteilt wird.

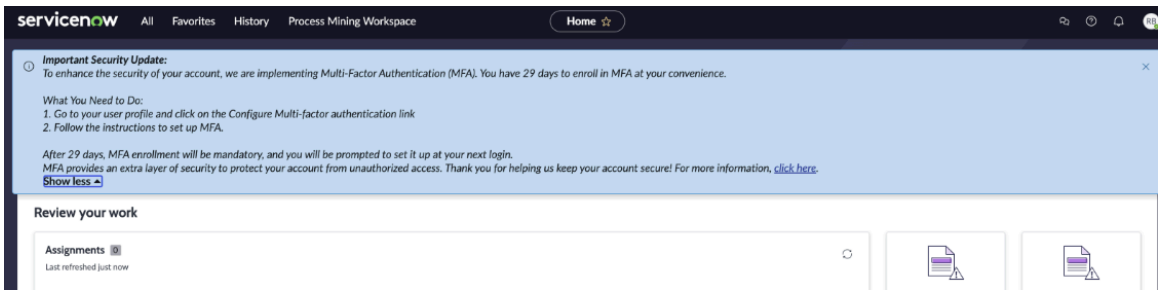
Zeitleiste für MFA-Durchsetzung

Häufig gestellte Fragen im Zusammenhang mit Zeitleisten für die MFA-Durchsetzung und warum dies wichtig ist.

1. Wann wird MFA erzwungen?

Gemäß der MFA-Richtlinie haben berechtigte Anwender, die das MFA-Setup nicht abgeschlossen haben, einen 30-tägigen Selbstregistrierungszeitraum. Das Verhalten wird mithilfe der Systemeigenschaft gesteuert glide.authenticate.multifactor.self_enrolment_period . Der Standardwert der Eigenschaft ist 30 Tage. Sie kann auf maximal 90 Tage aktualisiert werden.

Alle internen Anwender (Anwender, die keinen haben snc_external Rolle) die Anmeldung mit lokaler oder LDAP-Authentifizierung muss MFA innerhalb von 30 Tagen nach der ersten erfolgreichen Anmeldung einrichten. Während dieser Zeit können Sie sich normal anmelden, aber zum Zeitpunkt der Anmeldung wird eine Meldung angezeigt, um sich bei MFA zu registrieren.



Nach 90 Tagen des Upgrades auf Yokohama oder ein späteres Release, wenn ein interner Anwender (Anwender ohne snc_external Rolle) meldet sich zum ersten Mal mit lokaler oder LDAP-Authentifizierung an. Sie müssen MFA sofort verwenden. Sie haben nicht das 30-tägige MFA-Selbstregistrierungsfenster. Dieser Zeitraum wird von einer Systemeigenschaft gesteuert: glide.authenticate.multifactor.enforcement.max_relaxation_period . Der Höchstwert für diese Eigenschaft beträgt 270 Tage.

2. Wie kann die Zeitleiste für die MFA-Durchsetzung angepasst werden?

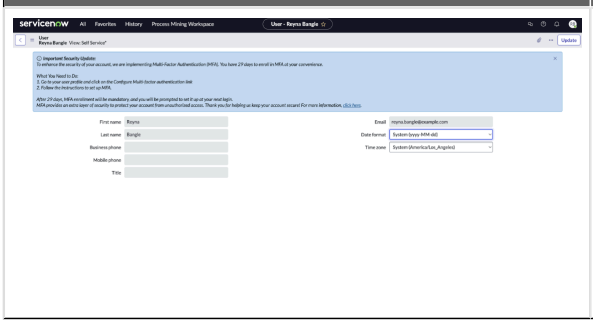
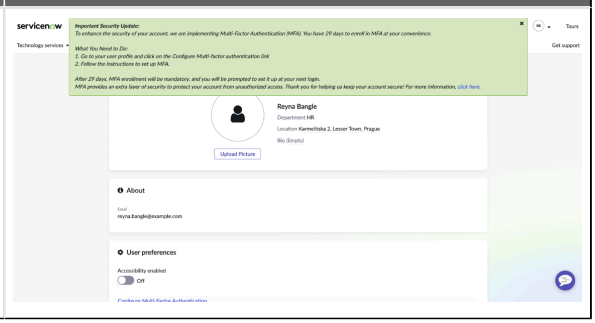
- Durch Aktualisieren des Werts der Eigenschaft glide.authenticate.multifactor.self_enrolment_period , Administratoren können ein kleineres oder größeres Selbstregistrierungsfenster bereitstellen. Legen Sie den Eigenschaftswert auf 0 fest. Die Anwender müssen das MFA-Setup nach ihrem ersten Anmeldeversuch mit lokaler oder LDAP-Anmeldung nach dem Upgrade auf Yokohama oder ein späteres Release abschließen. Die maximale Dauer des Selbstregistrierungsfensters kann 90 Tage betragen. Eigenschaftswert, der höher als 90 festgelegt ist, wird als 90 behandelt.
- Durch Aktualisieren des Werts der Eigenschaft glide.authenticate.multifactor.enforcement.max_relaxation_period der administrator kann entscheiden, wie viele Tage nach dem Upgrade auf Yokohama oder ein späteres Release das MFA-Selbstregistrierungsfenster erhalten.

3. Wie werden Endanwender über diesen bevorstehenden Change informiert?

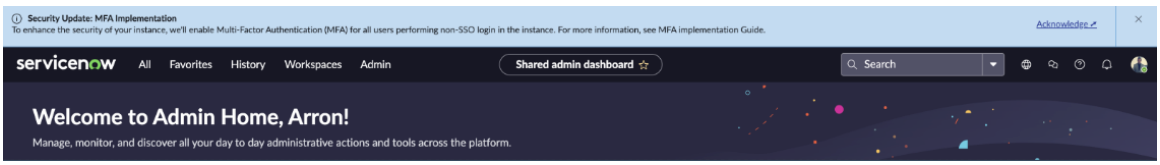
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Endanwender, die eine lokale oder LDAP-Authentifizierung durchführen und mit MFA erzwungen werden, sehen nach der Anmeldung eine Informationsnachricht. Dieselbe Nachricht ist verfügbar, wenn Anwender ihr Profil besuchen.

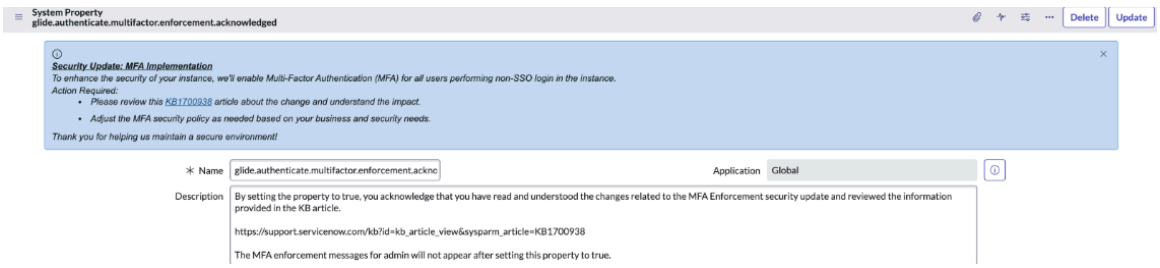
Durchsetzungsnachricht

Im Anwenderprofil	Im Mitarbeiter-Servicecenter
	

Diese Nachricht wird für nicht-Administratoranwender, die SSO-Anmeldungen durchführen, nicht angezeigt. Die Administratorrolle zeigt nach einer erfolgreichen Anmeldung unabhängig von der für die Anmeldung verwendeten Authentifizierungsmethode eine andere Informationsnachricht an.



Diese Nachricht wird weiterhin angezeigt, bis einer der Administratoren die Aktualisierung durch Festlegen von bestätigt `glide.authenticate.multifactor.enforcement.acknowledged` Eigenschaftswert auf „wahr“.



4. Wie kann die Meldung deaktiviert werden, die Endanwendern über den Abschluss des MFA-Setups angezeigt wird, wenn sie sich anmelden?

   Administratoren können den Wert von aktualisieren `glide.authenticate.multifactor.enforcement.show_user_info_message` Systemeigenschaft auf „falsch“, um die Meldung mit Informationen zur MFA-Registrierung zu deaktivieren, die Endanwendern nach der Anmeldung angezeigt wird.

5. Wie kann die Meldung deaktiviert werden, die Administratoren zur MFA-Durchsetzung angezeigt wird?

   Die Informationsnachricht zur MFA-Durchsetzung, die Administratoranwendern nach der Anmeldung angezeigt wird, wird nicht mehr angezeigt, wenn einer der Administratoren dies durch Aktualisieren des Werts von bestätigt `glide.authenticate.multifactor.enforcement.acknowledged` Systemeigenschaft auf „wahr“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Es ist bereits eine MFA-Richtlinie mit adaptiver Authentifizierung basierend auf den Sicherheitsanforderungen meiner Organisation in der Instanz definiert. Ist die Richtlinie von dem Mandat betroffen?

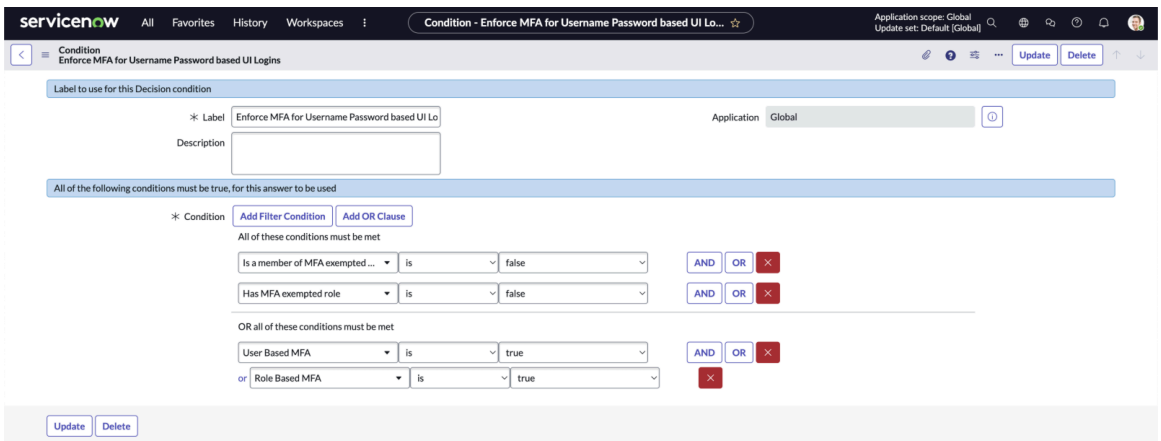
   Nein, wenn die Instanz bereits über eine aktive MFA-Kontextrichtlinie für adaptive Authentifizierung verfügt, wird die neue sichere MFA-Standardrichtlinie nicht erzwungen. Wenn für die Instanz die MFA-Eigenschaft aktiviert war (`glide.authenticate.multifactor`), aber die MFA-Richtlinie war nicht aktiv, dann die standardmäßige sichere MFA-Richtlinie zum Erzwingen von MFA für alle internen Anwender (Anwender, die nicht haben) `snc_external` Rolle) die Ausführung der lokalen oder LDAP-Anmeldung für Anwendernamen und Passwort ist aktiviert.

MFA-Durchsetzungsausnahme

Häufig gestellte Fragen zur MFA-Durchsetzungsausnahme und warum dies wichtig ist.

1. Wie kann das MFA-Mandat für bestimmte Anwender gelockert werden?

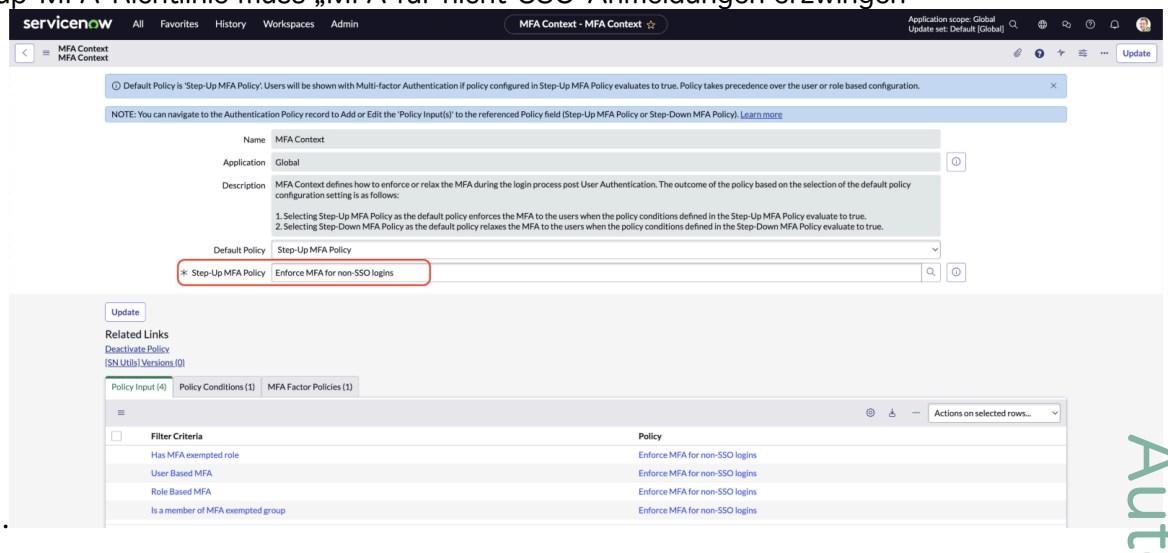
   Im Yokohama-Release wird eine neue Anwendergruppe, ein MFA-befreiter Anwendergruppendatensatz hinzugefügt. Basierend auf der Standardbedingung wird eine MFA-Richtlinie hinzugefügt. Jeder Anwender, der Mitglied dieser Gruppe ist, wird mit MFA erzwungen.



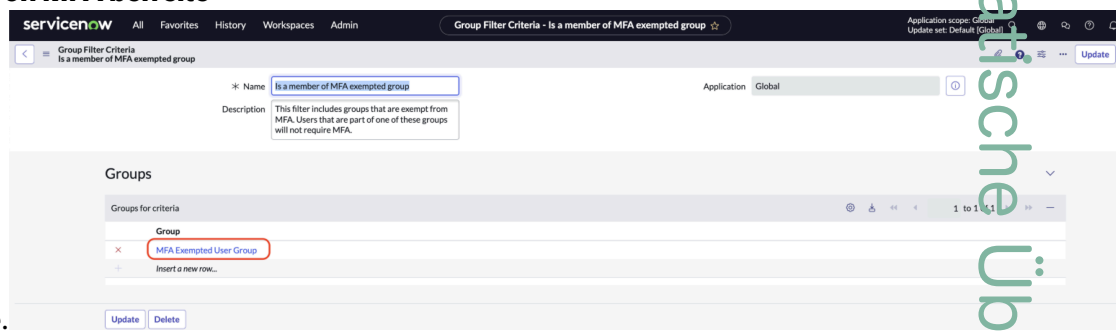
   Um MFA für bestimmte Anwender zu entspannen, gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

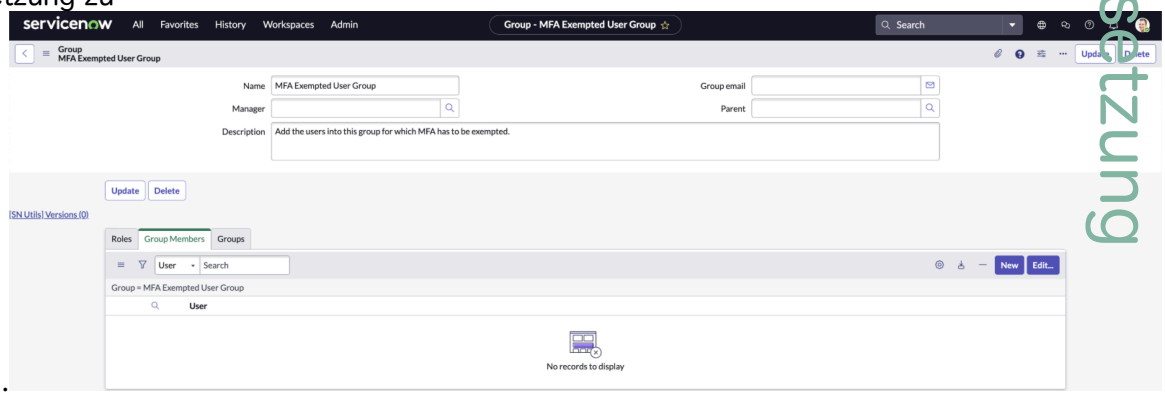
- Navigieren Sie zu **MFA-Kontext**. Die dem MFA-Kontextdatensatz zugeordnete Step-up-MFA-Richtlinie muss „MFA für nicht-SSO-Anmeldungen erzwingen“ lauten.



- Unter **Richtlinieneingabe** Zugehörige Liste wählen Sie aus **Ist Mitglied der von MFA befreiten Gruppe** Filterkriteriendatensatz.
- Wählen Sie Aus **Von MFA befreite Anwendergruppe**.



- Fügen Sie dieser Gruppe Anwender als Mitglied hinzu, um sie von der MFA-Durchsetzung zu befreien.



Hinweis: Wenn dem MFA-Kontext eine andere Richtlinie zugeordnet ist, können Sie Ihrer Richtlinie Filterkriterien „ist Mitglied der von MFA befreiten Gruppe“ hinzufügen und die Richtlinienbedingungen ändern, um Anwender dieser Gruppe von der MFA-Durchsetzung zu befreien.

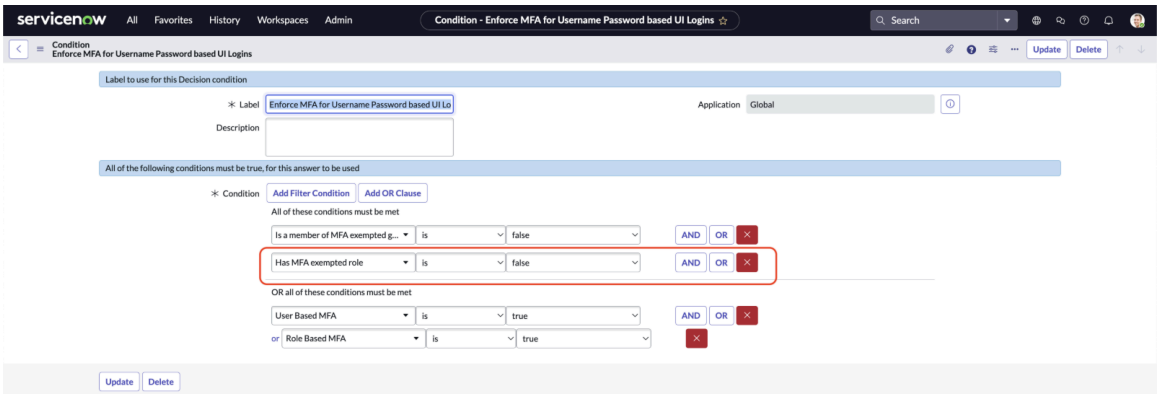
2. Wie kann das MFAs-Mandat für bestimmte Rollen gelockert werden?

Im Yokohama-Release eine leere neue Rolle **Hat von MFA befreite Rolle** Filterkriterium wird hinzugefügt. Der MFA-Richtlinie wurden Bedingungen hinzugefügt, um Anwender,

Automatische Übersetzung

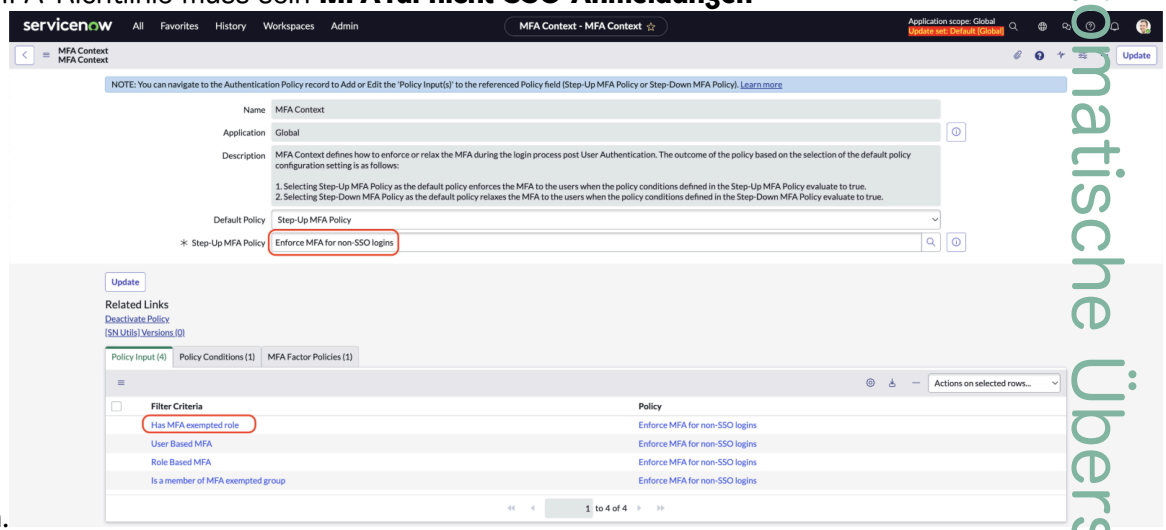
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

deren Rollen Teil der Kriterien für ausgenommene Rollen sind, von der MFA-Durchsetzung auszunehmen.

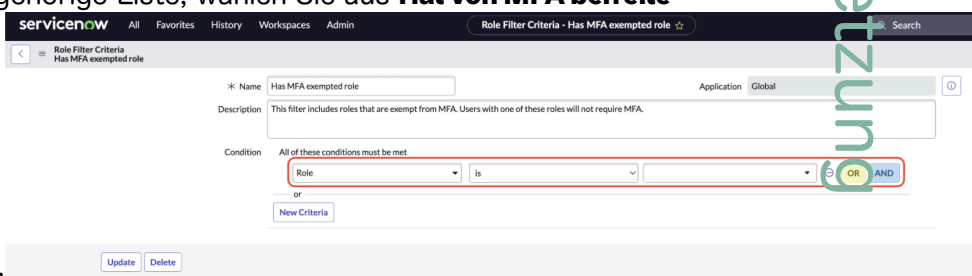


Um MFA für bestimmte Rollen zu entspannen, gehen Sie wie folgt vor:

- Navigieren Sie zu **MFA-Kontext** . Die dem MFA-Kontextdatensatz zugeordnete Step-up-MFA-Richtlinie muss sein **MFA für nicht-SSO-Anmeldungen erzwingen**.



- Unter **Richtlinieneingabe** Zugehörige Liste, wählen Sie aus **Hat von MFA befreite Rolle**Filterkriteriendatensatz.



- Fügen Sie die Rollen hinzu, die Sie der Bedingung hinzufügen möchten. Mit dem Operator ODER können Sie mehrere Rollen hinzufügen.

> **Hinweis:** Wenn dem MFA-Kontext eine andere Richtlinie zugeordnet ist, können Sie hinzufügen **Hat von MFA befreite Rolle** Filterkriterien für Ihre Richtlinie. Ändern Sie die Richtlinienbedingungen, um Anwender mit ausgenommenen Rollen von der MFA-Durchsetzung zu befreien.

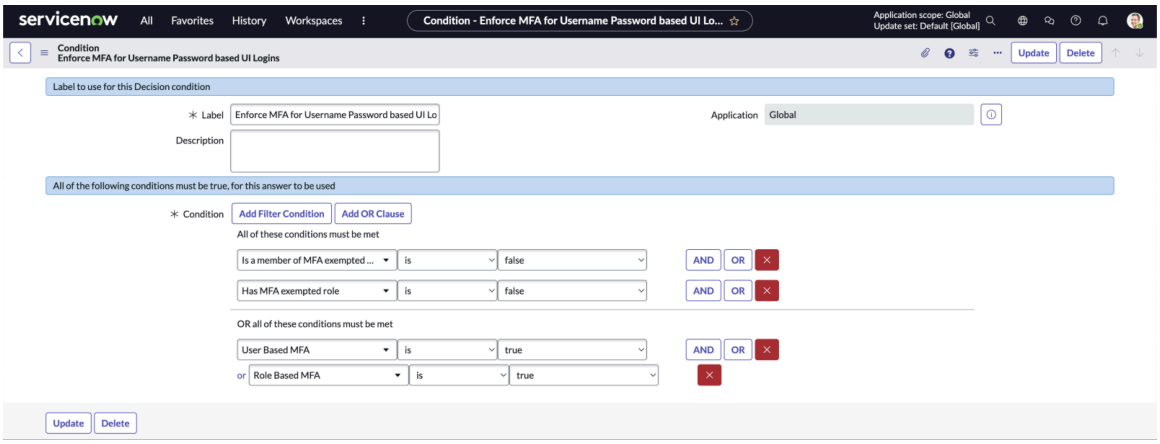
3. Wie kann das MFAs-Mandat für bestimmte Gruppen gelockert werden?

Im Yokohama-Release eine Anwendergruppe **Von MFA befreite Anwendergruppe** Wird hinzugefügt. Basierend auf der Standardbedingung, die der MFA-Richtlinie hinzugefügt

Automatische Übersetzung

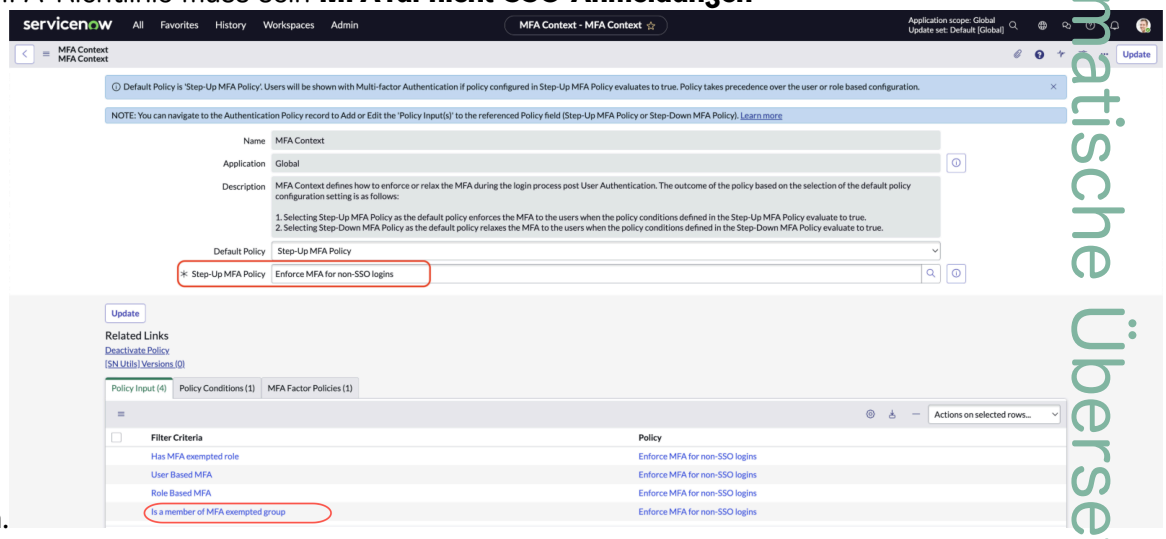
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wurde, wird der Anwender oder die Gruppe, der bzw. die Mitglied dieser Gruppe ist, nicht mit MFA erzwungen.



Um MFA für bestimmte Gruppen zu entspannen, gehen Sie wie folgt vor:

- Navigieren Sie zu **MFA-Kontext** . Die dem MFA-Kontextdatensatz zugeordnete Step-up-MFA-Richtlinie muss sein **MFA für nicht-SSO-Anmeldungen erzwingen**.

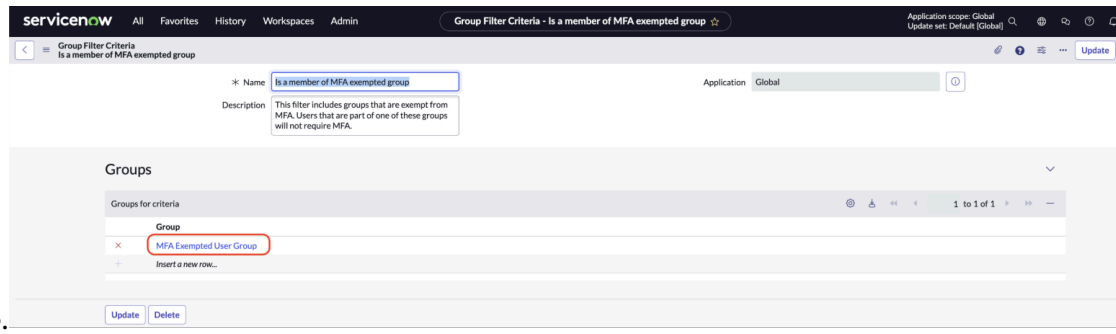


- Unter **Richtlinieneingabe** Zugehörige Liste wählen Sie aus **Ist Mitglied der von MFA befreiten Gruppe** Filterkriteriendatensatz.

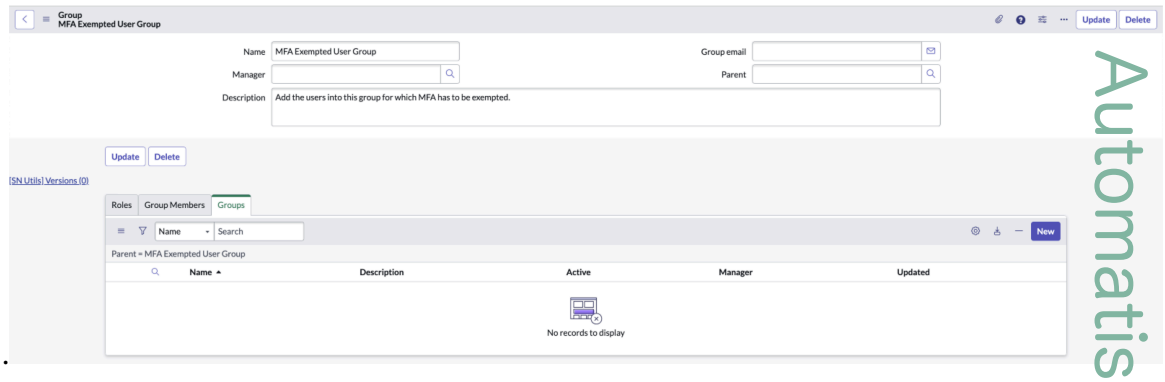
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie Aus **Von MFA befreite Anwendergruppe**.

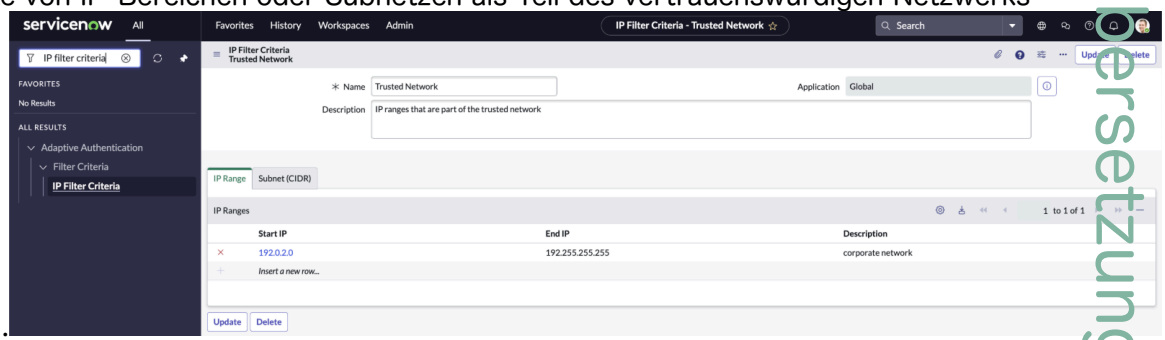


- Fügen Sie dieser Gruppe die Gruppen hinzu, die Sie von der MFA-Durchsetzung ausnehmen möchten.

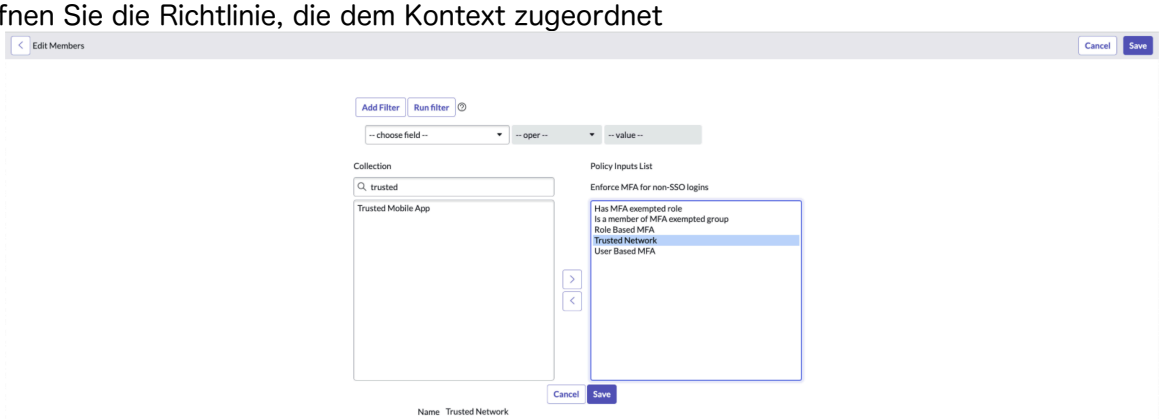


4. Wie kann das MFAs-Mandat für vertrauenswürdige Netzwerke gelockert werden?

- Navigieren zu **Adaptive Authentifizierung** > **Filterkriterien** > **IP-Filterkriterien**an.
- Erstellen Sie ein Kriterium, um ein vertrauenswürdiges Netzwerk anzugeben. Sie können eine Liste von IP-Bereichen oder Subnetzen als Teil des vertrauenswürdigen Netzwerks angeben.



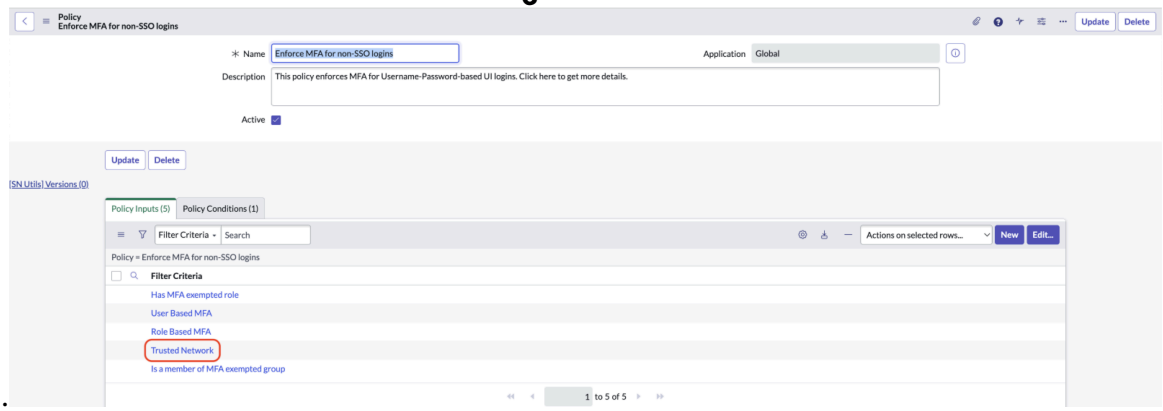
- Navigieren zu **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **MFA-Kontext**an.
- Öffnen Sie die Richtlinie, die dem Kontext zugeordnet ist.



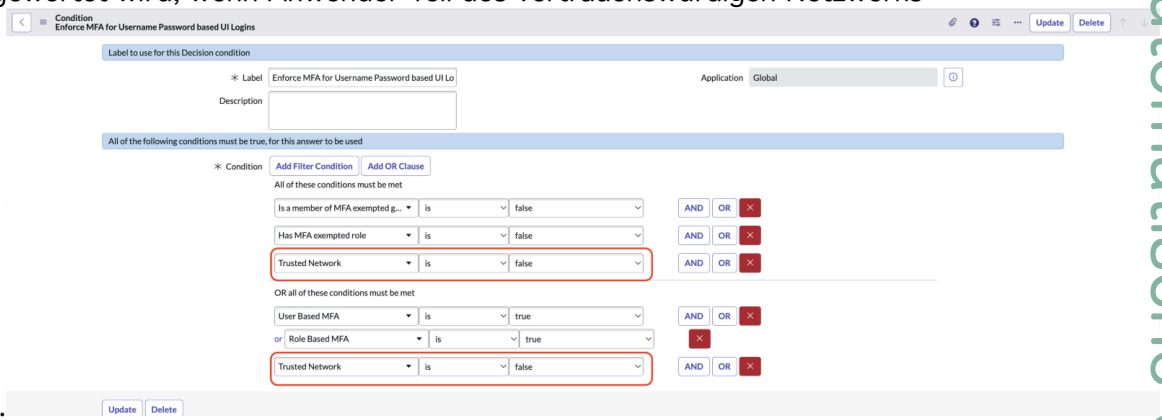
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie die Bearbeitung aus, um hinzuzufügen **IP-Filterkriterien** Die Sie für erstellt haben **Richtlinieneingaben** **bezogen**Liste.



- Ändern Sie die Richtlinienbedingung, um zu bestätigen, dass sie als „falsch“ ausgewertet wird, wenn Anwender Teil des vertrauenswürdigen Netzwerks sind.



Hinweis: Wenn dem MFA-Kontext eine andere Richtlinie zugeordnet ist, können Sie Ihrer Richtlinie die als Teil von Schritt 1 erstellten IP-Filterkriterien hinzufügen und die Richtlinienbedingungen ändern, um die MFA-Durchsetzung im vertrauenswürdigen Netzwerk auszuschließen.

5. Wie kann das MFAs-Mandat für vertrauenswürdige Standorte gelockert werden?

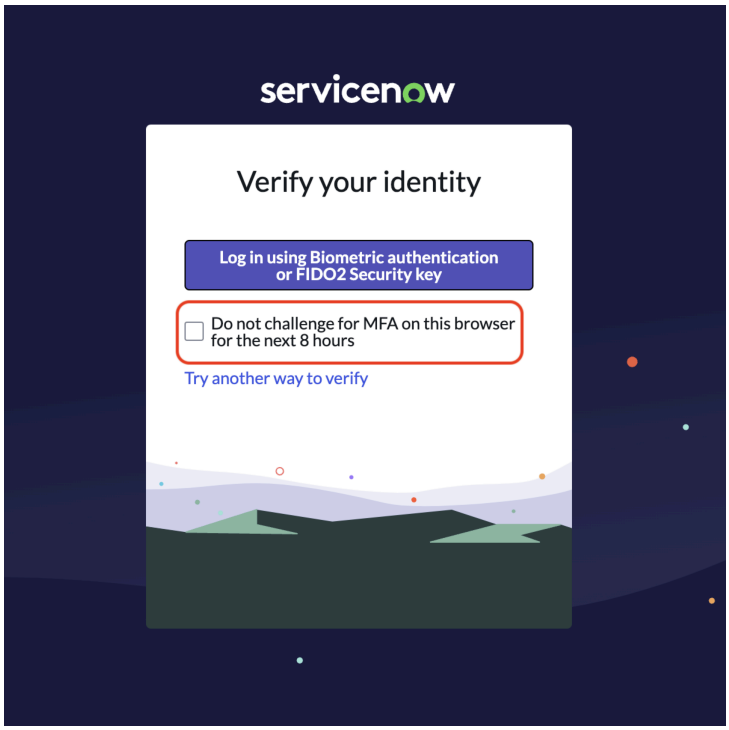
Sie können Standortfilterkriterien verwenden, die mit verfügbar sind **Zero Trust: Standortbasierter Zugriff** Plugin (erfordert ein zusätzliches Abonnement).

6. Wie kann die häufige MFA-Durchsetzung gesteuert werden?

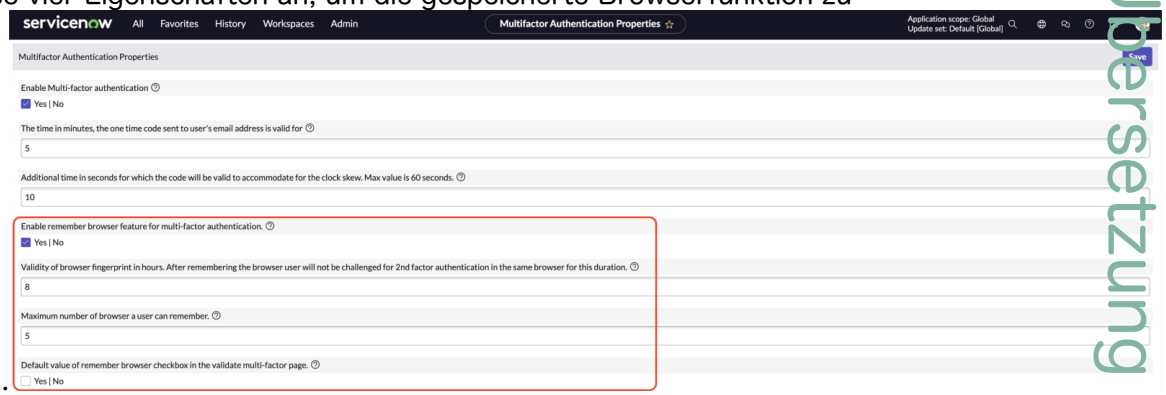
Verwenden Sie die Standortfilterkriterien, die mit verfügbar sind **Zero Trust: Standortbasierter Zugriff** Plugin (erfordert ein zusätzliches Abonnement).

Auf der MFA-Validierungsseite ist ein Kontrollkästchen zum Speichern eines Browsers vorhanden. MFA wird im gespeicherten Browser nicht erzwungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Die von dieser Systemeigenschaft angegebene Dauer. glide.authenticate.multifactor.browser.fingerprint.validity . Der Standardwert der Eigenschaft ist 8 Stunden. Diese Dauer kann um bis zu 24 Stunden verlängert werden. In ähnlicher Weise wird verwendet glide.authenticate.multifactor.remember.browser.default Systemeigenschaft der Standardwert des Kontrollkästchens kann auf „wahr“ festgelegt werden.
- Navigieren zu **Multi-Faktor-Authentifizierung** > **Eigenschaften** Und passen Sie diese vier Eigenschaften an, um die gespeicherte Browserfunktion zu steuern.



7. Wie funktioniert MFA für Accounts, die von Anwendern freigegeben werden?

Einzelne Accounts, die von mehreren Anwendern geteilt werden, sind ein Sicherheitsrisiko. Es wird nicht empfohlen, einen Account für mehrere Anwender freizugeben.

MFA-Metriken

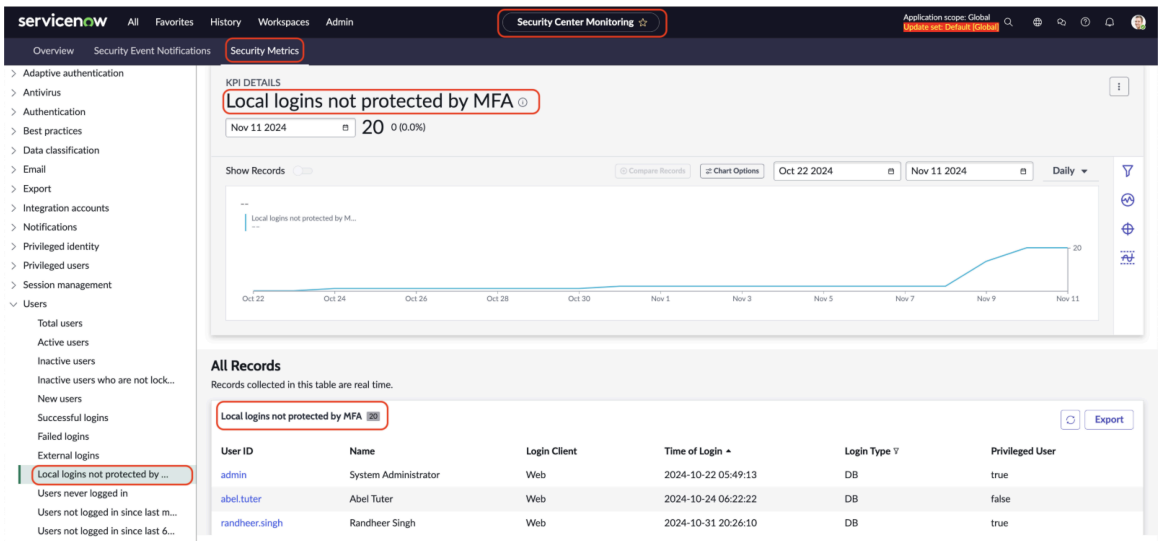
Häufig gestellte Fragen zum Verständnis der MFA-Metriken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wie kann ich die Anzahl der lokalen Anmeldungen überprüfen, für die keine MFA durchgeführt wird?

   Sie können zu navigieren **Sicherheitscenter** > **Sicherheitskonsole** > **Sicherheitsmetriken**an. Klicken Sie unter „Metriken für Anwender“ auf die lokale Anmeldung, die nicht durch MFA geschützt ist.



2. Wie kann ich die Anzahl der Anwender überprüfen, die das MFA-Setup noch abschließen müssen und die lokale Anmeldung durchführen?

   Sie können zu navigieren **Sicherheitscenter** > **Sicherheitskonsole** > **Sicherheitsmetriken**an. Klicken Sie unter „Metriken für Anwender“ auf die lokale Anmeldung, die nicht durch MFA geschützt ist.

MFA-Typen

Häufig gestellte Fragen zu MFA-Typen und warum dies wichtig ist.

1. Welche Arten von Verifizierungsmethoden sind für MFA mit verfügbar ServiceNow?

   ServiceNow Das Basissystem unterstützt diese Verifizierungsmethoden.

   a. Passkey

   b. TOTP-Authentifikator-Apps wie Google Authenticator, Okta Verify, Microsoft Authenticator, Authy, DUO

   c. Biometric Authenticator (FIDO2), z. B. Windows Hello, Apple Touch ID, Face ID, android-Fingerabdrucksensor.

   d. Hardware-Sicherheitsschlüssel (FIDO2) wie YubiKey, Thetis

   e. Einmaliges Passwort per E-Mail (OTP)

   f. SMS-OTP: Multifaktor-Authentifizierung mit SMS com.snc.authentication.sms_mfaplugin-Installation und Faktorkonfiguration sind erforderlich, um SMS-OTP-basierte MFA zu aktivieren.

2. Kann ein Anwender mehrere MFA-Faktoren oder Verifizierungsmethoden konfigurieren?

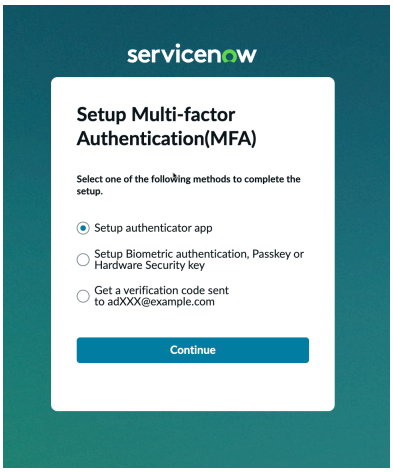
   Ja, Sie können sich für mehrere MFA-Faktoren registrieren, indem Sie ihr Anwenderprofil aufrufen. Sie können beispielsweise einen Laptop mit dem biometrischen Authentifikator registrieren, das Mobiltelefon mit einem Passkey verwenden und eine Authentifikator-App einrichten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Welche Schritte müssen Anwender ausführen, um das MFA-Setup abzuschließen?

   Der Anwender kann eine der folgenden MFA-Optionen ausführen.



   Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung Dokumentation für weitere Informationen zum MFA-Setup.

4. Kann die SMS- und E-Mail-OTP-basierte MFA auf bestimmte Anwender beschränkt werden?

   Der Administrator kann MFA-Faktorrichtlinien für E-Mail- und SMS-OTP-basierte MFA-Faktoren einrichten, um diese Faktoren auf bestimmte Anwendergruppen oder Rollen zu beschränken.

5. Die Anwender haben kein Mobiltelefon, auf dem sie eine Authentifikator-App einrichten können. Wie können diese Anwender MFA aktivieren?

   Ab dem Xanadu-Release können Sie einen biometrischen Authentifikator, Passkeys, FIDO2-Hardwaresicherheitsschlüssel und E-Mail-OTP-basierte MFA verwenden, ohne dass auf dem Mobiltelefon ein Authentifikator-App-Setup erforderlich ist.

6. Wie kann MFA als Endanwender eingerichtet werden?

   Weitere Informationen finden Sie unter Multifaktor-Authentifizierung wird verwendet Dokumentation für weitere Informationen zum MFA-Setup.

MFA-Zurücksetzung

Häufig gestellte Fragen zur MFA-Zurücksetzung und warum dies wichtig ist.

1. Setup der Authentifikator-App verloren. Wie kann ich zurücksetzen?

   Es ist besser, wenn sich Anwender bei mehreren Faktoren registrieren, damit sie nicht aufgrund von MFA gesperrt sind. Sie können beispielsweise die TOTP-Authentifikator-App, den Passkey und die E-Mail-OTP-basierte MFA haben.

   Wenn Anwender keinen der registrierten MFA-Faktoren verwenden können, kann der Administrator die MFA zurücksetzen, indem er die folgenden Schritte befolgt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Setup der Authentifikator-App wird gelöscht:

- Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Anwendereinrichtung**an.
- Suchen Sie in der Tabelle nach dem Anwender.
- Löschen Sie den dem Anwender zugeordneten Datensatz

b. Löschen der FIDO2-Authentifikatoren und Passkeys:

- Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Webauthentifizierung** > **Öffentliche Anmeldeinformationen des Anwenders**an.
- Suchen Sie in der Tabelle nach dem Anwender
- Löschen Sie die dem Anwender zugeordneten Datensätze

c. Löschen anderer Multifaktor-Setups, die dem Anwender zugeordnet sind

- Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Anwendereinrichtung**an.
- Suchen Sie in der Tabelle nach dem Anwender
- Löschen Sie die dem Anwender zugeordneten Datensätze

Falls niemand, einschließlich des Administrators, auf die Instanz zugreifen kann. Der Administrator kann eine Selfservice-MFA-Zurücksetzung mithilfe eines Katalogelements durchführen, das unter verfügbar ist Now-Support .

2. Wie kann verhindert werden, dass Administratoren aufgrund von MFA gesperrt werden?

Die Administratoren registrieren sich für mehrere MFA-Faktoren, damit der Zugriff auf die Instanz nicht blockiert wird.

Falls niemand, einschließlich des Administrators, auf die Instanz zugreifen kann. Der Administrator kann eine Selfservice-MFA-Zurücksetzung mithilfe eines Katalogelements durchführen, das unter verfügbar ist Now-Support .

Multifaktor-Authentifizierung erkunden

Multifaktor-Authentifizierung (MFA) ist eine Authentifizierungsmethode, bei der Anwender andere Informationen als ihre grundlegenden Anmeldeinformationen angeben müssen.

MFA ist ein Sicherheitsprozess, bei dem ein Anwender zwei oder mehr verschiedene Verifizierungsfaktoren angeben muss, um auf einen Service oder Account zuzugreifen. Sie fügt Ihrem Service eine zusätzliche Sicherheitsebene hinzu, die über ein Passwort hinausgeht, was es nicht autorisierten Personen erschwert, Zugriff zu erhalten.

Durch die Anforderung mehrerer Faktoren verbessert MFA die Sicherheit erheblich und hilft beim Schutz vor verschiedenen Cyberbedrohungen, einschließlich Phishing und Identitätsdiebstahl. Hier finden Sie einen Einblick in die Funktionsweise von MFA:

- **Erster Faktor** : Der Anwender, der seinen Anwendernamen und sein Passwort für die Anmeldung verwendet.
- **Zweiter Faktor** : Der Anwender wird nach einem zweiten Faktor gefragt, der beim Anwender liegt (eine Identitätsverifizierungsmethode wie eine Authentifikator-App oder ein Sicherheitsschlüssel).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Darüber hinaus können diese Faktoren in der Regel basierend auf ihrem Schutzniveau vor allgemeinen Sicherheitsbedrohungen in gesichert und weniger gesichert kategorisiert werden.

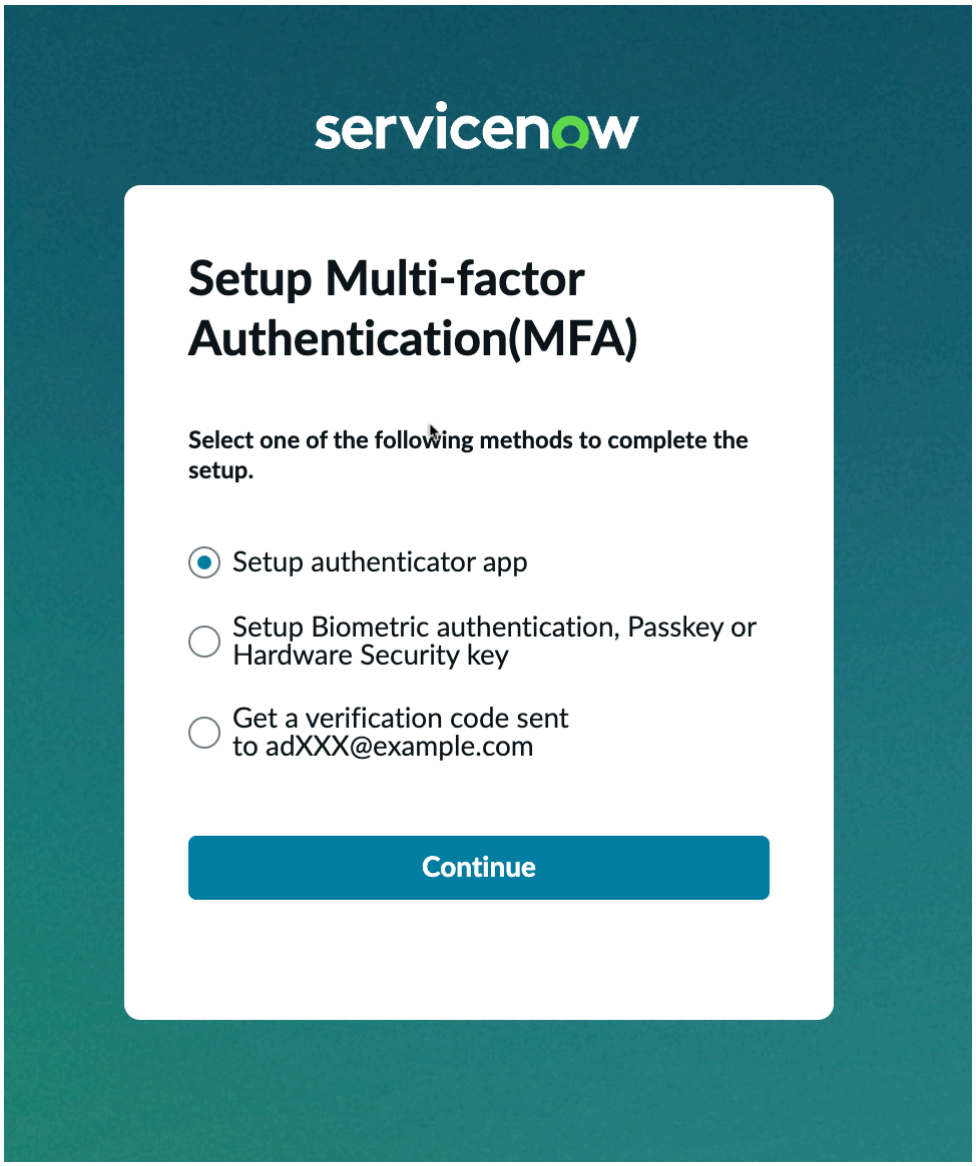
- Gesicherte Faktoren:
  - FIDO (Fast Identity Online): Dieser Faktor verwendet Hardware-Token oder biometrische Authentifizierungsmethoden, die ein hohes Sicherheitsniveau bieten, indem bestätigt wird, dass der Anwender über ein physisches Gerät oder ein eindeutiges biometrisches Merkmal verfügt, um seine Identität zu verifizieren.
  - **TOTP (zeitbasiertes Einmalpasswort):** Dieser Faktor generiert ein einmaliges Passwort, das für einen kurzen Zeitraum gültig ist, normalerweise 30 Sekunden. Sie wird normalerweise über eine mobile App bereitgestellt, wodurch eine zusätzliche Sicherheitsebene hinzugefügt wird, indem der Anwender Zugriff auf ein bestimmtes Gerät und eine bestimmte App hat.
- Weniger Gesicherte Faktoren:
  - **E-MAIL:** Dieser Faktor sendet einen Verifizierungscode oder Link an die E-Mail-Adresse des Anwenders. Es ist zwar praktisch, aber weniger sicher, da E-Mail-Accounts gefährdet werden können.
  - **SMS:** Dieser Faktor sendet einen Verifizierungscode per Textnachricht an die Telefonnummer des Anwenders. Außerdem ist sie aufgrund des potenziellen SIM-Tauschens und anderer Schwachstellen für Mobiltelefone weniger sicher.

Zur Verbesserung der Sicherheit wird empfohlen, die Verwendung gesicherter Faktoren wie FIDO und TOTP gegenüber weniger gesicherten Faktoren wie E-MAIL und SMS zu priorisieren.

Hinweis:

- MFA ist standardmäßig auf aktiviert ServiceNow.
- MFA ist mit aktiviert `glide.authenticate.multifactor`Eigenschaft. Wenn Sie diese Eigenschaft deaktivieren möchten, müssen Sie eine geschäftliche Begründung angeben, warum Sie MFA deaktivieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



ServiceNow MFA von unterstützt Verifizierungsmethoden wie Authenticator App, Fast Identity Online 2 (FIDO2), Passkey und zeitbasiertes Einmalpasswort (OTP). Im Folgenden finden Sie die Details der verfügbaren Verifizierungsmethoden:

- **Authentifikator-App** : Apps, die eindeutige, temporäre Verifizierungscodes generieren. Beispiel: Okta, Google Authenticator, Microsoft Authenticator usw.
- **FIDO2** : Physische Geräte, die Kryptografie mit öffentlichen Schlüsseln verwenden, um Anwenderidentitäten zu validieren. Beispiel: Hardwareschlüssel (YubiKey), biometrische Scanner (Apple Touch ID).
- **Passkey** : Melden Sie sich mit einem Passkey an, indem Sie das Gerät mit einem biometrischen Sensor, einer PIN oder einem Muster entsperren.
- **OTP** : Der geheime Schlüssel und die aktuelle Zeit zur Generierung eines eindeutigen Passworts, das nur für einen kurzen Zeitraum gültig ist. Beispiel: SMS (OTP) und E-Mail (OTP).

Sie können MFA zusammen mit folgenden verwenden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Lokale Datenbankauthentifizierung (nativ ServiceNow Authentifizierung) oder Integration von Lightweight Directory Access Protocol
- SSO SAML ODER SSO OIDC. Weitere Informationen finden Sie unter Single Sign-on (SSO) für mehrere Anbieter.

Zugehörige Informationen

Verifizierungsmethoden für Multifaktor-Authentifizierung

Systemeigenschaften der Multifaktor-Authentifizierung

Multifaktor-Authentifizierung wird konfiguriert

Konfigurieren Sie Multifaktor-Authentifizierung (MFA), um die Sicherheit Ihrer Anwender bei Verwendung zu verbessern ServiceNow.

Um MFA zu implementieren, bestimmen Sie zunächst die MFA Verifizierungsmethoden Basierend auf Geschäfts- und Anwenderanforderungen.

Nach Identifizierung der Anforderungen mit ServiceNow MFA von , können Sie die richtige Methode oder die Kombination daraus für Ihre Anwender auswählen. Darüber hinaus können Sie auch die verschiedenen Multifaktor-Authentifizierungseigenschaften verwenden, um MFA zu aktivieren, zu deaktivieren und zu konfigurieren, um die MFA-Experience des Anwenders basierend auf den Authentifizierungskriterien weiter zu verbessern.

Hier sind einige der wichtigen Themen im Zusammenhang mit der Konfiguration von MFA:

- Verifizierungsmethoden für Multifaktor-Authentifizierung
- Systemeigenschaften der Multifaktor-Authentifizierung
- Multifaktor-Authentifizierungskriterien

Multifaktor-Authentifizierungskontext

Der Richtlinienkontext für Multifaktor-Authentifizierung (MFA) verwendet eine Richtlinie, um zu definieren, wie und wann MFA während des Anmeldevorgangs erzwungen wird.

MFA-Kontextdatensatz

Der MFA-Richtlinienkontext definiert, ob Ihre Anwender bei der Anmeldung eine zweite Form der Authentifizierung bereitstellen müssen. Dieser Kontext verweigert nicht den Zugriff auf Ihre Instanz als Richtlinien nach der Authentifizierung und vor der Authentifizierung. Die in diesem Kontext ausgewählte Richtlinie hat Vorrang vor Anwender- oder rollenbasierten Konfigurationen für die Multifaktor-Authentifizierung.

Um auf den MFA-Kontext zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.

Verwenden Sie die Felder im Richtlinienkontextdatensatz nach der Authentifizierung, um zu definieren, wie Ihre Instanz Ihre Richtlinie verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn die Standardrichtlinie ist **STEP-up-MFA-Richtlinie** , Anwender werden mit Multifaktor-Authentifizierung angezeigt, wenn die Richtlinie in konfiguriert ist **STEP-up-MFA-Richtlinie** Wird als „wahr“ ausgewertet. Richtlinie hat Vorrang vor der Anwender- oder rollenbasierten Konfiguration.
- MFA mit SSO-Anmeldung ist nur verfügbar, wenn glide.authenticate.mfa.with.multisso.enabled Eigenschaft ist auf „wahr“ festgelegt.
- Sie können zum Datensatz der Authentifizierungsrichtlinie navigieren, um „Richtlinieneingabe(en)“ zum Feld „Referenzierte Richtlinie“ hinzuzufügen oder zu bearbeiten (**STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie**).
- Die MFA-Kontextrichtlinie gilt nur für Anwenderanmeldungen. Sie gilt nicht für die API-Authentifizierung, die Standardauthentifizierung und die Erteilung von Anmeldeinformationen für das Passwort des OAuth-Ressourcenbesitzers.

MFA-Kontextformular

Feld	Beschreibung
Name	Name des Richtlinienkontexts. Dieses Feld ist statisch und kann nicht geändert werden.
Beschreibung	Beschreibung des Kontexts
Standardrichtlinie	Definiert das Standardverhalten dieses Kontexts bei der Bewertung der Richtlinie. Wählen Sie unter den folgenden Optionen aus. **Step-Up-MFA-Richtlinie** Erzwingt MFA für Anwender, wenn die Richtlinienbedingungen in definiert sind **STEP-up-MFA-Richtlinie** Feld wird als „wahr“ ausgewertet. **Step-Down-MFA-Richtlinie** Erzwingt standardmäßig MFA. MFA wird nur dann erzwungen, wenn die Richtlinienbedingungen in definiert sind **STEP-Down-MFA-Richtlinie** Feld wird als „wahr“ ausgewertet.
Step-Up-MFA-Richtlinie	Die Richtlinie, die für diesen Kontext verwendet wird. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **STEP-up-MFA-Richtlinie** .
Step-Down-MFA-Richtlinie	Die Richtlinie, die für diesen Kontext verwendet wird. Dieses Feld wird nur angezeigt, wenn **Standardrichtlinie** Feld ist auf festgelegt **STEP-Down-MFA-Richtlinie** .

Richtlinieneingaben und -Bedingungen

Die **Richtlinieneingabe** Und **Richtlinienbedingungen** Registerkarten zeigen die Eingaben und Bedingungen der in ausgewählten Richtlinie an **STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie** Feld. Diese Registerkarten dienen als Referenz, können jedoch nicht zum Ändern der Richtlinieneingaben oder -Bedingungen verwendet werden. Um Ihre Richtlinieneinstellungen zu ändern, navigieren Sie über das Referenzsymbol (zur Richtlinie) Neben **STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie** Feld.

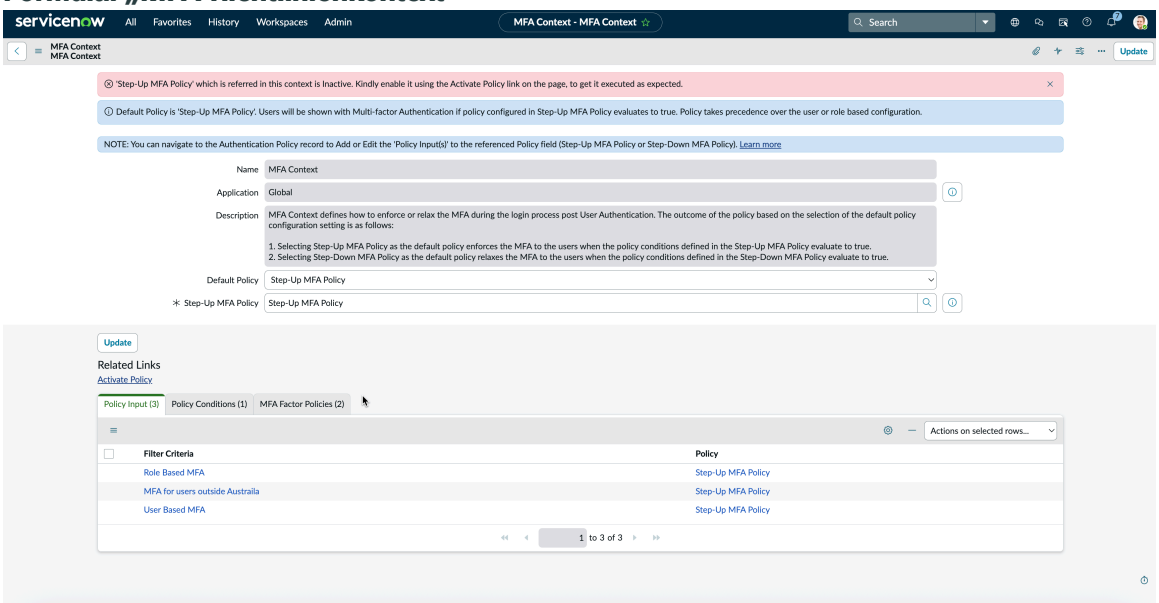
Hinweis: Richtlinienbedingungen können von hier aus erstellt werden, es wird jedoch empfohlen, neue Richtlinienbedingungen auf der Richtlinienseite hinzuzufügen.

Dieses Beispiel zeigt einen MFA-Kontextdatensatz, der mit einer Step-up-MFA-Richtlinie konfiguriert wurde. Diese Standardrichtlinie bedeutet, dass MFA nur erzwungen wird, wenn die in der Richtlinie definierten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungen als „wahr“ ausgewertet werden. Der Kontext verwendet eine Richtlinie namens **STEP-up-MFA-Richtlinie** . Diese Richtlinie verfügt über eine Reihe von Eingaben und Bedingungen, die in angezeigt werden **Richtlinieneingabe** Und **Richtlinienbedingung** Registerkarten.

Formular „MFA-Richtlinienkontext“



MFA-Faktorrichtlinien

MFA-Faktorrichtlinien sind eine kritische Komponente der Sicherheitslage einer Organisation, sodass Sie zusätzliche Verifizierungsschritte über Passwörter hinaus erzwingen können. Diese Richtlinien definieren die Authentifizierungsmethoden, die Anwender für den Zugriff verwenden müssen, und bieten einen flexiblen und anpassbaren Ansatz für die Authentifizierung. Weitere Informationen finden Sie unter Richtlinien für Multifaktor-Authentifizierungsfaktor.

Verifizierungsmethoden für Multifaktor-Authentifizierung

ServiceNow MFA von unterstützt Verifizierungsmethoden wie die Authenticator-App, Fast Identity Online 2 (FIDO2) und das zeitbasierte Einmalpasswort (TOTP).

Die Anwender können zusätzlich zu ihrem Anwendernamen und ihrem Passwort die folgenden Optionen verwenden, um die Anforderungen der Multifaktor-Authentifizierung zu erfüllen. Die Anwender können MFA-Faktoren wie Authentifikatoranwendungen, biometrische Scanner, Hardwareschlüssel und SMS unabhängig einrichten.

Authentifikatoranwendungen

Eine Authentifikator-Anwendung ist eine Drittanbietersoftware, die temporäre Passcodes generiert. Benutzer können diese Passcodes zusammen mit ihrem Passwort verwenden, um sich bei einer Instanz anzumelden, die Multifaktor-Authentifizierung (MFA) erfordert. Weitere Informationen zu diesen Anwendungen finden Sie unter Authentifikatoranwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hardwareschlüssel und biometrische Scanner (Webauthentifizierung)

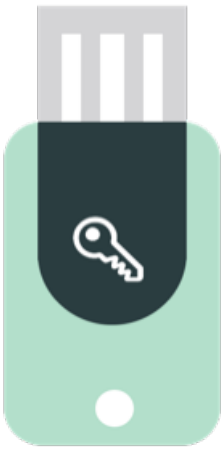
Die *`Integration - Web Authentication`*(com.snc.integration.webauthn) Plugin ermöglicht die Authentifizierung von Hardwareschlüsseln oder biometrischem Lesegeräten in Ihrer Instanz.

Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Anwender zu identifizieren. Ihre Anwender können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Details zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden in einen Port Ihres Geräts eingefügt, um die Authentifizierung bereitzustellen. Details zum Registrieren von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.



Passkey

Die Passkey-Authentifizierung ist eine sichere, passwortlose Methode der Anmeldung, bei der Anwender einen Passkey verwenden, indem sie ihr Gerät mit einem biometrischen Sensor, einer PIN oder einem Muster entsperren.

SMS

Der Administrator kann konfigurieren ServiceNow Instanz, die Anwender erfordert, die versuchen, sich mit SMS-basiertem OTP bei der Instanz anzumelden.

Wenn Anwender versuchen, sich bei anzumelden ServiceNow, SMS-OTP wird an die Mobiltelefonnummer gesendet, die dem sys_user-Datensatz zugeordnet ist. Benutzer können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen. Weitere Informationen finden Sie unter SMS als MFA-Faktor.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail

Der Administrator kann konfigurieren ServiceNow Instanz, die Anwender erfordert, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden.

Wenn Anwender versuchen, sich bei anzumelden ServiceNow, E-Mail-OTP wird an die E-Mail-Adresse des Anwenders gesendet. Benutzer können den sechsstelligen Verifizierungscode eingeben, der an die E-Mail-Adresse gesendet wurde, und ihre Identität überprüfen. Weitere Informationen finden Sie unter E-Mail als MFA-Faktor.



Zugehörige Informationen

Webauthentifizierung: MFA

Verifizierungsmethoden für Multifaktor-Authentifizierung

E-Mail als MFA-Faktor

Webauthentifizierung: MFA

Verwenden Sie **Integration – Webauthentifizierung (com.snc.integration.webauthn)** Um die Authentifizierung von Hardwareschlüsseln oder biometrischen Lesegeräten in Ihrer Instanz zuzulassen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden in einen Port Ihres Geräts eingefügt, um die Authentifizierung bereitzustellen. Details zum Registrieren von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.



Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Anwender zu identifizieren. Ihre Anwender können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Details zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

Multifaktor-Authentifizierung mit Biometrik konfigurieren

Administratoren können die Liste „öffentliche Anwenderanmeldeinformationen“ verwenden, um vom Anwender erstellte Anmeldeinformationen anzuzeigen und zu verwalten.

Wenn ein Anwender eine Authentifikatoranwendung, eine biometrische Authentifizierung oder einen Hardwareschlüssel registriert, erstellt die Instanz einen Datensatz im **Öffentliche**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen Des Anwenders Tabelle [sys_user_public_credential]. Verwenden Sie diese Tabelle, um anzuzeigen, welche Anwender einen Authentifikator registriert haben, welche Typen und wann sie registriert und verwendet wurden. Sie können diese Datensätze auch als inaktiv markieren, um zu verhindern, dass Anwender diese Anmeldeinformationen verwenden.

Die **Integration – Webauthentifizierung (com.snc.integration.webauthn)** Plugin muss für die Webauthentifizierung (FIDO2) aktiviert sein.

Hinweis: Die **Integration – Webauthentifizierung (com.snc.integration.webauthn)** Plugin ist standardmäßig installiert.

Formular „öffentliche Anwenderanmeldeinformationen“

Feld	Beschreibung
Kurzname der Anmeldeinformationen	Kurzname für die Anmeldeinformationen. Dieser Spitzname wird vom Anwender ausgewählt, wenn er einen Authentifikator registriert.
Anwender	Anwender, der den Anmeldeinformationen zugeordnet ist
Aktiv	Gibt an, ob die Anmeldeinformationen aktiv sind. Administratoren können einen Datensatz auf „inaktiv“ festlegen, um zu verhindern, dass sich ein Anwender mit diesen Anmeldeinformationen authentifiziert.
Authentifikator	Der Typ des vom Anwender registrierten Authentifikators.
Registrierungszeit	Datum und Uhrzeit der Erstellung dieser Anmeldeinformationen durch den Anwender
Zuletzt verwendet um	Datum und Uhrzeit der letzten Anmeldung des Anwenders mit diesen Anmeldeinformationen.

Eingeschränkte Authentifikatortypen

Wenn Sie eine Authentifizierungsmethode wie biometrische Authentifikatoren eingeschränkt haben, können Anwender keine neuen Anmeldeinformationen dieses Typs erstellen. Alle Anmeldeinformationen, die vor der Einschränkung erstellt wurden, funktionieren jedoch weiterhin. Sie können Datensätze auf der deaktivieren **Öffentliche Anmeldeinformationen Des Anwenders** Tabelle, um zu verhindern, dass diese Anmeldeinformationen nach der Erstellung verwendet werden.

Authentifikator-Konfigurationsoptionen

Verwenden Sie die Seite „Authentifikatorkonfiguration“, um Authentifikatoroptionen in Ihrer Instanz zu verwalten.

Navigieren zu **Multi-Faktor-Authentifizierung** > **Webauthentifizierung** > **Konfiguration des Authentifikators** Zum Anzeigen und Bearbeiten der Standardkonfigurationsoptionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Authentifikatorkonfiguration“

Feld	Beschreibung
Zulässiger Authentifikatortyp	Typ der Authentifikatoren, die registriert werden dürfen. Wählen Sie aus: • **Plattform** Authentifikatoren werden an ein Gerät angehängt oder in ein Gerät integriert. Fingerabdruckleser oder Gesichtserkennung auf Mobilgeräten verfügbar (z. B. Apple FaceID oder TouchID) fallen unter diese Kategorie. • **Roaming** Authentifikatoren können von einem Computer oder einem anderen Client-Gerät entfernt und an anderer Stelle verwendet werden. Hardwareschlüssel fallen unter diese Kategorie.
Nachweistyp	Wenn Sie den Wert auf „direkt“ oder „indirekt“ festlegen, müssen Authentifikator-Metadaten importiert werden, um die Herkunft eines Authentifikators während der Registrierung zu bestätigen. • Keine • Direkt • Indirekt
Plattform-Selbstnachweis	Gibt an, ob der Selbstnachweis für Plattformauthentifikatoren aktiviert ist.
Plattformübergreifender Selbstnachweis	Gibt an, ob der Selbstnachweis für Roaming-Authentifikatoren aktiviert ist.
Anwenderverifizierung	Wählen Sie aus **Bevorzugt** Oder **Erforderlich** . Bei Bedarf fordert der Web-Authentifizierungs-Flow Anwender zur Verifizierung mithilfe von PIN oder Biometrics auf.
Anwenderpräsenz verifizieren	Gibt an, ob der Web-Authentifizierungs-Flow die Verifizierung der Anwenderpräsenz erfordert.
Residenter Schlüssel	Wählen Sie aus **Bevorzugt** Oder **Erforderlich** . Bei Bedarf behält der Authentifikator die Anmeldeinformationen des öffentlichen Schlüssels im Authentifikatorspeicher bei.
Zeitüberschreitung (in ms)	Maximale Zeitgrenze für den Abschluss der Registrierung und Authentifizierung der Webauthentifizierung. Die Zeit wird in Millisekunden angegeben.

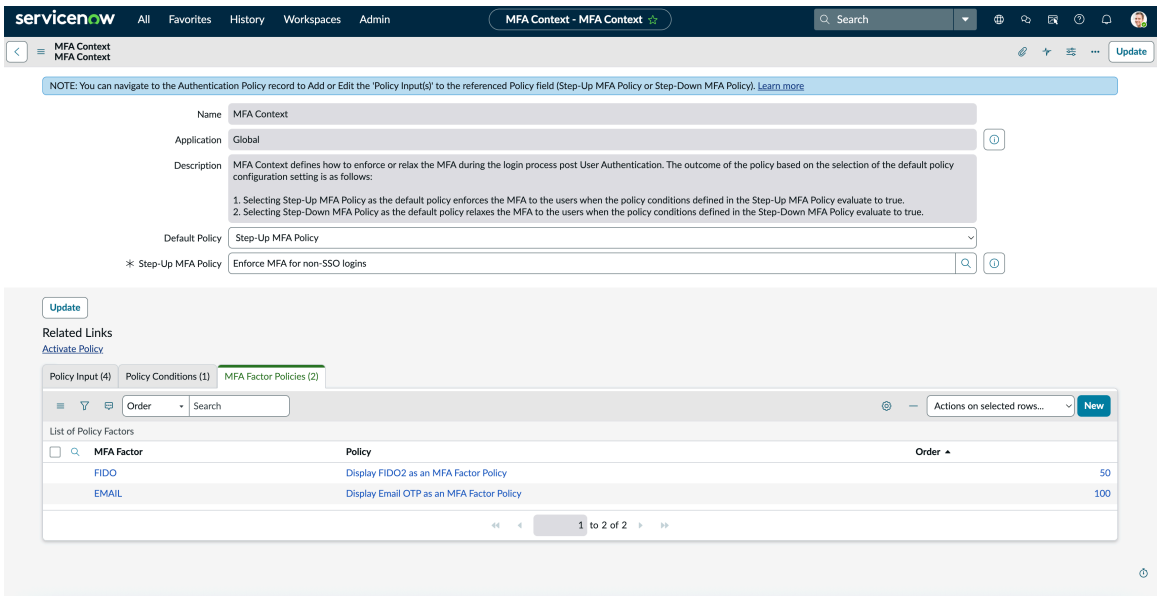
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinien für Multifaktor-Authentifizierungsfaktor

Verwenden Sie die MFA-Faktorrichtlinien, um die Typen von Authentifizierungsfaktoren anzugeben, die Sie für Ihre Instanz zulassen möchten.

MFA-Faktorrichtlinien sind eine kritische Komponente der Sicherheitslage einer Organisation, sodass Sie zusätzliche Verifizierungsschritte über Passwörter hinaus erzwingen können. Diese Richtlinien definieren die Authentifizierungsmethoden, die Anwender verwenden müssen, um auf die Ressourcen Ihrer Organisation zuzugreifen, und bieten einen flexiblen und anpassbaren Ansatz für die Authentifizierung.

Die Implementierung von MFA-Faktorrichtlinien ist wichtig, um die Sicherheit der Systeme und Daten Ihrer Organisation zu verbessern. Diese Richtlinien bieten eine zusätzliche Schutzebene vor Cyberbedrohungen, wodurch es Angreifern erschwert wird, nicht autorisierten Zugriff zu erhalten.



Zur Verwendung der MFA-Faktorrichtlinien müssen Sie die Richtlinieneingaben und Richtlinienbedingungen zusammen mit einem MFA-Kontext konfigurieren. Weitere Informationen finden Sie unter Multifaktor-Authentifizierungskontext.

Im Folgenden finden Sie die in verfügbaren MFA-Faktorrichtlinien ServiceNow Damit können Sie die Typen von Authentifizierungsfaktoren angeben, die zulässig oder erforderlich sind:

- FIDO2
- SMS
- E-Mail

Um MFA-Faktorrichtlinien optimal nutzen zu können, müssen Sie verstehen, wie sie effektiv konfiguriert und verwaltet werden. Dies umfasst die Definition der Authentifizierungsmethoden, die Angabe von Richtlinieneingaben und -Bedingungen und die Konfiguration der Richtliniendurchsetzung (MFA-Kontext). Durch das Verständnis und die Implementierung von MFA-Faktorrichtlinien können Sie die Sicherheit und Integrität der Systeme und Daten Ihrer Organisation erheblich verbessern.

Zugehörige Informationen

Multifaktor-Authentifizierungskontext

FIDO2 als MFA-Faktor

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SMS als MFA-Faktor

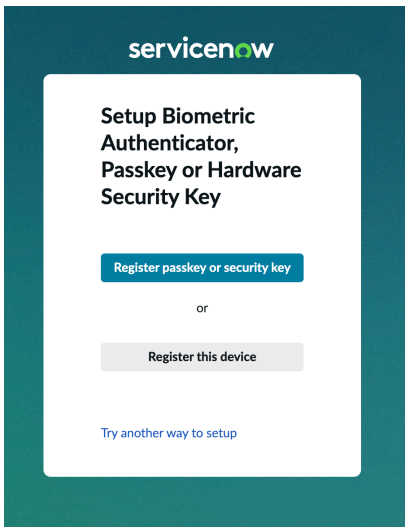
E-Mail als MFA-Faktor

FIDO2 als MFA-Faktor

Sie können FIDO2 als MFA-Faktorrichtlinie konfigurieren, um MFA für Sie zu erzwingen.

FIDO2 ist ein passwortloser Authentifizierungsstandard, mit dem Anwender sich mithilfe eines physischen Sicherheitsschlüssels oder einer biometrischen Authentifizierung authentifizieren können. Es bietet eine sicherere Alternative zu herkömmlichen MFA-Methoden und reduziert das Risiko von Phishing und anderen Cyberangriffen.

Die Erweiterung der FIDO2-Faktor-Richtlinie bietet eine sichere Authentifizierungsmethode für Ihre MFA-Richtlinien (Multifaktor Authentication). Sie können FIDO2 als MFA-Faktor-Richtlinienoption konfigurieren, die im Vergleich zu herkömmlichen Methoden wie E-Mail und SMS ein höheres Sicherheitsniveau bietet.



Sie können die FIDO2-Faktorrichtlinie konfigurieren und wenn die Anwender die Faktorrichtlinienbedingung erfüllen, während Sie sich bei anmelden ServiceNow, Das FIDO2-Setup wird für die Anwender angezeigt, die ihrem Profil noch keinen registrierten Hardwareschlüssel oder Biometrik hinzugefügt haben.

Wenn die Registrierung abgeschlossen ist, wird der zweite Bildschirm zur Faktorvalidierung angezeigt, um sich anzumelden.

Hinweis: FIDO2 kann auch von den Anwendern selbst registriert werden. Weitere Informationen zur Selbstregistrierung finden Sie unter Richten Sie die Multifaktor-Authentifizierung für Ihr Anwenderprofil ein.

Wichtige Vorteile

Im Folgenden finden Sie einige der wichtigsten Vorteile der Verwendung von FIDO2 als MFA-Faktor:

Exklusive FIDO2-Authentifizierung

Stellen Sie sicher, dass sich Accounts mit hohen Berechtigungen nur mit den starken Authentifizierungsfunktionen von FIDO2 (Biometrik, Passschlüssel oder Hardware-Sicherheitsschlüssel) authentifizieren können.

Ausschluss weniger sicherer Methoden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterdrücken Sie andere Authentifizierungsmethoden, wenn FIDO2 die einzige übereinstimmende Richtlinie ist.

Erzwungene Registrierung

Benutzer müssen einen FIDO2-Schlüssel registrieren, wenn er nicht bereits registriert ist.

Granulare Steuerung

Wenden Sie strikte Durchsetzung auf bestimmte Rollen oder Gruppen mit richtlinienbasierter Zielvorgabe an.

Als höherer Sicherheitsfaktor verfügt FIDO2 über exklusive Durchsetzungsfähigkeiten. Wenn dies die einzige übereinstimmende Richtlinie für einen Anwender ist:

- Überschreibt andere registrierte Faktoren.
- Erzwingt die FIDO2-Registrierung, wenn der Anwender nicht registriert ist.
- Wird zur exklusiven Authentifizierungsoption.

Beispielkonfigurationen und Anwenderverhalten

Die folgende Tabelle zeigt, wie verschiedene Anwenderszenarien basierend auf ihren Rollen und registrierten Faktoren behandelt werden.

Beispielanwender	Hat Rollen	Bereits registrierte Faktoren	Übereinstimmende Richtlinien	Verhalten
andrew.och	**ITIL**	Keine	FIDO2	Der Anwender wird nur mit FIDO2 zum MFA-Setup weitergeleitet. Nach der Registrierung ist FIDO2 die einzige Authentifizierungsoption.
abel.tuter	**ITIL**	Authentifikator	FIDO2	Der Anwender wird nur zum MFA-Setup mit FIDO2 weitergeleitet, auch wenn der Anwender über den Authentifikator als Selbstregistrierungsfaktor verfügt. **Hinweis:** Wenn sich der Anwender bei keinem MFA-Faktor registriert hat, wird der Anwender mit FIDO2 zum MFA-Setup weitergeleitet.
aileen.motterm	**ASSET**	Authentifikator	E-Mail	Zeigt die Optionen „E-Mail“ und „Authentifikator“ während der Anmeldung an. Der Anwender kann entweder den Faktor auswählen oder FIDO2 optional registrieren.
abraham.lincoln	**ASSET**, **ITIL**	Authentifikator	E-Mail und FIDO2	Zeigt die Option „E-Mail“ und „Authentifikator“ während der Anmeldung an. Der Anwender kann FIDO2 während der Validierung registrieren. Nach der Registrierung kann der Anwender alle 3 Faktoren anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Indem Sie FIDO2 als MFA-Faktorrichtlinie konfigurieren, können Sie die Sicherheit Ihrer Authentifizierungsprozesse erheblich verbessern.

Konfigurieren Sie FIDO2 als MFA-Faktor

Konfigurieren Sie Richtlinieneingabe und -Bedingung, um FIDO2 als MFA-Faktorrichtlinie für die Authentifizierung anzuzeigen.

Vorbereitungen
Erforderliche Rolle: Administrator

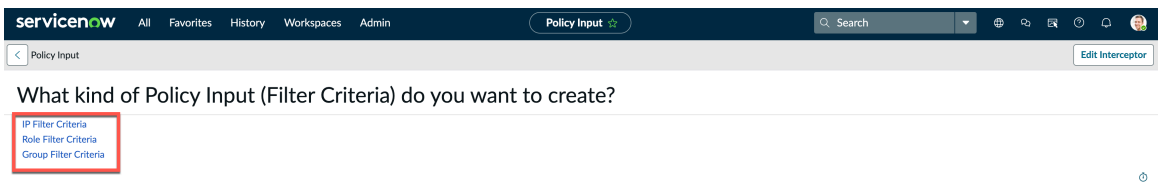
Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.
2. Wählen Sie aus **MFA-Faktorrichtlinien** Registerkarte.
3. Wählen Sie aus **Zeigen Sie FIDO2 als MFA-Faktorrichtlinie an** .
4. Wählen Sie Aus **Neu** Zum Hinzufügen **Richtlinieneingaben** .
5. Wählen Sie die Filterkriterien aus, die Sie erstellen möchten.

   Im Folgenden sind die Arten von Filterkriterien aufgeführt:

   - IP-Filterkriterien
   - Rollen-Filterkriterien
   - Gruppenfilterkriterien

   Beispiel: Rollenfilterkriterien.



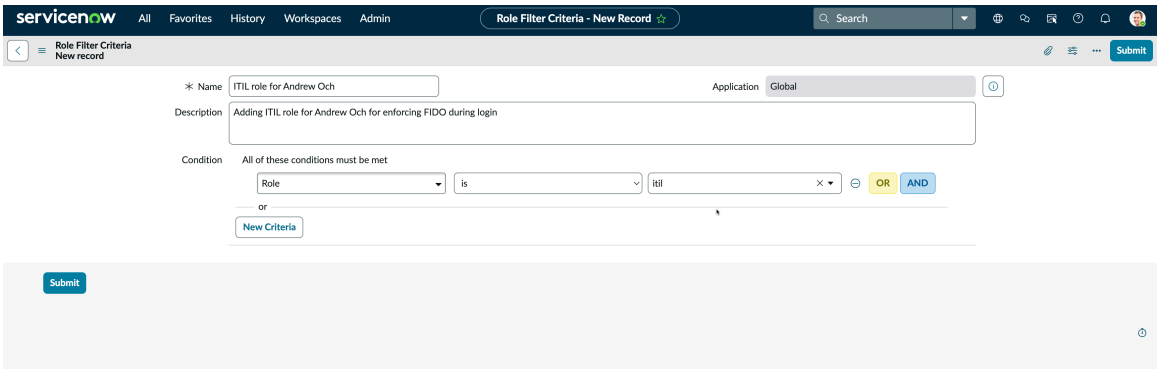
6. Wählen Sie Aus **Rollenfilterkriterien** , Füllen Sie die Felder für die Rollenfilterkriterien aus, und übermitteln Sie den Datensatz.

   Die neue Richtlinie wird erstellt. Weitere Informationen finden Sie unter Rollenfilterkriterien .

   Nehmen wir ein Beispiel für die Verwendung **ITIL** Rolle für den Anwender (**andrew.och**) Als Richtlinieneingabe und -Übermittlung.

Automatische Übersetzung

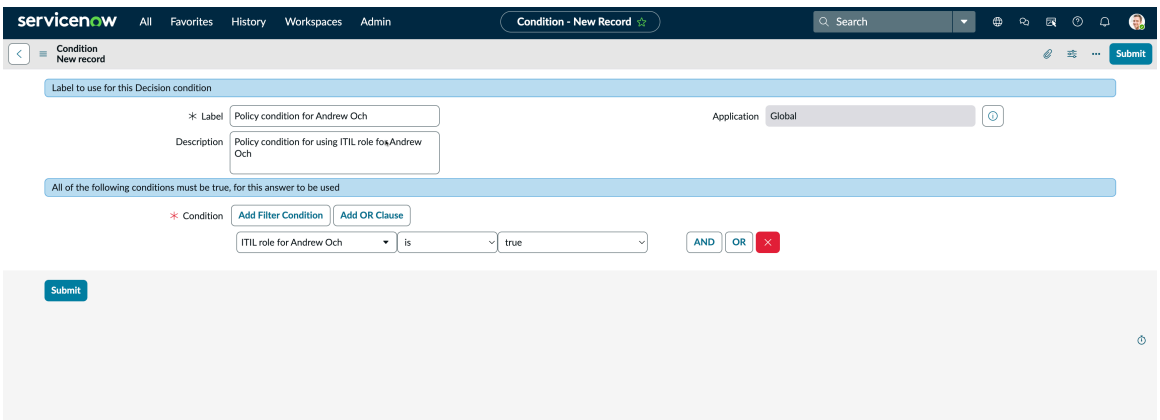
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Wählen Sie auf der Seite Richtlinie – FIDO2 als MFA-Faktor-Richtlinie anzeigen die Option aus **Richtlinienbedingungen** .
8. Wählen Sie Aus **Neu** Zum Hinzufügen von Richtlinienbedingungen.
9. Füllen Sie im Formular die Felder aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Wählen Sie die rollenbasierte Filterkriterienrichtlinie aus, die für die Bedingung erstellt wurde.

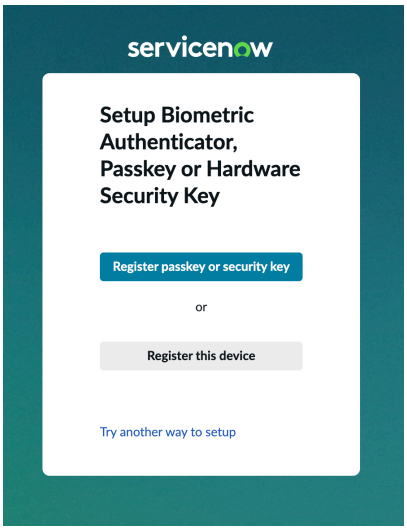


10. Wählen Sie **Absenden**.

Basierend auf der Richtlinieneingabe und -Bedingung, wenn der Anwender (**andrew.och**) Versucht, sich bei der Instanz anzumelden. Der Anwender wird als FIDO-Bildschirm angezeigt, um sich entweder zu registrieren und zu registrieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Weitere Informationen zu verschiedenen Konfigurationsbeispielen und Anwenderverhalten finden Sie unter Beispielkonfigurationen und Anwenderverhalten.

11. **Wahlweise:** Wiederholen Sie Schritt 8, um zusätzliche Richtlinienbedingungen zu erstellen.

Hinweis: Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen ODER der Ausgabe aller Richtlinienbedingungen ab. Basierend auf den Bedingungen wird die Richtlinie ausgewertet.

SMS als MFA-Faktor

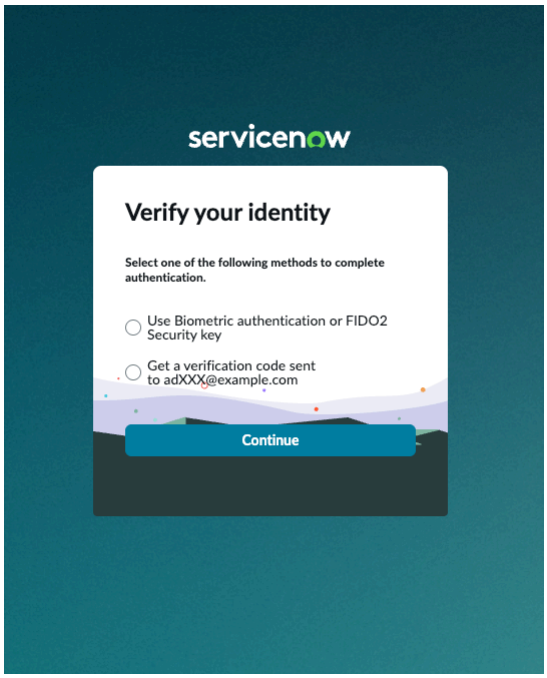
Multifaktor-Authentifizierung (MFA) mit SMS als Faktor für Ihre Authentifizierung.

Der Administrator kann konfigurieren ServiceNow Instanz, die Anwender erfordert, die versuchen, sich mit SMS-basiertem OTP anzumelden.

Wenn Anwender versuchen, sich bei anzumelden ServiceNow, SMS-OTP wird an die Mobiltelefonnummer gesendet, die dem sys_user-Datensatz zugeordnet ist. Anwender können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.

Sie können MFA mit SMS konfigurieren, indem Sie sofort einsatzbereit sind Twilio Auch. Weitere Informationen finden Sie unter Anbieter der Multifaktor-Authentifizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Darüber hinaus kann die MFA mit SMS basierend auf der Richtlinieneingabe und den Bedingungen mithilfe von Filterkriterien gesteuert werden. Im Folgenden sind die Arten von Filterkriterien aufgeführt:

- IP-Filterkriterien
- Rollen-Filterkriterien
- Gruppenfilterkriterien

Aktivieren Sie das Plugin „MFA mit SMS“

Installieren Sie für MFA mit SMS die Multifaktor-Authentifizierung mit SMS (`com.snc.authentication.sms_mfa`)-Plugin.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit der Multifaktor-Authentifizierung mit SMS installiert:

- Adaptive Authentifizierung (`Com.snc.adaptive_authentication`
- Notify – Twilio Direct-Treiber (`com.snc.notify.twilio_direct`)

Abhängiges Plugin: Integration – Multifaktor-Authentifizierung (`com.snc.integration.multifactor.authentication`)

Hinweis: Sie können die Demodaten beim Installieren des Plugins laden, wenn Sie einen anwenderdefinierten Anbieter zum Generieren der SMS konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie das Plugin „Multifaktor-Authentifizierung mit SMS“ (`com.snc.authentication.sms_mfa`) Mithilfe der Filterkriterien und der Suchleiste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

> **Hinweis:** Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Konfigurieren Sie SMS als MFA-Faktor

Konfigurieren Sie Richtlinieneingabe und -Bedingung, um SMS OTP als MFA-Faktorrichtlinie für die Authentifizierung anzuzeigen.

Vorbereitungen

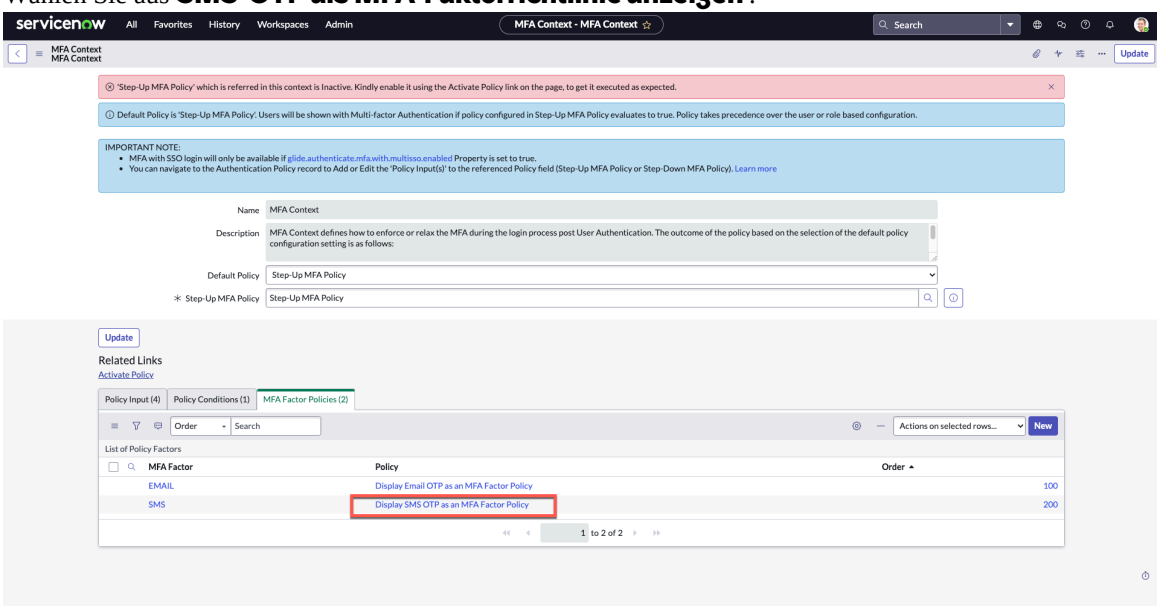
Plugin erforderlich: Multifaktor-Authentifizierung mit SMS (`com.snc.authentication.sms_mfa`).

Erforderliche Rolle: Administrator

> **Hinweis:** Die MFA-Kontextrichtlinie muss als ausgewertet werden `Wahr` Zum Anwenden der SMS-Faktorrichtlinie.

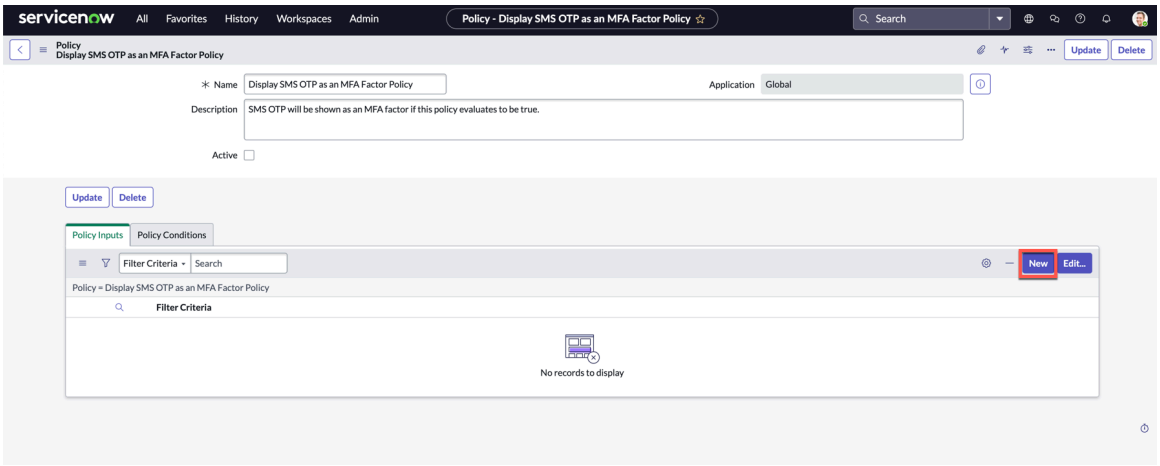
Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.
2. Klicken Sie auf **MFA-Faktorrichtlinien** Registerkarte.
3. Wählen Sie aus **SMS-OTP als MFA-Faktorrichtlinie anzeigen** .



4. Klicken Sie Auf **Neu** Zum Hinzufügen **Richtlinieneingaben** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

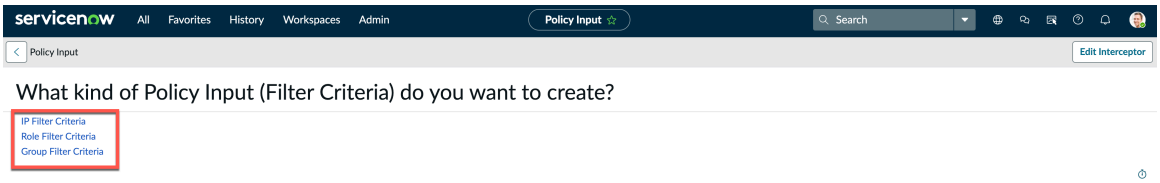


5. Wählen Sie die Filterkriterien aus, die Sie erstellen möchten.

Im Folgenden sind die Arten von Filterkriterien aufgeführt:

- IP-Filterkriterien
- Rollen-Filterkriterien
- Gruppenfilterkriterien

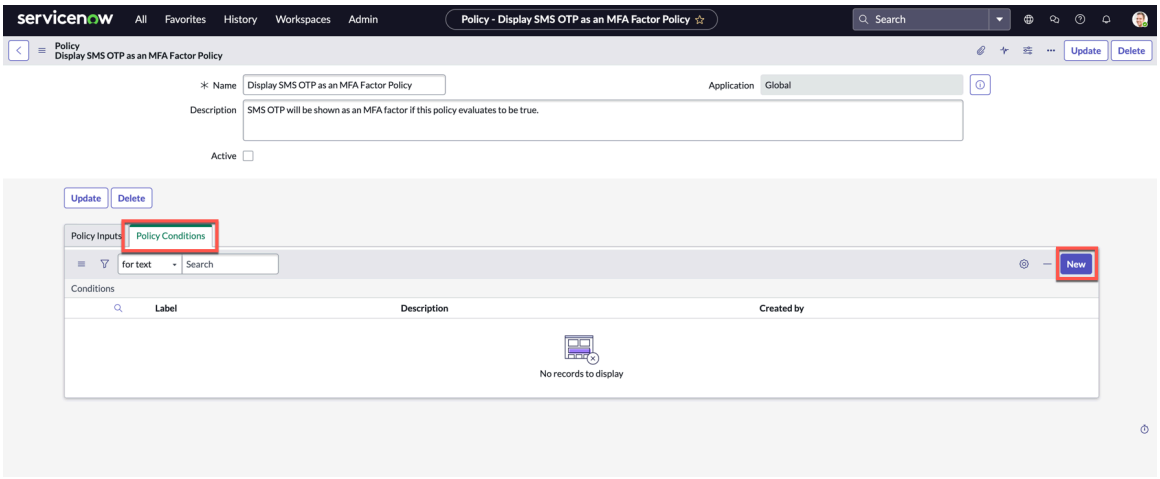
Beispiel: Rollenfilterkriterien.



6. Klicken Sie Auf **Rollenfilterkriterien** , Füllen Sie die Felder für die Rollenfilterkriterien aus, und übermitteln Sie den Datensatz.
Die neue Richtlinie wird erstellt. Weitere Informationen finden Sie unter Rollenfilterkriterien .

7. Klicken Sie auf der Seite Richtlinie – SMS-OTP als MFA-Faktor-Richtlinie anzeigen auf Richtlinienbedingungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Klicken Sie Auf **Neu** Zum Hinzufügen **Richtlinienbedingungen** .
9. Füllen Sie im Formular die Felder aus.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Wählen Sie die rollenbasierte Filterkriterienrichtlinie aus, die für die Bedingung erstellt wurde.

10. Klicken Sie auf **Absenden**.
11. **Wahlweise:** Wiederholen Sie Schritt 8, um zusätzliche Richtlinienbedingungen zu erstellen.

> **Hinweis:** Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen ODER der Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als „wahr“ ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

Basierend auf der Rollenfilter-Richtlinie (Anwender) und den für die Rolle angegebenen Bedingungen wird der Faktor „SMS als MFA“ als Option für die Authentifizierung für die Anwender angezeigt.

Anbieter der Multifaktor-Authentifizierung

Verwenden Sie MFA-Anbieter, um die SMS- und E-Mail-basierte Authentifizierung zu konfigurieren, um sicherzustellen, dass sich jeder Anwender sicher anmelden kann.

Auf der ServiceNow AI Platform, Sie können MFA-Anbieter mit dem Mechanismus zur Verwendung der Multifaktor-Authentifizierung wie E-Mail und SMS konfigurieren.

Sie können die folgende Anbieterkonfiguration verwenden, die für MFA in verfügbar ist ServiceNow AI Platform:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- E-Mail-Provider-Konfiguration
- Twilio-Provider-Konfiguration
- Infobip-Anbieterkonfiguration.

Hinweis: Twilio- und Infobip-Anbieterkonfiguration werden automatisch ausgefüllt, indem das Laden von Demodaten bei der Installation der Multifaktor-Authentifizierung mit SMS (`com.snc.authentication.sms_mfa`) Und Notify: Twilio Direct-Treiber (`com.snc.notify.twilio_direct`) Plugins.

Sie können auch eine eigene Anbieterkonfiguration erstellen, um die Multifaktor-Authentifizierung mit SMS und E-Mail zu aktivieren.

Hinweis: Die Infobip-Anbieterkonfiguration wird als Teil von Demodaten bereitgestellt. Sie können die Felder basierend auf Ihren Anforderungen für die Konfiguration Ihres eigenen Anbieters bearbeiten.

Konfigurieren Sie den MFA-Provider

Konfigurieren Sie SMS und E-Mail mit dem Anbieter, um sicherzustellen, dass sich jeder Anwender sicher anmelden kann.

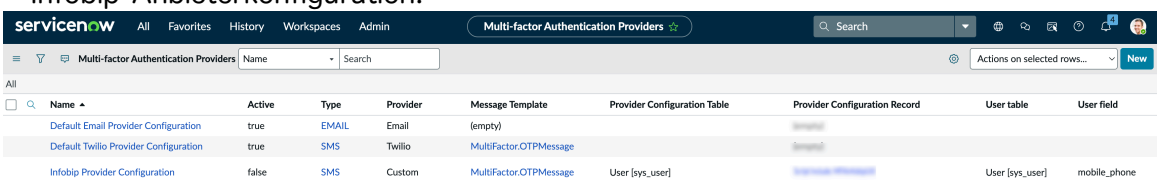
Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Anbieter**an.

   Die folgenden Anbieterkonfigurationen sind für MFA innerhalb von verfügbar ServiceNow AI Platform:

   - E-Mail-Provider-Konfiguration
   - Twilio-Provider-Konfiguration
   - Infobip-Anbieterkonfiguration.



2. Klicken Sie auf, um einen neuen Anbieter zu erstellen **Neu** .
3. Füllen Sie die Felder im Formular aus.

Formular für Bedingungen

Feld	Beschreibung
Name	Name des Datensatzes.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	Beschreibung des Datensatzes.
Anbieter	Wählen Sie Aus **Twilio** Oder **Anwenderdefiniert** . **Hinweis:** Informationen zum Konfigurieren von Twilio finden Sie unter Konfigurieren Sie Notify mit Twilio . Bei Auswahl von **Anwenderdefiniert** , Sie müssen die folgenden Felder angeben: ○ Konfigurationstabelle des Anbieters ○ Konfigurationsdatensatz des Anbieters ○ Skript ○ Anwendertabelle ○ Anwenderfeld
Nachrichtenvorlage	Die Nachrichtenvorlage für den Datensatz.
Aktiv	Option zum Aktivieren der Anbieterkonfiguration.

4. Klicken Sie auf **Absenden**.

   Basierend auf der Nachrichtenvorlage und den Anbieterkonfigurationen wird die SMS oder E-Mail als Faktor für die Authentifizierung während des Anmeldevorgangs an Anwender gesendet.

Anwenderdefinierte Konfiguration des Vonage-Providers (Tutorial)

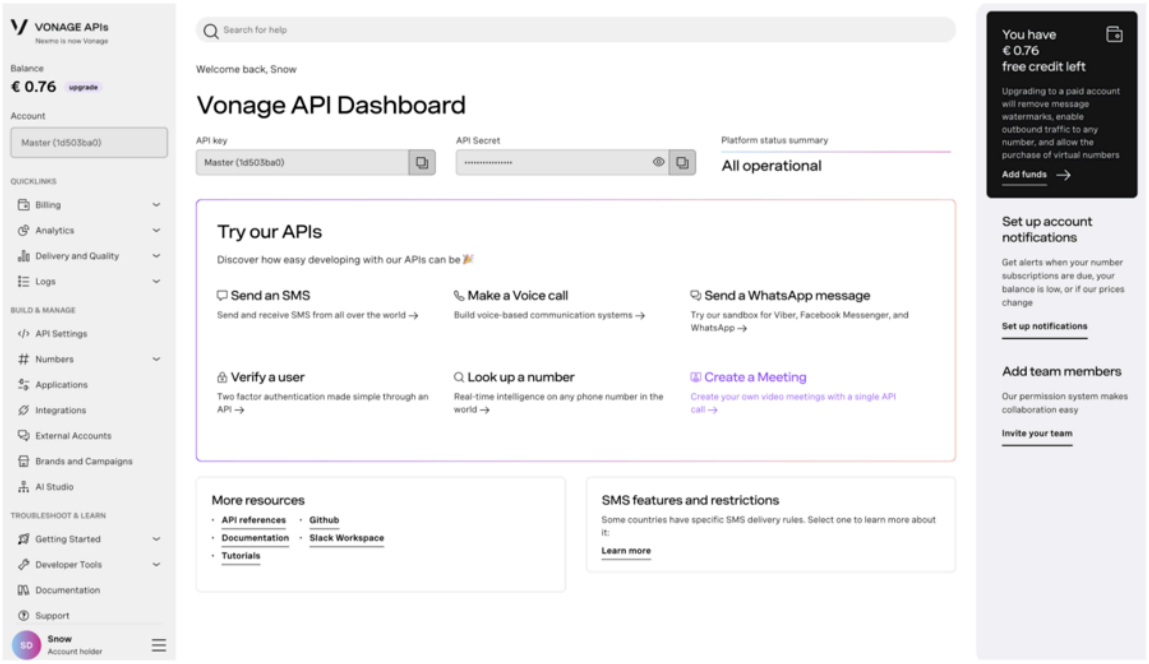
Konfigurieren Sie eine SMS mit dem Vonage-Anbieter, um sicherzustellen, dass sich jeder Anwender sicher anmelden kann.

Vorbereitungen
Erforderliche Rolle: Administrator

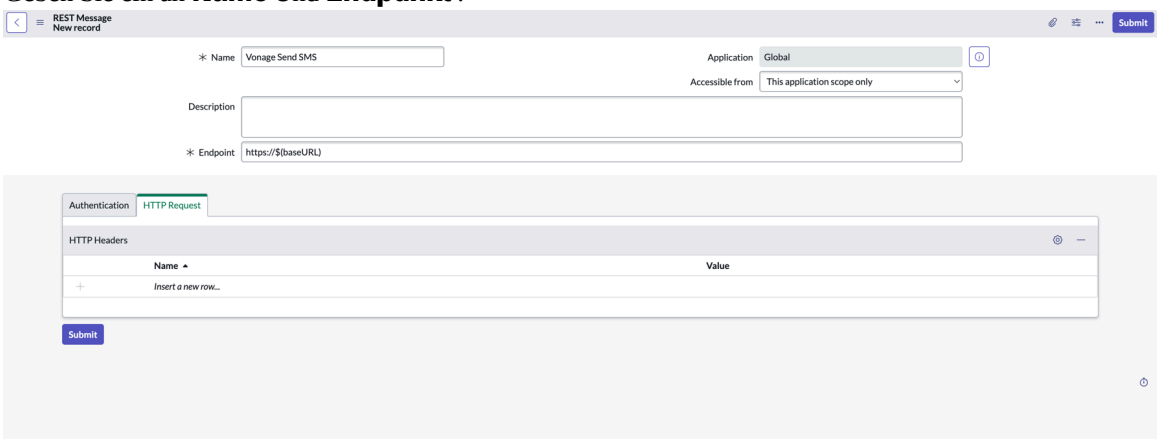
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **Ausgehend** > **REST-Nachricht** Und führen Sie die REST-Nachrichtenkonfiguration basierend auf den Informationen aus dem Vonage API-Dashboard durch.



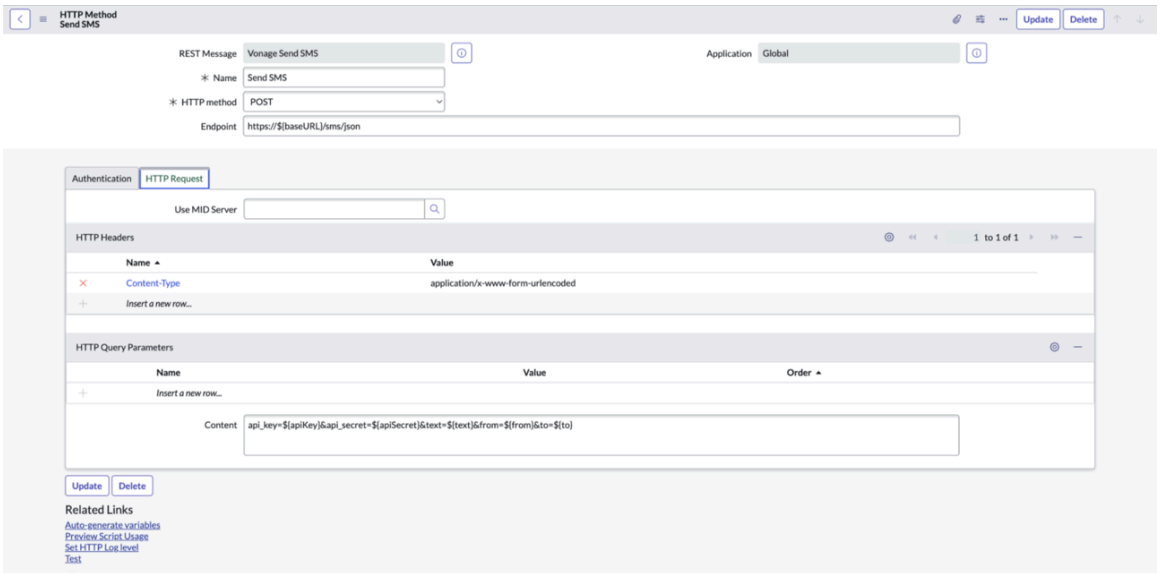
2. Klicken Sie Auf **Neu** Um eine neue zu erstellen **REST-Nachricht** .
3. Geben Sie ein an **Name** Und **Endpunkt** .



4. Klicken Sie auf **Absenden**.
5. Öffnen Sie den erstellten Datensatz im **HTTP-Methoden** Zugehörige Liste, klicken Sie auf **Neu** Und wählen Sie die HTTP-Methode als aus **VERÖFFENTLICHEN** .
6. Füllen Sie die folgenden Felder aus:
   - Endpunkt: `https://${baseURL}/sms/json`
   - Inhalt: `api_key=${apiKey}&api_Secret=${apiSecret}&Text=${Text}&from=${from}&to=${to}`
   - Inhaltstyp: `Application/x-www-Form-urlencoded`

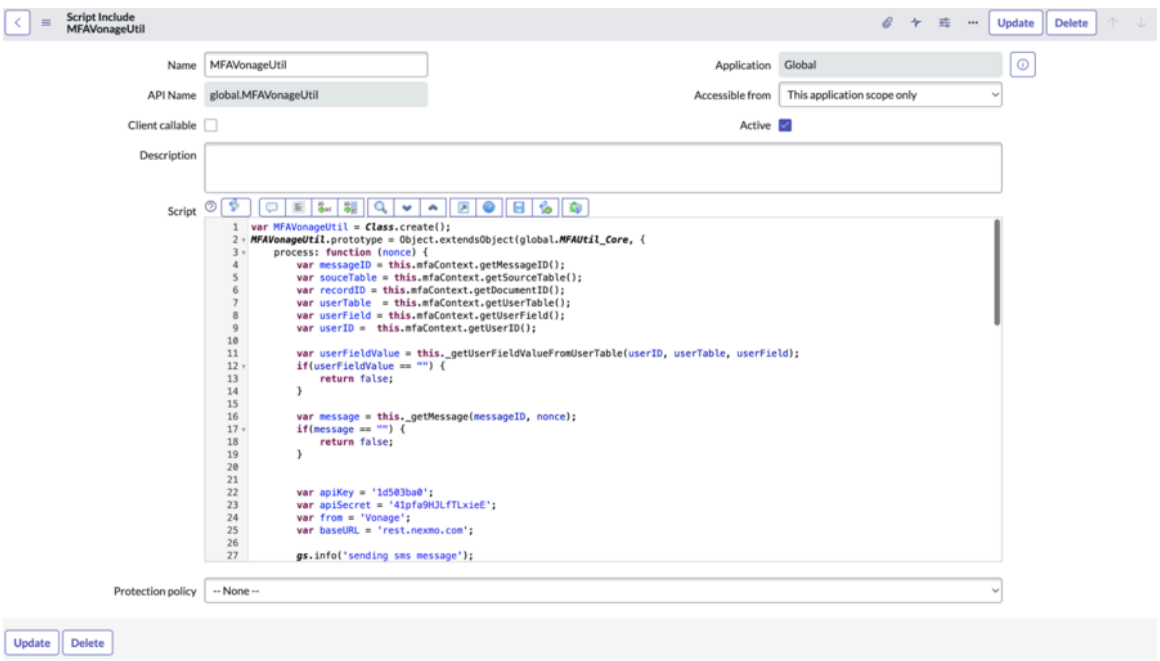
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



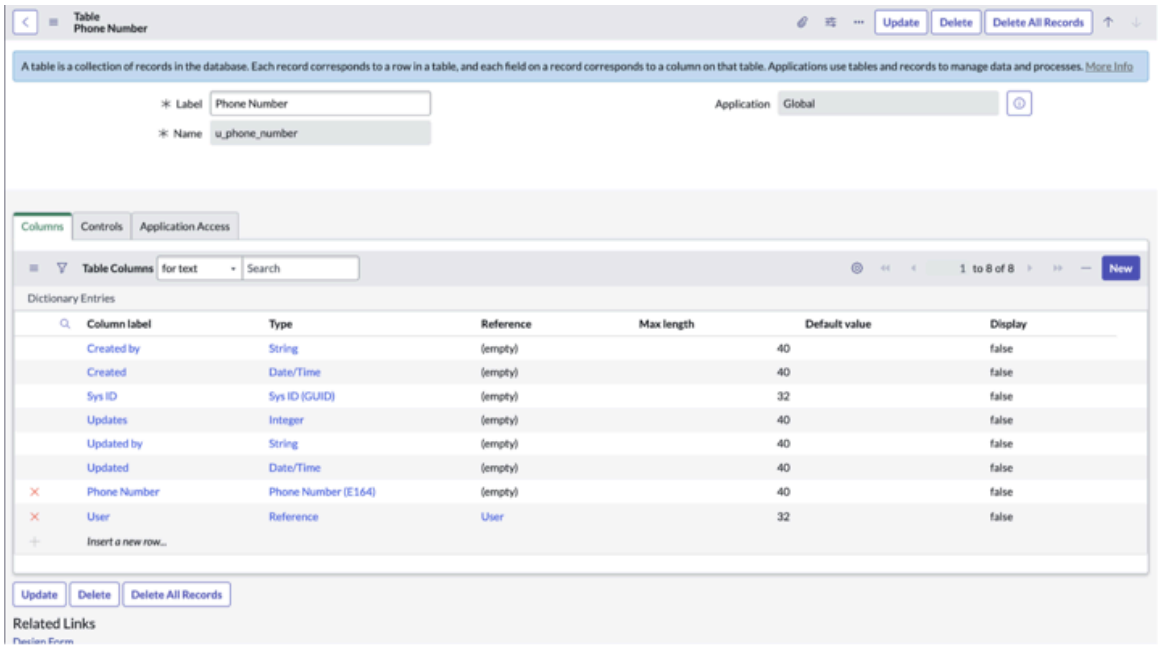
7. Aktualisieren Sie den Datensatz.
8. Klicken Sie Auf **Variablen automatisch generieren** Von **Zugehörige Links** Abschnitt.
9. Importieren Sie SI, die im Ordner freigegeben ist, und kopieren Sie den apiKey und den geheimen Schlüssel aus dem Vonage API-Dashboard.

> **Hinweis:**
>
> Der apiKey und das Geheimnis befinden sich in Ihren Vonage-Account-Einstellungen im Vonage-Dashboard.

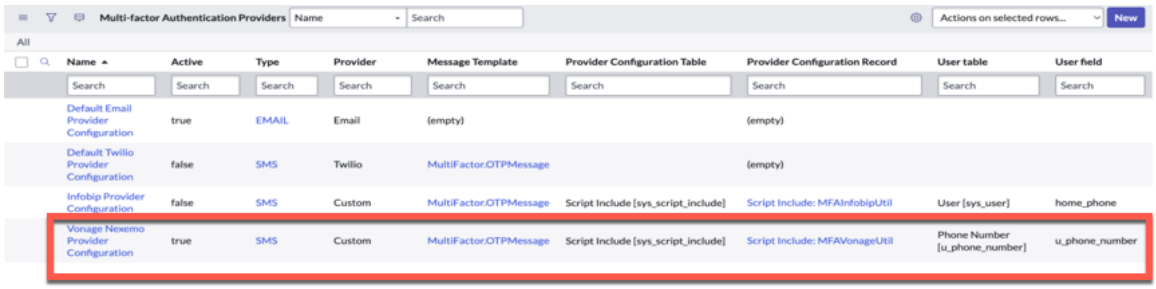


10. Erstellen Sie eine anwenderdefinierte Tabellentelefonnummern mit zwei Spalten, z. B.:
    - **Spaltenbezeichnung** : Anwender, **Typ** : Referenz, **Referenz** : Anwender (sys_user).
    - **Spaltenbezeichnung** : Telefonnummer, **Typ** : Telefonnummer (E164).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Erstellen Sie einen anwenderdefinierten Anbieter in der Multifaktor-Provider-Tabelle.



Weitere Informationen zur Anbieterkonfiguration finden Sie unter Konfigurieren Sie den MFA-Provider.

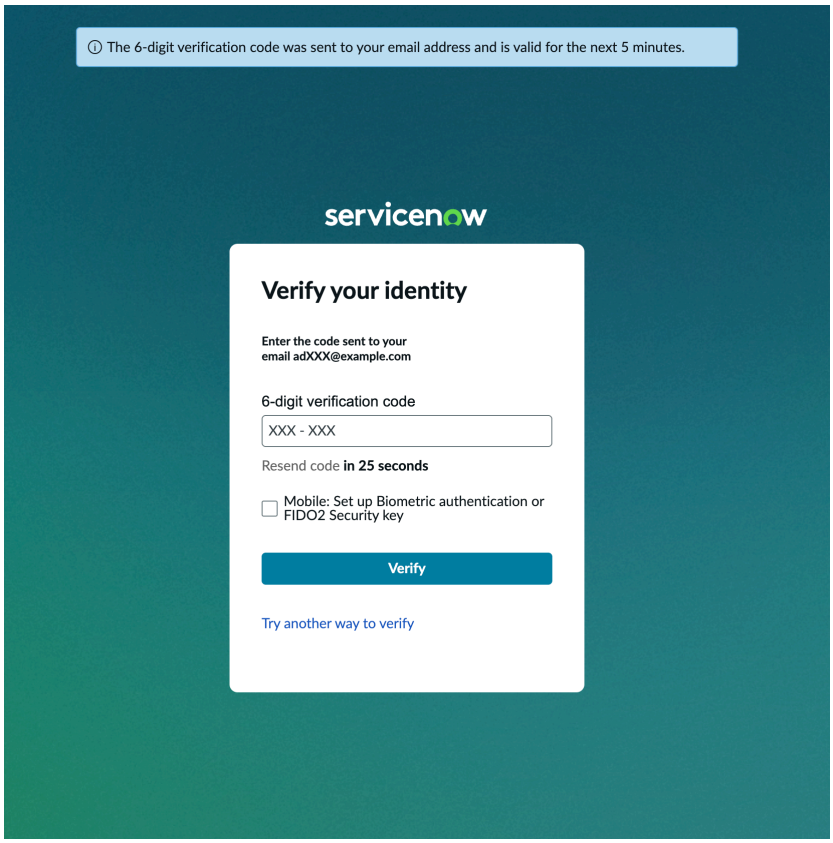
E-Mail als MFA-Faktor

Multifaktor-Authentifizierung (MFA) mit E-Mail als Faktor für Ihre Authentifizierung.

Der Administrator kann konfigurieren ServiceNow Instanz, die Anwender erfordert, die versuchen, sich mit E-Mail-basiertem OTP bei der Instanz anzumelden.

Hinweis: MFA mit E-Mail wird mit Integration – Multifaktor-Authentifizierung aktiviert (`com.snc.integration.multifactor.authentication`)-Plugin standardmäßig. Sie müssen die Richtlinieneingaben und -Bedingungen konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Anwender versuchen, sich bei anzumelden ServiceNow, E-Mail-OTP wird an die zugeordnete E-Mail-Adresse gesendet. Anwender können den sechsstelligen Verifizierungscode eingeben, der an die E-Mail-Adresse gesendet wurde, und ihre Identität überprüfen.

Konfigurieren Sie E-Mail als MFA-Faktor

Konfigurieren Sie Richtlinieneingabe und -Bedingung, um E-Mail-OTP als MFA-Faktorrichtlinie für die Authentifizierung anzuzeigen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

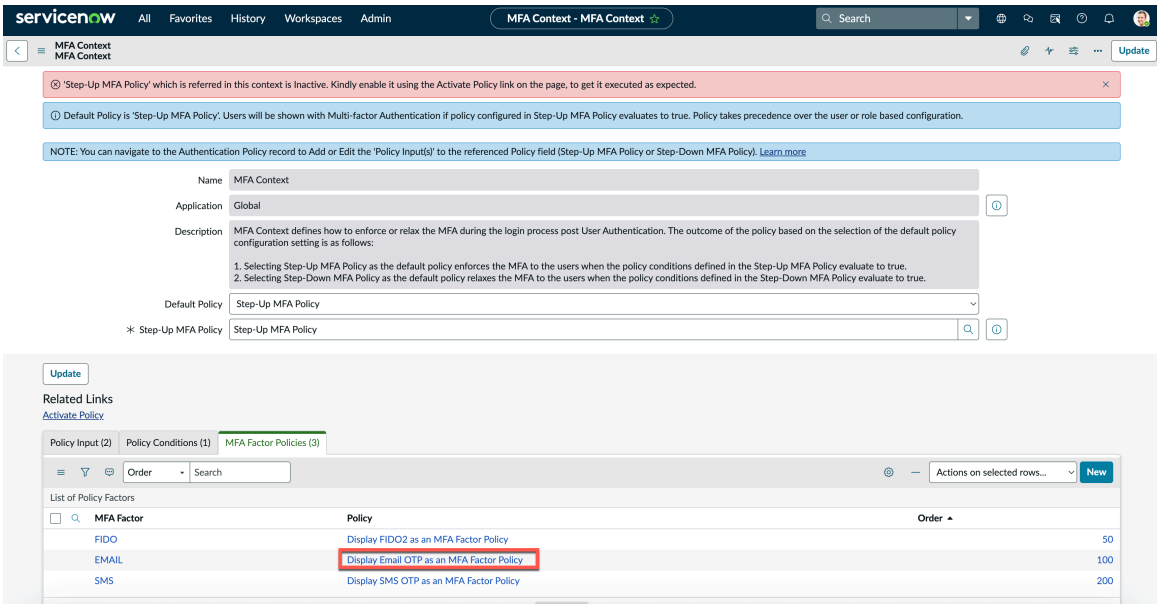
1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.
2. Klicken Sie Auf **MFA-Faktorrichtlinien** Registerkarte.

   Hinweis: Die **E-MAIL** Als **MFA-Faktor mit einer Richtlinie** Ist standardmäßig verfügbar. Sie können die Richtlinie bearbeiten und die Richtlinieneingaben und -Bedingungen angeben.

3. Wählen Sie aus **E-Mail-OTP als MFA-Faktorrichtlinie anzeigen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

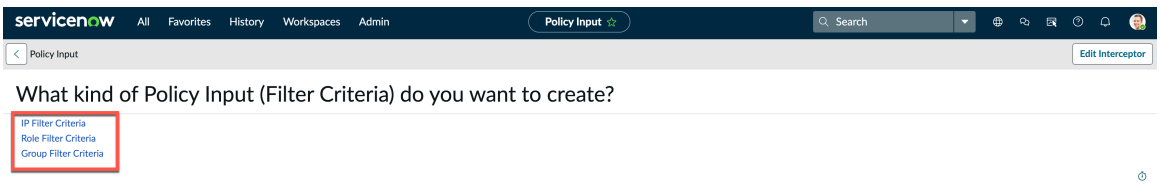


4. Klicken Sie Auf **Neu** Zum Hinzufügen **Richtlinieneingaben** .
5. Wählen Sie die Filterkriterien aus, die Sie erstellen möchten.

   Im Folgenden sind die Arten von Filterkriterien aufgeführt:

   - IP-Filterkriterien
   - Rollen-Filterkriterien
   - Gruppenfilterkriterien

   Beispiel: Rollenfilterkriterien.



6. Klicken Sie Auf **Rollenfilterkriterien** , Füllen Sie die Felder für die Rollenfilterkriterien aus, und übermitteln Sie den Datensatz.
   Die neue Richtlinie wird erstellt. Weitere Informationen finden Sie unter Rollenfilterkriterien .
7. Klicken Sie auf der Seite Richtlinie – E-Mail-OTP als MFA-Faktor-Richtlinie anzeigen auf **Richtlinienbedingungen** .
8. Klicken Sie Auf **Neu** Zum Hinzufügen **Richtlinienbedingungen** .
9. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Bedingungen

Feld	Beschreibung
Bezeichnung	Name zur Identifizierung der Bedingung.
Beschreibung	Beschreibung der Bedingung.
Bedingung	Logische Kombination aus mehreren Richtlinieneingaben (Filterkriterien), die zur Auswertung von Authentifizierungsanforderungen verwendet wird. Wählen Sie die rollenbasierte Filterkriterienrichtlinie aus, die für die Bedingung erstellt wurde.

10. Klicken Sie auf **Absenden**.
11. **Wahlweise:** Wiederholen Sie Schritt 8, um zusätzliche Richtlinienbedingungen zu erstellen.

> **Hinweis:** Wenn Sie mehrere Richtlinienbedingungen erstellen, hängt die endgültige Ausgabe der Zugriffsrichtlinie von der logischen ODER der Ausgabe aller Richtlinienbedingungen ab. Dies bedeutet, dass die Richtlinie als „wahr“ ausgewertet wird, wenn eine Ihrer Richtlinienbedingungen erfüllt ist.

Basierend auf der Rollenfilter-Richtlinie (Anwender) und den für die Rolle angegebenen Bedingungen, wird der E-Mail-MFA-Faktor als Optionen für die Authentifizierung für die Anwender angezeigt.

Systemeigenschaften der Multifaktor-Authentifizierung

Verwenden Sie Systemeigenschaften, um MFA zu aktivieren und anzupassen, um Ihre Sicherheitsanforderungen zu erfüllen.

Eigenschaften der Multifaktor-Authentifizierung

Eigenschaft	Beschreibung
`glide.authenticate.multifactor`	Aktivieren Sie die Multifaktor-Authentifizierung.
`glide.authenticate.multifactor.setup.bypass.count`	Gibt an, wie oft ein Anwender das Setup von MFA überspringen kann. Der Standardwert ist 0.
`glide.multifactor.onetime.code.validity`	Anzahl der Minuten, für die der Rücksetzcode gültig ist. Weitere Informationen finden Sie unter Melden Sie sich mit Multifaktor-Authentifizierung an. Der Standardwert ist 5. **Hinweis:** Diese Eigenschaft gilt für die E-Mail-OTP-Validierungszeit.
`glide.authenticate.multifactor.clock_skew`	Anzahl der zusätzlichen Sekunden, für die der Rücksetzcode gültig ist. Der Höchstwert beträgt `60` . Der Standardwert ist `10`. Die Instanz validiert den vom Anwender eingegebenen Code mit dem einzelnen App-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Multifaktor-Authentifizierung (Fortsetzung)

Eigenschaft	Beschreibung
	generierten Code, der in generiert wird Aktuelle Uhrzeit . Sie können das Zeitfenster mit dieser Eigenschaft verzerren und zulassen, dass während eines Zeitfensters ein oder mehrere Codes als gültig gelten. Der Wert der Eigenschaft wird in der folgenden Berechnung verwendet: Aktuelle Zeit – X/2 Und Aktuelle Zeit + X/2 , Wo X Ist der Wert dieser Eigenschaft. Wenn Sie den Wert von verwenden 10 , Beispielsweise berücksichtigt die Instanz alle Codes, die die App innerhalb des Zeitbereichs generiert [Aktuelle Zeit – 5 Sekunden] Und [Aktuelle Zeit + 5 Sekunden] Gültig sein. Verwenden Sie diese Eigenschaft, um Anmeldungsprobleme zu verhindern, bei denen der Anwender in der zugewiesenen Standardzeit nicht den richtigen Code eingeben kann.
glide.authenticate.multifactor.remember.browser.enable	Legen Sie hier fest, dass ein Anwender zur MFA aufgefordert wird, wenn er sich über ein neues Gerät oder einen neuen Browser anmeldet. Der Standardwert ist „Ja“.
glide.authenticate.multifactor.browser.validity	Nachdem sich ein Anwender für diese Dauer nicht mehr für MFA im selben Browser angefordert. Der Standardwert ist 8 Stunden.
glide.authenticate.multifactor.remember.browser.max	Die maximale Anzahl der Browser-Cookie-Erinnerungen für diesen Anwender.
glide.authenticate.multifactor.remember.browser.default	Standardwert des Kontrollkästchens „Browser speichern“ auf der Seite „Multifaktor validieren“.
glide.webauthn.enabled)	Option zum Aktivieren passwortloser Authentifizierungsmethoden (FIDO2-basierte MFA) wie Hardwareschlüssel und biometrische Authentifizierung.
glide.authenticate.multifactor.email.otp.enable	Option zum Aktivieren von E-Mail-basiertem OTP als Faktor für MFA.
glide.auth.mfa.ui.v2.enabled	Option zum unabhängigen Aktivieren des MFA-Faktors für die Anwender, ohne eine Authentifikator-App einzurichten.

Multifaktor-Authentifizierungskriterien

Verwenden Sie MFA-Kriterien, um zu bestimmen, welche Anwender und Rollen eine zweistufige Verifizierung verwenden müssen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multifaktor-Kriterien

Verwenden Sie MFA-Kriterien, um zu bestimmen, welche Anwender und Rollen eine zweistufige Verifizierung verwenden müssen. Sie können eines dieser Kriterien oder eine Kombination davon verwenden, um Ihre Geschäftsanforderungen zu erfüllen. Sie können eines dieser Kriterien oder eine Kombination davon verwenden, um Ihre Geschäftsanforderungen zu erfüllen.

Hinweis: Es wird empfohlen, die richtlinienbasierte MFA für die adaptive Authentifizierung zu verwenden.

Anwenderbasierte Multifaktor-Kriterien

Verwenden Sie anwenderbasierte Multifaktor-Kriterien, um einzelne Anwender auszuwählen, die sich mit MFA anmelden müssen. -Administratoren aktualisieren **Aktivieren Sie Die Multifaktor-Authentifizierung** Feld in einem Anwenderdatensatz zum Aktivieren oder Deaktivieren von MFA-Anforderungen für einen Anwender. Details zu diesem Vorgang finden Sie unter Konfigurieren Sie anwenderbasierte Multifaktor-Kriterien.

Rollenbasierte Multifaktor-Kriterien

Verwenden Sie rollenbasierte Multifaktor-Kriterien, um die MFA-Anmeldung für alle Anwender zu erfordern, die einer bestimmten Rolle zugewiesen sind. Die **Rollenbasierte Multifaktor-Authentifizierung** Datensatz in **Multifaktor-Kriterien** Die Tabelle [Multi_factor_Criteria] enthält die Liste der Rollen, die eine MFA-Anmeldung erfordern. Weitere Informationen zum Verwalten dieser Liste finden Sie unter Konfigurieren Sie rollenbasierte Multifaktor-Kriterien.

Richtlinienbasierte Multifaktor-Kriterien für die adaptive Authentifizierung

Verwenden Sie die adaptive Authentifizierung, um zu bestimmen, wann Ihre Instanz MFA erfordert. Die adaptive Authentifizierung verwendet Authentifizierungsrichtlinien, um Kriterien wie die IP-Adresse oder Anwendergruppen eines Anwenders auszuwerten. Weitere Informationen zur Funktion der adaptiven Authentifizierung finden Sie unter Adaptive Authentifizierung.

Konfigurieren Sie anwenderbasierte Multifaktor-Kriterien

Verwenden Sie anwenderbasierte Multifaktor-Kriterien, um MFA für einen Anwender zu aktivieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.
2. Konfigurieren Sie die Liste so, dass sie angezeigt wird **Aktivieren Sie die Multifaktor-Authentifizierung** Spalte.
3. Ändern Sie die Werte von **Aktivieren Sie die Multifaktor-Authentifizierung** Spalte für die ausgewählten Anwender bis **Wahr** .

   Wenn sich der Anwender mit seinem Anwendernamen und Passwort anmeldet, wird er aufgefordert, die Multifaktor-Authentifizierung einzurichten.

Konfigurieren Sie rollenbasierte Multifaktor-Kriterien

Verwenden Sie rollenbasierte Multifaktor-Kriterien, um die Multifaktor-Authentifizierung für alle Anwender zu erzwingen, die bestimmten Rollen zugewiesen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Multifaktor-Kriterien**an.
2. In **Multifaktor-Kriterien** Liste, öffnen Sie **Rollenbasierte Multifaktor-Authentifizierung** Datensatz.
3. Verwenden Sie **Multifaktor-Rollen** Liste zum Hinzufügen oder Entfernen von Rollen.

Option	Bezeichnung
Eine Rolle hinzufügen	Doppelklicken Sie auf **Neue Zeile einfügen...** Und geben Sie einen Rollennamen ein, oder wählen Sie ihn aus. Klicken Sie auf **Symbol „Speichern“** ( ), um den Eintrag zu speichern.
Entfernen Sie eine Rolle	Klicken Sie auf das Löschsymbol ( ), um eine Rolle aus der Liste zu entfernen.

4. Klicken Sie auf **Aktualisieren**.

Ergebnis
Ihre Instanz erzwingt die Multifaktor-Authentifizierung für alle Anwender, die Mitglieder der in aufgeführten Rollen sind **Multifaktor-Rollen** Liste.

Wichtig: Der Datensatz muss aktiv sein, um die rollenbasierte Multifaktor-Authentifizierung zu erzwingen.

Konfigurieren Sie richtlinienbasierte Multifaktor-Kriterien für die adaptive Authentifizierung

Verwenden Sie adaptive Richtlinien, um zu bestimmen, welche Anwender die zweistufige Multifaktor-Verifizierung (MFA) verwenden müssen.

Vorbereitungen
Erforderliche Rolle: Administrator

Hinweis:

- Wenn die Standardrichtlinie ist **STEP-up-MFA-Richtlinie** , Anwender werden mit Multifaktor-Authentifizierung angezeigt, wenn die Richtlinie in konfiguriert ist **STEP-up-MFA-Richtlinie** Wird als „wahr“ ausgewertet. Richtlinie hat Vorrang vor der Anwender- oder rollenbasierten Konfiguration.
- MFA mit SSO-Anmeldung ist nur verfügbar, wenn `glide.authenticate.mfa.with.multisso.enabled` Eigenschaft ist auf „wahr“ festgelegt.
- Sie können zum Datensatz der Authentifizierungsrichtlinie navigieren, um „Richtlinieneingabe(en)“ zum Feld „Referenzierte Richtlinie“ hinzuzufügen oder zu bearbeiten (**STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie**).

Prozedur

1. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Kontexte der Authentifizierungsrichtlinie** > **MFA-Kontext**an.
   Die **MFA-Kontext** Richtlinienkontextdatensatz wird geöffnet.
2. Wählen Sie die Standardrichtlinie in aus **Standardrichtlinie** Feld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Auswahl bestimmt, wie Ihre Instanz die Richtlinienbedingungen verwendet, um zu bestimmen, ob MFA erforderlich ist.

Standardrichtlinien

Standardrichtlinie	Definition
Step-Up-MFA-Richtlinie	Wählen Sie diese Option aus, um MFA zu erzwingen, wenn die Richtlinienbedingungen in definiert sind **STEP-up-MFA-Richtlinie** Auswertung auf „wahr“.
Step-Down-MFA-Richtlinie	Wählen Sie diese Option aus, um MFA zu umgehen, wenn die Richtlinienbedingungen in definiert sind **STEP-Down-MFA-Richtlinie** Auswertung auf „wahr“.

3. In **STEP-up-MFA-Richtlinie** Wählen Sie eine Richtlinie aus, die mit diesem Kontext verwendet werden soll.
4. Klicken Sie auf **Aktualisieren**.
   Nach dem Speichern des Datensatzes wird **Richtlinieneingabe** Und **Richtlinienbedingungen** Listen aktualisieren, um die Richtlinieneingaben und -Bedingungen anzuzeigen, die der in ausgewählten Richtlinie zugeordnet sind **STEP-up-MFA-Richtlinie** Feld.

Multifaktor-Authentifizierung mit Single Sign-on

Sie können MFA mit einem SSO-Anbieter für verwenden ServiceNow Instanz.

Da sich viele Anwender in Ihrer Organisation bei Ihrem Unternehmensnetzwerk anmelden und auf zugreifen ServiceNow Instanz besteht ein stärkerer Bedarf an einer sicheren Authentifizierung.

MFA mit der Kombination von SSO bietet eine verbesserte Sicherheit für Ihre Instanz. Diese Fähigkeit bietet Flexibilität, MFA für Anwender bedingt zu aktivieren.

Hinweis:

- ServiceNow MFA wird erzwungen, nachdem der Anwender nach der erfolgreichen Authentifizierung beim Identitätsanbieter umgeleitet wurde.
- MFA wurde vor dem San Diego-Release nicht mit SSO erzwungen.

Wenn Sie beispielsweise Ihren externen Anwendern ein zusätzliches Sicherheitsprotokoll geben möchten, können Sie MFA nur für diese Anwender erzwingen. Auf diese Weise können Sie zusätzliche Authentifizierungsfunktionen hinzufügen und Ihren Anwenderzugriff steuern.

Für SSO-basierte Anmeldungen wie SAML, OpenID Connect und Digest können Sie MFA für die Authentifizierung erzwingen.

MFA mit SSO kann je nach Anforderung konfiguriert werden. Mit Hilfe von Authentifizierungsschemata und Identitätsanbietern können Sie MFA für bestimmte Anwender mit einem bestimmten Anmeldemechanismus erzwingen.

Sie können MFA für die folgenden Bedingungen erzwingen:

- Authentifizierungsschema
- Identitätsanbieter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA mit SSO wird als Teil des Plugins „Adaptive Authentication“ (com.snc.adaptive_authentication) angeboten. Weitere Informationen zum Einrichten der adaptiven Authentifizierung finden Sie unter Adaptive Authentifizierung.

Konfigurieren von MFA mit SSO

Erzwingen Sie MFA mit SSO für Ihre Anwender innerhalb oder außerhalb Ihrer Organisation.

Vorbereitungen

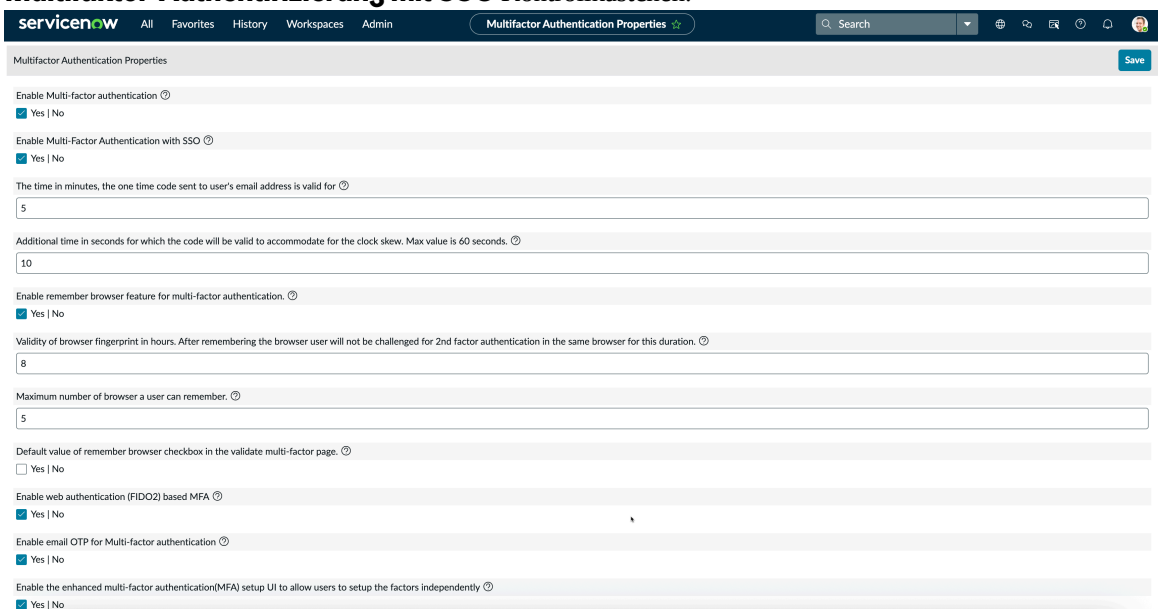
Die MFA mit SSO-Funktion wird als Teil des Plugins „Adaptive Authentication“ (com.snc.adaptive_authentication) angeboten. Sie müssen die Eigenschaft „Adaptive Authentifizierung“ für die Verwendung der MFA mit SSO-Funktion aktivieren. Weitere Informationen zum Einrichten der adaptiven Authentifizierung finden Sie unter Adaptive Authentifizierung.

Hinweis: MFA mit SSO-Anmeldung ist verfügbar, wenn `glide.authenticate.mfa.with.multisso.enabled`Eigenschaft ist auf festgelegt **Wahr** .

Erforderliche Rolle: Administrator

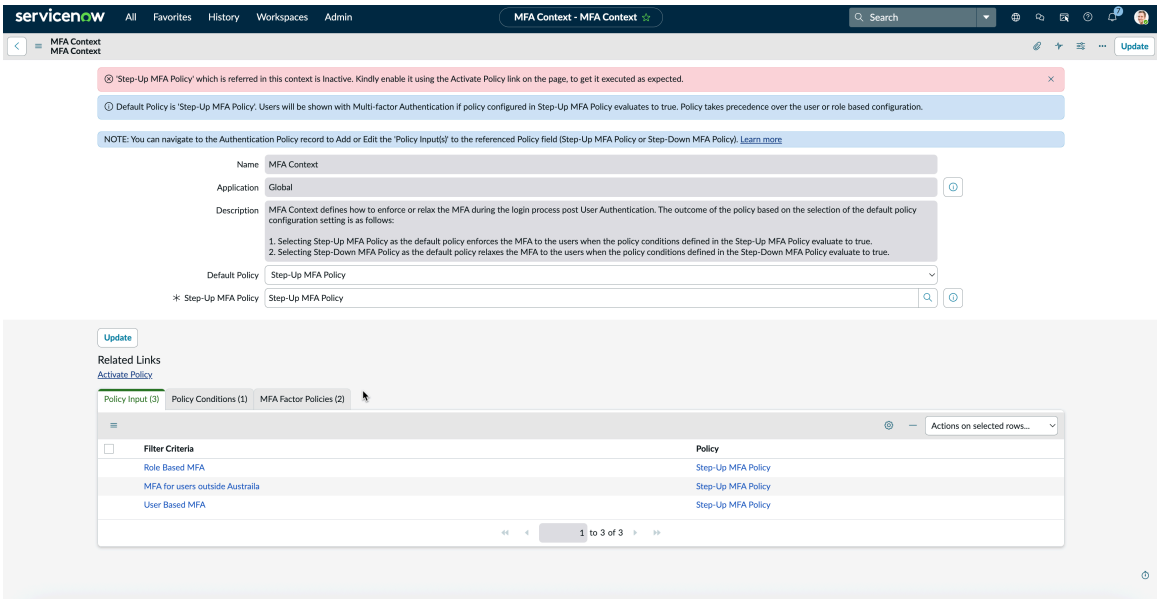
Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Eigenschaften**an.
2. Aktivieren Sie **Aktivieren Sie die Multifaktor-Authentifizierung** Und **Aktivieren Sie die Multifaktor-Authentifizierung mit SSO** Kontrollkästchen.



3. Klicken Sie auf **Speichern**.
4. Navigieren zu **Multi-Faktor-Authentifizierung** > **MFA-Kontext**an.
   Das Formular „MFA-Kontext“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



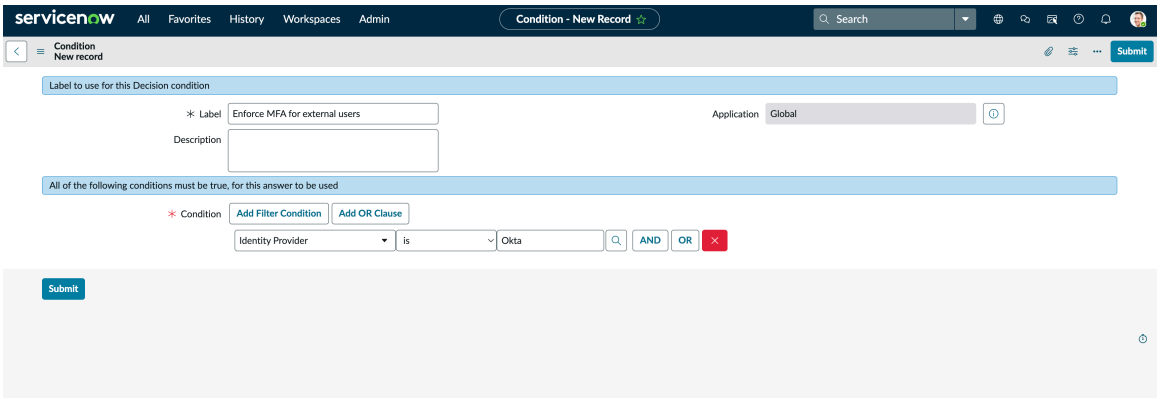
Hinweis: Standardmäßig lautet die Richtlinie **STEP-up-MFA-Richtlinie** . Anwender werden mit Multifaktor-Authentifizierung angezeigt, wenn eine Bedingung in konfiguriert ist **STEP-up-MFA-Richtlinie** Wird ausgewertet bis **Wahr** . Richtlinie hat Vorrang vor der Anwender- oder rollenbasierten Konfiguration.

5. **Wahlweise:** Um eine Richtlinie zu bearbeiten, kehren Sie zum Datensatz der Authentifizierungsrichtlinie zurück, ändern Sie die Bedingungen, und kehren Sie zurück.
   Wenn Sie zum Datensatz der Authentifizierungsrichtlinie navigieren, können Sie den referenzierten Richtlinienfeldern „Richtlinieneingaben“ hinzufügen oder bearbeiten. **STEP-up-MFA-Richtlinie** Oder **STEP-Down-MFA-Richtlinie** .
6. Um eine neue Richtlinienbedingung festzulegen, klicken Sie auf **Richtlinienbedingungen** .
7. Klicken Sie auf **Neu**.
8. Füllen Sie im Formular die Felder aus.

Formular „Bedingungen“

Felder	Beschreibung
Bezeichnung	Eindeutiger Name für die Bedingung, die Sie für die Bezeichnung erstellen möchten.
Beschreibung	Die Beschreibung der Richtlinienbedingung.
Bedingungen	Der Typ der Bedingung, die Sie für die Richtlinie anwenden möchten. Sie können Filterbedingungen und „ODER“-Klauseln hinzufügen. **Hinweis:** Durch das Hinzufügen verschiedener Filterbedingungen und -Klauseln können Sie MFA für bestimmte Anwender herausfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Example

Betrachten Sie das folgende Beispiel, um Ihre Bedingungen einzurichten. Angenommen, Sie möchten das Authentifizierungsschema mit dem Identitätsanbieter als Bedingung für externe Anwender verwenden. Sie können die Bedingungen wie folgt festlegen:

a. Wählen Sie Aus **Authentifizierungsschema** Und legen Sie die Kriterien als fest **Single Sign-On** Oder **Anwendername und Passwort** .

   Basierend auf dieser Auswahl wird dem Anwender ein SSO-basiertes Anmelde- oder Anmeldeformular zur Angabe des Anwendernamens und Passworts bereitgestellt.

b. Wählen Sie Aus **Identitätsanbieter** Und geben Sie den Anbieter als IDP-Datensatz an, für den Sie MFA aktivieren möchten. Beispiel: **Okta** .

   Basierend auf dieser Auswahl wird der Anwender, wenn er sich mit SSO anmeldet, nicht mit MFA herausgefordert. Im Gegensatz dazu, wenn sich der Anwender mit anmeldet Okta, Dann wird der Anwender mit MFA herausgefordert.

9. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Adaptive Authentifizierung

Multifaktor-Authentifizierung mit Single Sign-on

Multifaktor-Authentifizierung (MFA) für Anwender zurücksetzen

Administratoren können MFA für Anwender zurücksetzen, die die App gelöscht haben, den Zugriff auf das Gerät verloren haben oder ihrem Gerät keine alternative MFA zugeordnet ist.

Vorbereitungen

Erforderliche Rolle: Administrator

Im folgenden Verfahren wird beschrieben, wie ein ServiceNow® Der Administrator kann die MFA-Validierung zurücksetzen, um Anwender zu entsperren und sie in die Lage zu versetzen, MFA erneut zu registrieren.

Prozedur

1. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Anwendereinrichtung**an.
2. Suchen Sie nach dem Anwender, den Sie entsperren möchten.
3. Legen Sie Validieren auf fest **Falsch** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Webauthentifizierung** > **Öffentliche Anmeldeinformationen des Anwenders (sys_user_public_credential**an.
5. Suchen Sie nach dem Anwender, den Sie entsperren möchten.
6. Löschen Sie alle Datensätze für diesen Anwender.
7. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Aktuelle Anwenderfaktoren Des Anwenders**an.
8. Suchen Sie nach demselben Anwender.
9. Löschen Sie alle Datensätze für diesen Anwender.

Ergebnis

Wenn der entsperrte Anwender die Anmeldeinformationen eingibt und sich anmeldet, wird der **Multifaktor-Authentifizierung (MFA) aktivieren** Seite wird angezeigt. Der Anwender kann die Schritte auf der Seite ausführen, um MFA erneut zu registrieren.

Referenzthema – Multifaktor-Authentifizierung

Referenzthema im Zusammenhang mit der Konfiguration von MFA.

Multifaktor-Authentifizierung für Anwender

Um auf die Details zur MFA des Anwenders zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Anwendereinrichtung**an.

Multifaktor-Authentifizierung für Anwender

Feld	Beschreibung
Anwender	Der Anwendername des Anwenders
Verbleibende Umgehungen	Die Gesamtzahl der Umgehungen, die für den Anwender verbleiben.
Multifaktor-Geheimnis	Die Details des Multifaktor-Geheimnisses.
Überprüft	Ist der Multifaktor validiert. Der Wert wird in geändert **Falsch** Macht das vorhandene Setup der Authentifikator-App ungültig.

Hinweis: Die von den Anwendern zuletzt verwendeten MFA-Faktoren sind im Modul „zuletzt verwendete Faktoren“ des Anwenders verfügbar. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Aktuelle Anwenderfaktoren Des Anwenders**an. Weitere Informationen finden Sie unter Zuletzt verwendete Faktoren des Anwenders.

Mehrstufige Browser-Fingerabdrücke

Um auf die Details zu den Browser-Fingerabdrücken des Anwenders zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **Mehrstufige Browser-Fingerabdrücke**an.

Mehrstufige Browser-Fingerabdrücke

Feld	Beschreibung
Anwender	Der Anwendername des Anwenders
Browser	Der vom Anwender verwendete Browser.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrstufige Browser-Fingerabdrücke (Fortsetzung)

Feld	Beschreibung
Browser-Fingerabdruck	Die Details des Browser-Fingerabdrucks.
Cookie des Browser-Fingerabdrucks	Die Details des Browserfingerabdruck-Cookies.
Ablauf des Browser-Fingerabdruckcookies	Die Details zum Ablauf des Browserfingerabdruck-Cookies.

Zuletzt verwendete Faktoren des Anwenders

Um auf die Details zu den zuletzt verwendeten Faktoren des Anwenders zuzugreifen, navigieren Sie zu **Alle** > **Multi-Faktor-Authentifizierung** > **Aktuelle Anwenderfaktoren Des Anwenders**an.

Multifaktor-Setups für Anwender

Feld	Beschreibung
Anwender	Der Anwendername des Anwenders
Multifaktor-Typ	Der Multifaktor-Typ, den der Anwender für die Anmeldung verwendet hat.
Ist aktueller Faktor	Die letzten Multifaktor-Ziele des Anwenders.

MFA-Metriken

Zeigen Sie die verschiedenen MFA-Metriken an, um die Einführung und Nutzung von MFA zu verstehen.

MFA-bezogene Metriken sind im Sicherheitscenter verfügbar. Das Sicherheitscenter ist eine kostenlose Anwendung, die Sie aus dem herunterladen können ServiceNow Speichern. Weitere Informationen zum Sicherheitscenter finden Sie unter Zielseite des Sicherheitszentrums.

Verwenden Sie im Sicherheitscenter die Leiste oben auf der Seite, um zwischen den Abschnitten der Sicherheitsüberwachungskonsole zu navigieren und auszuwählen **Sicherheitsmetriken** Registerkarte.

Im Folgenden finden Sie die MFA-Metriken:

- Für MFA registrierte Anwender: Gesamtanzahl der Anwender, die für die Verwendung von MFA registriert sind.
- Anwender, die MFA-Umgehung verwenden: Gesamtanzahl der Anwender, die die Multifaktor-Authentifizierung umgehen.
- Anwender mit hohen Berechtigungen ohne mfa: Gesamtanzahl der Anwender mit hohen Berechtigungen, die MFA nicht verwenden.
- Aktive MFA-Anwender: Gesamtanzahl der MFA-Anwender, die in Ihrer Instanz aktiv sind.
- Gesperrte MFA-Anwender: Gesamtanzahl der MFA-Anwender, die in Ihrer Instanz gesperrt sind.
- Lokale Anmeldungen, die nicht durch MFA geschützt sind: Anwender, die sich ohne MFA angemeldet haben.

Weitere Informationen zu Sicherheitsmetriken finden Sie unter Sicherheitsmetriken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multifaktor-Authentifizierung wird verwendet

Erfahren Sie, wie Sie Multifaktor-Authentifizierungstools verwenden, um sicher auf Ihre Instanz zuzugreifen.

Melden Sie sich bei MFA an

ServiceNow Erfordert Authentifikatoranwendungen, die zeitbasierte Einmalpasswörter (TOTP) unterstützen. ServiceNow Testet MFA mit den folgenden Authentifikatoren:

- Google Authentifikator
- Microsoft Authentifikator
- LastPass-Authentifikator
- Authy
- FreeOTP
- Duo
- Okta Verifizieren

Hinweis:

- Andere nicht aufgelistete Authentifikatoren sind möglicherweise ebenfalls kompatibel, werden jedoch nicht von getestet ServiceNow.
- Informationen zu browserspezifischen Verhaltensänderungen finden Sie hier KB-artikel .

Registrieren Sie eine Authentifizierungs-App

Authentifikator-App Sie können Authentifikator-Apps verwenden, um einen zweiten Authentifizierungsfaktor zu verwenden.	Wenn Ihr Administrator Multifaktor-Authentifizierung (MFA) in Ihrer Instanz aktiviert hat, werden Sie nach Eingabe Ihres Anwendernamens und Passworts zur zweiten Authentifizierung aufgefordert. Weitere Informationen zum MFA-Anmeldeprozess finden Sie unter Melden Sie sich mit Multifaktor-Authentifizierung an.
Validierung mit Authentifikator-App Geben Sie den Code ein, der in Ihrer Authentifikator-App angezeigt wird, um sich anzumelden.	Wenn Sie keine zweite Form der Authentifizierung konfiguriert haben, wird nach der Anmeldung eine Konfigurationsseite angezeigt, die Sie durch den Prozess zum Einrichten einer Authentifizierungs-App führt. Weitere Informationen zu diesem Setup finden Sie unter Richten Sie die Multifaktor-Authentifizierung zum ersten Mal ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Registrieren Sie ein Authentifizierungsgerät

Nachdem Sie eine Authentifizierungs-App konfiguriert haben, können Sie andere Methoden für die Authentifizierung registrieren.



Biometrische Authentifikatoren

Sie können biometrische Authentifikatoren wie Fingerabdruck oder Gesichtserkennung als zweite MFA-Authentifizierung verwenden. Wenn Ihr Administrator diese Option zulässt, können Sie biometrische Authentifikatoren mithilfe der Schritte in konfigurieren Registrieren Sie einen biometrischen Authentifikator.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardwareschlüssel-Authentifikatoren

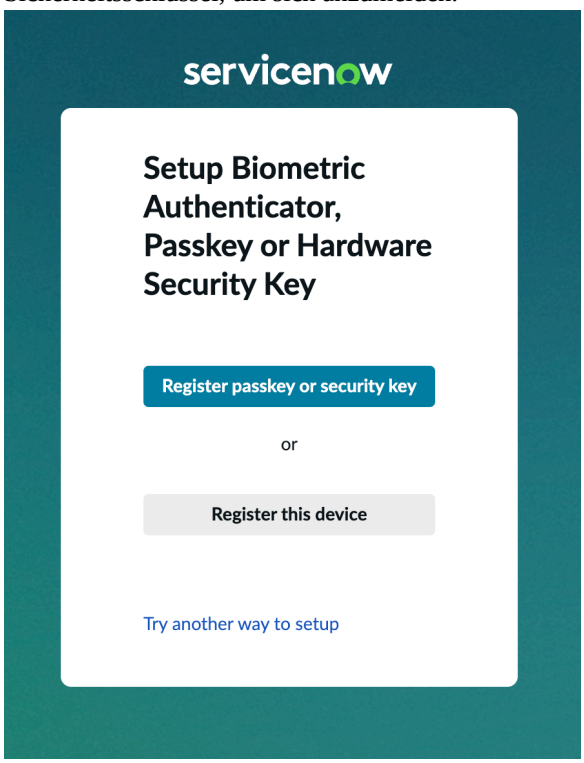
Hardwareschlüssel sind physische Sicherheitsgeräte, die Sie für die Authentifizierung verwenden können. Sie können ein Hardwaregerät für die Verwendung mit Ihrer -Instanz registrieren, indem Sie die Schritte in ausführen Registrieren Sie einen Hardware-Sicherheitsschlüssel.



Validierung mit biometrischem Schlüssel oder Hardwareschlüssel

Verwenden Sie den biometrischen Schlüssel oder den Hardwareschlüssel, um sich anzumelden.

Verwenden Sie den biometrischen Schlüssel oder den Sicherheitsschlüssel, um sich anzumelden.



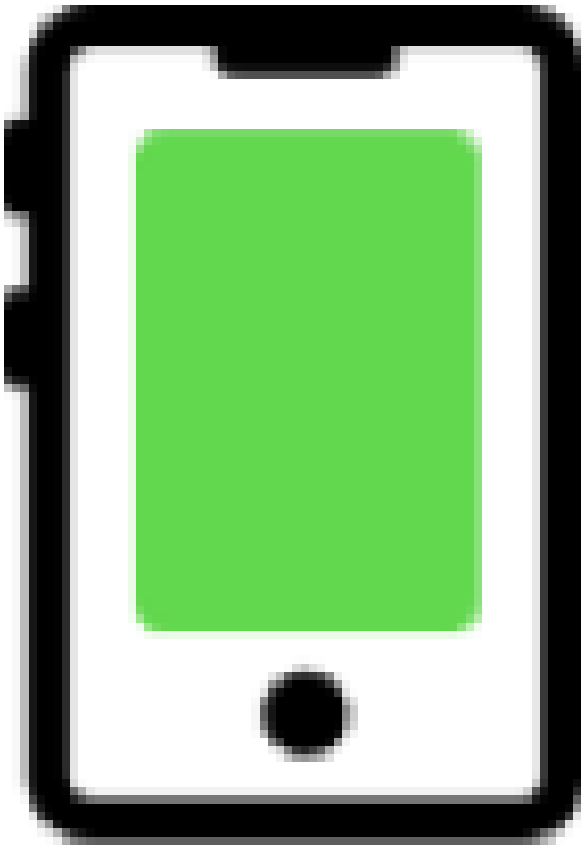
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registrieren Sie eine Telefonnummer für OTP

SMS

Verwenden Sie SMS-basiertes OTP, um Anwender zu benötigen, die versuchen, sich anzumelden.

Wenn Anwender versuchen, sich bei anzumelden ServiceNow, SMS-OTP wird an die Mobiltelefonnummer gesendet, die dem sys_user-Datensatz zugeordnet ist. Benutzer können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.



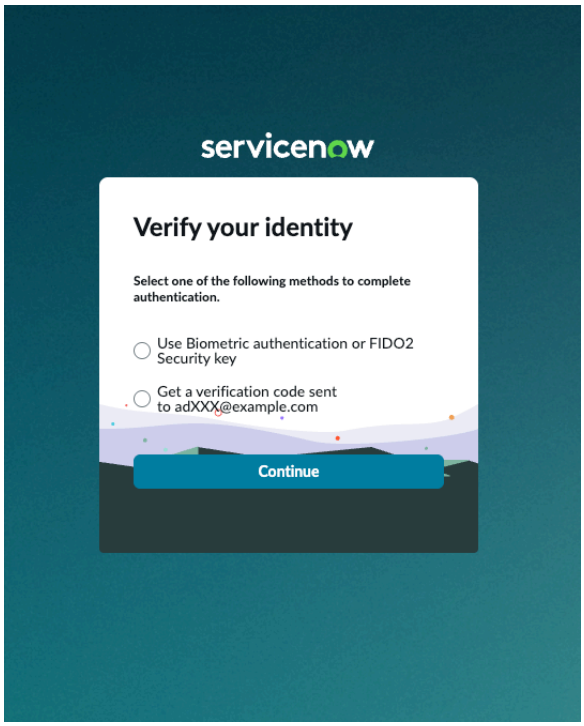
Validierung mit SMS

Verwenden Sie die Validierung mit SMS, um sich basierend auf dem generierten OTP anzumelden.

Geben Sie den sechsstelligen Code ein, der an die Mobiltelefonnummer gesendet wird, um sich anzumelden. Der gesendete Code ist für die nächsten 5 Minuten gültig. Sie können Code erneut senden, um den Code erneut zu senden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Registrieren Sie eine E-Mail-Adresse für OTP

E-Mail-Adresse

Verwenden Sie E-Mail-basiertes OTP, um Anwender zu benötigen, die versuchen, sich anzumelden.

Wenn Anwender versuchen, sich bei anzumelden ServiceNow, E-Mail-OTP wird an die E-Mail-Adresse gesendet, die dem Anwender zugeordnet ist. Anwender können den sechsstelligen Verifizierungscode eingeben, der an das Mobilgerät gesendet wurde, und ihre Identität überprüfen.



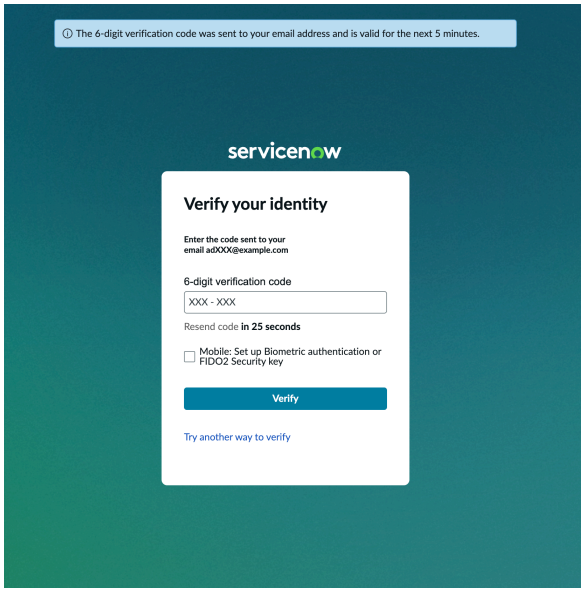
Validierung mit E-Mail

Geben Sie den sechsstelligen Code ein, der an die E-Mail-Adresse gesendet wird, um sich anzumelden. Der gesendete Code ist für die nächsten 5 Minuten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die Validierung mit E-Mail, um sich basierend auf dem generierten OTP anzumelden.

gültig. Sie können Code erneut senden, um den Code erneut zu senden.



Richten Sie die Multifaktor-Authentifizierung zum ersten Mal ein

Wenn Ihr Administrator MFA in Ihrem Profil aktiviert hat, Sie die Anwendung jedoch noch nicht eingerichtet haben, können Sie sie bei der Anmeldung einrichten.

Vorbereitungen

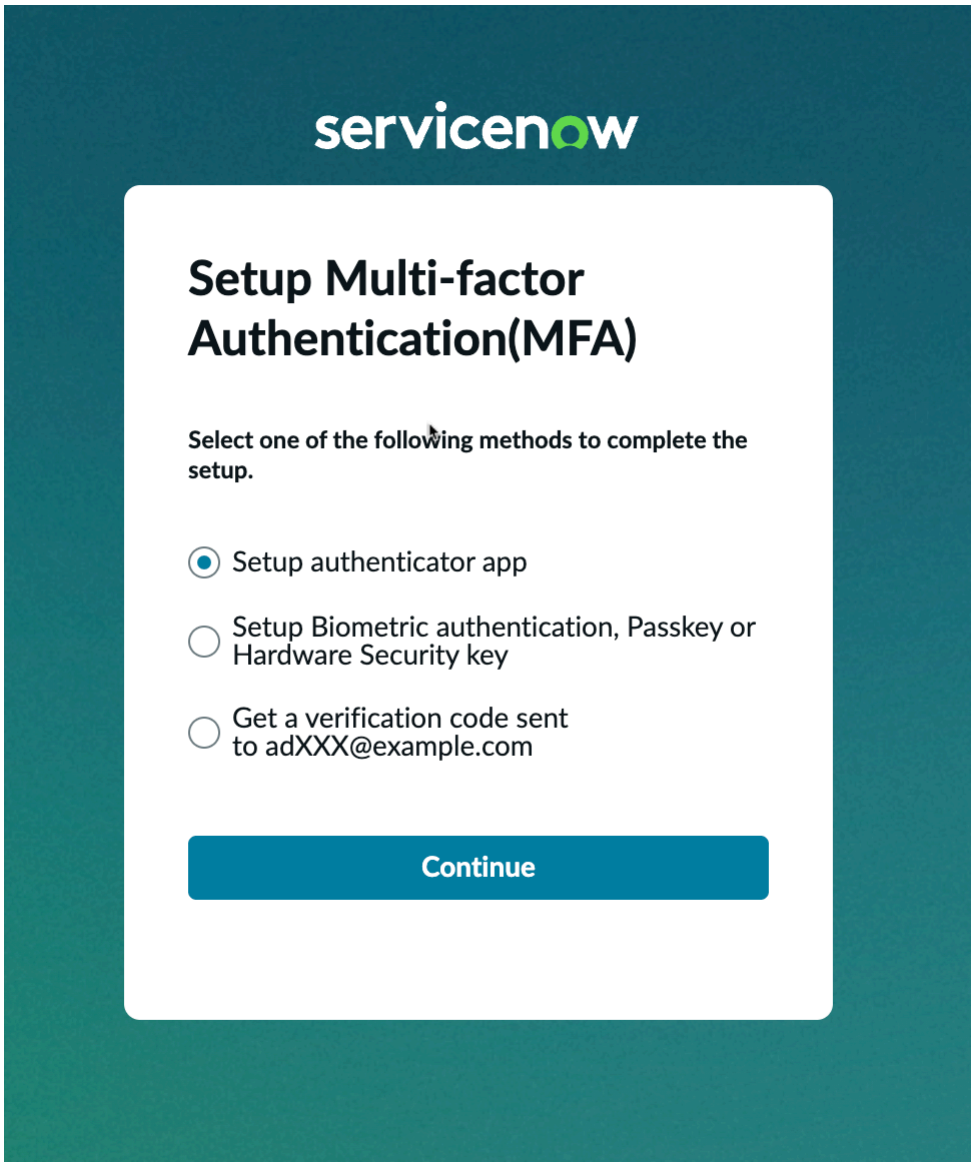
Erforderliche Rolle: keine

Prozedur

1. Melden Sie sich mit Ihrem Anwendernamen und Passwort bei Ihrer Instanz an.

   Der Einrichtungsbildschirm für die Multifaktor-Authentifizierung fängt Ihre Anmeldung ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Wenn Sie die Authentifizierungseinrichtung jetzt überspringen möchten, klicken Sie auf **Setup Umgehen** . Sie können die Multifaktor-Authentifizierung für eine begrenzte Anzahl von Zeiten umgehen, die Ihr Administrator zulässt. Schließlich müssen Sie die Multifaktor-Authentifizierung konfigurieren.

2. Wählen Sie eine der folgenden Methoden aus, um das mfa-Setup abzuschließen.

a. Authentifikator-App einrichten

Befolgen Sie die Anweisungen auf dem Bildschirm, um das Gerät zu koppeln und sich anzumelden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

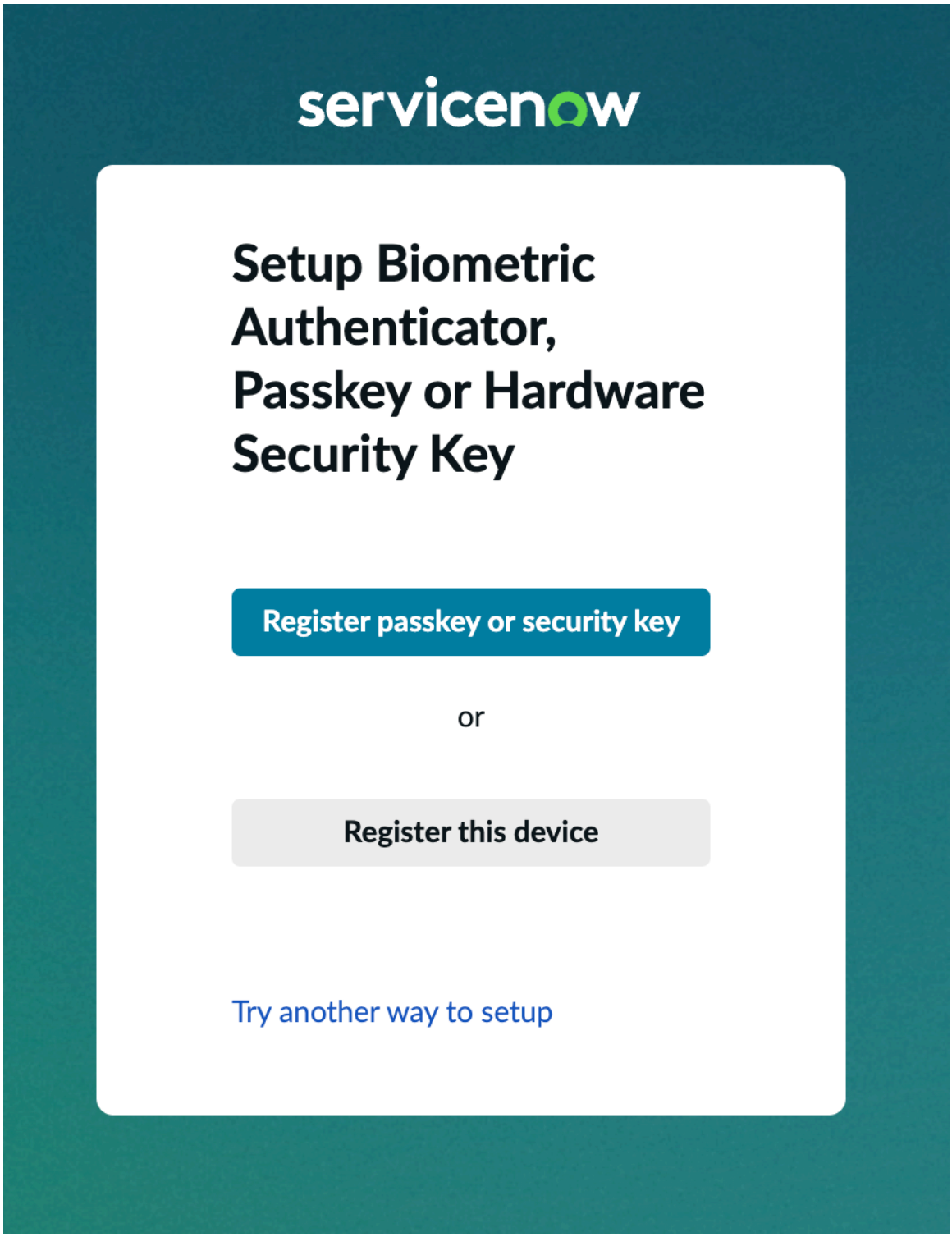


Automatische Übersetzung

b. Biometrischen Authentifikator, Passkey oder Hardware-Sicherheitsschlüssel einrichten

Wählen Sie eine der Optionen aus, um das Setup abzuschließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

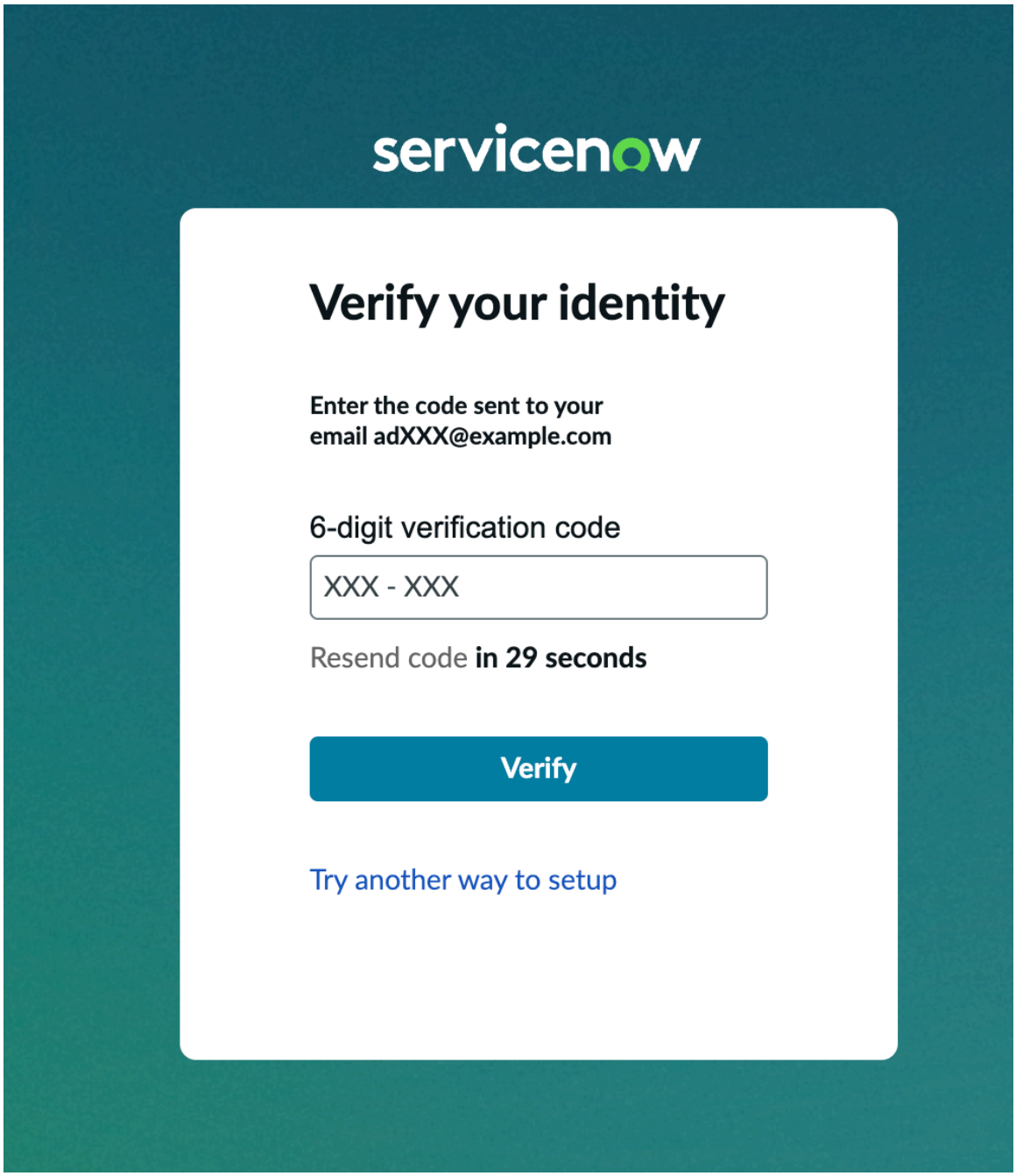


Automatische Übersetzung

c. Rufen Sie einen Verifizierungscode an Ihre E-Mail-Adresse ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geben Sie den Verifizierungscode ein, der an Ihre E-Mail gesendet wird.



Automatische Übersetzung

Nach dem erfolgreichen Abschluss eines der Setups sind Sie bei der -Instanz angemeldet.

Richten Sie die Multifaktor-Authentifizierung für Ihr Anwenderprofil ein

Aktivieren Sie die Multifaktor-Authentifizierung für Ihren Account in Ihren Anwenderprofileinstellungen.

Vorbereitungen
Erforderliche Rolle: keine

Die Multifaktor-Authentifizierung muss in Ihrer Instanz aktiviert sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Ihr Administrator erfordert möglicherweise die Verwendung der Multifaktor-Authentifizierung. In diesem Fall werden Sie automatisch aufgefordert, wenn Sie sich anmelden. Weitere Informationen finden Sie unter Richten Sie die Multifaktor-Authentifizierung zum ersten Mal ein. Verwenden Sie den folgenden Prozess, wenn Ihr Administrator Ihnen erlaubt, die Multifaktor-Authentifizierung zu aktivieren.

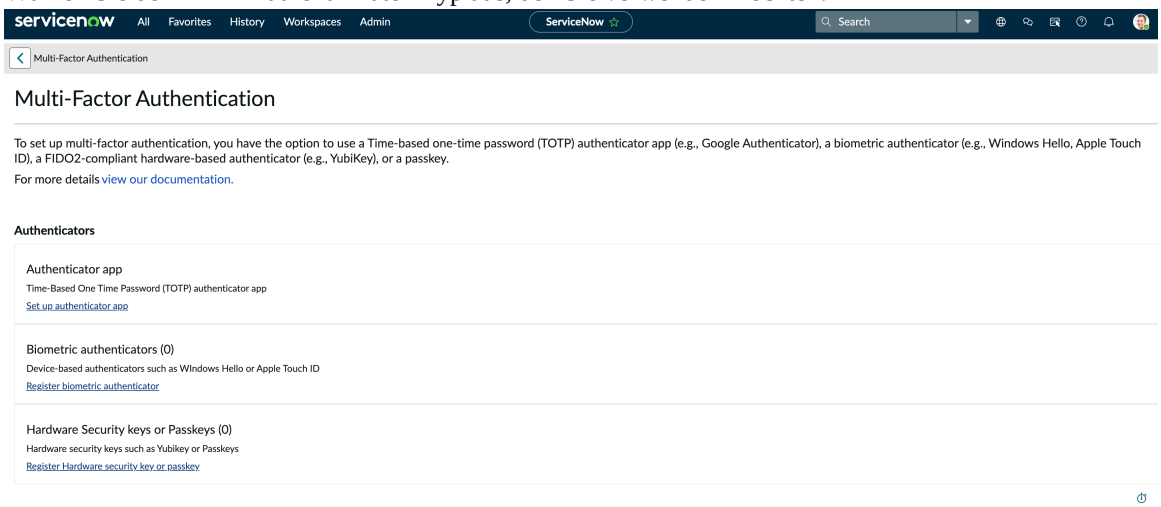
Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Mein Profil**an.

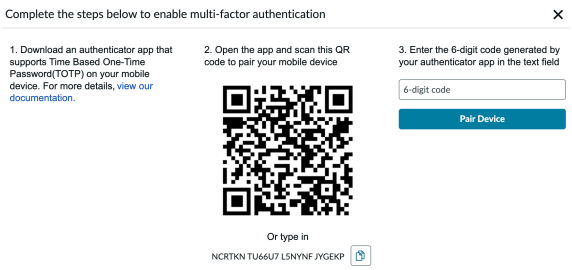
   Hinweis: Sie können auch auf Ihr Profil zugreifen, indem Sie im Instanzheader auf Ihren Anwendernamen klicken.

2. Klicken Sie in Ihrem Anwenderprofil auf **Konfigurieren Sie die Multifaktor-Authentifizierung** In **Zugehörige Links** Abschnitt.

3. Wählen Sie den MFA-Authentifikator-Typ aus, den Sie verwenden möchten.

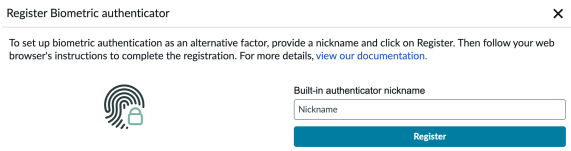
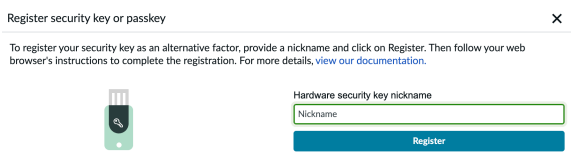


MFA-Authentifikatoren

MFA-Authentifikatoren	Beschreibung
Authentifikator-App	Authentifikator-App auf Basis eines zeitbasierten Einmalpassworts (TOTP) Wählen Sie Aus **Richten Sie die Authentifikator-App ein** Und befolgen Sie die Anweisungen auf dem Bildschirm, um sich für eine Authentifikator-App als zweiten Faktor für die Authentifizierung zu registrieren. 

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MFA-Authentifikatoren	Beschreibung
Biometrische Authentifikatoren	Gerätebasierte Authentifikatoren wie Windows Hello oder Apple Touch ID Wählen Sie Aus **Registrieren Sie die biometrische Authentifizierung** Und befolgen Sie die Anweisungen auf dem Bildschirm, um sich für eine Authentifikator-App als zweiten Faktor für die Authentifizierung zu registrieren. 
Hardware-Sicherheitsschlüssel	Hardware-Sicherheitsschlüssel wie YubiKey Wählen Sie Aus **Registrieren Sie Hardware-Sicherheitsschlüssel** Und befolgen Sie die Anweisungen auf dem Bildschirm, um sich für eine Authentifikator-App als zweiten Faktor für die Authentifizierung zu registrieren. 

Ergebnis

Die Multifaktor-Authentifizierung ist für Ihren Anwenderaccount aktiviert. Sie werden bei der nächsten Anmeldung zur Verwendung der Multifaktor-Authentifizierung aufgefordert.

Hinweis: Sie können die Multifaktor-Authentifizierung für Ihren Account nicht deaktivieren, nachdem Sie ihn aktiviert haben. Wenn Sie die Multifaktor-Authentifizierung deaktivieren müssen, wenden Sie sich an Ihren Administrator.

Melden Sie sich mit Multifaktor-Authentifizierung an

Melden Sie sich bei MFA an, wenn es von Ihrem Administrator in Ihrer Instanz aktiviert wird.

Vorbereitungen

MFA muss für Ihr Profil aktiviert sein. Sie können sie selbst in Ihrem Anwenderprofil aktivieren, oder Ihr Administrator kann sie für Sie aktivieren.

Erforderliche Rolle: keine

Hinweis: Der zuletzt verwendete MFA-Verifizierungsfaktor wird für die Anwender bei der nachfolgenden Anmeldung automatisch angezeigt.

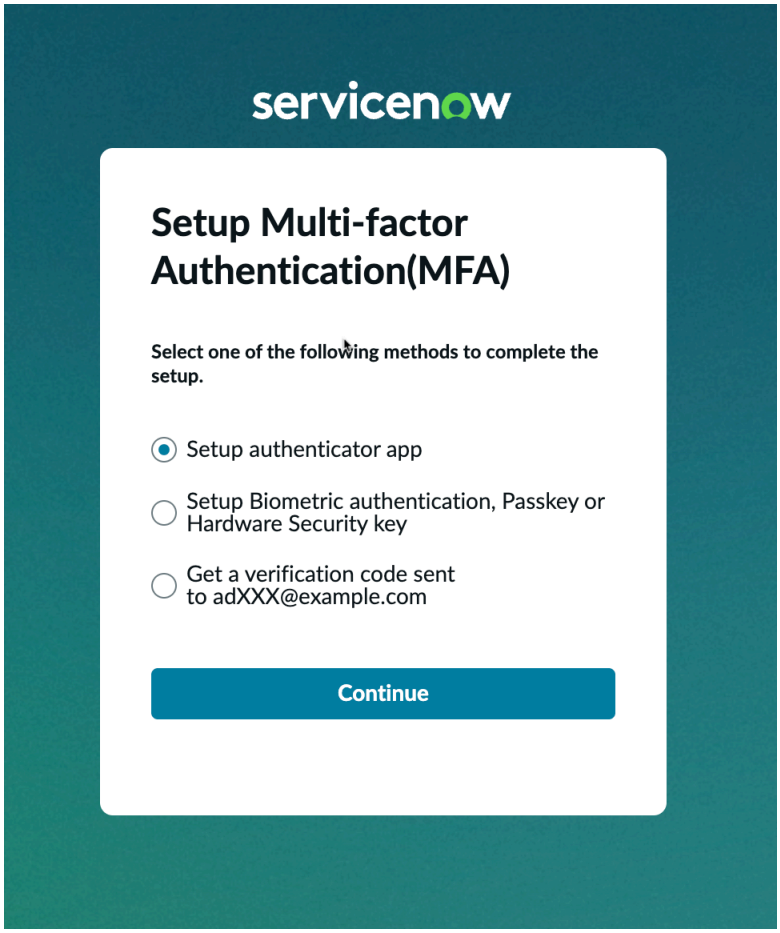
Prozedur

1. Wechseln Sie zur URL Ihrer Instanz, um den Anmeldebildschirm zu öffnen.
2. Geben Sie Ihren Anwendernamen und Ihr Passwort ein.
3. Klicken Sie auf **Anmelden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Bildschirm für die Multifaktor-Authentifizierung wird angezeigt.



4. Wählen Sie eine der Methoden aus, um das MFA-Setup abzuschließen.
   Weitere Informationen zu den einzelnen Setups finden Sie unter Richten Sie die Multifaktor-Authentifizierung zum ersten Mal ein.

   Wenn Sie das Setup verschieben möchten, wählen Sie aus **Setup verschieben** . Die maximale Zeit, die Sie das Setup verschieben können, wird auf dem Bildschirm angezeigt, und dieser Wert wird von Ihrem Administrator konfiguriert.

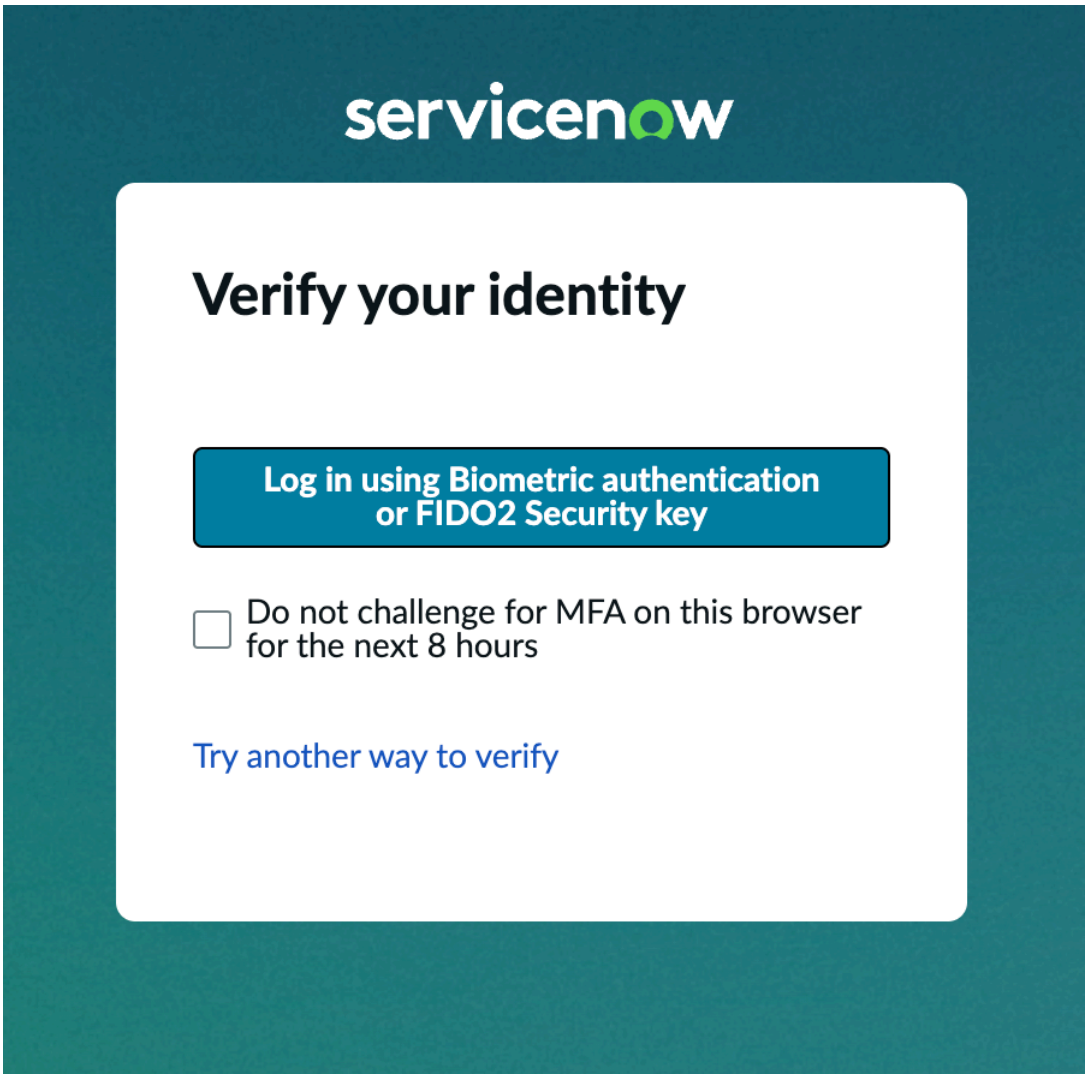
Ergebnis
Wenn Sie MFA bereits eingerichtet haben, wird der zuletzt verwendete Faktor angezeigt, wenn Sie sich nach Eingabe Ihres Anwendernamens und Passworts bei Ihrer Instanz anmelden.

Example: Kürzlich verwendeter MFA-Faktor

Wenn der zuletzt verwendete Faktor biometrische Anmeldung war, werden Sie nach der Anmeldung mit Ihrem Anwendernamen und Passwort direkt mit dem biometrischen MFA-Setup-Bildschirm angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Authentifikatoranwendungen

Verwenden Sie Drittanbieter-Authentifikatoranwendungen, um temporäre MFA-Passcodes zu generieren.

Eine Authentifikator-Anwendung ist eine Drittanbietersoftware, die temporäre Passcodes generiert. Sie können diese Passcodes zusammen mit Ihrem Passwort verwenden, um sich bei einer Instanz anzumelden, die Multifaktor-Authentifizierung (MFA) erfordert.

Wenn Ihr Administrator MFA in Ihrer Instanz aktiviert hat, wird nach Eingabe Ihres Anwenders und Passworts während der Anmeldung eine Aufforderung zur Eingabe eines Passcodes angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



ServiceNow Erfordert Authentifikatoranwendungen, die zeitbasierte Einmalpasswörter (TOTP) unterstützen.

ServiceNow Testet MFA mit den folgenden Authentifikatoren:

- Google Authentifikator
- Microsoft Authentifikator
- LastPass-Authentifikator
- Authy
- FreeOTP
- Duo
- Okta Verifizieren

Hinweis: Andere nicht aufgelistete Authentifikatoren sind möglicherweise ebenfalls kompatibel, werden jedoch nicht von getestet ServiceNow.

Ändern Sie eine Authentifikator-App

Generieren Sie einen neuen Code, um eine Authentifikator-App auf Ihrem Gerät zu ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

MFA muss für Ihr Profil aktiviert sein. Sie können sie selbst in Ihrem Anwenderprofil aktivieren, oder Ihr Administrator kann sie für Sie aktivieren.
Erforderliche Rolle: keine

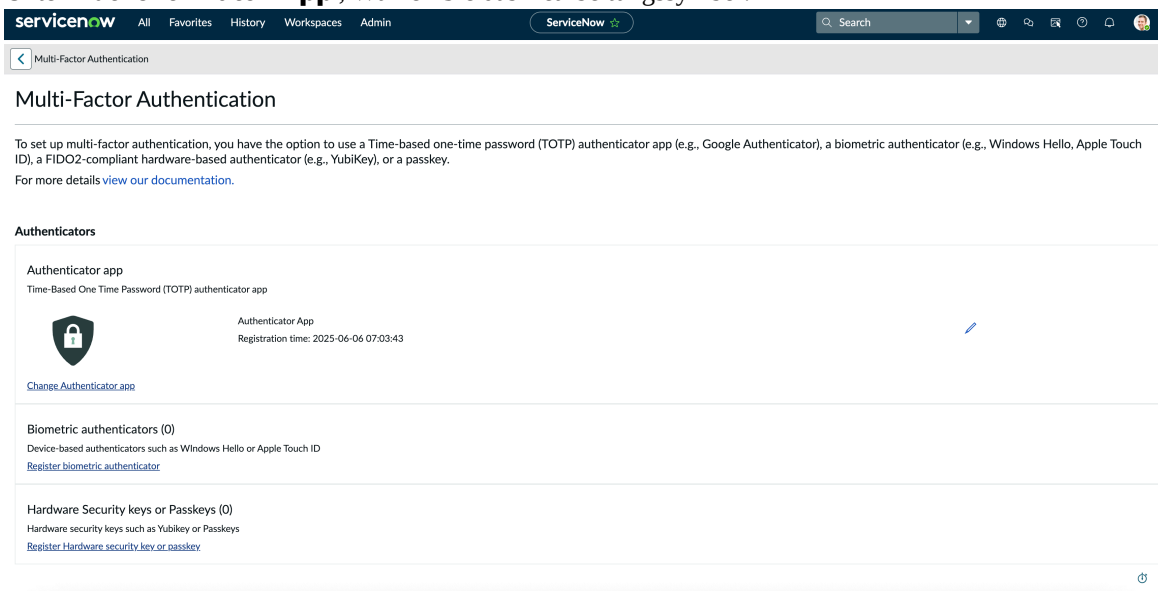
Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Mein Profil**an.

   Hinweis: Sie können auch auf Ihr Profil zugreifen, indem Sie im Instanzheader auf Ihren Anwendernamen klicken.

2. Klicken Sie in Ihrem Anwenderprofil auf **Muti-Faktor-Authentifizierung** In **Zugehörige Links** Abschnitt.

3. Unter **Authentifikator-App** , Wählen Sie das Bearbeitungssymbol.



4. Klicken Sie im Fenster „Authentifikatorcode ändern“ auf **Ändern** .

5. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Authentifikator-App beim Gerät zu registrieren.

Webauthentifizierung

Ihre Anwender können Hardwareschlüssel oder die biometrischen Leser ihres Geräts (FIDO2) verwenden, um sich bei einer Instanz zu authentifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardwareschlüssel



Hardwareschlüssel sind physische Hardware, die Sie zur Authentifizierung verwenden können. Hardwareschlüssel werden in einen Port Ihres Geräts eingefügt, um die Authentifizierung bereitzustellen. Details zum Registrieren von Hardwareschlüsseln finden Sie unter Registrieren Sie einen Hardware-Sicherheitsschlüssel.

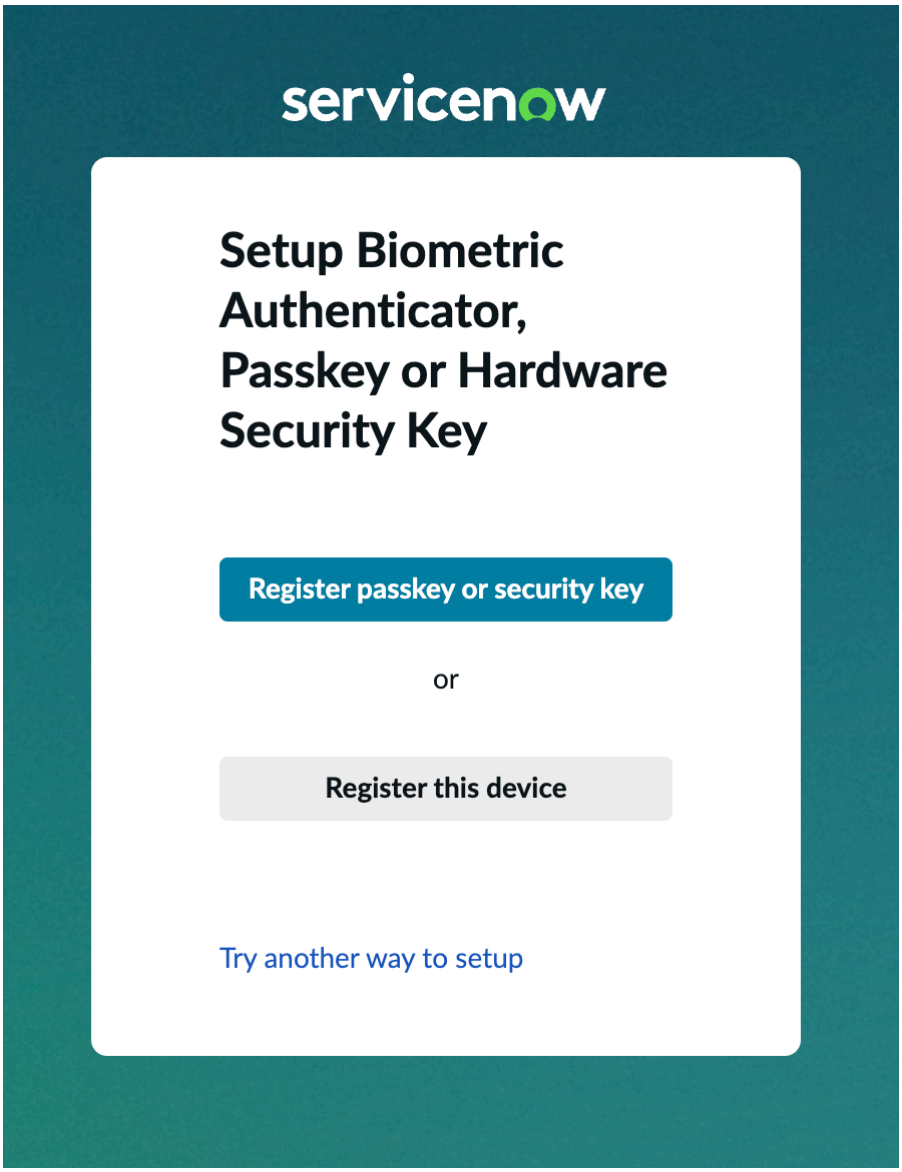
Biometrik



Biometrische Authentifikatoren verwenden Fingerabdruck- oder Gesichtserkennung, um Anwender zu identifizieren. Ihre Anwender können diese Authentifikatoren auf ihren Geräten als Teil des Multifaktor-Anmeldevorgangs verwenden. Details zur Registrierung biometrischer Authentifikatoren finden Sie unter Registrieren Sie einen biometrischen Authentifikator.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie den zweiten Faktor aus, den Sie authentifizieren und bei Ihrer Instanz authentifizieren möchten.



Informationen zum Konfigurieren des Plugins für die Webauthentifizierung finden Sie unter .

Registrieren Sie einen biometrischen Authentifikator

Registrieren Sie einen biometrischen Authentifikator, der als Teil Ihrer MFA-Anmeldung verwendet werden soll.

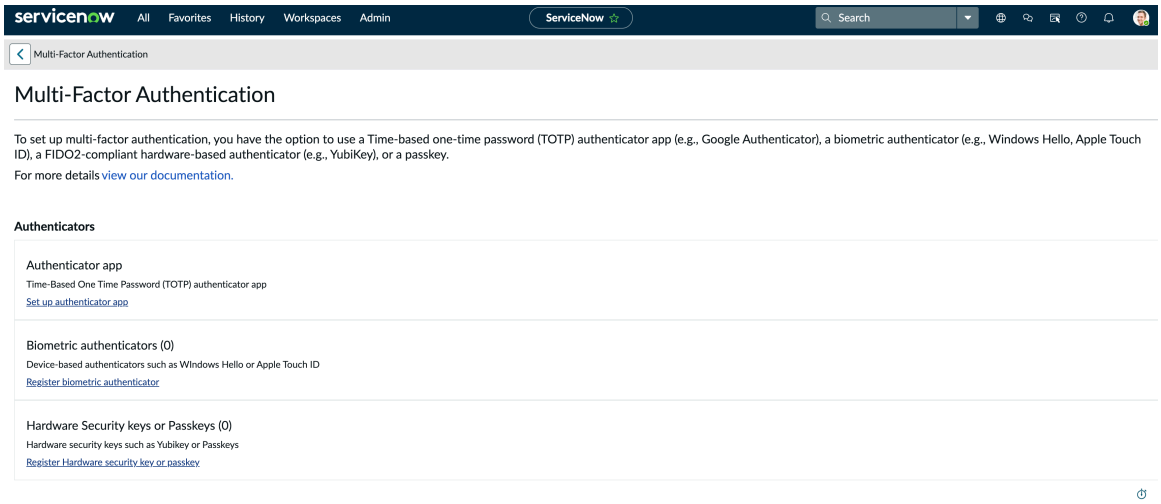
Vorbereitungen
Erforderliche Rolle: keine

Prozedur

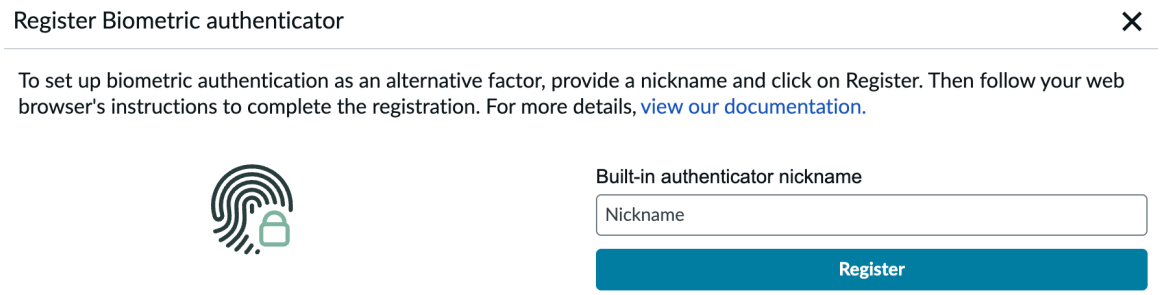
1. Navigieren zu **Alle** > **Self-Service** > **Mein Profil**an.
2. Unter **Zugehörige Links** , Klicken Sie auf **Multifaktor-Authentifizierung** .
   Die Seite für die Multifaktor-Authentifizierung wird geöffnet.
3. Klicken Sie Auf **Registrieren Sie die biometrische Authentifizierung** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

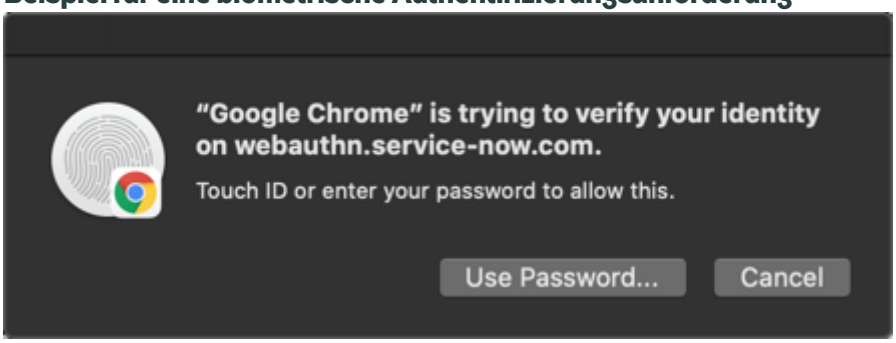


4. Geben Sie einen Kurznamen für Ihren Authentifikator ein, und klicken Sie auf **Registrieren** .



5. Befolgen Sie bei Aufforderung die Anweisungen auf dem Bildschirm, um sich bei Ihrem biometrischen Authentifikator zu authentifizieren.
   Diese Nachricht variiert je nach Ihrem spezifischen Authentifikator.

Beispiel für eine biometrische Authentifizierungsanforderung



   Nach der erfolgreichen Authentifizierung wird ein Bestätigungsfenster angezeigt. Klicken Sie auf X, um die Bestätigung zu schließen.

Ergebnis

Ihr biometrischer Authentifikator ist registriert. Der biometrische Authentifikator wird auf der Seite „Multifaktor-Authentifizierung“ aufgeführt.

Registrieren Sie einen Hardware-Sicherheitsschlüssel

Registrieren Sie einen Hardwareschlüssel, der als Teil Ihrer MFA-Anmeldung verwendet werden soll.

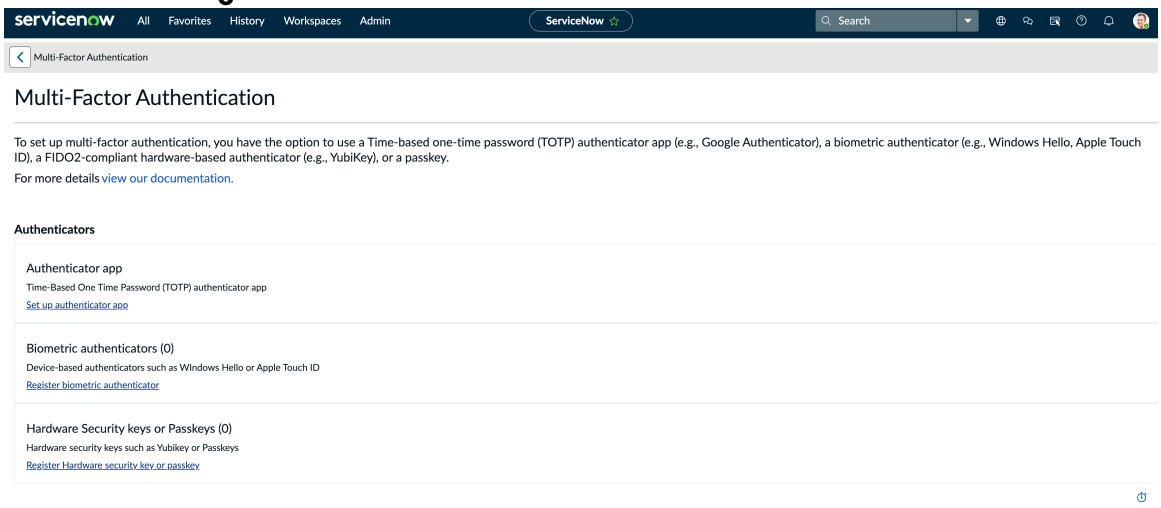
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

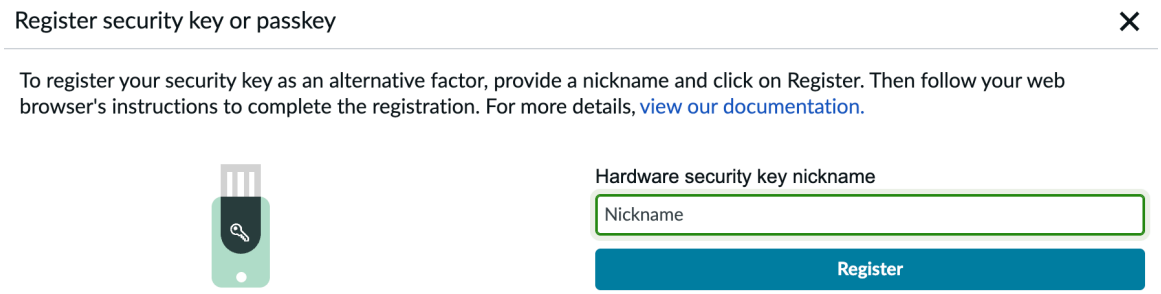
Vorbereitungen
Erforderliche Rolle: keine

Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Mein Profil**an.
2. Unter **Zugehörige Links** , Klicken Sie auf **Multifaktor-Authentifizierung** .
   Die Seite „Multifaktor-Authentifizierung“ wird geöffnet.
3. Klicken Sie Auf **Registrieren Sie den Hardware-Sicherheitsschlüssel** .



4. Geben Sie einen Kurznamen für Ihren Hardwareschlüssel ein, und klicken Sie auf **Registrieren** .



5. Wenn Sie dazu aufgefordert werden, fügen Sie Ihren Hardware-Sicherheitsschlüssel ein, und aktivieren Sie ihn.
   Nach der erfolgreichen Authentifizierung wird ein Bestätigungsfenster angezeigt. Klicken Sie auf X, um die Bestätigung zu schließen.

Ergebnis
Ihr Hardwareschlüssel ist registriert. Der Hardwareschlüssel wird auf der Seite „Multifaktor-Authentifizierung“ aufgeführt.

MFA-Dashboard

Zeigen Sie die verschiedenen MFA-Metriken an, um die Einführung und Nutzung von MFA zu verstehen.

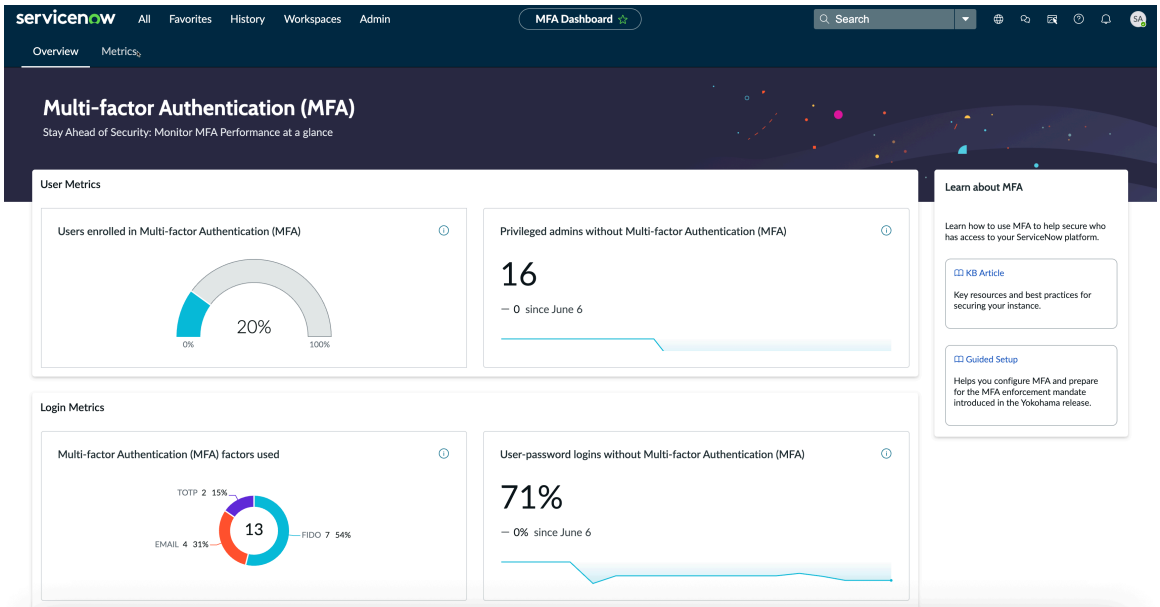
Die MFA erhöht die Sicherheit, indem während des Anmeldevorgangs ein zusätzlicher Verifizierungsschritt erforderlich ist. Das MFA-Dashboard hilft Ihnen, MFA-Einstellungen für Ihre Organisation zu überwachen und zu verwalten. Dieses Dashboard bietet einen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überblick über die MFA-Anwenderregistrierung, privilegierte Administratoren, die MFA nicht ausgewählt haben, und die Compliance. Sie können damit sicherstellen, dass MFA für alle Anwender aktiviert ist, um die Sicherheit zu erhöhen.

Navigieren Sie, um auf das MFA-Dashboard zuzugreifen **Alle** > **Multi-Faktor-Authentifizierung** > **MFA-Dashboard**an.



Hinweis: Sie müssen MFA aktivieren, um die Metriken anzuzeigen. Weitere Informationen finden Sie unter Systemeigenschaften der Multifaktor-Authentifizierung.

Im Folgenden finden Sie die Arten von Metriken, die im MFA-Dashboard angezeigt werden:

- Anwendermetriken
- Anmeldungsmetriken

Anwendermetriken

Die folgende Tabelle enthält Details zu den Anwendermetriken im MFA-Dashboard.

Anwendermetriken

Metriken	Beschreibung
Für Multifaktor-Authentifizierung (MFA) registrierte Anwender	Der Prozentsatz der Anwender, die sich auf Anwendername und Passwort anmelden und bei MFA registriert haben. Diese Metrik bietet einen Einblick in die Einführung von MFA durch die Anwender über einen bestimmten Zeitraum. **Hinweis:** Idealerweise sollte die Punktzahl schrittweise steigen und über einen Zeitraum 100 % betragen (einmal täglich aktualisiert, um Datensätze für einen Tag zuvor zu erfassen).
Privilegierte Administratoren ohne Multifaktor-Authentifizierung (MFA)	Privilegierte Administratoren, die MFA nicht verwenden, stellen ein erhebliches Risiko für die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendermetriken (Fortsetzung)

Metriken	Beschreibung
	Plattformsicherheit dar. Es wird empfohlen, dass diese Personen MFA verwenden. **Hinweis:** Privilegierte Administratoren sind die Anwender, die mindestens eine Rolle aus der Tabelle „sys_icenter_role_config“ haben. (Wird einmal täglich aktualisiert, um Datensätze für einen Tag zuvor zu erfassen).

Anmeldungsmetriken

Die folgende Tabelle enthält Details zu den Anmeldemetriken im MFA-Dashboard.

Anmeldungsmetriken

Für Multifaktor-Authentifizierung (MFA) genutzte Faktoren	Klassifizierung der MFA-Faktoren, die während der passwortbasierten Anmeldung verwendet werden.
Anmeldungen mit Anwenderpasswort ohne Multifaktor-Authentifizierung (MFA)	Der Prozentsatz der auf Anwendernamen basierenden passwortbasierten Anmeldungen ohne MFA. Diese Metrik bietet einen Einblick in die Einführung von MFA über einen bestimmten Zeitraum. **Hinweis:** Idealerweise sollte die Punktzahl schrittweise abnehmen und über einen bestimmten Zeitraum Null sein (wird einmal täglich aktualisiert, um Datensätze für einen Tag zuvor zu erfassen).

Anwendermetriken

Anwendermetriken zeigen die Trends der MFA-Registrierung für Anwender an ServiceNow.

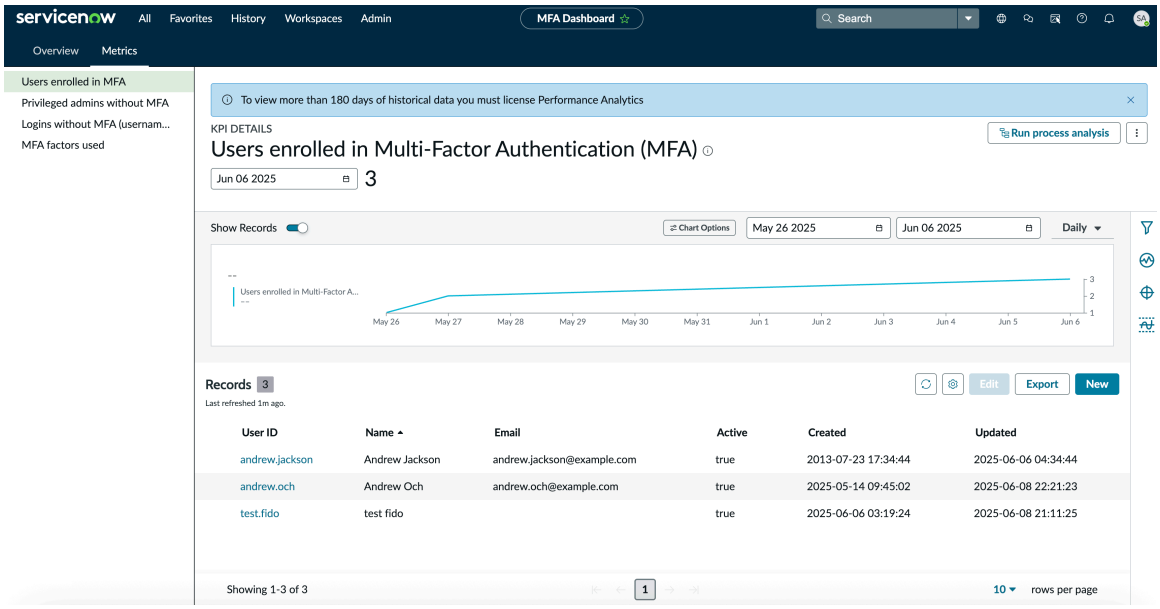
Anwendermetriken im MFA-Dashboard lauten wie folgt:

- Für Multifaktor-Authentifizierung (MFA) registrierte Anwender
- Privilegierte Administratoren ohne Multifaktor-Authentifizierung (MFA)

Für Multifaktor-Authentifizierung (MFA) registrierte Anwender

Der Prozentsatz der Anwender, die sich auf Anwendername und Passwort anmelden und bei MFA registriert haben. Diese Metrik bietet einen Einblick in die Einführung von MFA durch die Anwender über einen bestimmten Zeitraum.

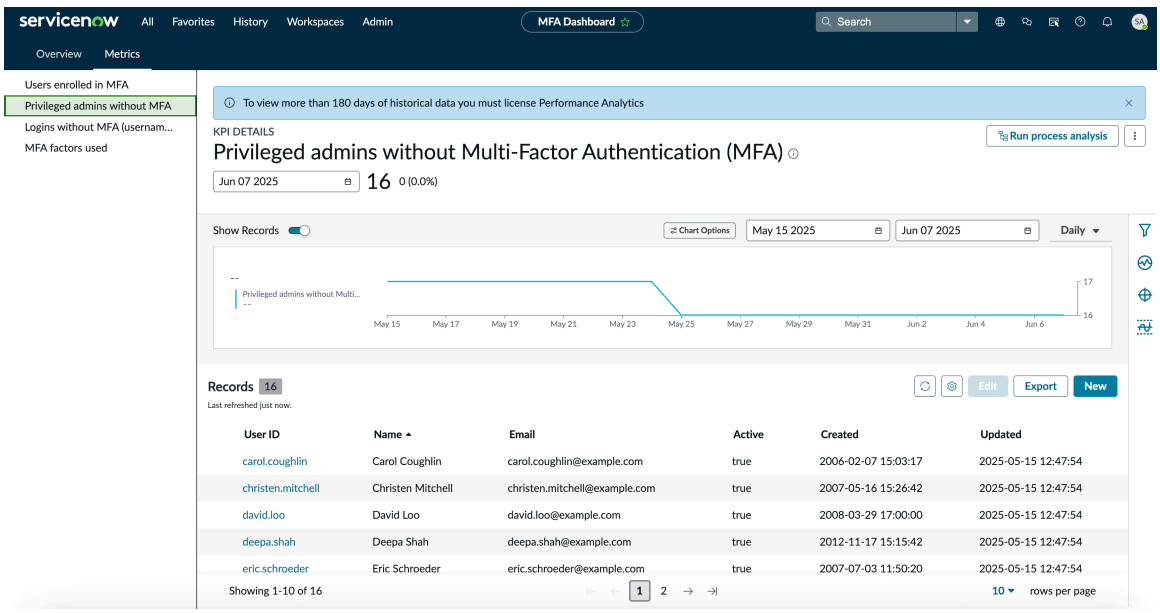
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Idealerweise sollte die Punktzahl schrittweise steigen und über einen Zeitraum 100 % betragen (einmal täglich aktualisiert, um Datensätze für einen Tag zuvor zu erfassen).

Privilegierte Administratoren ohne Multifaktor-Authentifizierung (MFA)

Privilegierte Administratoren, die MFA nicht verwenden, stellen ein erhebliches Risiko für die Plattformsicherheit dar. Es wird empfohlen, dass diese Personen MFA verwenden.



Hinweis: Privilegierte Administratoren sind die Anwender, die mindestens eine Rolle von haben **sys_icenter_role_config** Tabelle. (Wird einmal täglich aktualisiert, um Datensätze für einen Tag zuvor zu erfassen).

Melden Sie sich Metriken an

Anmeldungsmetriken zeigt die Anmeldetrends im an ServiceNow.

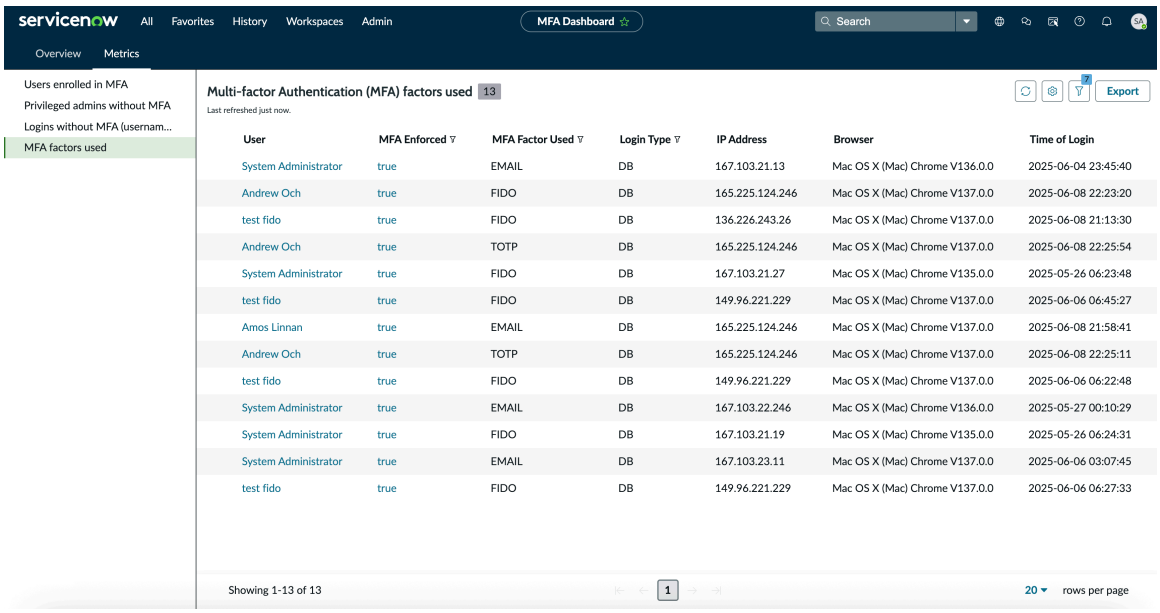
Anmeldemetriken im MFA-Dashboard lauten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Multifaktor-Authentifizierung (MFA) genutzte Faktoren
- Anmeldungen mit Anwenderpasswort ohne Multifaktor-Authentifizierung (MFA)

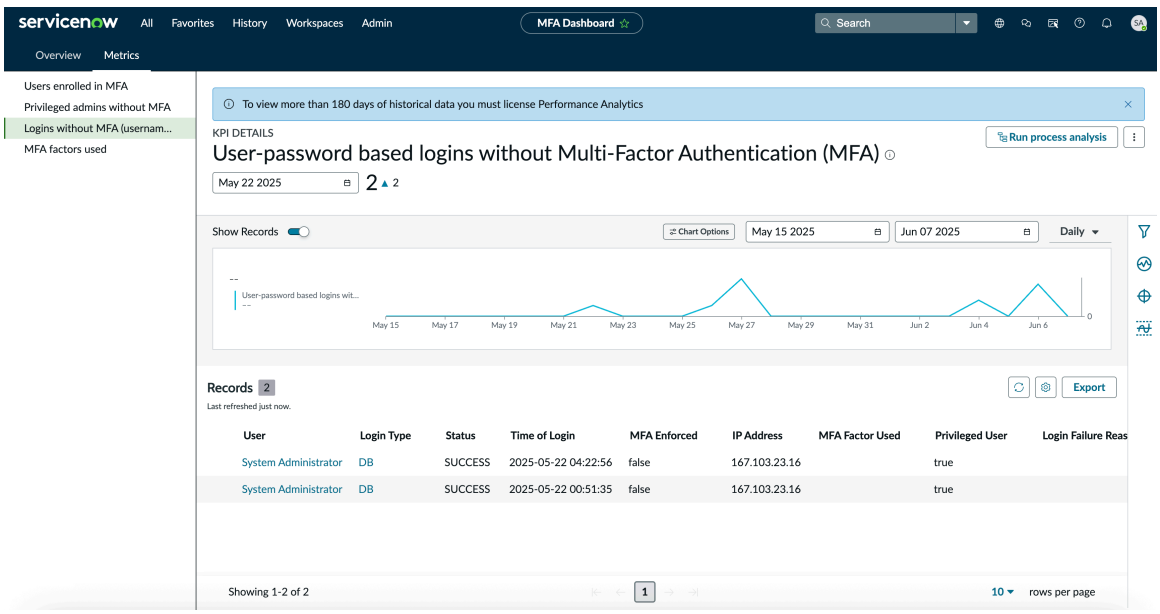
Für Multifaktor-Authentifizierung (MFA) genutzte Faktoren

Klassifizierung der MFA-Faktoren, die während der passwortbasierten Anmeldung verwendet werden.



Anmeldungen mit Anwenderpasswort ohne Multifaktor-Authentifizierung (MFA)

Der Prozentsatz der auf Anwendername und Passwort basierenden Anmeldungen ohne Multifaktor-Authentifizierung. Diese Metrik bietet einen Einblick in die Einführung von MFA über einen bestimmten Zeitraum.



Hinweis: Idealerweise sollte die Punktzahl schrittweise abnehmen und über einen bestimmten Zeitraum Null sein (wird einmal täglich aktualisiert, um Datensätze für einen Tag zuvor zu erfassen).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

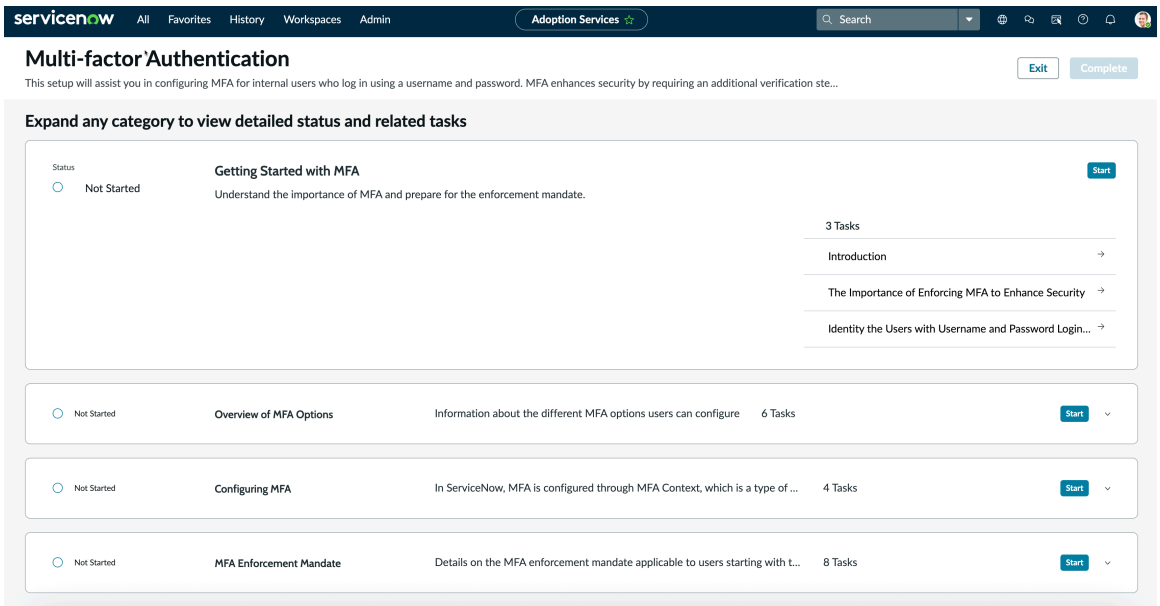
Geführtes Setup – MFA

Verwenden Sie das geführte Setup für MFA, um die Erstkonfiguration des MFA-Moduls zu durchlaufen und die Anforderungen für MFA-Erzwingungen zu verstehen.

Das geführte Setup für MFA unterstützt Sie bei der Konfiguration von MFA für interne Anwender, die sich mit einem Anwendernamen und einem Passwort anmelden.

Um auf das geführte Setup für MFA zuzugreifen, navigieren Sie zu **Alle** > **Adoption-Services** > **Geführtes Setup**an. Sie können auswählen **Alle Anwendungen** Und wählen Sie aus **Multifaktor-Authentifizierung** .

Das geführte Setup für Multifaktor-Authentifizierung wird in einer neuen Registerkarte geöffnet. Erweitern Sie eine beliebige Kategorie, um einen detaillierten Status und zugehörige Aufgaben auf der angezeigten Seite anzuzeigen.



Führen Sie die folgende Aufgabe aus, um sich mit den MFA-Konfigurationen vertraut zu machen:

- Erste Schritte mit MFA
- Übersicht über MFA-Optionen
- MFA wird konfiguriert
- MFA-Durchsetzungsauftrag
- Anwenderkommunikation und Onboarding
- Überwachung

Weitere Informationen zur Verwendung des geführten Setups finden Sie unter Geführtes Setup .

Single Sign-on (SSO) für mehrere Anbieter

Mit externem SSO können Organisationen mehrere SSO-Identitätsanbieter (IDPs) verwenden, um die Authentifizierung zu verwalten und die Authentifizierung der lokalen Datenbank (Standard) beizubehalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Provider Single Sign-on (SSO) ist eine Authentifizierungsmethode, mit der Anwender mit einer Anmeldung und einem Satz von Anmeldeinformationen auf mehrere Anwendungen zugreifen können.

Für die Verwendung von SSO müssen Sie Folgendes verstehen:

- *`Service Providers`*: Wenn Anwender versuchen, auf zuzugreifen ServiceNow Die Instanz wird an einen Identitätsanbieter (Identity Provider, IdP) weitergeleitet, um ihre Anmeldeinformationen zu validieren, nachdem Anwender erfolgreich validiert wurden, auf die Instanz zugreifen können. Hier, ServiceNow Fungiert als Service Provider und stützt sich auf einen Identitätsanbieter (Identity Provider, IdP), um die Anwenderauthentifizierung zu verarbeiten und Zugriff auf die Instanz zu gewähren.
- Identitätsanbieter: IDPs sind externe Systeme, die die Identität und Anmeldeinformationen des Anwenders für den Zugriff auf ein System validieren.

Dient zum Einrichten eines SSO mit für den Zugriff ServiceNow, Sie müssen Multi-Provider Single Sing-on (SSO) aktivieren, Sie müssen installieren *`Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer)`*Plugin. Weitere Informationen finden Sie unter Aktivieren Sie das Multi-Provider-SSO-Plugin.

Nach der erfolgreichen Installation des Plugins können Sie die SSO-Eigenschaften, Zugriffstabellen und Skripts anpassen, die mit dem Plugin geliefert werden. Weitere Informationen finden Sie unter Multi-Provider-SSO-Eigenschaften, -Tabellen und -Skripts.

ServiceNow Unterstützt die folgenden SSO-Methoden:

- OpenID Connect
- SAML 2.0
- Digest-Authentifizierung (Tokenbasierte Authentifizierung).

Wählen Sie die SSO-Methode basierend auf Ihren Anforderungen aus, und erfahren Sie mehr darüber, wie Sie sich auf die Konfiguration von SSO vorbereiten müssen. Sie müssen mehrere Schritte ausführen, um Multi-Provider-SSO einzurichten, einschließlich der Konfiguration von Eigenschaften, der Erstellung von Identitätsanbietern (IDPs) und der Konfiguration von Anwendern für die Verwendung von SSO. Weitere Informationen finden Sie unter Multi-Provider-SSO-Konfigurationen.

Nach einer erfolgreichen Konfiguration werden die aktiven IDPs in der -Instanz im aufgelistet ServiceNow. Sie können verschiedene SAML- oder OIDC-Identitätsanbieter (IDPs) auflisten.

Hinweis: Auf der Anmeldeseite können maximal 10 IDPs aufgelistet werden. Die IdP-Optionen sind nicht sichtbar, wenn die Instanz über das Installationsprogramm „Domänenunterstützung – Domänenerweiterungen“ (*`com.glide.domain.msp_extensions.installer`*) Plugin installiert und aktiviert.

Die Zurich-Version von ServiceNow Fügen Sie die folgenden Erweiterungen für SSO hinzu:

- **Listet SAML-IDPs auf der Anmeldeseite auf** : Melden Sie sich mit SAML- und OIDC-IDPs an, die in der Anmelde-Experience sowohl auf den Anmeldeseiten der Plattform als auch des Portals aufgeführt sind, sodass Anwender ihren bevorzugten IdP leichter auswählen können. Früher wurden nur OIDC-IDPs aufgelistet.
- **Wählen Sie eine Gruppe für die automatische Bereitstellung aus** : Wählen Sie während der Konfiguration der automatischen Bereitstellung für SAML und OIDC bestimmte Gruppen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aus, um sicherzustellen, dass Anwender automatisch den richtigen Gruppen zugewiesen werden.

- **Konfigurieren Sie mehrere OIDC-Datensätze mit derselben bekannten URL** : Vereinfachen Sie das OIDC-Setup, indem Sie die Erstellung von OIDC-Datensätzen mit derselben bekannten URL zulassen, wodurch der Konfigurationsprozess optimiert wird.
- **Erweiterte Seite „Abschließen der externen Abmeldung“** : Anzeige des Fehlers bei der Anmeldung für den Anwender. Bereitstellung, um sich erneut bei anzumelden ServiceNow Auf der Seite „externe Abmeldung abgeschlossen“ im Falle einer erfolgreichen Abmeldung.
- **Erweiterte Fehlermeldung** : Anzeige der generischen Fehlermeldung, wenn Single Logout (SLO) nicht erfolgreich ist, um eine konsistente und sichere Kommunikation sicherzustellen.
- **Benachrichtigungserweiterungen für SAML-Zertifikat und Verschlüsselungsschlüsselspeicher** : Erhalten Sie rechtzeitig Benachrichtigungen an die Administratoren, wenn SAML-Zertifikat- und Verschlüsselungsschlüsselspeicher-Updates ablaufen, um sicherzustellen, dass Ihre SSO-Konfigurationen sicher und aktuell bleiben.

Example: Warum die Organisation SSO benötigt

Ein global verteiltes Unternehmen benötigt möglicherweise einen SSO-Anbieter für seine Mitarbeiter, einen anderen für seine Lieferanten und eine lokale Datenbankauthentifizierung für seine Administratoren. Alternativ kann ein Unternehmen SAML 2,0 und eine Digest-Token-Authentifizierungslösung auf derselben Instanz implementieren.

Aktivieren Sie das Multi-Provider-SSO-Plugin

Diese Integration erfordert das Plugin Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter (com.snc.integration.sso.multi.installer).

Vorbereitungen

Erforderliche Rolle: admin.

Das Plugin com.snc.integration.sso.multi.installer kann auch für OIDC, SAML und Digest verwendet werden.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach dem Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“ (com.snc.integration.sso.multi.installer).

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Multi-Provider-SSO-Eigenschaften, -Tabellen und -Skripts

Das Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“ enthält die folgenden Systemeigenschaften, Tabellen und Skripts.

Eigenschaften

Multi-Provider-SSO fügt die folgenden Systemeigenschaften hinzu.

Multi-Provider-SSO-Eigenschaften

Name	Beschreibung
`glide.authenticate.multisso.debug`	Aktiviert (wahr) oder deaktiviert (falsch) die Debug-Protokollierung für die SSO-Integration mehrerer Anbieter. • Typ: Wahr | Falsch • Standardwert: falsch
`glide.authenticate.multisso.enabled`	Aktiviert (wahr) oder deaktiviert (falsch) Multi-Provider-SSO. • Typ: Wahr | Falsch • Standardwert: falsch **Hinweis:** Wenn Sie diese Eigenschaft auf „falsch“ festlegen, wird SSO für mehrere Anbieter nicht deaktiviert, wenn die Accountwiederherstellung (ACR) auch in der Instanz aktiviert ist. Um sich mit einem Anwendernamen und Passwort anzumelden, muss ACR auch mit deaktiviert werden `glide.sso.acr.enabled`Eigenschaft. Einzelheiten zu dieser Eigenschaft finden Sie unter Accountwiederherstellungseigenschaften.
`glide.authenticate.multissov2_feature.enabled`	Diese Eigenschaft bestimmt, ob die MultiSSOv2-Version in der Instanz aktiviert ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Provider-SSO-Eigenschaften (Fortsetzung)

Name	Beschreibung
glide.authenticate.show.max.sso.login.option	Diese Eigenschaft bestimmt die maximale Anzahl von SSO-Optionen, die auf dem Anmeldebildschirm angezeigt werden. **Hinweis:** Der Standardwert ist 5. Der Höchstwert der Eigenschaft ist 10.
glide.authenticate.show.max.sso.login.option	Diese Eigenschaft bestimmt die maximale Anzahl von IDPs, die auf dem Anmeldebildschirm angezeigt werden. „glide.authenticate.show.max.sso.login.option" **Hinweis:** Der Standardwert ist 10.

Tabellen

Multi-Provider-SSO fügt die folgenden Tabellen hinzu.

Multi-Provider-SSO-Tabellen

Name	Beschreibung
SSO-Eigenschaften [sso_properties]	Speichert Daten für jeden IdP, jedes Schema, allgemeine SSO-Daten usw.
Eigenschaften von SAML 2 Update 1 [saml2_update1_properties]	Speichert Daten für SAML 2,0 Update 1-Konfigurationen, z. B. SAML-Zertifikate.
Digest-Eigenschaften [Digest_properties]	Speichert Daten für Konfigurationen der Digest-Token-Authentifizierung.
SSO-Föderation [sso_Federation]	Speichert Daten für jeden SSO-Verbund.
OIDC-Identitätsanbieter [oidc_Identity_Provider]	Speichert Daten für Open ID Connect-basierte Identitätsanbieter.

Skripte

Multi-Provider-SSO fügt die folgenden Skripts hinzu.

Multi-Provider-SSO-Skripts

Name	Beschreibung
MultiSSO	Ermöglicht einem Kunden, einen SSO-Typ auf Unternehmensbasis zu definieren.
MultiSSOLogin	Ermöglicht jeder Domäne, ihr eigenes Anmeldeskript zu haben.
MultiSSOLogout	Ermöglicht jeder Domäne, ihr eigenes Abmeldeskript zu haben.
MultiSSO_OIDC_custom	Ermöglicht einem Anwender, ein anwenderdefiniertes Single Sign-on-Skript für die OIDC-Verbindung zu definieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Provider-SSO-Skripts (Fortsetzung)

Name	Beschreibung
MultiSSO_OIDC_logout_custom	Ermöglicht einem Anwender, ein anwenderdefiniertes Abmeldeskript für die OIDC-Verbindung zu definieren.
MultiSSO_Abstract_Core	Stellt eine Basisklasse für alle SSO-Klassen mit mehreren Anbietern bereit.
MultiSSO_ClientHelper	Stellt vom Client aufrufbare Dienstprogrammfunktionen für SSO mit mehreren Anbietern bereit.
MultiSSO_DigestedToken	Stellt eine Basissystemlogik für die Authentifizierung von verarbeiteten Token bereit.
MultiSSO_SAML2_Update1	Bietet Logik zur Verarbeitung der SAML 2,0 Update 1-Authentifizierung für ein Single Sign-on mit mehreren Mandanten.

Multi-Provider-SSO-Konfigurationen

Sie müssen mehrere Schritte ausführen, um Multi-Provider-SSO einzurichten, einschließlich der Konfiguration von Eigenschaften, der Erstellung von Identitätsanbietern (IDPs) und der Konfiguration von Anwendern für die Verwendung von SSO.

Weitere Informationen zu den einzelnen Konfigurationen finden Sie in den folgenden Themen.

- Multianbieter-SSO (SAML)-IdP-Authentifizierungs-Flow
- Konfigurieren Sie SSO-Eigenschaften für mehrere Anbieter
- Erstellen Sie einen externen Identitätsanbieter
- Konfigurieren Sie Anwender für Multi-Provider-SSO

Konfigurieren Sie SSO-Eigenschaften für mehrere Anbieter

Konfigurieren Sie SSO-Eigenschaften, und fügen Sie der Tabelle „Systemeigenschaften“ eine Eigenschaft hinzu, um eine IdP-Aufnahmeliste zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

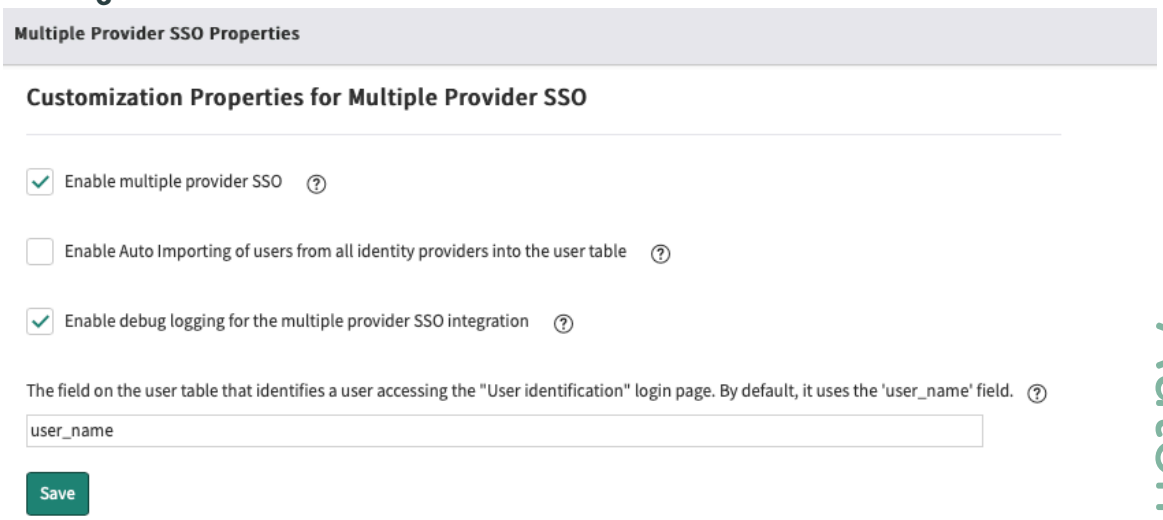
1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Administration** > **Eigenschaften**an.
2. Wählen Sie aus **Aktivieren Sie Multi-Provider-SSO** Kontrollkästchen.
   Diese Auswahl fügt der Anmeldeseite den Link „externe Anmeldung verwenden“ hinzu.
3. Bis Aktualisieren Sie die Anwendertabelle Wählen Sie mit den Anwendern im IdP die aus **Aktivieren Sie Den Automatischen Import** Option.
4. Damit die Debug-Nachrichten unten im Inhalts-Frame angezeigt werden, wählen Sie aus **Aktivieren Sie die Debug-Protokollierung für die SSO-Integration mit mehreren Anbietern** Kontrollkästchen.
   Wenn diese Option aktiviert ist, verlangsamt die Debug-Protokollierungsfunktion die Leistung und verbraucht Speicherplatz, um Protokolle zu generieren.
5. In der Eigenschaft **Das Feld in der Anwendertabelle, das einen Anwender identifiziert, der auf die Anmeldeseite „Anwenderidentifizierung“ zugreift** , Geben Sie das Feld in der Anwendertabelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ein, das den Wert enthält, den der IdP zur Identifizierung des Anwenders verwendet. Der Standardwert ist **Anwendername** .

Der Standardwert ist **Anwendername** .

SSO-Eigenschaften mehrerer Anbieter



6. Klicken Sie auf **Speichern**.
7. Weisen Sie Ihre Anwender an, auf zu klicken **Externe Anmeldung verwenden** Link, wenn sie sich bei der Instanz anmelden.

Zugehörige Informationen

SAML-Anwenderbereitstellung

Erstellen Sie einen externen Identitätsanbieter

Nachdem Sie die SSO-Eigenschaften für mehrere Anbieter konfiguriert haben, können Sie den Identitätsanbieter für SAML 2,0- oder Digest-Token aktualisieren oder neu erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Klicken Sie auf den Datensatz, um einen Identitätsanbieter-Datensatz zu bearbeiten.
   - Aktualisieren Sie für Digest-Token-Konfigurationen die Eigenschaften manuell.
   - Aktualisieren Sie für Konfigurationen von SAML2 Update 1 die Metadaten des Identitätsanbieters automatisch mit **Importieren Sie Metadaten Des Identitätsanbieters** Zugehöriger Link oder aktualisieren Sie die Eigenschaften manuell.
   - Aktualisieren Sie für OpenID Connect-Konfigurationen die Eigenschaften manuell.
3. Klicken Sie auf, um einen neuen Identitätsanbieter zu erstellen **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Digest-Token-Konfigurationen: Klicken Sie auf **Digest-SSO** Und geben Sie die Digest-Eigenschaften für Single Sign-on für mehrere Anbieter ein.
- Für SAML2-Konfigurationen: Klicken Sie auf **MultiSSOV2_SAML2_custom** Und importieren Sie die Metadaten des Identitätsanbieters aus einer URL als XML, oder geben Sie die Informationen des Identitätsanbieters manuell ein.



- Für OpenID Connect: Klicken Sie auf **OpenID Connect** Und geben Sie die Client-ID, den geheimen Client und die bekannte Konfigurations-URL ein.

4. Um den IdP zum Failover-IdP zu machen, der verwendet wird, wenn der Standard-IdP nicht verfügbar ist, wählen Sie aus **Standard** Kontrollkästchen.

   Wenn Sie SAML 2 Update 1 aktiv haben und ein Upgrade auf das Fuji-Release durchführen, wird SAML 2 Update 1 IdP als Standard-Failover ausgewählt. Für neue Instanzen oder wenn Sie ein Upgrade von einem Release durchführen, in dem SAML 2 Update 1 nicht aktiv ist, ist kein Standard-Failover-IdP ausgewählt.

   Hinweis: Der Metadatenimport erstellt automatisch einen Zertifikatdatensatz für den Identitätsanbieter. Navigieren Sie zu **x509-Zertifikat** Modul zum Anzeigen des Zertifikats.

   Hinweis: Zertifikate für Single Sign-on müssen immer im PEM-Format vorliegen, um mit SAML-Zertifikaten zu arbeiten.

5. Wenn E-Signatur aktiv ist, konfigurieren Sie das Formular „Identitätsanbieter“, und fügen Sie hinzu **Assertion-Verbraucher-URL für eSignature-Authentifizierung** Feld.
   In den meisten Fällen lautet diese URL: `https://YOURINSTANCE.service-now.com/consumer.do` .
   Wenn Sie jedoch eine anwenderdefinierte Methode zur Verarbeitung der SAML-Authentifizierung für E-Signatur verwenden, können Sie Ihre eigene Verbraucher-URL einrichten. Wenn Sie nur SAML 2,0 Update 1 verwenden und nicht Single Sign-on für mehrere Anbieter verwenden, konfigurieren Sie die Assertion-Verbraucher-URL mit SAML-Eigenschaften der E-Signatur .

Generieren Sie SP-Metadaten (Instanzservice Provider) für SAML

Im Rahmen Ihrer SSO-Konfiguration können Sie die Instanz-SP-Metadaten generieren, die dem IdP bereitgestellt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der IdP benötigt die SP-Metadaten der Instanz, um Anforderungen zu authentifizieren und weiterzuleiten.

Prozedur

1. Wählen Sie Ihr installiertes SSO-Plugin aus:

Option	Bezeichnung
Mehrfachanbieter-SSO	Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an. Wählen Sie einen IdP aus, und klicken Sie auf **Generieren Sie Metadaten** Schaltfläche. Die Integration generiert automatisch die SP-Metadaten der Instanz aus den Systemeigenschaftseinstellungen.
SAML 2 SSO	Navigieren zu **SAML 2 Single Sign-on** > **Metadaten**an. Die Integration generiert automatisch die SP-Metadaten der Instanz aus den Systemeigenschaftseinstellungen.

2. Kopieren Sie die SP-Metadaten in das Textfeld.

   Zum Beispiel:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Geben Sie die Instanz-SP-Metadaten für den IdP an.
   Beispielsweise ermöglicht SSOCircle einem Anwender, die SP-Metadaten online bereitzustellen.

Konfigurieren Sie Anwender für Multi-Provider-SSO

Administratoren können Multi-Provider-SSO für einzelne Anwender oder für alle Anwender konfigurieren, die einem Unternehmen angehören. Sie können Multi-Provider-SSO für Gruppen nicht konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Klicken Sie mit der rechten Maustaste auf den Datensatz eines Identitätsanbieters und wählen Sie **sys_id kopieren**.
3. Kopieren Sie die Daten in Ihre Zwischenablage.
4. Navigieren Sie zu einem Anwenderdatensatz oder einem Unternehmensdatensatz.
5. Konfigurieren Sie das Formular, und fügen Sie hinzu **SSO-Quelle** Feld.
6. In **SSO-Quelle** Geben Sie einen der folgenden Felder ein:
   - **SAML-Anwender** : Eingabetaste **sso:** Gefolgt von der sys_ID des Datensatzes des Identitätsanbieters.
   - **SSO-Verbundanwender** : Eingabetaste **föderation:** Gefolgt von der sys_ID des Verbunddatensatzes.
7. Klicken Sie auf **Aktualisieren**.

Testen Sie IdP-Verbindungen

Durch das Testen der Verbindung zu einem IdP werden die Einstellungen validiert, bevor die externe Authentifizierung aktiviert wird.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Das Jakarta-Release unterstützt die Testverbindung in einem Popup-Fenster. Wenn Ihr IdP mit dieser Option nicht ordnungsgemäß funktioniert, können Sie diese Standardeinstellung deaktivieren.

Der Auftrag „MultiSSO-IDP-Metadaten aktualisieren“ ruft das Zertifikat für den IdP ab und aktualisiert es, während die Verbindung erstellt, aktualisiert oder getestet wird.

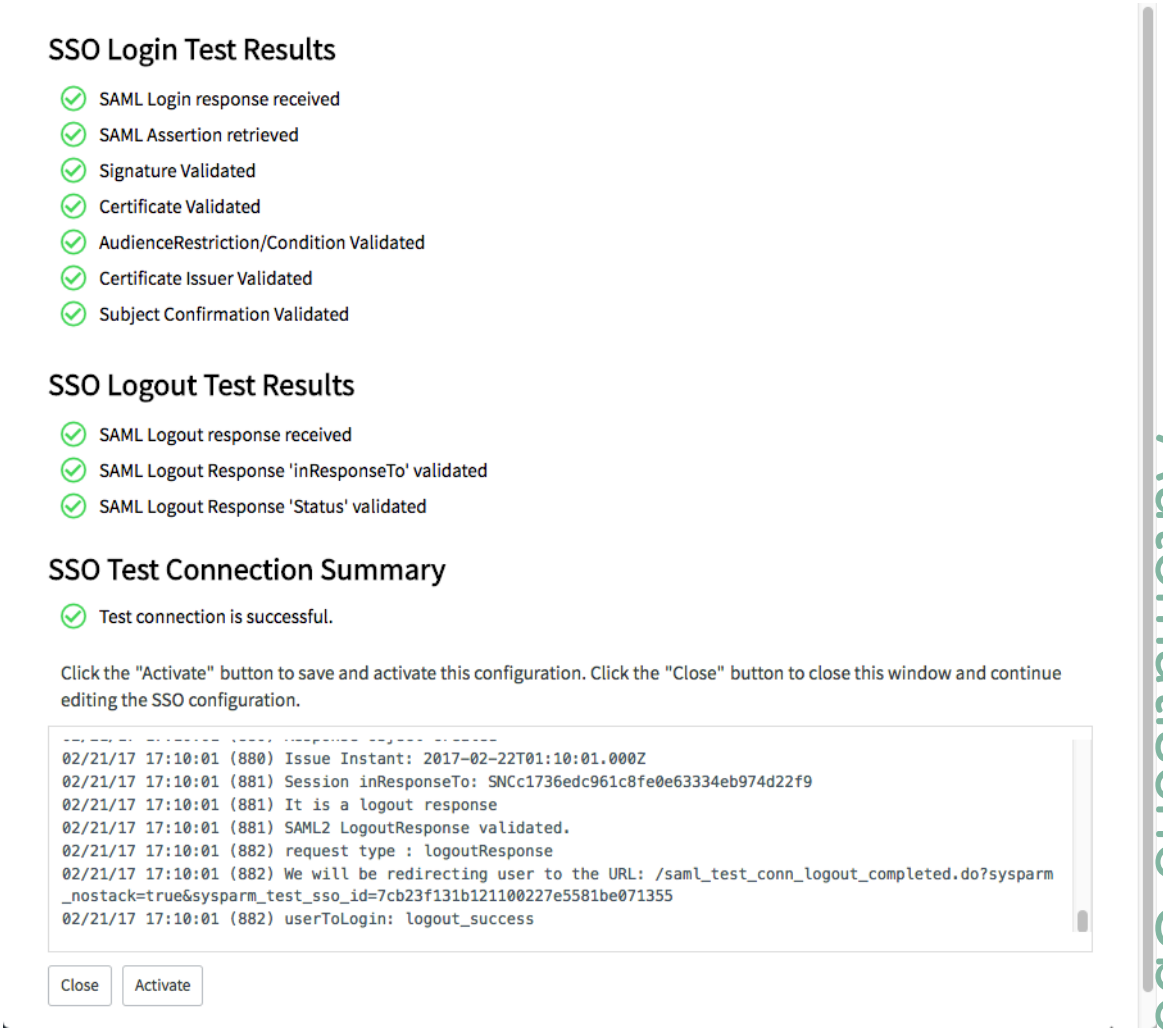
Hinweis: Wenn die Testverbindung fehlgeschlagen ist, müssen in einigen idp-Fällen glide.authenticate.multisso.test.connection.mandatory mit dem Wert „falsch“ erstellt werden, und Sie können den idp ohne Testverbindung aktivieren.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Wählen Sie einen definierten IdP aus, oder klicken Sie auf **Neu** Zum Definieren eines neuen IdP.
3. **Wahlweise:** Konfigurieren Sie einen Identitätsanbieter, wenn Sie einen neuen IdP einrichten.
4. Klicken Sie Auf **Verbindung Testen** , Geben Sie Anmeldeinformationen für den IdP ein, um die Anmeldung zu überprüfen.
   Sie können den IdP erst aktivieren, wenn Sie eine erfolgreiche Testverbindung haben. Wenn der Test fehlschlägt, können Sie aktualisieren, um Ihre Konfigurationsinformationen zu speichern, Sie können diese Konfiguration jedoch nicht aktivieren.
5. Überprüfen Sie die Ergebnisse mit **SSO-Testergebnisse/Zusammenfassung** Oder **SSO-Protokolle werden getestet** Abschnitt zum Anzeigen von Protokollnachrichten.
   Informationen zu Fehlern finden Sie unter Multi-SSO (SAML 2,0) – Fehler und Korrekturen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie Auf **Abbrechen** Wenn der Test abgeschlossen ist.



Allgemeine IdP-Verbindungsfehler

In der folgenden Tabelle werden einige der häufigsten IdP-Verbindungsfehler und ihre Lösungen beschrieben.

Fehlerbehebung bei IdP-Testverbindungen

Fehlermeldungen	Lösung
Validierung des Anwenderfelds fehlgeschlagen. Ungültiges Anwenderfeld „<field name>“ ist kein Feld in der Tabelle „sys_user“.	Überprüfen Sie, ob der Inhalt des von Ihnen ausgewählten Anwendertabellenfelds mit dem SAML NameID-Token übereinstimmt.
Assertionsaussteller ist ungültig.	Verifizieren **URL des Identitätsanbieters** Enthält eine gültige URL für Ihren IdP. Jede IdP-URL muss eindeutig sein.
Validierung von AudienceRestriction fehlgeschlagen.	Verifizieren Sie **Zielgruppen-URI** Enthält eine gültige URL für Ihre Instanz.
Abmeldung von IdP-Sitzung nicht möglich.	Verifizieren Sie **SingleLogoutRequest** URL enthält eine gültige URL für den Abmeldeservice Ihres IdP.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlerbehebung bei IdP-Testverbindungen (Fortsetzung)

Fehlermeldungen	Lösung
Signatur wurde nicht anhand des Schlüssels der Anmeldeinformationen validiert.	Überprüfen Sie, ob für den IdP ein gültiges Zertifikat installiert ist.

Beheben Sie Skriptprobleme mit SAML

Beheben Sie Skriptprobleme mit SAML. Möglicherweise treten Skriptprobleme auf, wenn SAML zum Zeitpunkt der Aktivierung mehrerer Single Sign-on bereits aktiv ist und wenn Sie die Installation bereits angepasst haben.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Sichern Sie den geänderten Installationsausgang SAML2SingleSignon_update1 und die Skripteinbindung SAML2_update1.
2. Setzen Sie sowohl den Installationsausgang als auch die Skripteinbindung auf die Version zurück, die mit dem Baseline-System verfügbar ist.
3. Aktivieren oder aktualisieren Sie **Integration: Single Sign-On-Installationsprogramm Für Mehrere Anbieter** Plugin.
   Das System aktualisiert SAML und alle erforderlichen Dateien auf SAML 2 Update 1.
4. Öffnen Sie die Seite mit mehreren SSO-Eigenschaften, und wählen Sie aus **Aktivieren Sie Multi-Provider-SSO** Kontrollkästchen zum Aktivieren.
5. Fügen Sie die SAML2SingleSignon_update1-Installationsausgangsänderungen in die Baseline-Skripteinbindung ein **MultiSSO_SAML2_Update1 und SAML2_update1** Skripteinbindung ändert sich in der Baseline-Skripteinbindung SAML2_update1.

Melden Sie sich mit Multi-Provider-SSO an

Die empfohlene und effizienteste Methode für Anwender, sich mit Multi-Provider-SSO anzumelden, besteht in der Verwendung einer speziell konfigurierten URL.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Nachdem SSO für mehrere Anbieter konfiguriert ist, können Sie eine URL mit dem richtigen IdP in der Parameterzeichenfolge an Ihre Anwender senden. Zum Beispiel:

```
/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Nachdem sich ein Anwender erfolgreich bei der IdP-Seite angemeldet hat, wird dem Browser ein Cookie mit der IdP-sys_ID hinzugefügt. Wenn der Anwender das nächste Mal versucht, sich anzumelden, leitet das System den Anwender um, sich beim IdP-Server anzumelden, der sich automatisch bei der Instanz anmeldet.

Wenn kein URL-Parameter festgelegt ist oder der Browsercache gelöscht wurde, können Anwender auch Folgendes tun:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie auf **Externe Anmeldung verwenden** Link auf der Anmeldeseite.

   Die externe Anmeldeseite wird angezeigt. Anwender können auf klicken **Lokale Anmeldung verwenden** Um zur Standard-Anmeldeseite zurückzukehren.

2. Geben Sie den Wert für das angegebene Feld in der Anwendertabelle ein, die Sie in Multi-Provider-SSO-Eigenschaften konfiguriert haben.

   Der Anwender wird zum IdP-Server weitergeleitet, auf dem er sich anmeldet.

Ergebnis

Nachdem sich Anwender erfolgreich bei einem IdP angemeldet haben, werden sie automatisch zu diesem IdP weitergeleitet, wenn sie versuchen, auf die Instanz zuzugreifen. Damit ein Anwender auf einen anderen IdP zugreifen kann, senden Sie dem Anwender eine URL mit den neuen IdP-Informationen im Parameter. Der neue IdP überschreibt den alten IdP im Cookie, wenn sich der Anwender erfolgreich anmeldet. Wenn sich der Anwender nicht erfolgreich anmeldet, werden die alten IdP-Informationen im Cookie beibehalten.

Ermöglichen Sie Anwendern, den Identitätsanbieter für die Anmeldung auszuwählen

Mit der Unterstützung von SSO-Verbund können Anwender auswählen, bei welchem IdP Sie sich anmelden möchten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

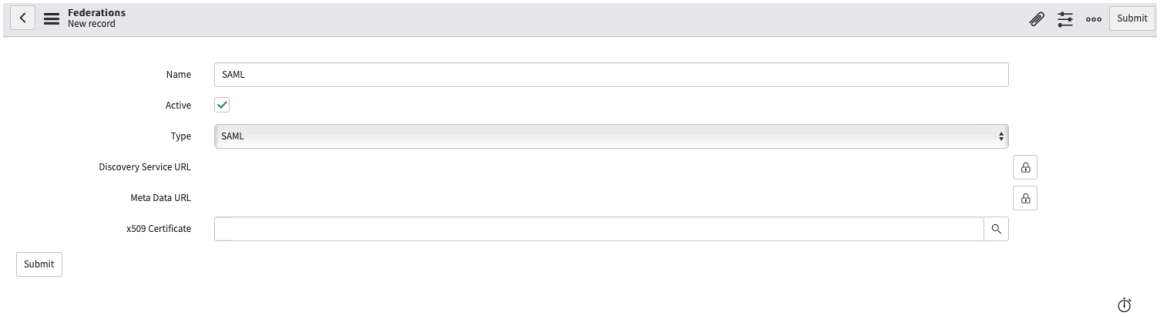
SSO-Verbände aggregieren Metadaten von mehreren IDPs und Service Providern, einschließlich Ihrer Instanz. Verbünde veröffentlichen die Metadaten dann als XML-Datei, die Informationen wie IdP-Namen und IdP-Zertifikate enthält. Administratoren können dann die Instanz anweisen, die XML-Datei zu lesen und die Tabelle „SSO-Eigenschaften“ automatisch mit allen erforderlichen IdP-Informationen auszufüllen.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Verbund**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.
5. Nachdem Sie einen Verbund konfiguriert haben, aktivieren Sie die geplante Aufgabe SSO-Metadaten aktualisieren und dann Konfigurieren Sie die Anwender, die Sie auf die Verbund-IDPs zugreifen möchten . Verwenden Sie die sys_ID des soeben erstellten Verbunddatensatzes.

   Verwenden Sie die sys_ID des Verbund-Datensatzes, den Sie gerade erstellt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Instanz füllt die SSO-Eigenschaftentabelle mit den IdP-Informationen aus. Wenn sich Anwender anmelden, die für die Verwendung des Verbunds konfiguriert sind, werden sie zur von Ihnen konfigurierten Discovery-Service-URL weitergeleitet. Dann wählen sie den IdP aus und stellen die erforderlichen Anmeldeinformationen bereit. Alternativ können Sie Anwendern eine URL mit dem IdP im Parameter senden.

Ermöglicht Anwendern, den Identitätsanbieter für die Anmeldung auszuwählen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für die Vereinigung ein.
Aktiv	Aktivieren Sie das Kontrollkästchen, damit die Instanz die XML-Datei aus dem Verbund abrufen kann.
Typ	Wählen Sie die Art der Authentifizierung aus, die diese Vereinigung unterstützt.
Discovery Service-URL	Geben Sie die URL des Discovery-Service für diesen Verbund ein. Dies ist die Website, auf der Anwender angewiesen werden, einen IdP auszuwählen und sich anzumelden.
Metadaten-URL	Geben Sie die URL der XML-Datei ein, die die Verbundmetadaten enthält.
x509-Zertifikat	Wählen Sie das Verbundzertifikat aus.
Domäne	Wählen Sie die Domäne aus, zu der die Daten gehören sollen.

Hinweis: Der InCommon-IdP für das föderierte Identitätsmanagement ist vorkonfiguriert.

Verwenden Serviceportal Mit Multi-Provider-SSO zum Umleiten einer URL

Serviceportal Verwendet eine Kombination aus Systemeigenschaften und Skripteinbindungen, um zu bestimmen, wie das System URL-Weiterleitungen für Benutzer vornimmt, die sich beim Portal anmelden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die Systemeigenschaft verwenden, um automatisch zu Ihrem primären Identitätsanbieter (IdP) umzuleiten, dann Serviceportal Leitet automatisch zu diesem IdP um. Wenn Sie mehrere IDPs haben, Serviceportal Zeigt einen Link auf der Anmeldeseite zu an **Externe Anmeldung verwenden** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Service Portal-Anmeldeseite konfigurieren
2. Nach der Anmeldung zum Serviceportal umleiten

Accountwiederherstellung (ACR)

Administratoren können die Accountwiederherstellung (ACR) konfigurieren, um Wiederherstellungsaktivitäten durchzuführen, z. B. die Behebung von SSO-Fehlkonfigurationen oder abgelaufenen Zertifikaten.

Hinweis: Durch Aktivieren von ACR werden die lokalen interaktiven Anmeldungen (basierend auf Anwendername oder Passwort) deaktiviert, wenn SSO für Ihre Instanzen aktiviert ist.

ACR bietet die folgenden Fähigkeiten:

- Umgehen Sie Ihre SSO-Anmeldung (Single Sign-on), um Probleme mit der SSO-Konfiguration als Administrator zu beheben.
- Melden Sie sich mit SSO an, um Aufgaben mit einem Administrator-Account auszuführen, der als Accountwiederherstellung konfiguriert ist.
- Mit ACR-Flows können Administratoren Selfservice-Fähigkeiten verwenden, um die Accountwiederherstellung zu beheben, wenn eine Wiederherstellung erforderlich ist, z. B. SSO-Fehlkonfiguration oder abgelaufene Zertifikate.
- Reduzieren Sie nicht autorisierten Zugriff auf die Instanz, und stellen Sie eine solide Grundlage für die Verwendung von ACR außerhalb von SSO-Anwendungsfällen bereit.

Neue Instanz

Damit eine neue Instanz ACR verwenden kann, müssen Sie Folgendes tun:

- Mutli-SSO-Plugin aktivieren (`com.snc.integration.sso.multi.installer`)
- ACR aktivieren (`Glide.sso.acr.aktiviert`): Diese Option ist im Falle einer neuen Instanz standardmäßig aktiviert.
- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`), muss sich der Administrator als ACR-Anwender registrieren.

  Hinweis: Wenn Sie diese Eigenschaft auf „falsch“ festlegen, wird SSO für mehrere Anbieter nicht deaktiviert, wenn die Accountwiederherstellung (ACR) auch in der Instanz aktiviert ist. Um sich mit einem Anwendernamen und Passwort anzumelden, muss ACR auch mit deaktiviert werden `glide.sso.acr.enabled`Eigenschaft. Einzelheiten zu dieser Eigenschaft finden Sie unter Accountwiederherstellungseigenschaften.

- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Anwender registriert.

Instanz Aktualisiert

Damit eine aktualisierte Instanz ACR verwenden kann, müssen Sie Folgendes tun:

- Mutli-SSO-Plugin aktivieren (`com.snc.integration.sso.multi.installer`)
- ACR aktivieren (`Glide.sso.acr.aktiviert`)

  Hinweis: Im Falle einer aktualisierten Instanz muss der Administrator ACR aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`), muss sich der Administrator als ACR-Anwender registrieren.
- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Anwender registriert.

Konfigurieren Sie Benutzer der Accountwiederherstellung

Um die Accountwiederherstellung zu verwenden, müssen Sie mindestens einen Administratoraccount als Accountwiederherstellungsanwender registrieren. Single Sign-on kann in Ihrer Instanz erst aktiviert werden, wenn mindestens ein Account konfiguriert ist. Details zu diesem Vorgang finden Sie unter Konfigurieren Sie einen Accountwiederherstellungsanwender auf der Seite Accountwiederherstellungseigenschaften.

Hinweis: Wenn Sie ein Upgrade einer Instanz durchführen, die bereits Single Sign-on auf verwendet Rome Oder in einem späteren Release funktioniert die Single Sign-on weiterhin, ohne dass ein Wiederherstellungsanwender konfiguriert ist.

Konfiguration der Accountwiederherstellung

Die Accountwiederherstellungsfunktion ist im enthalten **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter (com.snc.integration.sso.multi.installer)-Plugins** . Die Funktion ist standardmäßig aktiviert. Sie können diese und andere Einstellungen für die Accountwiederherstellung mithilfe von Systemeigenschaften ändern. Weitere Informationen zu diesen Eigenschaften finden Sie unter Accountwiederherstellungseigenschaften.

Kontext der Account-Wiederherstellungsrichtlinie

Nachdem Sie einen Benutzer zur Accountwiederherstellung registriert und Single Sign-on (SSO) aktiviert haben, schränkt Ihre Instanz alle lokalen Anmeldungen ein. Diese Einschränkung ist in definiert **SSO: ACR-Kontext** Authentifizierungsrichtlinienkontext. Weitere Informationen zum Kontext finden Sie unter Account-Wiederherstellungskontext.

Details zur Funktionsweise von Authentifizierungsrichtlinien und Richtlinienkontexten in Ihrer Instanz finden Sie unter Adaptive Authentifizierung.

Konfigurieren Sie einen Accountwiederherstellungsanwender

Konfigurieren Sie einen Accountwiederherstellungsanwender, um Accountwiederherstellungsaktivitäten in Ihrer Instanz durchzuführen.

Ein Benutzer der Accountwiederherstellung ist ein Anwenderaccount, mit dem Administratoren Accountwiederherstellungsaufgaben ausführen können, z. B. die Behebung einer SSO-Fehlkonfiguration oder die Behebung abgelaufener Zertifikate.

Hinweis: Wenn Sie die Accountwiederherstellung in Ihrer Instanz verwenden, müssen Sie einen Accountwiederherstellungsanwender konfigurieren. Dieser Schritt ist erforderlich, bevor Single Sign-on für mehrere Anbieter auf einer Instanz aktiviert wird.

Konfigurieren Sie einen Accountwiederherstellungsanwender auf der Seite Accountwiederherstellungseigenschaften

Konfigurieren Sie eine Accountwiederherstellung auf der Seite mit den Accountwiederherstellungseigenschaften.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um ACR in einer neuen Instanz zu konfigurieren, müssen Sie Folgendes tun:

- Mutli-SSO-Plugin aktivieren (`com.snc.integration.sso.multi.installer`)
- ACR aktivieren (`Glide.sso.acr.aktiviert`): Diese Option ist im Falle einer neuen Instanz standardmäßig aktiviert.
- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`), muss sich der Administrator als ACR-Anwender registrieren.
- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Anwender registriert.

Damit eine aktualisierte Instanz ACR verwenden kann, müssen Sie Folgendes tun:

- Mutli-SSO-Plugin aktivieren (`com.snc.integration.sso.multi.installer`)
- ACR aktivieren (`Glide.sso.acr.aktiviert`)

  Hinweis: Im Falle einer aktualisierten Instanz muss der Administrator ACR aktivieren.

- Vor dem Aktivieren der SSO-Eigenschaft (`glide.authenticate.multisso.enabled`), muss sich der Administrator als ACR-Anwender registrieren.

  Hinweis: Wenn Sie diese Eigenschaft auf „falsch“ festlegen, wird SSO für mehrere Anbieter nicht deaktiviert, wenn die Accountwiederherstellung (ACR) auch in der Instanz aktiviert ist. Um sich mit einem Anwendernamen und Passwort anzumelden, muss ACR auch mit deaktiviert werden *`glide.sso.acr.enabled`*Eigenschaft. Einzelheiten zu dieser Eigenschaft finden Sie unter Accountwiederherstellungseigenschaften.

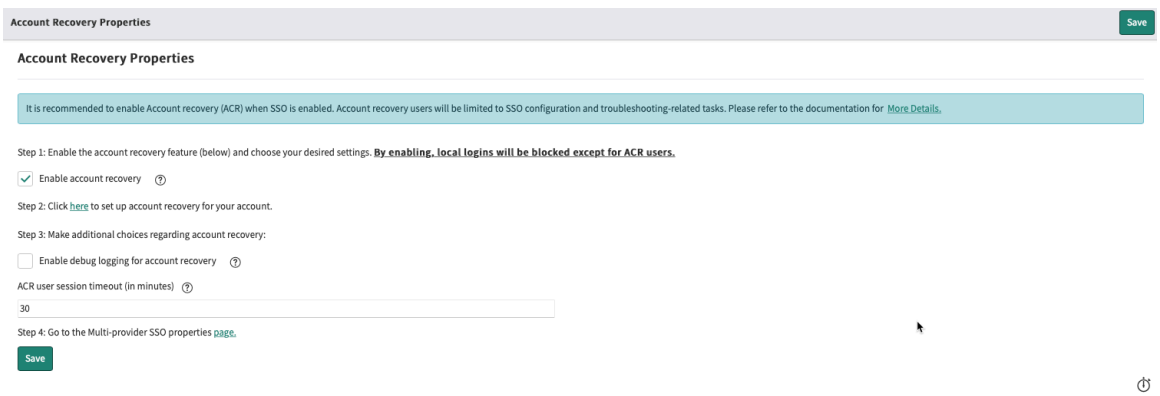
- Der Administrator muss ein Passwort für die lokale Anmeldung festlegen und MFA registrieren, bevor er sich als ACR-Anwender registriert.

Prozedur

1. Navigieren zu **Alle** > **Accountwiederherstellung** > **Eigenschaften**an.
2. Klicken Sie Auf **Aktivieren Sie die Accountwiederherstellung** .

   Hinweis: Sie müssen die Accountwiederherstellung aktivieren, wenn SSO aktiviert ist. Benutzer der Accountwiederherstellung sind auf SSO-Konfigurations- und Fehlerbehebungsaufgaben beschränkt.

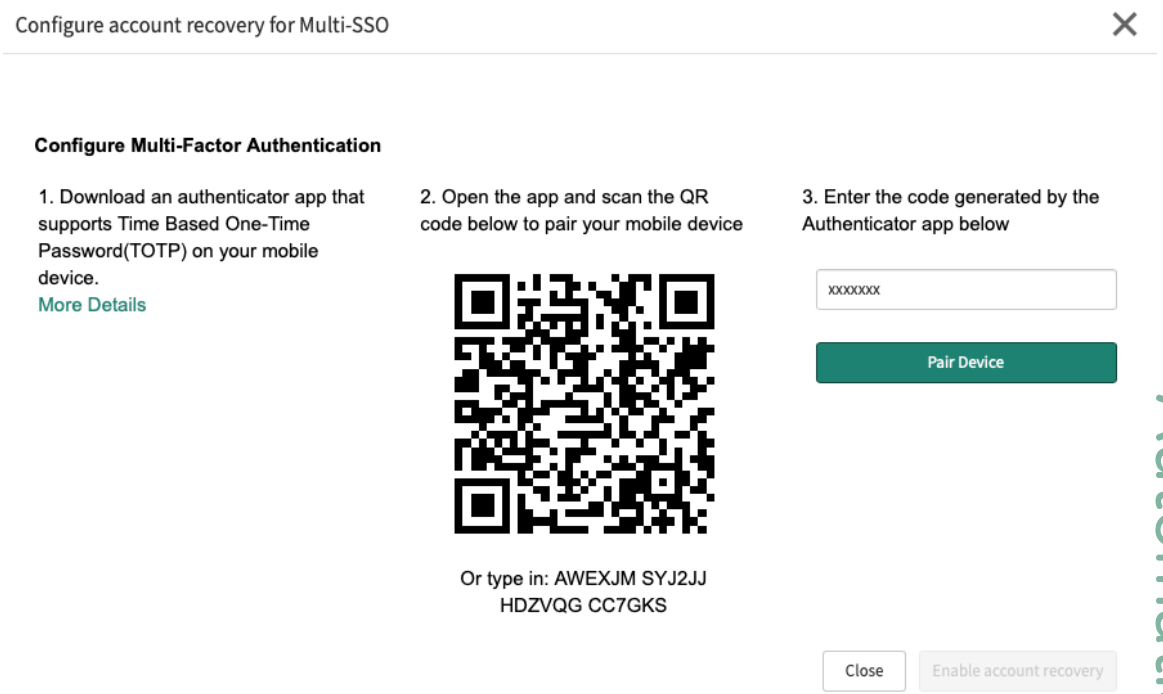
3. Klicken Sie auf **Hier** Text in Schritt 2.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Befolgen Sie die Anweisungen auf dem Bildschirm in **Konfigurieren Sie die Accountwiederherstellung für Multi-SSO** Modal.



Nach Abschluss der Schritte auf dem Bildschirm wird die **Aktivieren Sie die Accountwiederherstellung** Ist aktiviert.

5. Klicken Sie Auf **Aktivieren Sie die Accountwiederherstellung** .

Ergebnis

Sie haben Ihren Anwenderaccount als Anwender der Accountwiederherstellung konfiguriert. Sie können diesen Account verifizieren und alle anderen konfigurierten Benutzer der Accountwiederherstellung anzeigen, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Anwender**an.

Konfigurieren Sie einen Accountwiederherstellungsanwender über ein Administrator-Anwenderprofil

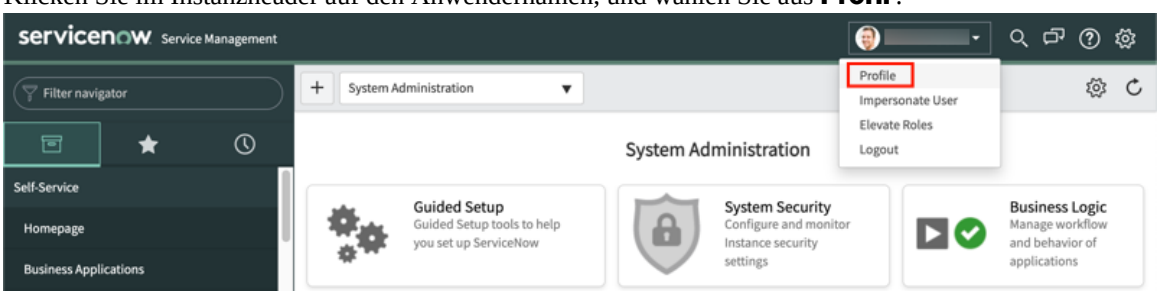
Konfigurieren Sie einen Administrator als Benutzer der Accountwiederherstellung über das Administratoranwenderprofil.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

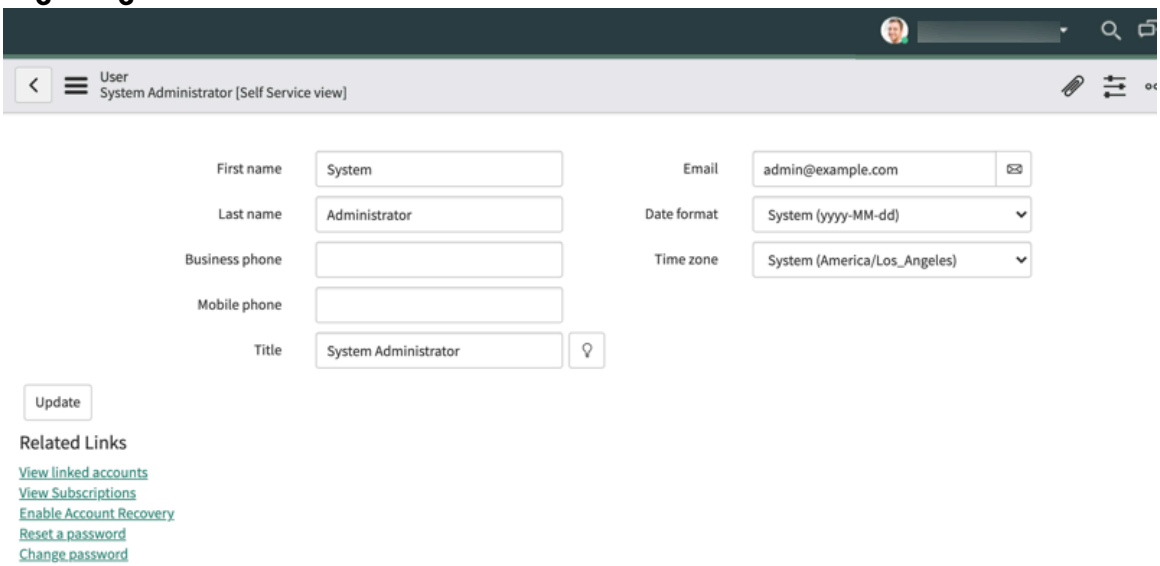
1. Melden Sie sich mit einem Administrator-Account bei Ihrer Instanz an.
2. Klicken Sie im Instanzheader auf den Anwendernamen, und wählen Sie aus **Profil** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

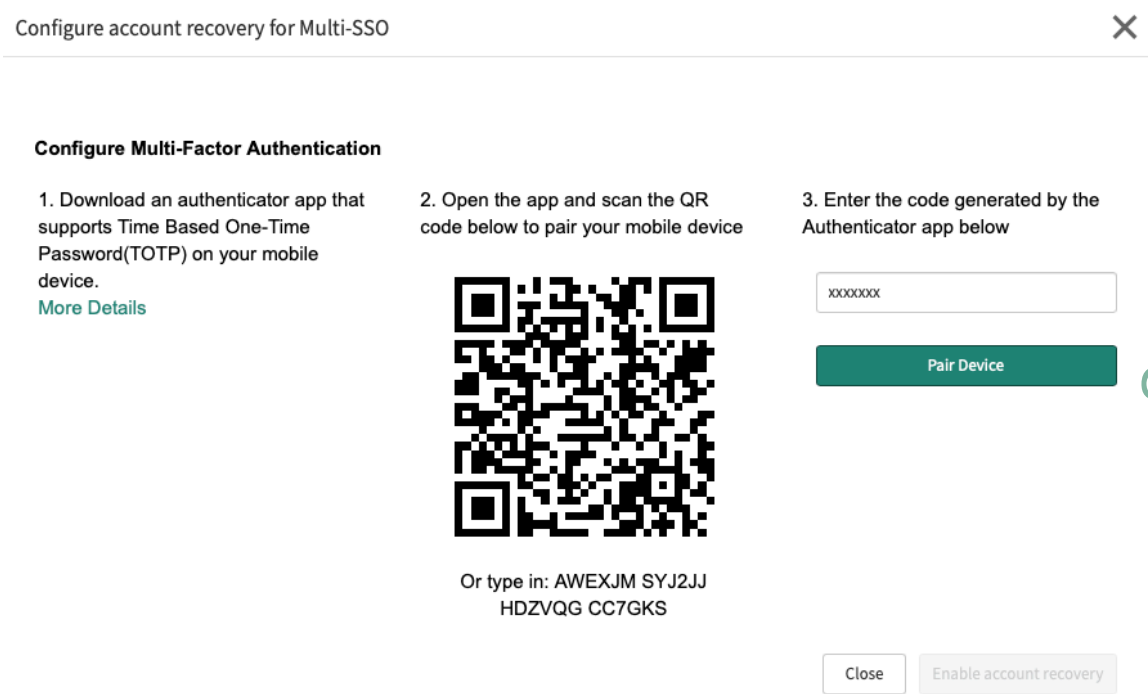
3. In **Anwender** Formular klicken Sie auf **Aktivieren Sie Die Accountwiederherstellung** In **Zugehörige Links** Abschnitt.



Hinweis:

Wenn für den ausgewählten Anwender die Accountwiederherstellung bereits aktiviert ist, **Aktivieren Sie Die Accountwiederherstellung** Wird nicht in den zugehörigen Links angezeigt. Es wird ein geben **Deaktivieren Sie Die Accountwiederherstellung** Stattdessen Option.

4. Befolgen Sie die Anweisungen auf dem Bildschirm in **Konfigurieren Sie die Accountwiederherstellung für Multi-SSO** Modal.



Nach Abschluss der Schritte auf dem Bildschirm wird die **Aktivieren Sie die Accountwiederherstellung** Ist aktiviert.

5. Klicken Sie Auf **Aktivieren Sie die Accountwiederherstellung** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Sie haben Ihren Anwenderaccount als Anwender der Accountwiederherstellung konfiguriert. Sie können diesen Account verifizieren und alle anderen konfigurierten Benutzer der Accountwiederherstellung anzeigen, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Anwender**an.

Accountwiederherstellungseigenschaften

Verwenden Sie Systemeigenschaften, um die Accountwiederherstellung (ACR) in Ihrer Instanz zu konfigurieren.

Greifen Sie auf die Accountwiederherstellungseigenschaften in Ihrer Instanz zu, indem Sie zu navigieren **Mehrfachanbieter-SSO** > **Accountwiederherstellung** > **Eigenschaften**an.

Systemeigenschaften der Accountwiederherstellung

Eigenschaft	Beschreibung
Accountwiederherstellungsfunktion aktivieren [Glide.sso.acr.enabled]	Gibt an, ob die Accountwiederherstellungsfunktion in Ihrer Instanz aktiviert ist. Diese Eigenschaft ist standardmäßig aktiviert.
Debug-Protokollierung für Accountwiederherstellung aktivieren [glide.sso.acr.debug.log.enabled]	Gibt an, ob Ihre Instanz Accountwiederherstellungsinformationen in der Debug-Protokollierung enthält. Diese Eigenschaft ist standardmäßig deaktiviert.
Zeitüberschreitung der ACR-Anwendersitzung (in Minuten) [glide.sso.acr.ui.session.timeout]	Minuten Inaktivität, bevor Ihre Instanz eine Anwendersitzung zur Accountwiederherstellung beendet. Diese Eigenschaft hat den Standardwert 30.

E-Signatur für Multi-Provider-SSO

Mit E-Signatur mit Multi-Provider-SSO können Sie die E-Signatur-Eigenschaften anstelle der SAML- oder OIDC-Eigenschaften für die Authentifizierung verwenden.

Für die Verifizierung von Single Sign-on (SSO) während der Authentifizierung und damit Anwender Anmeldeinformationen angeben müssen, bevor sie ihre elektronische Signatur übermitteln, können Sie die Authentifizierung so konfigurieren, dass vor dem Senden einer Signatur die Anmeldeinformationen des Anwenders eingegeben werden.

Sie können die Genehmigungen mit E-Signatur (`Com.Glide.e_Signature_Approvals`) Plugin, um die E-Signatur-Konfiguration für SSO-Anmeldungen zu haben.

Hinweis: Sie müssen die Codesignatursignaturen (`Com.Glide.Code_Signature.Signatures`), um das E-Signatur-Plugin zu installieren.

Die Genehmigung mit dem E-Signatur-Plugin aktivieren

Die Genehmigung mit dem E-Signatur-Plugin (com.glide.e_signature_approvals) ermöglicht es Benutzern, Anforderungen zu genehmigen, indem sie ihre Anmeldeinformationen erneut eingeben.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: Sie müssen die Codesignatursignaturen (`Com.Glide.Code_Signature.Signatures`), um das E-Signatur-Plugin zu installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Verwenden Sie Multi-Provider-SSO, um eine SSO-Genehmigung für eine SAML 2,0-Authentifizierung einzurichten

Eine SSO-Genehmigung mit E-Signatur erfordert die Konfiguration der SAML-IdP und der ServiceNow-Instanz.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Das SAML-IdP muss das forceAuthn-Attribut in SAML-Bestätigungsanforderungen unterstützen und berücksichtigen. E-Signatur funktioniert ohne diese IdP-Einstellung nicht. Richten Sie eine Genehmigung mit E-Signatur mit Anmeldeinformationen aus einer SAML 2,0-Authentifizierung ein.

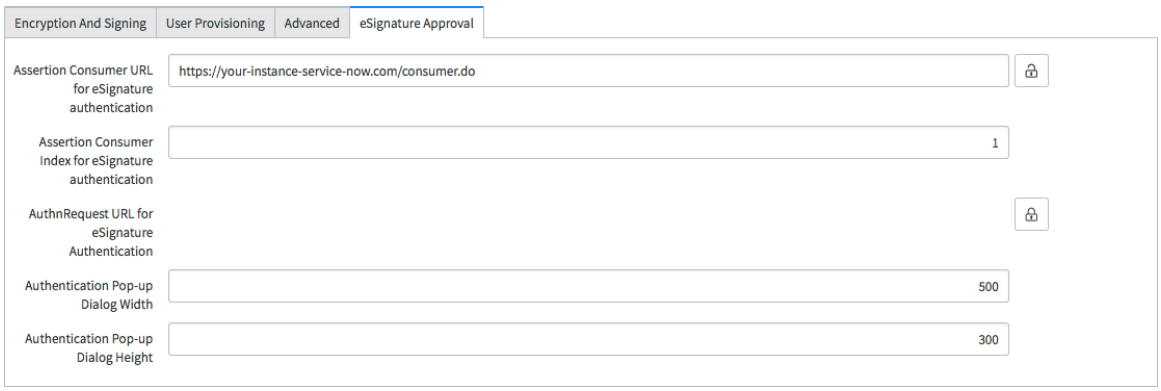
Prozedur

1. Aktivieren Sie mit SAML 2,0, oder führen Sie ein Upgrade auf SAML durch Aktivieren Sie das Multi-Provider-SSO-Plugin .
2. Aktivieren Sie das Plugin für die Genehmigung mit E-Signatur.
3. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider** Und überprüfen Sie, ob auf der Registerkarte Erweitert für die SAML-IdP-Konfiguration 2,0 angezeigt wird **AuthnRequest erzwingen** Attribut aktiviert.
   Ihr SAML 2,0-IdP muss unterstützen **AuthnRequest erzwingen** Attribut oder E-Signatur werden nicht unterstützt.
4. Geben Sie auf der Registerkarte E-Signatur-Genehmigung die folgenden SAML-Eigenschaften für E-Signatur ein.

Option	Bezeichnung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Diese Eigenschaft ist standardmäßig auf die entsprechende URL voreingestellt. Um diese Eigenschaft zu konfigurieren, wählen Sie das Schlosssymbol, um dieses Feld bearbeitbar zu machen. Wählen Sie nach der Bearbeitung das Symbol aus, um das Feld zu sperren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Assertionen-Verbraucher-Index für eSignatur-Authentifizierung	Wenn für Ihren Dienstanbieter mehr als eine URL für die AssertionConsumerURL festgelegt ist, können Sie den Index für die E-Signatur beginnend mit Index 1 oder höher festlegen.
AuthnRequest-URL für die E-Signatur-Authentifizierung	Sie können die URL eingeben, die auf die SAML 2.0 IdP AuthnRequest-URL für die E-Signatur-Authentifizierung verweist. Wenn die URL mit der Assertion Consumer-URL identisch ist, können Sie diese Einstellung leer lassen.
Breite des Popup-Dialogfelds für Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Breite dieses Dialogfelds. Der Standardwert ist 500.
Höhe des Popup-Dialogfelds für Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Höhe dieses Dialogfelds. Der Standardwert ist 300.



5. Wählen Sie aus **Generieren Sie Metadaten** Schaltfläche unter den Registerkarten, um die Metadaten des Service Providers erneut zu generieren.
6. Kopieren Sie die Metadaten des Service Providers, und aktualisieren Sie sie im SAML-IdP.

Verwenden Sie Multi-Provider-SSO, um eine SSO-Genehmigung für eine OIDC-Authentifizierung einzurichten

Eine SSO-Genehmigung mit E-Signatur erfordert die Konfiguration der SAML-IdP und der ServiceNow-Instanz.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

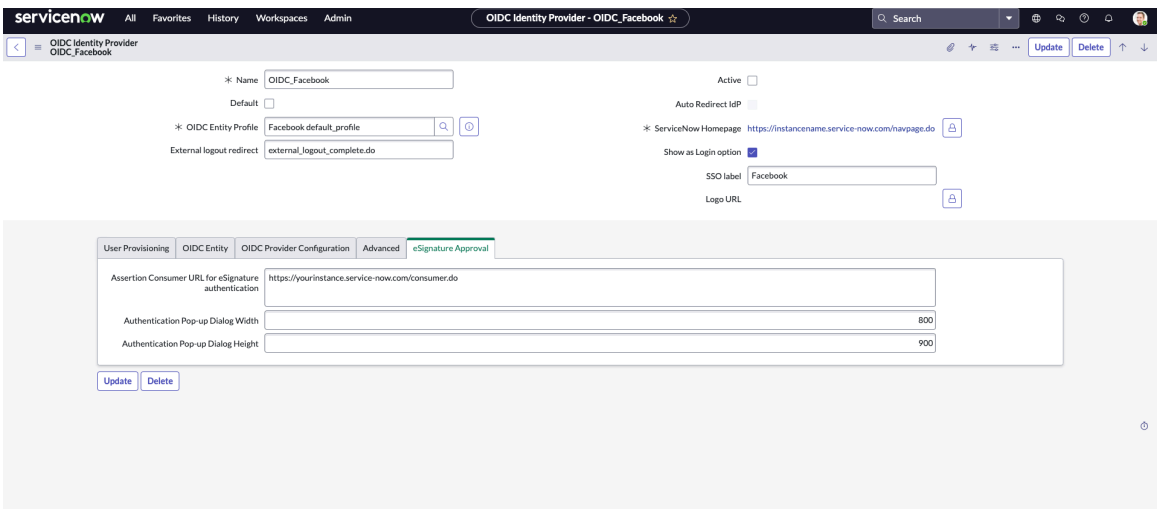
Das SAML-IdP muss das forceAuthn-Attribut in SAML-Bestätigungsanforderungen unterstützen und berücksichtigen. E-Signatur funktioniert ohne diese IdP-Einstellung nicht. Richten Sie eine Genehmigung mit E-Signatur mit Anmeldeinformationen aus einer SAML 2,0-Authentifizierung ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie das Plugin für die Genehmigung mit E-Signatur.
2. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider** Und überprüfen Sie Ihre OIDC-Anbieterkonfigurationen
3. Geben Sie auf der Registerkarte E-Signatur-Genehmigung die folgenden SAML-Eigenschaften für E-Signatur ein.

Option	Bezeichnung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Diese Eigenschaft ist standardmäßig auf die entsprechende URL voreingestellt. Um diese Eigenschaft zu konfigurieren, wählen Sie das Schlosssymbol, um dieses Feld bearbeitbar zu machen. Wählen Sie nach der Bearbeitung das Symbol aus, um das Feld zu sperren.
Breite des Popup-Dialogfelds für Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Breite dieses Dialogfelds. Der Standardwert ist 800.
Höhe des Popup-Dialogfelds für Authentifizierung	Wenn ein Benutzer eine Anforderung mit E-Signatur genehmigt, wird ein Dialogfeld geöffnet und ein Benutzer kann Anmeldeinformationen eingeben. Diese Einstellung steuert die Höhe dieses Dialogfelds. Der Standardwert ist 900.



4. Wählen Sie Aus **Übermitteln** Wenn Sie die E-Signatur während des ersten OIDC-Setups oder konfigurieren **Aktualisieren** Wenn Sie die Details in der E-Signatur aktualisieren möchten.

OpenID Connect (OIDC) als Single Sign-on (SSO)-Identitätsanbieter (IdP)

OpenID Connect (OIDC) ist eine Identitätsebene, die auf dem OAuth-Protokoll basiert und Ihnen und Ihren Endanwendern eine moderne und intuitive Single Sign-on (SSO)-Experience bietet.

OIDC verbessert die Anmelde-Experience für mobile Anwendungen, indem Anwender sich bei anmelden können ServiceNow Anwendungen, die ihren Social Identity Provider verwenden. Beispielsweise können Administratoren Single Sign-on mit einem Drittpartei-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identitätsanbieter konfigurieren, der OpenID Connect unterstützt. Anwender haben dann die Möglichkeit, sich bei Ihrem anwenderdefinierten anzumelden ServiceNow Anwendung mit ihren Identitätsanbieter-Anmeldeinformationen.

Sie können Social Identity Provider wie verwenden Google Für Ihre Business-to-Customer-Anwender (B2C) und Enterprise Identity Provider wie Okta, Microsoft Azure AD Für Ihre Business-to-Business-Anwender.

OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen

Erstellen oder aktualisieren Sie eine OpenID Connect-Konfiguration (OIDC) mit dem Multi-Provider SSO-Plugin.

OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO)

Vorbereitungen

- Registrieren Sie eine OIDC-Anwendung bei Ihrem Identitätsanbieter (Identity Provider, IdP), und notieren Sie sich die Client-ID, das geheime Clientgeheimnis und die bekannte Konfigurations-URL.
- Aktivieren Sie das Multi-Provider-SSO-Plugin . Die Multi-Provider-SSO-Funktion unterstützt die Domänentrennung. Sie können verschiedene IdPs für verschiedene Domänen angeben.
- Konfigurieren Sie SSO-Eigenschaften für mehrere Anbieter
- Aktivieren Sie das Plugin „Genehmigung mit E-Signatur“ Dient zum Aktivieren von eSignature für den OIDC-IdP.
- Erforderliche Rolle: Administrator

Wenn Sie über eine Client-ID, einen geheimen Client und eine bekannte Konfigurations-URL des Identitätsanbieters verfügen, können Sie die OIDC-Konfiguration für SSO direkt importieren.

Hinweis:

- Die **Melden Sie sich bei OIDC an** Die Schaltfläche wird auf der Anmeldeseite für OIDC-basierte IDPs nicht angezeigt, wenn das Plugin „Domänentrennung“ installiert ist.
- Der Administrator kann OIDC-basierte IdP verwenden, um SSO für einen Anwender eines bestimmten Unternehmens oder einer bestimmten Domäne zu aktivieren.

Wenn Sie nicht über die erforderlichen Informationen zum Identitätsanbieter verfügen, können Sie OIDC für SSO manuell konfigurieren. Nach Abschluss der Konfiguration können sich Anwender bei anmelden ServiceNow Anwendungen, die Drittanbieter für soziale Identität wie verwenden Google Okta.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Wählen Sie eine der folgenden Optionen aus.
   - Um eine vorhandene Konfiguration zu aktualisieren, klicken Sie auf einen OIDC-Identitätsanbieter-Datensatz.
   - Klicken Sie auf, um eine neue Konfiguration zu erstellen **Neu** Und wählen Sie aus **OpenID Connect** .
3. Geben Sie für eine neue Konfiguration die OIDC-Konfigurationsinformationen in eine der folgenden Methoden ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Importieren Sie die bekannte OpenID Connect-Konfiguration	Wenn Sie die bekannte Konfigurations-URL zusammen mit Ihren zugehörigen Client-Anmeldeinformationen haben, können Sie direkt eine OIDC-Konfiguration importieren. **Hinweis:** Wenn Sie die bekannte OIDC-Konfiguration importieren, werden alle zugehörigen Felder automatisch ausgefüllt.
Konfigurieren Sie das Formular „OIDC-Identitätsanbieter“ manuell	Wenn Sie keine vorhandene OAuth-OIDC-Entität haben, schließen Sie das Popup OpenID Connect-bekannte Konfiguration importieren, und füllen Sie die Felder im Formular „OIDC-Identitätsanbieter“ manuell aus.

Importieren Sie bekannte OpenID Connect-Konfigurationsfelder

Eigenschaft	Beschreibung
Name	Eindeutiger Name für die Konfiguration des OIDC-Identitätsanbieters.
Client-ID	Client-ID der Anwendung, die beim externen OIDC-Identitätsanbieter registriert ist.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die beim externen OIDC-Identitätsanbieter registriert ist.
Bekannte Konfigurations-URL	URL, die Metadaten zum Drittpartei-OIDC-Identitätsanbieter enthält.

Alle Pflichtfelder müssen im Formular „OIDC-Identitätsanbieter“ ausgefüllt werden.

Bevor Sie das Formular „OIDC-Identitätsanbieter“ manuell ausfüllen, stellen Sie sicher, dass Sie bereits über ein OAuth-Entitätsprofil für den OIDC-IdP verfügen.

Wenn Sie kein OAuth-Entitätsprofil haben, können Sie es mithilfe der standardmäßigen externen OIDC-Anbietervorlagen wie Okta, Azure und andere erstellen.

Der Gewährungstyp des OAuth-Entitätsprofils muss einen Autorisierungscode aufweisen. Weitere Informationen finden Sie unter Konfigurieren Sie einen OAuth-OIDC-Provider auf dem ServiceNow AI Platformanan.

Hinweis: Sie können die Vorlagen von Drittpartei-Identitätsanbietern verwenden, Auth0, Azure AD, Google und Okta sind in den Demodaten des Plugins „Single Sign-on-Installationsprogramm für mehrere Anbieter“ verfügbar.

OIDC-Identitätsanbieter-Felder

Eigenschaft	Beschreibung
Name	Name des OIDC-Identitätsanbieterdatensatzes.
Aktiv	Option zum Aktivieren der OIDC-IdP-Konfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Hinweis: Diese Option kann erst nach einer erfolgreichen Testverbindung auf „aktiv“ festgelegt werden.
Standard	Option zum Festlegen der OIDC-IdP-Konfiguration als Standard, wenn mehr als eine OIDC-Konfigurationen vorhanden sind.
Automatische IdP-Weiterleitung	Option zum Aktivieren der automatischen Weiterleitung der Anwender zur Anmeldeseite des Identitätsanbieters. Dieses Feld zeigt an, wenn **Als IdP für automatische Umleitung festlegen** Die Option wird im Abschnitt zugehörige Links festgelegt. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Umleitung aktivieren, wird die aktiviert `glide_sso_id`Cookie wird automatisch mit dem neuen IdP für automatische Weiterleitung aktualisiert. Die `glide.authenticate.sso.update.idp.cookie` Die Systemeigenschaft steuert diese Funktion.
OIDC-Entitätsprofil	OAuth-Entitätsprofil für die OIDC-Konfiguration.
ServiceNow Homepage	Die URL der Anmeldeseite, die für die Authentifizierung verwendet wird. Dieses Feld wird automatisch auf Ihre Instanz-URL festgelegt. Das Format der URL ist: https://yourinstance.service-now.com/navpage.do
Weiterleitung für externe Abmeldung	Die URL, an die die Integration Anwender nach der Abmeldung weiterleitet. Normalerweise das Portal, das für SSO verwendet wird. Dieses Feld wird automatisch auf festgelegt External_logout_complete.do Beispiel: https://yourinstance.service-now.com/external_logout_complete.do
Als Anmeldeoption anzeigen	Option zum Anzeigen des OIDC-IdP als Anmeldeoption auf der Anmeldeseite. Die Anmeldeoption wird als angezeigt **Melden Sie sich beim Identitätsanbieter an** Schaltfläche.
SSO-Bezeichnung	Bezeichnung des OIDC-IdP, der auf der Anmeldeseite angezeigt wird. Dieses Feld wird nur angezeigt, wenn **Als Anmeldeoption anzeigen** Ist aktiviert.
Logo-URL	Öffentlich verfügbare URL, die das Logo des OIDC-IdP-Anbieters enthält. Dieses Feld wird nur angezeigt, wenn **Als Anmeldeoption anzeigen** Ist aktiviert.

4. **Wahlweise:** Aktivieren Sie die automatische Anwenderbereitstellung auf der Registerkarte Anwenderbereitstellung>Registerkarte Anwenderbereitstellung.

(Optional) Sie können die automatische Anwenderbereitstellung während der Anwenderanmeldung aktivieren. Wenn die automatische Anwenderbereitstellung aktiviert ist, wird automatisch ein Anwenderdatensatz in der ServiceNow-Instanz erstellt, wenn dieser Anwenderdatensatz nicht vorhanden ist.

Felder „Anwenderbereitstellung“

Eigenschaft	Beschreibung
Anwender automatisch bereitstellen	Option zum Aktivieren der automatischen Anwenderbereitstellung. Diese Eigenschaft erstellt einen Anwender in der Instanzanwendertabelle (sys_user), wenn der Anwender IdP beendet, aber nicht in der Anwendertabelle vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Bereitstellen mit	Datenquelle, die für die Transformation verwendet werden soll ID-Token , Anwenderinformationen Endpunkt, oder Sowohl ID-Token als auch Anwenderinformationen An einen ServiceNow-Anwender. Verwenden Sie die Suchliste, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Tabellenzuordnung für Transformationen zu konfigurieren.
Datenquelle bereitstellen	ID-Token-Datenquelle, die für die Anwenderbereitstellung verwendet wird.
Datenquelle von Anwenderinformationen	Die Endpunktdatenquelle für Anwenderinformationen, die für die Anwenderbereitstellung verwendet wird. Dieses Feld wird angezeigt, wenn Anwenderinformationen Oder Sowohl ID-Token als auch Anwenderinformationen Sind für ausgewählt **Stellen Sie mithilfe von bereit** Feld.
Anwender bei der nächsten Anmeldung aktualisieren	Option zum Aktivieren der Anwenderaktualisierung während der nächsten Anmeldung.
Anwenderintervallzeit aktualisieren (Sekunden)	Mindestzeitintervall in Sekunden zum Aktualisieren eines Anwenderdatensatzes zwischen nachfolgenden Anmeldungen. Dieses Feld wird automatisch auf 3.600 Sekunden festgelegt. Beispiel: Nachdem sich ein Anwender angemeldet hat, wird der Anwenderdatensatz nach 3.600 Sekunden bis zur nächsten Anmeldung aktualisiert. Dieses Feld ist nur verfügbar, wenn **Aktualisieren Sie den Anwender bei der nächsten Anmeldung** Feld ist aktiviert.
Auf bereitgestellte Anwender angewendete Anwenderrollen	Liste der Rollen, die auf die neu bereitgestellten Anwender angewendet werden.

5. Registerkarte „OIDC-Entität“
   Sie können die OIDC-Client-Konfiguration und den OIDC-Connect-Flow mithilfe des Entitätsdatensatzes anzeigen und ändern.
6. Registerkarte „OIDC-Provider-Konfiguration“
   Sie können die bekannte Konfigurations-URL der Validierung des OIDC-IdP- oder ID-Token-Anspruchs anzeigen und ändern.
7. **Wahlweise:** Registerkarte „Erweitert“

   (Optional) Skripts, die während der einmaligen Anmeldung und Abmeldung ausgeführt werden.

   Erweiterte Felder

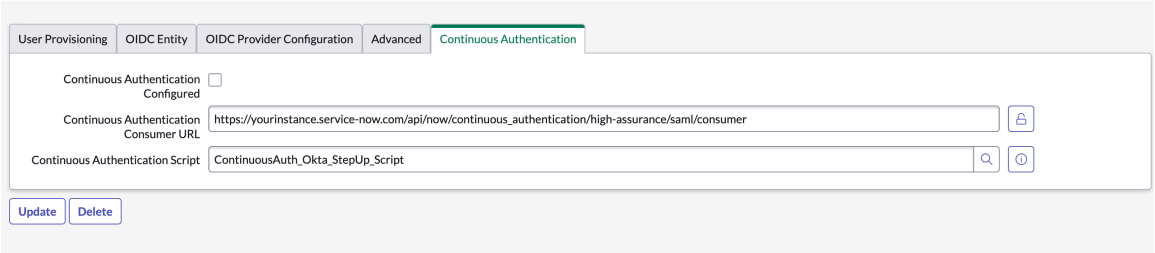
Eigenschaft	Beschreibung
Single Sign-on-Skript	Skript, das während der Single Sign-on ausgeführt wird. Dieses Feld wird automatisch auf festgelegt MultiSSO_OIDC_custom .
Abmeldeskript	Skript, das ausgeführt wird, nachdem sich der Anwender abgemeldet hat. Dieses Feld wird automatisch auf festgelegt MultiSSO_OIDC_logout_custom .

8. **Wahlweise:** Konfigurieren Sie auf der Registerkarte kontinuierliche Authentifizierung die folgenden Felder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die Registerkarte kontinuierliche Authentifizierung wird nur angezeigt, wenn Sie installieren **Zero Trust: Kontinuierliche Authentifizierung** (`Com.snc.Zero_Trust_Continuous_authentication`) Plugin, das eine Lizenz erfordert.
- Wenn Sie die Richtlinie für die kontinuierliche Authentifizierung verwenden, um den Zugriff auf die Tabelle oder Datenklasse zu schützen, finden Sie weitere Informationen unter Kontinuierliche Authentifizierung (CA).



Kontinuierliche Authentifizierung

Feld	Beschreibung
Kontinuierliche Authentifizierung konfiguriert	Aktivieren Sie das Kontrollkästchen, um die Konfiguration aktiv zu machen.
Verbraucher-URL für kontinuierliche Authentifizierung	Geben Sie die Verbraucher-URL vom Identitätsanbieter an.
Skript für kontinuierliche Authentifizierung	(Optional) Wählen Sie das Suchsymbol aus, um das von der Plattform bereitgestellte Skript auszuwählen. In dieser Konfiguration für OIDC Okta: **ContinuousAuth_Okta_StepUp_Script**

9. **Wahlweise:** Konfigurieren Sie auf der Registerkarte eSignature-Genehmigung die eSignature für den OIDC-IDP.

Hinweis: Die Registerkarte eSignature-Genehmigung wird nur angezeigt, wenn Sie installieren **Genehmigung mit E-Signatur** Plugin (com.Glide.e_Signature_Approvals).

E-Signatur-Genehmigungsfelder

Eigenschaft	Beschreibung
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Wenn Sie eine anwenderdefinierte Methode zur Verarbeitung der OIDC-Authentifizierung für eSignature verwenden, können Sie Ihre eigene Verbraucher-URL einrichten. Wenn Sie beispielsweise Multi-Provider-SSO verwenden, müssen Sie diese Eigenschaft nicht verwenden. Dieses Format der URL ist `https://yourinstance.service-now.com/consumer.do`
Breite des Popup-Dialogfelds für Authentifizierung	Breite des Popup-Dialogfelds für die Authentifizierung. Dieses Feld wird automatisch auf festgelegt `800` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Höhe des Popup-Dialogfelds für Authentifizierung	Höhe des Popup-Dialogfelds für die Authentifizierung. Dieses Feld wird automatisch auf festgelegt 900 .

10. **Wahlweise:** Navigieren Sie zur Anmeldeseite der Instanz, um sicherzustellen, dass IdP als Anmeldeoption angezeigt wird.
Die URL muss das folgende Format haben: https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP

> **Hinweis:** Wenn Sie aktiviert haben **Als Anmeldeoption ausgewählt** , Sie können zur Anmelde-URL der Instanz wechseln.

Facebook-basiertes Single Sign-on (SSO) verwenden

Melden Sie sich bei an ServiceNow-Instanz mithilfe von Facebook Anmeldeinformationen im Facebook-basierten SSO.

Vorbereitungen

Das Facebook-basierte SSO wird mit Ihrem geliefert ServiceNow Instanz.

Sie können die Konfigurationen des Identitätsanbieters (Identity Provider, IDP) für definieren **OIDC_Facebook** IDP als Ihr **Identitätsanbieter** . Weitere Informationen zu IDP-Konfigurationen finden Sie unter Facebook-basiertes Single Sign-on (SSO) konfigurieren.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Wählen Sie Aus **OIDC_Facebook** .
3. Geben Sie auf der Seite „OIDC_Facebook“ die folgenden Felder an:

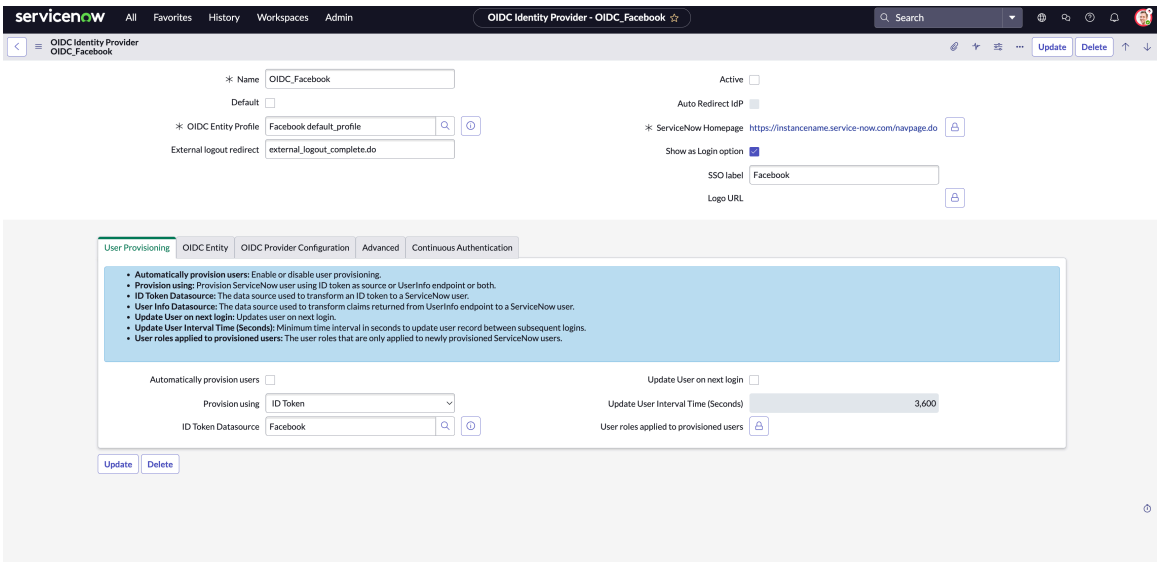
> **Hinweis:**
> - Die meisten Felder werden bei Verwendung des Standard-IdP automatisch ausgefüllt.
> - Details von ServiceNow Homepage muss angegeben werden.
> - Anwenderbezogene Details wie Client-ID und geheimer Client-Schlüssel von Facebook Muss innerhalb des IdP angegeben werden.

OIDC_Facebook – Details zum Identitätsanbieter

Feld	Beschreibung
Name	Name des OIDC-IdP-Datensatzes. Geben Sie Ein OIDC_Facebook .
Standard	Option zum Festlegen der OIDC-IdP-Konfiguration als Standard.
OIDC-Entitätsprofil	OAuth-Entitätsprofil für die OIDC-Konfiguration. Geben Sie Ein Facebook default_Profile .
Weiterleitung für externe Abmeldung	Die URL, an die die Integration Anwender nach der Abmeldung weiterleitet. Normalerweise ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	diese URL das Portal, das für SSO verwendet wird. Dieses Feld wird automatisch auf festgelegt **External_logout_complete.do** . Beispiel: https://<yourinstance>.service-now.com/external_logout_complete.do .
Aktiv	Option zum Aktivieren der OIDC-IdP-Konfiguration. **Hinweis:** Diese Option kann erst nach einer erfolgreichen Testverbindung auf „aktiv“ festgelegt werden.
Automatische IdP-Weiterleitung	Option zum Aktivieren der automatischen Weiterleitung der Anwender zur Anmeldeseite des Identitätsanbieters.
ServiceNow Homepage	Die URL der Anmeldeseite, die für die Authentifizierung verwendet wird. Dieses Feld wird automatisch auf Ihre Instanz-URL festgelegt. Das Format der URL ist https://<yourinstance>.service-now.com/navpage.do
Als Anmeldeoption anzeigen	Option zum Anzeigen des OIDC-IdP als Anmeldeoption auf der Anmeldeseite. In diesem Fall wird die Anmeldeoption als angezeigt **Melden Sie sich mit Facebook an** Schaltfläche.
SSO-Bezeichnung	Bezeichnung des OIDC-IdP, der auf der Anmeldeseite angezeigt wird. Dieses Feld wird nur angezeigt, wenn **Als Anmeldeoption anzeigen** Ist aktiviert.
Logo-URL	Öffentlich verfügbare URL, die das Logo des OIDC-IdP-Anbieters enthält. Dieses Feld wird nur angezeigt, wenn **Als Anmeldeoption anzeigen** Ist aktiviert.



4. **Wahlweise:** Öffnen Sie **Anwenderbereitstellung** Und füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie müssen die OIDC-bezogenen Informationen wie Client-ID und Client-Geheimnis Ihrer Anwender in konfigurieren Facebook.

Registerkarte „Anwenderbereitstellung“

Feld	Beschreibung
Anwender automatisch bereitstellen	Option zum Aktivieren der automatischen Anwenderbereitstellung. Diese Eigenschaft erstellt einen Anwender in der Tabelle „Instanzanwender“ [sys_user], wenn der Anwender im IdP vorhanden ist, aber nicht in der Anwendertabelle vorhanden ist. **Hinweis:** Sie können die automatische Anwenderbereitstellung während der Anwenderanmeldung aktivieren. Wenn die automatische Anwenderbereitstellung aktiviert ist, wird automatisch ein Anwenderdatensatz in erstellt ServiceNow Instanz, wenn dieser Anwenderdatensatz nicht vorhanden ist.
Bereitstellen mit	Die Datenquelle, die für die Transformation in einen verwendet werden soll ServiceNow Anwender. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Ein ID-Token** ○ **Anwenderinformationsendpunkt** ○ **Sowohl ID-Token als auch Anwenderinformationen** Verwenden Sie die Suchliste, um die vordefinierte Datenquellenvorlage auszuwählen, und öffnen Sie dann den Datensatz, um die Tabellenzuordnung für Transformationen zu konfigurieren.
Datenquelle bereitstellen	Die ID-Token-Datenquelle, die für die Anwenderbereitstellung verwendet wird.
Datenquelle von Anwenderinformationen	Die Endpunktdatenquelle für Anwenderinformationen, die für die Anwenderbereitstellung verwendet wird. Dieses Feld wird nur angezeigt, wenn **Anwenderinformationen** Oder **Sowohl ID-Token als auch Anwenderinformationen** Ist aus ausgewählt **Stellen Sie mithilfe von bereit** Feld.
Anwender bei der nächsten Anmeldung aktualisieren	Option zum Aktivieren von Anwenderaktualisierungen während der nächsten Anmeldung.
Anwenderintervallzeit aktualisieren (Sekunden)	Mindestzeitintervall (in Sekunden) zum Aktualisieren eines Anwenderdatensatzes zwischen nachfolgenden Anmeldungen. Dieses Feld wird automatisch auf 3600 Sekunden festgelegt. Beispiel: Nachdem sich ein Anwender angemeldet hat, wird der Anwenderdatensatz nach 3.600 Sekunden bis zur nächsten Anmeldung aktualisiert. Dieses Feld ist nur verfügbar, wenn **Aktualisieren Sie den Anwender bei der nächsten Anmeldung** Feld ist aktiviert.
Auf bereitgestellte Anwender angewendete Anwenderrollen	Liste der Rollen, die auf die neu bereitgestellten Anwender angewendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. In **OIDC-Entität** Auf der Registerkarte können Sie die OIDC-Client-Konfiguration und den OIDC-Connect-Flow mithilfe des Entitätsdatensatzes anzeigen und ändern.
   Weitere Informationen zur OIDC-basierten Konfiguration finden Sie unter Konfigurieren Sie einen OAuth-OIDC-Provider für die Annahme eines Drittpartei-Tokens
6. In **OIDC-Provider-Konfiguration** Registerkarte, zeigen Sie die bekannte Konfigurations-URL des OIDC-IdP an, und ändern Sie sie.
7. **Wahlweise:** Öffnen Sie **Erweitert** Und füllen Sie die Felder aus.

Registerkarte „Erweitert“

Eigenschaft	Beschreibung
Single Sign-on-Skript	Das Skript, das während des Single Sign-on ausgeführt wird.
Abmeldeskript	Das Skript, das ausgeführt wird, nachdem sich der Anwender abgemeldet hat.

Hinweis: Skripts werden während der einmaligen Anmeldung und Abmeldung ausgeführt.

8. Um die Konfiguration zu aktivieren und zu testen, klicken Sie auf **Aktiv** .
9. Klicken Sie auf, um den Datensatz zu aktualisieren **Aktualisieren** .
   Die Facebook-basierte Anmeldeoption wird im Anmeldeformular angezeigt.
10. Gehen Sie beim Anmelden im Anmeldeformular wie folgt vor:
    a. Wählen Sie aus Facebook Option.
    b. Um sich bei anzumelden ServiceNow Instanz, geben Sie an Facebook Anmeldeinformationen.

Facebook-basiertes Single Sign-on (SSO) konfigurieren

Konfigurieren Sie ein Facebook-basiertes SSO für Ihren ServiceNow Instanz.

Vorbereitungen

Haben eine gültige Client-ID, die als IdP von konfiguriert ist Facebook.

Aktivieren Sie die folgenden Eigenschaften:

- Aktivieren Sie SSO für mehrere Anbieter.
- Aktivieren Sie die Debug-Protokollierung für SSO-Integrationen mehrerer Anbieter.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Um eine neue zu erstellen Facebook Identitätsanbieter, klicken Sie auf **Neu** .
3. Klicken Sie Auf **OpenID Connect** .
4. Füllen Sie im Formular die Felder aus.

Formular „OpenID Connect – bekannte Konfiguration importieren“

Felder	Beschreibung
Name	Eindeutiger Name für die Konfiguration des OIDC-Identitätsanbieters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
Client-ID	Die Client-ID der Anwendung, die beim externen OIDC-Identitätsanbieter registriert ist.
Geheimer Clientschlüssel	Das geheime Clientgeheimnis der Anwendung, die beim externen OIDC-Identitätsanbieter registriert ist.
Bekannte Konfigurations-URL	Die URL, die Metadaten zum Drittpartei-OIDC-Identitätsanbieter enthält.

5. Klicken Sie auf **Importieren**.
   Der Facebook-basierte IdP wird erstellt.
6. Wählen Sie aus Facebook IDP.
7. In Facebook IDP: Gehen Sie wie folgt vor:
   a. Validieren Sie alle Felder wie **Name** , **OIDC-Entitätsprofil** , **Externe Abmeldeumleitung** , Und **ServiceNow-Homepage** .
   b. Geben Sie an **SSO-Bezeichnung** .
8. In **Anwenderbereitstellung** Geben Sie die Felder an, die Sie benötigen, um Anwender für bestimmte Anwenderbereitstellungen und -Rollen zu konfigurieren.

   Nur die Pflichtfelder sind erforderlich. Sie können die verbleibenden Felder je nach Bedarf angeben.
9. In **OIDC-Entität** Führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf die Entität.
   b. Legen Sie fest **Umleitungs-URL** Feld zu Ihrem Facebook Umleitungs-URL.
10. In **OAuth-Entitätsprofile** Führen Sie die folgenden Schritte aus:
    a. Klicken Sie in den Profildetails auf ein Profil.
    b. Wählen Sie einen Bereich aus, und überprüfen Sie die Details.
       Wählen Sie beispielsweise aus **Umfang-1**
11. In **Bereiche der OAuth-Entität** Klicken Sie auf die Registerkarte **Umfang-1** Verknüpfen Sie den Bereich, und fügen Sie ihn als hinzu E-Mail .
12. Um die Konfiguration zu speichern, klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie auf **Speichern** .
13. Um die Konfiguration als aktiv festzulegen, wählen Sie aus **Aktiv** .

Ergebnis
Anwender werden mit angezeigt Facebook SSO-Option im Anmeldeformular.

SAML

Die Security Assertion Markup Language (SAML) ist ein XML-basierter Standard für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen.

SAML tauscht Sicherheitsinformationen zwischen einem Identitätsanbieter (einem Ersteller von Assertions) und einem Service Provider (einem Verbraucher von Assertions) aus. SAML ist ein Produkt des technischen Komitees für OASIS Security Services. Bei korrekter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Implementierung ist SAML eine der sichersten verfügbaren Methoden für Single Sign-on (SSO).

Die SAML 2,0 Die Integration ermöglicht SSO, indem XML-Token mit einem externen Identitätsanbieter (Identity Provider, IdP) ausgetauscht werden. Der IdP authentifiziert den Anwender und übergibt ein NameID-Token an das System. Wenn das System einen Anwender mit einem übereinstimmenden NameID-Token findet (z. B. die E-Mail-Adresse), protokolliert die Instanz diesen Anwender in.

Wenn Sie das SAML 2,0-Plugin für die SSO-Authentifizierung verwenden, müssen Sie die Eigenschaft „Glide.ui.rotate_Sessions“ auf „falsch“ festlegen. Andernfalls wird die gemeinsame Nutzung von Sitzungsinformationen zwischen der Instanz und dem Identitätsanbieter beeinträchtigt. Benutzer mit der erhöhten Berechtigung Security_admin können auf diese Eigenschaft zugreifen.

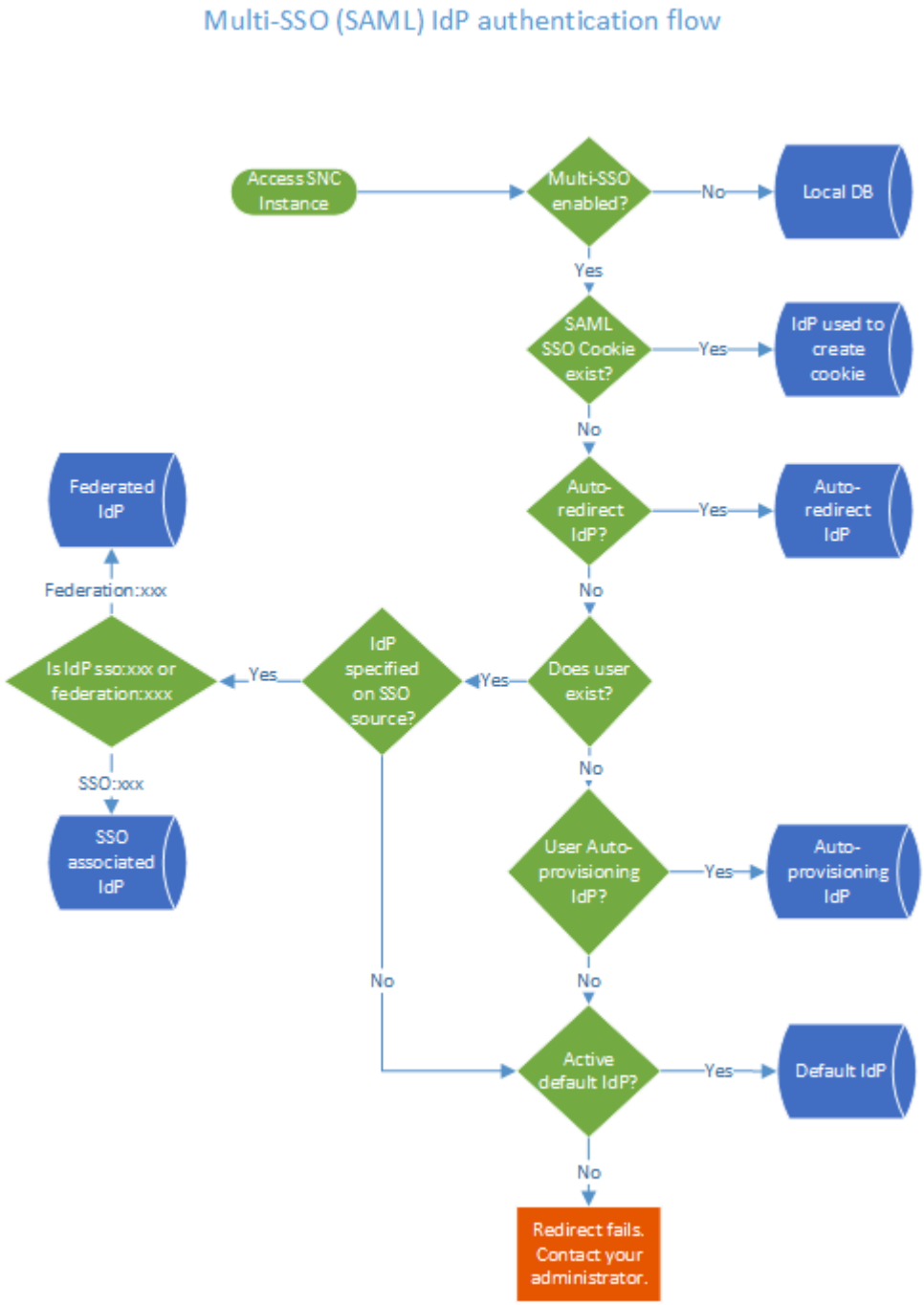
Hinweis: Kunden, die ein vorhandenes SAML 2,0-Integrations-Upgrade auf verwenden, werden empfohlen Multi-Provider-SSO-Plugin.

Multianbieter-SSO (SAML)-IdP-Authentifizierungs-Flow

Beschreibt die verschiedenen Entitäten, die einen Anwender über SAML Multi-SSO authentifizieren können.

Sie können dem Authentifizierungs-Flow folgen, um zu verstehen, wann eine Entität einen Anwender mit Multi-SSO authentifiziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Lokale Datenbank

Wenn Multi-SSO nicht aktiviert ist, wird die Authentifizierung an eine lokale DB weitergeleitet.

SAML-SSO-Cookie-IdP

Wenn ein SAML-SSO-Cookie vorhanden ist, authentifiziert der mit diesem Cookie angegebene IdP den Anwender.

IdP automatisch umleiten

Wenn die automatische IdP-Umleitung aktiviert ist, authentifiziert dieser IdP den Anwender.

Föderierter IdP

Wenn der Anwenderbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) weitergeleitet wird und der Anwender in der Anwendertabelle mit dem in festgelegten IdP vorhanden ist **SSO-Quelle** Feld als Verbund: xxx, dann authentifiziert der Verbund-IdP den Anwender.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugeordneter IdP

Wenn der Anwenderbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) weitergeleitet wird und der Anwender in der Anwendertabelle mit dem in festgelegten IdP vorhanden ist **SSO-Quelle** Feld als sso: xxx, dann authentifiziert der zugehörige IdP den Anwender.

IdP für automatische Bereitstellung

Wenn der Anwenderbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) weitergeleitet wird und der Anwender nicht in der Anwendertabelle vorhanden ist, die automatische Bereitstellung jedoch aktiviert ist, authentifiziert der IdP für die automatische Bereitstellung den Anwender.

Hinweis: Wenn mehr als ein IdP für die automatische Bereitstellung aktiviert ist, kann der Anwender den IdP für die automatische Bereitstellung auswählen, den er verwenden kann.

Standard-IdP

Wenn der Anwenderbrowser zum Anmeldebildschirm für die externe Autorisierung (login_locate_sso.do) weitergeleitet wird und der Anwender entweder:

- Ist in der Anwendertabelle nicht vorhanden, die automatische Bereitstellung ist nicht aktiviert, und es ist ein aktiver Standard-IdP vorhanden
- Ist in der Anwendertabelle vorhanden, im SSO-Quellanwender- oder Unternehmensdatensatz ist kein IdP angegeben, und es ist ein aktiver Standard-IdP vorhanden

Dann authentifiziert der Standard-IdP den Anwender.

Systemeigenschaften des Identitätsanbieters (Identity Provider, IdP)

Ein IdP bietet im Allgemeinen ein XML-Dokument mit seinen Authentifizierungs- und Abmeldemetadaten an.

Beispiel: SSOCircle Veröffentlicht ihre Metadaten Online.

Durchsuchen Sie die IdP-Metadaten, um diese Einträge zu finden:

- Die SingleSignOnService Element mit Bindung Attribut, das einen Wert von enthält HTTP-Umleitung . Die Standort Attribut listet die URL auf, die die Integration für den AuthnRequest-Service erfordert.
- Die SingleLogoutService Element mit Bindung Attribut, das einen Wert von enthält HTTP-Umleitung .Die Standort Attribut listet die URL auf, die die Integration für den SingleLogoutRequest-Service erfordert.

Hinweis: Die SAML 2,0-Integration unterstützt nur die Bindung an IdP-Services durch HTTP-Umleitung.

Zum Beispiel:

```
<SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location
="https://idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
```

```
<SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location
="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"ResponseLocation="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie die IdP-Aussteller-URL fest

Geben Sie die URL für die IDPs an, die das Sicherheitstoken ausstellen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Integration verifiziert, dass jede SAML-Antwort dieselbe URL enthält, die in dieser Systemeigenschaft aufgeführt ist wie die URL, die in aufgeführt ist *Aussteller* Element. Zum Beispiel:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
     ...
  </saml:Assertion></samlp:Response>
```

Prozedur

1. Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**an.
2. In der Eigenschaft *Die Identitätsanbieter-URL, die das SAML2-Sicherheitstoken mit Anwenderinformationen ausgibt.* Geben Sie die URL für Ihren IdP ein.

   Jede IdP-URL muss eindeutig sein. Standardmäßig enthält die Integration die URL zu SSOCircle. Weitere Informationen finden Sie unter http://idp.ssocircle.com .

Legen Sie die AuthnRequest-Service-URL fest

Legen Sie mithilfe der Metadaten des IdP die Anforderungsservice-URLs für den IdP der Integration fest.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. In der Eigenschaft *Die Basis-URL zum AuthnRequest-Service des Identitätsanbieters. Die AuthnRequest wird als SAMLRequest-Parameter an diese URL veröffentlicht* Geben Sie die URL für die HTTP-Umleitungsbindung ein, die von abgerufen wurde SingleSignOnService Element.
2. Aktivieren Sie das Kontrollkästchen neben *AuthnRequest signieren* Damit der Single Sign-on-Service des Identitätsanbieters eine signierte AuthnRequest erhält.
3. In der Eigenschaft *Wenn die SAML 2,0-Einzelanmeldung fehlschlägt, da die Sitzung nicht authentifiziert ist oder dies die erste Anmeldung ist, leiten Sie zu dieser URL um. Dies ist die Basis-URL, an die die erste SAML 2,0 AuthnRequest mit dem SAMLRequest-Parameter gesendet wird* Geben Sie die URL für die HTTP-Umleitungsbindung ein, die von abgerufen wurde SingleSignOnService Element.

   Standardmäßig enthält die Integration die URL zum SSOCircle-Service.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie die SingleLogoutRequest-Service-URL fest

Legen Sie die Anforderungsservice-URLs für den IdP der Integration fest, indem Sie die Metadaten des IdP verwenden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. In *Die Basis-URL zum SingleLogoutRequest-Service des Identitätsanbieters. LogoutRequest wird als SAMLRequest-Parameter an diese URL gesendet* Eigenschaft: Geben Sie die URL ein, die aus dem abgerufen wurde `SingleLogoutService` Element.
   LogoutRequest wird als SAMLRequest-Parameter an diese URL gesendet. Standardmäßig enthält die Integration die URL zum SSOCircle-Service.
2. In *URL zur Weiterleitung von Anwendern nach der Abmeldung, normalerweise zurück zu dem Portal, das SSO aktiviert hat (z. B. http://portal.companya.com/logout)* Eigenschaft: Geben Sie die URL ein, an die Anwender weitergeleitet werden sollen, nachdem sie sich erfolgreich abgemeldet haben.

   Wenn Ihr IdP eine formularbasierte Authentifizierung verwendet, geben Sie die URL für das Anmeldeformular Ihres IdP ein. Wenn Ihr IdP eine nicht formularbasierte Authentifizierungsmethode wie Kerberos verwendet, sollten Sie die URL auf eine statische Abmeldeseite festlegen. Auf diese Weise werden Anwender, die sich abmelden, nicht sofort zum IdP weitergeleitet und melden sich erneut an. Standardmäßig enthält die Integration die URL zur statischen UI-Seite `External_logout_complete.do` .

(Optional) Aktivieren Sie signierte Abmeldeanforderungen

Einige IDPs erfordern, dass der Service Provider Abmeldeanforderungen mit einem Zertifikat signiert.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihr IdP signierte Abmeldeanforderungen erfordert, verwenden Sie die Metadaten des IdP, um die folgenden Systemeigenschaften festzulegen.

Prozedur

1. In **Erweitert** Registerkarte in der Eigenschaft *LogoutRequest signieren. Legen Sie diese Eigenschaft auf „wahr“ fest, wenn der SingleLogoutRequest-Service des Identitätsanbieters signierte LogoutRequest erfordert* , Wählen Sie aus **Ja** Um anzugeben, dass Ihr IdP eine signierte Abmeldeanforderung erfordert, oder wählen Sie aus **Nein** Dient zur Verwendung von nicht signierten Abmeldeanforderungen.
2. Wenn Sie ausgewählt haben **Ja** Bis *LogoutRequest signieren* , Dann in *Die Protokollbindung für den SingleLogoutRequest-Service des Identitätsanbieters. (Wert kann entweder „urn:Oasis:names:tc:SAML:2,0:Bindings:HTTP-Redirect“ oder „urn:Oasis:names:tc:SAML:2,0:Bindings:HTTP-POST“ sein.)* Eigenschaft: Geben Sie einen der unterstützten Werte ein, die in aufgeführt sind `Bindung` Attribut aus `SingleLogoutService` Element.

   Standardmäßig verwendet die Integration eine HTTP-Umleitungsbindung.
3. Klicken Sie auf **Aktualisieren**.
4. Installieren Sie einen Service Provider (SP)-Schlüsselspeicher .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften des Service Providers (SP)

Diese Systemeigenschaften definieren, wie die Instanz mit dem IdP als Service Provider interagiert.

Befolgen Sie den sequenziellen Prozess, um IdP als Service Provider zu definieren.

Legen Sie die Instanz-URL für SAML fest

Legen Sie die instanzspezifischen URLs fest, damit der IdP Anwender authentifizieren kann.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. In der Eigenschaft *Die URL zur Service-Now-Instanz (normalerweise diese Instanz)* Geben Sie die URL (einschließlich Anmeldeseite) der Instanz ein, für die sich der IdP authentifiziert.
   Beispiel: https://yourinstance.service-now.com/navpage.do
2. In der Eigenschaft *Die Entitätsidentifizierung oder der Aussteller* Geben Sie die Basis-URL (ohne Anmeldeseite) der Instanz ein, für die sich der IdP authentifiziert.
   Beispiel: https://yourinstance.service-now.com/

Legen Sie die Zielgruppen-URL für SAML fest

Aktivieren Sie Ihre Instanz, um sicherzustellen, dass sie der beabsichtigte Empfänger einer SAML-Antwort ist, indem Sie die Eigenschaft „Zielgruppe“ verwenden.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Integration verifiziert, dass jede SAML-Antwort dieselbe URL enthält, die in dieser Systemeigenschaft aufgeführt ist wie die URL, die in aufgeführt ist *Zielgruppe* Element. Zum Beispiel:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
Destination="https://dloomac.service-now.com/navpage.do">
...
<saml:Conditions NotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
...
</samlp:Response>
```

Prozedur

1. Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**an.
2. In der Eigenschaft *Der Zielgruppen-URI, der das SAML2-Token akzeptiert. (Normalerweise ist dies Ihr Instanz-URI. Beispiel: https://<instance name>.service-now.com.)* Geben Sie die URL Ihrer Instanz ein.
   Beispiel: https://demoi2.service-now.com. Diese URL muss mit dem Wert von übereinstimmen *Zielgruppe* Element in der SAML-Antwort.
3. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie eine NameID-Richtlinie für SAML ein

Richten Sie eine NameID-Richtlinie für SAML ein. SAML 2,0 erfordert den IdP, um ein NameID-Token mit dem Service Provider auszutauschen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Für die SAML 2,0-Integration muss das NameID-Token einem bestimmten Feld in der Anwendertabelle zugeordnet werden. Die Integration verwendet den Wert des NameID-Tokens, um zu bestimmen, welchen Anwender der IdP authentifiziert.

Prozedur

1. Durchsuchen Sie die IdP-Metadaten, um zu finden `NameIDFormat` Element, das einen Wert von enthält `E-Mail-Adresse` .
   Der Wert dieses Elements ist das Standardformat, das die Integration verwendet.
2. Überprüfen Sie andere `NameIDFormat` Elemente, um zu bestimmen, ob Formate vorhanden sind, die anderen Feldern in der Anwendertabelle entsprechen.

Bestimmen Sie, welches Anwendertabellenfeld dem NameID-Token entspricht

Identitätsanbieter geben an, welches Format verwendet wird `NameID` Token hat.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Das Einrichten von SAML 2,0 erfordert die Auswahl eines Felds aus der Anwendertabelle, das dem Format von entspricht `NameID` Token. Normalerweise bieten IDPs die Möglichkeit, eine E-Mail-Adresse als zu verwenden `NameID` Token. Da die Anwendertabelle ein E-Mail-Feld enthält, ist dieses Feld eine logische Auswahl für die Verwendung als `NameID` Token. Dient zur Verwendung eines anderen Felds aus der Anwendertabelle als `NameID` Token: Überprüfen Sie zuerst, ob der IdP ein anbietet `NameID` Format, das dem Wert eines Anwendertabellenfelds entspricht. Dies erfordert möglicherweise das Hinzufügen des Felds zur Anwendertabelle.

Prozedur

1. Vergleichen Sie die verfügbaren Formate in den IdPs `NameIDFormat` Element für Felder in der Anwendertabelle.
2. Wählen Sie ein aus `NameID` Format, bei dem ein übereinstimmender Wert in der Anwendertabelle vorhanden ist.
3. In *Das Feld „Anwendertabelle“, das mit dem NameID-Element des Antragstellers in der SAMLResponse abgeglichen werden soll* Geben Sie den Namen des Felds Anwendertabelle ein, um nach übereinstimmenden Werten in zu suchen `NameID` Token.

   Standardmäßig verwendet die Integration das E-Mail-Feld.

Legen Sie die IdP-NameID-Richtlinie fest

Geben Sie an, welches Format der IdP für verwendet `NameID` Token.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Dieses Format wird als Teil der Metadaten des IdP aufgeführt.

Prozedur

1. In der Eigenschaft *Die NameID-Richtlinie, die für die Rückgabe der NameID des Antragstellers in der SAMLResponse verwendet werden soll. Ihr SAML-Identitätsanbieter muss dies unterstützen, indem die Richtlinie in seinen Metadaten deklariert wird. Der NameID-Wert wird verwendet, um mit dem angegebenen Feld in der Anwendertabelle abzugleichen, um den Anwender zu suchen.* , Geben Sie den Wert des ein `NameIDFormat` Element, das die Integration verwendet.

   Standardmäßig verwendet die Integration SSOCircle `NameIDFormat` Für E-Mail-Adressen.

2. Klicken Sie auf **Speichern**.

Werte im Feld Anwendertabelle für SAML

Stellen Sie sicher, dass das Anwendertabellenfeld der Integration entsprechende übereinstimmende Werte enthält.

Beispiel: Wenn die Integration das E-Mail-Feld als verwendet `NameID` Token: Stellen Sie sicher, dass die Instanz dieselbe E-Mail-Adresse wie der IdP auflistet. Die Integration kann keinen Anwender authentifizieren, der keinen übereinstimmenden Wert für hat `NameID` Token.

(Optional) Aktivieren Sie die Bereitstellung einer Authentifizierungskontextklasse für SAML

Sie können die Instanz aktivieren, um eine Anforderung der Authentifizierungskontextklasse an den IdP zu senden, die das bevorzugte Format der Authentifizierungsanforderung Ihrer Instanz enthält.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie die Erstellung einer AuthContextClass-Nachricht aktivieren, müssen Sie auch ein Referenzformat für die Authentifizierungskontextklasse angeben.

Hinweis: Einige IdPs erlauben es dem Service Provider nicht, die Authentifizierungskontextklasse festzulegen. Durch Deaktivieren dieser Einstellung kann der IdP die Authentifizierungskontextklasse auswählen.

Prozedur

1. Aus der Eigenschaft *Erstellen Sie eine AuthnContextClass-Anforderung in der AuthnRequest-Anweisung* , Wählen Sie aus **Ja** Um eine bestimmte Kontextklasse anzugeben, z. B. passwortgeschützter Transport, oder wählen Sie aus **Nein** Damit der IdP die am besten geeignete Kontextklasse auswählen kann.
2. Wenn Sie ausgewählt haben **Ja** Bis *Erstellen Sie eine AuthnContextClass-Anforderung in der AuthnRequest-Anweisung* , Dann in *Die AuthnContextClassRef-Methode, die wir in unserer SAML 2,0 AuthnRequest an den Identitätsanbieter anfordern* Eigenschaft: Geben Sie den URN der Kontextklasse ein, die Sie für die Authentifizierung verwenden möchten (siehe Tabelle).

AuthnContextClass-URN-Optionen

Authentifizierungstyp	Authentifizierungskontextklasse-URN
Formularbasierte Authentifizierung	URN:Oasis:names:tc:SAML:2,0:ac:classes:PasswordProtectedTransport

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Authentifizierungstyp	Authentifizierungskontextklasse-URN
Kerberos-basierte Authentifizierung	URN:Federation:Authentication:Windows

Standardmäßig verwendet die Integration eine passwortgeschützte Transportauthentifizierungsmethode.

3. Klicken Sie auf **Aktualisieren**.

(Optional) Legen Sie Schlüsselspeichereigenschaften für das Signieren von Abmeldeanforderungen für SAML fest

Legen Sie die Schlüsselspeichereigenschaften fest, damit die Integration Abmeldeanforderungen mithilfe Ihres signierten Servers und signierter CA-Zertifikate signieren kann.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. In der Eigenschaft *Der Alias des Schlüsseleintrags, der im SAML 2,0 SP-Schlüsselspeicher gespeichert ist und zum Signieren von SAML 2-Anforderungen verwendet wird* Geben Sie den Aliasnamen ein, den Sie für den SAML 2,0-Schlüsselspeicher erstellt haben.
   Standardmäßig sucht die Integration nach dem Alias *Saml2sp* .
2. In der Eigenschaft *Das Passwort des Schlüsseleintrags, der im SAML 2,0 SP-Schlüsselspeicher gespeichert ist und zum Signieren von SAML 2-Anforderungen verwendet wird* Geben Sie das Passwort für Ihren SAML 2,0-Schlüsselspeicher ein.
   Standardmäßig ist das Passwort mit dem Standardaliasnamen identisch.
3. Klicken Sie auf **Aktualisieren**.
4. Generieren Sie Ihre SP-Metadaten erneut.
   Weitere Informationen finden Sie unter SP-Metadaten .

Erstellen Sie einen Schlüsselspeicher des Service Providers für SAML

Erstellen Sie einen Java-Schlüsselspeicher mit den folgenden Elementen für Ihre Instanz, um Abmeldeanforderungen zu signieren.

Vorbereitungen
Erforderliche Rolle: administrator

Warum und wann dieser Vorgang ausgeführt wird

- Signiertes Serverzertifikat für die Instanz
- Signiertes CA-Zertifikat
- Öffentliches und privates Schlüsselpaar

Sie können ein eigenes signiertes Zertifikat bei einer privaten Zertifizierungsstelle erstellen oder eines bei einer öffentlichen Zertifizierungsstelle erwerben.

Die folgenden Schritte veranschaulichen, wie Sie eine neue Java Keytool-Schlüsselspeicherdatei generieren, eine Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) erstellen und Zertifikate importieren. Alle Stamm- oder Zwischenzertifikate müssen importiert werden, bevor das primäre Zertifikat für Ihre Domäne importiert wird. Geben Sie diese Befehle in eine Befehlszeilenschnittstelle ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Anweisungen sind nicht spezifisch für die Plattform und erfordern technische Kenntnisse über Sicherheitszertifikate. Der technische Support kann beim Erstellen der Zertifikate nicht helfen.

Prozedur

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Importieren Sie ein CA-Zertifikat einer Stamm- oder Zwischenzertifizierungsstelle in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. Importieren Sie ein signiertes primäres Zertifikat in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

Installieren Sie einen Service Provider-Schlüsselspeicher zum Signieren von SAML-Anforderungen

Führen Sie die folgenden Schritte aus, um den vorhandenen Beispiel-Schlüsselspeicher zu entfernen und Ihren eigenen Service Provider-Schlüsselspeicher zu installieren, der Ihr öffentliches und privates Schlüsselpaar enthält.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Erstellen Sie einen Schlüsselspeicher des Service Providers .
2. Navigieren zu **SAML 2 Single Sign-on** > **Zertifikat** oder **Multi-Provider** > **Administrator** > **x509-Zertifikat**an.
3. Klicken Sie Auf **SAML 2,0 Keystore_Key2048_SHA256** .
4. Klicken Sie auf **Verwalten Sie Anhänge** Link.
5. Aktivieren Sie das Kontrollkästchen Löschen neben *Saml2sp_key2048withsha256.jks* .
6. Klicken Sie Auf **Entfernen** .
7. Klicken Sie Auf **Wählen Sie Dateien** Und wählen Sie den Schlüsselspeicher aus, der Ihre signierten Zertifikate enthält.
8. Klicken Sie auf **Anhängen**.
9. Schließen Sie das Popup „Anhänge“.

Hinweis: Es wird empfohlen, einen anderen Namen für das neu angehängte Zertifikat anzugeben.

10. In *Schlüsselspeicher-Passwort* Geben Sie das Passwort ein, um auf den SAML 2-Alias zuzugreifen.
11. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) Erweiterte SAML-Eigenschaften

Mit den folgenden erweiterten Einstellungen können Sie die Sicherheit weiter erhöhen und die Integration debuggen.

Erweiterte Einstellungen

Navigieren zu **Alle** > **SAML 2 Single Sign-on** > **Eigenschaften**an.

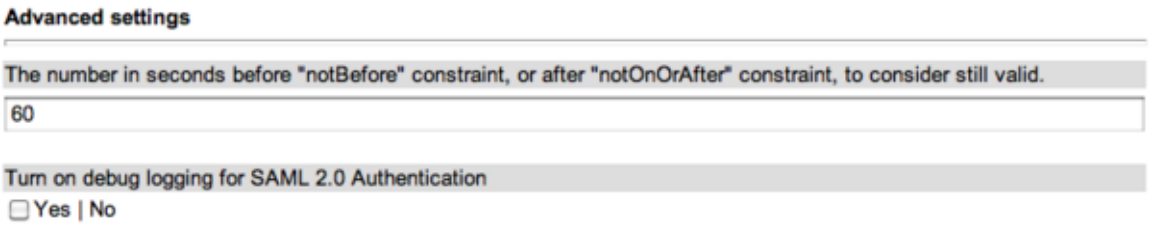


Tabelle mit erweiterten Systemeigenschaften

Eigenschaft	Beschreibung
Die Anzahl der Sekunden, die die Einschränkung „notBefore“ oder nach der Einschränkung „notOnOrAfter“ als gültig gelten sollen	Geben Sie die Anzahl der Sekunden ein, die der hinzugefügt werden soll *Nicht vorher* Und *Nicht OnOrAfter* Einschränkungen zur Berücksichtigung von Zeitunterschieden zwischen IdP-Uhr und SP-Uhr. Diese Einschränkungen verhindern Wiedergabeangriffe, indem Anforderungen abgelehnt werden, die nicht innerhalb des angegebenen Zeitrahmens gestellt werden. Wenn sich die IdP-Uhr und die SP-Uhr erheblich unterscheiden, kann die Netzwerklatenz dazu führen, dass die SAML-Anforderung nicht autorisiert wird. Diese Eigenschaft fügt einen Toleranzzeitraum hinzu, während dessen SAML-Anforderungen und -Antworten noch als gültig gelten.
Debug-Protokollierung für SAML 2.0-Authentifizierung aktivieren	Wählen Sie Aus **Ja** Zum Aktivieren zusätzlicher Protokollierungsinformationen für SAML 2,0-Ereignisse.

Installieren Sie das Zertifikat des Identitätsanbieters

Sie können ein PEM-Zertifikat in ein X.509-Zertifikatformular einfügen, damit der Identify Provider die Kommunikation mit dem Service Provider überprüfen kann.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

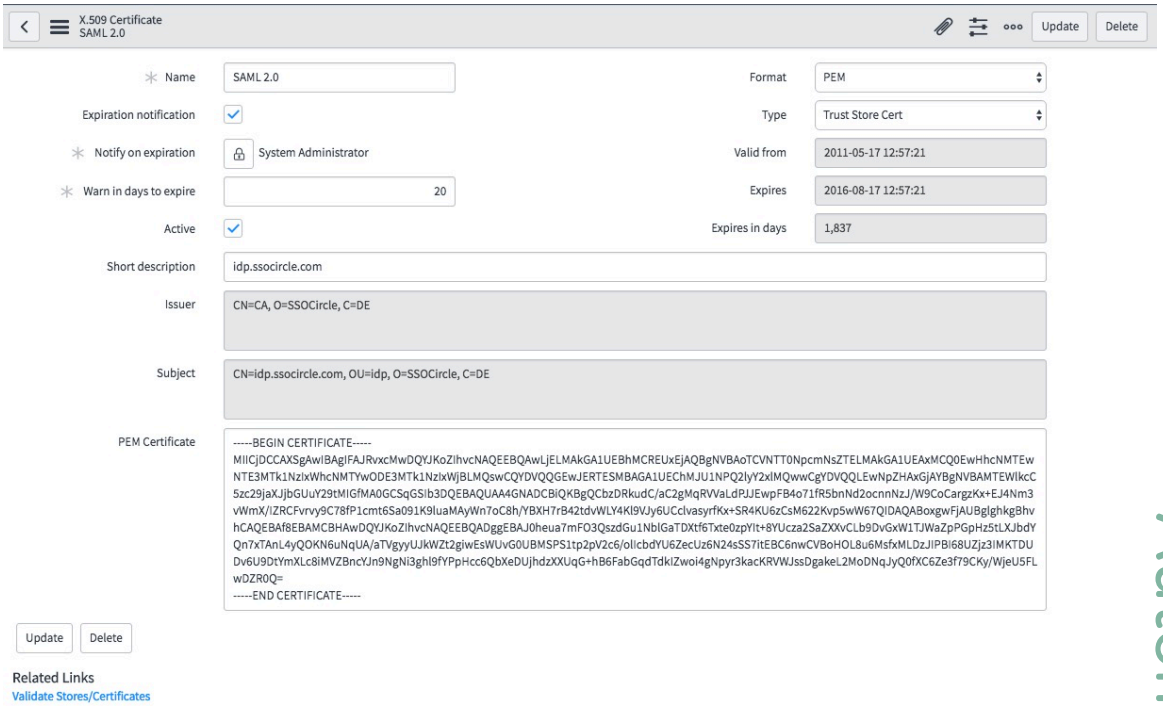
Das Zertifikat des IdP befindet sich in den Metadaten des IdP. Der IdP-Entwickler bestimmt beim Erstellen des lokalen IdP, wo sich die Zertifikatmetadaten befinden.

Hinweis: Zertifikate für Single Sign-on müssen immer im PEM-Format vorliegen, um mit SAML-Zertifikaten zu arbeiten.

Prozedur

1. Navigieren zu **Alle** > **SAML Single Sign-on** > **Zertifikat**an.
2. Füllen Sie die Formularfelder aus (siehe Tabelle).
3. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Die Integration signiert das Zertifikat derzeit in der Kommunikation zwischen der Instanz und dem IdP nicht.

Feld	Beschreibung
Name	Der Zertifikatname. Ändern Sie nicht *Name* Eintrag. Der Name des X.509-Zertifikats muss lauten *SAML 2,0* Damit die Integration sie verwenden kann. Diese Anforderung ist nur wahr, wenn Sie nicht verwenden Single Sign-on (SSO) für mehrere Anbieter.
Ablaufbenachrichtigung	Wählen Sie diese Option aus, um eine Benachrichtigung an die in ausgewählten Anwender zu senden **Benachrichtigen Sie bei Ablauf** Feld. Standardmäßig ist dies aktiviert.
Benachrichtigung bei Ablauf	Wählen Sie die Anwender aus, um die Benachrichtigung über den Ablauf des Zertifikats zu überarbeiten. Wenn keine Anwender ausgewählt sind, wird standardmäßig der angemeldete Anwender zusammen mit den letzten beiden angemeldeten Anwendern mit der Administratorrolle hinzugefügt.
Tage vor Ablauf benachrichtigen	Die Anzahl der Tage vor Ablauf, die die Instanz die Benachrichtigung sendet. Geben Sie einen Wert von mindestens 20 ein. Für Instanzen, die auf Istanbul und spätere Releases aktualisiert wurden, ist dieser Wert auf 20 festgelegt, es sei denn, ein größerer Wert ist angegeben.
Aktiv	Ein Kontrollkästchen, das angibt, dass dieses Zertifikat aktiv ist.
Format	Das Format des Zertifikats. SAML verwendet das PEM-Format.
Typ	Der Zertifikatcontainer. Die Instanz erkennt Zertifikate aus Truststores, Java-Schlüsselspeicher und PKCS#12-Schlüsselspeicher.
Gültig ab	Die Instanz fügt diesem Feld automatisch das Zertifikat „gültig ab“ hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Läuft ab	Die Instanz fügt diesem Feld automatisch das Ablaufdatum des Zertifikats hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Läuft in Tagen ab	Die berechnete Anzahl von Tagen bis zum Ablauf.
Kurzbeschreibung	Eine Beschreibung für das Zertifikat.
Problem	Die Instanz fügt diesem Feld automatisch den Zertifikataussteller hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
Betreff	Die Instanz fügt diesem Feld automatisch den Zertifikatbetreff hinzu. Hängen Sie das Zertifikat an den X.509-Zertifikatdatensatz an, um dieses Feld auszufüllen.
PEM-Zertifikat	Geben Sie den Wert des X509-Zertifikats ein.

Nächste Maßnahme
Klicken Sie Auf **Validiert Speicher/Zertifikate** Zum Testen des Truststores und des Zertifikats.

Ersetzen Sie ein fehlendes Zertifikat für SAML

Wenn **Zertifikat** Das Modul zeigt eine leere Seite an. Der SAML 2,0-Zertifikatdatensatz wurde gelöscht. Sie können das fehlende Zertifikat ersetzen, indem Sie manuell einen Zertifikatdatensatz erstellen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Zertifikate**an.
2. Erstellen Sie einen neuen Datensatz mit `SAML 2,0` .

> **Wichtig:** Sie MÜSSEN diesen Namen verwenden. Diese Anforderung ist nur wahr, wenn Sie nicht verwenden Single Sign-on (SSO) für mehrere Anbieter.

3. Klicken **SAML 2 Single Sign-on** > **Zertifikat**an.
4. In *PEM-Zertifikat* Geben Sie den Wert des ein `ds: X509Zertifikat` Element aus den Metadaten Ihres IdP.
5. Klicken Sie auf **Speichern**.

Testen Sie die SAML-Integration

Testen Sie die SAML-Integration, nachdem Sie alle anderen Setup-Aufgaben abgeschlossen haben.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz als Anwender mit der Administratorrolle an.
2. Navigieren zu **SAML 2 Single Sign-on** > **Eigenschaften**an.
3. In der Eigenschaft *Aktivieren Sie die externe Authentifizierung* , Wählen Sie aus **Ja** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Zum Aktivieren der externen Authentifizierung müssen alle Anwender SAML 2,0 Single Sign-on verwenden. Wenn jemand versucht, in einem nicht authentifizierten Status auf die Anwendung zuzugreifen, sendet die Instanz automatisch eine Authentifizierungsanforderung an (IdP) und leitet den Anwender zur SAML-IdP-Authentifizierungsseite weiter.

4. Klicken Sie auf **Speichern**.
5. Melden Sie sich von der Instanz ab.
6. Navigieren Sie zur Instanz-URL.
   Wenn die Integration ordnungsgemäß funktioniert, sollte der IdP die Anmeldeinformationen des Anwenders anfordern.

Zugehörige Informationen

Multi-SSO (SAML 2,0) – Fehler und Korrekturen

Multi-SSO (SAML 2,0) – Fehler und Korrekturen

Eine Liste allgemeiner Fehler und zugehöriger Korrekturen für ein Multi-SSO-Setup und eine Konfiguration (SAML 2,0).

Fehler beim Multi-SSO-Setup (SAML 2,0)

Fehler in Instanzprotokollen	Verbindungs Testen	SAML-Eigenschaft	Diagnose	Beheben
NotNachher: <Do Jun 05 22:57:44 PDT 2014>.	Stellen Sie sicher, dass das IDP x509-Zertifikat vorhanden, gültig und aktiv ist.	N/V	Das aktuelle Zertifikat oder die SAML-Assertion ist abgelaufen.	• Synchronisieren Sie die SNC-Uhr mit der SAML-IdP-Serveruhr. • Aktualisieren Sie den SAML 2,0-Zertifikatdatensatz.
• SAML 2.0-Zertifikat wurde nicht gefunden. • Es wurde keine digitale Signatur gefunden, die in der ServiceNow-Instanz gespeichert ist.	Stellen Sie sicher, dass das IDP x509-Zertifikat vorhanden, gültig und aktiv ist	Die PEM-formatierte Zeichenfolge muss in das Feld PEM-Zertifikat eingegeben werden.	Das SAML-Zertifikat ist nicht vorhanden. Möglicherweise ist sie inaktiv.	Stellen Sie sicher, dass das richtige PEM-formatierte Zertifikat in die Instanz hochgeladen wird.
Zertifikate stimmen nicht überein. Erwartet: <certStr>, ist-Wert: <inboundCert>.	Stellen Sie sicher, dass das IDP x509-Zertifikat vorhanden,	N/V	Das in SNC verfügbare Zertifikat stimmt nicht mit dem Zertifikat in der Assertion überein. Ursachen sind:	Bestätigen Sie, dass die PEM-formatierte Zeichenfolge im SAML 2,0-Zertifikatdatensatz mit dem X509-Zertifikat in der SAMLResponse

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Multi-SSO-Setup (SAML 2,0) (Fortsetzung)

Fehler in Instanzprotokollen	Verbindungs Testen	SAML-Eigenschaft	Diagnose	Beheben
	gültig und aktiv ist.		• Das Zertifikat wird im IdP aktualisiert, aber nicht in der ServiceNow-Instanz. • Das Zertifikat hat das falsche Format.	für den Anwender-IdP übereinstimmt.
Fehler beim Überprüfen der Gültigkeit des Zertifikats.	Stellen Sie sicher, dass das IDP x509-Zertifikat vorhanden, gültig und aktiv ist	N/V	Das aktuelle Zertifikat ist möglicherweise abgelaufen.	Aktualisieren Sie den SAML 2,0-Zertifikatdatensatz.
Fehler beim Validieren des Signaturprofils.	Stellen Sie sicher, dass das IDP x509-Zertifikat vorhanden, gültig und aktiv ist.	N/V	Die Assertion kann mit einem anderen Zertifikat signiert werden.	Überprüfen Sie, ob der IdP dasselbe Zertifikat wie die SNC-Instanz hat.
InResponseTo-Attribut in SubjectConfirmationData stimmt nicht überein. Erwartet: <inResponseTo>, ist-Wert: <inResponseTo>.	Validierung der Antragsteller fehlgeschlagen.	N/V bestätigung	Dieser Fehler wird angezeigt, wenn eine der folgenden Situationen auftritt: • Der IdP gibt eine SAMLResponse für eine andere SAMLRequest zurück • Ein Anwender markiert die URL mit der SAMLRequest anstelle nur der Instanz-URL mit einem Lesezeichen • Wenn ein Nullwert erwartet wird, wird die Antwort möglicherweise an einen anderen Knoten gesendet,	Der IdP-Administrator muss bestätigen, dass die erwartete SAMLReponse zurückgegeben wird. Diese Situation kann ein Lastenausgleichsmodul- oder Infrastrukturproblem sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Multi-SSO-Setup (SAML 2,0) (Fortsetzung)

Fehler in Instanzprotokollen	Verbindungs Testen	SAML-Eigenschaft	Diagnose	Beheben
			wenn die Instanz mehrere Knoten hat.	
SessionIndex-Wert nicht gefunden: <message>...	SessionIndex ungültig.	N/V	Der SessionIndex ist in der SNC-Instanz erforderlich. Der IdP gibt ihn in der SAML-Antwort zurück, um sich erfolgreich zu authentifizieren.	Der IdP-Administrator muss bestätigen, dass der SessionIndex in der SAMLResponse definiert ist.
Es konnte kein gültiges SubjectConfirmation-Element gefunden werden.	Validierung der Antragsteller fehlgeschlagen.	N/V bestätigung	Bedingungen könnten aufgrund eines Fehlers im IdP fehlen. Der Statuscode in der Antwort enthält den Beantworter anstelle des erwarteten Erfolgs.	Überprüfen Sie SAMLResponse, um festzustellen, ob Bedingungen in der SAMLResponse enthalten sind. Die gültigen Bestätigungsdaten des Antragstellers können für die richtige Zielgruppe abgelaufen sein oder nicht.
Assertion-Zielgruppe stimmt nicht überein. Erwartet: <propAudience>, ist-Wert: <audienceUri>. oder Validierung von AudienceRestriction fehlgeschlagen. Keine übereinstimmende Zielgruppe gefunden.	Stellen Sie sicher, dass das Feld „Zielgruppen-URI“ richtig festgelegt ist	Der Zielgruppen-URI, der das SAML2-Token akzeptiert. (Normalerweise ist dies Ihr Instanz-URI. Beispiel: https://demo.service-now.com .)	Der konfigurierte Zielgruppen-URI der SNC-Instanz muss mit dem Wert im IdP übereinstimmen.	Suchen Sie <saml2:Audience> in der SAMLResponse in den Protokollen, und stellen Sie sicher, dass der Wert mit dem in der Instanz übereinstimmt.
Assertionsaussteller ist ungültig. Erwartet: <Wert in Instanz>, ist-Wert: <von IdP zurückgegebener Wert>	Assertionsaussteller ist ungültig.	Der Identitätsanbieter-URL, die das SAML2-Sicherheitstoken mit Anwenderinformationen ausgibt.	Die IdP-Entitäts-ID (Aussteller) stimmt nicht mit dem in der SNC-Instanz definierten Wert überein.	• Überprüfen Sie, ob IdP oder SP nicht ordnungsgemäß konfiguriert ist. • Bestätigen Sie, dass die SAML-Eigenschaft (die Identitätsanbieter-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Multi-SSO-Setup (SAML 2,0) (Fortsetzung)

Fehler in Instanzprotokollen	Verbindungs Testen	SAML-Eigenschaft	Diagnose	Beheben
				URL, die das SAML2-Sicherheitstoken mit Anwenderinformationen ausgibt) richtig festgelegt ist.
Betreff ist in der Zukunft gültig. Now: <now>, nicht vorstehend: <notBefore> oder Betreff ist abgelaufen. Now: <now>, nicht OnOrNachher: <notOnOrAfter>	Bestätigung der Antragstellervalidierung fehlgeschlagen.	Die Anzahl in Sekunden vor der notBefore-Einschränkung oder nach der notOnOrAfter-Einschränkung, die als noch gültig betrachtet werden soll.	Die IdP-Uhr wird nicht mit der SP-Uhr synchronisiert.	Aktualisieren Sie die SAML-Eigenschaft glide.authenticate.sso.saml2.clockskew auf einen größeren Wert. Der Standardwert ist 180 Sekunden. In einigen Fällen ist eine Einstellung von 300 oder höher erforderlich. Möglicherweise müssen Sie auch die Zeit auf Ihrem IdP-Server überprüfen.
Assertion ist in der Zukunft gültig, jetzt: <now>, nicht vor: <notBefore> oder Assertion ist abgelaufen, jetzt: <now>, notOnOrAfter: <notOnOrAfter>	Assertion ist ungültig.	Die Anzahl in Sekunden vor der notBefore-Einschränkung oder nach der notOnOrAfter-Einschränkung, die als noch gültig betrachtet werden soll.	IDP-Uhr ist nicht mit SP-Uhr synchronisiert	Aktualisieren Sie die SAML-Eigenschaft auf einen größeren Wert. Standard: 60 Sekunden. In einigen Fällen ist eine Einstellung von 300 oder höher erforderlich. Möglicherweise müssen Sie auch die Zeit auf Ihrem IdP-Server überprüfen.

Allgemeine Anmelde- und IdP-Fehler

Fehler oder Symptom	Diagnose	Beheben
Anmeldeanforderungen erzeugen eine Endlosschleife zwischen dem System und dem IdP, wenn hohe Sicherheit aktiv ist.	• Normalerweise ist der URL-Endpunkt eine Fehlerseite oder Abmeldeseite. • Logout_redirect.do erstellt diese Schleife möglicherweise, wenn Sie definieren	Legen Sie die Systemeigenschaft glide.authenticate.failed_redirect fest (oder erstellen), um fehlgeschlagene Authentifizierungsanforderungen an diese URL umzuleiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Anmelde- und IdP-Fehler (Fortsetzung)

Fehler oder Symptom	Diagnose	Beheben
	`glide.security.url.whitelist`Ohne Hinzufügen des IdP-Hostnamens zum Eigenschaftswert. **Hinweis:** Weitere Informationen zu dieser Eigenschaft finden Sie unter Prüfung der URL-Zulässigkeitsliste erzwingen [aktualisiert in Security Center 1,3, 1,5 und 2,0] In Instanzsicherheitshärtungseinstellungen.	
Das zur Authentifizierung des Anwenders oder der Anforderung verwendete Token wird mit dem Signaturalgorithmus http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 signiert, der nicht dem erwarteten Signaturalgorithmus http://www.w3.org/2000/09/xmldsig#rsa-sha1 entspricht.	Auf der Registerkarte Warnungskontext finden Sie Ereignisdetails.	Navigieren Sie zur Registerkarte Erweitert des Konfigurationsdialogfelds „Vertrauenswürdige Partei“, und überprüfen Sie, ob der Algorithmus auf SHA-1 und nicht auf SHA-256 festgelegt ist.
Die Fehlermeldung `URN:Oasis:names:tc:SAML:2,0:Status:Anforderer` `Person` Wird in Ihrer Systemprotokolltabelle (Syslog) angezeigt.	Wenn Ihr IdP (z. B. ADFS) mit dem Status antwortet `Oasis:names:tc:SAML:2,0:Status:Anforderer` `Person` , Bedeutet, dass der IdP die Anmeldung aufgrund eines Problems mit der an ihn gesendeten Anforderung abgelehnt hat. Leider enthält die vom IdP empfangene SAML-Antwort in den meisten Fällen keine weiteren Details zum Fehler.	Überprüfen Sie die an den IDP gesendete SAML-Anforderung, und arbeiten Sie mit Ihrem IDP-Administrator zusammen, um Ihre SAML-Einstellungen für die Instanz zu aktualisieren, um den Fehler zu vermeiden. Möglicherweise müssen Sie sich an Ihren IDP-Anbieter wenden, um den Grund für den Anmeldefehler zu verstehen.

SSO-Anmeldungen (Single Sign-on) umleiten

Wenn SSO aktiviert ist, können Sie Anwender zu bestimmten Seiten umleiten oder Anwender dazu weisen, sich lokal anzumelden.

Beispiel: Wenn ein Anwender versucht, zu zu zu wechseln `https://customerX.service-now.com` , Kann anstelle der standardmäßigen Anmeldeseite ein internes Unternehmensportal angezeigt werden. Oder wenn sich ein Anwender von einer Anwendung abmeldet, kann er vom Browser zu einer bestimmten internen Seite weitergeleitet werden. Sie können Umleitungseigenschaften innerhalb der Instanz festlegen, um sicherzustellen, dass Anwender eine SSO-Anmeldeseite anstatt die Standardanmeldeseite sehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die folgenden Eigenschaften erzwingen SSO nicht. Die Seite „login.do“ ist weiterhin zugänglich, und Anwender können sich beim System anmelden, wenn sie ein lokales Passwort festgelegt haben.

Umleitungseigenschaften

Wenn sich ein Anwender abmeldet oder ein fehlgeschlagener Versuch, sich mit SSO anzumelden, können Sie definieren, wohin der Anwender als Nächstes führt, z. B. eine Hauptportalseite oder einen Knowledge Base-artikel mit SSO-Anmeldeinformationen. Verwenden Sie die folgenden Eigenschaften, um die URLs anzugeben. Wenn eine dieser Eigenschaften in Ihrer Instanz nicht vorhanden ist, können Sie die Eigenschaft erstellen.

glide.authenticate.failed_requirement_redirect

URL zur Weiterleitung von Anwendern, wenn sie versuchen, auf eine private Seite zuzugreifen (z. B. um einen Incident anzuzeigen), und keine SSO-Anmeldeinformationen bereitstellen. Die Eigenschaft ist normalerweise auf das Anmeldeportal eines Kunden festgelegt (z. B. `http://portal.companya.com/`).

glide.authenticate.failed_redirect

URL zur Weiterleitung von Anwendern nach einem fehlgeschlagenen SSO-Versuch. Sie können zu einem öffentlichen wissensartikel umleiten, der den Fehler beschreibt und hilfreiche Links enthält (z. B. `http://portal.companya.com/error`).

glide.authenticate.external.logout_redirect

URL zur Weiterleitung von Anwendern nach der Abmeldung, normalerweise zurück zu dem Portal, das die Single Sign-on-Anmeldung aktiviert hat (z. B. `http://portal.companya.com/logout`).

glide.authentication.external.disable_local_login

Bei „wahr“ sind SSO-Anmeldeinformationen für die Hauptanmeldeseite erforderlich. Standardmäßig ist „falsch“. Diese Eigenschaft muss in Verbindung mit verwendet werden *`glide.authenticate.failed_requirement_redirect`*Eigenschaft.

Die folgende Tabelle zeigt die Beziehung zwischen den Rückgabewerten für den Installationsausgang, den Eigenschaften und dem erwarteten Verhalten.

Erzwingen der Anmeldung nur mit SSO

Rückgabewert	Eigenschaft	Verhalten
Failed_missing_Request	*`glide.authenticate.failed_requirement_redirect`*	Wenn dieser Wert zurückgeg gibt er an, dass die erforderlic Anmeldeinformationen in der vorhanden sind. Die Anmeldu fehl, und die Sitzung wird an Eigenschaft angegebene URL Dies ist normalerweise die UR Anbieter, bei dem die Anmeld und Anmeldeinformationen e
Failed_authentication	*`glide.authenticate.failed_redirect`*	Wenn dieser Wert zurückgeg gibt er an, dass die Authentifi angegebenen SSO-Anmeldein fehlgeschlagen ist, der Anwen vorhanden ist oder der Anwen ist. Die Anmeldung schlägt fe Sitzung wird an die in der Eig angegebene URL weitergeleit

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erzwingen der Anmeldung nur mit SSO (Fortsetzung)

Rückgabewert	Eigenschaft	Verhalten
		normalerweise die URL für d Anbieter, bei dem die Anmeld und Anmeldeinformationen e
< *Anwender_ID* >	N/V	Anmeldung autorisiert für den von < angegebenen Anwende *Anwender_ID* >. Dieser W stimmt mit dem Feldnamen ü der in der SSO-Eigenschaft d *glide.authenticate.h* Feldname der Instanz, der mit eingehenden Header abgeglic soll“)

Lokale Anmeldung wird eingeschränkt

Aus Sicherheitsgründen sollten Sie sich mehr als auf Umleitungseigenschaften verlassen, um die lokale Anmeldung zu verbieten. Wenn sich ein Anwender nie lokal anmelden sollte und immer von Ihrem internen Single Sign-on-System authentifiziert wird, sollte jedem Anwender, der in die Instanz importiert wird, ein zufälliges Passwort zugewiesen werden. Das zufällige Passwort wird am einfachsten zum Zeitpunkt des Anwenderimports festgelegt. Wenn die Anwenderdaten über einen Importsatz in Ihr System importiert werden, können Sie mit dem folgenden Code ein onBefore-Transformationsskript erstellen.

```
var r  = new Packages. java. util. Random ( ) ;

var str1  = Packages. java. lang. Long. toString (Packages. java. lang.
Math. abs (r. nextLong ( ) ) , 36 ) ; var str2  = Packages. java. lang.
Long. toString (Packages. java. lang. Math. abs (r. nextLong ( ) ) , 36
) ;

var newPass  = str1  + str2 ;

target. user_password = newPass ;

//password now set to a random string like this:
//qvm81zdrn7cwwylpvw94eebk
```

Klont eine Instanz mit einer SAML-Integration

Klont eine Instanz mit einer SAML-Integration. Bevor Sie eine Instanz klonen, die SAML 2,0 verwendet, behalten Sie die SAML SSO-bezogenen Einstellungen in der Zielinstanz bei, oder Sie können die Zielinstanz nicht zugänglich machen.

Vorbereitungen

Erforderliche Rolle: Administrator

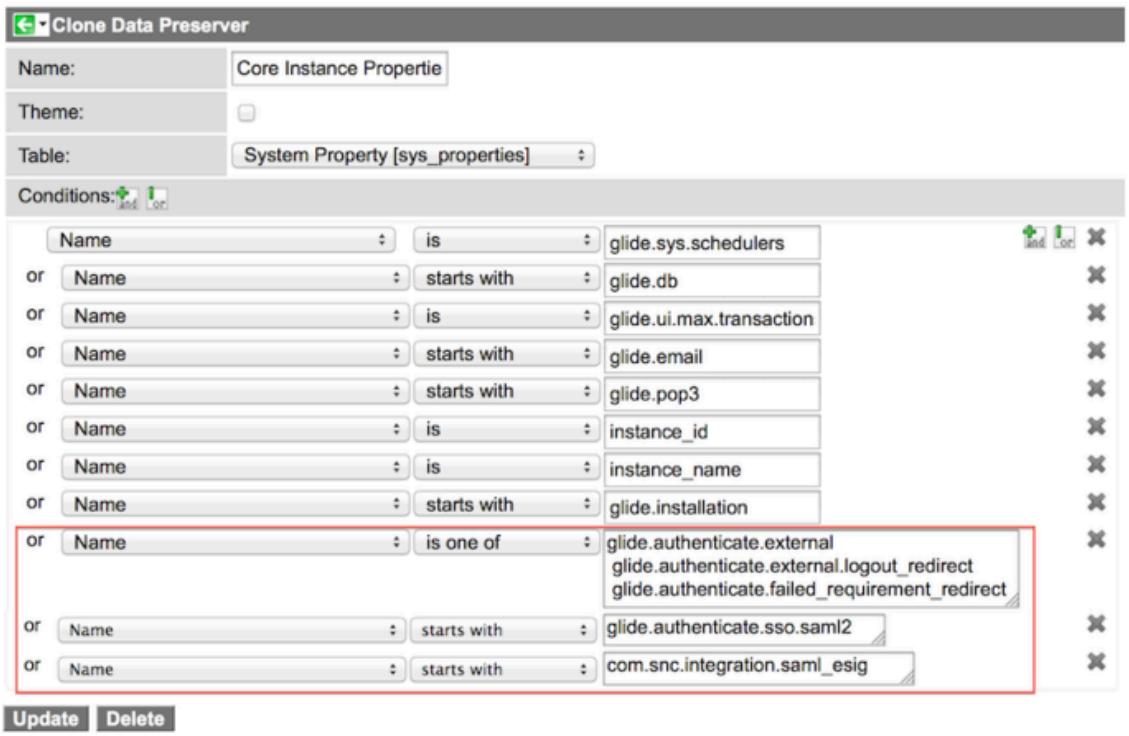
Prozedur

1. Navigieren Sie in der Quellinstanz zu **Systemklon** > **Daten erhalten** > **Kerninstanzeigenschaften**an.
2. Stellen Sie sicher, dass die folgenden SAML-SSO-bezogenen Eigenschaften mithilfe von Bedingungen beibehalten werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- glide.authenticate
- glide.security
- Glide.entry
- Glide.Skript
- glide.session
- Glide.saml2
- com.glide.communications
- com.snc.integration.saml_esig



Hinweis: Fügen Sie beim Erstellen des Klons Anhänge hinzu, damit Zertifikate an die Zielinstanz übertragen werden. Stellen Sie außerdem sicher, dass **Design** Das Kontrollkästchen ist deaktiviert, sodass diese Eigenschaften unabhängig davon beibehalten werden, ob Sie das Instanzdesign beibehalten.

3. Navigieren Sie in der Quellinstanz zu **Systemklon** > **Daten erhalten** Dient zum Beibehalten der SAML-Zertifikate für sys_certificate- und SAML-Anwender für sys_user im Zusammenhang mit SAML/SSO/Multi SSO.

   Wenn Sie sie benötigen, exportieren Sie sie in XML, und importieren Sie sie dann manuell im Ziel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

> **Warnung:** Versuchen Sie nicht, das SAML/SSO/Multi SSO-Setup von einem System auf ein anderes zu klonen. Die meisten Übertragungen von SAML/SSO- oder Multi-SSO-Einstellungen funktionieren NICHT, da sie im Identitätsanbieter konfiguriert werden müssen. Wenn Sie ein funktionierendes Setup überschreiben, kann sich die Zielinstanz nicht authentifizieren, sodass Ihre Zielinstanz nicht mehr zugänglich ist. Ändern Sie auch die sys_ID Ihres Multi-SSO-Anbieterdatensatzes nicht. Dadurch werden Ihre Anwender gezwungen, ihre Cookies zu löschen. Weitere Informationen zu Vorsichtsmaßnahmen zum Klonen finden Sie unter Prüfliste vor dem Klonen einer Instanz .

4. Schließen Sie die Multi-SSO-Tabellen sso_properties, Digest_properties und saml2_update1_properties aus.
5. Erstellen Sie die SAML-/SSO-/Multi-SSO-Datensätze manuell auf jeder Instanz unabhängig, und richten Sie die Datensätze auch in Ihrem Identitätsanbieter ein.
6. Stellen Sie sicher, dass Sie manuell einen LOKALEN Administratoraccount im Datensatz „sys_user“ (nicht in LDAP oder SAML) in der Zielinstanz und mit einer sys_ID erstellen, die in der Quellinstanz nicht vorhanden ist.
7. Klicken Sie auf **Aktualisieren**.

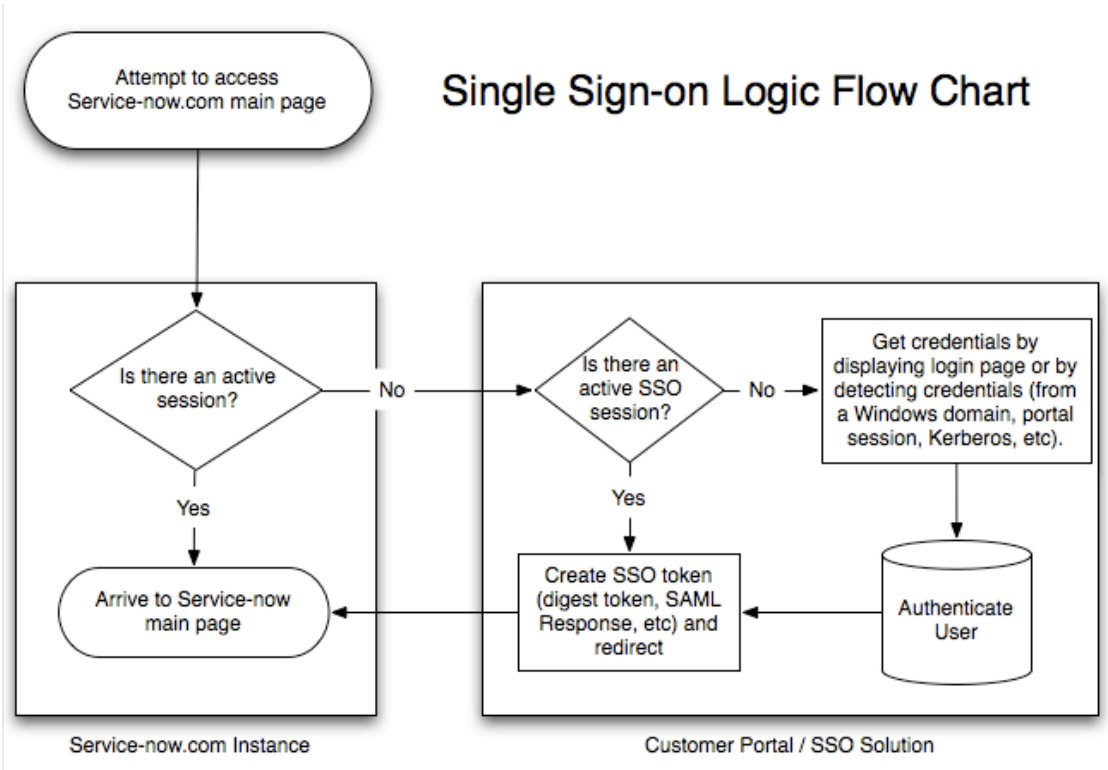
SAML 2,0-Konzepte

Machen Sie sich mit diesen SAML-Konzepten vertraut.

Typischer SAML-Prozess-Flow (Diagramm)

Ein typischer SSO-Logik-Flow umfasst die Suche nach einer aktiven Sitzung, die Überprüfung der Anmeldeinformationen des Anwenders und die Erstellung des erforderlichen Tokens.

SSO-Standard



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozess-Flow „Anmeldung“ (AuthnRequest)

SAML 2,0 gibt ein Webbrowser-SSO-Profil an, das den Austausch von Informationen zwischen einem Identity Provider (IdP), einem Service Provider (SP) und einem Prinzipal (Anwender) in einem Webbrowser umfasst.

Der Identitätsanbieter kann ein beliebiger SSO-Service sein, der SAML-Authentifizierungsservices anbietet (z. B. SSOCircle). Der Service Provider ist immer eine Instanz. Der Nachrichten-Flow beginnt mit einer Anforderung für eine gesicherte Ressource beim Service Provider.

Fordern Sie die Zielressource im SP an

Der Prinzipal fordert eine Zielressource beim Service Provider an:

https://instance.service-now.com/

Die Instanz überprüft die Anforderung, um festzustellen, ob die Parameter SAMLRequest und RelayState URL vorhanden sind. Wenn sie vorhanden sind, hat der Anwender bereits mit dem IdP validiert und kann die Schritte 2–6 überspringen.

AuthnRequest an Identitätsanbieter ausstellen

Die Instanz erstellt einen `AuthnRequest` Soll mithilfe von an den IdP gesendet werden `SAMLRequest` Wert. Die Instanz erstellt und sendet auch einen `RelayStatus` URL-Parameterwert.

Die `RelayStatus` Token ist ein undurchsichtiger Verweis auf Statusinformationen, die beim Service Provider verwaltet werden. Der Wert von `SAMLRequest` Parameter ist der Deflated- und base64-codierte Wert von `<samlp:AuthnRequest>` Element:

```
<samlp:AuthnRequest    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"    ID="identifier_1"
   Version="2.0"    IssueInstant="2004-12-05T09:21:59Z"
 AssertionConsumerServiceIndex="0"><saml:Issuer>https://
sp.example.com/SAML2</saml:Issuer><samlp:NameIDPolicy      AllowCreate="true"
 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/></samlp:AuthnRequest>
```

Die -Integration codiert dann die URL `<samlp:AuthnRequest>` Element und sendet es als `SAMLRequest` URL-Parameter.

Der SSO-Service verarbeitet `<samlp:AuthnRequest>` Element durch URL-Decodierung, base64-Decodierung und Aufblähung der Anforderung in dieser Reihenfolge. Anschließend wird eine Sicherheitsprüfung durchgeführt. Wenn der Anwender keinen gültigen Sicherheitskontext hat, identifiziert der IdP den Anwender, indem er zur Eingabe der Anmeldeinformationen auffordert. Wenn der Anwender bereits angemeldet ist, antwortet der IdP einfach mit `SAMLResponse` <tt>Und <tt>`RelayStatus` URL-Parameter (siehe Schritt 3).

Antworten Sie mit SAMLResponse und RelayState

Nach dem Sammeln der erforderlichen Anmeldeinformationen validiert der SSO-Service die Anforderung und antwortet mit einem Dokument, das ein XHTML-Formular enthält:

```
<formmethod="post"action="https://instance.service-now.com/navpage.do" ...><input
 type="hidden" name="SAMLResponse" value="response ..." /><input type="hidden"
 name="RelayState" value="token ..." />
   ...
   <input type="submit" value="Submit" /></form>
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Wert von RelayStatus Parameter stammt aus diesem Schritt. Der Wert von SAMLResponse Parameter ist die base64-Codierung des folgenden Elements <samlp:Response> Element:

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
Destination="https://dloomac.service-now.com/navpage.do"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer><samlp:Status
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><samlp:StatusCode
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode></samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="s23e536bfc51b8487d4d3299dec162d9c2e338823b"
IssueInstant="2010-04-29T23:21:51Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#">

...
    </Signature><saml:Subject><saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        NameQualifier="http://idp.ssocircle.com"
SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml:NameID><saml:Su
bjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData
          InResponseTo="90AA6073F01567BFB0DF194F596314E2"
          NotOnOrAfter="2010-04-29T23:31:51Z"
Recipient="https://dloomac.service-now.com/navpage.do" /
></saml:SubjectConfirmation></saml:Subject><saml:Conditions
NotBefore="2010-04-29T23:11:51Z"
NotOnOrAfter="2010-04-29T23:31:51Z"><saml:AudienceRestriction><saml:Audience>http
s://
dloomac.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
<saml:AuthnStatement AuthnInstant="2010-04-29T23:21:51Z"
SessionIndex="s2dbf89ab99001e0e8cdaed67266d9d4b21b968a04"><saml:AuthnContext><sa
ml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspo
rt</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement></saml:Asse
rtion></samlp:Response>
```

Validieren Sie SAMLResponse

Die SAMLResponse Der Wert ist base64 decodiert und aufbläht, um das XML-Dokument in Schritt 3 anzuzeigen. Das Anmeldeskript extrahiert den XML-Wert aus dem //Betreff/NameID Element und verwendet es, um einen vorhandenen Anwender in der Anwendertabelle zu suchen.

Das Anmeldeskript extrahiert auch die Sitzungs-ID aus //AuthnStatement/@SessionIndex Element und speichert es für LogoutRequest .

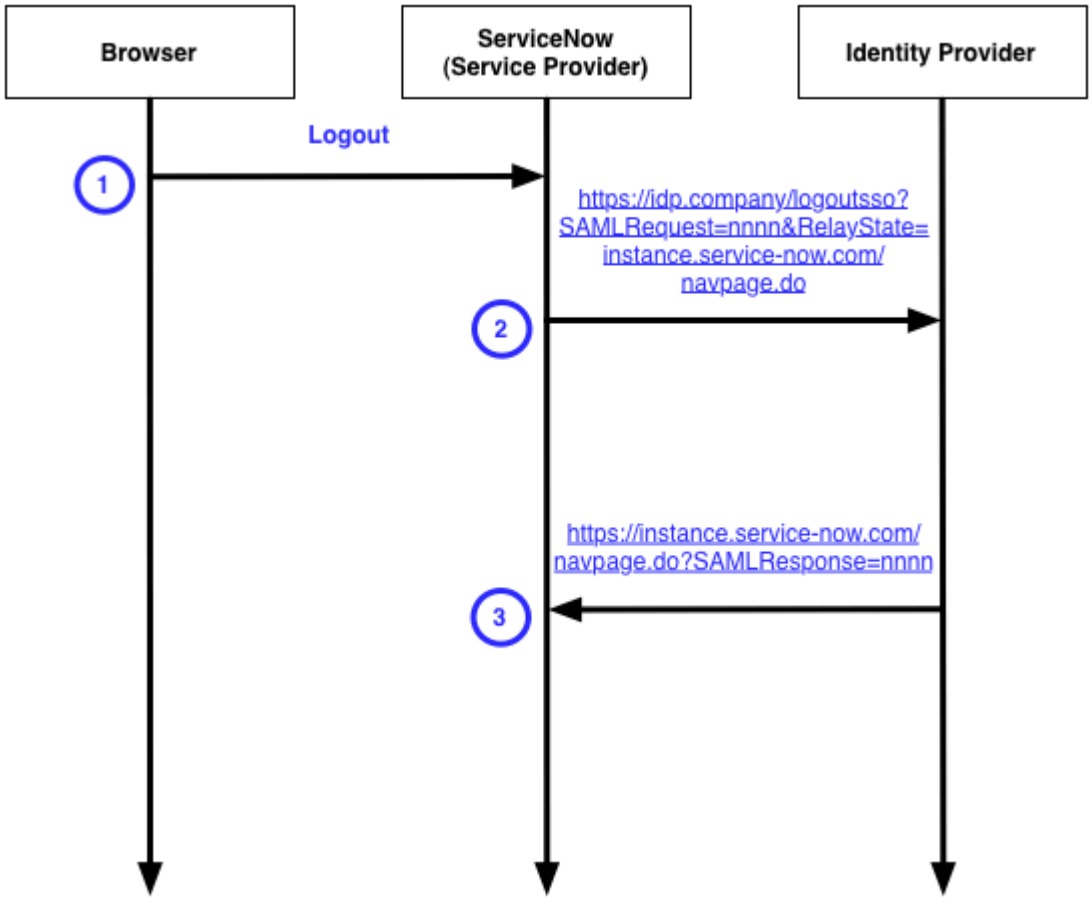
Prozess-Flow „Abmelden“ (LogoutRequest)

Während der Abmeldung gibt die Instanz SAML 2,0 aus *LogoutRequest* Serviceaufruf an den IdP.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Service meldet den Anwender ab und leitet ihn dann zur angegebenen Abmelde-URL zurück.

SAML 2-Abmeldung



Der Anwender klickt auf die Schaltfläche Abmelden

Der Anwender klickt auf **Melden Sie Sich Ab** Schaltfläche und die Instanz führt das Abmeldeskript aus.

LogoutRequest ausgestellt

Das Abmeldeskript erstellt ein SAML 2,0 `LogoutRequest` Und veröffentlicht sie im vorkonfigurierten SingleLogoutRequest SAML 2,0-Service im IdP. Der IdP entleert die Anforderung und codiert sie dann von base64. Ein Beispiel `LogoutRequest` Sieht wie folgt aus:

```
<saml2p:LogoutRequestxmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="21B78E9C6C8ECF16F01E4A0F15AB2D46"  IssueInstant="2010-04-28T21:36:11.230Z"
 Version="2.0"><saml2:Issuer
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://dloomac.service-now.com
 </saml2:Issuer><saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml2:NameID><saml2
p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104
 </saml2p:SessionIndex></saml2p:LogoutRequest>
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

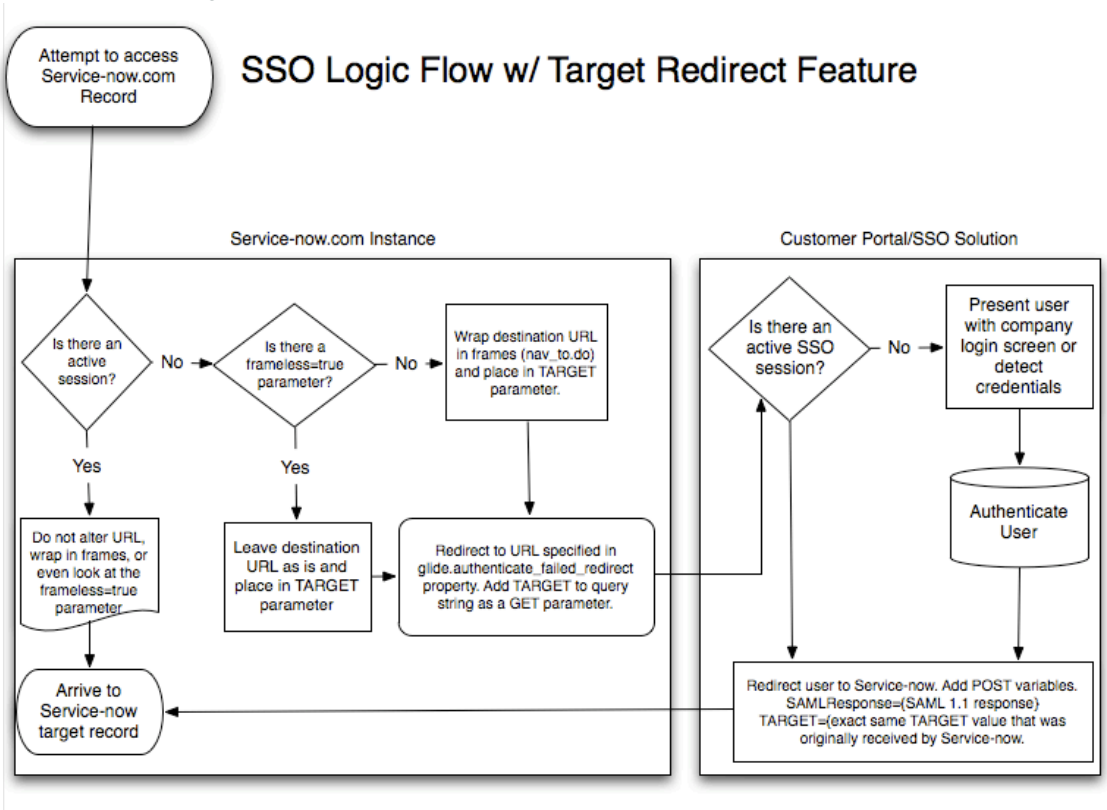
Anwender Meldet Sich Ab

Der Anwender meldet sich vom IdP ab. Der IdP leitet zurück zur Instanz, die wiederum zurück zum IdP leitet, da der Anwender nicht angemeldet ist.

URL-Informationen für einen SSO-Provider

Während einer Anmeldeabfrage, die aus einem URL-Link in die Instanz resultiert, die eine SSO-Sitzung erfordert, muss möglicherweise die verweisende URL an den SSO-Anbieter angegeben werden, damit die URL nach der Authentifizierung an die Instanz zurückgegeben und mit der richtigen Ressource verknüpft werden kann.

SSO-Zielumleitung



Die Rückgabewerte für den Installationsausgang wurden erweitert, um eine URL anstelle von oder zusätzlich zur durch die Eigenschaften definierten URL zu übergeben. Normalerweise geben Sie einen Anwendernamen oder einen vordefinierten Zeichenfolgenwert zurück, um die SSO-Sitzung zu steuern, zu autorisieren oder herauszufordern. Die folgenden Beispiele zeigen das erweiterte Verhalten der Übergabe einer URL.

```
return
 "failed_missing_requirement:%26amp;TARGET=https://
instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

Im obigen Beispiel wird die URL übergeben `https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345` An den SSO-Provider in Form eines URL-Parameters namens „ZIEL“.

Hinweis: Es wird davon ausgegangen, dass der SSO-Anbieter diese Informationen im ZIELPARAMETER verwendet, um zurück zur Instanz zu leiten, wenn die Anwenderanmeldeinformationen erfasst und die Authentifizierung übergeben wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Doppelpunkt : trennt die beiden Rückgabewerte, und ein codiertes & (%26amp;) verkettet die in der Eigenschaft definierte URL *glide.authenticate.failed_missing_requirement*Und der ZIELPARAMETER.

SAML 2,0-Konfiguration mit Multi-Provider-SSO

Sie können eine SAML 2,0 SSO-Konfiguration über die Multi-Provider-SSO-Funktion erstellen oder aktualisieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Neu in Jakarta Release, müssen Sie Ihre Konfiguration mit der Funktion „Verbindung testen“ validieren, bevor Sie Ihre IdP-Konfiguration aktivieren können. Sie können weiterhin die Funktionalität „Aktualisieren“ verwenden, um Ihre Konfigurationsdaten zu speichern, aber es handelt sich nicht um eine aktive Konfiguration ohne erfolgreiche Testverbindung.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Sie haben folgende Möglichkeiten.
   - Um eine Konfiguration zu aktualisieren, klicken Sie auf einen SSO-Konfigurationsdatensatz.
   - Klicken Sie auf, um eine neue Konfiguration zu erstellen **Neu** > **SAML**an.
3. Geben Sie die IdP-Informationen mit einer der folgenden Methoden ein.

Option	Bezeichnung
Mit einer Metadaten-Deskriptor-URL	Klicken Sie auf das Kontrollkästchen URL, und geben Sie die URL des verwendeten IdP ein.
XML-Datei des Metadatendeskriptors wird verwendet	Klicken Sie auf das Kontrollkästchen XML, und fügen Sie die XML-Daten ein, die aus dem verwendeten IdP generiert wurden.
Metadaten werden manuell eingegeben	Schließen Sie das Popup-Fenster, und geben Sie die Daten manuell in die Eigenschaftsfelder ein.

Hinweis: Alle Pflichtfelder müssen im Formular „Identitätsanbieter“ ausgefüllt werden.

Single Sign-on-Felder für mehrere Anbieter

Eigenschaft	Erforderlich	Beschreibung
Name	Ja	Geben Sie den Namen für den IdP ein. Dieser IdP ist die SYS-ID der automatischen Umleitung
Aktiv	Ja	„Aktiv“ muss auf „wahr“ festgelegt werden, damit der IdP für die Authentifizierung verwendet werden soll. **Hinweis:** Die Option zum Festlegen dieser Eigenschaft erfolgt erst nach einer erfolgreichen Testverbindung.
Standard	Nein	Der IdP für automatische Umleitung, früher als primärer IdP bekannt, leitet Anwender automatisch um, um auf die Basisinstanz-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

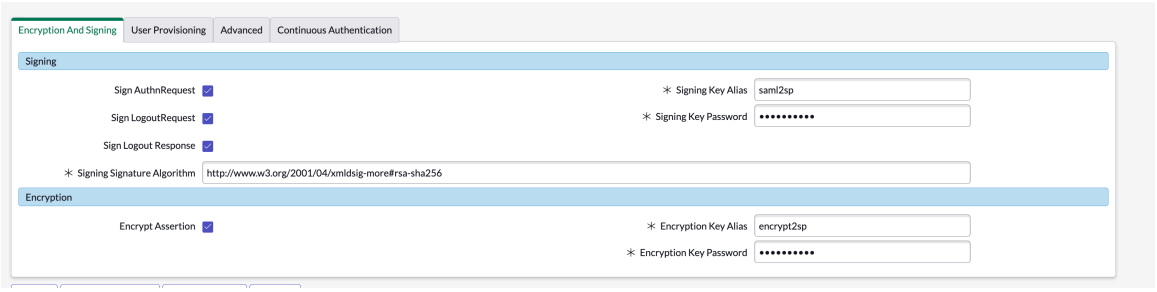
Eigenschaft	Erforderlich	Beschreibung
		URL zuzugreifen. Diese Eigenschaft legt diese IdP-Konfiguration als Standard fest.
Automatische IdP-Weiterleitung	Nein	Legt diese IdP-Konfiguration als IdP für automatische Umleitung fest. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Umleitung aktivieren, wird die aktiviert `glide_sso_id` Cookie-Updates mit dem neuen automatischen Umleitungs-IdP. Die `glide.authenticate.sso.update.idp.cookie`Die Systemeigenschaft, die automatisch aktiviert ist, steuert diese Funktion.
URL des Identitätsanbieters	Ja	Geben Sie die URL für Ihren IdP ein. Jede IdP-URL muss eindeutig sein.
AuthnRequest des Identitätsanbieters	Ja	Geben Sie die URL für die HTTP-Umleitungsbindung ein, die aus dem SingleSignOnService-Element abgerufen wurde.
SingleLogoutRequest des Identitätsanbieters	Nein	Geben Sie die URL ein, die aus dem SingleLogoutService-Element abgerufen wurde.
ServiceNow Homepage	Ja	Geben Sie die URL, einschließlich Anmeldeseite, der Instanz ein, für die sich der IdP authentifiziert. Beispiel: https://yourinstance.service-now.com/navpage.do
Entitäts-ID/Aussteller	Ja	Geben Sie die Basis-URL ohne Anmeldeseite ein. Der Instanz, für die sich der IdP authentifiziert. Beispiel: https://yourinstance.service-now.com/
Zielgruppen-URI	Ja	Geben Sie die Basis-URL ohne Anmeldeseite ein. Der Instanz, für die sich der IdP authentifiziert. Beispiel: https://yourinstance.service-now.com/
NameID-Richtlinie	Ja	Geben Sie den Wert des NameIDFormat-Elements ein, das die Integration verwendet.
Weiterleitung für externe Abmeldung	Nein	Geben Sie die URL ein, an die die Integration Anwender weiterleitet, nachdem sie sich abgemeldet haben.
Fehlerhafte Anforderungsumleitung	Nein	Geben Sie die URL für die Umleitung fehlgeschlagener Authentifizierungsanforderungen ein. Standardmäßig ist dies der URL-Endpunkt einer Fehlerseite oder Abmeldeseite, die im IdP konfiguriert ist. Sie können diesen Wert im Feld glide.authenticate.failed_requirement_redirect ausfüllen.
Client-Typ	Nein	Wählen Sie den Client-Typ basierend auf dem Typ Ihres Clients aus. Optionen: **Iframe Eingebettet** . **Hinweis:** Wenn das Feld „Client-Typ“ für Ihre Konfiguration erforderlich ist, können Sie das Formular bearbeiten und das Feld hinzufügen. Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

4. **Wahlweise:** Registerkarte „Verschlüsselung und Signatur“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Es wird empfohlen, eigene Zertifikate für die Verschlüsselung und Signierung zu verwenden.
- Die **FIPS-genehmigter Modus** Erfordert verschiedene Zertifikate für **Verschlüsselung** Und **Signieren**
- Achten Sie bei der Verwendung der Zertifikate darauf, die folgenden Systemeigenschaften mit der sys_ID der Zertifikate (x.509-Zertifikate) zu aktualisieren:
  - **Signieren** (glide.authenticate.sso.saml2.keystore)
  - **Verschlüsselung** (glide.authenticate.sso.saml2.encryption.keystore)
- Stellen Sie sicher, dass Sie den Schlüsselalias und das Schlüsselpasswort des aktualisieren **Signieren** Und **Verschlüsselung** Schlüsselspeicher im Identitätsanbieter-Datensatz und generieren die Metadaten (Auswählen **Generieren Sie Metadaten**).
- Laden Sie die in den generierten Metadaten (XML) vorhandenen Signier- und Verschlüsselungszertifikate zum Identitätsanbieter hoch.



Verschlüsselungs- und Signaturfelder

Eigenschaft	Beschreibung
Signaturschlüsselalias	Geben Sie den Signaturalias des in gespeicherten Schlüsseleintrags ein SAML 2,0 SP-Schlüsselspeicher .
Signaturschlüssel-Passwort	Geben Sie das Signaturpasswort des in gespeicherten Schlüsseleintrags ein SAML 2,0 SP-Schlüsselspeicher .
Verschlüsselungsschlüsselalias	Geben Sie den Verschlüsselungsalias des in gespeicherten Schlüsseleintrags ein SAML 2,0 SP-Schlüsselspeicher .
Passwort des Verschlüsselungsschlüssels	Geben Sie das Verschlüsselungspasswort des in gespeicherten Schlüsseleintrags ein SAML 2,0 SP-Schlüsselspeicher .
Assertion verschlüsseln	Aktivieren Sie das Kontrollkästchen, um die Assertion in der SAML-Antwort zu verschlüsseln. Die für den IDP generierten Metadaten bettet das x509-Zertifikat ein, das der IDP verwendet, um die Assertion in der von ihm generierten SAML-Antwort zu verschlüsseln.
Signaturalgorithmus für Signieren	Geben Sie die URL ein, die auf den SAML 2,0-Identitätsanbieter AuthnRequest-Verbraucher für eSignature-Authentifizierung verweist.
AuthnRequest signieren	Aktivieren Sie das Kontrollkästchen, um zu aktivieren, dass der IdP-Single Sign-on-Service eine signierte AuthnRequest erhält.
LogoutRequest signieren	Aktivieren Sie das Kontrollkästchen, um zu aktivieren, dass der IdP-Single-Sign-on-Service eine signierte LogoutRequest erhält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

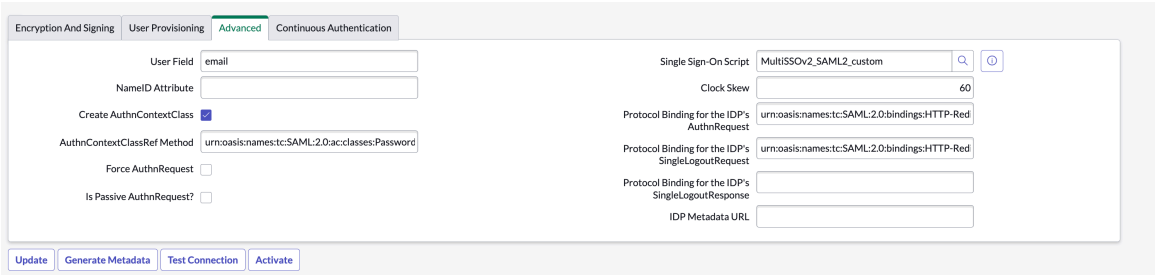
Eigenschaft	Beschreibung
Abmeldeantwort signieren	Aktivieren Sie das Kontrollkästchen, um zu aktivieren, dass der IdP-Single-Sign-on-Service eine signierte Abmeldeantwort erhält.

5. **Wahlweise:** Registerkarte „Anwenderbereitstellung“

Felder „Anwenderbereitstellung“

Eigenschaft	Beschreibung
Automatische Bereitstellung von Anwender	Aktivieren Sie die automatische Anwenderbereitstellung. Erstellt die Anwender, wenn der Anwender basierend auf den vom IdP bereitgestellten Informationen nicht in der Instanz-Anwendertabelle vorhanden ist.
Anwenderdatensatz bei jeder Anmeldung aktualisiere	Aktualisiert Anwenderinformationen in der Instanzanwendertabelle jedes Mal, wenn sich der Anwender mit SAML anmeldet, mit den Informationen im IdP.

6. **Wahlweise:** Registerkarte „Erweitert“



Erweiterte Felder

Eigenschaft	Beschreibung
Anwenderfeld	Geben Sie das Feld in der Anwendertabelle ein, das den Wert enthält, den der IdP zur Identifizierung des Anwenders benötigt. Dies ist eine eindeutige ID als Teil der Antwort. Zum Beispiel Anwendername, Mitarbeiter-ID usw. In der SYS-Anwendertabelle wird diese eindeutige ID mit den Anwenderdetails abgeglichen.
Attribut NameID	Lassen Sie dieses Feld leer, es sei denn, Sie konfigurieren eine neue NameID-Richtlinie. Wenn Sie eine neue Richtlinie konfigurieren, benötigt das System die Anwendertabelle, die es verwenden muss, um den Anwender zu identifizieren, der sich anmeldet. Das System stimmt das NameID-Token mit dem Namen dieses Anwendertabellenfelds hier ab.
AuthnContextClass erstellen	Aktivieren Sie das Kontrollkästchen, um eine bestimmte Kontextklasse anzugeben, z. B. passwortgeschützter Transport. Wenn das Kontrollkästchen deaktiviert ist, wählt der IdP die am besten geeignete Kontextklasse aus.
AuthnContextClassRef-Methode	Geben Sie den URN des Anmeldemechanismus ein, den der IdP zur Authentifizierung von Anwendern verwenden soll.
AuthnRequest erzwingen	Aktivieren Sie das Kontrollkästchen, um das Auftreten von AuthnRequests zu erzwingen.
Ist passive AuthnRequest	Aktivieren Sie das Kontrollkästchen, wenn AuthnRequest passiv ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

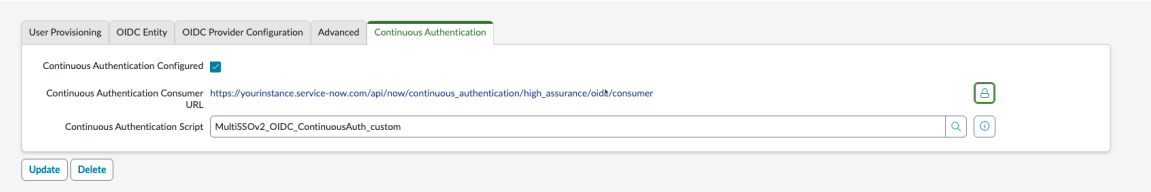
Eigenschaft	Beschreibung
Single Sign-on-Skript	Wählen Sie das Single Sign-on-Skript aus. Der Standardwert ist *MultiSSOV2_SAML2_custom* .
Abmeldeantwort signieren	Geben Sie die Details der Abmeldeantwort in dieses Feld ein.
Taktversatz	Geben Sie die Anzahl der Sekunden zwischen den beiden Attributen ein, aus denen die SAMLResponse-Nonce besteht. Der Standardwert ist 60. Eine gültige SAMLResponse muss zwischen liegen *Nicht vorher* Und *NotOnOrAfter* Datums-/Uhrzeitwerte. Siehe Beispiel für SAML 2-Antwort mit den Elementen SubjectConfirmation und SubjectConfirmationData und Beispiel für SAML 2-Antwort mit den Elementen AudienceRestrictions und Zielgruppe für eine Beispiel-SAMLResponse-Nachricht.
Protokollbindung für SingleLogoutReuqest des IDP	Geben Sie einen der unterstützten Werte ein, die im Bindungsattribut aus dem SingleLogoutService-Element aufgeführt sind.
Metadaten-URL, aus der IDP-Eigenschaften importiert werden	Die IdP-Eigenschaften werden aus dieser URL importiert. Wenn festgelegt, wird der automatische Import von SAML-Zertifikaten aus dem IdP aktiviert, wenn das vorherige Zertifikat abgelaufen ist. **Hinweis:** Wenn Sie ein Upgrade von SAML2 Update 1 auf Multi-Provider-SSO durchführen oder Ihre SSO-Verbindung manuell einrichten, wird die IdP-Metadaten-URL nicht automatisch ausgefüllt.
Anforderung	Eine eindeutige ID als Teil der Anforderung. Die ID kann Anwendername, Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl Umleitung als auch Post-Bindung werden für die Anforderung unterstützt. Die Option zum Festlegen dieses Felds wird erst nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter Testen Sie IdP-Verbindungen.
Antwort	Eine eindeutige ID als Teil der Antwort. Die ID kann Anwendername, Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl Umleitung als auch Post-Bindung werden für die Antwort unterstützt. Die Option zum Festlegen dieses Felds wird erst nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter Testen Sie IdP-Verbindungen.

7. **Wahlweise:** Konfigurieren Sie auf der Registerkarte kontinuierliche Authentifizierung die folgenden Felder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die Registerkarte kontinuierliche Authentifizierung wird nur angezeigt, wenn Sie installieren **Zero Trust: Kontinuierliche Authentifizierung** (`Com.snc.Zero_Trust_Continuous_authentication`) Plugin, das eine Lizenz erfordert.
- Wenn Sie die Richtlinie für die kontinuierliche Authentifizierung verwenden, um den Zugriff auf die Tabelle oder Datenklasse zu schützen, finden Sie weitere Informationen unter Kontinuierliche Authentifizierung (CA).



Kontinuierliche Authentifizierung

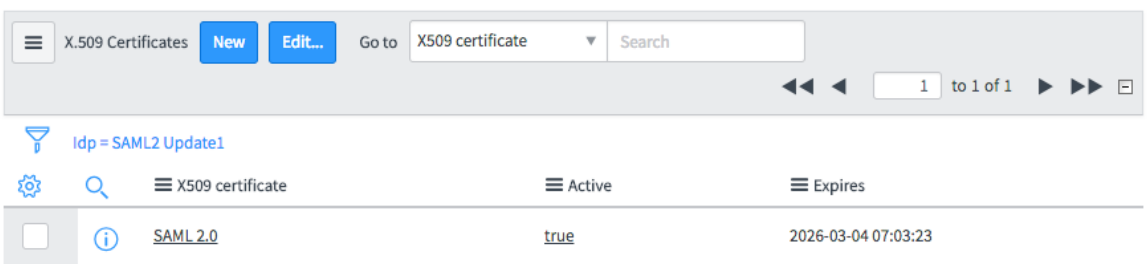
Feld	Beschreibung
Kontinuierliche Authentifizierung konfiguriert	Aktivieren Sie das Kontrollkästchen, um die Konfiguration aktiv zu machen.
Verbraucher-URL für kontinuierliche Authentifizierung	Geben Sie die Verbraucher-URL vom Identitätsanbieter an.
Skript für kontinuierliche Authentifizierung	(Optional) Wählen Sie das Suchsymbol aus, um das von der Plattform bereitgestellte Skript auszuwählen. In dieser Konfiguration für SAML: **MultiSSOv2_SAML2_ContinuousAuth_custom**

X.509-Zertifikate für SAML

Speichern und aktivieren Sie die erforderlichen IdP-Zertifikate für Ihre SAML-Konfiguration.

Die X.509-Zertifikate sind die IdP-Zertifikate, die eine SAML-Konfiguration verwendet. Nachdem Sie ein Zertifikat installiert haben, können Sie beliebig viele Zertifikate hinzufügen. Wenn mehrere Zertifikate vorhanden sind, verwendet das System das erste gefundene aktive Zertifikat. Wenn Sie die URL für festlegen **Metadaten-URL, aus der IDP-Eigenschaften importiert werden, Feld** , Fragt das System den IdP automatisch nach einem aktuellen, gültigen Zertifikat ab, wenn Ihr Zertifikat nicht mehr gültig ist. Sie hängt dieses Zertifikat an Ihre Instanz an und verwendet es für Ihre aktive SAML-Konfiguration.

Hinweis: Die Abfrage erfolgt, wenn der IdP außerhalb Ihres Netzwerks zugänglich ist.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geführte Tour für SAML

Verwenden Sie die geführte SAML-Tour, um SAML für Single Sign-on zu konfigurieren.

Die geführte SAML-Tour hilft Ihnen beim Trainieren und Konfigurieren des SSO für Ihren ServiceNow® Instanz. Administratoren können die geführte Tour auswählen, um schnell die erforderlichen Aktionen bei der Konfiguration von SSO für die Instanzen zu erfahren.

Bevor Sie die geführte Tour verwenden, müssen Sie eine SAML-Anwendung in Ihrem bevorzugten Identitätsanbieter konfigurieren, z. B. Okta, Microsoft Azure, ADFS usw. Informationen zum Konfigurieren einer SAML-Anwendung finden Sie in der folgenden Dokumentation:

- Okta: Für Okta müssen Sie Folgendes ausführen:
  - Fügen Sie eine Okta-SAML-Anwendung hinzu
  - Konfigurieren Sie SAML 2,0 für ServiceNow®
- Microsoft Azure: Single Sign-on (SSO)-Integration mit ServiceNow®
- Ping: Konfigurieren von SAML SSO mit ServiceNow®
- ADFS: Integration mit SAML 2,0

Um die geführte SAML-Tour zu verwenden, aktivieren Sie das Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“. Weitere Informationen finden Sie unter Aktivieren Sie das Multi-Provider-SSO-Plugin.

Um die geführte SAML-Tour zu verwenden, führen Sie die folgenden Schritte aus:

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identitätsanbieter**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie Aus **SAML** .
4. Klicken Sie auf **Hilfe** Symbol.
5. Klicken Sie Auf **Nehmen Sie an einer Tour Teil** .

Geführte SAML-Tour Verwenden Sie eine Reihe von Schritten, die sich über mehrere Seiten erstrecken, um die Konfiguration abzuschließen, befolgen Sie die Schritte und Anweisungen, die im Rahmen der Tour bereitgestellt werden, und schließen Sie die Tour ab. Weitere Informationen zur SAML-Konfiguration finden Sie unter SAML 2,0-Konfiguration mit Multi-Provider-SSO.

Integration von SAML 2,0 mit anderen Funktionen

Sie können Ihre SAML 2,0-Lösung mit anderen Funktionen wie E-Signatur, Deep Linking und ADFS integrieren.

Fügen Sie Deep Linking-Unterstützung für SAML hinzu

Deep Linking ermöglicht es Instanzen, direkte E-Mail-Links zu einem bestimmten Datensatz im System zu unterstützen.

Wenn die SAML 2,0-Integration aktiviert ist, müssen Deep-Linking-URLs eine Authentifizierungsprüfung bestehen, bevor der IdP den Anwender zur ursprünglich angeforderten URL umleitet. Betrachten Sie beispielsweise eine E-Mail, die diese URL enthält: `https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Instanz sendet eine Authentifizierungsanforderung an den IdP und verwendet den RelayStatus URL-Parameter zum Beibehalten der ursprünglich angeforderten Ressource (in diesem Fall uri=Incident.do?sys_ID=46c88ac1a9fe1981014de1c831fbcf6d). Nachdem der IdP den Anwender authentifiziert hat, liest die Instanz den Wert des Parameters „RelayState URL“ und leitet den Anwender zur angeforderten Ressource weiter (sofern sie in der Instanz vorhanden ist).

Um Unterstützung für Deep Linking hinzuzufügen, stellen Sie sicher, dass der Identitätsanbieter unterstützt RelayStatus URL-Parameter.

ADFS-Integration mit SAML 2,0

Die ServiceNow Das Multi-Provider-SSO-Plugin unterstützt SAML 2. Single Sign-on (SSO)-Integration mit Microsoft ADFS.

Informationen zum Installieren und Konfigurieren von ADFS finden Sie unter Active Directory Federation Services – Übersicht . Das Multi-Provider-SSO-Plugin ha, das mit einer SAML 2,0 SSO-Integration mit ADFS 2,0, 3,0, Azure AD.ributes konfiguriert und getestet wurde, unterstützt SAML Response in nicht

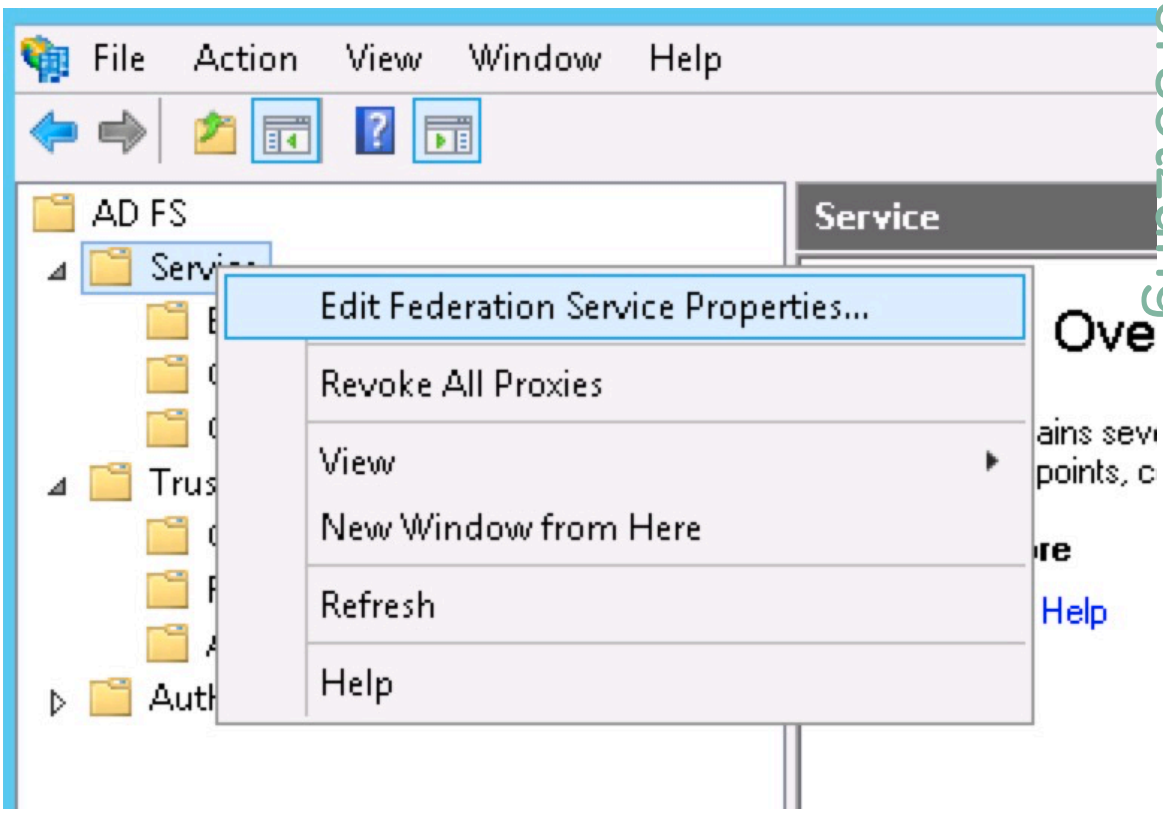
Richten Sie ADFS für SAML ein

Richten Sie ADFS für SAML ein. Dieses Verfahren verwendet ADFS 2,0 und zeigt samportal.example.com als ADFS-Website an. Ersetzen Sie dies durch Ihre ADFS-Website-Adresse.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

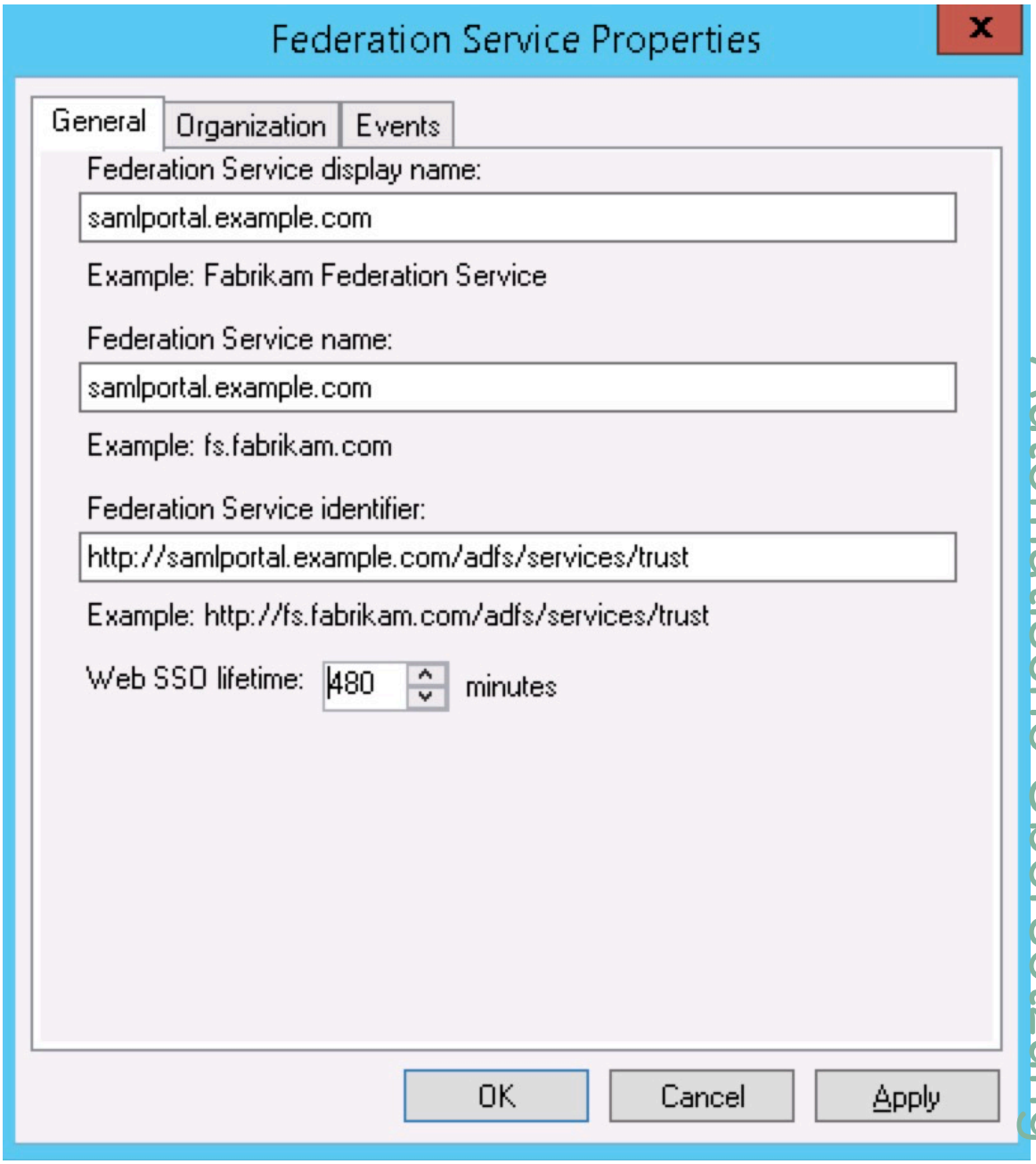
1. Melden Sie sich beim ADFS 3,0-Server an, und öffnen Sie die Verwaltungskonsole.
2. Rechtsklick **Service** Und wählen Sie aus **Bearbeiten Sie Verbundservice-Eigenschaften** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Bestätigen Sie, dass die allgemeinen Einstellungen mit Ihren DNS-Einträgen und Zertifikatnamen übereinstimmen.



4. Navigieren Sie zu den Zertifikaten, und exportieren Sie das Token-Signaturzertifikat.

   a. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und wählen Sie aus **Zeigen Sie Das Zertifikat An** .

   b. Wählen Sie die Registerkarte **Details** aus.

   c. Klicken Sie Auf **In Datei kopieren** .
   Der Zertifikatexport-Assistent wird geöffnet.

   d. Wählen Sie **Weiter**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Stellen Sie sicher, dass **Nein, exportieren Sie den privaten Schlüssel nicht** Option ist ausgewählt, und klicken Sie dann auf **Als Nächstes** .

f. Wählen Sie Aus **DER-codierte binäre X.509 (.cer)** , Und klicken Sie dann auf **Als Nächstes** .

g. Wählen Sie aus, wo Sie die Datei speichern möchten, geben Sie ihr einen Namen, und klicken Sie auf **Als Nächstes** .

h. Wählen Sie **Fertigstellen** aus.
Die Instanz erfordert, dass dieses Zertifikat im PEM-Format vorliegt. Sie können dieses Zertifikat mithilfe von Client-Tools oder Online-Tools wie SSL Shopper konvertieren.

5. Verwenden Sie das soeben erstellte DER/Binärzertifikat, und exportieren Sie es im Standard-PEM-Format.

Richten Sie die Instanz für ADFS ein

Konfigurieren Sie Ihre Instanz- und SAML 2,0-Einstellungen für die Arbeit mit ADFS.

Vorbereitungen
Führen Sie diese Schritte erst aus, nachdem Sie ADFS für SAML eingerichtet haben. Weitere Informationen zu diesem Prozess finden Sie unter Richten Sie ADFS für SAML ein .

Erforderliche Rolle: Administrator

Prozedur

1. Wenn nicht bereits aktiv, Aktivieren Sie das Multi-Provider-SSO-Plugin.
2. Konfigurieren SAML, Wenn Sie das IdP-Zertifikat installieren, hängen Sie das PEM-Zertifikat an, das Sie bei der Installation erstellt haben Richten Sie ADFS für SAML ein.
3. Klicken Sie auf **Speichern**.
4. Überprüfen Sie, ob **Problem** Und **Betreff** Felder haben Werte und, die keine Fehler aufweisen.
Wenn ein Fehler auftritt, öffnen Sie das gespeicherte PEM-formatierte Zertifikat in Notepad, kopieren Sie das Zertifikat, und fügen Sie es in das Feld PEM-Zertifikat ein.
5. Stellen Sie sicher, dass der Installationsausgang SAML2SingleSignon_update1 aktiv ist.
6. Setzen Sie die SAML 2,0-Konfiguration fort.

Hinweis: Wenn ein Zertifikat auf dem ADFS-Server aktualisiert wird, müssen Sie auch ein aktualisiertes Zertifikat in die Instanz hochladen.

Konfigurieren Sie eine ADFS-abhängige Partei

Importieren Sie die Instanzmetadaten in Ihren ADFS-Server. Die manuelle Konfiguration der vertrauenden Partei scheint jedoch einfacher zu implementieren.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider** > **SAML2-Aktualisierung1** > **Verschlüsselung und Signatur** Und überprüfen Sie, ob die SAML-Eigenschaft AuthnRequest signieren (`glide.authenticate.sso.saml2.require_signed_authnrequest`) Ist nicht aktiv.
   Lassen Sie diese Eigenschaft nur aktiv, wenn Ihr ADFS-Administrator verifizieren kann, dass Sie signierte Anforderungen benötigen.
2. Kopieren Sie die Metadaten, die Sie über den SAML 2-Metadaten-Link generiert haben, und speichern Sie sie in einer Datei.
3. Melden Sie sich beim ADFS-Server an, und öffnen Sie die Verwaltungskonsole.
4. Wählen Sie Aus **Trusts Der Vertrauenden Partei** .
5. Wählen Sie Aus **Fügen Sie Vertrauenspartei Hinzu** Von der oberen rechten Ecke des Fensters.

   Der Assistent zum Hinzufügen wird angezeigt.
6. Klicken Sie Auf **Starten** Um zu beginnen.
7. Verwenden Sie **Datei Importieren** Option zum Importieren der Metadatendatei.
8. Geben Sie ihm einen Anzeigenamen wie ServiceNow Und geben Sie alle gewünschten Notizen ein.
9. Wählen Sie Aus **ADFS 3,0-Profil** .
10. Wählen Sie kein Token-Verschlüsselungszertifikat aus.
    Es wird das Zertifikat verwendet, das für den Service definiert ist, der bereits exportiert wurde. Das Definieren eines Zertifikats verhindert eine ordnungsgemäße Kommunikation mit der Instanz.
11. Aktivieren Sie keine Einstellungen für **URL konfigurieren** .
12. Geben Sie die Instanz-Site ein, mit der Sie eine Verbindung hergestellt haben, als Trust-Bezeichner der vertrauenden Partei.
    Verwenden Sie in diesem Fall https://company.service-now.com Und klicken Sie auf **Hinzufügen** .
13. Allen Anwendern den Zugriff auf diese vertrauende Partei erlauben.
14. Klicken Sie Auf **Als Nächstes** Und löschen Sie **Öffnen Sie die Ansprüche, wenn dies abgeschlossen ist** Kontrollkästchen.
15. Schließen Sie diese Seite.
    Der neue Vertrauenspartei wird im Fenster angezeigt.
16. Klicken Sie mit der rechten Maustaste auf das Vertrauen der vertrauenden Partei, und wählen Sie aus **Eigenschaften** .
17. Navigieren Sie zu **Erweitert** Registerkarte und legen Sie fest **Sicherer Hash-Algorithmus** Entweder als SHA-256 oder SHA-1.
18. Navigieren Sie zur Registerkarte Endpunkte, und fügen Sie ein hinzu **SAML-Assertionsverbraucher** Mit **Veröffentlichen** Bindung und eine URL von https://company.service-now.com/navpage.do .

Konfigurieren Sie die ADFS-Anspruchsregeln für vertrauende Parteien

Bearbeiten Sie die Anspruchsregeln, um eine ordnungsgemäße Kommunikation mit der Instanz zu ermöglichen.

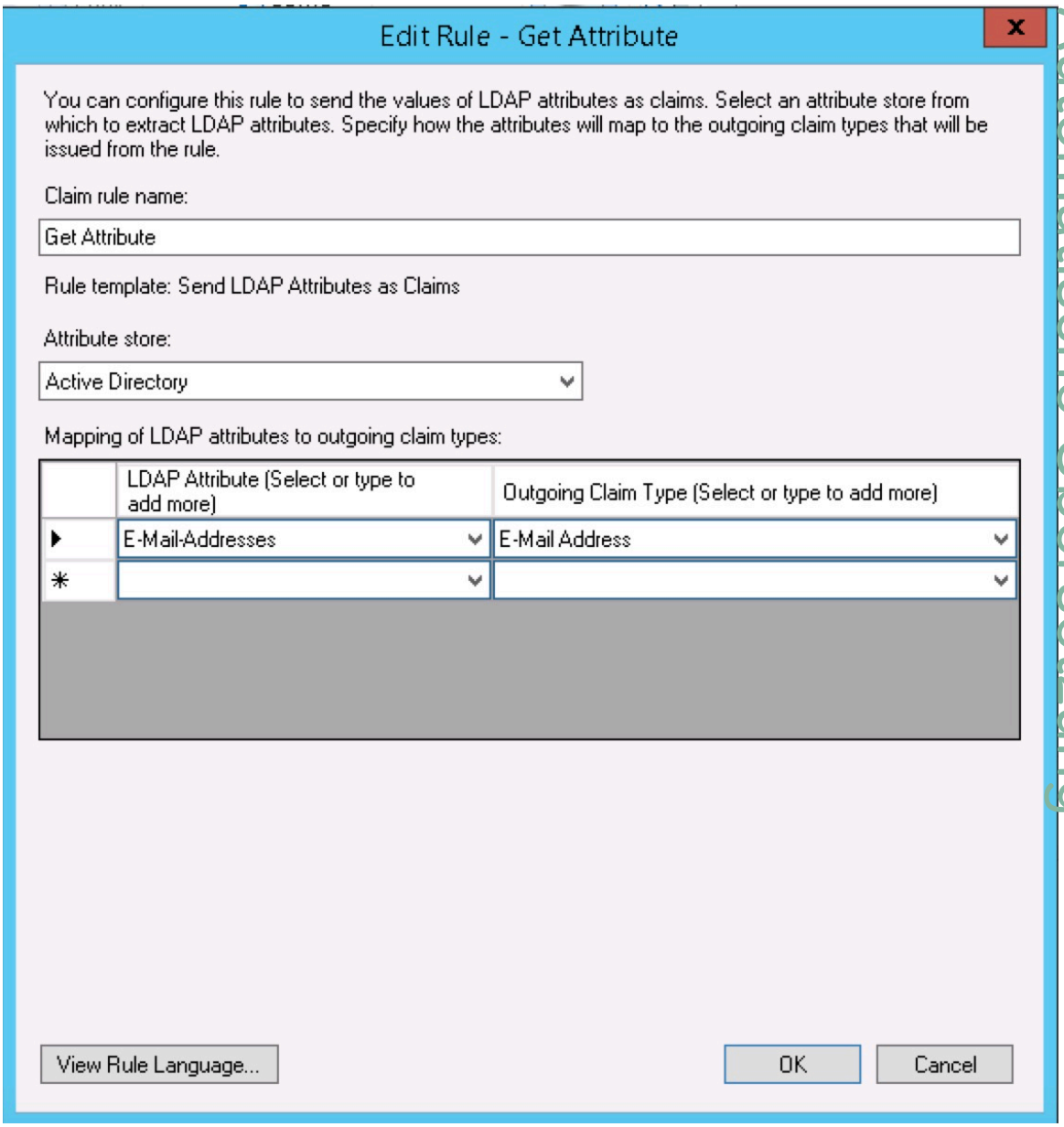
Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich beim ADFS-Server an, und öffnen Sie die Verwaltungskonsole.
2. Klicken Sie mit der rechten Maustaste auf das Vertrauen der vertrauenden Partei, und wählen Sie aus **Bearbeiten Sie Anspruchsregeln** .
3. Klicken Sie auf **Regeln Für Ausgabetransformation** Registerkarte.
4. Wählen Sie Aus **Fügen Sie Regeln Hinzu** .
5. Wählen Sie Aus **LDAP-Attribut als Ansprüche senden** Als zu verwendende Anspruchsregelvorlage.
6. Geben Sie dem Anspruch einen Namen wie LDAP-Attribute abrufen .
7. Legen Sie fest **Attributspeicher** Bis Active Directory , **LDAP-Attribut** Bis E-Mail-Adressen , Und **Typ Des Ausgehenden Anspruchs** Bis E-Mail-Adresse .



Automatische Übersetzung

```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
 == "AD AUTHORITY"]
=> issue(store = "Active Directory",
```

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

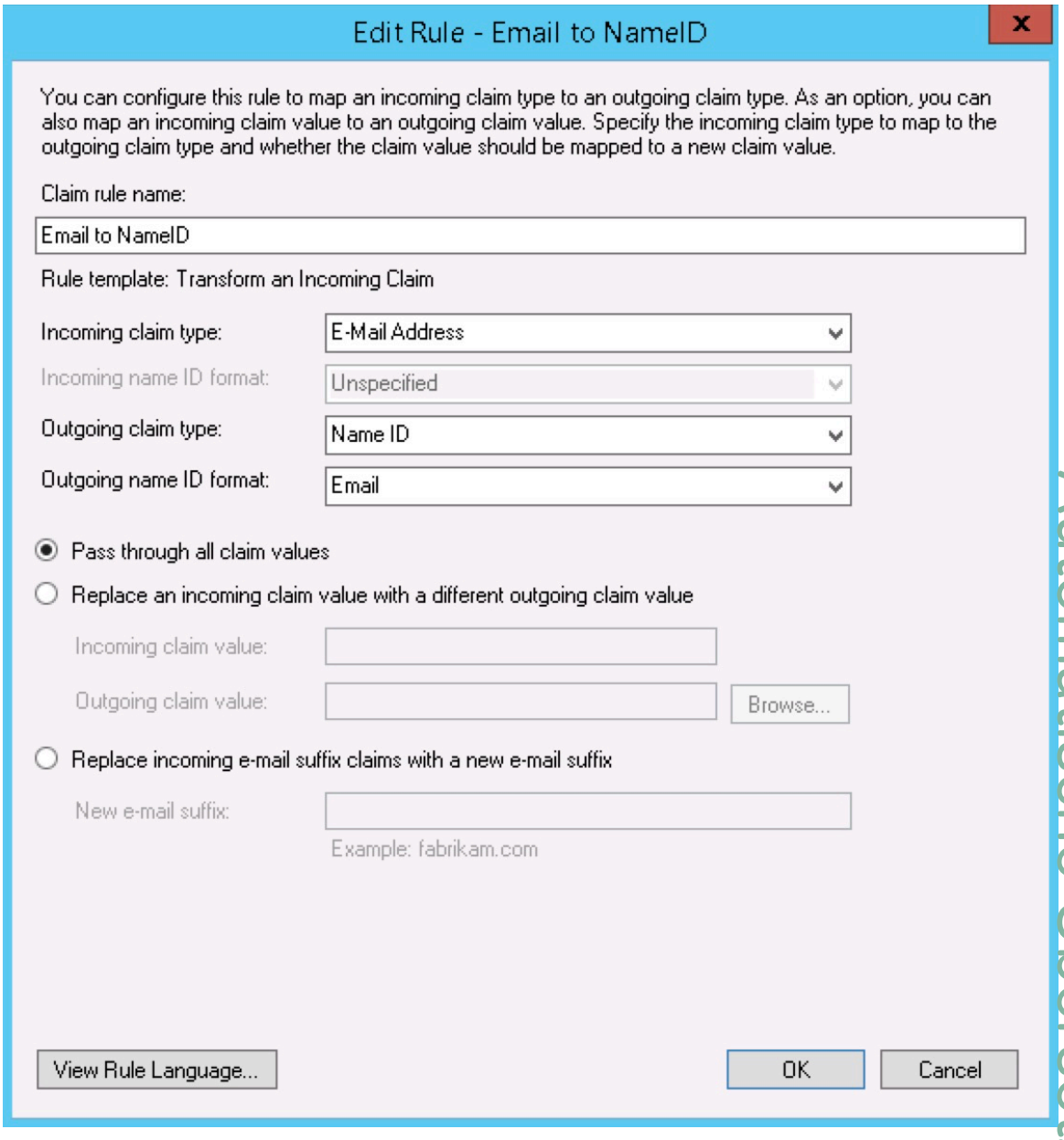
```
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
query = ";mail;{0}", param = c.Value);
```

8. Wählen Sie **Fertigstellen** aus.
9. Wählen Sie Aus **Fügen Sie Regeln Hinzu** .
10. Wählen Sie Aus **Transformieren Sie einen eingehenden Anspruch** Als zu verwendende Anspruchsregelvorlage.
11. Geben Sie dem Anspruch einen Namen wie E-Mail-Empfänger-Name-ID .
12. Legen Sie fest **Typ des eingehenden Anspruchs** Zu **Typ Des Ausgehenden Anspruchs** In der vorherigen Regel.
    Beispiel: E-Mail-Adresse .
13. Legen Sie fest **Typ des ausgehenden Anspruchs** Bis Name-ID Und **Format der ausgehenden Namens-ID** Bis E-Mail .

    Hinweis: Diese Werte müssen mit übereinstimmen Name-ID-Richtlinie Sie definieren während der SAML 2,0-Konfiguration.

14. Wählen Sie Aus **Übergeben Sie alle Anspruchswerte** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Diese Anspruchsregel sollte der folgenden Regelsprache ähnlich aussehen.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

15. Klicken Sie auf **Fertigstellen**.

Erstellen Sie einen SAML-Abmeldeendpunkt

Erstellen Sie einen SAML-Abmeldeendpunkt, um eine einzelne Abmeldung zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Siehe Dieser artikel zur ADFS-Anmeldung Weitere Informationen finden Sie unter .

Prozedur

1. Gehe zu **ADFS-Manager** > **Vertrauensbeziehungen** > **Trusts Der Vertrauenden Partei** > **Eigenschaften**an.
2. Klicken Sie auf der Registerkarte Endpunkte auf **Fügen Sie SAML hinzu** .
3. Konfigurieren Sie die Einstellungen:
   - **Endpunkttyp** : SAML-Abmeldung
   - **Bindung** : VERÖFFENTLICHEN
   - **Vertrauenswürdige URL** : Die URL Ihres ADFS-Servers. Beispiel:

     ```
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
     ```

   - **Antwort-URL** : Die Abmelde-URL der Anwendung. Beispiel:

     ```
     https://{instancename}.service-now.com/external_logout_complete.do
     ```

Testen Sie die ADFS-Konfiguration

Testen Sie Ihre ADFS-Konfiguration, um sicherzustellen, dass sie als Identitätsanbieter ordnungsgemäß funktioniert.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie einen Internet Explorer-Browser.
2. Navigieren Sie zu Ihrem ADFS-Portal.

   Beispiel: `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx` . Diese Seite enthält eine Dropdown-Liste aller konfigurierten Trusts der vertrauenden Partei.
3. Wählen Sie die vertrauende Partei aus, die Ihrer Instanz zugeordnet ist.
4. Klicken Sie Auf **Fahren Sie mit der Anmeldung fort** .

   Wenn Sie die externe SAML 2,0-Authentifizierung ordnungsgemäß konfiguriert haben, sollten Sie automatisch bei der Instanz angemeldet werden.
5. Testen Sie eine URL für die direkte Anmeldung, indem Sie zu navigieren `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://company.service-now.com` .

(Problemumgehung) Aktivieren Sie die vom Service Provider initiierte Authentifizierung

Verwenden Sie diese Problemumgehung, wenn die Authentifizierung fehlschlägt, da Sie kein SAML 2,0 Update 1 haben. Dieses Problem kann auftreten, wenn Anwender versuchen, die IdP-Authentifizierung zu überspringen und direkt zur Instanz zu navigieren.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieser Fehler tritt auf, wenn die Instanz ADFS nicht mit der erforderlichen Definition und Semantik für das SPNameQualifier-Attribut in der SAMLResponse bereitstellt.

Aktivieren Sie die vom Service Provider initiierte Authentifizierung, indem Sie eine der folgenden Aktionen ausführen:

Prozedur

- Führen Sie ein Upgrade auf SAML 2,0 Update 1 durch, und deaktivieren Sie die Option zum Erstellen einer AuthnContextClass-Anforderung.
- Ändern Sie **SAML2** Skripteinbindung zum Kommentieren der Definitionen von SPNameQualifier Attribut, wenn SAML 2,0 aktiv ist (nicht SAML 2,0 Update 1).

  Kommentieren Sie diese Zeilen in den Funktionen createNameID und createNameIDPolicy:

```
//nid.setSPNameQualifier (serviceURL ) ;

 //nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

Nächste Maßnahme

Wenn die Anmeldeaufforderung Ihres ADFS-Servers beim Zugriff auf die Instanz nicht angezeigt werden soll, legen Sie die folgende SAML 2,0 Update 1-Eigenschaft auf „falsch“ fest: **Erstellen Sie eine AuthnContextClass-Anforderung in AuthnRequest** Anweisung (*`glide.authenticate.sso.saml2.createrequestedauthncontext`*).

(Problemumgehung) unterstützt die Kerberos-Authentifizierung

Für die SAML 2,0-Integration ist eine Problemumgehung verfügbar, die den Authentifizierungskontext von formularbasierter Authentifizierung in Windows-basierte Authentifizierung ändert.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Derzeit verwendet die SAML 2-Integration einen PasswordProtectedTransport- oder „formularbasierte Authentifizierung“-Authentifizierungskontext. Dieser Authentifizierungskontext erfordert, dass der IdP Anwendern ein Formular für Anmeldeinformationen zur Authentifizierung vorlegt. Bei Kerberos ist bereits eine SAML-Sitzung über eine etablierte Windows-Anmeldung aktiv, sodass der Anwender sich nicht beim IdP authentifizieren muss.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Öffnen Sie **SAML2-Aktualisierung1** IDP-Datensatz.
3. Legen Sie fest **Die AuthnContextClassRef-Methode, die wir in unsere SAML 2,0 AuthnRequest an den Identitätsanbieter aufgenommen werden** Zu einem der folgenden Elemente:

AuthnContextClassRef-Methodenwerte
URN:Oasis:names:tc:SAML:2,0:ac:classes:PasswordProtectedTransport (Standard)
URN:Federation:Authentication:Windows

4. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure AD-Integration mit SAML 2,0

Integrieren ServiceNow Mit Azure Active Directory (Azure AD).

Integration ServiceNow Mit Azure AD können Sie:

- Kontrollieren Sie in Azure AD, wer Zugriff auf hat ServiceNow.
- Ermöglichen Sie Anwendern, sich automatisch bei anzumelden ServiceNow Mit ihren Azure AD-Accounts.
- Verwalten Sie Ihre Accounts im Azure-Portal.

Voraussetzungen

Um zu beginnen, müssen Sie Folgendes ausführen:

- Ein Azure AD-Abonnement. Wenn Sie kein Abonnement haben, können Sie einen kostenlosen Account erhalten.
- A ServiceNow Single Sign-on (SSO) aktiviert.
- A ServiceNow Instanz oder Mandant von ServiceNow Die San Diego-Versionen oder höher unterstützt.
- A ServiceNow Für den Mandanten muss das Single Sign-on-Plugin für mehrere Anbieter aktiviert sein.
- Aktivieren Sie für die automatische Konfiguration das Multi-Provider-Plugin für ServiceNow.

Satz von Aktionen für die Konfiguration

Im Folgenden sind die Aktionen aufgeführt, die zum Konfigurieren von Azure AD ausgeführt werden müssen:

- Hinzufügen ServiceNow Aus der Galerie zu Azure AD.
- Konfigurieren Sie Azure AD SSO
- Erstellen Sie einen Azure AD-Testanwender
- Weisen Sie den Azure AD-Testanwender zu
- ServiceNow konfigurieren

Hinzufügen ServiceNow Aus der Galerie

Hinzufügen ServiceNow Aus der Galerie zu Ihrer Liste der verwalteten SaaS-Apps in Azure AD.

Vorbereitungen

Erforderliche Rolle: Azure admin

Prozedur

1. Melden Sie sich mit einem Microsoft-Account beim Azure-Portal an.
2. Wählen Sie aus **Azure Active Directory** Service aus dem linken Bereich.
3. Navigieren zu **Enterprise-Anwendungen** > **Alle Anwendungen**an.
4. Um eine neue Anwendung hinzuzufügen, wählen Sie aus **Neu** Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie im Abschnitt aus der Galerie hinzufügen ein ServiceNow Im Suchfeld.
6. Wählen Sie Aus ServiceNow Im Ergebnisbereich und fügen Sie dann die App hinzu.
7. Warten Sie einige Sekunden, während die App Ihrem Mandanten hinzugefügt wird.

Konfigurieren Sie Azure AD SSO

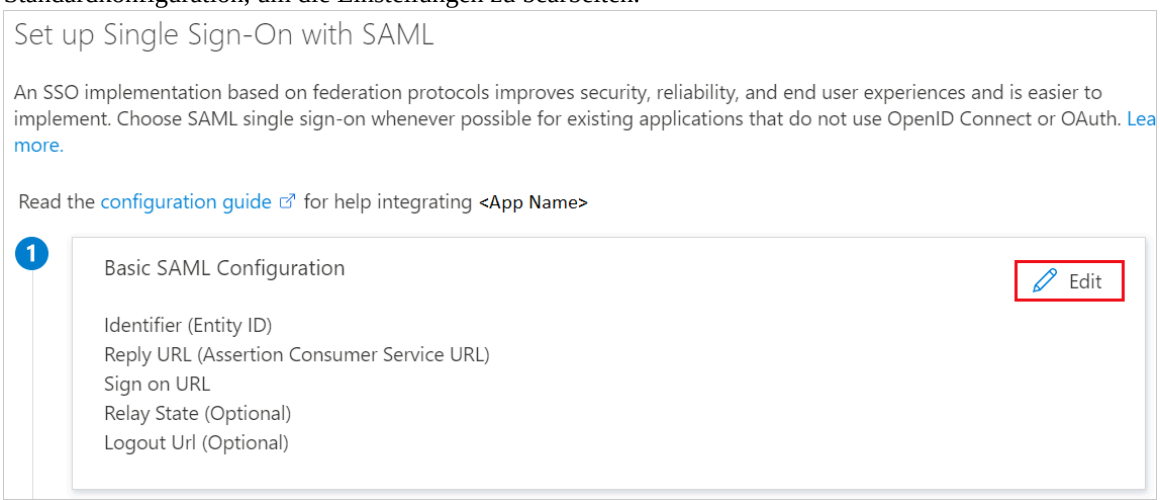
Konfigurieren Sie Azure AD SSO im Azure-Portal.

Vorbereitungen

Erforderliche Rolle: Azure admin

Prozedur

1. Im Azure-Portal auf der ServiceNow Anwendungsintegrationsseite finden Sie den Abschnitt Verwalten.
2. Wählen Sie Single Sign-on aus.
   Wählen Sie auf der Seite Single Sign-on-Methode auswählen die Option SAML aus.
3. Wählen Sie auf der Seite Single Sign-on mit SAML einrichten das Pen-Symbol für SAML-Standardkonfiguration, um die Einstellungen zu bearbeiten.



4. Führen Sie im Abschnitt SAML-Standardkonfiguration die folgenden Schritte aus:

   a. In **Anmelde-URL** , Geben Sie eines der folgenden URL-Muster ein:

   ```
   https://<instancename>.service-now.com/navpage.do
   https://<instance-name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
   ```

   Hinweis: Sie müssen die sys_ID innerhalb dieser URL angeben.

   b. Geben Sie unter Bezeichner (Entitäts-ID) eine URL mit dem Muster ein: `https://<instance-name>.service-now.com` .

   c. Für **Antwort-URL** , Geben Sie eines der folgenden URL-Muster ein:

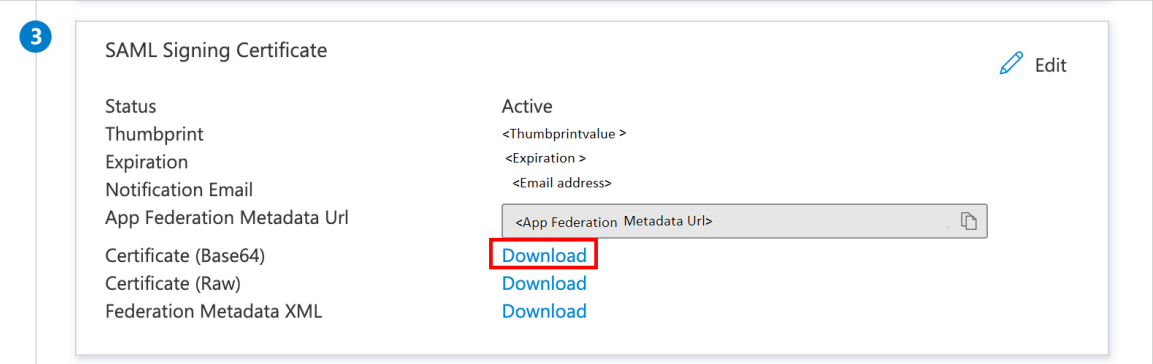
   ```
   https://<instancename>.service-now.com/navpage.do
   https://<instancename>.service-now.com/customer.do
   ```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Geben Sie unter Abmelde-URL eine URL mit dem Muster ein: `https://<instancename>.service-now.com/navpage.do`

> **Hinweis:** Sie müssen die tatsächliche Anmelde-URL, die Antwort-URL, die Abmelde-URL und den Bezeichner aktualisieren. Die in diesen URLs angezeigten Werte dienen zu Demozwecken.

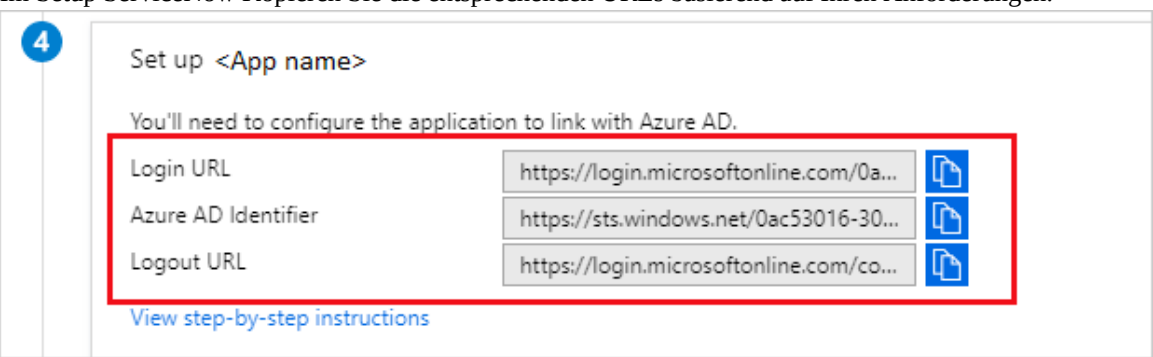
5. Suchen Sie auf der Seite Single Sign-on mit SAML einrichten im Abschnitt SAML-Signaturzertifikat nach **Zertifikat (Base64)** .



a. Wählen Sie die Schaltfläche „Kopieren“ aus, um zu kopieren **Metadaten-Url Der App-Föderation** , Und fügen Sie es in Notepad ein.
Diese URL ist für die weitere Konfiguration erforderlich.

b. Wählen Sie Aus **Herunterladen** Zum Herunterladen des Zertifikats (Base64).

6. Im Setup ServiceNow Kopieren Sie die entsprechenden URLs basierend auf Ihren Anforderungen.



Erstellen Sie einen Azure AD-Testanwender

Erstellen Sie einen Testanwender in Azure AD.

Vorbereitungen

Erforderliche Rolle: Azure admin

Prozedur

1. Navigieren Sie im Azure-Portal zu **Alle** > **Azure Active Directory** > **Anwender** > **Alle Anwender**an.

2. Wählen Sie Aus **Neuer Anwender** .

3. Geben Sie in den Anwendereigenschaften die folgenden Informationen an:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Name
- Benutzername
- Passwort

4. Klicken Sie auf **Erstellen**.

Weisen Sie den Azure AD-Testanwender zu

Weisen Sie den Azure AD-Testanwender zu, der für die Verwendung von Azure Single Sign-on erstellt wurde, indem Sie Zugriff auf gewähren ServiceNow.

Vorbereitungen
Erforderliche Rolle: Azure admin

Prozedur

1. Navigieren Sie im Azure-Portal zu **Alle** > **Enterprise-Anwendungen** > **Alle Anwendungen**an.
2. Wählen Sie in der Anwendungsliste aus ServiceNow.
3. Wählen Sie auf der Seite der App im Abschnitt Verwalten die Option aus **Anwender und Gruppen** .
4. Wählen Sie **Anwender hinzufügen** aus.
5. In **Fügen Sie Die Zuweisung Hinzu** Fenster auswählen **Anwender und Gruppen** .
6. In **Anwender und Gruppen** Wählen Sie im Fenster aus Testanwender Das aus der Anwenderliste erstellt wurde.
7. Wählen Sie die Rolle für den zugewiesenen Anwender aus der aus **Wählen Sie eine Rolle aus** Dropdownliste, falls erforderlich.
8. In **Fügen Sie Die Zuweisung Hinzu** Fenster auswählen **Zuweisen** .

ServiceNow konfigurieren

Konfigurieren ServiceNow Mit Azure AD-Details zur Verwendung von SSO.

Vorbereitungen
Plugin: Integration: Single Sign-on-Installationsprogramm für mehrere Anbieter

Aktivieren Sie die Multi-Provider-SSO-Eigenschaften:

- Wählen Sie Aus **Aktivieren Sie SSO für mehrere Anbieter** .
- Wählen Sie Aus **Aktivieren Sie das automatische Importieren von Anwendern aus allen Identitätsanbietern in die Anwendertabelle** .
- Wählen Sie Aus **Aktivieren Sie die Debug-Protokollierung für die SSO-Integration mehrerer Anbieter** .
- Geben Sie Ein **E-Mail** , Das Feld in der Anwendertabelle, das….

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Wählen Sie auf der Seite „Identitätsanbieter“ die Option aus **Neu** .
3. Wählen Sie im Fenster „Identitätsanbieter“ die Option aus **SAML** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Im Dialogfeld Metadaten des Identitätsanbieters importieren können Sie:
   - **URL** : Metadaten-URL der App-Föderation, um die Details auf der Konfigurationsseite des Identitätsanbieters automatisch auszufüllen.
   - **Importieren** : Importieren Sie die XML, um die Details auf der Konfigurationsseite des Identitätsanbieters zu importieren.
5. Klicken Sie mit der rechten Maustaste oben auf dem Bildschirm, und klicken Sie auf **Kopieren Sie die sys_ID** , Und verwenden Sie diesen Wert für **Anmelde-URL** In **SAML-Standardkonfiguration** Abschnitt.
6. Füllen Sie im Formular die Felder aus.

Single Sign-on-Felder für mehrere Anbieter

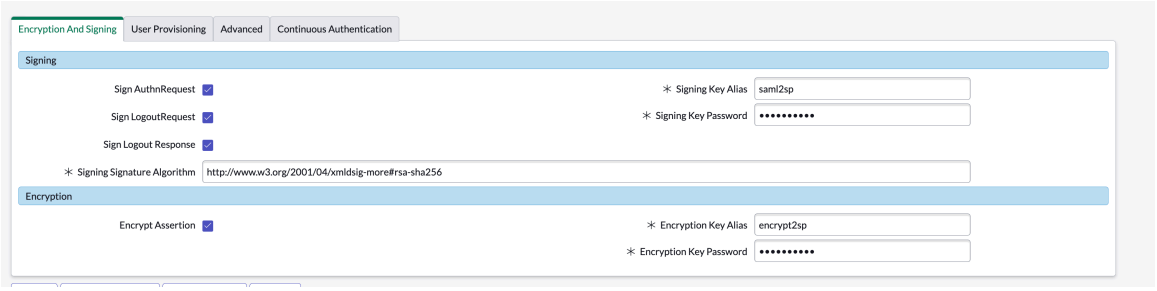
Eigenschaft	Erforderlich	Beschreibung
Name	Ja	Name für den IdP. Dieser IdP ist die SYS-ID der automatischen Umleitung
Aktiv	Ja	„Aktiv“ muss auf „wahr“ festgelegt werden, damit der IdP für die Authentifizierung verwendet werden soll. **Hinweis:** Die Option zum Festlegen dieser Eigenschaft erfolgt erst nach einer erfolgreichen Testverbindung.
Standard	Nein	IdP automatisch umleiten, früher als primärer IdP bekannt, leitet Anwender automatisch um, um auf die Basisinstanz-URL zuzugreifen. Diese Eigenschaft legt diese IdP-Konfiguration als Standard fest.
Automatische IdP-Weiterleitung	Nein	IDP-Konfiguration, die Sie als IdP für automatische Umleitung festlegen können. **Hinweis:** Wenn Sie eine neue IdP-Konfiguration für die automatische Umleitung aktivieren, wird die aktiviert `glide_sso_id` Cookie-Updates mit dem neuen automatischen Umleitungs-IdP. Die `glide.authenticate.sso.update.idp.cookie`Die Systemeigenschaft, die automatisch aktiviert ist, steuert diese Funktion.
URL des Identitätsanbieters	Ja	URL zu Ihrem IdP. Jede IdP-URL muss eindeutig sein.
AuthnRequest des Identitätsanbieters	Ja	URL zur HTTP-Umleitungsbindung, die vom SingleSignOnService-Element abgerufen wurde.
SingleLogoutRequest des Identitätsanbieters	Nein	URL, die aus dem SingleLogoutService-Element abgerufen wurde.
ServiceNow Homepage	Ja	URL, einschließlich Anmeldeseite, der Instanz, für die sich der IdP authentifiziert. Beispiel: https://yourinstance.service-now.com/navpage.do
Entitäts-ID/Aussteller	Ja	Basis-URL mit Ausnahme der Anmeldeseite der Instanz, für die sich der IdP authentifiziert. Beispiel: https://yourinstance.service-now.com/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Erforderlich	Beschreibung
Zielgruppen-URI	Ja	Basis-URL mit Ausnahme der Anmeldeseite der Instanz, für die sich der IdP authentifiziert. Beispiel: https://yourinstance.service-now.com/
NameID-Richtlinie	Ja	Wert des NameIDFormat-Elements, das die Integration verwendet.
Weiterleitung für externe Abmeldung	Nein	URL, an die die Integration Anwender nach der Abmeldung weiterleitet.
Fehlerhafte Anforderungsumleitung	Nein	URL für die Weiterleitung fehlgeschlagener Authentifizierungsanforderungen. Standardmäßig ist dies der URL-Endpunkt einer Fehlerseite oder Abmeldeseite, die im IdP konfiguriert ist. Sie können diesen Wert im Feld glide.authenticate.failed_requirement_redirect ausfüllen.

7. **Wahlweise:** Registerkarte „Verschlüsselung und Signatur“

Hinweis: Verwenden Sie Ihre eigenen Zertifikate für die Verschlüsselung und Signierung.



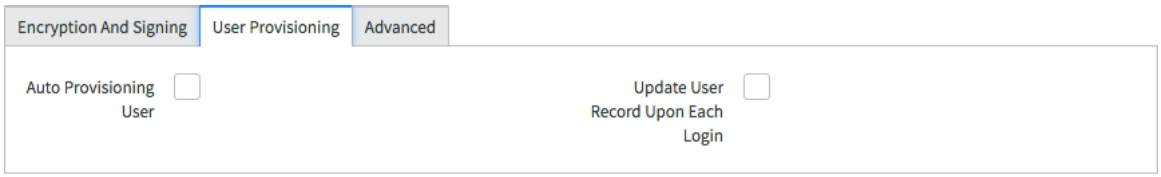
Verschlüsselungs- und Signaturfelder

Eigenschaft	Beschreibung
Signier-/ Verschlüsselungsschlüsselalias	Alias des in gespeicherten Schlüsseleintrags SAML 2,0 SP-Schlüsselspeicher .
Signaturschlüssel-Passwort	Passwort des in gespeicherten Schlüsseleintrags SAML 2,0 SP-Schlüsselspeicher .
Assertion verschlüsseln	Kontrollkästchen zum Verschlüsseln der Assertion in der SAML-Antwort. Die für den IDP generierten Metadaten bettet das x509-Zertifikat ein, das der IDP verwendet, um die Assertion in der von ihm generierten SAML-Antwort zu verschlüsseln.
Signaturalgorithmus für Signieren	URL, die auf den SAML 2,0 Identitätsanbieter AuthnRequest-Verbraucher für eSignature-Authentifizierung verweist.
AuthnRequest signieren	Kontrollkästchen, um zu aktivieren, dass der IdP-Single Sign-on-Service eine signierte AuthnRequest empfängt.
LogoutRequest signieren	Kontrollkästchen, um zu aktivieren, dass der IdP-Single-Sign-on-Service eine signierte LogoutRequest empfängt.

8. **Wahlweise:** Registerkarte „Anwenderbereitstellung“

Automatische Übersetzung

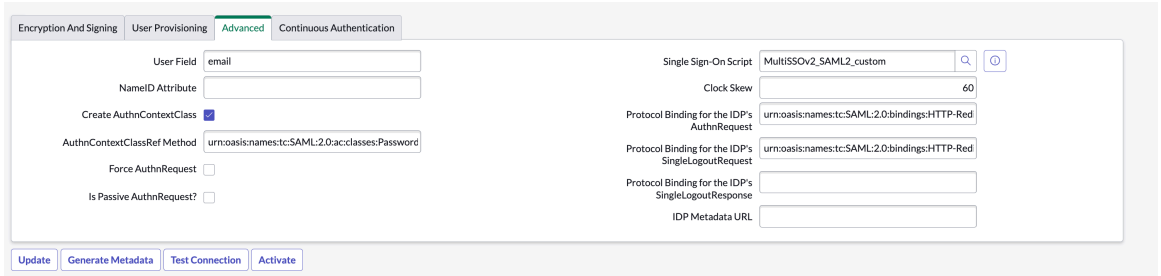
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Felder „Anwenderbereitstellung“

Eigenschaft	Beschreibung
Automatische Bereitstellung von Anwender	Automatische Anwenderbereitstellung: Erstellt die Anwender, wenn der Anwender basierend auf den vom IdP bereitgestellten Informationen nicht in der Instanz-Anwendertabelle vorhanden ist.
Anwenderdatensatz bei jeder Anmeldung aktualisiere	Aktualisieren Sie die Anwenderinformationen in der Instanzanwendertabelle mit den Informationen im IdP jedes Mal, wenn sich der Anwender mit SAML anmeldet.

9. Wahlweise: Registerkarte „Erweitert“



Erweiterte Felder

Eigenschaft	Beschreibung
Anwenderfeld	Feld in der Anwendertabelle, das den Wert enthält, den der IdP zur Identifizierung des Anwenders benötigt. Diese eindeutige ID ist Teil der Antwort. Zum Beispiel ein Anwendername, eine Mitarbeiter-ID usw. In der SYS-Anwendertabelle wird diese eindeutige ID mit den Anwenderdetails abgeglichen.
Attribut NameID	Feld, das Sie leer lassen, es sei denn, Sie konfigurieren eine neue NameID-Richtlinie. Wenn Sie eine neue Richtlinie konfigurieren, benötigt das System die Anwendertabelle, die es verwenden muss, um den Anwender zu identifizieren, der sich anmeldet. Das System stimmt das NameID-Token mit dem Namen dieses Anwendertabellenfelds ab.
AuthnContextClass erstellen	Kontrollkästchen, um eine bestimmte Kontextklasse anzugeben, z. B. passwortgeschützter Transport. Wenn das Kontrollkästchen deaktiviert ist, wählt der IdP die am besten geeignete Kontextklasse aus.
AuthnContextClassRef-Methode	URN des Anmeldemechanismus, den der IdP zur Authentifizierung von Anwendern verwenden soll.
AuthnRequest erzwingen	Kontrollkästchen, um das Auftreten von AuthnRequests zu erzwingen.
Ist passive AuthnRequest	Kontrollkästchen, wenn AuthnRequest passiv ist.
Single Sign-on-Skript	Single Sign-on-Skript. Der Standardwert ist *MultiSSOV2_SAML2_custom* .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Abmeldeantwort signieren	Details zur Abmeldeantwort in diesem Feld.
Taktversatz	NAnzahl der Sekunden zwischen den beiden Attributen, aus denen die SAMLResponse-Nonce besteht. Der Standardwert ist 60. Eine gültige SAMLResponse muss zwischen liegen *Nicht vorher* Und *NotOnOrAfter* Datums-/Uhrzeitwerte. Siehe Beispiel für SAML 2-Antwort mit den Elementen SubjectConfirmation und SubjectConfirmationData und Beispiel für SAML 2-Antwort mit den Elementen AudienceRestrictions und Zielgruppe für eine Beispiel-SAMLResponse-Nachricht.
Protokollbindung für SingleLogoutReuqest des IDP	Einer der unterstützten Werte, die im Bindungsattribut aus dem SingleLogoutService-Element aufgeführt sind.
Metadaten-URL, aus der IDP-Eigenschaften importiert werden	Import von IDP-Eigenschaften aus dieser URL. Wenn festgelegt, wird der automatische Import von SAML-Zertifikaten aus dem IdP aktiviert, wenn das vorherige Zertifikat abgelaufen ist. **Hinweis:** Wenn Sie ein Upgrade von SAML2 Update 1 auf Multi-Provider-SSO durchführen oder Ihre SSO-Verbindung manuell einrichten, wird die IdP-Metadaten-URL nicht automatisch ausgefüllt.
Anforderung	Eindeutige ID als Teil der Anforderung. Die ID kann ein Anwendername, eine Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl Umleitung als auch Post-Bindung werden für die Anforderung unterstützt. Die Option zum Festlegen dieses Felds wird erst nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter Testen Sie IdP-Verbindungen.
Antwort	Eindeutige ID als Teil der Antwort. Die ID kann ein Anwendername, eine Mitarbeiter-ID usw. sein. **Hinweis:** Sowohl Umleitung als auch Post-Bindung werden für die Antwort unterstützt. Die Option zum Festlegen dieses Felds wird erst nach einer erfolgreichen Testverbindung angezeigt. Weitere Informationen finden Sie unter Testen Sie IdP-Verbindungen.

10. Wählen Sie Aus **Verbindung Testen** In der oberen rechten Ecke der Seite.
11. Geben Sie Ihre Anmeldeinformationen ein.
    Die Ergebnisse des SSO-Abmeldungstests werden angezeigt.
12. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Konfiguration.

E-Mail-Links mit externer Authentifizierung

Sie können E-Mail-Links verwenden, wenn Sie die externe Authentifizierung des Digestive-Tokens verwenden. Sie müssen jedoch festlegen, wie Sie Links in E-Mail-Benachrichtigungen behandeln.

Die Standardlinks enthalten eine URL, die Sie zu einem bestimmten Standort in der Instanz leitet, z. B. zu einem Incident oder einer Change-Anforderung, ohne SSO-Anmeldeinformationen zu enthalten. Im Folgenden finden Sie Beispiele für die Weiterleitung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

des Anwenders zum Standort in der Instanz, ohne sich auf der Instanzanmeldeseite anzumelden.

- Unverschlüsselte HTTP-Technik zum Herstellen einer Verbindung mit der Instanz „/Demo“ (es wird nicht zu einem bestimmten Datensatz navigiert):

```
https://<instance
 name>.service-now.com/?SM_USER=user_name&DE_USER=lQjlVp7aRJtyPx5+2O/vgU24t
bE=
```

- Link (in einer E-Mail-Benachrichtigung) zu einem bestimmten Datensatz, damit der Anwender zuerst zum unternehmenseigenen Anmeldeportal wechselt:

```
https://login.company_portal_page.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2
b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true
```

  Sie müssen festlegen `glide.email.override.url`Eigenschaft in Ihrer Instanz, die die URL der Unternehmensportalseite enthält. Wenn diese Eigenschaft nicht vorhanden ist, können Sie sie erstellen.

- Das Unternehmensportal muss dann diese URL verwenden und die Umleitungs-URL zur Instanz erstellen, wobei das für den Zugriff auf den spezifischen Datensatz erforderliche Segment beibehalten und die SSO-Anmeldeinformationen am Ende der URL hinzugefügt werden:

```
https://<instance
 name>.service-now.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2b01ab4eb0942
23466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true&SM_USER=user_
name&DE_USER=lQjlVp7aRJtyPx5+2O/vgU24tbE=
```

Fügen Sie E-Signatur-Unterstützung für SAML hinzu

Konfigurieren Sie die folgenden Eigenschaften für E-Signatur mit Security Assertion Markup Language (SAML) 2,0 Update 1.

Wenn E-Signatur mit Multi-SSO aktiv ist, werden keine SAML-Eigenschaften verwendet. Das System fügt der Tabelle „SAML2 Update1-Eigenschaften“ [saml2_update1_properties] E-Signatur-Eigenschaften hinzu:

Eigenschaft	Beschreibung	Standard
Assertionen-Verbraucher-Index für eSignatur-Authentifizierung	Eine Indexnummer, die den Endpunkt identifiziert.	1
Assertionen-Verbraucher-URL für eSignatur-Authentifizierung	Die URL, die den Verbraucher identifiziert.	https://yourinstance.service-now.com/consumer.do
AuthnRequest-URL für eSignature-Authentifizierung	Die URL für die Authentifizierung	Keine

Wenn Sie E-Signatur mit SAML 1,0 oder SAML 2,0 verwenden (ohne Update 1), lesen Sie die speziellen Konfigurationsanweisungen: E-Signatur für Multi-Provider-SSO.

Hinweis: Wenn Sie ein Life Science-Kunde sind, der E-Signatur verwendet, deaktivieren Sie die Business-Regel zur Verhinderung der Selbstsperrung des Anwenders.

Migrieren einer vorhandenen SAML 1,1-Integration zu SAML 2,0

Um von einer SAML 1,1-Integration zu einer SAML 2,0-Integration zu migrieren, wenden Sie sich an den Kundensupport.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisieren Sie Ihre vorhandene SAML 2,0-Integration

Aktualisieren Sie Ihre vorhandene SAML 2,0-Integration.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Fordern Sie das Plugin SAML 2,0 Update 1 an. Kontakt Kundenservice und Support Um anzufordern *SAML 2,0 Single Sign-on – Update 1: Sicherheitserweiterungen* Plugin. Das Plugin wendet aktualisierte Versionen von an *SAML2SingleSignon* Installationsausgang (Anmeldeskript), *SAML2Logout* Installationsausgang (Abmeldeskript), und *SAML2* Skripteinbindung (Skriptobjekt).

Führen Sie Anpassungen aus vorhandenen Installationsausgangsskripts in neue Skripts zusammen. Das Update speichert eine inaktive Kopie der ursprünglichen Installationsausgangsskripts der Integration. Sie können diese Kopien verwenden, um alle Anpassungen zusammenzuführen, die Sie an den Anmelde- und Abmeldeskripts für die neuen Versionen dieser Installationsausgänge vorgenommen haben.

Führen Sie Anpassungen aus vorhandenen Installationsabschlussskripts in neue Skripts zusammen

Name Des Ursprünglichen Installationsabbruchskripts	Ursprünglicher Skriptstatus	Name Des Neuen Installationsbeendigungsskripts	Neuer Skriptstatus
SAML2SingleSignon	Inaktiv	SAML2SingleSignon_update1	Aktiv
SAML2	Inaktiv	SAML2_update1	Aktiv
SAML2Logout	Inaktiv	SAML2Logout_update1	Aktiv

Sie können mit diesen Pfaden zu den SAML 2,0-Installationsabmelde- und -Abmeldeabmeldeskripts navigieren:

- **SAML 2 Single Sign-on** > **Anmeldeskript**an.
- **SAML 2 Single Sign-on** > **Abmeldeskript**an.
- **Systemdefinition** > **Installationsausgänge**an.

Sie können mit diesen Pfaden zur Skripteinbindung SAML 2,0 Update 1 navigieren:

- **SAML 2 Single Sign-on** > **Skriptobjekt**an.
- **Systemdefinition** > **Skripteinbindungen**an.

Testen Sie das Update.

Prozedur

1. Fügen Sie eine Systemeigenschaft hinzu Angerufen `glide.authenticate.sso.saml2.debug` Mit einem Wert von *Wahr* .
2. Versuchen Sie, sich bei SAML 2,0 anzumelden.
3. Überprüfen Sie das Systemprotokoll.
   SAML2-Validierungsfehler beginnen mit dem Text *SAML2ValidationError* .
4. Identifizieren und beheben Sie typische Anmeldefehler.
   Weitere Informationen finden Sie unter Multi-SSO (SAML 2,0) – Fehler und Korrekturen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für SAML 2-Antworten nach dem Update

Die folgenden Abschnitte veranschaulichen die neuen erforderlichen Elemente und Attribute, die der IdP in der SAML-Antwort bereitstellen soll.

Beispiel für eine SAML 2-Antwort mit Ausstellerelement

Die folgende SAML 2-Antwort verwendet *Aussteller* Element.

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
    ...
  </saml:Assertion></samlp:Response>
```

Beispiel für eine SAML 2-Antwort mit den Elementen SubjectConfirmation und SubjectConfirmationData

Die folgende SAML 2-Antwort verwendet *SubjectConfirmation* Und *SubjectConfirmationData* Elemente mit *Nicht OnOrAfter* Und *Empfänger* Attribute.

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:Subject
ConfirmationData InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 NotOnOrAfter="2012-01-30T20:17:10Z"
 Recipient="https://demoi2.service-now.com/navpage.do"/></saml:SubjectConfirmation>
```

Beispiel für eine SAML 2-Antwort mit den Elementen „AudienceRestrictions“ und „Zielgruppe“

Die folgende SAML 2-Antwort verwendet *AudienceRestrictions* Und *Zielgruppe* Elemente mit *Nicht vorher* Und *Nicht OnOrAfter* Attribute.

```
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
```

SAML-Anwenderbereitstellung

Wenn Anwender in Ihrem IdP vorhanden sind, sich aber nicht in Ihrer Instanz befinden, kann die SAML-Anwenderbereitstellung die Anwender automatisch in der Anwendertabelle [sys_user] Ihrer Instanz erstellen.

Die SAML-Anwenderbereitstellung wird für SAML 2,0 Update 1 unterstützt, wenn Multi-SSO aktiviert ist.

Funktionsweise der SAML-Anwenderbereitstellung

Wenn die SAML-Anwenderbereitstellung aktiviert ist und das System einen neuen Anwender empfängt, der sich nicht in der Instanz befindet, erstellt die Instanz automatisch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einen Datensatz in einer temporären Tabelle mit dem Namen u_imp_saml_user_<suffix> , Wo <suffix> Ist ein automatisch generierter Textbezeichner. Das System erstellt auch eine Transformationszuordnung, die die Datenbeziehungen zwischen der Importtabelle und der Anwendertabelle angibt. Jeder im System identifizierte IdP hat eine eigene Transformationszuordnung. Die Transformationszuordnung wird einmal für jeden IdP erstellt. Administratoren können sie nach Bedarf aktualisieren.

Wenn sich der Anwender anmeldet, greift er auf einen IdP zu, um sich anzumelden.

- Das System zeigt eine Liste aller IDPs an, die die SAML-Anwenderbereitstellung verwenden können. Wenn nur ein IdP vorhanden ist, der die SAML-Anwenderbereitstellung verwenden kann, wird dieser automatisch verwendet.
- Wenn keine der obigen Bedingungen wahr ist, verwendet das System IdP automatisch umleiten .

Verwalten Sie die SAML-Anwenderbereitstellung

Aktualisieren Sie die Anwendertabelle mit den Anwendern in Ihrem IdP, indem Sie zuerst die Feldzuordnung einrichten und dann die Anwenderbereitstellung über Multi-SSO-IdP-Einstellungen aktivieren.

Vorbereitungen

Richten Sie Ihre IdP-Zuordnung ein, um zu identifizieren, welche Felder im IdP den richtigen Feldern in der Anwendertabelle zugeordnet sind.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Eigenschaften**an.
2. Wählen Sie Aus **Aktivieren Sie das automatische Importieren von Anwendern aus allen Identitätsanbietern in die Anwendertabelle** (*glide.authenticate.multisso.user.autoprovision*), um diese Funktion zu aktivieren.
3. Klicken Sie auf **Speichern**.
4. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an.
5. Öffnen Sie den Identitätsanbieter-Datensatz, den Sie verwenden möchten.
6. Erstellen Sie einen Datensatz in der Anwendertabelle, wenn der Anwender noch nicht vorhanden ist, indem Sie auswählen **Anwender automatisch bereitstellen** .
   Wenn Sie auf dieses Release aktualisiert haben, müssen Sie das Formular konfigurieren und dieses Feld hinzufügen.
7. Aktivieren Sie die Aktualisierung von Anwenderdatensätzen, wenn sich Anwender beim IdP anmelden und die Informationen im IdP mit den Informationen in der Anwendertabelle veraltet sind, indem Sie auswählen **Aktualisieren Sie Den Anwenderdatensatz Bei Jeder Anmeldung** .
   Wenn Sie auf dieses Release aktualisiert haben, müssen Sie das Formular konfigurieren und dieses Feld hinzufügen.
8. Klicken Sie Auf **Anwenderbereitstellung – Transformationszuordnung** Um die vom System automatisch erstellte Karte anzuzeigen.
9. Nehmen Sie bei Bedarf Änderungen an der Karte vor.

Ergebnis

Wenn die ersten unbekannten Anwender versuchen, sich anzumelden, erstellt das System die Felder in der Importsatztabelle aus der Datei metadata.xml.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können die Felder aus der IdP-Tabelle erst zuordnen, wenn sich dieser erste Anwender anmeldet.

SAML 2,0-Fehlerbehebung

Bevor Sie sich an den Support wenden, probieren Sie die Problembehandlungslösungen aus, die in der Knowledge Base unter Hallo verfügbar sind.

Hinweis: Die Instanz unterstützt keine Lösungen, die von externen Sites bereitgestellt werden.

Siehe folgenden Knowledge Base-artikel: KB0540617 „“„SAML-Fehlermatrix““ .

Andere Häufige Probleme

Fehler oder Symptom	Lösung
Fehlermeldung: „Ist keine Funktion.“ Dieses Problem kann in einer Umgebung mit mehreren Knoten auftreten. Wenn das Plugin nicht auf allen Knoten aktiviert wird, wird ein Fehler wie der folgende angezeigt: Org.mozilla.javascript.EcmaFehler: `[JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder]`ist keine Funktion.	Dieser Fehler tritt auf, da das Plugin nicht aktiv war und die JAR-Datei nicht geladen wurde. Daher scheint der Code zu fehlen. Wenden Sie sich an den technischen Support, um Knoten neu zu starten, denen das Plugin fehlt.
SAML authentifiziert keine Anwender, die auf CMS-Seiten zugreifen.	Standardmäßig sind CMS-Seiten öffentlich und erfordern daher keine Authentifizierung. Wenn SAML CMS-Seiten authentifizieren soll, ändern Sie *View_content.do* Öffentliche Seite von *Aktiv=wahr* Bis *Aktiv=falsch* .
Ein Anwender kann nach der SAML-Authentifizierung nicht zu einer CMS-Seite zurückgeleitet werden.	Standardmäßig verwendet die SSO-Integration einen URL-Parameter namens *URI* Dient zur Steuerung, wohin der Anwender nach der Authentifizierung am IdP geleitet wird. SSO ignoriert relative URLs. Beispielsweise kann SSO Anwender nicht zu einem umleiten */ess* Relative URL. Stattdessen muss der Anwender zu einer URL wie navigieren */ NAV_to.do?URI=/ess* , Die Deep-Linking-Syntax verwendet. Dadurch wird das ESS-Portal jedoch in den iFrame des Hauptnavigationsinhalts eingefügt. Mit anderen Worten: Die Website nimmt nicht die ganze Seite ein, sondern wird als Seite in Ihrer Instanz geladen. Weitere Informationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere Häufige Probleme (Fortsetzung)

Fehler oder Symptom	Lösung
	finden Sie unter CMS-Sites und Single Sign-on. Wenn Sie die CMS-Eintragsseite ändern, um sie durch Einstellung privat zu machen *View_content.do* Bis *Aktiv=falsch* , Deep-Linking-Verhalten erfordert dann eine Anpassung an *Installation Beenden* Anmeldeskript. Erstellen Sie ein Skript, das nach sucht *URI* Teil der URL und erstellt einen *RelayStatus* URL-Parameter, der den relativen URL-Pfad zur Weiterleitung von Anwendern nach der Authentifizierung am IdP enthält.
SAML leitet Anwender nach der Authentifizierung nicht zur entsprechenden Seite um.	Bestimmen Sie, ob der Relaisstatus an den IdP übergeben und dann während der Authentifizierung zurückgegeben wird. Sie können dies mit einem Browser tun, der HTTP-Anforderungsheader und Informationen speichern kann, z. B. Chrome mit seinen integrierten Entwicklertools oder Firefox mit dem Add-on HTTPfox. Verwenden Sie für Internet Explorer eine Drittanbieteranwendung wie Fiddler. Das Ziel besteht darin, zu beobachten, wie die Anforderungen vom Client (Browser) an die Instanz und vom Client an den IdP übergeben werden.

Überwachen Sie die Ereigniswarteschlange auf Anmeldeaktivitäten

Jede Single Sign-on-Integration erstellt Ereignisse für Anmeldeaktivitäten.

Sie können diese Ereignisse verwenden, um Anmeldefehler zu überwachen und festzustellen, ob Sicherheitsbedenken behoben werden müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen der Ereigniswarteschlange auf Anmeldefehler

Ereignisname	Beschreibung	Datensatz	Parameter 1	Parameter 2
external.authentication.succeeded	Externe Authentifizierung erfolgreich, und der Anwender hat auf die Instanz-URL zugegriffen.	Sitzungs-ID	Anwender-ID des Anwenders, der sich erfolgreich angemeldet hat	Die URL, auf die der Anwender zugegriffen hat (kann ein Deep-Link sein)
external.authentication.failed	Die Single Sign-on-Anforderungen sind nicht vorhanden oder fehlen.		Sitzungs-ID	Die fehlenden Authentifizierungsanforderungen
external.authentication.failed	Der Anwender ist im Anwender nicht vorhanden [sys_user] Tabelle		Anwender-ID	Die Zeichenfolge „Anwender ist nicht vorhanden“
external.authentication.failed	Der Anwender ist gesperrt.		Anwender-ID	Die Zeichenfolge „Anwender gesperrt“.

Anmeldereignisse für Ereigniswarteschlange

Die SAML 2,0-Integration erstellt Ereignisse für Anmeldeaktivitäten.

Sie können diese Ereignisse verwenden, um Anmeldefehler zu überwachen und festzustellen, ob Sicherheitsbedenken behoben werden müssen.

Ereignisse für Anmeldeaktivitäten

Ereignisname	Beschreibung	ID, die mit dem Ereignis verwendet wird	Ereigniszeichenfolge
saml2.logout.validieren.fehlgeschlagen	Die Abmeldeantwort vom IdP konnte für Ihre Abmeldeanforderung nicht validiert werden. Das Ereignis validiert das <inResponseTo>-Element anhand der Sitzungs-ID (ID-Attribut des <saml2p:LogoutRequest>-Elements). Sehen Sie sich beispielsweise den Workflow für die ausgestellte Abmeldeanforderung an.	Sitzungs-ID	Die Zeichenfolge „SAML2 LogoutResponse-Validierung fehlgeschlagen.“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignisse für Anmeldeaktivitäten (Fortsetzung)

Ereignisname	Beschreibung	ID, die mit dem Ereignis verwendet wird	Ereigniszeichenfolge
external.authentication.succeeded	Externe Authentifizierung erfolgreich.		Die Zeichenfolge „Authentifizierung erfolgreich“
external.authentication.succeeded	Externe Authentifizierung erfolgreich, und der Anwender hat auf die Instanz-URL zugegriffen.	Sitzungs-ID und Anwender-ID des Anwenders, der sich erfolgreich angemeldet hat	Die URL, auf die der Anwender zugegriffen hat (kann ein Deep-Link sein)
external.authentication.failed	Die Single Sign-on-Anforderungen sind nicht vorhanden oder fehlen.	Sitzungs-ID	Die fehlenden Authentifizierungsanforderungen
external.authentication.failed	Der Anwender ist in der Anwendertabelle [sys_user] nicht vorhanden.	Anwender-ID	Die Zeichenfolge „Anwender ist nicht vorhanden“
external.authentication.failed	Der Anwender ist gesperrt.	Anwender-ID	Die Zeichenfolge „Anwender gesperrt“

Eingehende und ausgehende OAuth-Authentifizierung

Die OAuth-basierte Authentifizierung validiert die Identität des Clients, der versucht, mithilfe eines Authentifizierungsprotokolls eine Vertrauensbasis für das System herzustellen.

OAuth 2,0 – offene Autorisierung ist das branchenübliche Autorisierungsprotokoll, das die Einfachheit von Cliententwicklern berücksichtigt und gleichzeitig spezifische Autorisierungs-Flows für Webanwendungen, Desktop-Anwendungen und Mobilgeräte bereitstellt.

Es handelt sich um einen Standard, der es einer Website oder Anwendung ermöglicht, auf Ressourcen zuzugreifen, die von anderen Web-Apps im Namen eines Anwenders gehostet werden.

Anstatt die Anmeldeinformationen des Ressourcenanwenders für den Zugriff auf geschützte Ressourcen zu verwenden, erhält der Client ein Zugriffstoken. Zugriffstoken werden mit Genehmigung des Anwenders an Drittpartei-Clients ausgegeben. Der Client verwendet dann das Zugriffstoken, um auf die geschützten Ressourcen zuzugreifen.

In Zürich können Sie die OAuth-Integration mit den folgenden Erweiterungen konfigurieren:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erhöhen Sie die Länge des geheimen Clientschlüssels auf 2048 Zeichen, um die Sicherheitsanforderungen von Drittparteisystemen wie Azure DevOps (ADO) zu erfüllen.
- Geben Sie eine JSON-Webschlüsselsatz-URL (JWKS) an, um den öffentlichen Schlüssel für die JSON-Webtoken (JWT)-Signaturvalidierung automatisch zu verwalten und zu aktualisieren.
- Fordern Sie OAuth-Token mit dem JWT-Gewährungstyp an, der mit Enhanced Security (es)-Algorithmen signiert ist.
- Konfigurieren Sie einen eindeutigen Bezeichner für JWT-Token.

Eingang

Erstellen Sie einen Endpunkt für externe Clients, die auf Ihre Instanz zugreifen möchten. Dadurch wird ein OAuth-Client-Anwendungsdatensatz erstellt und eine Client-ID und ein geheimer Client generiert, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt. Weitere Informationen finden Sie unter OAuth eingehend.

Ausgehend

Verwenden Sie einen OAuth-Drittanbieter, der die Autorisierung für den Zugriff auf Ihre Instanz bereitstellt. Geben Sie ein OAuth-Profil und einen OAuth-Bereich an, wenn Sie eine Verbindung zu einem anderen OAuth-Provider herstellen. Weitere Informationen finden Sie unter OAuth ausgehend.

OAuth 2.0

Mit OAuth 2,0 können Anwender über externe Clients auf Instanzressourcen zugreifen, indem sie ein Token abrufen, anstatt bei jeder Ressourcenanforderung Anmeldeinformationen einzugeben.

Sie müssen über die Rolle „Security_admin“ verfügen, um die OAuth-Integration zu verwalten. Konfigurieren Sie OAuth 2,0 für die folgenden Szenarien:

- **Szenario des externen OAuth-Clients** (Eingehend): Ihre Instanz stellt einen Endpunkt für Drittpartei-Clients bereit, um Daten aus der Instanz abzurufen.
- **OAuth-Anbieterszenario** (Ausgehend): Ihre Instanz ruft Daten von einem Drittanbieter ab.

Hinweis: Sie müssen sich zum ersten Mal vom Anwender authentifizieren, um den Token-Post abzurufen. Sie müssen sich vor Ablauf des Tokens nicht mit einem Anwenderaccount authentifizieren.

Sowohl einfache Sicherheits- als auch Hochsicherheits-Frameworks unterstützen OAuth 2,0. Hohe Sicherheit wird empfohlen. Unter finden Sie Informationen darüber, welche Versionen mit hoher Sicherheit bereits aktiv sind und wie hohe Sicherheit aktiviert werden kann.

Schlüsselkonzepte der OAuth 2,0-Implementierung

Konzept	Beschreibung
Ressourcenbesitzer	Eine Entität, die Zugriff auf eine geschützte Ressource gewähren kann. Ein Ressourcenbesitzer, der eine Person ist, wird als bezeichnet *Endanwender* . Der Ressourcenbesitzer ist immer ein Anwenderaccount.
Client	Eine Anwendung, die mit der Autorisierung des Ressourcenbesitzers Anforderungen für geschützte Ressourcen im Namen des Ressourcenbesitzers stellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konzept	Beschreibung
Ressourcenserver	Der Server, der die geschützten Ressourcen hostet und Anforderungen für geschützte Ressourcen annehmen und beantworten kann.
Autorisierungsserver	Der Server, der Zugriffstoken für den Client ausgibt, nachdem der Ressourcenbesitzer erfolgreich authentifiziert und die Autorisierung erhalten wurde.
Autorisierungsanforderung	Die Berechtigung, die ein Client für den Zugriff auf eine geschützte Ressource benötigt. Die Autorisierungsanforderung ist immer eine HTTP-POST-Nachricht, die die ID des Clients enthält, der im Namen des Ressourcenbesitzers handelt, und Anmeldeinformationen, die die Anforderung autorisieren.
Autorisierungsgewährung	Eine Anmeldeinformation, die die Autorisierung des Ressourcenbesitzers für den Zugriff auf eine Ressource darstellt. Die Autorisierungsgewährung ist entweder Anmeldeinformationen für die Anwenderanmeldung oder ein Aktualisierungstoken.
Zugriffstoken	Eine sichere Zeichenfolge, die ein Client für den Zugriff auf geschützte Ressourcen verwendet. Eine Instanz stellt Zugriffstoken für Clients aus, die über eine gültige Autorisierungsgewährung verfügen. Jedes Zugriffstoken hat einen bestimmten Umfang, eine bestimmte Lebensdauer und andere Attribute. Standardmäßig gibt eine Instanz Zugriffstoken mit einer Lebensdauer von 30 Minuten aus, wenn die Instanz der OAuth-Anbieter ist. Für Drittpartei-Token 30 Tage.
Token neu laden	Anmeldeinformationen, die ein Client verwendet, um neue Zugriffstoken zu erhalten, ohne dass eine zusätzliche Anwenderautorisierung erforderlich ist. Eine Instanz gibt ein Aktualisierungstoken für einen Client aus, wenn er zum ersten Mal berechtigt ist, ein Zugriffstoken zu haben. Standardmäßig gibt eine Instanz Aktualisierungstoken mit einer Lebensdauer von 100 Tagen aus, wenn die Instanz der OAuth-Anbieter ist. Für Drittpartei-Token 365 Tage.
Selbstsignierte Zertifikate	Die ServiceNow AI Platform Unterstützt keine selbstsignierten Zertifikate. Der OAuth-Client verwendet nicht den Zertifikatvertrauensspeicher oder lässt keine Verbindung zu OAuth-Endpunkten zu, die ein selbstsigniertes Zertifikat enthalten.
Anwenderagent	Der Anwender, der Zugriffsrechte für eine Client-Anwendung delegiert, bei der es sich häufig um eine Website handelt. Die Zugriffsrechte ermöglichen es der Client-Anwendung oder -Website, auf Daten in der Instanz zuzugreifen, für die der Anwender Zugriffsrechte hat. Der Anwender-Agent wird im Szenario verwendet.

OAuth-Gewährungstypen

A *Gewährungstyp* Ist die Art und Weise, wie der Client das Zugriffstoken erhält. Die folgenden Gewährungstypen werden unterstützt:

- **Autorisierungscode** : Der Verbraucher erhält zuerst einen Autorisierungscode und verwendet ihn dann, um ein Zugriffstoken zu erhalten. Sie können Geben Sie ein OAuth-Profil an Und geben Sie diesen Gewährungstyp an. Der Prozess, der den Autorisierungscode verwendet, wird auch als bezeichnet *Authentifizierungscode-Flow* Oder *Autorisierungscode-Flow* .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Passwortanmeldeinformationen des Ressourcenbesitzers** : Der Verbraucher der Ressource verfügt bereits über die Anwenderanmeldeinformationen zum Abrufen des Zugriffstoken. Dieser Prozess wird auch als bezeichnet *Passwort-Flow* .
- **Client-Anmeldeinformationen** : Der Verbraucher der Ressource verwendet die Client-ID und das geheime Clientgeheimnis, die bereits in der Anwendungsregistrierung konfiguriert sind.

Speicherung der Anmeldeinformationen für die Authentifizierung

Das geheime OAuth-Client-Geheimnis wird als gespeichert `password2`Typfeld, das mit KMF verschlüsselt ist. Anwenderpasswörter, die zum Überprüfen eingehender Endpunktanforderungen verwendet werden, werden als Hash-Wert in der Anwendertabelle in einem gespeichert `password`Typfeld (SHA 256). Weitere Informationen zu dieser Verschlüsselung finden Sie unter Passwort2-Verschlüsselung mit KMF

Richten Sie OAuth ein

Richten Sie OAuth ein und aktivieren Sie sie, aktivieren Sie die OAuth-Systemeigenschaft, erstellen Sie einen OAuth-Anwendungsendpunkt für externe Client-Anwendungen, um auf die Instanz zuzugreifen, und legen Sie OAuth-Parameter fest.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Stellen Sie sicher, dass OAuth-Plugin Ist aktiv und OAuth-Aktivierungseigenschaft Ist auf „wahr“ festgelegt.
2. Erstellen Sie eine OAuth-Anwendungsregistrierung mit einer der folgenden Methoden:
   - Erstellen Sie einen Endpunkt für externe Clients Die auf Ihre Instanz zugreifen möchten. Dadurch wird ein erstellt **OAuth-Client-Anwendung** Zeichnen Sie eine Client-ID und ein geheimes Clientgeheimnis auf, die der Client für den Zugriff auf die eingeschränkten Ressourcen in der Instanz benötigt.
   - Verwenden Sie einen OAuth-Drittanbieter Die die Autorisierung für den Zugriff auf Ihre Instanz bereitstellt.

     Geben Sie ein OAuth-Profil an Und Geben Sie einen OAuth-Bereich an Wenn Sie eine Verbindung zu einem anderen OAuth-Provider herstellen.
3. Konfigurieren Sie Ihre Client-Anwendungen, um einen HTTP-POST ZU erstellen, der ein OAuth-Token anfordert.
   Die Anwendung muss auch die JSON-Antwort analysieren können, um das zurückgegebene Zugriffstoken und das Aktualisierungstoken zu verwenden.

Aktivieren Sie OAuth

Standardmäßig ist **OAuth 2,0 (com.snc.platform.security.oauth)** Plugin ist in neuen und aktualisierten Instanzen aktiv. Wenn das Plugin in Ihrer Instanz nicht aktiv ist, können Sie es aktivieren.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Legen Sie die OAuth-Eigenschaft fest

Um OAuth 2,0-Token für registrierte Anwendungen zu generieren, die com.snc.platform.security.oauth.is.active Eigenschaft muss für die Instanz aktiv sein.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Um OAuth 2,0 zu verwenden, geben Sie ein **sys_properties.list** Wählen Sie im Navigator aus **Neu** . Sie können auch die Liste der Systemeigenschaften öffnen, indem Sie zu navigieren **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** > an.
2. Füllen Sie das Formular mit den folgenden Einstellungen aus:

   - **Name** : com.snc.platform.security.oauth.is.active
   - **Typ**: true | false
   - **Wert**: true

Ändern Sie den OAuth-Passwortparameter

Verwenden Sie diese Eigenschaft, um sicherzustellen, dass nur POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert werden.

Das Senden vertraulicher Informationen über URI-Abfrageparameter kann dazu führen, dass Clients, der Server oder ein beliebiger Host zwischen den Anforderungen vertrauliche Informationen offenlegen. Ab dem Madrid-Release stellt diese neue Eigenschaft sicher, dass nur die POST-Textparameter als Eingabe für alle unterstützten Gewährungstypen akzeptiert werden. Unterstützte Gewährungstypen sind:

- Autorisierungscode
- Passwort
- Client-Anmeldeinformationen
- Aktualisierungstoken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametereigenschaft für OAuth-Passwort

Eigenschaft	Beschreibung
glide.oauth.allow.parameters.in.post.body.only	Diese Eigenschaft ist nur für zBoots als Teil des OAuth 2,0-Plugins auf „wahr“ festgelegt. Wenn Sie diese Einstellung für Ihre Instanz benötigen, erstellen Sie, und legen Sie die Eigenschaft auf „wahr“ fest.

OAuth eingehend

Die eingehende OAuth-Authentifizierung ermöglicht vertrauenswürdigen externen Anwendungen den sicheren Zugriff auf ServiceNow-APIs, wodurch kontrollierte und autorisierte Verbindungen sichergestellt werden.

Sie müssen über eine der folgenden Rollen verfügen, um OAuth-Integrationen im System zu konfigurieren oder zu verwalten:

- oauth_admin
- Mi_admin
- admin

Die eingehende Authentifizierung ermöglicht externe Anwendungen wie Drittparteisysteme oder andere ServiceNow® Instanzen, mit denen eine sichere Verbindung hergestellt werden soll ServiceNow APIs. Die eingehende Authentifizierung bestätigt, dass nur vertrauenswürdige Clients kontrolliert und sicher auf Ihre ServiceNow-Instanz zugreifen können. ServiceNow Unterstützt mehrere OAuth 2,0-Gewährungstypen, die jeweils für bestimmte Integrationsszenarien konzipiert sind. Verwenden Sie die folgenden Informationen, um den Gewährungstyp auszuwählen, der am besten zu Ihrem Anwendungsfall passt:

Autorisierungscode-Gewährung

Ideales Nutzungsszenario	Funktionalität
Anwendungen, die im Namen des Anwenders mit Zustimmung des Anwenders auf Anwenderdaten zugreifen müssen. Beispiel: Web-, Mobile- oder Desktop-Anwendungen, die im Namen eines Anwenders handeln.	Der Anwender initiiert den Anmeldeprozess von der Client-Anwendung aus, die ihn an eine umleitet ServiceNow Anmeldeseite. Nachdem sich der Anwender angemeldet hat und seine Zustimmung erteilt hat, erhält die Client-Anwendung einen Autorisierungscode. Die Client-Anwendung tauscht den Autorisierungscode mit aus ServiceNow Instanz für ein Zugriffstoken. Die Autorisierungscodegewährung ist der sicherste und am häufigsten verwendete Workflow für anwenderorientierte Integrationen. Es unterstützt sowohl vertrauliche Clients (mit einem geheimen Client) als auch öffentliche Clients, die den Nachweisschlüssel für Code Exchange (PKCE) verwenden.

Weitere Informationen zum Workflow und zur Konfiguration der Autorisierungscodegewährung finden Sie unter Autorisierungscodegewährung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Client-Anmeldeinformationen Gewähren

Ideales Nutzungsszenario	Funktionalität
Client-Anwendungen wie Back-End-Services oder automatisierte Systemintegrationen, auf die zugegriffen werden muss ServiceNow APIs ohne Anwenderbeteiligung.	Die Client-Anwendung authentifiziert sich direkt bei ServiceNow Instanz mit eigenen Anmeldeinformationen (Client-ID und Geheimnis). Nach der Authentifizierung erhält die Anwendung ein Zugriffstoken für den Zugriff auf ServiceNow APIs.

Weitere Informationen zum Workflow und zur Konfiguration von Client-Anmeldeinformationen finden Sie unter Gewährung von Client-Anmeldeinformationen.

Drittpartei-ID-Token-Flow

Ideales Nutzungsszenario	Funktionalität
Verbundauthentifizierungsszenarien, wo ServiceNow Vertraut auf Identitäts- oder Zugriffstoken, die von externen Identitätsanbietern wie ausgestellt wurden Azure AD oder Okta.	Die Clientanwendung ruft eine ID oder ein Zugriffstoken von einem vertrauenswürdigen Drittanbieter von Identitäten ab und fügt sie in den Autorisierungsheader ein, wenn API-Anforderungen an den gestellt werden ServiceNow Instanz. ServiceNow Validiert das Token und gewährt, wenn vertrauenswürdig, Zugriff basierend auf der von ihm bestätigten Identität. Dies ermöglicht nahtloses Single Sign-on (SSO) und die systemübergreifende Verbundauthentifizierung.

Weitere Informationen zum Flow und zur Konfiguration von Drittpartei-Token finden Sie unter Drittpartei-Tokengewährung.

JWT-Bearer-Gewährung

Ideales Nutzungsszenario	Funktionalität
Client-Anwendungen, die sicheren Zugriff auf benötigen ServiceNow Ressourcen, entweder im Namen eines Anwenders oder als sich selbst, ohne Anwenderinteraktion oder Speicherung eines gemeinsam genutzten Geheimnisses zu erfordern. Die Clientanwendung erstellt ein signiertes JSON-Webtoken (JWT), das identitätsbezogene Ansprüche enthält, z. B. den Anwender oder das System, das sie darstellt. Dann wird sie dem angezeigt ServiceNow Instanz, um das Zugriffstoken anzufordern.	**Wenn Sie im Namen eines Anwenders handeln:** Das Token stellt einen zuvor authentifizierten Anwender dar. Dies ermöglicht einen sicheren, nahtlosen Zugriff, ohne den Anwender erneut zur Eingabe von Anmeldeinformationen oder Einwilligung aufzufordern. Das signierte Token bestätigt die Identität des Anwenders, wodurch aktiviert wird ServiceNow Um der Anforderung zu vertrauen, ohne dass eine Echtzeitinteraktion des Anwenders erforderlich ist. **Wenn Sie als sich selbst agieren:** Das Token identifiziert und authentifiziert die Client-Anwendung direkt. Anstatt ein gemeinsames Geheimnis zu verwenden, signiert der Client das Token mit einem privaten Schlüssel, was es zu einer sichereren Alternative zur Gewährung von Client-Anmeldeinformationen macht.

Weitere Informationen zum Workflow und zur Konfiguration der JWT-Bearer-Gewährung finden Sie unter JSON-Webtoken-Bearer-Gewährung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuteilung Von Passwortanmeldeinformationen Des Ressourcenbesitzers

Ideales Nutzungsszenario	Funktionalität
Sehr vertrauenswürdige interne Client-Anwendungen in kontrollierten Umgebungen, in denen die App die Anmeldeinformationen des Anwenders direkt erfasst.	Die Client-Anwendung erfasst den Anwendernamen und das Passwort des Anwenders und leitet sie an den weiter ServiceNow Instanz zum Abrufen eines Zugriffstoken. Der Workflow umgeht Umleitungs- und Einwilligungsbildschirme, stellt der Client-Anwendung jedoch Anwenderanmeldeinformationen zur Verfügung. ServiceNow Empfiehlt, dass Sie die Zuteilung von Passwortanmeldeinformationen für den Ressourcenbesitzer nur in Legacy- oder kontrollierten Umgebungen implementieren.

Weitere Informationen zum Workflow und zur Konfiguration von Passwortanmeldeinformationen des Ressourcenbesitzers finden Sie unter Zuteilung der Passwortanmeldeinformationen des Ressourcenbesitzers.

Implizite Zuschüsse

Ideales Nutzungsszenario	Funktionalität
Legacy-einseitige Anwendungen (SPAs) oder browserbasierte Apps, die ein geheimes Clientgeheimnis nicht sicher speichern können und einen schlanken, clientseitigen Authentifizierungs-Flow erfordern.	Der Anwender meldet sich über einen Browser an. Die Clientanwendung empfängt das Zugriffstoken nach der Anmeldung direkt in der URL, wobei der Schritt des Zwischen-Autorisierungscodes umgangen wird. Dieser Flow wurde ursprünglich für öffentliche Clients konzipiert, die vollständig im Browser ausgeführt werden, bei denen das sichere Speichern von Geheimnissen nicht möglich ist. Die Implementierung wird zwar vereinfacht, aber Token werden im Browser bereitgestellt, was das Abfangerrisiko erhöht. Für mehr Sicherheit ServiceNow Empfiehlt die Implementierung einer Autorisierungscodegewährung mit PKCE.

Weitere Informationen zum Workflow und zur Konfiguration impliziter Zuschüsse finden Sie unter Implizite OAuth-Berechtigungen.

OAuth-Bereiche

Sie können den Umfang der Unterstützung des OAuth-Authentifizierungsbereichs für DIE REST-API erweitern. Der OAuth-Bereich bietet nur Zugriff auf die bestimmten REST-APIs. Weitere Informationen finden Sie unter REST-API-Authentifizierungsbereich.

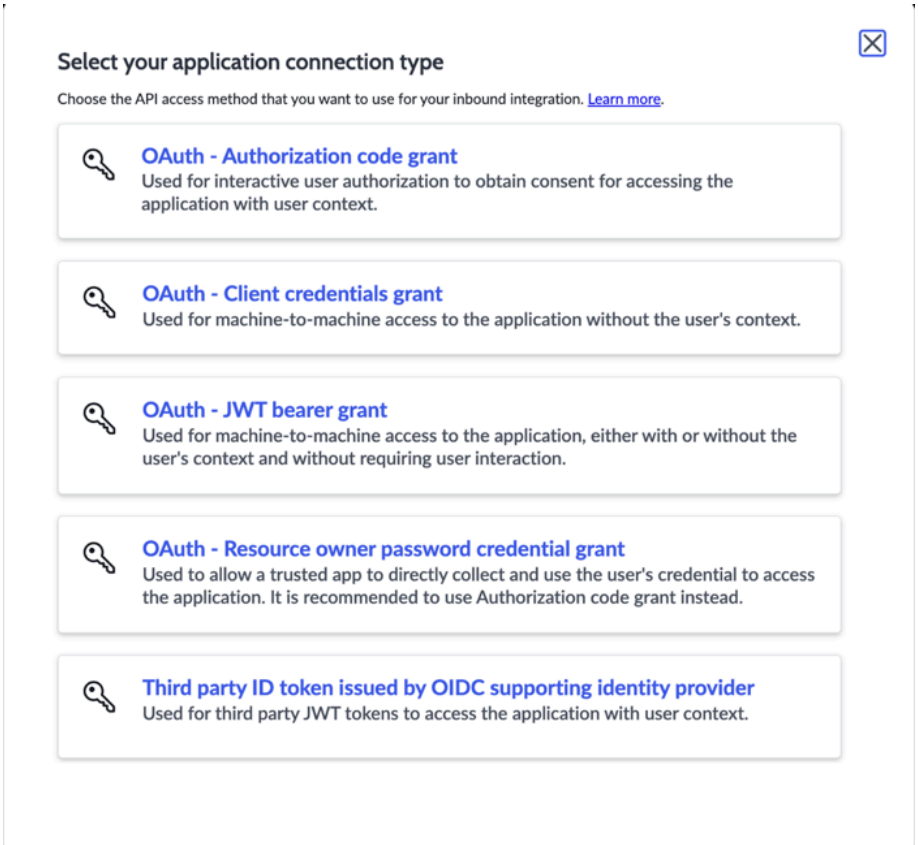
Neue Experience für eingehende Integrationen

Der neue eingehende Integrations-Workflow in der ServiceNow Die Machine Identity Console bietet eine erweiterte Experience für die Verwaltung eingehender Integrationen.

Methoden für eingehende Integrationen

Navigieren Sie in der -Instanz zu **Alle** > **Rechneridentitätskonsole** > **Eingehende Integrationen** > **Neue Integration**an. Wählen Sie den Anwendungsverbindungstyp (Gewährungstyp) aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Weitere Informationen zu den verschiedenen Gewährungstypen und ihrer Konfiguration finden Sie in den folgenden Themen:

- Autorisierungscodegewährung
- Gewährung von Client-Anmeldeinformationen
- JSON-Webtoken-Bearer-Gewährung
- Zuteilung der Passwortanmeldeinformationen des Ressourcenbesitzers
- Drittpartei-Tokengewährung

Autorisierungscodegewährung

Die OAuth-Autorisierungscodegewährung ist ein sicherer und weit verbreiteter Flow für Web-, Mobile- oder Desktop-Apps, die mit Zustimmung des Anwenders auf Anwenderdaten zugreifen. Es unterstützt sowohl private Clients (mit einem geheimen Client) als auch öffentliche Clients (mit PKCE).

Im Flow „Autorisierungscode-Gewährung“ ServiceNow Fungiert sowohl als Autorisierungsserver (für die Verarbeitung der Anwenderauthentifizierung und Tokenausgabe) als auch als Ressourcenserver (Hosting der APIs). Wenn SSO aktiviert ist, ServiceNow Leitet den Anwender zur Authentifizierung an den konfigurierten Identitätsanbieter (Configured Identity Provider, IdP) weiter. Nachdem der IdP den Anwender erfolgreich authentifiziert hat, kehrt die Steuerung zu zurück ServiceNow, Der dann den Autorisierungscode ausgibt. Dieser Prozess stellt sicher, dass auch bei externer Authentifizierung ServiceNow Bleibt die Autorität für die Ausgabe von Token und die Verwaltung des API-Zugriffs.

Hinweis: Wenn Sie Ihren eigenen Identitätsanbieter verwenden möchten (z. B. Azure AD oder Okta) Erwägen Sie als Autorisierungsserver die Verwendung von Drittpartei-Tokengewährung Flow.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Workflow zur Autorisierungscodegewährung

Konfigurieren Sie eine OAuth-Autorisierungscodegewährung

Workflow zur Autorisierungscodegewährung

Die OAuth-Autorisierungscodegewährung ist ein sicherer und weit verbreiteter Flow für Web-, Mobile- oder Desktop-Apps, die mit Zustimmung des Anwenders auf Anwenderdaten zugreifen. Es unterstützt sowohl private Clients (mit einem geheimen Client) als auch öffentliche Clients (mit PKCE).

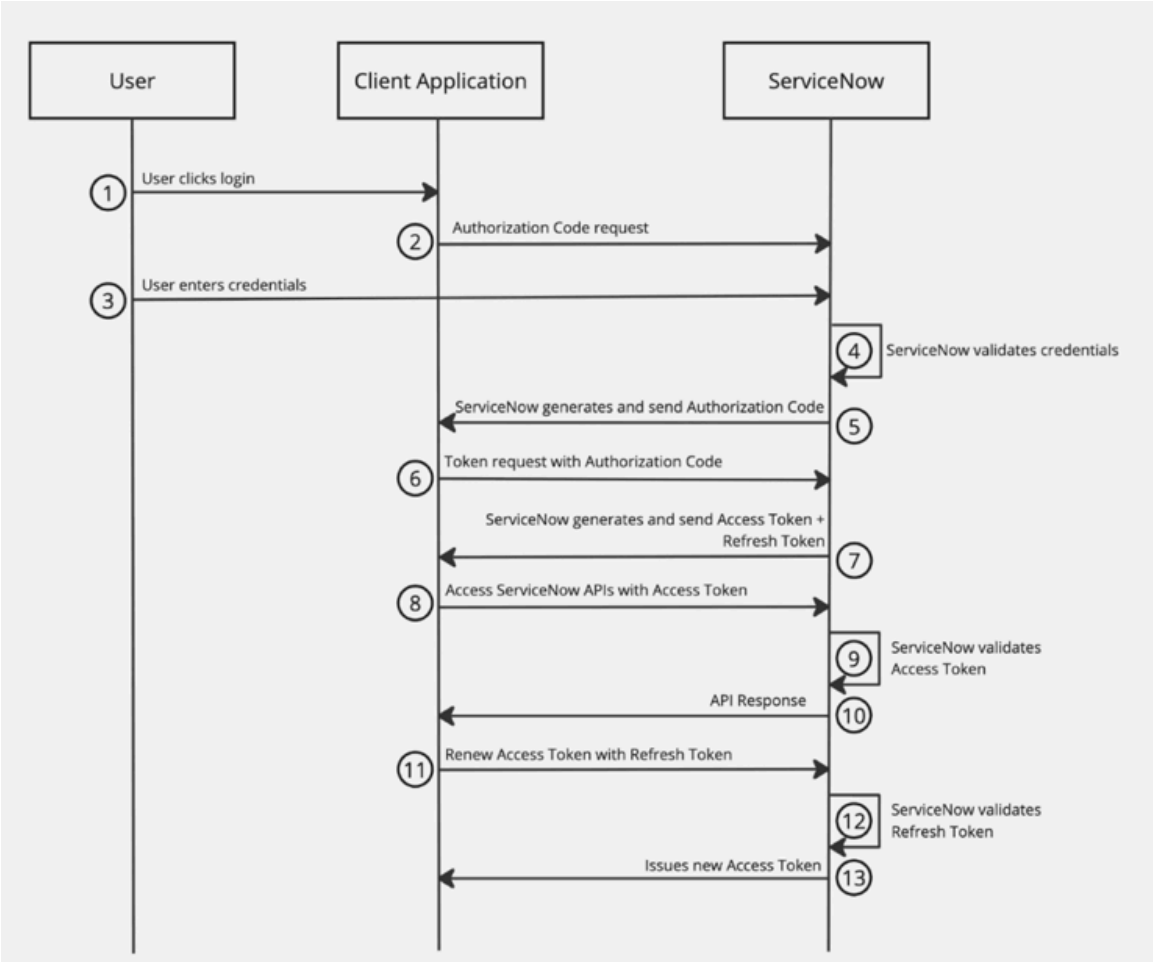
Vorbereitungen

Erforderliche Rolle: `oauth_admin, mi_admin, admin`

Warum und wann dieser Vorgang ausgeführt wird

Diese Themensammlung enthält Informationen dazu, wie eine Client-Anwendung den Flow Autorisierungscode-Gewährung verwenden kann, um ein Token von ServiceNow abzurufen und API-Aufrufe mit diesem Token durchzuführen. Private Clients verwenden das geheime Clientgeheimnis, während öffentliche Clients die PKCE-Code-Challenge verwenden.

Autorisierungs-Workflow



Prozedur

1. Melden Sie sich über die Client-Anwendung an.

Der Anwender beginnt den Anmeldevorgang über die Client-Anwendungsschnittstelle.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Initiieren Sie die Autorisierungsanforderung.

   Der Client leitet den Anwender zum ServiceNow-Autorisierungs-Endpunkt um. Die Methode zum Initiieren der Autorisierungsanforderung hängt vom Typ des Clients ab: Öffentlich oder privat.

   Öffentliche Clients

   Öffentliche Clients (Beispiel: Mobile oder einseitige Anwendungen) können kein geheimes Clientgeheimnis sicher speichern. Daher müssen sie verwenden **Nachweisschlüssel für Codeaustausch (PKCE)** Um die Sicherheit zu verbessern.

   - Fügen Sie in die Autorisierungsanforderung ein **PKCE-Code-Herausforderung** Und geben Sie an **Code-Abfragemethode** .
   - Während der Tokenanforderung muss der Client den senden **Codeverifizierer** Dient zum Validieren des Autorisierungscodes.

   Führen Sie eine GET-Anforderung an den Autorisierungsendpunkt mit den folgenden Parametern aus:

   ```
   Method: GET
   Endpoint: https://<servicenow_base_url>/oauth_auth.do
   ```

   Autorisierungsanforderungsparameter (öffentlicher Client – PKCE)

Parameter	Erforderlich	Beschreibung
Response_type	Ja	Legen Sie den Wert auf fest `Code` Zum Initiieren des Autorisierungscode-Flows.
client_id	Ja	Der eindeutige Bezeichner für Ihre Client-Anwendung. FORMAT: YOUR_CLIENT_ID
Umleiten_URI	Ja	Der URI, an den ServiceNow den Autorisierungscode sendet. Beispiel: https://yourapp.com/callback
Code_Challenge	Ja	Ein base64url-codierter SHA-256-Hash des Codeverifizierers. Dies wird als Teil des PKCE-Flows verwendet.
Code_Challenge_method	Ja	Gibt die für die Codeabfrage verwendete Transformationsmethode an. Auf festlegen `S256` .
scope	Optional	Eine durch Leerzeichen getrennte Liste der angeforderten Bereiche.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Erforderlich	Beschreibung
		Beispiel: Incident_read Incident_write .
state	Ja	Ein vom Client generierter Wert, der zur Vermeidung von CSRF-Angriffen verwendet wird. Der Wert wird im Umleitungs-URI unverändert zurückgegeben, sodass der Client ihn validieren kann.

Hinweis: Ab Madrid-Release die Systemeigenschaft Glide.oauth.State.Parameter.erforderlich Schreibt die Verwendung von vor status Parameter in den OAuth-Anforderungen. Die status Eigenschaft ist auf festgelegt Wahr Standardmäßig in den neuen Instanzen und Optional In aktualisierten Instanzen. Falls fehlt status Parameter, die Autorisierungsanforderung schlägt fehl, und der folgende Fehler wird angezeigt: Fehlender Statusparameter in Anforderung .

Private Clients

Private Clients (Beispiel: Serverseitige Anwendungen) können ein geheimes Clientgeheimnis sicher speichern und erfordern keine PKCE.

- Die Autorisierungsanforderung wird initiiert, indem der Anwender zum Autorisierungsendpunkt umgeleitet wird. **Es ist keine geheime Clientcodeabfrage oder PKCE-Code erforderlich** In diesem Schritt.
- Während der Tokenanforderung enthält der Client den **Geheimer Clientschlüssel** Zusammen mit **Autorisierungscode** Um das Zugriffstoken zu erhalten.

Führen Sie eine GET-Anforderung an den Autorisierungsendpunkt mit den folgenden Parametern aus:

```
Method: GET
Endpoint: https://<servicenow_base_url>/oauth_auth.do
```

Autorisierungsanforderungsparameter (Private Client-Secret)

Parameter	Erforderlich	Beschreibung
Response_type	Ja	Legen Sie den Wert auf fest Code Zum Initiieren des Autorisierungscode-Flows.
client_id	Ja	Der eindeutige Bezeichner für Ihre Client-Anwendung. FORMAT: YOUR_CLIENT_ID
Umleiten_URI	Ja	Der URI, an den ServiceNow den Autorisierungscode sendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Erforderlich	Beschreibung
		Beispiel: https://yourapp.com/callback
scope	Optional	Eine durch Leerzeichen getrennte Liste der angeforderten Bereiche. Beispiel: Incident_read Incident_write .
state	Ja	Ein vom Client generierter Wert, der verwendet wird, um Site-übergreifende Angriffe auf Anforderungsfälschung (CSRF) zu vermeiden. Der Wert wird im Umleitungs-URI unverändert zurückgegeben, sodass der Client ihn validieren kann.

3. Melden Sie sich an, und gewähren Sie die Zugriffseinwilligung für die Client-Anwendung.
   Melden Sie sich bei an ServiceNow(Oder IdP, wenn SSO aktiviert ist) und gewähren Sie die Zugriffseinwilligung für die Clientanwendung.
4. ServiceNow(Oder IdP, wenn SSO aktiviert ist) validiert die Anmeldeinformationen und ServiceNow Gibt einen Autorisierungscode an den Client zurück.

   Nach der erfolgreichen Authentifizierung wird der Browser zu weitergeleitet Umleiten_URI , Und der Autorisierungscode ist in der Abfragezeichenfolge enthalten:

   ```
   https://yourapp.com/callback?code=AUTH_CODE&state=xyz123
   ```

5. Initiieren Sie die Autorisierungsanforderung.

   Der Client leitet den Anwender für ein Zugriffstoken zum ServiceNow-Autorisierungs-Endpunkt um. Die Methode zum Initiieren der Autorisierungsanforderung hängt vom Typ des Clients ab: Öffentlich oder privat.

   Öffentliche Clients

   Öffentliche Clients (Beispiel: Mobile oder einseitige Anwendungen) können kein geheimes Clientgeheimnis sicher speichern. Daher müssen sie verwenden **Nachweisschlüssel für Codeaustausch (PKCE)** Um die Sicherheit zu verbessern.

   - Fügen Sie in die Autorisierungsanforderung ein **PKCE-Code-Herausforderung** Und geben Sie an **Code-Abfragemethode** .
   - Während der Tokenanforderung muss der Client den senden **Codeverifizierer** Dient zum Validieren des Autorisierungscodes.

   Der Client sendet eine POST-Anforderung an den Token-Endpunkt mit den folgenden Parametern:

   ```
   Method: POST
   ```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Endpoint: https://<servicenow_base_url>/oauth_token.do
Headers: Content-Type: application/x-www-form-urlencoded
```

Token-Anforderungsparameter (öffentlicher Client-PKCE)

Parameter	Erforderlich	Beschreibung
Grant_type	Ja	Legen Sie den Wert auf fest Authorization_Code Um den Code gegen ein Token auszutauschen.
Code	Ja	Der vom Autorisierungsendpunkt empfangene Autorisierungscode.
Umleiten_URI	Ja	Der in der anfänglichen Autorisierungsanforderung verwendete URI. Beispiel: https://yourapp.com/callback
client_id	Ja	Der eindeutige Bezeichner für Ihre Client-Anwendung.
Code_Verifier	Ja	Die ursprüngliche Zeichenfolge, die zum Generieren der PKCE verwendet wird Code_Challenge .
state	Ja	Ein vom Client generierter Wert, der verwendet wird, um CSRF-Angriffe zu verhindern. Der Wert wird im Umleitungs-URI unverändert zurückgegeben, sodass der Client ihn validieren kann.

Private Clients

Private Clients (Beispiel: Serverseitige Anwendungen) können ein geheimes Clientgeheimnis sicher speichern und erfordern keine PKCE.

- Die Autorisierungsanforderung wird initiiert, indem der Anwender zum Autorisierungsendpunkt umgeleitet wird. **Es ist keine geheime Clientcodeabfrage oder PKCE-Code erforderlich** In diesem Schritt.
- Während der Tokenanforderung enthält der Client den **Geheimer Clientschlüssel** Zusammen mit **Autorisierungscode** Um das Zugriffstoken zu erhalten.

Führen Sie eine POST-Anforderung an den Autorisierungsendpunkt mit den folgenden Parametern aus:

```
Method: POST
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Endpoint: https://<servicenow_base_url>/oauth_token.do
Headers: Content-Type: application/x-www-form-urlencoded
```

Token-Anforderungsparameter (Privater Client-Client-Geheimschlüssel)

Parameter	Erforderlich	Beschreibung
Grant_type	Ja	Legen Sie den Wert auf fest Authorization_Code Um den Code gegen ein Token auszutauschen.
Code	Ja	Der vom Autorisierungsendpunkt empfangene Autorisierungscode.
Umleiten_URI	Ja	Der in der anfänglichen Autorisierungsanforderung verwendete URI. Beispiel: https://yourapp.com/callback
client_id	Ja	Der eindeutige Bezeichner für Ihre Client-Anwendung.
client_secret	Ja	Das Geheimnis des Clients, das zur Authentifizierung beim Token-Endpunkt verwendet wird.
state	Ja	Ein vom Client generierter Wert, der verwendet wird, um CSRF-Angriffe zu verhindern. Der Wert wird im Umleitungs-URI unverändert zurückgegeben, sodass der Client ihn validieren kann.

6. Greifen Sie auf zu ServiceNow APIs mit dem Zugriffstoken.

   Beispiel:

   Stellen Sie mithilfe des Zugriffstoken eine GET-Anforderung an die APIs. Schließen Sie das Zugriffstoken in ein Autorisierung Header.

```
Method: GET
End Point: https://<servicenow_base_url>/api/now/incident
Authorization: Bearer YOUR_ACCESS_TOKEN
```

7. Verlängern Sie das Zugriffstoken, wenn es abgelaufen ist.
   Stellen Sie eine POST-Anforderung, um das Zugriffstoken (nur private Clients) mit den folgenden Parametern zu aktualisieren:

```
Method: POST
Endpoint: https://<servicenow_base_url>/oauth_token.do
Headers: Content-Type: application/x-www-form-urlencoded
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Token-Anforderungsparameter Aktualisieren (Privater Client)

Parameter	Erforderlich	Beschreibung
Grant_type	Ja	Legen Sie den Wert auf fest REFRESH_Token Um ein neues Zugriffstoken anzufordern.
REFRESH_Token	Ja	Das Aktualisierungstoken, das zuvor vom Token-Endpunkt ausgegeben wurde.
client_id	Ja	Der eindeutige Bezeichner für Ihre Client-Anwendung.
client_secret	Ja	Das geheime Clientgeheimnis, das zur Authentifizierung beim Token-Endpunkt verwendet wird.

Konfigurieren Sie eine OAuth-Autorisierungscodegewährung

Konfigurieren Sie die OAuth-Autorisierungscodegewährung, um eine sichere und interaktive Anwenderauthentifizierung zu ermöglichen, damit Anwendungen im Namen von Anwendern auf Ressourcen zugreifen können. Die OAuth-Autorisierungscodegewährung überprüft, ob der API-Zugriff basierend auf der Anwenderidentität und den Berechtigungen gewährt wird.

Vorbereitungen

Erforderliche Rolle: oauth_admin, mi_admin, admin

Prozedur

1. Navigieren zu **Rechneridentitätskonsole** > **Eingehende Integrationen** > **Neue Integration** > > **OAuth-Autorisierungscode-Gewährung**an.
   Die Seite „neuer Datensatz“ wird angezeigt.
2. Aktualisieren Sie die Textfelder im Formular „Details“ mit den entsprechenden Informationen.

Detailformular

Feld	Beschreibung
Name der OAuth-Entität	Name der OAuth-Entität.
Umleitungs-URL	URL, an die der Autorisierungscode nach der Authentifizierung gesendet werden soll.
Client-ID	Eindeutige ID, die zur Identifizierung der Anwendung zugewiesen ist.
Geheimer Clientschlüssel	Der geheime Schlüssel, den nur die Anwendung und der Autorisierungsserver identifizieren können. Die Anwendung verwendet diesen Schlüssel, um Zugriffstoken zu authentifizieren und zu erhalten.

Wählen Sie aus **Dies ist ein öffentliches Client-Kontrollkästchen** Wenn die Anwendung Anmeldeinformationen nicht sicher speichern kann und keinen geheimen Schlüssel erfordert, um ihre Identität während der Autorisierung nachzuweisen. Die geheimen Clientinformationen werden für öffentliche Clients verarbeitet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Aktualisieren Sie die Textfelder im Formular „Erweiterte Optionen“ (optional) mit den entsprechenden Informationen.

Formular „Erweiterte Optionen“

Feld	Beschreibung
Lebensdauer des Zugriffstokens	Dauer (in Sekunden), für die das OAuth-Zugriffstoken gültig bleibt, bevor es abläuft. **Hinweis:** Der Standardwert ist 1800 Sekunden.
Lebensdauer von Aktualisierungstoken	Dauer (in Sekunden), für die das OAuth-Aktualisierungstoken gültig bleibt, bevor es abläuft. **Hinweis:** Der Standardwert ist 8.640.000 Sekunden.
Anmelde-URL	HTTP-Umleitungsendpunkt zur Authentifizierung beim Autorisierungsserver.
Logo-URL	Webadresse eines Bildes, das die Anwendung während des Authentifizierungs- und Autorisierungsprozesses darstellt. Sie wird auf dem Einwilligungsbildschirm des Autorisierungsservers angezeigt, damit Sie die anfordernde Anwendung erkennen können.

Durch das Erzwingen der Tokenbeschränkung werden Einschränkungen hinsichtlich der Verwendung eines OAuth-Zugriffstokens angewendet. Dies erhöht die Sicherheit, indem überprüft wird, ob Token nur unter bestimmten Bedingungen gültig sind. Aktivieren Sie **Token-Einschränkung erzwingen** Kontrollkästchen, um OAuth-Zugriffstoken auf bestimmte APIs zu beschränken, die in der API-Zugriffsrichtlinie definiert sind. Wenn die Tokenbeschränkung erzwingen deaktiviert ist, kann das Token für andere REST APIs verwendet werden.

4. Aktualisieren Sie die Textfelder in **Authentifizierungsbereich (optional)** Formular mit den entsprechenden Informationen. Der Authentifizierungsbereich definiert die Zugriffsstufe, die eine Anwendung auf eine Ressource hat. Wählen Sie den Authentifizierungsbereich für die spezifischen REST APIs aus, auf die Sie zugreifen möchten.

Formular „Authentifizierungsbereich“

Feld	Beschreibung
Authentifizierungsbereich	Die Zugriffsstufe, die eine Anwendung auf eine Ressource hat. Der Authentifizierungsbereich schränkt die Aktionen ein, die ein Zugriffstoken für APIs oder Daten ausführen kann.
Autorisierung beschränken	Die Namen der APIs, für die Sie die Autorisierung einschränken möchten.

5. Wählen Sie Aus **Erstellen Sie einen neuen Authentifizierungsbereich** Um einen neuen Authentifizierungsbereich hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie **Speichern**.
   Eine neue OAuth-Autorisierungscodegewährung wird erstellt.
7. Gehe zu **Alle** > **Eingehende Integrationen** > **Anwendungsregistrierungen** Zum Anzeigen der neu erstellten OAuth-Autorisierungscodegewährung.

Gewährung von Client-Anmeldeinformationen

Verwenden Sie den Berechtigungstyp „OAuth-Client-Anmeldeinformationen“ für Back-End-Services oder automatisierte Integrationen, die darauf zugreifen ServiceNow® APIs ohne Anwenderinteraktion. Die Client-Anwendung authentifiziert sich direkt mithilfe ihrer Client-ID und ihres Geheimnisses und erhält ein Zugriffstoken, das die Anwendung selbst und nicht den Anwender darstellt.

Zugehörige Informationen

Workflow zur Gewährung von Client-Anmeldeinformationen

Konfigurieren Sie eine OAuth-Client-Anmeldeinformationsgewährung

Workflow zur Gewährung von Client-Anmeldeinformationen

Authentifizieren Sie eine Client-Anwendung mithilfe eines Client-Anmeldeinformations-Workflows. Der Workflow für die Erteilung von Client-Anmeldeinformationen wird von Back-End-Services oder Systemintegrationen für den Zugriff verwendet ServiceNow® APIs ohne Anwenderbeteiligung.

Vorbereitungen

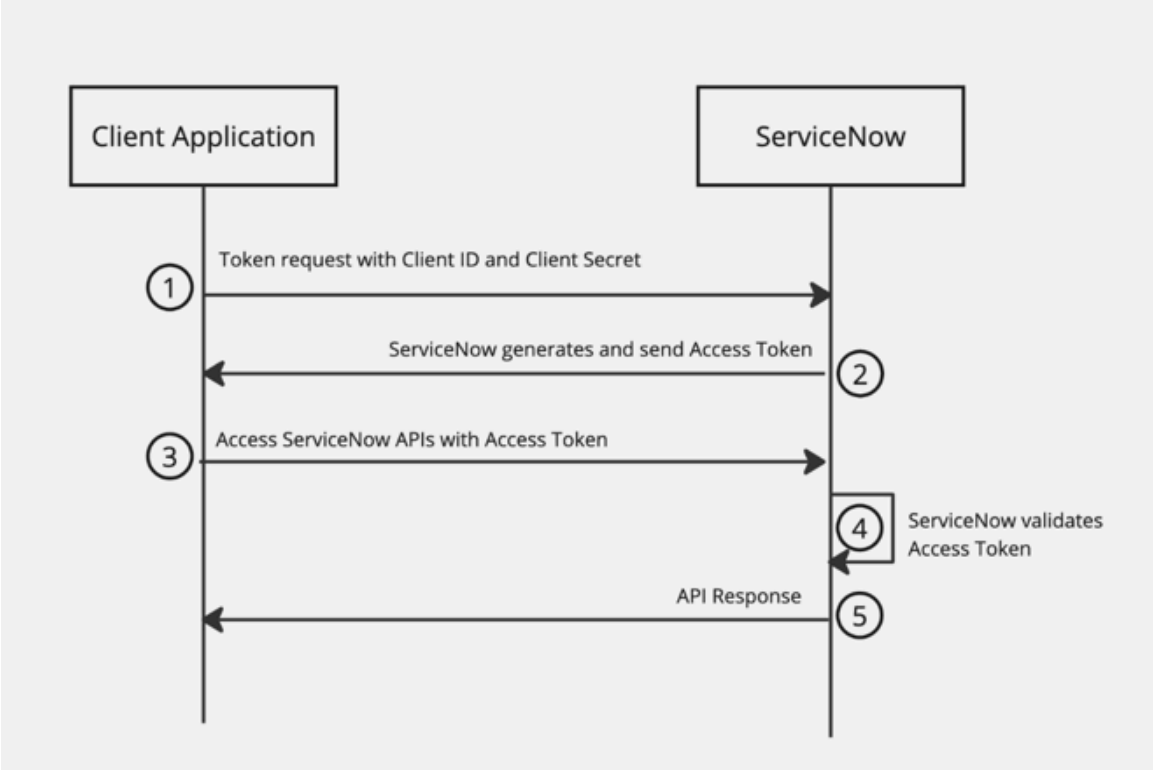
Erforderliche Rolle: `oauth_admin, mi_admin, admin`

Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow beschreibt, wie sich eine Client-Anwendung (Back-End-Service oder Systemintegration) direkt bei authentifiziert ServiceNow Verwendung der Client-Anmeldeinformationen ohne Anwenderinteraktion. Die Anwendung fordert ein Zugriffstoken mit ihrer Client-ID und dem geheimen Clientschlüssel an ServiceNow Validiert vor Ausgabe des Tokens. Der Client verwendet dann dieses Token für den Zugriff ServiceNow APIs. ServiceNow Validiert jede Anforderung, bevor die entsprechende Antwort zurückgegeben wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow zur Gewährung von Client-Anmeldeinformationen



Prozedur

1. **Die Clientanwendung stellt eine Tokenanforderung** Zum ServiceNow-Endpunkt mit den folgenden Parametern:

```
Method: POST
Endpoint: https://<servicenow_base_url>/oauth_token.do
```

Token-Anforderungsparameter

Parameter	Erforderlich	Beschreibung
Grant_type	Ja	OAuth 2,0-Gewährungstyp. Beispiel: Client_credentials
client_id	Ja	Eindeutiger Bezeichner für die Client-Anwendung. Beispiel: Y UNSERE_CLIENT_ID
client_secret	Ja	Geheimnis, das der Client-ID zugeordnet ist. Beispiel: IHR_CLIENT_SECRET
scope	Optional	Berechtigungen für das Zugriffstoken angefordert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Erforderlich	Beschreibung
		Beispiel: Incident_read Incident_write

2. ServiceNow Validiert die Anmeldeinformationen und gibt das Zugriffstoken zurück.
3. Stellen Sie eine API-Anforderung mit dem Zugriffstoken.

   Schließen Sie das Zugriffstoken in ein `Autorisierung` Header jeder API-Anforderung.

```
Method: POST
Endpoint: https://<servicenow_base_url>/api/now/incident
Authorization: Bearer YOUR_ACCESS_TOKEN
```

4. ServiceNow Validiert das Token und gibt die entsprechende API-Antwort zurück.

> **Hinweis:** Verwenden Sie den Workflow für die Erteilung von Client-Anmeldeinformationen nur mit vertrauenswürdigen serverseitigen Anwendungen. Verwalten Sie `Client_Secret` Sicher. Stellen Sie sicher, dass Sie nicht verwenden `Client_Secret` In clientseitigen Umgebungen wie Browsern oder mobilen Apps.

Konfigurieren Sie eine OAuth-Client-Anmeldeinformationsgewährung

Konfigurieren Sie die OAuth-Client-Anmeldeinformationen für eine sichere Computer-zu-Computer-Authentifizierung ohne Anwenderinteraktion. Es authentifiziert Anwendungen mithilfe von Client-Anmeldeinformationen und gewährt gesteuerten API-Zugriff mit bereichsbezogenen Berechtigungen.

Vorbereitungen

Erforderliche Rolle: `oauth_admin, mi_admin, admin`

Prozedur

1. Navigieren zu **Rechneridentitätskonsole** > > **Eingehende Integrationen** > > **Neue Integration** > **Gewährung von OAuth-Client-Anmeldeinformationen**an.
   Die Konfigurationsseite für OAuth-Client-Anmeldeinformationen wird angezeigt.
2. Aktualisieren Sie die Textfelder im Formular „Details“ mit den entsprechenden Informationen.

Detailformular

Feld	Beschreibung
Name	Der Name der OAuth-Entität.
OAuth-Anwendungsanwender	Der Anwendername des Service-Accounts, den eine Anwendung über OAuth authentifiziert und autorisiert.
Client-ID	Die eindeutige ID, die zur Identifizierung der Anwendung zugewiesen ist.
Geheimer Clientschlüssel	Der geheime Schlüssel, den nur die Anwendung und der Autorisierungsserver identifizieren können. Die Anwendung verwendet diesen Schlüssel, um Zugriffstoken zu authentifizieren und zu erhalten.

Aktivieren Sie die Checkbox **Aktiv**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Aktualisieren Sie die Textfelder im Formular „Erweiterte Optionen“ (optional) mit den entsprechenden Informationen.
4. Aktualisieren Sie die Textfelder in **Authentifizierungsbereich (optional)** Formular mit den entsprechenden Informationen.
   Der Authentifizierungsbereich definiert die Zugriffsstufe, die eine Anwendung auf eine Ressource hat. Wählen Sie den Authentifizierungsbereich für die spezifischen REST APIs aus, auf die Sie zugreifen möchten.

Formular „Authentifizierungsbereich“

Feld	Beschreibung
Authentifizierungsbereich	Die Zugriffsstufe, die eine Anwendung auf eine Ressource hat. Der Authentifizierungsbereich schränkt die Aktionen ein, die ein Zugriffstoken für APIs oder Daten ausführen kann.
Autorisierung beschränken	Die Namen der APIs, für die Sie die Autorisierung einschränken möchten.

   a. Wählen Sie Aus **Erstellen Sie einen neuen Authentifizierungsbereich** Um einen neuen Authentifizierungsbereich hinzuzufügen.
5. Wählen Sie **Speichern**.
   Eine neue Berechtigung für OAuth-Client-Anmeldeinformationen wird erstellt.
6. Gehe zu **Alle** > **Eingehende Integrationen** > **Anwendungsregistrierungen** Zum Anzeigen der neu erstellten Client-Anmeldeinformationsgewährung.

Drittpartei-Tokengewährung

Die Drittpartei-Tokengewährung aktiviert ServiceNow® Dient zum Akzeptieren von Identitätstoken von vertrauenswürdigen externen Identitätsanbietern, z. B. Azure AD oder Okta. Die Tokengewährung von Drittparteien bietet sicheren, tokenbasierten Zugriff. Diese Methode unterstützt sicheren Zugriff und Single Sign-on (SSO) in Szenarien der Verbundauthentifizierung.

Die Client-Anwendung fordert eine ID oder ein Zugriffstoken von einem vertrauenswürdigen externen Identitätsanbieter wie Azure AD oder Okta an und schließt sie in ein Autorisierung Header der API-Anforderungen an ServiceNow®. ServiceNow® Validiert das Token und gewährt, wenn vertrauenswürdig, Zugriff basierend auf der bestätigten Identität.

Sie können Accounts von einem Drittpartei-Identitätsanbieter (IdP) verwenden, um auf zuzugreifen ServiceNow® API für:

- Drittanbieter-Token-Workflow für Anwenderaccounts
- Drittpartei-Token-Workflow für Service-Accounts

Drittanbieter-Token-Workflow für Anwenderaccounts

Dieser Workflow basiert auf dem Token-Verbund-Konzept. Dadurch können Clientanwendungen Token direkt von einem IdP abrufen und für den Zugriff verwenden ServiceNow APIs.

Vorbereitungen

Erforderliche Rolle: `oauth_admin`, `mi_admin`, `admin`

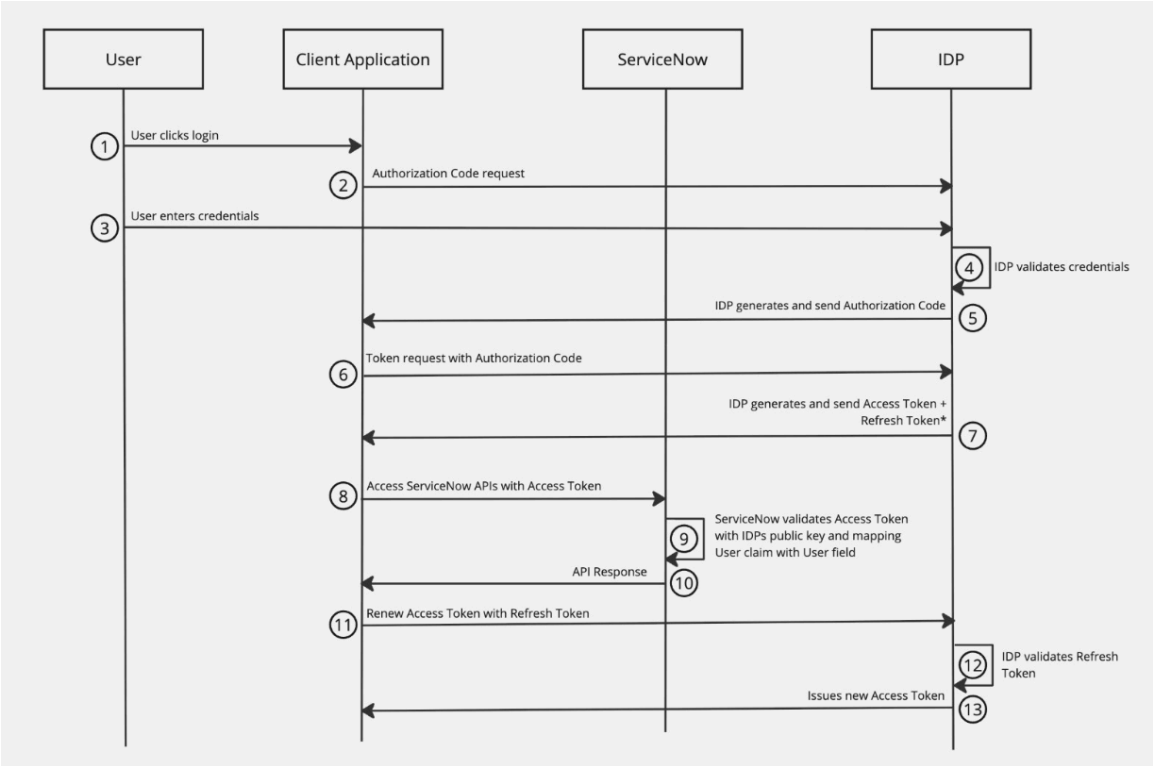
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die Drittpartei-Client-Anwendung fordert Token direkt von Ihrem Identitätsanbieter (Identity Provider, IdP) an. Die Authentifizierungsmethode zwischen dem Client und dem IdP ist flexibel und kann entsprechend Ihren spezifischen Anforderungen konfiguriert werden. Nach erfolgreicher Authentifizierung gibt der IdP ein ID-Token oder Zugriffstoken und optional ein Aktualisierungstoken aus. Diese Token werden direkt an die Client-Anwendung gesendet, die sie dann für den Zugriff verwendet ServiceNow APIs.

Hinweis: ServiceNow Validiert das Token mithilfe des öffentlichen Schlüssels, der während des Setups konfiguriert wurde, und gewährt Zugriff auf die angeforderten APIs. Stellen Sie sicher, dass das Token im JSON-Webtoken-Format (JWT) vorliegt.

Anwenderaccount-Workflow



Hinweis: Dieses Diagramm dient der Veranschaulichung. Zeigt den Autorisierungscode-Gewährungs-Flow zwischen Ihrer Client-Anwendung und dem Identitätsanbieter an. Der Workflow ist flexibel. Sie können einen anderen Flow basierend auf Ihren Anforderungen verwenden.

Automatische Übersetzung

Prozedur

1. Konfigurieren Sie Ihre Drittpartei-Client-Anwendung.

   Richten Sie Ihre Drittpartei-Client-Anwendung ein, um Token direkt von Ihrem Identitätsanbieter (Identity Provider, IdP) anzufordern. Wählen Sie eine Authentifizierungsmethode aus, die Ihren Sicherheits- und Integrationsanforderungen am besten entspricht.

2. Erstellen Sie einen OAuth-Client in ServiceNow.

   Geben Sie die erforderlichen Details an, um die Validierung eingehender Token von Ihrem Identitätsanbieter (Identity Provider, IdP) zu ermöglichen. Weitere Informationen zur Konfiguration finden Sie unter Konfigurieren Sie ein Drittpartei-ID-Token

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Drittpartei-Token-Workflow für Service-Accounts

Führen Sie die Schritte aus, um einen Drittanbieter-Token-Workflow für Anwenderaccounts zu erstellen. Erstellen Sie darüber hinaus eine entsprechende `sys_user` Account in ServiceNow für Ihren Service-Account. Im Gegensatz zu menschlichen Anwendern, die normalerweise über Datensätze in ServiceNow verfügen, sind Service-Accounts anwendungsspezifisch und erfordern manuelle Erstellung, um eine gültige Identität auf der Plattform zu etablieren.

Vorbereitungen

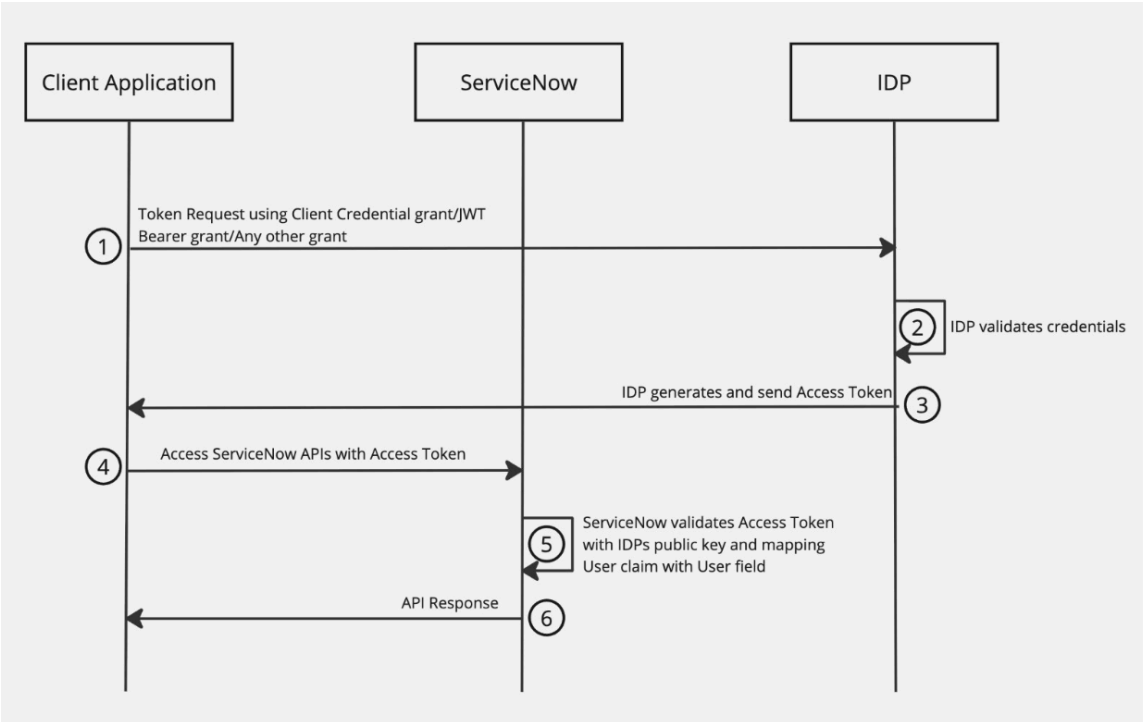
Erforderliche Rolle: `oauth_admin`, `mi_admin`, `admin`

Warum und wann dieser Vorgang ausgeführt wird

Wenn sich eine Drittpartei-Anwendung mithilfe eines Tokens von einem externen Identitätsanbieter (IdP) authentifiziert, ServiceNow Benötigt einen entsprechenden Anwenderdatensatz, um die Identität zuzuordnen und Zugriffssteuerungen anzuwenden.

Der Wert des Anspruchs, der während des ersten Setups in dem von Ihrem IdP ausgestellten Token konfiguriert wurde, wird dem während dieses Setups angegebenen Anwenderfeld zugeordnet. Dieser Account stellt die Service-Identität in ServiceNow dar. Sie können diesen Account nur auf API-Zugriff beschränken und die erforderlichen Berechtigungen zuweisen, indem Sie die entsprechenden Rollen und Gruppen hinzufügen.

Service-Account-Workflow



Prozedur

1. Führen Sie die im angegebenen Schritte aus Setup des ID-Token-Flows des Anwenderaccounts .
2. Erstellen Sie einen `sys-user` Account in ServiceNow Zur Darstellung der Identität Ihres Service-Accounts. Stellen Sie sicher, dass der Token-Anspruchswert mit dem Wert im zugeordneten Anwenderfeld (z. B. user_Name oder email) im Anwenderdatensatz übereinstimmt. Beispiel: User_Name, email.
   a. Wählen Sie die Option nur Webservice-Zugriff aus, um den Account auf API-Zugriff zu beschränken.
   b. Weisen Sie die erforderlichen Rollen und Gruppen zu, um die entsprechende Berechtigung zu gewähren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ServiceNow Die Plattform ordnet den konfigurierten Anspruch dem angegebenen Anwenderfeld in zu `sys_user` Datensatz. Sie erzwingt den Zugriff basierend auf den zugewiesenen Rollen und Gruppen dieses Anwenders.

3. Stellen Sie eine GET-Anforderung mit dem Autorisierungsheader an den folgenden Endpunkt:

```
Method: GET
Endpoint: https:// <servicenow_base_url> /api/now/incident
Authorization: Bearer YOUR_ACCESS_TOKEN
```

Konfigurieren Sie ein Drittpartei-ID-Token

Konfigurieren Sie ein Drittpartei-ID-Token, um eine sichere Authentifizierung zu ermöglichen, indem Sie Anwenderidentitäten über einen externen IdP verifizieren. Das Drittpartei-ID-Token verbessert die Sicherheit, indem gespeicherte Anmeldeinformationen reduziert werden, die nahtlose Authentifizierung bestätigt und die Interoperabilität mit Branchenstandards wie OpenID Connect (OIDC) unterstützt wird.

Vorbereitungen

Erforderliche Rolle: `oauth_admin, mi_admin, admin`

Prozedur

1. Navigieren zu **Rechneridentitätskonsole** > > **Eingehende Integrationen** > **Neue Integration** > **Drittpartei-ID-Token**an.
2. Aktualisieren Sie die Textfelder in **Details** Formular mit den entsprechenden Informationen.

Detailformular

Feld	Beschreibung
Name	Der Name, der vom Ressourcenbesitzer (Anwender) während der Authentifizierung angegeben wurde.
Client-ID	Die eindeutige ID, die zur Identifizierung der Anwendung zugewiesen ist.
Geheimer Clientschlüssel	Der geheime Schlüssel, den nur die Anwendung und der Autorisierungsserver identifizieren können. Die Anwendung verwendet diesen Schlüssel, um Zugriffstoken zu authentifizieren und zu erhalten.

Durch das Erzwingen der Tokenbeschränkung werden Einschränkungen hinsichtlich der Verwendung eines OAuth-Zugriffstokens angewendet. Dies erhöht die Sicherheit, indem überprüft wird, ob Token nur unter bestimmten Bedingungen gültig sind. Aktivieren Sie **Token-Einschränkung erzwingen** Kontrollkästchen, um OAuth-Zugriffstoken auf bestimmte APIs zu beschränken, die in der API-Zugriffsrichtlinie definiert sind. Wenn **Token-Einschränkung erzwingen** Ist deaktiviert, kann das Token für andere REST APIs verwendet werden.

3. Aktualisieren Sie die Textfelder in **Erweiterte Optionen (optional)** Formular mit den entsprechenden Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Optionen“

Feld	Beschreibung
Lebensdauer des Zugriffstokens	Die Dauer (in Sekunden), für die das OAuth-Zugriffstoken gültig bleibt, bevor es abläuft. **Hinweis:** Der Standardwert ist 1800 Sekunden.
Lebensdauer von Aktualisierungstoken	Die Dauer (in Sekunden), für die das OAuth-Aktualisierungstoken gültig bleibt, bevor es abläuft. **Hinweis:** Der Standardwert ist 8.640.000 Sekunden.

4. Aktualisieren Sie die Textfelder in **Authentifizierungsbereich (optional)** Formular mit den entsprechenden Informationen. Der Authentifizierungsbereich definiert die Zugriffsstufe, die eine Anwendung auf eine Ressource hat. Wählen Sie den Authentifizierungsbereich für die spezifischen REST APIs aus, auf die Sie zugreifen möchten.

Formular „Authentifizierungsbereich“

Feld	Beschreibung
Authentifizierungsbereich	Die Zugriffsstufe, die eine Anwendung auf eine Ressource hat. Der Authentifizierungsbereich schränkt die Aktionen ein, die ein Zugriffstoken für APIs oder Daten ausführen kann.
Autorisierung beschränken	Die Namen der APIs, für die Sie die Autorisierung einschränken möchten.

   a. Wählen Sie Aus **Erstellen Sie einen neuen Authentifizierungsbereich** Um einen neuen Authentifizierungsbereich hinzuzufügen.

5. Wählen Sie **Speichern**.
   Ein neues Drittpartei-ID-Token wird erstellt.
6. Gehe zu **Alle** > **Eingehende Integrationen** > **Anwendungsregistrierungen** Zum Anzeigen des neu erstellten Drittpartei-ID-Tokens.

JSON-Webtoken-Bearer-Gewährung

Verwenden Sie diesen Flow, wenn eine Client-Anwendung sicheren, unbeaufsichtigten Zugriff auf benötigt ServiceNow Ressourcen, entweder als sich selbst oder im Namen eines Anwenders.

Die Client-Anwendung generiert ein signiertes JWT, das identitätsbezogene Ansprüche wie den Anwender oder das System enthält, das sie darstellt. Wird an gesendet ServiceNow Instanz zum anfordern eines Zugriffstoken.

JWT-Struktur

Das JWT muss mit dem privaten Schlüssel des Clients signiert werden. Er muss die folgenden Standardansprüche enthalten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- iss – Aussteller (Client-ID)
- Sub – Betreff (Anwender- oder Systemidentität)
- aud – Zielgruppe (ServiceNow-Token-Endpunkt)
- exp: Ablaufzeit
- iat: Ausgestellt um

Hinweis: ServiceNow Verwendet den öffentlichen Schlüssel (im OAuth-JWT-Profil hochgeladen), um die Signatur zu validieren und den Unteranspruch einem Anwenderdatensatz zuzuordnen.

Zugehörige Informationen

Workflow zur Gewährung von JSON-Webtoken

Konfigurieren Sie eine OAuth-JSON-Webtoken-Bearer-Gewährung

Workflow zur Gewährung von JSON-Webtoken

Verwenden Sie diesen Flow, wenn eine Client-Anwendung sicheren, unbeaufsichtigten Zugriff auf benötigt ServiceNow Ressourcen, entweder als sich selbst oder im Namen eines Anwenders.

Vorbereitungen

Erforderliche Rolle: oauth_admin, mi_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Die Client-Anwendung generiert ein signiertes JWT mit identitätsbezogenen Ansprüchen, z. B. dem Anwender oder System, das sie darstellt. Die Client-Anwendung sendet das JWT an die ServiceNow Instanz zum anfordern eines Zugriffstoken.

- **Wenn Sie im Namen eines Anwenders handeln:**

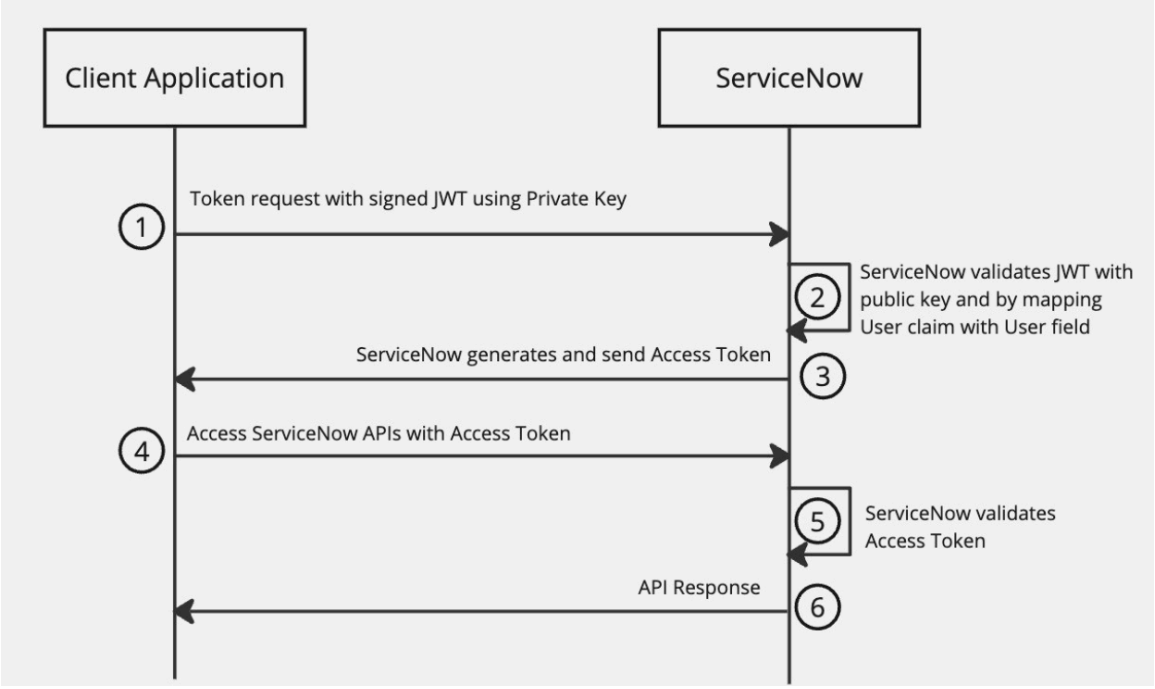
  Das Token stellt einen zuvor authentifizierten Anwender dar. Sie ermöglicht einen sicheren, nahtlosen Zugriff, ohne den Anwender zur Eingabe von Anmeldeinformationen oder Einwilligungen aufzufordern. ServiceNow Vertraut der Anforderung, indem die Identität des Anwenders anhand des signierten Tokens validiert wird, sodass keine Echtzeitinteraktion von Anwendern erforderlich ist.

- **Wenn Sie als sich selbst agieren:**

  Das Token identifiziert und authentifiziert die Client-Anwendung. Anstatt ein gemeinsames Geheimnis zu verwenden, signiert die Anwendung das Token mit einem privaten Schlüssel. Dies bietet eine sicherere Alternative zur Gewährung von Client-Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow für JWT-Gewährung



Prozedur

1. Die Clientanwendung sendet eine Tokenanforderung an ServiceNow, Mit einem mit seinem privaten Schlüssel signierten JWT.
2. ServiceNow Validiert das JWT mit dem entsprechenden öffentlichen Schlüssel.
   Er ordnet zu `Untergeordnet` (Betreff) Anspruch im Token auf einen `sys_user` Datensatz.
3. ServiceNow Validiert das JWT und gibt das Zugriffstoken aus.
4. Der Client enthält das Zugriffstoken in den API-Anforderungen an ServiceNow.
5. ServiceNow Validiert das Zugriffstoken und gibt die entsprechende API-Antwort zurück.

Konfigurieren Sie eine OAuth-JSON-Webtoken-Bearer-Gewährung

Durch die Konfiguration einer OAuth-JSON-Webtoken-Bearergewährung (JWT) wird die tokenbasierte Authentifizierung ohne Anwenderinteraktion gesichert. Es verbessert die Sicherheit mit signierten JWTs und reduziert den Authentifizierungsaufwand, indem wiederholte Anmeldeversuche vermieden werden.

Vorbereitungen

Erforderliche Rolle: `oauth_admin, mi_admin, admin`

Die unterstützten Algorithmen für JSON Web Token (JWT): RS256, RS384, RS512, ES256, ES384, ES512.

Prozedur

1. Navigieren zu **Rechneridentitätskonsole** > > **Eingehende Integrationen** > > **Neue Integration** > **JWT-Bearer-Gewährung**an.
2. Aktualisieren Sie die Textfelder im Formular „Details“ mit den entsprechenden Informationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detailformular

Feld	Beschreibung
Name	Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie JWT OAuth-Zugriff benötigen.
Client-ID	Die automatisch generierte eindeutige ID der Anwendung. Das System verwendet den Wert dieses Felds, um den öffentlichen oder freigegebenen Schlüssel abzurufen und das JWT zu validieren. Der Wert dieses Felds muss mit dem Wert der Ansprüche des Ausstellers und der Zielgruppe in JWT übereinstimmen.
Geheimer Clientschlüssel	Die Zeichenfolge des gemeinsamen Geheimnisses, die sowohl die Instanz als auch die Client-Anwendung oder -Website verwenden, um Kommunikation miteinander zu autorisieren. Lassen Sie dieses Feld leer, damit die Instanz automatisch ein geheimes Clientgeheimnis generiert. Um vorhandene geheime Clientgeheimnisse anzuzeigen, wählen Sie das Sperrsymbol aus.
Anwenderfeld	Feld in der Anwendertabelle (sys_user), das das System verwendet, um den Wert des Antragstellungsanspruchs in der JWT abzugleichen. Beispiel: Wenn Sie ein Token hinzufügen, das einen Anspruchswert des Antragstellers von user.name@example.com hat, legen Sie fest **Anwenderfeld** Bis **E-Mail** . Dieses Feld weist das System an, das E-Mail-Feld nach dem Wert user.name@example.com zu durchsuchen und den übereinstimmenden Anwenderdatensatz in der eingehenden Anforderung zu verwenden.
JTI-Verifizierung aktivieren	Wählen Sie diese Option aus, um bei jedem Tokenaustausch ein neues Token anzufordern. Standard: Ausgewählt.
JWKS-URL	Die URL des JSON-Webschlüsselsatzes. Es handelt sich um eine Sammlung öffentlicher Schlüssel im JSON-Format. Identitätsanbieter veröffentlichen ein JWKS unter einer bekannten URL, damit Client-Anwendungen und -Services die Schlüssel abrufen und die Signaturen von JSON-Webtoken (JWTs) validieren können.
JTI-Anspruch	Eindeutiger Bezeichner für jedes Token. ServiceNow verwendet diesen Anspruch, um die Tokenwiedergabe zu erkennen und zu verhindern, indem überprüft wird, dass ein Token nicht wiederverwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kommentare	Fügen Sie relevante Kommentare hinzu.
JWT-Verifizierungszuordnung	Geben Sie den Identitätsanbieter, die Verifizierungsmethode (z. B. eine JWKS-URL oder ein Zertifikat) und die Zuordnung von JWT-Ansprüchen zu ServiceNow-Anwenderfeldern an. Klicken Sie auf das Plus-Symbol, um die Karten hinzuzufügen oder zu bearbeiten. Geben Sie die folgenden Details in an **JWT-Verifiziererzuordnung** Seite: ○ Name: Der eindeutige Name der JWT-Verifiziererzuordnungskonfiguration. ○ Anwendung: Die Anwendung, in der die Überprüfungszuordnung verwendet wird. ○ Kid (Schlüssel-ID): Der Bezeichner des Schlüssels, der zur Validierung der JWT-Signatur verwendet wird. ○ SYS-Zertifikat: Der ServiceNow-Zertifikatdatensatz, der für die Tokenverifizierung verwendet wird ○ Freigegebener Schlüssel: Ein symmetrischer Schlüssel, der zum Validieren von Token verwendet wird.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die OAuth-Anwendung zu aktivieren.

3. Aktualisieren Sie die Textfelder im Formular „Erweiterte Optionen“ (optional) mit den entsprechenden Informationen.

Formular „Erweiterte Optionen“ (optional)

Feld	Beschreibung
Tokenbeschränkung erzwingen	Wählen Sie diese Option aus, um nur Token für die Verwendung mit APIs zu aktivieren, die festgelegt sind, um das Authentifizierungsprofil zu aktivieren. Sie können Zugriffsgewährung mithilfe einer API-Zugriffsrichtlinie festlegen. Standard: Nicht Ausgewählt.
JWKS-Cache-Lebensdauer	Die Dauer (in Minuten), für die ServiceNow den JSON-Webschlüsselsatz (JWKS) vom Identitätsanbieter zwischenspeichert.
Lebensdauer des Zugriffstokens	Die Dauer (in Sekunden), für die das Zugriffstoken gültig bleibt, bevor es abläuft.
Taktversatz	Kleine Unterschiede in den Systemuhren von Servern oder Geräten, die an der Generierung und Validierung eines Tokens beteiligt sind, können zu Problemen bei der Validierung zeitsensibler

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Ansprüche führen. Passen Sie die Zeit oben an. Standardwert ist: 0 Sekunden.

4. Aktualisieren Sie die Textfelder im Formular „Authentifizierungsbereich“ (optional) mit den entsprechenden Informationen.

   Hinweis: Wenn Sie eine auswählen **Authentifizierungsbereich** , Alle zugehörigen APIs werden automatisch in ausgefüllt **Autorisierung beschränken** Textfeld.

   Formular „Authentifizierungsbereich“

Feld	Beschreibung
Authentifizierungsbereich	Zugriffsebene einer Anwendung. Der Authentifizierungsbereich schränkt die Aktionen ein, die ein Zugriffstoken für APIs oder Daten ausführen kann.
Autorisierung beschränken	Namen der APIs, für die Sie die Autorisierung einschränken möchten.

   a. Wählen Sie Aus **Fügen Sie eine weitere Zeile hinzu** Zum Hinzufügen von Authentifizierungsbereichen.

   b. Wählen Sie Aus **Erstellen Sie einen neuen Authentifizierungsbereich** Um einen neuen Authentifizierungsbereich hinzuzufügen.
   Geben Sie den Namen des Authentifizierungsbereichs in ein **Feld „Umfang“** Textfeld zum Auswählen des neu erstellten Authentifizierungsbereichs. Sie können die APIs, die dem neuen Authentifizierungsbereich zugeordnet werden müssen, manuell hinzufügen und bearbeiten.

      Hinweis: Hinzufügen oder Bearbeiten von APIs aus **Authentifizierungsbereich** Das Menü betrifft alle OAuth-Entitäten, die demselben Autorisierungsbereich zugeordnet sind.

5. Wählen Sie **Speichern**.
   Eine neue OAuth-JSON-Web-Token-Bearer-Berechtigung wird erstellt.
6. Gehe zu **Alle** > **Eingehende Integrationen** > **Anwendungsregistrierungen** Zum Anzeigen der neu erstellten JWT-Bearer-Berechtigung.

Zuteilung der Passwortanmeldeinformationen des Ressourcenbesitzers

Durch die Konfiguration einer ROPC-Gewährung (OAuth Resource Owner Password Credential) können Anwendungen Anwender authentifizieren, indem sie ihre Anmeldeinformationen direkt verwenden, um ein Zugriffstoken zu erhalten.

Sicherheitsüberlegungen

Der ROPC-Flow stellt Anwenderanmeldeinformationen direkt für die Client-Anwendung bereit, wodurch sie inhärent weniger sicher ist als moderne Alternativen. Sie sollte nur in Szenarien verwendet werden, in denen der Client vollständig vertrauenswürdig, streng kontrolliert und sicher verwaltet wird.

Vermeiden Sie die Verwendung dieser Berechtigung in modernen Anwendungen, es sei denn, dies ist absolut erforderlich. Für einen sicheren anwenderbasierten Zugriff wird dringend empfohlen, den Autorisierungscode-Flow mit PKCE zu verwenden,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Anmeldeinformationen vom Client fernhält und sichere Umleitungs- und Tokenverarbeitungspraktiken nutzt.

Zugehörige Informationen

Workflow zur Gewährung von Anmeldeinformationen für den Ressourcenbesitzer

Konfigurieren Sie die Gewährung der Passwortanmeldeinformationen für den OAuth-Ressourcenbesitzer

Workflow zur Gewährung von Anmeldeinformationen für den Ressourcenbesitzer

Dieser Flow wird in Legacy- oder stark kontrollierten Umgebungen verwendet, in denen sichere Alternativen nicht möglich sind. Die Client-App erfasst Anwenderanmeldeinformationen direkt an und sendet sie an ServiceNow Um ein Zugriffstoken zu erhalten, sodass es nur für vertrauenswürdige interne Verwendung geeignet ist.

Vorbereitungen

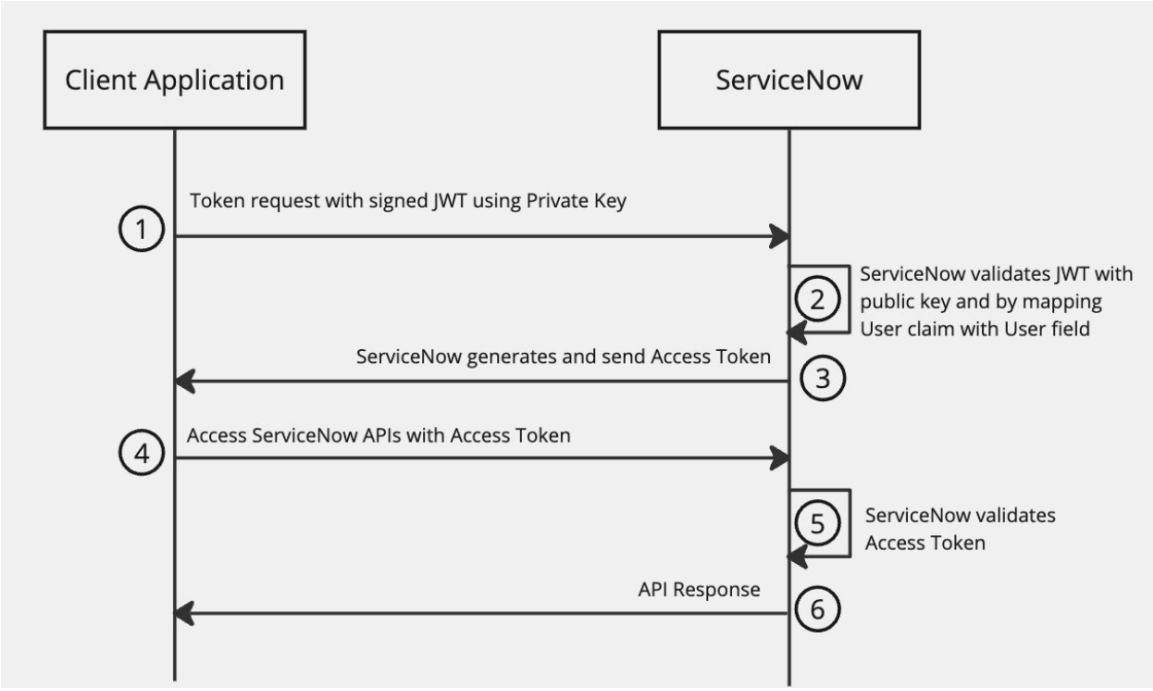
Erforderliche Rolle: `oauth_admin, mi_admin, admin`

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt, wie eine vertrauenswürdige Client-Anwendung ein Zugriffstoken erhält, indem sie Anwenderanmeldeinformationen direkt verarbeitet und es für den Zugriff auf ServiceNow-APIs verwendet.

Der Anwender meldet sich über die App an, die sowohl seine eigenen Anmeldeinformationen als auch die des Anwenders an sendet ServiceNow. ServiceNow Validiert die Anmeldeinformationen und gibt ein Zugriffstoken aus, das die App zum Aufrufen von APIs verwendet.

Workflow zur Gewährung von Anmeldeinformationen für den Ressourcenbesitzer



Prozedur

1. Der Anwender meldet sich bei der Client-Anwendung an.
2. Die Clientanwendung sendet eine Tokenanforderung an mit den folgenden Parametern:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Client-ID und geheimer Client-Schlüssel.
- Anwendername und Passwort des Anwenders.

Beispiel

```
Method: POST
Endpoint: https://<servicenow_base_url>/oauth_token.do
Headers: Content-Type: application/x-www-form-urlencoded
```

Token-Anforderungsparameter

Parameter	Erforderlich	Beschreibung
Grant_type	Ja	Gibt den OAuth-Gewährungstyp an.
client_id	Ja	Der eindeutige Bezeichner für Ihre Client-Anwendung. FORMAT: YOUR_CLIENT_ID
client_secret	Ja	Der geheime Schlüssel der Clientanwendung. FORMAT: YOUR_CLIENT_SECRET
username	Ja	Des Anwenders ServiceNow Anwendername.
Passwort	Ja	Des Anwenders ServiceNow Passwort.
scope	Optional	Definiert die angeforderte Zugriffsebene. Beispiel: ○ Incident_read ○ Incident_write

3. ServiceNow validiert sowohl die Client- als auch die Anwenderanmeldeinformationen und gibt das Zugriffstoken zurück.
4. Der Client verwendet das Zugriffstoken, um ServiceNow-APIs aufzurufen.

Beispiel

```
Method: GET
Endpoint: https://<servicenow_base_url/api/now/incident
Authorization: Bearer YOUR_ACCESS_TOKEN
```

5. ServiceNow Validiert das Zugriffstoken und gibt die API-Antwort zurück.

Konfigurieren Sie die Gewährung der Passwortanmeldeinformationen für den OAuth-Ressourcenbesitzer

Durch die Konfiguration einer ROPC-Gewährung (OAuth Resource owner Password Credential) können Anwendungen Anwender authentifizieren, indem sie ihre

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen direkt verwenden, um ein Zugriffstoken zu erhalten. Diese Methode ist ideal für vertrauenswürdige Anwendungen und Legacy-Systeme, die eine Authentifizierung ohne browserbasierte Flows erfordern, und ermöglicht eine sichere Tokenvalidierung und kontrollierten API-Zugriff.

Vorbereitungen

Erforderliche Rolle: `oauth_admin, mi_admin, admin`

Prozedur

1. Navigieren zu **Rechneridentitätskonsole** > > **Eingehende Integrationen** > > **Neue Integration** > **Gewährung von Passwortanmeldeinformationen für OAuth-Ressourcenbesitzer**an.
2. Aktualisieren Sie die Textfelder in **Details** Formular mit den entsprechenden Informationen.

Detailformular

Feld	Beschreibung
Name	Der Name, der vom Ressourcenbesitzer (Anwender) während der Authentifizierung angegeben wurde.
Client-ID	Die eindeutige ID, die zur Identifizierung der Anwendung zugewiesen ist.
Geheimer Clientschlüssel	Der geheime Schlüssel, den nur die Anwendung und der Autorisierungsserver identifizieren können. Die Anwendung verwendet diesen Schlüssel, um Zugriffstoken zu authentifizieren und zu erhalten.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die OAuth-Anwendung zu aktivieren.

3. Aktualisieren Sie die Textfelder in **Erweiterte Optionen (optional)** Formular mit den entsprechenden Informationen.

   Durch das Erzwingen der Tokenbeschränkung werden Einschränkungen hinsichtlich der Verwendung eines OAuth-Zugriffstokens angewendet. Dies erhöht die Sicherheit, indem überprüft wird, ob Token nur unter bestimmten Bedingungen gültig sind. Aktivieren Sie das Kontrollkästchen Tokenbeschränkung erzwingen, um OAuth-Zugriffstoken auf bestimmte APIs zu beschränken, die in der API-Zugriffsrichtlinie definiert sind. Wenn Tokenbeschränkung erzwingen deaktiviert ist, kann das Token für andere REST-API verwendet werden.

Detailformular

Feld	Beschreibung
Lebensdauer des Zugriffstokens	Die Dauer (in Sekunden), für die das Zugriffstoken gültig bleibt, bevor es abläuft.
Lebensdauer von Aktualisierungstoken	Die Dauer (in Sekunden), die ein Aktualisierungstoken nach der Ausgabe gültig bleibt, wird im Feld Lebensdauer angegeben.

4. Aktualisieren Sie die Textfelder im Formular „Authentifizierungsbereich“ (optional) mit den entsprechenden Informationen. Der Authentifizierungsbereich definiert die Zugriffsstufe, die eine Anwendung auf eine Ressource hat. Wählen Sie den Authentifizierungsbereich für die spezifischen REST APIs aus, auf die Sie zugreifen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie eine auswählen **Authentifizierungsbereich** , Alle zugehörigen APIs werden automatisch in ausgefüllt **Autorisierung beschränken** Textfeld.

Formular „Authentifizierungsbereich“

Feld	Beschreibung
Authentifizierungsbereich	Zugriffsebene einer Anwendung. Der Authentifizierungsbereich schränkt die Aktionen ein, die ein Zugriffstoken für APIs oder Daten ausführen kann.
Autorisierung beschränken	Namen der APIs, für die Sie die Autorisierung einschränken möchten.

Hinweis: Hinzufügen oder Bearbeiten von APIs aus **Authentifizierungsbereich** Das Menü betrifft alle OAuth-Entitäten, die demselben Autorisierungsbereich zugeordnet sind.

a. Wählen Sie Aus **Erstellen Sie einen neuen Authentifizierungsbereich** Um einen neuen Authentifizierungsbereich hinzuzufügen.

5. Wählen Sie Aus **Fügen Sie eine weitere Zeile hinzu** Um einen weiteren Authentifizierungsbereich mit den zugehörigen APIs zu erstellen.
6. Wählen Sie **Speichern**.
   Eine neue Zuteilung der Passwortanmeldeinformationen für den OAuth-Ressourcenbesitzer wird erstellt.
7. Gehe zu **Alle** > **Eingehende Integrationen** > **Anwendungsregistrierungen** Zum Anzeigen der neu erstellten Erteilung der Passwortanmeldeinformationen für den OAuth-Ressourcenbesitzer.

Alte Experience für eingehende Integrationen

Alte Experience: Eingehende Integrationen.

Hinweis:

Sie können die eingehende OAuth-Konfiguration abhängig vom folgenden Gewährungstyp ausführen:

- Flow zur Gewährung von OAuth-Autorisierungscode

  Hinweis: Für den Autorisierungscode-Flow muss der Anwender die Authentifizierung durch lokale Anmeldung, SSO oder MFA abschließen und dann seine Zustimmung erteilen.

- Passwortgewährung
- JWT-Bearer-Gewährungs-Flow
- ID-Token-Flow
- Implizite OAuth-Berechtigungen
- Client-Anmeldeinformationen

Konfigurieren Sie die OAuth-Integration, die die folgenden Erweiterungen aus dem Zurich-Release enthält:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erhöhen Sie die Länge des geheimen Clientschlüssels auf bis zu 4096 Zeichen, um die Sicherheitsanforderungen von Systemen von Drittparteien zu erfüllen.
- Geben Sie eine JSON-Webschlüsselsatz-URL (JWKS) an, um den öffentlichen Schlüssel für die JSON-Webtoken (JWT)-Signaturvalidierung automatisch zu verwalten und zu aktualisieren.
- Fordern Sie OAuth-Token mit dem JWT-Gewährungstyp an, der mit Signieralgorithmen des Elliptic Curve Digital Signature Algorithm (es) signiert ist, einschließlich ES256, ES384 und ES512, für eingehende JSON-Webtoken (JWT).
- Passen Sie den JWT-ID-Anspruchsnamen (JTI) sowohl in eingehenden OpenID Connect- (OIDC)- als auch in JWT-Bearer-Flows an.

Flow zur Gewährung von OAuth-Autorisierungscode

Der Flow zur Autorisierungscodegewährung ermöglicht einem Anwender den Zugriff auf eine Ressource, indem er sich direkt bei einem OAuth-Server authentifiziert, der der Ressource vertraut, im Gegensatz zur Authentifizierung mit Anwendernamen-/Passwort-Anmeldeinformationen.

Diese Implementierung des OAuth-Autorisierungscode-Flows ermöglicht den Zugriff auf eine Ressource über REST. Das Autorisierungscode-Framework ruft das Zugriffstoken über die autorisierte URL ab, die der Anwender konfiguriert, anstatt den Anwender zu zwingen, einen Anwendernamen/ein Passwort einzugeben. Der Anwendername/das Passwort wird nie dem Client zugänglich gemacht, der Zugriff auf die Ressource anfordert.

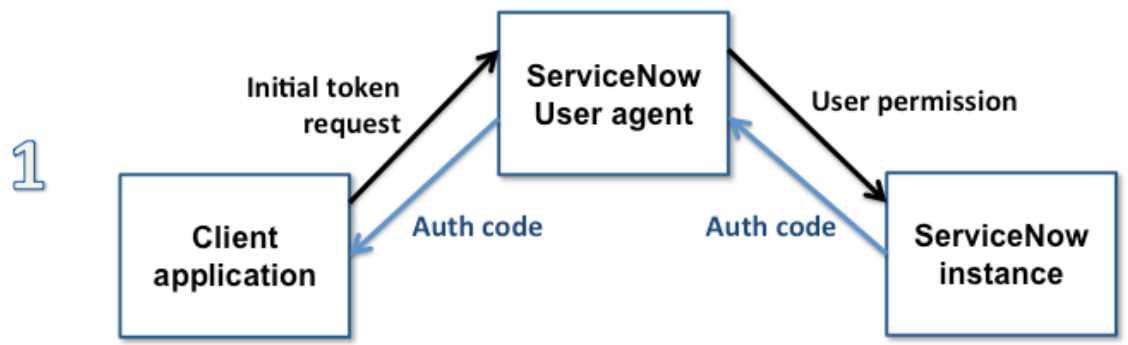
A ServiceNow Instanz als Autorisierungsserver

Der OAuth-Server ist normalerweise ein Autorisierungsserver von Drittanbietern. Sie können auch angeben ServiceNow Instanz als Autorisierungsserver, der die Token für den Autorisierungscode-Flow ausgibt.

Der Anwender, der die eingeschränkte Ressource besitzt, muss den Zugriff autorisieren. Der Anwender kann das ausgestellte Zugriffstoken auch jederzeit widerrufen, um den Zugriff zu beenden.

Flow-Prozess für Autorisierungscodegewährung

Der Flow-Prozess für die Autorisierungscodegewährung besteht aus diesen drei Schritten:



In Schritt 1 initiiert die Client-Anwendung oder -Website einen REST API-Aufruf in Form einer GET-Anforderung an die Instanz über den Anwender-Agent. Normalerweise wird der REST-Aufruf initiiert, wenn der Endanwender auf eine Schaltfläche oder einen Link in der Client-Anwendung oder -Website klickt, um ein Zugriffstoken anzufordern. In der Client-Anwendung muss der Endanwender auch die Autorisierungs-URL, die Token-URL, die Client-ID und das geheime Clientgeheimnis angeben. Eine Erklärung dieser Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden Sie in den Feldbeschreibungen in diesem Thema: Verwenden Sie einen OAuth-Drittanbieter . Wenn der Client einen Gewährungstyp anfordert, muss der Endanwender auswählen **Autorisierungscode** .

Beispiel: Anforderung von der Client-Anwendung an die Instanz ABRUFEN:

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Hinweis: Die **Response_type** Muss sein **Code** Dient zur Verwendung des standardmäßigen OAuth-Codegewährungs-Flows.

Der Endanwender muss manuell Zugriff auf die eingeschränkte Ressource in der Instanz zulassen. In ServiceNow Implementierung muss der Endanwender bei der Instanz angemeldet sein. Die Instanz fordert den Endanwender mit einer UI-Seite auf, die hat **Zulassen** Und **Ablehnen** Schaltflächen.

Das Element, von dem die Clientanwendung das Token tatsächlich anfordert, ist der von Ihnen erstellte Registrierungsdatensatz der OAuth-Provider-Anwendung, auch als Autorisierungs-Endpunkt bezeichnet (siehe Verwenden Sie einen OAuth-Drittanbieter). Der Authentifizierungscode wird vom Autorisierungsendpunkt an den Client gesendet. Es wird nicht direkt an den Client weitergeleitet, sondern an **Umleitungs-URL** Die Sie im Formular „Autorisierungs-Endpunkt“ angeben. Diese URL wird auch als Rückruf-URL bezeichnet. Sie können diese URL von der Client-Anwendung oder -Website abrufen.

Beispielantwort der Instanz an die Client-Anwendung mit einem Autorisierungscode:

```
https/http://{callbackURL}?code={the actual auth code}
```



Jetzt, da die Client-Anwendung über den Autorisierungscode verfügt, verwendet der Client den Code, um das Zugriffstoken anzufordern. Der Autorisierungscode belegt, dass der Anwender in Schritt 1 zugestimmt hat.

Beispiel für eine POST-Anforderung von der Client-Anwendung an die ServiceNow Instanz, die den Authentifizierungscode bereitstellt und das Zugriffstoken anfordert:

```
https://myinstance.service-now.com/oauth_token.do?grant_type=authorization_code&code={the auth
 code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_identifier}&client_secret={client_secret_value}
```

Der Endpunkt in der Instanz gibt ein Zugriffstoken und ein Aktualisierungstoken zurück. Das Aktualisierungstoken kann verwendet werden, um zusätzliche Zugriffstoken anzufordern.

Sie können die Token in der Instanz verwalten, einschließlich des Widerrufs des Tokens. Siehe Verwalten Sie OAuth-Token .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Clientanwendung verwendet das Zugriffstoken, um sich bei der REST API zu authentifizieren. Nach der Authentifizierung der Client-Anwendung gibt die REST API die angeforderten Daten in einer JSON-Nutzlast zurück.

Beispiel für die Anforderung ZUM ABRUFEN der JSON-Nutzlast von Daten für die Tabelle „Incident“ [Incident]:

```
https://myinstance.service-now.com/api/now/table/incident?access_token={the_token}
```

Hinweis: Das System unterstützt auch Implizite OAuth-Berechtigungen , Auch als Flow für implizite Zuteilung bezeichnet.

Integrationsunterstützung

Der Autorisierungscode-Flow unterstützt die folgenden Integrationen in der Instanz:

- Multi-SSO
- SAML 2,0-Update 1
- Multifaktor-Authentifizierung

Die mobile Schnittstelle wird ebenfalls unterstützt.

Autorisieren Sie den Zugriff auf einen OAuth-Endpunkt mithilfe des Authentifizierungscode-Flows

Endanwender, die im Besitz einer geschützten Ressource sind ServiceNow Die Instanz muss den Zugriff auf die Ressource autorisieren, bevor die Instanz das Zugriffstoken bereitstellen kann.

Vorbereitungen

Erforderliche Rolle: keine Sie müssen bereits bei der Instanz angemeldet sein, die die geschützte Ressource enthält. Alternativ können Sie sich mit der Authentifizierungsmethode (z. B. Multifaktor-Authentifizierung oder SAML) anmelden, die Sie verwenden ServiceNow Administrator ist bereits eingerichtet.

Prozedur

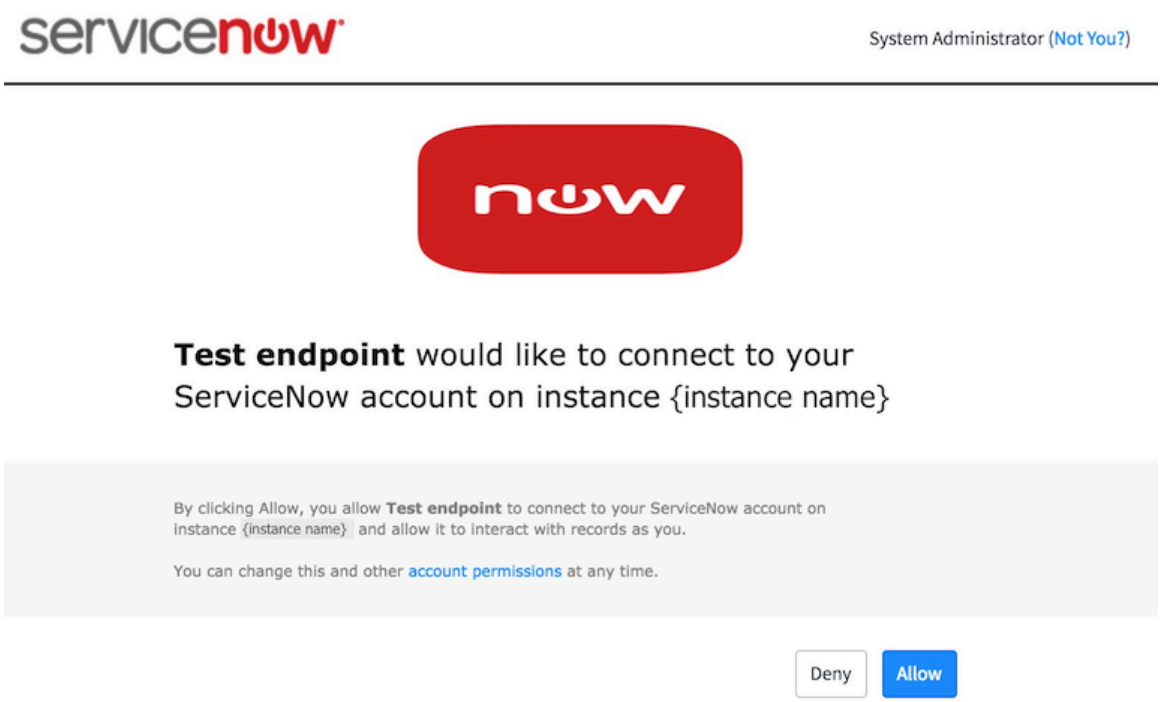
1. Klicken Sie auf den Link oder die Schaltfläche in der Client-Anwendung, in der Sie Zugriff auf die geschützte Ressource in der Instanz anfordern.
   Dadurch wird die Tokenanforderung gestartet. Wenn Sie einen REST-Aufruf von einer Instanz zu einer anderen tätigen, ist dieser Link **OAuth-Token abrufen** Im Formular „REST-Nachricht“.
2. Wenn Sie nicht angemeldet sind, melden Sie sich jetzt an.
   Wenn Sie nicht derselbe Anwender sind wie der in der oberen rechten Ecke angegebene Anwender, klicken Sie auf **Nicht Sie?** Und melden Sie sich an.
3. Klicken Sie auf Accountberechtigungen, um die Liste der Zugriffstoken zu öffnen, die Sie bereits ausgegeben haben.
   Dies ist mit identisch **Self-Service** > **Meine verbunden** App-Tokenliste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Zulassen** Um den Zugriff zuzulassen und die Instanz zu veranlassen, den Autorisierungscode (bei Verwendung des Authentifizierungscode-Flows) oder das Zugriffstoken (bei Verwendung des impliziten Gewährungstyps) auszugeben.

   Wenn Sie auf klicken **Ablehnen** , Die Autorisierung ist nicht zulässig, Sie sind jedoch nicht von der Instanz abgemeldet.



   Eine Nachricht, die bestätigt, dass der Zugriff angezeigt werden soll. Wenn Sie Zugriff über das REST-Nachrichtenformular für eine Instanz anfordern, wird oben im Formular die folgende Meldung angezeigt: OAuth-Aktualisierungstoken ist verfügbar und läuft am {date} ab.

Anforderung des Autorisierungscode-Flow-Statusparameters

Mit der Systemeigenschaft „Glide.oauth.State.paramater.required“ kann der Parameter Status in einer OAuth-Anforderung für den Autorisierungscode-Flow erforderlich sein.

Statusparameter

Erforderliche Rolle: keine

Ab Madrid-Release die Systemeigenschaft `glide.oauth.state.parameter.required`Fügt einen Statusparameter für eine OAuth-Anforderung hinzu. Für zboote Instanzen ist die Eigenschaft „wahr“. Für aktualisierte Instanzen ist die Eigenschaft nicht vorhanden, daher ist der Parameter Status nicht aktiviert. Der Parameter Status ist ein Zeichenfolgenwert und darf keine Sonderzeichen enthalten. Der Parameter „Status“ darf nicht leer oder „“ sein.

Statusparameter wird validiert

Erstellen Sie einen Endpunkt für Clients, um auf die Instanz zuzugreifen. Initiieren Sie einen Autorisierungscode-Flow für eine oauth_auth.do. Zum Beispiel:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie den Statusparameter in der Anforderung nicht angeben, erhalten Sie einen Fehler, und der Autorisierungscode wird nicht zurückgegeben.Fehlender Statusparameter in Anforderung.

Hinzufügen des Parameters Status zur Anforderung:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code&state=123
```

Durch das Hinzufügen des Parameters Status werden Sie zum Anmeldebildschirm weitergeleitet, und der reguläre Autorisierungscode-Flow gibt den Autorisierungscode zurück.

Hinweis: Die Antwort-URL enthält den in der Anforderung übergebenen Statusparameter. Im Beispiel ist der hinzugefügte Parameter `status = 123` .

Wenn der Autorisierungscode-Flow von oauth_initiator.do startet:

```
http://myinstance.service-now.com/oauth_initiator.do?oauth_requestor_context=sys_rest_message&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fec0d1300964f214a2c2fcf51&response_type=code
```

Der Parameter Status wird automatisch hinzugefügt, wenn er von oauth_auth.do weitergeleitet wird.

```
http://myinstance.service-now.com/oauth_auth.do?response_type=code&state=-790938844&redirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_id=e9dba45b380d1300e676ccc91cef468f
```

Beispiel für Autorisierungscode-Flow: ServiceNow Instanz als Autorisierungsserver

Sie können eine Instanz als Autorisierungsserver verwenden, um Token mithilfe des Autorisierungscode-Flows an einen Client auszugeben.

Vorbereitungen

Erforderliche Rolle: keine

In diesem Beispiel werden zwei Instanzen verwendet: Eine als Autorisierungsserver und die andere als Client. Eine Instanz verwendet einen REST-Aufruf, um Token von einer anderen Instanz anzufordern.

Sie müssen Aktivieren Sie OAuth Auf beiden Instanzen.

Prozedur

1. Navigieren Sie in der Autorisierungsserverinstanz (mit Istanbul oder neuerem Release) zu **System-OAuth** > **Applikationsregistrierung** Und klicken Sie dann auf **Neu** .
2. Klicken Sie Auf **Erstellen Sie einen OAuth-API-Endpunkt für externe Clients** .
3. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz aus, wie in beschrieben Erstellen Sie einen Endpunkt für Clients, um auf die Instanz zuzugreifen.
   Wenn Sie diese Schritte ausführen, wird ein Autorisierungsserver eingerichtet. Führen Sie die nächsten Schritte aus, um den Client-Server einzurichten.
4. Navigieren Sie in der Clientinstanz zu **System-OAuth** > **Applikationsregistrierung** Und klicken Sie dann auf **Neu** .
5. Klicken Sie Auf **Stellen Sie eine Verbindung mit einem OAuth-Drittanbieter her** .
6. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz aus, wie in beschrieben.
   Beachten Sie die folgenden Feldwerte:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Name** : Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie OAuth-Zugriff benötigen.
- **Client-ID** : Client-ID des Anwendungsregistrierungsdatensatzes, den Sie für den Autorisierungsserver erstellt haben.
- **Geheimer Client-Schlüssel** : [Schreibgeschützt] die automatisch generierte eindeutige ID der Anwendung. Die Instanz verwendet die Client-ID, wenn ein Zugriffstoken angefordert wird.
- **Standardgewährungstyp** : Wählen Sie Aus **Autorisierungscode** .
- **Autorisierungs-URL** : URL der Instanz, die der Autorisierungsserver ist. Denken Sie daran, anzuhängen `oauth_auth.do` Am Ende der URL.
- **Logo-URL** : Die URL, die ein Bild enthält, das als Anwendungslogo verwendet werden soll. Das Logo wird auf der Genehmigungsseite angezeigt, wenn der Anwender eine Anforderung erhält, einer Client-Anwendung Zugriff auf eine eingeschränkte Ressource in der Instanz zu gewähren.
- **Token-URL** : URL der Instanz, die der Autorisierungsserver ist. Denken Sie daran, anzuhängen `oauth_Token.do` Am Ende der URL.
- **Umleitungs-URL** : URL der Instanz: Die Client-Serverinstanz. Denken Sie daran, anzuhängen `oauth_redirect.do` Am Ende der URL.

7. Erstellen Sie mit ein Profil für den Datensatz **Autorisierungscode** Gewährungstyp.
   Der Client-Server ist eingerichtet. Sie können jetzt eine ausgehende REST-Nachricht erstellen und ein OAuth-Token abrufen.

Erstellen Sie einen Endpunkt für Clients, um auf die Instanz zuzugreifen

Erstellen Sie einen OAuth-Anwendungsendpunkt für externe Client-Anwendungen, um auf zuzugreifen ServiceNow Instanz.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** Und klicken Sie dann auf **Neu** .
2. Klicken Sie auf der Seite „Interceptor“ auf **Erstellen Sie einen OAuth-API-Endpunkt für externe Clients** Und füllen Sie dann das Formular aus.

Feld	Beschreibung
Name	Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie OAuth-Zugriff benötigen.
Client-ID	[Schreibgeschützt] die automatisch generierte eindeutige ID der Anwendung. Die Instanz verwendet die Client-ID, wenn ein Zugriffstoken angefordert wird.
Geheimer Clientschlüssel	[Erforderlich] die gemeinsam genutzte geheime Zeichenfolge, die sowohl die Instanz als auch die Client-Anwendung oder -Website verwenden, um Kommunikation miteinander zu autorisieren. Die Instanz verwendet das geheime Clientgeheimnis, wenn ein Zugriffstoken angefordert wird. Lassen Sie dieses Feld leer, damit die Instanz automatisch ein geheimes Clientgeheimnis generiert. Klicken Sie auf das Schlosssymbol, um vorhandene Client-Geheimnisse anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Umleitungs-URL	Die Rückruf-URL, zu der der Autorisierungsserver umleitet. Geben Sie die vollständigen URLs der Clients ein, die Zugriff auf die Ressource anfordern, angehängt von `/oauth_redirect.do` . Beispiel: `http://token_consumer:port/oauth_redirect.do` . Geben Sie so viele URLs wie erforderlich für alle möglichen Token-Verbraucher ein. Die Instanz stimmt die URL der eingehenden Anforderung mit einer der Umleitungs-URLs ab. Wenn keine Übereinstimmung erzielt wird, verwendet die Instanz die erste Umleitungs-URL.
Logo-URL	Die URL, die ein Bild enthält, das als Anwendungslogo verwendet werden soll. Das Logo wird auf der Genehmigungsseite angezeigt, wenn der Anwender eine Anforderung erhält, einer Client-Anwendung Zugriff auf eine eingeschränkte Ressource in der Instanz zu gewähren.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die Anwendungsregistrierung zu aktivieren.
Lebensdauer von Aktualisierungstoken	Die Anzahl der Sekunden, die ein Aktualisierungstoken gültig ist. Die Instanz verwendet den Lebensdauerwert, wenn ein Aktualisierungstoken angefordert wird. Standardmäßig laufen Aktualisierungstoken in 100 Tagen (8640000 Sekunden) ab.
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um die Verwendung von Token nur mit APIs zuzulassen, die so festgelegt sind, dass das Authentifizierungsprofil zugelassen wird. Sie können Zugriffsgewährung mithilfe einer API-Zugriffsrichtlinie festlegen. Weitere Informationen finden Sie unter Erstellen Sie EINE REST-API-Zugriffsrichtlinie . Standard: Nicht Ausgewählt.
Mobile-Client	Stellt die Entität für die mobile App oder das Web dar. Diese Informationen werden verwendet, um die Anmeldeinformationen mit Mobile oder Web zu analysieren.
Lebensdauer von Zugriffstoken	Die Anzahl der Sekunden, die ein Zugriffstoken gültig ist. Die Instanz verwendet den Lebensdauerwert, wenn ein Zugriffstoken angefordert wird. Standardmäßig laufen Zugriffstoken in 30 Minuten (1800 Sekunden) ab.
Kommentare	Die der Anwendung zuzuordnenden Informationen.
Client-Typ	Wählen Sie den Client-Typ basierend auf dem Typ Ihres Clients aus. Optionen: ○ **iFrame – eingebettet** ○ **Integration als Anwender** ○ **Integration als Service** Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

3. Klicken Sie auf **Absenden**.

Ergebnis

Das System erstellt einen Datensatz in der Tabelle „Anwendungsregistrierungen“ [oauth_Entity] vom Typ „OAuth-Client“. Wenn die Instanz tatsächlich Token und Autorisierungscodes ausgibt, werden sie in der Tabelle gespeichert. Siehe Verwalten Sie OAuth-Token Weitere Informationen finden Sie unter .

OAuth-API-Antwortparameter

Die OAuth 2,0-API erstellt eine JSON-Antwort, die die folgenden Parameter als Name:Wert-Paare enthält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortparameter für Zugriffstoken

Antwortparameter	Beschreibung
scope	Zugriffsmenge, die vom Zugriffstoken gewährt wird. Der Umfang ist immer **Anwenderaccount** , Bedeutet, dass das Zugriffstoken dieselben Rechte hat wie der Anwenderaccount, der das Token autorisiert hat. Wenn Abel Tuter beispielsweise eine Anwendung durch Angabe von Anmeldeinformationen autorisiert, gewährt das resultierende Zugriffstoken dem Tokenträger die gleichen Zugriffsrechte wie Abel Tuter.
Token_type	Typ des Tokens, das von der Anforderung ausgegeben wird, wie im OAuth-RFC definiert. Der Tokentyp ist immer **Bearer** , Bedeutet, dass jeder im Besitz des Zugriffstokens auf eine geschützte Ressource zugreifen kann, ohne einen kryptografischen Schlüssel bereitzustellen. Siehe RFC6750 Weitere Informationen dazu, wie OAuth 2,0 Bearer-Token verwendet.
EXISTRIES_in	Lebensdauer des Zugriffs-Tokens in Sekunden.
REFRESH_Token	Zeichenfolgenwert des Aktualisierungs-Tokens.
access_token	Zeichenfolgenwert des Zugriffs-Tokens. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Zugriffstokens gestellt werden, geben immer das aktuelle Zugriffstoken zurück.
format	[Optional] Ausgabeformat der Antwort. Dieser Wert ist immer JSON.

Hinweis: Wenn ein OAuth-Provider den Antworttext als „content-type“ anstelle von „Content-Type“ sendet, analysiert der OAuth-HTTP-Client die Antwort möglicherweise nicht korrekt. Um dieses Problem zu beheben, erstellen Sie eine Systemeigenschaft mit diesen Parametern.

Feld	Wert
Name	glide.oauth.inhouse.httpclient.enabled
Typ	Wahr|Falsch
Wert	falsch

Weitere Informationen zum Erstellen von Systemeigenschaften finden Sie unter Fügen Sie eine Systemeigenschaft hinzu

Das folgende Beispiel veranschaulicht die JSON-Zeichenfolge, die von einer Zugriffstoken-Anforderung zurückgegeben wird. (Bereiche wurden hinzugefügt, um die Lesbarkeit zu verbessern.)

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,
"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FM
xHW40H8yOO3Hoe",
"access_token":"F0jh9korTyzd9kaZqZ0SzjKZuS3ut0i4P46Lc52m2JYHiLIcqzFAumpyxshU9mMQ
13gJHtxD2fy"}
```

OAuth-API-Anforderungsparameter

Erfahren Sie mehr über die OAuth-API-Anforderungsparameter, die Zugriffstoken-Anforderungen verwenden.

Hinweis: Der Inhaltstyp der OAuth-API muss sein `Application/x-www-Form-urlencoded` . Ein Inhaltstyp von `Anwendung/JSON` Führt zu einem nicht angegebenen Fehler.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter für Zugriffstoken-Anforderung

Anforderungsparameter	Beschreibung
Grant_type	[Erforderlich] der Typ der Anmeldeinformationen, die die Anforderung für ein Zugriffstoken autorisieren. Dieser Parameter muss einen der folgenden Werte haben: • **Passwort** : Eine Reihe von Anwenderanmeldeinformationen zum Autorisieren der Zugriffstoken-Anforderung. Geben Sie die Anwenderanmeldeinformationen in den Parametern Anwendername und Passwort an. • **REFRESH_Token** : Ein vorhandenes Aktualisierungstoken autorisiert die Zugriffstoken-Anforderung. Geben Sie das Aktualisierungstoken im Parameter „refresh_Token“ an.
client_id	[Erforderlich] automatisch generierte eindeutige ID der Clientanwendung, die das Zugriffstoken anfordert.
client_secret	[Erforderlich] Gemeinsame geheime Zeichenfolge, die die Instanz und die OAuth-Anwendung verwenden, um Kommunikation miteinander zu autorisieren.
username	Anwenderaccount-Name, der die Zugriffstoken-Anforderung autorisiert. Dieser Parameter ist für Zugriffstoken-Anforderungen mit erforderlich **Grant_type** Von **Passwort** .
Passwort	Passwort für den Anwenderaccount, der die Zugriffstoken-Anforderung autorisiert. Dieser Parameter ist für Zugriffstoken-Anforderungen mit erforderlich **Grant_type** Von **Passwort** .
REFRESH_Token	Vorhandenes Aktualisierungstoken, das die Zugriffstoken-Anforderung autorisiert. Dieser Parameter ist für Zugriffstoken-Anforderungen mit erforderlich **Grant_type** Von **REFRESH_Token** .

Anforderungen Mit Anwenderanmeldeinformationen

Die Instanz erfordert, dass Clients Anwenderanmeldeinformationen angeben, wenn sie den Client zum ersten Mal autorisieren oder die Erstellung eines neuen Aktualisierungstoken autorisieren. Dieser Anforderungstyp gibt immer zwei Token zurück:

- Ein Zugriffstoken
- Ein Aktualisierungstoken

Die Instanz überprüft, ob der Anwender aktiv ist, derzeit nicht gesperrt ist und eine interaktive Sitzung hat. Wenn eine dieser Bedingungen falsch ist, erstellt die Instanz kein Zugriffstoken. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Zugriffstoken gestellt werden, geben immer das aktuelle Zugriffstoken zurück.

Hinweis: Diese Art der Autorisierungsgewährung basiert auf TLS-Verschlüsselung, um die Anmeldeinformationen des Anwenders während der Übertragung zu schützen.

Das folgende Beispiel veranschaulicht die Anforderung eines Zugriffstokens mit einer Reihe von Anwenderanmeldeinformationen (Bereiche wurden hinzugefügt, um die Lesbarkeit zu verbessern).

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
&client_secret=client_password
&username=admin&password=admin"
https://instancename.service-now.com/oauth_token.do
```

Anforderungen mit einem Aktualisierungstoken

Die Instanz kann ein vorhandenes Aktualisierungstoken verwenden, um ein neues Zugriffstoken zu erstellen. Dieser Anforderungstyp gibt nur ein Zugriffstoken zurück. Die Instanz bestätigt, dass das Aktualisierungstoken nicht abgelaufen ist, bevor ein neues Zugriffstoken generiert wird. Zugriffsanforderungen, die innerhalb der Ablaufzeit des Aktualisierungstokens gestellt werden, geben immer das aktuelle Aktualisierungstoken zurück. Die Übertragung von Aktualisierungstoken ist im Allgemeinen sicherer als die Übertragung von Anwenderanmeldeinformationen. Das folgende Beispiel veranschaulicht die Anforderung eines Zugriffstokens mit einem vorhandenen Aktualisierungstoken (Bereiche wurden hinzugefügt, um die Lesbarkeit zu verbessern).

```
$ curl -d"grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FM
xHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

OAuth-JWT-API-Endpunkt für externe Clients erstellen (Computer-zu-Computer-Integration)

Mit dem OAuth-JWT-Bearer-Token können sich Client-Webanwendungen nahtlos mit dem eingehenden JWT-Gewährungstyp bei Ihrer Instanz authentifizieren, anstatt dass der Endanwender sich manuell anmelden oder das Passwort freigeben muss.

Bevor Sie beginnen

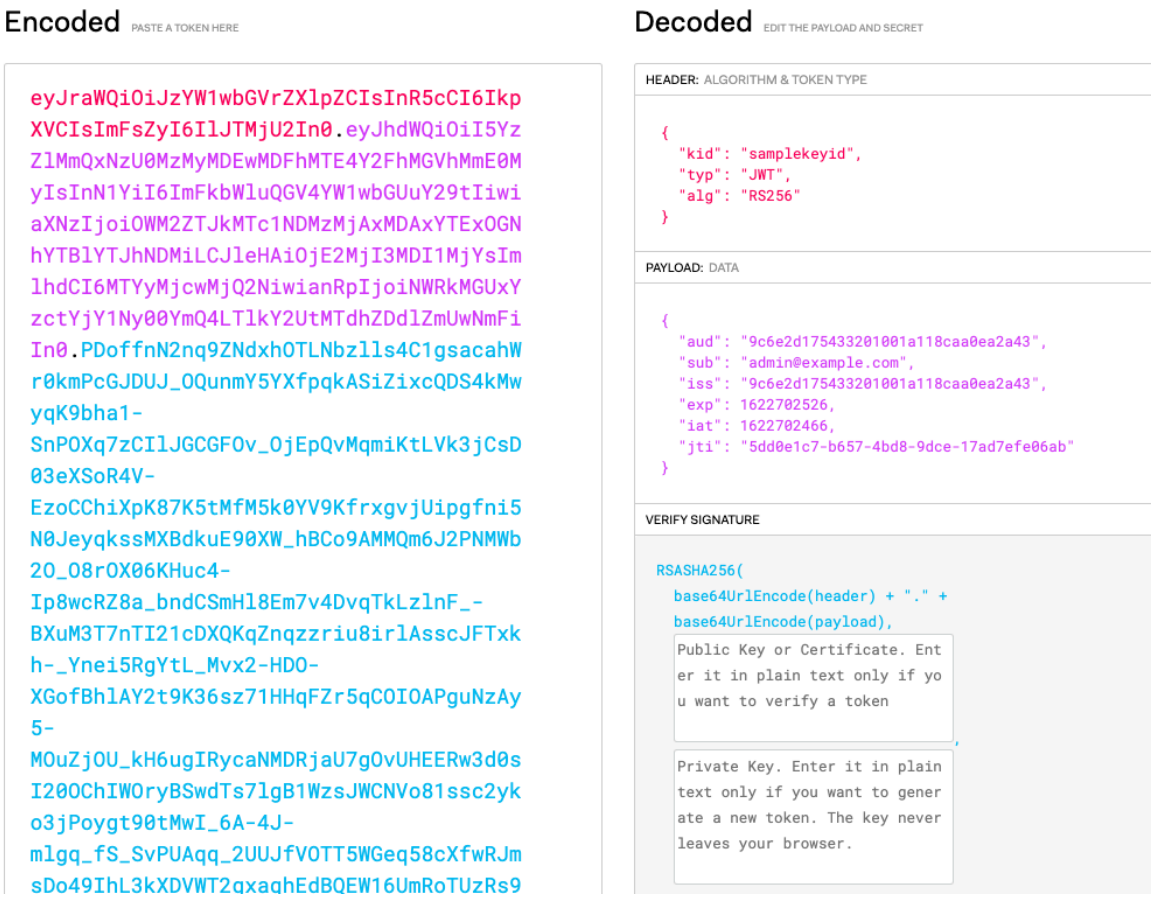
Die unterstützten Algorithmen für JSON Web Token (JWT): RS256, RS384, RS512, ES256, ES384, ES512.

Generieren Sie ein JWT mit den folgenden Ansprüchen auf Clientseite:

- `aud` : Muss mit dem Wert der Client-ID übereinstimmen.
- `Untergeordnet` : Muss ein Anwenderbezeichner sein, z. B. die E-Mail-Adresse des Anwenders, der Sie das Token zuordnen möchten.
- `iss` : Empfohlene Übereinstimmung mit dem Wert der Client-ID. Wenn `aud` Und `iss` Stimmt nicht überein, fügen Sie dann hinzu `iss` Wert in der Anspruchsvalidierung.
- `Verwendbar bis` : Beliebiger gewünschter Ablauf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für decodierte JSON-Webtoken



Konfiguration in ServiceNow

Warum und wann dieser Vorgang ausgeführt wird

Da die Verwendung des JWT-Gewährungstyps das Passwort nicht in der Anforderung enthält, ermöglicht dies eine höhere Sicherheit zwischen Webservices. Sie können beispielsweise eine externe Anwendung entwickeln und Token verwenden, um eingehende Anforderungen bei zu authentifizieren ServiceNow Instanz.

Erforderliche Rolle: Administrator

Weitere Informationen zu JSON-Webtoken finden Sie unter https://jwt.io/ .

Prozedur

1. Fügen Sie den öffentlichen Schlüssel der Client-App zu hinzu **sys_certificate** Tabelle.
2. Richten Sie die Konfiguration in ein ServiceNow Instanz zur Verifizierung des eingehenden JWT.
   a. Navigieren zu **System-OAuth** > **Applikationsregistrierung**an.
   b. Wählen Sie Aus **Erstellen Sie einen OAuth-JWT-API-Endpunkt für externe Clients** .
   c. Füllen Sie das Formular mit Informationen zu Ihrem Token aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth-JWT-Tabelle

Feld	Beschreibung
Name	Ein eindeutiger Name, der die Anwendung identifiziert, für die Sie JWT OAuth-Zugriff benötigen.
Client-ID	Die automatisch generierte eindeutige ID der Anwendung. Das System verwendet den Wert dieses Felds, um den öffentlichen oder freigegebenen Schlüssel abzurufen und das JWT zu validieren. Der Wert dieses Felds muss mit dem Wert der Ansprüche des Ausstellers und der Zielgruppe in JWT übereinstimmen.
Geheimer Clientschlüssel	Die Zeichenfolge des gemeinsamen Geheimnisses, die sowohl die Instanz als auch die Client-Anwendung oder -Website verwenden, um Kommunikation miteinander zu autorisieren. Lassen Sie dieses Feld leer, damit die Instanz automatisch ein geheimes Clientgeheimnis generiert. Um vorhandene geheime Clientgeheimnisse anzuzeigen, wählen Sie das Sperrsymbol aus. **Hinweis:** Wenn **Öffentlicher Client** Ist ausgewählt, können Sie auslassen **Geheimer Client-Schlüssel** .
Anwenderfeld	Feld in der Anwendertabelle (sys_user), das das System verwendet, um den Wert des Antragstellungsanspruchs in der JWT abzugleichen. Wenn Sie beispielsweise ein Token hinzufügen, das den Anspruchswert des Antragstellers user.name@example.com hat, legen Sie fest **Anwenderfeld** Bis **E-Mail** . Dieses Feld weist das System an, das E-Mail-Feld nach dem Wert user.name@example.com zu durchsuchen und den übereinstimmenden Anwenderdatensatz in der eingehenden Anforderung zu verwenden.
JTI-Verifizierung aktivieren	Wählen Sie diese Option aus, um bei jedem Tokenaustausch ein neues Token anzufordern. Standard: Ausgewählt.
Anwendung	Schreibgeschützter Anwendungsbereich. Dieses Feld wird automatisch gefüllt.
Zugänglich von	Bereichsübergreifende Zugriffsrichtlinie. Weitere Informationen finden Sie unter Einstellungen für Anwendungszugriff .
Lebensdauer von Zugriffstoken	Zeitraum, für den das Token gültig ist. Einheit: Sekunden
Taktversatz	Zulässige Zeitdifferenz zwischen Server- und Client-Uhren bei der Validierung von `Verwendbar bis` Und `nbf` Ansprüche im JWT. Einheit: Sekunden Standard: 300
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um nur Token für die Verwendung mit APIs zu aktivieren, die festgelegt sind, um das Authentifizierungsprofil zu aktivieren. Sie können Zugriffsgewährung mithilfe einer API-Zugriffsrichtlinie festlegen. Weitere Informationen finden Sie unter Erstellen Sie EINE REST-API-Zugriffsrichtlinie . Standard: Nicht Ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kommentare	Die der Anwendung zuzuordnenden Informationen.
Öffentlicher Client	Fügen Sie dieses Feld dem Formular hinzu, wenn der JWT-Client öffentlich ist. Wenn diese Option ausgewählt ist, müssen Sie keinen einschließen **Geheimer Client-Schlüssel** . Standard: Nicht Ausgewählt.
Client-Typ	Wählen Sie den Client-Typ basierend auf dem Typ Ihres Clients aus. Optionen: ▪ **IFrame eingebettet** ▪ **Integration als Anwender** ▪ **Integration als Service** Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

d. Speichern Sie das Formular.

e. Fügen Sie der zugehörigen Liste „JWT-Verifiziererzuordnungen“ Datensätze hinzu, um die JWT-Signatur zu überprüfen.

Tabelle „JWT-Verifiziererzuordnungen“

Feld	Beschreibung
Name	Name des JWT-Zuordnungsdatensatzes.
Kind	Schlüssel-ID aus JWT.
Freigegebener Schlüssel	Der freigegebene Schlüssel für die angegebene Schlüssel-ID.
Anwendung	Schreibgeschützter Anwendungsbereich.
Sys-Zertifikat	Zertifikatdatensatz in der Tabelle „X.509-Zertifikate“ (sys_certificate). Das Zertifikat, das in Schritt 1 hochgeladen wurde.

f. Fügen Sie der zugehörigen Liste „OAuth-JWT-Anspruchsvalidierungen“ alle anwenderdefinierten Ansprüche hinzu, die Ihrem JWT zugeordnet sind.

Sie müssen keine Datensätze für die folgenden erforderlichen Ansprüche hinzufügen:

- iss
- aud
- Untergeordnet
- exp

Hinweis:

- Wenn `aud` Und `iss` Stimmt nicht überein, fügen Sie dann hinzu `iss` Wert in der Anspruchsvalidierung.
- Für Zertifikate können Sie mehrere Überprüfungszuordnungen hinzufügen, die mehreren Schlüsseln zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „OAuth-JWT-Anspruchsvalidierungen“

Feld	Beschreibung
Mein externer Client	Wird automatisch mit dem OAuth-JWT-Datensatz ausgefüllt.
Anspruchwerttyp	Datentyp des Anspruchswerts.
Anspruchname	Name des Anspruchs, den Sie hinzufügen möchten.
Anspruchwert	Wert des Anspruchs.
Anwendung	Schreibgeschützter Anwendungsbereich.

3. Senden Sie eine Curl-Anforderung mit dem JWT-Token, um ein Zugriffstoken von Ihrer Instanz zu erhalten.

Example

Es folgt ein Beispiel für einen Curl-Befehl, der ein Zugriffstoken anfordert:

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&assertion=
 eyJraWQiOiJzYW1wbGVrZXIpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIIJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHI8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HflcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

Wenn der JWT-Client ein öffentlicher Client ist, z. B. das Mobile SDK, können Sie die Parameter „Client_ID“ und „Client_Secret“ aus der Anforderung auslassen. Es folgt ein Beispiel für einen Curl-Befehl, der ein Zugriffstoken anfordert, das Client_ID und Client_Secret auslässt:

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&assertion=
 eyJraWQiOiJzYW1wbGVrZXIpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIIJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHI8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HfIcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

Die Instanz gibt das Zugriffstoken in ihrer Antwort zurück:

```
{
   "access_token":
 "KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxNA",
   "scope": "useraccount",
   "token_type": "Bearer",
   "expires_in": 1799
}
```

Hinweis: Der eingehende JWT-Gewährungstyp enthält keine Aktualisierungstoken.

4. Führen Sie einen REST-API-Aufruf durch, um mit dem Zugriffstoken auf eine Ressource zuzugreifen.

Example

Im Folgenden finden Sie einen Curl-Befehl, um mit dem Token auf die Incident-Tabelle zuzugreifen.

```
$ curl -H "Authorization: Bearer
 KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxN"
https://instancename.service-now.com/api/now/v1/table/incident
```

Ergebnis

Das System ruft das Zugriffstoken im REST-Aufruf ab und ermöglicht den Zugriff auf die angeforderte Ressource.

Konfigurieren Sie einen OAuth-OIDC-Provider für die Annahme eines Drittpartei-Tokens

Sie können einen OAuth-OIDC-Provider so konfigurieren, dass Identitätstoken akzeptiert werden, die von einem externen OIDC-Anbieter mithilfe eingehender API-Aufrufe mit der Single Sign-on-Option (Multi-Provider SSO) generiert wurden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die ServiceNow AI Platform Unterstützt OIDC über unsere externe Single Sign-on (SSO)-Implementierung zusätzlich zu eingehenden API-Aufrufen. Ein Beispiel für eine OIDC-Anbieterkonfiguration finden Sie unter Azure AD wird eingerichtet . Ein SSO-spezifisches Beispiel für eine OIDC-Anbieterkonfiguration finden Sie unter OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.
   - Wählen Sie Aus **Neu** , Wählen Sie aus **Konfigurieren Sie einen OIDC-Provider, um ID-Token zu verifizieren** , Und füllen Sie dann das Formular aus.
   - Wählen Sie eine vorhandene Vorlage für einen OIDC-Provider aus (ADFS, Auth0, Azure AD, Google, Okta), und füllen Sie dann das Formular aus.

     Hinweis: OIDC-Provider-Vorlagen sind nach dem Laden von Demodaten mit dem Plugin OAuth 2.0 verfügbar.

Feld	Beschreibung
Name	Ein eindeutiger Name, der die OAuth-OIDC-Entität identifiziert.
Client-ID	Die Client-ID der Anwendung, die auf dem OAuth-OIDC-Server des Drittanbieters registriert ist. Dieser Wert muss mit dem Wert von übereinstimmen `aud` Anspruch im JWT-Token.
OAuth-API-Skript	Ein Skript, mit dem Sie Anforderungen und Antworten an einen externen OAuth-Provider anpassen können.
OAuth-OIDC-Providerkonfiguration	Die OIDC-Anbieter (ADFS, Auth0, Azure AD, Google, Okta) können zur Validierung des JWT-Tokens verwendet werden. Wählen Sie den Datensatz Ihrer OIDC-Anbieterkonfiguration aus, um zu validieren **Anwenderanspruch** Und **Anwenderfeld** Sind entsprechend festgelegt. Stellen Sie außerdem sicher, dass Sie die folgenden Felder ausfüllen: ○ **Aktivieren Sie die JTI-Anspruchsverifizierung** : Wenn aktiviert,die ServiceNow Die JWT-Tokenvalidierung validiert auch das vom Provider gesendete JTI. ○ **OIDC-Metadaten-URL** : Details der bekannten Konfiguration des OIDC-Anbieters. **Hinweis:** Wenn die Validierung nicht aktiviert ist, wird `jti` Kann nicht validiert werden, unabhängig davon, ob es im JWT-Token vorhanden ist. Der Anspruchsname im Token muss sein `jti` .
Taktversatz	Die Anzahl in Sekunden, für die die Einschränkung als gültig gilt. Der Standardwert ist 300.
Tokenbeschränkungen erzwingen	Wählen Sie diese Option aus, um nur Token für die Verwendung mit APIs zu aktivieren, die festgelegt sind, um das Authentifizierungsprofil zu aktivieren. Sie können Zugriffsgewährung mithilfe einer API-Zugriffsrichtlinie festlegen. Weitere Informationen finden Sie unter Erstellen Sie EINE REST-API-Zugriffsrichtlinie . Standard: Nicht Ausgewählt.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die OAuth-Anwendung zu aktivieren.
Client-Typ	Wählen Sie den Client-Typ basierend auf dem Typ Ihres Clients aus. Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **iFrame – eingebettet** ○ **Integration als Anwender** ○ **Integration als Service** Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

2. Wählen Sie **Absenden**.
   Der Datensatz wird in der Tabelle der Anwendungs-Registrys [oauth_entity] gespeichert.
   Wenn Ihre Instanz Token und Autorisierungscodes ausgibt, wird ein Datensatz in der Tabelle „Anwendungsregistrierungen“ [oauth_Entity] mit dem Typ erstellt **Externer OIDC-Anbieter** . Weitere Informationen finden Sie unter .
3. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsprofile“, um ein vom System generiertes Standardprofil für den neuen OAuth-Provider ohne Umfang zu validieren.
   Sie können ein OAuth-Anbieterprofil ändern oder hinzufügen, einschließlich Name, Gewährungstyp und OAuth-Umfang.
4. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsbereiche“, um alle verfügbaren OAuth-Bereiche für diesen OAuth-Provider zu definieren.
   Die definierten Umfänge können ausgewählt werden, wenn Sie ein Profil erstellen oder aktualisieren. Jeder definierte OAuth-Bereich enthält einen Namen und einen Umfang, den Sie aus der Anbieterspezifikation abrufen müssen, z. B. einen Lese- oder Schreibbereich. Jeder Umfang muss separat definiert werden.
5. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz Anwenderbereitstellung, um die automatische Anwenderbereitstellung zu aktivieren.

Option	Bezeichnung
Anwender automatisch bereitstellen	Option zum Aktivieren der erzwungenen Authentifizierung für Anwender.
Datenquelle bereitstellen	Die Datenquelle, die zum Transformieren eines OIDC-Tokens in ein verwendet werden soll ServiceNow Anwender. Verwenden Sie **Suchliste** Um die vordefinierte Datenquellenvorlage auszuwählen, öffnen Sie dann den Datensatz, um die transformierte Tabellenzuordnung zu konfigurieren. Beim Konfigurieren der Transformationszuordnung stammen die Quellfelder aus dem `JWT token`, Die Zielfelder stammen aus dem `sys_user`Tabelle.
Auf bereitgestellte Anwender angewendete Anwenderrollen	Die Anwenderrollen, die auf die neu bereitgestellten angewendet werden ServiceNow Anwender.

Example: Im Folgenden finden Sie ein Beispiel für eine Curl-Anforderung zum Aufrufen eines REST API-Aufrufs

Rufen Sie einen REST-API-Aufruf auf.

Führen Sie die nachfolgenden Schritte durch:

- Registrieren Sie die App im OpenID Connect-Provider.
- Konfigurieren Sie die OAuth-OIDC-Entität.
- Konfigurieren Sie den OIDC-Provider:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OIDC-Provider

OIDC-Provider	Name des OIDC-Providers.
OIDC-Metadaten-URL	Geben Sie die OIDC-Metadaten-URL (bekannte Konfigurations-URL) an. Diese Informationen werden verwendet, um die öffentlichen Schlüssel abzurufen, um das Token über zu validieren JWKS Endpunkt.
Anwenderanspruch	Der Anspruch, der anhand der Anwendertabelle validiert wird.
Anwenderfeld	Anwenderanspruch, der den Anwenderdatensatz identifiziert.
JTI-Anspruchzertifizierung aktivieren	Wenn diese Option aktiviert ist, validiert die Validierung des ServiceNow-JWT-Tokens auch das vom Anbieter gesendete JTI. **Hinweis:** Wenn die Validierung nicht aktiviert ist, wird `jti` Kann nicht validiert werden, unabhängig davon, ob es im JWT-Token vorhanden ist. Der Anspruchsname im Token muss sein `jti` . Diese Informationen werden verwendet, um Wiederholungsangriffe zu verhindern.

- Ruft ein JWT-Token ab.
- Rufen Sie einen REST-API-Aufruf auf.
  - Das ID-Token im Autorisierungsheader für den Zugriff auf die Tabellen-API oder den geskripteten Webservice.

```
curl -X GET --header "Accept:application/json"
 https://<instance_name>.service-now.com/api/now/table/incident/897b04f2dbd4a300a1
35364e9d961952 -k
--header "Authorization: Bearer
 eyJraWQiOiJjNTZtZTlXU0xPVnY3UFMwcTg4Qzl1b0lzNjFQYTdmUG4yZFVFOW9RNUg4Iiwi
YWxnIjoiUlMyNTYifQ.eyJzdWIiOiIwMHVnZDg1OD
VkczI1WXpUSjBoNyIsIm5hbWUiOiJpbXJhbiBhbGkiLCJsb2NhbGUiOiJlbi1VUyIsImVtYWlsIjoi
aW1yb241NDNAZ21haWwuY29tIiwidmVyIjoxLCJpc3MiOiJodHRwczovL2Rldi05MzQ
xMjEub2t0YXByZXZpZXcuY29tIiwiYXVkIjoiMG9hZ2Q4bzk3a2ICT3dwd0IwaDciLCJpYXQiOj
E1Mzc5MzMzMjYsImV4cCI6MTUzNzkzNjkyNiwianRpIjoiSUQueThVdXpWNUg2bm16SzRs
OTI1RFVrQnJoR1o1MmJzVVpGVHRVTEphQjg3ayIsImFtciI6WyJwd2QiXSwiaWRwIjoiMDBvZ
2Q4NTgycEFqZDZTemcwaDciLCJub25jZSI6InNub3ciLCJwcmVmZXJyZWRfdXNlcm5hbW
UiO
iJpbXJvbjU0M0BnbWFpbC5jb20iLCJnaXZlbl9uYW1lIjoiaW1yYW4iLCJmYW1pbHlfbmFtZSI6I
mFsaSIsInpvbmVpbmZvIjoiQW1lcmljYS9Mb3NfQW5nZWxlcyIsInVwZGF0ZWRfYXQiOj
E1Mzc5MzAxOTcsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJhdXRoX3RpbWUiOjE1Mzc5Mjk2Nj
F9.OG87SYxWFgHGlhBYby2H79diRm9rlYZTeEkIINRUatwg-p4739htB8xEY-5_t6yU_6k5w1
0pdgtt5M5QFZRPXVbQZNoGtY-Bxn0BjaimcFgoWfhY_0ldnGTkzN2RYyIHvrf9-yhxg347zvcz
mLrgMMa_VwG4rxrtE6rUXaIpIeIK5b-Deq8ADz8UTUTKpF_5RWk4X-oh5xK6BLniFHk4ShO
Zq2v_mjproXwKk5euJKrVrar2lQ4adZCOSTRuTf3ThMO5WDh0sel-82LngXtLzRJJ51IqxAsXns
0kJHLLqLtH1hXNRKfwT1ScQoE_OfWm4t0KryI2j4wSMEanFtLXIw"
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn der Anwender authentifiziert ist, wird eine gültige Anwendungs-/JSON-Antwort zurückgegeben. Andernfalls wird eine Fehlermeldung „Anwender nicht authentifiziert“ zurückgegeben.

```
User Not Authenticated
{"error":{"message":"User Not Authenticated","detail":"Required to provide Auth
 information"},"status":"failure"}
```

Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze

Konfigurieren Sie **Client-Typ** Feld für Konfigurationen im Zusammenhang mit OAuth- und SSO-Datensätzen.

Beim Einrichten von Sitzungen für verschiedene Anmeldetypen wie Web-UI (interaktive Anmeldung), iFrame Embedded, Embedded oder Integration können Sie den Clienttyp für die Datensätze OIDC (OAuth-Entität), SAML und Digest konfigurieren, die für verschiedene Anmeldungen verwendet werden.

Die Auswahlmöglichkeiten für den Client-Typ lauten wie folgt:

- **Iframe Eingebettet** : Kann für interaktive Anwendungen verwendet werden ServiceNow Instanz, die sich in einem iFrame auf den Websites von Drittparteien befindet. Wenn beispielsweise eine vertrauliche Tabelle vorhanden ist (Tabelle „sys_user“ – Telefonnummer des Anwenders), können Sie als Administrator die ACL konfigurieren, wobei das Attribut „sec“ (iframe Embedded) auf „falsch“ festgelegt ist, um zu verhindern, dass der Anwender in der eingebetteten iframe-Sitzung in der Drittpartei auf die Daten (Tabelleninformationen) zugreift.
- **Integration als Anwender** : Kann für Virtual Agent-Chat-Bot verwendet werden, die in Desktop-Apps wie Slack, Teams usw. installiert sind
- **Integration als Service** : Kann für die Integration von Computer zu Computer (Kommunikation zwischen Services) verwendet werden.

Hinweis:

- Für OIDC (OAuth-Entität): Alle Auswahlmöglichkeiten sind verfügbar.
- Für SAML und Digest: Nur iFrame eingebettet. Sie müssen das Formular bearbeiten und hinzufügen **Client-Typ** Feld zum Datensatz, und wählen Sie aus **Iframe Eingebettet** Client-Typ.
- Wenn **Client-Typ** Ausgewählt ist „keine“, dann gibt es keine Klassifizierung der Sitzung.

Es wird empfohlen, das Clienttypfeld für alle Datensätze zu verwenden, die für OIDC (OAuth-Entität), SAML und Digest erstellt wurden. Dadurch haben Sie eine bessere Kontrolle über alle Anmeldemethoden, die dieselben Konfigurationen haben, sich jedoch vom Client-Typ unterscheiden.

Wenn sich ein Anwender nach der Konfiguration des Felds über die entsprechende Konfiguration (OAuth oder SSO) anmeldet, wird nach erfolgreicher Authentifizierung die Sitzung basierend auf dem konfigurierten Clienttyp berücksichtigt, und dementsprechend wird die Sitzungszeitüberschreitung genutzt.

Für die aktuelle Sitzung ist das entsprechende Sicherheitsattribut enthalten oder kann verwendet werden, um zu verhindern, dass Anwender innerhalb des ausgewählten Clienttyps auf tabellenspezifische Informationen zugreifen. Weitere Informationen finden Sie unter OOB-Sicherheitsattribute (sofort einsatzbereit).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sitzungszeitüberschreitung für die Client-Typen

Im Folgenden finden Sie die Systemeigenschaften im Zusammenhang mit der Sitzungszeitüberschreitung für die verschiedenen Client-Typen:

- glide.session_timeout.iframe_embedded
- glide.session_timeout.integration_as_a_user
- glide.session_timeout.integration_as_a_service

Implizite OAuth-Berechtigungen

ServiceNow Instanzen unterstützen die implizite Gewährung eines Zugriffstokens.

Der implizite Gewährungstyp, auch bekannt als *`implicit grant code flow`*, Ermöglicht es, das Zugriffstoken direkt über den Anwender-Agent an die Client-Anwendung zu vergeben, bei dem es sich normalerweise um den Webbrowser oder das Mobilgerät handelt. Es werden keine Aktualisierungstoken gewährt. Der Endanwender muss weiterhin Zugriff auf die geschützte Ressource in der Instanz gewähren, genau wie beim Standard.

Flow-Prozess für implizite OAuth-Gewährung

Genau wie beim standardmäßigen Autorisierungscode-Flow-Prozess fordert die Client-Anwendung die Verwendung der eingeschränkten Ressource in der Instanz an, und der Endanwender genehmigt sie. Die Anforderung hat die Form einer URL, die an die Instanz gesendet wird. Die URL muss die folgenden Parameter enthalten:

- Client_ID=<erforderliche Client-ID> . Dies ist obligatorisch, um zu identifizieren, auf welche geschützte Ressource die Clientanwendung Zugriff hat.
- Response_type=Token . Dies ist obligatorisch, um das Zugriffstoken direkt anzufordern (im Gegensatz zur Anforderung eines Autorisierungscodes). Der Wert muss sein `Token` Für implizite Zuschüsse. Im Beispiel des Standard-Autorisierungscode-Flows lautet der Antworttyp `Code` .
- Redirect_URI= <a URL>: Der Standort, an den das Token gesendet wird.

Der Autorisierungsserver sendet das Zugriffstoken anstelle eines Autorisierungscodes über den Anwender-Agent an die Client-Anwendung.

Hier ist ein Beispiel für eine Anforderung zum ABRUFEN der JSON-Nutzlast von Daten für die Tabelle „Incident“ [Incident]:

```
https://myinstance.servicenow.com/oauth_auth.do?response_type=token&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Wenn der Anwender Zugriff gewährt, wird das Token in der Umleitungs-(Rückruf-)URL enthalten:

```
https/http://{callbackURL}?access_token={the_token}
```

Client-Anmeldeinformationen

Verwenden Sie den Berechtigungstyp „OAuth-Client-Anmeldeinformationen“ für eingehende Integrationen von einem OAuth-Client eines Drittanbieters für ServiceNow® Plattform.

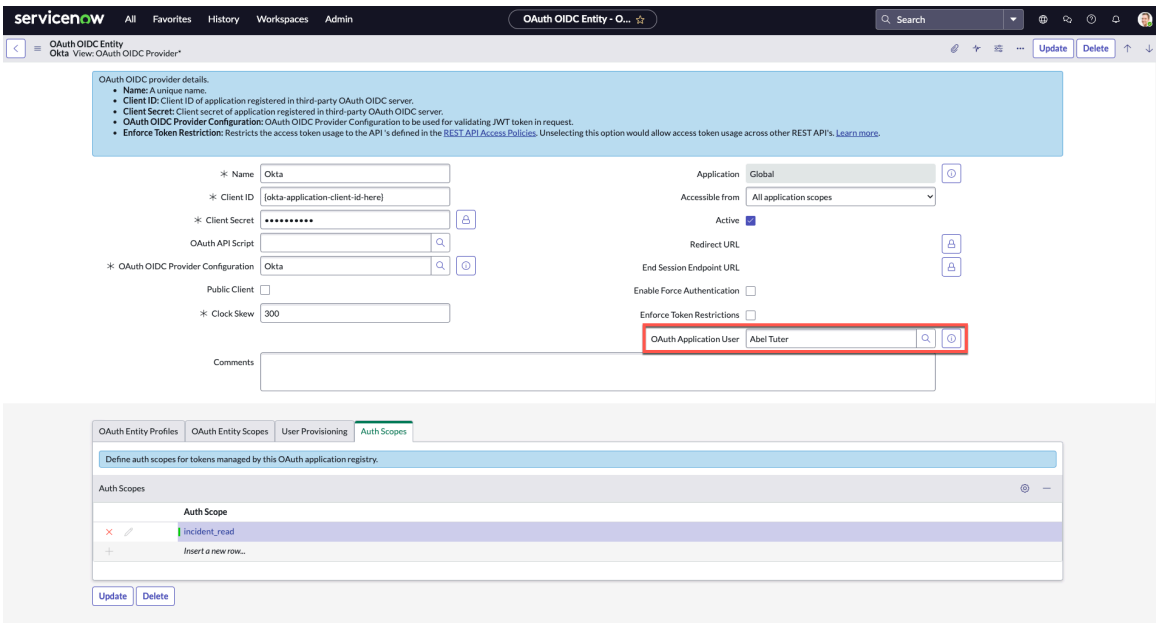
Die Administratoren können den Gewährungstyp „Client-Anmeldeinformationen“ (CC) verwenden, um die Integration von einem OAuth-Client eines Drittanbieters in zu aktivieren ServiceNow Plattform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Gewährungstyp für eingehende Client-Anmeldeinformationen ist eine Fähigkeit, die über eine Systemeigenschaft gesteuert werden kann. Standardmäßig ist die Systemeigenschaft „falsch“.

Um den Gewährungstyp „Client-Anmeldeinformationen“ zu verwenden, müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie `glide.oauth.inbound.client.credential.grant_type.enabled` Systemeigenschaft.
- Fügen Sie hinzu **OAuth-Anwendungsanwender** Feld zum Formular „OAuth-Entität“.



Erstellen Sie die Systemeigenschaft Client-Anmeldeinformationen

Erstellen Sie `glide.oauth.inbound.client.credential.grant_type.enabled` Systemeigenschaft zur Verwendung des Gewährungstyps „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen.

Vorbereitungen

Erforderliche Rolle: Administrator

Erforderliches Plugin: OAuth 2,0.

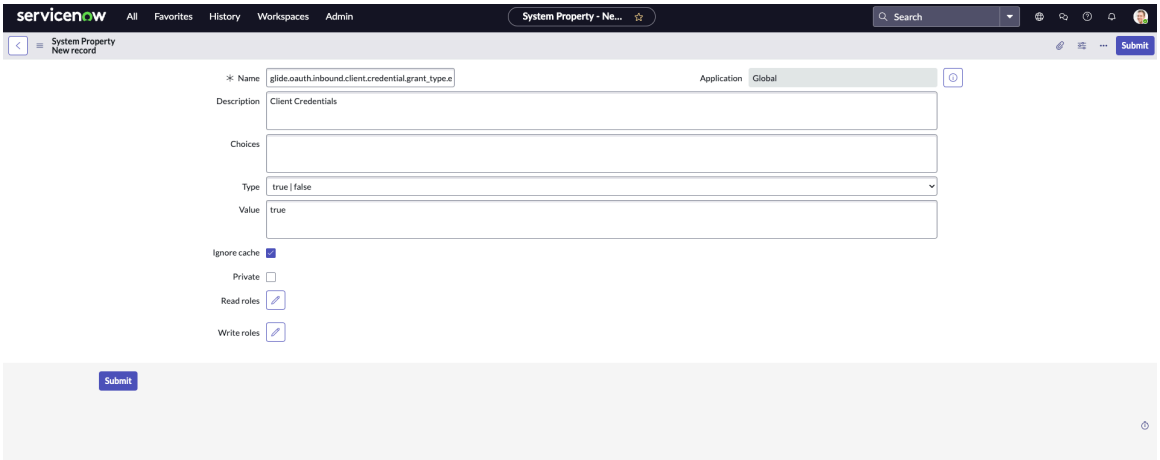
Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein.
   Die gesamte Liste der Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties] wird angezeigt.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die folgenden Felder aus.

Feld	Beschreibung
Name	Name der Eigenschaft, die Sie erstellen. In diesem Fall `glide.oauth.inbound.client.credential.grant_type.enabled`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Geben Sie einen kurzen, beschreibenden Ausdruck ein, der die Funktion der Eigenschaft beschreibt.
Typ	Wählen Sie den entsprechenden Datentyp aus der Liste aus. In diesem Fall Wahr| falsch .
Wert	Legen Sie den gewünschten Wert für die Eigenschaft fest. In diesem Fall Wahr Zum Aktivieren des Gewährungstyps für Client-Anmeldeinformationen für eingehende OAuth-Integrationen.



Hinweis: Andere Felder im Formular wie Auswahlmöglichkeiten, Cache ignorieren, Privat, Rollen lesen und Rollen schreiben können entsprechend Ihren Anforderungen konfiguriert werden S .

4. Wählen Sie **Absenden**.

Hinweis: Wenn **Cache ignorieren** Ist das Kontrollkästchen aktiviert, leert das System den Server-Cache, wenn der Parameter geändert wird.

Als Nächstes müssen Sie einen OAuth-Client (OAuth-API-Endpunkt für externen Client) erstellen und dem OAuth-Client-Datensatz das Feld „OAuth-Anwendungsanwender“ hinzufügen.

Fügen Sie den OAuth-Anwendungsanwender hinzu

Fügen Sie das Feld OAuth-Anwendungsanwender im Formular „OAuth-Entität“ hinzu, um den Gewährungstyp „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen zu verwenden.

Vorbereitungen

Erforderliche Rolle: Administrator

Erforderliches Plugin: OAuth 2,0.

Sie müssen einen OAuth-Client erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Endpunkt für Clients, um auf die Instanz zuzugreifen.

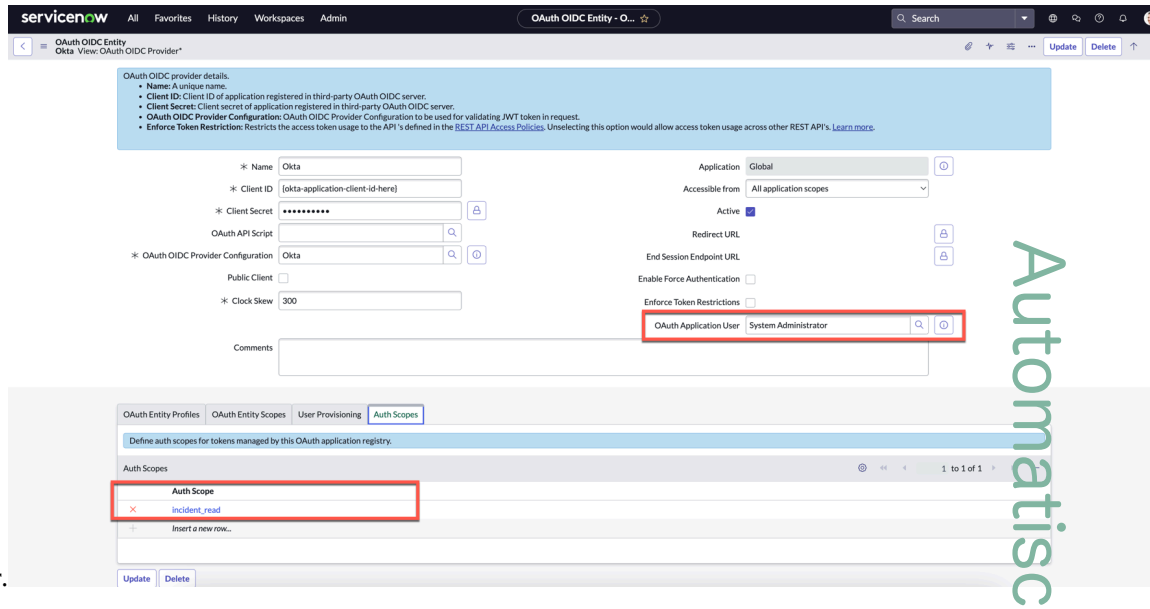
Prozedur

1. Öffnen Sie den erstellten OAuth-Client-Datensatz.
2. Wählen Sie im Seitenheader das Symbol weitere Optionen aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Auswahlvorgang **Konfigurieren** > **Formulardesign**an.
4. Fügen Sie auf der Seite „Formulardesign“ hinzu **OAuth-Anwendungsanwender** Aus der Liste der Felder.
5. Speichern oder aktualisieren Sie das Formular.
6. Wählen Sie den Anwender für aus **OAuth-Anwendungsanwender** .
   Beispiel:



Systemadministrator.

> **Hinweis:** Sie müssen den REST API-Authentifizierungsbereich mit dem Gewährungstyp Client-Anmeldeinformationen verwenden, um den Zugriff zu steuern, der dem Drittanbieterclient bereitgestellt wird.

7. Speichern oder aktualisieren Sie das Formular.

Jede Autorisierungsanforderung mit **Gewährungstyp** Als **Client-Anmeldeinformationen** , **Client-ID** , Und **Geheimnis** Wird für den zugehörigen OAuth-Anwendungsanwender in übergeben ServiceNow®.

> **Hinweis:** Wenn der OAuth-Anwendungsanwender im OAuth-Client-Datensatz nicht ausgewählt ist oder die Eigenschaft „Client-Anmeldeinformationen“ auf festgelegt ist `Falsch` , Wird die Autorisierungsanforderung nicht übergeben.

Verwalten Sie OAuth-Token

Öffnen Sie OAuth-Token, um Zugriff auf eingeschränkte Ressourcen zu gewähren.

Vorbereitungen

Erforderliche Rolle: Beliebiger Anwender oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

OAuth-Token, die von der Instanz und dem externen OAuth-Anbieter ausgegeben werden, werden in der Tabelle „oauth_credential“ gespeichert.

Einige der wichtigen Spalten in dieser Tabelle:

- Token: Wert des Tokens, das von ausgegeben wurde ServiceNow Instanz.
- Typ: Bestimmt, ob das Token Zugriffstoken oder Aktualisierungstoken ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Läuft ab: Daten/Uhrzeit, zu der das Zugriffs- oder Aktualisierungstoken abläuft.
- Erhaltenes Token: Wert des Tokens, das von einem Drittanbieter-OAuth ausgegeben wurde. Dieser Wert hat ein verschlüsseltes Format.

Token-Ablauf und -Gültigkeit sind wie folgt:

- Zugriffstoken: Standardmäßig gibt eine Instanz Zugriffstoken mit einer Lebensdauer von 30 Minuten aus, wenn die Instanz der OAuth-Anbieter ist.
- Aktualisierungstoken: Standardmäßig gibt eine Instanz Aktualisierungstoken mit einer Lebensdauer von 100 Tagen aus, wenn die Instanz der OAuth-Anbieter ist.

Prozedur

1. Navigieren Sie zu einer der folgenden Menüoptionen:
   - **Self-Service** > **Meine verbundenen Apps** Um die Token anzuzeigen, die die Instanz erstellt hat, wenn Sie Zugriff auf eine Ressource in der Instanz gewährt haben.
   - **System-OAuth** > **Tokens verwalten** Um alle Token anzuzeigen. Nur Administratoren können auf dieses Modul zugreifen.
2. Klicken Sie auf **Name** Zum Öffnen des Tokens.
3. Klicken Sie Auf **Zugriff Widerrufen** Um den Zugriff auf die eingeschränkte Ressource zu verhindern.

   Sie können auch andere Informationen zum Token anzeigen, einschließlich des Bereichs, auf den es Zugriff zulässt, und des Ablaufdatums.

   Sie können auswählen **Abgelaufene OAuth-Anmeldeinformationen bereinigen** Datensatz auf der Seite „Zeitplan“ (sys.Auslöser.Liste) Und konfigurieren Sie Folgendes:

   - **com.snc.platform.security.oauth.is.active** : Standardmäßig ist der Wert auf „wahr“ festgelegt.
   - **com.snc.platform.security.oauth.hours.expired.credential.is.kept** : Legen Sie den Wert basierend auf Ihren Anforderungen fest, um die Anzahl der Stunden zu bestimmen, die abgelaufen bleiben sollen `oauth` Anmeldeinformationen im System.
   - **com.snc.platform.security.oauth.day.old.credential.is.kept** : Legen Sie den Wert basierend auf Ihrer Anforderung fest, um die Anzahl der Tage zu bestimmen, die abgelaufen bleiben sollen `oauth` Anmeldeinformationen im System.

Widerrufen Sie ein OAuth-Token

Sie können aus Sicherheitsgründen einen OAuth-Zugriff widerrufen oder ein Aktualisierungstoken aktualisieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Das Widerrufen des Tokens bezieht sich auf die Situation, in der Ihre Instanz als OAuth-Ressourcenserver fungiert. Sie können das Token über eine URL widerrufen.

Prozedur

Greifen Sie mit auf Ihre Instanz zu `oauth_revoke_Token.do` Und fügen Sie das Zugriffs- oder Aktualisierungstoken an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: https://[Your_ServiceNow_Instance]:[port]/oauth_revoke_token.do?token=[access oder Aktualisierungstoken] Ohne die Klammern [ ] .

Ergebnis
Für diesen Endpunktzugriff ist keine Authentifizierung erforderlich. Das Token in dieser Anforderung ist als abgelaufen markiert.

OAuth ausgehend

Mit OAuth ausgehend können Sie Daten von einem Drittanbieter in Ihre Instanz abrufen.

Sie müssen über die Rolle „Security_admin“ verfügen, um die OAuth-Integration zu verwalten.

Sie können ausgehende OAuth 2,0 für die folgenden Gewährungstypen konfigurieren:

- **Stellen Sie eine Verbindung zum Drittanbieter her** : Verwenden Sie die Client-ID und das Geheimnis, um es an den OAuth-Provider zu senden. Weitere Informationen finden Sie unter Stellen Sie eine Verbindung zu einem OAuth-Drittanbieter her.
- **JWT Bearer**: Ein Autorisierungsserver validiert ein JWT-Token, das die Weitergabe von Identitäts- und Sicherheitsinformationen zwischen Sicherheitsdomänen ermöglicht. Weitere Informationen finden Sie unter Richten Sie den OAuth-Provider mit dem JWT-Bearer-Gewährungstyp ein.
- **SAML2-Bearer** : Generiert die SAML2-Assertion und tauscht die Assertion dann für die Zugriffstoken mit dem Provider aus.

  Hinweis: Für ausgehende Anforderung an SuccessFactors Verwenden Sie **SAML2-Bearer** Als Standardgewährungstyp. Um mehr über die Konfiguration zu erfahren **SAML2-Bearer** , Siehe Beispiel in Richten Sie ein v4.x.x .

- **Autorisierungscode**: Der Code, der dem Client gewährt wird, um ein Zugriffstoken zu erhalten, das dann verwendet wird, um Zugriff auf die Ressource zu erhalten. Wenn Sie diese Option auswählen, benötigen Sie eine Autorisierungs-URL (die URL des Autorisierungsservers).
- **Anmeldeinformationen des Ressourcenbesitzers**: Der Benutzername und das Passwort des Benutzers, der versucht, auf die Ressource zuzugreifen.
- **Client-Anmeldeinformationen**: Die Client-ID und der Client-Secret, die beide zum Abrufen des Zugriffstokens verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt.
- **MID-Server** : Die MID-Server erleichtern die Kommunikation und den Datenverkehr zwischen einem einzelnen ServiceNow® Instanz und externe Anwendungen, Datenquellen und Services. Verwenden Sie die OAuth-Gewährungstypen Autorisierungscode, Passwortanmeldeinformationen des Ressourcenbesitzers, SAML-Bearer und JWT-Bearer-OAuth-Gewährungstypen für ausgehende Integrationsanforderungen über den MID-Server. Persönliche Authentifizierung wird auch über den MID-Server unterstützt.

Sie können konfigurieren **OAuth-Anbieterszenario** (Ausgehend): Ihre Instanz ruft Daten von einem Drittanbieter ab.

Hinweis: Sie müssen sich zum ersten Mal vom Anwender authentifizieren, um den Token-Post abzurufen. Sie müssen sich vor Ablauf des Tokens nicht mit einem Anwenderaccount authentifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie eine Verbindung zu einem OAuth-Drittanbieter her

Konfigurieren Sie, wie die Client-ID und das Geheimnis an Ihren OAuth-Provider gesendet werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** Und klicken Sie dann auf **Neu** .
2. Klicken Sie auf der Seite „Interceptor“ auf **Stellen Sie eine Verbindung zu einem OAuth-Drittanbieter her** Und füllen Sie dann das Formular aus.

Feld	Beschreibung
Name	Eindeutiger Name für die Drittpartei-OAuth-Verbindung.
Client-ID	Die Client-ID der Anwendung, die auf dem OAuth-Server des Drittanbieters registriert ist.
Geheimer Clientschlüssel	Das geheime Clientgeheimnis der Anwendung, die auf dem OAuth-Server des Drittanbieters registriert ist.
OAuth-API-Skript	Das Skript, das zum Anpassen der Anforderung und Antwort an den externen OAuth-Provider verwendet wird.
Logo-URL	Die URL des OAuth-Anwendungslogos.
Standardgewährungstyp	Der Standardgewährungstyp, der zum Erstellen des Tokens verwendet wird. Zur Auswahl stehen: ○ **Autorisierungscode**: Der Code, der dem Client gewährt wird, um ein Zugriffstoken zu erhalten, das dann verwendet wird, um Zugriff auf die Ressource zu erhalten. Wenn Sie diese Option auswählen, benötigen Sie eine Autorisierungs-URL (die URL des Autorisierungsservers). ○ **Anmeldeinformationen des Ressourcenbesitzers**: Der Benutzername und das Passwort des Benutzers, der versucht, auf die Ressource zuzugreifen. ○ **Client-Anmeldeinformationen**: Die Client-ID und der Client-Secret, die beide zum Abrufen des Zugriffstokens verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt. ○ **JWT Bearer**: Ein Autorisierungsserver validiert ein JWT-Token, das die Weitergabe von Identitäts- und Sicherheitsinformationen zwischen Sicherheitsdomänen ermöglicht. ○ **SAML2-Bearer** : Generiert die SAML2-Assertion und tauscht die Assertion dann für die Zugriffstoken mit dem Provider aus. **Hinweis:** Für ausgehende Anforderung an SuccessFactors Verwenden Sie **SAML2-Bearer** Als Standardgewährungstyp.
Lebensdauer von Aktualisierungstoken	Zeit in Sekunden, die das Aktualisierungstoken gültig ist. Die Standardzeit beträgt 8.640.000 Sekunden.
Öffentlicher Client	Ermöglicht öffentlichen Clients, PKCE für eine Autorisierung zu benötigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie können nur den Autorisierungscode als verwenden *Default Grant type*Wenn PKCE aktiviert ist.
Abfragecodemethode	Die im OAuth-PCKE-Workflow verwendete Code-Abfragemethode. Zur Auswahl stehen: ○ S256 [Standard] ○ Nur ○ Keine
Kommentare	Fügen Sie Kommentare zur OAuth-App hinzu.
Anwendung	Anwendung und Umfang, die diesen Datensatz enthalten.
Zugänglich von	Machen Sie diese App über alle Anwendungsbereiche oder nur über diesen Bereich zugänglich.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die App zu aktivieren.
Autorisierungs-URL	Der OAuth-Autorisierungscode-Endpunkt.
Token-URL	Der OAuth-Server-Token-Endpunkt.
Token-Sperr-URL	Der OAuth-Server-Token-Widerrufsendpunkt.
Umleitungs-URL	Der OAuth-Rückrufendpunkt. Wenn leer, generiert die Instanz automatisch einen Eintrag.
Gegenseitige Authentifizierung aktivieren	Aktivieren Sie das Kontrollkästchen, um die gegenseitige Authentifizierung für die Tokenanforderung und den Widerruf zu verwenden. Für diese Funktion muss ein Profil für gegenseitige Authentifizierung angegeben werden.
Anmeldeinformationen senden	Der OAuth-Client füllt die Client-Anmeldeinformationen in der Anforderung aus: ○ In Anforderungstext (URL-codiertes Formular) ○ Header für Basisautorisierung ○ Als Private Key JWT
Client-Typ	Wählen Sie den Client-Typ basierend auf dem Typ Ihres Clients aus. Optionen: ○ **iFrame – eingebettet** ○ **Integration als Anwender** ○ **Integration als Service** Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

3. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsprofile“, um ein vom System generiertes Standardprofil für den neuen OAuth-Provider ohne Umfang zu validieren.
   Sie können ein OAuth-Anbieterprofil ändern oder hinzufügen, einschließlich Name, Gewährungstyp und OAuth-Umfang.
4. **Wahlweise:** Wechseln Sie zur zugehörigen Liste im Datensatz „OAuth-Entitätsbereiche“, um alle verfügbaren OAuth-Bereiche für diesen OAuth-Provider zu definieren.
   Sie können die Bereiche auswählen, wenn Sie ein Profil erstellen oder aktualisieren. Jeder OAuth-Bereich enthält einen Namen und einen Umfang, den Sie aus der Spezifikation des Anbieters abrufen müssen, z. B. einen Lese- oder Schreibbereich. Jeder Umfang muss separat definiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JWT Bearer

JSON-Webtoken (JWTs) ermöglichen die Konfiguration von Server-zu-Server-API-Interaktionen zwischen ServiceNow Und externe API-Anbieter, ohne dass ein Anwendereingriff erforderlich ist.

Die Bearer-Gewährung für JSON-Webtoken (JWT) ist eine JSON-Zeichenfolge, die Anspruchswerte enthält, die von den JWT-Grant-Handlern am Ende des Autorisierungsservers ausgewertet und validiert werden, bevor ein Zugriffstoken ausgegeben wird.

Mit dem JWT-Bearer-Gewährungstyp können Sie den OAuth 2,0-JWT-Bearer-Gewährungs-Flow für ausgehende Rest-Nachrichten konfigurieren.

Richten Sie den OAuth-Provider mit dem JWT-Bearer-Gewährungstyp ein

JSON-Webtoken (JWTs) ermöglichen die Konfiguration von Server-zu-Server-API-Interaktionen zwischen ServiceNow Und externe API-Anbieter, ohne dass ein Anwendereingriff erforderlich ist. Diese Unterstützung ermöglicht IntegrationHub Oder andere automatisierte Aufgaben, die JWTs verwenden, um API- und Serviceintegrationen mit verschiedenen Anbietern zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Aufgaben zeigen, wie ServiceNow Kann so eingerichtet werden, dass JWTs für OAuth 2,0-Client-Authentifizierungs- und Autorisierungsberechtigungen verwendet werden. ServiceNow Ist der OAuth-Client, und Sie können einen OAuth-Provider wie Box oder DocuSign konfigurieren.

Prozedur

1. Laden Sie das Java Key Store-Zertifikat hoch
   Hängen Sie ein JKS-Zertifikat an Ihre Instanz an, um die JWT-Client-Authentifizierung zu aktivieren.
2. Konfigurieren Sie einen JWT-Signaturschlüssel
   Erstellen Sie einen JWT-Signaturschlüssel, der Ihrem Java Keystore-(JKS-)Zertifikat zugewiesen werden soll.
3. Erstellen Sie einen JWT-Provider mit einem JWT-Signaturschlüssel
   Fügen Sie Ihrem einen JWT-Provider hinzu ServiceNow Instanz.
4. Stellen Sie eine Verbindung zu einem OAuth-Drittanbieter her
   Erstellen Sie einen OAuth-Drittanbieter mit einem JWT-Bearer als Standardgewährungstyp in ServiceNow Anwendungsregistrierung.
5. OAuth-Profile angeben
   Öffnen Sie das OAuth-Entitätsprofil des OAuth-Providers, und weisen Sie einen JWT-Provider zu.

Laden Sie das Java Key Store-Zertifikat hoch

Sie können ein Java Keystore-(JKS-)Zertifikat an Ihre Instanz anhängen, um die JWT-Clientauthentifizierung zu aktivieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **x509-Zertifikat**an.
2. Füllen Sie das Formular nach Bedarf aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Name	Ein eindeutiger Name für Ihr Zertifikat.
Benachrichtigung bei Ablauf	Geben Sie an, wer benachrichtigt werden soll, wenn das Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Senden Sie eine E-Mail-Benachrichtigung an Ihren Zertifikatmanager, bevor Ihr Zertifikat abläuft.
Aktiv	Aktiviert die Verwendung des Zertifikats für Token-anforderungen.
Typ	Der Typ des Zertifikats, das Sie hochladen.
Läuft in Tagen ab	Die Anzahl der Tage, bis das Zertifikat abläuft.
Schlüsselspeicher-Passwort	Das dem Zertifikat zugeordnete Passwort.
Kurzbeschreibung	

3. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen JWT-Signaturschlüssel

Erstellen Sie einen JSON Web Token (JWT)-Signaturschlüssel, der Ihrem Java Keystore (JKS)-Zertifikat zugewiesen werden soll.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: Wenn Sie hinzufügen möchten **X.509-Zertifikat SHA-1 Fingerabdruck-int (x5t)** Dem Header als Teil des JWT-Schlüssels müssen Sie das Formular konfigurieren und hinzufügen **X.509-Zertifikat SHA-1 Fingerabdruck-int (x5t)** Feld.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Schlüssel**an.
2. Füllen Sie das Formular nach Bedarf aus.

Option	Bezeichnung
Name	Ein eindeutiger Name für Ihre JWT-Schlüsselsignaturkonfiguration.
Signatur-Schlüsselspeicher	Der Schlüsselspeicher, der beim Signieren der JWT festgelegt wurde.
Schlüssel-ID	Die Schlüssel-ID (Kid) hilft zu identifizieren, welcher Schlüssel verwendet wird, wenn mehrere Schlüssel zum Signieren von Token verwendet werden. **Hinweis:** Wenn Sie dieses Feld konfigurieren, ist der Schlüssel-ID-Anspruch in JWT enthalten. Wenn Sie dieses Feld nicht konfigurieren, hat Ihr JWT keinen Schlüssel-ID-Anspruch.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Signaturalgorithmus	Der Algorithmus, der zum Signieren mit dem JWT-Schlüssel verwendet werden soll. RSA 256 ist der einzige verfügbare Algorithmus.
Signaturschlüssel-Passwort	Das dem Signaturschlüssel zugeordnete Passwort.
Aktiv	Legen Sie fest, dass der JWT-Schlüsselalias aktiv von einem JWT-Provider referenziert wird.

3. Klicken Sie auf **Absenden**.

Erstellen Sie einen JWT-Provider mit einem JWT-Signaturschlüssel

Fügen Sie Ihrem einen JSON-Webtoken-Anbieter (JWT) hinzu ServiceNow Instanz.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Anbieter**an.
2. Füllen Sie das Formular aus, und klicken Sie auf **Übermitteln** .

Option	Bezeichnung
Name	Ein eindeutiger Name für Ihre JWT-Provider-Konfiguration.
Ablaufintervall (Sek.)	Die Lebensdauer der vom JWT-Provider generierten Token in Sekunden.
Signierkonfiguration	Die ServiceNow Anzuwendende JWT-Signaturschlüsselkonfiguration.

JSON-Webtoken (JWT) generieren

Erstellen Sie ein JSON-Webtoken (JWT), um Ansprüche zwischen zwei Parteien auf der sicher darzustellen ServiceNow AI Platform.

Die GlideJWT-API Ist eine bereichsbezogene, skriptfähige API, die eine generiert JWT . Vor dem Generieren der JWT sind drei Argumente erforderlich:

- SYS_ID von JWT Anbieter
- Serialisierter JSON-Header
- Serialisierte JSON-Nutzlast

Es gibt zwei JWT-API-Skripts, JWTTokenInternal und JWTTokenRestricted, die Sie beim Konfigurieren eines JWT-Providers verwenden können. Mit dem Skript JWTTokenRestricted können Administratoren konfigurieren, wer eine JWT generieren kann. Das JWTTokenInternal-Skript ist schreibgeschützt und ermöglicht nur angemeldeten Anwendern das Generieren einer JWT.

So generieren Sie eine JWT:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- JWT-Schlüssel mit einem gemeinsam genutzten Schlüssel (HMAC) oder einem Signaturschlüsselspeicher (RSA) erstellen
- Ordnen Sie einen JWT-Provider der Signaturkonfiguration zu, die einen JWT-Schlüssel referenziert

Sie können die API verwenden, um Ihr Token zu erstellen.

Sie können Standard und anwenderdefiniert verwenden Ansprüche Beim Konfigurieren eines JWT-Providers. Sie können Übergeben Sie dynamische Header- und Nutzlastansprüche Als Teil der generateJWT-API-Signatur.

Beispielskript zum Testen der API:

```
var jwtAPI = new sn_auth.GlideJWTAPI();
var headerJSON = {  "kid": "a1234"  };
var header = JSON.stringify(headerJSON);

var payloadJSON = { "jti": "testjti", "iss": "testiss", "sub": "testsub" };
var payload = JSON.stringify(payloadJSON);

var jwtProviderSysId = "7a40dde2d5303300964fb7c8f3c14ab5";
var jwt = jwtAPI.generateJWT(jwtProviderSysId, header, payload);

gs.info("JWT:" + jwt);
```

OAuth-Client-APIs

Die OAuth-Client-API bietet Methoden zum anfordern und Widerrufen von OAuth-Token.

Der OAuth-Client stellt diese Klassen bereit:

- GlideOAuthClient : Methoden zum anfordern und Widerrufen der Aktualisierungs- und Zugriffstoken.
- GlideOAuthClientRequest : Methoden für die Verarbeitung von Client-Anforderungen.
- GlideOAuthClientResponse : Methoden für die Verarbeitung von Clientantworten.
- GlideOAuthToken : Methoden zum Abrufen des Zugriffstoken und Informationen zum Zugriffstoken.

Sie können auch die OAuthUtil-Skripteinbindung anpassen, um die Anforderungsparameter abzufangen und auch die Antworten externer OAuth-Anbieter zu analysieren.

Wenn Sie OAuth-Klassen in einem bereichsbezogenen Skript verwenden, verwenden Sie `sn_auth` Namespace-Bezeichner.

OAuth-Parameter für die Unterstützung von Standardprofilen

Für das Standardprofil-Feature ist ein Parametersatz erforderlich, den Sie mit dem API *`setParameter()`* zur Angabe des OAuth-Anforderers, eines Kontexts für die Anforderung und des Anbieterprofils verwenden können.

Im OAuth-Provider-Szenario müssen drei Parameter festgelegt werden, die dem OAuth-Provider mitteilen, welches OAuth-Profil standardmäßig verwendet werden soll. Wenn diese drei Parameter festgelegt sind, wird das Zugriffs-Token in der Instanzdatenbank gespeichert. Verwenden Sie die Parameter mit *`GlideOAuthClientRequest`*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth-Parameter für die Unterstützung von Standardprofilen

Parameter	Beschreibung
oauth_requestor	Die sys_id des Objekts. Dies kann ein Benutzerdatensatz oder ein E-Mail-Account sein.
oauth_requestor_context	Deskriptor, der den Kontext für den OAuth-Anforderer bereitstellt. Verwenden Sie als bewährte Methode den Namen der Tabelle, in der das Objekt oauth_requestor gespeichert wird.
oauth_provider_profile	Die sys_ID des OAuth-Profildatensatzes, der der Standard ist (siehe Geben Sie ein OAuth-Profil an).

Sie müssen keine Parameter zum Festlegen von Grant-Typ und Gültigkeitsbereich verwenden, da die Werte im OAuth-Profildatensatz konfiguriert sind. Wenn Sie die Parameter nicht verwenden, können Sie die GlideOAuthClientRequest-API-Methoden *setScope* und *setGrantType* verwenden. Weitere Informationen finden Sie unter SetScope Und SetGrantType .

JWT-Unterstützung für privaten Schlüssel für OAuth 2,0-Clientauthentifizierung

Unterstützt JWT-Unterstützung für OAuth 2,0-Clientauthentifizierung.

Die JWT-Clientauthentifizierung mit privatem Schlüssel ist eine Authentifizierungsmethode, die von Clients zur Authentifizierung beim Autorisierungsserver verwendet werden kann, wenn der Token-Endpunkt verwendet wird.

In diesem Authentifizierungsmechanismus können sich nur Clients authentifizieren, die einen öffentlichen Schlüssel registriert und eine JWT mit diesem Schlüssel signiert haben.

Das JWT muss ERFORDERLICHE Anspruchswerte enthalten und kann OPTIONALE Anspruchswerte enthalten. Um mehr über die Anspruchswerte zu erfahren, die für JWT für erforderlich sind Private_key_jwt Authentifizierung siehe Abschnitt „Clientauthentifizierung“ in OpenID Connect-Core Dokumentation.

Hinweis: Das Authentifizierungstoken muss als Wert des Parameters „Client_Assertion“ gesendet werden. Der Wert von **Client_Assertion_type** Parameter muss sein URN:ietf:params:oauth:Client-Assertion-type:jwt-Bearer .

Für die OAuth 2,0-Clientauthentifizierung mit JWT-Token erforderliche Plugins:

- **OAuth 2,0 (com.snc.platform.security.oauth)** : Dieses Plugin ist in neuen und aktualisierten Instanzen aktiv. Wenn das Plugin in Ihrer Instanz nicht aktiv ist, können Sie es aktivieren.
- **Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter (com.snc.integration.sso.multi.installer)** : Für OIDC-basierten Single Sign-on-Anwendungsfall.

Sie können die OAuth 2,0-Client-Authentifizierung mit privatem Schlüssel JWT für Folgendes verwenden:

- OIDC-basiertes Single Sign-on
- Ausgehende OAuth-Integrationen

Konfigurieren Sie JWT für privaten Schlüssel für OIDC-basiertes SSO

Konfigurieren Sie JWT für privaten Schlüssel für OIDC-basierte SSO-Integrationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie müssen die folgenden Aufgaben ausführen, bevor Sie Private Key JWT für OIDC-basiertes SSO auswählen.

- Laden Sie das Java Key Store-Zertifikat hoch: Anhängen Sie ein JKS-Zertifikat an Ihre Instanz an, um die JWT-Clientauthentifizierung zu aktivieren.
- Konfigurieren Sie einen JWT-Signaturschlüssel: Erstellen Sie einen JWT-Signaturschlüssel, der Ihrem Java Keystore-Zertifikat (JKS) zugewiesen werden soll.

  Hinweis: Wenn Sie hinzufügen möchten **X.509-Zertifikat SHA-1 Fingerabdruck-int (x5t)** Dem Header als Teil des JWT-Schlüssels müssen Sie das Formular konfigurieren und hinzufügen **X.509-Zertifikat SHA-1 Fingerabdruck-int (x5t)** Feld.

- Erstellen Sie einen JWT-Provider mit einem JWT-Signaturschlüssel: Fügen Sie einen JWT-Provider zu hinzu ServiceNow Instanz.

Um einen JWT-Schlüssel für OIDC-basierten Identitätsanbieter einzubeziehen, müssen Sie:

- Installieren Sie **Integration: Single Sign-On-Installationsprogramm Für Mehrere Anbieter** (`com.snc.integration.sso.multi.installer`)-Plugin.
- Aktivieren Sie die Eigenschaften für **SSO-Eigenschaften mehrerer Anbieter** . Weitere Informationen finden Sie unter Multi-Provider-SSO-Eigenschaften, -Tabellen und -Skripts.
- Erstellen Sie einen OIDC-Identitätsanbieter. Weitere Informationen finden Sie unter OpenID Connect-Konfiguration (OIDC) für Single Sign-on (SSO) erstellen.

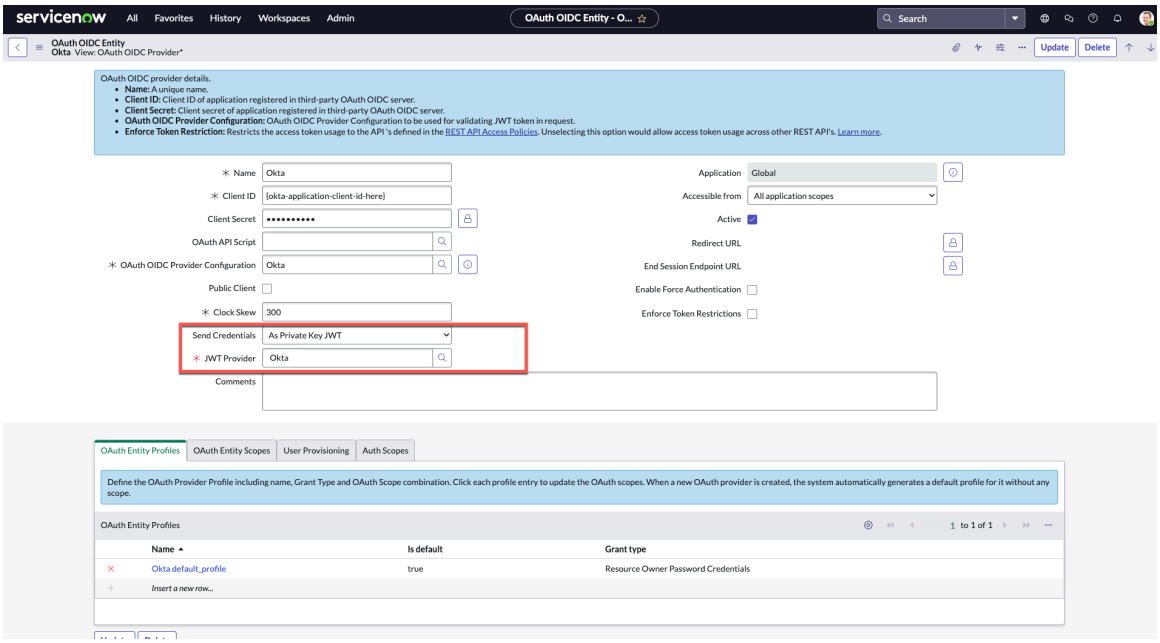
Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.
2. Wählen Sie den von Ihnen erstellten OIDC-Identitätsanbieter aus.
3. Wählen Sie oben im Formular aus **Konfigurieren** > **Formulardesign**an.

   Hinweis: Sie müssen hinzufügen **Anmeldeinformationen Senden** Und **JWT-Anbieter** Felder im Formular zur Verwendung des privaten Schlüssel-JWT für OIDC-basierte Authentifizierungsanforderungen des Identitätsanbieters.

4. Wählen Sie aus **Als privater Schlüssel-JWT** Für Anmeldeinformationen senden.
5. Wählen Sie aus **JWT-Anbieter** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn sich der Anwender authentifiziert, verfügt die Authentifizierungsseite über Optionen zur Anmeldung über Okta.

Konfigurieren Sie JWT des privaten Schlüssels für ausgehende OAuth

Konfigurieren Sie JWT des privaten Schlüssels für ausgehende OAuth-Integrationen.

Vorbereitungen

Erforderliche Rolle: Administrator

Bevor Sie JWT mit privatem Schlüssel für ausgehende OAuth-Integrationen konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

- Laden Sie das Java Key Store-Zertifikat hoch: Anhängen Sie ein JKS-Zertifikat an Ihre Instanz an, um die JWT-Clientauthentifizierung zu aktivieren.
- Konfigurieren Sie einen JWT-Signaturschlüssel: Erstellen Sie einen JWT-Signaturschlüssel, der Ihrem Java Keystore-Zertifikat (JKS) zugewiesen werden soll.

  Hinweis: Wenn Sie hinzufügen möchten **X.509-Zertifikat SHA-1 Fingerabdruck-int (x5t)** Dem Header als Teil des JWT-Schlüssels müssen Sie das Formular konfigurieren und hinzufügen **X.509-Zertifikat SHA-1 Fingerabdruck-int (x5t)** Feld.

- Erstellen Sie einen JWT-Provider mit einem JWT-Signaturschlüssel: Fügen Sie einen JWT-Provider zu hinzu ServiceNow Instanz.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** Und klicken Sie dann auf **Neu** .
2. Klicken Sie auf der Seite „Interceptor“ auf **Stellen Sie eine Verbindung zu einem OAuth-Drittanbieter her** Und füllen Sie dann das Formular aus.

   Hinweis: Sie müssen hinzufügen **Anmeldeinformationen Senden** Und **JWT-Anbieter** Felder im Formular zur Verwendung des privaten Schlüssel-JWT für ausgehende OAuth-Authentifizierungsanforderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Eindeutiger Name für die Drittpartei-OAuth-Verbindung.
Client-ID	Die Client-ID der Anwendung, die auf dem OAuth-Server des Drittanbieters registriert ist.
Geheimer Clientschlüssel	Das geheime Clientgeheimnis der Anwendung, die auf dem OAuth-Server des Drittanbieters registriert ist.
OAuth-API-Skript	Das Skript, das zum Anpassen von Anforderungen und Antworten an den externen OAuth-Provider verwendet wird.
Logo-URL	Die URL des OAuth-Anwendungslogos.
Standardgewährungstyp	Wählen Sie: **Client-Anmeldeinformationen** : Die Client-ID und der geheime Client-Schlüssel, die beide zum Abrufen des Zugriffstoken verwendet werden. Bei dieser Methode werden keine Aktualisierungstoken bereitgestellt.
Lebensdauer von Aktualisierungstoken	Zeit in Sekunden, die das Aktualisierungstoken gültig ist. Die Standardzeit ist 8.640.000 Sekunden.
Öffentlicher Client	Ermöglicht öffentlichen Clients, PKCE für eine Autorisierung zu benötigen. **Hinweis:** Sie können nur den Autorisierungscode als verwenden `Default Grant type`Wenn PKCE aktiviert ist.
Kommentare	Fügen Sie Kommentare zur OAuth-App hinzu.
Anwendung	Anwendung und Umfang, die diesen Datensatz enthalten.
Zugänglich von	Machen Sie diese App über alle Anwendungsbereiche oder nur über diesen Bereich zugänglich.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die App zu aktivieren.
Autorisierungs-URL	Der OAuth-Autorisierungscode-Endpunkt.
Token-URL	Der OAuth-Server-Token-Endpunkt.
Token-Sperr-URL	Der OAuth-Server-Token-Widerrufsendpunkt.
Umleitungs-URL	Der OAuth-Rückrufendpunkt. Wenn leer, generiert die Instanz automatisch einen Eintrag.
Gegenseitige Authentifizierung aktivieren	Aktivieren Sie das Kontrollkästchen, um die gegenseitige Authentifizierung für die Tokenanforderung und den Widerruf zu verwenden. Für diese Funktion muss ein Profil für gegenseitige Authentifizierung angegeben werden.
Anmeldeinformationen senden	Wählen Sie: **Als privater Schlüssel-JWT**
JWT-Anbieter	JWT-Anbieterdetails. Sie können die Suche verwenden, um den JWT-Provider auszuwählen.

Das System erstellt einen Datensatz in der Tabelle „Anwendungsregistrierungen“ [oauth_Entity] mit dem Typ „OAuth-Provider“, der für die private JWT-Schlüsselauthentifizierung verwendet werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine ausgehende REST-Nachricht

Erstellen Sie eine ausgehende Rest-Nachricht, um die Instanz als Autorisierungsserver zu autorisieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **System-Webservices** > **Ausgehend** > **REST-Nachricht** Und klicken Sie dann auf **Neu** .
2. Füllen Sie die Formularfelder für den OAuth-Anwendungsdatensatz aus, wie in beschrieben.
   Beachten Sie die folgenden Feldwerte:
   - **Endpunkt** : URL der Instanz, die der Autorisierungsserver ist.
   - **Authentifizierungstyp** : **OAuth 2,0** .
   - **OAuth-Profil** : OAuth-Profil, das Sie für den Client-Server erstellt haben.
3. Klicken Sie im REST-Nachrichtendatensatz auf **OAuth-Token abrufen** .
4. Authentifizieren Sie sich mit der Instanz, die das Token bereitstellt. Die Methode hängt vom Single Sign-on-Integration ab.
   Sie können Folgendes verwenden:
   - Ihr Anwendername und Ihr Passwort, mit dem Sie sich bei der Instanz authentifizieren.
   - Der Anwendername und das Passwort für den IdP, wenn aktiviert ist. Klicken Sie Auf **Externe Anmeldung Verwenden** Um auf den IdP-Anmeldebildschirm zuzugreifen.

     Hinweis: Um automatisch zur IdP-Anmeldeseite weitergeleitet zu werden, müssen Sie die Systemeigenschaft glide.authenticate.external festlegen.

   - Ihr Code, wenn MFA aktiviert ist.
5. Klicken Sie Auf **Zulassen** Oder **Ablehnen** Um die Autorisierung abzuschließen und die Token auszugeben.
   Der folgende Prozess ist in beschrieben Flow zur Gewährung von OAuth-Autorisierungscode.

Persönliche Authentifizierung

Mit der persönlichen Authentifizierung können Sie Ihre OAuth-basierten Integrationen wie sicher verbinden und verwalten Microsoft OneDrive Oder Google Drive.

OAuth 2.0-Anmeldeinformationen

Das OAuth 2,0-Anmeldeinformationsmodul in ServiceNow (oauth_2_0_Anmeldeinformationen) Ermöglicht Ihnen das Konfigurieren und Verwalten von Zugriffstoken, die für die Verbindung mit externen OAuth 2,0-konformen Systemen verwendet werden. Verwenden Sie den Integrationstyp „persönlich“, wenn sich jeder Anwender mit seiner eigenen Identität bei einem externen System authentifizieren muss.

Verwenden Sie das Anmeldeinformationsformular, um OAuth 2,0-Anmeldeinformationen mit zu konfigurieren Integration_type = persönlich . Weitere Informationen finden Sie unter OAuth 2.0-Anmeldeinformationen.

Die persönliche Authentifizierung wird nur für die folgenden OAuth 2,0-Gewährungstypen unterstützt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Autorisierungscode
- Passwortanmeldeinformationen des Ressourcenbesitzers (ROPC)

Gewährungstypen wie Client-Anmeldeinformationen und JWT-Bearer-Gewährung werden mit nicht unterstützt Integration_type = persönlich .

Hinweis: Die persönliche Authentifizierung wird auch über einen MID-Server für die Typen Autorisierungscode und ROPC-Gewährung unterstützt. Weitere Informationen finden Sie unter OAuth-Token wird über MID abgerufen .

Dashboard für persönliche Authentifizierung

Verwenden Sie Ihre persönlichen Anmeldeinformationen, um eine Verbindung zu Drittpartei-Integrationen herzustellen. Zeigen Sie Ihre persönlichen Authentifizierungen über eine vereinfachte, konsolidierte Schnittstelle an, authentifizieren Sie sie, widerrufen Sie sie und verlängern Sie sie. Weitere Informationen finden Sie unter Verwenden des Dashboards für persönliche Authentifizierung .

Hinweis: Auf das Dashboard für die persönliche Authentifizierung können nur Anwender zugreifen, die der folgenden Rolle zugewiesen sind: sn_Personal_auth.Personal_auth_user

Konfigurieren Sie Die Persönliche Authentifizierung

Sie können die persönliche OAuth-Authentifizierung mit dem REST-Schritt in Flow Designer konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Stellen Sie sicher, dass Sie das IntegrationHub-Starterpaket-Installationsprogramm (com.glide.hub.integrations) Oder eine höhere Version.

Warum und wann dieser Vorgang ausgeführt wird

Diese Aufgabe führt Sie durch die Konfiguration der persönlichen OAuth-Authentifizierung für REST-Schritte in ServiceNow® Flow Designer. Es ermöglicht die Ausführung von REST-Aufrufen mit den Anmeldeinformationen des Sitzungsanwenders, wodurch ein sicherer und personalisierter API-Zugriff gewährleistet wird.

Informationen zum Überprüfen, ob ein persönliches OAuth-Token für einen Anwender vorhanden ist, finden Sie unter Persönliches OAuth-Token abrufen (mit GlideOAuthClient).

Informationen zum Generieren des ersten Tokens für einen Anwender, der keinen Zugriff auf die Anmeldeinformationsseite hat, finden Sie unter Generieren Sie die URL des Initiators für die persönliche Authentifizierung.

Prozedur

1. Navigieren Sie zu **Anwendungsregistrierungen** , Und erstellen Sie eine OAuth-Anwendungsregistrierung, um eine Verbindung zu einem externen Endpunkt herzustellen.
2. Navigieren Sie zu **Aliasse Für Verbindungen Und Anmeldeinformationen** , Und erstellen Sie einen Verbindungsalias.
   Dieser Alias wird in den REST-Schritten verwendet. Weitere Informationen finden Sie unter Verbindungs- und Anmeldealias erstellen.
3. Navigieren Sie zu **HTTP(s)-Verbindung** , Und aktualisieren Sie die externen Endpunktdetails für den im vorherigen Schritt erstellten Verbindungsdatensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erstellen Sie einen **OAuth-Anmeldeinformationen** .
   a. Navigieren Sie zu **OAuth 2,0-Anmeldeinformationen** .
   b. Erstellen Sie einen neuen OAuth-Anmeldeinformationsdatensatz, und verknüpfen Sie ihn mit dem in Schritt 1 erstellten OAuth-Profil.
5. Fügen Sie hinzu **IntegrationType** Feld zum Anmeldeinformationsformular.
6. Aktualisieren Sie **IntegrationType** Feld der in Schritt 4 bis erstellten Anmeldeinformationen **Persönlich** .
7. Generieren Sie ein persönliches Zugriffstoken.
   a. Öffnen Sie als angemeldeter Anwender den Anmeldeinformationsdatensatz.
   b. Wählen Sie Aus **OAuth-Token abrufen** Dient zum Erstellen eines persönlichen Tokens.
   c. Wählen Sie Aus **Verwalten Sie Token** Zum Anzeigen und Verwalten der Token.

   Hinweis: Fügen Sie Ihrer Anwendung eine UI-Aktion hinzu, damit Endanwender Token generieren können. Nur Administratoren können das Anmeldeinformationsformular direkt öffnen.

8. Navigieren Sie zu **Aktion** Um eine Aktion für Ihren Anwendungsfall zu erstellen.
9. Fügen Sie der Aktion einen REST-Schritt hinzu.
   Wählen Sie den in Schritt 2 erstellten Verbindungsalias aus.

   Hinweis: Testen Sie die Aktion mit dem ausgehenden REST-Aufruf. Die Anmeldeinformationen sind zur Verwendung für die persönliche Integration markiert. Der REST-Schritt zeigt möglicherweise einen Fehler an, da die Aktion mit der Systemintegrationsrolle ausgeführt wird.

10. Erstellen Sie einen neuen Subflow, und fügen Sie die in Schritt 8 erstellte Aktion hinzu.
    a. In **Subflow-Eigenschaften** Fenster auswählen **Anwender, der die Sitzung initiiert** In **Ausführen Als** Textfeld.
    Nicht auswählen **Systemanwender** Stattdessen von **Ausführen Als** Textfeld.
11. Testen Sie den Subflow.
    Der REST-Schritt verwendet das für den Sitzungsanwender erstellte Token. Der Subflow kann auch über FlowAPIs aufgerufen werden.

    Beispielskript zum Aufrufen eines Subflows:

```
try {
   // Execute synchronously in the foreground. Allows access to subflow
 outputs.
   var result = sn_fd.FlowAPI.getRunner()
      .subflow('global.getpersonalincidentssubflow')
      .inForeground()
      .run();

   var outputs = result.getOutputs();
} catch (ex) {
   var message = ex.getMessage();
   gs.error(message);
}
```

12. Fehlende oder abgelaufene Token verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Sitzungsanwender kein Zugriffstoken hat, gibt die REST-Anforderung einen zurück **Nicht autorisierter HTTP 401-Statuscode** Antwort. Stellen Sie sicher, dass das Token erstellt wurde, bevor Sie den Flow initiieren.

Wenn das Zugriffstoken abgelaufen ist, aber ein gültiges Aktualisierungstoken vorhanden ist, verlängert das System das Zugriffstoken automatisch.

Persönliches OAuth-Token abrufen (mit GlideOAuthClient)

Überprüfen Sie, ob der Anwender über ein persönliches OAuth-Token verfügt. Verwenden Sie es, um einen gültigen Zugriff zu bestätigen, bevor Sie REST-Schritte oder Integrationen ausführen, die persönliche OAuth-Anmeldeinformationen erfordern.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie GlideOAuthClient API, um zu überprüfen, ob für den derzeit angemeldeten Anwender ein persönliches OAuth-Token vorhanden ist. Sie können auch verwenden ScopedPersonalAuthAPI Um das persönliche OAuth-Token abzurufen. Weitere Informationen finden Sie unter PersonalAuthAPI: Bereichsbezogen .

Prozedur

1. Verwenden Sie das folgende Beispielskript, um nach einem persönlichen Zugriffstoken zu suchen, das dem aktuellen Sitzungsanwender zugeordnet ist:

```
function dumpToken(token) {
  if (token) {
    gs.info("Access token: " + token.getAccessToken());
    gs.info("Expires in: " + token.getExpiresIn());
    gs.info("Refresh token: " + token.getRefreshToken());
  }
}

var oAuthClient = new sn_auth.GlideOAuthClient();
oAuthClient.setPersonal(true); // Returns the token for the logged-in user

var token = oAuthClient.getToken('<credential_sys_id>', '<oauth_profile_sys_id>');
dumpToken(token);
```

2. Ersetzen <credential_sys_id> Und <oauth_profile_sys_id> Mit den entsprechenden Datensatzwerten. Die SetPersonal (wahr) Die Methode bestätigt, dass das zurückgegebene Token zum derzeit angemeldeten Anwender gehört.

Hinweis: Weitere Informationen zu den Methoden zum anfordern und Widerrufen von OAuth-Aktualisierungs- und Zugriffstoken finden Sie unter: Glide-OAuth-Client-API-Dokumentation .

Generieren Sie die URL des Initiators für die persönliche Authentifizierung

Generieren Sie das anfängliche Token für einen Anwender, der keinen Zugriff auf die Anmeldeinformationsseite hat, um die persönliche Authentifizierung zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: connection_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Anwender ohne **Connection_admin** Rolle kann nicht auf die Anmeldeinformationsseite zugreifen, um OAuth-Token zu generieren. Diese Anwender müssen mit ein persönliches Token generieren `oauth_Initiator` URL mit zusätzlichem Parameter, der angibt, dass das Token persönlich ist und für den Sitzungsanwender angefordert wird.

Sie können auch bereichsbezogene verwenden `PersonalAuthAPI` Mit `sn_Personal_auth` Plugin zum Generieren der Initiator-URL. Weitere Informationen finden Sie unter PersonalAuthAPI – getInitiatorURL(Zeichenfolge aliasId)

Hinweis: Wenn das Plugin „persönliche Authentifizierung“ (`Com.snc.sn_ihub_Personal_auth`) Aktiviert ist. Verwenden Sie die bereichsbezogene API, um die Initiator-URL zu generieren. Dies. API ist nur verfügbar, wenn das Plugin installiert ist.

Prozedur

1. Verwenden Sie das folgende Format, um die Token-Generierungs-URL für den Typ der Passwortgewährung zu erstellen:

```
https://<instance-name>.service-now.com/oauth_password_input.do?
sysparm_oauth_requestor_context=oauth_2_0_credential&sysparm_oauth_requestor=
<credential  sys_id>&sysparm_oauth_provider_profile=<OAUTH profile sys_id>
&sysparm_oauth_personal=true
```

2. Verwenden Sie das folgende Format, um die Token-Generierungs-URL für den Autorisierungscode-Gewährungstyp zu erstellen:

```
https:// ://<instance-name>.service-now.com /oauth_initiator.do?
oauth_requestor_context=oauth_2_0_credentials&oauth_requestor=
<credential  sys_id>&oauth_provider_profile=<OAUTH profile sys_id>&respons
e_type=code&personal=true
```

Aktivieren Sie Das Dashboard Für Persönliche Authentifizierung

Sie können aktivieren Persönliche Authentifizierung Plugin (Com.snc.sn_ihub_Personal_auth) Für IntegrationHub Wenn Sie die Administratorrolle innehaben. Die Anwendung enthält Demodaten und zugehörige Installationen ServiceNow® Store Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

IntegrationHub erfordert ein vom Rest der ServiceNow AI Platform getrenntes Abonnement.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Wenn Sie ein Abonnement erwerben, werden bestimmte Plugins automatisch aktiviert. Wenn ein kostenpflichtiges Plugin nicht automatisch aktiviert wird, können Sie es manuell in der Liste „Alle Anwendungen“ in Ihrer Instanz aktivieren.

Hinweis:

Bevor Sie ein Abonnement kaufen, können Sie die Funktion in einer Instanz außerhalb der Produktion kostenlos testen, indem Sie sie über den Now Support Servicekatalog anfordern.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit IntegrationHub installiert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach Persönliche Authentifizierung Plugin (Com.snc.sn_ihub_Personal_auth) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Selbstregistrierung bei ServiceNow Instanz

Verwenden Sie die Selbstregistrierung externer Anwender, um ein großes Volumen externer Anwender in Ihrer Instanz zu integrieren. Diese Funktion verbessert die Identitätsverifizierung, um die Kunden-Experience zu verbessern, und unterstützt häufig verwendete Registrierungs-Flows.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen der Selbstregistrierung.

Aktivieren



Erfahren Sie, wie Sie die externe Selbstregistrierung aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren



Konfigurieren Sie die Selbstregistrierung.

Aktivieren



Informieren Sie sich über die Eigenschaften in der Selbstregistrierung.

Selbstregistrierung erkunden

Verwenden Sie die Selbstregistrierung externer Anwender, um ein großes Volumen externer Anwender in Ihrer Instanz zu integrieren. Diese Funktion verbessert die Identitätsverifizierung, um die Kunden-Experience zu verbessern, und unterstützt häufig verwendete Registrierungs-Flows.

Die Selbstregistrierung externer Anwender ermöglicht es einer großen Gruppe von Anwendern, sich bei einem zu registrieren ServiceNow App ohne Hilfe eines Administrators. Beispielsweise könnte sich eine Universität mit einer großen Gruppe von Studenten, die auf dem Campus parken müssen, bei der App „Campus-Parkplatz“ registrieren. Jeder Student erhält einen begrenzten Satz von Berechtigungen, die für das Parken spezifisch sind, und würde einen automatisierten Registrierungsprozess abschließen. Dieses System könnte eine Parknummer generieren, die für jeden Studenten eindeutig ist, und sicherstellen, dass er einen Parkplatz hatte.

Ein Selbstregistrierungs-Flow besteht aus einem anwenderdefinierten ServiceNow App, in diesem Fall eine Campus-Park-App. Nach der Konfiguration einer App mit den erforderlichen Tabellen konfiguriert ein Administrator die Registrierung, einschließlich eines Flows vor der Registrierung, Feldzuordnung, Zuordnung nach der Registrierung, Captcha, Rollenzuordnung und Flow nach der Registrierung.

Aktivieren Selbstregistrierung Externer Anwender

Sie können das Plugin „Selbstregistrierung externer Anwender“ (com.snc.external_user_Self_Registration) aktivieren, wenn Sie die Administratorrolle innehaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie das Plugin über die Filterkriterien und die Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

   Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Externe Rollen in der Selbstregistrierung

Um zu verhindern, dass externe Anwender versehentlich Zugriff erhalten, können Sie allen externen Anwendern die Rolle „snc_external“ zuweisen.

Externen Anwendern, die sich selbst registrieren, muss die Rolle „snc_external“ zugewiesen werden, die über die geringsten Berechtigungen verfügt. Die Rolle snc_external gibt an, dass es sich um einen für Ihre Organisation externen Benutzer handelt, der keinen Zugriff auf Ressourcen hat, solange der Rolle snc_external oder anderen Rollen, die die Rolle snc_external übernehmen, keine expliziten Zugriffsrechte über ACLs erteilt wurden.

Standardmäßig haben Benutzer mit der Rolle snc_external keinen Zugriff auf:

- Tabellen ohne die Rolle, die die Rolle snc_external oder public erbt
- Ressourcen, die keine Datensatztypen sind, z. B. Prozessoren und UI-Seiten ohne die Rolle snc_external oder eine Rolle, die die Rolle snc_external erbt
- Platform Analytics-Dashboards.

Ab dem Release Paris müssen Sie eine ausschlusslisteneigenschaft aktivieren, um die explizite Zuweisung der Rollen „snc_external“ zu erzwingen. Informationen zum Aktivieren der Eigenschaft finden Sie unter Verhindern Sie zukünftige interne Rollenzuweisungen für externe Anwender .

Konfigurieren Sie eine Anwenderregistrierungskonfiguration für externe Anwender

Erstellen Sie einen Konfigurationsdatensatz für die Anwenderregistrierung, um den Onboarding-Prozess externer Anwender auf anwenderdefinierte zu bootstrap ServiceNow Anwendungen. Dieses Formular führt die externen Anwender durch den Selbstregistrierungsprozess.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Erforderliche Rolle: Administrator
- Aktivieren Selbstregistrierung Externer Anwender

Prozedur

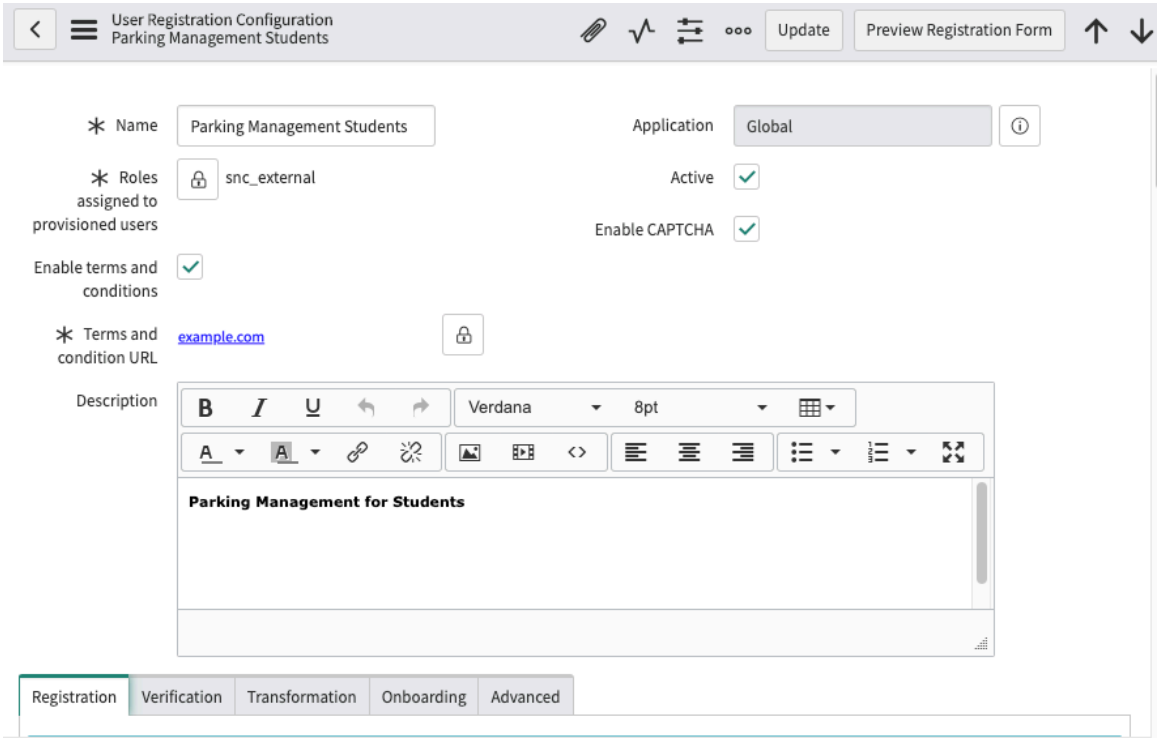
1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Konfigurationen der Anwenderregistrierung** Und klicken Sie auf **Neu** .
2. Füllen Sie im Formular die Felder aus.

Formular für Konfiguration der Anwenderregistrierung

Feld	Beschreibung
Name	Name Des Registrierungsformulars. Beispielsweise kann eine Studentenparkregistrierung Studenten des Parkmanagements sein.
Bereitgestellten Anwendern zugewiesene Rollen	Rollen, die den bereitgestellten Anwendern zugewiesen sind. Die angegebenen Rollen müssen erweitern oder enthalten `snc_external` Rolle. Die angegebene Rolle kann auch sein `snc_external` Rolle. Für externe Anwender muss jede Rolle einen haben `snc_external` Zum Notieren eines externen Anwenders. Wenn Sie über vorkonfigurierte Rollen verfügen, sollten die Rollen zugänglich sein, wenn Sie die Rollen entsperren und nach Anwendern suchen.
Nutzungsbedingungen aktivieren	Option zum Hinzufügen einer URL für Nutzungsbedingungen zur Registrierungsseite.
URL der Nutzungsbedingungen	Die öffentlich zugängliche URL, die die Nutzungsbedingungen des Registrierungsformulars enthält. Dieses Feld wird nur angezeigt, wenn **Aktivieren Sie Nutzungsbedingungen** Ist ausgewählt.
Beschreibung	Die Beschreibung des Registrierungsformulars. Dieses Feld wird nur angezeigt, wenn Sie die Konfiguration speichern oder übermitteln. In diesem Feld können Sie weitere Informationen zum Registrierungsformular hinzufügen. **Hinweis:** Sie können eine Beschreibung erst hinzufügen, nachdem Sie eine Anwenderregistrierungskonfiguration gespeichert oder aktualisiert haben.
Anwendung	Anwendung, die diesen Datensatz enthält. Die Anwendung wird automatisch auf festgelegt `Global` .
Aktiv	Option, mit der die Konfiguration der Anwenderregistrierung aktiv wird. Diese Option ist standardmäßig ausgewählt.
CAPTCHA aktivieren	Option zum Hinzufügen eines CAPTCHA zum Registrierungsformular. Der standardmäßige CAPTCHA-Anbieter ist Google reCAPTCHA. **Hinweis:** Um CAPTCHA für die Anwenderregistrierung zu aktivieren, führen Sie die Schritte in aus Konfigurieren Google reCAPTCHA Für die Selbstregistrierung externer Anwender.

3. Klicken Sie auf **Absenden**.
   Eine Anwenderregistrierungskonfiguration mit den Standardeinstellungen wird erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



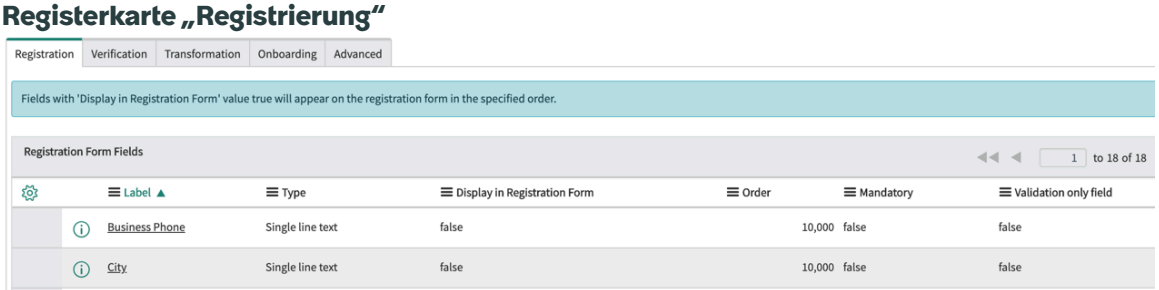
4. **Wahlweise:** Konfigurieren Sie **Registrierung** Registerkarte zum Anzeigen von Feldern und der Reihenfolge, in der sie angezeigt werden:

Registrierungsformularfelder

Spalte	Beschreibung
Im Registrierungsformular anzeigen	Legen Sie ein beliebiges Feld fest, als das Sie anzeigen möchten Wahr .
Reihenfolge	Legen Sie eine Reihenfolgenummer fest, um Felder in Ihrem Formular anzuzeigen.
Obligatorisch	Legen Sie ein Feld fest, als das Sie es als Pflichtfeld festlegen möchten Wahr .
Nur Validierungsfeld	Legen Sie ein Feld fest, das Sie nur zur Validierung verwenden möchten. Beispiel: Registrierungscode.

Sie können die Standardformularfelder anzeigen oder dem Registrierungsformular anwenderdefinierte Formularfelder hinzufügen. Weitere Informationen finden Sie unter Felder des Standardregistrierungsformulars.

Registerkarte „Registrierung“



Sie können auch anwenderdefinierte Registrierungsformularfelder hinzufügen. Weitere Informationen finden Sie unter Fügen Sie ein anwenderdefiniertes Registrierungsformularfeld hinzu.

Automatische Übersetzung

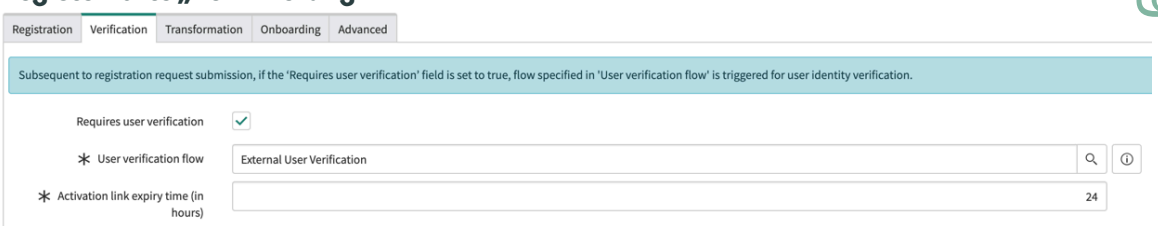
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wahlweise:** Konfigurieren Sie die Registerkarte **Verifizierung**, um die Identität der registrierten Benutzer zu überprüfen. Wenn der Flow der Anwenderverifizierung ausgelöst wird, wird ein Aktivierungslink an die registrierte E-Mail-Adresse des Anwenders gesendet.

Felder der Registerkarte „Verifizierung“

Feld	Beschreibung
Anwenderverifizierung erforderlich	Option zum Auslösen eines Subflows zur Anwenderverifizierung, der nach der Anwenderregistrierung ausgeführt wird. Der Subflow dient zur Verifizierung der Anwenderidentität.
Flow der Anwenderverifizierung	Der Subflow, der zum Überprüfen der Identität des Anwenders verwendet wird. Der Subflow wird nur ausgelöst, wenn Sie die Anwenderverifizierung aktivieren. (Optional) Die **Verifizierung Externer Anwender** subflow ist standardmäßig verfügbar. Sie können eine Kopie des Standard-Subflows in erstellen Flow Designer Und ändern Sie sie entsprechend Ihren Anforderungen. Weitere Informationen finden Sie unter Flow Designer . **Hinweis:** Um eine Vorschau von anzuzeigen **Verifizierung Externer Anwender** subflow in einer neuen Registerkarte verwenden Sie die folgenden Verknüpfungen: ○ Macintosh: Befehl + Klicken ○ Windows: Steuerung + Klick
Ablaufzeit des Aktivierungslinks (in Stunden)	Die Anzahl der Stunden, nach denen ein Aktivierungslink abläuft. Der Standardwert ist 24.

Registerkarte „Verifizierung“

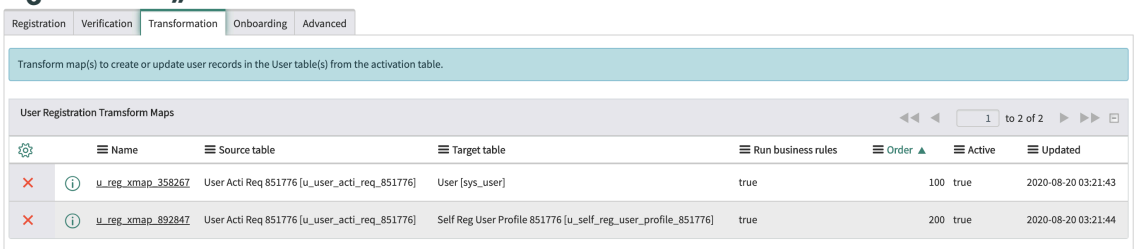


6. **Wahlweise:** Konfigurieren Sie **Transformation** Registerkarte zum Zuordnen von selbst registrierten Anwendern und aktivierten Anwendern.
Es gibt zwei Transformationszuordnungen (u_reg_xmap_[number]), die die registrierten Anwender aus der Tabelle „Anwenderaktionsanforderung“ [number] automatisch der Tabelle „Selbstregistrierter Anwender“ [number] zuordnen. Sie können eine Kopie dieser Standard-Transformationszuordnungen erstellen und die Zuordnung entsprechend Ihren Anforderungen ändern. Weitere Informationen finden Sie unter Transformationszuordnungen .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

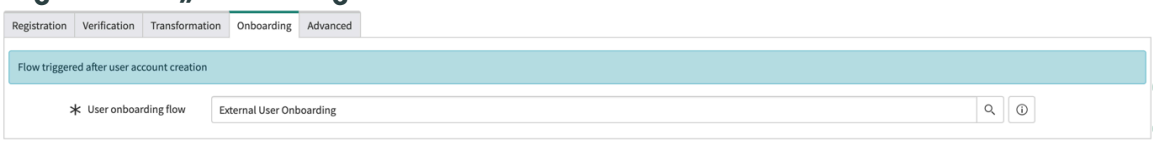
Registerkarte „Transformation“



7. Konfigurieren Sie **Onboarding** Registerkarte zum Auslösen von Subflows für Onboarding-aktivierte Anwender.
   Der Standard **Onboarding Externer Anwender** subflow sendet eine E-Mail an den Anwender, die einen Link zum Zurücksetzen seines Passworts enthält. Sie können eine Kopie des Standard-Subflows erstellen und entsprechend Ihren Anforderungen ändern.

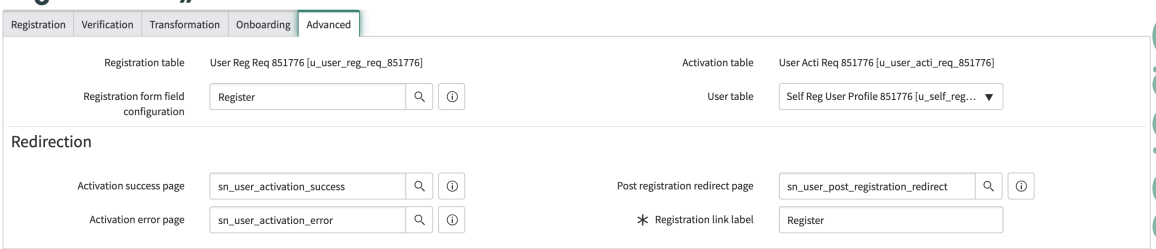
   Hinweis: Wenn **Onboarding Externer Anwender** subflow-Auslöser: Der Subflow sendet eine E-Mail an den Anwender, die einen Link zum Zurücksetzen des Passworts enthält.

Registerkarte „Onboarding“



8. **Wahlweise:** Konfigurieren Sie **Erweitert** Registerkarte zum Zuordnen von Anwendertabellen und Umleitungsseiten des Registrierungsformulars.

Registerkarte „Erweitert“



Registerkarte „Erweitert“

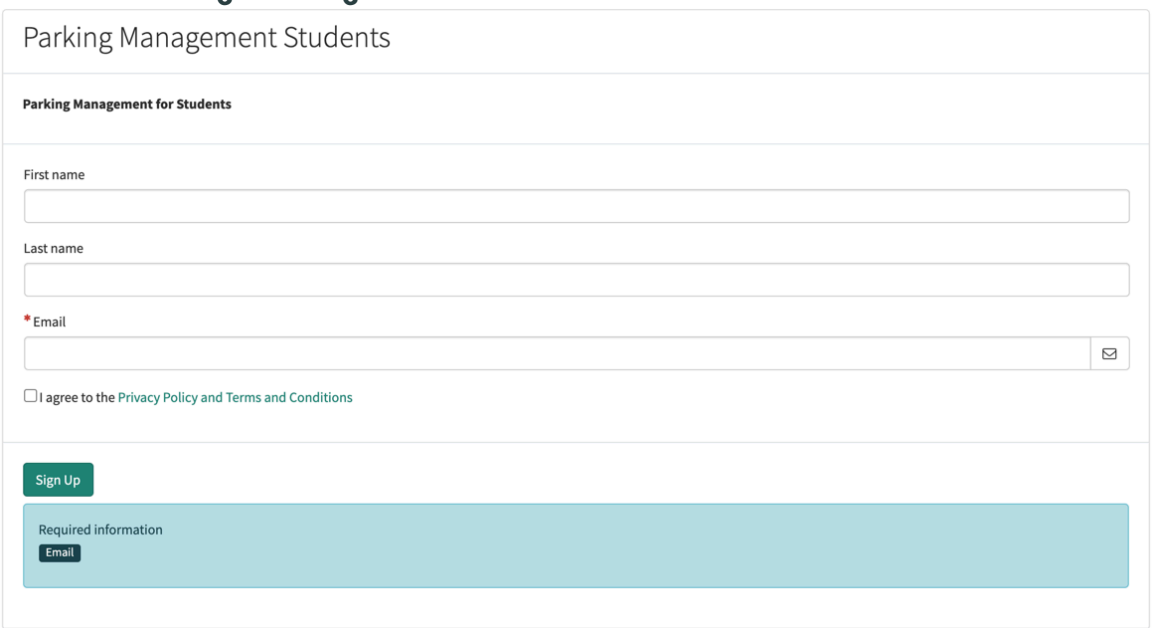
Feld	Beschreibung
Registrierungstabelle	Name der Tabelle, in der Informationen zum Registrierungsformular gespeichert werden.
Konfiguration des Registrierungsformularfelds	Der Datensatz, der dem Registrierungsformular im Datensatzersteller zugeordnet ist.
Aktivierungstabelle	Bezeichnung und Name der Tabelle, die für die Anwenderaktivierung verwendet wird. Die Aktivierungstabelle enthält Datensätze der Anwender, die die Verifizierung abgeschlossen haben.
Anwendertabelle	Bezeichnung und Name der Anwenderprofiltabelle.
Aktivierungserfolgsseite	Die Seite, zu der ein Anwender nach erfolgreicher Aktivierung umgeleitet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktivierungsfehlerseite	Die Seite, zu der ein Anwender umleitet, wenn die Aktivierung fehlschlägt.
Weiterleitungsseite nach Registrierung	Die Seite, zu der der Anwender nach der Registrierung weitergeleitet wird.
Registrierungslinkbezeichnung	Der Schaltflächenname, der für die Registrierung über das Serviceportal verwendet wird. Der Standardwert ist Registrieren.

Wenn Sie Änderungen vornehmen oder alle Änderungen an der Anwenderregistrierungskonfiguration abgeschlossen haben, können Sie verwenden **Vorschau Des Registrierungsformulars Anzeigen** Schaltfläche zum Anzeigen der Vorschau der Änderungen im Registrierungsformular.

Vorschau Des Registrierungsformulars



Automatische Übersetzung

Konfigurieren Google reCAPTCHA Für die Selbstregistrierung externer Anwender

Zur Verwendung von Google reCAPTCHA Service, müssen Sie ein API-Schlüsselpaar von anfordern Google Und konfigurieren Sie dann die zugehörigen Systemeigenschaften.

Vorbereitungen

- Fordern Sie ein API-Schlüsselpaar (einen Site-Schlüssel und ein Geheimnis) von an Google Um https://www.google.com/recaptcha .
- Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie nach den folgenden Eigenschaften, und legen Sie die Werte fest:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Wert
glide.user.registration.google.recaptcha.secret	Das Geheimnis autorisiert die Kommunikation zwischen der Anwendung und dem reCAPTCHA-Server. Typ: password2
glide.user.registration.google.recaptcha.site_key	Der Standortschlüssel, der zum Aufrufen des reCAPTCHA-Service auf Ihrer Registrierungsseite verwendet wird. Typ: Zeichenfolge
glide.user.registration.captcha.widget	Die SYS_ID des Captcha-Widgets. Typ: Zeichenfolge

Felder des Standardregistrierungsformulars

Sie können die standardmäßigen Registrierungsformularfelder verwenden oder anwenderdefinierte Registrierungsformularfelder erstellen.

Registrierungsformularfelder

Die folgenden Formularfelder werden standardmäßig im Registrierungsformular hinzugefügt.

Feldbezeichnung	Typ
Geschäftstelefon	Einzeiliger Text
Stadt	Einzeiliger Text
Land	Auswahlfeld
EDU-Status Wird verwendet, um Mitarbeiter, Studenten und Besucher zu unterscheiden. **Hinweis:** Dieses Feld ist nützlich, wenn das Registrierungsformular für eine Bildungseinrichtung gilt.	Auswahlfeld
E-Mail	E-Mail
Vorname	Einzeiliger Text
Geschlecht	Einzeiliger Text
Telefon (privat)	Einzeiliger Text
Sprache	Auswahlfeld
Nachname	Einzeiliger Text

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Typ
Zweiter Vorname	Einzeiliger Text
Mobiltelefon	Einzeiliger Text
Name	Einzeiliger Text
Präfix Titel des Anwenders. Zum Beispiel Mr. , Dr. und so weiter.	Auswahlfeld
Bundesland/Region	Einzeiliger Text
Straße	Breite einzeilige Textzeile
Titel: Stellenbezeichnung	Auswahlfeld
Postleitzahl	Einzeiliger Text

Hinweis: Sie können die Standardformularfelder für die Registrierung nicht löschen.

Fügen Sie ein anwenderdefiniertes Registrierungsformularfeld hinzu

Sie können anwenderdefinierte Felder im Formular zur Anwenderselbstregistrierung hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Konfigurationen der Anwenderregistrierung**an.
2. Öffnen Sie den Datensatz für die erforderliche Anwenderregistrierungskonfiguration.
3. Navigieren Sie zum Ende des Abschnitts „Registrierungsformularfelder“, und klicken Sie auf **Neue Zeile einfügen...** .
4. Geben Sie den Feldnamen unter ein **Bezeichnung** Spalte und Klicken Sie auf Häkchen .
   Eine neue Zeile mit den Standardwerten wird hinzugefügt. Sie können das anwenderdefinierte Registrierungsformularfeld basierend auf Ihren Anforderungen konfigurieren.

Registrierungsformular-Feldspalten

Spalte	Beschreibung
Bezeichnung	Der Feldname, der im Registrierungsformular angezeigt wird.
Typ	Der Typ des Anwenderoberflächenelements. Im Folgenden sind die unterstützten Typen aufgeführt: ○ Einzeiliger Text ○ E-Mail ○ Datum ○ Datum/Zeit ○ Ja/Nein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	○ Breite einzeilige Textzeile ○ Multiple-Choice ○ Auswahlfeld
Im Registrierungsformular anzeigen	Option zum Anzeigen des Felds im Registrierungsformular.
Reihenfolge	Die Reihenfolge, in der die Formularfelder im Registrierungsformular angezeigt werden. Das Feld mit dem niedrigsten Reihenfolgewert wird zuerst angezeigt, und das Feld mit dem höchsten Reihenfolgewert wird zuletzt angezeigt. Der Standardwert ist 10.000.
Obligatorisch	Option, um ein Feld im Registrierungsformular als Pflichtfeld festzulegen.
Nur Validierungsfeld	Option, ein Feld nur zu Validierungszwecken zu verwenden. Beispiel: Registrierungscode. Bei „wahr“ wird dieses Feld nicht in der Anwendertabelle (sys_user) gespeichert.

5. Speichern oder aktualisieren Sie die Änderungen.

Aktivieren Sie die Selbstregistrierung externer Anwender für Serviceportal

Ermöglichen Sie externen Benutzern die Registrierung für ServiceNow-Apps über Serviceportal.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Serviceportal** > **Portale**an.
2. Öffnen Sie einen Portaldatensatz.
3. Füllen Sie im Formular aus **Konfiguration der Registrierung externer Anwender** Feld.

   Wählen Sie eine Anwenderregistrierungskonfiguration aus.
4. Klicken Sie auf **Aktualisieren**.

Ergebnis
Das Anmelde-Widget enthält einen Link zum Registrierungsformular, das Sie zuvor konfiguriert haben.

Überprüfen Sie die Anforderungen zur Selbstregistrierung des Anwenders

Nachdem sich ein Anwender über registriert hat Serviceportal , Wird dem Modul Registrierungsanforderungen ein Anwenderdatensatz hinzugefügt. Sie können die Liste der registrierten Anwender anzeigen, die sich erfolgreich in registriert haben Serviceportal .

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Selbstregistrierung für externe Anwender** > **Anforderungen zur Registrierung**an.
   Die Liste der Anwenderdatensätze wird angezeigt.
2. (Optional) R Zeigen Sie die einzelnen Anwenderdatensätze an, und ändern Sie sie entsprechend Ihren Anforderungen. Sie können beispielsweise den Status eines Anwenderdatensatzformulars ändern **Ausstehend** Bis **Verarbeitet** .

Token-basierte Authentifizierung (Anwenderanmeldungen)

Verbessern Sie den Sicherheitsmechanismus für Anwender, die über die tokenbasierte Authentifizierung auf ein Netzwerk zugreifen können.

Zeitlich begrenzte Authentifizierung



Die tokenbasierte Authentifizierung ist ein Protokoll, mit dem Anwender ihre Identität verifizieren und im Gegenzug ein eindeutiges Zugriffstoken erhalten können.

Es hilft, den Sicherheitsmechanismus für Anwender für den Zugriff auf ein Netzwerk zu verbessern.

Digest-Token-Authentifizierung



Die Digest-Token-Authentifizierung übergibt Benutzeranmeldeinformationen und ein Digest-Token in einem unverschlüsselten HTTP-Header.

Automatische Übersetzung

Zeitlich begrenzte Authentifizierung

Authentifizierung mit begrenzter Supportzeit für Ihren ServiceNow Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen der zeitlich begrenzten Authentifizierung.

Aktivieren



Erfahren Sie, wie Sie die zeitlich begrenzte Authentifizierung aktivieren.

Tutorial: Zeitlich begrenzte Authentifizierung



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informieren Sie sich über die Eigenschaften in Zero Trust Access.

Erkunden Sie die zeitlich begrenzte Authentifizierung

Authentifizierung mit begrenzter Supportzeit für Ihren ServiceNow Instanz.

Hinweis: Die zeitlich begrenzte Authentifizierung ist sehr spezifisch für ServiceNow Instanz können die anwenderdefinierten Links für Anwender nur in erstellt werden ServiceNow.

Administratoren können die linkbasierte Authentifizierung auf konfigurieren ServiceNow Instanz. Der konfigurierte Link kann für den Anwender per E-Mail oder SMS freigegeben werden, und der Anwender kann diese Links verwenden, um sich bei der Instanz anzumelden.

Die Anmeldung bei der Instanz mit diesem Authentifizierungsschema wird durch die Richtlinien für adaptive Authentifizierung gesteuert, die auf konfiguriert sind ServiceNow Instanz.

Mit der zeitbasierten Authentifizierung können Sie Folgendes ausführen:

- Der Administrator kann die linkbasierte Authentifizierung so konfigurieren, dass sie innerhalb einer Ablaufzeit verwendet wird.
- Das Anwendungsteam kann Nonce abrufen, die mit dem Link für das spezifische Konfigurationselement verwendet werden soll, indem die bereitgestellte skriptfähige API verwendet wird. Die Linkgenerierung wird vom Anwendungsteam übernommen.
- Das Anwendungsteam kann den Link generieren und über einen vorhandenen Kanal an den Anwender senden.
- Anwender mit dem Link können sich einmal und innerhalb der im Rahmen der Konfiguration angegebenen Ablaufzeit bei der Instanz anmelden.
- Administratoren können die Rollen mit geringen Berechtigungen für das Authentifizierungsschema konfigurieren.
- Administratoren können MFA für das Authentifizierungsschema als zweiten Faktor für die Authentifizierung mit dem TLA-Link erzwingen.

Aktivieren Sie die zeitlich begrenzte Authentifizierung

Die zeitlich begrenzte Authentifizierung wird über das Plugin „Integration – Single Sign-on-Installationsprogramm für mehrere Anbieter“ aktiviert.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: Die zeitlich begrenzte Authentifizierung ist sehr spezifisch für ServiceNow Instanz können die anwenderdefinierten Links für Anwender nur in erstellt werden ServiceNow.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie die zeitlich begrenzte Authentifizierung (`com.snc.authenticate.time_limited_authentication`) Plugin mithilfe der Filterkriterien und der Suchleiste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Zeitlich begrenzte Authentifizierung mit SMS – Twilio Tutorial

Richten Sie eine zeitlich begrenzte Authentifizierung mit MFA-Faktoren wie SMS mit ein Twilio.

Vorbereitungen

Erforderliche Rolle: Administrator

Erforderliche Plugins:

- `com.snc.authenticate.time_limited_authentication` (Zeitlich Begrenzte Authentifizierung)
- `com.snc.authentication.sms_mfa` (Multifaktor-Authentifizierung mit SMS)

Hinweis: Die zeitlich begrenzte Authentifizierung (TLA) ist sehr spezifisch für ServiceNow Instanz können die anwenderdefinierten Links für Anwender nur in erstellt werden ServiceNow.

Die bereitgestellten Tutorial-Anweisungen ermöglichen es dem Administrator, Anwendern mit einer bestimmten Rolle eine linkbasierte Anmeldung mit SMS als Zweitfaktor (MFA) bereitzustellen.

Nach einer erfolgreichen Konfiguration generiert das System einen Link und gibt den Link dann über den Benachrichtigungskanal (E-Mail/SMS) für den Anwender frei. Wenn Sie auf den Link klicken, wird der Anwender aufgefordert, den Faktor „an E-Mail gesendete OTP“ oder „SMS“ basierend auf der Anwenderrolle (Konfiguration) anzugeben.

Hinweis:

- TLA muss immer von MFA gefolgt werden, und MFA sollte vom Administrator mithilfe der adaptiven Authentifizierung für die TLA-Anmeldung aktiviert werden. Weitere Informationen zur Konfiguration von MFA mit adaptiver Authentifizierung finden Sie unter Multifaktor-Authentifizierungskontext.
- TLA sollte für Anwender mit eingeschränkten Berechtigungen verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wird erstellt Twilio Konfiguration.
   a. Erstellen Sie einen Twilio Test-Account. Weitere Informationen finden Sie unter Twilio an.
   b. Navigieren zu **Alle** > **Benachrichtigen** > **Administration** > **Twilio Direct-Konfiguration**an.
   c. Geben Sie an **Account-SID** Und **Authentifizierungstoken** (Erstellt aus Twilio) Und speichern Sie den Datensatz.

   Hinweis: Sie können eine eigene Anbieterkonfiguration erstellen und diese für TLA verwenden. In diesem Beispiel ist es Twilio. Weitere Informationen zum Erstellen einer MFA-Anbieterkonfiguration finden Sie unter Konfigurieren Sie den MFA-Provider.

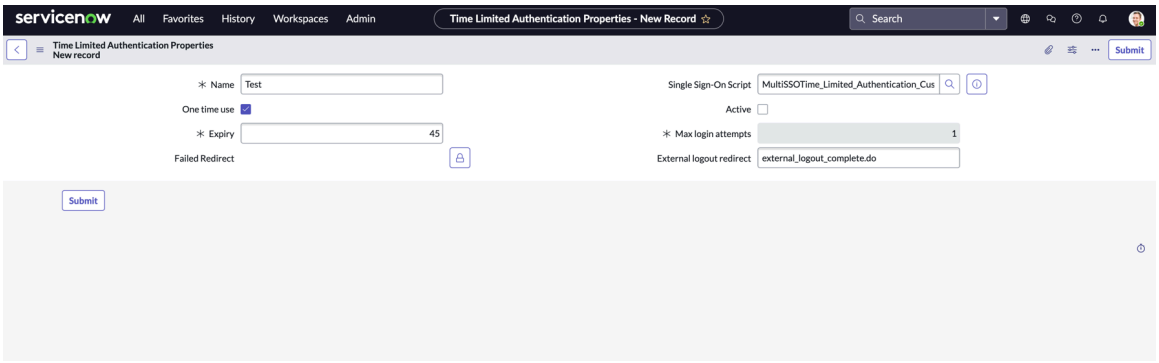
2. Konfigurieren und Aktivieren des Datensatzes für die zeitlich begrenzte Authentifizierung (TLA).
   a. Navigieren zu **Alle** > **Konfigurationsdatensätze für zeitlich begrenzte Authentifizierung** Und klicken Sie auf **Neu** .
   b. Füllen Sie die Felder im Formular aus.

Eigenschaften der zeitlich begrenzten Authentifizierung

Feld	Beschreibung
Name	Name des Datensatzes.
Einmalige Nutzung	Aktivieren Sie diese Option, um den TLA-Link einmal zu verwenden.
Ablauf	Geben Sie die Sekunden für den Ablauf des Links an. Der Standardwert ist 45 Minuten.
Fehlerhafte Umleitung	Geben Sie die URL ein, um Anwender nach einer fehlgeschlagenen Authentifizierung umzuleiten.
Single Sign-on-Skript	Details des SSO-Skripts, das Sie verwenden möchten.
Aktiv	Option zum Aktivieren der Konfiguration.
Max. Anmeldeversuche	Geben Sie die Anzahl der Versuche an, die mit dem generierten TLA-Link für die Anmeldung zulässig sind. Deaktivieren Sie **Einmalige Verwendung** Kontrollkästchen zur Angabe der maximalen Anzahl von Versuchen.
Weiterleitung für externe Abmeldung	Geben Sie die URL ein, um Anwender nach der Abmeldung umzuleiten.

   c. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Administration** > **Eigenschaften** Und aktivieren Sie **Aktivieren Sie SSO für mehrere Anbieter** Eigenschaft und **Speichern** .

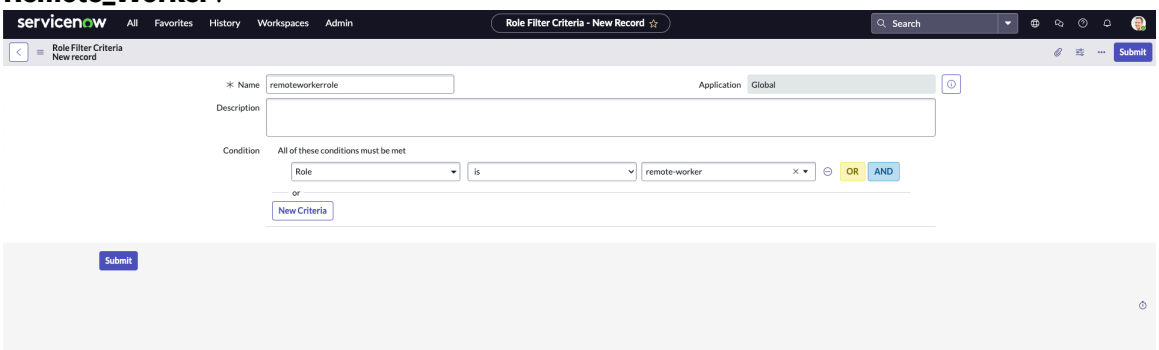
3. Zulassen, dass TLA nur für eine bestimmte Anwenderpersona mithilfe der Kontextrichtlinie nach der Authentifizierung verwendet wird.

a. Navigieren Sie zu **Rollen** Und erstellen Sie eine Rolle. Beispiel: Remote_Worker.

b. Erstellen Sie einen Anwender mit einer gültigen E-Mail-ID und Mobiltelefonnummer. Informationen zum Erstellen eines Anwenders finden Sie unter . Erstellen Sie einen Anwender .

c. Weisen Sie dem Anwender die Rolle zu. Informationen zum Zuweisen der Rolle zum Anwender finden Sie unter Weisen Sie einem Anwender eine Rolle zu .

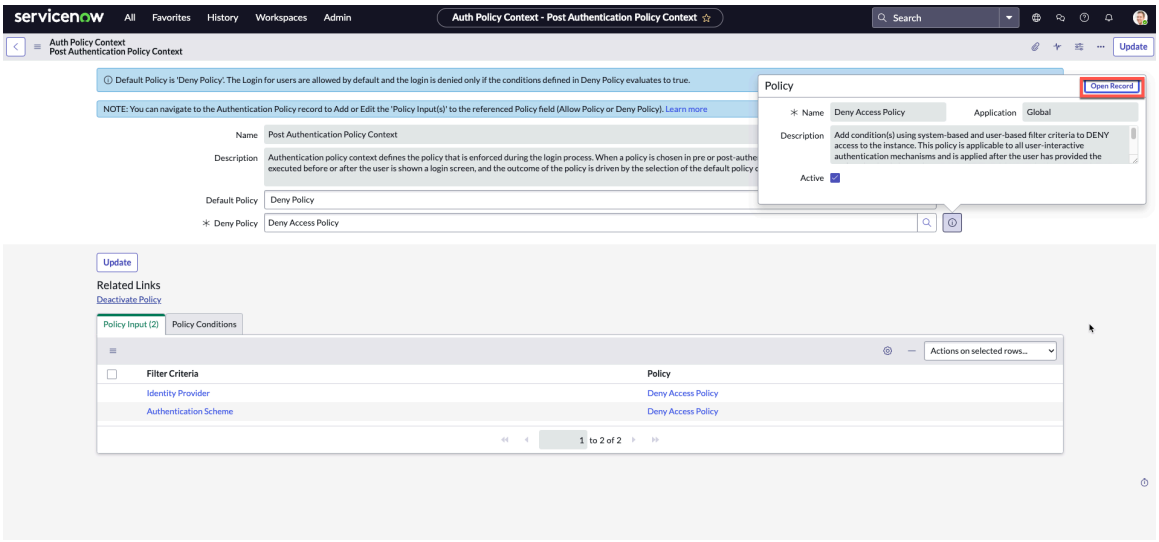
d. Navigieren Sie zum Erstellen eines Rollenfilterkriteriums zu **Alle** > **Adaptive Authentifizierung** > **Rollen-Filterkriterien**, Erstellen Sie einen neuen Filter **Remoteworkerrole** Und-Bedingung **Rolle ist Remote_Worker** .



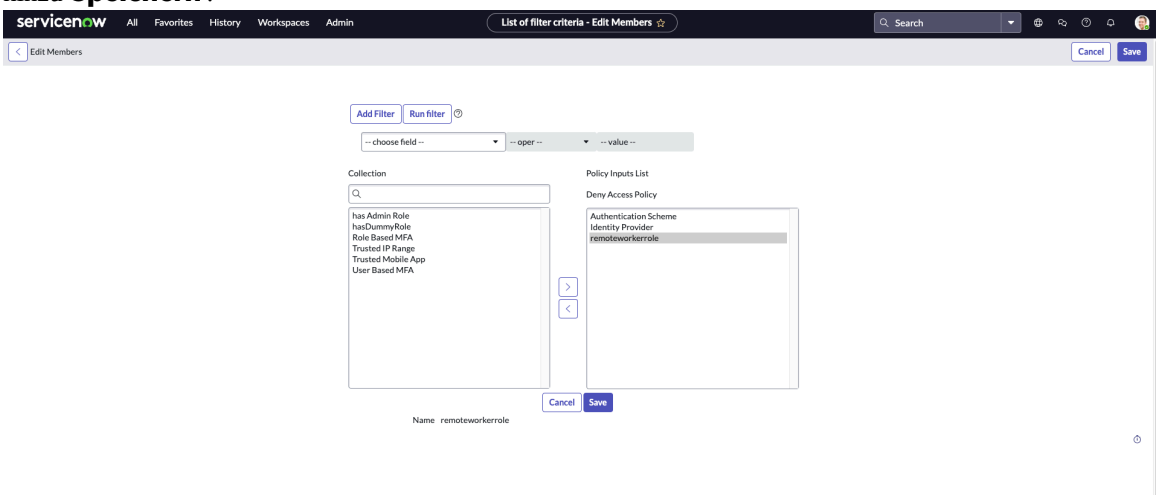
e. Um Richtlinienbedingung basierend auf dem Deny-Richtlinienkontext basierend auf den IdP- und Rollenfilterkriterien hinzuzufügen, navigieren Sie zu **Alle** > **Adaptive Authentifizierung** > **Kontext nach der Authentifizierung**an.

f. Klicken Sie auf das Informationssymbol und **Öffnen Sie den Datensatz** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



g. Klicken Sie in der Richtlinieneingabe auf **Bearbeiten** Und fügen Sie die Rolle (remoteworkerrole) und hinzu **Speichern** .



h. Fügen Sie in der Richtlinienbedingung die Bedingung für die Richtlinieneingabe und hinzu **Übermitteln** Der Datensatz.

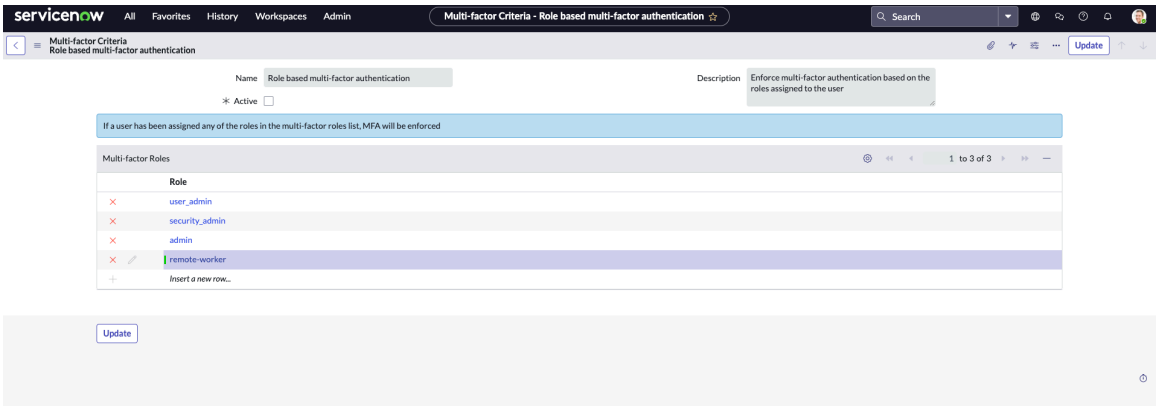
4. Konfigurieren der Step-up-Authentifizierungsrichtlinie – MFA-Kontext.

a. Navigieren zu **Alle** > **Multifaktor-Kriterien**an.

b. Wählen Sie aus **Rollenbasierte Multifaktor-Authentifizierung** Und fügen Sie die Rolle im Abschnitt Multifaktor-Rollen und hinzu **Aktualisieren** . In diesem Beispiel: **Remote_Worker** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

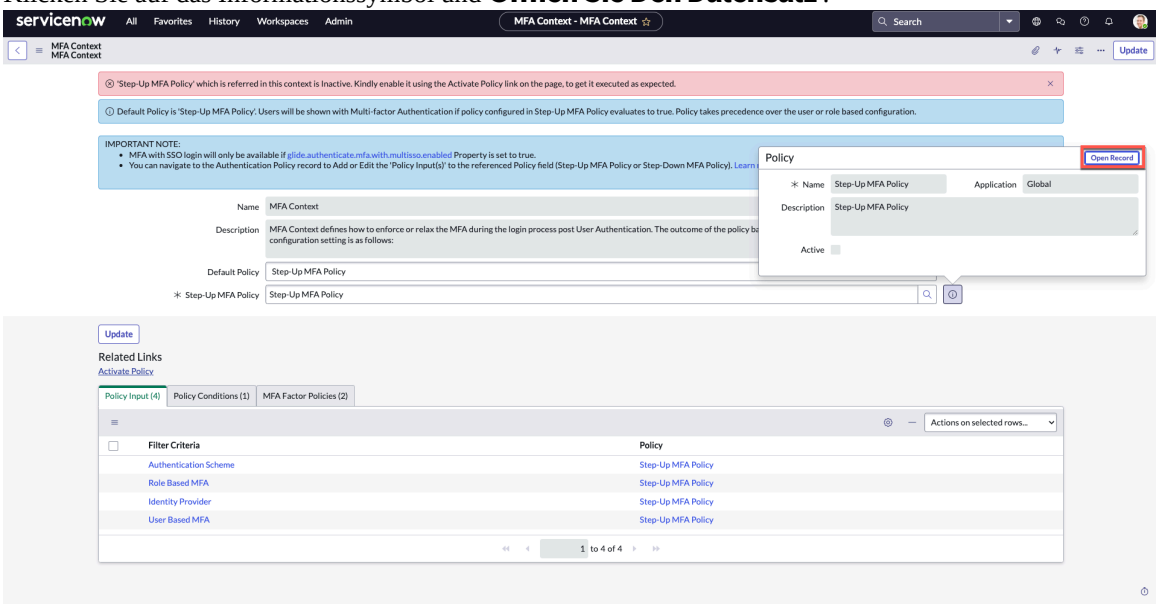


c. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **MFA-Kontext**an.

d. Stellen Sie Folgendes sicher:

- Standardrichtlinienfeld ist **STEP-up-MFA-Richtlinie**
- STEP-up-MFA-Richtlinie ist **STEP-up-MFA-Richtlinie**

e. Klicken Sie auf das Informationssymbol und **Öffnen Sie Den Datensatz** .



f. Klicken Sie im Formular „Step-up MFA-Richtlinie“ in den Richtlinieneingaben auf **Bearbeiten** .

g. Fügen Sie hinzu **Rollenbasierte Multifaktor-Authentifizierung** In die Liste und **Speichern** . In diesem Beispiel **Remoteworkerrolle** .

h. Klicken Sie in der Richtlinienbedingung auf **MFA erzwingen, wenn rollenbasierte oder anwenderbasierte MFA-Einstellungen auf „wahr“ festgelegt sind** .

i. Stellen Sie auf der Seite „MFA erzwingen, wenn rollenbasierte oder anwenderbasierte MFA-Einstellungen auf „wahr“ festgelegt sind, sicher, dass Sie dies tun **Rollenbasierte MFA** Ist **Wahr** .

5. MFA wird erzwungen, SMS als MFA-Faktorrichtlinie zu verwenden.

Automatische Übersetzung

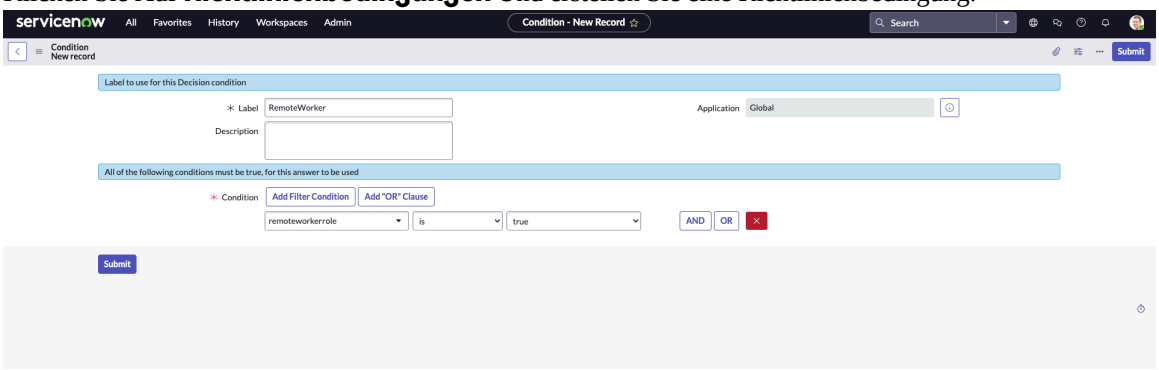
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **MFA-Kontext**an.

b. Klicken Sie auf der MFA-Kontextseite auf **MFA-Faktorrichtlinien** Und klicken Sie auf Richtlinie **SMS-OTP als MFA-Faktorrichtlinie anzeigen** .

c. Klicken Sie Auf **Bearbeiten** Und hinzufügen **Remoteworkerrole** In **Richtlinieneingaben** .

d. Klicken Sie Auf **Richtlinienbedingungen** Und erstellen Sie eine Richtlinienbedingung.



e. Klicken Sie auf **Absenden**.

Der TLA-Link wurde generiert und für die Anwender freigegeben, die zugewiesen sind **Remoteworkerrolle** Als Rolle wird heraufgestuft, um den SMS-Code als zweiten Faktor zum Anmelden der Instanz zu verwenden.

6. Aktivieren der anderen erforderlichen Eigenschaften.

a. Navigieren zu **Alle** > **Multi-Faktor-Authentifizierung** > **Eigenschaften**an.

b. Aktivieren Sie die folgenden Kontrollkästchen.

- **Multi-Faktor-Authentifizierung aktivieren**
- **Aktivieren Sie die Multifaktor-Authentifizierung mit SSO**

c. Speichern Sie den Datensatz.

d. Navigieren zu **Alle** > **Adaptive Authentifizierung** > **Authentifizierungsrichtlinien** > **Eigenschaften**an.

e. Aktivieren Sie **Aktivieren Sie Die Authentifizierungsrichtlinie** Kontrollkästchen.

f. Speichern Sie den Datensatz.

7. TLA-Link wird generiert – Beispiel.

a. Navigieren zu **Alle** > **Systemdefinition** > **Skripts: Hintergrund**an.

b. Verwenden Sie die folgende API, indem Sie die SYS-ID und die Konfigurations-ID des Anwenders angeben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VAR tla=New global.TimeLimitedAuthentication(); gs.info(tla.generateNonce("user_sysid", „config1_sys_ID“,„IAR2“);

Hinweis: Die Quelle (IAR2) ist kein obligatorischer Parameter.

c. Abfrageparameter wird wie gezeigt zurückgegeben:
Nonce=VCeinfboDt0M&Glide_sso_ID=b3277f1b4351110f879b5a2d9909f3&user=3b0277d344351110f879b5a2

d. Erstellen Sie eine URL im folgenden Format:
https://<instance-url> /login_with_sso.do?URI=<encoded url>&
nonce=2olIQSxdgkjs&Glide_sso_ID=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf0371020004e0bfc8

8. Klicken Sie auf die URL. Der folgende MFA-Bildschirm wird für die Anmeldung angezeigt.

Digest-Token-Authentifizierung

Die Digest-Token-Authentifizierung übergibt Benutzeranmeldeinformationen und ein Digest-Token in einem unverschlüsselten HTTP-Header.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen der Digest-Token-Authentifizierung.

Konfigurieren



Erfahren Sie, wie Sie die Digest-Token-Authentifizierung konfigurieren.

Digest-Token-Authentifizierung erkunden

Die Instanz liest den HTTP-Headerwert und vergleicht den berechneten Hash-Wert des Digest-Tokens. Wenn der berechnete Hash-Wert mit dem Digest-Token-Wert übereinstimmt, sucht die Instanz nach einem übereinstimmenden Wert in der Anwendertabelle. Wenn in der Anwendertabelle ein übereinstimmender Wert vorhanden ist, berücksichtigt die Instanz den Anwender als vorab authentifiziert und meldet ihn an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Digest-Token-Authentifizierung ist sicherer als einfache unverschlüsselte HTTP-Header, da jede versehentliche oder absichtliche Änderung des unverschlüsselten HTTP-Headers einen anderen Hash-Wert erzeugt. Wenn der Hash-Wert nicht übereinstimmt, verweigert die Instanz dem Anwender den Zugriff auf die angeforderte Instanz. Dies verhindert, dass Anwender versuchen, sich mit den Anmeldeinformationen eines anderen Anwenders anzumelden.

Weitere Informationen zum Ablauf des Digest-Links finden Sie hier KB-artikel .

Hinweis: Verwenden Sie Time Limited Authentication (TLA), um zeitbasierte Ablauflinks zu konfigurieren. Weitere Informationen finden Sie unter Zeitlich begrenzte Authentifizierung.

Integrationsanforderungen

Eine Integration der Digest-Token-Authentifizierung erfordert:

- Ein Webserver
- SiteMinder oder eine andere Single Sign-on-Anwendung zur Vorauthentifizierung des Anwenders im lokalen Netzwerk
- Eine Webseite oder ein Portal, die Anwenderanmeldeinformationen in einem dieser Formate an die Zielinstanz übergibt
  - HTTP-Header
  - URL-Parameter
  - Cookie
- Eine Webseite oder ein Portal, die ein Digest-Token mit einer dieser Codierungstechniken erstellt und an die Zielinstanz übergibt
  - SHA1
  - MD5
  - SHA 256 (empfohlen)

Digest-Eigenschaften für Single Sign-on (SSO) für mehrere Anbieter konfigurieren

Nachdem Sie ein Digest-Installationsskript aktiviert haben, konfigurieren Sie Eigenschaften für SSO mit mehreren Anbietern.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie nicht Single Sign-on für mehrere Anbieter verwenden, konfigurieren Sie standardmäßige Single Sign-on-Eigenschaften.

Prozedur

1. Navigieren zu **Alle** > **Mehrfachanbieter-SSO** > **Identity Provider**an.
2. Füllen Sie die Felder des Formulars „Digest-Eigenschaften“ aus.

Option	Bezeichnung
Name	Geben Sie den Namen des Digest-Tokens ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Benutzer	Geben Sie das Feld sys_user ein, das die übereinstimmenden Daten für den eingehenden Header enthält.
HTTP-Digest-Headername	Geben Sie den von Ihnen generierten HTTP-Header ein. Beispiel: DE_USER .
HTTP-Headername	Geben Sie den HTTP-Header ein, den Sie für das erstellte verarbeitete Token generiert haben. Beispiel: SM_USER .
Geheime Passphrase	Geben Sie den geheimen Schlüssel ein, der zum Codieren von Digest-Schlüsseln verwendet werden soll. Beispiel: 32 oder mehr Zeichen .
Fehlgeschlagenes SSO-Umleitungsfeld	Geben Sie die URL ein, um Anwender nach einer fehlgeschlagenen Authentifizierung umzuleiten.
Weiterleitung für externe Abmeldung	Geben Sie die URL ein, um Anwender nach einer Abmeldung umzuleiten.
Single Sign-on-Skript	Wählen Sie Aus **MultiSSO_DigestedToken** .
Client-Typ	Wählen Sie den Client-Typ basierend auf dem Typ Ihres Clients aus. Optionen: **Iframe Eingebettet** . **Hinweis:** Wenn das Feld „Client-Typ“ für Ihre Konfiguration erforderlich ist, können Sie das Formular bearbeiten und das Feld hinzufügen. Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

3. Klicken Sie auf **Aktualisieren**.
4. Legen Sie Ihren Digest Token-Standard auf „wahr“ fest.
   Wenn Sie den Standardwert auf „wahr“ festlegen, wird der dem SSO zugeordnete Standard-Digest-Token-Datensatz des Systems überschrieben. Sobald der erste IdP-Datensatz für SSO mit mehreren Anbietern aktiviert ist, werden nur Datensätze verwendet, die SSO mit mehreren Anbietern zugeordnet sind.

   Digest-Token-Datensätze, die in der Digest-Eigenschaftentabelle vorhanden sind, können einzeln aufgerufen werden, indem die SYS_ID des IdP angehängt wird. Beispiel: Ein Digest-Token-Datensatz in der folgenden Authentifizierungs-URL: https://<instance_name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id_of_Digest_token_record>&SM_USER=<user_name>&DE_USER=<digested_token>

Beispiel für Digest-Token-Implementierungen

Hier sind mehrere Beispiele für die Erstellung eines Digest-Tokens.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Digest-Authentifizierungsimplementierungen

Digest mit erstellt	Wert des geheimen Schlüssels	Hash-Methode	Beispiel
Java	32 und mehr Zeichen	SHA256	Beispiel für Java Digest-Algorithmus für Verschlüsselung
C	Wert des Parameters „sharedKey“	Wert des Parameters „strEncryptionMethod“ (SHA256 oder MD5)	Beispiel C

Beispiel für einen Java-Digest-Algorithmus für die Verschlüsselung

Dieser Java-Algorithmus veranschaulicht die Erstellung eines Digest-Tokens aus einem HTTP-Header.

Dieses Beispiel setzt Folgendes voraus:

- Der Webserver unterstützt Java
- Die Hash-Berechnungsmethode ist SHA1
- Der Wert des geheimen Schlüssels ist abc123
- Der unverschlüsselte HTTP-Headername ist user_Name

Ändern Sie den Java-Code, um einen anderen Hash-Berechnungsmechanismus (z. B. MD5) zu verwenden, und ändern Sie den Wert des geheimen Schlüssels oder den HTTP-Headernamen.

```
public class DigestTest
{
   private static final String MAC_ALG = "HmacSHA256";
     fKey  = {32 or more characters};
   public byte[] getDigest(String acct) {
      try {
         byte[] bkey = fKey.getBytes();
         byte[] data = acct.getBytes();
         Mac mac = null;
         try {
            mac = Mac.getInstance(MAC_ALG);
            mac.init(new SecretKeySpec(bkey, MAC_ALG));
         } catch (Exception e) {
            e.printStackTrace();
         }
         byte[] sig = mac.doFinal(data);
         String signature = new String(sig);
         System.out.println("value:" + acct);
         System.out.println("digested value:  " + signature);
         return sig;
      } catch (IllegalStateException e) {
         e.printStackTrace();
      }
      return null;
   }
   public static void main(String[] args) {
      BASE64Encoder encoder = new BASE64Encoder();
      DigestTest test = new DigestTest();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        String userName = "user_name";
        System.out.println("base 64 digest username: " +
encoder.encode(test.getDigest(userName)));
    }
}
```

Beispiel C

Diese C-Klasse veranschaulicht die Erstellung eines Digest-Tokens aus drei Eingabeparametern.

- StrEncryptionMethod: Listet die Hash-Berechnungsmethode auf (SHA1, SHA256 oder MD5)
- Nachricht: Listet den Wert auf, der in ein Digest-Token konvertiert werden soll
- SharedKey: Listet den geheimen Schlüssel auf

Hinweis: Verwenden Sie einen stärkeren sicheren Hash-Algorithmus wie SHA256 für die Generierung von Digest-Token.

Dieses Beispiel setzt Folgendes voraus:

- Der Webserver unterstützt C
- Ein anderer Code ruft diese Klasse auf und übergibt die erwarteten Parameter

Beispielcode

```
private stringdigestData(string strEncryptionMethod , string message , string sharedKey ) {
        UnicodeEncoding myUnicodeEncoding  = new UnicodeEncoding ( ) ;

        byte [ ] messageBytes  = System. Text. Encoding. ASCII. GetBytes (message ) ;
        byte [ ] sharedKeyBytes  = System. Text. Encoding. ASCII. GetBytes (sharedKey ) ;
        byte [ ] hashedMessage ;

        string b64SHA1Message ;

         if (this. DEBUG ) {
           TextBoxMessage. Text = message ;
           TextBoxSecret. Text = sharedKey ; }

         switch ( (strEncryptionMethod ) )

         { case "SHA1" :

              HMACSHA1 hmacsha1  = new HMACSHA1 ( ) ;
              hmacsha1. Key = sharedKeyBytes ;
              hashedMessage  = hmacsha1. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;

            case "MD5" :

              HMACMD5 hmacmd5  = new HMACMD5 (sharedKeyBytes ) ;
              hashedMessage  = hmacmd5. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            default :
              b64SHA1Message  = "Unknown Encryption Method" ; break ;
          }

        TextBoxBase64. Text = b64SHA1Message ; return b64SHA1Message ;
      }
```

Webservice – Sicherheit

Erzwingen Sie die Sicherheit mithilfe von Standardauthentifizierung, gegenseitiger Authentifizierung oder WS-Security.

Websicherheit erkunden



Erfahren Sie mehr über die Funktionen und Geschäftsvorteile der Webservicesicherheit.

Konfigurieren Sie die gegenseitige Authentifizierung



Verwenden Sie die gegenseitige Authentifizierung, um Vertrauen herzustellen, indem Sie SSL-Zertifikate (Secure Sockets Layer) austauschen.

Webservice-Sicherheit erkunden

Erzwingen Sie die Sicherheit mithilfe von Standardauthentifizierung, gegenseitiger Authentifizierung oder WS-Security.

Standardauthentifizierung

Um die Standardauthentifizierung für jede Anforderung eines WSDL-Dokuments oder das Veröffentlichen von SOAP-Nachrichten zu erzwingen, können Sie die Eigenschaft festlegen *`glide.basicauth.required`*Bis `Wahr` . Wenn Sie dies tun, muss jede WSDL- oder SOAP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderung den Header „Autorisierung“ enthalten, wie in angegeben Standardauthentifizierung protokoll. Da die Anforderung nicht interaktiv ist, wird **Autorisierung** Header ist während einer Anforderung immer erforderlich.

Die Bereitstellung von Informationen zur Standardauthentifizierung, unabhängig davon, ob sie erforderlich sind oder nicht, hat den zusätzlichen Vorteil, dass die Daten, die als Ergebnis des Webservice-Aufrufs erstellt oder aktualisiert wurden, im Namen des Anwenders erfolgen, der in den Anmeldeinformationen für die Standardauthentifizierung angegeben ist. Beispiel: Beim Erstellen eines Incident-Datensatzes haben die Journalfelder die Anwender-ID des authentifizierten Basisanwenders anstelle des Standardwerts **Gast** Anwender.

Damit der Autorisierungsheader die Kapitalisierungsregeln ignoriert, verwenden Sie *`glide.security.script.include.name.case.insensitive.list`*Eigenschaft. Sie können diese Eigenschaft in der Tabelle „Systemeigenschaften“ [sys_properties] ändern und die Skripteinbindungen hinzufügen, die zum Verarbeiten der Authentifizierung erforderlich sind. Standardmäßig hat diese Eigenschaft diese Werte:

- BasicAuth
- Anwenderdefinierte Authentifizierung

Fügen Sie nach Bedarf weitere Skripteinbindungen hinzu.

Um die Basic Authentication bei Verwendung von Perl und der SOAP::Lite-Bibliotheken bereitzustellen, können Sie die folgende Funktion implementieren:

```
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return 'user_name' =>
 'password' ; }
```

- Wenn Sie C# .NET VS 2005 oder älter verwenden, können Sie das Anmeldeinformationsobjekt nutzen, z. B.:

```
System.Net . ICredentials cred  = new System.Net . NetworkCredential ( "user_name",
 "password" ) ;

service . ServiceNow proxy  = new service . ServiceNow ( ) ;
service . get getService  = newservice . get ( ) ;
service . getResponse getServiceResponse  = new service . getResponse ( ) ;

 try {
  proxy . Credentials = cred ;
  getService . sys_id = "bf522c350a0a140701972dbf876f1610" ;
  getServiceResponse  = proxy . get (getService ) ; catch (Exception ex ) { }
```

- Bei Verwendung von C# .NET VS 2008 können Sie das ClientCredentials-Objekt nutzen, z. B.:

```
Demo_Incident. ServiceNowSoapClient client  = new Test08WebService . Demo_Incident .
 ServiceNowSoapClient ( ) ;
client . ClientCredentials . UserName . UserName = "admin" ;
client . ClientCredentials . UserName . Password = "admin" ;
```

Suchen Sie dann in Ihrer Datei „App.config“ nach dem folgenden, und ändern Sie es `Keine` Bis `Standard` :

```
<transport clientCredentialType= "None" proxyCredentialType= "None" realm= "" />
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bei der Verwendung von VB .NET würde das Objekt „Anmeldeinformationen“ folgendermaßen aussehen:

```
Sub Main()
       Dim cred  As New System.Net.NetworkCredential( "user_name",  "password")

       Dim proxy  As New VB_Democm.incident.ServiceNow
       Dim getIncident  As New VB_Democm.incident. get Dim getResponse  As New
VB_Democm.incident.getResponse

      proxy.Credentials = cred

      getIncident.sys_id =  "[your sysID here]"

      getResponse = proxy. get(getIncident)

   End Sub
```

Die resultierende Antwort, wenn die Basic Authentication aktiviert ist und keine Anmeldeinformationen angegeben werden, sieht folgendermaßen aus:

```
<html> <head > <title >Apache Tomcat/5.0.28 - Error report </ title > <style > <!--H1
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
 H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;}
 H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;}
   BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;}
 B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}    P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}   A
{color : black;}   A.name {color : black;}   HR {color : #525D76;}--> </
style > </ head > <body > <h1 >HTTP Status 401 -\ </ h1 > <HR size = "1" noshade =
"noshade" > <p >< b >type </ b > Status report </ p > <p >< b >message </ b > <u >< /
u >< / p > <p >< b >description </ b > <u >This request requires HTTP authentication ().
</ u >< / p > <HR size = "1" noshade = "noshade" > <h3 >Apache Tomcat/5.0.28 </ h3 >
</ body > </ html >
```

Konfigurieren Sie die gegenseitige Authentifizierung

Durch die gegenseitige Authentifizierung wird Vertrauen durch den Austausch von SSL-Zertifikaten (Secure Sockets Layer) hergestellt.

Während des SSL-Handshake stellt der Server dem Client sein Zertifikat vor. Anschließend kann je nach Konfiguration des Servers ein Zertifikat vom Client angefordert werden. Sowohl der Server als auch der Client führen Zertifikatvalidierungsverfahren durch, um die Authentizität und Integrität der vorgelegten Zertifikate sicherzustellen.

Nach einer erfolgreichen Validierung werden Bestätigungen ausgetauscht, bevor die HTTPS-Verbindung initiiert wird.

Hinweis: Informationen zur Verwendung eines anwenderdefinierten HTTPS-Protokollprofils zum Aktivieren der gegenseitigen Authentifizierung finden Sie unter Protokollprofile erstellen .

Administratoren führen die Vorarbeiten zur Einrichtung des Client-Schlüsselspeichers und zum Generieren von Zertifikaten durch, bevor Zertifizierungsanforderungen erfüllt werden.

Warnung: Diese Funktion aktiviert nur die gegenseitige Authentifizierung für ausgehende HTTP-Verbindungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselspeicher wird erstellt

Die Instanz unterstützt derzeit das Hochladen einer Java Key Store-Datei, die einen privaten Schlüssel und ein öffentliches Zertifikatpaar enthält. Das öffentliche Zertifikat enthält eine vollständige Kette einschließlich des Stammzertifikats.

So richten Sie Ihren Client-Schlüsselspeicher ein:

- Sie benötigen ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle (CA) signiert wurde.
- Ihr API-Endpunktanbieter kann Sie beim Generieren des Schlüsselspeichers unterstützen.

Wenn Sie den Schlüsselspeicher generieren müssen, umfasst der Prozess mehrere Schritte mit Befehlszeilenschnittstellenbefehlen, um eine neue Schlüsselspeicherdatei zu generieren, eine Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) zu erstellen und signierte Zertifikate zu importieren. Vor dem Importieren des primären Zertifikats Ihrer Domäne sollten alle Stamm- oder Zwischenzertifikate zuerst importiert werden. Hier ist eine Schritt-für-Schritt-Anweisung:

1. Generieren Sie einen Java-Schlüsselspeicher und ein Schlüsselpaar.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Generieren Sie eine CSR für einen vorhandenen Java-Schlüsselspeicher.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Senden Sie die CSR an Ihre ZERTIFIZIERUNGSSTELLE, um die Zertifikatdateien zu signieren und zurückzugeben, die Zwischen- und Stammzertifikate zusammen mit dem signierten Zertifikat enthalten.
4. Importieren Sie ein CA-Zertifikat einer Stamm- oder Zwischenzertifizierungsstelle in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

Hinweis: Sie können alle Zertifikate in einer Datei bündeln und importieren. Dies ist eine bevorzugte Option. Wenn Sie dies tun, können Sie 5 überspringen

```
keytool -import -alias mydomain -file merged.crt -keystore my.keystore
```

5. Importieren Sie ein signiertes primäres Zertifikat in einen vorhandenen Java-Schlüsselspeicher.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

Schlüsselspeicher wird eingerichtet

Nachdem der Schlüsselspeicher jetzt erstellt wurde, kann er in die Zertifikattabelle hochgeladen werden. Auf der **Systemdefinition** > **Zertifikate** Seite klicken Sie auf **Neu** Und legen Sie die folgenden Felder fest:

- Geben Sie ein Zertifikat ein **Name** .
- Speichern Sie den Schlüsselspeicher als **Aktiv** .
- Festlegen **Typ = Java Key Store** .
- Geben Sie ein an **Schlüsselspeicher-Passwort** . Dies ist das Passwort, das zum Erstellen des Schlüsselspeichers verwendet wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie Auf **Übermitteln** Zum Erstellen des Java Key Store-Eintrags.

Schlüsselspeicher

X.509 Certificate | = Required field — Update | Delete

Attachments: my.keystore [view]

Name:	Key store	Type:	Java Key Store
Active:	☑	Key store password:	••••••••••••••••••••••
Short description:	key store used for mutual authentication		

Angabe eines vertrauenswürdigen Serverzertifikats

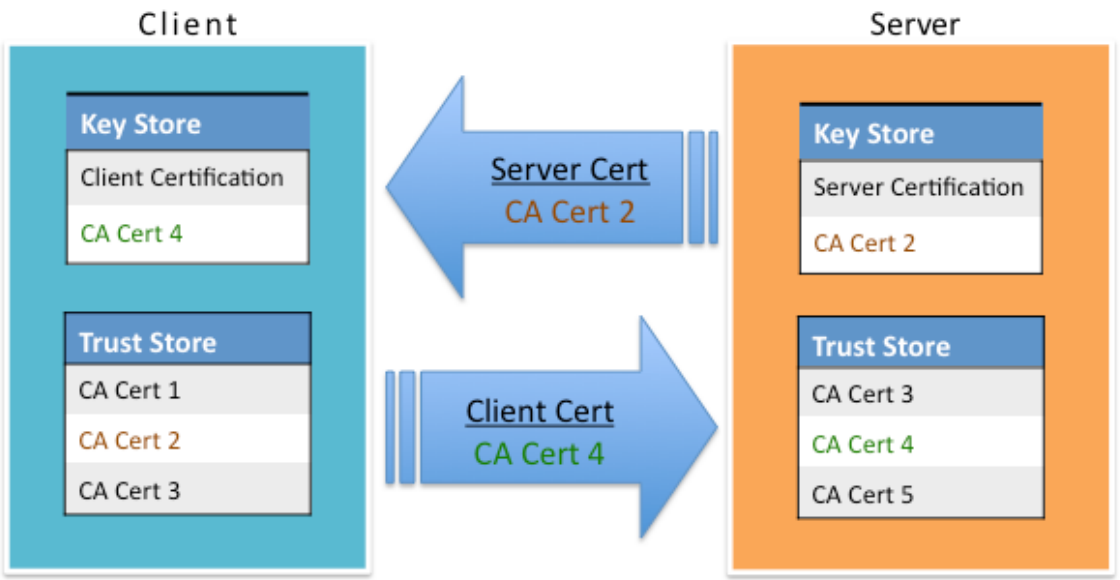
Während einer ausgehenden SSL-Verbindung, bei der es sich um einen HTTPS-Webserviceaufruf handelt, kann ein vom Service Provider bereitgestelltes Zertifikat angegeben werden, das die Gültigkeit des Service Providers während der SSL-Verbindung sicherstellt. Zum Beispiel ein Browser, der versucht, eine Verbindung zu einem sicheren Service herzustellen, der sich durch ein Zertifikat identifiziert.

Durch Hochladen des vertrauenswürdigen Serverzertifikats ServiceNow Stellt sicher, dass der Service, mit dem eine Verbindung hergestellt wird, gültig und sicher ist.

Erstellen Sie einen neuen Zertifikateintrag mit dem Typ „Trust Store-Zertifikat“, und hängen Sie ein DER-formatiertes Zertifikat an, oder kopieren Sie das PEM-Format, und fügen Sie es in ein **PEM-Zertifikat** Feld.

Protokollprofil

Zertifikataustausch



- Wenn ein Client das Serverzertifikat zur Authentifizierung anfordert, wird eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) generiert.
- Um auf eine CSR zu antworten, generiert der Server zwei eindeutige kryptografische Schlüssel: Einen öffentlichen Schlüssel, der zum Verschlüsseln von Nachrichten an den Server verwendet wird, und einen privaten Schlüssel, der zum Entschlüsseln von Nachrichten verwendet wird. Beide Schlüssel werden im Schlüsselspeicher aufbewahrt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schlüssel werden verwendet, um die sicheren Nachrichten des Clients zu entschlüsseln, damit sie vom Server gelesen werden können. Jede ausgehende Verbindung, die HTTPS sein wird, verifiziert die Zertifizierung, indem sie den Schlüsselspeicher überprüft, seine öffentliche Zertifizierung anbietet und die Truststore-Zertifikate verwendet, um das gegenseitige Vertrauen zurückzugeben.
- Um die sichere Verknüpfung zwischen dem Client und dem Server abzuschließen, stimmt der Server das Zertifikat mit dem entsprechenden privaten Schlüssel ab. Da nur der Server Zugriff auf den privaten Schlüssel hat, kann der Server die Daten vom Client entschlüsseln.

Hinweis: Informationen zur Verwendung eines anwenderdefinierten HTTPS-Protokollprofils zum Aktivieren der gegenseitigen Authentifizierung finden Sie unter Protokollprofile erstellen .

Der Server antwortet, indem er ein Zertifikat sendet. Ist dies ein Zertifikat, das der Client akzeptiert? Wenn ja, wird eine Nachricht an den Server gesendet, der das Zertifikat akzeptiert, und ein sicherer Kanal wird initiiert. Wenn das Zertifikat nicht akzeptiert wird, kann dies bedeuten, dass die Stammberechtigung für die Zertifizierung erforderlich ist.

Regeln Für Zugriffssteuerungsliste

Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

ACLs erkunden



Erfahren Sie mehr über Zugriffssteuerungslisten (ACLs).

Konfigurieren Sie ACLs



Konfigurieren Sie ACLs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontextbezogener Sicherheitsmanager



Erfahren Sie mehr über den kontextbezogenen Sicherheitsmanager.

Erweiterte ACL-Konfiguration



Erfahren Sie mehr über erweiterte ACL-Konfigurationen und -Tools.

Zugriffssteuerungslisten Erkunden

Untersuchen Sie Zugriffssteuerungslisten (ACLs).

Alle Regeln für Zugriffssteuerungslisten geben Folgendes an:

- Die *Entscheidungstyp* , *Regeltyp* Und *Vorgang* Welche die ACL definiert
- Die *Objekt* Wird gesichert
- Die *Bedingungen* Erforderlich für den Zugriff auf das Objekt

Komponenten der ACL

Der Entscheidungstyp definiert, ob Anwender auf das Objekt zugreifen dürfen, wenn Bedingungen erfüllt sind, oder verweigert den Zugriff auf das Objekt, es sei denn, die Bedingungen sind erfüllt.

Entscheidungstyp	Beschreibung
Verweigern – Es Sei Denn	Beschränken Sie den Zugriff auf die Ressource, indem Sie den Zugriff explizit verweigern, es sei denn, Bedingungen werden übergeben. Weitere Informationen finden Sie unter #unique_1461_Connect_42_section_qnd_snl_zbc.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entscheidungstyp	Beschreibung
Zulassen, Wenn	Zugriff auf Ressource zulassen, wenn Bedingungen übergeben werden.

Die *Objekt* Ist das Ziel, auf das der Zugriff gesteuert werden muss. Jedes Objekt besteht aus einem Typ und einem Namen, die eine bestimmte Tabelle, ein bestimmtes Feld oder einen bestimmten Datensatz eindeutig identifizieren. Mit *Gilt für* Feldanwender haben eine granulare Kontrolle darüber, für welche spezifischen Datensätze diese ACL gilt.

Beispielsweise geben alle diese Einträge ein Objekt an:

Typ	Name	Objekt gesichert
record	[Incident].[--keine--]	Die Incident-Tabelle.
record	[Incident].[aktiv]	Das Feld aktiv in der Incident-Tabelle.
record	[incident] Gilt für: Priorität = P1	Nur Incidents mit Priorität 1 in der Incident-Tabelle.
REST_Endpoint	User_role_inheritance	Der Datensatz für die geskriptete REST API user_role_inheritance.

Jeweils *Vorgang* Beschreibt einen gültigen *Aktion* Das System kann das angegebene Objekt übernehmen. Einige Objekte, z. B. Datensätze, unterstützen mehrere Vorgänge, während andere Objekte, z. B. ein REST_Endpoint, nur einen Vorgang unterstützen.

Beispiel: Alle diese Einträge geben einen Vorgang an:

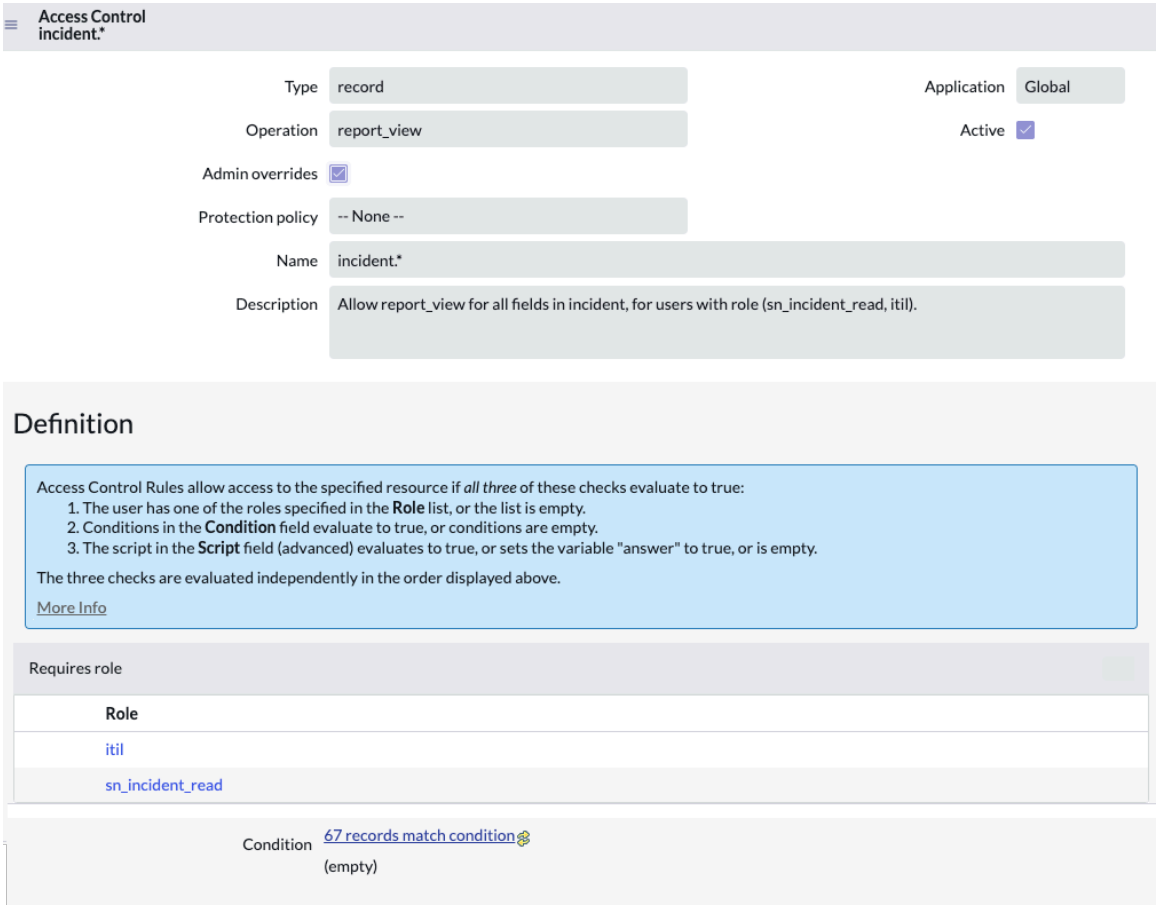
Typ	Name	Vorgang	Vorgang gesichert
record	[Incident].[--keine--]	Erstellen	Erstellen von Datensätzen in der Incident-Tabelle.
record	[Incident].[aktiv]	Schreiben	Das Feld aktiv in der Incident-Tabelle wird aktualisiert.
REST_Endpoint	User_role_inheritance	ausführen	Ausführung der geskripteten REST API user_role_inheritance.

Die *Bedingungen* Geben Sie an, wann jemand auf das benannte Objekt und den benannten Vorgang zugreifen kann. Sicherheitsadministratoren können Bedingungsanforderungen angeben, indem sie Folgendes hinzufügen:

- Eine oder mehrere Anwenderrollen für den **Erfordert Rolle** Liste.
- Mindestens ein Sicherheitsattribut muss als „wahr“ ausgewertet werden.
- Mindestens eine Datenbedingung.
- Ein Skript, das als „wahr“ oder „falsch“ ausgewertet oder festgelegt wird `Antwort` Variable auf „wahr“ oder „falsch“.

Um Zugriff auf ein Objekt und einen Vorgang zu erhalten, muss ein Anwender alle in einer Zugriffssteuerung aufgeführten Bedingungen erfüllen. Diese Zugriffssteuerung schränkt beispielsweise den Zugriff auf die Anzeige von Vorgängen in der Incident-Tabelle ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Um einen Datensatz in der Incident-Tabelle zu aktualisieren, muss ein Anwender über die aufgelisteten Rollen verfügen, und der Datensatz muss die Bedingung erfüllen.

Bedingungstyp	Anforderung	Beschreibung
Erfordert Rolle	**Erfordert Rolle** : itil	Erlauben Sie nur Anwendern mit der Rolle itil, Incidents zu aktualisieren.
Sicherheitsattribute	UserIsAuthenticated	Nur authentifizierte Anwender zum Aktualisieren von Incidents.
Datenbedingung	[Incident-Status] [ist nicht] [Geschlossen]	Nur Aktualisierungen aktiver Incident-Datensätze zulassen.

Gilt für Verhalten

Die *Gilt für* Das Feld bestimmt, ob eine ACL für Datensätze gilt, während die Datenbedingung eine bereits angewendete ACL auswertet. *Gilt für* Gibt an, ob sich die ACL auf einen bestimmten Datensatz auswirkt. Wenn sie leer ist, gilt die ACL für alle Datensätze. *Gilt für* Kann für die granulare ACL-Durchsetzung verwendet werden, während „Datenbedingung“ ein Bewertungskriterium ist.

Hinweis: *Gilt für* Ist Groß-/Kleinschreibung beachten.

Standardmäßiges Verhalten ablehnen

Standardmäßig verweigert die ACL-Engine den Zugriff vollständig, wenn eine ACL leer oder ungültig ist. Leere ACLs sind als ACLs ohne eine oder mehrere dieser Komponenten definiert:

Automatische Übersetzung

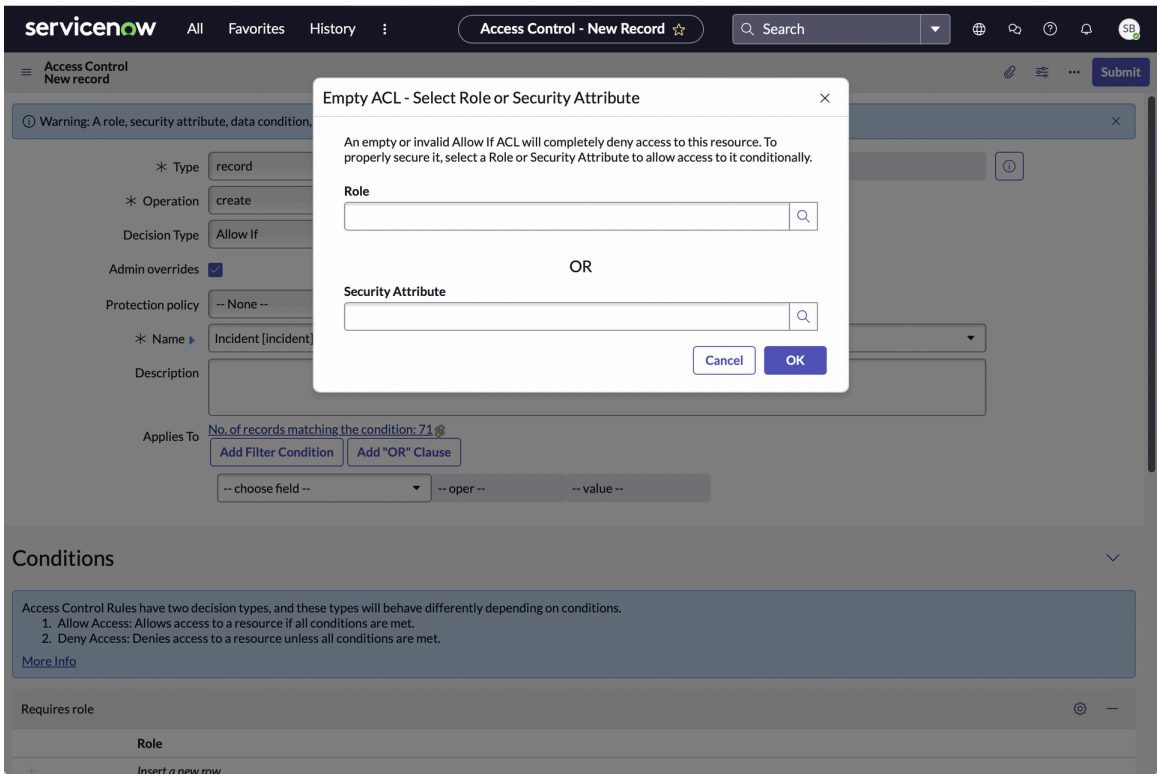
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Definierte Rolle
- Sicherheitsattribut
- Datenbedingung
- Skript

Ungültige ACLs sind definiert als:

- ACLs mit Rollen, die nicht vorhanden sind (z. B. keine Zeile in der Datenbank)
- ACLs mit nicht vorhandenen Sicherheitsattributen (z. B. keine Zeile in der Datenbank)
- ACLs mit einem Skript, das „answer=true“ oder „wahr“ enthält

Wenn das System erkennt, dass der Anwender eine ACL erstellt, fordert es den Anwender auf, eine Rolle oder ein vorhandenes Sicherheitsattribut auszuwählen.



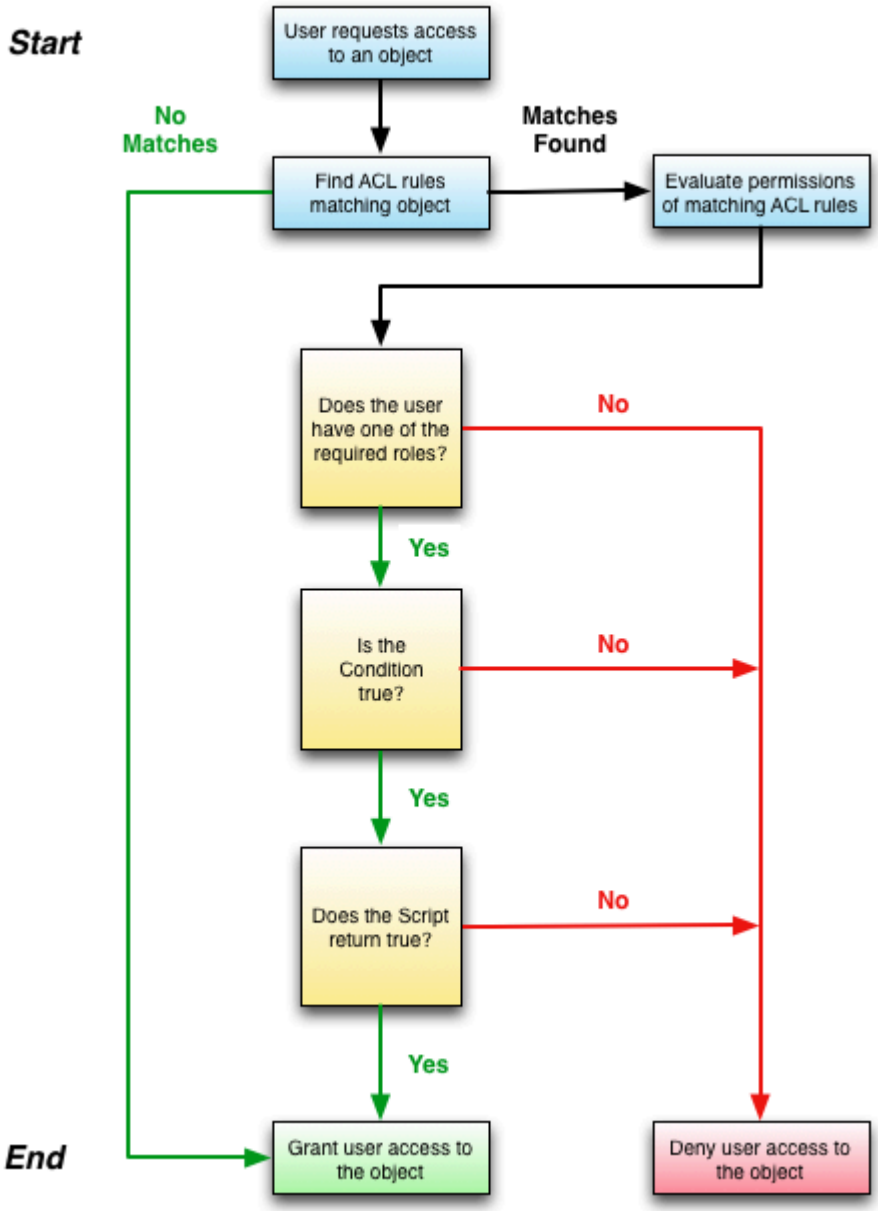
ACL-Bewertungsprozess

Eine ACL-Regel gewährt einem Anwender nur Zugriff auf ein Objekt, wenn der Anwender alle Bedingungen erfüllt, die für die übereinstimmende ACL-Regel erforderlich sind.

- Die Bedingung muss bis ausgewertet werden *Wahr* .
- Das Skript muss bis ausgewertet werden *Wahr* Oder geben Sie eine Antwortvariable mit dem Wert zurück *Wahr* .
- Der Anwender muss über eine der Rollen in der Liste der erforderlichen Rollen verfügen. Wenn die Liste leer ist, wird diese Bedingung als ausgewertet *Wahr* .
- [Nur Datensatz-ACL-Regeln] die übereinstimmenden ACL-Regeln auf Tabellenebene und Feldebene müssen beide als ausgewertet werden *Wahr* .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL-Auswertungsbedingungen



Wenn eine Sitzung Daten anfordert, sucht das System nach Zugriffssteuerungsregeln, die dem angeforderten Objekt und Vorgang entsprechen. Wenn eine übereinstimmende Zugriffssteuerungsregel vorhanden ist, bewertet das System, ob der Anwender über die Bedingungen verfügt, die für den Zugriff auf das Objekt und den Vorgang erforderlich sind. Wenn eine Zugriffssteuerungsregel mehr als eine Bedingung angibt, muss der Anwender alle Bedingungen erfüllen, um Zugriff auf das Objekt und den Vorgang zu erhalten. Wenn eine Bedingungsprüfung fehlschlägt, kann der Anwender nicht auf das übereinstimmende Objekt und den entsprechenden Vorgang zugreifen.

Wenn ein Anwender die Bedingungen der ersten Übereinstimmungsregel nicht erfüllt, wertet das System die Bedingungen der nächsten übereinstimmenden Zugriffssteuerungsregel aus, wie in der Verarbeitungsreihenfolge der Zugriffssteuerung angegeben. Wenn der Anwender die Bedingungen einer übereinstimmenden Zugriffssteuerungsregel nicht erfüllt, verweigert das System den Zugriff auf das angeforderte Objekt und den angeforderten Vorgang.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn keine übereinstimmenden Zugriffssteuerungsregeln für das angeforderte Objekt und den angeforderten Vorgang vorhanden sind, gewährt das System dem Anwender Zugriff darauf. In der Praxis findet das System selten keine übereinstimmenden Regeln, da das System über eine Reihe von standardmäßigen Zugriffssteuerungsregeln verfügt, die alle Datensatzvorgänge schützen.

Die Auswirkungen, die der Zugriff auf ein Objekt verweigert wird, hängen von der ACL-Regel ab, die der Anwender fehlgeschlagen ist. Wenn beispielsweise eine ACL-Regel für Lesevorgänge fehlschlägt, kann der Anwender das Objekt nicht sehen. Je nach gesichertem Objekt blendet die ACL-Regel ein Feld in einem Formular aus, blendet Zeilen in einer Liste aus oder verhindert, dass ein Anwender auf eine UI-Seite zugreift. Die folgende Tabelle enthält eine vollständige Liste der Ergebnisse des Fehlschlags einer ACL-Regel für einen bestimmten Vorgang und Objekttyp.

ACL-Prüfungen vor und nach der Abfrage

Ihre Instanz überprüft ACL-Regeln sowohl vor als auch nachdem ein Anwender eine Abfrage erstellt hat. Da vor und nach einer Abfrage verschiedene Informationen verfügbar sind, können die Ergebnisse unterschiedlich sein.

ACL-Prüfung vorab abfragen

Bevor Ihre Instanz eine Datenbankabfrage ausführt, überprüft sie die ACL-Regeln für jedes Feld in der abgefragten Tabelle, um zu bestimmen, auf welche Felder ein Anwender zugreifen kann. Diese Prüfung untersucht nur die Rollen des Anwenders und überprüft, ob diese Rollen Zugriff auf Felder zulassen. Da diese Prüfung vor der Abfrage ausgeführt wird, hat die ACL keinen Zugriff auf die Datensätze in der Tabelle, daher kann sie diese Daten nicht berücksichtigen. Skripts und Bedingungen, die davon abhängen, den Inhalt eines Datensatzes zu kennen, werden nicht ausgewertet.

Wenn der Anwender zu diesem Zeitpunkt keinen Lesezugriff hat, wird dem Anwender der Wert für das Feld nicht angezeigt.

ACL-Prüfung nach Abfrage

Nach der Abfrage überprüft Ihre Instanz jeden von der Abfrage zurückgegebenen Datensatz. Während dieser Prüfung gibt es Kontext für die ACL, sodass die Rollen-, Bedingungs- und Skriptabschnitte der ACL ausgewertet werden. Wenn der Anwender zu diesem Zeitpunkt keinen Lesezugriff hat, wird dem Anwender der Wert für das Feld nicht angezeigt. Der Anwender sieht jedoch die Feldbezeichnung, wenn seine Rollen den Zugriff auf das Feld zulassen.

Vorgang	Ergebnisse des Fehlschlags einer ACL-Regel für ein Objekt
ausführen	Anwender kann keine Skripts auf einem Datensatz oder einer UI-Seite ausführen.
Erstellen	Anwender kann nicht sehen **Neu** UI-Aktion aus Formularen. Der Anwender kann auch keine Datensätze mithilfe von API-Protokollen wie Webservices in eine Tabelle einfügen. A **Erstellen** ACL mit einer Bedingung, die erfordert, dass ein Feld einen bestimmten Wert enthält, kann als falsch ausgewertet werden. Felder in neuen Datensätzen werden als leer betrachtet, bis der Datensatz gespeichert wurde.
gelesen	Der Anwender kann das Objekt in Formularen oder Listen nicht sehen. Der Anwender kann auch keine Datensätze mit API-Protokollen wie Webservices abrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang	Ergebnisse des Fehlschlags einer ACL-Regel für ein Objekt
Schreiben	Der Anwender sieht ein schreibgeschütztes Feld in Formularen und Listen, und der Anwender kann Datensätze nicht mithilfe von API-Protokollen wie Webservices aktualisieren.
löschen	Anwender kann nicht sehen **Löschen** UI-Aktion aus Formularen. Der Anwender kann auch keine Datensätze aus einer Tabelle mithilfe von API-Protokollen wie Webservices entfernen.
Edit_Task_Relations	Anwender kann keine Beziehungen zwischen Aufgabentabellen definieren.
Edit_ci_Relations	Anwender kann keine Beziehungen zwischen Konfigurationselement-Tabellen [cmdb_ci] definieren.
Save_as_template	Wird verwendet, um die Felder zu steuern, die beim Erstellen einer Vorlage gespeichert werden sollen.
Add_to_list	Anwender kann bestimmte Spalten in der Listenmechanik nicht anzeigen oder personalisieren.
List_Edit	Anwender kann Datensätze (Zeilen) aus einer Liste nicht aktualisieren.
report_on	Anwender kann keinen Bericht in der ACL-Tabelle erstellen. Weitere Informationen finden Sie unter Beschränken Sie die Berichterstellung mit einer ACL-Regel .
report_view	Der Anwender kann den Inhalt eines Berichts nicht in der ACL-Tabelle oder im ACL-Feld anzeigen. Weitere Informationen finden Sie unter Reporting .
Personalize_choices	Anwender kann nicht mit der rechten Maustaste auf ein Listenfeld klicken und auswählen **Konfigurieren Sie Auswahlmöglichkeiten** .

ACL-übereinstimmende Anforderungen für Objekte

Objekttyp	Übereinstimmende ACL-Regeln, die für den Zugriff auf das Objekt erforderlich sind	Vorhandene Platzhalter-ACL-Regeln
Vom Client aufrufbare Skripteinbindungen Prozessoren	Anwender müssen die Bedingungen von zwei ACL-Regeln erfüllen: 1. Alle ACL-Regeln mit Platzhaltern für das Objekt (wenn für den Vorgang eine ACL-Regel vorhanden ist). 2. Die erste ACL-Regel, die dem Namen des Objekts entspricht (wenn für den Vorgang eine ACL-Regel vorhanden ist).	Standardmäßig gibt es keine Platzhalterregeln (*) für diese Objekttypen. Wenn Sie eine Platzhalter-ACL-Regel für eines dieser Objekte erstellen, gilt die ACL-Regel für alle Objekte dieses Typs.
UI-Seiten Datensatz	Anwender müssen die Bedingungen von zwei ACL-Regeln erfüllen: 1. Die erste ACL-Regel, die dem Feld des Datensatzes entspricht (wenn für den	Standardmäßig gibt es Platzhaltertabellenregeln (*) für die Vorgänge „Erstellen“, „Lesen“, „Schreiben“ und „Löschen“ sowie Platzhalterfeldregeln (*.*) für die Vorgänge „Personalize_choices“,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objekttyp	Übereinstimmende ACL-Regeln, die für den Zugriff auf das Objekt erforderlich sind	Vorhandene Platzhalter-ACL-Regeln
	Vorgang eine ACL-Regel vorhanden ist). 2. Die erste ACL-Regel, die der Tabelle des Datensatzes entspricht (wenn für den Vorgang eine ACL-Regel vorhanden ist).	„create“ und „Save_as_template“. Wenn Sie eine Tabelle erstellen, erstellen Sie ACL-Regeln für die Tabelle, es sei denn, Sie möchten die bereitgestellten ACL-Regeln mit Platzhaltern verwenden.

Hinweis: Das Standardverhalten des Sicherheitsmanagers (`glide.sm.default_mode` Die Eigenschaft) bestimmt, ob Anwender auf Objekte zugreifen können, die nur ACL-Regeln für Platzhaltertabellen entsprechen. Wenn diese Eigenschaft auf festgelegt ist *Zugriff verweigern* , Nur Administratoren können auf Objekte zugreifen, die den ACL-Regeln der Platzhaltertabelle entsprechen.

Hinweis: Die ACL-Regel für Platzhalterfeld (*.*) für den Erstellungsvorgang verwendet dieselben Bedingungen wie der Schreibvorgang. Dies bedeutet, dass die Erstellungsbedingungen mit den Schreibbedingungen identisch sind, es sei denn, Sie definieren eine explizite ACL-Regel für Erstellungsvorgänge.

Mehrere ACL-Regeln am selben Punkt in der Verarbeitungsreihenfolge

Wenn zwei oder mehr Regeln an demselben Punkt in der Verarbeitungsreihenfolge übereinstimmen, muss der Anwender eine der ACL-Regelbedingungen übergeben, um auf das Objekt zuzugreifen. Wenn Sie beispielsweise ACL-Regeln für zwei Felder erstellen `incident.number`, Dann hat ein Anwender, der eine Regel übergibt, Zugriff auf das Nummernfeld, unabhängig davon, ob der Anwender eine andere Feld-ACL-Regel am selben Punkt in der Verarbeitungsreihenfolge fehlgeschlagen ist.

Erforderliche Rolle

Normale Administratorbenutzer können Zugriffssteuerungsregeln anzeigen und debuggen. Um jedoch vorhandene Zugriffssteuerungsregeln zu erstellen oder zu aktualisieren, müssen Administratoren Berechtigungen auf die Rolle „Security_admin“ erhöhen. Siehe Auf eine privilegierte Rolle hochstufen für Anweisungen.

ACL-Regeln in bereichsbezogenen Anwendungen

Sie können ACL-Regeln für Objekte im selben Umfang wie die ACL-Regel erstellen. Sie können auch ACL-Regeln für Tabellen mit mindestens einem Feld erstellen, das sich im gleichen Umfang wie die ACL-Regel befindet.

Für Tabellen, die sich in einem anderen Umfang als der ACL-Regeldatensatz befinden, sind die Arten von Regeln beschränkt.

- Sie können eine ACL-Regel für jede Tabelle, UI-Seite oder ein anderes Objekt erstellen, das sich im selben Umfang wie die ACL-Regel befindet.
- Sie können eine ACL für ein Feld erstellen, das sich im selben Umfang wie die ACL-Regel befindet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn sich die Tabelle im selben Umfang befindet, können Sie ein Skript zum Auswerten von Bedingungen verwenden.
- Wenn sich die Tabelle in einem anderen Bereich befindet, können Sie kein Skript zum Auswerten von Bedingungen verwenden.

- Sie können keine ACL-Regeln für Objekte erstellen oder ändern, die sich in einem anderen Bereich als der Anwendung befinden, die Sie in der Anwendungsauswahl ausgewählt haben, einschließlich dem Hinzufügen einer Rolle zu einer ACL in einem anderen Bereich.
- Sie können Platzhaltertabellenregeln (*) nur im globalen Bereich erstellen.
- Sie können Platzhalterfeldregeln (*) nur für Tabellen im selben Umfang wie die ACL-Regel erstellen.

ACL_Regeltypen

Erstellen Sie ACL-Regeln für verschiedene Komponenten des Systems.

Datensatz-ACL-Regeln

Datensatz-ACL-Regeln bestehen aus Tabellen- und Feldnamen.

- Der Tabellenname ist die Tabelle, die Sie sichern möchten. Wenn andere Tabellen aus dieser Tabelle erweitert werden, wird die Tabelle als übergeordnete Tabelle betrachtet. ACL-Regeln für übergeordnete Tabellen gelten für alle Tabellen, die die übergeordnete Tabelle erweitern.
- Der Feldname ist das Feld, das Sie sichern möchten. Einige Felder sind aufgrund der Tabellenerweiterung Teil mehrerer Tabellen. ACL-Regeln für Felder in einer übergeordneten Tabelle gelten für jede Tabelle, die die übergeordnete Tabelle erweitert.

ACL-Regeln können die folgenden Datensatzvorgänge sichern:

Vorgang	Beschreibung
ausführen	Ermöglicht Anwendern die Ausführung aufrufbarer Clientskripteinbindungen und die Ausführung von REST-Endpunkten.
Query_match	Ermöglicht Anwendern das Senden von Übereinstimmungsabfragen („ist“, „ist nicht“, „ist leer“ usw.).
Conditional_table_query_Range	Ermöglicht Anwendern, partiellen ACL-Zugriff basierend auf Lese-ACLs zu gewähren. Erstellt für die Tabellen, die die Lese-ACLs ohne Datenbedingung und Skript haben.
Query_Range	Ermöglicht Anwendern das Senden von Bereichsabfragen („beginnt mit“, „endet mit“, „enthält“ usw.), und die Sortierung ist uneingeschränkt.
Erstellen	Ermöglicht Anwendern das Einfügen neuer Datensätze (Zeilen) in eine Tabelle.
gelesen	Ermöglicht Anwendern das Anzeigen von Datensätzen aus einer Tabelle.
Schreiben	Ermöglicht Anwendern das Aktualisieren von Datensätzen in einer Tabelle.
löschen	Ermöglicht Anwendern das Entfernen von Datensätzen aus einer Tabelle oder das Ablegen einer Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang	Beschreibung
Edit_Task_Relations	Ermöglicht Anwendern das erweitern der Aufgabentabelle [Task].
Edit_ci_Relations	Ermöglicht Anwendern, die Tabelle „Konfigurationselement“ [cmdb_ci] zu erweitern.
Save_as_template	Ermöglicht Anwendern das Speichern eines Datensatzes als Vorlage.
Add_to_list	Verhindert, dass Anwender bestimmte Spalten in der Listenmechanik anzeigen oder personalisieren. **Hinweis:** Bedingungen und Skripts werden nicht unterstützt.
List_Edit	Ermöglicht Anwendern das Aktualisieren von Datensätzen (Zeilen) aus einer Liste.
report_on	Ermöglicht Anwendern, Berichte über Tabellen zu erstellen.
report_view	Ermöglicht Anwendern, Berichte zu Feld-ACLs zu erstellen.
Personalize_choices	Ermöglicht Anwendern das Konfigurieren der Tabelle oder des Felds.
Data_Fabric	Ermöglicht es einer Daten-Fabric-Tabelle, auf eine lokale Tabelle zu verweisen.

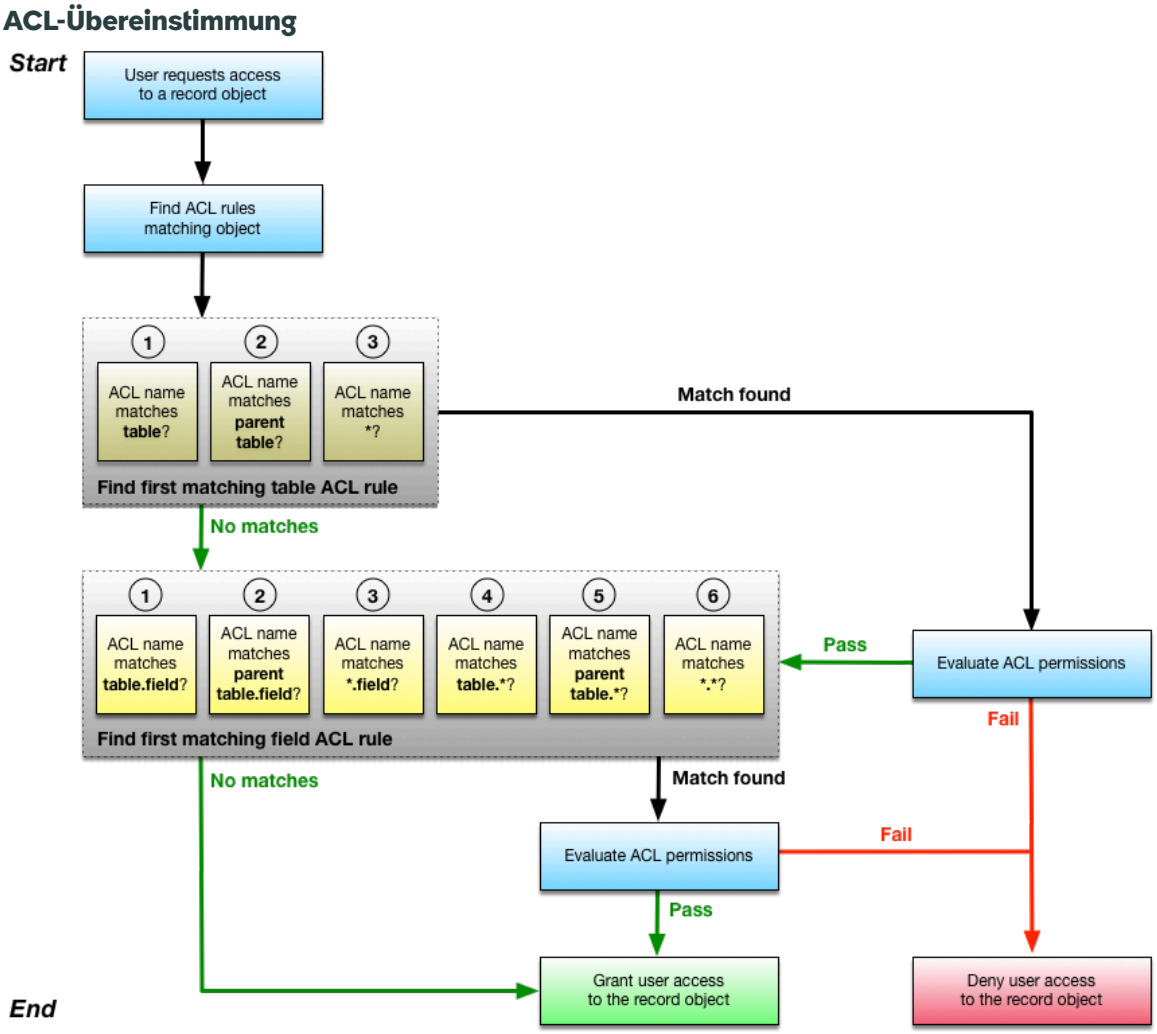
Datensatz-ACL-Regeln werden in der folgenden Reihenfolge verarbeitet:

- Objekt mit Tabellen-ACL-Regeln abgleichen.
- Gleicht das Objekt mit Feld-ACL-Regeln ab.

Diese Verarbeitungsreihenfolge stellt sicher, dass Anwender Zugriff auf spezifischere Objekte erhalten, bevor sie Zugriff auf allgemeinere Objekte erhalten. Ein Anwender muss sowohl Tabellen- als auch Feld-ACL-Regeln übergeben, um auf ein Datensatzobjekt zuzugreifen.

- Wenn ein Anwender eine Tabellen-ACL-Regel nicht erfüllt, wird dem Anwender der Zugriff auf alle Felder in der Tabelle verweigert, auch wenn der Anwender eine Feld-ACL-Regel übergibt.
- Wenn ein Anwender eine Tabellen-ACL-Regel übergibt, aber eine Feld-ACL-Regel fehlschlägt, kann der Anwender nicht auf das von der Feld-ACL-Regel beschriebene Feld zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Prozessor-ACL-Regeln

Prozessor-ACL-Regeln geben den Prozessor an, den Sie sichern möchten. Eine Liste der verfügbaren Prozessoren finden Sie unter **Systemdefinition** > **Prozessoren**an.

Standardmäßig ist eine ACL-Regel für den EmailClientProcessor enthalten, um den E-Mail-Client auf Anwender mit der Rolle itil zu beschränken.

Prozessor-ACL-Regeln berücksichtigen die STAR-Regel (*), wenn sie keine spezifischere ACL für diese Ressourcen finden können.

Tabellen-ACL-Regeln

Der Anwender muss zuerst die Tabellen-ACL-Regel übergeben. Da das Basissystem ACL-Regeln für STERNTABELLEN (*) enthält, die jeder Tabelle entsprechen, muss der Anwender immer mindestens eine Tabellen-ACL-Regel übergeben. Das Basissystem bietet zusätzliche Tabellen-ACL-Regeln, um den Zugriff auf bestimmte Tabellen zu steuern.

Tabellen-ACL-Regeln werden in der folgenden Reihenfolge verarbeitet:

1. Stimmen Sie mit dem Tabellennamen überein. Beispiel: Incident.
2. Stimmen Sie mit dem Namen der übergeordneten Tabelle überein. Beispiel: Aufgabe.
3. Stimmen Sie mit einem beliebigen Tabellennamen (*) überein. Beispiel: *.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Anwender alle Tabellen-ACL-Regeln nicht erfüllt, kann er nicht auf Felder in der Tabelle zugreifen. Wenn ein Anwender eine Tabellen-ACL-Regel übergibt, wertet das System die Feld-ACL-Regeln aus.

Feld-ACL-Regeln

Nachdem ein Anwender eine Tabellen-ACL-Regel übergeben hat, werden Feld-ACL-Regeln in der folgenden Reihenfolge verarbeitet:

1. Stimmen Sie dem Tabellen- und Feldnamen zu. Beispiel: Incident.number.
2. Stimmen Sie mit der übergeordneten Tabelle und dem Feldnamen überein. Beispiel: Task.number.
3. Stimmen Sie mit einer beliebigen Tabelle (*) und einem Feldnamen überein. Beispiel: *.number.
4. Ordnen Sie die Tabelle und ein beliebiges Feld (*) zu. Beispiel: Incident.*.
5. Ordnen Sie die übergeordnete Tabelle und ein beliebiges Feld (*) zu. Beispiel: Aufgabe.*.
6. Stimmen Sie mit einer beliebigen Tabelle (*) und einem beliebigen Feld (*) überein. Beispiel: *.*.

Ein Anwender muss die Tabellen-ACL-Regel übergeben, um Zugriff auf die Felder der Tabelle zu erhalten. Beispielsweise muss der Anwender zuerst die Tabellen-ACL-Regel übergeben, damit die Incident-Tabelle auf zugreifen kann **Nummer** Feld in der Incident-Tabelle.

Die erste erfolgreiche Feld-ACL-Auswertung stoppt die ACL-Regelverarbeitung auf Feldebene. Wenn ein Anwender eine Feld-ACL-Regel übergibt, stoppt das System die Suche nach anderen ACL-Regeln für übereinstimmende Felder. Wenn ein Anwender beispielsweise die Feld-ACL-Regel für Incident.number übergibt, sucht das System nicht mehr nach anderen ACL-Regeln, die den sichern **Nummer** Feld in der Incident-Tabelle.

Der Zugriff auf Abfrageinformationen von abgeleiteten Daten ist für geschützte Felder eingeschränkt, wodurch die Rückgabe von Vorhersageinformationen verhindert wird.

ACL-Regeln der UI-Seite

ACL-Regeln für UI-Seiten geben die zu sichernde UI-Seite an. Um eine Liste der verfügbaren UI-Seiten zu erhalten, navigieren Sie zu **System-UI** > **UI-Seiten**an. Verwenden Sie beim Definieren einer ACL-Regel für eine UI-Seite den vollständigen bereichsbezogenen Seitennamen. Beispiel: **X_myApp_Mypage** .

Hinweis: Sie können das STERNZEICHEN (*) in verwenden **Name** Feld ein **ui_page** Geben Sie ACLs ein, um UI-Seiten abzugleichen.

ACL-Regeln der UI-Seite berücksichtigen die STAR-Regel (*), wenn sie keine spezifischere ACL für diese Ressourcen finden können. Beispiel: Wenn Sie eine UI-Seite mit dem Namen haben Meine Sekretseite Definieren Sie jedoch keine ACL für diese UI-Seite. Die STAR-Regel (*) für den UI-Seitenprozessor wird für die Zugriffsprüfung verwendet.

ACL-Regeln können den folgenden UI-Seitenvorgang sichern:

Vorgang	Beschreibung
gelesen	Ermöglicht Anwendern das Anzeigen der UI-Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vom Client aufrufbare Skripteinbindungsregeln

ACL-Regeln für Skripteinbindung geben die vom Client aufrufbare Skripteinbindung an, die gesichert werden soll. Eine Liste der verfügbaren Skripteinbindungen finden Sie unter **Systemdefinition** > **Skripteinbindungen**an. Sie können die Liste personalisieren, um anzuzeigen *Vom Client aufrufbar* Spalte.

Das Basissystem enthält keine ACL-Regeln für vom Client aufrufbare Skripteinbindungen.

Vom Client aufrufbare Skripteinbindungsregeln berücksichtigen die STAR-Regel (*), wenn sie keine spezifischere ACL für diese Ressourcen finden können.

Datentyp-ACL

Mit der Datentyp-ACL können Sie ACL-Regeln schreiben, die für alle Felder eines bestimmten Typs gelten.

Datentyp-ACLs bieten einen gezielten Ansatz für Zugriffssteuerungen, indem Tabellenfelder basierend auf dem Datentyp eingeschränkt werden. Dies ermöglicht umfassendere Sicherheitsbeschränkungen als Wildcard(*)-ACLs. Die Syntax für Datentyp-ACLs folgt dem Format *.[(Feld, das eingeschränkt werden soll)].

Herkömmliche Feld-ACLs sind auf bestimmte Tabellen-Feld-Bezeichner, alle Felder in einer Tabelle oder alle Tabellen mit einem bestimmten Feldnamen beschränkt. Im Gegensatz dazu ermöglichen die Datentyp-ACLs es Ihnen, die Sicherheit einheitlich auf Felder anzuwenden, die bestimmte Metadaten teilen. Dadurch wird verhindert, dass zusätzliche ACLs erstellt werden, um die Sicherheit einheitlich auf alle Felder anzuwenden.

Bei der Implementierung von Datentyp-ACLs müssen alle betroffenen Felder vor und nach dem Hinzufügen validiert werden, um unerwartete Sicherheitsprobleme zu vermeiden. Siehe Erstellen Sie eine Datentyp-ACL Um eine eigene Datentyp-ACL zu erstellen.

Um vorhandene Datentyp-ACLs zu überprüfen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Zugriffssteuerungen** Und verwenden **Name** Feld für die Suche nach ACLs, die mit beginnen *.[.

Hinweis: Skripting-Governance verwendet standardmäßig ACLs vom Datentyp für Skripting-Einschränkungen. Weitere Informationen finden Sie unter _.

Erstellen Sie eine Datentyp-ACL

Erfahren Sie, wie Sie eine Datentyp-ACL erstellen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

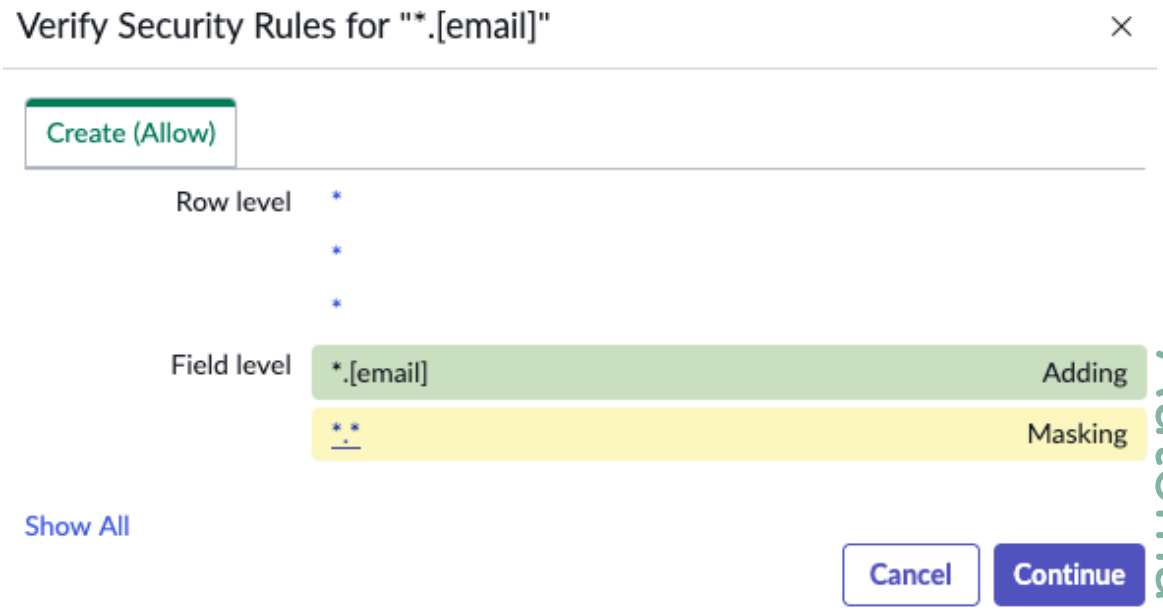
1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffssteuerungen**an.
2. Wählen Sie aus **Neu** Schaltfläche.
3. Wählen Sie aus **Change-Modus** Symbol In der Nähe von **Name** Feld
4. Geben Sie Ihren Datentyp im Format ein *.[Anwenderdatentyp] In **Name** Feld.
5. Wählen Sie ein aus **Rolle** Oder **Sicherheitsattribut** Zur Zuordnung zur ACL.
6. **Wahlweise:** Geben Sie zusätzliche Details in ein **Erstellen Sie eine ACL** Formular. Weitere Informationen finden Sie unter Konfigurieren Sie eine ACL-Regel.
7. Wählen Sie **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Überprüfen Sie die Sicherheitsregeln für die ACL im Popup **Überprüfen Sie Die Sicherheitsregeln** Fenster.

Beispiel für Sicherheitsregeln verifizieren



ACL-Steuerung von Funktionsfeldern

Bei der Auswertung des Zugriffs auf ein Funktionsfeld überprüft das System zusätzlich zum Überprüfen des Zugriffs auf das Funktionsfeld selbst auch den Zugriff auf die beitragenden Felder der Funktion. Beitragende Felder sind diejenigen, die als Argumente in einer bestimmten Funktionsdefinition verwendet werden.

Weitere Informationen zu Funktionsfeldern finden Sie unter Funktionsfeld .

In Rome Und früher überprüft das System einfach den Zugriff auf das Funktionsfeld selbst (wie bei jedem anderen Feld). Wenn die ACLs in diesem Feld Zugriff zulassen, erhält der Anwender den resultierenden Wert, unabhängig davon, ob der Anwender Zugriff auf die beitragenden Felder hat.

In Zurich Später erfordert das System auch Zugriff auf alle beitragenden Felder, um Zugriff auf das Funktionsfeld zu ermöglichen. Wenn eine oder mehrere der beitragenden Feld-ACLs den Zugriff verweigern, verweigert das Funktionsfeld auch den Zugriff.

Die einzigen Vorgänge, die von der neuen Anforderung betroffen sind, sind read und Report_View. Report_View hat eigene zusätzliche Anforderungen.

Vorgang	Beschreibung
Lesevorgang	Ein Anwender hat nur Lesezugriff auf ein Funktionsfeld, wenn beide der folgenden Aussagen wahr sind: • Der Anwender hat Lesezugriff auf das Funktionsfeld. • Der Anwender hat Lesezugriff auf alle beitragenden Felder, die in der Funktion verwendet werden.
Vorgang „Report_View“	Ein Anwender hat nur dann Report_View-Zugriff auf ein Funktionsfeld, wenn alle der folgenden Elemente wahr sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang	Beschreibung
	• Der Anwender hat Report_View-Zugriff auf das Funktionsfeld. • Der Anwender hat Report_View-Zugriff auf jedes der beitragenden Felder. • Es gibt eine nur-Rollen-Lese-ACL ohne Bedingungen und ohne Skript, und der Anwender hat diese Rolle. • Der Anwender hat schreibgeschützten Zugriff auf die beitragenden Felder, sodass nur ACLs ohne Bedingung oder Skript zulassen können.

Beispiele

Angegeben:

- Tabelle: Gehalt
- Spalten: Base, Bonus, total (in diesem Beispiel sind alle Ganzzahlen)
- Funktionsfeld: Die Gesamtspalte ist als Funktionsfeld mit Funktionsdefinition markiert `Glidefunktion:hinzufügen (Basis, Bonus)` .
- Beitragende Felder: Basis und Bonus, da sie in der Funktionsdefinition verwendet werden
- Rollen: Salary_admin, Bonus_admin

Beispiel 1: Alle Felder erlauben Zugriff

ACLs	Ergebnis
Gesamt, Basis, Bonus: Read und Report_View für die Rolle „Salary_admin“ ohne Bedingungen oder Skripts	Einem Anwender mit der Rolle „Salary_admin“ wird Lese- und Report_View-Zugriff auf total gewährt, da er über die erforderliche Rolle verfügt.

Beispiel 2: Beitragendes Feld verweigert Lesezugriff

ACLs	Ergebnis
• Gesamt, Basis: Read und Report_View für die Rolle „Salary_admin“ ohne Bedingungen oder Skripts • Bonus: Report_View für die Rolle „Salary_admin“ ohne Bedingungen oder Skripts • Bonus: Lesen Sie für die Rolle „Bonus_admin“, ohne Bedingungen oder Skripts	Einem Anwender mit der Rolle „Salary_admin“ wird der Lese- und Report_View-Zugriff auf „total“ verweigert, da der Bonus den Lesezugriff auf seine Rolle verweigert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel 3: ACL für Beitragende Felder hat Skript

ACLs	Ergebnis
• Gesamt, Basis: Read und Report_View für die Rolle „Salary_admin“ ohne Bedingungen oder Skripts • Bonus: Report_View für Rolle Bonus_admin, ohne Bedingungen oder Skripts • Bonus: Lesen Sie für die Rolle „Salary_admin“ mit einem Skript (beachten Sie, dass es keine Rolle spielt, was im Skript enthalten ist, nur dass es vorhanden ist)	Einem Anwender mit der Rolle „Salary_admin“ wird Lesezugriff auf total gewährt, da er über die erforderliche Rolle für alle Felder verfügt. Der Zugriff auf Report_View wird jedoch für denselben Anwender mit dem Skript „Salary_admin“ abgelehnt, da die Lese-ACL mit dem Skript den Zugriff standardmäßig für diesen Fall verweigert, obwohl sie über die erforderliche Rolle verfügen.

Sicherheits-Starthilfe – Plugin „ACL-Regeln“

Das Plugin „Sicherheit Starthilfe-Zugriffssteuerungsebene“ (ACL-Regeln) wird automatisch auf allen neuen Instanzen installiert. Verwenden Sie dieses Plugin, um schnell mehrere Systemtabellen zu sichern und den Produktionsstartprozess für Ihre Organisation zu beschleunigen.

Dieses Plugin ist nicht für vorhandene Instanzen vorgesehen, da es den Sicherheitszugriff auf Tabellen ändern kann, die bereits in einer Produktionsumgebung verwendet werden. Wenn ein Administrator dieses Plugin unbedingt auf einer vorhandenen Instanz installieren möchte, sollten Sie es zuerst gründlich in einer Testinstanz testen. Dies hilft, die Kompatibilität mit der aktuellen Implementierung der Organisation zu überprüfen.

Wenn ein Administrator an den neuen ACL-Regeln interessiert ist, die von diesem Plugin bereitgestellt werden, kann er eine oder mehrere in einer vorhandenen Instanz manuell erstellen, indem er die Liste der ACLs als Richtlinie verwendet.

Die folgenden ACLs sind in diesem Plugin enthalten. Wählen Sie das Symbol in einer Kopfzeile aus, um diese Spalte in aufsteigender oder absteigender Reihenfolge zu sortieren. Der Vorgangsschlüssel lautet wie folgt:

- R=gelesen
- W=schreiben
- D=Löschen
- C=erstellen

Name	Vorgang	Beschreibung
cmdb_ci	WCD	Asset- oder itil-Rolle, die zum Schreiben/Erstellen/Löschen von Konfigurationselementdatensätzen erforderlich ist
cmn_Department	WD	Rolle „user_admin“ zum Schreiben/Löschen von Abteilungsdatensätzen erforderlich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
cmn_location	WC	Rolle „user_admin“ zum Schreiben/Erstellen von Standortdatensätzen erforderlich
core_company	WD	Rolle „user_admin“ zum Schreiben/Löschen von Unternehmensdatensätzen erforderlich
kb_knowledge	Erstellen	Wissensrolle, die zum Erstellen von Wissensdatensätzen erforderlich ist
ldap_ou_config	RWCD	Rolle „user_admin“ zum Lesen/Schreiben/Erstellen/Löschen von LDAP-OU-Definitionsdatensätzen erforderlich
ldap_Server_config	RWCD	Rolle „user_admin“ zum Lesen/Schreiben/Erstellen/Löschen von LDAP-Server-Datensätzen erforderlich
Process_Guide	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Prozessleitfadendatensätzen erforderlich ist
Process_STEP	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Prozessschritt-Datensätzen erforderlich ist
sc_category	Erstellen	Rolle „Catalog_admin“ zum Erstellen von Servicekatalog-Kategoriedatensätzen erforderlich
sc_category	löschen	Rolle „Catalog_admin“ zum Löschen von Servicekatalog-Kategoriedatensätzen erforderlich
sc_category	Schreiben	Rolle „Catalog_admin“ zum Schreiben in Servicekatalog-Kategoriedatensätze erforderlich
Katalogelement	Schreiben	Catalog_admin-Rolle, die zum Schreiben in Katalogelementdatensätze erforderlich ist
Katalogelement	löschen	Rolle „Catalog_admin“ zum Löschen von Katalogelementdatensätzen erforderlich
Katalogelement	Erstellen	Rolle „Catalog_admin“ ist zum Erstellen von Katalogelementdatensätzen erforderlich
Sysevent_email_action	gelesen	Alle Anwender können E-Mail-Benachrichtigungsdatensätze lesen (zu Abonnementzwecken)
Sysevent_Register	RWCD	administratorrolle, die zum Lesen/Schreiben/Erstellen/Löschen von Ereignisregistrierungsdatensätzen erforderlich ist
Sysevent_script_action	RWCD	administratorrolle, die zum Lesen/Schreiben/Erstellen/Löschen von Skriptaktionsdatensätzen erforderlich ist
syslog	RWCD	administrator erforderlich, um Protokolleintragsdatensätze zu lesen/zu schreiben/zu erstellen/zu löschen
Sysrule	RWCD	administrator zum Lesen/Schreiben/Erstellen/Löschen von Regeldatensätzen (E-Mail-Benachrichtigungen, Aktionen für eingehende E-Mails, Genehmigungsregeln usw.) erforderlich
Sysrule	gelesen	Alle Anwender können E-Mail-Benachrichtigungsdatensätze für lesen (abonnementbasierte Benachrichtigungen)
sys_App_Application	WCD	administrator erforderlich, um Anwendungsdatensätze zu schreiben/zu erstellen/zu löschen
sys_App_category	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Anwendungskategorie-Datensätzen erforderlich ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_App_Module	WCD	administrator ist zum Schreiben/Erstellen/Löschen von Moduldatensätzen erforderlich
sys_audit	RWCD	administrator erforderlich, um Audit-Datensätze zu lesen/zu schreiben/zu erstellen/zu löschen
sys_dictionary	RWC	Rolle „Personalize_dictionary“, die zum Lesen/Schreiben/Erstellen von Wörterbuchdatensätzen erforderlich ist
sys_dictionary .*	gelesen	Die Rolle „Personalize_dictionary“ kann Wörterbuchfelder lesen
sys_documentation	löschen	Rolle „personalize_dictionary“ erforderlich, um Feldbezeichnungsdatensätze zu löschen
sys_documentation	Erstellen	Rolle „personalize_dictionary“ erforderlich, um Feldbezeichnungsdatensätze zu erstellen
sys_documentation	Schreiben	Rolle „personalize_dictionary“ erforderlich, um in Feldbezeichnungsdatensätzen zu schreiben
sys_Gauge	RWCD	administratorrolle, die zum Lesen/Schreiben/Erstellen/Löschen von Anzeigedatensätzen erforderlich ist
sys_Gauge_count	RWCD	administratorrolle, die zum Lesen/Schreiben/Erstellen/Löschen von Anzeigenanzahldatensätzen erforderlich ist
sys_Group_has_role	gelesen	itil-Rolle, die zum Anzeigen von Gruppenrollendatensätzen erforderlich ist
sys_HOME	WCD	Rolle „itil_admin“ zum Schreiben/Erstellen/Löschen von Datensätzen des Willkommensseitenabschnitts erforderlich
sys_Installation_exit	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Installationsbeendigungsdatensätzen erforderlich ist
sys_Job	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von SYS-Auftragsdatensätzen erforderlich ist
sys_NAV_Link	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Navigationslink-Datensätzen erforderlich ist
sys_perspective	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Menülistendatensätzen erforderlich ist
sys_Portal	RWCD	administratorrolle, die zum Lesen/Schreiben/Erstellen/Löschen von Portaldatensätzen erforderlich ist
sys_Portal_page	RWCD	administratorrolle, die zum Lesen/Schreiben/Erstellen/Löschen von Homepage-Datensätzen erforderlich ist
sys_Portal_preferences	RWCD	administratorrolle, die zum Lesen/Schreiben/Erstellen/Löschen von Portaleinstellungen-Datensätzen erforderlich ist
sys_processor	WC	administratorrolle, die zum Schreiben/Erstellen von Prozessordatensätzen erforderlich ist
sys_properties	WC	administratorrolle, die zum Schreiben/Erstellen von Systemeigenschaftsdatensätzen erforderlich ist
sys_properties_category	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Eigenschaftskategorie-Datensätzen erforderlich ist
sys_Report	löschen	Rollen, die Berichtsdatensätze löschen können (schränkt das Löschen über die Berichts-UI nicht ein)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_Report	Schreiben	Rollen, die in Berichtsdatensätze schreiben können (schränkt die Bearbeitung über die Berichts-UI nicht ein)
sys_Report	gelesen	Anwender können ihre eigenen Berichtsdatensätze, die ihrer Gruppen und GLOBALE lesen (hat keine Auswirkungen auf die Anzeige über die Berichts-UI)
sys_Report	gelesen	Rollen, die Berichtsdatensätze lesen können (schränkt die Anzeige über die Berichts-UI nicht ein)
sys_Reportroles	gelesen	administratorrolle, die zum Lesen von Berichtsrollen-Datensätzen erforderlich ist
sys_script	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Business-Regel-Datensätzen erforderlich ist
sys_script_ajax	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von AJAX-Skriptdatensätzen erforderlich ist
sys_script_Client	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Clientskriptdatensätzen erforderlich ist
sys_script_include	WCD	administratorrolle, die zum Schreiben/Erstellen/Löschen von Skripteinbindungsdatensätzen erforderlich ist
sys_Security_acl	Schreiben	administratorrolle, die zum Schreiben in Zugriffssteuerungsdatensätze erforderlich ist
sys_Security_acl_role	Erstellen	administratorrolle, die zum Erstellen von Zugriffsrollen-Datensätzen erforderlich ist
sys_Security_acl_role	löschen	administratorrolle, die zum Löschen von Zugriffsrollen-Datensätzen erforderlich ist
sys_Security_acl_role	Schreiben	administratorrolle, die zum Schreiben in Zugriffsrollen-Datensätze erforderlich ist
sys_Security_Operation	löschen	administratorrolle, die zum Löschen von Sicherheitsvorgangsdatensätzen erforderlich ist
sys_Security_Operation	Erstellen	administratorrolle, die zum Erstellen von Sicherheitsvorgangsdatensätzen erforderlich ist
sys_Security_Operation	Schreiben	administratorrolle, die zum Schreiben in Sicherheitsvorgangsdatensätze erforderlich ist
sys_Security_Operation	Query_Range	
sys_Security_Operation		
sys_Security_type	Schreiben	administratorrolle, die zum Schreiben in Sicherheitstypdatensätze erforderlich ist
sys_Security_type	Erstellen	administratorrolle, die zum Erstellen von Sicherheitstypdatensätzen erforderlich ist
sys_Security_type	löschen	administratorrolle, die zum Löschen von Sicherheitstypdatensätzen erforderlich ist
sys_Status	Erstellen	administratorrolle, die zum Erstellen von Systemstatusdatensätzen erforderlich ist
sys_Status	löschen	administratorrolle, die zum Löschen von Systemstatusdatensätzen erforderlich ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_Status	Schreiben	administratorrolle, die zum Schreiben in Systemstatusdatensätze erforderlich ist
sys_template	Schreiben	Template_Editor-Rolle erforderlich, um in Vorlagendatensätze zu schreiben
sys_template	Erstellen	Rolle „Emplate_Editor“ ist zum Erstellen von Vorlagendatensätzen erforderlich
sys_template	löschen	Rolle „Template_Editor“ zum Löschen von Vorlagendatensätzen erforderlich
sys_template	gelesen	Template_Editor-Rolle, die zum Lesen von Datensätzen von Vorlagenrollen erforderlich ist
sys_ui_action	Erstellen	administratorrolle, die zum Erstellen von UI-Aktionsdatensätzen erforderlich ist
sys_ui_action	löschen	administratorrolle, die zum Löschen von UI-Aktionsdatensätzen erforderlich ist
sys_ui_action	Schreiben	administratorrolle, die zum Schreiben in UI-Aktionsdatensätze erforderlich ist
sys_ui_action_View	Schreiben	administratorrolle, die zum Schreiben in Datensätze der UI-Ansichtsaktion erforderlich ist
sys_ui_action_View	Erstellen	administratorrolle, die zum Erstellen von Datensätzen der UI-Ansichtsaktion erforderlich ist
sys_ui_action_View	löschen	administratorrolle, die zum Löschen von Datensätzen der UI-Ansichtsaktion erforderlich ist
sys_ui_Policy	Erstellen	administratorrolle, die zum Erstellen von UI-Richtliniendatensätzen erforderlich ist
sys_ui_Policy	löschen	administratorrolle, die zum Löschen von UI-Richtliniendatensätzen erforderlich ist
sys_ui_Policy	Schreiben	administratorrolle, die zum Schreiben in UI-Richtliniendatensätze erforderlich ist
sys_ui_Policy_action	Erstellen	administratorrolle, die zum Erstellen von UI-Richtlinienaktionsdatensätzen erforderlich ist
sys_ui_Policy_action	löschen	administratorrolle, die zum Löschen von UI-Richtlinienaktionsdatensätzen erforderlich ist
sys_ui_Policy_action	Schreiben	administratorrolle, die zum Schreiben in UI-Richtlinienaktionsdatensätze erforderlich ist
sys_ui_script	Schreiben	administratorrolle, die zum Schreiben in UI-Skriptdatensätze erforderlich ist
sys_ui_script	löschen	administratorrolle, die zum Löschen von UI-Skriptdatensätzen erforderlich ist
sys_ui_script	Erstellen	administratorrolle, die zum Erstellen von UI-Skriptdatensätzen erforderlich ist
sys_user	Schreiben	Anwender ohne Rolle können keinen Anwenderdatensatz aktualisieren, sondern ihren eigenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Vorgang	Beschreibung
sys_user_grmember	löschen	Rolle „user_admin“ zum Löschen von Gruppenmitgliedsdatensätzen erforderlich
sys_user_grmember	Schreiben	Rolle „user_admin“ erforderlich, um in Gruppenmitgliedsdatensätze zu schreiben
sys_user_group	Erstellen	Nur itil und höher können Gruppendatensätze erstellen
sys_user_group	Schreiben	Nur itil und höher können in Gruppendatensätze schreiben
sys_user_has_role	gelesen	itil-Rolle, die zum Anzeigen von Anwenderrollendatensätzen erforderlich ist
sys_user_role	Erstellen	administratorrolle, die zum Erstellen von Rollendatensätzen erforderlich ist
sys_user_role	löschen	administratorrolle zum Löschen von Rollendatensätzen erforderlich
sys_user_role	Schreiben	administratorrolle, die zum Schreiben in Rollendatensätze erforderlich ist
sys_user_role_contains	gelesen	itil-Rolle, die erforderlich ist, um enthaltene Rollendatensätze anzuzeigen
sys_user_role_contains	Schreiben	administratorrolle, die zum Schreiben in enthaltene Rollendatensätze erforderlich ist
sys_user_Token	RWCD	administratorrolle, die zum Lesen/Schreiben/Erstellen/Löschen von Anwendertoken-Datensätzen erforderlich ist

Hinweis: Weitere Informationen zu diesem Plugin finden Sie unter Plugin „Security Jump Start“ aktivieren (ACL-Regeln) [aktualisiert in Security Center 1,3] In Instanzsicherheitshärtungseinstellungen.

Konfigurieren Sie eine ACL-Regel

Konfigurieren Sie eine anwenderdefinierte ACL-Regel (Access Control List), um den Zugriff auf neue Objekte zu sichern oder das standardmäßige Sicherheitsverhalten zu ändern.

Vorbereitungen

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

Um ACL-Regeln zu erstellen, müssen Sie Berechtigungen auf die Rolle „Security_admin“ erhöhen.

Für Tabellen, die sich in einem anderen Umfang als der ACL-Regeldatensatz befinden, sind die Arten von Regeln beschränkt. Legen Sie für Umfangsmaster-Tabellen fest, um den Umfang abzuleiten und bereichsbezogene ACLs auszuführen *glide.enforce_security_scope.<scope_name>*Eigenschaft bis **Wahr** . Dadurch wird sichergestellt, dass ACLs im globalen Bereich nicht übereinstimmen, wenn bereichsspezifische ACLs in der relevanten Tabelle erstellt werden. Beispiele sind das Sichern von Daten in gemeinsam genutzten Anwendungstabellen im globalen Bereich, z. B. Tabellen „sys_attachment“ oder „sys_question_answer“.

Prozedur

1. Rollen mit erhöhten Berechtigungen Zur Rolle Security_admin.
2. Navigieren zu **Systemsicherheit** > **Zugriffssteuerung (ACL)**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Neu**.

   Tipp: Beim Erstellen einer neuen ACL ist es hilfreich, die zu überprüfen Verweigern – außer ACL.

4. Füllen Sie das Formular aus.

Zugriffssteuerungsfelder

Feld	Beschreibung
Typ	Wählen Sie aus, welche Art von Objekt diese ACL-Regel sichert. Der Typ des Objekts bestimmt, wie das Objekt benannt wird und welche Vorgänge verfügbar sind. Dieses Feld wird schreibgeschützt, nachdem die ACL-Regel erstellt wurde. Wenn Sie den Typ ändern möchten, müssen Sie die ACL löschen und eine neue mit dem richtigen Typ erstellen.
Vorgang	Wählen Sie den Vorgang aus, den diese ACL-Regel sichert. Jeder Objekttyp verfügt über eine eigene Liste von Vorgängen. Eine ACL-Regel kann nur einen Vorgang sichern. Um mehrere Vorgänge zu sichern, erstellen Sie für jeden eine separate ACL-Regel. Wenn Sie eine Regel für einen Report_View-Vorgang erstellen, finden Sie weitere Informationen unter Berichtsansichts-Zugriffskontrolle .
Entscheidungstyp	Wählen Sie den Entscheidungstyp der ACL aus. **Zulassen, Wenn** Ermöglicht den Zugriff nach erfolgreicher Auswertung. **Ablehnen, Es Sei Denn** Verweigert den Zugriff, es sei denn, die Auswertung ist erfolgreich.siehe Verweigern – außer ACL Weitere Informationen finden Sie unter .
Admin-Aufhebungen	Aktivieren Sie dieses Kontrollkästchen, damit Anwender mit der Administratorrolle die Berechtigungsprüfung für diese ACL-Regel automatisch bestehen. Administratoranwender bestehen, unabhängig davon, welche Skript- oder Rollenbeschränkungen gelten. Jedoch ist **Niemand** Rolle, die nur ServiceNow Mitarbeiter können zuweisen, hat Vorrang vor der Administratorüberschreibungsoption. Wenn eine ACL zugewiesen ist **Niemand** Rolle, Administratoranwender können nicht auf die Ressource zugreifen, auch wenn **Administrator-Überschreibungen** Ist ausgewählt. Siehe Basissystemrollen . Deaktivieren Sie dieses Kontrollkästchen, wenn Administratoren die in dieser ACL-Regel definierten Berechtigungen erfüllen müssen, um Zugriff auf das gesicherte Objekt zu erhalten. Da Administratoren Rollenprüfungen immer bestehen (siehe Beschreibung von **Erfordert Rolle** Feld), verwenden Sie den Bedingungsgenerator oder **Skript** Feld zum Erstellen einer Berechtigungsprüfung, die Administratoren bestehen müssen.
Schutzrichtlinie	Wählen Sie diese Option aus, um die Schutzrichtlinie für die ACL festzulegen
Name	Geben Sie den Namen des zu sichernden Objekts ein, entweder den Datensatznamen oder die Tabellen- und Feldnamen. Je spezifischer der Name, desto spezifischer ist die ACL-Regel. Sie können das Platzhalterzeichen Sternchen (*) anstelle eines Datensatzes, einer Tabelle oder eines Feldnamens verwenden, um alle Objekte auszuwählen, die einem Datensatztyp entsprechen, alle Tabellen oder alle Felder. Sie können ein Platzhalterzeichen nicht mit einer Textsuche kombinieren. Beispiel: INC* ist kein gültiger ACL-Regelname, aber Incident.* und *.number sind gültige ACL-Regelnamen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Klicken Sie auf das blaue Dreieck, um den Datensatznamen oder die Tabellen- und Feldnamen des gesicherten Objekts manuell einzugeben. Verwenden Sie diese Option, um ein Objekt zu sichern, das nicht in der Dropdown-Liste angezeigt wird.
Beschreibung	Geben Sie eine Beschreibung des Objekts oder der Berechtigungen ein, die diese ACL-Regel sichert.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese ACL-Regel zu erzwingen.
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um anzuzeigen **Erweiterte Bedingung** Felder. Siehe Schritt 6.

5. **Wahlweise:** Um den Umfang der ACL einzugrenzen, füllen Sie aus **Bedingungen** Felder nach Bedarf.

Erfordert Rolle	Verwenden Sie diese Liste, um die Rollen anzugeben, die ein Anwender haben muss, um auf das Objekt zuzugreifen. Wenn Sie mehrere Rollen auflisten, kann ein Anwender mit einer der aufgeführten Rollen auf das Objekt zugreifen. Die *Erfordert Rolle* Liste wird als zugehörige Liste angezeigt. **Hinweis:** Anwender mit der Administratorrolle bestehen diese Berechtigungsprüfung immer, da die Administratorrolle Anwendern automatisch alle anderen Rollen gewährt.
Datenbedingung	Verwenden Sie dies Bedingungsgenerator Um die Felder und Werte auszuwählen, die für Anwender auf das Objekt „wahr“ sein müssen. **Hinweis:** Im Bedingungsfeld wird zwischen Groß- und Kleinschreibung unterschieden

6. **Wahlweise:** Wenn **Erweitert** Kontrollkästchen ist aktiviert, füllen Sie aus **Erweiterte Bedingungen** Felder nach Bedarf

Durch Referenzen gesteuert	Erzwingt die ACL für zugehörige Datensätze. Unter Zugehöriger Datensatzzugriff finden Sie weitere Details.
Skript	Geben Sie ein anwenderdefiniertes Skript ein, das die für den Zugriff auf das Objekt erforderlichen Berechtigungen beschreibt. Das Skript kann die Werte von verwenden *Aktuell* Und *Zurück* Globale Variablen in Business-Regeln Sowie Systemeigenschaften. Das Skript muss eine wahr- oder falsch-Antwort auf eine von zwei Arten generieren: ○ Geben Sie einen zurück *Antwort* Variable auf den Wert „wahr“ oder „falsch“ festgelegt ○ Wird als „wahr“ oder „falsch“ ausgewertet In beiden Fällen erhalten Anwender nur Zugriff auf das Objekt, wenn das Skript als „wahr“ ausgewertet wird und der Anwender alle Bedingungen erfüllt, die die ACL-Regel hat. Sowohl die Bedingungen als auch das Skript müssen als „wahr“ ausgewertet werden, damit ein Anwender auf das Objekt zugreifen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Skript in vorhanden ist **Skript** Feld. Dieses Skript wird auch ausgeführt, wenn das Feld nicht im Formular angezeigt wird.

Hinweis: Wenn sich das ausgewertete Element in einer zugehörigen Liste befindet, **Aktuell** Verweist auf das Element, in dem sich die zugehörige Liste befindet, nicht auf das aktuelle Element, für das die ACL bestimmt ist. Wenn sich das Element, für das Sie die ACL auswerten, jedoch nicht in einer zugehörigen Liste befindet, **Aktuell** Verweist auf das tatsächliche Element.

---

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

Verweigern – außer ACL

Erfahren Sie mehr über Deny-außer-ACLs.

Deny-es sei denn, ACLs werden mit dem Ansatz „Deny-es“ ausgewertet. Die ACL definiert die Anwender, die NICHT abgelehnt werden. Auf andere Weise wird dem Anwender der Zugriff verweigert **Es sei denn** Die Rollen-, Bedingungen- und Skriptanforderungen sind erfüllt.

Wichtig: Verweigern – es sei denn, ACLs haben Priorität gegenüber Allow-if-ACLs in der ACL-Auswertung, da sie zuerst ausgewertet werden.

Ein Deny-es sei denn, die ACL erstellt Zwei Ergebnisse

Auswertungsergebnis	Ergebnis
Bestanden	Die definierten Rollen, Datenbedingungen, Sicherheitsattribute und Skriptanforderungen sind erfüllt. Die ACL fährt mit der weiteren Auswertung fort **Wichtig:** Zulassen, wenn ACLs weiterhin Zugriff gewähren müssen, damit der Betreff auf die Ressource zugreifen kann.
Fehlgeschlagen	Verweigern, es sei denn, die ACL ist als fehlgeschlagen markiert, und der Zugriff wird verweigert.

Im Folgenden finden Sie ein erklärtes Beispiel für eine Deny-außer-ACL:

- ACL hat Rollen `sn_HR_Core.Manager` Und itil
- Bedingung hat aktiv = Wahr
- Skript hat Antwort = `gs.isLoggedIn();`

Dem Anwender wird der Zugriff verweigert, es sei denn, alle Drei Die Anforderungen für diese ACL sind erfüllt. Damit diese Ablehnung – es sei denn, die ACL wird übergeben – ein Anwender Benötigt entweder `sn_HR_Core.Manager` Oder itil Rollen, die auf einen Datensatz zugreifen, der das aktive Feld = hat Wahr , Und angemeldet sein. Die Deny-es sei denn, die ACL schlägt fehl, wenn eine der drei Anforderungen nicht erfüllt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL zulassen

Erfahren Sie mehr über Allow ACLs (Zugriffssteuerungslisten).

Allow-ACLs sind so konzipiert, dass standardmäßig Zugriff auf Ressourcen gewährt wird, es sei denn, eine bestimmte Regel verweigert dies. Dies ist das Gegenteil von einem „Deny-sofern“-Modell.

Abfrage-ACLs

Mit Abfrage-ACLs können Sie eine granulare Zugriffssteuerung definieren, indem explizit definiert wird, wer die Daten abfragen kann.

Was ist eine Abfrage-ACL

Eine Abfrage-ACLs Der Vorgang ist auf einen der beiden festgelegt `Query_Range` Oder `Query_match` . Abfrage-ACLs ermöglichen eine spezifischere Steuerung von Anwenderabfragen und beschränken oder aktivieren den Zugriff Basierend auf ihrem Setup . Abfrage-ACLs sind leistungsstarke Tools gegen Angriffe mit blinden Abfragen, Wenn ein Angreifer die Daten blind abfragt, um Informationen aus Ergebnissen zu extrahieren, auch wenn er die Werte nicht sehen kann.

Wann eine Abfrage-ACL verwendet werden soll

Überall, wo eine Spalte sensible Werte enthält und zulässt Teilweise/bedingt Zugriff auf Daten eine Abfrage-ACL sollte basierend auf der Vertraulichkeit der Daten berücksichtigt und bei Bedarf implementiert werden. Überall dort, wo ein partieller/bedingter Zugriff auf Zeilen und ihre Spalten in Tabellen besteht, insbesondere wenn dieser Zugriff nicht durch Datenfilter erzwungen wird, sollten Abfrage-ACLs je nach Bedarf basierend auf der Vertraulichkeit der Daten implementiert werden.

Hinweis: Ziehen Sie Abfrage-ACLs in Betracht, wenn einige Anwender Zugriff auf einige Zeilen oder Spalten haben und nicht andere .

Example: Abfragesteuerung für Gehaltsabrechnung

Ich kann eine Zeile in der Gehaltsabrechnungstabelle mit meinem Gehalt sehen, aber es gibt keinen Grund für mich, Bereichsabfragen ausgeben zu können, um Anwender mit einem Gehalt innerhalb von 2 Grenzen abzufragen. A `Query_Range` ACL für Gehalt würde verhindern, dass ich diese Abfrage ausstelle.

Example: HR-Abfragesteuerung

Ich kann alle HR_profiles anzeigen, aber nur SSN für mich selbst. Ich habe keine geschäftliche SSN-Abfrage, und Abfrage-ACLs sollten mich daran hindern, Abfragen für SSN anderer HR-Profile auszuführen, um zu versuchen, SSN-Zuordnungen zu extrahieren.

Abfrage-ACL-Verhalten

Abfrage-ACLs verwenden `Query_match` Und `Query_Range` Vorgänge für sicheres und granulares Tabellenabfrageverhalten. Ihr Verhalten wird unten beschrieben:

`Query_match`

`Query_match` Besteht aus: EQUALS, NOT_EQUALS, IN, NOT_IN, SAMEAS, NSAMEAS, ANYTHING, ISEMPTYSTRING, ISEMPTY, ISNOTEMPTY, ISNULL, ISNOTNULL. `Query_match` Besteht aus den „Safe Operators“, in dem Sinne, dass sie so erstellt wurden, dass bestimmte Datensätze abgerufen werden können und nicht genutzt werden können, um andere zurückzugeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswertungsergebnis	Ergebnis
Bestanden	Der Anwender kann Übereinstimmungsabfragen übermitteln
Fehlgeschlagen	Anwender kann keine Übereinstimmungsabfragen übermitteln: • IST GLEICH • NICHT_GLEICH • IN • NOT_IN • SAMEAS • NSAMEAS • ALLES • ISEMPTYSTRING • ISEMPTY • ISNOTEMPTY • IST NULL • ISNOTNULL

Query_Range

Query_Range Besteht aus allen anderen (STARTET_MIT, ENTHÄLT, >=, <= USW.), die gefährlicher sind, da Anwender durch Anpassen der Grenzwerte nach weiteren Datensätzen abfragen können.

Auswertungsergebnis	Ergebnis
Bestanden	Der Anwender kann Bereichsabfragen übermitteln, und die Sortierung ist uneingeschränkt
Fehlgeschlagen	Der Anwender kann keine Bereichsabfragen mit (STARTS_WITH, CONTAINS, >=, <= usw.) übermitteln Die Sortierung nach Spalte ist eingeschränkt

Wichtig:

Abfrage-ACLs (sowohl query_match als auch query_Range) sind standardmäßig eine Star.Star-ACL, die den Lesezugriff delegiert. Dies bedeutet, wenn ACLs für Abfragen erzwungen werden. Wenn keine Abfrage-ACL erstellt wurde, wird der Lesezugriff auf die Spalte ausgewertet. Wenn Abfrage-ACLs definiert sind, überschreiben sie das Standardverhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichern Sie Datensätze in einer eingebetteten Liste

Um die Sicherheit auf die Datensätze in eingebetteten Listen anzuwenden, beschränken Sie die Bearbeitung und das Löschen von Datensätzen in eingebetteten Listen auf bestimmte Rollen.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffssteuerung (ACL)**an.
2. Öffnen Sie **Schreiben** Oder **Löschen** Datensatz für die entsprechende Tabelle.
3. Fügen Sie im Abschnitt erfordert Rolle des Formulars die Rollen hinzu, die über Schreib- oder Löschberechtigungen für diese Tabelle verfügen.
4. Speichern Sie die Änderungen.
   Wenn Datensätze aus der zugehörigen Tabelle in einer eingebetteten Liste angezeigt werden, sind die Optionen zum Bearbeiten und Löschen nur für Anwender mit den angegebenen Rollen verfügbar.

Zugehöriger Datensatzzugriff

Der Zugriff auf zugehörige Datensätze ermöglicht eine konsistente Steuerung darüber, auf welche Datensätze Anwender zwischen zugehörigen Tabellen zugreifen können.

Zugehöriger Datensatzzugriff – Details

Mit dem Zugriff auf zugehörige Datensätze können Sie den Zugriff auf den zugehörigen Datensatz konfigurieren und bestimmen, ob die ACL der zugehörigen übergeordneten Tabelle für Daten erzwungen werden soll, die Zugriff über die ACL haben. Betrachten Sie den folgenden Anwendungsfall: Ein Anwender hat über ACL Zugriff auf einen Datensatz, dann ermöglicht der Zugriff auf zugehörige Datensätze den Zugriff der Anwender auf alle anderen zugehörigen Datensätze, entweder über Referenz- oder bidirektionale Beziehung.

Kontextbezogener Sicherheitsmanager

Der kontextbezogene Sicherheitsmanager schützt Ihre Daten, indem er die Autorisierung für Lese-, Schreib-, Erstellungs- und Löschvorgänge steuert.

Hauptvorteile

Der kontextbezogene Sicherheitsmanager ist sich der Systemtabellenhierarchie bewusst, sodass Sie bestimmte Sicherheitsregeln für ein Feld erstellen können, basierend darauf, wo es in der Hierarchie angezeigt wird. Vorteile des kontextbezogenen Sicherheitsmanagers:

- **Kontextbezogene Sicherheit** : Sichern Sie einen Datensatz basierend auf dem Inhalt des Datensatzes.
- **Hierarchische Sicherheit** : Wendet Sicherheitsregeln auf eine beliebige Ebene in der Objekthierarchie an.

Felder und Tabellen werden gesichert

Mit dem Legacy Simple Security Manager können Sie Felder und Tabellen sichern, indem Sie dem entsprechenden Wörterbucheintrag Rollen hinzufügen. Mit dem kontextbezogenen Sicherheitsmanager werden diese Wörterbuchrollen nicht mehr getestet. Stattdessen sucht das System nach ACL-Regeln für Felder und Tabellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Nach der Installation des kontextbezogenen Sicherheitsmanagers müssen Sie Felder und Tabellen über ACL-Regeln sichern. Auch wenn Sie Konfigurieren des Formularlayouts Das Wörterbuchformular und fügen Sie einem Wörterbucheintrag Rollen hinzu. Die Rechte werden nicht geändert.

Kontextbezogene Sicherheit und Rollen

Sie können Anwendern oder Gruppen Rollen gewähren. Nach der Installation des kontextbezogenen Sicherheitsmanagers jedoch wird der **Rollen** Das Feld im Anwenderdatensatz ist nicht mehr aktiviert und wird nicht mehr in Ihren Anwender- und Gruppenformularen angezeigt. Stattdessen müssen Sie der zugehörigen Liste „Rollen“ anstelle des Anwender- oder Gruppendatensatzes Rollen hinzufügen.

Anwendungen und Module enthalten Listen der Rollen, die zum Anzeigen erforderlich sind. Zum Anzeigen der Anwendung „Systemdefinition“ ist beispielsweise die Administratorrolle erforderlich. Sicherheitsrechte für Anwendungen und Module werden weiterhin mithilfe von Rollen-Arrays definiert.

Sowohl Katalogelemente als auch Katalogvariablen enthalten Listen der Rollen, die zum Anzeigen erforderlich sind. Sicherheitsrechte für Katalogelemente und Katalogvariablen werden weiterhin über diese Rollen-Arrays definiert.

Unter dem kontextbezogenen Sicherheitsmanager erbt eine Gruppe weiterhin automatisch jede Rolle, die der Gruppe gewährt wird, wenn die Kennzeichnung „Erben“ für die Rolle auf festgelegt ist *Wahr* .

Kontextbezogener Sicherheitsmanager wird aktiviert

Der kontextbezogene Sicherheitsmanager ist im Basissystem aktiv. Wenn in der Tabelle „Anwenderrollen“ viele doppelte Einträge vorhanden sind, müssen Sie möglicherweise ein Upgrade auf kontextbezogene Sicherheit: Rollenverwaltung V2 durchführen, um doppelte Rollen zu beseitigen. Zu den Plugins gehören:

Kontextbezogene Sicherheit: Rollenverwaltung [com.Glide.role_Management]

Stellt kontextbezogene Sicherheitsfunktionen bereit. Dieses Plugin wird automatisch installiert.

Kontextbezogene Sicherheit: Rollenverwaltung V2 [com.glide.role_management.inh_count]

Verhindert doppelte Einträge, die durch geerbte Rollen in der Tabelle „Anwenderrollen“ [sys_user_has_role] verursacht werden. Dieses Plugin wird automatisch auf neuen Instanzen installiert und kann für Upgrades aktiviert werden. Das Plugin „kontextbezogene Sicherheit: Rollenmanagement Enhancements“ ist eine vorherige Version dieses Plugins. Das Plugin „Rollenmanagement-Erweiterungen“ enthält das Skript RoleManagementVerify() nicht. Dieses Skript gibt eine Liste der Änderungen zurück, die ein Upgrade durchführt, sodass Sie die vom Plugin vorgenommenen Änderungen überwachen können.

Hinweis: Nach der Aktivierung von Rollenverwaltung V2 müssen Sie die Systemeigenschaft glide.role_management.v2.audit_roles festlegen, damit die Tabelle „Audit-Rollen“ Audit-Datensätze im Zusammenhang mit Anwenderrollen erstellen kann. Weitere Informationen zum Festlegen dieser Eigenschaft und zur Tabelle „Audit-Rollen“ finden Sie unter:

- Aktivieren Sie das Rollenaudit mit kontextbezogener Sicherheit: Rollenverwaltung V2.
- Härtungseinstellungen In Instanzsicherheitshärtungseinstellungen.
- Audit-Anwenderrollen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verhindern Sie doppelte Einträge mit kontextbezogener Sicherheit: Rollenverwaltung V2

Von anderen Rollen geerbte Rollen werden als einzelne Einträge in der Tabelle „Anwenderrollen“ [sys_user_has_role] hinzugefügt, wodurch eine Rolle möglicherweise doppelte Einträge enthält. Kontextbezogene Sicherheit: Rollenverwaltung V2 entfernt diese doppelten Einträge und verhindert zukünftige Duplikate.

Beseitigen Sie doppelte Einträge durch die Anzahl der Vererbungen

Kontextbezogene Sicherheit: Rollenverwaltung V2 verwendet die Spalte „Anzahl der Vererbungen“ (inh_count), um nachzuverfolgen, wie oft eine Rolle von einer anderen Rolle oder Gruppe geerbt wird. In der Tabelle „Anwenderrollen“ [sys_user_has_role] kann ein Anwender eine bestimmte Rolle nur einmal erben, wodurch doppelte Einträge vermieden werden. Die Spalte „Anzahl der Vererbungen“ (inh_count) ist schreibgeschützt und berechnet, wie oft der Anwender eine Rolle erbt.

Aktivierungsänderungen

Kontextbezogene Sicherheit: Rollenverwaltung V2 wird automatisch auf neuen Instanzen installiert und kann für Upgrades aktiviert werden. Wenn diese Option aktiviert ist, ersetzt Kontextsicherheit: Rollenverwaltung V2 sowohl kontextbezogene Sicherheit als auch kontextbezogene Sicherheit: Rollenverwaltung Erweiterungen.

Wenn kontextbezogene Sicherheit: Rollenverwaltung V2 aktiviert ist, sind die folgenden Spalten veraltet, verbleiben jedoch aus Gründen der Abwärtskompatibilität in der Tabelle „Anwenderrollen“:

- Granted_by (wird nur von Rollendelegierung verwendet)
- Include_in_role
- Include_in_role_instance

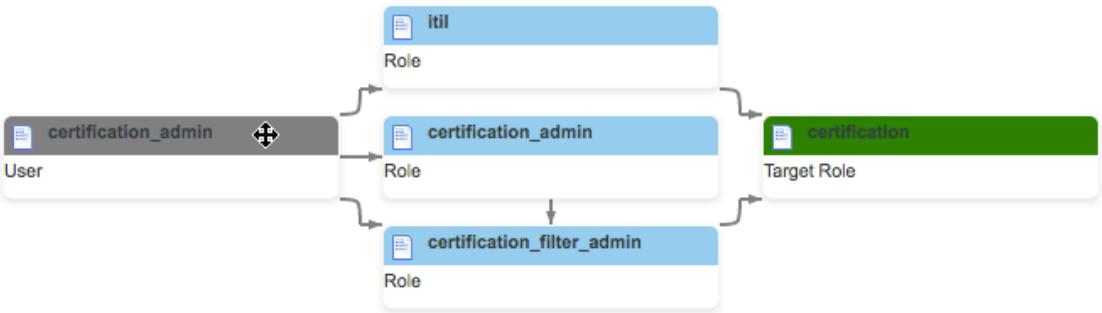
⚠ **Warnung:** Wenn diese Spalten in anwenderdefinierten Skripts in Ihrer Instanz verwendet werden, führen Sie kein Upgrade auf Rollenverwaltung V2 durch.

Visualisieren Sie die Rollenvererbung über die Rollenvererbungszuordnung

Die Rollenvererbungszuordnung zeigt eine visuelle Darstellung der geerbten Rollen an. Sie können diese Zuordnung verwenden, um die Rollen zu verstehen, die in der Spalte „Anzahl der Vererbungen“ (inh_count) dargestellt werden. Um die Rollenvererbungszuordnung anzuzeigen, konfigurieren Sie die Tabelle „Anwenderrollen“ [sys_user_has_role], um die Spalte „Rollenvererbungszuordnung“ anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenvererbungskarte



Hinweis: Die gleichzeitige Aktualisierung der Gruppen- oder Rollenzuweisung kann zu einer falschen Anzahl von Vererbungen führen. Sie müssen aktivieren glide.security.inh_count_patcher.enabled Eigenschaft zum Abrufen der genauen Anzahl der Vererbungen.

Upgrade auf kontextbezogene Sicherheit: Rollenverwaltung V2

Kontextbezogene Sicherheit: Rollenverwaltung V2 wird automatisch auf neuen Instanzen installiert. Sie können ein Upgrade von kontextbezogener Sicherheit: Rollenverwaltung auf kontextbezogene Sicherheit: Rollenverwaltung V2 durchführen, um doppelte Rollen in der Tabelle „Anwenderrollen“ zu beseitigen und zukünftige Duplikate zu verhindern.

Vorbereitungen

Erforderliche Rolle: admin, Security_admin

Sie müssen über die Administratorrolle und verfügen Auf eine privilegierte Rolle hochstufen Zum Abrufen der effektiven Rolle „Security_admin“.

Hinweis: Vor dem Upgrade auf kontextbezogene Sicherheit: Rolle: Management V2 müssen Sie die Tabelle „Audit-Rollen“ aktivieren, um Audit-Datensätze im Zusammenhang mit Anwenderrollen zu erstellen. Weitere Informationen zum Festlegen der erforderlichen Systemeigenschaft finden Sie unter Aktivieren Sie das Rollenaudit mit kontextbezogener Sicherheit: Rollenverwaltung V2.

Warum und wann dieser Vorgang ausgeführt wird

In diesem Verfahren wird beschrieben, wie Sie Ihre Rolle „kontextbezogene Sicherheit“ aktualisieren und die zugehörigen Plugins aktivieren, die in der folgenden Tabelle beschrieben werden.

Plugins für kontextbezogene Sicherheit: Rollenverwaltung V2

Plugin	Beschreibung
Kontextbezogene Sicherheit: Rollenverwaltung V2 [com.glide.role_management.inh_count]	Verhindert doppelte Einträge in der Tabelle „Anwenderrollen“ [sys_user_has_role]. Die Rolle Security_admin oder ein Benutzer mit erhöhten Berechtigungen ist erforderlich, um das Plugin oder den Kontakt zu aktivieren Kundenservice und Support.
Kontextbezogene Sicherheit: Rollenverwaltung V2 REST API	Aktiviert API-Funktionalität für die Rollenverwaltung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugins für kontextbezogene Sicherheit: Rollenverwaltung V2 (Fortsetzung)

Plugin	Beschreibung
[com.glide.role_management.inh_count.rest_api]	

Testen Sie vor dem Upgrade von kontextbezogene Sicherheit: Rollenverwaltung auf kontextbezogene Sicherheit: Rollenverwaltung V2 die Ergebnisse eines Upgrades, indem Sie das Skript ausführen. Das Skript gibt eine Liste der Änderungen zurück, die ein Upgrade durchführt. Wenn die Änderungen akzeptabel sind, installieren Sie das Plugin Contexttual Security: Role Management V2. Wenn die Änderungen nicht akzeptabel sind, installieren Sie das Plugin Contexttual Security: Role Management V2 nicht. Alternativ können Sie das Upgrade durchführen und dann alle erforderlichen Änderungen manuell vornehmen.

Prozedur

1. Testen Sie die Auswirkungen eines Upgrades vor dem Upgrade, indem Sie das folgende Skript ausführen.

   a. Navigieren zu **Systemdefinition** > **Skripts – Hintergrund**an.

   b. Führen Sie das folgende Skript im globalen Bereich aus.

   ```
   new RoleManagementVerify().verifyInheritedRoles();
   ```

   Bei großen Tabellen „sys_user_has_role“ kann die Ausführung mehrere Stunden dauern. Bearbeiten oder fügen Sie während dieser Zeit keine Anwenderrollen hinzu.
   Beispielergebnis basierend auf Testdaten:

   ```
   *** Script: 2016-12-01 19:58:54 Starting checking of inherited roles for all users...
   *** Script: User: itam, inherited roles to be ADDED: financial_mgmt_user
   *** Script: User: bernard.laboy, inherited roles to be DELETED:
    api_analytics_read,pa_viewer,rest_api_explorer,a123
   *** Script: User: bernard.laboy, inherited roles to be ADDED: dependency_views
   *** Script: Number of inherited-role records in sys_user_has role, current: 260, after
    re-calculation: 258
   *** Script: Number of users with discrepancies for inherited roles: 2
   *** Script: 2016-12-01 19:58:55 Finished checking of inherited roles for all users!
   ```

   c. Bewerten Sie die Skriptergebnisse, um festzustellen, ob die vorgeschlagenen Änderungen akzeptabel sind.

2. Aktivieren Sie das Plugin „kontextbezogene Sicherheit: Rollenverwaltung V2“.

   Wichtig: Die Rolle Security_admin oder ein Benutzer mit erhöhten Berechtigungen ist erforderlich, um das Plugin oder den Kontakt zu aktivieren Kundenservice und Support.

   a. Navigieren zu **Systemdefinition** > **Plugins**an.

   b. Suchen Sie nach dem Namen des Plugins, und klicken Sie darauf.

   c. Überprüfen Sie im System-Plugin-Formular die Plugin-Details, und klicken Sie dann auf den zugehörigen Link **Aktivieren/Aktualisieren**.

   d. Klicken Sie auf **Aktivieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Nach der Aktivierung von Rollenmanagement V2 werden die im Skriptergebnis dargestellten Änderungen umgesetzt. Die Spalte „Anzahl der Vererbungen“ (inh_count) in der Tabelle „Anwenderrollen“ ist schreibgeschützt und gibt automatisch an, wie oft der Anwender eine Rolle erbt.

Aktivieren Sie das Rollenaudit mit kontextbezogener Sicherheit: Rollenverwaltung V2

Legen Sie eine Systemeigenschaft fest, damit die Tabelle „Audit-Rollen“ Audit-Datensätze im Zusammenhang mit Anwenderrollen erstellen kann.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn diese Option aktiviert ist, werden in der Tabelle „Audit-Rollen“ [sys_Audit_role] Änderungen an Anwenderdatensätzen verwaltet. Weitere Informationen zu Rollenaudits finden Sie unter Audit-Anwenderrollen . Wenn das Plugin „kontextbezogene Sicherheit: Rollenverwaltung V2“ [com.glide.role_management.inh_count] installiert ist, müssen Sie eine Systemeigenschaft auf festlegen **Wahr** Zum Aktivieren des Rollenaudits.

Prozedur

1. Navigieren Sie zur Tabelle „Systemeigenschaften“ [sys_properties].
2. Fügen Sie hinzu `glide.role_management.v2.audit_roles` Systemeigenschaft und legen Sie sie auf fest **Wahr** .

   Wenn das Plugin „kontextbezogene Sicherheit: Rollenverwaltung V2“ [com.glide.role_management.inh_count] installiert ist, wird diese Eigenschaft auf festgelegt **Wahr** Aktiviert die Tabelle „Audit-Rollen“ [sys_Audit_role], um Datensätze zu erstellen, wenn sich Anwenderrollen ändern.

Überprüfen Sie die Formularübermittlung erneut

Wenn das System feststellt, dass ein bestimmtes Feld (z. B. „Task.number“) nicht vom aktuellen Anwender geschrieben werden soll, rendert das System dieses Feld in einem schreibgeschützten Modus, weshalb das Nummernfeld bei den meisten Incidents nicht schreibgeschützt ist.

Wenn Sie das System so festlegen, dass die Werte eingehender Felder auf Schreibfähigkeit überprüft werden, wendet das System dieselben Sicherheitsregeln auf den eingehenden Teil einer Transaktion an. Wenn Sie beispielsweise einen Incident übermitteln, überprüft das System doppelt, ob das Nummernfeld geschrieben werden kann, bevor Änderungen veröffentlicht werden.

Wenn Sie dem System anweisen, eingehende Transaktionen nicht zu überprüfen, ermöglicht das System Ihnen, in ein nominell schreibgeschütztes Feld zu schreiben, wenn dies die Transaktion ist, die der Client zurücksendet. In vielen Bereitstellungen ist dies tatsächlich ein wünschenswertes Verhalten, wenn Sie beispielsweise Client-Skripts verwenden, um nominell schreibgeschützte Felder als Antwort auf die Anwenderauswahl in anderen schreibbaren Feldern festzulegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Standort	Standard
Sicherheit eingehender Transaktionen bei der Formularübermittlung nochmals überprüfen (Rechte werden immer bei der Formularerstellung überprüft)	**Systemeigenschaften** > **Sicherheit**	Deaktiviert (keine Doppelprüfung)

Standardmäßige Deny-Eigenschaft

Die standardmäßige Deny-Eigenschaft (`glide.sm.default_mode`) Steuert das Standardverhalten des Sicherheitsmanagers, wenn die einzigen übereinstimmenden ACL-Regeln die ACL-Regeln der Platzhaltertabelle sind.

Eine Reihe von ACL-Regeln für Platzhaltertabellen für die häufigsten datensatzbasierten Vorgänge ist verfügbar: Lesen, Schreiben, Erstellen und Löschen. Eine bedeutende Anzahl von ACLs für rollenbasierten Zugriff auf Systemtabellen ist ebenfalls verfügbar. Beispielsweise gibt es ACLs, die sys_script-Zugriff auf die Rolle „Business_rule_admin“ gewähren, da diese Rolle dokumentiert ist, dass sie Business-Regeln verwalten kann.

Verwenden Sie `glide.sm.default_mode` Eigenschaft, um diese Vorgänge für alle Tabellen abzulehnen oder zuzulassen:

- **Zugriff Verweigern** : Die ACL-Regeln für Platzhaltertabellen schränken die Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen ein, es sei denn, der Anwender hat die Administratorrolle oder erfüllt die Anforderungen einer anderen Tabellen-ACL-Regel. Andere Vorgänge, z. B. Report_on und Personalize_choices, sind von dieser Einstellung nicht betroffen.
- **Zugriff Zulassen** : Die ACL-Regeln für Platzhaltertabellen ermöglichen Lese-, Schreib-, Erstellungs- und Löschvorgänge für alle Tabellen, es sei denn, es sind bestimmte Tabellen-ACL-Regeln vorhanden, um solche Vorgänge einzuschränken.

Sie können nicht zurücksetzen `glide.sm.default_mode` Bis **Zugriff Zulassen** Sobald sie auf festgelegt wurde **Zugriff Verweigern** .

Hinweis: Standardmäßig sind die ACL-Regeln der Platzhaltertabelle die einzigen ACL-Regeln, die den Wert von überprüfen `glide.sm.default_mode` Eigenschaft. Wenn Sie andere Vorgänge mit dieser Einstellung steuern möchten, erstellen Sie eigene ACL-Regeln, um diesen Eigenschaftswert zu überprüfen.

Weitere Informationen zu dieser Eigenschaft finden Sie unter Standardmäßig mit leeren ACLs ablehnen [aktualisiert in Security Center 1,3] In Instanzsicherheitshärtungseinstellungen.

Erweiterte ACL-Konfiguration

Sie können nicht nur neue ACLs erstellen oder vorhandene ACLs ändern, sondern auch andere Aspekte der ACL-Funktionalität konfigurieren.

Lehnen Sie ACL-Regeln ab

Verweigern – Es Sei Denn

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abfrage-ACL-Regeln

Aufgabe	Beschreibung
Wenden Sie ACL-Skriptbedingungen auf Referenzfelder an	Aktivieren Sie eine Eigenschaft, damit Skriptbedingungen auf Referenzfelder angewendet werden können, wenn Sie den Zugriff auf die Daten steuern möchten, die ein Referenzfeld in einem Formular oder in einer Liste anzeigt. Wenn Sie diese Option aktivieren, kann sich dies auf die Leistung Ihrer Instanz auswirken.
ACLs auf AJAXGlideRecord anwenden (clientseitiger Glide-Datensatz)	ACLs auf anwenden `GlideAjax` API-Aufrufe, sodass das System nur die Daten abfragt, für die der derzeit verbundene Anwender Zugriffsrechte hat.
Bewerten Sie die Administratorüberschreibung auf Zugriffsebene	Erzwingen Sie die ACL-Auswertung für Administratorüberschreibungen auf Zugriffsebene. Standardmäßig bestehen Anwender mit der Administratorrolle die Berechtigungsprüfung für diese ACL-Regel automatisch, wenn die Option Administratorüberschreibungen auf ausgewählt ist Formular „ACL-Regeln“ .
Verwenden Sie ACL-Debugging- und -Fehlerbehebungstools	Verwenden Sie Tools wie den ACL-Beobachter, das Debugging auf Feldebene und den Zugriff auf ACL-Regelausgabenachrichten, um Probleme mit ACLs zu beheben und zu debuggen.

Externen Benutzern Zugriff auf eine Tabelle bereitstellen

Um Benutzern mit nur der Rolle snc_external den Zugriff auf die Listenansicht einer Tabelle zu ermöglichen, müssen Sie eine Reihe von ACLs erstellen.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Auf eine privilegierte Rolle hochstufen .
2. Erstellen Sie eine ACL-Regel Mit den folgenden Einstellungen:
   - **Typ**: ui_page
   - **Operation**: Lesen
   - **Name**: {table_name}_list
   - **Erforderliche Rolle**: snc_external
3. Fügen Sie in der standardmäßigen **Lese**-ACL für die Tabelle **snc_external** in die Liste „Erforderliche Rolle“ hinzu.
   Erstellen Sie die ACL, wenn sie nicht bereits vorhanden ist.
4. Verwenden Sie diese Einstellungen, um eine andere ACL zu erstellen:
   - **Typ**: ui_page
   - **Operation**: Lesen
   - **Name**: {table_name}
   - **Erforderliche Rolle**: snc_external
5. Verwenden Sie diese Einstellungen, um eine weitere ACL zu erstellen, um dem Benutzer Schreibzugriff für ein Feld in der Tabelle zu gewähren:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Typ**: Datensatz
- **Operation**: Erstellen
- **Name**: {table_name} {column_name}
- **Erforderliche Rolle**: snc_external

Wiederholen Sie diesen Schritt für jedes Feld, auf das Sie dem Benutzer Schreibzugriff gewähren möchten. Verwenden Sie ein Sternchen * anstelle des Spaltennamens, um Zugriff auf alle Felder gleichzeitig bereitzustellen.

Wenden Sie ACL-Skriptbedingungen auf Referenzfelder an

Verwenden Sie `glide.sys_reference_row_check`Systemeigenschaft zum Aktivieren geskripteter Bedingungen für Referenzfelder.

Das Standardverhalten soll die Instanzleistung verbessern. Wenn Sie Skriptbedingungen für Referenzfelder aktivieren möchten, fügen Sie die folgende Systemeigenschaft hinzu.

Hinweis: Weitere Informationen zum Erstellen von Systemeigenschaften finden Sie unter Systemeigenschaft hinzufügen .

Systemeigenschaft

Eigenschaft	Beschreibung
glide.sys_reference_row_check	Steuert, ob die Skriptbedingungen von Zugriffskontrollregeln für Referenzfelder einer Tabelle gelten. • Typ: Wahr | Falsch • Standardwert: **false** • Standort: Fügen Sie eine Systemeigenschaft hinzu Zur Tabelle „Systemeigenschaften“ [sys_properties]

Hinweis: Wenn `glide.sys_reference_row_check`Systemeigenschaft ist nicht vorhanden oder wurde auf „falsch“ festgelegt. Skriptbedingungen für Zugriffssteuerungsregeln werden nicht angewendet. Dies bedeutet, dass eine ACL, die geskriptete Bedingungen enthält, ihre Prüfung besteht, solange die anderen ACL-Kriterien erfüllt sind (z. B. Rollenanforderungen).

ACLs auf AJAXGlideRecord anwenden (clientseitiger Glide-Datensatz)

Verwenden Sie eine Systemeigenschaft, um die Validierung von Zugriffssteuerungslisten (ACL) durchzuführen, wenn serverseitige Datensätze (z. B. Tabellen) mithilfe von GlideAjax-APIs innerhalb eines Client-Skripts aufgerufen werden.

Wenn Sie Zugriffssteuerungslisten (ACL) auf anwenden möchten `GlideAjax` API-Aufrufe, dann können Sie nur Daten abfragen, auf die der derzeit verbundene Anwender Zugriffsrechte hat. Beispiel: Wenn der Anwender als ESS-Anwender angemeldet ist, der keine Rechte zum Lesen von hat `cmn_location` Tabelle und dann beliebig `GlideAjax` API-Aufruf des Anwenders schlägt fehl.

Wenn ServiceNow AI Platform Wird ohne GlideAjax ACL-Aufrufüberprüfung ausgeführt. Eine API kann Informationen zurückgeben, auf die der derzeit angemeldete Anwender andernfalls nicht zugreifen konnte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie GlideRecordSecure beim Abfragen von Daten, um ein Höchstmaß an Sicherheit sicherzustellen. GlideRecord basiert auf der ACL-Durchsetzung durch Konfigurationen, während GlideRecordSecure strengere Sicherheitskontrollen anwendet. GlideRecordSecure bietet eine sicherere, sofort einsatzbereite Lösung für den Umgang mit sensiblen Daten.

Hinweis: Legen Sie diese Eigenschaft in fest **Systemeigenschaften** > **Sicherheit**an.

Eigenschaft	Standard
Wenden Sie standardmäßige Sicherheits-ACLs auf an `AJAXGlideRecord` Anrufe	ACL-Prüfung erzwungen

Warnung: Die sys_class_Name, sys_ID Und sys_Domain Werden für ACL-Prüfungen ignoriert.

Weitere Informationen zu dieser Eigenschaft finden Sie unter Überprüfung der AJAXGlideRecord-ACL erfordern [aktualisiert in Security Center 1,3] In Instanzsicherheitshärtungseinstellungen.

Bewerten Sie die Administratorüberschreibung auf Zugriffsebene

Wenn Sie die ACL-Auswertung für Administratorüberschreibungen auf Zugriffsebene erzwingen möchten, können Sie eine Systemeigenschaft hinzufügen.

Vorbereitungen

Erforderliche Rolle: security_admin

Warum und wann dieser Vorgang ausgeführt wird

ACLs werden kumulativ ausgewertet. Wenn in einem bestimmten Feld und der eine Anzahl von ACLs vorhanden ist **Administrator-Überschreibungen** Option ist **Falsch** (Nicht ausgewählt) für eine von ihnen werden die effektiven Administratorüberschreibungen für alle ACLs als betrachtet **Falsch** . Dies führt dazu, dass Administratoren nicht einmal die ACL übergeben können, für die die Überschreibung gelten soll.

Prozedur

Fügen Sie der Tabelle mit den Systemeigenschaften die folgende Eigenschaft hinzu:

Eigenschaft	Beschreibung
`glide.security.admin.override.accessterm`	Wertet die Administratorüberschreibungsbedingung auf Ebene der Zugriffsbedingung aus. • Typ: Wahr | Falsch • Standardwert: **Wahr** Für neue Instanzen **Falsch** Für Upgrades • Speicherort: Fügen Sie den Systemeigenschaften hinzu `[sys_properties]`Tabelle **Hinweis:** Wenn die Eigenschaft nicht in der Instanz definiert ist, wird der Wert als falsch ausgewertet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

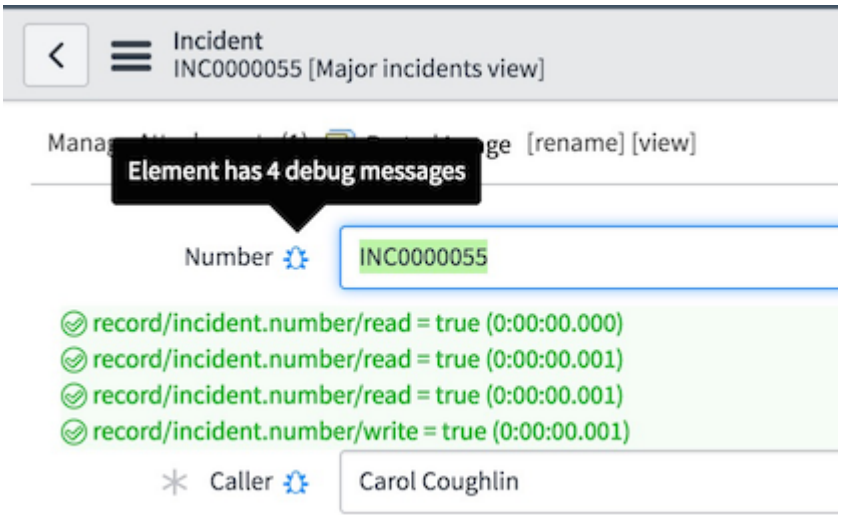
ACL-Debugging-Tools

Debugging- und Zugriffsregelausgabemeldungen auf Feldebene sind verfügbar, um Ihnen bei der Problembehandlung und dem Debuggen von ACLs zu helfen. Die ACL-Konfigurationsbeobachtung informiert Sie, welche zugehörigen ACLs vorhanden sind, wenn Sie eine ändern.

Debugging auf Feldebene

Wenn Debugging aktiviert ist, wird ein kleines Fehlersymbol ( ) Wird neben jedem Feld mit einer ACL-Regel angezeigt. Wenn Sie auf das Symbol klicken, werden die ACL-Regeln aufgelistet, die für das Feld und die Auswertungsergebnisse gelten. Aktivieren Sie das Debugging, indem Sie zu navigieren **Systemsicherheit** > **Debugging** > **Sicherheitsregeln debuggen**an.

Sicherheit auf Feldebene für einen Incident



Nachdem Sie das ACL-Debugging aktiviert haben, können Sie die Identität eines anderen Anwenders annehmen, um zu sehen, welche ACL-Regeln der Anwender übergibt und fehlschlägt. Wenn Sie die Identität eines Anwenders annehmen, können Sie nur sehen, was dieser Anwender sehen darf. Sie können beispielsweise keinen Datensatz anzeigen, den eine ACL verhindert, dass der Anwender angezeigt wird. Um das Debugging zu erleichtern, ist standardmäßig schreibgeschützter Zugriff auf bestimmte ACL-bezogene Tabellen aktiviert, auch wenn die Identität eines Anwenders angenommen wird, der keinen Lesezugriff auf die Tabellen hat. Um diese Funktionalität zu ändern, legen Sie die folgende Eigenschaft auf fest **Falsch** .

Um das Debugging von ACL-Regeln zu aktivieren, navigieren Sie zu **Systemsicherheit** > **Sicherheitsregeln debuggen**an.

Systemeigenschaft	Beschreibung	Standardeinstellung
glide.security.access_acl	Ermöglicht schreibgeschützten Zugriff auf die folgenden Tabellen, während die Identität eines	wahr

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaft	Beschreibung	Standardeinstellung
	Anwenders angenommen wird: sys_Security_acl, sys_Security_Operation, sys_Security_type und sys_user_role. Infolgedessen kann der Anwender, dessen Identität angenommen wird, Daten lesen, die der Anwender, dessen Identität angenommen wurde, nicht lesen kann.	**Hinweis:** Wenn die Eigenschaft auf „falsch“ festgelegt ist, kann der Anwender, dessen Identität angenommen wurde, daran gehindert werden, ACL-bezogene Daten zu lesen. In diesem Fall ist möglicherweise eine zweite Sitzung erforderlich, die als admin oder Security_admin angemeldet ist, um ACLs zu debuggen.

ACL-Regelausgabemeldungen

ACL-Debugging zeigt ACL-Regelausgabemeldungen am unteren Rand jeder Liste und jedes Formulars an. In der Ausgabemeldung wird Folgendes angezeigt:

Nachrichtenelement	Beschreibung
TIME	Die Gesamtzeit, die für die Verarbeitung dieser ACL-Regel verwendet wird.
PFAD	Informationen, die jede ACL-Regel eindeutig identifizieren, im folgenden Format: <ACL-Regeltyp>/<ACL-Regelname>/<Operation> .
KONTEXT	Das Objekt, das von der ACL-Regel ausgewertet wird.
RC	Der Rückgabecode der ACL-Regel. Ein Wert „wahr“ übergibt die ACL-Regel. Ein falscher Wert schlägt bei der ACL-Regel fehl.
REGEL	Eine kurze Zusammenfassung der Prozessoren und Skripts, gefolgt von ACL-Ergebnissen für jede ACL-Auswertung auf Tabellen- und Feldebene. Die meisten ACL-Auswertungen zeigen ein Gesamtergebnis für bestanden oder nicht bestanden, gefolgt von einer Aufgliederung der Ergebnisse für jeden Typ von ACL-Kriterien: • IAccessHandler: Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. Dies ist eine Systemsicherheitsprüfung, die Sie nicht ändern können. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet. Sie können die IAccessHandler-Prüfungen in keiner Weise ändern. Beispielsweise wird eine IAccessHandler-Implementierung für Zugriffsprüfungen für Anwendungsressourcen verwendet, und diese kann nicht geändert werden. Dies ist ab verfügbar Istanbul Release. • Rollen: Verifizierung, ob der Anwender über die richtige Rolle verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachrichtenelement	Beschreibung
	• Bedingung: Verifizierung, dass der Anwender die in der ACL-Regel angegebene Bedingung (falls vorhanden) bestanden hat. • Skript: Verifizierung, dass der Anwender das in der ACL-Regel angegebene Skript (falls vorhanden) übergeben hat.

Die angezeigten Symbole zeigen, wie die ACL ausgewertet wurde:

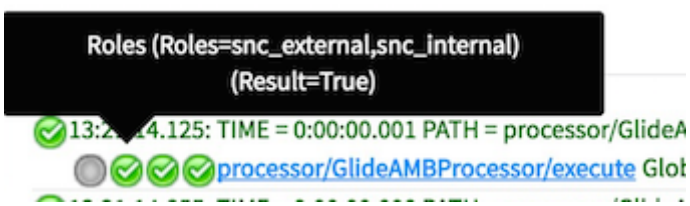
Symbol	Beschreibung
Ein grünes Häkchen ( )	Gibt an, dass die Tabelle oder das Feld die Kriterien erfüllt hat.
Ein rotes x-Symbol ( )	Gibt an, dass die Tabelle oder das Feld nicht bestanden wurde.
Ein leeres grauer Kreissymbol ( )	Gibt an, dass die ACL-Auswertung nicht durchgeführt werden musste.
Ein blaues Häkchen, x oder ein leerer Kreis	Gibt an, dass die ACL aus einem zwischengespeicherten Ergebnis einer vorherigen ACL-Prüfung entnommen wurde. Die Symbole bedeuten dasselbe wie oben.

Sie können diese Aktionen für die ACL-Debug-Ausgabe ausführen:

- Aktivieren oder deaktivieren Sie diese Kontrollkästchen oben in der Debug-Ausgabe:
  - **Sicherheitsregeln**: Zeigt die Ergebnisse der ACL-Prüfungen an oder blendet sie aus.
  - **Andere**: Andere Warnungen oder Nachrichten anzeigen oder ausblenden.
- Klicken Sie neben einer der Ausgabenachrichten auf den Namen der ACL, um diesen ACL-Datensatz zu öffnen.



- Bewegen Sie den Cursor über eines der Symbole für die vier ACL-Prüfungen, um weitere Informationen anzuzeigen.



ACL-Fehlerbehebungsreferenz

Eine Liste allgemeiner ACL-Regelfehler und ihrer Lösungen.

Aktivieren Sie das Debugging, um bei der Behebung eines Problems zu helfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung

Fehler oder Symptom	Lösung
Sie können nicht über eine anwenderdefinierte Tabelle auf Datensätze zugreifen.	Erstellen Sie eine Tabellen-ACL-Regel für die anwenderdefinierte Tabelle, die Anwendern Zugriff auf die Tabelle gewährt. Ohne eine explizite Tabellen-ACL-Regel müssen Anwender die Berechtigungen in der Tabelle-Platzhalter-ACL-Regel (*) übergeben, die standardmäßig den Zugriff nur auf Administratoren beschränkt. Aktivieren Debugging Und bestimmen Sie, welche ACL-Regeln für die anwenderdefinierte Tabelle ausgewertet werden.
Sie erstellen eine anwenderdefinierte ACL-Regel, die nicht ordnungsgemäß funktioniert.	Die wahrscheinlichsten Probleme bestehen darin, dass eine andere Regel in der Verarbeitungsreihenfolge Vorrang vor Ihrer anwenderdefinierten Regel hat oder dass der Anwender nicht alle Berechtigungsanforderungen für den Objekttyp erfüllt. Aktivieren Debugging Und verifiziert, dass die ACL-Regel ausgewertet wird.
Ihre Feld-ACL-Regel funktioniert nicht ordnungsgemäß.	Wahrscheinlich gibt es eine Tabellen-ACL-Regel, die der Anwender nicht erfüllt hat. Aktivieren Debugging Und bestimmen Sie, welche ACL-Regeln für das Feld ausgewertet werden. Stellen Sie sicher, dass keine in Konflikt stehende Tabellen-ACL-Regel oder ACL-Regel für doppelte Felder vorhanden ist.
Ihre Tabellen-ACL-Regel funktioniert nicht ordnungsgemäß.	Es gibt entweder eine ACL-Regel höher in der Verarbeitungsreihenfolge oder eine ACL-Regel für doppelte Tabellen, die die ACL-Regel der Tabelle stört. Aktivieren Debugging Und bestimmen Sie, welche ACL-Regeln für die Tabelle ausgewertet werden.
Sie können ein Feld in einer Liste anzeigen, aber nicht im Formular.	Es ist möglich, dass die ACL-Regelbedingungen oder das Skript in der Liste, aber nicht im Formular ausgelöst werden. Aktivieren Debugging Und bestimmen, wann die ACL-Regeln als „wahr“ ausgewertet werden. Aktualisieren Sie die Bedingungen oder das Skript, um dasselbe Verhalten in der Liste und im Formular zu haben.
Sie erhalten eine Fehlermeldung, wenn Sie versuchen, eine Prozessor- oder vom Client aufrufbare Skripteinbindung auszuführen.	Es gibt eine ACL-Regel für die Prozessor- oder vom Client aufrufbare Skripteinbindung, die der Anwender nicht erfüllt hat. Wenn der Anwender Zugriff auf das Objekt haben soll, aktivieren Sie Debugging Und bestimmen Sie, welche ACL-Regeln für den Prozessor oder die Skripteinbindung ausgewertet werden. Aktualisieren Sie die ACL-Regel oder die Anwenderrollen nach Bedarf, um auf das Objekt zuzugreifen.

ACL-Konfigurationsbeobachter

Die ACL-Konfigurationsbeobachtung informiert Sie, welche zugehörigen ACLs in einer Tabelle vorhanden sind, wenn Sie eine ACL in derselben Tabelle einfügen, aktualisieren oder löschen.

Der ACL-Konfigurationsbeobachter ist ein Interceptor-Fenster, das jedes Mal angezeigt wird, wenn Sie wichtige Änderungen an der Tabelle „Zugriffssteuerung“ [sys_Security_acl] vornehmen. Es wird ein Zusammenfassungsfenster für Sicherheitsregeln angezeigt, in dem Sie ACLs anzeigen können, die sich auf die von Ihnen geänderte Zugriffssteuerungsliste beziehen. Sie können keine ACLs im Fenster „Sicherheitsregeln“ ändern. Um Änderungen vorzunehmen, schließen Sie das Beobachtungsfenster, und wechseln Sie zu diesen ACLs.

Der ACL-Konfigurationsbeobachter wird in den folgenden Situationen nicht angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie einen ACL-Datensatz speichern oder aktualisieren, ohne tatsächlich Änderungen vorzunehmen.
- Wenn Sie geringfügige Aktualisierungen vornehmen (nicht einfügen oder löschen), z. B. das Aktualisieren von Skripts, Bedingungen und der Option admin-overrides.
- Wenn der ACL-Datensatz nicht aktiv ist.

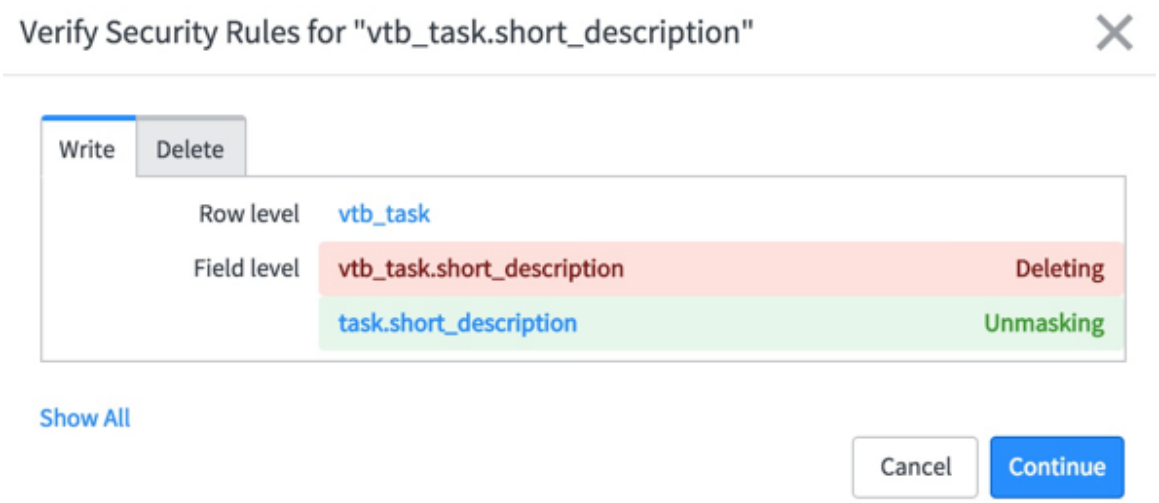
Fenster „ACL-Sicherheitsregeln“

Der Konfigurationsbeobachter zeigt an ACL-Ausführungsplan . Der Ausführungsplan wird im Popup-Fenster „Sicherheitsregeln“ angezeigt. Sie können diese Art von Informationen anzeigen:

Elemente des ACL-Konfigurationsfensters

Element	Beschreibung
Rote Hervorhebung	Eine ACL, die gelöscht oder deaktiviert wird.
Blaue Hervorhebung	Eine geänderte ACL.
Grüne Hervorhebung	Eine ACL, die hinzugefügt wird oder aktiv wird.
Maskierung	Eine ACL, die wirksam war, bis Sie eine Änderung vorgenommen haben.
Maskierung Aufgehoben	Eine ACL, die gerade wirksam wurde, als Sie eine Änderung vorgenommen haben.

Beispiel für Konfigurationsbeobachter



ACL-Ausführungsplan anzeigen

Administratoren können anzeigen, wie ACLs miteinander verknüpft sind, indem sie einen Ausführungsplan für eine beliebige ACL in der Instanz anzeigen.

Vorbereitungen

Erforderliche Rolle: security_admin

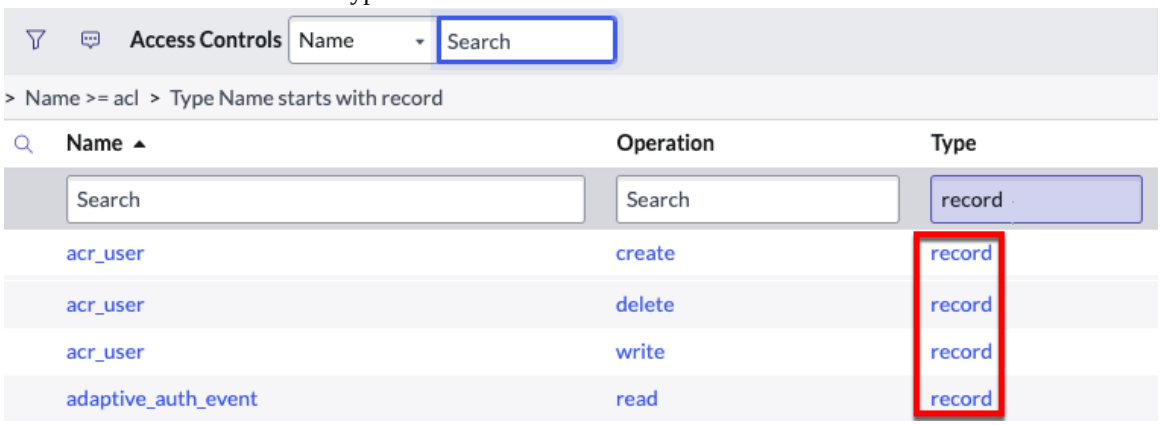
Prozedur

1. Auf eine privilegierte Rolle hochstufen.
2. Navigieren zu **Systemsicherheit** > **Zugriffssteuerung (ACL)**an.

Automatische Übersetzung

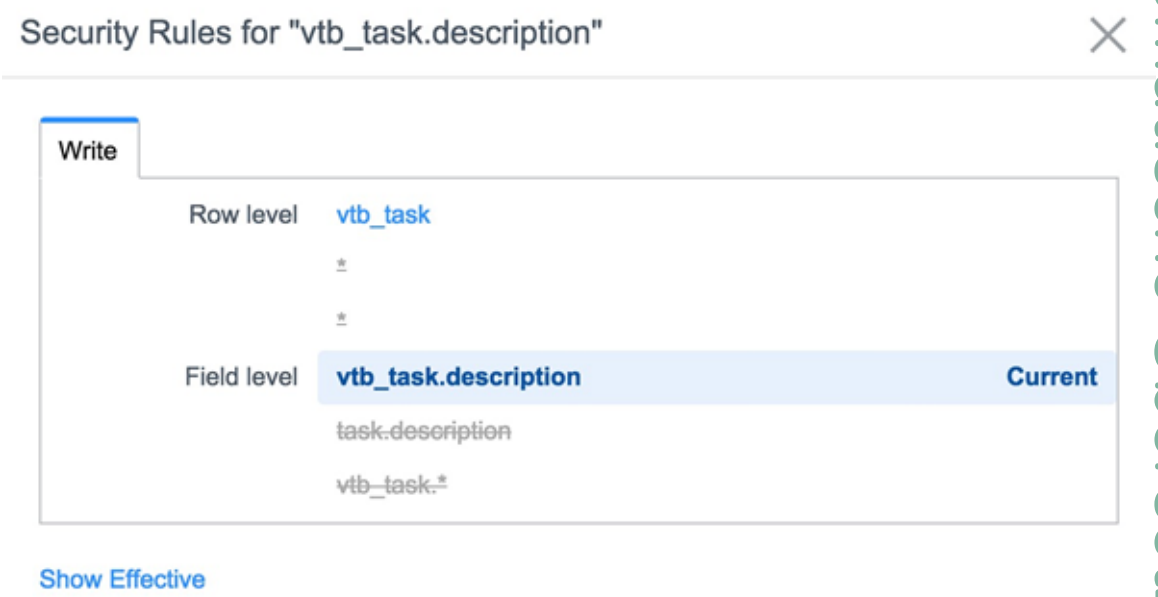
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie eine ACL mit dem Typ *record*.



4. Klicken Sie Auf **ACL-Ausführungsplan anzeigen** Im Abschnitt zugehörige Links.

Das Fenster „Sicherheitsregeln“ wird für die ACL angezeigt. Das Beispiel zeigt den Ausführungsplan für „vtb_Task“ an.



ACL-Ausführungsplan-Fenster

UI-Element	Beschreibung
Titel	Der Name der ACL.
Registerkartenname	Wenn die ACL „Erstellen“, „Lesen“, „Schreiben“ oder „Löschen“ ist.
Zeilenebene	ACLs auf Zeilenebene, die in dieser Tabelle ausgeführt werden.
Feldebene	ACLs auf Feldebene, die nur für dieses Feld (oder diese Spalte in der Tabelle) ausgeführt werden.

5. Klicken Sie Auf **Alle anzeigen** Zum Anzeigen aller zugehörigen ACLs, einschließlich der überschriebenen ACLs und generischen ACLs, die für alle Datensätze gelten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überschriebene ACLs haben eine Linie durch den Namen, und generische ACLs haben das Platzhalterzeichen Sternchen (*) für den Namen.

6. Zeigen Sie nur die unmittelbaren ACLs an, die sich auf die von Ihnen angezeigte beziehen, und blenden Sie die ACLs in Tabellen aus, aus denen die ACL-Tabelle erweitert wird, und die generischen Platzhalter-ACLs (*) aus, indem Sie klicken **Effektiv Anzeigen** .

Verwenden Sie den ACL-Konfigurationsbeobachter

Verwenden Sie den ACL-Konfigurationsbeobachter, nachdem Sie die Rolle „Security_admin“ erhöht haben.

Vorbereitungen

Erforderliche Rolle: security_admin

Auf eine privilegierte Rolle hochstufen

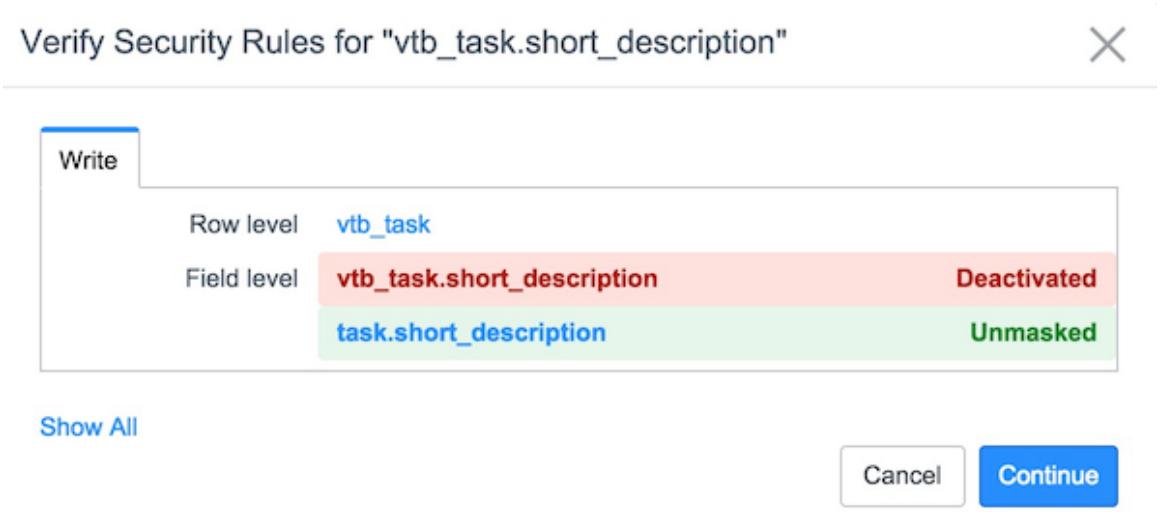
Prozedur

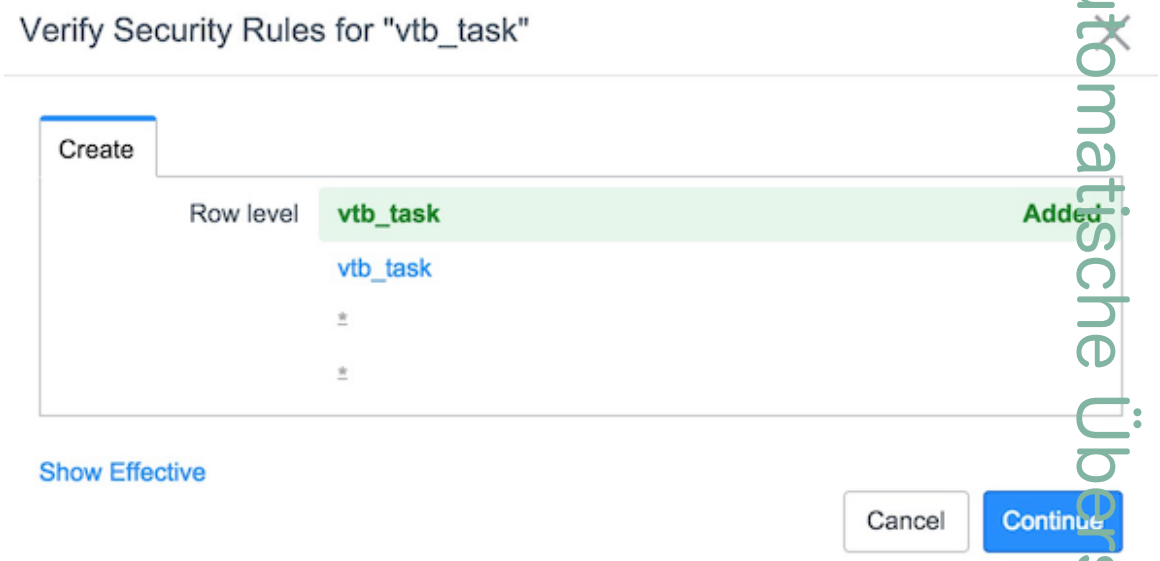
1. Öffnen Sie eine ACL, die eine Datensatztyp-ACL ist.
2. Führen Sie eine Aktion für die ACL aus, z. B. Ändern oder Auswählen einer Option aus dem Kontextmenü wie **Einfügen** .
3. Wenn Sie Werte im Formular „Zugriffssteuerung“ geändert haben, klicken Sie mit der rechten Maustaste auf den Header, und wählen Sie aus **Speichern** Oder klicken Sie auf **Aktualisieren** Oder **Löschen** .

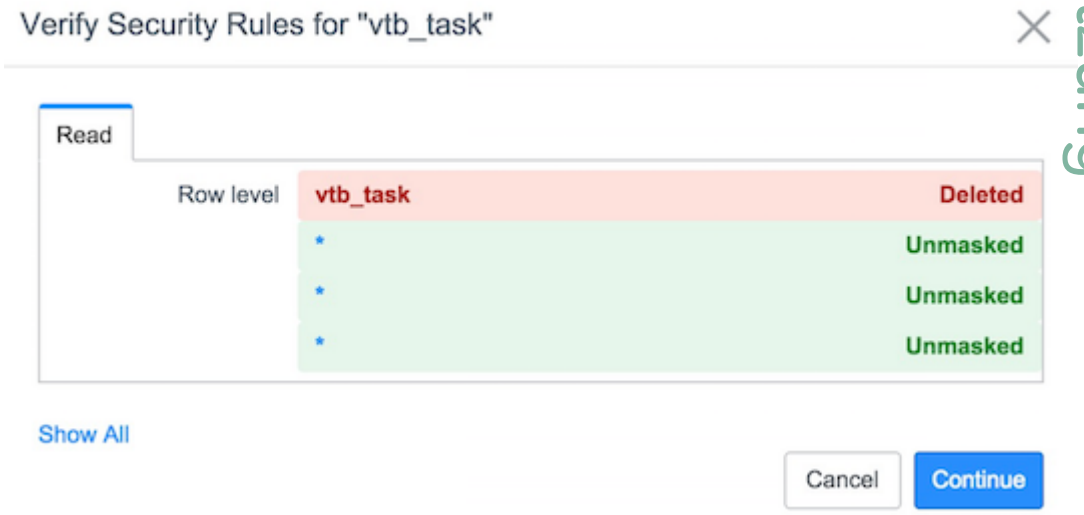
   Das Fenster Sicherheitsregeln wird angezeigt. Das System hat die Datenbankaktion für die ACL noch nicht ausgeführt, daher wurden die Änderungen noch nicht gespeichert.

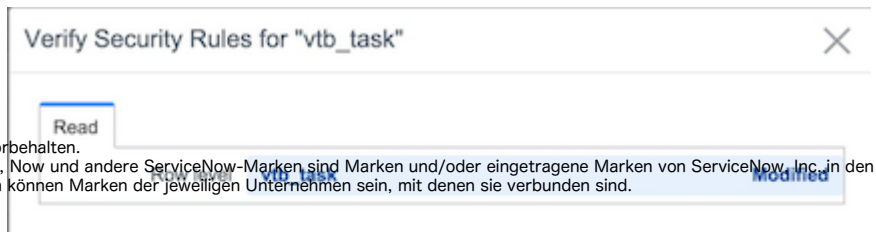
   Dies sind Beispiele für Sicherheitsregeln in der Tabelle „Private Task“ [vtb_Task] der Anwendung „Visual Taskboard“. Siehe ACL-Konfigurationsbeobachter Für eine Beschreibung der Elemente in diesem Fenster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.









Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc. in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

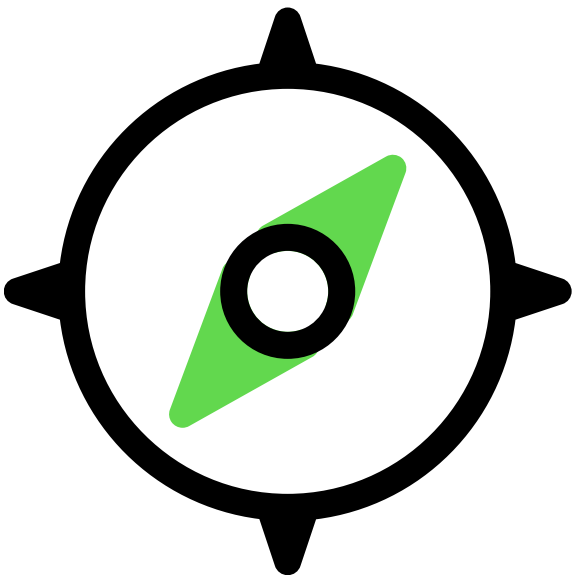
4. Genau wie bei Ausführungsplan , Sie können auf klicken **Alle anzeigen** Um alle zugehörigen ACLs anzuzeigen, einschließlich der überschriebenen und generischen ACLs, die für alle Datensätze gelten, oder klicken Sie auf **Effektiv Anzeigen** Um nur die unmittelbaren ACLs anzuzeigen, die sich auf die von Ihnen angezeigte zugehörig beziehen.
5. Bewegen Sie den Mauszeiger über eine der ACLs, um eine Beschreibung anzuzeigen.

Sicherheitsattribute

Sicherheitsattribute bieten eine flexible Alternative zu Zugriffssteuerungslisten.

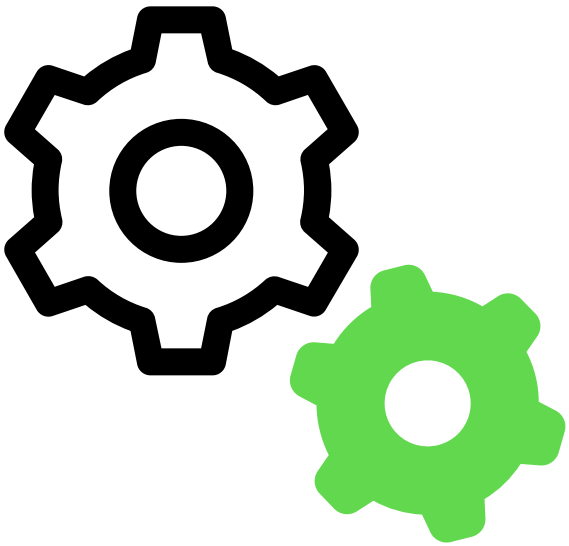
Erste Schritte

Erkunden Sie Sicherheitsattribute



Erfahren Sie mehr über die Grundlagen von Sicherheitsattributen

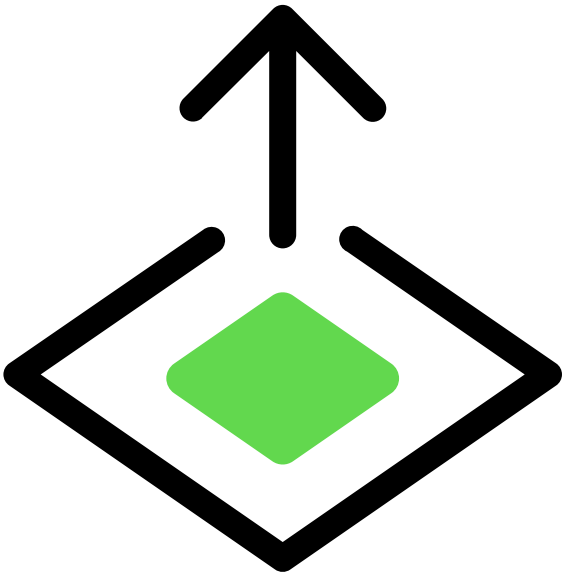
Erstellen Sie Sicherheitsattribute



Erstellen Sie neue Sicherheitsattribute

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OOB-Sicherheitsattribute (sofort einsatzbereit)



Erklären Sie die OOB-Sicherheitsattribute

Protokollierung Von Sicherheitsattributen

Überprüfen Sie die Protokollierung des Sicherheitsattributs

Grundlagen Der Sicherheitsattribute

A Sicherheit Attribut ist eine in hohem Maße konfigurierbare Information über ein Thema oder seine Umgebung. Bei Verwendung in Zugriffssteuerungen ermöglicht es eine feinkörnige Sicherheitskonfiguration auf nicht komplexe Weise.

Übersicht

Sicherheitsattribute bieten eine alternative Methode für die Zugriffssteuerung über Rollendefinitionen zur derzeit praktizierten ACL-Konfiguration (Zugriffssteuerungslisten). Sicherheitsattribute bieten verschiedene Vorteile für ACL-basierte Konfigurationen:

Bessere Sicherheit

Die verbesserte Verschleierung der Berechtigungsauswertung stellt sicher, dass Ihre Organisation sicher bleibt.

Visuell Lesbar

Sicherheitsattribute sollen die Erstellung und Anwenderfreundlichkeit von Sicherheitsberechtigungen vereinfachen.

Flexible Sicherheit

Erstellen Sie Persona-Definitionen aus beiden sofort einsatzbereiten Konfigurationen in Kombination mit kundendefinierten Personas.

Protokollierung und Auditing

Sicherheitsattribute bieten detaillierte Audits und Protokollierung, um mehr Einblick in Sicherheitsmaßnahmen und -Theorie zu erhalten.

Erstellen Sie Sicherheitsattribute

Erstellen Sie neue Sicherheitsattribute mit einer Schritt-für-Schritt-Anleitung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **System Sicherheit** > **Sicherheitsattribute**an.
2. Wählen Sie in der Liste Sicherheitsattribute die Option aus **Neu** .
3. Füllen Sie die Felder im Formular „Sicherheitsattribute-Felder“ aus.

Sicherheitsattribut-Felder

Feld	Beschreibung
Bezeichnung	Bezeichnung des Sicherheitsattributs.
Name	Name des Sicherheitsattributs.
Typ	Der Typ des Sicherheitsattributs. ○ Verbindung **Hinweis:** Weitere Informationen zu zusammengesetzten Sicherheitsattributen finden Sie unter Zusammengesetzte Sicherheitsattribute ○ Ganzzahl ○ Liste ○ Zeichenfolge ○ boolescher wert (wahr|falsch)
Ist dynamisch	Ob der Wert des Sicherheitsattributs pro neu bewertet werden muss
Beschreibung	Vom Anwender generierte Beschreibung des Sicherheitsattributs
Anwendung	Statisches Feld, Anwendungsbereich.
Suchtabelle	Verweisen Sie zur Auswertung auf eine externe Tabelle.
Tabellenspalte suchen	Referenzieren Sie eine Tabellenspalte zur Auswertung.
Skript	Leiten Sie einen Wert aus einem Skript ab.

OOB-Sicherheitsattribute (sofort einsatzbereit)

Häufig verwendete, generalisierte Sicherheitsattribute-Rollen, die einsatzbereit sind.

Übersicht

Die OOB-Sicherheitsattribute (sofort einsatzbereit) sind eine einfache Möglichkeit, die Fähigkeiten von Sicherheitsattributen mit einer Reihe vorkonfigurierter Sicherheitsattribut-Rollen zu verwenden und zu lernen. Die OOB-Sicherheitsattribut-Rollen sind häufig verwendete Zugriffssteuerungsrollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Erstellen eines eigenen Sicherheitsattributs oder zum erweitern einer OOB-Sicherheitsattribute-Funktionalität finden Sie unter Zusammengesetzte Sicherheitsattribute

OOB-Sicherheitsattribute

Attribut	Beschreibung
Gruppe	Anwender ist Mitglied einer angegebenen Gruppe
GroupExplicit	Anwender ist ein explizites Mitglied einer bestimmten Gruppe
HasAdminRole	Anwender hat die Administratorpersona
Verwendung einer anderen Identität	Identität des Anwenders wird angenommen
InteractiveSession	Aktuelle Sitzung interaktiv
AngemeldetIn	Anwender ist angemeldet und authentifiziert
Netzwerkkriterien	Zusätzliche Netzwerkkriterien
Rolle	Anwender hat eine bestimmte Rolle
RoleExplicit	Für den Anwender ist eine bestimmte Rolle explizit definiert

Sicherheitsattribute für Client-Sitzung

Die folgenden Sicherheitsattribute werden für die Client-Sitzung hinzugefügt (Plugin: `Com.Glide.Client_Session_Security_attributes`):

- **IsIframeEinbettSitzung** : Das Attribut wird im eingebetteten iFrame in Drittparteiportalen verwendet. Zum Beispiel Engagement Messenger, Virtual Agent Web Client, eingebettete Sitzung usw.
- **IsIntegrationAsAServiceSession** : Das Attribut wird in Messaging-Apps wie Virtual Agent in Teams, Virtual Agent in Slack, Virtual Agent in WhatApp verwendet.
- **IsIntegrationAsAUserSession** : Das Attribut wird im Integrations-Account-Anwender oder Webservice-Anwender verwendet.
- **Ist Servicenow-Websitzung** : Das Attribut wird in einer interaktiven Websitzung verwendet.
- **Ist Mobile-App-Sitzung** : Das Attribut wird verwendet, wenn **Mobile_Client** Eigenschaft ist in „wahr“ **oauth_Entität** Datensatz.

Hinweis: Sie müssen verwenden **IsIframeEinbettSitzung** , **IsIntegrationAsAServiceSession** , Und **IsIntegrationAsAUserSession** Nur beim Konfigurieren des Clienttyps für OAuth- und SSO-Datensätze. Weitere Informationen finden Sie unter Konfigurieren Sie den Clienttyp für OAuth- und SSO-Datensätze.

Unexplizites und explizites Verhalten erklärt

Sicherheitsattribute erfüllen nuancierte Berechtigungsanforderungen mit einer expliziten vs. Nicht expliziten (geerbten) Bewertung von Rollenberechtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammengesetzte Sicherheitsattribute

Mit zusammengesetzten Sicherheitsattributen können Sie konsistente und wiederverwendbare Sicherheitsattribut-Profile erstellen, die Ihren Geschäftsanforderungen entsprechen

Übersicht

Zusammengesetzte Sicherheitsattribute werden aus einem oder mehreren bereits vorhandenen Sicherheitsattributen definiert, um eine einzelne Referenzkombination von Sicherheitsattributen für die Berechtigungsauswertung zu erstellen.

Zusammengesetzte Sicherheitsattribute erstellen

Erstellen Sie ein zusammengesetztes Sicherheitsattribut zur einfachen Wiederverwendung.

Vorbereitungen
Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Systemsicherheit** > **Sicherheitsattribute**an.
2. Wählen Sie in der Liste Sicherheitsattribute die Option aus **Neu** .
3. Wählen Sie Aus Verbindung In **Typ** Feld.
4. Füllen Sie die Felder im Formular „Sicherheitsattribute-Felder“ aus.

Sicherheitsattribut-Felder

Feld	Beschreibung
Bezeichnung	Bezeichnung des Sicherheitsattributs.
Name	Name des Sicherheitsattributs.
Beschreibung	Vom Anwender generierte Beschreibung des Sicherheitsattributs
Bedingung	Die spezifischen Sicherheitsattribut-Bedingungen, die zum Definieren der Bewertung der Sicherheitsattribute verwendet werden.
Neues Kriterium	Fügen Sie einen zusätzlichen Satz hinzu **Oder** Bedingungen für die Auswertung.

Sicherheitsattribut Umfang

Sicherheitsattribute unterstützen Umfangsfunktionen.

Umfang Des Sicherheitsattributs

Das bereichsbezogene Verhalten von Sicherheitsattributen stimmt mit dem bereichsbezogenen Verhalten der Plattform überein. Sicherheitsattribute, die innerhalb eines Bereichs erstellt wurden, sind nur in Zugriffssteuerungen im selben Bereich verfügbar.

Lokale und vorhandene Sicherheitsattribute

Mit vorhandenen und lokalen Sicherheitsattributen können Kunden Sicherheitsattribut-Bedingungssätze wiederverwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lokale Und Vorhandene Attribute

Mit dem Bedingungsgenerator für ACL-Sicherheitsattribute können Kunden angeben, ob ein Sicherheitsattribut entweder vorhanden oder lokal ist.

Hinweis: Die Bedingungen für Sicherheitsattribute sind standardmäßig auf „Lokal“ festgelegt.

Ein lokal definiertes Sicherheitsattribut wird nur in der einzelnen ACL gespeichert, in der es erstellt wird.

Mit der Option „vorhanden“ können Anwender vorhandene Sicherheitsattribut-Bedingungen auf den Bedingungsgenerator verweisen.

Feldabfragerollen und Einschränkungen

Die **Feldabfragerollen** Und **Einschränkungen Der Feldabfrage** Mit Attributen können Sie besser steuern, welche Informationen Anwendern in Tabellen zur Verfügung stehen.

Übersicht

Die **Feldabfragerollen** Und **Einschränkungen Der Feldabfrage** Attribute ermöglichen eine genauere Steuerung darüber, welche Aktionen Anwender für Tabellen ausführen können.

Feldabfragerollen

Verhindert das Abfragen vertraulicher Felder basierend auf der Anwenderrolle.

Einschränkungen Der Feldabfrage

Beschränken Sie den Zugriff auf den Datensatz, wenn der Zugriff auf das entsprechende Feld verweigert wird.

Konfigurieren Sie eine Feldabfragerolle

Erfahren Sie, wie Sie ein Rollenattribut für Feldabfragen aktivieren und konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Tabellen**an.
2. Wählen Sie eine **Tabelle** aus.
3. Wählen Sie ein aus **Spaltenbezeichnung** Um anzuzeigen **Wörterbuch** Eintrag.
4. Wählen Sie die Registerkarte **Attribute** aus.
5. **Tipp:** Wenn Sie nicht haben **Feldabfragerollen** Feld auswählen **Neu** Um eines zu erstellen

   Wählen Sie aus **Feldabfragerollen** Attribut.
6. Geben Sie die Rollen ein, die zum Anzeigen dieser Tabellenspalte in erforderlich sind **Wert**
7. Wählen Sie Aus **Aktualisieren**

Ergebnis

Die Tabellenspalte kann nur von den in definierten Rollen abgefragt werden **Feldabfragerollen** Attribut. Wenn ein Anwender ohne die definierten Rollen die Tabellenspalte abfragt, wird ihm der Zugriff auf den Vorgang verweigert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Einschränkungen Für Feldabfragen

Erfahren Sie, wie Sie eine Feldabfrageeinschränkung konfigurieren

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Tabellen**an.
2. Wählen Sie eine **Tabelle** aus.
3. Wählen Sie ein aus **Spaltenbezeichnung** Um anzuzeigen **Wörterbuch** Eintrag.
4. Wählen Sie die Registerkarte **Attribute** aus.
5. **Tipp:** Wenn Sie nicht haben **Feldabfrage Schränkt Den Datensatzzugriff Ein** Feld auswählen **Neu** Um eines zu erstellen

   Wählen Sie aus **Feldabfrage Schränkt Den Datensatzzugriff Ein** Attribut.
6. Geben Sie Ein `Wahr` In **Wert** Feld, um den Datensatzzugriff nur auf Anwender zu beschränken, die das Feld anzeigen können. Andernfalls geben Sie ein `Falsch` .
7. Wählen Sie Aus **Aktualisieren**

Ergebnis

Die Tabellenspalte schränkt die Ergebnisse aller Abfragen ein. Eingeschränkte Anwender werden darüber informiert, wie viele Ergebnisse eine Abfrage zurückgegeben hat, aber keine weiteren Informationen.

Skripting-Governance-Tool

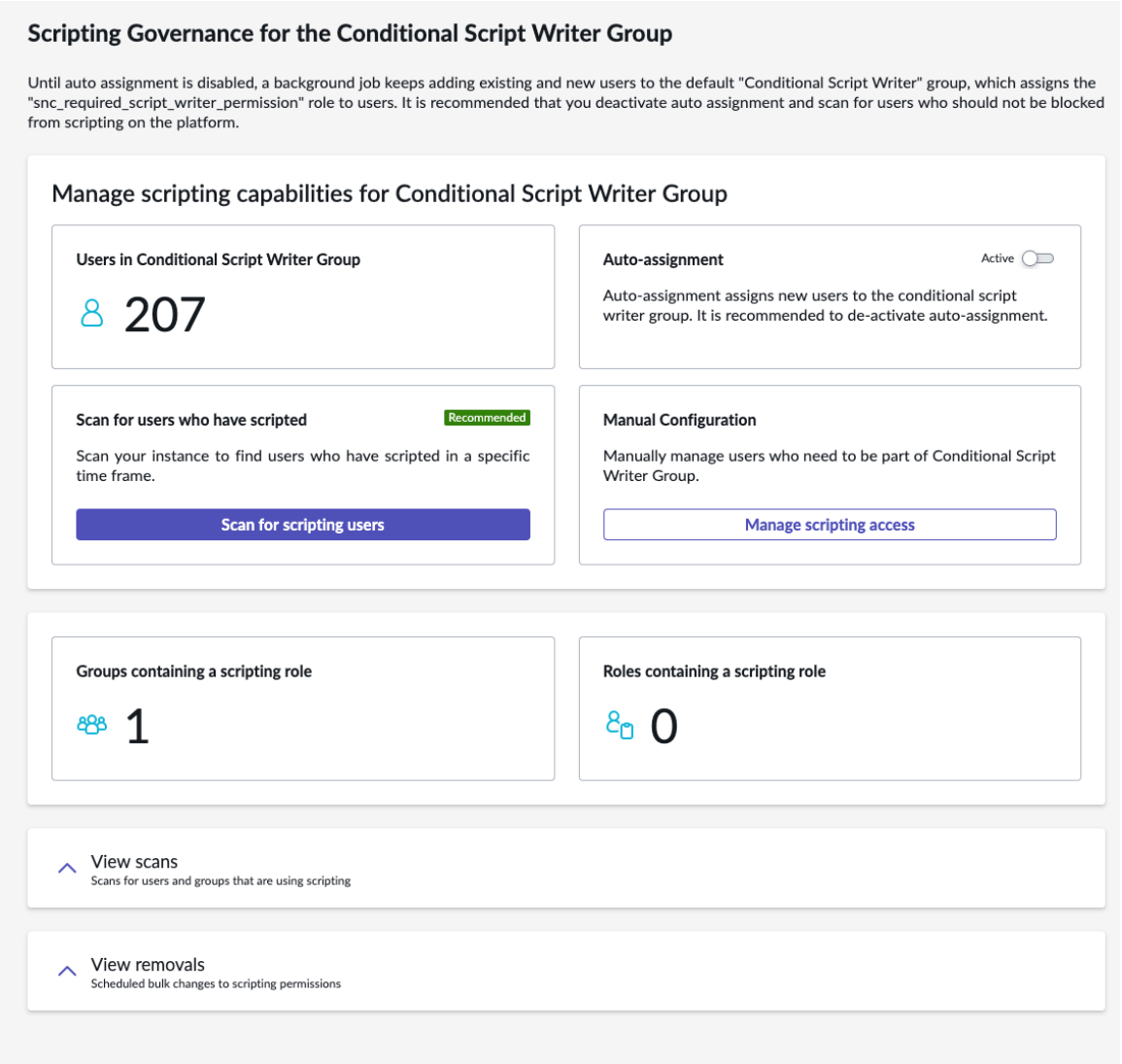
Verwalten Sie Anwenderberechtigungen für das Skripting auf der Plattform über das Skripting-Governance-Tool.

Die **Skript-Governance-Tool** Hilft Ihnen, Governance-Metriken für Anwenderskripting zu überprüfen und die bedingte Skriptschreibergruppe zu verwalten. Diese Gruppe gewährt ihren Mitgliedern über die Rolle „snc_required_script_Writer_permission“ Skriptberechtigungen. Anwender werden der Gruppe entweder durch eine automatisierte Zuweisung oder eine manuelle Konfiguration hinzugefügt. Sie können beide Einstellungen über verwalten **Skript-Governance-Tool** .

Um auf zuzugreifen **Skript-Governance-Tool** Navigieren Sie zu **Alle** > **Systemsicherheit** > **Skripting-Governance-Tool**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard für Skripting-Governance-Tool



Übersicht über das Skripting-Governance-Tool

Anwender in der bedingten Skriptverfasser-Gruppe

Zeigt die Anzahl der Autoren in der bedingten Skriptverfasser-Gruppe an. Diesen Anwendern wird die „snc_required_script_Writer_permission“ gewährt, bis sie aus der Gruppe entfernt werden.

Automatische Zuweisung

Durch die automatische Zuweisung werden neue Anwender der bedingten Skriptverfasser-Gruppe zugewiesen. Wählen Sie den Schieberegler aus, um die automatische Zuweisung zu aktivieren oder zu deaktivieren

Nach Anwendern scannen, die geskriptet haben

Suchen Sie nach Anwendern in der bedingten Skriptverfasser-Gruppe, die im letzten Zeitraum geskriptet haben. Wählen Sie aus **Scannen Sie nach Skriptanwendern** Schaltfläche und füllen Sie das kurze Formular aus, um einen Scan zu planen.

Manuelle Konfiguration

Sie können manuell Anwender auswählen, die in der Gruppe „Bedingter Skriptverfasser“ bleiben. Wählen Sie aus **Verwalten Sie den Skripterstellungszugriff** Schaltfläche und geben Sie die Anwender in das Textfeld ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Anwender, die nicht als Teil der Writer-Gruppe für bedingte Skripterstellung ausgewählt sind, werden aus der Gruppe entfernt.

Gruppen, die eine Skripting-Rolle enthalten

Zeigt die Anzahl der Gruppen an, die eine Skriptrolle enthalten. Standardmäßig hat die bedingte Skriptverfasser-Gruppe immer eine Skripting-Rolle.

Rollen, die eine Skripting-Rolle enthalten

Zeigt die Anzahl der Rollen an, die eine Skriptrolle enthalten

Scans anzeigen

Eine erweiterbare Tabelle mit den Anwendern und Gruppen, die Skripting verwenden. Ausgefüllt von **Scannen Sie nach Skriptanwendern** Schaltfläche.

Skripting-Scan-Tabellenfelder

Bezeichnung	Beschreibung
Scan-Nummer	Die Nummer-ID des Scanauftrags.
Status	Status des Scans
Abgeschlossen	Abschlussstatus des Scans
Geplant	Geplante Ausführungszeit für den Scan
Erstellt von	Anwender, der den Scan initiiert hat
Aktion	Aktionen, die der Scan ausgeführt hat

Entfernungen anzeigen

Eine erweiterbare Tabelle, die die geplanten Massenänderungen an Skripterstellungsberechtigungen enthält. Dies wird entweder von ausgefüllt **Scannen Sie nach Skriptanwendern** Widget oder mit **Manuelle Konfiguration** .

Felder der Entfernungstabelle

Bezeichnung	Beschreibung
Nummer des Entfernungsauftrags	Die Nummer-ID des Entfernungsauftrags.
Status	Status des Entfernungsauftrags
Abgeschlossen	Abschlussstatus des Entfernungsauftrags
Geplant	Planen Sie die Ausführungszeit für den Entfernungsauftrag
Erstellt von	Anwender, der den Entfernungsauftrag initiiert hat

Zugriffssteuerungen für Rechneridentität

Definieren und erzwingen Sie granulare Zugriffssteuerungsrichtlinien für bestimmte Ressourcen für Integration Anwender.

Mit den Zugriffssteuerungen für die Rechneridentität können Administratoren granulare Zugriffssteuerungsrichtlinien für Integrationsanwender erstellen. Diese zusätzliche Sicherheitsebene ermöglicht es Administratoren, die genauen Ressourcen (REST APIs,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SOAP APIs und Tabellen) anzugeben, auf die ein Integrationsanwender zugreifen kann, wodurch eine engere Zugriffssteuerung sichergestellt wird.

Hinweis: Gilt nur für Anwender, die mit Webservicezugriff gekennzeichnet sind.

Siehe Erstellen Sie eine Zugriffssteuerung für die Rechneridentität Um zu erfahren, wie Sie eine Zugriffssteuerung für die Rechneridentität erstellen

Erstellen Sie eine Zugriffssteuerung für die Rechneridentität

Ermöglichen Sie Administratoren, granulare Steuerungen für Integrationsanwender zu definieren und durchzusetzen, indem Sie Anwenderzugriffsprofile einführen. Diese Funktion bietet eine zusätzliche Sicherheits- und Kontrollebene, sodass Administratoren die genauen Ressourcen (REST-APIs und SOAP-APIs) angeben können, auf die ein Integrationsanwender zugreifen kann, wodurch eine engere Governance sichergestellt und Sicherheitsrisiken minimiert werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffssteuerungen für Rechneridentität**an.
2. Wählen Sie aus **Neu** Schaltfläche.
3. Füllen Sie die Felder des Formulars aus.

Felder für die Zugriffssteuerung für Rechneridentität

Feld	Beschreibung
Name	Name des Zugriffssteuerungsdatensatzes.
Anwendung	Anwendung, die den Datensatz enthält.
Beschreibung	Beschreibung des Datensatzes.
Aktiv	Bestimmt, ob die Richtlinie aktiv ist
REST API-Richtlinie	Wählen Sie die Ziel-REST API-Richtlinie aus. **Hinweis:** Wählen Sie aus Und Symbol zum Hinzufügen einer Richtlinie.
SOAP-API-Richtlinie	Wählen Sie die Ziel-SOAP-API-Richtlinie aus. **Hinweis:** Wählen Sie aus Und Symbol zum Hinzufügen einer Richtlinie.
Tabellen	Wählen Sie die Tabellen aus, für die diese Richtlinie gilt
Gilt für untergeordnete Tabelle	Aktivieren Sie diese Option, um die Richtlinie auf untergeordnete Tabellen von anzuwenden **Tabellen** Feld

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

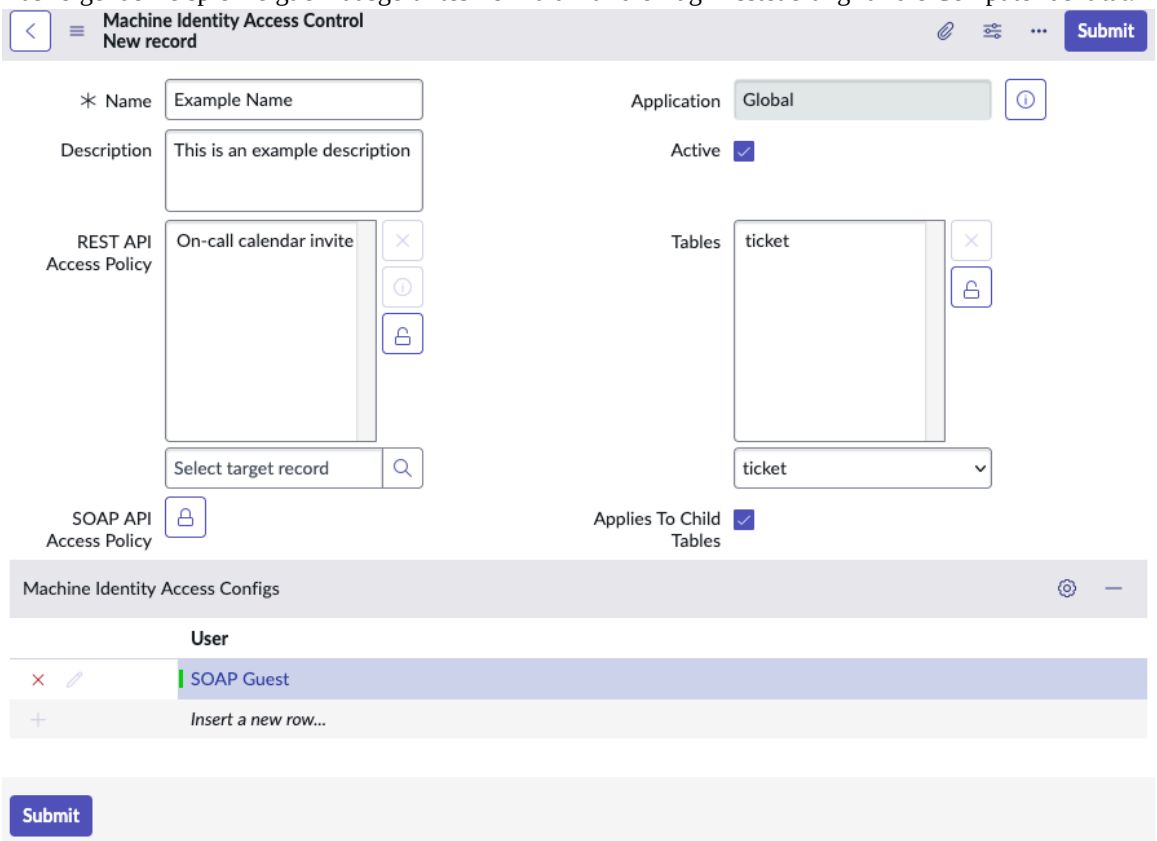
4. Wählen Sie aus Fügen Sie unten eine Zeile ein Fordern Sie Anwender auf, und fügen Sie sie hinzu, auf die die Steuerung angewendet werden soll.
   Sie können der Zugriffssteuerung mehrere Anwender hinzufügen.

   Hinweis: Sie können nur Anwender mit Webservice-Zugriff auswählen.

5. Wählen Sie **Absenden**.

Ergebnis

Das folgende Beispiel zeigt ein ausgefülltes Formular für die Zugriffssteuerung für die Computeridentität:



Ein Anwender mit einer Computeridentitätszugriffssteuerung kann nicht auf andere APIs (REST oder SOAP) zugreifen und kann nur auf die Ressourcen zugreifen, die explizit in der Zugriffssteuerung angegeben sind, auch wenn er über die erforderlichen Rollen verfügt.

Datenfilterung

Verwenden Sie die Datenfilterung, um bei Leseabfragen den Zugriff auf Tabellen und Datensätze basierend auf Themenattributen zu steuern.

Wichtig:

Beginnend mit Yokohama Release, Datenfilterung wird für zukünftige Veraltet vorbereitet. Sie wird ausgeblendet und in neuen Instanzen nicht mehr aktiviert. Erwägen Sie die Verwendung von Sicherheitsdatenfiltern, um den Zugriff auf Datensätze basierend auf Rollen- oder sicherheitsattributbezogenen Assertionen zu beschränken. Nähere Informationen hierzu finden Sie unter Erstellen Sie einen Sicherheitsdatenfilter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie die Datenfilterung



Erfahren Sie mehr über Datenfilterung.

Erstellen Sie Datenfilterungsregeln



Erstellen Sie Ihre eigenen Datenfilterungsregeln, die Ihren Anforderungen entsprechen.

Debug-Daten



Erfahren Sie, wie Sie Ihre Datenfilterungsergebnisse debuggen.

Erkunden Sie die Datenfilterung

Verwenden Sie Datenfilterung, um den Zugriff auf Tabellen und Datensätze basierend auf Betreffattributen bei Leseabfragen zu steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Datenfilterung ist eine separate Form der Zugriffssteuerung, die mit den vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz kompatibel ist. Die Datenfilterung verweigert den Zugriff auf Tabellen und Datensätze, die nicht mit den von einem Administrator definierten Betreffattributen übereinstimmen. Die Datenfilterung soll Audits, Berichterstellung und Problembehandlung erleichtern.

Dies ist eine optionale Funktion, die Administratoren auf ihrer Instanz aktivieren können.

Datenfilterfunktionen

Datenfilter

Verwenden Sie Datenfilter, um Zugriff basierend auf Informationen in einem Datensatz zu gewähren. Datenfilter verwenden Daten in einem Tabellenfeld, um zu bestimmen, ob ein Datensatz für Ihre Anwender verfügbar ist.

Bedingungsgenerator auf Betreffattribut

Verwenden Sie Betreffattribute, um Anwenderrolle, Gruppe, Betreffkriterien oder IP-Netzwerkadresse zu bewerten.

Die Datenfilterung verwendet ein Deny-basiertes Modell

Die Datenfilterung verwendet ein Deny-basiertes Modell, um den Zugriff auf Datensätze zu steuern. Mit der Datenfiltration verweigert Ihre Instanz den Zugriff auf Datensätze, es sei denn, ein Datensatz erfüllt die von der Datenfiltration definierten Kriterien.

Durchsetzung der Datenfilterung

Datenfilterregeln werden nach der Datenbankabfrage für Lesevorgänge ausgeführt und vor ACLs ausgewertet. Ein Datensatz, der von einer Datenfilterregel abgelehnt wurde, wird nicht fortgesetzt und wird durch ACL-Regeln ausgewertet. Die Durchsetzung der Datenfilterregel stimmt mit der von Lese-ACLs überein.

Datenfilterung und Berichterstellung

Datenfilterung und ACLs werden nur beim Erstellen von Listenansichtsberichten angewendet. Beim Reporting wird keine Zugriffssteuerung angewendet, wenn zusammengefasste Daten erfasst werden. In diesem Fall werden weder Datenfilterung noch ACLs überprüft.

Für zusammengefasste Berichte funktioniert die Datenfilterung in Verbindung mit vorhandenen *`Report_view access control list`*Verhalten. Siehe Zugriffssteuerung „Report_View“ Weitere Details zum Konfigurieren dieser Berichtssteuerungen.

Sitzungs-Debugging

Die Datenfilterung unterstützt das Sitzungs-Debugging. Verwenden Sie Sitzungs-Debugging, um zu sehen, welche Datenfilterdatensätze für eine bestimmte Abfrage gelten. Administratoren können diese Informationen verwenden, um Probleme mit dem Anwenderzugriff auf Datensätze zu beheben.

Komponenten der Datenfilterung

Die Datenfilterung funktioniert mit den folgenden Datensatztypen:

Datenfilterungsdatensätze

Erstellen Sie einen Datensatz für die Datenfilterung [sys_df_Data_Filtration], um Tabellenzugriff auf Ihre Instanz zu gewähren. Der Datenfilterdatensatz enthält **Datenfilter** Und **Betreffattribut** Oben beschriebene Bedingungen, um den Umfang der Regel und die betroffenen Anwender zu begrenzen.

Datensätze der Betreffkriterien

Automatische Übersetzung

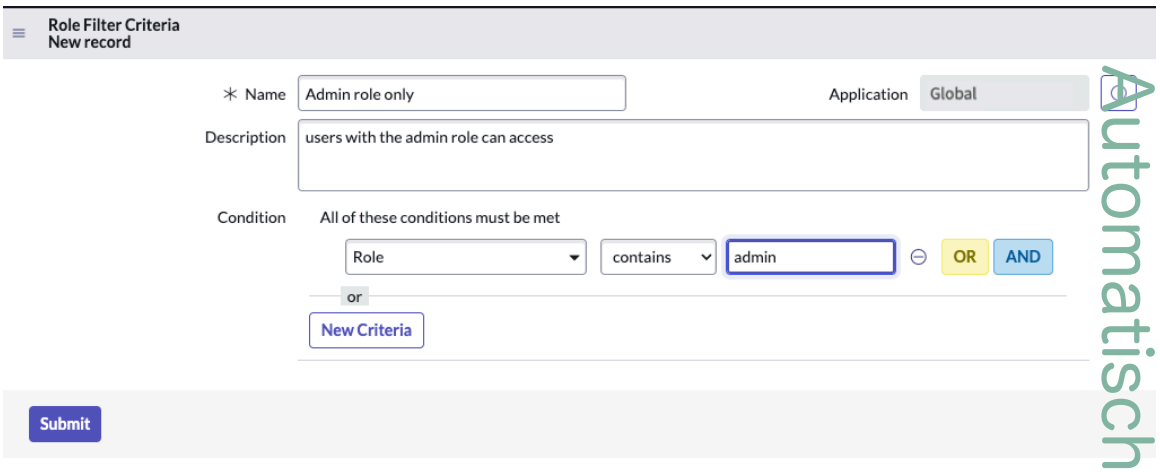
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensätze für Betreffkriterien [sys_df_subject_Criteria] stellen bestimmte Anwenderattribute dar, mit denen Sie bestimmen können, ob Sie Zugriff mit einer Datenfilterregel gewähren möchten. Diese Attribute können die Gruppen, Rollen oder IP-Adresse eines Anwenders sein. Um Betreffkriterien zu erstellen, müssen Sie den Betreffkriteriendatensatz sowie Kriterieneingabe- und Kriterienbedingungsdatensätze erstellen. Details zu diesem Vorgang finden Sie unter Erstellen Sie Betreffkriterien.

Nachdem Sie Datensätze für Betreffkriterien erstellt haben, können Sie sie auf eine Regel anwenden. Dies wird auf durchgeführt **Betreffbedingung** Registerkarte Ihrer Datenfilterregel.

Beispiele für Kriterieneingabedatensätze

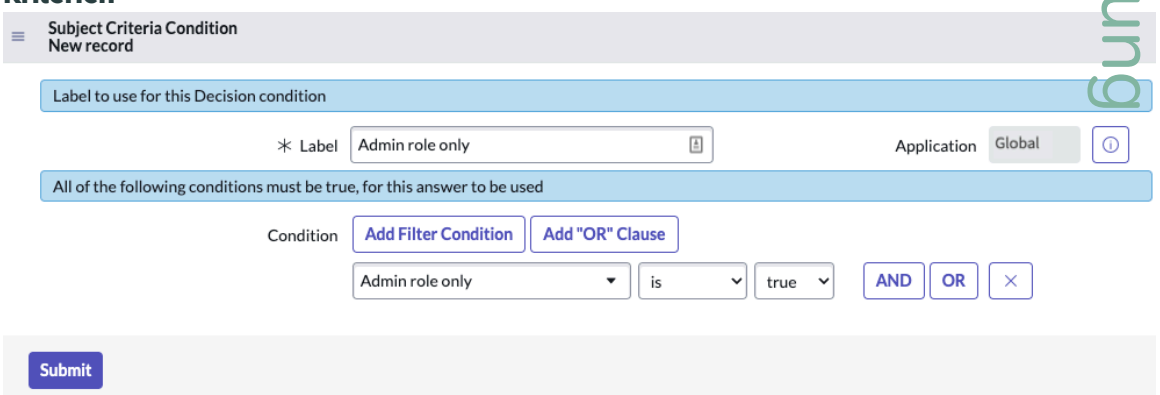
Beispielkriterieneingabe für alle Rollen, die den Administrator enthalten



Kriterieneingaben [sys_df_subject_Filter_Criteria_m2m] sind Datensätze, die Kriterien zum Vergleich mit dem Anwender enthalten. Dies kann eine Liste von Anwendergruppen oder -Rollen, ein IP-Adressbereich oder ein IP-Adressensubnetz sein. Diese Datensätze werden zusammen mit Betreffkriterien-Bedingungsdatensätzen verwendet, um die Gruppen, Rollen oder IP-Adresse eines Anwenders zu bewerten, um den Zugriff auf eine Tabelle oder ihre Datensätze zu bestimmen.

Bedingungsdatensätze für Betreffkriterien

Beispielkriterienbedingung mit der Eingabe nur Administratoren-Kriterien



Verwenden Sie Datensätze für Betreffkriterienbedingung [sys_df_subject_Criteria_condition], um zu definieren, wie Anwenderattribute mit den Rollen, Gruppen oder IP-Adressen verglichen werden, die in den Kriterieneingaben definiert sind. Sie können mehrere Kriterieneingaben in einer einzelnen Betreffkriterienbedingung verwenden, um den Zugriff auf Ihre Datensätze weiter einzugrenzen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie die Datenfilterung

Erfahren Sie, wie Sie die Datenfilterung in Ihrer Instanz aktivieren.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.
2. Verwenden Sie das Suchfeld, um das Plugin „Datenfiltration“ (com.Glide.Data_Filtration) zu finden.
3. Klicken Sie auf **Installieren**, und klicken Sie dann im Dialogfeld „Plugin aktivieren“ auf **Aktivieren**.

Erstellen Sie Datenfilterungsregeln

Erfahren Sie, wie Sie Datenfilterungsregeln erstellen, um Ihren Anwendern Zugriff auf Tabellen mit Datensätzen zu gewähren.

Vorbereitungen

Erforderliche Rolle: security_admin

Hinweis: Um Datenfilterungsregeln zu erstellen oder zu ändern, müssen Sie auf die privilegierte Rolle hochstufen. Weitere Informationen zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle hochstufen .

Prozedur

1. Navigieren zu **Alle** > **Datenfilterung** > **Datensätze der Datenfilterung**an.
2. Klicken Sie Auf **Neu** In **Datenfilterung** Liste.
   Ein neues Datenfilterformular wird angezeigt.
3. Füllen Sie die Felder im Formular nach Bedarf aus.

Formular „Datenfilterung“

Feld	Beschreibung
Tabelle	Tabelle, für die diese Datenfilterregel gilt. **Hinweis:** Nicht-Wartungsanwender können für einige Tabellen keine Datenfilterung erstellen. Um dies zu umgehen, entfernen Sie das Attribut tableChoicesScript=DataFiltrationTableList. Stellen Sie jedoch sicher, dass keine Filter für eine der sys_df_xxx-Tabellen oder für eine Tabelle in sys_df_table_Exclusion erstellt werden.
Aktiv	Legt die Datenfilterregel als aktiv fest. **Hinweis:** Lassen Sie Datenfilterregeln inaktiv, bis Sie zum Testen bereit sind, um zu vermeiden, dass Anwender unbeabsichtigt aus Datensätzen gesperrt werden.
Beschreibung	Beschreibung der Datenfilterregel.
Kaskadierend	Wählen Sie diese Option aus, um festzulegen, dass die Datenfilterregel auf erweiterte Tabellen angewendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie wählen beispielsweise die Tabelle „Aufgabe“ [Aufgabe] aus, und aktivieren die Kaskadierung. In diesem Fall gilt die Datenfilterregel auch für alle Tabellen, die aus der Aufgabe erweitert wurden, z. B. Incident[Incident] und Change-Anforderung[Change_Request]. Weitere Informationen zur Tabellenerweiterung finden Sie unter Tabellenerweiterung und -Klassen **Hinweis:** Dieses Feld ist standardmäßig aktiviert.

4. **Wahlweise:** Um den Umfang der Regel einzugrenzen, füllen Sie aus **Bedingungen** Felder nach Bedarf.

Feld	Beschreibung
Betreffbedingung	Für den Zugriff müssen alle Bedingungen erfüllt sein.
Bedingung des Sicherheitsattributs	Für den Zugriff müssen alle Bedingungen erfüllt sein. **Gebietsschema** Das Attribut ist nur im Umfang der Datenfilterregel definiert. **Ist vorhanden** Das Attribut wird durch Verweis auf ein bereits vorhandenes definiert **Sicherheitsattribut**
Datenbedingung	Definiert die Bedingungen für Daten, die der Regel unterliegen sollen. **Hinweis:** Eine leere Datenbedingung gilt für alle Datensätze in der ausgewählten Tabelle.

5. Wählen Sie Aus **Speichern** Aus dem Formularmenü.
   Nachdem Sie Ihre Datenfilterregel gespeichert haben, gilt diese Regel automatisch für alle Datensätze in der ausgewählten Tabelle, sofern nicht anders durch die Datenbedingung angegeben.

Fügen Sie einen Datenfilter für Ihre Datenfilterregel hinzu

Sie können optional einen Datenfilter verwenden, um den Umfang Ihrer Datenfilterregel so einzugrenzen, dass sie nur auf bestimmte Datensätze in einer Tabelle angewendet wird.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

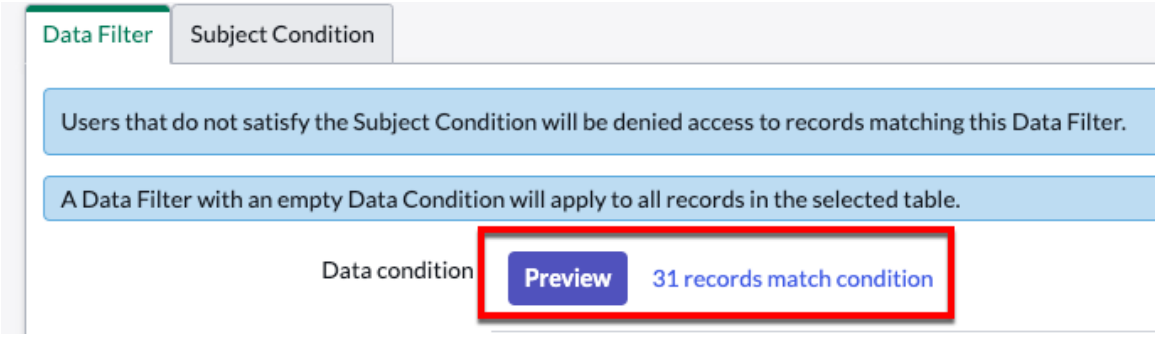
1. Öffnen Sie in Ihrem Datenfilterdatensatz **Datenfilter** Registerkarte.
2. Verwenden Sie den Bedingungsgenerator, um die Feldwerte der Tabellendatensätze zu filtern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Datenfilter verwendet denselben Bedingungsgenerator, der in anderen Teilen der Plattform verwendet wird. Weitere Informationen zur Verwendung dieser Schnittstelle finden Sie unter Bedingungsgenerator .

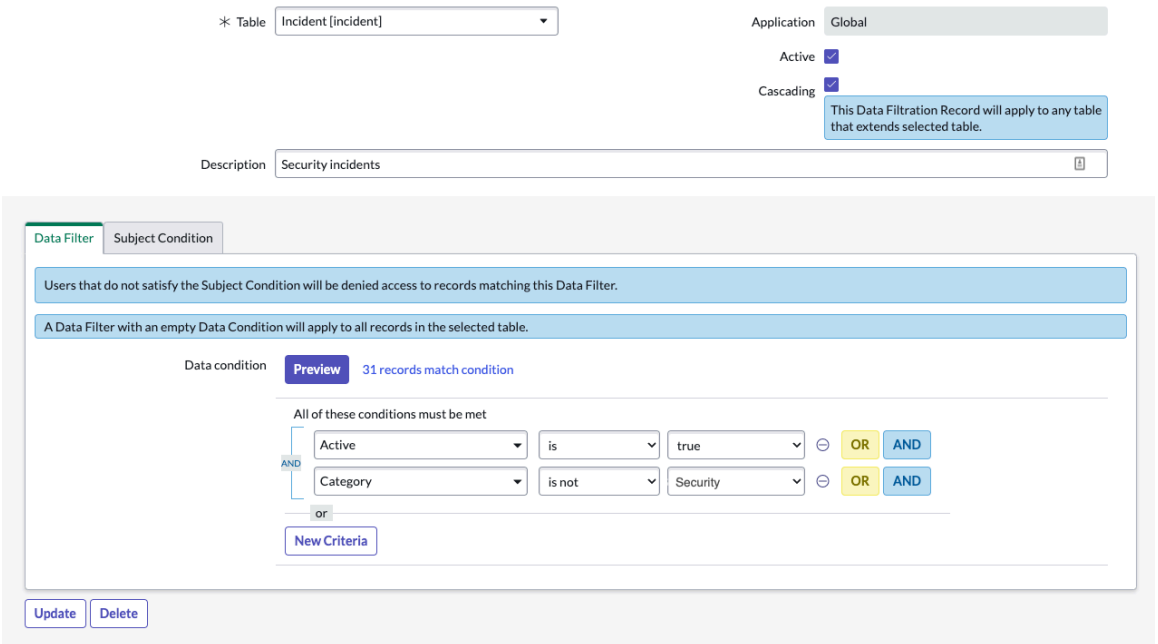
Wichtig: Die **Datenfilter** Die Registerkarte wird leer angezeigt, bis Sie eine Tabelle in auswählen **Tabelle** Feld.

3. Verwenden Sie **Vorschau** Schaltfläche, um die Anzahl der Datensätze anzuzeigen, die mit Ihrem Datenfilter übereinstimmen.
4. Wählen Sie die Anzahl der Datensätze aus, um eine Liste der übereinstimmenden Datensätze zu öffnen.



5. Wählen Sie **Speichern**.

Example:
Dieses Beispiel zeigt eine Datenfilterregel für die Tabelle „Incident“ [Incident]. Der Datenfilter ist so festgelegt, dass alle aktiven Datensätze ausgewählt werden, die sich nicht in befinden **Sicherheit** Kategorie. Wenn diese Regel aktiv ist, können Anwender diese Datensätze anzeigen. Im folgenden Abschnitt finden Sie weitere Informationen zur Verwendung von Kriterien außerhalb des Inhalts des Datensatzes.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Die **Nicht** Der Vorgang unter Ihren Bedingungen kann je nach Datenbanktyp, den Ihre Instanz verwendet, unerwartete Ergebnisse zurückgeben. Nehmen Sie beispielsweise die folgende Bedingung:

Für diese Bedingung wäre das erwartete Ergebnis, dass der Ergebnissatz alle Datensätze enthält, bei denen sich das Unternehmen nicht befindet ServiceNow Und alle Datensätze, die keinen Wert in haben **Unternehmen** Feld. Instanzen, die andere Datenbanken als MySQL und Maria verwenden, geben keine Wertdatensätze mit einem leeren zurück **Unternehmen** Feld. Bei Verwendung von **Nicht** Abfragen für diese Instanzen enthalten Bedingungen, um sicherzustellen, dass leere Werte zurückgegeben werden.

Fügen Sie Ihrer Datenfilterregel Betreffattribute hinzu

Verwenden Sie optional Betreffattribute, um den Umfang Ihrer Datenfilterregel basierend auf Attributen wie IP-Netzwerkadresse, Anwendergruppen und Rollen oder Betreffkriterien einzugrenzen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie in Ihrem Datenfilterdatensatz **Betreffkriterien** Registerkarte.
2. Verwenden Sie den Bedingungsgenerator, um die Tabellendatensätze basierend auf einem oder mehreren der folgenden Kriterien zu filtern.

Optionen für Betreffkriterien

Option	Beschreibung
Netzwerkkriterien	Ermöglicht den Zugriff auf Datensätze basierend auf dem Netzwerk-IP-Bereich oder dem IP-Subnetz.
Betreffkriterien	Ermöglicht den Zugriff auf Datensätze basierend auf Betreffkriterien. Wählen Sie einen Betreffkriteriendatensatz aus, um seine Bedingungen auf Ihre Datenfilterregel anzuwenden. Details zum Erstellen von Betreffkriterien-Datensätzen finden Sie unter Erstellen Sie Betreffkriterien.
Betreffgruppe	Zugriff zulassen, wenn der Anwender Mitglied einer bestimmten Gruppe ist. Wählen Sie eine Gruppe aus dem aus **Gruppen** Tabelle [sys_user_Group].
Betreffrolle	Zugriff zulassen, wenn der Anwender Mitglied einer bestimmten Gruppe ist. Wählen Sie eine Gruppe aus dem aus **Rollen** Tabelle [sys_user_role].

Wichtig: Betreffkriterienbedingungen unterstützen nur **Ist** Operator.

3. Klicken Sie nach dem Hinzufügen Ihrer Betreffkriterien auf **Speichern** .

Erstellen Sie Betreffkriterien

Erstellen Sie Datensätze für Betreffkriterien zur Verwendung in Datenfilterregeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: security_admin

Wichtig: Um Datenfilterungsregeln zu erstellen oder zu ändern, müssen Sie auf eine privilegierte Rolle hochstufen. Weitere Informationen zu diesem Prozess finden Sie unter Auf eine privilegierte Rolle hochstufen .

Prozedur

1. Navigieren zu **Alle** > **Datenfilterung** > **Betreffkriterien**an.
2. In **Betreffkriterien** Klicken Sie auf die Liste **Neu** Schaltfläche.
   Ein neues Betreffkriterienformular wird angezeigt.
3. Füllen Sie die Felder im Formular nach Bedarf aus.

Betreffkriterienfelder

Feld	Beschreibung
Name	Name für die Betreffkriterien.
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung ausgefüllt.
Beschreibung	Beschreibung für die Betreffkriterien.

4. Klicken Sie mit der rechten Maustaste auf den Formularheader, und klicken Sie auf **Speichern** Aus dem Kontextmenü.
   Nach dem Speichern wird die **Kriterieneingaben** Und **Kriterienbedingungen** Felder werden angezeigt.

Erstellen Sie eine Betreffkriterieneingabe

Erstellen Sie eine Betreffkriterieneingabe, um Kriterien zu definieren, nach denen Ihre Datenfilterregeln filtern.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Öffnen Sie in Ihrem Betreffkriteriendatensatz **Kriterieneingaben** Registerkarte.
2. In **Kriterieneingaben** Liste, klicken Sie auf **Neu** .
3. Wählen Sie die Richtlinieneingabe für die Kriterien aus, die Sie erstellen möchten.

Richtlinieneingaben

Richtlinieneingabe	Beschreibung
IP-Filterkriterien	Erstellen Sie eine Richtlinieneingabe basierend auf der IP-Adresse
Rollenfilterkriterien	Erstellen Sie eine Richtlinieneingabe basierend auf der Rolle „Verwenden“
Gruppenfilterkriterien	Erstellen Sie eine Richtlinieneingabe basierend auf der Anwendergruppe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

A **IP-Filterkriterien** , **Rollenfilterkriterien** , Oder **Gruppenfilterkriterien** Das Formular wird je nach Auswahl in diesem Schritt angezeigt.

4. Füllen Sie die Felder im Formular „Filterkriterien“ nach Bedarf aus.

Filterkriterienfelder

Feld	Beschreibung
Name	Name für die Filterkriterien
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung ausgefüllt.
Beschreibung	Beschreibung der Filterkriterien

5. Unter den Formularfeldern befinden sich Registerkarten, die zum Definieren der IP-Adressen, Gruppen oder Rollen für die Filterkriterieneingaben verwendet werden.

Filterkriterienfelder für bestimmte Eingabetypen

Richtlinieneing	Beschreibung	Erstellung
IP-Filterkriterien	IP-Filterkriterien des Anwenders zum Erstellen eines Bereichs oder Subnetzes von IP-Adressen. Ihre Betreffkriterien können dann mit der IP-Adresse des Anwenders mit diesem Bereich oder Subnetz verglichen werden.	Verwenden Sie **IP-Bereich** Oder **Subnetz (CIDR)** Zum Definieren von IP-Adressen für Ihre Eingabe. **IP-Bereich** In **IP-Bereiche** Liste, doppelklicken Sie auf **Fügen Sie eine neue Zeile ein** , Und geben Sie eine IP-Startadresse in ein **Start-IP** . Drücken Sie dann die Tabulatortaste, und geben Sie eine IP-Endadresse in ein **End-IP** Feld. Drücken Sie abschließend die Eingabetaste, um den Listeneintrag zu speichern. **Subnetz (CIDR)** In **Subnetze** Liste, doppelklicken Sie auf **Fügen Sie eine neue Zeile ein** , Und geben Sie eine Netzwerk-IP in ein **Netzwerk-IP** Feld. Drücken Sie dann die Tabulatortaste, und geben Sie eine Netzmaske in ein **Netzmaske** Feld. Drücken Sie abschließend die Eingabetaste, um den Listeneintrag zu speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinieneing	Beschreibung	Erstellung
		Hinweis: Geplante Aufgaben, die von einem Planer ausgelöst werden, sind nicht dafür vorgesehen, Daten anhand von Netzwerkkriterien zu filtern, da sie nicht den Kontext der anfordernden Client-IP haben. Eine geeignetere Art der Filterung kann die Betreffbedingung für Rollen/Gruppen sein.
Rollenfilterkriterien	Verwenden Sie Rollenfilterkriterien, um eine Auswahl von Rollen zu erstellen. Ihre Betreffkriterien können dann mit den zugewiesenen Rollen des Anwenders für diese Auswahl verglichen werden.	Verwenden Sie den Bedingungsgenerator in **Bedingungsfeld** Um Rollen für Ihre Eingabe auszuwählen.
Gruppenfilterkriterien	Verwenden Sie Gruppenfilterkriterien, um eine Auswahl von Anwendergruppen zu erstellen. Ihre Betreffkriterien können dann mit den zugewiesenen Gruppen des Anwenders verglichen werden.	In **Gruppen für Kriterien** Tabelle, doppelklicken Sie auf **Fügen Sie eine neue Zeile ein** , Und wählen Sie eine Anwendergruppe aus. Drücken Sie die Eingabetaste, oder klicken Sie auf das grüne Häkchensymbol, um die Gruppe zu speichern. Klicken Sie auf **Fügen Sie eine neue Zeile ein** Text unter dem ersten Eintrag zum Erstellen zusätzlicher Einträge.

6. Nachdem Sie Ihre Eingabe definiert haben, klicken Sie auf **Übermitteln** .

Hinweis: Sie können nicht nur Kriterieneingaben für Ihre Betreffkriterien erstellen, sondern auch vorhandene hinzufügen. Klicken Sie Auf **Bearbeiten** In **Kriterieneingaben** Und wählen Sie aus einer vorhandenen Eingabe aus.

Erstellen Sie eine Betreffkriterienbedingung

Erstellen Sie eine Bedingung, um Anwenderinformationen mit vorhandenen Betreffkriterieneingaben zu vergleichen.

Vorbereitungen

Erforderliche Rolle: security_admin

Kriterienbedingungen vergleichen Anwenderattribute mit vorhandenen Kriterieneingaben, um zu bestimmen, ob der Zugriff auf Datensätze zugelassen werden soll. Um eine Kriterienbedingung zu erstellen, müssen Sie Betreffkriterien erstellt haben. Details zu diesem Prozess finden Sie unter . Erstellen Sie eine Betreffkriterieneingabe.

Prozedur

1. Öffnen Sie in Ihrem Betreffkriteriendatensatz **Kriterienbedingungen** Registerkarte.
2. In **Kriterienbedingungen** Liste, klicken Sie auf **Neu** .
3. Auf der **Betreffkriterienbedingung** Füllen Sie die Felder nach Bedarf aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Betreffkriterien-Bedingung“

Feld	Beschreibung
Bezeichnung	Eine beschreibende Bezeichnung für Ihre Bedingung
Anwendung	Bereichsbezogene Anwendung für die Betreffkriterien. Dieses Feld ist schreibgeschützt und wird automatisch mit der aktuellen bereichsbezogenen Anwendung ausgefüllt.

4. Erstellen Sie mit dem Bedingungsgenerator eine Bedingung für Ihre Betreffkriterienbedingung, indem Sie aus den folgenden Bedingungsoptionen auswählen.
   Diese Bedingungsoptionen enthalten alle Eingaben für Betreffkriterien, die Sie erstellt haben.
5. **Wahlweise:** Erstellen Sie weitere Bedingungen, indem Sie auf klicken **Fügen Sie eine Filterbedingung hinzu** Oder **Fügen Sie die Klausel „ODER“ hinzu** Schaltflächen.

   Hinweis: Es sei denn, Ihre Bedingungen sind durch getrennt **Oder** Klausel, alle Bedingungen müssen als „wahr“ ausgewertet werden, damit die Betreffkriterienbedingung als „wahr“ ausgewertet wird.

6. Klicken Sie Auf **Übermitteln** Zum Speichern der Betreffkriterienbedingung.

Nächste Maßnahme

Verwenden Sie Betreffkriterien in Ihren Datenfilterregeln, um den Zugriff auf Tabellen und Datensätze zu beschränken. Weitere Informationen zur Verwendung von Betreffkriterien in Datenfilterregeln finden Sie unter Erstellen Sie Betreffkriterien.

Debugging der Datenfiltration

Verwenden Sie das Sitzungsprotokoll, um zu sehen, wie sich die Datenfilterung auf Ihre Datensätze auswirkt, und um Anwenderzugriffsprobleme zu debuggen.

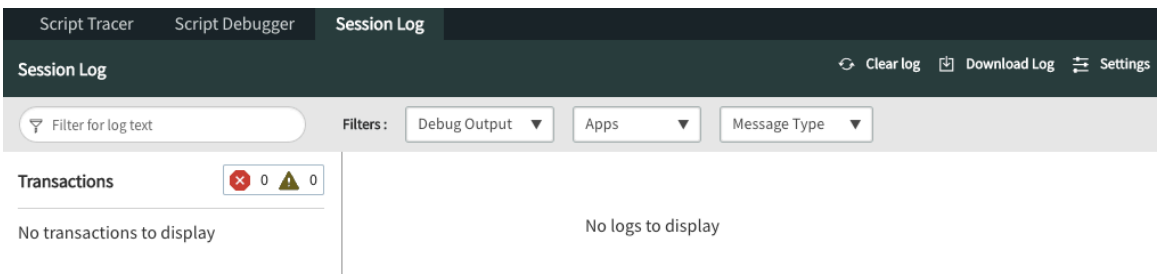
Vorbereitungen

Erforderliche Rolle: Administrator

Ausgabeinformationen werden in den Sitzungsprotokollen angezeigt, wenn Anwender auf Datensätze zugreifen. Sie können diese Protokollierungsinformationen zusammen mit Identitätswechsel verwenden, um zu erfahren, warum Anwender Datensätze sehen oder nicht sehen. Sie können diese Informationen dann verwenden, um Ihre Datenfilterregeln anzupassen und sicherzustellen, dass Anwender nur sehen, was Sie beabsichtigen.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Debugging** > **Alle Sicherheitseinstellungen debuggen**an.
   Die **Skript-Debugger** Wird in einer neuen Browserregisterkarte oder einem neuen Browserfenster geöffnet.



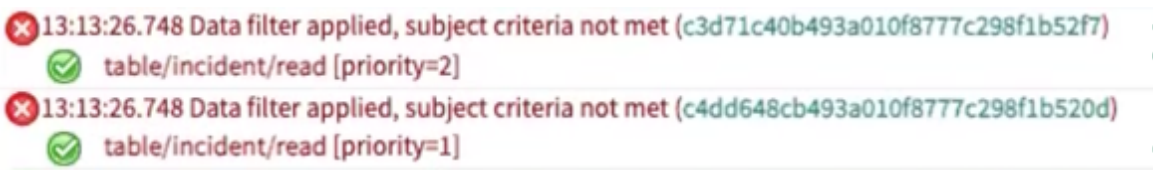
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. In **Skript-Debugger** Wählen Sie im Fenster aus **Sitzungsprotokoll** Registerkarte.
3. Geben Sie auf einer anderen Browserregisterkarte oder einem anderen Browserfenster die Identität eines Anwenders an, um Probleme mit dem Zugriff dieses Anwenders zu beheben.

   Hinweis: Durch die Identitätswechsel kann ein Administrator eine Instanz mit Einstellungen und Zugriff anderer Anwender sehen. Weitere Informationen zum Identitätswechsel finden Sie unter Identität eines Anwenders annehmen .

4. Greifen Sie beim Identitätswechsel eines Anwenders auf eine Liste oder einen Datensatz zu, in der Sie unerwartetes Verhalten sehen.
   Dieses Verhalten kann ein Datensatz sein, den der Anwender sieht, aber nicht sehen sollte, oder eine Liste von Datensätzen, die für einen Anwender nicht wie erwartet angezeigt werden.
   Nachdem Sie mit dem Anwender, dessen Identität angenommen wurde, auf Datensätze zugegriffen haben, sollten Sie die Ausgabe im Sitzungs-Debugger anzeigen.
5. Suchen Sie im Sitzungs-Debugger nach Informationen zur Datenfilterung.



   Dieses Beispiel zeigt zwei Protokollnachrichten, bei denen ein Datenfilter den Zugriff auf Datensätze verweigert hat. Die Protokolleinträge werden als roter Text angezeigt und enthalten die Gründe, warum der Datenfilter den Zugriff verweigert hat, sowie die sys_ID des Datenfilters. Sie können auf diese sys_ID klicken, um den Datenfilterdatensatz zu öffnen.



   Dieses Beispiel zeigt eine Protokollnachricht, in der ein Datenfilter den Zugriff auf einen Datensatz ermöglicht hat. Diese Protokolleinträge werden als grüner Text angezeigt. Wie bei der ersten Nachricht können Sie auf diese sys_ID klicken, um den Datenfilterdatensatz zu öffnen.

6. Verwenden Sie diese Informationen, um Anpassungen an Ihren Datenfilterregeln vorzunehmen. Wiederholen Sie diese Schritte, um Ihre Regeln zu verfeinern und Anwendern den benötigten Zugriff zu gewähren.

Sicherheitsdatenfilter

Sicherheitsdatenfilter schränken den Zugriff auf Datensätze basierend auf Rollen- oder sicherheitsattributbezogenen Assertionen ein.

Sicherheitsdatenfilter erkunden

Sicherheitsdatenfilter ermöglichen die Zugriffsbeschränkung auf Datensätze basierend auf der Rolle eines Anwenders oder anderen Assertions im Zusammenhang mit Sicherheitsattributen. Sicherheitsdatenfilter stellen sicher, dass nur autorisierte Anwender Datensätze anzeigen können, unabhängig davon, wie auf Daten zugegriffen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsdatenfilter werden angewendet, bevor eine Abfrage ausgeführt wird, sodass eingeschränkte Daten die Datenbank nie verlassen. Im Gegensatz dazu Bedingte ACLs Filtern Sie Daten, nachdem eine Abfrage ausgeführt wurde, möglicherweise undichte Daten.

Hinweis: Koppeln Sie Sicherheitsdatenfilter mit Verweigern – außer ACL Um eine konsistente Sicherheit zu gewährleisten

Funktionen von Sicherheitsdatenfiltern

Die wichtigsten Funktionen von Sicherheitsdatenfiltern sind:

- Sicherheitsdatenfilter werden in der Abfrage angewendet.
- Filterbedingungen für Sicherheitsdaten UND Zur Abfrage in der Zieltabelle und miteinander.
- Sicherheitsdatenfilter werden nicht von überprüft `CanRead` . Siehe Wann Sicherheitsdatenfilter verwendet werden sollen Für weitere Details
- Umfangsregeln für Datenfilter basieren auf dem Umfang der Tabelle. Datenfilter entsprechen nicht den Umfangsregeln für ScopeMaster oder sys_scope

Anwendung und Durchsetzung des Sicherheitsdatenfilters

Im Allgemeinen werden Sicherheitsdatenfilter nach absoluten ACLs (auch als ACLs auf Tabellenebene bezeichnet) und nach Zeilen-ACLs angewendet. Sicherheitsdatenfilter werden standardmäßig angewendet und wirken sich auf das Systemverhalten aus, wenn sie nicht sorgfältig verwendet werden. Siehe Standardsicherheitsfilter Für eine Liste der standardmäßigen Sicherheitsdatenfilter.

Sicherheitsdatenfilter werden standardmäßig nur auf GlideRecordSecure-, GlideRecordSandbox- und GlideAggregateSandbox-Abfragen angewendet. Es gibt zwei neue GlideRecord-APIs EnableSecurityFeature Und Deaktivieren Sie die Sicherheitsfunktion Das sowohl in Java- als auch serverseitigen Skripts verwendet werden kann, um Datenfilter für eine bestimmte Abfrage zu aktivieren oder zu deaktivieren.

Wichtig: Sie sollten Datenfilter explizit für anwenderorientierte Abfragen aktivieren, die GlideRecordSecure nicht verwenden.

Wann Sicherheitsdatenfilter verwendet werden sollen

Sicherheitsdatenfilter eignen sich am besten für:

- Verhindern Sie, dass vertrauliche Daten die Datenbank verlassen
- Unterdrücken Sie die Meldung „Zeilen durch Sicherheit ausgeblendet“
- Verhindern Sie, dass vertrauliche Daten durch Berichte weitergegeben werden

Wann Sicherheitsdatenfilter nicht verwendet werden sollen

Sicherheitsdatenfilter dürfen nicht verwendet werden:

- Als Sichtbarkeitssteuerung
- Als Ersatz für ACLs
- Mit einer großen Anzahl von Filterbedingungen
- In nicht indizierten Spalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verhalten des Sicherheitsdatenfilters

Mehrere Sicherheitsdatenfilter werden zur Auswertung kombiniert, z. B. `UND` Kombiniert Operanden. Beispiel: Anhand von drei Sicherheitsdatenfiltern:

- Filter 1: „Active=true“
- Filter 2: `Priorität=1`
- Filter 3: `state=Offen`

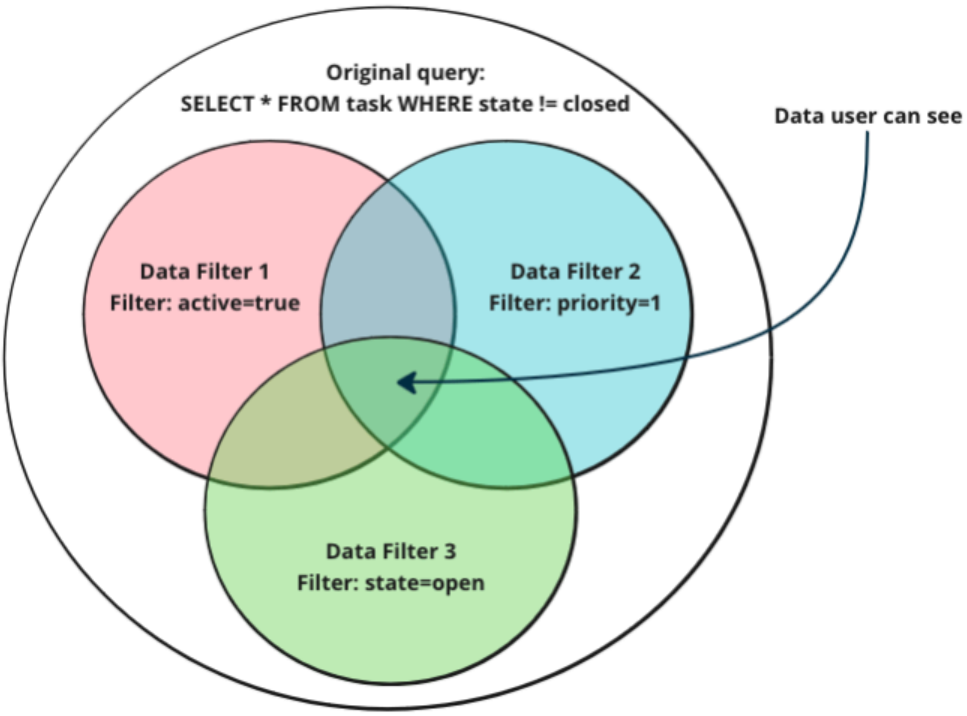
Und eine erste Abfrage:

```
SELECT * FROM task WHERE state != closed AND active = true AND
    priority = 1
```

Die endgültige Abfrage lautet:

```
SELECT * FROM task WHERE state != closed
    AND active = true AND priority = 1 AND state = open
```

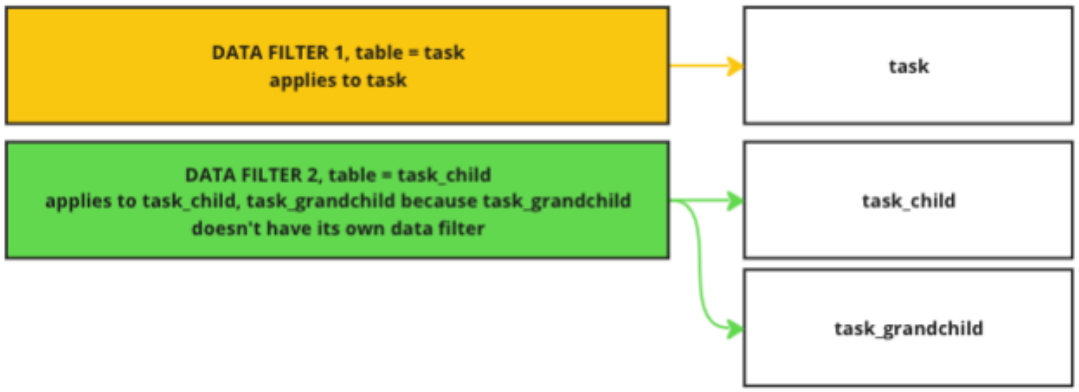
Im folgenden Diagramm finden Sie eine visuelle Darstellung dieses Beispiels:



Ein wichtiger Unterschied bei der Anwendung von Sicherheitsdatenfiltern und ACLs besteht darin, dass Datenfilter in einer untergeordneten Tabelle nicht auf die übergeordnete Tabelle angewendet werden, wenn Daten aus der übergeordneten Tabelle abgefragt werden. Fügen Sie einen Datenfilter für untergeordnete und übergeordnete Tabellen hinzu, um den Zugriff auf Datensätze in der übergeordneten

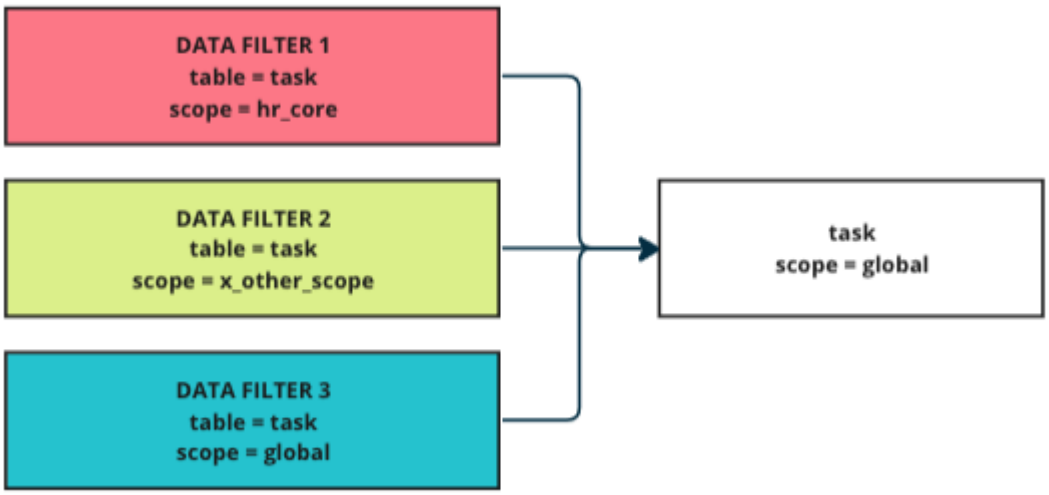
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle zu beschränken. Das folgende Diagramm hebt die Hierarchie hervor:



Hinweis: Eine allgemeine Lösung hierfür besteht darin, dem übergeordneten Element einen Datenfilter hinzuzufügen, der untergeordnete Datensätze in der übergeordneten Tabelle vollständig ausblendet.

Datenfilter werden mit Umfangsregeln angewendet, die ACLs ähnlich sind, jedoch mit einigen wichtigen Unterschieden, da Datenfilter vor der Abfrage angewendet



werden.

Erstellen Sie einen Sicherheitsdatenfilter

Erfahren Sie, wie Sie Sicherheitsdatenfilterregeln erstellen, um Ihren Anwendern Zugriff auf Tabellen mit Datensätzen zu gewähren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Sicherheitsdatenfilter**an.
2. Klicken Sie Auf **Neu** In **Sicherheitsdatenfilter** Liste.
3. Füllen Sie die Felder im Formular nach Bedarf aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Datenfilterung“

Feld	Beschreibung
Tabellenname	Die Tabelle, für die der Sicherheitsdatenfilter gilt.
Beschreibung	Beschreibung der Sicherheitsdatenfilterregel.
Aktiv	Legt die Sicherheitsdatenfilterregel als aktiv fest. **Hinweis:** Lassen Sie Sicherheitsdatenfilterregeln inaktiv, bis Sie zum Testen bereit sind, um zu vermeiden, dass Anwender unbeabsichtigt aus Datensätzen gesperrt werden.
In UI anzeigen	Bestimmt, ob eine Benachrichtigung in der Anwenderoberfläche angezeigt wird, wenn der Sicherheitsdatenfilter für eine Abfrage gilt
Anwendung	Der Anwendungsbereich des Sicherheitsdatenfilters.
Modus	Der Modus des Datenfilters.
Filter	Die Filterbedingung, die bestimmt, für welche Datensätze der Datenfilter gilt
Sicherheitsattribute	Die Sicherheitsattribute, die steuern, ob der Datenfilter angewendet wird oder nicht

4. Wählen Sie Aus **Speichern** Aus dem Formularmenü.

Ergebnis

Nachdem Sie Ihre Sicherheitsdatenfilterregel gespeichert haben, gilt diese Regel automatisch für alle Datensätze in der ausgewählten Tabelle, sofern nicht anders durch die Datenbedingung angegeben.

Standardsicherheitsfilter

Im Allgemeinen werden Datenfilter nach absoluten ACLs (auch als ACLs auf Tabellenebene bezeichnet) und nach ACLs auf Zeilenebene angewendet. Sie werden standardmäßig angewendet und können sich auf das Systemverhalten auswirken, wenn sie nicht sorgfältig verwendet werden.

Standardmäßig angewendete Sicherheitsdatenfilter

Sicherheitsdatenfilter werden standardmäßig auf die folgenden Orte angewendet:

Kategorie	Anwendung
Liste und Formulare	• UI16 • Arbeitsbereiche • Servicekatalog • Serviceportal • Mobil
Berichte und Dashboards	• Berichte • Datenvisualisierungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Anwendung
	• Core-UI-Dashboards • Platform Analytics-Experience-Dashboards
Datenexport	• XML exportieren • CSV • Excel • JSON • PDF
Flow-Engine	Schritte der Datensatzsuche
Suchen	• KI-Suche • Textsuche
GlideRecord	• GlideRecordSecure • GlideRecordSandbox • GlideAggregateSandbox
REST- und GraphQL-APIs	• REST-Tabellen-API • REST-Statistiken-API • Entspricht GraphQL-Tabelle und Statistik-API

Sicherheitsrollen

Sicherheitsrollen bieten zusätzliche Sicherheit. Jeder Anwender muss mindestens eine Rolle haben, damit die Instanz zwischen internen und externen Anwendern unterscheiden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie Explizite Rollen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen expliziter Rollen kennen.

Erweiterte Berechtigung Erkunden



Erfahren Sie, wie die Rolle mit erhöhten Berechtigungen sitzungsbasierte Berechtigungen ermöglicht.

Explizite Rollen

Sie können internen Benutzern und externen Benutzern Zugriff auf Ihre Instanz gewähren. Möglicherweise möchten Sie jedoch nicht, dass beide Benutzertypen dieselben Zugriffsrechte haben. Um die Sicherheit zu erhöhen, muss jeder Benutzer mindestens eine Rolle besitzen, damit die Instanz zwischen internen und externen Benutzern unterscheiden kann.

Ab Release Paris können Benutzer nicht mehr beide expliziten Rollen (snc_internal und snc_external) haben. Auch durch Gruppen- und Rolleneinschluss dürfen nicht beide Rollen enthalten sein, da dies dazu führen würde, dass jedes Gruppenmitglied oder jeder Benutzer, der einer solchen Gruppe oder Rolle zugeordnet ist, automatisch beide Rollen hätte. ServiceNow AI Platform bricht jeden Vorgang ab, der ein solches Szenario hervorrufen würde.

Hinweis: Sie können keine anderen Rollen als enthaltene Rollen zu „ `snc_external`„ Oder “ `snc_internal`„ Rollen.

Externe Benutzer müssen mindestens die Rolle snc_external erhalten. Die Rolle snc_external gibt an, dass es sich gegenüber Ihrer Organisation um einen externen Benutzer handelt. Sie sollten keinen Zugriff auf Ressourcen haben, es sei denn, dies wird ausdrücklich erlaubt durch ACLs für die Rolle snc_external oder zusätzliche Rollen, die die Rolle snc_external erben. Standardmäßig haben Benutzer mit der Rolle snc_external keinen Zugriff auf:

- Tabellen ohne die Rolle, die die Rolle snc_external oder public erbt
- Ressourcen vom Typ „nicht Datensatz“, z. B. Prozessoren und UI-Seiten, ohne Zugriff auf die Rolle „snc_external“ oder eine Rolle zu gewähren, die die Rolle „snc_external“ erbt.
- Platform Analytics-Dashboards.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Markieren Sie die Rolle snc_internal nicht als erweitert. Andernfalls können interne Benutzer nicht auf die Instanz zugreifen.

Plugin „Explicit Roles“

Wenn das „Explicit Roles“-Plugin aktiviert ist, gilt Folgendes:

- Alle Anwender müssen über die Rolle „snc_internal“ verfügen, um auf interne Ressourcen zuzugreifen, oder über die Rolle „snc_external“, um auf externe Ressourcen zuzugreifen. Benutzer ohne eine dieser expliziten Rollen können nur auf öffentliche Ressourcen zugreifen.
- Allen vorhandenen Benutzern wird automatisch die Rolle snc_internal zugewiesen. Durch diese Rolle werden die vorhandenen Zugriffsebenen und das Systemverhalten nicht geändert. Stattdessen stellt sie eine Kategorie bereit, um interne Benutzer von externen Benutzern zu unterscheiden. Alle internen Benutzer behalten dieselbe Zugriffsebene bei wie vor der Aktivierung des Plugins.

  Tipp: Um Änderungen an vorhandenen Funktionen für Benutzer zu verhindern, wird durch die Aktivierung des Plugins „Explicit Roles“ die Benutzerrolle snc_internal allen vorhandenen Benutzern in der Instanz zugewiesen. Dies schließt alle externen Benutzer ein, die hinzugefügt wurden, bevor das Plugin „Explicit Roles“ aktiviert wurde. Nachdem das Plugin „Explicit Roles“ aktiviert wurde, gehen Sie für alle externen Benutzer, die vor Aktivierung des Plugins „Explicit Roles“ hinzugefügt wurden, wie folgt vor:

  - Entfernen Sie die Rolle snc_internal.
  - Fügen Sie die Rolle snc_external hinzu.

  Durch die vorstehenden Maßnahmen können Sie sicherstellen, dass externe Benutzer, die vor der Aktivierung des Plugins „Explicit Roles“ hinzugefügt wurden, keinen Zugriff auf interne Ressourcen haben, die nur internen Benutzern zur Verfügung stehen sollten.

- Neu erstellten Benutzern wird automatisch die Rolle snc_internal zugewiesen, wenn sie erstmalig versuchen, sich bei der Instanz anzumelden, es sei denn, ihnen wurde explizit die Rolle snc_external zugewiesen. Sie können die Rolle snc_external einem neuen Benutzer hinzufügen, bevor er sich zum ersten Mal bei der Instanz anmeldet, um externe Benutzerrechte bereitzustellen.

  Wichtig:

  Aktivieren Sie dieses Plugin während eines Wartungsfensters oder wenn nur wenige Benutzer angemeldet sind. Benutzern, die derzeit bei der Aktivierung des Plugins angemeldet sind, wird die Rolle snc_internal nicht dynamisch zugewiesen. Stattdessen müssen sich Benutzer abmelden und wieder anmelden, um die Rolle snc_internal zu erhalten. Sobald das Plugin aktiviert ist, können Sie die Rollen snc_internal und snc_external jederzeit hinzufügen oder entfernen, um Benutzerrechte zu ändern.

  Nach der Aktivierung des Plugins erhält der Benutzer bei jeder Anmeldung die Rolle snc_internal, sofern das Konto diese Rolle noch nicht hatte, oder die Rolle snc_external. Dies schließt per Identitätswechsel angemeldete Benutzer ein.

- Allen vorhandenen ACLs ohne Rollenanforderung wird automatisch die Rolle snc_internal zugewiesen. Da sowohl vorhandenen ACLs als auch Benutzern die Rolle „snc_internal“ zugewiesen ist, ändern sich die vorhandenen Zugriffsebenen nicht.
- Neu erstellten ACLs ohne Rollenanforderung wird automatisch die Rolle snc_internal zugewiesen. Diese Rollenzuweisung gilt nicht für neu erstellte ACLs mit zugewiesener Rolle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für alle vorhandenen Prozessor-Datensätze [sys_processor] oder neu erstellte Prozessor-Datensätze [sys_processor] mit **Typ = Skript** wird die Rolle snc_internal automatisch zum Feld **Rollen** hinzugefügt, wenn das Feld leer ist.
- Um den Zugriff auf UI-Seiten auf interne Benutzer zu beschränken, weist das Plugin automatisch die Rolle snc_internal der * ACL mit dem **Typ ui_page** zu.
- Um den Zugriff auf Prozessoren auf interne Benutzer zu beschränken, weist das Plugin automatisch die Rolle snc_internal der * ACL mit dem **Typ processor** zu.
- Externe Benutzer müssen mindestens die Rolle snc_external erhalten, um auf die Instanz zuzugreifen. Diese Rolle muss externen Benutzern manuell erteilt werden. Der Zugriff auf Datensätze wird über ACLs gewährt.

Verschieben Sie keine System-Update Sets zwischen Instanzen, unabhängig davon, ob das Plugin „Explicit Roles“ aktiviert oder deaktiviert ist. Weitere Informationen finden Sie unter System-Update Sets .

Hinweis: Dieses Plugin erfordert auch das Plugin Contextual Security Manager.

glide.security.explicit_roles.do_not_fix Verhalten

Ab Xanadu Lassen Sie den los glide.security.explicit_roles.do_not_fix Wurde mit Änderungen an „snc_internal“ angepasst. Die Rolle „snc_internal“ ist jetzt sowohl im Arbeitsspeicher als auch in „sys_user_has_role“ identisch. Das neue Verhalten für glide.security.explicit_roles.do_not_fix Ist:

glide.security.explicit_roles.do_not_fix Neues Verhalten

Wert	Ergebnis
Falsch	Fügen Sie die Rolle „snc_internal“ sowohl im Arbeitsspeicher als auch „sys_user_has_role“ hinzu
True	Fügen Sie keine Rolle „snc_internal“ im Arbeitsspeicher oder „sys_user_has_role“ hinzu

Um die Rolle „snc_internal“ für bestimmte Anwender auszuschließen, verwenden Sie glide.security.explicit_roles.ignore.snc_internal.exclude_role_list Eigenschaft.

Tipp: Um zum vorherigen zurückzukehren glide.security.explicit_roles.do_not_fix Verhalten Verwenden Sie glide.security.explicit_roles.do_not_fix_in_memory Eigenschaft.

Externen Benutzer Zugriff auf Tabellen gewähren

Sie können externen Benutzern Zugriff auf eine Tabelle gewähren, indem Sie der Tabelle eine Rolle hinzufügen, die die Rolle snc_external erbt. Weitere Informationen finden Sie unter Externen Benutzern Zugriff auf eine Tabelle bereitstellen .

Die hasRoles()-Methode

Die Methode hasRoles() ist zwar noch verfügbar, wird aber im Geneva-Release abgeschafft. Verwenden Sie stattdessen die Methode hasRole(role name).

Wenn Sie die Methode hasRoles() verwenden, beachten Sie die folgenden Änderungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Diese Methode schließt die snc_internal-Standardrolle automatisch aus, wenn sie nach Rollen sucht. Dies bedeutet, dass die Methode hasRoles() immer noch **false** zurückgibt, wenn ein Benutzer nur über die Rolle snc_internal verfügt.
- Wenn der Benutzer die Rolle „snc_external“ hat, gibt die Methode **false** zurück, da die Instanz externe Benutzer als ohne Rolle betrachtet.

Gegenseitiger Ausschluss: snc_external und snc_internal

Die ServiceNow AI Platform verhindert, dass Benutzer gleichzeitig über beide Rollen snc_external und snc_internal verfügen. Die ServiceNow AI Platform wendet diesen gegenseitigen Ausschluss überall im System an und schreibt Fehlermeldungen für jeden Konflikt in die Protokolle.

Hinweis: ACLs können beide Rollen haben, wenn die ACL-Ressourcen für alle Benutzer zugänglich sein sollen.

Beispiel: Einem Benutzer beide expliziten Rollen hinzufügen (direkte Kollision):

1. Weisen Sie Benutzer Abel Tuter die Rolle snc_internal zu.
2. Weisen Sie Benutzer Abel Tuter die Rolle snc_external zu.

Ergebnis: Das Hinzufügen der Rolle snc_external schlägt fehl, da Abel Tuter die Rolle snc_internal hat.

Beispiel: Einer Gruppe beide expliziten Rollen hinzufügen (direkte Kollision):

1. Stellen Sie sich eine Gruppe namens Testgruppe vor, der derzeit keine expliziten Rollen zugewiesen sind.
2. Fügen Sie Abel Tuter der Testgruppe hinzu.
3. Fügen Sie die Rolle snc_external der Testgruppe hinzu.

Ergebnis: Das Hinzufügen der Rolle snc_external schlägt fehl, da Abel Tuter die Rolle snc_internal hat und nicht beide Rollen haben kann.

Beispiel: Eine explizite Rolle einer Gruppe zuweisen, in der ein Gruppenmitglied die explizite Rolle hat, die einen Konflikt verursacht (indirekte Kollision):

1. Weisen Sie Benutzer Abel Tuter die Rolle snc_internal zu.
2. Stellen Sie sich eine Gruppe namens Testgruppe vor, der derzeit keine expliziten Rollen zugewiesen sind.
3. Fügen Sie Abel Tuter der Testgruppe hinzu.
4. Fügen Sie die Rolle snc_external der Testgruppe hinzu.

Ergebnis: Das Hinzufügen der Rolle snc_external zur Gruppe schlägt fehl, da Abel Tuter die Rolle snc_external durch seine Zugehörigkeit zur Gruppe erben würde. Beide expliziten Rollen würden demselben Benutzer zugewiesen, was nicht zulässig ist.

Weitere Beispiele finden Sie in der folgenden Tabelle:

Rolle	Versuchte Aktion	Ergebnis
Direkte Kollision		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Versuchte Aktion	Ergebnis
Der Benutzer hat die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Der Benutzer hat die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Der Benutzer hat keine explizite Rolle.	Fügt die Rolle snc_internal oder snc_external hinzu.	Die Rolle wird hinzugefügt.
Der Benutzer hat beide explizite Rollen (vorhandene Kollision).	Fügen Sie den Benutzer einer Gruppe ohne Rollen hinzu.	Die Aktion wird abgebrochen.
Eine Rolle, die keinem Benutzer zugeordnet ist, enthält die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Eine Rolle, die keinem Benutzer zugeordnet ist, enthält die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Der Rolle enthält beide explizite Rollen (vorhandene Kollision).	Fügen Sie die Rolle einem Benutzer, einer Rolle oder einer Gruppe hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat die Rolle snc_internal.	Fügen Sie die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat die Rolle snc_external.	Fügen Sie die Rolle snc_internal hinzu.	Die Aktion wird abgebrochen.
Eine Gruppe ohne Mitglieder hat keine Rollen.	Fügt die Rolle snc_internal oder snc_external hinzu.	Die Rolle wird hinzugefügt.
Indirekte Kollision		
Rolleneinschluss mit Kollision	1. Gewähren Sie einem Benutzer mit der Rolle snc_internal die Testrolle. 2. Fügen Sie der Testrolle die Rolle snc_external hinzu.	Die Aktion wird abgebrochen.
Rolleneinschluss ohne Kollision	1. Gewähren Sie einem Benutzer ohne Rolle die Testrolle. 2. Fügen Sie der Testrolle die Rolle snc_external hinzu.	Die Rolle wird sowohl dem Benutzer als auch der Testrolle hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Versuchte Aktion	Ergebnis
Gruppeneinschluss mit Kollision	1. Fügen Sie einen Benutzer mit der Rolle snc_internal der „Testgruppe 2“ (untergeordnete Gruppe von Testgruppe 1) hinzu. 2. Fügen Sie Testgruppe 2 die Rolle snc_external hinzu. 3. Fügen Sie die Rolle snc_external der übergeordneten Gruppe „Testgruppe 1“ (übergeordnete Gruppe von Testgruppe 2) hinzu.	Die Aktion wird abgebrochen.
Gruppeneinschluss ohne Kollision	1. Fügen Sie einen Benutzer ohne Rolle der Gruppe „Testgruppe 2“ (untergeordnete Gruppe von Testgruppe 1) hinzu. 2. Fügen Sie die Rolle snc_external oder snc_internal der „Testgruppe 1“ (übergeordnete Gruppe der Testgruppe 2) hinzu.	Die Rolle wird der übergeordneten Gruppe, der untergeordneten Gruppe und dem Benutzer hinzugefügt.
Gruppeneinschluss plus Rolleneinschluss mit Kollision	Fügen Sie contains_external der Testgruppe 1, der übergeordneten Gruppe von Testgruppe 2, hinzu.	Testgruppe 1 und Testgruppe 2 erhalten beide contains_external, aber sie erhalten nicht explizit die Rolle snc_external.
	Fügen Sie die Rolle snc_internal der Testgruppe 2, der untergeordneten Gruppe von Testgruppe 1, hinzu.	Die Aktion wird abgebrochen.
Änderung der übergeordneten Gruppe plus Gruppeneinschluss	1. Entfernen Sie Testgruppe 1 als übergeordnete Gruppe von Testgruppe 2. 2. Fügen Sie der Testgruppe 1 die Rolle snc_internal hinzu. 3. Fügen Sie Testgruppe 2 die Rolle snc_external hinzu. 4. Legen Sie in Testgruppe 2 die Testgruppe 1 als übergeordnete Gruppe fest, und speichern Sie.	Die Aktion wird abgebrochen. Wiederholen Sie diesen Vorgang für bereits geschachtelte Gruppen, erwarten Sie derselbe Ergebnis.

Die Ursache einer abgebrochenen Aktion wird in der Fehlermeldung angezeigt und muss behoben werden, bevor ein erneuter Versuch erfolgreich verlaufen kann.

Für direkte Fälle, z. B. Hinzufügen einer expliziten Rolle zu einem einzelnen Benutzer, überprüfen Sie, welche explizite Rolle der Benutzer haben soll. Wenn der Benutzer über die falsche explizite Rolle verfügt, muss diese zuerst entfernt und dann die richtige explizite Rolle hinzugefügt werden.

Für indirekte Fälle, z. B. Hinzufügen einer expliziten Rolle zu einer Gruppe (sodass einem Gruppenmitglied beide expliziten Rollen zugewiesen werden), überlegen Sie, ob

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dieser Benutzer in der Gruppe sein soll. Bestimmen Sie auch, ob die explizite Rolle der Gruppe zugewiesen werden soll. Dies schließt auch Fälle ein, in denen die Rolle durch die Gruppenhierarchie und durch Rolleneinschluss geerbt wird.

Beachten Sie, dass die ServiceNow AI Platform nur die erste mögliche Kollision meldet. Wenn nach Aufhebung der Kollision erneute Versuche wieder fehlschlagen, wobei eine andere Ursache vorliegt, sollten Sie die relevanten gegenseitigen Abhängigkeiten von Benutzern/Gruppen/Rollen umfassender analysieren. Dabei sollten Sie gegebenenfalls überdenken, wie Gruppen- und Rolleneinschlüsse aufgebaut sind.

Fordern Sie Explizite Rollen An

Aktivieren Sie explizite Rollen, indem Sie das Plugin Explicit Roles (com.Glide.Explicit_roles) über anfordern Now Support Servicekatalog.

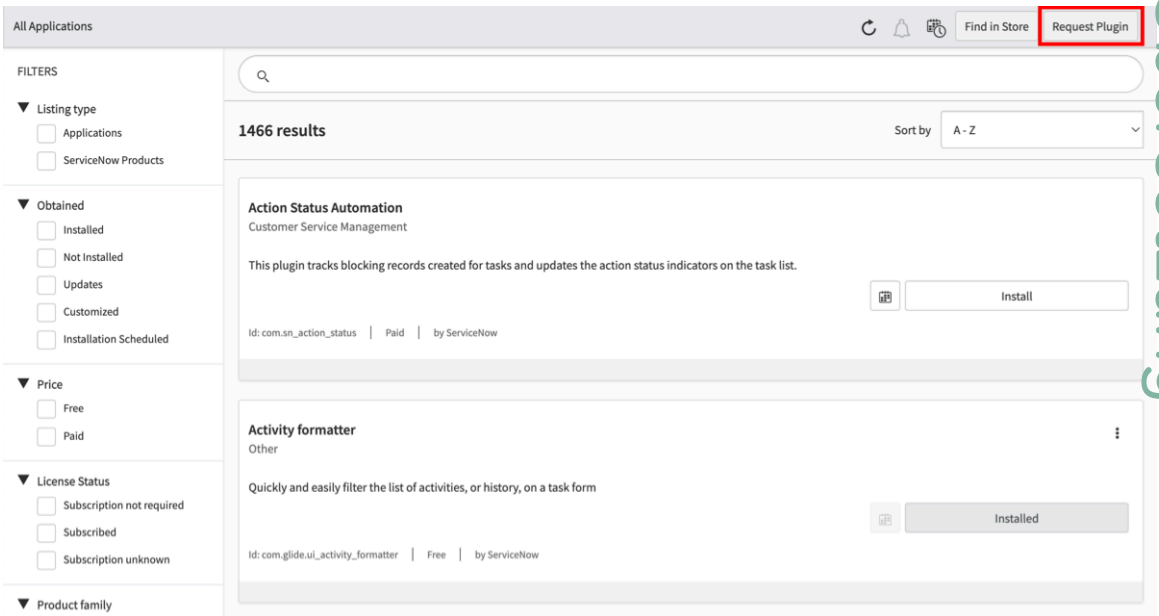
Vorbereitungen

Erforderliche Rolle: Administrator

Wichtig: Aktivieren Sie dieses Plugin während eines Wartungsfensters oder wenn nur wenige Benutzer angemeldet sind. Benutzern, die derzeit bei der Aktivierung des Plugins angemeldet sind, wird die Rolle snc_internal nicht dynamisch zugewiesen. Stattdessen müssen sich Benutzer abmelden und wieder anmelden, um die Rolle snc_internal zu erhalten. Sobald das Plugin aktiviert ist, können Sie die Rollen snc_internal und snc_external jederzeit hinzufügen oder entfernen, um Benutzerrechte zu ändern.

Prozedur

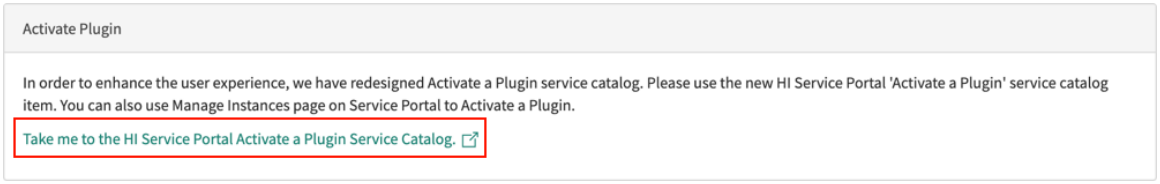
1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

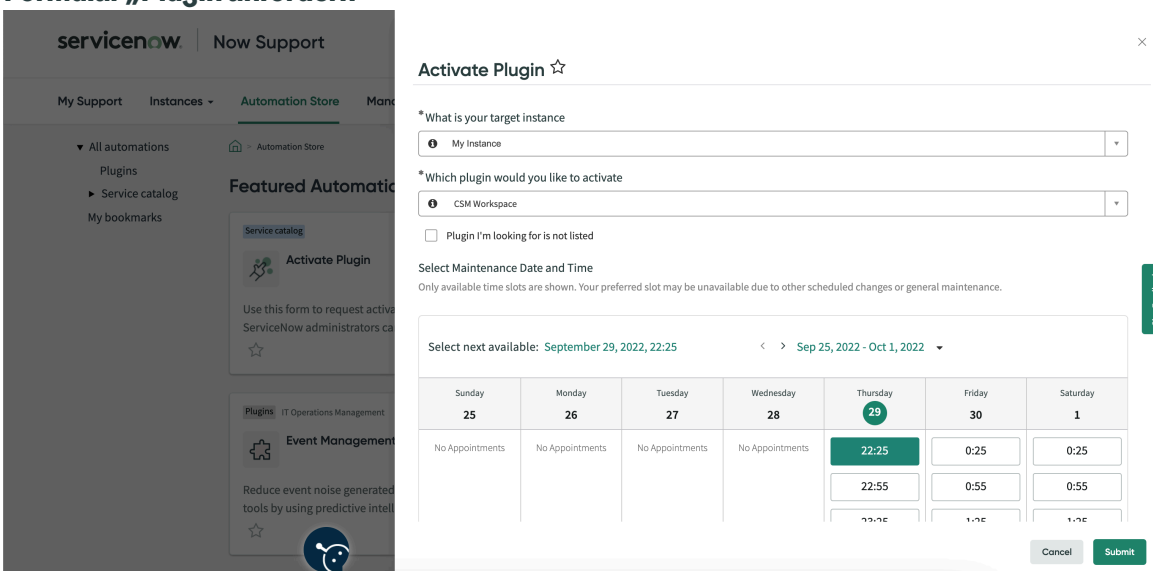
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Rollen mit erhöhten Rechten

Rollen mit erhöhten Berechtigungen erfordern, dass Sie die Verantwortung für die Verwendung der Rolle manuell übernehmen, bevor Sie auf die Funktionen der Rolle zugreifen können.

Standardmäßig haben Sie bei der Anmeldung keine Rollen mit erhöhten Berechtigungen. Sie müssen manuell auf die Berechtigung der Rolle erhöhen. Eine Rolle mit erhöhten Berechtigungen gilt nur für die Dauer Ihrer Anwendersitzung. Sitzungszeitüberschreitung oder Abmeldung entfernt die Rolle.

Sie können jede Rolle als Rolle mit erhöhten Berechtigungen festlegen und diese Rolle dann einem oder mehreren Anwendern zuweisen. Führen Sie diese Option aus, wenn Sie verhindern möchten, dass Anwender unmittelbar nach der Anmeldung Zugriff auf die Rechte haben, die die Rolle bereitstellt. Sie können die Berechtigungsrolle im Rollenformular festlegen. Siehe Erstellen Sie eine Rolle Für Anweisungen.

Um eine erhöhte Rolle zu verwenden, müssen Sie die folgenden Bedingungen erfüllen:

- Die erhöhte Rolle muss Ihnen zugewiesen werden.
- Sie müssen manuell auf eine bestimmte erhöhte Rolle hochstufen, um ihre Berechtigungen zu erhalten, auch wenn Sie bereits auf eine zweite erhöhte Rolle hochgestuft sind, die die erste erweiterte Rolle enthält.

  Beispiel: Wenn die erhöhte Rolle A die erhöhte Rolle B enthält, müssen Sie auch bei einer Erhöhung auf Rolle A dennoch auf Rolle B erhöhen, um ihre Berechtigungen zu erhalten.

Die Administratorrolle

Um einem Anwender die Administratorrolle zu gewähren, muss der gewährende Anwender auch über die Administratorrolle verfügen. Beispielsweise kann ein Anwender mit nur der Rolle user_admin anderen Anwendern die Administratorrolle nicht gewähren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

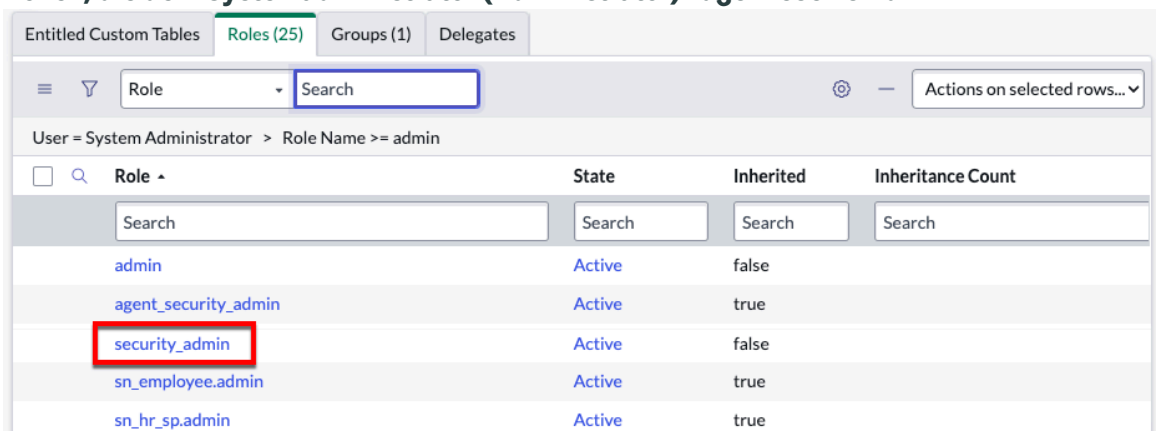
- Nicht-Administratoranwender können einer Gruppe, die die Administratorrolle enthält, keinen Anwender hinzufügen.
- Um einem Anwender die Rolle „Security_admin“ zu gewähren, muss der gewährende Anwender auch über die Administratorrolle verfügen und auf die Rolle „Security_admin“ steigen, bevor er anderen Anwendern die Rolle „Security_admin“ gewährt. Ein Anwender mit nur der Administratorrolle kann anderen Anwendern die Rolle „Security_admin“ nicht gewähren.
- Ein Anwender ohne die Rolle „Security_admin“ kann keinen Anwender zu einer Gruppe hinzufügen, die die Rolle „Security_admin“ enthält.

Warnung: Die Verwendung von erhöhten Berechtigungen für eine Administratorrolle wird nicht unterstützt. Fordern Sie stattdessen Administratoren auf, manuell zu erhöhen, siehe Erzwingen Sie Administratoren, manuell zu erhöhen

Die Rolle Security_admin

Im Basissystem ist die Rolle „Security_admin“ die einzige Rolle mit erhöhten Berechtigungen. Diese Rolle wird automatisch dem Anwender zugewiesen, der der standardmäßige Systemadministrator-Anwender (Administrator) ist. Bietet Zugriff auf ACLs Und Einstellungen Für Hohe Sicherheit .

Rollen, die dem Systemadministrator (Administrator) zugewiesen sind



Hinweis: Um diese Rolle anzuzeigen, müssen Sie zuerst die Rolle „Security_admin“ erhöhen. Wenn Sie nur als Systemadministrator (admin)-Anwender angemeldet sind, wird der Datensatz „Security_admin“ in der Liste der Rollen nicht angezeigt.

Rolle „Security_admin“

Die Rolle „Security_admin“ ist eine Rolle mit erhöhten Berechtigungen, die mit hohen Sicherheitseinstellungen bereitgestellt wird, mit denen Anwender Zugriffssteuerungen erstellen und ändern und Einstellungen für hohe Sicherheit ändern können.

Im Basissystem hat nur der Standardsystemadministrator (admin) die Rolle Security_admin. Da erhöhte Berechtigungen erforderlich sind, verfügt der Administratoranwender bei der Anmeldung nicht über diese Rolle. Nach der Erhöhung der Berechtigungen hat der Administratoranwender die Rolle Security_admin für die Dauer der Anwendersitzung. Weitere Informationen finden Sie unter Auf eine privilegierte Rolle hochstufen.

Um eine hohe Sicherheit aufrechtzuerhalten, erfordert die Rolle „Security_admin“ erhöhte Berechtigungen. Beschränken Sie die Anwender und Gruppen, denen Sie diese Rolle zuweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf eine privilegierte Rolle hochstufen

Der Basissystemadministrator kann auf eine privilegierte Rolle aufsteigen, um Zugriff auf die Funktionen der Einstellungen für hohe Sicherheit zu haben.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: Wenn Sie zusätzlichen Anwendern die Administratorrolle gewähren, können sie nicht zu einer privilegierten Rolle hochgestuft werden. Nur der Basissystemadministrator kann erhöhen.

Prozedur

1. Klicken Sie im Bannerrahmen auf Ihr Bild, oder klicken Sie auf Ihre Initialen, wenn Sie kein Bild hochgeladen haben.
2. Wählen Sie Aus **Rollen Erhöhen** .
   Ein Dialogfeld mit verfügbaren Rollen für die Erhöhung wird angezeigt.
3. Wählen Sie die erhöhten Rollen aus, die zugewiesen werden sollen, und klicken Sie auf **OK** .
   Diese Rolle gewährt dem Anwender für den Rest der Sitzung erhöhte Berechtigungen für alle von der Rolle gesteuerten Ressourcen. Wenn sich der Anwender abmeldet, werden die erhöhten Berechtigungen mit der Sitzung beendet, können jedoch bei der nächsten Anmeldung wiederhergestellt werden.
4. Beenden Sie die Rollenerhöhung, indem Sie zum Dialogfeld in Schritt 2 zurückkehren und die Auswahl der Rolle deaktivieren.

Erzwingen Sie Administratoren, manuell zu erhöhen

Eine Eigenschaft ist verfügbar, um alle Anwender mit der Administratorrolle zu zwingen, die Rolle manuell auszuwählen, auf die sie hochstufen möchten.

Vorbereitungen

Erforderliche Rolle: security_admin

Prozedur

1. Melden Sie sich als Administrator an.
2. Erhöhen Sie Ihre Rolle auf Security_admin.
3. Navigieren Sie zu **sys_properties.list**.
4. Suchen Sie nach , und wählen Sie aus `glide.security.strict_elevate_privilege`Eigenschaft.
5. Legen Sie das Wertfeld auf fest **Wahr** Und klicken Sie auf **Übermitteln** .

Ergebnis

Wenn sich der Anwender anmeldet, wird ihm ein Dialogfeld angezeigt, in dem er die Rolle auswählen kann, auf die er hochstufen kann.

Verbindung und Anmeldeinformationen

Anmelde- und Verbindungsinformationen sind erforderlich, um auf einen Computer oder ein Netzwerkgerät für Discovery, Service-Mapping und Cloud-Management zuzugreifen oder um mit Orchestration zu arbeiten. Beim Hinzufügen von Inhalten zu Share oder App-Store können Sie für Ihre Umgebung relevante Verbindungen und Anmeldeinformationen konfigurieren, ohne den integrierten Inhalt zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über Anmeldeinformationen.

Konfigurieren



Konfigurieren Sie Anmeldeinformationen.

Referenz



Ruft Details zu Anmeldeinformationen ab.

Problembehandlung



Erfahren Sie, wie Sie Probleme in Verbindungen und Anmeldeinformationen beheben können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden Sie Anmeldeinformationen, Verbindungen und Aliasse

Alle Anwendungsintegrationen in ServiceNow AI Platform Verwenden Verbindungen, Anmeldeinformationen und Aliasse, damit Anwendungen auf Ressourcen zugreifen können.

Bevor Sie eine Anwendungsintegration in ausführen können ServiceNow AI Platform, Sie müssen Verbindungsinformationen und die entsprechenden Anmeldeinformationen erstellen und konfigurieren und einen Alias hinzufügen. Um zu verstehen, wie ServiceNow Definiert diese Begriffe:

Verbindung

A *Verbindung* Ist eine Integration in ein System, z. B. eine IP-Adresse oder ein Endpunkt mit Protokollen. Bei der Integration in eine Datenbank enthalten sie bestimmte Daten, z. B. Angaben zur Datenbank.

Anmeldeinformation

A *Anmeldeinformationen* Sind die Authentifizierungsdaten erforderlich, um die Verbindung herzustellen, z. B. eine ID und ein Passwort.

Alias

Ein *Alias* Ist eine Benennungskonvention oder ein Tag, die an eine Reihe von Verbindungen oder Anmeldeinformationen in Ihrer Instanz gebunden ist. Ein Alias enthält die erforderlichen Verbindungs- und Anmeldeinformationen für eine Anwendungsintegration. Anstatt diese Informationen bei jeder Integration einzugeben, können Sie einen Alias verwenden.
Sie können beispielsweise einen Alias festlegen, der Ihre QA-, Entwicklungs- und Produktionsanmeldeinformationen für dieselbe Anwendungsintegration enthält. Der Alias löst die Anwendungsintegration für jede Umgebung auf.

Die ServiceNow AI Platform Unterscheidet verschiedene Arten von Aliassen:

Anmeldeinformationsalias

Dieser Alias ist nur Anmeldeinformationsdaten zugeordnet und wird während der Laufzeit aufgelöst.

Aliasse für Verbindungen und Anmeldeinformationen

Dieser Alias wird den Verbindungsinformationen und den Anmeldeinformationsdaten zugeordnet, die zum Abschließen der Integration erforderlich sind, und wird während der Laufzeit aufgelöst.

Innerhalb von Aliasse für Verbindungen und Anmeldeinformationen können Sie auch zusätzliche Aliasse erstellen, die aufgerufen werden *Untergeordnete Aliasse* . Mit untergeordneten Aliassen können Sie mehrere Verbindungen innerhalb derselben Anwendungsintegration erstellen. Wenn Sie einen untergeordneten Alias erstellen, wird der Alias, unter dem Sie ihn erstellt haben, zu einem *Übergeordneter Alias* . Während untergeordnete Aliasse Eigenschaften von ihrem übergeordneten Alias erben, enthalten untergeordnete Aliasse ihre eigenen Verbindungs- und Anmeldeinformationen.

Vorteile bei der Verwendung von Verbindungen, Anmeldeinformationen und Aliassen

- Zentraler Standort zum Speichern und Verwalten von Anmeldeinformationen für einen externen Service
- Einmal definieren und für mehrere Plattformfunktionen wiederverwenden
- Minimieren Sie die Konfiguration anderer Plattformfunktionen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zulassen, dass nicht-Administratoren vordefinierte Verbindungen und Anmeldeinformationen verwenden
- Erhöhte Sicherheit

Funktionen mit Verbindungen, Anmeldeinformationen und Aliassen

Die folgenden Funktionen verwenden Verbindungen, Anmeldeinformationen und Aliasse:

- Flow Designer
- IntegrationHub
- Cloud-Management
- Discovery
- Orchestration
- Service-Mapping

Sie können Aliasse auf einrichten ServiceNow AI Platform Auf eine von zwei Arten:

- Mit Verbindungen und Anmeldeinformationen Modul. Weitere Informationen finden Sie unter Verbindungs- und Anmeldealias erstellen.
- Im Dashboard „Verbindungen“ von IntegrationHub. Siehe Fügen Sie eine Verbindung hinzu .

Hinweis: IntegrationHub Erfordert ein separates Abonnement. Weitere Informationen finden Sie unter Anforderung IntegrationHub an.

Synchronisierung der Anmeldeinformationen auf MID Servern

Jeweils *MID-Server* In Ihrem Netzwerk, das mit der Instanz synchronisiert ist, wird eine Kopie aller von Ihnen erstellten Anmeldeinformationen aufbewahrt. Der MID-Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die die Kommunikation und die Verschiebung von Daten zwischen einer ServiceNow-Instanz und externen Anwendungen, Datenquellen und Services ermöglicht. Diese Synchronisierung beschleunigt das Lesen von Anmeldeinformationen, wenn Anwendungen wie Discovery oder Service-Mapping im Netzwerk auf mehrere Geräte zugreifen müssen. Die MID Server führen eine Synchronisierung durch, wenn sie einen `credentials_reload`-Auftrag in der ECC-Warteschlange finden. Der Auftrag zum Neuladen weist den MID Server an, einen SOAP-Aufruf an die Instanz auszuführen, um die gesamte Liste der Anmeldeinformationen in der Tabelle „Anmeldeinformationen“ [discovery_credentials] einschließlich aller Feldwerte abzurufen. Weitere Informationen finden Sie unter MID-Server .

Die SOAP-Antwort, die Ihre Instanz an die einzelnen MID Server sendet, enthält auch benutzerdefinierte Felder, die Sie von Ihnen angepassten Formularen für Anmeldeinformationen hinzugefügt haben. Wenn Sie Referenzfelder hinzugefügt haben, werden die Daten in der referenzierten Tabelle ebenfalls als Teil der SOAP-Antwort gesendet. Dies kann zu Leistungsproblemen führen, wenn die Anmeldeinformationen mit mehreren MID Servern synchronisiert werden. Dieses Problem können Sie am besten in den Griff bekommen, wenn Sie der Tabelle „Systemeigenschaften“ [sys_properties] folgende Eigenschaften manuell hinzufügen:

Hinweis: Um die Werte in diesen Eigenschaften zu ändern, fügen Sie sie der Tabelle „Systemeigenschaften“ [sys_properties] hinzu. Wenn Sie sie nicht hinzufügen, verwendet das System den Standardwert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
com.snc.credentials_user_fields	Schließt alle benutzerdefinierten Felder in die Synchronisierung der Anmeldeinformationen ein. Legen Sie diese Eigenschaft auf „falsch“ fest, wenn Sie die Felder, die Sie den Anmeldeinformationsformularen hinzugefügt haben, nicht einschließen möchten. • **Typ**: true | false • **Standardwert**: true
com.snc.credentials_recursion_depth	Definiert die Anzahl der Tabellen, die durchlaufen werden sollen, wenn der Mechanismus zur Synchronisierung von Anmeldeinformationen Felder aus Referenztabellen erfasst. Verringern Sie diese Anzahl, wenn Leistungsprobleme auftreten und Sie über angepasste Formulare für Anmeldeinformationen verfügen, die Referenzfelder für Tabellen enthalten, die ebenfalls Referenzfelder enthalten. • **Typ**: Ganzzahl • **Standardwert**: 3

Umfangsschutz für Anmeldeinformationen und Verbindungen

Sie können bestimmte Typen von Verbindungs- und Anmeldeinformationsdatensätzen als zu einem Bereich gehörend klassifizieren und den Schutz des Bereichs darauf erweitern. Diese Bereichsrichtlinien dienen dem Schutz von Datensätzen, die Sie in einer Tabelle erstellen, und verhindern Interaktionen mit Datensätzen, die für einen anderen Bereich privat sind.

Ein **Anwendung** Das Feld ist in den Tabellen „Verbindung“ [sys_connection] und „Discovery-Anmeldeinformationen“ [Discovery_credentials] verfügbar, um diese Datensatztypen bestimmten Bereichen zuzuordnen. Sie ist in UI-Formularen in nicht sichtbar Zurich, Aber Sie können es ihnen einfach hinzufügen. Weitere Informationen zu diesen Datensatztypen und dem Hinzufügen des Felds zu ihren UI-Formularen finden Sie unter:

- Erste Schritte mit Verbindungen
- Erste Schritte mit Anmeldeinformationen
- Anmeldeinformationsaliasse für Discovery
- Formularlayout konfigurieren

Die Beschränkung der Verwendung eines Verbindungs- und Anmeldeinformationsdatensatzes auf einen bestimmten Bereich ist wichtig für die Verwaltung von Anwendungen, die erzwungene Sicherheit erfordern. Diese Anwendungen umfassen HR-Servicebereitstellung Oder Security Operations In bereichsbezogenen verwalteten Anwendungen erstellte Verbindungs- und Anmeldeinformationsdatensätze sind für Administratoranwender nicht sichtbar. Das Zuordnen eines Datensatzes für Verbindungen und Anmeldeinformationen zu einem bestimmten Anwendungsbereich bietet folgende Schutzmaßnahmen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wendet Zugriffssteuerungslistenregeln (Access Control List Rules, ACLs) auf eingeschränkte Bereiche an. Weitere Informationen zu bereichsbezogenen ACLs finden Sie unter Regeln für Zugriffssteuerungsliste .

  Hinweis: Einige Anwendungen, die Umfangsverwaltung und erzwungene Sicherheit verwenden, erfordern möglicherweise zusätzliches Setup. Weitere Informationen finden Sie unter Verwalten Sie HR-Rollen

- Schützt Datensätze, wenn sie mithilfe eines Skripts abgefragt werden. Wenn Sie eine Abfrage aus dem globalen Bereich ausführen und sich der Datensatz für Verbindungen und Anmeldeinformationen in einem geschützten Bereich befindet, wird er nicht in der Abfrage angezeigt, es sei denn, es wurde Zugriff darauf gewährt.

Sie können Datensätze mit eingeschränktem Anruferzugriff anpassen und Zugriff auf diese gewähren. Weitere Informationen finden Sie unter Einstellungen für eingeschränkte Anruferzugriffsberechtigung . Umfangsbeschränkungen gelten auch für alle untergeordneten Tabellen der Tabellen „Verbindung“ [sys_connection] und „Discovery-Anmeldeinformationen“ [Discovery_credentials]. Leere Felder und andere Bereiche sind nicht eingeschränkt.

Hinweis: Umfangsschutz ist nur für bestimmte gesicherte Bereiche aktiviert, um Verwirrung beim Einrichten neuer Datensätze zu vermeiden. Wenn jemand eine Verbindung in seinem bereichsbezogenen Anwendungsbereich herstellt, hat er keine automatische Umfangsbeschränkung.

Domänentrennung sowie Anmeldeinformationen und Verbindungen

Domänentrennung wird in Anmeldeinformationen und Verbindungen unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Enthält alle Aspekte von **Standard** Level-Support.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung.

Übersicht

Die Anmeldeinformationen sind an verschiedene ServiceNow-Funktionen gebunden, die auf Systeme außerhalb der Instanz zugreifen. Die Anmeldeinformationen folgen der Domain

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Separation, die an diejenige Funktion gebunden ist, welche die Anmeldeinformationen verwendet.

Verbindungen sind protokollspezifische Informationen, die auf einen Zielhost außerhalb der Instanz verweisen. Eine Verbindung kann die Domäne angeben, um eine Aktivität auszuführen.

Funktionsweise der Domain Separation für Anmeldeinformationen und Verbindungen

Anmeldeinformationen greifen auf Ressourcen außerhalb der Instanz zu und werden von verwendet Discovery , Orchestration , Service-Mapping , und Cloud Provisioning and Governance Anwendungen. Diese Anmeldeinformationen sind nicht an eine bestimmte Domäne gebunden, sondern können an eine Anwendung gebunden sein und folgen dann der von der Anwendung verwendeten Domain Separation. Anmeldeinformationen können auch einem zugewiesen werden MID-Server , Und folgen Sie dann der von angegebenen Domänentrennung MID-Server Konfiguration.

Verbindungen greifen auf einen Zielhost zu, der eine *JMS*-, *JDBC*-oder *HTTP(s)*-Verbindung verwendet. Sie können eine globale oder eine bestimmte Domäne angeben, zu der die Verbindung gehört.

Zugehörige Informationen

Domänentrennung für Service Provider

Konfigurationsvorlagen für Verbindungen und Anmeldeinformationen

Ermöglichen Sie Benutzern mit der Rolle „admin“ und „flow_designer“, Spoke-Integrationen mit Drittanbietersystemen über ein einzelnes, anpassbares Formular einzurichten.

Sie können beispielsweise eine OAuth-Integration einrichten, die einen OAuth-Provider registriert, ein Token generiert und Verbindungs- und Anmeldeinformationsdatensätze erstellt. Ein Aktionsdesigner oder -Entwickler kann eine Konfigurationsvorlage verwenden, um die Spoke an einem Ort einzurichten, und das System erstellt die zugehörigen Datensätze.

Vorteile

Konfigurationsvorlagen aktivieren:

- Administratoren oder Flow-Designer, um komplexe Integrationen mit einem einzigen Formular einzurichten.
- Entwickler zum Festlegen statischer Werte in einer Integration, um den Setup-Prozess für Administratoren und Flow Designer zu vereinfachen.

Unterstützte Anmeldeinformationstypen

Sie können Konfigurationsvorlagen für Integrationen mit diesen Anmeldeinformationstypen erstellen:

- Basisauth.
- API Key
- OAuth-JWT-Bearer-Gewährungstyp

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Gewährungstyp für OAuth-Autorisierungscode
- Anwenderdefinierte Authentifizierung

Konfigurationsvorlagenkomponenten

Standarddatenvorlage

Damit werden statische Informationen festgelegt, die für jede Integration gelten. Beispielsweise können Sie die API und die Token-URL festlegen, wenn der Wert für jede Integration gilt.

Dynamische Datenvorlage

Damit werden Informationen festgelegt, die der Benutzer zum Einrichten der Integration eingeben muss. Beispielsweise können Sie Schlüssel-Wert-Paare aus Benutzername und Passwort hinzufügen, um benutzerdefinierte Werte zu erfassen.

Nachbearbeitungsskript

Damit werden zusätzliche Datensätze erstellt, die für die Integration erforderlich sind. Wenn Ihre Spoke beispielsweise benutzerdefinierte Tabellen enthält, können Sie Datensätze in diesen Tabellen auf der Grundlage von Benutzereingaben in der Konfigurationsvorlage erstellen. Dieses Skript wird ausgeführt, nachdem die Verbindungs- und Anmeldeinformationsdatensätze erstellt wurden.

Skript Vorbearbeiten

Füllt die anwenderdefinierten Felder in vorab aus **Zusätzliche Informationen** Abschnitt, wenn Sie eine vorhandene Verbindung bearbeiten. Wenn Sie die anwenderdefinierten Felder vorab ausfüllen, können Sie den aktuellen Wert anzeigen, der dem anwenderdefinierten Feld zugeordnet ist.

Testaktion

Ermöglicht Ihnen das Testen einer Verbindung direkt über eine Integrationsaktion in der Flow-Ansicht von Workflow-Studio. Die Testaktion verwendet eine Aktionsdefinition, um den Alias zu testen, an den die Vorlage derzeit angehängt ist. Details finden Sie unter Erstellen Sie eine Testaktion, um einen Verbindungsalias aus einer Konfigurationsvorlage zu testen .

Demodaten

Die Tabelle „Verbindungs- und Anmeldeinformationsvorlagen“ [sys_alias_Templates] enthält Beispielvorlagen, um zu demonstrieren, wie Vorlagen für allgemeine Authentifizierungstypen eingerichtet werden. Verwenden Sie diese Beispiele als Leitfaden, wenn Sie eigene erstellen.

Konfigurieren Sie eine Vorlage für den Gewährungstyp „OAuth JWT-Bearer“

Diese Beispielkonfigurationsvorlage richtet Anmeldeinformations- und Verbindungsdatensätze mit dem JWT-Bearer-Gewährungstyp ein, um Anforderungen bei DocuSign zu authentifizieren.

Standarddatenvorlage

Jedes Element der obersten Ebene in der Standarddatenvorlage erstellt einen zugehörigen Datensatz. Die Vorlage enthält diese Abschnitte:

- `Anmeldeinformationen` : Erstellt einen Datensatz in der Tabelle „Anmeldeinformationen“.
- `Verbindung` : Erstellt einen Datensatz in der Tabelle „Verbindungen“ [sys_connection] und alle zugehörigen Verbindungsdatensätze.
- `Zusätzlich` : Erstellt optional Datensätze in einer anwenderdefinierten Tabelle. Das Nachverarbeitungsskript teilt dem System mit, was mit diesen Datensätzen zu tun ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im folgenden Beispiel werden die Datensätze erstellt, die für die Authentifizierung des OAuth-JWT-Bearer-Gewährungstyps erforderlich sind.

```
{
 "credential": {
  "oauth_entity": {
   "oauth_entity_profile": [
    {
     "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
     "name": "Docusign Profile",
     "default": true,
     "oauth_entity_profile_scope": [
      "users:read.email"
     ]
    }
   ],
   "code_challenge_method": "S256",
   "type": "consumer",
   "oauth_entity_scope": [
    {
     "oauth_entity_scope": "users:read.email",
     "name": "email"
    }
   ],
   "client_id": "<provider-client-id>",
   "use_mutual_auth": false,
   "revoke_token_url": "https://<provider-domain-name>.com/oauth2/revoke",
   "default_grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
   "public_client": false,
   "oauth_api_script": "3e3a3a11c333210016194ffe5bba8f70",
   "name": "Docusign Spoke OAuth",
   "client_secret": "<provider-client-secret>",
   "auth_url": "https://<provider-domain-name>.com/oauth2/auth",
   "token_url": "https://<provider-domain-name>.com/oauth2/token",
   "redirect_url": "https://<instance-name>.service-now.com/oauth_redirect.do"
  },
  "jwt_provider": {
   "jwt_keystore_aliases": {
    "kid": "<provider-key-id>",
    "name": "Docusign Spoke JWT Key",
    "signing_keystore": "<signing-keystore-sys-id>",
    "signing_algorithm": "rsa_256",
    "signing_key_password": "password"
   },
   "jwt_claim_validation" : [ {
    "name" : "iss",
    "is_standard" : true,
    "data_type" : "string",
    "value":"<docusign-iss-claim>"
   }, {
    "name" : "sub",
    "is_standard" : true,
    "data_type" : "string",
    "value":"<docusign-sub-claim>"
   }, {
    "name" : "aud",
    "is_standard" : true,
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      "data_type" : "string",
      "value":"<docusign-aud-claim>"
    }, {
      "name" : "scope",
      "is_standard" : false,
      "data_type" : "string",
      "value" : "signature impersonation"
    } ],
    "name": "Docusign Spoke JWT Provider",
    "jwt_api_script": "9ef6af86ff10330001d3cd6bd53bf144"
  },
  "name": "Docusign Spoke Credential",
  "table": "oauth_2_0_credentials"
 },
 "connection": {
  "use_mid": false,
  "connection_url": "https://<provider-domain-name>.com",
  "name": "Docusign Spoke Connection",
  "table": "http_connection"
 },
"additional":{
  "docusign_account_name": "<docusign-account-name>",
  "docusign_account_email": "<docusign-account-email>"
}
}
```

Dynamisches Datenschema

Das dynamische Datenschema definiert, was der Anwender sieht, wenn er einen Alias für Verbindungen und Anmeldeinformationen erstellt, und sammelt seine Eingaben. Verwenden Sie die DOT-Walking-Syntax, um Anwendereingaben Feldern zuzuordnen, die in der Standarddatenvorlage erstellt wurden. Beispiel: `Connection_fields` Ordnet Anwendereingaben zu `Connection_url` Feld in `Verbindung` Objekt, das von der Standarddatenvorlage erstellt wurde.

```
{
 "connection_fields": [
  {
   "name": "connection.connection_url",
   "label": "Connection URL",
   "type": "text",
   "defaultValue": "https://demo.docusign.net",
   "hint": "Connection URL for Docusign"
  }],
"additional_fields":[
  {
   "name": "additional.docusign_account_id",
   "label": "Docusign Account Number",
   "type": "text",
   "hint": "Docusign Account Number"
  },
  {
   "name": "additional.docusign_account_name",
   "label": "Docusign Account Name",
   "type": "text",
   "hint": "Name to identify the Docusign account"
  },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  {
    "name": "additional.docusign_account_email",
    "label": "Docusign Account Email",
    "type": "text",
    "hint": "Docusign Account Email"
  }
 ],
 "credential_fields": [
  {
    "name": "credential.oauth_entity.client_id",
    "label": "OAuth Client ID",
    "type": "text",
    "hint": "Client ID for Docusign"
  },
  {
    "name": "credential.oauth_entity.redirect_url",
    "label": "OAuth Redirect URL",
    "type": "text",
    "defaultValue": "https://<instance-name>.service-now.com/oauth_redirect.do",
    "hint": "Callback URL for Docusign"
  },
{
    "name": "credential.jwt_provider.jwt_claim_validation[0].value",
    "label": "Issuer (iss) Claim value",
    "type": "text",
    "hint": "The integrator key (also known as client ID) of the application"
  },
{
    "name": "credential.jwt_provider.jwt_claim_validation[1].value",
    "label": "Subject (sub) Claim value",
    "type": "text",
    "hint": "The user ID of the user to be impersonated"
  },
{
    "name": "credential.jwt_provider.jwt_claim_validation[2].value",
    "label": "Audience (aud) Claim value",
    "type": "text",
    "defaultValue": "account-d.docusign.com",
    "hint": "The URI of the authentication service instance to be used e.g.
account.docusign.com"
  },
  {
    "name": "credential.jwt_provider.jwt_keystore_aliases.kid",
    "label": "Key ID (kid)",
    "type": "text",
    "hint": "Indicates which key was used to secure the JWS"
  },
  {
    "name": "credential.jwt_provider.jwt_keystore_aliases.signing_keystore",
    "label": "Key Store",
    "type": "file"
  }
 ]
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachbearbeitungsskript

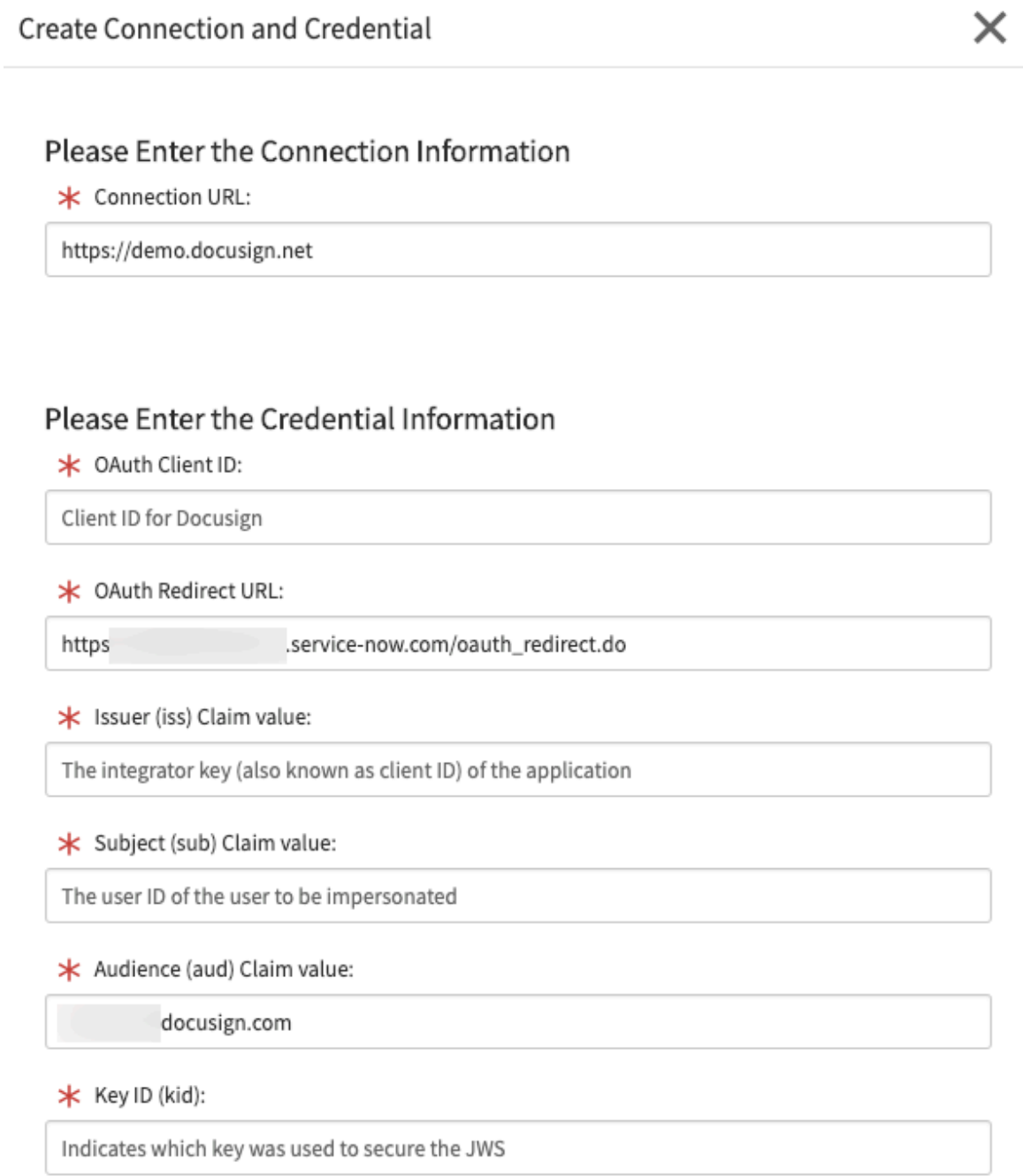
Das folgende Nachverarbeitungsskript ordnet Anwendereingaben Feldern in der Tabelle „sn_docusign_Spoke_Accounts“ zu.

```
(function execute(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData) {
 var jsonDynamicDataP = JSON.parse(jsonDynamicData);
 var accountGR = new GlideRecord("sn_docusign_spoke_accounts");
    accountGR.setValue("account_name",
 jsonDynamicDataP["additional.docusign_account_name"]);
    accountGR.setValue("alias", aliasId);
    accountGR.setValue("email", jsonDynamicDataP["additional.docusign_account_email"]);
    accountGR.setValue("id", jsonDynamicDataP["additional.docusign_account_id"]);
    accountGR.insert();
})(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData);
```

Resultierendes Konfigurationsformular für DocuSign-Verbindungen und -Anmeldeinformationen

Wenn der Anwender zum zugehörigen DocuSign-Alias für Verbindungen und Anmeldeinformationen navigiert und auswählt **Neue Verbindung Und Anmeldeinformationen Erstellen** , Das folgende Dialogfeld wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erstellen Sie eine Konfigurationsvorlage

Erstellen Sie eine Vorlage, die die Eingaben definiert, die zum Einrichten einer Spoke erforderlich sind. Legen Sie statische Schlüssel-Wert-Paare fest, um Datensätze zu erstellen und Werte festzulegen, die für jede Integration gelten. Legen Sie dynamische Schlüssel-Wert-Paare fest, um Anwendereingaben zu erfassen und Feldwerte festzulegen, die variieren können. Mit dieser Vorlage können Administratoren und Flow-Designer die Spoke über ein einzelnes Formular einrichten.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Konfigurationsvorlagen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie den Typ der Konfigurationsvorlage aus, die Sie erstellen möchten.

Konfigurationstyp	Beschreibung
HTTP-Verbindung mit Gewährungstyp „OAuth-Autorisierungscode“	Erstellt eine Vorlage zum Registrieren des Drittparteisystems als OAuth-Anbieter mithilfe eines Autorisierungscodes.
HTTP-Verbindung mit Gewährungstyp „OAuth JWT Bearer“	Erstellt eine Vorlage zum Registrieren des Drittparteisystems als OAuth-Anbieter mithilfe eines JSON-Webtoken.
HTTP-OAuth mit Gewährungstyp „Client-Anmeldeinformationen“	Erstellt eine Vorlage zur Integration mit einer Drittanbieteranwendung über die OAuth 2,0-Authentifizierung, die den Gewährungstyp „Client-Anmeldeinformationen“ verwendet.
HTTP-Verbindung mit Gewährungstyp für OAuth-Client-Anmeldeinformationen (externer Speicher)	Erstellt eine Vorlage, die das Senden einer OAuth-Tokenanforderung ermöglicht, die Client-Anmeldeinformationen enthält, die von einem externen Speicher an einen OAuth-Server über den MID-Server gespeichert werden.
HTTP-Verbindung mit Anmeldeinformationsformular für Standardauthentifizierung	Erstellt eine Vorlage zur Integration mit dem Drittparteisystem mithilfe der Standardauthentifizierung.
HTTP-Verbindung mit Anmeldeinformationen für API-Schlüssel	Erstellt eine Vorlage zur Integration mit dem Drittparteisystem mithilfe eines API-Schlüssels.
Andere Konfiguration	Erstellt eine leere Vorlage, mit der Sie eine Vorlage für die anwenderdefinierte Authentifizierung einrichten können.

4. In **Name** Feld einen Namen hinzufügen, um die Vorlage zu identifizieren.
5. In **Standarddatenvorlage** Nehmen Sie alle erforderlichen Änderungen vor.

   Dieses Feld legt statische Informationen fest, die für jede Integration gelten. Beispielsweise können Sie die API und die Token-URL festlegen, wenn der Wert für jede Integration gilt.

   Diese Objekte in der Standarddatenvorlage sind erforderlich:

   - `Anmeldeinformationen` : Erstellt einen Anmeldeinformationsdatensatz mit den erforderlichen Feldern.
   - `Verbindung` : Erstellt einen Verbindungsdatensatz mit den erforderlichen Feldern. Greifen Sie mit auf Verbindungsattribute zu `Extended_attributes` Untergeordnetes Objekt. Zum Beispiel:

```
"connection": {
        "extended_attributes": {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "api_version": "v1"

        },
    "connection_url": "https://<provider-domain-name>.com",
    "name": "Spoke Connection",
    "table": "http_connection"
}
```

Sie können verwenden `Zusätzlich` Objekt zum Einrichten von Daten für eine anwenderdefinierte Tabelle und Verwenden des Nachverarbeitungsskripts, um die Daten in die Tabelle einzufügen.

Hinweis: In der Standarddatenvorlage für den Gewährungstyp „OAuth-Autorisierungscode“ die Werte für `oauth_Entity_Profile_scope` Und `oauth_Entity_scope` Schlüssel müssen übereinstimmen. Im folgenden Beispiel haben beide Schlüssel die `E-Mail-Adresse des Anwenders lesen` Wert.

```
"oauth_entity_profile": [
      {
       "grant_type": "authorization_code",
       "name": "<provider-name> Profile",
       "default": true,
       "oauth_entity_profile_scope": [
        "Read user's email"
       ]
      }
    ],
    "code_challenge_method": "S256",
    "type": "consumer",
    "oauth_entity_scope": [
      {
       "oauth_entity_scope": "Read user's email",
       "name": "email"
      }
    ],
```

6. In **Dynamisches Datenschema** Nehmen Sie alle erforderlichen Änderungen vor.

   Dieses Feld Damit werden Informationen festgelegt, die der Benutzer zum Einrichten der Integration eingeben muss. Beispielsweise können Sie Schlüssel-Wert-Paare aus Benutzername und Passwort hinzufügen, um benutzerdefinierte Werte zu erfassen.

   Felder im dynamischen Datenschema enthalten diese Eigenschaften:

   - `Name` : Das Feld, dem die Eingabe des Anwenders zugeordnet ist. Um beispielsweise Anwendereingaben dem Feld Verbindungs-URL im Verbindungsdatensatz zuzuordnen, geben Sie ein `Connection.connection_url` .
   - `Bezeichnung` : Die Feldbezeichnung, die dem Anwender beim Abschließen der Vorlage angezeigt wird.
   - `Typ` : Der Feldtyp. Stellen Sie sicher, dass dieser Datentyp mit dem Datentyp des Felds übereinstimmt, dem Sie den Wert zuordnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- DEFAULTVALUE : Optional. Der Standardwert des Felds. Wenn kein Standard angegeben ist, wird der Tipp angezeigt.
- Tipp : Optional. Hinweistext, der angezeigt werden soll, wenn kein Standardwert vorhanden ist.

Hinweis: Wenn Sie eine Vorlage für die Authentifizierung des OAuth-JWT-Bearer-Gewährungstyps einrichten, möchten Sie möglicherweise eine Anwendereingabe für ein einzelnes Schlüssel-Wert-Paar in eingeben jwt_claim_validation Array. Sie können auf ein einzelnes Schlüssel-Wert-Paar im dynamischen Datenschema verweisen, indem Sie auf seinen Index im Array verweisen. Beispielsweise kann Ihre Standarddatenvorlage dieses Fragment enthalten.

```
"jwt_claim_validation" : [ {
      "name" : "iss",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-iss-claim>"
    }, {
      "name" : "sub",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-sub-claim>"
    }, {
      "name" : "aud",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-aud-claim>"
    }, {
      "name" : "scope",
      "is_standard" : false,
      "data_type" : "string",
      "value" : "signature impersonation"
    } ],
```

Weitere Informationen finden Sie unter iss Schlüssel-Wert-Paar mit dem Null-basierten Index des Elements: Credential.jwt_Provider.jwt_claim_validation[0].value .

7. **Wahlweise:** In **Nachverarbeitungsskript** Ein Skript hinzufügen, das c Damit werden zusätzliche Datensätze erstellt, die für die Integration erforderlich sind. Wenn Ihre Spoke beispielsweise benutzerdefinierte Tabellen enthält, können Sie Datensätze in diesen Tabellen auf der Grundlage von Benutzereingaben in der Konfigurationsvorlage erstellen. Dieses Skript wird ausgeführt, nachdem die Verbindungs- und Anmeldeinformationsdatensätze erstellt wurden.
Das Nachverarbeitungsskript hat Zugriff auf diese globalen Objekte.

Globales Objekt	Beschreibung
aliasId	SYS_ID des Alias-Datensatzes aus der Tabelle „Alias für Verbindungen und Anmeldeinformationen“ [sys_alias].
connectionSysId	SYS_ID des Verbindungsdatensatzes, der von der Vorlage erstellt wurde.
JsonDefaultData	JSON-Inhalt aus dem **Standarddatenvorlage** Feld im Zeichenfolgenformat.
JsonDynamicData	JSON-Inhalt aus dem **Dynamische Datenvorlage** Feld im Zeichenfolgenformat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. In **Skript Vorbearbeiten** Ein Skript hinzufügen, um die zusätzlichen Felder beim Bearbeiten einer Verbindung vorab auszufüllen.

   Dieses Skript gibt ein Array von Objekten zurück. Jedes Objekt verfügt über ein Name-Wert-Paar zum Ausfüllen der zusätzlichen Felder. Wenn die Verbindung beispielsweise Felder erfordert, die sich in einer anwenderdefinierten Tabelle befinden, können Sie diese Felder der anwenderdefinierten Tabelle zuordnen.

   Die **Skript Vorbearbeiten** Hat Zugriff auf die folgenden globalen Objekte:

Globales Objekt	Beschreibung
aliasId	SYS_ID des Alias-Datensatzes aus der Tabelle „Alias für Verbindungen und Anmeldeinformationen“ [sys_alias].
connectionSysId	SYS_ID des Verbindungsdatensatzes, der von der Vorlage erstellt wurde.
JsonDefaultData	JSON-Inhalt aus dem **Standarddatenvorlage** Feld im Zeichenfolgenformat.
JsonDynamicData	JSON-Inhalt aus dem **Dynamische Datenvorlage** Feld im Zeichenfolgenformat.

   Jedes Objekt im Skript verfügt über die folgenden Eigenschaften:

   - `Name` : Name des anwenderdefinierten Felds zur Angabe des Werts in der Verbindung.
   - `Wert` : Wert, den Sie zuordnen möchten, um das anwenderdefinierte Feld auszufüllen. Sie können das Feld entweder mithilfe einer Funktion, einer Variable oder durch hartes Codieren zuordnen.

   Die folgenden Datentypen werden für die Felder unterstützt:

   Unterstützte Datentypen für die Felder

Typ	Beschreibung
Text	Zeichenfolgenwert.
Boolean	Auswahlfeld. Auswahl gibt den Wert „wahr“ an, und wenn die Auswahl aufgehoben wird, wird der Wert „falsch“ angezeigt
Anzahl	Numerischer Wert.
Datum	Datumswert im Format JJJJ-mm-TT. Sie können auch das GlideDate-Objekt verwenden.
Auswahl	Liste der gültigen Auswahlmöglichkeiten, die in definiert sind **Dynamisches Datenschema** Feld.
Referenz	Gültiger GlideRecord.
Auswahlgruppe	Gruppen, die einen anderen Satz von Feldern enthalten. Diese Gruppen sind als Auswahl in einer Dropdown-Liste verfügbar, wenn Sie eine Verbindung bearbeiten. Die Felder in jeder Gruppe werden angezeigt, wenn Sie die erforderliche Gruppe aus der Dropdown-Liste auswählen. Betrachten Sie beispielsweise die folgende Struktur der Optionsgruppe, die in definiert ist **Dynamisches Datenschema** Feld:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung

	<pre>{
	"name": "radio_groups",
	"label": "Radio Groups",
	"type": "radio",
	"groups": [{
	"name": "radio_group1",
	"label": "Radio Group 1",
	"fields": [{
	"name": "radio_field1",
	"label": "Radio Field 1",
	"type": "text",
	"defaultValue": "efgh",
	"mandatory": true
	}]
	}, {
	"name": "radio_group2",
	"label": "Radio Group 2",
	"fields": [{
	"name": "radio_field2",
	"label": "Radio Field 2",
	"type": "text",
	"defaultValue": "abcd",
	"mandatory": true
	}],
	"default_group": true
	}</pre>
	In diesem Beispiel können Sie das folgende Codeausschnitt verwenden, um zu verstehen, wie Optionsgruppen im Skript verwendet werden, indem Sie Dot-Walking verwenden:
	<pre>{
	name: "radio_field.first_radio_group.radio_field1",
	value: "radio field 1"
	}, {
	name:
	"radio_field.second_radio_group.radio_field2",
	value: "radio field 2"
	}, {
	name: “radio_groups”,
	value: gr.getValue(‘radio_groups’)
	}</pre>
	Weitere Informationen zur Verwendung von Dot-Walking finden Sie unter Dot-Walking .

Tipp: Wenn die vorab ausgefüllten Werte beim Bearbeiten einer Verbindung nicht in den Feldern angezeigt werden, navigieren Sie zu **Systemdiagnostik** > **Sitzung debuggen** > **Protokoll debuggen** Zur Diagnose des Problems.

9. **Wahlweise:** In **Testaktion** Geben Sie den Namen der Testaktion ein.
   Durch das Erstellen einer Testaktion können Sie eine Verbindung direkt aus einer Integrationsaktion in der Flow-Ansicht von testen Workflow-Studio. Die Testaktion verwendet eine Aktionsdefinition, um den Alias

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu testen, an den die Vorlage derzeit angehängt ist. Details finden Sie unter Erstellen Sie eine Testaktion, um einen Verbindungsalias aus einer Konfigurationsvorlage zu testen .

10. Fügen Sie die Vorlage einem Alias für Verbindungen und Anmeldeinformationen hinzu.
    a. Navigieren zu **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
    b. Öffnen Sie den Aliasdatensatz für die Spoke.
    c. In **Konfigurationsvorlage** Klicken Sie auf das Suchsymbol.
    d. Wählen Sie die von Ihnen erstellte Vorlage aus der Liste aus.
    e. Klicken Sie auf **Aktualisieren**.

Ergebnis

Wenn der Anwender zum zugehörigen Alias für Verbindungen und Anmeldeinformationen navigiert und auswählt **Neue Verbindung Und Anmeldeinformationen Erstellen** , Wird ein Dialogfeld angezeigt, um die Eingabe zu erfassen. Wenn Sie eine Vorlage für den Gewährungstyp „OAuth-Autorisierungscode“ erstellt haben, können Sie auch ein OAuth-Token aus diesem Dialogfeld abrufen.

Nächste Maßnahme

Testen Sie die Vorlage, indem Sie zum zugehörigen Alias für Verbindungen und Anmeldeinformationen navigieren und auswählen **Neue Verbindung Und Anmeldeinformationen Erstellen** . Überprüfen Sie, ob das Dialogfeld die erwarteten Daten erfasst und die erforderlichen Datensätze im System erstellt.

Erste Schritte mit Verbindungen

Verwenden Sie die Verbindungstabelle, um eine Standard-, JMS-, JDBC- oder HTTP(s)-Verbindung mit einem Zielhost einzurichten.

Verbindungstabelle

Die Tabelle „Verbindung“ (sys_connection) ist die Basistabelle für alle Verbindungstabellen. Sie können Verbindungen für die folgenden Protokolle einrichten:

- Basisverbindung für PowerShell und SSH
- JDBC
- JMS
- HTTP(s)

Die Verbindungstabelle verweist auf die Verbindungsalias-Tabelle, die den Verbindungsalias mit Verbindungsinformationen koppelt. Jede Verbindung zeichnet die folgenden Informationen auf:

Basisverbindungseigenschaften

Feld	Beschreibung
Name	Name der Verbindung Dieses Feld muss in der Tabelle eindeutig sein.
Anmeldeinformationen	Geben Sie die Anmeldeinformationen an, die für diese Verbindung verwendet werden sollen. Dies ist optional.
Verbindungsalias	Der Verbindungsalias löst die Verbindung und die Anmeldeinformationen zur Laufzeit auf. Pro Verbindungsalias ist jeweils nur eine Verbindung aktiv.
Aktiv	Aktivieren Sie das Kontrollkästchen, um die aktuelle Verbindung zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basisverbindungseigenschaften (Fortsetzung)

Feld	Beschreibung
Domäne	Domäne, zu der die Verbindung gehört.

Die Anmeldeinformationen sind für alle aktiven Verbindungen eindeutig, sofern sie nicht leer sind.

Upgrade der Verbindungsinformationen

- Die Tabellen „JDBC-Verbindung“ [jdbc_connection] und „JMS-Verbindung“ [orch_jms_ds] sind vorhandene Orchestration-Verbindungstabellen, die jetzt von der Tabelle „Verbindung“ [sys_connection] erweitert werden. Die Tabellen wurden ursprünglich von „sys_metadata“ erweitert. Die auf „sys_metadata“ bezogenen Daten wurden entfernt.
- Die Tabellen werden aus dem Laufzeit-Plugin „Orchestration“ [com.snc.runbook_automation.runtime] zum Plugin „Anmeldeinformationen und Verbindungen“ verschoben.
- Der Upgrade-Prozess ruft JDBC- und JMS-Verbindungsinformationen ab, erstellt entsprechende Verbindungsaliasnamen und weist den Alias der zugehörigen Verbindung zu.
- JDBC-Feldnamenänderungen:
  - Der JDBC-Server wird in Host umbenannt
  - Der Datenbankport wird in Port umbenannt
  - Daten des JDBC-Servers und der Datenbank werden während des Upgrades zu Host und Port migriert

Basisverbindungen für PowerShell und SSH erstellen

Konfigurieren Sie die Verbindungsinformationen für die Verwendung mit einer benutzerdefinierten Aktivität oder Aktion, die das PowerShell- oder Secure Shell-Protokoll (SSH) verwendet.

Vorbereitungen

Erforderliche Rolle: admin oder catalog_admin

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Basisverbindung für PowerShell und SSH** aus.
4. Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Eindeutiger Name des Verbindungsdatensatzes
Anmeldeinformationen	Wählen Sie den Datensatz mit Anmeldeinformationen aus, der zur Autorisierung der Verbindung verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
Host	Vollständig qualifizierter Domänenname des Zielhosts, auf dem das System die Aktivität oder Aktion ausführt. Zum Beispiel: host.domain.com.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legt die Domäne fest, in der die Aktivität ausgeführt wird. Flow Designer unterstützt keine Domänentrennung und dieses Feld ignoriert.
Standardport überschreiben	Von der Verbindung verwendeter Zielport. Wenn Sie dieses Feld leer lassen, verwendet das System den Wert für den Standardport.
MID-Server verwenden	Aktivieren Sie das Kontrollkästchen, um eine Verbindung mit dem Zielhost über einen MID-Server herzustellen. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“. **Hinweis:** PowerShell erfordert einen MID-Server.
MID Auswahl	Option zum Auswählen eines bestimmten MID-Servers oder MID-Clusters. Wählen Sie eine der folgenden Optionen aus. ○ **MID-Server automatisch auswählen** : Ihr ServiceNow Instanz wählt aus MID-Server Ohne manuelle Eingabe. ○ **Bestimmter MID-Server** : Ihr ServiceNow Instanz verwendet MID-Server Die Sie angeben. ○ **Spezifischer MID-Cluster** : Ihr ServiceNow Instanz verwendet den von Ihnen angegebenen MID-Cluster. Ein MID-Cluster ist eine Gruppe von MID-Servern, die Ihren aktivieren ServiceNow Instanz zur Verarbeitung mehrerer Integrationen und zur Verbesserung der Integrationsgeschwindigkeit. Weitere Informationen finden Sie unter Ein MID-Server-Cluster konfigurieren . Dieses Feld ist verfügbar, wenn **MID-Server verwenden** Ist aktiviert. **Hinweis:** Stellen Sie sicher, dass IntegrationHub Verbindungsdatensatz wird referenziert, kein Orchestration Verbindungsdatensatz.
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Um mehr darüber zu erfahren, wie ein MID-Server Ist während der Laufzeit ausgewählt, siehe MID-Server-Auswahl . Dieses Feld ist nur sichtbar, wenn **MID-Server automatisch auswählen** Ist aus der MID-Auswahlliste ausgewählt.
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .
MID-Server	Spezifisch MID-Server Auf dem der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Bestimmter MID-Server** Ist aus der MID-Auswahlliste ausgewählt.
MID-Cluster	Der spezifische MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **MID-Server verwenden** Ist aktiviert, und **Spezifischer MID-Cluster** Ist aus der MID-Auswahlliste ausgewählt.

5. Klicken Sie auf **Absenden**.

HTTP(s)-Verbindung erstellen

Die HTTP(s)-Verbindung stellt die Informationen bereit, mit der benutzerdefinierte HTTP(s)-Aktionen oder -Aktivitäten eine Verbindung herstellen.

Vorbereitungen

Erforderliche Rolle: connection_admin

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**, Klicken Sie auf **Neu** , Und wählen Sie aus **HTTP(s)-Verbindung** .
2. Fügen Sie die folgenden Verbindungsinformationen hinzu, und klicken Sie auf **Absenden**:

Feld	Beschreibung
Name	Eindeutiger Name dieser HTTP(s)-Verbindung.
Anmeldeinformationen	Wählen Sie den Datensatz mit Anmeldeinformationen aus, der zur Autorisierung der Verbindung verwendet wird.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
URL-Builder	Geben Sie entweder die Verbindungs-URL manuell ein, oder verwenden Sie das System, um die URL basierend auf den Eingaben zu erstellen. Standardmäßig ist dieses Kontrollkästchen deaktiviert. Wenn diese Option aktiviert ist, wird die Verbindungs-URL aus den folgenden Feldern berechnet: ○ Gegenseitige Authentifizierung – Aktivieren Sie das Kontrollkästchen, wenn die gegenseitige Authentifizierung verwendet wird. ○ Protokoll – Wenn keine gegenseitige Authentifizierung verwendet wird, geben Sie das Protokoll ein. Der Standardwert ist HTTPs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Protokollprofil – Wenn die gegenseitige Authentifizierung verwendet wird, geben Sie das Protokollprofil aus „sys_protocol_profile“ ein. ◦ Host ◦ Port ◦ Basispfad – Pfad der Verbindungszeichenfolge. **Hinweis:** Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
Verbindungs-URL	Wenn der URL-Builder deaktiviert ist, geben Sie die Verbindungs-URL in dieses Feld ein. **Hinweis:** Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legen Sie die Domäne, fest in der die Aktion oder Aktivität ausgeführt wird.
MID-Server verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID-Auswahl	Option zum Auswählen eines bestimmten MID-Servers oder MID-Clusters. Wählen Sie eine der folgenden Optionen aus. ◦ **MID-Server automatisch auswählen** : Ihr ServiceNow Instanz wählt aus MID-Server Ohne manuelle Eingabe. ◦ **Bestimmter MID-Server** : Ihr ServiceNow Instanz verwendet MID-Server Die Sie angeben. ◦ **Spezifischer MID-Cluster** : Ihr ServiceNow Instanz verwendet den von Ihnen angegebenen MID-Cluster. Ein MID-Cluster ist eine Gruppe von MID-Servern, die Ihren aktivieren ServiceNow Instanz zur Verarbeitung mehrerer Integrationen und zur Verbesserung der Integrationsgeschwindigkeit. Weitere Informationen finden Sie unter Ein MID-Server-Cluster konfigurieren . Dieses Feld ist verfügbar, wenn **MID-Server verwenden** Ist aktiviert. **Hinweis:** Stellen Sie sicher, dass IntegrationHub Verbindungsdatensatz wird referenziert, kein Orchestration Verbindungsdatensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Um mehr darüber zu erfahren, wie ein MID-Server Ist während der Laufzeit ausgewählt, siehe MID-Server-Auswahl . Dieses Feld ist nur sichtbar, wenn **MID-Server automatisch auswählen** Ist aus der MID-Auswahlliste ausgewählt.
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .
MID-Server	Spezifisch MID-Server Auf dem der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Bestimmter MID-Server** Ist aus der MID-Auswahlliste ausgewählt.
MID-Cluster	Der spezifische MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **MID-Server verwenden** Ist aktiviert, und **Spezifischer MID-Cluster** Ist aus der MID-Auswahlliste ausgewählt.
Verbindungszeitüberschreitung	Anzahl der Millisekunden, die das System auf eine erfolgreiche Hostverbindung wartet. Wenn während dieser Zeit keine erfolgreiche Verbindung hergestellt wird, läuft die Verbindungsanforderung ab. Lassen Sie dieses Feld leer, um den Standard-Zeitüberschreitungswert für Verbindungen zu verwenden. **Hinweis:** Vermeiden Sie das Festlegen von **Verbindungszeitüberschreitung** Wert auf Null, da dies zu einer veralteten Verbindung führen kann.
Additional_http_Headers (Registerkarte „Attribute“)	Fügen Sie alle erforderlichen zusätzlichen Header hinzu, z. B. sap-Client=100. Wenn Sie mehrere Header hinzufügen, trennen Sie sie durch ein Semikolon.
odata_Ping_url (Registerkarte „Attribute“)	Die standardmäßige OData-Ping-URL ist /sap/bc/ping. Um die Ping-URL für den OData-Heartbeat zu bearbeiten, wählen Sie das Sperrsymbol, bearbeiten Sie die URL, und wählen Sie das Sperrsymbol erneut aus.

3. Klicken Sie auf **Absenden**.
   Sie können jetzt eine benutzerdefinierte HTTP(s)-Aktion oder -Aktivität erstellen.

JDBC-Verbindung erstellen

Die JDBC-Verbindung enthält die Informationen, mit der benutzerdefinierte JDBC-Aktionen oder -Aktivitäten eine Verbindung zu verschiedenen Zieldatenbanken herstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Sie müssen über eine geeignete JAR-Datei verfügen, unabhängig davon, ob sie mit der Instanz oder mit einer benutzerdefinierten JAR-Datei bereitgestellt wird.

Hinweis: Die ServiceNow-Instanz stellt die Dateien mysql-connector-java-5.1.21.jar, sql-server-jdbc-4.0.jar und ojdbc6.jar als Teil des aktuellen Release bereit, das MySQL-, SQLServer- und Oracle-Datenbanken unterstützt. Andere Datenbanken wie Sybase oder DB2 Universal müssen eine benutzerdefinierte JAR-Datei verwenden, die in die Instanz hochgeladen werden muss, bevor die JDBC-Verbindung festgelegt wird.

Erforderliche Rolle: connection_admin

Warum und wann dieser Vorgang ausgeführt wird

JDBC-Anmeldeinformationen werden von der Aktivitätendesignervorlage separat abgerufen und unterstützen externe Anmeldeinformationsspeicher wie CyberArk.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Verbindungen**, Klicken Sie auf **Neu** Und wählen Sie aus **JDBC-Verbindung** .
2. Füllen Sie das Formular anhand der Felder in der Tabelle aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

JDBC-Verbindungsfelder

Feld	Datenbankformat	Beschreibung
Name	Alle	Eindeutiger Name dieser JDBC-Verbindung. Zum Beispiel könnten Sie **JDBC MySQLProd** eingeben.
Berechtigung	Alle	Fügen Sie Anmeldeinformationen für den JDBC-Provider hinzu.
Verbindungsalias	Alle	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
Abfragezeitüberschreitung	Alle	Maximale Dauer, die die JDBC-Abfrage ohne Antwort ausgeführt werden darf.
Verbindungstimeout	Alle	Anzahl der Sekunden, die das System wartet, bevor eine JDBC-Verbindung oder eine Verbindungsanforderung geschlossen wird. Beispiel: Wenn **Verbindungszeitüberschreitung** Der Wert ist 10 Sekunden. Das System wartet 10 Sekunden auf eine erfolgreiche Verbindung. Wenn während dieser Zeit keine erfolgreiche Verbindung hergestellt wird, läuft die Verbindungsanforderung ab. Wenn eine erfolgreiche Verbindung auftritt, bleibt die Verbindung geöffnet, bis ein Zeitraum von 10 Sekunden inaktiv ist. Sobald die Verbindung 10 Sekunden lang inaktiv war, wird die Verbindung geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
		Hinweis: Vermeiden Sie das Festlegen von **Verbindungszeitüberschreitung** Wert auf Null, da dies zu einer veralteten Verbindung führen kann.
Aktiv	Alle	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Alle	Domäne für diese Tabelle. Standardmäßig wird die Tabelle „JDBC-Verbindung“ [jdbc_connection] in der Domäne **global** ausgeführt.
Format	Alle	Datenbanktyp für diese Verbindung. Die Standardoptionen sind: ○ **MySQL** ○ **Oracle** ○ **SQL Server** ○ **Keine** Sie können hinzufügen **Sybase** Oder **DB2 Universal** In die Auswahlliste, indem die entsprechende JDBC-Treiber-JAR-Datei in die Instanz hochgeladen wird. Orchestration Erkennt diese Treiber automatisch, wenn sie in das System geladen werden, und fügt sie dieser Liste hinzu.
Host	Oracle, MySQL, SQLServer	Hostname oder IP-Adresse des Datenbankservers.
Oracle-SID	Oracle	Der Site-Identifier der Oracle-Datenbank. Der Standardwert ist **orcl**.
Oracle-Anschluss	Oracle	Port, den die Oracle-Datenbank verwendet. Der Standardwert ist **1521**.
Datenbankname	MySQL, SQLServer	Name der Datenbank.
Port	MySQL, SQLServer	Port, den die ausgewählte Datenbank verwendet.
Instanzname	SQLServer	Instanzname für den ausgewählten SQLServer.
Verbindungs-URL	Alle	URL, mit der der MID Server eine Verbindung zu der angegebenen Datenbank herstellt. Die URL wird beim Speichern des Formulars automatisch erstellt und ist für die Standarddatenbanken schreibgeschützt. **Hinweis:** Wenn das ausgewählte Format keine der Standarddatenbanken ist, müssen Sie die Verbindungs-URL manuell erstellen, damit der MID Server darüber informiert ist, wie die Verbindung erstellt werden soll.
JDBC-Laufwerk	Keiner, DB2 Universal, Sybase	Der für diese Verbindung zu verwendende JDBC-Treiber, wenn es sich nicht um eine Standarddatenbank handelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
		Hinweis: Wenn Sie eine Sybase- oder DB2 Universal-Datenbank hinzufügen, müssen Sie den Treibernamen in dieses Feld eingeben und die Treiber-JAR-Datei in die Instanz hochladen.
MID Server verwenden	Alle	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID Auswahl	Alle	Option zum Auswählen eines bestimmten MID-Servers oder MID-Clusters. Wählen Sie eine der folgenden Optionen aus. ○ **MID-Server automatisch auswählen** : Ihr ServiceNow Instanz wählt aus MID-Server Ohne manuelle Eingabe. ○ **Bestimmter MID-Server** : Ihr ServiceNow Instanz verwendet MID-Server Die Sie angeben. ○ **Spezifischer MID-Cluster** : Ihr ServiceNow Instanz verwendet den von Ihnen angegebenen MID-Cluster. Ein MID-Cluster ist eine Gruppe von MID-Servern, die Ihren aktivieren ServiceNow Instanz zur Verarbeitung mehrerer Integrationen und zur Verbesserung der Integrationsgeschwindigkeit. Weitere Informationen finden Sie unter Ein MID-Server-Cluster konfigurieren . Dieses Feld ist verfügbar, wenn **MID-Server verwenden** Ist aktiviert. **Hinweis:** Stellen Sie sicher, dass IntegrationHub Verbindungsdatensatz wird referenziert, kein Orchestration Verbindungsdatensatz.
Fähigkeiten	Alle	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Erforderliche Fähigkeiten bestimmen, welcher MID-Server zur Laufzeit ausgewählt wird. Um mehr darüber zu erfahren, wie ein MID-Server Ist während der Laufzeit ausgewählt, siehe MID-Server-Auswahl . Dieses Feld ist nur sichtbar, wenn **MID-Server automatisch auswählen** Ist aus der MID-Auswahlliste ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Datenbankformat	Beschreibung
MID-Anwendung	Alle	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .
MID-Server	Alle	Spezifisch MID-Server Auf dem der Schritt ausgeführt wird. Dieses Feld ist nur sichtbar, wenn **Bestimmter MID-Server** Ist aus der MID-Auswahlliste ausgewählt.
MID-Cluster	Alle	Der spezifische MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **MID-Server verwenden** Ist aktiviert, und **Spezifischer MID-Cluster** Ist aus der MID-Auswahlliste ausgewählt.

3. Klicken Sie auf **Absenden**.

Zugehörige Informationen

JDBC-Anmeldeinformationen

JMS-Verbindung erstellen

Konfigurieren Sie Ihr System für die Verwendung von Java Messaging Service (JMS) mit einer benutzerdefinierten JMS-Aktivität oder -Aktion.

Vorbereitungen

Erforderliche Rolle: connection_admin

Warum und wann dieser Vorgang ausgeführt wird

Der MID Server muss über die richtigen JMS Connection Factorys für Ihre Organisation verfügen. Konfigurieren Sie diese Werte in `mid.property.jms.command.allowed_factory_names`Eigenschaft, gefunden in **MID-Server** > **Eigenschaften**an. Die Standardwerte für diese Eigenschaft können in einen beliebigen Wert oder eine durch Kommas getrennte Liste von Werten geändert werden, die der JMS-Provider eines Drittanbieters bekanntgibt.

Prozedur

1. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Verbindungen**an.
2. Klicken Sie Auf **Neu** , Wählen Sie aus **JMS-Verbindung** Füllen Sie das Formular aus, und klicken Sie dann auf **Übermitteln** .

Option	Bezeichnung
Name	Eindeutiger Name dieser Connection Factory.
Anmeldeinformationen	Fügen Sie Anmeldeinformationen für den JMS-Provider hinzu.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
Ursprüngliche Kontext-Werkseinstellung	Name der JNDI-Klasse, die zum Erstellen des Initial-Context verwendet wird. **Hinweis:** Um beispielsweise eine Verbindung zu ActiveMQ V5.10 (JMS-Provider) herzustellen, lautet der Wert org.apache.activemq.jndi.ActiveMQInitialContextFactory.
Provider-URL	Speicherort der laufenden JMS-Provider-Installation. **Hinweis:** So stellen Sie beispielsweise eine Verbindung zu ActiveMQ V5.1 her: tcp://ipAdresseOderHostname: 61616.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diese Verbindung zu aktivieren.
Domäne	Legen Sie die Domäne, fest in der die Aktion oder Aktivität ausgeführt wird.
MID Server verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen MID Server für diese Aktion oder Aktivität zu verwenden. Falls aktiviert, definieren Sie Felder im Abschnitt „Erweiterte MID Server-Konfiguration“.
MID-Auswahl	Option zum Auswählen eines bestimmten MID-Servers oder MID-Clusters. Wählen Sie eine der folgenden Optionen aus. ○ **MID-Server automatisch auswählen** : Ihr ServiceNow Instanz wählt aus MID-Server Ohne manuelle Eingabe. ○ **Bestimmter MID-Server** : Ihr ServiceNow Instanz verwendet MID-Server Die Sie angeben. ○ **Spezifischer MID-Cluster** : Ihr ServiceNow Instanz verwendet den von Ihnen angegebenen MID-Cluster. Ein MID-Cluster ist eine Gruppe von MID-Servern, die Ihren aktivieren ServiceNow Instanz zur Verarbeitung mehrerer Integrationen und zur Verbesserung der Integrationsgeschwindigkeit. Weitere Informationen finden Sie unter Ein MID-Server-Cluster konfigurieren . Dieses Feld ist verfügbar, wenn **MID-Server verwenden** Ist aktiviert.
MID-Cluster	Der spezifische MID-Cluster, den Sie verwenden möchten. Dieses Feld ist verfügbar, wenn **MID-Ser**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	ver verwenden Ist aktiviert, und **Spezifischer MID-Cluster** Ist aus der MID-Auswahlliste ausgewählt.
Fähigkeiten	Die Fähigkeiten, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion oder Aktivität von einem MID-Server aus, das die ausgewählten Fähigkeiten unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .
MID-Anwendung	Die Anwendung, die MID-Server unterstützten muss, um für die Auswahl in Frage zu kommen. Das System führt die Aktion einem MID-Server aus, das die ausgewählte Anwendung unterstützt. Wird nur angezeigt, wenn **MID-Server verwenden** ausgewählt ist. Um mehr darüber zu erfahren, wie MID-Server während der Laufzeit ausgewählt wird, siehe MID-Server-Auswahl .

3. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
4. Klicken Sie auf **Neu**, wählen Sie **JMS-Anmeldeinformationen** aus, und geben Sie dann den Benutzernamen und das Passwort ein, die der MID für die Kommunikation mit dem JMS-Provider verwenden soll.
   Weitere Informationen finden Sie unter JMS-Anmeldeinformationen.
5. Klicken Sie auf **Absenden**.
   Sie können jetzt eine benutzerdefinierte JMS-Aktion oder -Aktivität erstellen.

Verbindungsattribute für IntegrationHub erstellen

Definieren Sie verbindungsspezifische Variablen, die Sie in IntegrationHub-Integrationsschritten verwenden können.

Vorbereitungen

Erforderliche Rolle:

- Um Verbindungsattribute zu erstellen, ist die Administratorrolle erforderlich.
- Um Attributwerte zuzuweisen, ist die Rolle „connection_admin“ oder die Administratorrolle erforderlich.
- Die Rolle „action_designer“ oder die Administratorrolle ist erforderlich, Im Attribute in einer benutzerdefinierten Aktion zu verwenden, ist die Rolle „action_designer“ oder die Administratorrolle erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindungsattribute werden nur von Integrationsschritten verwendet, für die IntegrationHub abonniert werden muss. Weitere Informationen zum Aktivieren von finden Sie IntegrationHub, Siehe Fordern Sie an IntegrationHub Plugin an.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Integrationsschritt verwenden, müssen Sie eine Verbindung mit einem externen System herstellen. Verwenden Sie einen Alias für Verbindungen und Berechtigungen, anstatt die Verbindung inline zu definieren. Mit einem Alias können Sie die Verbindungsdetails einmal aktualisieren, ohne jede Aktion neu konfigurieren zu müssen. Jeder Aktionsschritt, bei dem ein Alias verwendet wird, erbt die ihm zugeordneten Attribute. Vom Flow Designer werden Attribute als Datenpillen angezeigt, die Sie in Ihren Aktionsschritt ziehen können. Sie können beispielsweise ein Seitengrößenattribut erstellen, das zu einem Abfrageparameter für den REST-Schritt wird.

Weitere Informationen zum Erstellen anwenderdefinierter Elemente Flow Designer Aktionen, siehe Aktionsdesigner an.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
2. Erstellen Sie einen Aliasdatensatz, oder wählen Sie einen aus.
3. Klicken Sie in der zugehörigen Liste „Verbindungsattribute“ auf **Neu**.
4. Legen Sie die Attributbezeichnung und den Feldtyp fest.
   Eine Liste der Feldtypen finden Sie unter Feldtypen .
5. Klicken Sie auf den zugehörigen Link „Erweiterte Ansicht“, um erweiterte Dictionary-Voreinstellungen für das Attribut festzulegen.
   Auf diese Weise lässt sich beispielsweise ein Attribut mit einem dynamisch berechneten Wert erstellen. Weitere Informationen finden Sie unter Wörterbucheintragsformular .
6. Klicken Sie auf **Absenden**.
7. Definieren Sie die Attributwerte im Verbindungsdatensatz.
   a. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Verbindungen**an.
   b. Erstellen Sie einen Verbindungsdatensatz mit demselben Verbindungstyp wie der Alias, oder wählen Sie einen aus.
   c. Wählen Sie unter **Verbindungsalias** den Alias mit Verbindungsattributen aus.
   d. Speichern Sie den Datensatz.
      Die Registerkarte „Attribute“ wird mit den im Aliasdatensatz definierten Verbindungsattributen gefüllt.
   e. Legen Sie Werte für die Attribute fest.
      Wenn für den Alias **Unterstützt mehrere aktive Verbindungen** aktiviert ist, können Sie einem Alias mehrere Verbindungsdatensätze zuordnen und in jedem Verbindungsdatensatz Attributwerte definieren. Wenn mehrere Verbindungsdatensätze mit Attributwerten für denselben Alias vorhanden sind, Die bei der Ausführung des Ablaufs verwendete Verbindung bestimmt die Attributwerte. Angenommen, Sie haben eine Aktion, die einen Alias mit zwei aktiven Verbindungsendpunkten verwendet: Produktion und Test. Das Attribut wird nach dem Wert aufgelöst, der von der zur Laufzeit verwendeten Verbindung festgelegt wird.
8. Fügen Sie den Alias einem Integrationsschritt im Aktionsdesigner hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren Sie zu Flow Designer, und erstellen oder wählen Sie eine Aktion.

b. Fügen Sie der Aktion einen Integrationsschritt hinzu.

c. Fügen Sie unter „Verbindungsdetails“ den Alias hinzu, für den Sie Attribute erstellt haben.

Die mit dem Alias verknüpften Verbindungsattribute werden als Datenpillen im Datenbereich angezeigt.

Hinweis: Das System verfolgt keinen Change an Bezeichnungen und Datentypen von Verbindungsattributen, nachdem Sie den Alias einem Schritt zugeordnet haben. Um die Bezeichnung oder den Datentyp eines Verbindungsattributs zu aktualisieren, löschen Sie den Alias aus dem Schritt, und fügen Sie ihn erneut hinzu.

Erste Schritte mit Anmeldeinformationen

Der MID Server verwendet die Anmeldeinformationen, die Sie in der Tabelle „Anmeldeinformationen“ [discovery_credentials] erstellen, um auf Ressourcen für Discovery, Orchestration, Service Mapping und Cloud Management zuzugreifen.

So verwenden MID Server Anmeldeinformationen

MID Server mit Windows verwenden standardmäßig die Anmeldeinformationen des MID Server-Service auf dem Hostcomputer zum Ermitteln von Windows-Geräten im Netzwerk. Das sollten Sie Konfigurieren Sie Anmeldeinformationen für Windows MID Server-Service Damit sie mindestens über lokale Administratorrechte verfügen. Für Linux Und UNIX Computer und Netzwerkgeräte verwendet der MID-Server die SSH- und SNMP-Anmeldeinformationen, die in der Instanz in konfiguriert sind **Discovery** > **Anmeldeinformationen**an.

MID-Server, die Orchestration Verwender müssen Zugriff auf die erforderlichen Anmeldeinformationen haben, um Befehle auf Computern im Netzwerk auszuführen, wie von angegeben Workflow-Aktivitäten . Orchestration kann dieselben SSH- und SNMP-Anmeldeinformationen wie verwenden Discovery, Hat aber zwei zusätzliche Anmeldeinformationen, die für bestimmte Workflow-Aktivitäten konzipiert sind: Windows(Für PowerShell-Aktivitäten) Und VMware.

Verschlüsselung und Entschlüsselung

Die Plattform speichert die Anmeldeinformationen in einem verschlüsselten Feld in der Tabelle „Anmeldeinformationen“ [discovery_credentials]. Einmal eingegeben, können sie nicht angezeigt werden.

Wenn der MID-Server Anmeldeinformationen anfordert ServiceNow AI Platform Entschlüsselt die Anmeldeinformationen mit dem folgenden Prozess:

1. Die Anmeldeinformationen werden in der Instanz mit dem festen Schlüssel „password2“ entschlüsselt.
2. Die Anmeldeinformationen werden in der Instanz mit dem öffentlichen Schlüssel des MID Servers erneut verschlüsselt.
3. Die Anmeldeinformationen werden im Lastenausgleichsmodul mit SSL verschlüsselt.
4. Die Anmeldeinformationen werden auf dem MID Server mit SSL entschlüsselt.
5. Die Anmeldeinformationen werden auf dem MID Server mit dem privaten Schlüssel des MID Servers entschlüsselt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Plattform verfügt nicht über separate Verschlüsselungsschlüssel für Instanzen mit mehreren Mandanten.

Reihenfolge der Anmeldeinformationen

Anmeldeinformationen kann ein Wert für die Reihenfolge im Anmeldeinformationsformular zugewiesen werden. Die Anwendung wird so gezwungen, alle verfügbaren Anmeldeinformationen in einer bestimmten Reihenfolge durchzugehen. Wenn Sie keinen Reihenfolgewert angeben, versucht die Anwendung zufällig die Anmeldeinformationen in der Tabelle „Anmeldeinformationen“ [Discovery_credential], bis sie eine findet, die funktioniert. Beispiel:

- Orchestration versucht, einen Befehl auf einem SSH-Server auszuführen, z. B. auf einem Linux- oder UNIX-Computer.
- Discovery versucht, ein SNMP-Gerät abzufragen, z. B. einen Drucker, einen Router oder eine USV.

Nach der Ermittlung der Anmeldeinformationen für ein Gerät erstellen Discovery und Orchestration anhand der Tabelle „Anmeldeinformationsaffinität“ [dscy_credentials_affinity] eine Affinität zwischen den Anmeldeinformationen und dem Gerät. Bei allen nachfolgenden Ermittlungen oder Orchestration-Aktivitäten wird versucht, die Anmeldeinformationen in dieser Tabelle einem Gerät zuzuordnen, für das eine Affinität besteht. Wenn sich die Anmeldeinformationen für ein Gerät ändern, testen Discovery und Orchestration alle verfügbaren Anmeldeinformationen erneut, bis sie eine neue Affinität herstellen.

Hinweis: Wenn Orchestration und Discovery installiert sind und der Anmeldeinformationsalias aktiviert ist, können mehrere Affinitäten vorhanden sein. In diesem Fall sucht die Plattform nach Anmeldeinformationen für jede Affinität und fügt die Anmeldeinformation für die Affinität mit der niedrigsten Reihenfolgenummer in die Probe ein.

Das Angeben einer Reihenfolge für die Anmeldeinformationen ist in den folgenden Situationen hilfreich:

- Die Tabelle „Anmeldeinformationen“ enthält viele Anmeldeinformationen, von denen einige häufiger als andere verwendet werden. Die Tabelle enthält beispielsweise 150 SSH-Anmeldeinformationen, und fünf dieser Anmeldeinformationen werden verwendet, um sich bei 90 % der Geräte anzumelden. Es empfiehlt sich, diese fünf Anmeldeinformationen mit Nummern niedriger Reihenfolge zu konfigurieren, die sie an den Anfang der Ausführungsliste setzen. Discovery Und Orchestration funktioniert schneller, wenn sie diese allgemeinen Anmeldeinformationen zuerst ausprobieren. Nach der ersten erfolgreichen Verbindung wird ServiceNow AI Platform Weiß, welche Anmeldeinformationen beim nächsten Mal für jedes Gerät verwendet werden sollen.
- Die ServiceNow AI Platform Hat aggressive Anmeldesicherheit. Konfigurieren Sie beispielsweise Datenbank-Anmeldeinformationen mit einem Wert niedriger Reihenfolge, wenn Solaris-Datenbankserver im Netzwerk nur drei fehlgeschlagene Anmeldeversuche bereitstellen, bevor Sie den MID-Server sperren.

Anmeldeinformationsaliasse

Anmeldeinformationsaliasse sind für verfügbar Discovery Und Orchestration .

Aliasse für Discovery ermöglichen einem Administrator Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwenden Sie ein Verhalten beim Filtern von Anmeldeinformationen mit konfigurierbaren Compliance-Ebenen.
- mehrere Anmeldeinformationsaliase einem Discovery-Zeitplan zuweisen.
- Verhindern Sie die Erstellung von Anmeldeinformationsaffinitäten, die unangemessene oder vertrauliche Anmeldeinformationen verwenden. Weitere Informationen finden Sie unter Anmeldeinformationsaffinitäten .

Aliasse für Orchestration ermöglichen Workflow-Erstellern Folgendes:

- jeder Aktivität in einem Orchestration-Workflow individuelle Anmeldeinformationen zuweisen
- jeder Aktion in Flow Designer individuelle Anmeldeinformationen zuweisen
- jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zuweisen.
- jedem Vorkommen derselben Aktion im Designer-Flow unterschiedliche Anmeldeinformationen zuweisen

Externe Anmeldeinformationsspeicher

Wenn Sie nicht möchten, dass Anmeldeinformationen in Ihrer Instanz gespeichert werden, können Sie externe Repositorien für Anmeldeinformationen verwenden. Externe Anmeldeinformationsspeicher speichern die Anmeldeinformationen an einem externen Standort, auf den Ihre Instanz zugreifen kann. CyberArk Ist der einzige unterstützte externe Anmeldeinformationsspeicher. Andere externe Speicher können jedoch mit der ServiceNow-API konfiguriert werden.

Verbindungs- und Anmeldealias erstellen

Definieren Sie einen Alias, um einen Anmelde- oder einen Verbindungsdatensatz zu kennzeichnen.

Vorbereitungen

Erforderliche Rolle:

- Die Administratorrolle ist erforderlich, um einen Alias zu erstellen.
- Die Rollen „credential_admin“ und „connection_admin“ haben Lesezugriff auf den Aliasdatensatz.

Warum und wann dieser Vorgang ausgeführt wird

Der Verbindungs- und Anmeldealias definiert einen Alias, der einen Anmelde- oder einen Verbindungsdatensatz kennzeichnet. Der Alias enthält diese Felder.

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aliasse für Verbindungen und Anmeldeinformationen

Feld	Beschreibung
Name	Name des Alias. Ein Alias darf nur Buchstaben, Zahlen und Unterstriche enthalten. Während eines Upgrades wird das Tag im Anmeldedatensatz zu einem Verbindungs- und Anmeldealias migriert. Wenn das Anmeldeinformations-Tag andere Sonderzeichen als Buchstaben, Zahlen und Unterstriche enthält, wird der Tag-Name nach dem Upgrade beibehalten. Sie können diesen migrierten Alias weiterhin verwenden, Sie können ihn allerdings erst aktualisieren, wenn Sie den Namen den Namensbeschränkungen entsprechend ändern.
ID	Eindeutiger Bezeichner für den Alias für Verbindungen und Anmeldeinformationen, basierend auf dem Format `Scope_Name.alias_Name` . ○ Wenn der Bereich global ist, ist die ID der Aliasname. Wenn Sie beispielsweise einen Workday-Alias im globalen Bereich erstellen, wird die ID auf festgelegt `workday` . ○ Wenn Sie einen Workday-Alias im Bereich der HR-App erstellen, wird die ID auf festgelegt `X_HR_App.Workday` .
Typ	Wählen Sie entweder aus **Anmeldeinformationen** Oder **Verbindung und Anmeldeinformationen** . Der Standardwert ist „Verbindung und Anmeldeinformationen“.
Anwendung	Anwendungsbereich, dem der Alias für Verbindungen und Anmeldeinformationen zugewiesen ist. Der aktuelle Sitzungsbereich, den Sie zuletzt in der Anwendungsauswahl ausgewählt haben, wird angezeigt. ○ Beispiel: **Global** Wird angezeigt, wenn es sich um den aktuellen Bereich für diese Sitzung handelt. ○ Sie können den Umfang in der Anwendungsauswahl ändern, bevor Sie einen Alias erstellen. Weitere Informationen zur Auswahl von Anwendungsbereichen finden Sie unter: ▪ Anwendungsbereich ▪ Anwendungen aus der Anwendungsauswahl auswählen
Verbindungstyp	Name des Verbindungstyps, entweder Standard, HTTP, JDBC, JMS, oder Kafka. Der Standardwert ist HTTP.
Unterstützt mehrere aktive Verbindungen	Bezeichner, der angibt, ob der Alias mehrere aktive Verbindungen unterstützt. Fügen Sie mithilfe der Tabelle „Verbindungen“ Verbindungen hinzu, und verknüpfen Sie sie mithilfe der zugehörigen Liste „Verbindungen“ mit dem Alias.
Standard-Wiederholungsrichtlinie	Wiederholungsrichtlinie für den Alias. Weitere Informationen finden Sie unter Wiederholungsrichtlinie .
Konfigurationsvorlage	Konfigurationsvorlage, die zum Erstellen eines Verbindungs- und Anmeldeinformationsdatensatzes verwendet werden soll.

4. Klicken Sie auf **Speichern**.
   Die zugehörige Liste Verbindungen und Verbindungsattribute wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
Verbindungen	Zugehörige Verbindungsdatensätze, die diesem Alias zugeordnet sind. Nachdem Sie den Alias erstellt haben, können Sie Verbindungsdatensätze definieren und diese mit dem Alias verknüpfen. Wenn **Unterstützt mehrere aktive Verbindungen** ausgewählt ist, können Sie einem Alias mehrere Verbindungen zuordnen.
Verbindungsattribute	Attribute für die Verbindung. Definieren Sie für eine Verbindung spezifische Daten, und verwenden Sie sie in einem IntegrationHub-Integrationsschritt. Weitere Informationen finden Sie unter Verbindungsattribute für IntegrationHub erstellen.
Untergeordnete Aliasse	Untergeordnete Aliasse, die dem übergeordneten Alias zugeordnet sind. Nachdem Sie einen Alias für Verbindungen und Anmeldeinformationen erstellt haben, können Sie erstellen *Untergeordneter Alias* Dient zum Konfigurieren mehrerer Verbindungen für dieselbe Anwendungsintegration.

Zugehörige Liste	Beschreibung
Verbindungen	Zugehörige Verbindungsdatensätze, die diesem Alias zugeordnet sind. Nachdem Sie den Alias erstellt haben, können Sie Verbindungsdatensätze definieren und diese mit dem Alias verknüpfen. Wenn **Unterstützt mehrere aktive Verbindungen** ausgewählt ist, können Sie einem Alias mehrere Verbindungen zuordnen.
Verbindungsattribute	Attribute für die Verbindung. Definieren Sie für eine Verbindung spezifische Daten, und verwenden Sie sie in einem IntegrationHub-Integrationsschritt. Weitere Informationen finden Sie unter Verbindungsattribute für IntegrationHub erstellen.

5. **Wahlweise:** Wenn Sie neue Anmeldeinformationen und Verbindungen erstellen möchten, die Ihrem Anmeldeinformationsalias zugeordnet sind, unter `Related Links`, Klicken Sie auf **Neue Verbindung Und Anmeldeinformationen Erstellen** .
   Die resultierenden Verbindungs- und Anmeldeinformationsdatensätze basieren auf einer vordefinierten Konfigurationsvorlage. Siehe Konfigurationsvorlagen für Verbindungen und Anmeldeinformationen .
6. **Wahlweise:** Wenn Sie einen untergeordneten Alias für Ihren Verbindungs- und Anmeldeinformationsalias erstellen möchten, unter **Untergeordnete Aliasse** Zugehörige Liste, wählen Sie aus **Neu** .
   a. Geben Sie einen Namen für den untergeordneten Alias ein, und wählen Sie aus **Übermitteln** .
      Der untergeordnete Alias erbt Eigenschaften vom übergeordneten Alias. Sie können dann einen untergeordneten Alias so konfigurieren, dass er seinen eigenen Satz von Verbindungs- und Anmeldeinformationen enthält.

Nächste Maßnahme

Erstellen Sie einen oder mehrere Verbindungsdatensätze, die dem Alias oder untergeordneten Aliasse zugeordnet werden sollen. Weitere Informationen zum Erstellen von Verbindungen finden Sie unter Erste Schritte mit Verbindungen. Fügen Sie dem Alias Verbindungsattribute hinzu, um Verbindungsmetadaten für Abläufe im Flow Designer verfügbar zu machen.

Richten Sie die OAuth-Integration über ein MID-Server

Erstellen Sie einen Verbindungsdatensatz, der das Senden einer OAuth-Tokenanforderung an einen Drittparteiserver über ermöglicht MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Bestätigen Sie, dass Sie das ServiceNow IntegrationHub Standard Pack-Installationsprogramm abonniert haben. Weitere Informationen finden Sie unter https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Erforderliche Rolle: admin

Prozedur

Konfigurieren Sie die Verbindung mit einer Konfigurationsvorlage.

a. Navigieren zu **Alle** > **IntegrationHub** > **Konfigurationsvorlagen**an.

b. Wählen Sie **Neu**.

c. Wählen Sie Aus **HTTP-Verbindung mit Gewährungstyp „OAuth-Client-Anmeldeinformationen“** .

d. Aktualisieren Sie das Formular nach Bedarf.
Sie können beispielsweise den Bereich in angeben `oauth_Entity_Profile_scope` Und `oauth_Entity_scope` Felder im Abschnitt Standarddatenvorlage. Informationen zum Erstellen einer Konfigurationsvorlage finden Sie unter Erstellen Sie eine Konfigurationsvorlage.

e. Wählen Sie **Absenden**.
Sie haben die Konfigurationsvorlage erstellt.

f. Navigieren zu **Alle** > **IntegrationHub** > **Aliasse für Verbindungen und Anmeldeinformationen**an.

g. Aktualisieren Sie das Formular.

Alias für Verbindungen und Anmeldeinformationen

Feld	Beschreibung
Name	Name des Alias. Ein Alias darf nur Buchstaben, Zahlen und Unterstriche enthalten. Während eines Upgrades wird das Tag im Anmeldedatensatz zu einem Verbindungs- und Anmeldealias migriert. Wenn das Anmeldeinformations-Tag andere Sonderzeichen als Buchstaben, Zahlen und Unterstriche enthält, wird der Tag-Name nach dem Upgrade beibehalten. Sie können diesen migrierten Alias weiterhin verwenden, Sie können ihn allerdings erst aktualisieren, wenn Sie den Namen den Namensbeschränkungen entsprechend ändern.
Anwendung	Eindeutiger Bezeichner für den Alias für Verbindungen und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Anmeldeinformationen, basierend auf dem Format `Scope_Name.alias_Name` . ○ Wenn der Bereich global ist, ist die ID der Aliasname. Wenn Sie beispielsweise einen Workday-Alias im globalen Bereich erstellen, wird die ID auf festgelegt `workday` . ○ Wenn Sie einen Workday-Alias im Bereich der HR-App erstellen, wird die ID auf festgelegt `X_HR_App.Workday` .
Übergeordneter Alias	Option zum Auswählen des Alias, unter dem Sie diesen Alias für Verbindungen und Anmeldeinformationen erstellen. Der Alias für Verbindungen und Anmeldeinformationen, den Sie erstellen, ist ein untergeordneter Alias. Ein untergeordneter Alias ist unter aufgeführt **Untergeordnete Aliasse** Registerkarte auf der übergeordneten Aliasseite für Verbindungen und Anmeldeinformationen. 
Typ	Option, um den Typ des Alias anzugeben, den Sie erstellen. Wählen Sie eine der folgenden Optionen aus: ○ Anmeldeinformationen: Alias, der einen Anmeldeinformationsdatensatz enthält. ○ Verbindung und Anmeldeinformationen: Alias, der sowohl den Verbindungs- als auch den Anmeldeinformationsdatensatz enthält. Diese Option ist standardmäßig ausgewählt. Bestätigen Sie, dass Verbindung und Anmeldeinformationen ausgewählt sind.
Unterstützt mehrere aktive Verbindungen	Bezeichner, der angibt, ob der Alias mehrere aktive Verbindungen unterstützt. Fügen Sie mithilfe der Tabelle „Verbindungen“ Verbindungen hinzu, und verknüpfen Sie sie mithilfe der zugehörigen Liste „Verbindungen“ mit dem Alias.
Standard-Wiederholungsrichtlinie	Wiederholungsrichtlinie für den Alias. Weitere Informationen finden Sie unter Wiederholungsrichtlinie .
Konfigurationsvorlage	Option zum Auswählen der Konfigurationsvorlage, auf der Sie den Alias für Verbindungen und Anmeldeinformationen erstellen. Wählen Sie die Vorlage des Typs aus **HTTP-Verbindung**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	mit Gewährungstyp „OAuth-Client-Anmeldeinformationen“ Die Sie erstellt haben.

h. Wählen Sie **Absenden**.
Sie haben den Alias-Datensatz für Verbindungen und Anmeldeinformationen erstellt.

i. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungs-Dashboard**an.

j. Geben Sie im Feld alle Verbindungen durchsuchen den Namen des von Ihnen erstellten Alias für Verbindungen und Anmeldeinformationen ein.

k. Wählen Sie im Datensatz des Alias für Verbindungen und Anmeldeinformationen die Option aus **Details Anzeigen** .

l. Wählen Sie **Konfigurieren**.

m. Füllen Sie das Formular aus.

Verbindungsdatensatz

Feld	Beschreibung
Verbindungsname	Name des Verbindungsdatensatzes. Sie können den Namen nicht aktualisieren.
Verbindungs-URL	Option zum Bereitstellen der URL, die eine Verbindung mit dem Drittparteiserver herstellt.
MID verwenden	Option, um anzugeben, dass Sie OAuth-Tokenanforderungen über einen MID-Server senden möchten. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
MID-Auswahl	Option, um anzugeben, ob Sie einen bestimmten MID-Server verwenden oder die automatische Auswahl eines MID-Servers aktivieren oder einen MID-Cluster verwenden möchten. Wählen Sie eine der folgenden Optionen aus. ○ MID-Server automatisch auswählen ○ Spezifischer MID-Server ○ Spezifischer MID-Server-Cluster
Fähigkeiten	Option zum Auswählen einer oder mehrerer MID-Server-Fähigkeiten. Fähigkeiten definieren die spezifischen Funktionen eines MID-Servers innerhalb eines IP-Adressbereichs, sodass eine Anwendung den am besten geeigneten MID-Server auswählen kann. Wählen Sie das Symbol für MID-Fähigkeiten ( ), um eine oder mehrere Fähigkeiten auszuwählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Diese Option wird angezeigt, wenn Sie auswählen **MID-Server automatisch auswählen** Im Feld MID-Auswahl.
MID-Anwendung	Option zum Angeben einer MID-Anwendung oder Akzeptieren der Standardanwendungsauswahl. **Hinweis:** Diese Option wird angezeigt, wenn Sie auswählen **MID-Server automatisch auswählen** Im Feld MID-Auswahl. Standardmäßig ist **ALLE** Option ist ausgewählt.
MID-Server	Option zum Auswählen eines MID-Servers. **Hinweis:** Diese Option wird angezeigt, wenn Sie auswählen **Bestimmter MID-Server** Im Feld MID-Auswahl.
MID-Cluster	Option zum Auswählen eines MID-Clusters. **Hinweis:** Diese Option wird angezeigt, wenn Sie auswählen **Spezifischer MID-Cluster** Im Feld MID-Auswahl.
OAuth-Client-ID	Option zum Angeben der Client-ID.
OAuth-Client-Geheimnis	Option zum Festlegen des geheimen Clientschlüssels.
Verbindung mit Auth-Server über MID-Server herstellen	Option, um anzugeben, dass die Verbindung zwischen der ServiceNow-Instanz und dem Authentifizierungsserver über den MID-Server erfolgt. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
OAuth-Token-URL	Option zum Angeben der OAuth-Token-URL, die zum anfordern von OAuth-Token verwendet wird.

n. Wählen Sie Aus **OAuth-Token konfigurieren und abrufen** .
Der Verbindungs- und Anmeldeinformationsdatensatz wird erstellt.

Anmeldeinformationsaliasse für Discovery

Anmeldeinformationsaliasse für Discovery Zulassen, dass ein Administrator bestimmte Anmeldeinformationen in Discovery-Zeitplänen verwendet. Sie können Verhaltensweisen für Ihre Aliasse konfigurieren, die bestimmen, wie strikt das System ihre Nutzung durchsetzt.

Ohne Anmeldeinformationsaliasse können Discovery-Zeitpläne auf alle Anmeldeinformationen zugreifen, die in der Instanz definiert sind. Dieses Verhalten ist unter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bestimmten Umständen nicht wünschenswert, insbesondere für Anmeldeinformationen mit erhöhten Berechtigungen. Anmeldeinformationsaliasse bieten mehr Kontrolle darüber, welche Anmeldeinformationen ein Discovery-Zeitplan verwenden darf, und verhindern, dass Anmeldeinformationen mit erhöhten Rechten unnötigerweise offengelegt werden.

Funktionsweise von Anmeldeinformationsaliassen

Eine Business-Regel namens *Fügen Sie Aliasse Für Discovery-Affinität Und -Anmeldeinformationen Ein* (Zuvor benannt *Fügen Sie Discovery-Affinity Ein*) Wird ausgeführt, wenn ein Datensatz (eine Aufgabe zum Ausführen von Discovery) in die ECC-Warteschlange eingefügt wird.

Die Geschäftsregel hängt die im Discovery-Zeitplan definierten Anmeldeinformationsaliasse an die Probe an. Wenn die Probe den MID-Server auf dem Weg zur Discovery erreicht, weiß der MID-Server genau, welche Anmeldeinformationen er verwenden kann, um auf das Gerät zuzugreifen, das die Probe zum Scannen gesendet wurde.

Der MID-Server filtert Anmeldeinformationen nach Affinität Und dann nach Tags, falls vorhanden. Anmeldeinformationen müssen mit allen Anmeldeinformations-Tags übereinstimmen. Der MID-Server wird iteriert, bis er eine funktionierende Anmeldeinformation findet.

Wenn mit der Geschäftsregel festgestellt wird, dass eine Affinität für das Gerät vorhanden ist, wird anhand der Regel die richtige *credential_id* identifiziert, die zu verwenden ist. Dies ist der *sys_ID* Des Datensatzes in den Anmeldeinformationen [Discovery_credentials] Tabelle.

Wenn die Plattform auf eine Affinität mit einem Aliaswert für Anmeldeinformationen stößt, der in der Geschäftsregel als *credential_alias* definiert ist, ermittelt die Geschäftsregel, ob die von der Affinität referenzierten Anmeldeinformationen den angegebenen Alias aufweisen. Wenn dies der Fall ist, wählt die Business-Regel aus *Anmeldeinformations-ID* Des Alias und übergibt diesen Wert an den MID-Server.

Wenn ein Anmeldeinformationsalias für einen Zeitplan definiert ist und der Zeitplan so konfiguriert ist, dass er diesen Alias verwendet, ignoriert der Zeitplan alle zuvor vorhandenen Anmeldeinformations-zu-Ziel-Affinitäten – *Aber nur, wenn die Anmeldeinformationen selbst keinem anderen Anmeldeinformationsalias zugeordnet sind* . Wenn die Anmeldeinformationen keinen Anmeldeinformationsalias haben, werden alle anderen Affinitäten überprüft, die für das Zielsystem vorhanden sind.

Discovery-Anmeldeinformationsalias erstellen

Erstellen Sie den Alias, und fügen Sie diesen Alias dann einer Anmeldeinformation im Anmeldeinformationsdatensatz hinzu. Sie können mehreren Aliasen Anmeldeinformationen und einem einzelnen Alias mehrere Anmeldeinformationen hinzufügen.

Vorbereitungen

Erforderliche Rolle: admin, credential_admin (nur Lesezugriff), connection_admin (nur Lesezugriff)

Warum und wann dieser Vorgang ausgeführt wird

Ein Discovery-Zeitplan verwendet nur Anmeldeinformationen, die in den für den betreffenden Zeitplan definierten Aliassen enthalten sind.

Hinweis: Wenn ein Anmeldeinformationsalias für einen Zeitplan definiert ist, ignoriert er alle zuvor vorhandenen Anmeldeinformationsaffinitäten zwischen den Anmeldeinformationen und dem Ziel, das in einem Zeitplan erkannt wird, der für die Verwendung dieses Anmeldeinformationsalias eingerichtet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

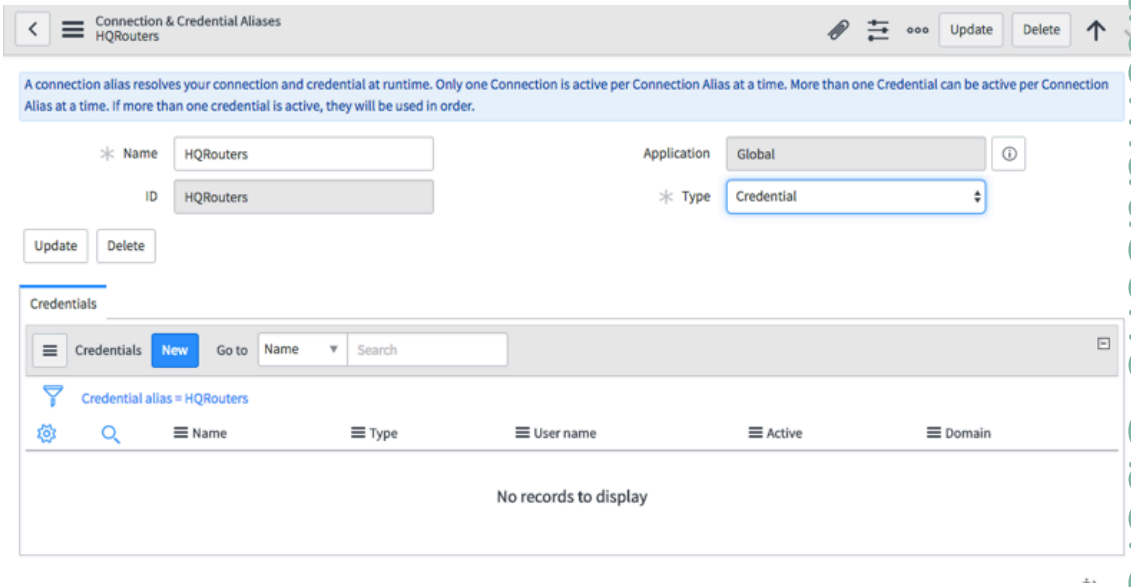
1. Erstellen Sie einen Alias.

   a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.

   b. Klicken Sie auf **Neu**.

   c. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie aus **Anmeldeinformationen** Für den Alias **Typ** .

   d. Klicken Sie auf **Absenden**.
   Die **Anmeldeinformationen** Zugehörige Liste wird angezeigt. Sie können für diesen Alias in dieser Liste neue Anmeldeinformationen hinzufügen, nicht jedoch bestehende Anmeldeinformationen.



2. Konfigurieren Sie Anmeldeinformationen für den neuen Alias.

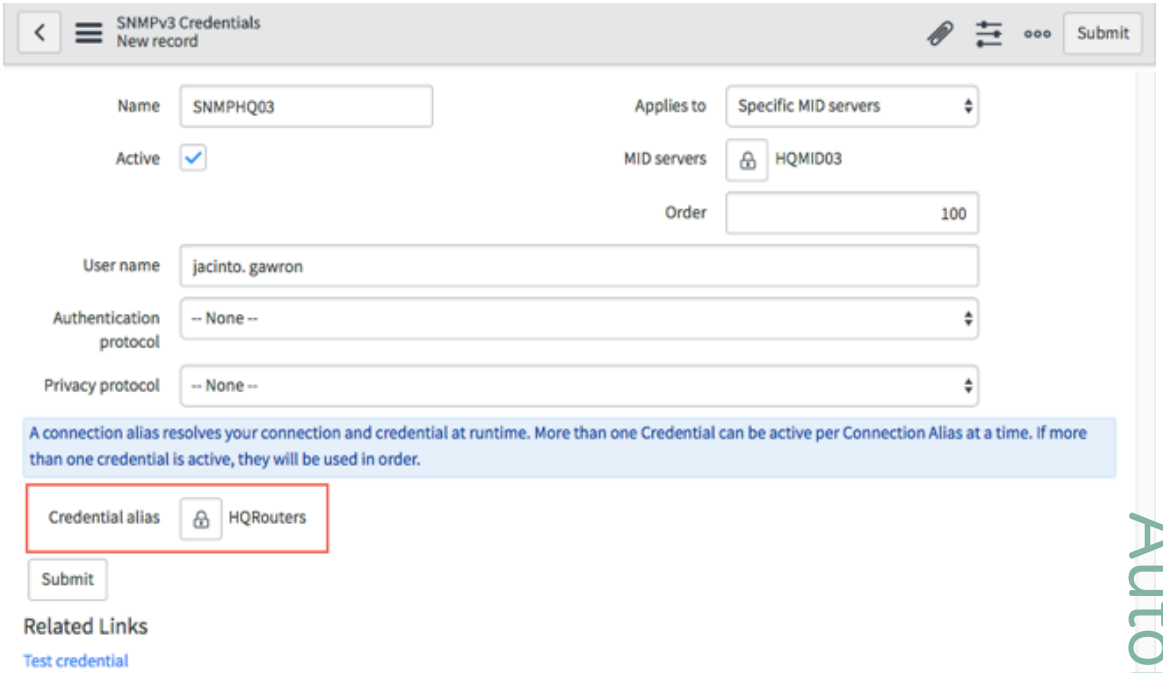
   a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

   b. Wählen Sie eine vorhandene Anmeldeinformation aus der Liste aus, oder klicken Sie auf **Neu** Um neue Anmeldeinformationen zu erstellen.

   c. Entsperren Sie im Anmeldeinformationsdatensatz die **Anmeldeinformationsalias** Feld und wählen Sie den erstellten Alias aus.

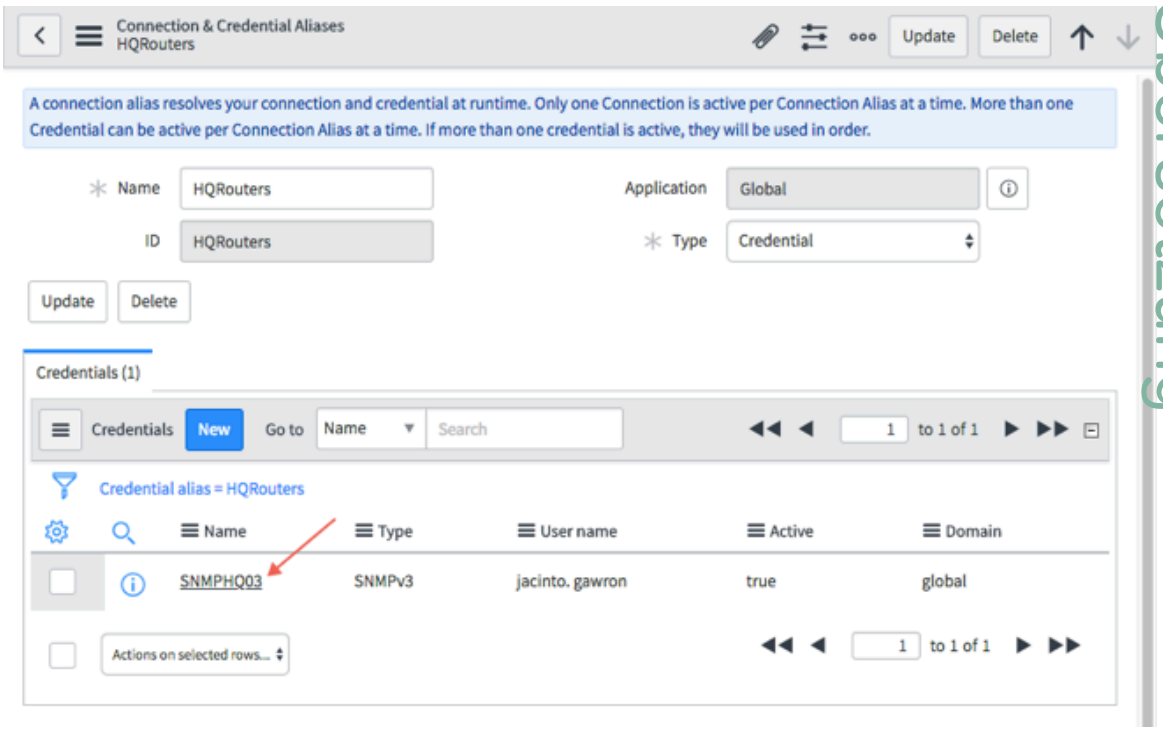
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Speichern Sie den Datensatz oder senden Sie ihn ab.

3. Zurück zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen** Und öffnen Sie Ihren neuen Alias.
Die Anmeldeinformationen, die Sie an den Alias angehängt haben, werden jetzt in der zugehörigen Liste angezeigt.



4. Klicken Sie auf, um zusätzliche Anmeldeinformationen für diesen Alias zu erstellen **Neu** Wählen Sie in der zugehörigen Liste einen Anmeldeinformationstyp aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Aliasname ist in vorab ausgefüllt **Anmeldeinformationsalias** Feld des Anmeldeinformationsdatensatzes.

5. Füllen Sie die Felder im Formular aus, und übermitteln Sie den Datensatz.

Anmeldeinformationsaliasse für Orchestration-Aktivitäten

Der Anmeldeinformationsalias ermöglicht einem Administrator mehr Kontrolle über die in Orchestration-Aktivitäten verwendeten Anmeldeinformationen.

Dies ist nützlich, wenn eine Aktivität zur Ausführung einer Aufgabe bestimmte Anmeldeinformationen benötigt. Sie können ein Anmeldeinformations-Tag verwenden, um bestimmten Aktivitäten in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zuzuweisen.

Anmeldeinformationsalias interagiert mit Affinität der Anmeldeinformationen Um zu bestimmen, welche Anmeldeinformationen für eine Orchestration-Aktivität verwendet werden sollen.

Funktionsweise des Anmeldeinformationsalias

A Business-Regel Angerufen *Fügen Sie Discovery-Affinity Ein* (Umbenannt aus Affinität für Anmeldeinformationen einfügen im Genf-Release) wird ausgeführt, wenn ein Datensatz in die ECC-Warteschlange eingefügt wird. Diese Regel bestimmt, ob eine Berechtigungsaffinität für das Gerät besteht, und identifiziert die richtige, zu verwendende *credential_id* (die *sys_id* des Datensatzes in der Tabelle „Anmeldeinformationen“ [discovery_credentials]). Wenn die Plattform auf eine Affinität mit einem definierten Aliaswert für Anmeldeinformationen (*credential_alias* in der Geschäftsregel) stößt, ermittelt die Geschäftsregel, ob die von der Affinität referenzierten Anmeldeinformationen den angegebenen Alias haben. Wenn dies der Fall ist, wählt die Geschäftsregel die *credential_id* des Anmeldeinformationsalias aus und übergibt diesen Wert an den MID Server. Wenn der Anmeldeinformationen nicht über den angegebenen Anmeldeinformationsalias verfügen, werden alle anderen für das Zielsystem vorhandenen Affinitäten geprüft. Wenn keine Affinität auf entsprechend gekennzeichnete Anmeldeinformationen verweist, durchläuft der MID Server die Tabelle „Anmeldeinformationen“ *[discovery_credentials]* und wählt die Anmeldeinformationen mit dem entsprechenden Tag aus. Der MID Server erstellt dann eine neue Affinität für diese Anmeldeinformationen.

Anmeldeinformationen erstellen und testen

Erstellen und testen Sie die Anmeldeinformationen, die Discovery, Service Mapping, Cloud Management und Orchestration für den Zugriff auf Hardware und Software in Ihrem Netzwerk benötigen.

Vorbereitungen

Erforderliche Rolle: Administrator

Überprüfen Sie Ihre Sicherheitsrichtlinie und -Optionen mit dem Sicherheitsteam Ihrer Organisation.

Warum und wann dieser Vorgang ausgeführt wird

Diese Aufgabe enthält allgemeine Verfahren zum Erstellen von Anmeldeinformationen. Weitere Informationen zu bestimmten Feldern und Anforderungen finden Sie in der Dokumentation zu Ihrem Anmeldeinformationstyp.

Unterstützte Anmeldeinformationstypen

Applicative-Anmeldeinformationen	Virtual Server Interface	Chef-Server-Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Anmeldeinformationstypen (Fortsetzung)

CIM-Anmeldeinformationen	Cloud-Anmeldeinformationen	Anmeldeinformationen für Container-Image-Repository
Infoblox-Anmeldeinformationen	JDBC-Anmeldeinformationen	JMS-Anmeldeinformationen
OAuth 2.0-Anmeldeinformationen	SAP-Anmeldeinformationen	SNMP-Anmeldeinformationen
SSH-Anmeldeinformationen	VMware-Anmeldeinformationen	Windows-Anmeldeinformationen

Hinweis: Um die Sicherheit zu verbessern, beschränken Sie den Umfang der Anmeldeinformationen auf einen bestimmten MID-Server oder Zeitplan, um unnötige Anmeldeinformationen zu vermeiden.

Prozedur

1. Navigieren Sie zu einem dieser Module:
   - **Discovery** > **Berechtigungen**
   - **Service Mapping** > **Berechtigungen**
   - **Orchestration** > **Anmeldeinformationen**
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf der Seite „Berechtigungen“ auf einen Link für den Anmeldeinformationstyp, und füllen Sie das Formular aus.

   Weitere Informationen finden Sie in der Dokumentation zum ausgewählten Anmeldeinformationstyp.

   Sie können einen Anmeldeinformationsdatensatz zuerst absenden und dann später testen oder die Anmeldeinformationen unmittelbar vor dem Speichern testen.

   Das Testen der Anmeldeinformationen wird für folgende Anmeldeinformationstypen unterstützt:
   - Private SSH-Schlüssel
   - Windows
   - SNMP v3
   - VMware
   - JDBC
   - JMS
4. Klicken Sie unter **Zugehörige Links** auf **Test-Anmeldedaten**.

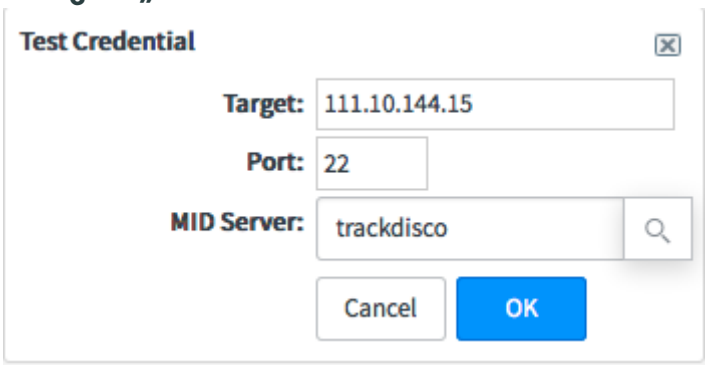
   Hinweis: Die Anmeldeinformationen sind während des Tests stets verschlüsselt.

5. Füllen Sie die Felder im Dialogfeld „Test-Anmeldeinformationen“ aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dialogfeld „Test-Anmeldeinformationen“



Felder im Dialogfeld „Test-Anmeldeinformationen“

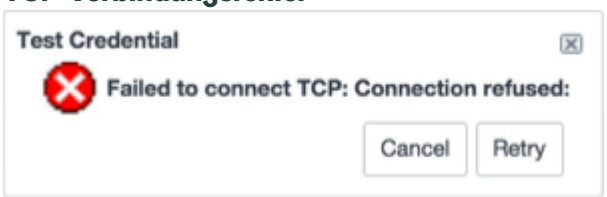
Feld	Beschreibung	Anmeldeinformationstyp
Ziel	Zielhost, auf dem diese Anmeldeinformationen ausgeführt werden. Dieser Wert muss für alle Anmeldeinformationstypen eine IP-Adresse sein, mit Ausnahme von VMware, für das die Host-URL angegeben werden kann. Sie können keine MID-Server als Ziel festlegen. **Hinweis:** Bei JMS ist dies die Provider-URL. Die Informationen in dieser URL teilen JNDI mit, wie der JMS-Provider gefunden und darauf zugegriffen werden kann. Ein Beispielwert für die Verbindung zu ActiveMQ V5.1 ist tcp://ipAdresseOderHostname:61616.	Alle
Port	Port des Ziels, der für diesen Test verwendet werden soll. Das System füllt dieses Feld vorab mit dem Standardport für den ausgewählten Anmeldeinformationstyp aus.	Alle
MID Server	Für diesen Test zu verwendender MID Server. Sie müssen einen Windows-MID-Server verwenden, um die Windows-Anmeldeinformationen zu testen. Nur MID-Server, die **In Betrieb** und **Überprüft** sind, stehen zur Verfügung.	Alle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung	Anmeldeinformationstyp
DB-Typ	Typ der Datenbank, für die diese Anmeldeinformationen getestet werden sollen.	JDBC
DB-Name	Name der Datenbank, für die diese Anmeldeinformationen getestet werden sollen.	JDBC
Ursprüngliche Kontext-Werkseinstellung	Name der JNDI-Klasse, die zum Erstellen des InitialContext verwendet wird. Bei Verwendung dieser **Ursprünglichen Kontext-Werkeinstellung** werden verschiedene JMS-Objekte, z. B. JMS-Verbindung, erstellt. Wenn Sie beispielsweise eine Verbindung zu ActiveMQ V5.10 (JMS-Provider) herstellen möchten, lautet der Wert in diesem Feld org.apache.activemq.jndi.ActiveMQInitialContextFactory	JMS

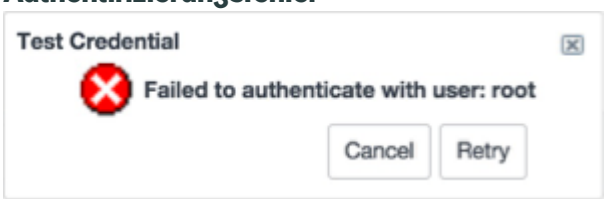
6. Klicken Sie auf **OK**, um den Test zu beginnen.
   Ein Indikator zeigt an, dass das System versucht, das Ziel mit den von Ihnen angegebenen Anmeldeinformationen zu kontaktieren. Wenn die Instanz eine Verbindung zum Ziel herstellt, wird eine Erfolgsmeldung angezeigt. Wenn die Instanz bei den von Ihnen angegebenen Testeingaben auf ein Problem stößt, wird die entsprechende Fehlermeldung angezeigt. Nachfolgend finden Sie einige häufige Fehlermeldungen.
   - Falsches Ziel oder falsche Portnummer:

     TCP-Verbindungsfehler

   - Falscher Benutzername oder falsches Passwort:

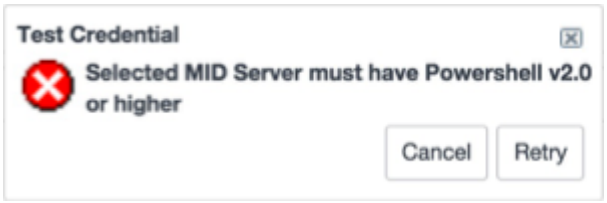
     Authentifizierungsfehler

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Falscher MID Server für Windows-Anmeldeinformationen:

MID Server-Fehler



7. Klicken Sie auf **Neuversuch**, um das Dialogfeld „Test-Anmeldedaten“ zu öffnen und den Eingabefehler zu korrigieren.
8. Wenn der Test der Anmeldeinformationen erfolgreich ist, klicken Sie auf **Absenden**, um den Datensatz zu speichern.

Wichtig: Durch das Testen der Anmeldeinformationen kann nicht sichergestellt werden, dass die Anmeldeinformationen über die erforderlichen Berechtigungen für die beabsichtigten Discovery- oder Orchestration-Workflow-Aufgaben verfügen.

Ansible Tower-Anmeldeinformationen

Ansible Tower-Anmeldeinformationen werden für den Zugriff auf den Account zur Ansible-Konfigurationsverwaltung benötigt. Verwenden Sie diese Anmeldeinformationen, um Ansible-Ressourcen über zu verwalten Cloud-Management Anwendung.

Zur Integration von Cloud Provisioning and Governance mit dem Ansible-Konfigurationsverwaltungskonto müssen Benutzername und Passwort für das Administratorkonto in Ansible konfiguriert werden.

Formularfelder für Ansible Tower-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Benutzername/ Passwort	Geben Sie die Authentifizierungsinformationen für den Ansible Tower-Benutzer mit Administratorrechten ein.

Hinweis: Sie müssen keine anderen Felder konfigurieren

Anmeldeinformationen für API-Keys

Ein API-Key ist ein eindeutiger Code, der an eine API übergeben wird, um die aufrufende Anwendung oder den aufrufenden Benutzer zu identifizieren.

Anmeldeinformationen für API-Keys

Formularfelder für Anmeldeinformationen für API-Keys

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Anmeldeinformationen für API-Keys (Fortsetzung)

Feld	Eingabewert
API Key	Geben Sie den API Key ein.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Flows und Workflows, jeder Aktivität in einem Flow oder Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Flow oder Workflow unterschiedliche Anmeldeinformationen zu.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Applicative-Anmeldeinformationen

Einige Anwendungen erfordern zusätzlich zu den vom Host-Computer benötigten weitere Anmeldeinformationen. Anmeldeinformationen, die für den Zugriff auf diese Anwendungen erforderlich sind, werden als Applicative-Anmeldeinformationen bezeichnet.

Typische Anmeldeinformationen enthalten einen Anwendernamen und ein Passwort für die Anmeldung bei einem Gerät oder einer Anwendung. Während die meisten Anwendungen nur einen Berechtigungsnachweis für den Zugriff auf sie benötigen, verfügen Hosts und Anwendungen manchmal über separate Anmeldeinformationen für zusätzliche Sicherheit. Beispielsweise benötigen ABAP SAP Central Services (ASCS) zusätzlich zu den SSH- oder Windows-Host-Anmeldeinformationen für den Server, auf dem ASCS gehostet wird, Applicative-Anmeldeinformationen.

Hinweis: ServiceNow Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Konfigurationselemente (Configuration Items, CIs) umfassen.

Wie bei Host-Anmeldeinformationen weisen Sie applikative Anmeldeinformationen zu MID Servers.

Sie erstellen anwendbare Anmeldeinformationen pro CI-Typ. Der CI-Typ für ASCS ist beispielsweise SAP ASCS-Anwendung [cmdb_ci_APL_sap_ascs]. Das vorkonfigurierte Muster zum Erkennen von CIs, die zu diesem CI-Typ gehören, enthält Befehle, für die von MID-Server die Verwendung des anwendbaren Berechtigungsnachweises für diesen CI-Typ erfordern. Wenn für diesen CI-Typ mehr als eine Anmeldeinformation konfiguriert ist, wird MID-Server Versucht, diese Anmeldeinformationen in der von Ihnen definierten Reihenfolge zu verwenden, bis die entsprechenden Anmeldeinformationen gefunden werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die Informationen zu den Discovery-Anforderungen in der ServiceNow-Dokumentation, um festzustellen, ob Sie Applicative-Anmeldeinformationen für bestimmte Anwendungs-CIs konfigurieren müssen. Es ist nicht erforderlich, anwendbare Anmeldeinformationen zu konfigurieren, wenn Discovery Voraussetzungen erwähnen dies nicht.

Felder für Applicative-Anmeldeinformationen

Feld	Beschreibung
Name	Name des Berechtigungsnachweises Verwenden Sie einen beschreibenden Namen wie Oracle DB oder London Oracle DB (für eine Oracle-Datenbank). Verwenden Sie keine Leerzeichen oder Sonderzeichen für den Anmeldeinformationsnamen.
Aktiv	Aktivieren Sie das Kontrollkästchen, um den Berechtigungsnachweis zu verwenden.
Benutzername	Geben Sie den tatsächlichen Benutzernamen des Antragsnachweises ein.
Passwort	Geben Sie das tatsächliche Passwort des Antragsnachweises ein. Verwenden Sie keine Leerzeichen oder Sonderzeichen für den Anmeldeinformationsnamen.
CI-Typ	Wählen Sie einen CI-Typ aus, zu dem das CI gehört.
Anmeldeinformationsalias	Erstellen Sie einen Alias, um bestimmten Discovery-Zeitplänen bestimmte Anmeldeinformationen zuzuweisen. Bei der Zuweisung eines Alias müssen Sie den Tabellennamen für den CI-Typ identifizieren, dessen Applicative-Anmeldeinformationen von der Anwendung verwendet werden. Von Anwendungen können Applicative-Anmeldeinformationen eines CI-Typs verwendet werden, der sich von ihrem eigenen unterscheidet. Informationen zu einer bestimmten Anwendung finden Sie in der entsprechenden Tabelle aus der Liste: • ABAP SAP Central Services (ASCS): cmdb_ci_appl_sap_ascs • IBM Security Access Manager-Appliance: cmdb_ci_app_server_webseal • SAP Central-Instanz: cmdb_ci_appl_sap_ascs • SAP Central Services (SCS): cmdb_ci_appl_sap_ascs • SAP Evaluated Receipt Settlement (ERS): cmdb_ci_appl_sap_ascs • SAP Java-Cluster: cmdb_ci_appl_sap_ascs • SAP NetWeaver Dialog Instance: cmdb_ci_appl_sap_ascs • Microsoft Exchange Mailbox (für Microsoft Exchange): cmdb_ci_exchange_mailbox • Microsoft SQL-Datenbank: cmdb_ci_db_mssql_instance • MySQL Server: cmdb_ci_db_mysql_instance • Oracle Advanced Queue-Warteschlange: cmdb_ci_db_ora_instance • Oracle-Datenbank: cmdb_ci_db_ora_instance • Oracle E-Business Suite: cmdb_ci_db_ora_instance

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Applicative-Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
	• Oracle WebLogic-Modul: cmdb_ci_app_server_weblogic • Tibco Enterprise Message Service (EMS): cmdb_ci_appl_tibco_message
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Virtual Server Interface

Der Anmeldeinformationstyp für die Standardauthentifizierung verwaltet den Zugriff zum Speichern von Anmeldeinformationen für die Standardauthentifizierung.

Diese Felder stehen im Formular „Anmeldeinformationen“ für die Standardauthentifizierung zur Verfügung.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **Standardauthentifizierung** nennen.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den eindeutigen Schlüssel ein, der für diese Anmeldeinformationen im externen CyberArk-Anmeldeinformationsspeichersystem konfiguriert wurde. Die Nachweis-ID kann als Safe-Überschreibung verwendet werden, wenn mehrere Safes verwendet werden. Standardmäßig die Syntax in **Anmeldeinformations-ID** Feld ist dieses: *<safe name>:<Credential ID>*. Wenn der Safe-Name weggelassen wird, muss ein Safe-Name in der Datei config.xml definiert sein. Um das Trennzeichen vom Standarddoppelpunkt in ein anderes Zeichen zu ändern, überschreiben Sie den Wert mit dem optionalen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationsformular für die Standardauthentifizierung (Fortsetzung)

Feld	Eingabewert
	`ext.cred.safe_name`Parameter. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Chef-Server-Anmeldeinformationen

Chef-Server-Anmeldeinformationen greifen auf Chef-Integrationen mit der Instanz zu.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „Chef-Server“ verfügbar. Diese Informationen stammen aus den Einstellungen, die Sie bei der Durchführung der Chef-Server-Installation konfiguriert haben.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Administratorname	Geben Sie den Administratornamen an, den Sie während der Chef-Server-Installation erstellt haben.
Administratorschlüssel	Geben Sie den privaten RSA-Schlüssel ein, den der Chef-Server beim Erstellen des Administrators generiert hat.
Validierungsname	Geben Sie den Namen des Prüfers ein.
Bestätigungsschlüssel	Geben Sie den privaten RSA-Schlüssel ein, den der Chef-Server beim Erstellen einer Organisation generiert hat.
Zertifikatname	Geben Sie den Zertifizierungsnamen ein.
Zertifikatschlüssel	Geben Sie den Zertifizierungsschlüssel ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIM-Anmeldeinformationen

Der CIM-Berechtigungstyp verwaltet den Zugriff auf einen CIM-Server (auch als CIMOM - Common Information Model Object Manager bezeichnet), um Informationen zu VMware ESX-Servern zu erhalten. Dieser Anmeldeinformationstyp ist für Discovery verfügbar.

Diese Felder sind im Anmeldeinformationsformular für CIM verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Auswahl Von Spezifisch **Bestimmte MID-Server** Hat keine Auswirkungen auf die Auswahl des MID-Servers. Es wird nur verwendet, um zu entscheiden, welche MID-Server Transparenz für die Anmeldeinformationen haben sollen. **Bestimmte MID-Server** Wird in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

NetApp-Speichergeräte für CIM-Anmeldeinformationen konfigurieren

NetApp-Speichergeräte erfordern eine zusätzliche Konfiguration für Discovery Um sie zu erkunden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Installieren Sie den SMI-S-Agenten auf dem Speichergerät-Host.

   Beachten Sie hinsichtlich Anweisungen und Anforderungen den Data ONTAP SMI-S Agent 5.2 Installation and Configuration Guide .

   Hinweis:

   ServiceNow Verwaltet die Dokumentation auf dieser Website nicht. Dieses Dokument kann ohne Ankündigung geändert werden.

2. Erstellen Sie einen Benutzer-Account und ein Passwort für den SMI-S-Agenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie einen Anmeldeinformationsdatensatz für die SMI-S-Agentenanmeldeinformationen. Legen Sie den Anmeldeinformationstyp auf **CIM** fest.

Cloud-Anmeldeinformationen

Cloud-Anmeldeinformationstypen verwalten den Zugriff auf cloudbasierte Anwendungen, einschließlich Amazon Web Services und der Microsoft Azure Cloud.

AWS Identity and Access Management (IAM)-Rollen

Wenn Sie einen MID-Server auf Amazon EC2 in einer AWS-Cloud installiert haben und dieser MID-Server so konfiguriert ist, dass er Ressourcen in der Cloud erkennt, können Sie Sicherheits-Anmeldeinformationen verwenden, die von AWS Identity and Access Management (IAM)-Rollen bereitgestellt werden, anstatt Anmeldeinformationen, die in Ihrer Instanz verwaltet werden. Diese AWS-Anmeldeinformationen gewähren Berechtigungen in der Cloud über einen *Instanzprofil* , Basierend auf Rollen. Diese Anmeldeinformationen sind temporär und werden automatisch in einem konfigurierbaren Intervall rotiert. Wenn eine IAM-Rolle auf dem MID-Server definiert ist. Weitere Informationen finden Sie unter Konfigurieren Sie den MID-Server für AWS IAM-Rollen .

Discovery ignoriert alle in der Instanz gespeicherten Anmeldeinformationen anstelle der Anmeldeinformationen, die von der Rolle im Instanzprofil gewährt werden. Weitere Informationen zu AWS-Instanzprofilen finden Sie unter IAM-Rollen für Amazon EC2 .

AWS-Anmeldeinformationen

Formularfelder mit AWS-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen.
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die **Zugriffsschlüssel-ID**, die Sie in der AWS-Verwaltungskonsole generiert haben, z. B: APIAIOSFODNN7BEISPIEL.
Geheimer Zugangsschlüssel	Der **geheime Zugriffsschlüssel**, den Sie in der AWS-Verwaltungskonsole generiert haben, z. B.: wPalrXUtnFEMI/K7MDENG/bPxRfiCYBEISPIELSCHLÜSSEL.

Formularfelder für Azure-Service-Prinzipal-Anmeldeinformationen

Feld	Wert
Name	Geben Sie den Namen des Service Principals ein, der bei der Instanz registriert werden soll.
Tenant-ID und	Fügen Sie den Wert der Azure-**Verzeichnis-ID** aus dem Azure-Portal in das Feld Cloud-Management **Tenant-ID** ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Client-ID	Fügen Sie die Azure-**Anwendungs-ID** der Anwendung, die Sie in Azure registriert haben, im Feld Cloud-Management **Client-ID** ein.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis**. **Hinweis: Client-Zusicherung** wird nicht unterstützt.
Geheimschlüssel	Fügen Sie den geheimen Schlüssel ein, der beim Erstellen des Azure Service Principal generiert wurde. Dieses Feld erscheint, wenn die **Authentifizierungsmethode Client-Geheimnis** ist.

Azure Enterprise Agreement-Anmeldeinformationen

Azure Enterprise Agreement-Anmeldeinformationen sind für die Abrechnungsfunktionen der Cloud Management-Anwendung erforderlich.

Formularfelder für Azure Enterprise Agreement-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen ein.
Registrierungsnummer	Geben Sie die Registrierungsnummer von Azure ein.
Zugriffsschlüssel	Fügen Sie den von Azure bereitgestellten Zugriffsschlüssel ein.

Cloud Management-Anmeldeinformationen

Dieser Anmeldeinformationstyp ist für Orchestration verfügbar.

Formularfelder für Cloud Management-Anmeldeinformationen

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **Cloud Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Typ	Geben Sie **AWS** an.
Benutzername	Geben Sie den CIM-Benutzernamen ein, um die Tabelle „Anmeldeinformationen“ zu erstellen. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt.
Passwort	Geben Sie das CIM-Passwort ein.
SSH-Passwortsatz	Geben Sie eine einprägsame Phrase für die Schlüsselgenerierung ein. Zum Beispiel könnten Sie **Freitag ist ein guter Tag** eingeben.
Privater SSH-Schlüssel	Geben Sie den privaten SSH-Schlüssel ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder für Cloud Management-Anmeldeinformationen (Fortsetzung)

Feld	Eingabewert
Authentifizierungsprotokoll	Wählen Sie das **MD5**- oder **SHA**-Authentifizierungsprotokoll aus, mit dem der **Authentifizierungsschlüssel** erstellt wurde.
Authentifizierungsschlüssel	Geben Sie einen von SSH generierten Authentifizierungsschlüssel ein.
Datenschutzprotokoll	Geben Sie eines der folgenden Datenschutzprotokolle ein, das die Verschlüsselung für die **Datenschutzschlüssel** beschreibt: • **3DES** für Triple Data Encryption Standard (DES) • **AES128** für Advanced Encryption Standard (AES) mit 128-Bit-Verschlüsselung • **AES192** für AES mit 192-Bit-Verschlüsselung • **AES256** für AES mit 256-Bit-Verschlüsselung • **DES** für die alte DES-Verschlüsselung
Geben Sie einen zusätzlichen Datenschutzschlüssel ein.	
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
Klassifizierung	Geben Sie die Anwendungsklassifizierung für die CI-Ermittlung ein.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen für CMP-Knoten (Cloud Management)

Anmeldeinformationen für CMP-Knoten (Cloud Management) verknüpfen Anmeldeinformationen für einen virtuellen Server, die von Cloud Management bereitgestellt werden. Die Cloud Management-Anwendung erstellt diese Anmeldeinformationen automatisch.

Hinweis: Möglicherweise müssen Sie diese Anmeldeinformationen deaktivieren, wenn Sie sie nicht mehr verwenden möchten, die Prioritätsreihenfolge ändern oder einen MID Server auswählen, der darauf zugreifen darf. Andernfalls müssen Sie diesen Anmeldeinformationstyp nicht manuell erstellen oder ändern.

Formularfelder für Anmeldeinformationen für CMP-Knoten

Feld	Beschreibung
Name	Der automatisch generierte Name basiert auf dem Rechenzentrum, in dem sich der virtuelle Computer befindet.
Aktiv	Ob die Anmeldeinformationen aktiv sind.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für einen bestimmten MID Server oder für alle MID Server verfügbar sind.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Benutzername und Passwort	Der Benutzername und das Passwort des virtuellen Servers.
SSH-Passwortsatz und Privater SSH-Schlüssel	Der private Schlüssel und der Passwortsatz, der den Schlüssel schützt, falls der virtuelle Server dies erfordert.
Authentifizierungsprotokoll und Authentifizierungsschlüssel	Der private Schlüssel und der Passwortsatz, der den Schlüssel schützt, falls der virtuelle Server dies erfordert.
Datenschutzprotokoll und Datenschutzschlüssel	Wählen Sie das mit dem virtuellen Server verwendete Verschlüsselungsprotokoll aus, und geben Sie den Datenschutzschlüssel ein.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.

Anmeldeinformationen für Cloud Management (CMP)-SSH-Schlüsselpaar

Cloud Management (CMP)-SSH-Schlüsselpaare speichern die Schlüssel, die die Cloud Management-Anwendung automatisch generiert, wenn Benutzer Stapelressourcen bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Möglicherweise müssen Sie diese Anmeldeinformationen deaktivieren, wenn Sie sie nicht mehr verwenden möchten. Andernfalls müssen Sie diesen Anmeldeinformationstyp nicht manuell erstellen oder ändern.

Formularfelder für Anmeldeinformationen für CMP-SSH-Schlüsselpaare

Feld	Beschreibung
Name	Der automatisch generierte Name
Aktiv	Ob die Anmeldeinformationen aktiv sind.
Öffentlicher SSH-Schlüssel	Der öffentliche Schlüssel
Privater SSH-Schlüssel	Ein sicherer privater Schlüssel, der anstelle eines Passworts für SSH-Anmeldungen verwendet werden kann.

Anmeldeinformationen für Container-Image-Repository

Die Anmeldeinformationen des Container-Image-Repositorys verwalten den Zugriff auf private Repositorys zum Scannen von Container-Images. Dieser Anmeldeinformationstyp ist für verfügbar Discovery.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationsbild-Repository-Anmeldeinformationen verfügbar.

Formular „Container-Image-Repository-Anmeldeinformationen“

Feld	Beschreibung
Name	Vom Anwender zugewiesener Anmeldeinformationsname.
Anwendername	Anwendername mit Leseberechtigungen für das Repository.
Passwort	Passwort mit Leseberechtigungen für das Repository.
Repository	Vollqualifizierter Domänenname des Repositorys. Beispiel: `docker.io/Snow_images` .

Infoblox-Anmeldeinformationen

Infoblox-Anmeldeinformationen sind erforderlich, um IP-Pools (IPAM) in der Cloud Management-Anwendung einzurichten.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „Infoblox“ verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für einen bestimmten MID Server oder für alle MID Server verfügbar sind.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert. Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
wapiversion	Geben Sie die Version von wAPI ein, die Sie verwenden.
Benutzername und Passwort	Geben Sie den InfoBlox-Benutzernamen und das Passwort ein.

JDBC-Anmeldeinformationen

Der JDBC-Anmeldeinformationstyp verwaltet den Zugriff auf eine JDBC-Verbindung (Java Database Connectivity). Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „JDBC“ verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Auswahl Von Spezifisch **Bestimmte MID-Server** Hat keine Auswirkungen auf die Auswahl des MID-Servers. Es wird nur verwendet, um zu entscheiden, welche MID-Server Transparenz für die Anmeldeinformationen haben sollen. **Bestimmte MID-Server** Wird in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JMS-Anmeldeinformationen

Der JMS-Anmeldeinformationstyp verwaltet den Zugriff auf einen Java Message Service (JMS). Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Anmeldeinformationsformular für JMS verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen. **Hinweis:** Auswahl Von Spezifisch **Bestimmte MID-Server** Hat keine Auswirkungen auf die Auswahl des MID-Servers. Es wird nur verwendet, um zu entscheiden, welche MID-Server Transparenz für die Anmeldeinformationen haben sollen. **Bestimmte MID-Server** Wird in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

OAuth 2.0-Anmeldeinformationen

OAuth 2.0-Anmeldeinformationen ermöglichen ServiceNow den Zugriff auf Benutzer-Accounts in einem HTTP-Service.

Diese Felder sind im Anmeldeinformationsformular für OAuth 2.0 verfügbar.

OAuth 2.0-Anmeldeinformationsformular

Feld	Eingabewert
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie **OAuth2-Anmeldeinformationen** nennen.
Aktiv	Geben Sie an, ob diese Anmeldeinformationen aktiv sind.
OAuth-Entitätsprofil	Ein OAuth-Profil ist eine Kombination aus einem Gewährungstyp und mindestens einem Bereich.
Verbindung mit Auth-Server über MID-Server herstellen	Verbindet mit ServiceNow Instanz für einen lokalen OAuth-Server, der sich hinter einer Firewall über befindet MID-Server. Es kann auch mit verbunden werden ServiceNow Instanz für einen cloudbasierten OAuth-Server über einen MID-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

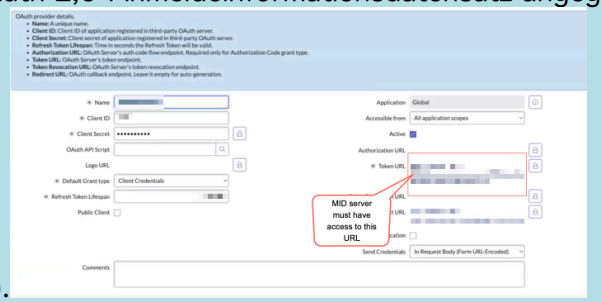
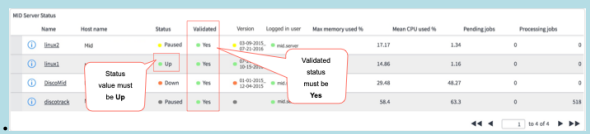
OAuth 2.0-Anmeldeinformationsformular (Fortsetzung)

Feld	Eingabewert
	Server. Wenn diese Option aktiviert ist, wird die Anforderung für ein OAuth-Token über gesendet MID-Server. **Wichtig:** • Die Option wird angezeigt, wenn der Wert in angezeigt wird **Gewährungstyp** Das Feld im OAuth-Entitätsprofil ist auf entweder festgelegt **Client-Anmeldeinformationen** , **Autorisierungscode** , Oder **Passwortanmeldeinformationen Des Ressourcenbesitzers** . Informationen zum Festlegen eines OAuth-Entitätsprofils für einen externen OAuth-Provider finden Sie unter Stellen Sie eine Verbindung zu einem OAuth-Drittanbieter her. • Wenn Sie auswählen **Stellen Sie über MID-Server eine Verbindung zum Authentifizierungsserver her** Kontrollkästchen müssen Sie die erforderlichen angeben MID-Server Oder MID Servers Von **Gilt für** Liste.
Betrifft	Geben Sie an, ob der Anmeldeinformationsdatensatz für alle MID-Server oder einen bestimmten MID-Server gilt. Wenn Sie „Spezielle MID Server“ auswählen, fügen Sie die entsprechenden MID Server hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Anmeldeinformationsformular (Fortsetzung)

Feld	Eingabewert
	Wichtig: Stellen Sie sicher, dass Sie sich dieser Überlegungen bewusst sind, wenn Sie ausgewählt haben **Stellen Sie über MID-Server eine Verbindung zum Authentifizierungsserver her** Kontrollkästchen. • Stellen Sie sicher, dass alle MID Servers Die in „gilt für“ ausgewählte Option kann mit dem Authentifizierungsserver kommunizieren. Dies ist erforderlich, um die Tokenanforderung für auszuführen **Token-URL**Erwähnt im OAuth-Anbieterdatensatz (der mit dem OAuth-Entitätsprofil verknüpft ist, das im OAuth 2,0-Anmeldeinformationsdatensatz angegeben ist).  • Stellen Sie sicher, dass mindestens eine vorhanden ist MID-Server(Im MID Servers In ausgewählt **Gilt für**) Mit diesen Konfigurationen: ◦ Der Wert von **Status** Feld ist **Aktiv** . ◦ Der Wert von **Validiert** Feld ist **Ja** . ◦ Die Fähigkeit von MID-Server Ist auf festgelegt **REST** Oder **ALLE** . Informationen zum Konfigurieren des MID-Servers finden Sie unter https://docs.servicenow.com/csh?topicname=t_ConfigureCapabilities&version=zurich&pubname=zurich-integrate-applications .  Weitere Informationen zu diesen Status finden Sie unter MID-Server-Dashboard .
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2.0-Anmeldeinformationsformular (Fortsetzung)

Feld	Eingabewert
	Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Anmeldeinformationsalias	Geben Sie den Anmeldeinformationsalias an, den Sie mit den OAuth 2,0-Anmeldeinformationen verknüpfen möchten.
Integrationstyp	Gibt den Integrationstyp für die Anmeldeinformationen an. Rufen Sie eine API einer Drittpartei mit einer OAuth-Anforderung auf, die ein System- oder anwenderspezifisches OAuth-Token generiert. Im Folgenden sind die Integrationstypen aufgeführt: • **System** : Ruft die Tokeninformationen basierend auf dem Profil der anfordernden Person ab. Die **System** Der Integrationstyp unterstützt die folgenden Authentifizierungsmechanismen: **1.** Security Assertion Markup Language (SAML) **2.** JSON-Webtoken (JWT) • **Persönlich** : Ruft die anwenderspezifischen Tokeninformationen ab. Der MID-Server-Anwender muss über verfügen `oauth_admin` Rolle. Die **Persönlich** Und **System** Integrationstypen unterstützen die folgenden Gewährungstypen: **1.** Autorisierungscode **2.** Passwort-Anmeldeinformationen des Ressourcenbesitzers Wenn dies der Fall ist **Persönlich** Ist auf der Seite „OAuth-Anfordererprofil“ ausgewählt, eine zusätzliche Kennzeichnung mit der Bezeichnung **Persönlich** Wird angezeigt. **Hinweis:** • Auf alle Informationen, die sich auf einen Anwender beziehen, kann nur mit anwenderspezifischen OAuth-Token mit dem Integrationstyp als zugegriffen werden **Persönlich** . • Um das anwenderbezogene Token für die Sitzung zu verwenden, müssen Sie auswählen **Ausführen Als** In den Flow-Eigenschaften als abgelegt **Anwender, der die Sitzung initiiert** .

SAP-Anmeldeinformationen

Der SAP-Anmeldeinformationstyp verwaltet den Zugriff auf SAP JCo-Systeme. Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Diese Felder sind im Formular „Anmeldeinformationen“ für Anmeldeinformationen des Typs „SAP“ verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Auswahl Von Spezifisch **Bestimmte MID-Server** Hat keine Auswirkungen auf die Auswahl des MID-Servers. Es wird nur verwendet, um zu entscheiden, welche MID-Server Transparenz für die Anmeldeinformationen haben sollen. **Bestimmte MID-Server** Wird in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

SNMP-Anmeldeinformationen

Discovery Untersucht viele Arten von Geräten (Switches, Router, Drucker usw.) mit dem SNMP-Protokoll. Anmeldeinformationen für SNMP enthalten keinen Anwendernamen, nur ein Passwort, genannt *`community-Zeichenfolge`* .

Die standardmäßige schreibgeschützte Community-Zeichenfolge für viele SNMP-Geräte ist öffentlich, und Discovery testet diese automatisch. Geben Sie die entsprechenden SNMP-Anmeldeinformationen ein, wenn sie sich von unterscheiden *`Öffentlich`* community-Zeichenfolge.

Beim Ermitteln von SNMP werden alle konfigurierten Community-Zeichenfolgen verwendet. Dieses Verhalten gilt nicht für das Ermitteln von SNMPv3.

Die standardmäßige SNMP-Abfrage der Orchestration-Aktivität gibt den Objektbezeichner (OID) eines Geräts zurück und erfordert SNMP-Anmeldeinformationen.

SNMP-Community Anmeldeinformationen

Der Anmeldeinformationstyp der SNMP-Community verwaltet den Zugriff, um viele Arten von Geräten (Switches, Router, Drucker usw.) mithilfe des SNMP-Protokolls zu ermitteln. Dieser Anmeldeinformationstyp ist für Discovery, Service-Mapping und Orchestration verfügbar.

SNMP-Anmeldeinformationen enthalten keinen Benutzernamen, nur ein Passwort (die Community-Zeichenfolge). Die standardmäßige schreibgeschützte Community-Zeichenfolge für viele SNMP-Geräte ist öffentlich, und das System testet diese automatisch. Geben Sie die entsprechenden SNMP-Anmeldeinformationen ein, falls diese sich von der öffentlichen Community-Zeichenfolge unterscheiden.

Diese Felder sind im Anmeldeinformationsformular für SNMP-Community verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Auswahl Von Spezifisch **Bestimmte MID-Server** Hat keine Auswirkungen auf die Auswahl des MID-Servers. Es wird nur verwendet, um zu entscheiden, welche MID-Server Transparenz für die Anmeldeinformationen haben sollen. **Bestimmte MID-Server** Wird in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

SNMPv3-Anmeldeinformationen

SNMPv3-Anmeldeinformationen akzeptieren ein Datenschutzprotokoll und einen zusätzlichen Datenschutzschlüssel und sind für Discovery und Orchestration verfügbar. Für externen Speicher in CyberArk können Sie einen Datenschutz-Account-Schlüssel auswählen.

Diese Felder sind im Anmeldeinformationsformular für SNMPv3 verfügbar.

SNMPv3-Anmeldeinformationsfelder

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel könnten Sie sie **SNMP-Community Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
MID-Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder (Fortsetzung)

Feld	Eingabewert
	Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Benutzername	Geben Sie den SNMP-Benutzernamen ein. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachfolgende Leerzeichen im Benutzernamen erkennt.
Authentifizierungsprotokoll	Wählen Sie den Authentifizierungstyp aus, der für diese Anmeldeinformationen verwendet werden soll. Die Auswahlmöglichkeiten sind: • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Authentifizierungsschlüssel	Geben Sie den mit diesen Anmeldeinformationen zu verwendenden Authentifizierungsschlüssel ein.
Datenschutzprotokoll	Wählen Sie das Verschlüsselungsprotokoll für diese Anmeldeinformationen aus. Die Auswahlmöglichkeiten sind: • 3DES • AES128 • AES192 • AES256 • DES
Datenschutzschlüssel	Geben Sie den Schlüssel ein, der dem ausgewählten Datenschutzprotokoll zugeordnet ist.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen in der JAR-Datei, die für einen externen Anmeldeinformationsanbieter auf den MID Server hochgeladen wurde, konfigurierten eindeutigen Schlüssel ein. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Speicher für Berechtigungsnachweise** aktiviert ist.
Datenschutz-Anmeldeinformations-ID	Geben Sie den für SNMPv3-Anmeldeinformationen konfigurierten Datenschutzkonto-Schlüssel in CyberArk ein. Wenn Sie ein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder (Fortsetzung)

Feld	Eingabewert
	Datenschutzprotokoll in CyberArk verwenden, muss dieses Feld denselben Wert aufweisen wie das Feld **Name** für das CyberArk-SNMPv3-Datenschutzkonto. Dieses Feld ist für SNMPv3 nur sichtbar, wenn Sie im Feld **Anmeldeinformationsspeicher-Typ** die Option **CyberArk** auswählen. Wenn Sie keinen Datenschutzschlüssel für CyberArk verwenden, lassen Sie dieses Feld leer.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn ein externer Speicher aktiviert ist, wird das Feld **Nachweis-ID** angezeigt. Eine externe Speicherung von Anmeldeinformationen ist nur verfügbar, wenn das External Credential Storage-Plugin aktiviert und die Ansicht **Externer Speicher** ausgewählt ist.
Anmeldeinformationsspeicher-Typ	Wählen Sie den Provider für den externen Speicher aus. Wählen Sie **CyberArk** nur aus, wenn Sie einen SNMPv3-Datenschutzschlüssel für CyberArk verwenden. Das Feld **Datenschutz-Anmeldeinformations-ID** wird zur Eingabe des Schlüssels angezeigt.
Kontext verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen Kontextwert für diese Anmeldeinformationen hinzuzufügen. Dieses Feld wird in der **Discovery**-Ansicht angezeigt. Kontexte werden derzeit für externe Anmeldeinformationsspeicher nicht unterstützt. **Hinweis:** Ein Kontext ist eine Sammlung von Verwaltungsinformationen, auf die SNMPv3-Anmeldeinformationen zugreifen, in denen auf eine bestimmte OID verwiesen wird. Auf Kontexte wird manchmal verwiesen, damit Informationen über das Gerät gesammelt werden können, auf die mit den normalen Anmeldeinformationen nicht zugegriffen werden kann. Ein Kontext kann vom Hersteller bereitgestellt oder separat konfiguriert werden. Wenn Sie über mehrere SNMPv3-Anmeldeinformationen mit demselben Benutzernamen und denselben Schlüsseln verfügen, einige Ihrer Geräte jedoch einen Kontext benötigen und andere nicht, müssen Sie für jedes Gerät separate Datensätze erstellen.
Kontextname	Geben Sie den Kontextnamenswert für diese Anmeldeinformationen ein. Diese Option sollte nur verwendet werden, wenn Sie über Geräte verfügen, die diesen Wert für einen vollständigen Zugriff benötigen. Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Kontext verwenden** aktiviert ist.

SSH-Anmeldeinformationen

Discovery, Orchestration und IntegrationHub Erkunden UNIX Und Linux Geräte, die SSH-Anmeldeinformationen verwenden, um Befehle über Secure Shell (SSH) auszuführen. SSH-Befehle müssen mit Stammberechtigungen ausgeführt werden, entweder mit Stamm-Anmeldeinformationen oder mit Sudo. Private SSH-Schlüsselanmeldeinformationen bieten zusätzliche Sicherheit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stammberechtigungen erteilen

Bevor Sie Stammberechtigungen gewähren, überprüfen Sie Ihre Sicherheitsrichtlinie und -optionen mit dem Sicherheitsteam Ihrer Organisation.

Verwenden Sie eine dieser Methoden, um Benutzern die Ausführung von SSH-Befehlen mit Stammberechtigungen zu ermöglichen:

- Erteilen Sie andere Anmeldeinformationen für Discovery, Orchestration oder IntegrationHub, aber gewähren Sie dem Benutzer in diesen Anmeldeinformationen das Recht, bestimmte Befehle mit Stammberechtigungen über sudo auszuführen. Dies ist eine sichere Methode zum Gewähren eingeschränkter Berechtigungen. Von Discovery, Orchestration oder IntegrationHub wird „sudo“ für jede Probe verwendet, für die der Parameter `must_sudo` auf **true** gesetzt ist (Standardeinstellung ist **false**). Hierfür muss allerdings jedes System so konfiguriert werden, dass es die Ausführung von sudo gestattet. Dies erfolgt durch Bearbeiten der Datei **/etc/sudoers** mit dem Befehl **visudo**.
- Teilen Sie **Stamm**-Anmeldeinformationen zu. Dies sind offenkundig die leistungsstärksten Anmeldeinformationen, unter Sicherheitsgründen aber möglicherweise nicht erstrebenswert. Wenn Discovery, Orchestration oder IntegrationHub über die Stammanmeldeinformationen für UNIX- oder Linux-Systeme verfügen, ist keine weitere Konfiguration erforderlich.

Privilegierte Befehle

Die Plattform bietet standardisierte privilegierte Befehle, die der MID Server verwenden kann, und die Möglichkeit, dem System zusätzliche Befehle hinzuzufügen. Weitere Informationen zur Verwendung von sudo und anderen privilegierten Befehlen finden Sie unter Privilegierte MID-Server-Befehle .

Anmeldeinformationstyp „Privater SSH-Schlüssel“

Hinweis: Die Anmeldeinformationen des privaten SSH-Schlüssels sollten in den meisten Fällen verwendet werden. Sie bieten eine bessere Sicherheit als SSH-Passwortanmeldeinformationen, einschließlich gegen MitM-Angriffe (man-in-the-Middle), bei denen die Kommunikation zwischen zwei Parteien abgefangen wird.

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel könnten Sie sie **SSH Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie einen UNIX- oder Linux-Benutzernamen ein. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt.
Passwort	Geben Sie das UNIX- oder Linux-Passwort ein. Geben Sie für Anmeldeinformationen vom Typ **Privater SSH-Schlüssel** das sudo-Passwort ein, wenn für den Benutzernamen ein Passwort erforderlich ist.
SSH-Passphrase	Geben Sie einen sicheren SSH-Passwortsatz ein. Dieses Feld ist nur für Anmeldeinformationen mit dem Typ **Privater SSH-Schlüssel** verfügbar.
Privater SSH-Schlüssel	Geben Sie einen sicheren, RSA-, DSA-, ECDSA- oder ED25519-privaten Schlüssel ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert

	Der private Schlüssel muss im richtigen Format eingegeben werden, um sicherzustellen, dass er ordnungsgemäß verschlüsselt ist. Der private Schlüssel muss mit der Zeichenfolge `-----BEGIN` beginnen.
	
	Hier ist ein Beispiel für einen korrekt formatierten privaten RSA-Schlüssel:
	
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8E`
	`RaStRZsh3IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i`
	`1Fs`
	`-----END RSA PRIVATE KEY-----`
	
	Ein Beispiel für einen DSA-Schlüssel:
	
	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8E`
	`RaStRZsh3IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i`
	`1Fs`
	`-----END DSA PRIVATE KEY-----`
	
	Ein Beispiel für einen ECDSA-Schlüssel:
	
	`-----BEGIN EC PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8E`
	`RaStRZsh3IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i`
	`1Fs`
	`-----END EC PRIVATE KEY-----`
	
	Und ein Beispiel für einen privaten ED25519-Schlüssel:
	
	`-----BEGIN OPENSSH PRIVATE KEY-----`
	`b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAA`
	`ABAAAAMwAAAAtzc2gtZW`
	`QyNTUxOQAAACAIYlqhcdwx8VQzZ5XaIC5ltQpjRr3lIlq/aE66mufmi`
	`wAAAKDQUtxZ0FLc`
	`WQAAAAtzc2gtZWQyNTUxOQAAACAIYlqhcdwx8VQzZ5XaIC5ltQpj`
	`Rr3lIlq/aE66mufmiw`
	`AAAECuvsTkFUPdpTh0kw23i8TYx19qsFOZ3TRgowkkHBh6wSVi`
	`WqFx3DHxVDNnldogLmW1`
	`CmNGveUiWr9oTrqa5+aLAAAAGmFiaGluYXYuc3V0YXJATVJFTU`
	`E3OTAzMkI3AQID`
	`-----END OPENSSH PRIVATE KEY-----`
	
	Hinweis: Für einen privaten ED25519-Schlüssel wird nur das OpenSSH-Schlüsselformat unterstützt, das mit dem OpenSSH SSH-keygen-Dienstprogramm generiert wird.
	
	Die ServiceNow AI Platform unterstützt private Schlüssel im PEM-Format, das vom OpenSSH-Dienstprogramm ssh-keygen generiert wird. So konvertieren Sie PPK-Schlüssel, die von PuTTY generiert wurden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	• Öffnen Sie Ihren privaten Schlüssel in PuTTYGen. • Exportieren Sie sie im OpenSSH-Format aus dem Menü **Konvertierungen** > **OpenSSH-Schlüssel exportieren**an. • Speichern Sie den neuen OpenSSH-Schlüssel.
SSH-Zertifikat	Geben Sie ein RSA- oder ED25519-basiertes OpenSSH-Zertifikat ein. Wenn das Zertifikat eingegeben wird, wird ein privater Schlüssel für die zertifikatbasierte Authentifizierung verwendet. Diese Authentifizierung wird ab OpenSSH 7,8 unterstützt.
Anmeldeinformationsalias	• Erlauben Sie Flow Designern die Verwendung von Aliassen zur Verwaltung von Verbindungs- und Berechtigungsinformationen. Wenn Sie ein Alias verwenden, müssen Sie nicht mehrere Anmeldeinformations- und Verbindungsinformationsprofile konfigurieren, wenn Sie mehrere Umgebungen verwenden. Wenn sich die Verbindungs- oder Anmeldeinformationen ändern, müssen Sie Aktionen, die die Verbindung verwenden, nicht aktualisieren. Weitere Informationen finden Sie unter Verbindung und Anmeldeinformationen. • Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
MID Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezielle MID-Server** aus dem Feld **Betrifft** auswählen.
Gilt für	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
Bestellung	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn Benutzer nach drei fehlgeschlagenen Anmeldeversuchen von den Sicherheitsfunktionen gesperrt werden. Wenn alle Anmeldeinformationen dieselbe Nummer (oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	keine) in der Reihenfolge haben, testet Discovery oder Orchestration die Anmeldeinformationen in zufälliger Reihenfolge.

SSH-Anmeldeinformationstyp

Diese Felder sind im SSH-Anmeldeinformationsformular verfügbar.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	• Erlauben Sie Flow Designern die Verwendung von Aliassen zur Verwaltung von Verbindungs- und Berechtigungsinformationen. Wenn Sie ein Alias verwenden, müssen Sie nicht mehrere Anmeldeinformations- und Verbindungsinformationsprofile konfigurieren, wenn Sie mehrere Umgebungen verwenden. Wenn sich die Verbindungs- oder Anmeldeinformationen ändern, müssen Sie Aktionen, die die Verbindung verwenden, nicht aktualisieren. Weitere Informationen finden Sie unter Verbindung und Anmeldeinformationen. • Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Nachweis-ID ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Bestellung	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Befehle, die Stammberechtigungen für Discovery, Orchestration und IntegrationHub erfordern

Diese Beispiele setzen voraus, dass der Benutzername **Disco** lautet. Setzen Sie den tatsächlichen Benutzernamen ein, und stellen Sie sicher, dass die Pfade für die Befehle mit den Pfaden im System übereinstimmen.

Hinweis: Sudo-Befehle funktionieren nicht mit Anmeldeinformationen mit privaten Schlüsseln, da für den Sudo-Befehl kein Passwort angegeben werden muss. Eine Lösung ist das Hinzufügen der Option *NOPASSWD* zur Sudo-Konfiguration. Zum Beispiel könnten Sie Folgendes eingeben: `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind

Befehl	Zweck
HP-UX	
adb	Erfasst CPU-Geschwindigkeit und Speicher. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/adb • **Verwendet von:** Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind (Fortsetzung)

Befehl	Zweck
Alle Linux- und UNIX-Versionen	
chage	Ändert die Anzahl der Tage zwischen Passwortänderungen und dem Datum der letzten Passwortänderung. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/chage • **Verwendet von**: Orchestration und IntegrationHub
chpasswd	Ändert Benutzerpasswörter. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /etc/chpasswd • **Verwendet von**: Orchestration und IntegrationHub
Alle Linux-Versionen	
dmidecode	Sammelt Informationen über die Hardware, einschließlich der Seriennummer des Motherboard. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /sbin/dmidecode • **Verwendet von:** Discovery
fdisk	Sammelt die Informationen über Datenträger und Größen im System. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/fdisk -l • **Verwendet von:** Discovery
multipath	Sammelt Gerätezuordnungen für MPIO. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/multipath -ll • **Verwendet von:** Discovery
ls	Sammelt den Inhalt eines Verzeichnisses. • **Zeilenbeispiel „/etc/sudoers“** : Disco ALL=(root) /usr/bin/LS, /bin/LS • **Verwendet von:** Discovery
Linux und Solaris	
dmsetup	Untersucht einen Low-Level-Datenträger.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind (Fortsetzung)

Befehl	Zweck
	• **Beispiel einer /etc/sudoers-Zeile**: ◦ Disco ALL=(root) /usr/bin/dmsetup table * ◦ Disco ALL=(root) /usr/bin/dmsetup ls • **Verwendet von:** Discovery
Alle UNIX-Versionen	
lsof	Ermittelt die Beziehung zwischen Prozessen und den Verbindungen, die zum System hergestellt werden. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /sbin/lsof • **Verwendet von:** Discovery
oratab	Ermöglicht den Lesezugriff auf die oratab-Datei zum Auffinden von Oracle Home und der Parameterdatei (pfile). • **Beispiel einer /etc/sudoers-Zeile**: Nicht zutreffend • **Verwendet von:** Discovery
Solaris	
iscsiadm	Ruft iSCSI-IQNs ab • **Beispiel einer /etc/sudoers-Zeile**: ${sudo:iscsiadm list target -S} • **Verwendet von:** Discovery
fcinfo	Ruft WWPNs für Ports ab. • **Beispiel einer /etc/sudoers-Zeile**: ${sudo:fcinfo remote-port -sl -p $port} • **Verwendet von:** Discovery
prtvtoc	Liefert Informationen zu Datenträgerpartitionen. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/prtvtoc • **Verwendet von:** Discovery
pfiles	Wird zum Sammeln von Informationen zu TCP-Verbindungen verwendet. • **/Etc/sudoers** Zeilenbeispiel: Disco ALL=(root) /usr/bin/pfiles • **Verwendet von:** Discovery

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX- und Linux-Befehle, für die Stammberechtigungen erforderlich sind (Fortsetzung)

Befehl	Zweck
Pgrep	Wird verwendet, um Prozess-IDs einer bestimmten Region aufzulisten, für die pfiles ausgeführt werden sollen. • **Zeile „/etc/sudoers“** Beispiel: Disco ALL=(root) /usr/bin/pgrep • **Verwendet von:** Discovery
/usr/bin/ps	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff eine proc_owner-Rolle hinzu. • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/bin/ps • **Verwendet von:** Discovery
/usr/ucb/ps	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff eine proc_owner-Rolle hinzu. Die Verwendung des Befehls `/usr/ucb/ps` ist ab Solaris 11 veraltet. Weil Discovery, Orchestration und IntegrationHub die Verwendung dieses Befehls für alle Solaris-Versionen erfordern, müssen Sie das ucb-Dienstprogramm auf Solaris 11-Systemen manuell installieren. Anweisungen dazu finden Sie in KB0564262 . • **Beispiel einer /etc/sudoers-Zeile**: Disco ALL=(root) /usr/ucb/ps • **Verwendet von:** Discovery

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern . Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Zugriffsanforderungen für Anmeldeinformationen ohne Root-Berechtigungen

Wenn Sie Discovery Anmeldeinformationen ohne Root-Zugriffsrechte erteilen, müssen Sie die folgenden Zugriffsanforderungen angeben.

Anwendung	Datei oder Verzeichnis	Erforderlicher Zugriff
Apache	httpd.conf	Lesen
Hbase	hbase-site.xml	Lesen
JBoss	jboss-service.xml	Lesen
	JBoss-Stammverzeichnis	Lesen
	web.xml	Lesen
MySQL	my.cnf	Lesen
NGINX	nginx.conf	Lesen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Datei oder Verzeichnis	Erforderlicher Zugriff
Oracle	oratab	Lesen
	Zugehörige Parameterdateien/Serverparameterdateien	Lesen
Oracle-Listener	lsnrctl	Ausführen
	listener.ora	Lesen
Tomcat	catalina.jar	Lesen
	server.xml	Lesen
	web.xml	Lesen
Unix	/etc/*release	Lesen
	/etc/bashrc	Lesen
	/etc/profile	Lesen
	/proc/cpuinfo	Lesen
	/proc/vmware/sched/ncpus	Lesen
	/var/log/dmesg	Lesen
	APD-Verzeichnis	Lesen
WebSphere	cell.xml	Lesen
	server.xml	Lesen
	serverindex.xml	Lesen

VMware-Anmeldeinformationen

Der VMware-Anmeldeinformationstyp verwaltet den Zugriff auf vCenter-Anmeldeinformationen.

Anwendungen, mit denen auf VMware-Cloud-Ressourcen zugegriffen wird, benötigen Zugriff auf VMware-Anmeldeinformationen. Der VMware-Anmeldeinformationstyp ermöglicht es Discovery beispielsweise, VMware vCenter auf einem Windows-Computer zu erkunden, um ESX-Computer, virtuelle Computer und Ressourcenpools zu erkennen. VMware DiscoveryUnd die Automatisierungs-API (vCenter-API) stellt jetzt die global eindeutige Seriennummer für Computer-CIs bereit. CIM-Anmeldeinformationen sind nicht erforderlich, um den Zugriff auf jeden VMware-Host zu ermöglichen.

Hinweis: Windows-Anmeldeinformationen sind für vCenter nicht erforderlich Discovery, Wenn gültige VMware-Anmeldeinformationen verwendet werden.

Wichtig: Verwenden Sie Anmeldeinformationen vom Typ **VMware** nicht für Orchestration-Aktivitäten, die auf den einzelnen von vCenter geklonten virtuellen Maschinen Aufgaben ausführen (z. B. Neustarten einer Linux-VM). Für diese Aktivitäten hängt der **Typ** der Anmeldeinformationen vom Betriebssystem der virtuellen Maschine ab (entweder **SSH** oder **Windows**).

Formular für VMWare-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für die VMware-Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für VMWare-Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
Anwendername	Geben Sie den Anwendernamen ein, den Sie für Ihren VMware-Account verwenden. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Die VMware-Anmeldeinformationen müssen in vCenter über die Rolle mit Lesezugriff verfügen.
Passwort	Geben Sie das Passwort für das VMware-Konto ein.
Betrifft	Wählen Sie mindestens eine aus MID ServersAus der Liste der verfügbaren MID Servers. Die in diesem Datensatz konfigurierten Anmeldeinformationen sind für verfügbar MID ServersIn dieser Liste. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Windows-Anmeldeinformationen

Windows-Anmeldeinformationen ermöglichen den Zugriff auf Windows-Computer. Dieser Anmeldeinformationstyp ist für Discovery und Orchestration verfügbar.

Anforderungen für Anmeldeinformationen

Für Discovery und Orchestration gelten die folgenden Anforderungen für Windows-Anmeldeinformationen:

- Installieren Sie einen MID Server auf einem Windows-Host als Service.
- Fügen Sie einer der folgenden Stellen Windows-Anmeldeinformationen hinzu:
  - Einem Eintrag in der Tabelle „Anmeldeinformationen“ [windows_credentials]
  - Einem MID Server-Service-Account, der als bestimmter Windows-Benutzer oder als Domänen-Account ausgeführt werden soll.

Richtige Berechtigungen erteilen

Um ausreichende Berechtigungen bereitzustellen, müssen Windows-Anmeldeinformationen eines der folgenden sein:

- Ein Domänenbenutzer mit lokalem Administratorzugriff auf Windows-Zielhosts
- Ein lokaler Account mit Administratorrechten und deaktivierter Benutzerzugriffssteuerung (User Access Control, UAC) auf demselben Zielhost

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Anwender, der die Anforderungen von erfüllt Windows Probes und Berechtigungen (Discovery Nur).
- Ein Benutzer, der die Anforderungen der auszuführenden Orchestration-Aktivität erfüllt (nur Orchestration)

Hinweis: Es sind keine Anmeldeberechtigungen erforderlich. Account muss NICHT interaktiv sein.

Die Sicherheit bei der Gewährung von privilegiertem Zugriff kann durch die Verwendung von JEA-Profilen zur Ausführung verbessert werden Discovery. Weitere Informationen finden Sie unter Microsoft Just Enough Administration (JEA) für Discovery .

Arbeitsgruppencomputer

Konfigurieren Sie die MID Server-Anmeldeinformationen für einen dieser Benutzer, um PowerShell-Befehle zum Ermitteln eines Arbeitsgruppencomputers auszuführen:

- Integrierter Administrator-Account auf dem Arbeitsgruppencomputer
- Domänenbenutzer auf dem Arbeitsgruppencomputer

Konfiguration für mehrere Domänen

Stellen Sie sicher, dass Sie die richtigen Namensformate und die richtige MID-Server-Konfiguration verwenden, damit Windows-Anmeldeinformationen für mehrere Domänen genutzt werden können.

Discovery und Orchestration unterstützen Windows-Domänenanmeldeinformationen der Benutzernamensformate **Benutzerprinzipalname** und **Kompatibler Anmeldename**. Zum Beispiel: **Domäne\Benutzername** oder **Benutzername@beispiel.domäne.com**. Sie können Anmeldeinformationen für Windows-Arbeitsgruppen im folgenden Format angeben: ARBEITSGRUPPE\Benutzername.

Hinweis: Sie können auch einen lokalen Account angeben, indem Sie den Benutzernamen **.** verwenden.

Diese zusätzlichen Aktionen sind erforderlich, damit die Anmeldeinformationen für mehrere Windows-Domänen verwendet werden können.

Bedingung	Zusätzlich erforderliche Aktionen
MID Server-Host in derselben Domäne wie das Windows-Ziel	Keine
MID Server-Host in einer anderen Domäne als das Windows-Ziel	Stellen Sie sicher, dass PowerShell 3,0 (oder höher bis zu 5,1) auf dem MID-Server-Host installiert ist.
MID Server-Host in einer anderen Domäne als das Microsoft SQL Server-Ziel	Siehe MSSQL-Server-Discovery .

Windows-Anmeldeinformationstyp

Diese Felder sind im Anmeldeinformationsformular für Windows verfügbar:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Für die CIM-Erkennung muss der Benutzer über die Administratorrolle verfügen.
Passwort	Geben Sie das Passwort ein.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen konfigurierten eindeutigen Schlüssel in der JAR-Datei ein, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Alias für Anmeldeinformationen	Erlauben Sie Workflow-Erstellern, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuzuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu. Geben Sie den Tabellennamen für den CI-Typ ein, zu dem das CI gehört (z. B. cmdb_ci_apache_web_server), um die Anmeldeinformationen zur Erkennung von CIs zu verwenden, die nicht zu diesem CI-Typ gehören und dafür Service Mapping- und Discovery-Muster nutzen.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn dasPlugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. **Hinweis:** Derzeit ist CyberArk das einzige unterstützte externe Speichersystem.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für **Spezielle MID-Server** angewendet werden sollen. Geben Sie an MID ServersDie diese Anmeldeinformationen in verwenden sollten **MID-Server** Feld.
MID Server verwenden	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Auswahl Von Spezifisch **Bestimmte MID-Server** Hat keine Auswirkungen auf die Auswahl des MID-Servers. Es wird nur verwendet, um zu entscheiden, welche MID-Server Transparenz für die Anmeldeinformationen haben sollen. **Bestimmte MID-Server** Wird in Orchestration-Aktivitäten nicht unterstützt.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Windows-MID-Server-Servicekonto	Wenn sie aktiv sind, stellen die definierten Anmeldeinformationen das MID-Server-Servicekonto dar.

Konfigurieren Sie Windows-Anmeldeinformationen für den MID-Server

Konfigurieren Sie den MID Server für die Verwendung der Anmeldeinformationen seines Windows-Service oder der Anmeldeinformationen aus der Tabelle „Anmeldeinformationen“ [discovery_credentials].

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Konfigurieren Sie den MID Server für die Verwendung von Anmeldeinformationen aus dem Service-Account des MID Servers.
   a. Legen Sie fest Konfigurieren Sie Anmeldeinformationen für Windows MID Server-Service An einen Anwender, der die Berechtigungsanforderungen erfüllt.
   b. Stellen Sie sicher, dass der Benutzername den Namensformatanforderungen entspricht.
   c. Füllen Sie die entsprechenden Felder im Formular aus.
   d. Stellen Sie sicher, dass die Anmeldeinformationen den Anforderungen der Domäne entsprechen.
2. Konfigurieren Sie den MID Server für die Verwendung der Anmeldeinformationen aus der Tabelle „Anmeldeinformationen“ [discovery_credentials].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Fügen Sie der Tabelle „Anmeldeinformationen“ [windows_credentials] Windows-Anmeldeinformationen hinzu.

- Stellen Sie sicher, dass jede Anmeldeinformation die Berechtigungsanforderungen erfüllt.
- Stellen Sie sicher, dass jeder Benutzername den Namensformatanforderungen entspricht.
- Stellen Sie sicher, dass jede Anmeldeinformation den Windows-Domänenanforderungen entspricht.

b. **Wahlweise:** Konfigurieren Sie den MID-Server für die Verwendung von Powershell, indem Sie festlegen mid.use_powershell Parameter bis **Wahr** .
Siehe MID-Server werden konfiguriert .

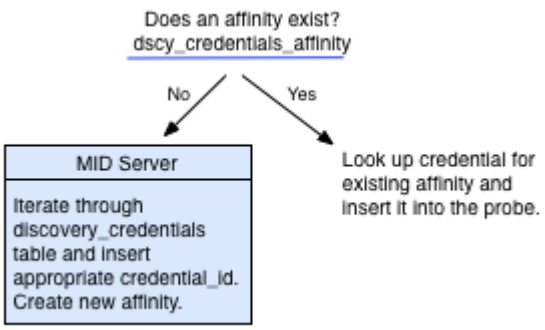
c. Aktivieren Sie das Kontrollkästchen Windows MID-Server-Servicekonto, um Anmeldeinformationen zu erstellen, die den Windows MID-Server-Servicekonto darstellen, der als bestimmter Windows-Anwender oder Domänenaccount ausgeführt werden soll.

Anmeldeinformationsaffinität für Discovery und Orchestration

Berechtigungsaffinität ist eine Verbindung zwischen einer Reihe von Anmeldeinformationen und einem Gerät im Netzwerk.

Beim ersten Versuch von Discovery oder Orchestration auf ein Gerät zuzugreifen, werden alle verfügbaren Anmeldeinformationen getestet, bis die richtigen gefunden werden. Nach der Ermittlung der Anmeldeinformationen für ein Gerät erstellen Discovery und Orchestration anhand der Tabelle „Anmeldeinformationsaffinität“ [dscy_credentials_affinity] eine Affinität zwischen den Anmeldeinformationen und dem Gerät. Bei allen nachfolgenden Ermittlungen oder Orchestration-Aktivitäten wird versucht, die Anmeldeinformationen in dieser Tabelle einem Gerät zuzuordnen, für das eine Affinität besteht. Wenn sich die Anmeldeinformationen für ein Gerät ändern, testen Discovery und Orchestration alle verfügbaren Anmeldeinformationen erneut, bis sie eine neue Affinität herstellen.

Berechtigungsaffinitäts-Diagramm



Hinweis: Wenn Orchestration und Discovery installiert sind und der Anmeldeinformationsalias aktiviert ist, können mehrere Affinitäten vorhanden sein. In diesem Fall sucht die Plattform nach Anmeldeinformationen für jede Affinität und fügt die Anmeldeinformation für die Affinität mit der niedrigsten Reihenfolgenummer in die Probe ein.

Behebung von Fehlern bei Anmeldeinformationen

Überprüfen Sie den Abschnitt <credentials_debug> des ECC-Warteschlangen-Payload, um Probleme mit Anmeldeinformationen zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestimmte Probes unterstützen das Debugging von Anmeldeinformationen. Beim Debugging von Anmeldeinformationen wird der Abschnitt <credentials_debug> in das Payload eingefügt, das der MID Server an die Instanz-ECC-Warteschlange zurückgibt. Sie können den Abschnitt <credentials_debug> anzeigen, um detaillierte Informationen zur Suche nach Anmeldeinformationen zu erhalten.

Der Abschnitt <credentials_debug> erscheint im Payload, wenn:

- Anmeldeinformationen für fehlgeschlagen WMIRunner-Probe , PowerShell-Probe , JMS , Oder SSHCommand-Probe .
- Setzen Sie den Parameter *credentials_debug* für die WMIRunner-, PowerShell- oder SSHCommand-Proben auf **true**. Wenn Sie diesen Parameter auf „true“ setzen, wird der Abschnitt <credentials_debug> auch dann angezeigt, wenn die Suche nach Anmeldeinformationen erfolgreich war.

Der Abschnitt <credentials_debug> enthält:

- Informationen über die Suche nach Anmeldeinformationen, z. B. Anmeldeinformationstypen, Tags und Affinitäten.
- Die Ziel-IP-Adresse.
- Informationen zu den einzelnen Anmeldeinformationen (in der Reihenfolge), die der MID-Server verwendet hat, einschließlich Typ, Klassifizierung, Tag, Name, SYS-ID und externe Anmeldeinformations-ID, falls vorhanden.

Beispiel-Payload mit ungültigen Anmeldeinformationen

Payload XML


```
<?xml version="1.0" encoding="UTF-8"?><results probe_time="6891" result_code="0"><result
id="6f10ed420a0a0b7e49052d83a32b586f" name="sh ${file:esx.sh}" order="1" topic="SSHCommand"><results
error="SSHCommand: Adding target to blacklist.  No valid credential found for types [SSH Password,SSH
Private Key]" probe_time="6860" result_code="42"><result error="SSHCommand: Adding target to blacklist.
No valid credential found for types [SSH Password,SSH Private Key]"><debug_info>{"debug_info":
[{"10.11.129.81":{"credentials_attempted":[{"credential_type":"SSH
Password","credential_name":"badCredential1","credential_order":"100","credential_success":false,"credenti
al_id":"6b43751d1362a200efffb6004244b0c3"},{"credential_type":"SSH
Password","credential_name":"badCredential2","credential_order":"200","credential_success":false,"credenti
al_id":"1553b11d1362a200efffb6004244b01b"},{"credential_type":"SSH
Password","credential_name":"badCredential3","credential_order":"300","credential_success":false,"credenti
al_id":"7d63f11d1362a200efffb6004244b0b0"}],"adding_key_to_target_blacklist":true,"connection_parameters":
{"credential_types":["SSH Password","SSH Private Key"],"target":"10.11.129.81"}}}]}</debug_info></result>
<parameters><parameter name="discover" value="CIs"/><parameter name="agent"
value="mid.server.demonightlyIstanbul_MID"/><parameter name="glide.xmlhelper.trim.enable" value="true"/>
<parameter name="use_class" value="discovery_classy_unix"/><parameter name="source" value="10.11.129.81"/>
<parameter name="priority" value="0"/><parameter name="use_snc_ssh" value="true"/><parameter name="probe"
value="10e0eebd0a0a0b4f61f46a5027df7fb6"/><parameter name="port_probe"
value="97ff2abd0a0a070300b7f37daa11a241"/><parameter name="port" value="22"/><parameter name="cidata"
value="&lt;CIData&gt;&lt;data&gt;&lt;fld name=&quot;ip_address&quot;&gt;10.11.129.81&lt;/fld&gt;&lt;/data&
gt;&lt;/CIData&gt;"/><parameter name="used_by_discovery" value="true"/><parameter name="name" value="sh
${file:esx.sh}"/><parameter name="topic" value="SSHCommand"/><parameter name="esx.sh" value="#!/bin
/sh&#13;&#10;# This command is rarely installed, so a Bourne shell script is used to squelch the exit
status and sensor warning when not found.&#13;&#10;# tcsh doesn't squelch exist status codes within
backticked statements&#13;&#10;echo `vmware -v 2&gt;&amp;1`"/><parameter name="ecc_queue" value=""/>
</parameters></results></result><result id="e5e075a2a9fe1561018f2a9636d5ec39" name="uname -a" order="1"
topic="SSHCommand"><results error="SSHCommand: Target is blacklisted.  No valid credential found for
```


Details werden für den PowerShell-Parameter angezeigt:

- Wenn die lokalen MID-Server-Anmeldeinformationen verwendet wurden, nachdem alle Windows-Anmeldeinformationen fehlgeschlagen sind.
- Wenn die Anmeldeinformationen übersprungen wurden, da Sie versuchen, denselben Computer zu erkennen, auf dem sich der MID-Server befindet.
- Wenn mid.powershell.use_credentials Parameter ist auf festgelegt Wahr .

Details werden für SSHCommand angezeigt:

- Wenn die Suche nach Anmeldeinformationen übersprungen wurde, da die Ziel-IP ausgeschlossen ist.
- Ob die Ziel-IP der Ausschlussliste hinzugefügt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der MID-Server speichert IP-Adressen für fehlgeschlagene Anmeldeinformationssuchen in einer Ausschlussliste im Cache-Speicher. Diese Ausschlussliste gibt an, auf welche Geräte der MID-Server nicht mehr zugreifen soll. IP-Adressen werden der Ausschlussliste hinzugefügt, nachdem alle Anmeldeinformationen fehlgeschlagen sind. Die IP-Adressen werden entweder nach fünf Minuten aus dem Cache der Ausschlussliste gelöscht, wenn der MID-Server neu gestartet wird oder wenn die Anmeldeinformationsdatensätze in der Instanz aktualisiert werden.

Externer Anmeldeinformationsspeicher

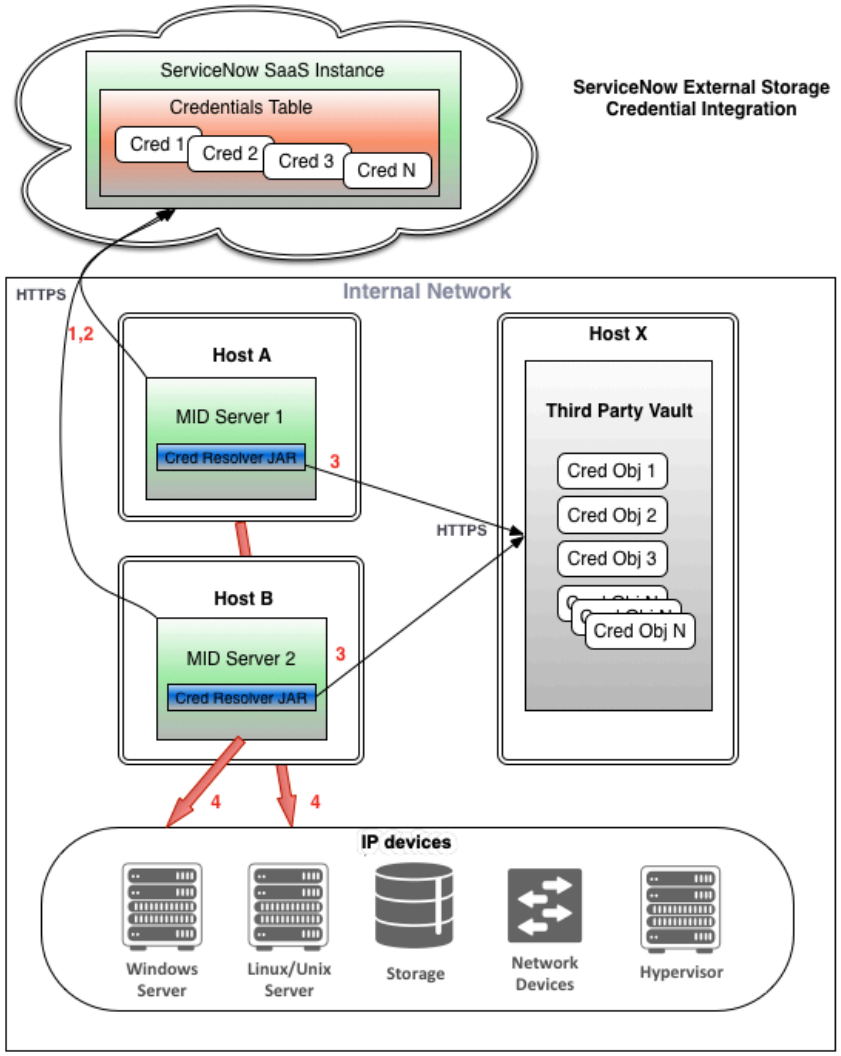
Eine Instanz kann Anmeldeinformationen, die von Discovery, Orchestration und Service-Mapping verwendet werden, in einem externen Anmeldeinformations-Repository anstatt direkt in einem ServiceNow-Anmeldeinformationsdatensatz speichern.

Die Instanz verwaltet einen eindeutigen Bezeichner für jede Anmeldeinformation, den Anmeldeinformationstyp (z. B. SSH, SNMP oder Windows) und alle Berechtigungsaffinitäten. Der MID Server erhält den Nachweis-Bezeichner von der Instanz und löst dann mithilfe einer vom Kunden bereitgestellten JAR-Datei den Bezeichner aus dem Repository in verwendbare Anmeldeinformationen auf. Derzeit ist ServiceNow® Die Plattform unterstützt die Verwendung von CyberArk-Tresor Oder BeyondTrust für externen Anmeldeinformationsspeicher.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Architektur des externen Anmeldeinformationsspeichers

Architektur des externen Anmeldeinformationsspeichers



Prozessablauf für Anmeldeinformationen

Der MID Server ruft Anmeldeinformationen anhand dieses Prozesses aus einem externen Speicher ab:

1. Der MID Server lädt Anmeldeinformationsobjekte aus der ServiceNow-Tabelle „Anmeldeinformationen“ [discovery_credentials] herunter, die die entsprechende Nachweis-ID aus dem Zieltresor enthalten.
2. Wie jede Probe oder jedes Muster von ausgeführt wird Discovery Oder Orchestration Aufträge fordert der MID-Server die Anmeldeinformationen an, indem Informationen wie Anmeldeinformations-ID, Ziel-IP-Adresse und Anmeldeinformationstyp an die Java JAR-Datei des Anmeldeinformations-Resolvers übergeben werden. Die Details zum richtigen Anmeldeinformationsobjekt, das aus dem Tresor abgerufen werden soll, werden vom Anmeldeinformations-Resolver bestimmt.

   Viele Anmeldeinformations-Resolver wie CyberArk rufen eine Anwendung auf, die vom Tresoranbieter des Drittanbieters bereitgestellt wird und auf demselben Computer wie der MID-Server ausgeführt wird. Diese Anwendung kann häufig so konfiguriert werden, dass Anmeldeinformationen zwischengespeichert werden. Sie weiß, den Cache

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu aktualisieren, wenn sich Anmeldeinformationen im Tresor ändern. Dies ist sehr wichtig, um unnötige Netzwerkaufrufe beim Tresor zu vermeiden, wenn der MID-Server eine Anmeldeinformation anfordert. Der Anmeldeinformations-Resolver (mit optionaler Lieferantenanwendung, falls vorhanden) ruft den Tresor an, um den tatsächlichen Anwendernamen, das Passwort usw. abzurufen

Für sofort einsatzbereite Anmeldeinformations-Resolver (heute nur CyberArk) speichert der MID-Server Anmeldeinformationen nur für bis zu mehrere Sekunden mithilfe von Verschlüsselung im MID-Server-Prozessspeicher. Dies bedeutet, dass der MID-Server mehrere Anforderungen an den Anmeldeinformations-Resolver stellen kann, auch wenn ein einzelnes Gerät erkannt wird. Wenden Sie sich an Drittpartei, um Informationen zu Caching-Implementierungen für andere Anmeldeinformations-Resolver zu erhalten.

3. Der MID Server führt die Probe mit den entsprechenden Anmeldeinformationen aus.

Hinweis: Berechtigungsaffinitäten gelten weiterhin. Der Mechanismus bleibt derselbe, da der einzige wirkliche Unterschied aus Sicht des MID Servers darin besteht, dass die tatsächlichen Anmeldeinformationen (Benutzername und Passwort) aus dem Tresor einer Drittpartei stammen.

Protokollierung des Speichers für externe Anmeldeinformationen

Der MID Server gibt Protokollnachrichten über den externen Anmeldeinformationsspeicher aus.

Wenn vom Repository beim Versuch, eine Anforderung für Anmeldeinformationen zu lösen, ein Fehler festgestellt wird, werden vom MID-Server Protokollnachrichten mit diesem Präfix ausgegeben: Problem with client's CredentialResolver: (Problem mit dem CredentialResolver des Clients).

Mit dem externen Anmeldeinformationsspeicher installierte Komponenten

Geschäftsregel

Mit der Geschäftsregel für externe Anmeldeinformationsspeicher werden die folgenden Aufgaben ausgeführt, wenn ein Administrator Änderungen an der Eigenschaft „Externen Anmeldeinformationsspeicher aktivieren“ vornimmt:

- Ändern der Ansicht für die Datensatzliste und des Formulars für Anmeldeinformationen in die Ansicht „Externer Speicher“. In dieser Ansicht können Anwender sehen **Anmeldeinformations-ID** Spalte in der Liste.
- Weist den MID-Server an, den Cache für Anmeldeinformationen zu aktualisieren. Dies dient der Vorbereitung auf eine geänderte Vorgehensweise zum Abrufen von Anmeldeinformationen.

Eigenschaft

Eine Eigenschaft mit der Bezeichnung „Extern Anmeldeinformationsspeicher aktivieren“ [com.snc.use_external_credentials] aktiviert oder deaktiviert das Plugin „Extern Anmeldeinformationsspeicher“, nachdem es aktiviert wurde. Die Eigenschaft befindet sich in **Discovery-Definition** > **Eigenschaften** und **Orchestration** > **MID-Server-Eigenschaften**, Und ist aktiviert, wenn Sie das Plugin aktivieren.

Wenn Sie die Speicherung von externen Anmeldeinformationen mit der Systemeigenschaft deaktivieren, werden alle externen Anmeldeinformationen in der Instanz vom System automatisch auf inaktiv festgelegt. Wenn Sie die Funktion mit dieser Eigenschaft erneut aktivieren, setzt das System die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

externen Anmeldeinformationsdatensätze nicht auf aktiv zurück. Sie müssen jeden Anmeldeinformationsdatensatz manuell erneut aktivieren.

Externen Anmeldeinformationsspeicher für Discovery und Orchestration anfordern

Das Plugin „Externer Anmeldeinformationsspeicher“ ist auf Anfrage erhältlich.

Vorbereitungen

Erforderliche Rolle: admin

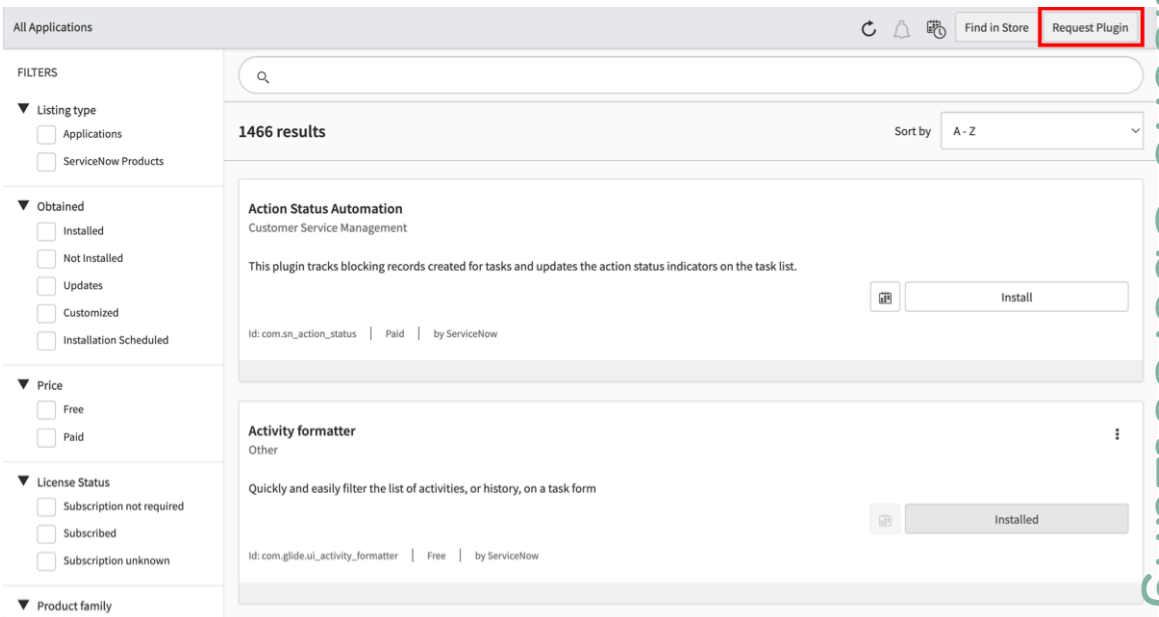
Warum und wann dieser Vorgang ausgeführt wird

Es gibt zwei Möglichkeiten, ein Plugin anzufordern:

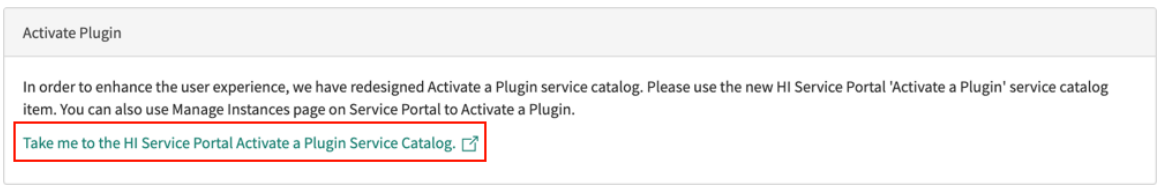
- Greifen Sie auf zu Now Support Servicekatalog direkt durch Auswahl **Alle** > **Servicekatalog** > **Plugin aktivieren** Ein Now Support.
- Greifen Sie über die Seite „Alle Anwendungen“ in Ihrer Instanz auf den Now Support-Servicekatalog zu, indem Sie die folgenden Schritte ausführen.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

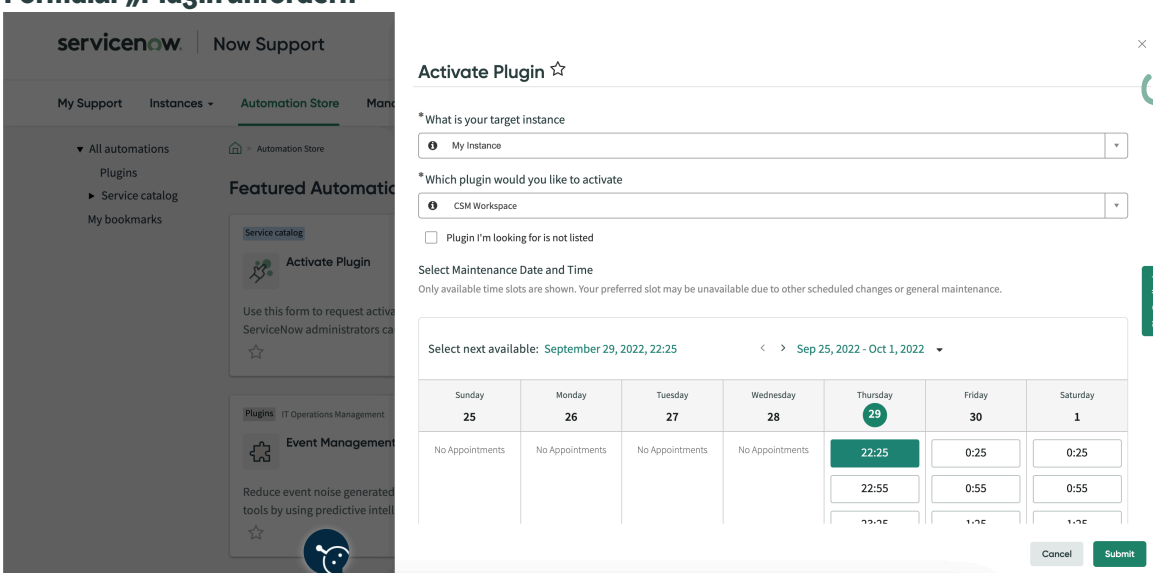
Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Konfiguration des externen Anmeldeinformationsspeichers

Konfigurieren Sie Ihre Instanz so, dass Anmeldeinformationen von einem Remote-Repository abgerufen werden.

Bei diesen Verfahren wird davon ausgegangen, dass Sie bereits ein externes Repository mit den Anmeldeinformationen konfiguriert haben, die Sie schützen möchten. Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss über die JAR-Datei den tatsächlichen Anmeldeinformationen im Repository zugeordnet werden.

Hinweis: ServiceNow unterstützt zwei externe Tresore gleichzeitig: Einen standardmäßigen CyberArk-Anmeldeinformations-Resolver und einen anwenderdefinierten externen Anmeldeinformations-Resolver. Beim Erstellen eines anwenderdefinierten CyberArk-Anmeldeinformations-Resolvers wird weiterhin der zweite anwenderdefinierte externe Tresor verwendet, und es können keine zusätzlichen anwenderdefinierten externen Tresore verwendet werden.

Führen Sie zum Konfigurieren des externen Anmeldeinformationsspeichers die folgenden Aufgaben in der angegebenen Reihenfolge aus.

JAR-Datei zum Auflösen der Anmeldeinformationen erstellen

Erstellen Sie eine JAR-Datei, um die vom MID Server gesendeten Anmeldeinformationen in tatsächliche Anmeldeinformationen aus dem Repository aufzulösen.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Stellen Sie sicher, dass alle Anmeldeinformationen enthalten sind, die die Instanz erwartet, wie z. B. der private Schlüssel.

So erstellen Sie eine JAR-Datei zum Auflösen von Anmeldeinformationen:

Prozedur

Verwenden Sie entweder die auf bereitgestellten Vorlagen ServiceNow github oder die Java-Beispieldatei.

Achtung: Diese Beispiele sind nur als Vorlage vorgesehen. Tun **NICHT** Verwenden Sie diesen Code in der Produktion, ohne ihn für Ihre Umgebung zu ändern.

a. Laden Sie die Open Source-JAR-Dateien mit Anweisungen aus dem herunter ServiceNow github:
   - HashiCorp – Resolver für externe Anmeldeinformationen
   - CyberArk – Resolver für externe Anmeldeinformationen

b. Verwenden Sie die folgende Java-Beispieldatei als Vorlage, und ändern Sie sie entsprechend Ihrer Umgebung:

Example

```
package com.snc.discovery;

import java.util.*;
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
import java.io.*;

/**
 * Basic implementation of a CredentialResolver that uses a properties file.
 */

public class CredentialResolver {

 private static String ENV_VAR = "CREDENTIAL_RESOLVER_FILE";
 private static String DEFAULT_PROP_FILE_PATH = "C:\\dummycredentials.properties";

 // These are the permissible names of arguments passed INTO the resolve()
 // method.

 // the string identifier as configured on the ServiceNow instance...
 public static final String ARG_ID = "id";

 // a dotted-form string IPv4 address (like "10.22.231.12") of the target
 // system...
 public static final String ARG_IP = "ip";

 // the string type (ssh, snmp, etc.) of credential as configured on the
 // instance...
 public static final String ARG_TYPE = "type";

 // the string MID server making the request, as configured on the
 // instance...
 public static final String ARG_MID = "mid";

 // These are the permissible names of values returned FROM the resolve()
 // method.

 // the string user name for the credential, if needed...
 public static final String VAL_USER = "user";

 // the string password for the credential, if needed...
 public static final String VAL_PSWD = "pswd";

 // the string pass phrase for the credential if needed:
 public static final String VAL_PASSPHRASE = "passphrase";

 // the string private key for the credential, if needed...
 public static final String VAL_PKEY = "pkey";

 // the string authentication protocol for the credential, if needed...
 public static final String VAL_AUTHPROTO = "authprotocol";

 // the string authentication key for the credential, if needed...
 public static final String VAL_AUTHKEY = "authkey";

 // the string privacy protocol for the credential, if needed...
 public static final String VAL_PRIVPROTO = "privprotocol";

 // the string privacy key for the credential, if needed...
 public static final String VAL_PRIVKEY = "privkey";
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
private Properties fProps;

public CredentialResolver() {
}

private void loadProps() {
 if(fProps == null)
  fProps = new Properties();

 try {
  String propFilePath = System.getenv(ENV_VAR);
  if(propFilePath == null) {
   System.err.println("Environment var "+ENV_VAR+" not found. Using default file:
"+DEFAULT_PROP_FILE_PATH);
   propFilePath = DEFAULT_PROP_FILE_PATH;
  }

  File propFile = new File(propFilePath);
  if(!propFile.exists() || !propFile.canRead()) {
   System.err.println("Can't open "+propFile.getAbsolutePath());
  }
  else {
   InputStream propsIn = new FileInputStream(propFile);
   fProps.load(propsIn);
  }

 //fProps.load(CredentialResolver.class.getClassLoader().getResourceAsStream("dummycred
entials.properties"));
 } catch (IOException e) {
  System.err.println("Problem loading credentials file:");
  e.printStackTrace();
 }
}

/**
 * Resolve a credential.
 */
public Map resolve(Map args) {
 loadProps();
 String id = (String) args.get(ARG_ID);
 String type = (String) args.get(ARG_TYPE);
 String keyPrefix = id+"."+type+".";

 if(id.equalsIgnoreCase("misbehave"))
  throw new RuntimeException("I've been a baaaaaaaaad CredentialResolver!");

 // the resolved credential is returned in a HashMap...
 Map result = new HashMap();
 result.put(VAL_USER, fProps.get(keyPrefix + VAL_USER));
 result.put(VAL_PSWD, fProps.get(keyPrefix + VAL_PSWD));
 result.put(VAL_PKEY, fProps.get(keyPrefix + VAL_PKEY));
 result.put(VAL_PASSPHRASE, fProps.get(keyPrefix + VAL_PASSPHRASE));
 result.put(VAL_AUTHPROTO, fProps.get(keyPrefix + VAL_AUTHPROTO));
 result.put(VAL_AUTHKEY, fProps.get(keyPrefix + VAL_AUTHKEY));
 result.put(VAL_PRIVPROTO, fProps.get(keyPrefix + VAL_PRIVPROTO));
 result.put(VAL_PRIVKEY, fProps.get(keyPrefix + VAL_PRIVKEY));
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 System.err.println("Error while resolving credential id/type["+id+"/"+type+"]");

 return result;
}


/**
 * Return the API version supported by this class.
 */
public String getVersion() {
 return "1.0";
}

public static void main(String[] args) {
 CredentialResolver obj = new CredentialResolver();
 obj.loadProps();

 System.err.println("I spy the following credentials: ");
 for(Object key: obj.fProps.keySet()) {
  System.err.println(key+": "+obj.fProps.get(key));
 }

}
}
```

JAR-Datei zum Auflösen der Anmeldeinformationen importieren

Importieren Sie eine JAR-Datei, um die vom MID Server gesendeten Nachweis-Bezeichner in tatsächliche Anmeldeinformationen aus dem Repository aufzulösen.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Nach dem Erstellen der JAR-Datei importieren Sie sie in die Instanz; dort kann der MID Server darauf zugreifen.

Prozedur

1. Kopieren Sie nach dem Erstellen der JAR- und Eigenschaftendateien die Eigenschaftendatei auf den MID-Server.
2. Navigieren zu **MID-Server** > **JAR-Dateien**an.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die folgenden Felder aus:

Feld	Beschreibung
Name	Ein eindeutiger und beschreibender Name zum Identifizieren der Datei in der Instanz.
Version	Eine Versionsnummer für die Datei, sofern verfügbar.
Quelle	Speicherort der JAR-Datei zu Referenzzwecken. Quellinformationen werden vom System nicht verwendet.
Beschreibung	Kurzbeschreibung der JAR-Datei und ihres Zwecks in der Instanz.

5. Klicken Sie auf das Büroklammersymbol im Banner, und hängen Sie die JAR-Datei an den Datensatz an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example

Eine JAR-Datei anhängen

6. Klicken Sie auf **Absenden**.
7. Starten Sie den MID-Server-Service neu.
   Die Plattform stellt die JAR-Datei jedem MID Server zur Verfügung, der für die Kommunikation mit der Instanz konfiguriert ist.

Nachweis-Bezeichner konfigurieren

Konfigurieren Sie den Nachweis-Bezeichner in der Instanz.

Vorbereitungen

Erforderliche Rolle: Administrator

Überprüfen Sie Folgendes:

- Das Plugin Externer Anmeldeinformationsspeicher muss aktiv sein.
- Die Discovery-Eigenschaft Externen Anmeldeinformationsspeicher aktivieren ist aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen** oder **Orchestration** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie einen Anmeldeinformationstyp aus.
4. Aktivieren Sie das Kontrollkästchen **Externer Anmeldeinformationsspeicher**.
   Die **Anwendername** Und **Passwort** Felder, und werden ausgeblendet **Anmeldeinformations-ID** Feld und **Anmeldeinformationsspeicher-Tresor** Menü wird angezeigt.
5. Von **Anmeldeinformationsspeicher-Tresor** Wählen Sie entweder keine, den CyberArk-Tresor oder einen anwenderdefinierten externen Anmeldeinformationsspeicher aus.

   Hinweis:

   Wenn CyberArk Vault ausgewählt ist, wird **Suchschlüssel** Das Menü wird mit vier Suchschlüsseloptionen angezeigt: Anmeldeinformations-ID, IP-Adresse, FQDN, alle oben genannten. Wenn Sie alle der oben genannten Optionen auswählen, kann die Leistung beeinträchtigt werden, da mehrmals auf den Tresor zugegriffen werden muss.

   a. Um einen anwenderdefinierten Tresor für einen externen Anmeldeinformationsspeicher zu verwenden, navigieren Sie in der Instanz zu Vault-Konfigurationen [Vault_Configuration.list].

   b. Erstellen Sie einen neuen Datensatz mit einem Namen, der einer importierten JAR-Datei für einen anwenderdefinierten Anmeldeinformations-Resolver zugeordnet ist.

   Siehe Verfahren JAR-Datei zum Auflösen der Anmeldeinformationen erstellen Und JAR-Datei zum Auflösen der Anmeldeinformationen importieren Informationen zum Erstellen eines anwenderdefinierten Tresors für einen Speicher mit externen Anmeldeinformationen.

6. Füllen Sie das Formular „Anmeldeinformationen“ mithilfe der Felder aus der folgenden Tabelle aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen in der JAR-Datei, die für ein externes Anmeldeinformationssystem auf den MID Server hochgeladen wurde, konfigurierten eindeutigen Schlüssel ein. Dies ist die ID, die an die Java-Klasse in der Parameterzuordnung übergeben wird: `public static final String ARG_ID = "id";` Der MID-Server verwendet diesen Identifier, um die tatsächlichen Anmeldeinformationen im Repositorium aufzulösen. **Hinweis:** Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Anmeldeinformationsspeicher** aktiviert ist.
Tag	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn Sie diese Option auswählen, werden die Felder **Benutzername** und **Passwort** durch das Feld **Nachweis-ID** ersetzt. Externe Anmeldeinformationsspeicher stehen nur zur Verfügung, wenn das Plugin „Externer Anmeldeinformationsspeicher“ aktiviert ist.
Anmeldeinformationsspeicher Tresor	Wählen Sie den Tresor des externen Anmeldeinformationsspeichers aus einer Liste verfügbarer Tresore aus. Das Menü besteht aus Datensätzen aus den Vault-Konfigurationen [Vault_Configuration.list]. Neue Datensätze können hinzugefügt werden und Namen verwenden, die anwenderdefinierten Anmeldeinformations-Resolver-JAR-Dateien zugeordnet sind. Siehe Verfahren JAR-Datei zum Auflösen der Anmeldeinformationen erstellen Und JAR-Datei zum Auflösen der Anmeldeinformationen importieren Informationen zum Erstellen eines anwenderdefinierten Tresors für einen Speicher mit externen Anmeldeinformationen.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
MID-Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Bestellung	Geben Sie die Reihenfolge ein, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto weiter oben werden diese Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn Benutzer nach drei fehlgeschlagenen Anmeldeversuchen von den Sicherheitsfunktionen gesperrt werden. Wenn alle Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	dieselbe Nummer (oder keine) in der Reihenfolge haben, testet Discovery oder Orchestration die Anmeldeinformationen in zufälliger Reihenfolge.

7. Klicken Sie auf **Absenden**.

Nachweis-Bezeichner für AWS konfigurieren

Konfigurieren Sie Ihre Instanz so, dass Anmeldeinformationen von einem Remote-Repository abgerufen werden.

Vorbereitungen

Erforderliche Rolle: cloud_admin

Überprüfen Sie, ob diese Plugins aktiv sind und der MID-Server installiert wurde:

- Discovery [com.snc.discovery]
- Cloud Provisioning and Governance [Com.snc.Cloud.mgmt]
- Externer Anmeldeinformationsspeicher [com.snc.Discovery.external_credentials]

Warum und wann dieser Vorgang ausgeführt wird

Bei diesen Verfahren wird davon ausgegangen, dass Sie bereits ein externes Repository mit den Anmeldeinformationen konfiguriert haben, die Sie schützen möchten. Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss über die JAR-Datei den tatsächlichen Anmeldeinformationen im Repository zugeordnet werden.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie eine Anmeldeinformation aus, die Ihr externer Anmeldeinformationsspeicher-Anbieter unterstützt.
3. Füllen Sie das Formular mithilfe der Felder aus der Tabelle aus.

Feld	Beschreibung
Name	Ein eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel „Amazon Web Services“.
Aktiv	Kontrollkästchen zum Aktivieren oder Deaktivieren der Anmeldeinformationen.
Anmeldeinformations-ID	Geben Sie den Namen ein, unter dem diese Anmeldeinformationen im externen Anmeldeinformationsspeicher-Anbieter gespeichert werden.
MID-Server	Wählen Sie einen oder mehrere MID-Server aus, die diese Anmeldeinformationen verwenden können.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn ein externer Speicher aktiviert ist, wird das Feld **Nachweis-ID** angezeigt. Wenn dieses Kontrollkästchen nicht sichtbar ist, klicken Sie auf das Menüsymbol in der Kopfzeile, und wählen Sie aus **Ansicht** > **Externer Speicher** Aus dem Kontextmenü.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anmeldeinformationsspeicher Tresor	Wählen Sie Aus **CyberArk** .

4. Klicken Sie auf **Absenden**.

CyberArk Integration des Anmeldeinformationsspeichers

Die MID-Server Integration mit CyberArk Tresor aktiviert ServiceNow® Orchestration, ServiceNow® Discovery, Und ServiceNow® Service-Mapping Zur Ausführung, ohne Anmeldeinformationen in der Instanz zu speichern.

Einführung in CyberArk

CyberArk Das Produkt „Application Identity Management“ (AIM) verwendet die Sicherheitslösung für Privileged Account, um die Speicherung von Anwendungspasswörtern, die in Anwendungen, Skripts oder Konfigurationsdateien eingebettet sind, zu überflüssig zu machen, und ermöglicht die zentrale Speicherung, Protokollierung und Verwaltung dieser hochsensiblen Passwörter innerhalb von CyberArk Tresor. Dieser Ansatz ermöglicht es Organisationen, die internen und behördlichen Anforderungen hinsichtlich der periodischen Ersetzung von Passwörtern zu erfüllen und Aktivitäten zu überwachen, die mit allen Arten von privilegierten Identitäten verbunden sind, ob vor Ort oder in der Cloud.

Die Instanz verwaltet einen eindeutigen Bezeichner für jede Anmeldeinformation, den Anmeldeinformationstyp (z. B. SSH, SNMP oder) Windows) Und alle Anmeldeinformationsaffinitäten. Die MID-Server Ruft den Anmeldeinformationsbezeichner, den Anmeldeinformationstyp und die IP-Adresse von der Instanz ab und verwendet dann CyberArk Tresor, um diese Elemente in nutzbare Anmeldeinformationen aufzulösen. Der Anmeldeinformations-Resolver kann auch den Hostnamen und den fqdn suchen und die umgekehrte DNS-Suche verwenden, um fqdn abzurufen.

Die CyberArk Für die Integration ist erforderlich ServiceNow® Plugin „externer Anmeldeinformationsspeicher“ , Der in verfügbar ist **Systemdefinitionen** > **Pluginsan**. Die MID-Server Und CyberArk AIM-/API-Client muss auf demselben Computer installiert sein. CyberArk Application Access Manager (AAM)-Anmeldeinformationsanbieter Version 12.0.1 und höher werden unterstützt.

Mit CyberArk installierte Komponenten

- **Business-Regel**: Die Business-Regel „Externer Anmeldeinformationsspeicher“ führt die folgenden Aufgaben aus, wenn ein Administrator Änderungen an der Eigenschaft „Externer Anmeldeinformationsspeicher“ vornimmt:
  - Ändern der Ansicht für die Datensatzliste und des Formulars für Anmeldeinformationen in die Ansicht „Externer Speicher“. In dieser Ansicht können Benutzer die Spalte „Nachweis-ID“ in der Liste sehen.
  - Weist an MID-Server Aktualisiert den Cache für nicht externe Anmeldeinformationen zur Vorbereitung auf eine Änderung in der Art und Weise, wie Anmeldeinformationen abgerufen werden.
- **Systemeigenschaft**: Die Eigenschaft „Externen Anmeldeinformationsspeicher aktivieren“ [com.snc.use_external_credentials] aktiviert oder deaktiviert das Plugin „Externer Anmeldeinformationsspeicher“, nachdem es aktiviert wurde. Diese Eigenschaft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

befindet sich in **Discovery-Definition** > **Eigenschaften** Und **Orchestration** > **MID-Server-Eigenschaften**, Und ist aktiviert, wenn Sie das Plugin aktivieren.

Hinweis: Wenn Sie die Einsatzbereitschaft des externen Anmeldeinformationsspeichers über die Systemeigenschaft widerrufen, setzt das System automatisch alle externen Anmeldeinformationen in der Instanz auf „Inaktiv“. Wenn Sie die Funktion mithilfe dieser Eigenschaft erneut in Einsatzbereitschaft versetzen, setzt das System die externen Anmeldeinformationsdatensätze nicht wieder auf „Aktiv“. Sie müssen jeden Anmeldeinformationsdatensatz manuell neu aktivieren.

Unterstützte Anmeldeinformationstypen

Die CyberArk Die Integration unterstützt diese ServiceNow Anmeldeinformationstypen:

- GCP
- Azure
- CIM
- JMS
- SNMP-Forum
- SNMPv3
- Basisauth.
- SSH-Schlüsselpaar
- Privater SSH-Schlüssel (mit Schlüssel, Passphrase und Passwort)
- VMware
- Windows
- Passende Anmeldeinformationen

Hinweis: Zu verwenden CyberArk Integration mit dem GCP-Anmeldeinformationstyp. Sie müssen die externe Anmeldeinformationsspeicher-JAR ändern. Weitere Informationen finden Sie unter ServiceNow GCP-Anmeldeinformations-Resolver mit CyberArk .

ServiceNow AI Platform Funktionen, die diese Netzwerkprotokolle verwenden, unterstützen auch die Verwendung von Anmeldeinformationen, die auf einem gespeichert sind CyberArk Tresor.

Vom Netzwerkprotokoll unterstützte Anmeldeinformationen

Netzwerkprotokoll	ServiceNow® Flow Designer Support	Orchestration -Unterstützung
SOAP	SOAP-Schritt	Erstellen Sie eine SOAP-Webserviceaktivität Mit Überschreibungen der Standardauthentifizierung
REST	REST-Schritt	Erstellen Sie eine REST-Webservice-Aktivität Mit Überschreibungen der Standardauthentifizierung
JDBC	JDBC-Schritt	JDBC-Aktivität
SSH	SSH-Schritt	SSH-Aktivität
PowerShell	PowerShell-Schritt	PowerShell-Aktivität
SFTP	SFTP-Schritt	SFTP-Aktivität

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vom Netzwerkprotokoll unterstützte Anmeldeinformationen (Fortsetzung)

Netzwerkprotokoll	ServiceNow® Flow Designer Support	Orchestration -Unterstützung
JMS		JMS-Aktivität

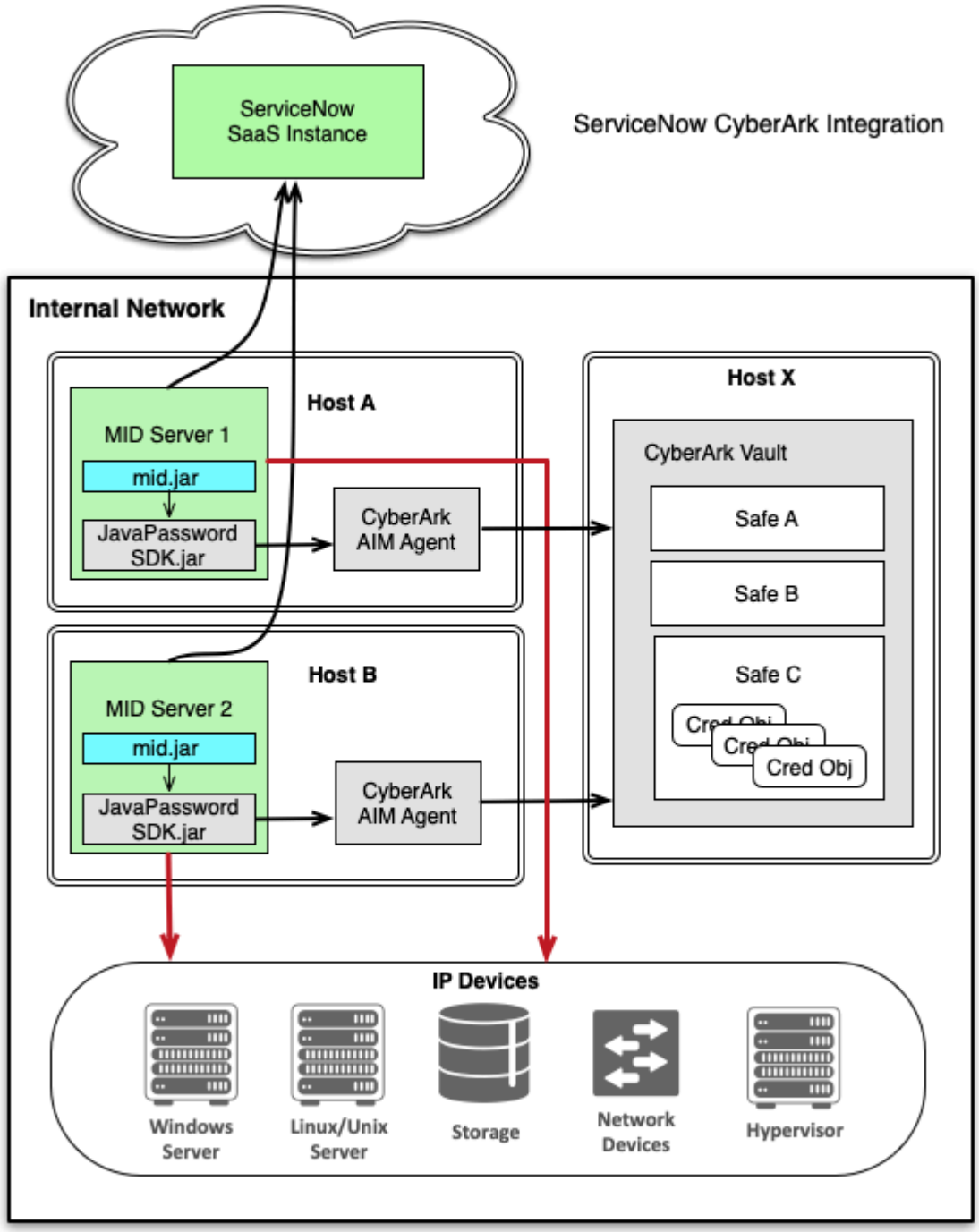
Wichtig: Sie können keine Anmeldeinformationen verwalten, die in einem gespeichert sind CyberArk Tresor und ein anwenderdefiniertes Externer Anmeldeinformationsspeicher System verwendet dasselbe MID-Server. Die MID-Server Und CyberArk AIM-/API-Client muss auf demselben Computer installiert sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CyberArk-Architektur

CyberArk Speicherarchitektur



Hinweis: CyberArk Verwendet das Basissystem `mid.jar` Datei zum Auflösen von Anmeldeinformationen.

Wie MID-Server Handles Windows Accounts

Bei der Anmeldeinformationssuche wird zunächst versucht, die angegebene Anmeldeinformations-ID mit einem vorhandenen Wert in abzugleichen CyberArk Tresor **Name** Feld. Wenn eine Übereinstimmung gefunden wird, werden die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen ausgegeben. Wenn keine Übereinstimmung gefunden wird, versucht die Anmeldeinformationssuche, mithilfe der IP-Adresse eine Übereinstimmung zu finden. Wenn die IP-Adressensuche mit mehr als einer Anmeldeinformation übereinstimmt, z. B. Windows Und Tomcat Auf demselben Server schlägt die Suche fehl. Um dieses Problem zu vermeiden, legen Sie fest *ext.cred.type_specifier*Parameter in MID-Server Datei config.xml in **Wahr** Zu erzwingen CyberArk Um Anmeldeinformationen zurückzugeben, die sowohl dem Anmeldeinformationstyp als auch der IP-Adresse entsprechen. Beispiel: Wenn eine IP-Adresse von beiden geteilt wird Windows Und Tomcat, Ein Anmeldeinformationstyp von Windows Gibt zurück Windows Nur Anmeldeinformationen.

Führen Sie ein Upgrade von durch CyberArk Bibliothek

Sie können ein Upgrade von durchführen CyberArk Bibliothek, wenn ein gesicherter Konfigurationsparameter erforderlich ist.

Überprüfen Sie den folgenden Konfigurationsparameter in **config.xml** : `<parameter name="mid.secure_config.provider" value="com.service_now.mid.services.config.CyberArkSecuredConfigProvider"/>`

Führen Sie die folgenden Schritte aus, um das Upgrade durchzuführen, wenn ein Provider für gesicherte Konfigurationsparameter konfiguriert ist.

1. Benennen Sie um CyberArk Client-Version bis `JavaPasswordSDK_MajorVersion_minorVersion_patchNum.jar` .
2. Erstellen Sie einen neuen JAR-Eintrag in `ecc_Agent` Tabelle, an die das Umbenennungs-JAR angehängt werden kann. Dieser neue Eintrag wird in heruntergeladen MID-Server. Dieser Schritt führt zu zwei JAR-Dateien (Passwordsdk.jar und JavaPasswordSDK _12_X_X.jar).
3. Löschen Sie den alten ecc_Agent-Eintrag aus der Instanz. Dieser Schritt löscht Passwordsdk.jar aus der MID-Server, Und JavaPasswordSDK _12_X_X.jar verbleibt im System.

Konfiguration der CyberArk-Integration

Diese Verfahren umfassen sowohl Konfigurationsaufgaben für CyberArk als auch ServiceNow, einschließlich Verweisen auf die entsprechende CyberArk-Dokumentation.

Der in der ServiceNow-Instanz konfigurierte Nachweis-Bezeichner muss dem Anmeldeinformationsnamen im CyberArk-Tresor zugeordnet sein. Bei der Suche nach Anmeldeinformationen findet der MID-Server die Anmeldeinformationen, indem er den Anmeldeinformationsbezeichner mit einem Namen im Tresor abgleicht, der eindeutig sein muss. Wenn der Nachweis-Bezeichner leer ist, ermittelt der MID Server die Anmeldeinformationen anhand der IP-Adresse. Um die Anmeldeinformationen anhand der IP-Adresse zu ermitteln, prüft das System den Anmeldeinformationstyp, um sicherzustellen, dass sich an dieser Adresse nur eine Anmeldeinformation dieses Typs befindet. Ein Beispiel hierfür könnte die Ausführung eines Windows-Servers und von vCenter auf derselben IP-Adresse sein. Um die strengen Anforderungen für Anmeldeinformationen in einer SSH-Umgebung zu unterstützen, können Sie in einem MID Server-Konfigurationsparameter angeben, dass der angeforderte Anmeldeinformationstyp dem von CyberArk zurückgegebenen Typ entsprechen muss.

Hinweis: Die **Anmeldeinformations-ID** Das Feld ist das einzige Feld, das erforderlich ist, um Ihre Anmeldeinformationen CyberArk zuzuordnen, in allen Fällen außer SNMPv3. Die **ID der Datenschutz-Anmeldeinformationen** Das Feld ist optional und nur erforderlich, wenn SNMPv3-Anmeldeinformationen und ein Datenschutzprotokoll für die Anmeldeinformationen verwendet werden. Unter Konfigurieren Sie den CyberArk-Anmeldeinformationsbezeichner finden Sie weitere Details.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um Ihre Instanz so zu konfigurieren, dass Anmeldeinformationen von einem CyberArk-Tresor abgerufen werden, führen Sie diese Aufgaben in der angegebenen Reihenfolge aus.

CyberArk-Tresor konfigurieren und die AIM-API installieren

Konfigurieren Sie den CyberArk-Tresor so, dass er dem MID Server Zugriff gewährt, und installieren Sie die CyberArk AIM-API auf dem MID Server-Computer.

Vorbereitungen

Erforderliche Rolle: Administrator

Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass das Plugin „Externer Anmeldeinformationsspeicher“ aktiviert ist. CyberArk Application Access Manager (AAM)-Anmeldeinformationsanbieter Version 12.0.1 und höher werden unterstützt.

Prozedur

1. Konfigurieren Sie den CyberArk-Tresor mit der Anwendungs-ID und den Authentifizierungsdetails, die alle MID Server, die Anmeldeinformationen anfordern, verwenden.
   Weitere Informationen finden Sie im Handbuch „CyberArk Credential Provider and ASCP Implementation“.

   a. Stellen Sie sicher, dass CyberArk so konfiguriert ist, dass der MID-Server auf den Tresor zugreifen kann, indem Sie eine App-ID in CyberArk namens erstellen `ServiceNow_MID_Server`.

   b. Stellen Sie sicher, dass jede Anmeldeinformation, die der MID Server benötigt, Zugriff auf die App-ID `ServiceNow_MID_Server` erhält.

   Hinweis: Sie können die Standard-App-ID **ServiceNow_MID_Server** in der MID-Server-Datei config.xml mit dem Parameter ext.cred.app_id überschreiben. Wenn Sie den Wert in diesem Parameter ändern, müssen Sie einen entsprechenden Wert im Tresor konfigurieren.

2. Installieren Sie den Credential Provider von CyberArk, einschließlich der AIM-API, auf jedem Computer, der einen für den Zugriff auf den Anmeldeinformationsspeicher verwendeten MID Server-Service hostet.
3. Stellen Sie CyberArk-Accounts bereit, und legen Sie Berechtigungen für den Anwendungszugriff fest.
   Weitere Informationen finden Sie im Handbuch „CyberArk Privileged Account Security Implementation“.

   a. Erstellen Sie in CyberArk-Passwortsafe die privilegierten Accounts, die von Discovery, Orchestration oder Service Mapping für den Zugriff auf verschiedene Geräte benötigt werden, und stellen Sie sicher, dass diese Accounts zu den Safes gehören, in denen die erforderlichen Anmeldeinformationen gespeichert sind.

   b. Fügen Sie den Credential Provider und die Anwendungsbenutzer als Mitglieder der Passwortsafes hinzu, in denen die Anwendungspasswörter gespeichert werden.

CyberArk-JAR-Datei importieren

Importieren Sie die CyberArk-Datei „JavaPasswordSDK.jar“ in die Instanz, damit der MID Server darauf zugreifen kann.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Bevor Sie mit diesem Verfahren beginnen, müssen Sie CyberArk so konfigurieren, dass der MID Server auf Anmeldeinformationen zugreifen kann. Stellen Sie sicher, dass die CyberArk AIM-API auf jedem Server installiert ist, auf dem sich ein MID Server befindet, der für den Zugriff auf den Tresor verwendet wird.

Hinweis: Zwei separate CyberArk-Integrationen werden vom MID-Server nicht unterstützt. Die gleiche Version der CyberArk AIM-API muss auf allen MID-Servern installiert sein, die mit derselben Instanz verbunden sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie diesen Prozess auch, wenn die Datei „JavaPasswordSDK.jar“ bereits auf dem MID-Server vorhanden ist.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **JAR-Dateien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus, indem Sie die Felder in der Tabelle verwenden.

Formularfelder für die JAR-Datei

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name zur Identifizierung der Datei in der Instanz.
Version	Optionale Versionsnummer für die Datei, sofern verfügbar.
Quelle	Provider der JAR-Datei. Quellinformationen werden vom System nicht verwendet.
Beschreibung	Optionale Kurzbeschreibung der JAR-Datei und ihres Zwecks in der Instanz.

4. Hängen Sie die JAR-Datei an diesen Datensatz an.
   Die AIM-Datei JavaPasswordSDK.jar wird mit den AIM-SDK-Installationsdateien geliefert und befindet sich normalerweise auf dem MID-Server im AIM-Installationsverzeichnis unter <Installationsverzeichnis>/CyberArk/ApplicationPasswordSdk.

   Hinweis: Das angehängte AIM JavaPasswordSDK.jar muss mit der installierten Version der CyberArk AIM-API übereinstimmen. Jede Nichtübereinstimmung in JavaPasswordSDK.jar-Dateien kann zu unvorhersehbarem Verhalten und potenziellen Funktionsproblemen führen.

5. Klicken Sie auf **Absenden**.
6. Starten Sie den MID-Server-Service neu.
   Die Plattform stellt die JAR-Datei jedem MID Server zur Verfügung, der für die Kommunikation mit der Instanz konfiguriert ist.

Konfigurieren Sie den MID-Server für CyberArk

Konfigurieren Sie die Datei config.xml, um dem MID Server Zugriff auf den CyberArk-Tresor zu gewähren.

Vorbereitungen

Erforderliche Rolle: Administrator

Bevor Sie dieses Verfahren beginnen, müssen Sie die Datei JavaPasswordSDK.jar in die Instanz importieren.

Prozedur

Konfigurieren Sie den MID-Server manuell Fügen Sie einen MID-Server-Parameter hinzu Datei mit diesen Parametern.

Diese Konfiguration kann nicht von der Instanz vorgenommen werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Konfigurationsparameter

Parameter	Wert	Beschreibung
ext.cred.safe_folder	NameOfFolder	Ordner für alle Suchen nach Anmeldeinformationen. Zum Beispiel: **root**.
ext.cred.use_cyberark	true	Boolescher Parameter, der angibt, dass dieser MID Server in CyberArk integriert ist.

Optionale Konfigurationsparameter

Parameter	Wert	Beschreibung
ext.cred.safe_timeout	5 (Sek.)	Zeitüberschreitung in Sekunden für jede Suche nach Anmeldeinformationen im Tresor.
ext.cred.safe_name	NameOfSafe	Standardname des Safes, der für alle Suchen nach Anmeldeinformationen verwendet wird. Wenn sich Parameter in mehreren Safes befinden, kann die Anmeldeinformations-ID im Format angegeben werden *<safeName>:<CredentialID>*. Bei dieser Konfiguration wird das Feld **NameOfSafe** ignoriert. Wenn für alle externen Anmeldeinformationen die Nachweis-IDs in diesem Format angegeben sind, lassen Sie das Feld **NameOfSafe** aus. **Hinweis:** Standardmäßig ist das Trennzeichen in diesem Format ein Doppelpunkt. Um ein beliebiges Zeichen als Trennzeichen zuzuweisen, fügen Sie diese Zeile der Datei CredMap.properties hinzu: safe.cred.split.string = <Zeichenfolge>.
ext.cred.app_id	ServiceNow_MID_Server	Gibt die App-ID an, mit der dem MID-Server die Berechtigung zum Zugriff auf den CyberArk-Tresor erteilt wird. Der Standardwert **ServiceNow_MID_Server** muss im CyberArk-Tresor definiert sein. Mit diesem Parameter können Sie den Standardwert überschreiben und eine eigene App-ID angeben. Wenn Sie die App-ID in diesem Parameter bearbeiten, müssen Sie CyberArk entsprechend konfigurieren.
ext.cred.type_specifier	wahr	Erzwingt, dass die IP-Adressen-Suche Anmeldeinformationen ausgibt, die sowohl mit der CyberArk-Plattform-ID als auch mit der IP-Adresse übereinstimmen. Wenn zum Beispiel eine IP-Adresse von Windows und Tomcat gemeinsam genutzt wird, geben Anmeldeinformationen mit einer Plattform-ID, die mit **Win** beginnt, nur die Windows-Anmeldeinformationen zurück. Wenn dieser Parameter auf „true“ festgelegt ist, sucht CyberArk nach Plattform-IDs, die mit Folgendem beginnen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert	Beschreibung
		• Win: Windows • Unix: SSH • VMWare: VMware
ext.cred.check_ssh_type	false	Ist der Wert auf „true“ festgelegt, müssen die von CyberArk zurückgegebenen SSH-Anmeldeinformationen mit dem angeforderten Anmeldeinformationstyp übereinstimmen. Wenn beispielsweise normale SSH-Anmeldeinformationen mit Benutzername/Passwort angefordert werden und nur SSH-Schlüssel verfügbar sind, schlägt die Suche nach Anmeldeinformationen fehl.

CyberArk für SNMPv2-Anmeldeinformationen konfigurieren

Wenn Ihr System SNMPv2 verwendet, können Sie eine spezielle Datei erstellen, um das Attribut in Anmeldeinformationen der Community-Zeichenfolge zuzuordnen.

Vorbereitungen

Erforderliche Rolle: Administrator

Bevor Sie dieses Verfahren beginnen, müssen Sie den MID Server für den Zugriff auf den CyberArk-Tresor konfigurieren.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Wenn die Community-Zeichenfolge im Passwortfeld der CyberArk-Anmeldeinformationen angezeigt wird, ist es nicht erforderlich, dieses Verfahren auszuführen.

SNMPv2 wird in CyberArk nicht nativ unterstützt. Wenn Ihre Organisation benutzerdefinierte SNMPv2-Anmeldeinformationen erstellt hat, bei denen die Community-Zeichenfolge nicht im Passwortfeld der Anmeldeinformationen angezeigt wird, verwenden Sie dieses Verfahren, um das Attribut in den Anmeldeinformationen der Community-Zeichenfolge zuzuordnen.

Prozedur

1. Erstellen Sie in einem Texteditor eine Datei mit dem Namen CredMap.properties mit diesem Code:
   `SNMPv2.Community=attribute_name`
2. Speichern Sie die Datei im Verzeichnis /agent Ihrer MID Server-Installation.
   Beim Suchen nach Anmeldeinformationen versucht der MID Server, dieses Attribut für die Anmeldeinformationen zu finden. Wenn das Attribut nicht gefunden wird, sucht der MID Server im Passwortfeld. Wenn das Passwortfeld leer ist, schlägt die Suche nach Anmeldeinformationen fehl.

Konfigurieren Sie den CyberArk-Anmeldeinformationsbezeichner

Erstellen Sie den eindeutigen Schlüssel, mit dem CyberArk bestimmte Anmeldeinformationen im externen Repository identifizieren kann.

Vorbereitungen

Erforderliche Rolle: Administrator

Bevor Sie mit diesem Verfahren beginnen, müssen Sie das Plugin „Externer Anmeldeinformationsspeicher“ aktivieren und die Systemeigenschaft com.snc.use_external_credentials auf „true“ setzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen** oder **Orchestration** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie aus der Liste der Anmeldeinformationstypen einen Typ aus, der den externen Speicher von CyberArk unterstützt.
4. Füllen Sie das Formular mit den Feldern des Anmeldeinformationstyps aus.
5. Aktivieren Sie das Kontrollkästchen **Externer Anmeldeinformationsspeicher**.
   Die Felder **Benutzername** und **Passwort** werden durch das Feld **Nachweis-ID** ersetzt.

   Hinweis: Wenn das Kontrollkästchen nicht sichtbar ist, klicken Sie auf das Menüsymbol in der Kopfzeile, und wählen Sie aus **Ansicht** > **Externer Speicher**an.

6. Geben Sie im Feld **Nachweis-ID** einen Ausdruck in einem der folgenden Formate ein:
   - Wenn sich alle Anmeldeinformationen im selben Safe befinden, konfigurieren Sie diesen Safe-Namen in der MID-Server-Datei config.xml mit dem Parameter ext.cred.safe_name, und geben Sie die Nachweis-ID nur mit dem Namen als **<Nachweis-ID>** an.
   - Um die Anmeldeinformationen für eine Plattform zu benennen, die sich in einem bestimmten Safe befinden, definieren Sie die Nachweis-ID als **<Safe>:<Nachweis-ID>:<Plattform-ID>**.
   - Wenn sich die Anmeldeinformationen in mehreren Safes befinden, geben Sie die Nachweis-ID in diesem Format an: **<Safe>:<Nachweis-ID>**.
   - Wenn CyberArk die Anmeldeinformationen anhand der IP-Adresse suchen soll, verwenden Sie einen alternativen Safe, und geben Sie die Nachweis-ID in diesem Format an: **<Safe>:**.
   - Wenn CyberArk die Anmeldeinformationen für eine alternative Plattform-ID im selben Safe suchen soll, verwenden Sie dieses Format: **::<Plattform-ID>**
   - Wenn CyberArk die Anmeldeinformationen in einem konfigurierten Safe anhand der IP-Adresse anstelle der Nachweis-ID suchen soll, lassen Sie dieses Feld leer. Dies ist die Best Practice für Installationen, bei denen jeder Server über eindeutige Anmeldeinformationen verfügt. Ohne diese Art von Suche müssen Sie in Ihrer Instanz für jeden Server in der Umgebung einen Nachweis-ID-Datensatz erstellen.

   Hinweis: Die Anmeldeinformations-ID muss mit dem Wert in übereinstimmen **Name** Feld für den CyberArk-Account. Die **Anmeldeinformations-ID** Das Feld darf maximal 180 Zeichen lang sein.

7. Wenn Sie SNMPv3-Anmeldeinformationen in CyberArk speichern und das Datenschutzprotokoll und den Datenschutzschlüssel verwenden, konfigurieren Sie die ID wie folgt:

   a. In **Anmeldeinformationsspeicher-Typ** Feld auswählen **CyberArk** .
   Die **ID der Datenschutz-Anmeldeinformationen** Feld wird angezeigt.

   b. Geben Sie ein **Name** Des CyberArk SNMPv3-Datenschutzkontos in **ID der Datenschutz-Anmeldeinformationen** Feld.

8. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Anmeldeinformationen in einem CyberArk-Tresor konfigurieren

Konfigurieren Sie Ihren CyberArk-Tresor mit den AWS-Anmeldeinformationen, die für die Verwendung durch Ihre Instanz abgerufen werden sollen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Speichern Sie die Anmeldeinformationen als Account im CyberArk-Tresor. Wenn Sie den Zugriff auf den Tresor in Ihrer Instanz konfigurieren, muss der Name, den Sie dem Account geben, auch als Anmeldeinformations-ID verwendet werden.

Hinweis: Das folgende Verfahren verweist auf CyberArk Password Vault v14.2.1. Wenn Sie eine andere Version verwenden, richten Sie die Konfiguration gemäß der offiziellen CyberArk Password Vault-Dokumentation ein.

Prozedur

1. Wechseln Sie in CyberArk zu **Accounts** > **Accounts Und Anforderungen** > **Account-Ansicht** > **Account hinzufügen**an.
2. Systemtyp auswählen: **Cloud-Service** .
3. Der Plattform zuweisen: **Amazon Web Services – AWS – Zugriffsschlüssel** .
4. In Safe speichern: Wählen Sie einen Safe aus der Liste aus.
5. Eigenschaften definieren: Geben Sie die folgenden Informationen ein:

CyberArk-Anmeldeinformationen

Feld	Wert
AWS IAM-Anwendername	Geben Sie den AWS-Zugriffsschlüssel, wie von AWS bereitgestellt, ein.
Geheimer AWS-Zugriffsschlüssel (optional)	Geben Sie den geheimen AWS-Zugangsschlüssel, wie von AWS bereitgestellt, ein.
Passen Sie den Account-Namen an	Schalten Sie den Schieberegler ein/aus, um einen anwenderdefinierten Namen für diesen Schlüssel einzugeben.
AWS Zugangsschlüssel-ID	Geben Sie den AWS-Zugriffsschlüssel erneut ein, wie von AWS bereitgestellt.
AWS-Account-ID-Nummer	Geben Sie den AWS-Zugriffsschlüssel erneut ein, wie von AWS bereitgestellt.
AWS-Account-Aliasname (optional)	Geben Sie einen Aliasnamen für den Account ein.

6. Wählen Sie Aus **Hinzufügen** .

Nächste Maßnahme
Wenn Sie dies noch nicht getan haben, erstellen Sie in Ihrer Instanz einen Nachweis-Identifier, um den Zugriff auf den CyberArk-Tresor zu konfigurieren. Weitere Einzelheiten finden Sie unter Zugriff auf den externen Anmeldeinformationsspeicher für AWS konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie AWS-Anmeldeinformationen in einem CyberArk Vault mithilfe der klassischen UI

Konfigurieren Sie Ihren CyberArk-Tresor mit den AWS-Anmeldeinformationen, die für die Verwendung durch Ihre Instanz abgerufen werden sollen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
CyberArk Password Vault v14.2.1 enthält Konfigurationsoptionen für die Accounts-Ansicht und die Accounts-Ansicht (klassische UI), um die Anmeldeinformationen als Account zu speichern. Wenn Sie den Zugriff auf den Tresor in Ihrer Instanz konfigurieren, muss der Name, den Sie dem Account geben, auch als Anmeldeinformations-ID verwendet werden.

Hinweis: Das folgende Verfahren verweist auf CyberArk Password Vault v14.2.1. Wenn Sie eine andere Version verwenden, richten Sie die Konfiguration gemäß der offiziellen CyberArk Password Vault-Dokumentation ein.

Prozedur

1. Wechseln Sie in CyberArk zu **Accounts** > **Accounts Und Anforderungen** > **Accounts-Ansicht (klassische UI)** > **Account hinzufügen**an.
2. Geben Sie die folgenden Informationen ein:

CyberArk-Anmeldeinformationen

Feld	Wert
Gerätetyp	Wählen Sie **Cloud Service** aus.
Plattformname	Wählen Sie **Amazon Web Services - AWS - Access Keys** aus.
AWS IAM-Anwendername	Geben Sie den AWS-Zugriffsschlüssel, wie von AWS bereitgestellt, ein.
AWS Zugangsschlüssel-ID	Geben Sie den AWS-Zugriffsschlüssel erneut ein, wie von AWS bereitgestellt.
AWS-Account-ID-Nummer	Geben Sie den AWS-Zugriffsschlüssel erneut ein, wie von AWS bereitgestellt.
Geheimer AWS-Zugriffsschlüssel	Geben Sie den geheimen AWS-Zugangsschlüssel, wie von AWS bereitgestellt, ein.
Name	Geben Sie einen anwenderdefinierten Namen für diesen Schlüssel ein.

3. Klicken Sie auf **Save**.

Nächste Maßnahme
Wenn Sie dies noch nicht getan haben, erstellen Sie in Ihrer Instanz einen Nachweis-Identifier, um den Zugriff auf den CyberArk-Tresor zu konfigurieren. Weitere Einzelheiten finden Sie unter Zugriff auf den externen Anmeldeinformationsspeicher für AWS konfigurieren.

Konfigurieren Sie Azure-Anmeldeinformationen in einem CyberArk-Tresor

Konfigurieren Sie Ihren CyberArk-Tresor mit den Azure-Anmeldeinformationen, die zur Verwendung durch Ihre Instanz abgerufen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Um Azure-Anmeldeinformationen zu speichern, erstellen Sie zuerst eine Azure-Anmeldeinformationsvorlage im CyberArk-Tresor. Dieser Prozess muss für den Tresor nur einmal abgeschlossen werden.

Prozedur

1. Melden Sie sich im Administrationsmodus bei CyberArk an.
2. Navigieren Sie zu **Verwaltung** Registerkarte.
3. In **Systemkonfiguration** , Bearbeiten **Plattformverwaltung** .
4. Navigieren Sie zu **Cloud-Provider-Vorlage** Und duplizieren.
5. Bearbeiten Sie die Vorlage für Azure-Anmeldeinformationen.
6. Fügen Sie die folgenden zwei Eigenschaften hinzu:
   - *Name*Als *Username*Und *Display Name*Als *Client ID*
   - *Name*Als *Address*Und *DisplayName*Als *Tenant ID*
7. Wenden Sie die Änderungen an.
8. Navigieren Sie zu **Account** Abschnitt und wählen Sie aus **Account hinzufügen** .
9. Wählen Sie Aus **Sicher** .
10. Legen Sie fest **Gerätetyp** Bis **Cloud-Service** .
11. Wählen Sie die Azure-Vorlage aus, die zuvor bearbeitet wurde.
12. Geben Sie die Informationen in für ein **Client-ID** , **Mandanten-ID** , Und **Passwort** Felder.
13. Wählen Sie **Speichern**.

OAuth 2,0-Authentifizierung über MID-Server Externer Anmeldeinformationsspeicher wird verwendet

Speichern Sie OAuth 2,0-Anmeldeinformationen – Client-ID und Client-Geheimnis – im CyberArk Tresor anstelle von ServiceNow Instanz. Die MID-Server Ruft die Anmeldeinformationen von ab CyberArk Tresor, falls erforderlich, um das OAuth-Token abzurufen. Das Token wird auf dem MID-Server gespeichert und nach Ablauf automatisch aktualisiert.

Die CyberArk Das Produkt „Application Identity Management“ (AIM) verwendet die Sicherheitslösung für Privileged Account, um die Speicherung von Anwendungspasswörtern, die in Anwendungen, Skripts oder Konfigurationsdateien eingebettet sind, zu überflüssig zu machen, und ermöglicht die zentrale Speicherung, Protokollierung und Verwaltung dieser hochsensiblen Passwörter innerhalb von CyberArk Tresor. Sie können konfigurieren CyberArk Tresor zum Speichern von OAuth 2,0-Anmeldeinformationen anstatt direkt in einem ServiceNow Datensatz mit Anmeldeinformationen. Weitere Informationen zu CyberArk finden Sie unter CyberArk Integration des Anmeldeinformationsspeichers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Architektur der OAuth 2,0-Authentifizierung von MID-Server Anforderung

Die Architektur besteht aus zwei Teilen: ServiceNow Instanz und die Umgebung, in der der Application Identity Manager (AIM)-Client und der MID-Server konfiguriert sind. Beispiele für Umgebungen sind die Cloud- oder eine Kundenumgebung.

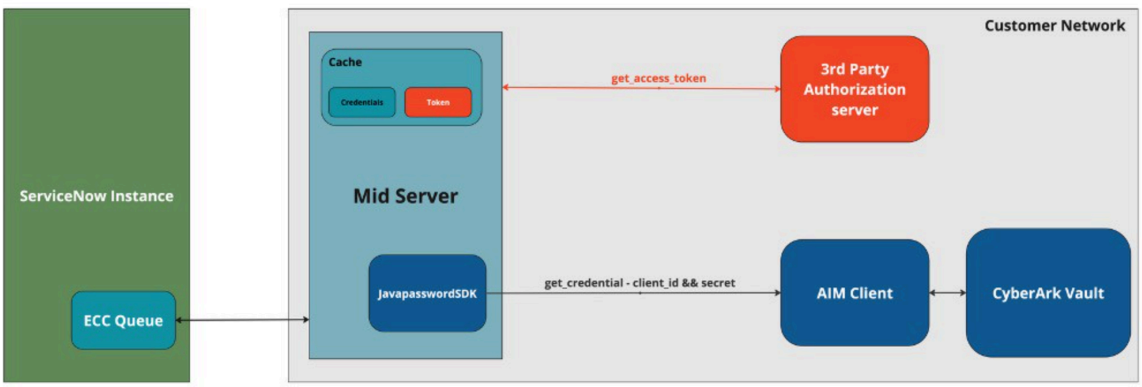
Die MID-Server Und Application Identity Manager (AIM) Client Muss in derselben Umgebung konfiguriert werden, und der Application Identity Manager (AIM) muss für die Interaktion mit konfiguriert sein CyberArk Externer Tresor. Die CyberArk Der externe Tresor kann in derselben Umgebung wie der MID-Server und des Application Identity Manager (AIM) oder einer anderen Umgebung gehostet werden.

Die ServiceNow Die Instanz verwaltet Anmeldeinformationsbezeichner, die bestimmten OAuth 2,0-Anmeldeinformationen zugeordnet sind, die in gespeichert sind CyberArk Tresor. Vor dem Senden einer OAuth-Tokenanforderung ruft der MID-Server den Anmeldeinformationsbezeichner von der Instanz ab und verwendet dann eine vom Kunden bereitgestellte JAR-Datei, um den Bezeichner an den AIM-Client zu senden. Der AIM-Client sendet die Anforderung an CyberArk Tresor. Die CyberArk Vault sendet OAuth 2,0 Anmeldeinformationen Zurück zum MID-Server über den AIM-Client. Nach Erhalt von OAuth 2,0 Anmeldeinformationen , Der MID-Server sendet die OAuth-Tokenanforderung an den Autorisierungsserver eines Drittpartei. Die Tokenanforderung enthält Informationen wie Client- und Client-Geheimnisinformationen, die CyberArk Speichert, und den OAuth-Bereich und die Token-URL, die die Instanz speichert. Nachdem der Autorisierungsserver das OAuth-Token ausgegeben hat, speichert der MID-Server es in seinem Cache-Speicher.

Hinweis: Diese Funktion unterstützt den Gewährungstyp „Client-Anmeldeinformationen“.

Die Abbildung zeigt den Authentifizierungsprozess der MID-Server-Anforderung.

Hinweis: Es wird davon ausgegangen, dass der Drittpartei-Autorisierungsserver und die CyberArk Tresore werden im Kundennetzwerk gehostet.



Konfigurieren Sie eine JAR-Datei und Anmeldeinformationsbezeichner

Konfigurieren Sie eine JAR-Datei und Anmeldeinformationsbezeichner so, dass die JAR-Datei die Anmeldeinformationsbezeichner in tatsächliche Anmeldeinformationen von auflöst CyberArk Externer Tresor. Mit diesem Prozess kann der MID-Server OAuth 2,0-Anmeldeinformationen abrufen und in die OAuth-Tokenanforderung aufnehmen.

Vorbereitungen
Erforderliche Rolle: agent_admin oder admin

Die CyberArk Im externen Tresor werden vertrauliche Anmeldeinformationen und gespeichert ServiceNow Die Instanz speichert Anmeldeinformationsbezeichner, die den spezifischen Anmeldeinformationsnamen zugeordnet sind, die der Tresor speichert. Die JAR-Datei

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ermöglicht die Zuordnung eines Anmeldeinformationsbezeichners zu einem bestimmten Anmeldeinformationsnamen im externen Tresor. Die Zuordnung aktiviert den MID-Server Dient zum Abrufen und Einbeziehen der erforderlichen Anmeldeinformationen in die OAuth-Tokenanforderung. Sie müssen die Anmeldeinformationsbezeichner und die JAR-Datei in der ServiceNow-Instanz bzw. auf dem MID-Server konfigurieren.

Prozedur

1. CyberArk-JAR-Datei importieren.
2. Konfigurieren Sie eine Verbindung, um OAuth-Anforderung über zu senden MID-Server Externer Tresor wird verwendet.

Konfigurieren Sie CyberArk

Konfigurieren Sie CyberArk Tresor zum Speichern von OAuth 2,0-Anmeldeinformationen und zum Beantworten von Anforderungen für OAuth 2,0-Anmeldeinformationen von MID-Server.

Vorbereitungen

Bestätigen Sie, dass Sie das ServiceNow IntegrationHub Standard Pack-Installationsprogramm abonniert haben. Weitere Informationen finden Sie unter https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Erforderliche Rolle: agent_admin oder admin

Prozedur

1. CyberArk-Tresor konfigurieren und die AIM-API installieren.
2. CyberArk-JAR-Datei importieren.
3. Konfigurieren Sie OAuth 2,0-Anmeldeinformationen in CyberArk.
4. Konfigurieren Sie eine Verbindung, um OAuth-Anforderung über zu senden MID-Server Externer Tresor wird verwendet.

Konfigurieren Sie OAuth 2,0-Anmeldeinformationen in CyberArk

Konfigurieren Sie Ihren CyberArk-Tresor mit OAuth 2,0-Anmeldeinformationen, die dem entsprechen ServiceNow Instanzanforderungen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Um OAuth 2,0-Anmeldeinformationen zu speichern, erstellen Sie zuerst eine OAuth 2,0-Anmeldeinformationsvorlage im CyberArk-Tresor. Dieser Prozess darf für den Tresor nur einmal abgeschlossen werden.

Prozedur

1. Führen Sie die folgenden Schritte aus, wenn Sie die OAuth 2,0-Anmeldeinformationen zum ersten Mal konfigurieren.

   a. Melden Sie sich im Administrationsmodus bei CyberArk an.

   b. Navigieren Sie zu **Verwaltung** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie Aus **Plattformverwaltung** .
Auf der Seite „Plattformverwaltung“ werden die Plattformen auf der Registerkarte „Ziele“ angezeigt.

d. Erweitern Sie einen Plattformtyp.

e. Wählen Sie das Einstellungssymbol ( ), die einer Plattformvorlage entspricht, und wählen Sie aus **Duplikat** .

f. Geben Sie im Fenster „Plattform duplizieren“ einen Namen für die Vorlage ein, und wählen Sie aus **Erstellen** .

Hinweis: Beachten Sie den Systemtyp, unter dem Sie eine doppelte Vorlage erstellt haben. Beispielsweise ist Cloud-Service ein Systemtyp.

g. Wählen Sie das Einstellungssymbol ( ), die der doppelten Plattformvorlage entspricht, die Sie erstellt und ausgewählt haben **Bearbeiten** .

h. Fügen Sie die Eigenschaft hinzu.
Name als Anwendername und Anzeigename als Client-ID.

i. Benennen Sie die anderen Eigenschaften um.

Tipp: Wählen Sie Eigenschaftsnamen aus, die für OAuth 2,0 relevant sind.

j. Wählen Sie **Übernehmen**.
Die Updates werden angewendet.

k. Wählen Sie **OK**.

l. Navigieren Sie im linken Bereich zu Accounts.

m. Wählen Sie Aus **Account Hinzufügen** .

n. Wählen Sie unter der Überschrift Systemtyp den Systemtyp aus, unter dem Sie die Plattformvorlage erstellt haben.
Der Systemtyp zeigt die Plattformvorlagen an.

o. Wählen Sie unter der Überschrift „Plattform auswählen“ die von Ihnen erstellte Plattformvorlage aus.

p. Wählen Sie Safe.
Speichern Sie den Safe-Wert zur späteren Verwendung.

q. Füllen Sie die Informationen in für die Client-ID, das Passwort (Clientgeheimnis als Wert angeben) und andere Felder nach Bedarf aus.

r. Wählen Sie **Hinzufügen**.
Der Account wird hinzugefügt.

s. Öffnen Sie auf der Seite „Account-Ansicht“ einen Account.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

t. Wählen Sie die Registerkarte **Details** aus.

u. Kopieren Sie den Wert, der im Abschnitt „Account-Name“ gespeichert ist, und speichern Sie ihn zur späteren Verwendung.
Der von Ihnen kopierte und gespeicherte Wert wird als Anmeldeinformationsbezeichner in der ServiceNow-Instanz verwendet.

2. Führen Sie die folgenden Schritte aus, wenn Sie die OAuth 2,0-Anmeldeinformationen nicht zum ersten Mal konfigurieren.

a. Melden Sie sich im Administrationsmodus bei CyberArk an.

b. Navigieren Sie zu **Account** Abschnitt und wählen Sie aus **Account hinzufügen** .

c. Wählen Sie den Systemtyp aus aus **Systemtyp** Unter der die Vorlage zum Speichern von OAuth 2,0 vorhanden ist.

d. Wählen Sie die erforderliche Plattformvorlage aus, die Sie erstellt haben, und wählen Sie sie aus **Sicher** . Speichern Sie den Safe-Wert zur späteren Verwendung.

e. Füllen Sie die Informationen in für die Client-ID, das Passwort (Clientgeheimnis als Wert angeben) und andere Felder nach Bedarf aus.

f. Wählen Sie **Hinzufügen**.
Der Account wird hinzugefügt.

g. Öffnen Sie auf der Seite „Account-Ansicht“ einen Account.

h. Wählen Sie die Registerkarte **Details** aus.

i. Kopieren Sie den Wert, der im Abschnitt „Account-Name“ gespeichert ist, und speichern Sie ihn zur späteren Verwendung.
Der von Ihnen kopierte und gespeicherte Wert wird als Anmeldeinformationsbezeichner in verwendet ServiceNow Instanz.

Konfigurieren Sie eine Verbindung, um OAuth-Anforderung über zu senden MID-Server Externer Tresor wird verwendet

Konfigurieren Sie eine Verbindung, um Anforderungen für OAuth 2,0-Token über an einen Authentifizierungsserver eines Drittanbieters zu senden MID-Server. Die MID-Server Fügt OAuth 2,0-Anmeldeinformationen (Client-ID und Client-Geheimnis) aus dem hinzu CyberArk Externer Tresor, OAuth-Bereich und Token-URL von der Instanz an die Anforderung und sendet sie an den Authentifizierungsserver der Drittpartei.

Vorbereitungen

Überprüfen Sie die folgenden Elemente.

- Bestätigen Sie, dass Sie das ServiceNow IntegrationHub Standard Pack-Installationsprogramm abonniert haben. Weitere Informationen finden Sie unter https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie haben eine JAR-Datei erstellt, mit der der MID-Server Anmeldeinformationen mit auflösen kann CyberArk Externer Tresor. Weitere Informationen finden Sie unter JAR-Datei zum Auflösen der Anmeldeinformationen erstellen.
- Sie haben die JAR-Datei auf den MID-Server importiert.
- Der MID-Server ist für CyberArk eingerichtet. Weitere Informationen finden Sie unter Konfigurieren Sie den MID-Server für CyberArk.
- OAuth 2,0 werden im externen CyberArk-Speicher konfiguriert. Weitere Informationen finden Sie unter Konfigurieren Sie OAuth 2,0-Anmeldeinformationen in CyberArk.

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Verbindung und die Anmeldeinformationen mit einer Konfigurationsvorlage oder manuell konfigurieren. Eine Konfigurationsvorlage definiert die Komponenten des Verbindungsdatensatz-Formulars und kann für andere Verbindungsdatensätze wiederverwendet werden. Manuell können Sie die Verbindung nur für diesen Zweck konfigurieren. Das Thema zeigt beide Ansätze.

Prozedur

1. Konfigurieren Sie die Verbindung mit einer Konfigurationsvorlage.

   a. Navigieren zu **Alle** > **IntegrationHub** > **Konfigurationsvorlagen**an.

   b. Wählen Sie **Neu**.

   c. Wählen Sie Aus **HTTP-Verbindung mit Gewährungstyp „OAuth-Client-Anmeldeinformationen“ (externer Speicher)** .

   d. Aktualisieren Sie das Formular nach Bedarf.
   Sie können beispielsweise den Bereich in angeben `oauth_Entity_Profile_scope` Und `oauth_Entity_scope` Felder im Abschnitt Standarddatenvorlage. Informationen zum Erstellen einer Konfigurationsvorlage finden Sie unter Erstellen Sie eine Konfigurationsvorlage.

   e. Wählen Sie **Absenden**.
   Sie haben die Konfigurationsvorlage erstellt.

   f. Navigieren zu **Alle** > **IntegrationHub** > **Aliasse für Verbindungen und Anmeldeinformationen**an.

   g. Aktualisieren Sie das Formular.

Alias für Verbindungen und Anmeldeinformationen

Feld	Beschreibung
Name	Name des Alias. Ein Alias darf nur Buchstaben, Zahlen und Unterstriche enthalten. Während eines Upgrades wird das Tag im Anmeldedatensatz zu einem Verbindungs- und Anmeldealias migriert. Wenn das Anmeldeinformations-Tag andere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sonderzeichen als Buchstaben, Zahlen und Unterstriche enthält, wird der Tag-Name nach dem Upgrade beibehalten. Sie können diesen migrierten Alias weiterhin verwenden, Sie können ihn allerdings erst aktualisieren, wenn Sie den Namen den Namensbeschränkungen entsprechend ändern.
Anwendung	Eindeutiger Bezeichner für den Alias für Verbindungen und Anmeldeinformationen, basierend auf dem Format `Scope_Name.alias_Name` . ▪ Wenn der Bereich global ist, ist die ID der Aliasname. Wenn Sie beispielsweise einen Workday-Alias im globalen Bereich erstellen, wird die ID auf festgelegt `workday` . ▪ Wenn Sie einen Workday-Alias im Bereich der HR-App erstellen, wird die ID auf festgelegt `X_HR_App.Workday` .
Übergeordneter Alias	Option zum Auswählen des Alias, unter dem Sie diesen Alias für Verbindungen und Anmeldeinformationen erstellen. Der Alias für Verbindungen und Anmeldeinformationen, den Sie erstellen, ist ein untergeordneter Alias. Ein untergeordneter Alias ist unter aufgeführt **Untergeordnete Aliasse** Registerkarte auf der übergeordneten Aliasseite für Verbindungen und Anmeldeinformationen. 
Typ	Option, um den Typ des Alias anzugeben, den Sie erstellen. Wählen Sie eine der folgenden Optionen aus: ▪ Anmeldeinformationen: Alias, der einen Anmeldeinformationsdatensatz enthält. ▪ Verbindung und Anmeldeinformationen: Alias, der sowohl den Verbindungs- als auch den Anmeldeinformationsdatensatz enthält. Diese Option ist standardmäßig ausgewählt. Bestätigen Sie, dass Verbindung und Anmeldeinformationen ausgewählt sind.
Unterstützt mehrere aktive Verbindungen	Bezeichner, der angibt, ob der Alias mehrere aktive Verbindungen unterstützt. Fügen Sie mithilfe der Tabelle „Verbindungen“ Verbindungen hinzu, und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	verknüpfen Sie sie mithilfe der zugehörigen Liste „Verbindungen“ mit dem Alias.
Standard-Wiederholungsrichtlinie	Wiederholungsrichtlinie für den Alias. Weitere Informationen finden Sie unter Wiederholungsrichtlinie .
Konfigurationsvorlage	Option zum Auswählen der Konfigurationsvorlage, auf der Sie den Alias für Verbindungen und Anmeldeinformationen erstellen. Wählen Sie die Vorlage des Typs aus **HTTP-Verbindung mit Gewährungstyp „OAuth-Client-Anmeldeinformationen“ (externer Speicher)** Die Sie erstellt haben.

h. Wählen Sie **Absenden**.
Sie haben den Alias-Datensatz für Verbindungen und Anmeldeinformationen erstellt.

i. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungs-Dashboard**an.

j. Geben Sie im Feld alle Verbindungen durchsuchen den Namen des von Ihnen erstellten Alias für Verbindungen und Anmeldeinformationen ein.

k. Wählen Sie im Datensatz des Alias für Verbindungen und Anmeldeinformationen die Option aus **Details Anzeigen** .

l. Wählen Sie **Konfigurieren**.

m. Füllen Sie das Formular aus.

Formular „Verbindung konfigurieren“

Feld	Beschreibung
Verbindungsname	Name der Verbindung Sie können den Namen nicht aktualisieren.
Verbindungs-URL	URL zum Drittparteiserver.
MID verwenden	Option zum Aktivieren DES MID-Servers. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
MID-Auswahl	Option zum Festlegen DER MID-Konfiguration für die Verbindung. ▪ **Bestimmter MID-Server** : Option, um eine manuelle Auswahl eines bestimmten MID-Servers anzugeben. ▪ **MID-Server automatisch auswählen** : Option, um anzugeben, dass der MID-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Server automatisch ausgewählt werden soll. ▪ **Spezifischer MID-Cluster** : Option, um eine manuelle Auswahl eines MID-Clusters von MID-Servern anzugeben. **Wichtig:** Bestätigen Sie, dass sich der von Ihnen ausgewählte MID-Server auf demselben Computer wie der CyberArk AIM-Client befindet, der für den Zugriff auf den CyberArk-Tresor konfiguriert ist. Weitere Informationen finden Sie unter CyberArk-Tresor konfigurieren und die AIM-API installieren.
MID-Server	Option zum manuellen Angeben eines MID-Servers. Diese Option wird angezeigt, wenn Sie auswählen **Bestimmter MID-Server** In **MID-Auswahl** Feld.
MID-Cluster	Option zum manuellen Angeben eines MID-Clusters. Diese Option wird angezeigt, wenn Sie auswählen **Spezifischer MID-Cluster** In **MID-Auswahl** Feld.
Externer Anmeldeinformationsspeicher	Option zur Verwendung des externen Anmeldeinformationsspeichers von CyberArk. Wenn Sie die Option auswählen, ruft der MID-Server die OAuth 2,0-Anmeldeinformationen (Client-ID und Client-Geheimnis) aus dem externen Anmeldeinformationsspeicher ab. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
Anmeldeinformations-ID	Bezeichner für den CyberArk-Account, der die Details der Client-ID und des geheimen Clientgeheimnisses enthält. Informationen zum Anzeigen des Verfahrens zum Abrufen des Anmeldeinformationsbezeichners finden Sie unter Konfigurieren Sie OAuth 2,0-Anmeldeinformationen in CyberArk. Geben Sie im Feld Anmeldeinformations-ID einen Ausdruck in einem dieser Formate ein. ▪ Wenn sich alle Anmeldeinformationen im selben Safe befinden, konfigurieren Sie diesen Safe-Namen in der MID-Server-Datei config.xml mit dem Parameter ext.cred.safe_name, und geben Sie die Nachweis-ID nur mit dem Namen als **<Nachweis-ID>** an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Um die Anmeldeinformationen für eine Plattform zu benennen, die sich in einem bestimmten Safe befinden, definieren Sie die Nachweis-ID als **<Safe>:<Nachweis-ID>:<Plattform-ID>**. ▪ Wenn sich die Anmeldeinformationen in mehreren Safes befinden, geben Sie die Nachweis-ID in diesem Format an: **<Safe>:<Nachweis-ID>**.
OAuth-Token-URL	URL, die den Endpunkt angibt, um das Zugriffstoken vom OAuth-Server abzurufen.

n. Wählen Sie Aus **Konfigurieren Sie Die Verbindung** .

2. Konfigurieren Sie eine Verbindung manuell.

a. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.

b. Wählen Sie **Neu**.

c. Wählen Sie Aus **Stellen Sie über einen externen Tresor eine Verbindung mit einem OAuth-Drittanbieter her** .

d. Füllen Sie das Formular aus.

Neue Anwendungsregistrierungsdetails

Feld	Beschreibung
Name	Name zur Identifizierung des Anwendungsregistrierungsdatensatzes. Geben Sie beispielsweise Folgendes ein: OAuth 2,0-Token-Anforderung über MID-App.
Anwendung	Option zum Angeben der Namen von Anwendungen, die auf diese Anwendungsregistrierung zugreifen können. Das Feld ist schreibgeschützt.
Standardgewährungstyp	Standardmethode zum Abrufen des Zugriffs-Tokens durch die Client-Anwendung vom OAuth-Server. Der standardmäßige und schreibgeschützte Gewährungstyp ist Client-Anmeldeinformationen.
Zugänglich von	Option zum Festlegen, welche Anwendungen auf diese Anwendungsregistrierung zugreifen können.
Token-URL	URL, die den Endpunkt angibt, um das Zugriffstoken vom OAuth-Server abzurufen.
Anmeldeinformationen senden	Option zum Festlegen der Methode zum Senden von OAuth 2,0 im Anforderungstext.
Kommentare	Geben Sie zugehörige Kommentare ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Unter **OAuth-Bereich** Spalte erstellen Sie einen oder mehrere OAuth-Bereiche, indem Sie die folgenden Schritte ausführen.

   i. Doppelklicken Sie unter der Spalte Name auf das Feld, und geben Sie einen Namen für den OAuth-Bereich ein.

   ii. Doppelklicken Sie in der Spalte OAuth-Bereich auf das Feld, und geben Sie den Umfang ein.

f. Wählen Sie **Absenden**.
Sie haben ein OAuth-Entitätsprofil und die Anwendungsregistrierung erstellt.

g. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

h. Wählen Sie **Neu**.

i. Wählen Sie **OAuth 2.0-Anmeldeinformationen** aus.

j. Wählen Sie Aus **Ansicht „Externer Speicher“** .

> **Wichtig:** Wählen Sie Aus **Ansicht „Externer Speicher“** Nur, wenn sich die Ansicht von der eines externen Speicherformulars für OAuth 2,0-Anmeldeinformationen unterscheidet.

k. Füllen Sie das Formular aus.

OAuth 2.0-Anmeldeinformationen

Feld	Beschreibung
Name	Name des Anmeldeinformationsdatensatzes.
Betrifft	Option zum Festlegen, ob der Anmeldeinformationsdatensatz für alle MID-Server oder einen bestimmten MID-Server gilt. Falls spezifisch, fügen Sie die MID-Server hinzu. Wählen Sie eine der folgenden Optionen aus. ▪ Alle MID-Server: Der MID-Server wird automatisch aus einer Sammlung von MID-Servern ausgewählt. ▪ Spezifische MID-Server: Option zum Angeben eines oder mehrerer MID-Server.
MID-Server	Option zum Angeben eines oder mehrerer MID-Server. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie auswählen **Bestimmte MID-Server** Im Feld gilt für.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option, um anzugeben, ob der Anmeldeinformationsdatensatz zur Verwendung verfügbar ist. Standardmäßig ist sie verfügbar.
OAuth-Einheitenprofil	Option zum Angeben eines OAuth-Entitätsprofils, das die Anmeldeinformationen verwenden. Wählen Sie das OAuth-Entitätsprofil aus, das Sie oben erstellt haben. Siehe Konfigurieren Sie ein OAuth-Entitätsprofil .
Externer Anmeldeinformationsspeicher	Option zum Festlegen, dass die Anmeldeinformationen in einem externen Speicher und nicht in der ServiceNow-Instanz gespeichert werden. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
Anmeldeinformations-ID	Option zum Angeben des Anmeldeinformationsbezeichners für das CyberArk-Konto, der die Client-ID und das geheime Clientgeheimnis enthält. Informationen zum Anzeigen des Verfahrens zum Abrufen des Anmeldeinformationsbezeichners finden Sie unter Konfigurieren Sie OAuth 2,0-Anmeldeinformationen in CyberArk.
Anmeldeinformationsspeicherung – Tresor	Option zum Angeben des Namens des Tresors des externen Anmeldeinformationsspeichers. Überprüfen Sie, ob Sie ausgewählt haben CyberArk.

l. Wählen Sie **Absenden**.
Sie haben den Anmeldeinformationsdatensatz erstellt.

m. Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen.
Informationen zu den Schritten finden Sie unter Verbindungs- und Anmeldealias erstellen.

n. Navigieren zu **Alle** > **IntegrationHub** > **Verbindungen**an.

o. Wählen Sie **Neu**.

p. Wählen Sie Aus **HTTP(s)-Verbindung** .

q. Füllen Sie das Formular aus.

Verbindungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieser HTTP(s)-Verbindung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option zum Festlegen der Verbindung, die Sie erstellen, aktiv. Die Option ist standardmäßig ausgewählt.
Anmeldeinformation	Wählen Sie den Datensatz mit Anmeldeinformationen aus, der zur Autorisierung der Verbindung verwendet wird. Wählen Sie die Anmeldeinformationen aus, die Sie oben erstellt haben.
Verbindungsalias	Wählen Sie den Alias-Datensatz aus, der dieser Verbindung zugeordnet werden soll. Mit einem Alias können Sie den Verbindungsdatensatz aktualisieren, ohne Aktionen oder Aktivitäten, die den Alias verwenden, neu zu konfigurieren.
URL-Builder	Geben Sie entweder die Verbindungs-URL manuell ein, oder verwenden Sie das System, um die URL basierend auf den Eingaben zu erstellen. Standardmäßig ist dieses Kontrollkästchen deaktiviert. Wenn diese Option aktiviert ist, wird die Verbindungs-URL aus den folgenden Feldern berechnet: ▪ Gegenseitige Authentifizierung – Aktivieren Sie das Kontrollkästchen, wenn die gegenseitige Authentifizierung verwendet wird. ▪ Protokoll – Wenn keine gegenseitige Authentifizierung verwendet wird, geben Sie das Protokoll ein. Der Standardwert ist HTTPs. ▪ Protokollprofil – Wenn die gegenseitige Authentifizierung verwendet wird, geben Sie das Protokollprofil aus „sys_protocol_profile“ ein. ▪ Host ▪ Port ▪ Basispfad – Pfad der Verbindungszeichenfolge. **Hinweis:** Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
Verbindungs-URL	Wenn der URL-Builder deaktiviert ist, geben Sie die Verbindungs-URL in dieses Feld ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn „Gegenseitige Authentifizierung“ aktiviert ist, wird die Verbindungs-URL erstellt: Protokoll + :// + Host:Port +URL. Wenn „Gegenseitige Authentifizierung“ nicht aktiviert ist, wird die Verbindungs-URL erstellt: Protokollprofil + :// + Host:Port +URL
MID-Server verwenden	Option, um anzugeben, dass Sie OAuth-Tokenanforderungen über einen MID-Server senden möchten. **Wichtig:** Bestätigen Sie, dass die Option ausgewählt ist.
Verbindungszeitüberschreitung	Anzahl der Millisekunden, die das System auf eine erfolgreiche Hostverbindung wartet. Wenn während dieser Zeit keine erfolgreiche Verbindung hergestellt wird, läuft die Verbindungsanforderung ab. Lassen Sie dieses Feld leer, um den Standard-Zeitüberschreitungswert für Verbindungen zu verwenden.
MID-Auswahl	Option zum Angeben einer der folgenden Optionen. ▪ MID-Server automatisch auswählen: Wählt MID-Server basierend auf MID-Server-Kriterien aus, unabhängig davon, ob sie Mitglieder eines Clusters sind. ▪ Spezifischer MID-Server: Wählen Sie manuell einen MID-Server aus. ▪ Spezifischer MID-Cluster: Die automatische Neuzuweisung an einen anderen MID-Server wählt nur Mitglieder des angegebenen Clusters aus. **Wichtig:** Bestätigen Sie, dass sich der von Ihnen ausgewählte MID-Server auf demselben Computer wie der CyberArk AIM-Client befindet, der für den Zugriff auf den CyberArk-Tresor konfiguriert ist. Weitere Informationen finden Sie unter CyberArk-Tresor konfigurieren und die AIM-API installieren.
Fähigkeiten	Option zum Auswählen einer oder mehrerer MID-Server-Fähigkeiten. Fähigkeiten definieren die spezifischen Funktionen eines MID-Servers innerhalb eines IP-Adressbereichs, sodass eine Anwendung den am besten geeigneten MID-Server auswählen kann. Wählen Sie das Symbol

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	für MID-Fähigkeiten ( ), um eine oder mehrere Fähigkeiten auszuwählen. **Hinweis:** ▪ Bestätigen Sie, dass sich der von Ihnen ausgewählte MID-Server auf demselben Computer wie der CyberArk AIM-Client befindet, der für den Zugriff auf den CyberArk-Tresor konfiguriert ist. Weitere Informationen finden Sie unter CyberArk-Tresor konfigurieren und die AIM-API installieren. ▪ Diese Option wird angezeigt, wenn Sie auswählen **MID-Server automatisch auswählen** Im Feld MID-Auswahl.
MID-Server	Wählen Sie manuell einen MID-Server aus. Diese Option wird angezeigt, wenn Sie im Feld MID-Auswahl die Option bestimmter MID-Server auswählen.
MID-Cluster	Wählen Sie manuell einen MID-Cluster aus. Diese Option wird angezeigt, wenn Sie im Feld MID-Auswahl die Option bestimmter MID-Cluster auswählen.
MID-Anwendung	Option zum Angeben einer MID-Anwendung oder Akzeptieren der Standardanwendungsauswahl. **Hinweis:** Diese Option wird angezeigt, wenn Sie auswählen **MID-Server automatisch auswählen** Im Feld MID-Auswahl. Standardmäßig ist **ALLE** Option ist ausgewählt.

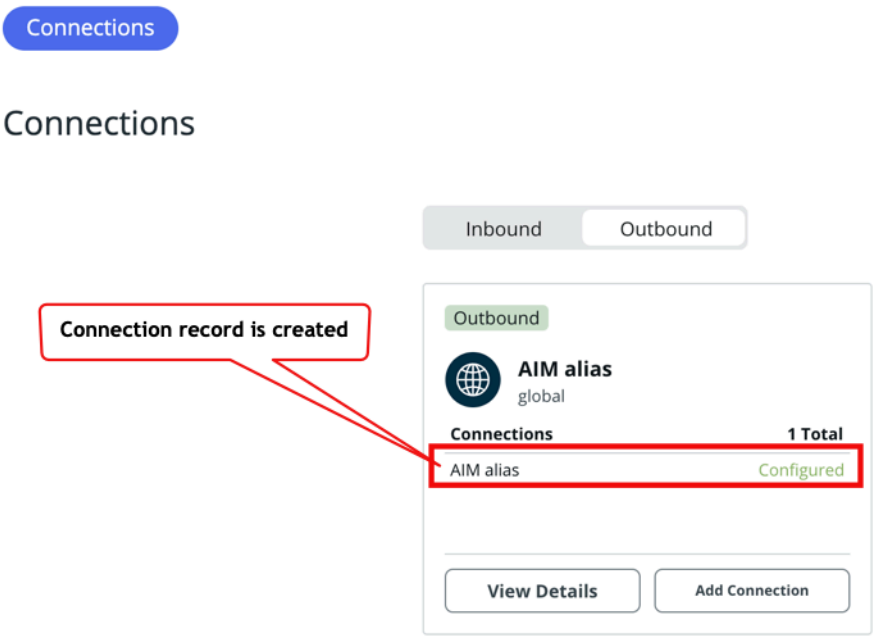
r. Wählen Sie **Absenden**.
Sie haben einen HTTP(s)-Verbindungsdatensatz erstellt.

s. Navigieren zu **Alle** > **Prozessautomatisierung** > **IntegrationHub** > **Verbindungs-Dashboard**an.

t. Geben Sie im Feld alle Verbindungen durchsuchen den Namen des erstellten Verbindungsdatensatzes ein.
Der Verbindungsalias-Datensatz wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OAuth 2,0-Verbindungsdatensatz wird erstellt



Authentifizierungsalgorithmen

Überprüfen Sie die Identität des Absenders mithilfe von Authentifizierungsalgorithmen

Zulassen, dass sich Integrationsschritte bei Webservices authentifizieren, die komplexe oder nicht standardmäßige Verbindungs- oder Anmeldeinformationsmechanismen erfordern. Ordnen Sie Authentifizierungsalgorithmen Anmeldeinformations- und Verbindungsaliasse zu, um die manuelle Konfiguration von Integrationsschritten zu reduzieren oder zu vermeiden.

Sie können einen Authentifizierungsalgorithmus verwenden, um anwenderdefinierte Authentifizierungsdaten für Ihre Integrationsschritte zu generieren. Integrationsschritte können diese dynamischen Daten verwenden, um anwenderdefinierte Artefakte zu erstellen, die für die Authentifizierung beim Ziel-Webservice erforderlich sind. Ein REST-Schritt könnte beispielsweise einen Authentifizierungsheader, Abfrageparameter oder ein Token erstellen.

Authentifizierungsalgorithmen unterstützen die folgenden Schritte:

- Schritt „Verbindungsinformationen Abrufen“
- REST-Schritt
- SOAP-Schritt

Weitere Informationen finden Sie unter Integrationsschritte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typen des Authentifizierungsalgorithmus

- **Amazon-Signaturversion 4** : Dies ist ein vorgefertigter Authentifizierungsalgorithmus für die Verbindung mit Amazon Web Services.
- **Anwenderdefinierte Authentifizierung** : Dies ist eine Vorlage, mit der Entwickler ihre eigenen Authentifizierungsalgorithmen erstellen können.

Weitere Informationen zur Konfiguration des Authentifizierungsalgorithmus finden Sie unter Konfigurieren Sie einen Authentifizierungsalgorithmus.

Skripte

Instanzauthentifizierungsskripts befinden sich in Instanzskripts, die Teil von sind *sys_script_include*Tabelle.

Instanzauthentifizierungsskripts

RequestAuthInternal	Schreibgeschütztes Skript in Instanz, das die Generierung der AWS V4-Signatur oder anwenderdefinierten Authentifizierung unterstützt, die mit ausgehender Anforderung gesendet wird.
RequestAuthAWSV4Signer	Skript zur Erweiterung von „RequestAuthInternal“, um den Unterzeichner zum Generieren der AWS V4-Signatur zu implementieren.
RequestAuthTwitterSigner	Skript zur Erweiterung von „RequestAuthInternal“, um den Unterzeichner zu implementieren, um die Twitter-Signatur mit OAuth 1.0a zu generieren.
RequestAuthSampleCustomSigner	Beispielskript zur Erweiterung von RequestAuthInternal, um zu verstehen, wie anwenderdefinierte Unterzeichner in der Instanz geschrieben werden.

MID-Authentifizierungsskripts befinden sich in MID-Skripts, die Teil von sind *ecc_agent_script_include*Tabelle.

MID-Authentifizierungsskripts

RequestAuthInternal	Schreibgeschütztes Skript auf MID, das die Generierung der AWS V4-Signatur oder anwenderdefinierten Authentifizierung unterstützt, die mit einer ausgehenden Anforderung gesendet wird.
AnforderungsAuthAWSV4MIDSigner	Skript zur Erweiterung von „RequestAuthInternal“, um den Unterzeichner zum Generieren der AWS V4-Signatur zu implementieren.
RequestAuthTwitterSigner	Skript zur Erweiterung von „RequestAuthInternal“, um den Unterzeichner zu implementieren, um die Twitter-Signatur mit OAuth 1.0a zu generieren.
RequestAuthSampleMidCustomSigner	Beispielskript zur Erweiterung von RequestAuthInternal, um zu verstehen, wie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID-Authentifizierungsskripts (Fortsetzung)

	anwenderdefinierte Unterzeichner auf MID geschrieben werden.

JavaScript-APIs

Im Folgenden finden Sie die JavaScript-APIs für den Authentifizierungsalgorithmus.

- Anmeldeinformationen
- HttpRequestAuthedData
- HttpRequestData
- RequestAuthAPI

Konfigurieren Sie einen Authentifizierungsalgorithmus

Konfigurieren Sie einen Authentifizierungsalgorithmus, damit Sie ausgehende HTTP-Anforderungen signieren können.

Vorbereitungen

Sie sollten eine Skripteinbindung konfigurieren, bevor Sie einen Authentifizierungsalgorithmus konfigurieren.
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**, Und klicken Sie auf **Neu** .
2. Füllen Sie im Formular die Felder aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.
Algorithmus	Typ der ausgehenden Anforderung.
Beschreibung	Beschreibung, was Ihr Algorithmus tut.
Anwendung	Bereich, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	Skript, das Sie aus der Tabelle „Skripteinbindungen“ auswählen.
MID-Authentifizierungsskript	Skript, das Sie aus der Tabelle „MID-Serverskripteinbindungen“ [Discovery-Ansicht] auswählen.

3. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen Amazon Signaturbasierter anwenderdefinierter Algorithmus

Generieren Sie Amazon Signaturbasierte Daten, die zur Authentifizierung bei einem Webservice durch Ausführen des Skripts erforderlich sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- JavaScript-Wissen
- REST-Wissen
- Wissen der Ziel-Webservice-API
- Wissen über Verbindungen, Anmeldeinformationen und Alias
- Erforderliche Rolle: Entwickler

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie einen Alias für Verbindungen und Anmeldeinformationen und Amazon Signaturversion 4-basierter Algorithmus für die Authentifizierung.

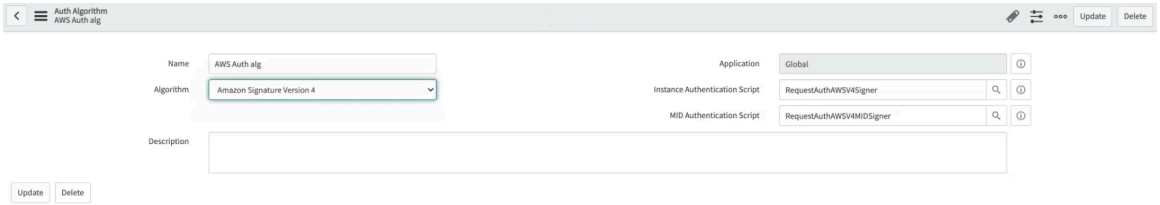
Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**, Und klicken Sie auf **Neu** .
2. Füllen Sie im Formular die Felder aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

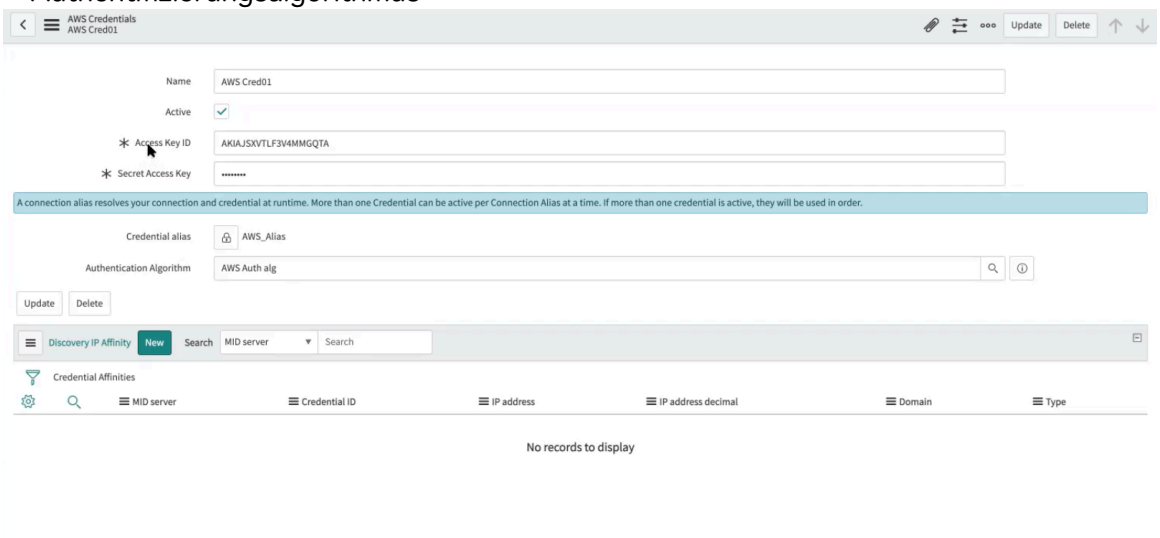
Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.
Algorithmus	Typ der ausgehenden Anforderung. Wählen Sie Aus **Amazon-Signaturversion 4** .
Beschreibung	Beschreibung, was Ihr Algorithmus tut.
Anwendung	Bereich, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	Skript, das Sie aus der Tabelle „Skripteinbindungen“ auswählen. Im Fall von **Amazon-Signaturversion 4** Algorithmus, wählen Sie aus **RequestAuthAWSV4Signer** . Folgende Skripts sind verfügbar: ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner **Hinweis:** Um mehr über das Skript zu erfahren, klicken Sie auf das Informationssymbol neben dem Feld. Die Details des Skripts, z. B. Name, API-Name, Anwendung, zugänglich von, Skript, und so weiter wird angezeigt.
MID-Authentifizierungsskript	Skript, das Sie aus der Tabelle „MID-Serverskripteinbindungen“ [Discovery-Ansicht] auswählen. Folgende Skripts sind verfügbar: ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Aktualisieren**.
4. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
5. Klicken Sie auf **Neu**.
6. Erstellen AWS Anmeldeinformationen mit Authentifizierungsalgorithmus.
   In diesem Fall **AWS-Authentifizierungsalg** .
7. Geben Sie Folgendes an:
   - Name
   - Aktiv
   - Zugangsschlüssel-ID
   - Geheimer Zugangsschlüssel
   - Anmeldeinformationsalias
   - Authentifizierungsalgorithmus



8. Klicken Sie auf **Aktualisieren**.

Ergebnis

Basierend auf den ausgewählten Skripts und dem Authentifizierungsalgorithmus werden die konfigurierten Anmeldeinformationen (**Zugriffsschlüssel-ID** Und **Geheimer Zugriffsschlüssel**) Oder Anmeldeinformationen des Anwenders (**Zugriffsschlüssel-ID** , **Geheimer Zugriffsschlüssel** , Und **Sitzungstoken**) Generiert einen Amazon V4-Signatur, die als ausgehende Anforderung von gesendet wird ServiceNow An den Anbieter (in diesem Fall AWS).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

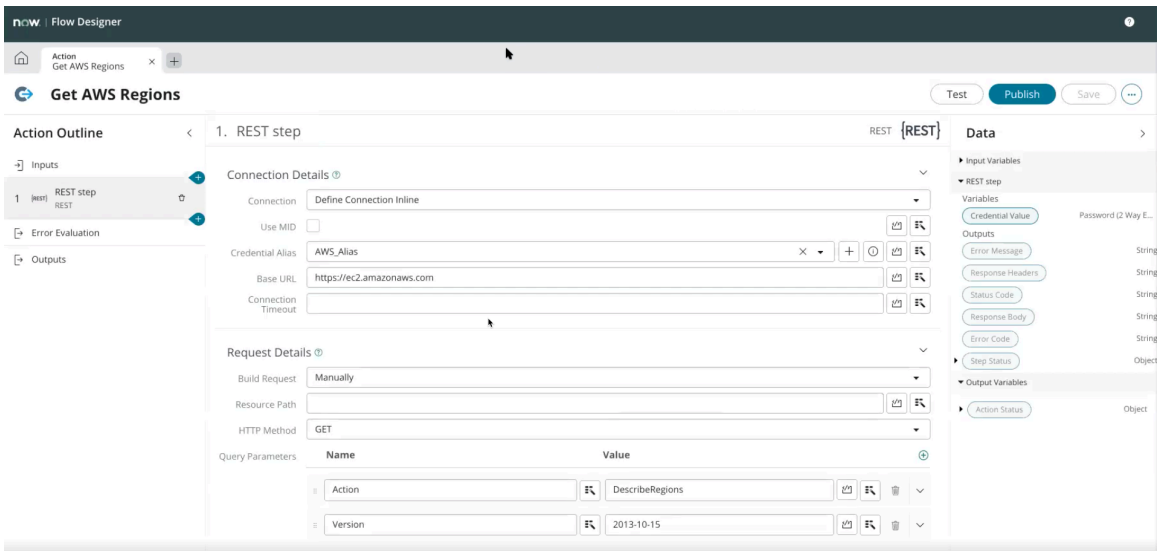
Example: REST-Schritt mit AWS

Hinweis: Amazon Die v4-Signatur-basierte Authentifizierung kann auch aus dem Skripthintergrund verwendet werden.

Aktion: Abrufen AWS Regionen

Geben Sie den REST-Schritt mit ein AWS Wie folgt:

- **Alias Für Anmeldeinformationen** : Der Alias, der für erstellt wird AWS.
- **Basis-URL** : Basis-URL-Details von AWS.
- **HTTPS-Methode** : In diesem Fall ist es die GET-Methode.
- **Abfrageparameter** : **Aktion** Als **BeschreibungRegionen** .



Sie können die Aktion testen. Die zugehörigen Regionen werden angezeigt. Der Antworttext lautet wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Amazon V4 ist mit einem Standardalgorithmus definiert, der den Authentifizierungsmechanismus unterstützt. Dieser Algorithmus fügt bei Verwendung die Signatur als Autorisierungsheader für die Authentifizierung (HTTP-Anforderung) mithilfe des REST-Schritts hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen anwenderdefinierten Authentifizierungsalgorithmus

Generieren Sie die anwenderdefinierten Daten, die zur Authentifizierung bei einem Webservice erforderlich sind, indem Sie ein Skript ausführen.

Vorbereitungen

- JavaScript-Wissen
- REST-Wissen
- Wissen der Ziel-Webservice-API
- Wissen über Verbindungen, Anmeldeinformationen und Alias
- Erforderliche Rolle: Entwickler

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie einen Alias für Verbindungen und Anmeldeinformationen sowie einen anwenderdefinierten Authentifizierungsalgorithmus für die Authentifizierung.

Prozedur

1. Navigieren zu **Alle** > **Anmeldeinformationen und Verbindungen** > **Authentifizierungsalgorithmen**, Und klicken Sie auf **Neu** .
2. Füllen Sie im Formular die Felder aus.
   Anhand der Auswahl der Datenbank im Feld **Format** wird festgelegt, welche Felder verfügbar sind.

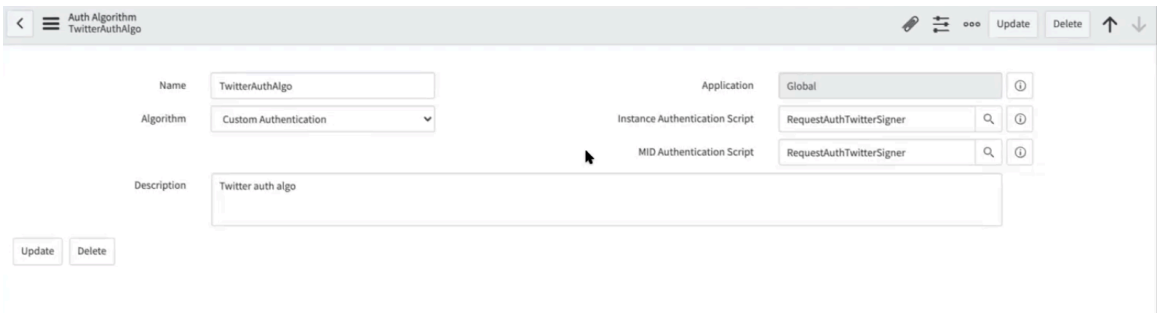
Authentifizierungsformular

Feld	Beschreibung
Name	Eindeutiger Name dieses Algorithmus.
Algorithmus	Typ der ausgehenden Anforderung. Wählen Sie Aus **Anwenderdefinierte Authentifizierung** .
Beschreibung	Beschreibung, was Ihr Algorithmus tut.
Anwendung	Bereich, in dem Ihre Anwendung ausgeführt wird.
Instanzauthentifizierungsskript	Skript, das Sie aus der Tabelle „Skripteinbindungen“ auswählen. Folgende Skripts sind verfügbar: ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ○ Um mehr über das Skript zu erfahren, klicken Sie auf das Informationssymbol neben dem Feld. Die Details des Skripts, z. B. Name, API-Name, Anwendung, zugänglich von, Skript, und so weiter wird angezeigt. ○ Im Falle einer anwenderdefinierten Authentifizierung mit Twitter können Sie auswählen **RequestAuthTwitterSigner** , Da eine OAuth 1.0a-Authentifizierungsmethode verwendet wird. Dies erfordert Informationen wie **API-Schlüssel und Geheimnis** Und **Zugriffstoken und Geheimnis** Die zum Erstellen von Signaturen verwendet werden kann, die in einem Autorisierungsheader übergeben werden sollen. Weitere Informationen finden Sie unter Authentifizierung in Twitter .
MID-Authentifizierungsskript	Skript, das Sie aus der Tabelle „MID-Serverskripteinbindungen“ [Discovery-Ansicht] auswählen. Folgende Skripts sind verfügbar: ○ RequestAuthAWSV4Signer ○ RequestAuthInternal ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

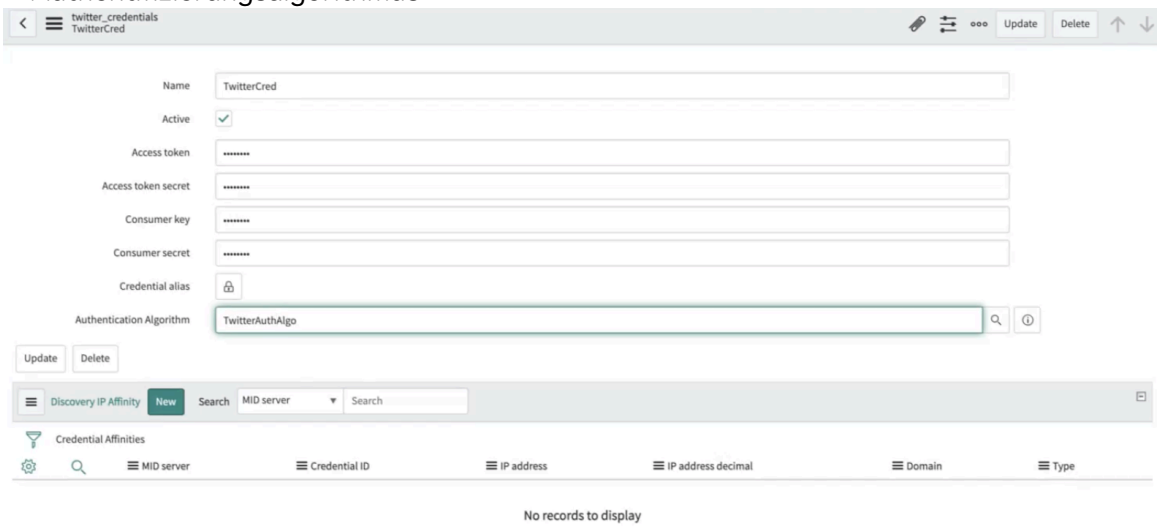


Basierend auf den ausgewählten Skripts und dem Authentifizierungsalgorithmus werden die konfigurierten Anmeldeinformationen als ausgehende Anforderung von gesendet ServiceNow An den Anbieter.

3. Klicken Sie auf **Aktualisieren**.
4. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
5. Klicken Sie auf **Neu**.
6. Erstellen Twitter Anmeldeinformationen mit Authentifizierungsalgorithmus.
   In diesem Fall **TwitterAuthAlgo** .
7. Geben Sie die Felder an:
   - Name
   - Aktiv
   - Zugriffstoken
   - Geheimer Zugriffstoken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verbraucherschlüssel
- Verbrauchergeheimnis
- Anmeldeinformationsalias
- Authentifizierungsalgorithmus



8. Klicken Sie auf **Aktualisieren**.

Example: REST-Schritt mit Twitter

Im Fall von Twitter, Sie müssen sicherstellen, dass die folgenden Spokes oder Anmeldeinformationen verfügbar sind:

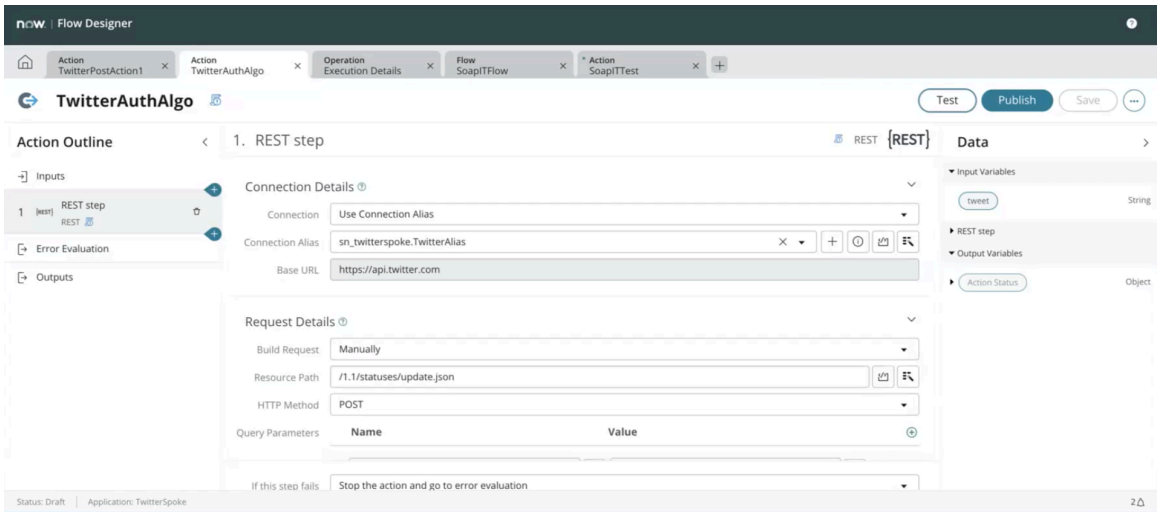
- Zugriffstoken
- Geheimer Zugriffstoken
- Verbraucherschlüssel
- Verbrauchergeheimnis
- Authentifizierungsalgorithmus

Aktion: TwitterAuthAlgo.

Geben Sie den REST-Schritt mit ein Twitter Wie folgt:

- **Alias Für Anmeldeinformationen** : Der Alias, der für erstellt wird Twitter.
- **Basis-URL** : Basis-URL-Details von Twitter.
- **HTTPS-Methode** : In diesem Fall handelt es sich um die POST-Methode. Veröffentlicht einen Tweet.
- **Abfrageparameter** : **Aktion** Als **Tweet** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Aktion testen. Der Tweet wird auf veröffentlicht Twitter Seite.

IP-Service-Affinität für Discovery und Orchestration prüfen

Sie können in der Tabelle „IP-Services“ nach einer Liste von IP-Adressen suchen, die einem Protokoll zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „IP-Services“ ordnet einen Port einem Protokoll zu. Für häufig verwendete Port-Protokoll-Kombinationen werden standardmäßig Zuordnungen bereitgestellt, z. B. Port 80 für HTTP, Port 22 für SSH und Port 161 für SNMP.

Mithilfe der Systemeigenschaft `glide.discovery.ip_service_affinity` kann sich Discovery den letzten Port der erkannten IP-Adresse merken.

Wichtig: Sie sollten IP-Services nur dann ändern, wenn Ihre Organisation benutzerdefinierte Ports verwendet.

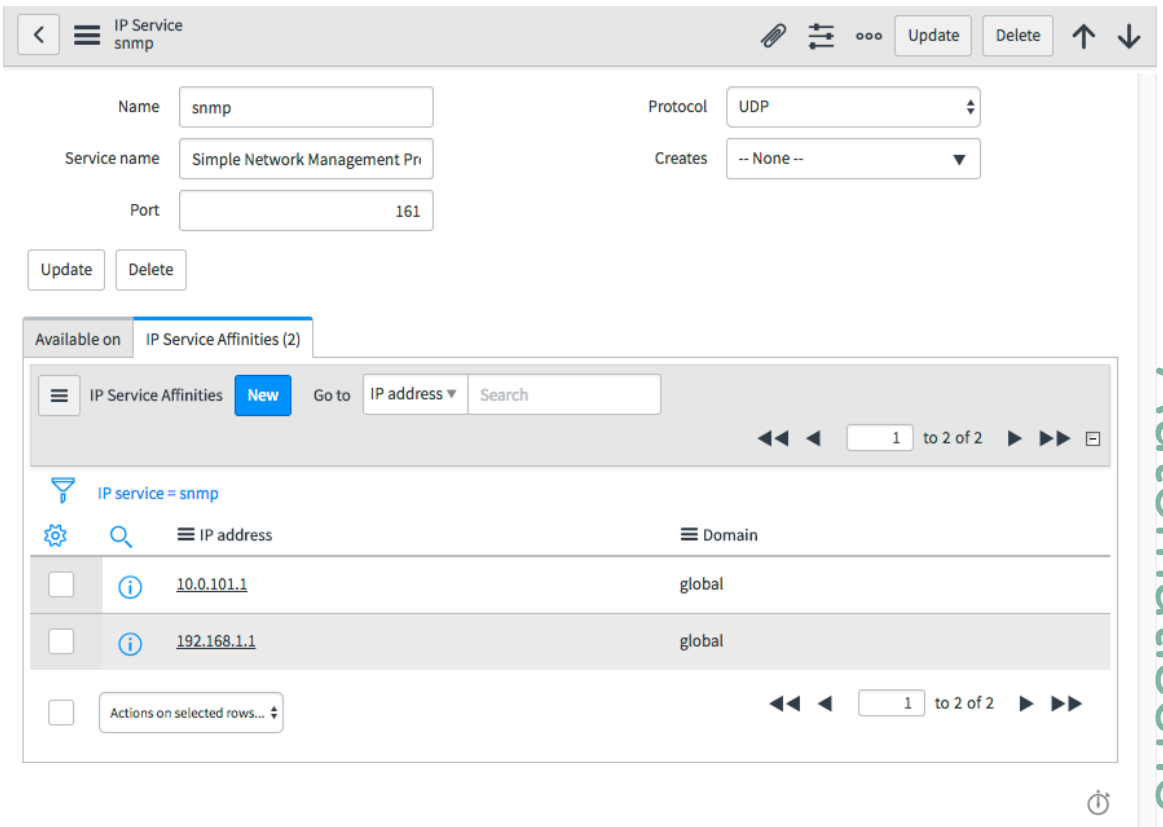
Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **IP-Services**an.
2. Filtern Sie die Liste, um den entsprechenden IP-Service zu finden.
3. Klicken Sie auf den Namen des Service, um zu dieser IP-Serviceseite zu gelangen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **IP-Serviceaffinitäten**, um die Liste der IP-Adressen anzuzeigen, die diesem Service zugeordnet sind.

IP-Serviceaffinitäten



ServiceNow®-Zugriffssteuerung

Mit dem Plugin „SNC-Zugriffssteuerung“ (com.snc.snc_Access_Control) können Sie steuern, welche Kundenservice und Support Mitarbeiter können auf Ihre Instanz zugreifen und wann.

Erkunden Sie die ServiceNow-Zugriffssteuerung



Aktivieren Sie die ServiceNow-Zugriffssteuerung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie mehr über die Funktionen von ServiceNow® Zugriffssteuerung.

Aktiv ServiceNow® Zugriffssteuerung.

Konfigurieren Sie die ServiceNow-Zugriffssteuerung



Erfahren Sie, wie Sie konfigurieren ServiceNow® Zugriffssteuerung.

Audit-Protokollierung



Erfahren Sie, und überprüfen Sie ServiceNow® Audit-Protokollierung der Zugriffssteuerung.

Erkunden E ServiceNow® Zugriffssteuerung

Mit dem Plugin „SNC-Zugriffssteuerung“ (com.snc.snc_Access_Control) können Sie steuern, welche Kundenservice und Support Mitarbeiter können auf Ihre Instanz zugreifen und wann.

Wenn Sie das Plugin zum ersten Mal aktivieren, Kundenservice und Support Mitarbeiter können sich nicht bei der Instanz anmelden. Alle derzeit angemeldeten Kundenservice und Support Mitarbeiter bleiben angemeldet. Sie erstellen Datensätze in der Tabelle „SNC-Zugriffssteuerung“, die bestimmten SNC-Mitarbeitern oder allen Mitarbeitern Zugriff gewähren.

Das Plugin verhindert Kundenservice und Support Mitarbeiter, die ohne Ihre ausdrückliche Erlaubnis auf die Instanzen zugreifen können. Jedoch andere autorisiert ServiceNow Betriebspersonal in ihrer Fähigkeit, das Produkt zu unterstützen und zu verwalten und zu überprüfen, ob die Nutzung erforderlich ist, um administrative Aktionen für die zugrunde liegende Infrastruktur durchzuführen. Diese Infrastruktur umfasst Server und Datenbanken sowie andere Infrastrukturkomponenten, aus denen die SaaS-Lösung besteht. Diese Zugriffsmethode ist vollständig auditierbar und wird nachverfolgt.

Mit diesem Plugin können Sie den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Berechtigung beschränken, sodass dies sich auf Support-Servicelevel und das

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbarkeits-SLA auswirken kann. Das Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeiter Zugriff auf Ihre Instanz erhalten.

Anmeldesicherheit

Sicherheit für autorisiert Kundenservice und Support Mitarbeiteranmeldungen bei Instanzen verwenden verschlüsselte Token, die von einem sicheren Server generiert werden. Nur ordnungsgemäß authentifiziert Kundenservice und Support Mitarbeitern wird Zugriff auf eine Instanz gewährt. Ohne das Plugin „SNC-Zugriffssteuerung“ stellt der Sicherheitsserver sicher, dass Zugriffsrechte auf hi.service-now.com durchgesetzt werden. Wenn das Plugin aktiviert ist, müssen die verschlüsselten Anmeldetoken mit den Namen in der vom Plugin bereitgestellten Zugriffsliste übereinstimmen, wobei die in diesen Datensätzen definierten Kriterien verwendet werden. Mit dieser Authentifizierungsmethode können Sie genau bestimmen, welche Kundenservice und Support Mitarbeiter können auf ihre Instanzen zugreifen, und wann diese Mitarbeiter dies tun können.

Die für dieses System ausgewählte Architektur verfügt über mehrere Funktionen, die die Sicherheit für Ihre Instanzen verbessern:

Sicherheitsserver

Der Sicherheitsserver ist ein gesperrter Linux-Host, der nur das ist ServiceNow Sicherheitspersonal kann darauf zugreifen. Dieser Server ist das einzige System, das Zugriff auf den kritischen privaten Verschlüsselungsschlüssel hat, der zum Erstellen der Anmeldetoken erforderlich ist. Durch die Verwendung dieser Abteilungspraxis (eine standardmäßige Sicherheitspraxis) wird der private Schlüssel geschützt, auch im unwahrscheinlichen Fall, dass ein Angreifer die HI-Instanz gefährdet.

Synthetic-Anwender

Die Einrichtung in Instanzen, die autorisiert aktiviert Kundenservice und Support Für Mitarbeiter, die sich bei ihrer Instanz anmelden können, muss in dieser Instanz kein Account bereitgestellt werden. Es ist kein Anwenderdatensatz bereitgestellt und keine permanenten oder beibehaltenen Anmeldeinformationen. Stattdessen wird für jeden ein Synthetic-Anwender erstellt Kundenservice und Support Mitarbeiteranmeldung. Dieser Anwender ist nur im Arbeitsspeicher vorhanden und gewährt keine laufenden Berechtigungen. Wenn das Plugin „SNC-Zugriffssteuerung“ aktiviert ist, können Sie die Autorisierung beliebiger Elemente aufheben Kundenservice und Support Mitarbeiter jederzeit.

Token

Die Sicherheitstoken sind spezifisch für eine Instanz und eine bestimmte Kundenservice und Support Mitarbeiter. Darüber hinaus funktioniert der Mechanismus, der die Token generiert, nur mit Actual Kundenservice und Support Mitarbeiter meldet sich bei HI an, keine Anwender, deren Identität angenommen wurde. Sobald ein Sicherheitstoken generiert wurde, nur ein bestimmtes Kundenservice und Support Mitarbeiter können sie verwenden, um sich bei einer Instanz anzumelden.

Zeitbegrenzung

Sicherheitstoken laufen vier Stunden nach der Generierung ab. Dieser Ablauf begrenzt das Dienstprogramm von gekapselten Token, die nur während dieses kurzen Fensters verwendet werden können.

Protokollierung

Anmeldungen durch Kundenservice und Support Mitarbeiter in Instanzen werden als Anmeldereignis aufgezeichnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Jede Aktion, die vom angemeldeten ausgeführt wird Kundenservice und Support Mitarbeiter wird dem Transaktionsprotokoll in der Datenbank hinzugefügt.
- Es wird auch dem Instanzprotokoll im Dateisystem hinzugefügt, das für die meisten nicht zugänglich ist ServiceNow Mitarbeiter.
- Kundenservice und Support Mitarbeiteranmeldungen und -Aktionen sind leicht zu identifizieren, da die Anwendernamen alle auf @snc enden (z. B. frodo.baggins@snc).

Diese Aktionen bieten Ihnen eine anwenderfreundliche, robuste und zuverlässige Sicherheitsprotokollierung für den Zugriff ohne Mitarbeiter.

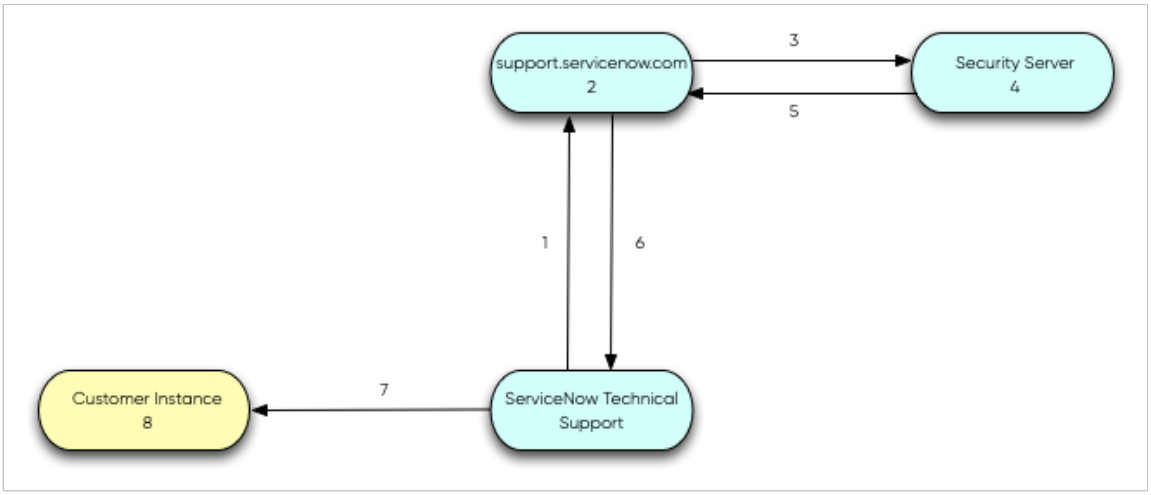
Sicherheitsverarbeitungs-Flow

Wenn ein Kundenservice und Support Mitarbeiter möchte sich bei einer Instanz anmelden. Der Sicherheitsverarbeitungs-Flow lautet wie folgt:

1. A Kundenservice und Support Der Techniker fordert eine Anmeldung für die Instanz über hi.service-now.com an.
2. HALLO überprüft, ob der Techniker über die richtige Rolle für die Autorisierung des Zugriffs auf Instanzen verfügt.
3. Wenn der Anwender über die richtige Rolle verfügt, sendet HI die Anforderung für den Zugriff auf den Sicherheitsserver.
4. Der Sicherheitsserver überprüft, ob die Anforderung von der HI-IP-Adresse stammt, und wertet die Anforderung aus (Anwender, Rolle und IP-Adresse der anfordernden Person). Wenn die Anforderung gültig ist, genehmigt der Sicherheitsserver sie und erstellt ein Token. Dieses Token enthält den Anwendernamen, die Rollen, die Instanz-ID und die Zeit (der Beginn der 4-Stunden-Token-Lebensdauer). Schließlich verschlüsselt der Sicherheitsserver das Token mit dem privaten Verschlüsselungsschlüssel.
5. Der Sicherheitsserver sendet das verschlüsselte Token an HI.
6. Hallo sendet das Token an den Browser des Support-Technikers.
7. Der Browser des Support-Technikers initiiert eine Anmeldung bei der Instanz mit dem speziellen Anwendernamen, der mit endet `@Snc` .
8. Die Instanz verwendet den öffentlichen Schlüssel, um das Token zu entschlüsseln. Um das Token zu verifizieren, stimmt die Instanz es mit dem im vorherigen Schritt angegebenen Anwendernamen, der Instanz-ID und dem autorisierten Zeitfenster ab. Wenn das Plugin „SNC-Zugriffssteuerung“ aktiviert ist, überprüft die Instanz, ob der Anwender:
   - Aufgeführt
   - Aktiv
   - Konfiguriert für den Zugriff auf die Instanz im aktuellen Zeitfenster
9. Wenn der Anwender authentifiziert ist, erstellt die Instanz einen *Synthetic-Anwender* Im Arbeitsspeicher mit den angegebenen Rollen. Dieser Anwender bleibt nicht bestehen, nachdem die Zeitbegrenzung abgelaufen ist, sich der Anwender abgemeldet hat oder die Instanz neu gestartet wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Prozess-Flow für Sicherheitszugriff



Audit-Protokollierung

Die folgende Protokollierung verfolgt Anmeldungen und Aktivitäten nach Kundenservice und Support Mitarbeiter:

- Ereignisprotokolle: Die Ereignisprotokolle zeigen alle an Kundenservice und Support Meldet sich bei einer Instanz an.
- Transaktionsprotokolle: Die Transaktionsprotokolle zeigen alle Aktivitäten in der Instanz an, einschließlich aller Maßnahmen zum Löschen von Protokollen.

Hinweis: Weitere Informationen zu diesem Plugin finden Sie unter Plugin für SNC-Zugriffssteuerung aktivieren [aktualisiert in Security Center 1,3] In Instanzsicherheitshärtungseinstellungen.

Aktivieren ServiceNow® Zugriffssteuerung

Sie fordern die Aktivierung des Plugins „SNC-Zugriffssteuerung“ (com.snc.snc_Access_Control) an.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

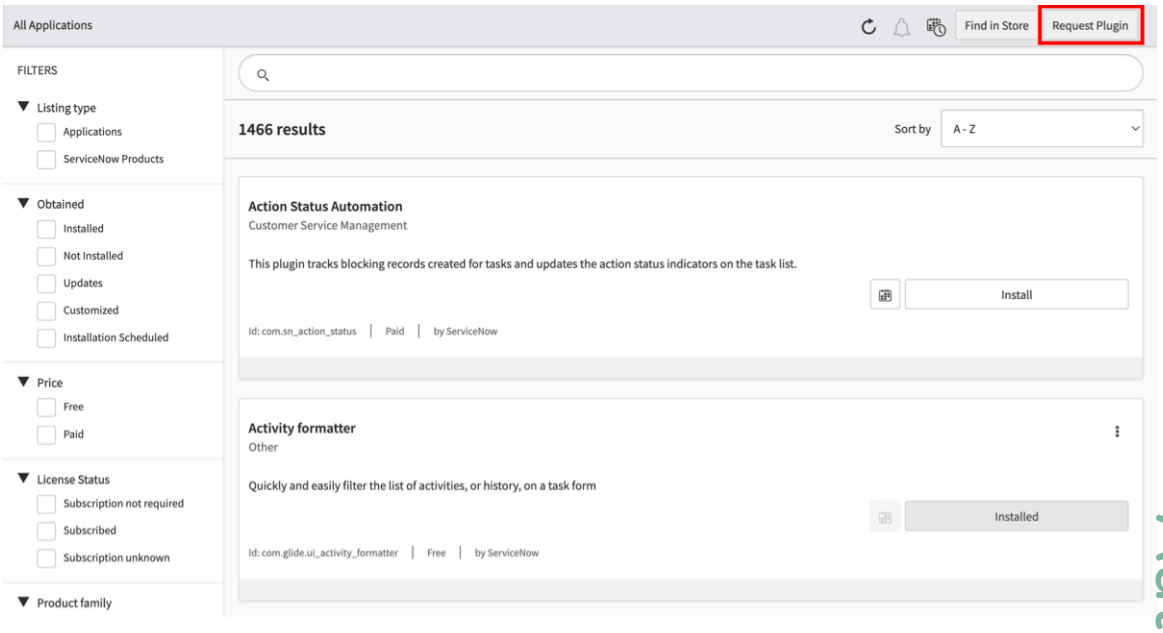
Es gibt zwei Möglichkeiten, ein Plugin anzufordern:

- Greifen Sie auf zu Now Support Servicekatalog direkt durch Auswahl **Alle** > **Servicekatalog** > **Plugin aktivieren** Ein Now Support.
- Greifen Sie über die Seite „Alle Anwendungen“ in Ihrer Instanz auf den Now Support-Servicekatalog zu, indem Sie die folgenden Schritte ausführen.

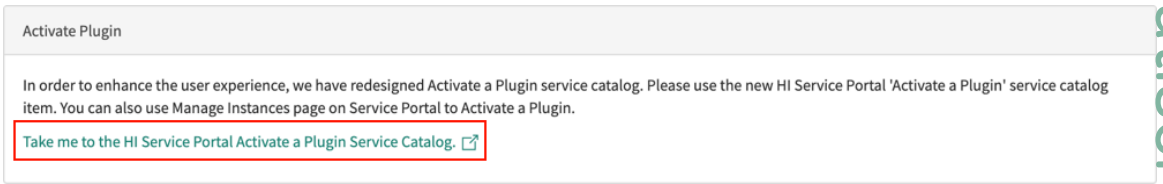
Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.

5. Wählen Sie **Aktionen > Plugin aktivieren** aus.

6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
	Datum und Uhrzeit zum Aktivieren des Plugins.

Automatische Übersetzung

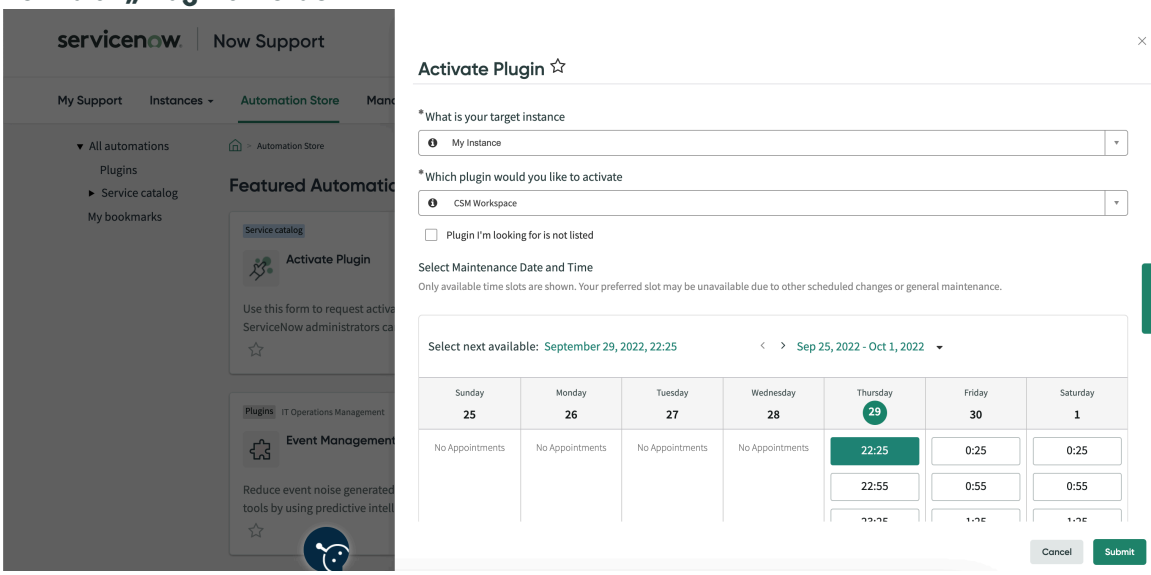
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	**Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Konfigurieren ServiceNow® Zugriffssteuerung

Konfigurieren Sie einen Zugriffssteuerungsdatensatz, um einen oder mehrere anzugeben Kundenservice und Support Mitarbeiter, die berechtigt sind, sich bei Ihrer Instanz anzumelden.

Vorbereitungen

Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Das Plugin „SNC Access Control“ (com.snc.snc_Access_Control) verhindert Kundenservice und Support Mitarbeiter, die ohne Ihre ausdrückliche Erlaubnis auf die Instanzen zugreifen können. Jedoch andere autorisiert ServiceNow Betriebspersonal in ihrer Eigenschaft zur Unterstützung und Verwaltung des Produkts müssen administrative Aktionen für die zugrunde liegende Infrastruktur ausführen. Diese Infrastruktur umfasst Server und Datenbanken sowie andere Infrastrukturkomponenten, aus denen die SaaS-Lösung besteht. Diese Zugriffsmethode ist vollständig auditierbar und wird nachverfolgt.

Mit diesem Plugin können Sie den Zugriff auf Ihre Instanz ohne Ihre ausdrückliche Berechtigung beschränken, sodass dies sich auf Support-Servicelevel und das Verfügbarkeits-SLA auswirken kann. Das Verfügbarkeits-SLA wird dann ab dem Zeitpunkt gemessen, zu dem Support-Mitarbeiter Zugriff auf Ihre Instanz erhalten.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **SNC-Zugriffssteuerung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).
4. Klicken Sie auf **Absenden**.

SNC-Zugriffssteuerung

Formularfelder	Beschreibung
Name	Namen jeweils Kundenservice und Support Mitarbeiter, der über die Berechtigung zum Anmelden in dieser Instanz verfügt. ○ Geben Sie die Namen als „Vorname.Nachname“ in Kleinbuchstaben getrennt durch einen Punkt an (z. B. john.smith). Jeder Name muss einen entsprechenden Anwenderdatensatz in haben *support.servicenow.com*. ○ Wenn mehr als eins Kundenservice und Support Mitarbeiter hat die Berechtigung, sich in dieser Instanz anzumelden, mehrere Namen einzugeben und sie durch Kommas zu trennen. ○ Um alle zu aktivieren Kundenservice und Support Anmelderechte von Mitarbeitern um auf die Instanz zuzugreifen, geben Sie ein Sternchen ein (*) Anstelle des Namens. ○ Wenn Sie einschränken möchten Kundenservice und Support Mitarbeiterzugriff auf die Instanz, die Werte in **Name** Feld darf kein Sternchen (*) An beliebiger Stelle im Feld.
Grund	Visuell lesbares Feld, das beschreibt, warum Sie Zugriffsberechtigung gewähren. Dieses Feld ist optional.
Start	Gibt das Startdatum und die Startzeit des Zeitraums an, in dem der angegebene Zeitraum liegt Kundenservice und Support Mitarbeiter haben Anmeldezugriff. Dieses Feld ist ein Pflichtfeld.
Ende	Gibt das Enddatum und die Endzeit des Zeitraums an, in dem der angegebene Zeitraum liegt Kundenservice und Support Mitarbeiter haben Anmeldezugriff. Dieses Feld ist ein Pflichtfeld.
Aktiv	Steuert, ob dieser Berechtigungsdatensatz aktiv ist. Der Standardwert ist aktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Audit-Protokollierung

Die folgende Protokollierung verfolgt Anmeldungen und Aktivitäten nach ServiceNow Mitarbeiter.

Ereignisprotokolle	Die Ereignisprotokolle zeigen alle an ServiceNow Meldet sich bei einer Kundeninstanz an.
Transaktionsprotokolle	Die Transaktionsprotokolle zeigen alle Aktivitäten in der Instanz an, einschließlich aller Maßnahmen zum Löschen von Protokollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identität

Erfahren Sie mehr über die Identitäten in der Instanz.

Zugriffsanalyse



Zugriffsanalyse ist ein ServiceNow® Store-App, bei der es sich um ein Zugriffsdiagnosetool handelt. Es hilft, zu bestimmen, wer Zugriff auf eine Ressource hat.

Globale Identität



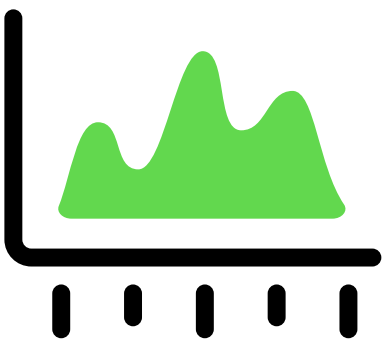
Globale Identität ist ein ServiceNow® Mit der Store-App können Sie Anwenderattribute von einer Instanz zu Instanz (mehrere Instanzen) aktualisieren.

Identity Center



Mit Identity Center können Sie identitätsbasierte Risiko- und Sicherheitslücken überwachen, verwalten und minimieren.

System für domänenübergreifendes Identitätsmanagement (SCIM)



Identitäts- und Zugriffsaudit



Verwenden Sie das Audit für Identität und Zugriff, um die Änderungen zu verstehen, die an einem Anwender, einer Gruppe, einer Rolle und einer ACL vorgenommen wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die System for Cross-Domain Identity Management (SCIM)-API stellt Endpunkte zum Erstellen, Lesen, Aktualisieren und Löschen von Vorgängen für Anwender und Gruppen bereit, die das SCIM-Protokoll verwenden.

Zugriffsanalyse

ServiceNow® Die Zugriffsanalyse ist ein Zugriffsdiagnosetool, mit dem die Berechtigungen einer Identität für eine Ressource angezeigt werden können.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen der Zugriffsanalyse.

Verwenden



Erfahren Sie, wie die Zugriffsanalyse verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungsauswertung



Erfahren Sie, wie die Berechtigungen ausgewertet werden.

Häufige Fragen



Rufen Sie Details zu häufig gestellten Fragen zur Zugriffsanalyse ab.

Zugriffsanalyse Erkunden

Analysieren Sie Identitäten auf der ServiceNow Instanz.

ServiceNow Die Zugriffsanalyse ist eine Anwendung, mit der Administratoren Berechtigungen für den ausgewählten Anwender, die ausgewählte Rolle oder die ausgewählte Gruppe anzeigen können.

Hinweis:

- Zugriffsanalyse ist ein ServiceNow Store-Produkt. Besuchen Sie die Website ServiceNow Store , um sich alle verfügbaren Apps anzusehen und Informationen zum Senden von Anforderungen an den Store zu erhalten.
- Die Zugriffsanalyse nimmt die Identität des Identitätsdatensatzes an, um Details zu den Berechtigungen abzurufen, und liest oder speichert keine persönlichen oder vertraulichen Daten der Identität.
- Die Ergebnisse der Auswertung der Zugriffsanalyse sind unabhängig von den für die Anwender definierten Zugriffsrichtlinien identisch, z. B. Zero Trust Access (ZTA). Die Richtlinien werden nur während der tatsächlichen Anwenderanmeldung ausgewertet und während des Zugriffsanalyseflusses nicht ausgewertet.
- Die Zugriffsanalyse hat Einschränkungen bei der genauen Bewertung des Zugriffs auf die Ressourcen im Zusammenhang mit verwalteten Umfangsressourcen und delegiertem Entwickler.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff Auswerten

„Zugriff auswerten“ ist eine Fähigkeit von ServiceNow Zugriffsanalyse, mit der Administratoren Berechtigungen für den ausgewählten Anwender, die ausgewählte Rolle oder die ausgewählte Gruppe anzeigen können.

Mit dieser Option können Sie die Berechtigungen von Anwendern, Gruppen, Rollen für eine Tabelle, vom Client aufrufbare Skripteinbindungen, UI-Seiten und REST-Endpunkte analysieren und anzeigen.

Mit der Zugriffsanalyse können Unternehmen ihre Sicherheitslage, Identitäts-Governance und Risikomanagement verbessern, ihre Compliance-Ziele erreichen und verstehen, wer (Identität) Zugriff auf was hat (Ressourcen).

Zugriff Vergleichen

Der Zugriff vergleichen ist eine Fähigkeit von ServiceNow Zugriffsanalyse V2, mit der Administratoren den Anwenderzugriff vergleichen und die richtige Zugriffsebene für die Anwender auf Ihrem bestimmen können ServiceNow Instanz.

Der Zugriff kann zwischen den Anwendern für die Anwenderdatensätze und die Zugriffssteuerung verglichen werden.

Mit Zugriff vergleichen können Sie die folgende Analyse durchführen:

- Ebene 1: Vergleichen Sie Anwenderdatensätze, um die Attribute, Rollen und Gruppen zu verstehen.
- Ebene 2: Vergleichen Sie die Zugriffssteuerungen, um die Ursachenanalyse durchzuführen, indem Sie Zugriffsprobleme finden.

Vorteile

Im Folgenden sind einige der Vorteile der Verwendung der Zugriffsanalyse aufgeführt:

- Analysieren Sie den Zugriff auf Ressourcen (Tabellen).
- Vergleichen Sie den Zugriff von 2 Anwendern.
- Vergleichen Sie die Rollen und Gruppen von 2 Anwendern.
- Generieren Sie einen Bericht, der anzeigt, ob eine Identität Zugriff auf eine Ressource (Tabelle) hat.
- Erfahren Sie, wer Zugriff auf kritische Sicherheitshygiene hat.
- Helfen Sie, die Überbereitstellung von Berechtigungen zu verhindern.
- Erreichen Sie bei der Implementierung von Zugriffssteuerungen die Prinzipale mit den geringsten Berechtigungen.
- Beschränken Sie den Zugriff auf bestimmte Daten, z. B. Anwendungen, Tabellen, Zeilen oder Spalten und andere Ressourcen.
- Stellen Sie Reportingfunktionen für die Analyseergebnisse bereit.
- Vergleichen Sie den Zugriff zwischen Anwenderdatensätzen und Zugriffssteuerungen.
- Bestimmen Sie die richtige Zugriffsebene für Anwender auf Ihrem ServiceNow Instanz.

Zugriffsanalyse Verwenden

Identitäten und deren Zugriff auf analysieren ServiceNow® Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin, Access_Analyzer_admin

Im folgenden Verfahren werden die Schritte für den Zugriff auf die Zugriffsanalyse und die Verwendung verschiedener Funktionen in der Zugriffsanalyse beschrieben.

Hinweis: Zugriffsanalyse ist ein ServiceNow® Store-Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.

   Die Zugriffsanalyse verfügt über die folgenden Fähigkeiten:

   - Zugriff Auswerten
   - Anwenderdatensätze vergleichen
   - Zugriffssteuerungen vergleichen
2. Wählen Sie die entsprechende Registerkarte aus, um die Zugriffsanalyse basierend auf Ihren Anforderungen zu verwenden.

Verwenden Sie „Zugriff auswerten“

Analysieren Sie Identitäten auf der ServiceNow® Instanz.

Vorbereitungen
Erforderliche Rolle: admin, Access_Analyzer_admin

Im folgenden Verfahren werden die Schritte für den Zugriff auf „Zugriff bewerten“ in der Zugriffsanalyse und die Verwendung der verschiedenen Funktionen beschrieben.

Hinweis: Zugriffsanalyse ist ein ServiceNow Store Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie aus **Zugriff bewerten** Registerkarte.
3. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Analysieren Sie den Zugriff für einen Anwender, eine Rolle oder eine Gruppe
Wählen Sie Anwender * aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll.
Regeltyp *	Analysieren Sie den Zugriff auf eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung.
Wählen Sie Tabelle * aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

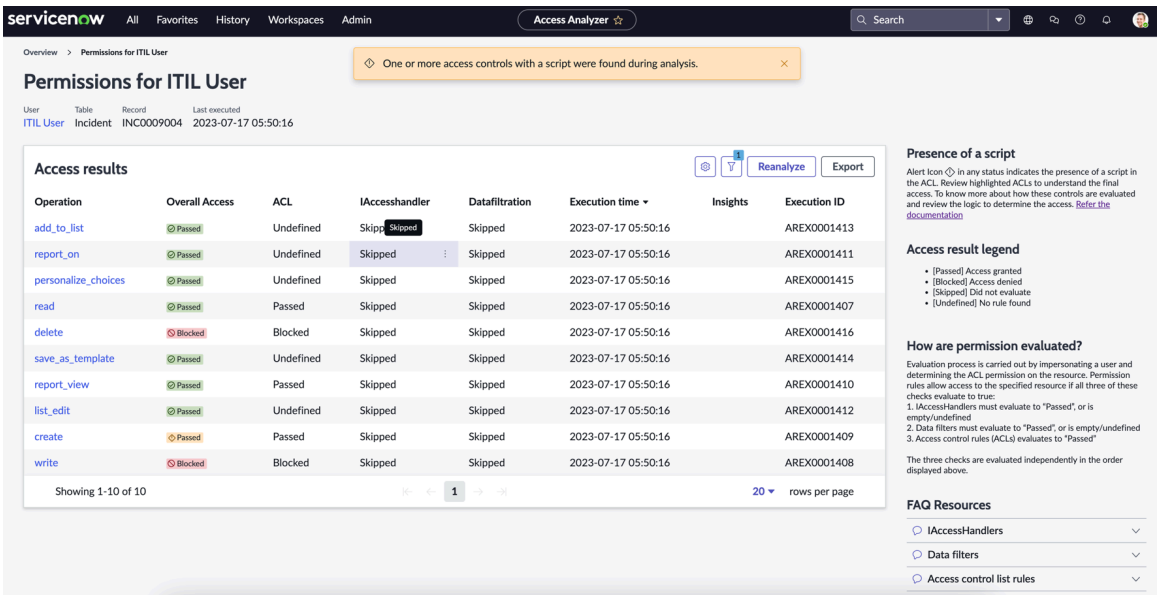
Feld	Beschreibung
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll.
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll.

4. Geben Sie die Beschreibung in an **Beschreibung** Feld.
5. Wählen Sie Aus **Berechtigungen analysieren** .

   Die Zugriffsergebnisse für den Anwender werden angezeigt. Ebenso können Sie die Berechtigungen einer Gruppe oder Rolle für die folgenden Regeltypen analysieren:

   - Tabelle (Datensatz)
   - Vom Client aufrufbare Skripteinbindung
   - REST-Endpunkte

   Die Zugriffsergebnisse werden angezeigt.



Die Tabelle „Zugriffsergebnisse“ enthält die folgenden Felder:

Auf Ergebnisse zugreifen

Felder	Beschreibung
Vorgang	Die Art des Vorgangs, den der Anwender, die Gruppe oder die Rolle für die ausgewählte Tabelle, den ausgewählten Datensatz oder das ausgewählte Feld ausführen kann.
Allgemeiner Zugriff	Ergebnis des Gesamtzugriffs. Die Ergebnisse lauten wie folgt: ○ [Bestanden] Zugriff gewährt ○ [Blockiert] Zugriff verweigert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	○ [Übersprungen] wurde nicht ausgewertet ○ [Nicht definiert] Keine Regel gefunden
ACL	Gibt an, ob eine ACL für den ausgewählten Vorgang definiert ist.
Zugriffs-Handler	Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet.
Datenfilterung	Ein Datenfilter ist eine Form der Zugriffssteuerung, die mit den vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz kompatibel ist.
Ausführungszeit	Der Zeitpunkt, zu dem die Zugriffsergebnisse ausgeführt wurden.
Einblicke	Weitere Informationen zum ausgewählten Vorgang.
Ausführungs-ID	Eine eindeutige ID für jede Ausführung des Zugriffsergebnisses.

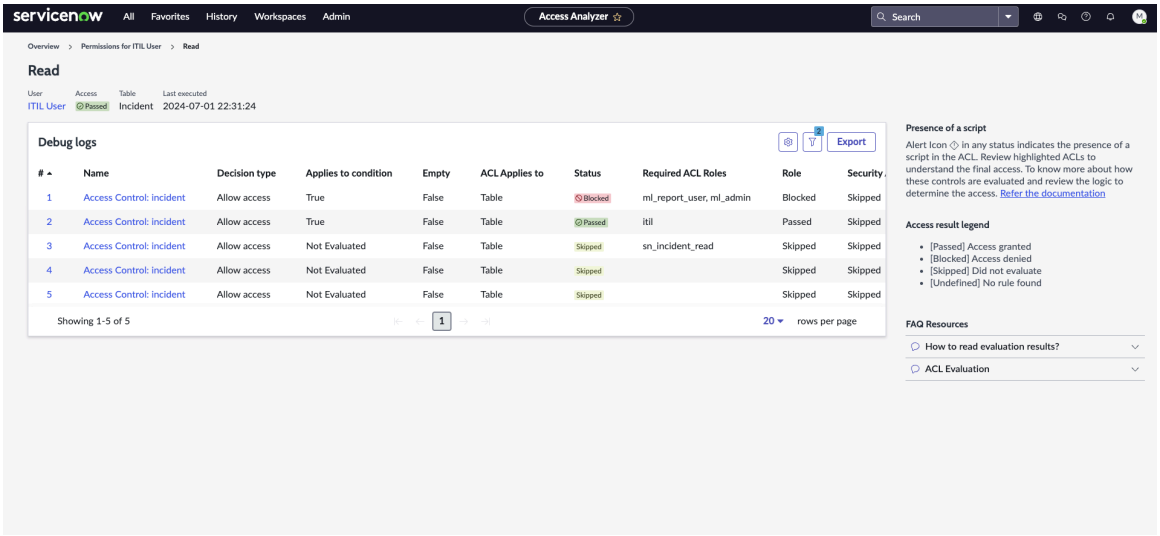
6. Wählen Sie den Vorgang aus, um weitere Informationen zur ACL zu erhalten.
Beispiel: Wenn Sie auswählen **Lesen** , Die Zugriffssteuerung im Zusammenhang mit dem Lesen wird angezeigt.

ACL-Details

Feld	Beschreibung
Name	Name der ACL.
Entscheidungstyp	Entscheidungstyp, der für die ACL konfiguriert ist. **Zugriff zulassen** Oder **Zugriff verweigern** .
Gilt für Bedingung	Gibt an, ob die ACL auf eine Bedingung angewendet wird.
ACL gilt für	Details zur Ressource, auf die die ACL angewendet wird.
Status	Status der ACL oder des Zugriffsergebnisses.
Erforderliche ACL-Rollen	Details der Rolle, die für den Zugriff auf die Ressource erforderlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rolle	Status der Rolle. Bestanden, übersprungen oder blockiert.



Zeigen Sie Berechtigungen für einen Anwender an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für einen ausgewählten Anwender anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Das folgende Verfahren beschreibt die Beispielschritte zum Anzeigen von Berechtigungen für einen ausgewählten Anwender (**ITIL-Anwender**), um die Berechtigungen von anzuzeigen **Incident** Tabelle mit dem Auswertungszugriff in der Zugriffsanalyse.

Hinweis: Zugriffsanalyse ist ein ServiceNow® Store-Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

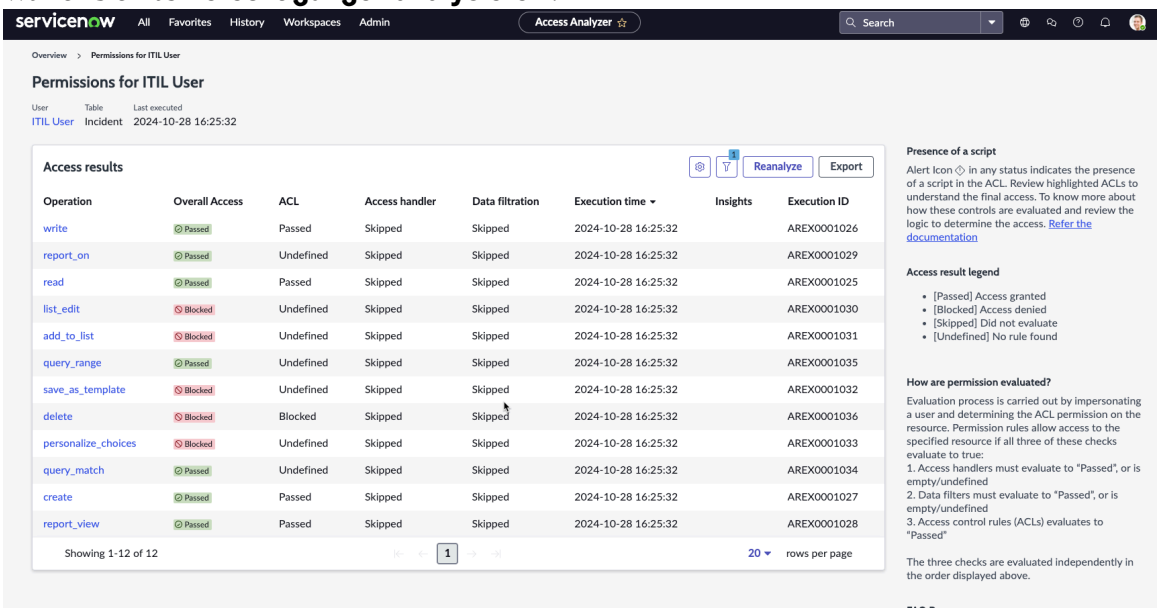
Feld	Beschreibung
Analysieren nach *	Wählen Sie **Benutzer** aus.
Wählen Sie Anwender * aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **ITIL-Anwender** .
Regeltyp *	Analysieren Sie den Zugriff für einen **Tabelle** , A **UI-Seite** , A **REST-Endpunkt** , Oder a **Vom Client aufrufbare Skripteinbindung** . Im Beispiel Tabelle .

Automatische Übersetzung

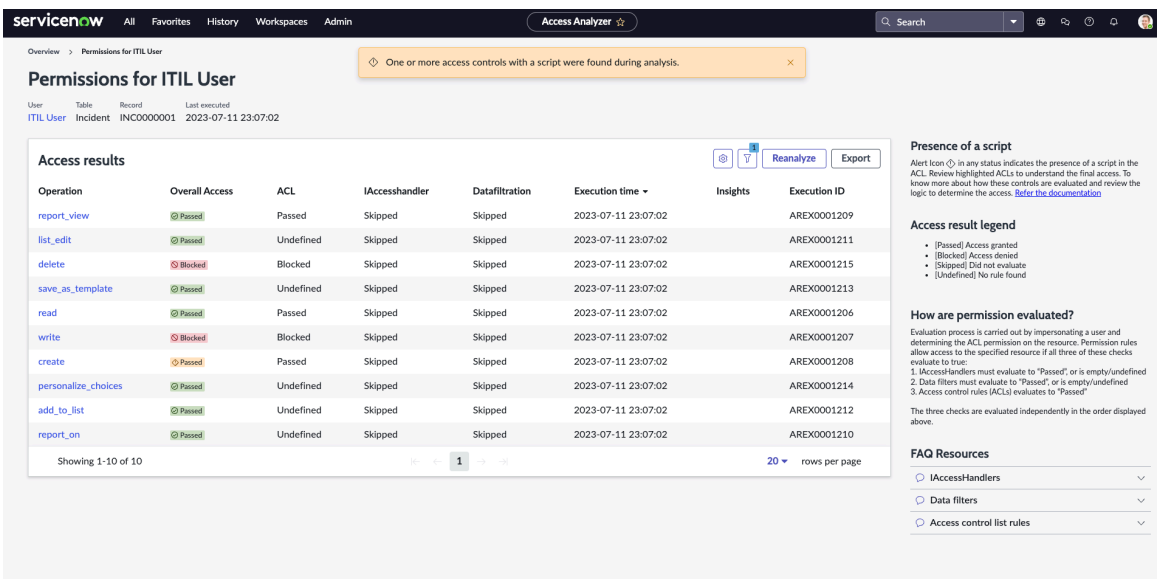
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wählen Sie Tabelle * aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident** .
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **INC0000001** .
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll. Dieses Feld kann verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel aktiv, erstellt von usw.

3. Geben Sie die Beschreibung in an **Beschreibung** Feld.
4. Wählen Sie Aus **Berechtigungen analysieren** .



Die **Greifen Sie auf Ergebnisse zu** Für **ITIL-Anwender** Wird angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

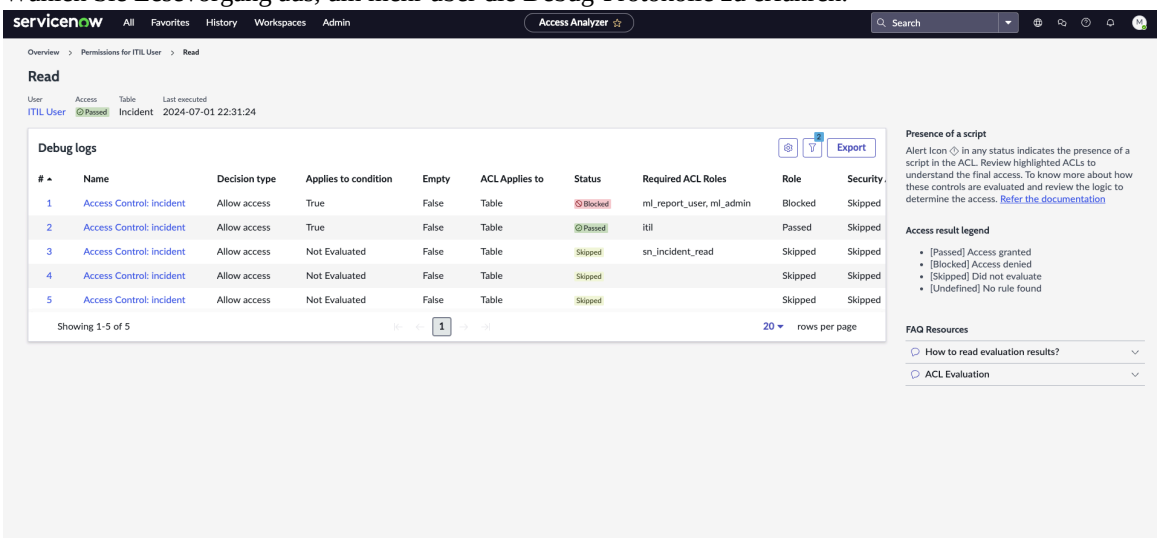
Die Ergebnisse können gelesen werden, indem Sie auf die Filter Legenden, Zugriffssteuerungsliste (ACL), IAccesshandler und Daten verweisen.

Nehmen wir das Beispiel von **Lesen** Vorgang. Für **ITIL-Anwender** Der Gesamtzugriff wird übergeben, was bedeutet, dass der Anwender den Datensatz mit den richtigen Berechtigungen (ACL) lesen kann.

Ähnlich für **Erstellen** Vorgang, wird der Gesamtzugriff mit einem Warnungssymbol übergeben, was bedeutet, dass ein Skript für die ACL-Auswertung vorhanden sein könnte.

Hinweis: Im Beispiel **Schreiben** Und **Löschen** Vorgänge sind für den ausgewählten Anwender blockiert, und der Anwender kann den ausgewählten Datensatz (INC0000001) nicht bearbeiten oder löschen.

5. Wählen Sie Lesevorgang aus, um mehr über die Debug-Protokolle zu erfahren.



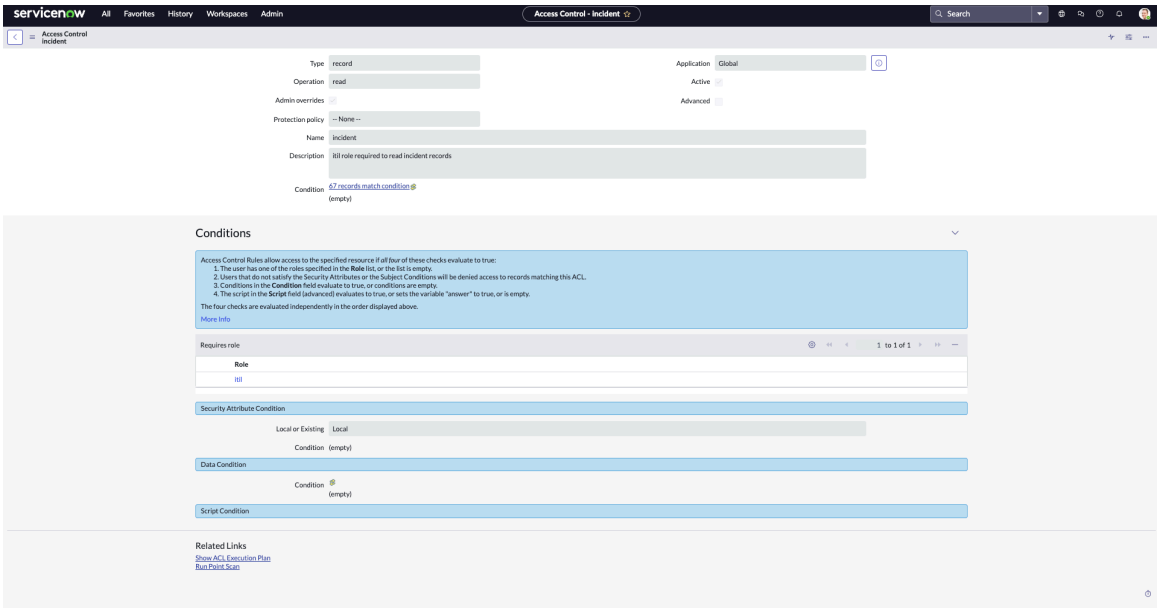
Auf der Seite „Debug-Protokolle“ wurden die Business-Regel und die zugehörigen ACLs angezeigt, die zum Ausführen von erforderlich sind **Lesen** Vorgang für den Datensatz.

Die Debug-Protokolle zeigen, dass dem Lesevorgang eine Business-Regel und 4 ACLs zugeordnet sind.

Es gibt einen Status **Bestanden** Für eine der ACL, d. h. zum Lesen des ausgewählten Datensatzes, verfügt der Anwender über die erforderliche ACL und kann den Datensatz lesen. Da eine der ACL ist **Bestanden** , Die anderen ACL-Auswertungen sind **Übersprungen** .

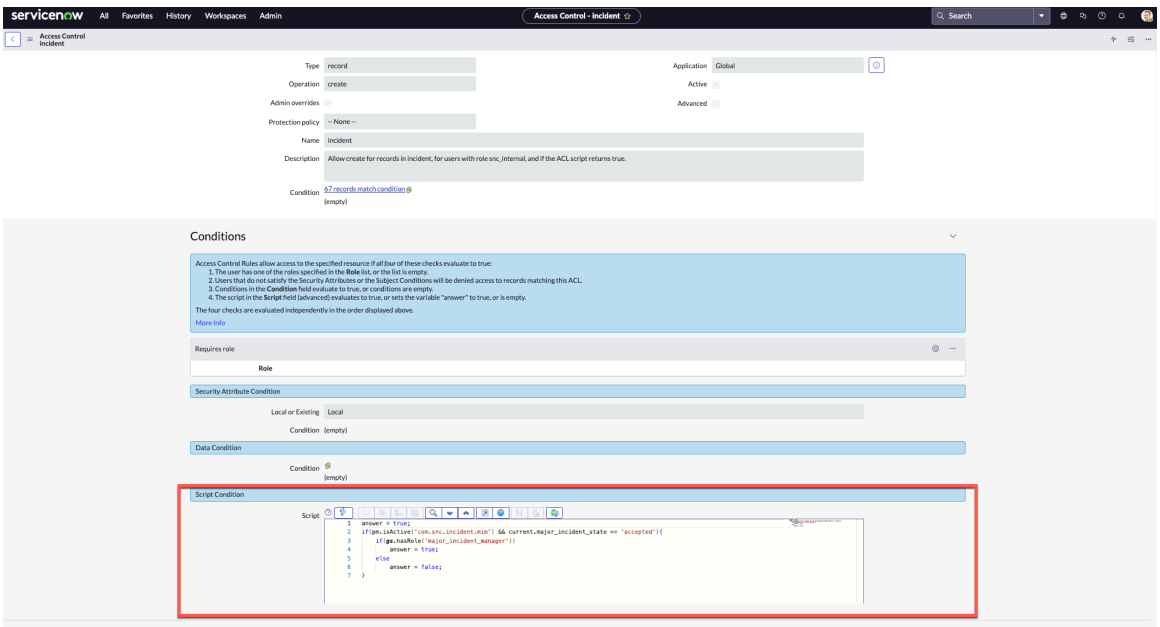
6. Wählen Sie die Zugriffssteuerung aus, die übergeben wird, um die Details der ACL zu erfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Details der Zugriffssteuerung für die ausgewählte ACL werden angezeigt.

Für einen ausgewählten Vorgang mit **Bestanden** Und Vorhandensein eines Skripts. Auf der Seite „Zugriffssteuerung“ wird das zugehörige Skript für den Datensatz angezeigt.



Zeigen Sie Berechtigungen für eine Rolle an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für eine ausgewählte Rolle anzuzeigen.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Das folgende Verfahren beschreibt die Beispielschritte zum Anzeigen von Berechtigungen für eine ausgewählte Rolle (**User_admin**), um die Berechtigung für einen REST API-Endpunkt mithilfe des Auswertungszugriffs in der Zugriffsanalyse anzuzeigen.

Hinweis: Zugriffsanalyse ist ein ServiceNow® Store-Produkt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

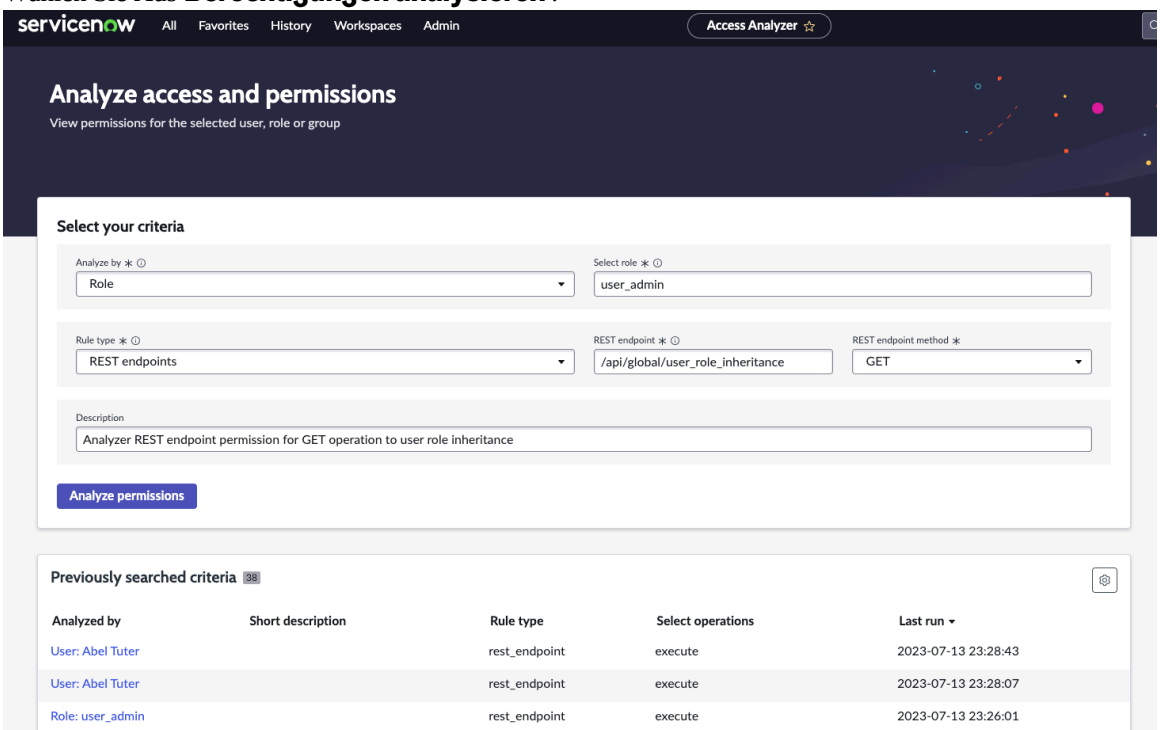
Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Wählen Sie Aus **Rolle** .
Wählen Sie Anwender * aus	Geben Sie eine Rolle an, die aus der Liste ausgewählt werden soll. Beispiel: **User_admin** .
Regeltyp *	Analysieren Sie den Zugriff auf eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung. Beispiel: **REST-Endpunkt** .
REST-Endpunkt*	Geben Sie einen REST-Endpunkt an. Beispiel: `/api/global/user_role_inheritance` . **Hinweis:** Der vollständige REST-Endpunkt muss verwendet werden, wenn das Feld ausgewählt verwendet wird.
REST-Endpunktmethode *	Geben Sie eine REST-Endpunktmethode an. Beispiel: GET.

3. Geben Sie die Beschreibung in an **Beschreibung** Feld.
4. Wählen Sie Aus **Berechtigungen analysieren** .



Die **Greifen Sie auf Ergebnisse zu** Für **User_admin** Rolle wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Ergebnisse können gelesen werden, indem Sie auf die Filter Legenden, Zugriffssteuerungsliste (ACL), IAccesshandler und Daten verweisen.

Der Gesamtzugriff für die Rolle wird übergeben, was bedeutet, dass die Rolle (**User_admin**) Kann auf zugreifen **REST-Endpunkt** Für den ausgewählten **ABRUFEN** Methode.

Zeigen Sie Berechtigungen für eine Gruppe an

Verwenden Sie die Zugriffsanalyse, um Berechtigungen für eine ausgewählte Gruppe anzuzeigen.

Vorbereitungen
Erforderliche Rolle: admin, Access_Analyzer_admin

Das folgende Verfahren beschreibt die Beispielschritte zum Anzeigen von Berechtigungen für eine ausgewählte Gruppe (**Incident-Management**), um die Berechtigungen von anzuzeigen **Incident-UI** Seite, die den Zugriff in der Zugriffsanalyse auswerten verwendet.

Hinweis: Zugriffsanalyse ist ein ServiceNow® Store-Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

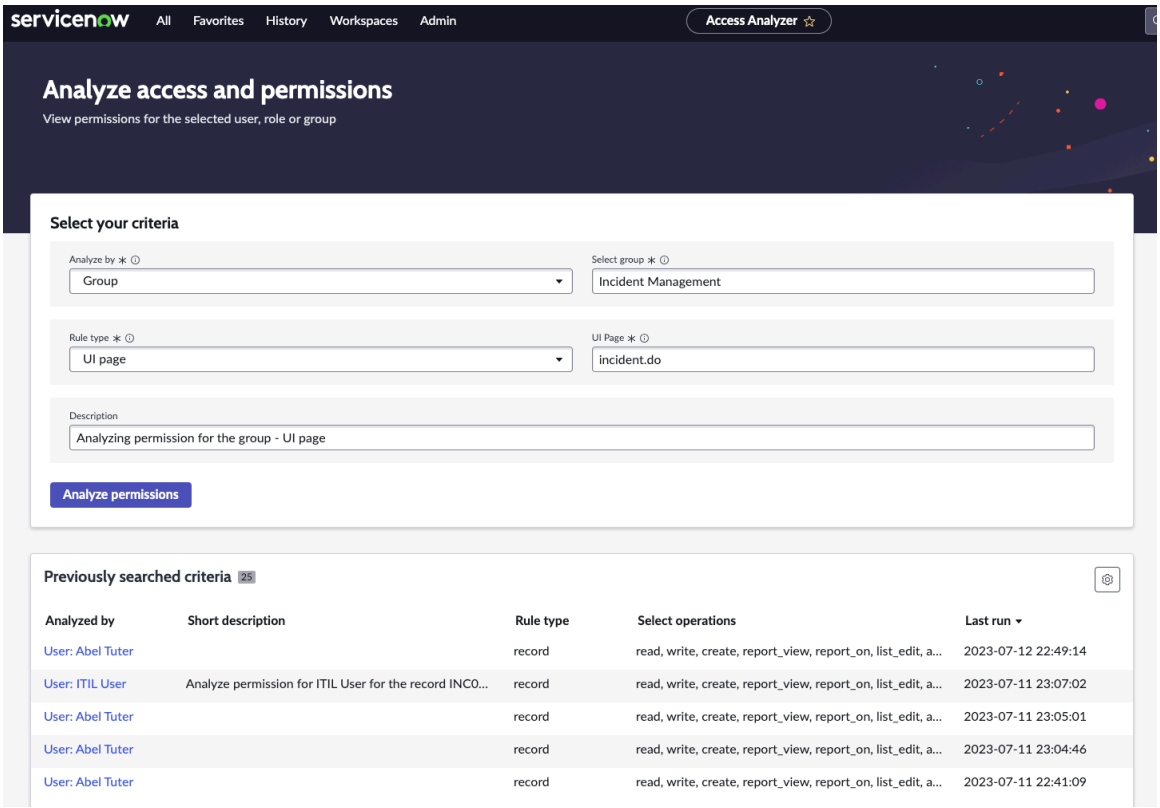
Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Wählen Sie Aus **Gruppe** .
Wählen Sie Anwender * aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll. Beispiel: **Incident-Management** .
Regeltyp *	Analysieren Sie den Zugriff auf eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung. Beispiel: **UI-Seite** .
UI-Seite *	Geben Sie die UI-Seite an. Beispiel: **Incident.tun** .

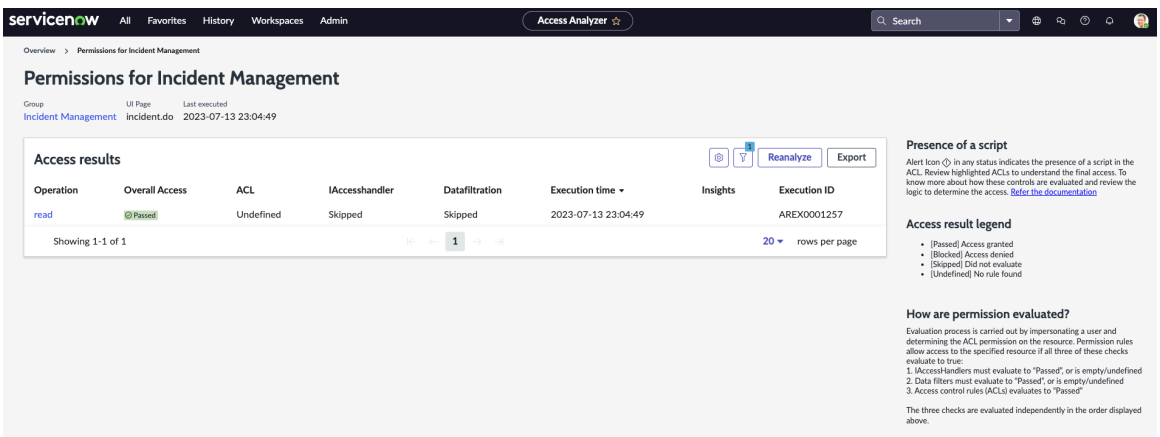
3. Geben Sie die Beschreibung in an **Beschreibung** Feld.
4. Wählen Sie Aus **Berechtigungen analysieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die **Greifen Sie auf Ergebnisse zu** Für **Incident-Management** Gruppe wird angezeigt.



Die Ergebnisse können gelesen werden, indem Sie auf die Filter Legenden, Zugriffssteuerungsliste (ACL), IAccesshandler und Daten verweisen.

Der Gesamtzugriff für die Gruppe wird übergeben, d. h. die Anwender innerhalb der Gruppe (**Incident-Management**) Können auf den Incident-Datensatz zugreifen.

Zugriffsanalyseabfragen exportieren

Exportieren Sie die mit der Zugriffsanalyse analysierten Abfragen.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Im folgenden Verfahren werden die Schritte für den Zugriff auf die Zugriffsanalyse und die Verwendung verschiedener Funktionen in der Zugriffsanalyse beschrieben.

Hinweis: Zugriffsanalyse ist ein ServiceNow® Store-Produkt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

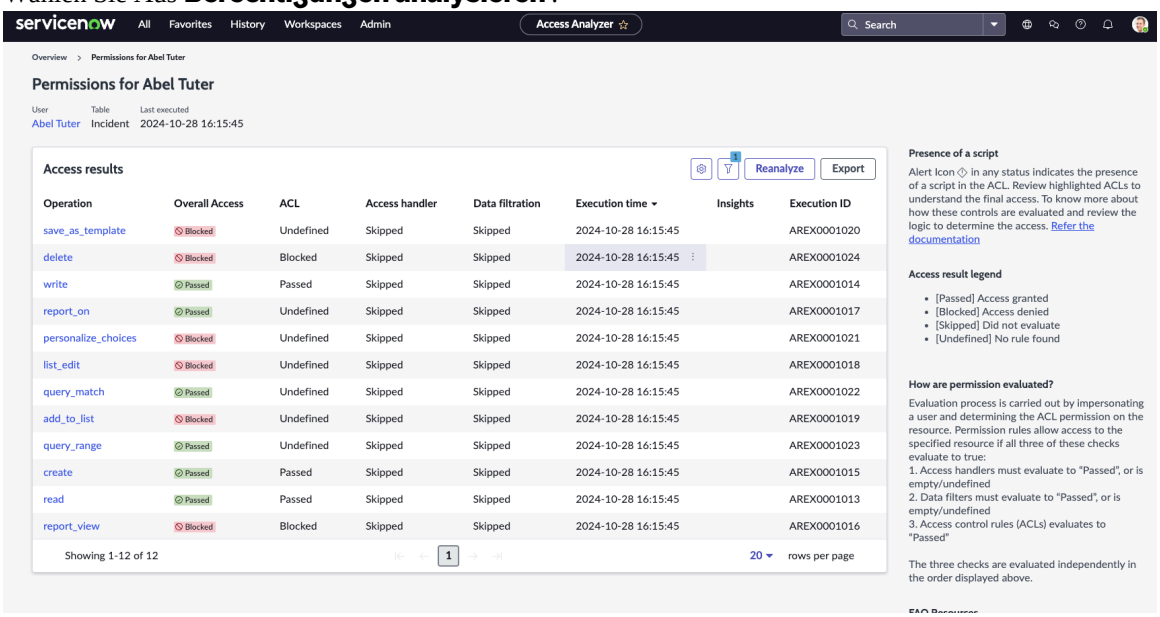
Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie Ihre Kriterien wie folgt aus:

Wählen Sie Ihre Kriterien für die Analyse von Zugriff und Berechtigungen aus

Feld	Beschreibung
Analysieren nach *	Analysieren Sie den Zugriff für einen Anwender, eine Rolle oder eine Gruppe
Wählen Sie Anwender * aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll.
Regeltyp *	Analysieren Sie den Zugriff auf eine Tabelle, eine UI-Seite, einen REST-Endpunkt oder eine vom Client aufrufbare Skripteinbindung.
Wählen Sie Tabelle * aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll.
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll.
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll.

3. Geben Sie die Beschreibung in an **Beschreibung** Feld.
4. Wählen Sie Aus **Berechtigungen analysieren** .



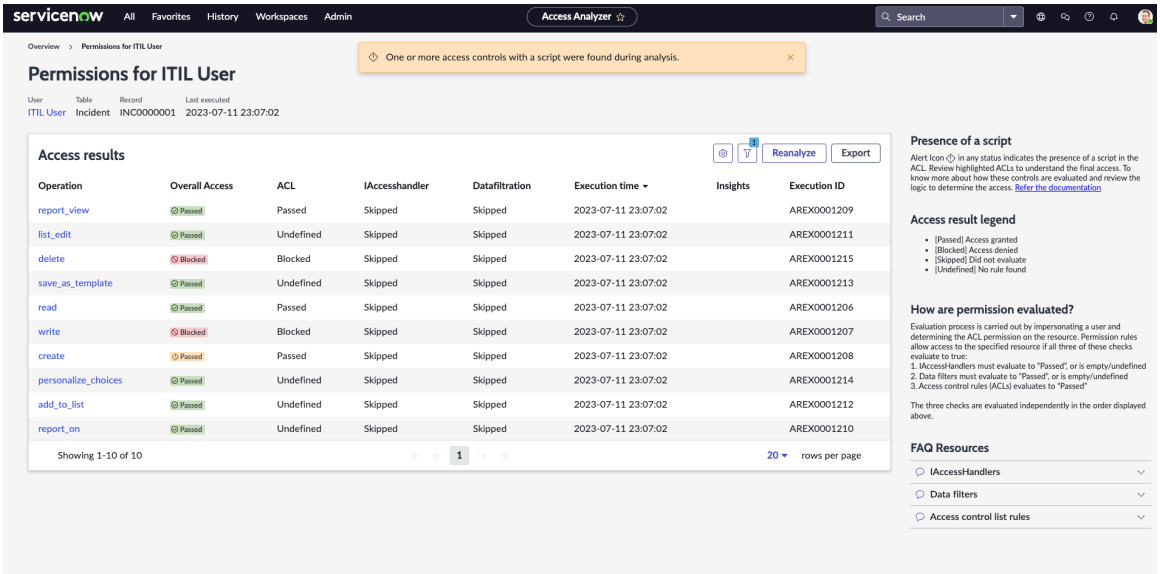
Die Zugriffsergebnisse für den Anwender werden angezeigt. Auf ähnliche Weise können Sie die Berechtigungen einer Gruppe oder Rolle für die folgenden Regeltypen analysieren:

- Tabelle (Datensatz)
- Vom Client aufrufbare Skripteinbindung
- REST-Endpunkte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

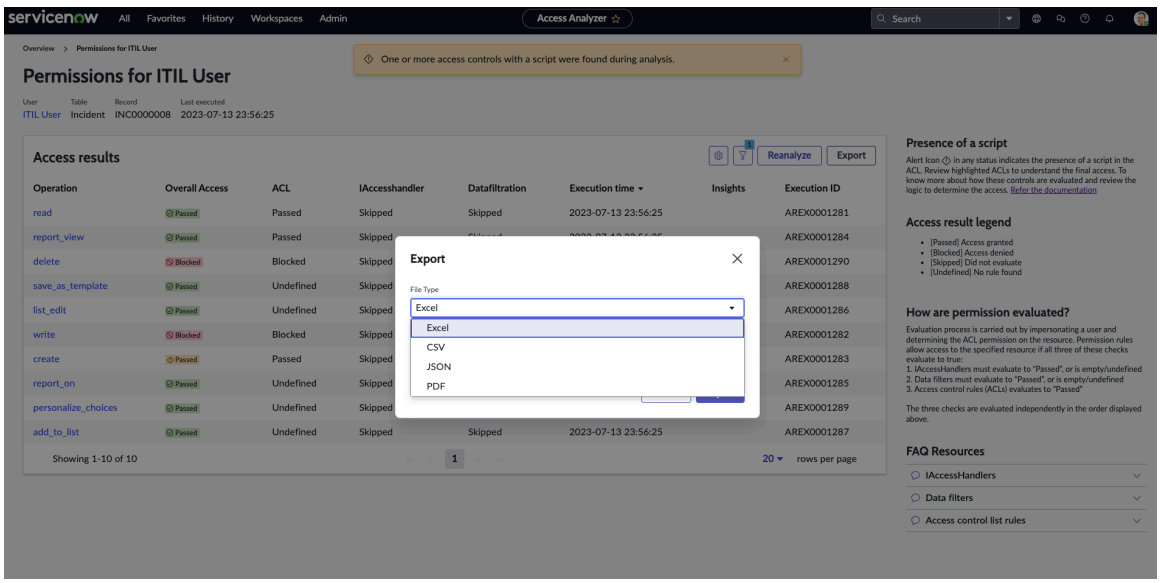
Die **Greifen Sie auf Ergebnisse zu** Für den ausgewählten Regeltyp wird angezeigt.



5. Klicken Sie auf **Exportieren**.

a. Wählen Sie den Dateityp aus.

Verfügbare Dateitypen sind Excel, CSV, JSON, PDF.

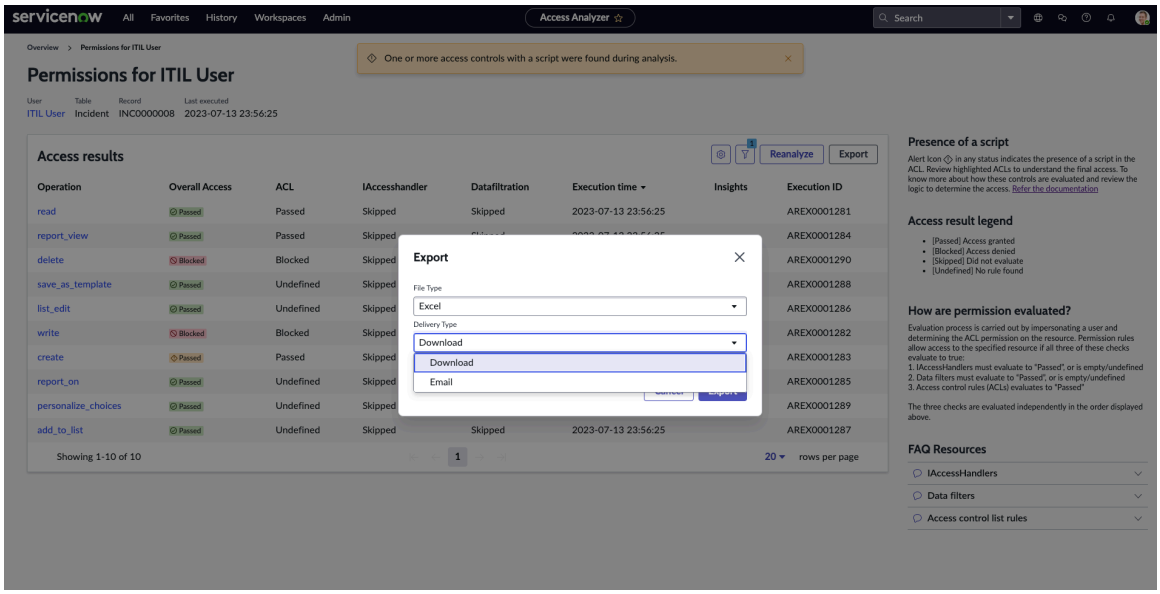


b. Wählen Sie den Liefertyp aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Liefertypen wie Download und E-Mail.



Vergleichen von Anwenderdatensätzen

Vergleichen Sie Anwenderdatensätze, um den Zugriff zwischen zwei Anwendern zu verstehen.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Im folgenden Verfahren werden die Schritte zum Vergleich von Anwenderdatensätzen mit der Zugriffsanalyse beschrieben.

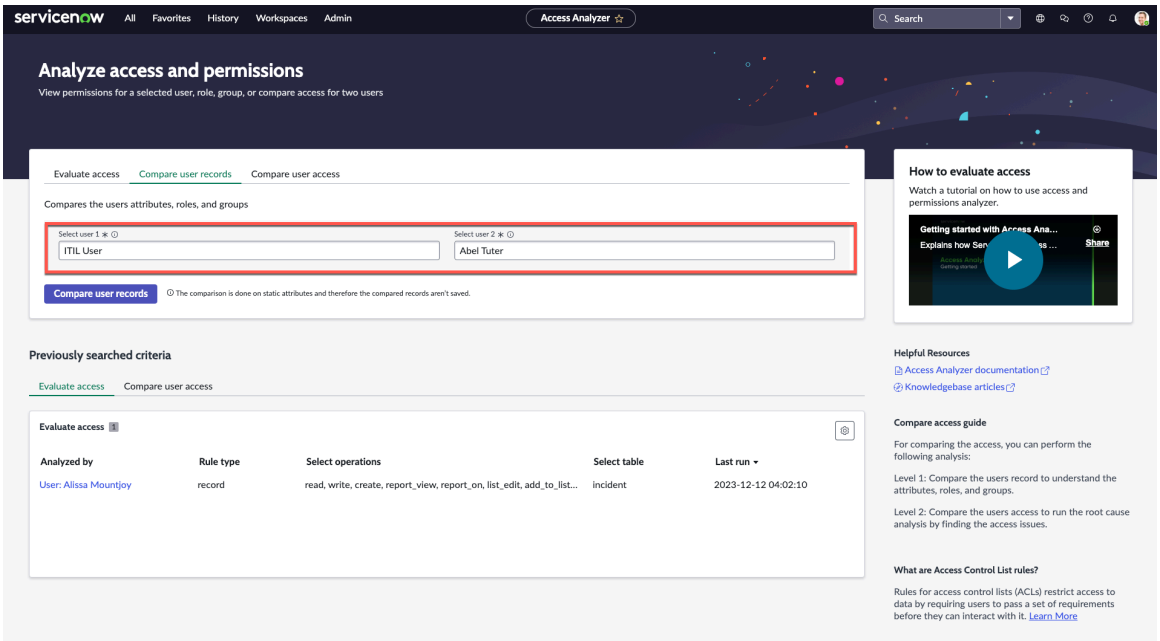
Hinweis: Zugriffsanalyse ist ein ServiceNow® Store Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie aus **Vergleichen Sie Anwenderdatensätze** Registerkarte.
3. Wählen Sie Aus **Anwender 1** Und **Anwender 2** Zum Vergleich.

   Beispiel: ITIL-Anwender Als **Anwender 1** Und Abel Tuter Als **Anwender 2** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



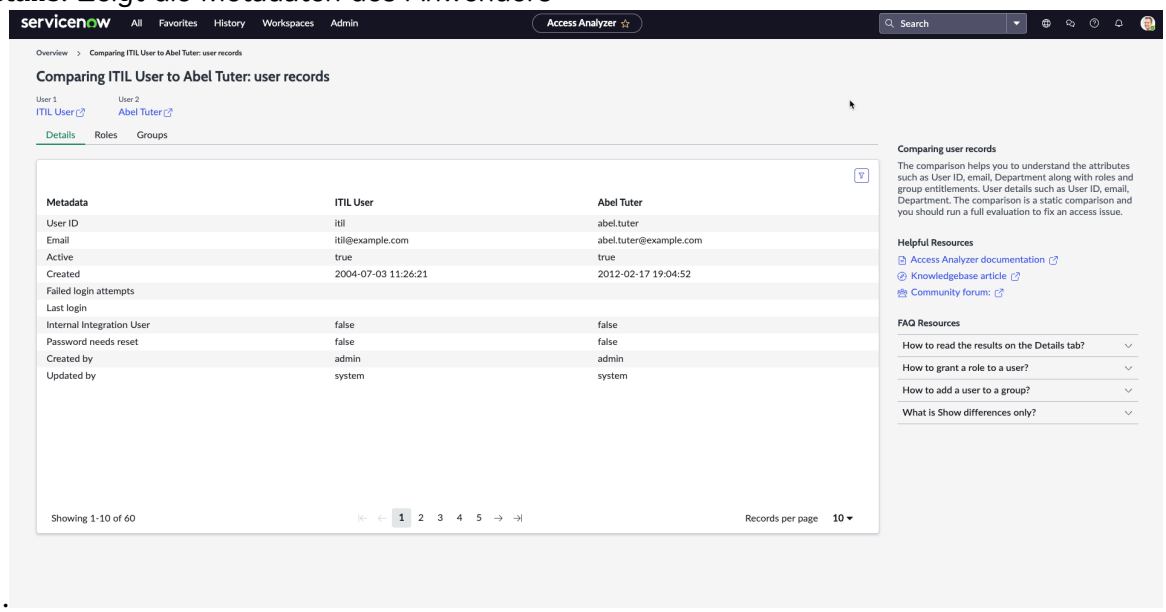
4. Wählen Sie Aus **Vergleichen Sie Anwenderdatensätze** .

   Die Ergebnisse werden mit den folgenden Registerkarten angezeigt:

Automatische Übersetzung

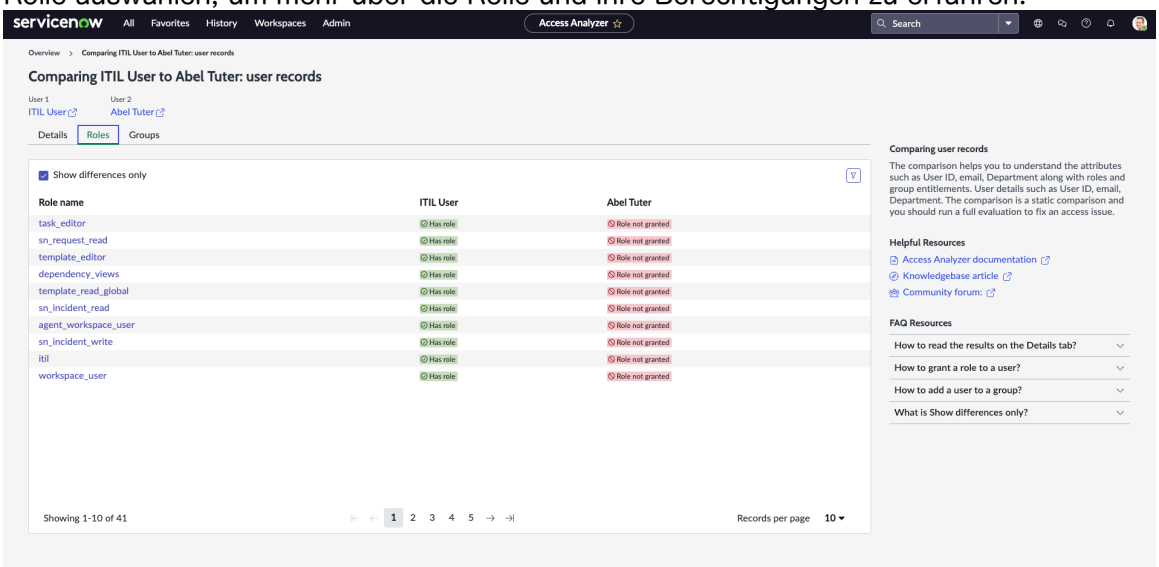
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Details**: Zeigt die Metadaten des Anwenders



an.

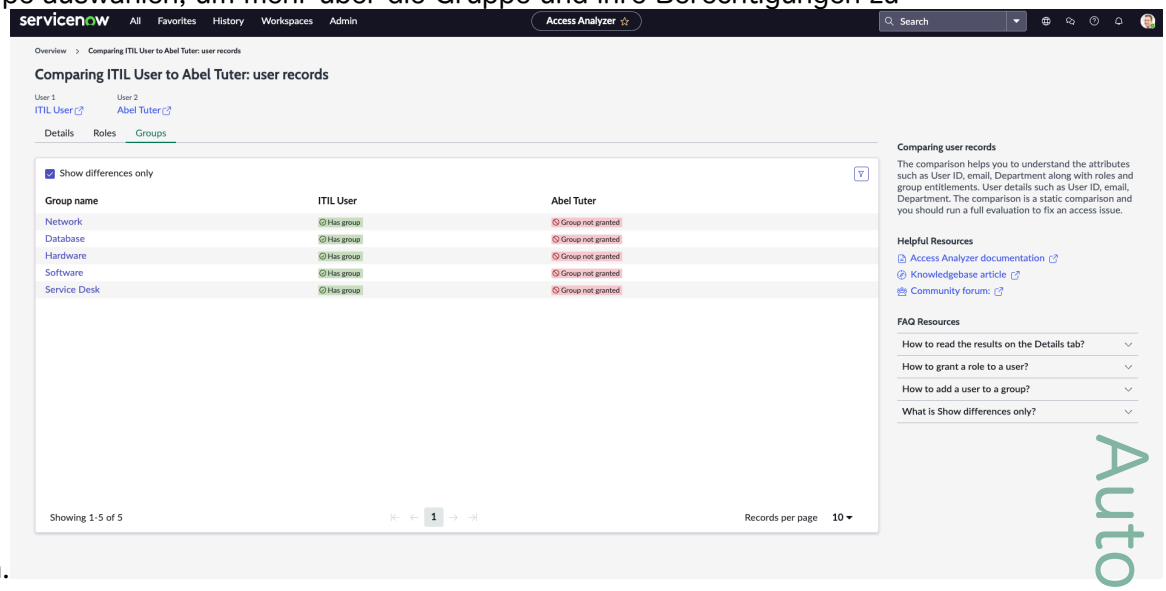
- **Rollen**: Zeigt die Rollen an, die dem Anwender zugewiesen sind. Sie können die Rolle auswählen, um mehr über die Rolle und ihre Berechtigungen zu erfahren.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Gruppen**: Zeigt die Gruppen an, die dem Anwender zugewiesen sind. Sie können die Gruppe auswählen, um mehr über die Gruppe und ihre Berechtigungen zu erfahren.



Auf ähnliche Weise können Sie verschiedene Anwender in vergleichen ServiceNow Instanz, um den Zugriff zu verstehen, der den Anwendern zugewiesen ist.

Vergleich des Anwenderzugriffs

Vergleichen Sie die Zugriffssteuerung des Anwenders mit der Zugriffsanalyse.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Im folgenden Verfahren werden die Schritte zum Vergleich der Zugriffssteuerung zwischen den Anwendern mit der Zugriffsanalyse beschrieben.

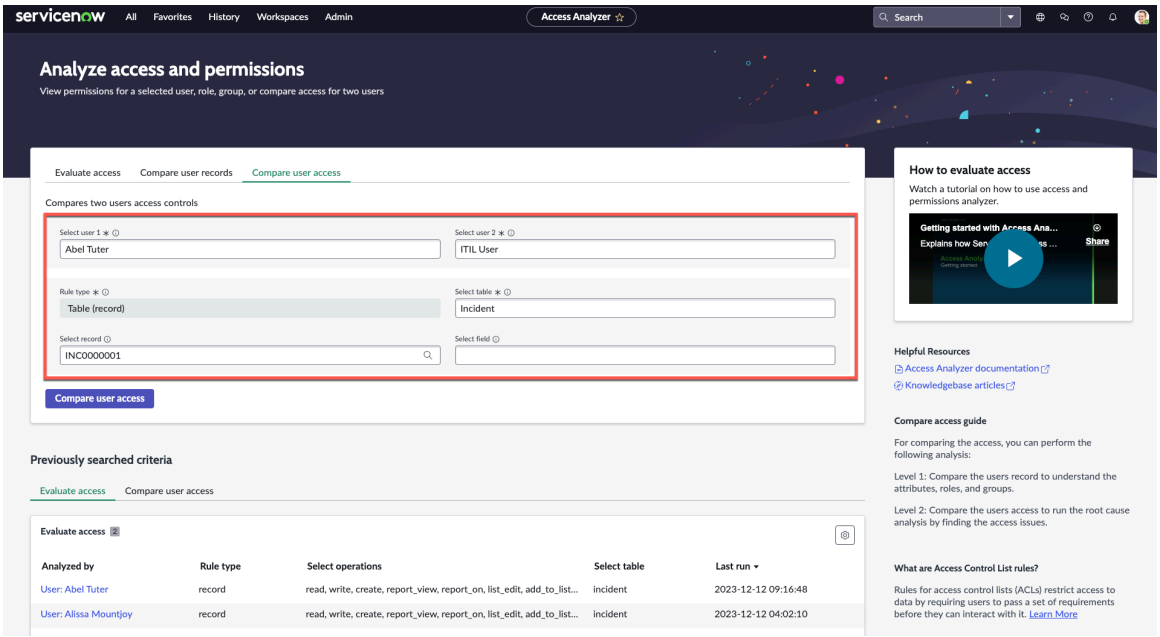
Hinweis: Zugriffsanalyse ist ein ServiceNow® Store Produkt.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie aus **Vergleichen Sie den Anwenderzugriff** Registerkarte.
3. Füllen Sie folgende Felder aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Anwenderzugriff vergleichen

Feld	Beschreibung
Wählen Sie Anwender 1* aus	Geben Sie einen Anwendernamen an, der aus der Liste für den Vergleich ausgewählt werden soll.
Wählen Sie Anwender 2* aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll, um ihn mit dem Anwender zu vergleichen 1.
Regeltyp*	Analysieren Sie Zugriffsberechtigungen für eine Tabelle. **Hinweis:** In können nur Zugriffsberechtigungen für eine Tabelle verwendet werden **Vergleichen Sie den Anwenderzugriff** .
Wählen Sie Tabelle* aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll.
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll.
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll.

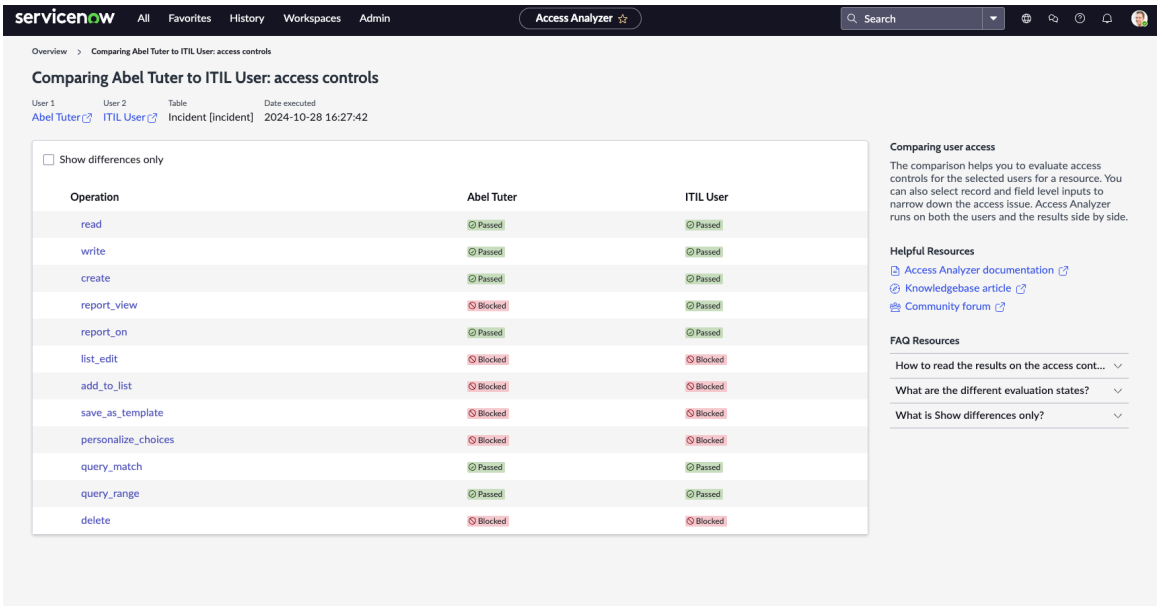
4. Wählen Sie Aus **Vergleichen Sie den Anwenderzugriff** .

   Die **Vergleichen Sie den Anwenderzugriff** Ergebnisse für die ausgewählten Anwender werden angezeigt.

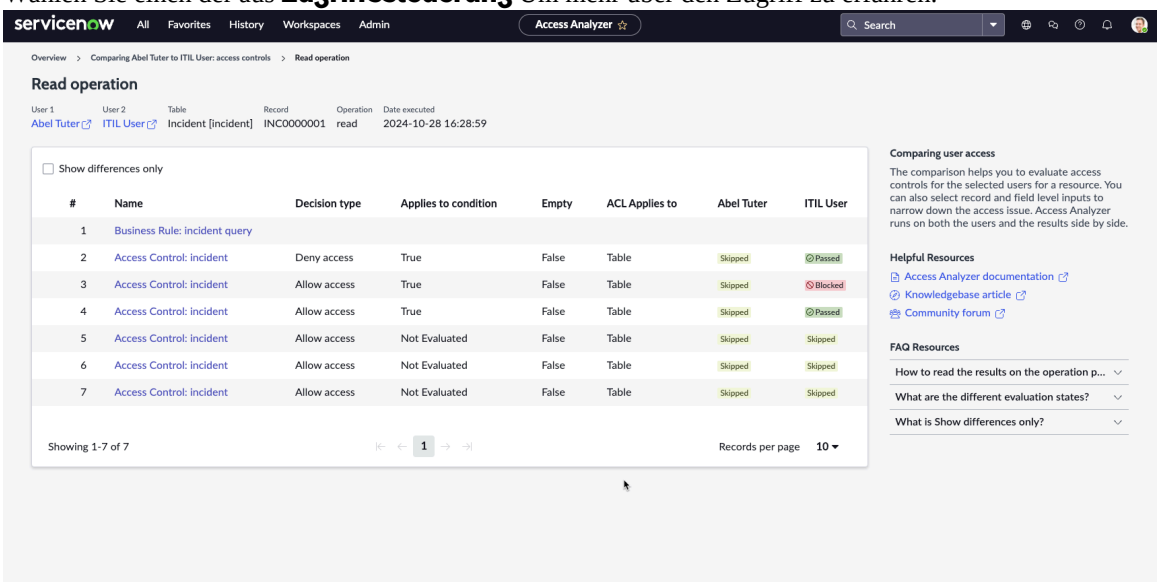
   Die Ergebnisse des Vergleichs des Anwenderzugriffs zeigen den Vorgang und den Status der Zugriffsauswertung für die Anwender an. Beispiel: Abel Tuter und ITIL-Anwender.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

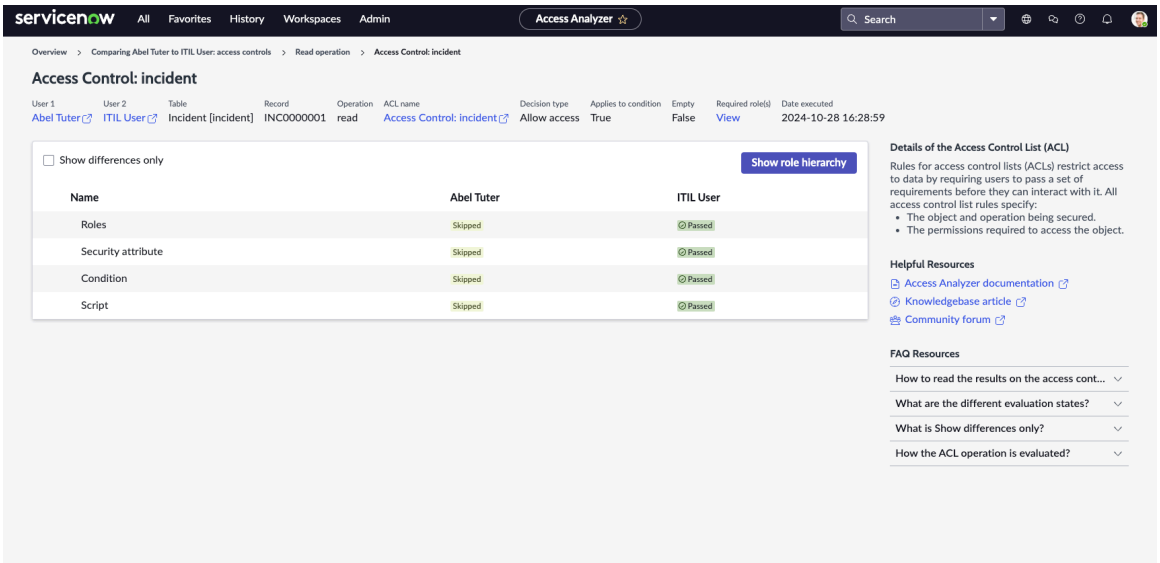


5. Wählen Sie den Vorgang aus, um mehr über die Berechtigungsauswertung und die Rollen zu erfahren, denen die Anwender zugewiesen sind.
   Beispiel: **Lesen** Vorgang.
6. Wählen Sie einen der aus **Zugriffssteuerung** Um mehr über den Zugriff zu erfahren.



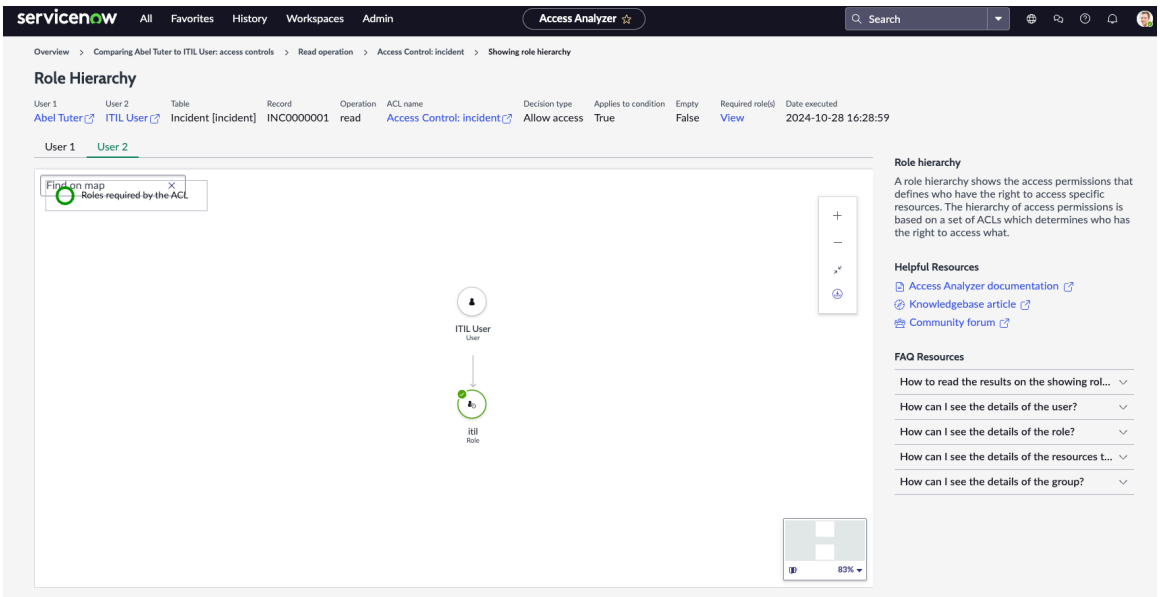
Die Zugriffssteuerungsdetails wie Rollen, Sicherheitsattribut, Bedingung und Skriptauswertungsstatus werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Wählen Sie Aus **Rollenhierarchie anzeigen** Um mehr über die Rollen und Gruppen zu erfahren, denen der Anwender zugewiesen ist, und beide Anwender zu vergleichen.

Basierend auf der Rollenhierarchie können Sie dem Anwender die erforderlichen Rollen- und Gruppenzuweisungen zuweisen, um Zugriff auf die Ressourcen (Tabelle) zu haben.



Im Beispiel **Abel Tuter** Hat nicht itil Zugewiesen. Sie können die erforderlichen Rollen- und Gruppenzuweisungen für den Anwender bestimmen, indem Sie sich die Rollenhierarchie ansehen.

Sie können den Knoten auswählen, um mehr über die Rolle, die Ressourcen, auf die die Rolle zugreifen kann, oder die Gruppe zu erfahren.

Anzeigen der zuvor gesuchten Kriterien in der Zugriffsanalyse

Zeigen Sie die zuvor gesuchten Kriterien in der Zugriffsanalyse an.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Hinweis: Zugriffsanalyse ist ein ServiceNow® Store Produkt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

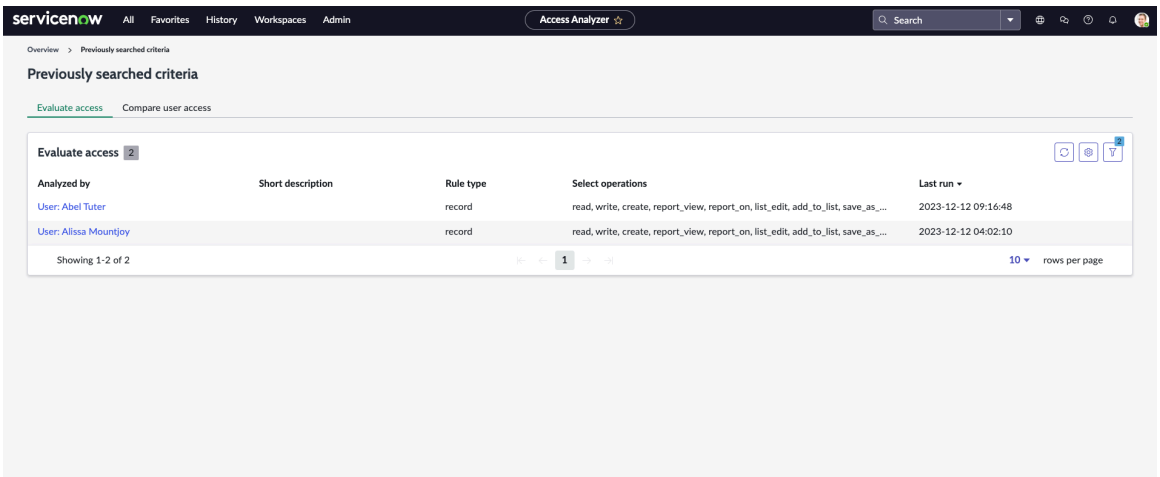
Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Abfragen der Zugriffsanalyse**an.

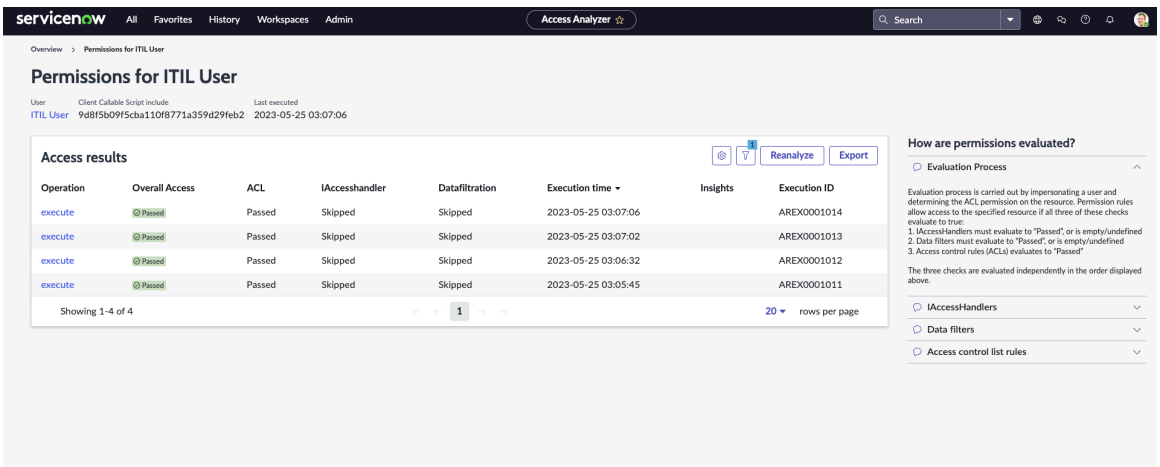
   Zuvor gesuchte Kriterien haben die folgenden Abschnitte:

   - **Zugriff bewerten** : Zeigt Ergebnisse basierend auf Abfragen an, die über durchgeführt wurden **Zugriff bewerten** Funktionen.
   - **Vergleichen Sie den Anwenderzugriff** : Zeigt Ergebnisse basierend auf Abfragen an, die über durchgeführt wurden **Vergleichen Sie den Anwenderzugriff** Funktionen.

   Hinweis: Die zuvor gesuchten Kriterien werden bei Verwendung der Funktion „Anwenderdatensätze vergleichen“ nicht gespeichert.



2. Wählen Sie aus **Analysiert von** Links zum Anzeigen zuvor gesuchter Kriterien im Abschnitt „Zugriff bewerten“.

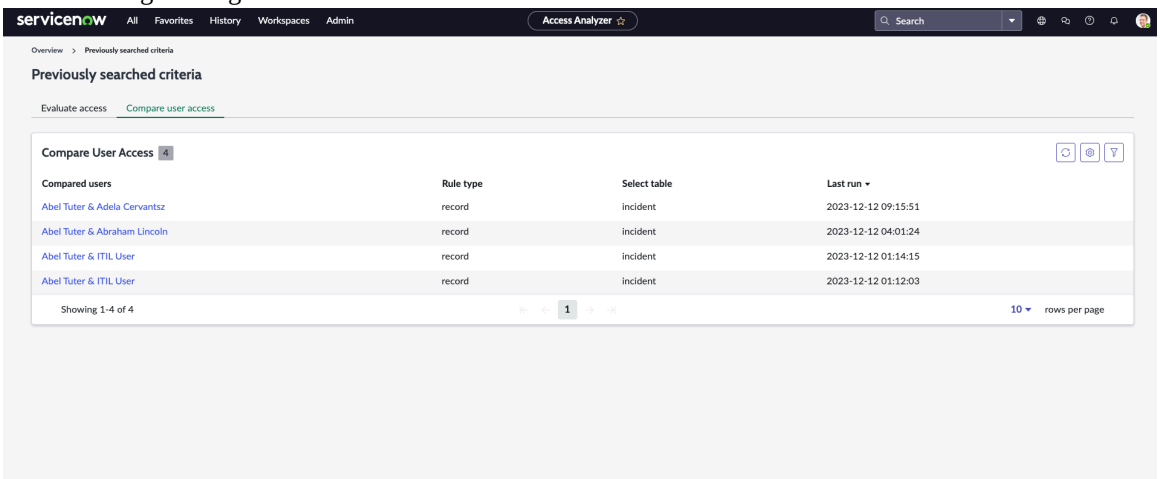


Sie können auswählen **Erneut Analysieren** Der Zugriff für den Anwender. Exportieren Sie die Details mit **Exportieren** Option.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie aus **Anwender verglichen** Links zum Anzeigen der zuvor gesuchten Kriterien im Abschnitt Anwenderzugriff vergleichen.



Berechtigungsauswertung

Kriterien für Berechtigungsauswertung bei Verwendung der Zugriffsanalyse.

Auswertungshierarchie

Die Berechtigung für den ausgewählten Anwender, die ausgewählte Gruppe oder die ausgewählte Rolle wird in der folgenden Hierarchie ausgewertet:

- Business-Regel: Eine Business-Regel ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder wenn eine Tabelle abgefragt wird.
- Zugriffs-Handler: Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform.
- Datenfiltration: Datenfilter ist eine Form der Zugriffssteuerung, die mit den vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz kompatibel ist. Datenfilter unterstützen nur Lesevorgänge.
- Zugriffssteuerungsliste (ACL): Regeln für Zugriffssteuerungslisten (ACLs) beschränken den Zugriff auf Daten, indem sie von Anwendern verlangen, eine Reihe von Anforderungen zu erfüllen, bevor sie mit ihnen interagieren können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet:
  - Rolle
  - Sicherheitsattribut
  - Bedingung
  - Skript

Mit der Zugriffsanalyse können Sie Zugriff und Berechtigungen für den ausgewählten Anwender, die ausgewählte Rolle oder die Gruppe analysieren. Die Berechtigungen werden basierend auf den folgenden Regeltypen ausgewertet:

- **Auswertung Auf Tabellenebene** : Rollen- und Sicherheitsattribut-ACLs werden für die Auswertung auf Tabellenebene verwendet.
- **Auswertung auf Datensatz- oder Feldebene** : ACLs für Rollen, Sicherheitsattribut, Bedingung und Skriptebene werden für die Auswertung auf Datensatz- oder Feldebene verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **UI-Seite** : Support nur bereit-Vorgänge. Nur ACLs auf Leseebene werden ausgewertet.
- **REST-Endpunkt** : Ausführungsvorgang nur unterstützen. Nur ACL auf Ausführungsebene wird ausgewertet.

Details zu den wichtigen Feldern in den Zugriffsergebnissen:

- Vorhandensein eines Skripts
- Auf die Ergebnislegende zugreifen
- Auswertungsvorgang
- IAccessHandler
- Datenfilter
- Regeln der Zugriffssteuerungsliste

Vorhandensein eines Skripts

Das Warnungssymbol in einem beliebigen Status gibt das Vorhandensein eines Skripts in der ACL an. Überprüfen Sie die hervorgehobenen ACLs, um den endgültigen Zugriff zu verstehen. Weitere Informationen zur Auswertung dieser Steuerungen und zur Bestimmung des Zugriffs finden Sie unter Debugging-Protokolle der Zugriffsanalyse.

Legende in Zugriffsanalyse

Bei der Analyse des Zugriffs und der Berechtigungen werden Legenden als Teil des Auswertungsprozesses angezeigt. Im Folgenden finden Sie die Legenden:

- [Bestanden] Zugriff gewährt
- [Blockiert] Zugriff verweigert
- [Übersprungen] Wurde nicht ausgewertet
- [Nicht definiert] Keine Regel gefunden

Auswertungsvorgang

Der Bewertungsprozess wird durchgeführt, indem die Identität eines Anwenders angenommen und die Zugriffssteuerungslistenberechtigung (ACL) für die Ressource bestimmt wird. Berechtigungsregeln ermöglichen den Zugriff auf die angegebene Ressource, wenn die folgenden Prüfungen als „wahr“ ausgewertet werden:

- IAccessHandler müssen als „Bestanden“ ausgewertet werden, sind leer oder nicht definiert
- Datenfilter müssen als „bestanden“ ausgewertet werden, sind leer oder nicht definiert
- Zugriffssteuerungsregeln (ACLs) werden als „bestanden“ ausgewertet.

IAccessHandler

Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. IAccessHandler kann den Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn IAccessHandler ignoriert wird, werden die ACLs ausgewertet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die IAccessHandler-Prüfungen nicht ändern. Beispielsweise wird eine IAccessHandler-Implementierung für Zugriffsprüfungen für Anwendungsressourcen wie Lesezugriff verwendet.

Datenfilter

Der Datenfilter ist eine Form der Zugriffssteuerung, die auf die vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz abgestimmt ist.

Regeln der Zugriffssteuerungsliste

Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Häufige Fragen

Häufig gestellte Fragen bei der Verwendung der Zugriffsanalyse.

Zugriff Auswerten

Im Folgenden finden Sie einige der häufig gestellten Fragen bei der Verwendung der Funktion „Zugriff bewerten“ in der Zugriffsanalyse:

Häufige Fragen

Fragen	Erklärung
Wie werden die Auswertergebnisse gelesen, die von der Zugriffsanalyse angezeigt werden?	Jede Zeile stellt eine individuelle Zugriffssteuerungsliste (ACL) dar. Die Sequenz (#) in den Ergebnissen die Reihenfolge, in der ACLs ausgewertet werden. Der Status zeigt an, ob der Gesamtzugriff gewährt (bestanden) oder verweigert (blockiert) wird.
Wie werden ACLs ausgewertet?	Auf Tabellenebene werden ACLs nur für Rollen und Sicherheitsattribute ausgewertet, Bedingungen und Skripts werden nicht ausgewertet. Rollen werden zuerst ausgewertet. Wenn Rollen blockiert sind, werden Bedingungen und Skripts übersprungen. Weitere Informationen finden Sie unter Konfigurieren Sie eine ACL-Regel.
Was sind die Legenden in der Zugriffsanalyse?	Bei der Analyse des Zugriffs und der Berechtigungen werden Legenden als Teil des Auswertungsprozesses angezeigt. Es folgen die Legenden: • [Bestanden] Zugriff gewährt • [Blockiert] Zugriff verweigert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen (Fortsetzung)

Fragen	Erklärung
	• [Übersprungen] wurde nicht ausgewertet • [Nicht definiert] Keine Regel gefunden
Was bedeutet das Warnungssymbol in den Zugriffsergebnissen?	Das Warnungssymbol in einem beliebigen Status gibt das Vorhandensein eines Skripts in der ACL an. Überprüfen Sie die hervorgehobenen ACLs, um den endgültigen Zugriff zu verstehen. Weitere Informationen zur Auswertung dieser Steuerungen und zur Bestimmung des Zugriffs finden Sie unter Debugging-Protokolle der Zugriffsanalyse.
Was ist **IAccesshandler** ?	Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform. Es handelt sich um eine Systemsicherheitsprüfung, die Sie nicht ändern können. **IAccessHandler** Kann Zugriff auf eine Ressource gewähren oder verweigern, ohne ACLs auszuwerten. Wenn dies der Fall ist **IAccessHandler** Wird ignoriert, werden die ACLs ausgewertet. Sie können den nicht ändern **IAccessHandler** Prüfungen in beliebiger Weise. Zum Beispiel ein **IAccessHandler** Die Implementierung wird für Zugriffsprüfungen auf Anwendungsressourcen verwendet, z. B. schreibgeschützten Zugriff.
Was sind Datenfilter?	Datenfilter sind eine Form der Zugriffssteuerung, die mit den vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz kompatibel ist.
Was ist eine ACL-Regel?	Regeln für Zugriffssteuerungslisten (ACLs) schränken den Zugriff auf Daten ein, indem sie von Anwendern die Erfüllung einer Reihe von Anforderungen verlangen, bevor sie mit der Interaktion beginnen können.

Für den Anwender gefundene zeitlich begrenzte Rollenzuweisungen, aufgrund derer die Ergebnisse beeinträchtigt werden können. Sie können hier die dem Anwender zugewiesenen zeitbegrenzten Rollen überprüfen.

Anwenderdatensätze vergleichen

Im Folgenden finden Sie einige der häufig gestellten Fragen bei der Verwendung der Funktion „Anwenderdatensatz vergleichen“ in der Zugriffsanalyse:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen

Fragen	Erklärung
Wie werden die Ergebnisse auf der Registerkarte „Details“ gelesen?	Auf der Registerkarte Details werden die Metadaten angezeigt, die dem Anwender 1 und Anwender 2 zugeordnet sind
Wie erteile ich einem Anwender eine Rolle?	Auf der Registerkarte Anwender können Sie die Rolle überprüfen, die dem Anwender gewährt werden muss, und diese Rolle zuweisen.
Wie füge ich einen Anwender einer Gruppe hinzu?	Auf der Registerkarte Gruppen können Sie die Gruppe überprüfen, die der Anwender hinzugefügt werden muss, und den Anwender zur Gruppe hinzufügen.
Was ist „nur Unterschied anzeigen“?	Wenn Sie das Kontrollkästchen nur Unterschiede anzeigen aktivieren, werden nur die Rollen oder Gruppen angezeigt, die sich zwischen Anwender 1 und Anwender 2 unterscheiden.

Anwenderzugriff vergleichen

Im Folgenden finden Sie einige der häufig gestellten Fragen bei der Verwendung der Funktion „Anwenderzugriff vergleichen“ in der Zugriffsanalyse:

Häufige Fragen

Fragen	Erklärung
Wie werden die Ergebnisse auf der Seite für Zugriffsvergleichsvorgänge gelesen?	Auf der Vergleichsseite der Zugriffssteuerung werden die Auswertungsstatus für verschiedene ACL-Vorgänge angezeigt.
Was sind die verschiedenen Auswertungsstatus?	Beim Vergleich der Zugriffssteuerungen zwischen den Anwendern sind die verschiedenen bewertungsstatus aufgeführt: • Bestanden • Blockiert
Was ist „nur Unterschiede anzeigen“?	Wenn Sie das Kontrollkästchen nur Unterschiede anzeigen aktivieren, wird nur der Bewertungsstatus des Vorgangs angezeigt, der sich zwischen Anwender 1 und Anwender 2 unterscheidet.
Wie wird der ACL-Vorgang ausgewertet?	Zugriffssteuerungsliste (Access Control List, ACL) ist die Regel für Zugriffssteuerungslisten (Access Control List, ACLs), die den Zugriff auf Daten einschränken, indem sie von Anwendern verlangt, eine Reihe von Anforderungen zu erfüllen, bevor sie mit ihnen interagieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen (Fortsetzung)

Fragen	Erklärung
	können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet: • Rolle • Sicherheitsattribut • Bedingung • Skript
Wie werden die Ergebnisse auf der Seite mit der angezeigten Rollenhierarchie gelesen?	Auf der Seite mit der Rollenhierarchie wird die Rolle angezeigt, die Anwender 1 und Anwender 2 zugewiesen ist. Sie können die Rolle verstehen, die für den Anwender für einen bestimmten ACL-Vorgang erforderlich ist.
Wie kann ich die Details des Anwenders anzeigen?	Sie können auswählen **Anwender (Knoten)** > **Weitere Aktionen** > **Zeigen Sie den Anwender an** Details, um mehr über den Anwender zu erfahren.
Wie kann ich die Details der Rolle anzeigen?	Sie können auswählen **Rolle (Knoten)** > **Weitere Aktionen** > **Rolle anzeigen** Details, um mehr über die Rolle zu erfahren.
Wie kann ich die Details der Ressourcen anzeigen, auf die die Rolle zugreifen kann?	Sie können auswählen **Rolle (Knoten)** > **Weitere Aktionen** > **Zeigen Sie alle Ressourcen an, auf die die Rolle Zugriff hat** Um die Ressourcen zu kennen, auf die die Rolle zugreifen kann.
Wie kann ich die Details der Gruppe anzeigen?	Sie können auswählen **Gruppe (Knoten)** > **Weitere Aktionen** > **Gruppe anzeigen** Details, um mehr über die Gruppe zu erfahren.

Debugging-Protokolle der Zugriffsanalyse

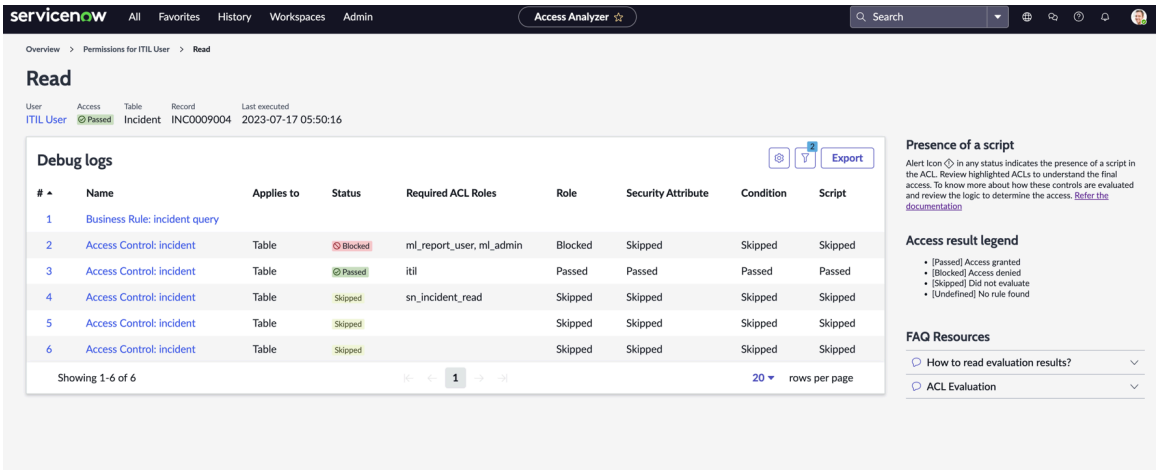
Debug-Protokolle zeigen die Details des Vorgangs „Zugriffsergebnis auswählen“ an.

Felder in Debug-Protokollen

Die Debug-Protokolle in der Zugriffsanalyse zeigen Informationen zum ausgewählten Vorgang an, um die mit dem Vorgang verknüpften Berechtigungen, Geschäftsregeln und ACLs zu verstehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Folgenden finden Sie die Felder und ihre Beschreibung in den Debug-Protokollen:

Protokolle debuggen

Felder	Beschreibung
Name	Die Details zur Business-Regel oder ACL. Sie können die Business-Regel der ACL auswählen, um weitere Informationen zu erhalten.
Betrifft	Die Details zur Anwendung von ACL auf Feld-, Datensatz- oder Tabellenebene.
Status	Status der ACL für die zugehörige Rolle und Berechtigung.
Erfordert ACL	Die Rolle, die für den Zugriff auf das Feld, den Datensatz oder die Tabelle erforderlich ist.
Rolle	Die Details zur Rolle, die für die Zugriffssteuerung blockiert, übergeben oder übersprungen wird.
Sicherheitsattribut	Die Details zum Sicherheitsattribut, das für die Zugriffssteuerung blockiert, übergeben und übersprungen wird.
Bedingung	Das Detail über die Bedingung, die für die Zugriffssteuerung blockiert, übergeben und übersprungen wird.
Skript	Die Details zum blockierten, übergebenen und übersprungenen Skript für die Zugriffssteuerung.
Angepasst	Die Details zur anwenderdefinierten ACL, falls vorhanden, für die Zugriffssteuerung.
Anwendung	Status der Anwendung. Global oder Store.

Auswertungshierarchie

Die Berechtigung für den ausgewählten Anwender, die ausgewählte Gruppe oder die ausgewählte Rolle wird in der folgenden Hierarchie ausgewertet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Business-Regel: Eine Business-Regel ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder wenn eine Tabelle abgefragt wird.
- Zugriffs-Handler: Eine interne Systemprüfung mit ausgeblendetem Quellcode auf der Plattform.
- Datenfilterung: Ein Datenfilter ist eine Form der Zugriffssteuerung, die mit den vorhandenen Zugriffssteuerungsregeln (ACLs) in Ihrer Instanz kompatibel ist. Datenfilter unterstützen nur Lesevorgänge.
- Zugriffssteuerungsliste (ACL): Regeln für Zugriffssteuerungslisten (ACLs) beschränken den Zugriff auf Daten, indem sie von Anwendern verlangen, eine Reihe von Anforderungen zu erfüllen, bevor sie mit ihnen interagieren können. Innerhalb einer ACL wird die folgende Hierarchie ausgewertet:
  - Rolle
  - Sicherheitsattribut
  - Bedingung
  - Skript

Auswertung der Zugriffssteuerungsliste

ACLs für die Vorgänge werden in der folgenden Reihenfolge ausgewertet:

- Rolle
- Sicherheitsattribut
- Bedingung
- Skript

Vorhandensein eines Skripts

Das Warnungssymbol in einem beliebigen Status gibt das Vorhandensein eines Skripts in der ACL an. Überprüfen Sie die hervorgehobenen ACLs, um den endgültigen Zugriff zu verstehen.

Hinweis: Während einer Zugriffsanalyseabfrage werden zuerst Business-Regeln und dann die Zugriffssteuerungsliste ausgeführt.

Reihenfolge der Ausführung

Die Ausführung des Zugriffsergebnisses in verschiedenen Szenarien ist wie folgt:

- **Vorhandensein einer geerbten oder Platzhalter-ACL** : Während der Ausführungssequenz werden zuerst die geerbten ACLs und dann die Platzhalter-ACL ausgewertet.
- **Eine ACL wird übergeben, die anderen werden übersprungen** : Während der Ausführung und Auswertung der Berechtigung, wenn eine ACL übergeben wird, wird die andere ACL-Ausführung und -Auswertung übersprungen. Da die Gesamtberechtigung für den ausgewählten Vorgang eine ACL erfordert, um auf ein Feld, einen Datensatz oder eine Tabelle für eine Identität zuzugreifen.
- **Ausführung von ACLs auf Feldebene und ACLs auf Tabellenebene** : Während der Ausführung werden ACLs auf Feldebene zuerst ausgeführt, gefolgt von ACL auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenebene, um bei der Analyse des Zugriffs auf eine Identität granulare Ergebnisse zu liefern.

- **Auswertung in Gegenwart einer geskripteten ACL** : Wenn ein Skript vorhanden ist, wird der Gesamtzugriff für den Vorgang mit einem Warnungssymbol übergeben, um das Skript in der ACL anzuzeigen.

Zugriffssimulator

Mit dem Zugriffssimulator können Sie simulieren, wie sich der Zugriff auf die angegebene Tabelle ändern würde, nachdem eine Rolle oder Gruppe dem Anwender zugewiesen oder von ihm entfernt wurde.

Untersuchen



Lernen Sie die Funktionen und den Geschäftsnutzen des Zugriffssimulators kennen.

Verwenden



Erfahren Sie, wie Sie den Zugriffssimulator verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren



Wissen, wie der Zugriffssimulator konfiguriert wird.

Häufige Fragen



Rufen Sie Details zu häufig gestellten Fragen für den Zugriffssimulator ab.

Zugriffssimulator Erkunden

Mit dem Zugriffssimulator können Sie simulieren, wie sich der Zugriff auf die angegebene Tabelle ändert, sobald eine Rolle oder Gruppe dem Anwender zugewiesen oder entfernt wird.

Administratoren können den Zugriffssimulator verwenden, um die Zugriffsanforderungen ihrer Anwender für eine angegebene Tabelle zu simulieren und zu verstehen, wie sich die Zugriffssteuerungen für einen Anwender ändern. Es hilft, den aktuellen Zugriff der Anwender schnell zu verstehen und die Auswirkungen der Bereitstellung oder Entfernung von Rollen für die Anwender zu verstehen.

https://player.vimeo.com/video/988627830?badge=0&autopause=0&player_id=0&app_id=58479

Der Zugriffssimulator kann für die Simulation des Zugriffs auf einen Anwender für die folgenden Szenarien verwendet werden:

- Hinzufügen von Rollen zu Anwendern
- Rollen werden von Anwendern entfernt
- Hinzufügen von Anwendern zu Gruppen
- Anwender werden aus Gruppen entfernt

Weitere Informationen zu den Einstellungen des Zugriffssimulators und zum Aktivieren von Aktionen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffssimulator konfigurieren (Aktionen ausführen)

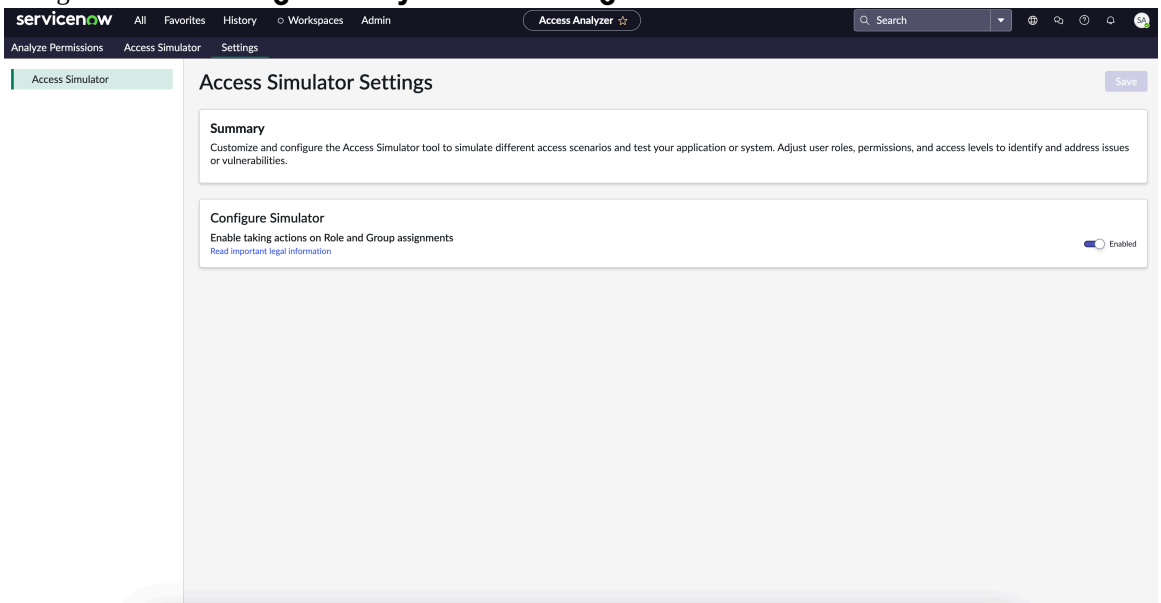
Konfigurieren Sie die Optionen „Aktionen ausführen“, um die Rollen- und Gruppenzuweisungen abzuschließen, die Sie nach der Simulation hinzufügen möchten.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Einstellungen**an.



2. Wählen Sie den Umschalter aus, um ihn zu aktivieren.
   Lesen Sie sich die rechtlichen Informationen durch, bevor Sie den Zugriffssimulator aktivieren (Aktionen ergreifen).
3. Wählen Sie **Akzeptieren** aus.
4. Wählen Sie Aus **Speichern** Zum Speichern der Konfiguration.

Mit dem Zugriffssimulator

Verwenden Sie den Zugriffssimulator, um zu simulieren, dass sich der Zugriff des Anwenders auf die angegebene Tabelle ändert, sobald eine Rolle oder Gruppe zugewiesen oder entfernt wird.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Aktivieren Sie Aktionen ausführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie aus **Simulieren** Option unter jedem Abschnitt basierend auf den folgenden Szenarien:
   - Hinzufügen von Rollen zu Anwendern
   - Rollen werden von Anwendern entfernt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Hinzufügen von Anwendern zu Gruppen
- Anwender werden aus Gruppen entfernt

Hinzufügen von Rollen zu Anwendern

Verwenden Sie **„Rolle Hinzufügen“ Simulieren** Zum Simulieren der Zugriffsänderungen des Anwenders für eine Ressource (Tabellen).

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Aktivieren Sie Aktionen ausführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).

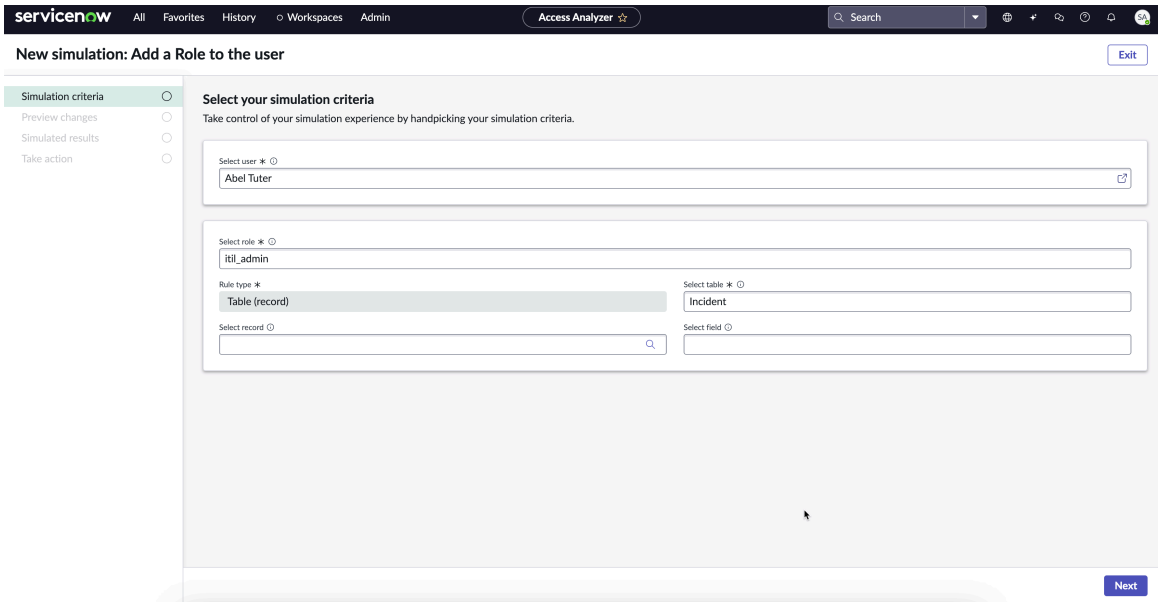
Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie Aus **Simulieren** Im Abschnitt „Rolle zum Anwender hinzufügen“.
3. Geben Sie die folgenden Felder für Ihre Simulationskriterien an:

Dem Anwender eine Rolle hinzufügen

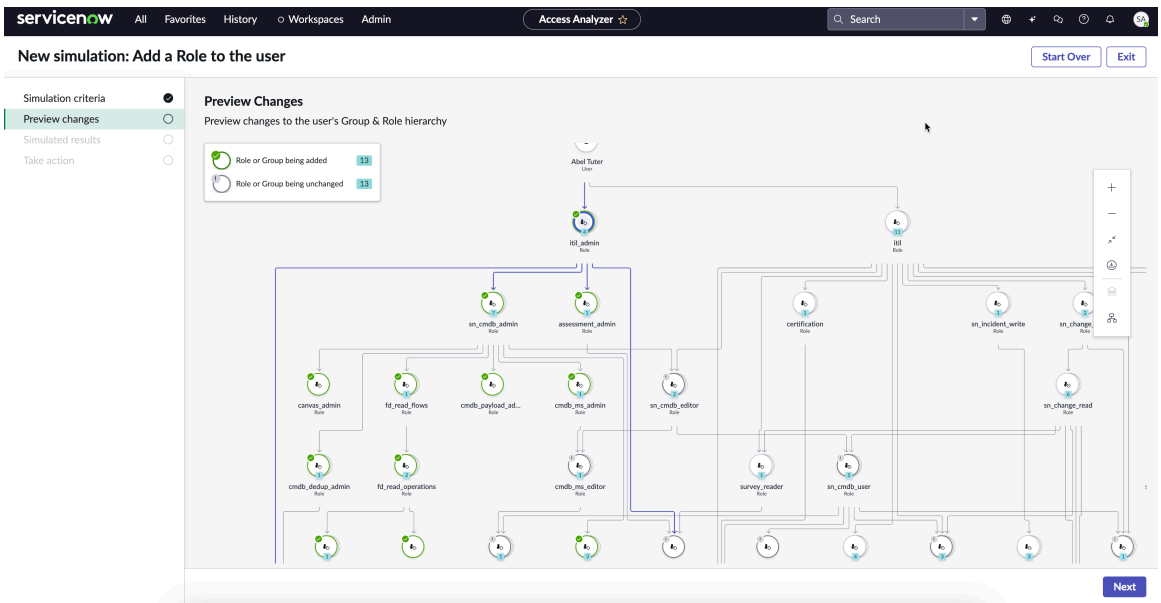
Feld	Beschreibung
Wählen Sie Anwender * aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **Abel Tuter** .
Wählen Sie Rolle * aus	Geben Sie eine Rolle an, die aus der Liste ausgewählt werden soll. In diesem Beispiel **itil_admin** .
Regeltyp *	Regeltyp wird automatisch ausgefüllt und kann nicht geändert werden.
Wählen Sie Tabelle * aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident** .
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll (optional).
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll. Dieses Feld kann verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel aktiv, erstellt von usw.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie **Weiter**.

5. Zeigen Sie eine Vorschau der Änderungen an.
   Die neu zugewiesenen Rollen werden in der Vorschau der Changes simuliert. Sie können die Rollen und untergeordneten Rollen validieren, die dem Anwender hinzugefügt werden, bevor Sie mit dem nächsten Schritt fortfahren.

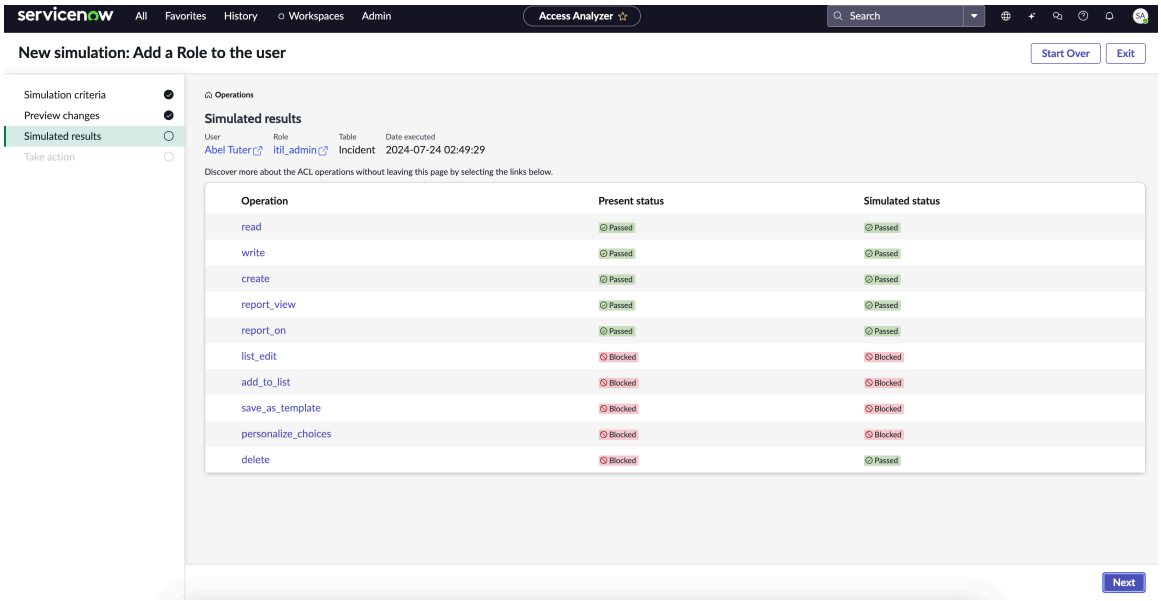


Sie können die neuen Rollen anzeigen, die als Teil von hinzugefügt werden **itil_admin** Rolle wird zusammen mit den vorhandenen Rollen des Anwenders angezeigt.

6. Wählen Sie **Weiter**.

7. Validieren Sie **Aktueller Status** Und **Simulierter Status** Dient zum Überprüfen des Zugriffs **Bestanden** Oder **Blockiert** An den simulierten Anwender.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

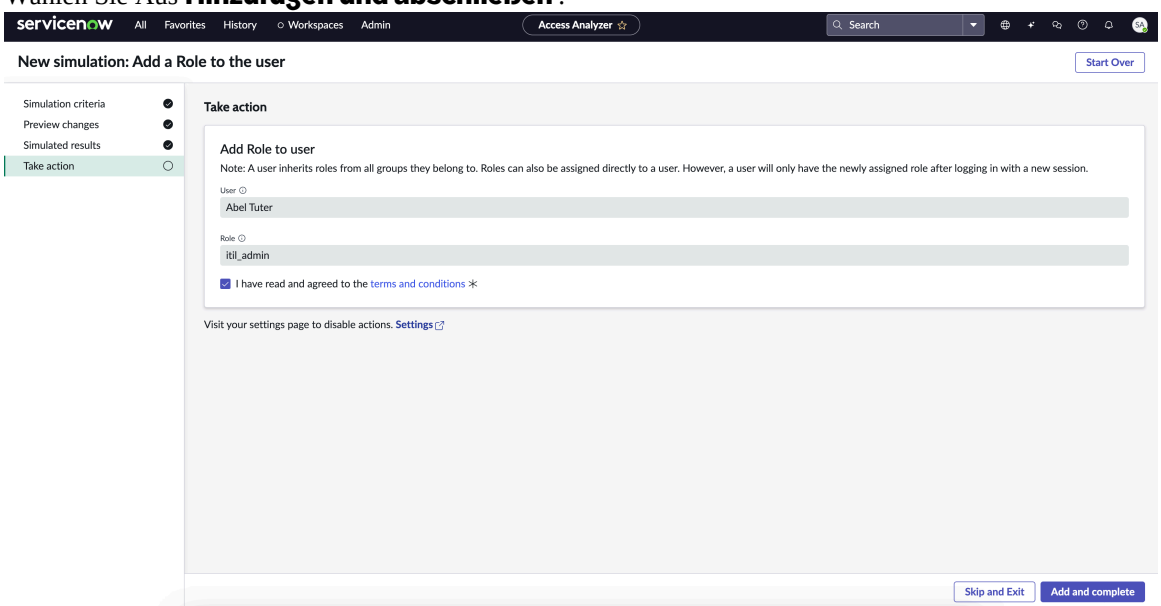


Hinzufügen von **itil_admin** Ermöglicht dem Anwender, einen Löschvorgang für die Tabelle auszuführen (Incident).

Hinweis:

- Wenn Sie mehr über die ACL (Vorgänge) erfahren möchten, wählen Sie die Vorgangslinks für jeden Datensatz aus.
- Wenn Sie die Simulation für eine andere Rolle erneut starten möchten, wählen Sie aus **Beginnen Sie von vorn** .
- Wenn Sie die Simulation beenden möchten, wählen Sie aus **Beenden** .

8. Wählen Sie **Weiter**.
9. Wählen Sie Aus **Hinzufügen und abschließen** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn der Zugriffssimulator nicht aktiviert ist, können Sie die Simulation nicht abschließen. Wählen Sie zum Aktivieren aus **Aktionen aktivieren** Und akzeptieren Sie die rechtlichen Informationen.
- Wenn Sie die Simulation ausblenden möchten, wählen Sie aus **Aktionen ausblenden** . Um Aktionen einzublenden und zu aktivieren, wechseln Sie zu den Einstellungen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).
- Wenn Sie die Simulation beenden möchten, wählen Sie aus **Überspringen und beenden** .

Die Rollen wurden dem Anwender erfolgreich hinzugefügt. Sie können den Zugriff mit der Zugriffsanalyse überprüfen. Weitere Informationen zum Überprüfen des Zugriffs eines Anwenders finden Sie unter Zugriffsanalyse.

Rollen werden von Anwendern entfernt

Verwenden Sie **„Rolle Entfernen“ Simulieren** Zum Simulieren der Zugriffsänderungen des Anwenders für eine Ressource (Tabellen).

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Aktivieren Sie Aktionen ausführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie Aus **Simulieren** Im Abschnitt Rolle aus dem Anwender entfernen.
3. Geben Sie die folgenden Felder für Ihre Simulationskriterien an:

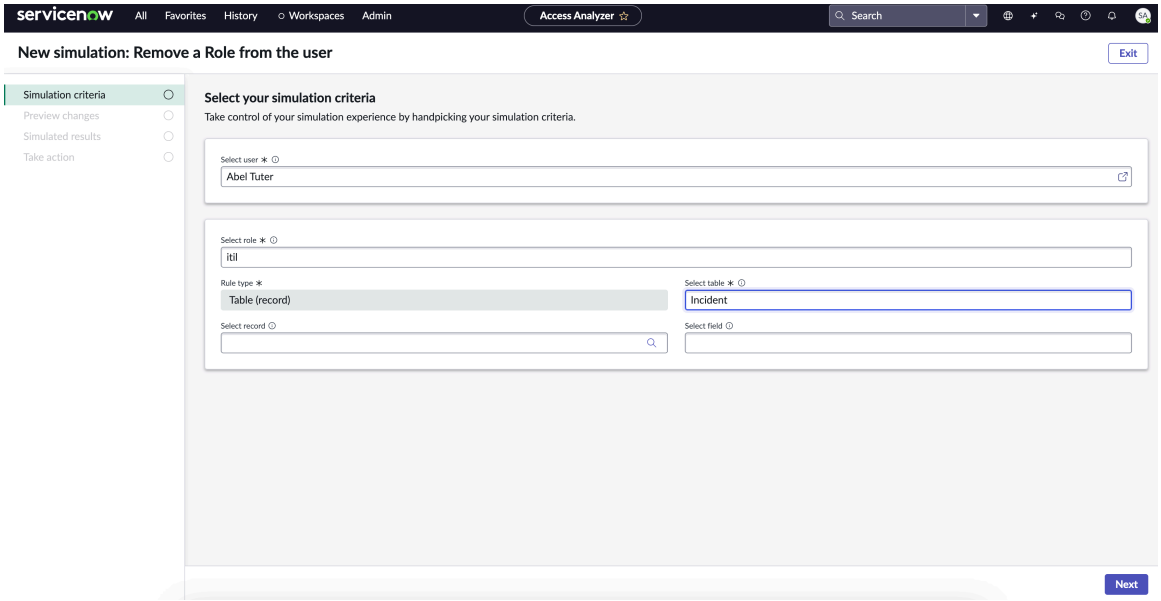
Eine Rolle vom Anwender entfernen

Feld	Beschreibung
Wählen Sie Anwender * aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **Abel Tuter** .
Wählen Sie Rolle * aus	Geben Sie eine Rolle an, die aus der Liste ausgewählt werden soll. In diesem Beispiel **itil** .
Regeltyp *	Regeltyp wird automatisch ausgefüllt und kann nicht geändert werden.
Wählen Sie Tabelle * aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident** .
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll.
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll. Dieses Feld kann verwendet

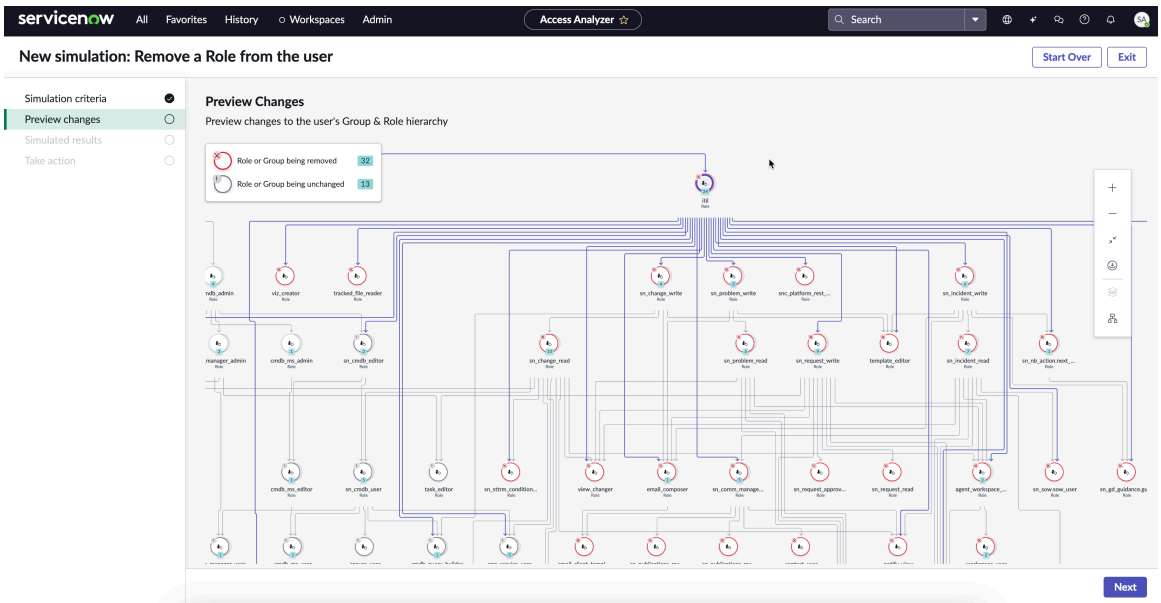
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel aktiv, erstellt von usw.



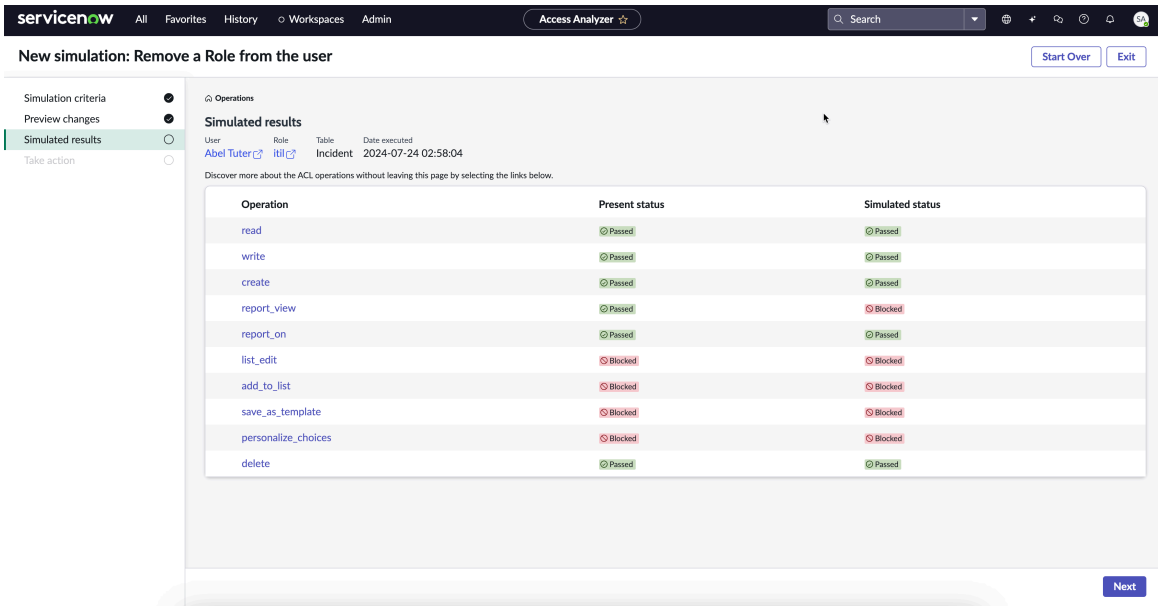
4. Wählen Sie **Weiter**.
5. Zeigen Sie eine Vorschau der Änderungen an.
   Die Rollen, die entfernt werden, werden in der Vorschau der Changes simuliert. Sie können die Rollen und untergeordneten Rollen validieren, die für den Anwender entfernt werden, bevor Sie mit dem nächsten Schritt fortfahren.



6. Wählen Sie **Weiter**.
7. Validieren Sie **Aktueller Status** Und **Simulierter Status** Dient zum Überprüfen des Zugriffs **Bestanden** Oder **Blockiert** An den simulierten Anwender.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- Wenn Sie mehr über die ACL (Vorgänge) erfahren möchten, wählen Sie die Vorgangslinks für jeden Datensatz aus.
- Wenn Sie die Simulation für eine andere Rolle erneut starten möchten, wählen Sie aus **Beginnen Sie von vorn** .
- Wenn Sie die Simulation beenden möchten, wählen Sie aus **Beenden** .

8. Wählen Sie **Weiter**.
9. Wählen Sie Aus **Entfernen und abschließen** .

Hinweis:

- Wenn der Zugriffssimulator nicht aktiviert ist, können Sie die Simulation nicht abschließen. Wählen Sie zum Aktivieren aus **Aktionen aktivieren** Und akzeptieren Sie die rechtlichen Informationen.
- Wenn Sie die Simulation ausblenden möchten, wählen Sie aus **Aktionen ausblenden** . Um Aktionen einzublenden und zu aktivieren, wechseln Sie zu den Einstellungen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).
- Wenn Sie die Simulation beenden möchten, wählen Sie aus **Überspringen und beenden** .

Die Rollen wurden erfolgreich aus dem Anwender entfernt. Sie können den Zugriff mit der Zugriffsanalyse überprüfen. Weitere Informationen zum Überprüfen des Zugriffs eines Anwenders finden Sie unter Zugriffsanalyse.

Hinzufügen von Anwendern zu Gruppen

Verwenden Sie **„Zu Gruppe hinzufügen“ simulieren** Zum Simulieren der Zugriffsänderungen des Anwenders für eine Ressource (Tabellen), wenn der Anwender einer Gruppe hinzugefügt wird.

Vorbereitungen
Erforderliche Rolle: admin, Access_Analyzer_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

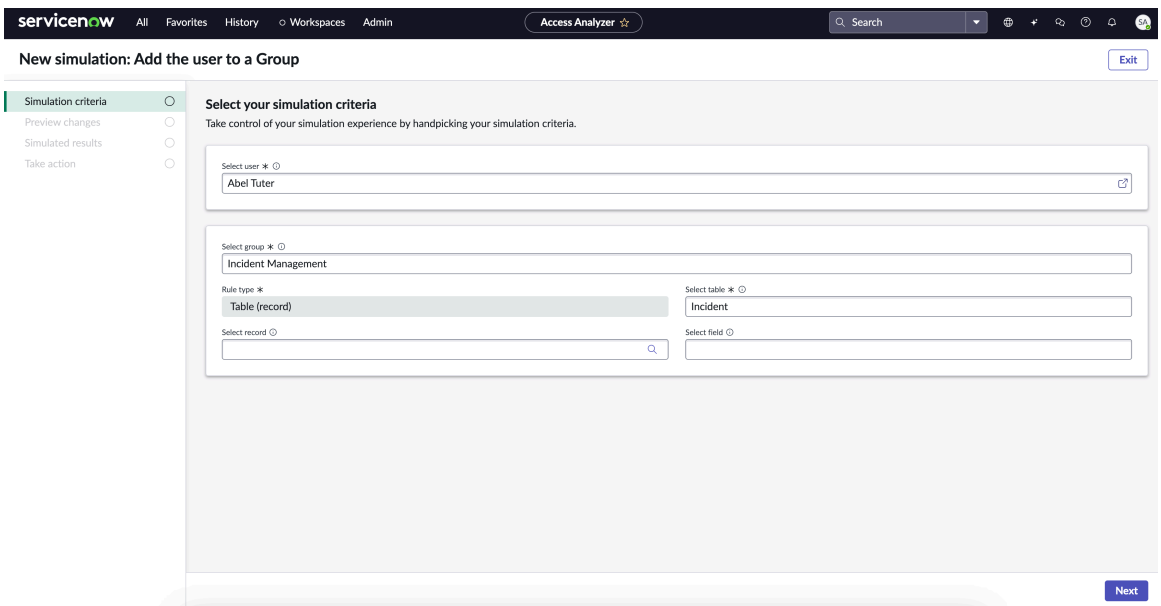
Aktivieren Sie Aktionen ausführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie Aus **Simulieren** Im Abschnitt Anwender zu einer Gruppe hinzufügen.
3. Geben Sie die folgenden Felder für Ihre Simulationskriterien an:

Fügen Sie den Anwender einer Gruppe hinzu

Feld	Beschreibung
Wählen Sie Anwender * aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **Abel Tuter** .
Wählen Sie Gruppe * aus	Geben Sie eine Gruppe an, die aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident-Management** .
Regeltyp *	Regeltyp wird automatisch ausgefüllt und kann nicht geändert werden.
Wählen Sie Tabelle * aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident** .
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll.
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll. Dieses Feld kann verwendet werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel aktiv, erstellt von usw.

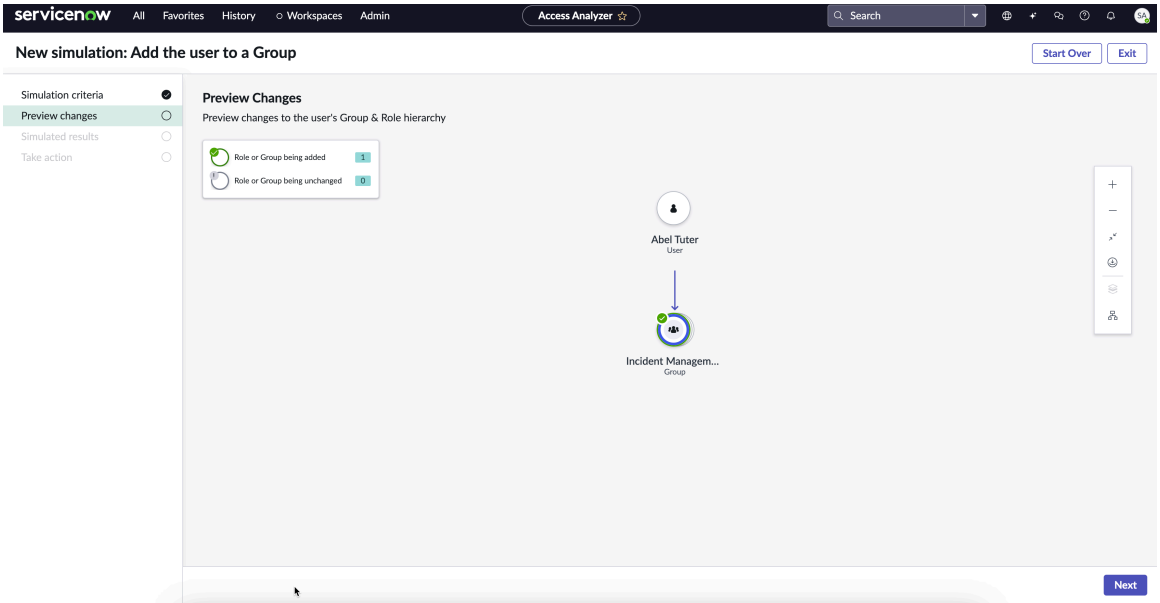


4. Wählen Sie **Weiter**.
5. Zeigen Sie eine Vorschau der Änderungen an.

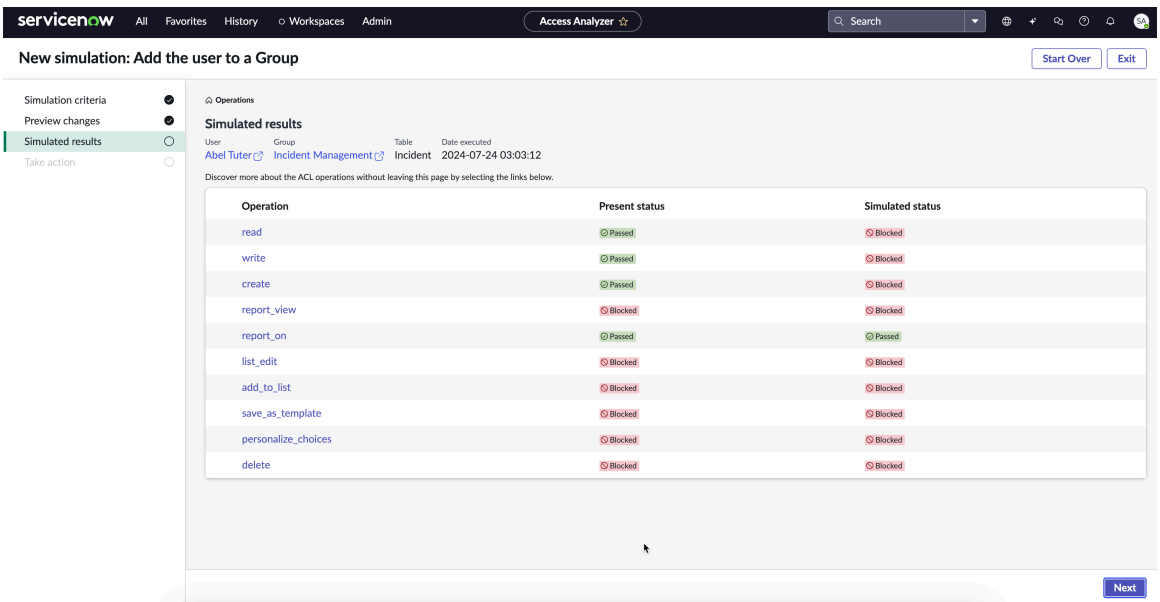
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Gruppe, der der Anwender zugewiesen ist, wird in der Vorschau der Änderungen simuliert. Sie können die Änderungen validieren, bevor Sie mit dem nächsten Schritt fortfahren.



6. Wählen Sie **Weiter**.
7. Validieren Sie **Aktueller Status** Und **Simulierter Status** Dient zum Überprüfen des Zugriffs **Bestanden** Oder **Blockiert** An den simulierten Anwender.



Hinweis:

- Wenn Sie mehr über die ACL (Vorgänge) erfahren möchten, wählen Sie die Vorgangslinks für jeden Datensatz aus.
- Wenn Sie die Simulation für eine andere Rolle erneut starten möchten, wählen Sie aus **Beginnen Sie von vorn** .
- Wenn Sie die Simulation beenden möchten, wählen Sie aus **Beenden** .

8. Wählen Sie **Weiter**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie Aus **Hinzufügen und abschließen** .

Hinweis:

- Wenn der Zugriffssimulator nicht aktiviert ist, können Sie die Simulation nicht abschließen. Wählen Sie zum Aktivieren aus **Aktionen aktivieren** Und akzeptieren Sie die rechtlichen Informationen.
- Wenn Sie die Simulation ausblenden möchten, wählen Sie aus **Aktionen ausblenden** . Um Aktionen einzublenden und zu aktivieren, wechseln Sie zu den Einstellungen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).
- Wenn Sie die Simulation beenden möchten, wählen Sie aus **Überspringen und beenden** .

Der Anwender wurde der Gruppe erfolgreich hinzugefügt.

Anwender werden aus Gruppen entfernt

Verwenden Sie **„Aus Gruppe entfernen" simulieren** Zum Simulieren der Zugriffsänderungen des Anwenders für eine Ressource (Tabellen), wenn der Anwender aus einer Gruppe entfernt wird.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Aktivieren Sie Aktionen ausführen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriffssimulator**an.
2. Wählen Sie Aus **Simulieren** Im Abschnitt Anwender aus einer Gruppe entfernen.
3. Geben Sie die folgenden Felder für Ihre Simulationskriterien an:

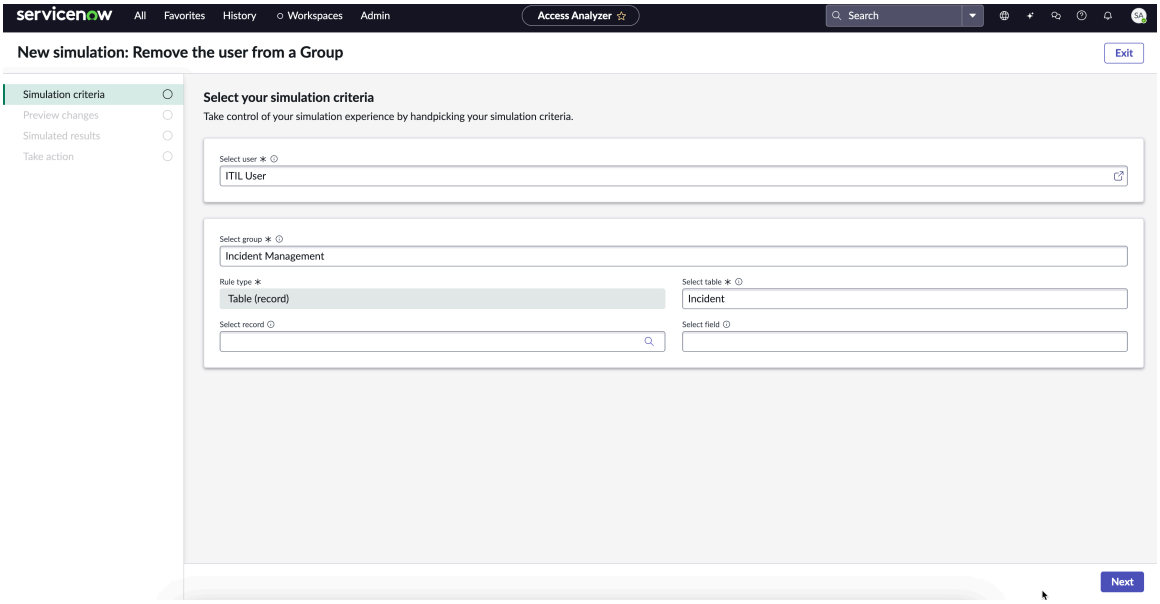
Entfernen Sie den Anwender aus einer Gruppe

Feld	Beschreibung
Wählen Sie Anwender * aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **ITIL-Anwender** .
Wählen Sie Gruppe * aus	Geben Sie eine Gruppe an, die aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident-Management** .
Regeltyp *	Regeltyp wird automatisch ausgefüllt und kann nicht geändert werden.
Wählen Sie Tabelle * aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll. In diesem Beispiel **Incident** .
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll.
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll. Dieses Feld kann verwendet

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

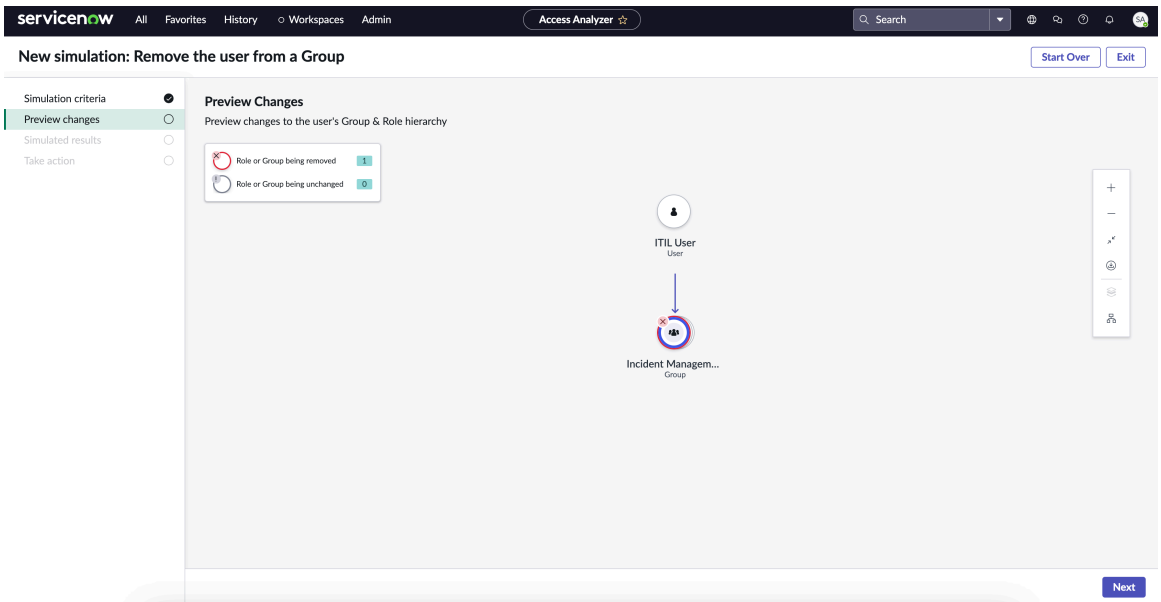
Feld	Beschreibung
	werden, um Berechtigungen auch auf Feldebene zu analysieren. Zum Beispiel aktiv, erstellt von usw.



d

4. Wählen Sie **Weiter**.
5. Zeigen Sie eine Vorschau der Änderungen an.

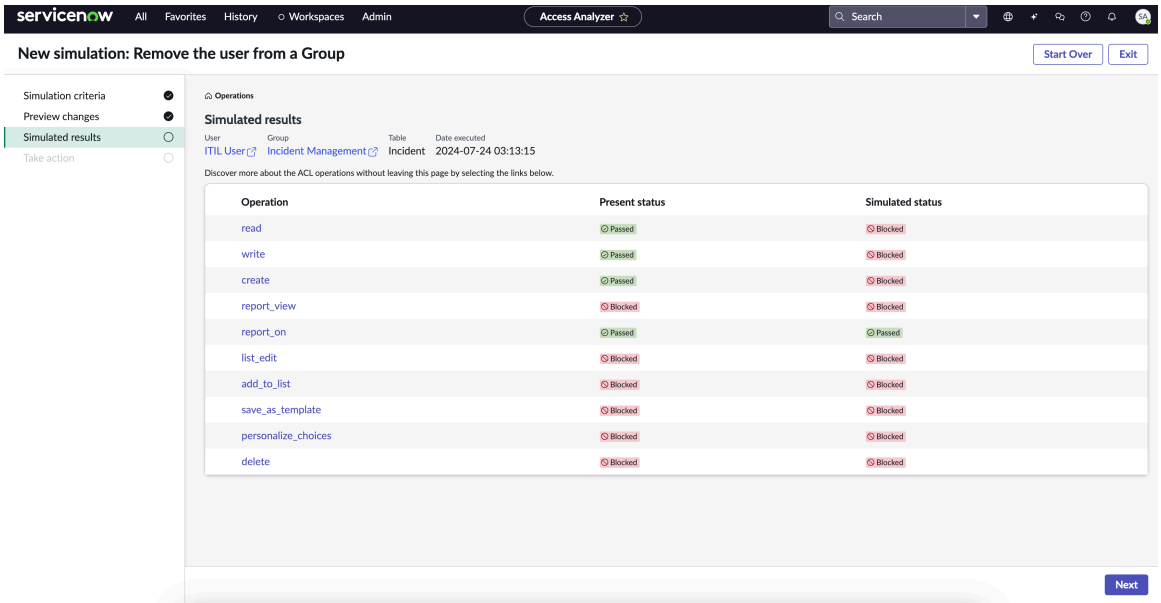
   Die Gruppe, aus der der Anwender entfernt wird, wird in der Vorschau der Änderungen simuliert. Sie können die Änderungen validieren, bevor Sie mit dem nächsten Schritt fortfahren.



6. Wählen Sie **Weiter**.
7. Validieren Sie **Aktueller Status** Und **Simulierter Status** Dient zum Überprüfen des Zugriffs **Bestanden** Oder **Blockiert** An den simulierten Anwender.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

- Wenn Sie mehr über die ACL (Vorgänge) erfahren möchten, wählen Sie die Vorgangslinks für jeden Datensatz aus.
- Wenn Sie die Simulation für eine andere Rolle erneut starten möchten, wählen Sie aus **Beginnen Sie von vorn** .
- Wenn Sie die Simulation beenden möchten, wählen Sie aus **Beenden** .

8. Wählen Sie **Weiter**.
9. Wählen Sie Aus **Entfernen und abschließen** .

Hinweis:

- Wenn der Zugriffssimulator nicht aktiviert ist, können Sie die Simulation nicht abschließen. Wählen Sie zum Aktivieren aus **Aktionen aktivieren** Und akzeptieren Sie die rechtlichen Informationen.
- Wenn Sie die Simulation ausblenden möchten, wählen Sie aus **Aktionen ausblenden** . Um Aktionen einzublenden und zu aktivieren, wechseln Sie zu den Einstellungen. Weitere Informationen finden Sie unter Zugriffssimulator konfigurieren (Aktionen ausführen).
- Wenn Sie die Simulation beenden möchten, wählen Sie aus **Überspringen und beenden** .

Der Anwender wurde erfolgreich aus dem Anwender entfernt.

Häufige Fragen

Häufig gestellte Fragen zur Verwendung des Zugriffssimulators.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufige Fragen

Fragen	Erklärung
Wie beginne ich mit dem Simulator?	Sie können die Option „Simulieren“ für das andere Szenario auswählen, das Sie für die Anwender simulieren möchten, und die Schritte ausführen.
Wie funktioniert der Simulator?	Der Zugriffssimulator simuliert den Zugriff auf die angegebene Tabelle für den ausgewählten Anwender und zeigt eine Vorschau der Zugriffsänderungen an, um Entscheidungen über die Zugriffsbereitstellung zu treffen.
Wie aktivieren oder deaktivieren Sie Aktionen im Simulator?	Sie können Aktionen im Zugriffssimulator aktivieren oder deaktivieren, indem Sie zu den Einstellungen navigieren, oder während der Schritte von „Aktionen ausführen“ im Simulationsprozess.

Access Insights

Mit Access Insights können Sie Vertrauen in Ihre Rollen- oder Gruppenzuweisungen gewinnen.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von Access Insights.

Konfigurieren



Erfahren Sie, wie Sie Access Insights konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden	
	
Wissen, wie Access Insights verwendet werden.	

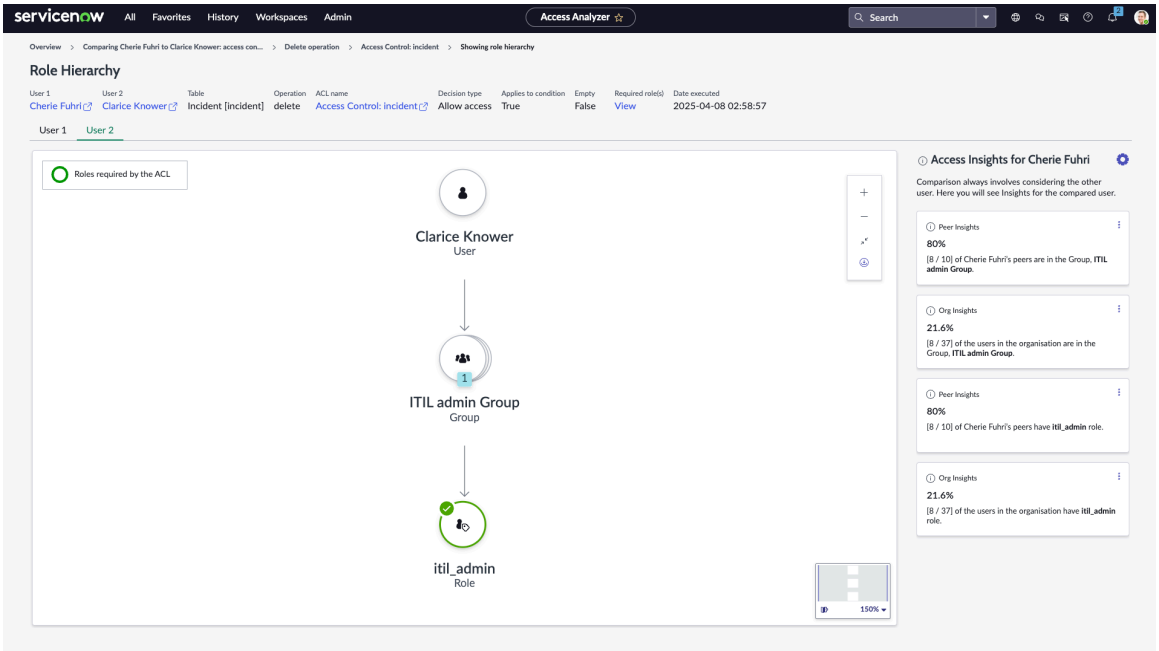
Access Insights Erkunden

Die Zugriffseinblicke in der Zugriffsanalyse helfen Ihnen, Vertrauen in Ihre Rollen- oder Gruppenzuweisungen zu gewinnen.

Die Zugriffseinblicke zeigen die Statistiken des Zugriffs auf Peer- und Organisationsebene Ihres Anwenders auf eine Ressource an. Damit können Sie sehen, ob die Rolle oder Gruppe dem Anwender zugewiesen werden kann, den Sie derzeit auf zusätzliche Berechtigungen überprüfen. Es hilft Ihnen, die Rollen- und Gruppenzuweisungen mit derselben Peer-Gruppe zu vergleichen.

Die Zugriffseinblicke werden nur angezeigt, wenn der Zugriff des Anwenders mithilfe der Funktion „Anwenderzugriff vergleichen“ in der Zugriffsanalyse verglichen wird. Weitere Informationen zur Verwendung von Access Insights finden Sie unter Verwenden Von Access Insights.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Basierend auf den Statistiken können Sie entscheiden, den Anwendern, die Sie innerhalb ihrer Kollegen vergleichen, die richtigen Rollen- oder Gruppenzuweisungen bereitzustellen.

Hinweis:

- Access Insights ist mit der Zugriffsanalyse V4 verfügbar.
- Sie sollten Anwender auf Peer-Ebene vergleichen (gleiche Organisation, gleiche Abteilung, gleicher Manager), während Sie die Statistiken in der Funktion „Access Insights“ anzeigen.

Um Zugriffseinblicke in der Zugriffsanalyse zu aktivieren, müssen Sie zu den Einstellungen navigieren. Weitere Informationen finden Sie unter Konfigurieren Von Access Insights.

Konfigurieren Von Access Insights

Aktivieren Sie die Funktion „Access Insights“ in der Zugriffsanalyse.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

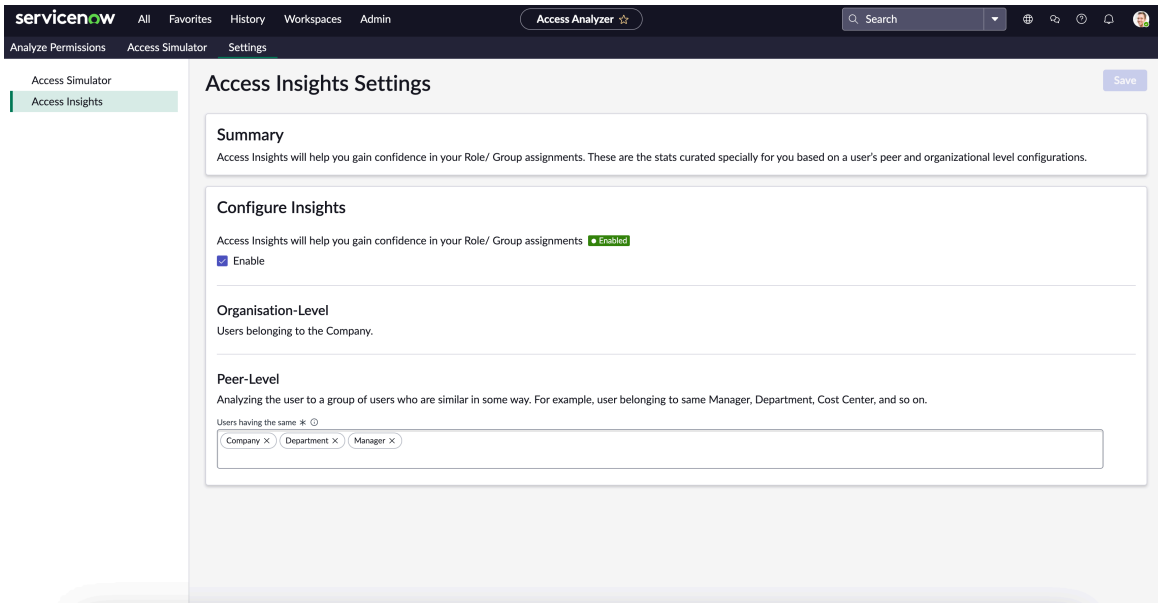
Im folgenden Verfahren werden die Schritte zum Aktivieren von Access Insights beschrieben.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Zugriff analysieren**an.
2. Wählen Sie die Registerkarte **Einstellungen**.
3. Wählen Sie Aus **Greifen Sie Auf Einblicke Zu** .
4. Aktivieren **Greifen Sie Auf Einblicke Zu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Standardmäßig werden Felder auf Peer-Ebene mit ausgewählt **Unternehmen** , **Abteilung** , **Manager** . Sie können weitere Felder hinzufügen, z. B. **Kostenstelle** , **Ländercode** , **Standort** , Und **Titel** .

5. Wählen Sie **Speichern**.

Ergebnis

Die Funktion „Access Insights“ ist aktiviert und wird angezeigt, wenn Sie anzeigen **Rollenhierarchie** Beim Vergleich des Anwenderzugriffs auf eine Ressource. Weitere Informationen zur Verwendung von Access Insights finden Sie unter Verwenden Von Access Insights.

Verwenden Von Access Insights

Verwenden Sie Access Insights, um den Peer-Level-Zugriff von Anwendern auf eine ausgewählte Ressource zu verstehen.

Vorbereitungen

Erforderliche Rolle: admin, Access_Analyzer_admin

Hinweis: Um die Details der Funktion „Durchgreifen auf Einblicke“ anzuzeigen, müssen Sie verwenden Vergleichen Sie den Anwenderzugriff Funktion.

Im folgenden Verfahren werden die Schritte zum Anzeigen der Statistiken für Rollen- oder Gruppenzuweisungen auf Peer-Ebene in der Funktion „Access Insights“ beschrieben.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsanalyse** > **Berechtigungen analysieren**an.
   Die Homepage „Zugriff und Berechtigungen analysieren“ wird angezeigt.
2. Wählen Sie aus **Vergleichen Sie den Anwenderzugriff** Registerkarte.
3. Füllen Sie folgende Felder aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderzugriff vergleichen

Feld	Beschreibung
Wählen Sie Anwender 1* aus	Geben Sie einen Anwendernamen an, der aus der Liste für den Vergleich ausgewählt werden soll.
Wählen Sie Anwender 2* aus	Geben Sie einen Anwendernamen an, der aus der Liste ausgewählt werden soll, um ihn mit dem Anwender zu vergleichen 1.
Regeltyp*	Analysieren Sie Zugriffsberechtigungen für eine Tabelle. **Hinweis:** In können nur Zugriffsberechtigungen für eine Tabelle verwendet werden **Vergleichen Sie den Anwenderzugriff** .
Wählen Sie Tabelle* aus	Geben Sie einen Tabellennamen an, der aus der Liste ausgewählt werden soll.
Datensatz auswählen	Geben Sie einen Datensatznamen an, der aus der Liste ausgewählt werden soll.
Feld auswählen	Geben Sie einen Feldnamen an, der aus der Liste ausgewählt werden soll.

4. Wählen Sie Aus **Vergleichen Sie den Anwenderzugriff** .

   Die **Vergleichen Sie den Anwenderzugriff** Ergebnisse für die ausgewählten Anwender werden angezeigt.

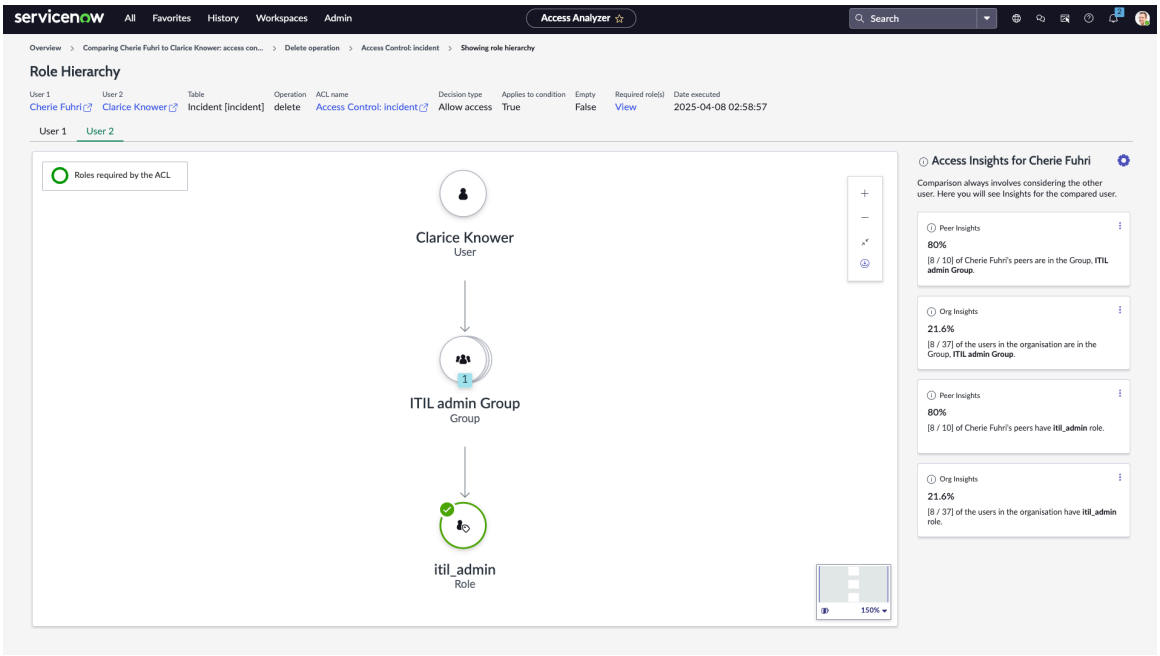
   Die Ergebnisse des Vergleichs des Anwenderzugriffs zeigen den Vorgang und den Status der Zugriffsauswertung für die Anwender an. Zum Beispiel Charlier Fuhri und Charlie Knower.

5. Wählen Sie einen Vorgang aus.
   Beispiel: **Lesen** Vorgang.
6. Wählen Sie einen der aus **Zugriffssteuerung** Um mehr über den Zugriff zu erfahren.
7. Wählen Sie Aus **Rollenhierarchie anzeigen** Dient zum Anzeigen des Zugriffsvergleichs auf Peer-Ebene.

   Die Zugriffseinblicke werden wie folgt angezeigt:

   - **Peer-Einblicke** : Zeigt an, wie viele Anwender innerhalb ihrer Kollegen dieselbe Rolle zugewiesen haben (derselbe Manager oder dieselbe Abteilung).
   - **Organisationseinblicke** : Zeigt an, wie viele Anwender innerhalb der Organisation dieselbe Rolle zugewiesen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Basierend auf diesen Informationen können Sie dem Anwender, den Sie verglichen haben, Zugriff gewähren oder widerrufen.

Globale Identität

Globale Identität ist ein ServiceNow® Produkt, mit dem eindeutige Anwender in mehreren Instanzen identifiziert werden können.

Globale Identität hilft bei mehreren ServiceNow® Instanzen zum Verwalten von Anwendern, deren Attributen und anderen grundlegenden Daten über mehrere hinweg ServiceNow® Instanzen.

Föderierte ID erkunden



Zugriff auf föderierte ID



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfahren Sie mehr über die wichtigsten Funktionen und den Geschäftsnutzen der föderierten ID.	Föderierte ID des Zugriffs.
ID-Felder werden aktualisiert  Aktualisieren und richten Sie die föderierte ID ein.	

Föderierte ID erkunden

Bestimmen Sie die Anwender in mehreren Instanzen basierend auf Anwendername und E-Mail-Adresse, und geben Sie dem Anwender instanzübergreifend eine eindeutige ID (Verbund-ID) an.

Die föderierte ID wird verwendet, um Anwender über mehrere hinweg zu identifizieren ServiceNow® Instanz. Basierend auf der föderierten ID kann der Anwender identifiziert werden, und die genaue Anzahl der Anwender in mehreren Instanzen kann ermittelt werden. Weitere Informationen finden Sie unter Föderierte ID .

Hinweis: Anwendername ist zum Generieren von Verbund-IDs erforderlich.

Die föderierte ID ist ein eindeutiger Bezeichner für eine Identität, der eine Hashing-Funktion im verwendet ServiceNow® Instanzen.

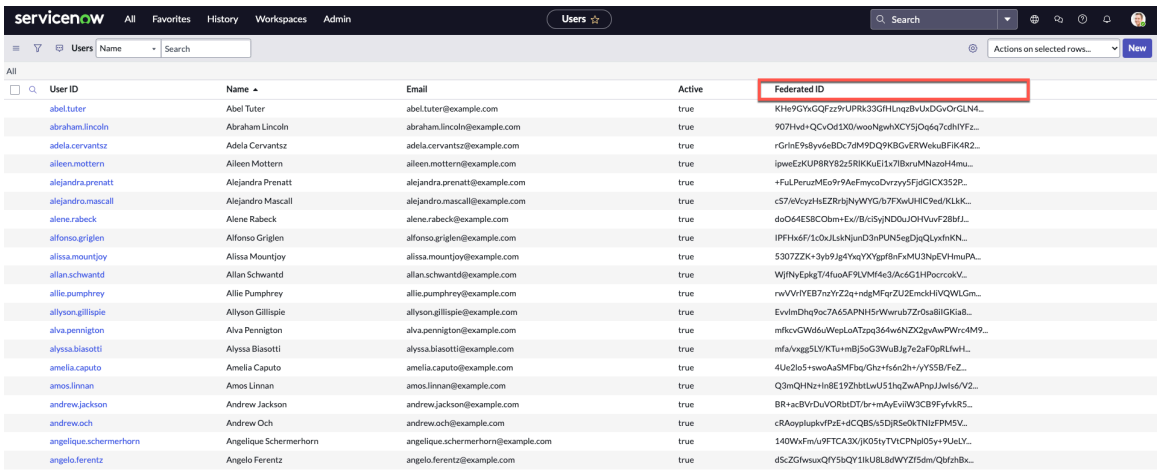
Mithilfe von **Anwender-ID** Und **E-Mail** Des Anwenders in allen Instanzen wird die föderierte ID erstellt und in der Tabelle „sys_user“ angezeigt.

Nach dem Upgrade auf Zurich Release, die föderierte ID-Generierung (Com.Glide.Identity.globalid) Das Plugin wird automatisch auf allen Instanzen installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Anwendername ist zum Generieren von Verbund-IDs erforderlich.
- Anwendername und E-Mail-Adresse werden standardmäßig zum Generieren von föderierten IDs verwendet. Informationen zum Aktualisieren der Felder zum Generieren von föderierten IDs basierend auf Ihren Anforderungen finden Sie unter ID-Felder werden aktualisiert.
- **Iamsync_admin** Zum Aktualisieren der Konfiguration ist eine Rolle erforderlich.
- Wenn Anwender mit doppelten Anwendernamen und E-Mail-Adressen vorhanden sind, wird die föderierte ID nur für einen Anwender generiert. Wenn der Anwendername null oder leer ist, ist die föderierte ID null.



Die Schemaänderungen nach der Installation des Plugins lauten wie folgt:

- Neue Spalte Federated_ID in `sys_user` Tabelle wird erstellt.
- Neue Tabelle – `Iamsync_type` Wird automatisch mit der Standardkonfiguration für ausgefüllt `sys_user` Tabelle.

Föderierte ID wird nur für unterstützt `sys_user` Tabelle und alle Tabellen, die die Tabelle sys_user erweitern.

Nach dem Upgrade auf Zurich Release, die föderierte ID-Generierung (`Com.Glide.Identity.globalid`) Das Plugin wird automatisch auf allen Instanzen installiert.

Zugriff auf Kriterien für föderierte ID

Greifen Sie auf die Kriterien für die föderierte ID zu, um mehr über die ID-Felder zu erfahren, die zum Generieren der föderierten ID verwendet werden.

Vorbereitungen

Erforderliche Rolle: Iamsync_admin

Prozedur

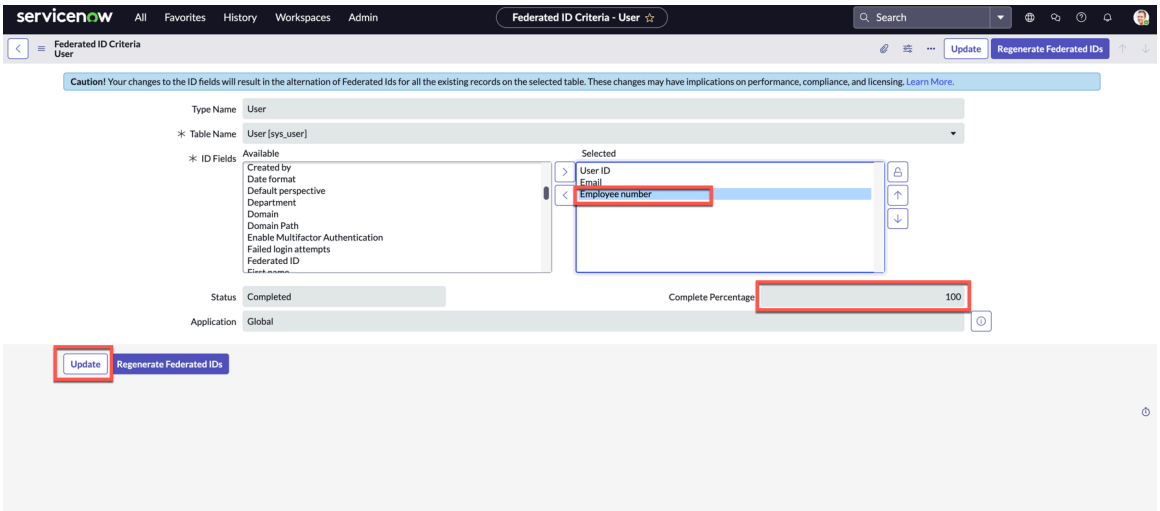
1. Navigieren zu **Alle** > **Verbund-ID verwalten** > **Kriterien für Verbund-ID**an.
2. Auf der Seite „Kriterien für föderierte ID“ wird der Datensatz mit den folgenden Details angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Typname: **Anwender**
- Tabellenname: **Anwender [sys_user]**
- ID-Felder: **User_Name (Anwender-ID), E-Mail** (Standardfelder, die für die Generierung von föderierten IDs verwendet werden).
- Status: **Abgeschlossen** (Generierungsstatus der föderierten ID). Verfügbarer Status: **Bereit** , **Wird Ausgeführt** , **Abgeschlossen** , **Fehler** .

Hinweis:

- Anwendername ist zum Generieren von Verbund-IDs erforderlich.
- Anwendername und E-Mail-Adresse werden standardmäßig zum Generieren von föderierten IDs verwendet.



Hinweis: Nur die ID-Felder können aktualisiert werden, um eine neue föderierte ID für die vorhandenen Datensätze zu generieren. Weitere Informationen finden Sie unter ID-Felder werden aktualisiert.

ID-Felder werden aktualisiert

Aktualisieren Sie die ID-Felder, um die föderierten IDs basierend auf den aktualisierten Feldern erneut zu generieren.

Vorbereitungen

Erforderliche Rolle: Iamsync_admin

Hinweis: Alle Änderungen an den ID-Feldern führen zur Änderung der föderierten IDs für alle vorhandenen Datensätze in der ausgewählten Tabelle. Diese Änderungen können Auswirkungen auf Leistung, Compliance und Lizenzierung haben.

Prozedur

1. Navigieren zu **Alle** > **Verbund-ID verwalten** > **Kriterien für Verbund-ID**an.
2. Wählen Sie den Typnamen (**Anwender**).
3. Wählen Sie die neuen ID-Felder auf der Seite „Verbund-ID-Kriterien – Anwender“ aus, die Sie mithilfe der Pfeilschaltflächen von „verfügbar“ zu „ausgewählt“ hinzufügen möchten.

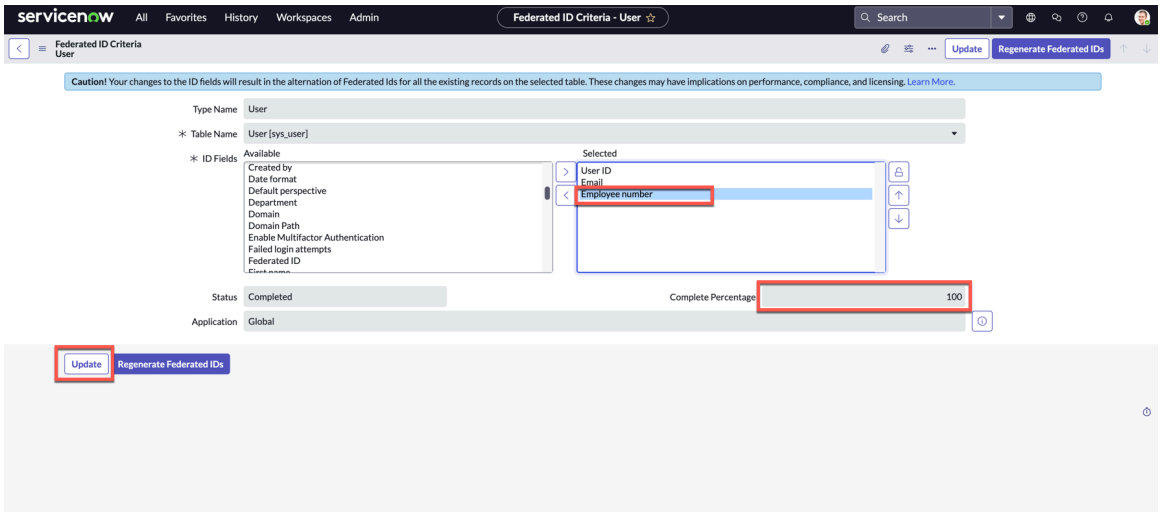
   Beispiel: **Personalnummer** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Anwendername ist zum Generieren von Verbund-IDs erforderlich.
- Anwendername und E-Mail-Adresse werden standardmäßig zum Generieren von föderierten IDs verwendet.
- Wenn Anwender mit doppelten Anwendernamen und E-Mail-Adressen vorhanden sind, wird die föderierte ID nur für einen Anwender generiert. Wenn der Anwendername null oder leer ist, ist die föderierte ID null.



Jetzt die **Personalnummer** Die Auswahl wird zu einem weiteren Attribut zum Generieren der föderierten ID.

4. Wählen Sie Aus **Aktualisieren** Dient zum Generieren von Verbund-IDs.

Hinweis: Wählen Sie Aus **Aktualisieren** Überprüfen Sie zuerst den Fertigstellungsprozentsatz (100), bevor Sie ein weiteres Update initiieren.

Der Statusprozentsatz gibt die Generierung der föderierten ID für alle Identitäten über Instanzen hinweg an.

Hinweis:

- Ändern Sie das Feld erst, wenn der vorherige Aktualisierungsauftrag abgeschlossen ist.
- Felder, die aktualisiert werden, müssen vom Typ Zeichenfolge sein.
- Felder, die nicht als ID-Felder ausgewählt werden können, lauten wie folgt:
  - Felder auf Systemebene
  - Edge Encryption-Felder
  - Passwortfelder.

5. Navigieren Sie zur Tabelle sys_user, um die neuen föderierten IDs anzuzeigen, die aufgrund der Aktualisierung der ID-Felder generiert werden.

Hinweis: Wählen Sie Aus **Föderierte IDs erneut generieren** Wenn ein Anwender über XML-Importe erstellt oder aktualisiert wird, funktioniert die Instanz nicht ordnungsgemäß. Auswählen **Föderierte IDs erneut generieren** , Generiert die IDs für alle Anwender anhand der aktuellen ID-Feldkriterien neu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identitäts- und Zugriffsaudit

Verwenden Sie das Audit für Identität und Zugriff, um Änderungen zu verstehen, die für Anwender, Gruppen, Rollen und ACLs vorgenommen wurden.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von Identitäts- und Zugriffsaudits.

Konfigurieren



Erfahren Sie, wie Sie das Audit für Identität und Zugriff konfigurieren.

Audit-Ergebnisse



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Ergebnisse aus dem Audit für Identität und Zugriff an.

Identitäts- und Zugriffsaudit erkunden

Verwenden Sie das Audit für Identität und Zugriff, um Änderungen zu verstehen, die für Anwender, Gruppen, Rollen und ACLs vorgenommen wurden.

Das Audit für Identität und Zugriff hilft, die kritischen Informationen darüber zu verstehen, wer was, wo und wann in Anwenderaccounts, Gruppen und Rollen geändert hat.

Hilft, böswillige Anwender zu erkennen und ungewöhnliche Aktivitäten in nachzuverfolgen ServiceNow® Instanz und Einhaltung von Compliance-Standards, um Zugriffsänderungen nachverfolgen zu können.

Identity and Access Audit (Identity Security Audit) ist ein Plugin (`com.glide.security.audit`), die automatisch installiert wird.

Die Auditfunktion kann durch Umschalten aktiviert oder deaktiviert werden `glide.identity.security.audit.enabled` Systemeigenschaft. Standardmäßig ist die Eigenschaft festgelegt `Wahr` .

Mit dem Audit für Identität und Zugriff können Sie:

- Zeigen Sie die in den letzten 30 Tagen vorgenommenen Änderungen an Anwendern, Gruppen, Rollen-ACL-Attributen, Rollenmitgliedschaften, Gruppenmitgliedschaften an. und ACL-Rollen.
- Verfolgen Sie die Änderungen in Ihrem ServiceNow Instanz.
- Helfen Sie bei der Minimierung potenzieller Sicherheits- und regulatorischer Risiken.
- Demonstrieren Sie Compliance mit Auditoren für verschiedene Gruppen innerhalb der Organisation.
- Demonstrieren Sie, dass die Organisation nicht angreifbar für Bedrohungen ist, die auf eine mangelnde Transparenz bei Anwendergruppen- und Rollenänderungen zurückzuführen sind.

Anwenderpersonas in Identitätszugriff und Audit

Im Folgenden finden Sie die verschiedenen Anwenderpersonas in Identitäts- und Zugriffsaudit:

- **Administrator** : Zeigen Sie die Audit-Datensätze und die Konfiguration an.
- **Sicherheitsadministrator** : Zeigen Sie diese Audit-Trails an. Ändern Sie die Konfiguration, um das Auditing für eine bestimmte Tabelle zu aktivieren oder zu deaktivieren, oder ändern Sie die Felder, die geprüft werden.

Audit-Tabellen

Die folgenden Tabellen können mithilfe des Identitäts- und Zugriffsaudits auditiert werden:

- Gruppe [sys_user_Group]
- Rolle [sys_user_role]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zugriffssteuerung [sys_Security_acl]
- Anwender [sys_user]
- Gruppenrolle [sys_Group_has_role]
- Anwenderrolle [sys_user_has_role]
- Zugriffsrollen [sys_Security_acl_role]
- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember]

Module in Identitäts- und Zugriffsaudit

Das Identitäts- und Zugriffsaudit verfügt über die folgenden Module auf der ServiceNow Instanz:

Modul	Beschreibung
Audit-Ergebnisse	Zeigt die Audits an, die in aufgetreten sind ServiceNow Instanz.
Konfigurieren Sie Tabelle Und Felder	Konfigurieren Sie die Systemtabellen und -Felder mit den verfügbaren Feldern aus dem Audit für Identität und Zugriff.
Aufbewahrungszeitraum konfigurieren	Konfigurieren Sie den Aufbewahrungszeitraum der geprüften Daten. Der maximale Zeitraum, der festgelegt werden kann, beträgt 30 Tage.
Anwenderpfade	Zeigt Audits von Anwendern an.
Gruppenpfade	Zeigt Audits von Gruppen an.
Rollenpfade	Zeigt Audits von Rollen an.
ACL-Pfade	Zeigt Audits von ACLs an.

Ergebnisse Des Identitätsaudits

Zeigt Audits an, die in aufgetreten sind ServiceNow® Instanz.

Audit-Ergebnisse zeigen Änderungen an, die für Anwender, Gruppen, Rollen und ACLs in vorgenommen wurden ServiceNow Instanz.

Navigieren Sie, um auf die Audit-Ergebnisse zuzugreifen **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Audit-Ergebnisse**an. Die Seite Audits der Sicherheitstabelle wird mit den folgenden Informationen angezeigt.

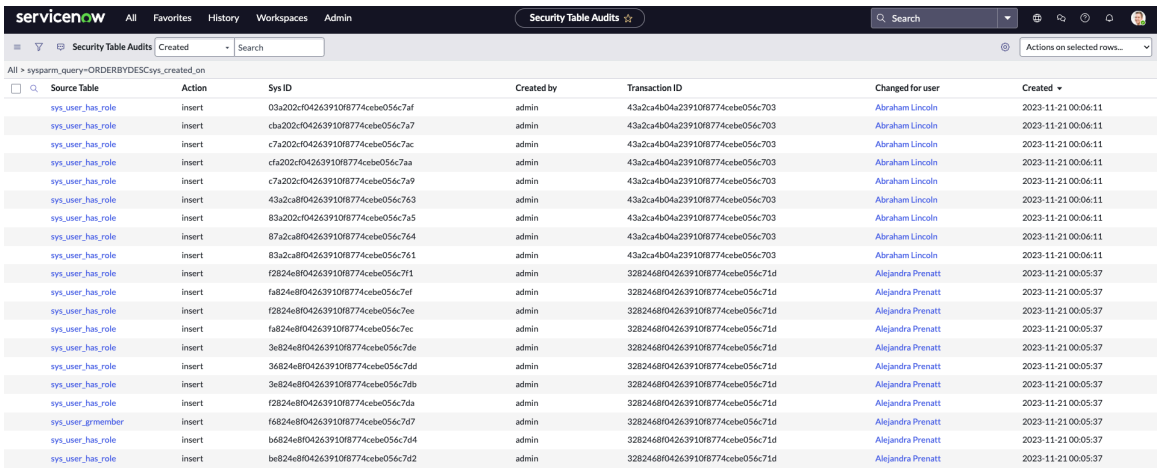
Sicherheitstabellen-Audits

Spaltenname	Beschreibung
Quelltabelle	Details der Quelltabelle, in der das Audit aufgetreten ist.
Aktion	Beschreibt die Audit-Aktion.
SYS_ID	Details zur sys_ID für den auditierten Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitstabellen-Audits (Fortsetzung)

Spaltenname	Beschreibung
Erstellt von	Details des Audits, das von erstellt wurde.
Transaktion-ID	Eine eindeutige ID, die jede Aktion für das bestimmte Audit darstellt.
Für Anwender geändert	Name des Anwenders, als das Audit durchgeführt wurde.
Erstellt	Zeitpunkt und Datum der Durchführung des Audits.



Anwenderpfade

Zeigt Audits von Anwendern in an ServiceNow® Instanz.

Anwenderpfade zeigen Identitätsattribut-Changes, Rollenmitgliedschaftsänderungen und Gruppenmitgliedschaftsänderungen für einen Anwender an.

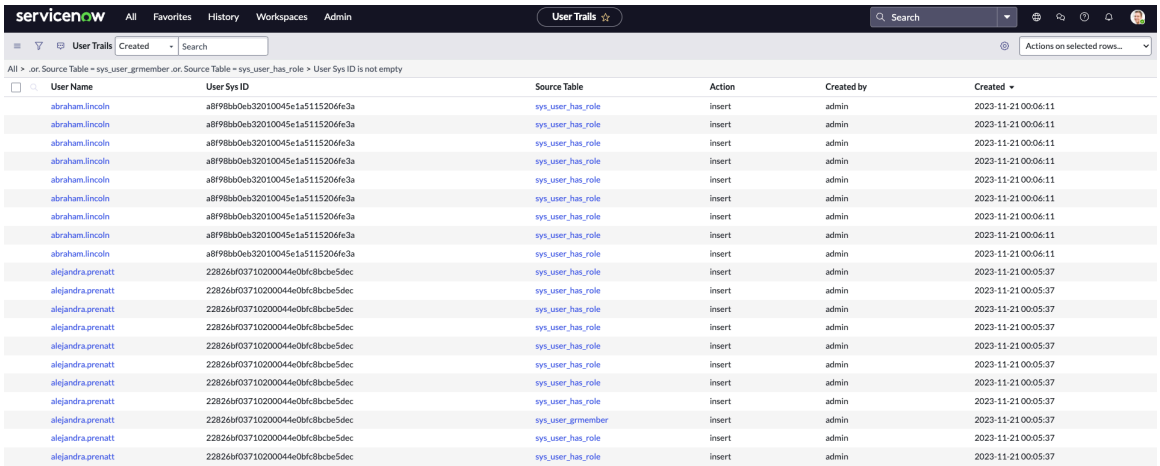
Um auf Anwenderpfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Anwenderpfade**an. Die Seite „Anwenderpfade“ wird mit den folgenden Informationen angezeigt.

Anwenderpfade

Anwendername	Der Name des Benutzers.
Anwender-SYS-ID	Details zur Anwender-sys_ID für den auditierten Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Anwender, der die Änderung vorgenommen hat.
Erstellt	Zeitpunkt und Datum der Durchführung des Audits.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Gruppenpfade

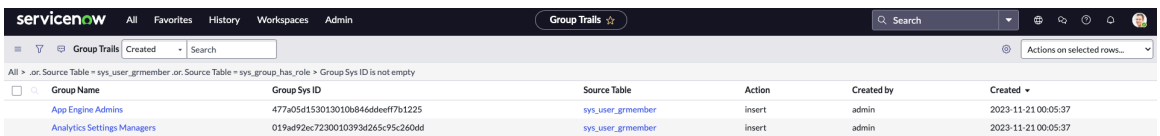
Zeigt Audits von Gruppen in an ServiceNow® Instanz.

Gruppenpfade zeigen Attributänderungen, Mitgliedschaftsänderungen und Rollenänderungen für eine Gruppe an.

Um auf Gruppenpfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Gruppenpfade**an. Die Seite „Gruppenpfade“ wird mit den folgenden Informationen angezeigt.

Gruppenpfade

Gruppenname	Name der Gruppe.
Gruppen-SYS-ID	Details zur Gruppen-sys_ID für den auditierten Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Anwender, der die Änderung vorgenommen hat.
Erstellt	Zeitpunkt und Datum der Durchführung des Audits.



Rollenpfade

Zeigt Audits von Rollen in an ServiceNow® Instanz.

Automatische Übersetzung

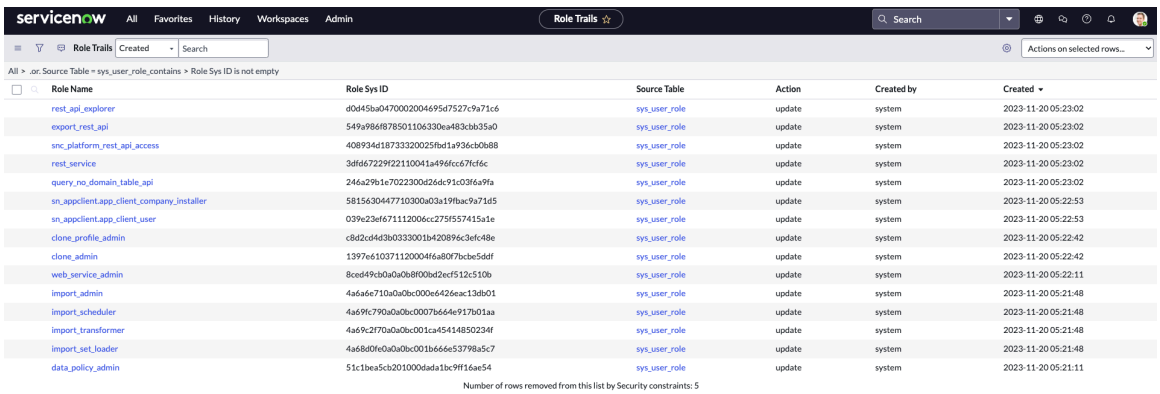
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenpfade zeigen Attributänderungen und über- und untergeordnete Beziehungsänderungen für eine Rolle an.

Um auf Rollenpfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Rollenpfade**an. Die Seite „Rollenpfade“ wird mit den folgenden Informationen angezeigt.

Rollenpfade

Rollenname	Name der Rolle.
Rollen-SYS-ID	Details zur sys_ID der Rolle für den auditierten Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.
Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Anwender, der die Änderung vorgenommen hat.
Erstellt	Zeitpunkt und Datum der Durchführung des Audits.



ACL-Pfade

Zeigt Audits von ACLs in an ServiceNow® Instanz.

ACL-Pfade zeigen Attributänderungen und erforderliche Rollenbeziehungsänderungen für eine ACL an.

Um auf die ACL-Pfade zuzugreifen, navigieren Sie zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **ACL-Pfade**an. Die Seite „ACL-Pfade“ wird mit den folgenden Informationen angezeigt.

ACL-Pfade

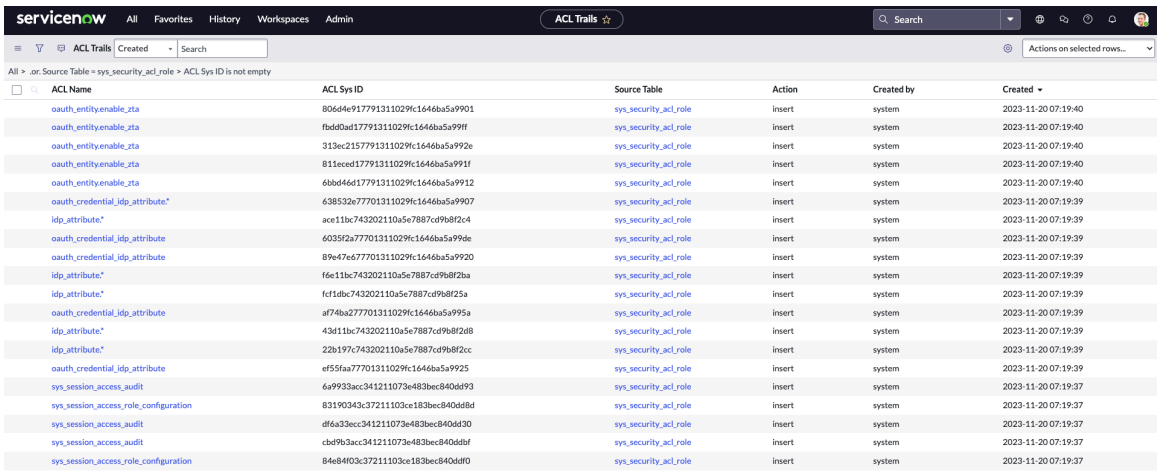
ACL-Name	Name der ACL.
ACL-SYS-ID	Details zur ACL-sys_ID für den auditierten Datensatz.
Quelltabelle	Details zur Quelltabelle, in der das Audit durchgeführt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACL-Pfade (Fortsetzung)

Aktion	Beschreibt die Audit-Aktion.
Erstellt von	Der Anwender, der die Änderung vorgenommen hat.
Erstellt	Zeitpunkt und Datum der Durchführung des Audits.



Prüfbare Felder für Sicherheit

Zeigt Details auf Tabellen- und Feldebene an, die in geprüft werden ServiceNow® Instanz.

Auditierbare Sicherheitsfelder zeigen die Details von Tabellen und Feldern an, die im auditiert werden ServiceNow Instanz.

Navigieren Sie zu , um auf die Seite für auditierbare Sicherheitsfelder zuzugreifen **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Tabellen und Felder konfigurieren**an. Die Seite „auditierbare Sicherheitsfelder“ wird mit den folgenden Informationen angezeigt.

Prüfbare Felder für Sicherheit

Spaltenname	Beschreibung
Zu prüfende Tabelle	Details der Tabelle, die geprüft wird.
Audit-Speicherziel	Details des Ziels, in dem die Audit-Details gespeichert werden.
Feldliste	Audits werden für in der Liste angegebene Felder durchgeführt.
Erstellen	Auditieren Sie die Changes, die sich auf den Vorgang „Erstellen“ beziehen.
Aktualisieren	Auditieren Sie die Changes, die sich auf den Aktualisierungsvorgang beziehen.
Löschen	Auditieren Sie die Changes, die sich auf den Löschvorgang beziehen.
Aktiv	Audit nur, wenn die Konfiguration für die Tabelle aktiv ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

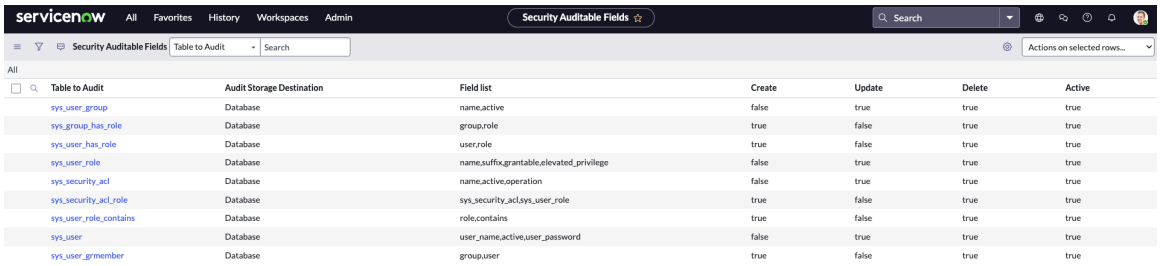


Table to Audit	Audit Storage Destination	Field list	Create	Update	Delete	Active
sys_user_group	Database	name,active	false	true	true	true
sys_group_has_role	Database	group,role	true	false	true	true
sys_user_has_role	Database	user,role	true	false	true	true
sys_user_role	Database	name,suffix,grantable,elevated_privilege	false	true	true	true
sys_security_acl	Database	name,active,operation	false	true	true	true
sys_security_acl_role	Database	sys_security_acl,sys_user_role	true	false	true	true
sys_user_role_contains	Database	role,contains	true	false	true	true
sys_user	Database	user_name,active,user_password	false	true	true	true
sys_user_grmember	Database	group,user	true	false	true	true

Die folgenden Tabellen können mit dem Audit für Identität und Zugriff geprüft werden:

- Gruppe [sys_user_Group]
- Rolle [sys_user_role]
- Zugriffssteuerung [sys_Security_acl]
- Anwender [sys_user]
- Gruppenrolle [sys_Group_has_role]
- Anwenderrolle [sys_user_has_role]
- Zugriffsrollen [sys_Security_acl_role]
- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember]

Tabellen und Felder werden konfiguriert

Audit für Identität und Zugriff, um die Änderungen zu verstehen, die für einen Anwender, eine Gruppe, eine Rolle und eine ACL vorgenommen wurden.

Vorbereitungen

Erforderliche Rolle: security_admin

Sie müssen Ihre Rolle auf Sicherheitsadministrator erhöhen, um Tabellen und Felder für das Audit von Identität und Zugriff zu konfigurieren.

Die folgenden Tabellen können für Audits konfiguriert werden

- Gruppe [sys_user_Group]
- Rolle [sys_user_role]
- Zugriffssteuerung [sys_Security_acl]
- Anwender [sys_user]
- Gruppenrolle [sys_Group_has_role]
- Anwenderrolle [sys_user_has_role]
- Zugriffsrollen [sys_Security_acl_role]
- Enthaltene Rolle [sys_user_role_contains]
- Gruppenmitglied [sys_user_grmember]

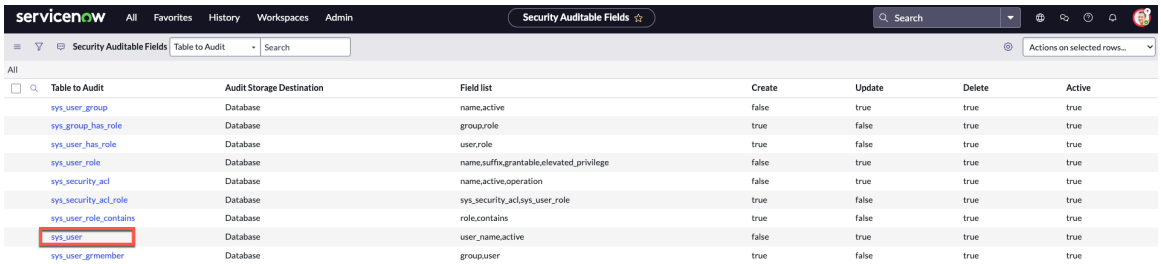
Hinweis: Informationen dazu, welche Felder für die Tabellen konfiguriert werden können, finden Sie unter Unterstützte und nicht unterstützte Felder in Identitätszugriff und Audit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

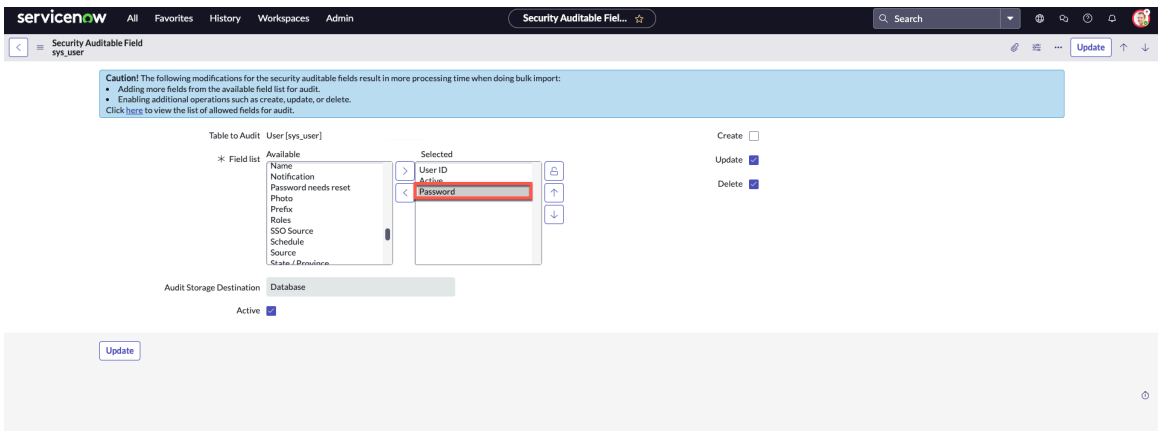
1. Navigieren zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Tabellen und Felder konfigurieren**an.
2. Wählen Sie die Tabelle aus, aus der Sie ein Feld auditieren möchten.

   Beispiel: **sys_user** .



3. Fügen Sie das zu prüfende Feld hinzu.

   Beispiel: **Passwort** .



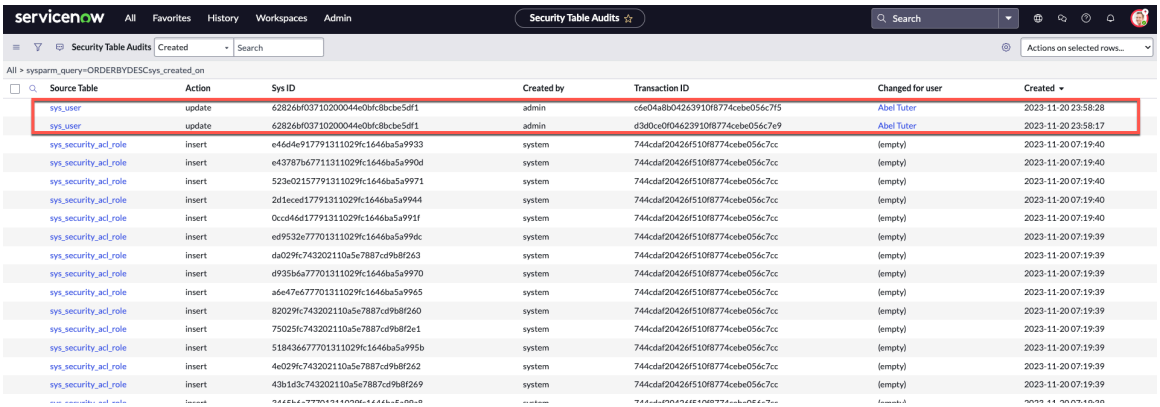
> **Hinweis:** Die folgenden Änderungen für die auditierbaren Sicherheitsfelder führen beim Massenimport zu mehr Verarbeitungszeit:
>
> - Hinzufügen weiterer Felder aus der Liste der verfügbaren Felder für Audit.
> - Aktivieren zusätzlicher Vorgänge wie Erstellen, Aktualisieren oder Löschen.

4. Aktualisieren Sie den Datensatz.

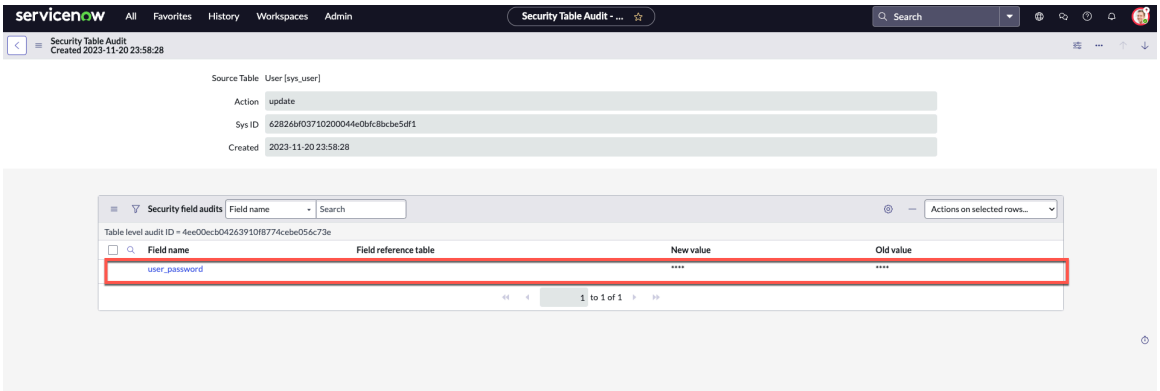
   Alle Änderungen am Passwortfeld fügen den Audits der Sicherheitstabelle einen neuen Datensatz hinzu. In diesem Beispiel zeigt das Audit ein geändertes Passwortfeld für den Anwender an **Abel Tuter** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie den erstellten Datensatz auswählen, werden die Details der Changes angezeigt.



Aufbewahrungszeitraum Wird Konfiguriert

Konfigurieren Sie den Aufbewahrungszeitraum für das Audit von Identität und Zugriff.

Vorbereitungen

Erforderliche Rolle: Administrator

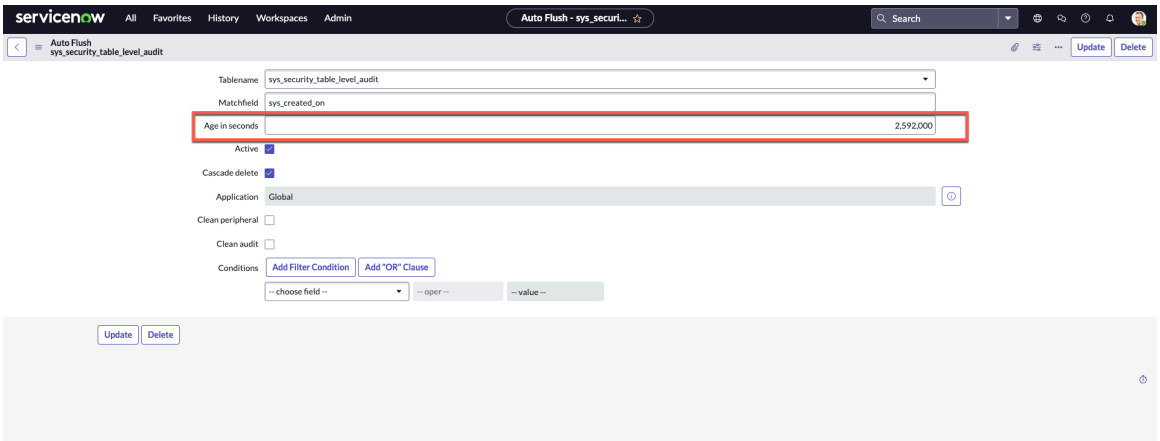
Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Identitäts- und Zugriffsaudit** > **Aufbewahrungszeitraum konfigurieren**an.
2. Im Formular können Sie das Alter in Sekunden ändern.

> **Hinweis:** Die maximale Anzahl von Tagen für das Identitäts- und Zugriffsaudit beträgt 30 Tage (2.592.000 Sekunden).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Speichern oder aktualisieren Sie den Datensatz.

Unterstützte und nicht unterstützte Felder in Identitätszugriff und Audit

Liste der Felder, die für das Audit unterstützt und nicht unterstützt werden.

Die Validierung von Audit-Feldern verhindert, dass einige Felder in der Tabelle „field_list“ in der Tabelle „Sicherheitsfeld-Audit-Konfiguration“ (sys_sec_field_Audit_config) ausgewählt werden.

Feld wird für Audit unterstützt oder nicht unterstützt

Tabelle	Felder unterstützt oder nicht unterstützt
Alle Tabellen	Felder, die nicht unterstützt werden: • Erstellt am (sys_created_on) • Erstellt von (sys_created_by) • Aktualisiert von (sys_updated_by) • Aktualisiert am (sys_updated_on)
Anwender hat Rolle (sys_user_has_role)	Unterstützte Felder: • Anwender • Rolle • Geerbt • Anzahl
Benutzer (sys_user)	Felder, die nicht unterstützt werden: • Letzte Anmeldung (Last_login) • Zeit der letzten Anmeldung (Last_login_time) • Letztes Anmeldegerät (Last_login_device)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld wird für Audit unterstützt oder nicht unterstützt (Fortsetzung)

Tabelle	Felder unterstützt oder nicht unterstützt
	• Multifaktor-Authentifizierung aktivieren (enable_multifactor_authn) • Standardperspektive (default_perspective) • Kalenderintegration (Calendar_Integration) • Föderierte ID (Federated_ID) • Passwort muss zurückgesetzt werden (password_needs_Reset) • Fehlgeschlagene Versuche (failed_attempts) • Letztes Passwort (Last_password) • LDAP-Server (ldap_Server) • Gesperrt (locked_out) • Benachrichtigung (Benachrichtigung) • Rollen (Rollen) • Domäne (sys_Domain) • Domänenpfad (sys_Domain_path) • Zeitformat (time_Format) • Anwender-ID mit Hash (Hash_user_ID) • Klassenname (sys_class_Name) • MOD-Anzahl (sys_mod_count)

Identity Center

Ermöglicht Ihnen das Überwachen, Verwalten und Minimieren identitätsbasierter Risiko- und Sicherheitslücken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen von Identity Center.

Aktivieren



Erfahren Sie, wie Sie Identity Center aktivieren.

Identitätsmetriken für Administratoren



Erfahren Sie, wie die Berechtigungen ausgewertet werden.

Identity Center für Anwender



Rufen Sie Details zu den häufig gestellten Fragen zur Zugriffsanalyse ab.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identity Center Erkunden

Identity Center ist eine Sammlung von Anwenderattributen, Zugriff, Geräten, Anmeldeverlauf, Sicherheitsaktivitäten, und vieles mehr.

Identity Center bietet Funktionen zum Überwachen, Verwalten und Minimieren identitätsbasierter Risiko- und Sicherheitslücken.

Identity Center ist eine zentrale Anlaufstelle für die Überwachung, Verwaltung und Minimierung identitätsbasierter Risiko- und Sicherheitslücken ServiceNow.

Um das Identity Center zu aktivieren, installieren Sie das Identity Center (Com.snc.Identity_Center)-Plugin. Identity Center ist für Endanwender verfügbar, um die Details zu den aktiven Sitzungen, dem Anmeldeverlauf und vertrauenswürdigen Geräten mit dem Identity Center anzuzeigen. Weitere Informationen finden Sie unter Identity Center für Anwender.

Identity Center wird aktiviert

Installieren Sie für Identity Center das Identity Center (Com.snc.Identity_Center)-Plugin.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie das Identity Center (Com.snc.Identity_Center) Plugin mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

   Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Identity Center für Anwender

Zeigen Sie Details zu Ihren aktiven Sitzungen, dem Anmeldeverlauf und vertrauenswürdigen Geräten im Identity Center an.

Identity Center ist eine Sammlung von Anwenderattributen, Geräten, Anmeldeverlauf, Sicherheitsaktivitäten und vielem mehr. Es bietet eine Einzelbereichsansicht aller Daten mit zusätzlichen Sicherheitssteuerungen und Benachrichtigungsfunktionen.

Mit dem Identity Center können Sie Details zu Ihren aktiven Sitzungen, dem Anmeldeverlauf und vertrauenswürdigen Geräten anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um auf das Identity Center für Anwender zuzugreifen, navigieren Sie zu einer der folgenden Optionen:

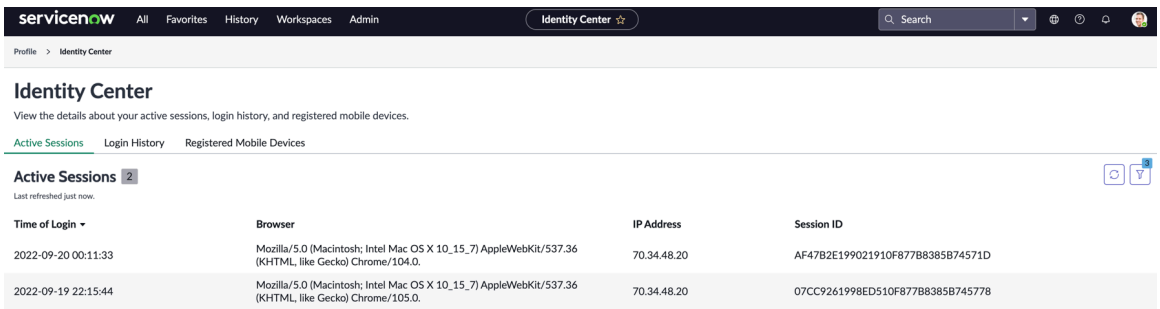
- Ein ServiceNow AI Platform, Navigieren Sie zu **Alle** > **Self-Service** > **Mein Profil** Und wählen Sie aus **Zeigen Sie Das Identity Center An** Im Abschnitt zugehörige Links.

  Hinweis: Sie können auch auf Ihr Profil zugreifen, indem Sie Ihren Anwendernamen im Instanzheader auswählen.



- Ein Now Support, Wählen Sie das Profil aus, und wählen Sie aus **Zeigen Sie Das Identity Center An** Unten auf der Seite.

Die Seite „Identity Center“ wird wie folgt angezeigt:



Identity Center verfügt über die folgenden Registerkarten:

- Aktive Sitzungen
- Anmeldungsverlauf
- Registrierte Mobilgeräte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können diese Registerkarten auswählen, um Details wie Browser, IP-Adressen, Sitzungsbeziehungsinformationen, Anmeldeinformationen und Ihre registrierten Mobilgeräte anzuzeigen.

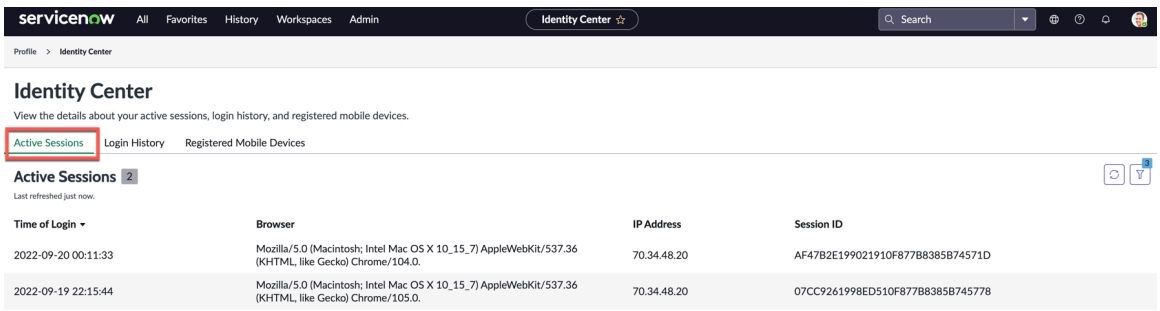
Aktive Sitzungen im Identity Center anzeigen

Zeigt die Informationen zu den Anwendersitzungen an.

Aktive Sitzungen sind die Sitzungen, die für die aktuelle geöffnet sind ServiceNow®#Instanz mit verschiedenen Browsern oder Geräten.

Die Registerkarte aktive Sitzungen im Identity Center hilft Ihnen, Ihre Sitzungen basierend auf Browser, IP-Adresse und Sitzungs-ID zu identifizieren. Mit diesen Informationen können Sie erforderliche Aktionen ausführen, z. B. die Sitzung verlängern oder beenden.

Die Verwendung dieser Informationen kann helfen, festzustellen, ob die Sitzungen real sind und keine Sicherheitsbedenken darstellen.



Anmeldeverlauf in Identity Center anzeigen

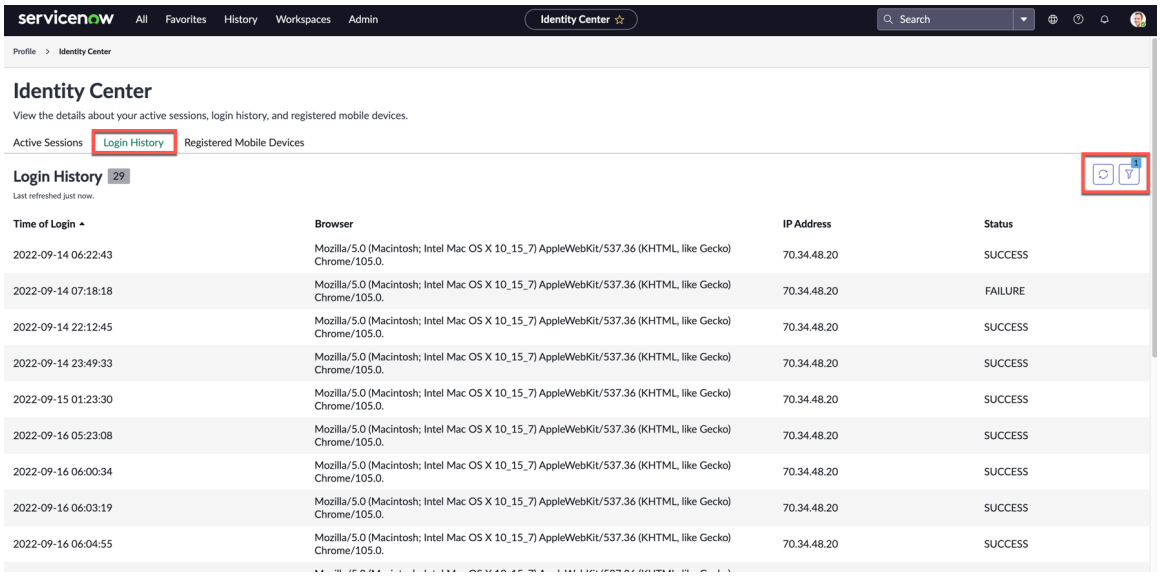
Stellt Details zu Ihrem Anmeldeverlauf bereit.

Die Registerkarte Anmeldeverlauf im Identity Center hilft Ihnen bei Ihren Anmeldeinformationen und dem Status Ihrer Anmeldung.

Sie können die Filter verwenden, um Anmeldeaktionen anzugeben, um Sicherheitsuntersuchungen zu unterstützen. Filter können helfen, festzustellen, ob die Aktivität echt oder verdächtig war, und die Informationen an Ihren Administrator zu melden.

Die Paginierung im Anmeldeverlauf ist standardmäßig 20 und kann auf maximal 100 festgelegt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Folgenden finden Sie einige der anderen Details aus dem Anmeldeverlauf:

- Die Zeit der Anmeldung ist die aktualisierte Zeit, zu der die Mobilgeräte für den Zugriff auf die Instanz verwendet werden.
- Die Datensätze werden 30 Tage lang im Identity Center gespeichert.

Registrierte Mobilgeräte im Identity Center anzeigen

Geben Sie Details zu Ihrem registrierten Mobilgerät auf der an ServiceNow Instanz.

Auf der Registerkarte registrierte Mobilgeräte im Identity Center werden Details zu Ihren registrierten Geräten angezeigt, die für den Zugriff auf verwendet wurden ServiceNow Instanz.

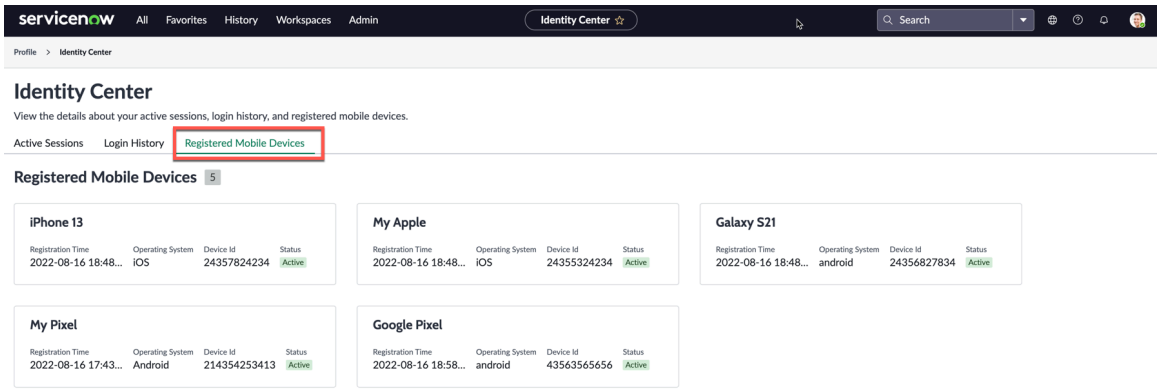
Wenn das Modul „Adaptive Authentifizierung“ aktiviert ist und ein registriertes Mobilgerät registriert ist, zeigt das Identity Center die Details zu Ihren registrierten Geräten an.

Darüber hinaus werden auch Details der Geräte angezeigt, z. B. Betriebssystem, Geräte-ID und Status des Geräts sowie die Registrierungszeit des Geräts.

Um Ihr Mobilgerät zu registrieren, müssen Sie sicherstellen, dass die adaptive Authentifizierung (`com.snc.adaptive_authentication`) Plugin ist installiert, und Sie haben Ihre Trusted Mobile App-Funktion aktiviert. Weitere Informationen finden Sie unter Aktivieren Sie Trusted Mobile App.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Identitätsmetriken für Administratoren

Zeigen Sie Trends der Anwender, privilegierten Anwender, aktiven Sitzungen und integrierten Accounts auf Ihrem an ServiceNow Instanz.

Identitätsmetriken für Administratoren haben die Trends für Folgendes:

- Anwender
- Privilegierte Anwender
- Integration oder nicht-menschliche Accounts
- Aktive Sitzungen
- Inaktive Sitzungen

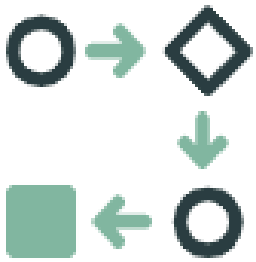
Weitere Informationen finden Sie unter Sicherheitscenter-Metriken.

Rechneridentitätskonsole

Verwalten Sie Ihre Service-Accounts, die für Integrationen mit verwendet werden ServiceNow.

Rechneridentitäten sind digitale Identitäten, die mit Systemen und Daten interagieren. Diese Identitäten werden verwendet, um Aufgaben autonom auszuführen. Die Computer-Identitätskonsole hilft Ihnen, die Sicherheitspunktzahl dieser Identitäten zu verstehen und Empfehlungen zu geben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen	Aktivieren	Konfigurieren
		
Erfahren Sie mehr über die Funktionen und den Geschäftsnutzen der Machine Identity Console.	Erfahren Sie, wie Sie die Konsole für die Computeridentität aktivieren.	Konfigurieren Sie eingehende Integrationen mit der Computer Identity Console.

Computeridentitätskonsole Erkunden

Verwalten Sie Ihre Service-Accounts, die für Integrationen mit verwendet werden ServiceNow.

Mit der Machine Identity Console können Sie Ihre nicht-menschlichen Identitäten (NHIs) verwalten, die zum Identifizieren, Authentifizieren und Autorisieren verschiedener Softwareentitäten für den Zugriff auf gesicherte Ressourcen von verwendet werden ServiceNow. Zu den Entitäten, die Zugriff erhalten, gehören Anwendungen, Arbeitsauslastungen, APIs, Bots und automatisierte Systeme. Im Gegensatz zu menschlichen Identitäten werden nicht-menschliche Identitäten (NHIs) nicht auf dieselbe Weise verwaltet und sind nicht direkt einem Menschen zugeordnet. Ihre Identitäts- und Verifizierungsmethoden unterscheiden sich von den menschlichen Anwendern, und standardmäßige menschliche Sicherheitsmaßnahmen gelten nicht für sie.

https://player.vimeo.com/video/1101308622?h=b01d69f65a&badge=0&autopause=0&player_id=0&app_id=58479

Folgendes ist auf der Seite „Übersicht über die Computeridentitätskonsole“ verfügbar:

- Gesamtzahl der Computer-Identitäts-Accounts (Integration) und die Accounts mit Rollen mit hohen Berechtigungen.
- Individuelle API-Aufrufe – Letzte 7 Tage
- Verwendete Authentifizierungsmethoden – Letzte 7 Tage
- Sicherheitspunktzahl für Rechneridentität und Ergebnisse im Zusammenhang mit der Identität.

Zugehörige Informationen

Machine Identity Console Wird Aktiviert

Sicherheitsergebnisse

Metriken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellungen Der Computeridentitätskonsole

Eingehende Integrationen

Eingehende Integrationen

Mit eingehenden Integrationen in der Computer-Identitätskonsole können Sie externe Anwendungen konfigurieren und verwalten, um auf ServiceNow-APIs zuzugreifen.

Die eingehenden Integrationen in der Machine Identity Console von ServiceNow helfen Ihnen, Integrationen und Anwendungen zu verwalten und zu konfigurieren, die eine Verbindung zur ServiceNow-Plattform herstellen. Es fungiert als zentraler Hub zum Speichern von Anwendungseinstellungen und API-Anmeldeinformationen und stellt eine sichere Kommunikation zwischen ServiceNow und externen Systemen sicher. Weitere Informationen finden Sie unter Neue Experience für eingehende Integrationen.

Verbindungstypen:

- OAuth – Autorisierungscodegewährung: Greifen Sie auf eine Ressource zu, indem Sie sich direkt bei einem OAuth-Server authentifizieren, der der Ressource vertraut. Weitere Informationen finden Sie unter Konfigurieren Sie eine OAuth-Autorisierungscodegewährung.
- OAuth: Client-Anmeldeinformationsgewährung: Wird für eingehende Integrationen von einem OAuth-Client eines Drittanbieters auf die ServiceNow-Plattform verwendet. Weitere Informationen finden Sie unter Konfigurieren Sie eine OAuth-Client-Anmeldeinformationsgewährung.
- OAuth: JWT-Bearer-Gewährung: Verwenden Sie eine JSON-Webtoken-Berechtigung (JWT), um sich bei Ihrer Instanz zu authentifizieren. Weitere Informationen finden Sie unter Konfigurieren Sie eine OAuth-JSON-Webtoken-Bearer-Gewährung.
- Drittpartei-ID-Token, das vom OIDC-unterstützenden Identitätsanbieter ausgegeben wird: Konfigurieren Sie einen OAuth-OIDC-Anbieter, um Identitätstoken zu akzeptieren, die von einem Drittpartei-OIDC-Anbieter mithilfe eingehender API-Aufrufe generiert wurden. Weitere Informationen finden Sie unter Konfigurieren Sie ein Drittpartei-ID-Token.
- OAuth: Gewährung von Passwortanmeldeinformationen des Ressourcenbesitzers: Autorisieren Sie den Zugriff auf einen OAuth-Endpunkt mithilfe des Authentifizierungscode-Flows. Weitere Informationen finden Sie unter Konfigurieren Sie die Gewährung der Passwortanmeldeinformationen für den OAuth-Ressourcenbesitzer.

> **Hinweis:** Für den Autorisierungscode-Flow muss der Anwender die Authentifizierung durch lokale Anmeldung, SSO oder MFA abschließen und dann seine Zustimmung erteilen.

Weitere Informationen finden Sie unter .

Zugehörige Informationen

Eingehende Integrationen

Konfigurieren Sie eine OAuth-Autorisierungscodegewährung

Konfigurieren Sie eine OAuth-JSON-Webtoken-Bearer-Gewährung

Konfigurieren Sie ein Drittpartei-ID-Token

Konfigurieren Sie eine OAuth-Client-Anmeldeinformationsgewährung

Konfigurieren Sie die Gewährung der Passwortanmeldeinformationen für den OAuth-Ressourcenbesitzer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsergebnisse

Stellt Sicherheitspunktzahl und -Ergebnisse für die Rechneridentität bereit.

Sicherheitspunktzahl und Ergebnisse der Rechneridentität

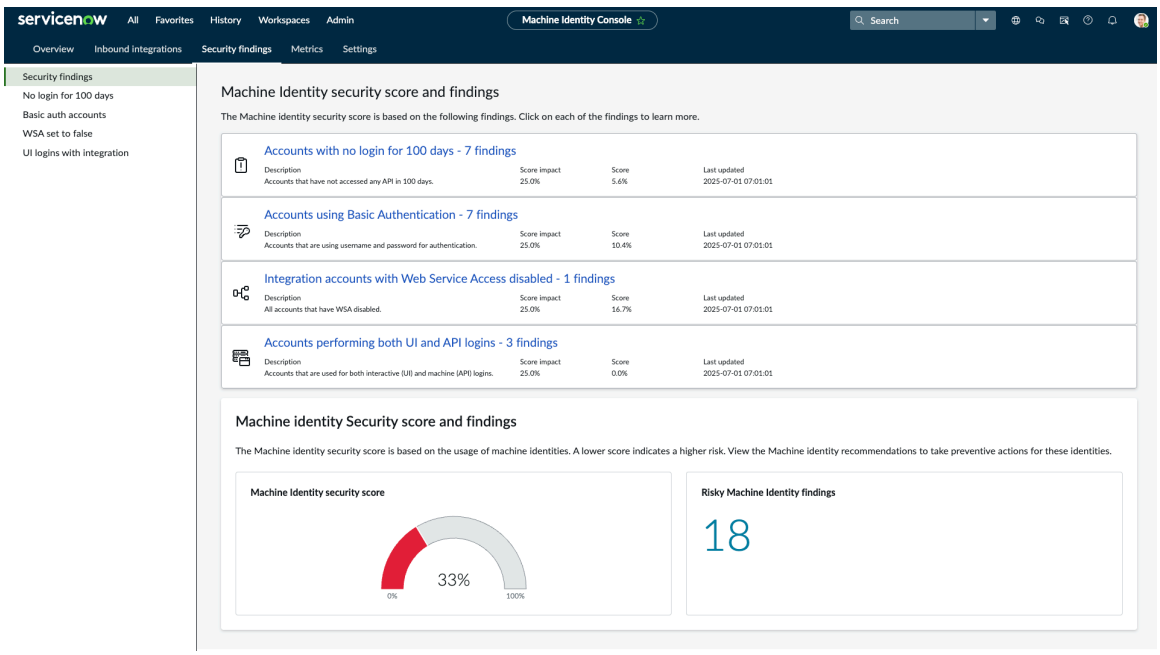
Die Sicherheitspunktzahl wird für die folgenden Sicherheitsergebnisse angezeigt. Sie können die einzelnen Ergebnisse auswählen, um weitere Informationen zu erhalten.

Sicherheitsergebnisse

Ergebnisse	Beschreibung
Accounts ohne Anmeldung seit 100 Tagen	Ergebnisse zu den Accounts, die seit 100 Tagen auf keine API zugegriffen haben.
Accounts mit Standardauthentifizierung	Ergebnisse zu den Accounts, die Anwendername und Passwort für die Authentifizierung verwenden.
Integrationsaccounts mit Webservice-Zugang deaktiviert	Ergebnisse zu allen Accounts, für die WSA deaktiviert ist.
Accounts, die sowohl UI- als auch API-Anmeldungen ausführen	Ergebnisse zu den Accounts, die für interaktive Anmeldungen (UI) und Computer (API) verwendet werden.

Sicherheitspunktzahl und Ergebnisse der Rechneridentität

Die Sicherheitspunktzahl basiert auf der Nutzung und Methode der Rechneridentitäten. Eine niedrigere Punktzahl weist auf ein höheres Risiko hin. Sie können die Empfehlungen anzeigen, um Präventivmaßnahmen für diese Identitäten durchzuführen.



Accounts ohne Anmeldung seit 100 Tagen

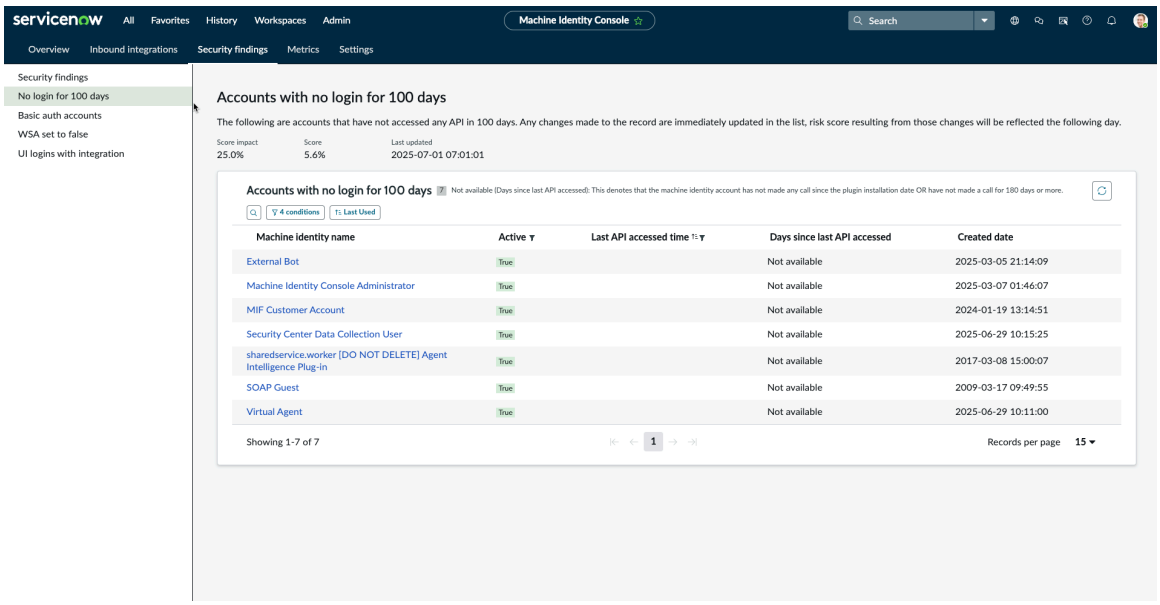
Zeigen Sie die Ergebnisse zu den Accounts an, die seit 100 Tagen nicht auf eine API zugegriffen haben, unter den Sicherheitsergebnissen in der Konsole für Computeridentität an.

Automatische Übersetzung

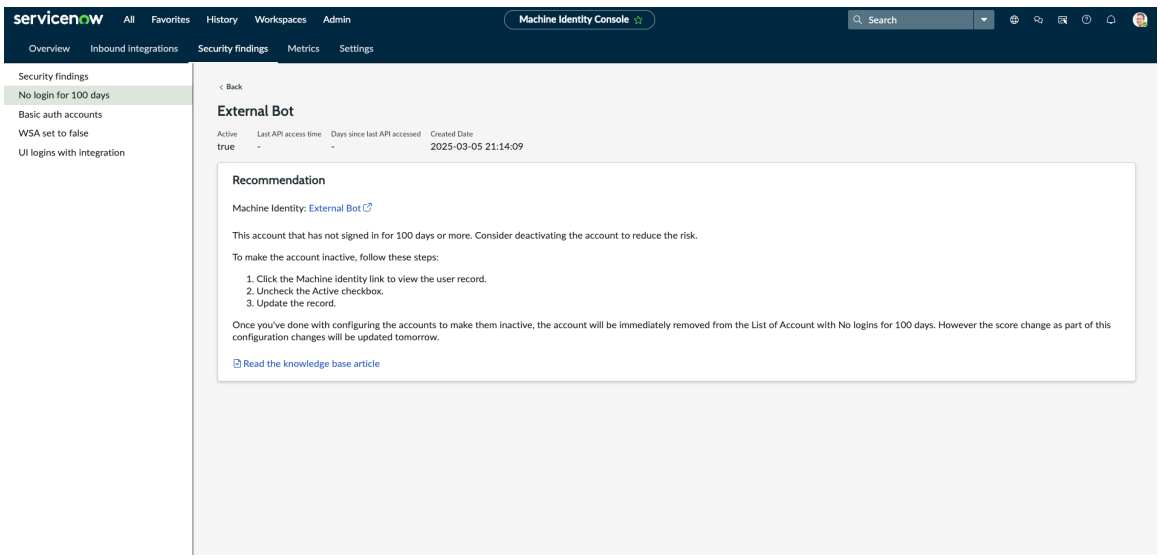
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Accounts ohne Anmeldung seit 100 Tagen zeigt die nicht-menschlichen Identität-Accounts an, die seit 100 Tagen auf keine API zugegriffen haben.

Hinweis: Alle Änderungen, die an dem auf dieser Seite angezeigten Datensatz vorgenommen wurden, werden sofort in der Liste aktualisiert. Die aus diesen Änderungen resultierende Risikopunktzahl wird am folgenden Tag berücksichtigt.



Sie können den Namen der Rechneridentität auswählen, um mehr über den Account und die Empfehlung zu erfahren, eine gute Sicherheitslage für den Account aufrechtzuerhalten.



Accounts mit Standardauthentifizierung

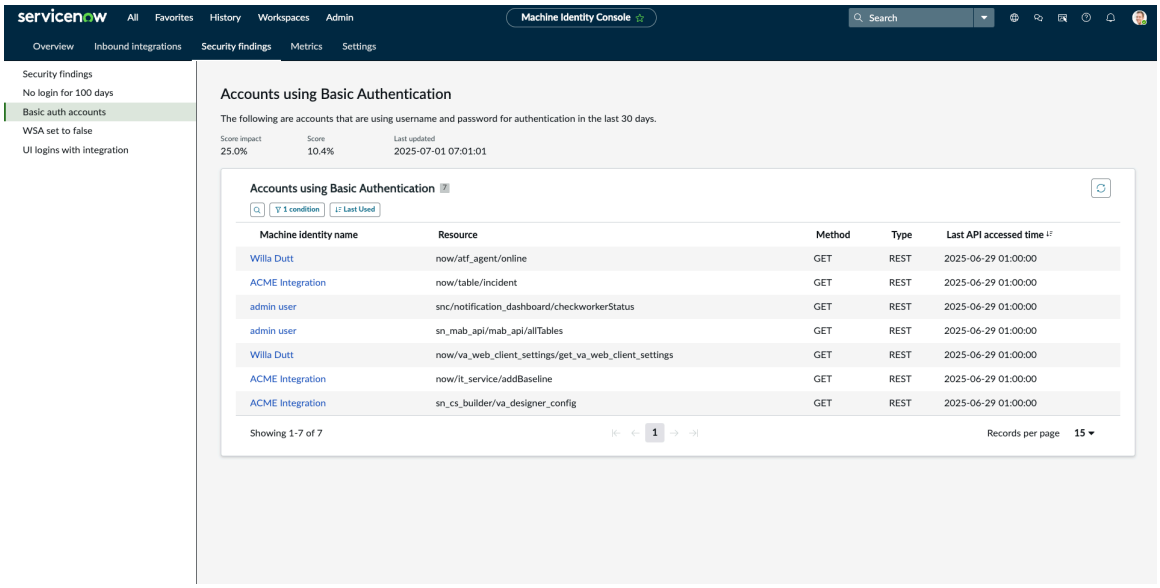
Zeigen Sie die Ergebnisse zu den Accounts an, die nur die Standardauthentifizierung zur Authentifizierung der APIs unter den Sicherheitsergebnissen in der Konsole für die Computeridentität verwenden.

Accounts mit Standardauthentifizierung zeigt die Accounts nicht menschlicher Identität an, die die Standardauthentifizierung für die APIs verwenden, um sich bei ServiceNow anzumelden.

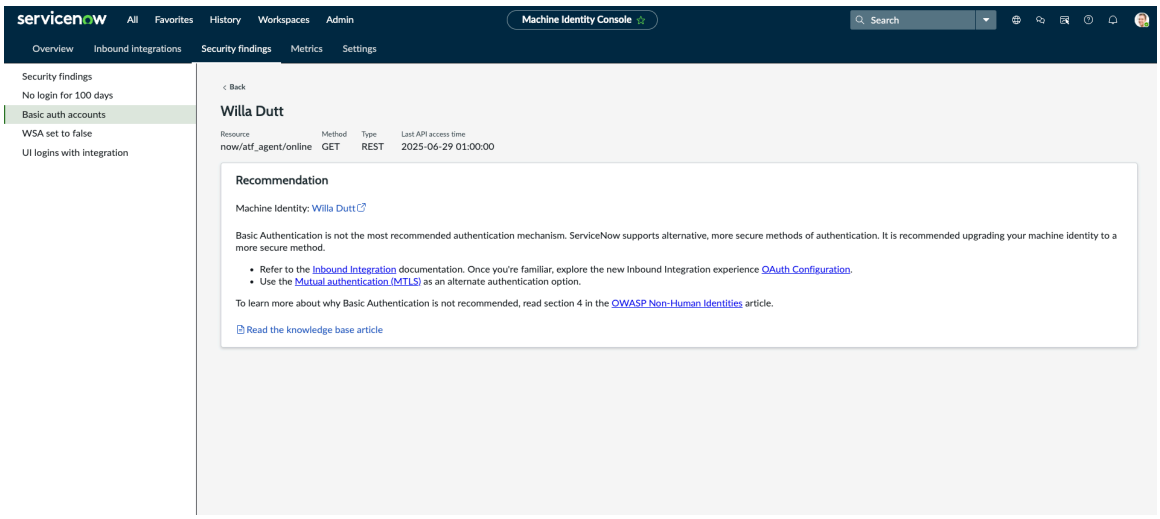
Hinweis: Die auf der Seite angezeigten Accounts sind die Accounts, die in den letzten 30 Tagen Anwendername und Passwort für die Authentifizierung verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung



Sie können den Namen der Rechneridentität auswählen, um mehr über den Account und die Empfehlung zu erfahren, eine gute Sicherheitslage für den Account aufrechtzuerhalten.



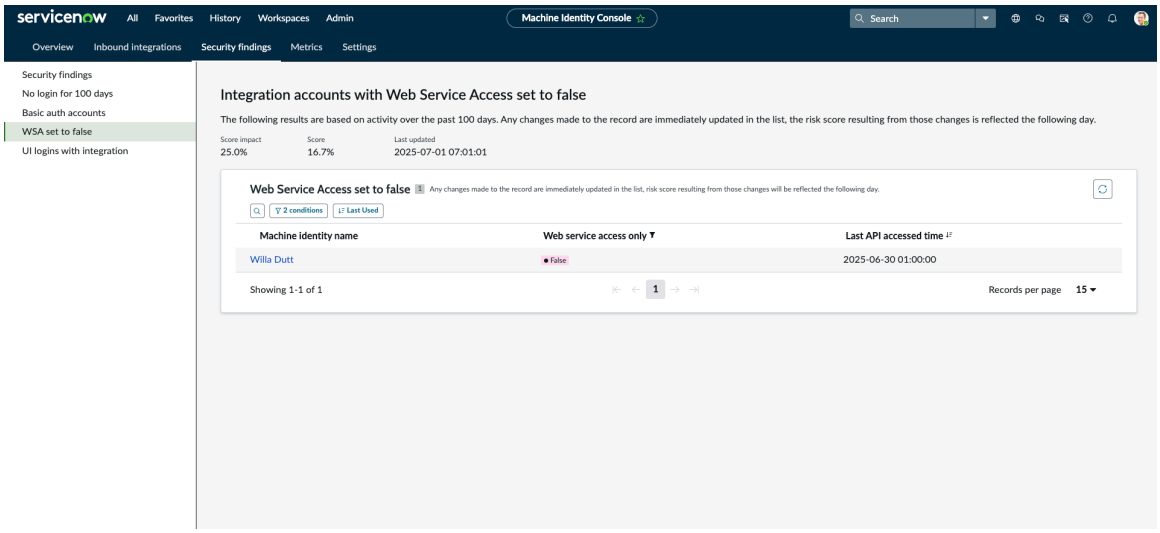
Integrationsaccounts mit Webservice-Zugang auf „falsch“ festgelegt

Zeigen Sie die Ergebnisse zu den Accounts an, die ServiceNow authentifizieren, wobei der Webservicezugriff unter den Sicherheitsergebnissen in der Konsole für die Computeridentität auf „falsch“ festgelegt ist.

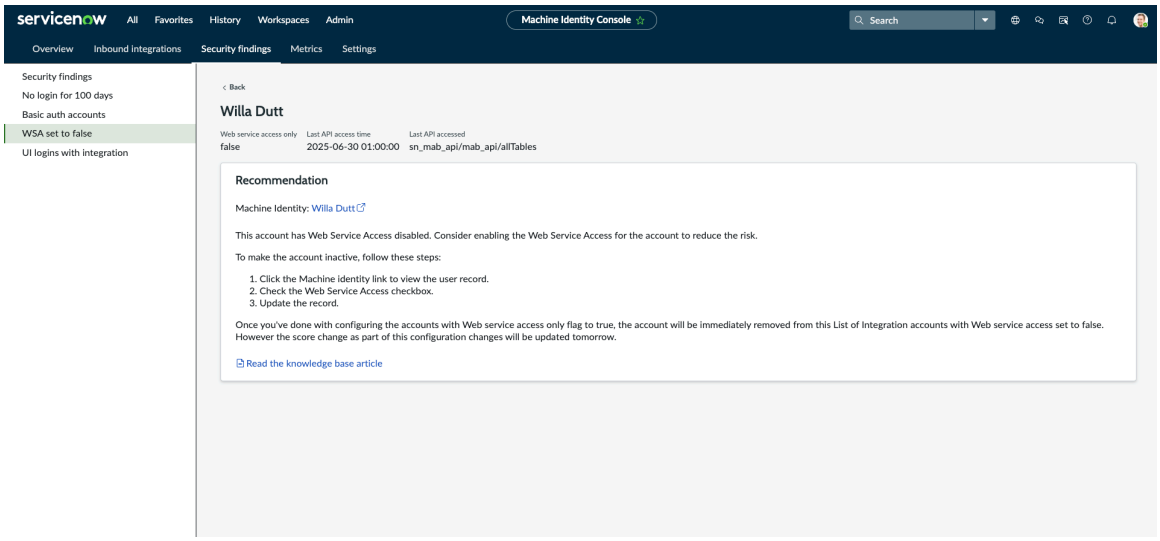
Integrationsaccounts mit Webservice-Zugriff auf „falsch“ zeigt die Accounts an, die die API verwenden, ohne dass der Webservice-Zugriff auf „falsch“ festgelegt ist.

Hinweis: Alle Änderungen, die an dem auf dieser Seite angezeigten Datensatz vorgenommen wurden, werden sofort in der Liste aktualisiert. Die aus diesen Änderungen resultierende Risikopunktzahl wird am folgenden Tag berücksichtigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können den Namen der Rechneridentität auswählen, um mehr über den Account und die Empfehlung zu erfahren, eine gute Sicherheitslage für den Account aufrechtzuerhalten.



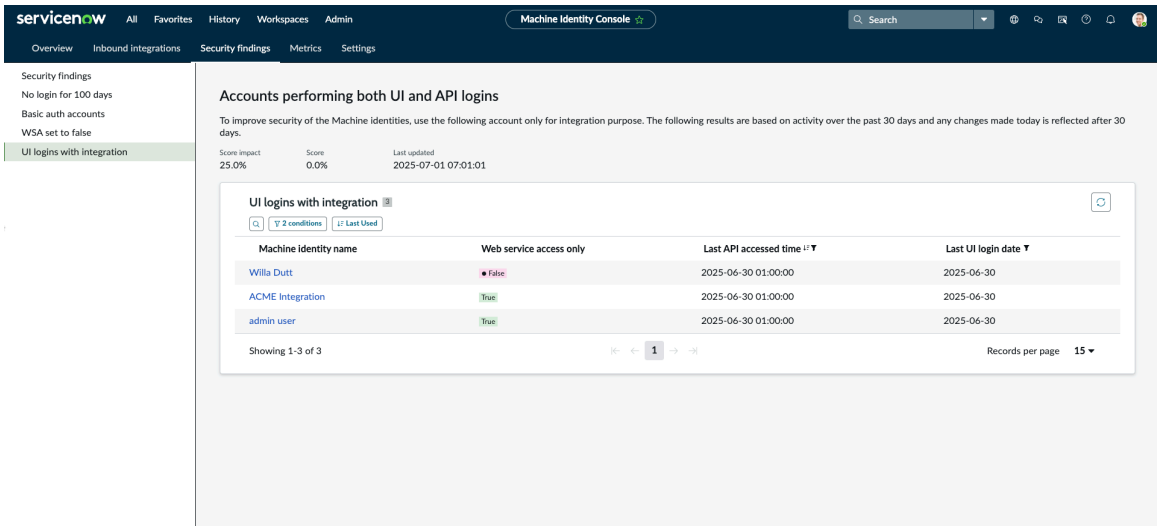
Accounts, die sowohl die UI- als auch die API-Anmeldung ausführen

Zeigen Sie die Ergebnisse zu den Accounts an, die eine UI- und API-Anmeldung durchführen, unter den Sicherheitsergebnissen in der Konsole für Computeridentität an.

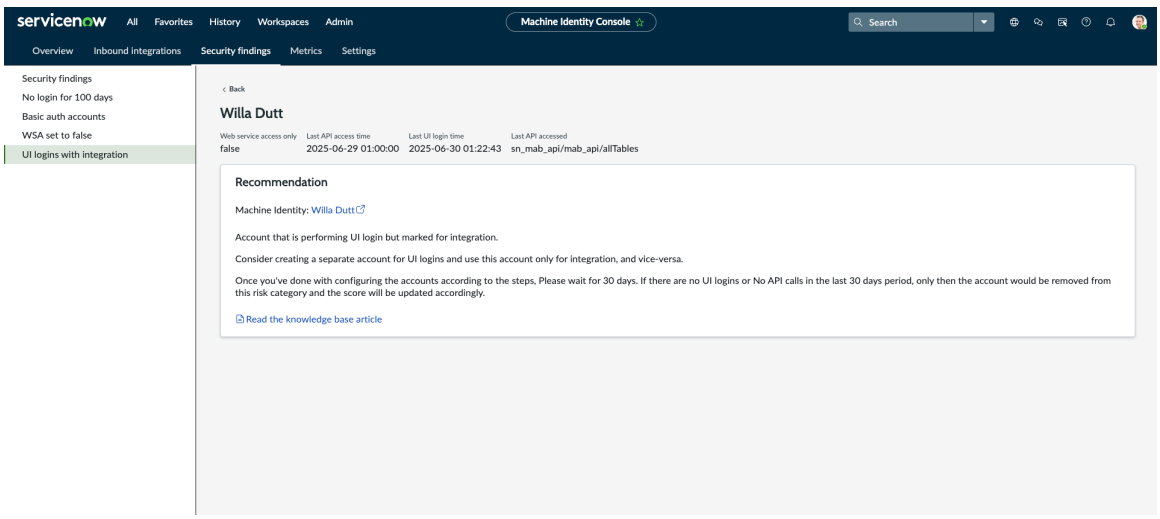
Accounts, die sowohl die UI- als auch die API-Anmeldung ausführen, zeigen die Accounts an, die die UI- und API-Anmeldung verwenden, um sich bei ServiceNow zu authentifizieren.

Hinweis: Die auf der Seite angezeigten Accounts basieren auf der Aktivität der letzten 30 Tage, und alle heute vorgenommenen Änderungen werden nach 30 Tagen berücksichtigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können den Namen der Rechneridentität auswählen, um mehr über den Account und die Empfehlung zu erfahren, eine gute Sicherheitslage für den Account aufrechtzuerhalten.



Metriken

Metriken der Rechneridentitäten.

Individuelle API-Aufrufe in den letzten 7 Tagen

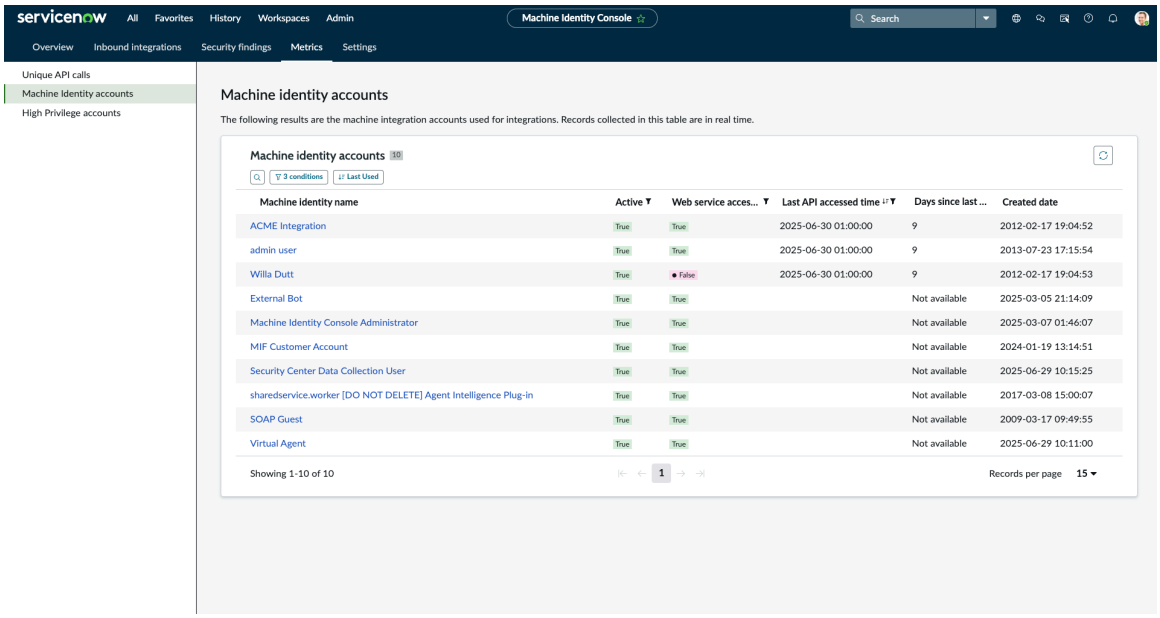
Die folgenden Ergebnisse sind eindeutige API-Aufrufe in den letzten 7 Tagen. In dieser Tabelle erfasste Datensätze werden in Echtzeit ausgeführt.

Computer-Identitätskonten

Die folgenden Ergebnisse sind die für Integrationen verwendeten Computer-Integrationsaccounts. In dieser Tabelle erfasste Datensätze werden in Echtzeit ausgeführt.

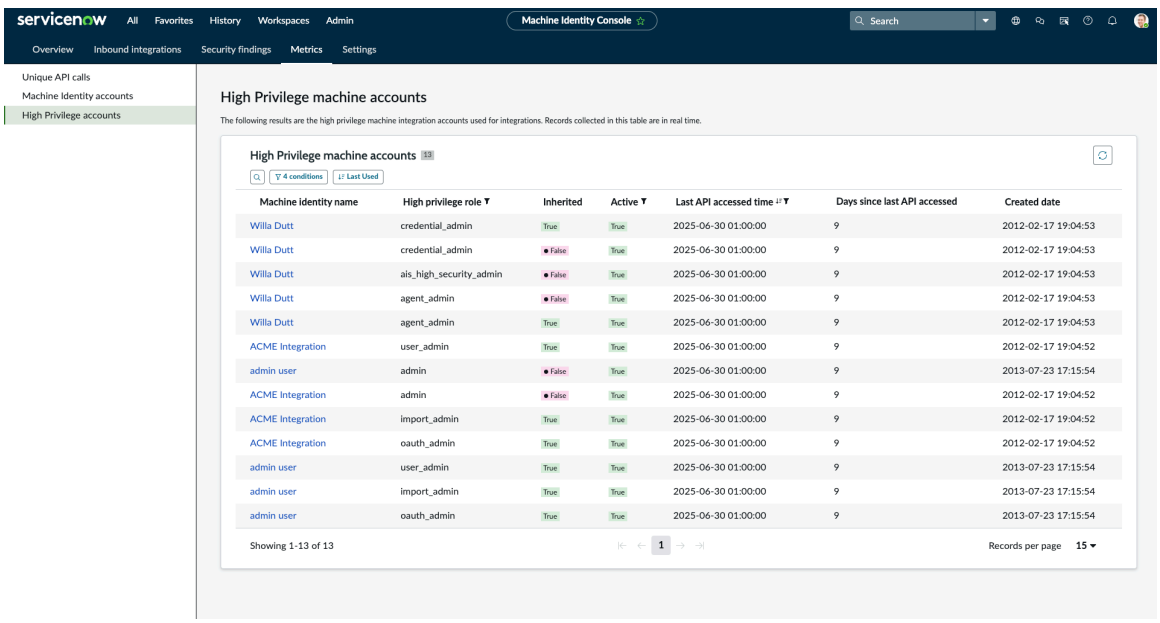
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Rechneraccounts mit hohen Berechtigungen

Die folgenden Ergebnisse sind die für Integrationen verwendeten Computer-Integrationsaccounts mit hohen Berechtigungen. In dieser Tabelle erfasste Datensätze werden in Echtzeit ausgeführt.



Einstellungen Der Computeridentitätskonsole

Konfigurieren Sie die Einstellungen für die Sicherheitspunktzahl der Computeridentität.

Vorbereitungen

Erforderliche Rolle: Mi_admin

Die folgende Aufgabe ist spezifisch für Ihre Organisation hinsichtlich der Handhabung der inaktiven Accounts.

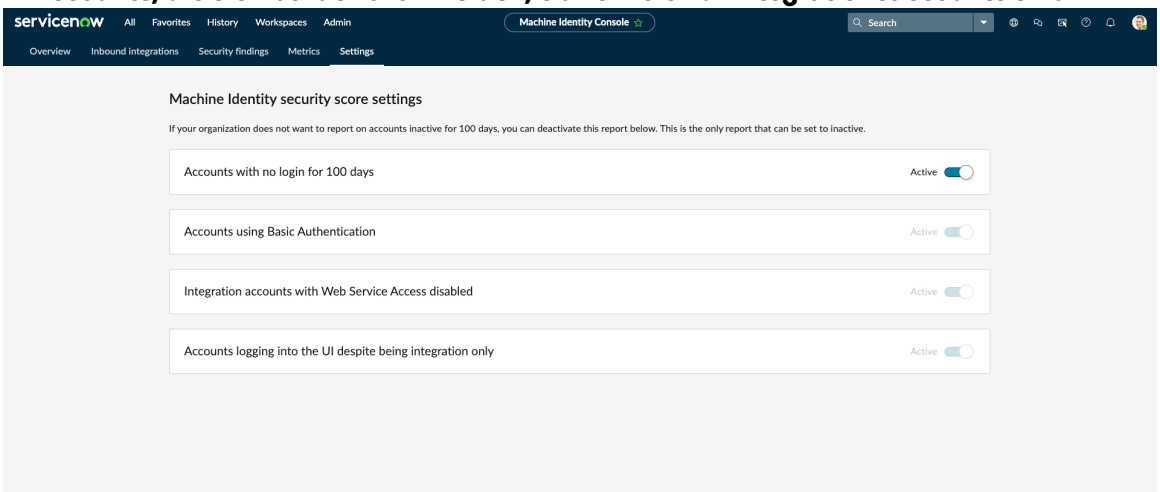
Hinweis: Wenn Ihre Organisation keine Berichte zu Accounts erstellen möchte, die seit 100 Tagen inaktiv sind, können Sie diesen Bericht unten deaktivieren. Dies ist der einzige Bericht, der auf „inaktiv“ festgelegt werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Rechneridentitätskonsole** > **Einstellungen**an.
2. Wählen Sie die Einstellungen basierend auf Ihren Anforderungen aus:
   - **Accounts ohne Anmeldung seit 100 Tagen**
   - **Accounts mit Standardauthentifizierung**
   - **Integrationsaccounts mit Webservice-Zugang deaktiviert**
   - **Accounts, die sich bei der UI anmelden, obwohl sie nur Integrationsaccounts sind**



Machine Identity Console Wird Aktiviert

Aktivieren Sie **Identitätsmanagement Für Computer** Com.Glide.Identity.Machine_Identity_Management Zum Verwalten Ihrer Service-Accounts, die für Integrationen mit verwendet werden ServiceNow.

Vorbereitungen

Erforderliche Rolle: Mi_admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach **Identitätsmanagement Für Computer** (Com.Glide.Identity.Machine_Identity_Management) Plugin mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Der Computer Identity Console

Verwalten Sie Ihre Service-Accounts, die für Integrationen mit ServiceNow verwendet werden, mithilfe der Machine Identity Console.

Vorbereitungen

Erforderliche Rolle: Mi_admin

Aktivieren Sie **Identitätsmanagement Für Computer** Com.Glide.Identity.Machine_Identity_Management Plugin. Weitere Informationen finden Sie unter Machine Identity Console Wird Aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Rechneridentitätskonsole** > **Rechneridentitätskonsole**an.
   Die Computer Identity Console verfügt über die folgenden Registerkarten:
   - Übersicht: Zeigt die Gesamtzahl der Computer-Identitätsaccounts und ihre Metriken an
   - Eingehende Integrationen: Konfigurieren Sie eingehende Integrationen für die APIs.
   - Sicherheitsergebnisse: Zeigt an, dass die Sicherheitspunktzahl auf verschiedenen Sicherheitsergebnissen basiert.
   - Metriken: Zeigt die verschiedenen Metriken für die Rechneridentitätsaccounts an
   - Einstellungen : Konfigurieren Sie die Konsole für die Rechneridentität.
2. Wählen Sie die entsprechenden Registerkarten basierend auf Ihren Sicherheitsanforderungen aus.

System für domänenübergreifendes Identitätsmanagement (SCIM)

Die System for Cross-Domain Identity Management (SCIM)-API stellt Endpunkte zum Erstellen, Lesen, Aktualisieren und Löschen von Vorgängen für Anwender und Gruppen bereit, die das SCIM-Protokoll verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Anbieter



Der SCIM-Anbieter synchronisiert die Änderungen, die an Identitäten im IdP vorgenommen werden, einschließlich Erstellen, Aktualisieren oder Löschen von Datensätzen.

SCIM-Client



Der SCIM-Client wird zum Erstellen, Aktualisieren und Löschen von Identitätsressourcen in einem System verwendet, das SCIM-konforme REST-Anforderungen unterstützt.

Das SCIM-Protokoll ist ein HTTP-basiertes Protokoll auf Anwendungsebene, das auf HTTP basiert (RFC7230) Standard. Verwenden Sie diese API für die Bereitstellung und Verwaltung von Identitätsdaten, z. B. Anwender und Gruppen. Verwenden Sie die API im Web und in domänenübergreifenden Umgebungen, z. B. Enterprise-to-Cloud-Service Provider oder Cloud-übergreifende Szenarien.

Um auf diese API zuzugreifen, müssen Sie SCIM v2 aktivieren – ServiceNow® Plugin „Domänenübergreifendes Identitätsmanagement“ (com.snc.integration.scim2).

Weitere Informationen zur SCIM-API finden Sie unter System für die SCIM-API (Cross-Domain Identity Management) .

SCIM-Anbieter

Der Service Provider stellt Anwender und Gruppen mithilfe der SCIM-API bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über den SCIM-Anbieter.

Aktivieren



Aktivieren Sie SCIM.

SCIM-Anpassung



Rufen Sie Details zur Anpassung von SCIM ab.

Quelldefinition



Erfahren Sie mehr über die Quelldefinition für SCIM.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Anbieter erkunden

Der Service Provider stellt Anwender und Gruppen mithilfe der SCIM-API bereit.

Als SCIM-Anbieter ServiceNow Schemas unterstützen SCIM-APIs zur Bereitstellung von Anwendern und Gruppen.

Der SCIM-Anbieter synchronisiert die Änderungen, die an Identitäten im IdP vorgenommen werden, einschließlich Erstellen, Aktualisieren oder Löschen von Datensätzen. Diese Änderungen werden gemäß dem SCIM-Protokoll automatisch mit dem Anbieter synchronisiert. Außerdem kann der IdP Identitäten vom Provider lesen, um sie dem IdP-Verzeichnis hinzuzufügen. Der IdP kann dann falsche Werte im Anbieter erkennen, die Sicherheitsschwachstellen verursachen könnten. Die Synchronisierung ermöglicht Endanwendern mit aktuellen Profilen und Berechtigungen nahtlosen Zugriff auf Anwendungen, denen sie zugewiesen sind.

Konfigurationen für SCIM-Provider

Führen Sie die folgenden Aufgaben aus, um den SCIM-Provider zu konfigurieren:

- Aktivieren Sie **SCIM v2: Domänenübergreifendes Identitätsmanagement von ServiceNow** Plugin. Weitere Informationen finden Sie unter Das SCIM-Plugin wird aktiviert.
- Aktivieren Sie die anderen Plugins, die für SCIM erforderlich sind:
  - OAuth 2.0
  - REST API-Provider
  - REST API-Zugriffsrichtlinie
- Fügen Sie die Rolle scim_admin als Teil des SCIM-Service hinzu.

> ⚠ **Warnung:** Gewähren Sie dieser Rolle sorgfältig. Die Rolle „scim_admin“ bedeutet, dem Anwender die Administratorrolle zu geben, in der der SCmin_admin personenbezogene Informationen (PII) hinzufügen oder aktualisieren kann.

Tabellen

Zwei Tabellen, sys_user und sys_Group, enthalten die SCIM-Attribute, die nicht vorhandenen zugeordnet sind ServiceNow Tabellen. Weitere Informationen zu den Tabellen finden Sie unter SCIM-spezifische Tabellen .

Das SCIM-Plugin wird aktiviert

Installieren Sie für die SCIM-Aktivierung SCIM v2 – ServiceNow Plugin „Domänenübergreifendes Identitätsmanagement“ (com.snc.integration.scim2).

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach SCIM v2 – ServiceNow Plugin „Domänenübergreifendes Identitätsmanagement“ (com.snc.integration.scim2) mithilfe der Filterkriterien und der Suchleiste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.

3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

Tutorial: Konfigurieren Sie SCIM für die Anwenderbereitstellung bei einem Provider

Durch die Konfiguration von SCIM werden Anwender und Gruppen automatisch für bereitgestellt und aufgehoben ServiceNow Durch Verwendung des Provisioning-Service des Providers.

Vorbereitungen

Installieren Sie das SCIM-Plugin.

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie dieser Rolle sorgfältig. Die Rolle „scim_admin“ bedeutet, dem Anwender die Administratorrolle zu geben, in der der SCmin_admin personenbezogene Informationen (PII) hinzufügen oder aktualisieren kann.

Warum und wann dieser Vorgang ausgeführt wird

Sie können Anwender mit SCIM mithilfe der folgenden Authentifizierungsmethoden bereitstellen:

- Bereitstellung des Anwenders mithilfe der Standardauthentifizierung
- Anwender wird mit OAuth bereitgestellt

Bereitstellung des Anwenders mithilfe der Standardauthentifizierung

Durch die Konfiguration von SCIM werden Anwender und Gruppen automatisch für bereitgestellt und aufgehoben ServiceNow Durch Verwendung des Bereitstellungsservice des Anbieters mit Standardauthentifizierung.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie dieser Rolle sorgfältig. Die Rolle „scim_admin“ bedeutet, dem Anwender die Administratorrolle zu geben, in der der SCmin_admin personenbezogene Informationen (PII) hinzufügen oder aktualisieren kann.

Sie müssen das SCIM-Plugin aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien** Zum Überprüfen der Details zu den REST API-Zugriffsrichtlinien.
2. Klicken Sie auf der Seite API-Zugriffsrichtlinie auf **SCIM-API-Richtlinie** Datensatz.
3. Verifizieren Sie **SCIM-API – Standardauthentifizierung** Datensatz ist in den Abschnitten Authentifizierungsprofile verfügbar.
4. Wählen Sie Aus **Standardauthentifizierung** Als Typ.
5. Erstellen Sie die erforderlichen Konfigurationen am Ende des Anbieters
6. Testen Sie die Verbindung, um sicherzustellen, dass der Anbieter eine Verbindung zu herstellen kann ServiceNow.

Hinweis: Wenn die Verbindung fehlschlägt, stellen Sie sicher, dass Ihr ServiceNow Account verfügt über Administratorberechtigungen, und versuchen Sie es erneut.

Anwender wird mit OAuth bereitgestellt

Konfigurieren Sie den Anbieter für SCIM, der Benutzer und Gruppen automatisch bereitstellt und die Bereitstellung von Benutzern und Gruppen für aufheben kann ServiceNow Durch Verwendung des Provisioning-Service des Providers mit OAuth.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie dieser Rolle sorgfältig. Die Rolle „scim_admin“ bedeutet, dem Anwender die Administratorrolle zu geben, in der der SCmin_admin personenbezogene Informationen (PII) hinzufügen oder aktualisieren kann.

Sie müssen das SCIM-Plugin aktivieren.

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.
2. Klicken Sie auf der Seite „Anwendungsregistrierungen“ auf **SCIM-API** Datensatz.
3. Verifizieren Sie **SCIM-API** Datensatzdetails.

   Diese Details sollten bei der Konfiguration von angegeben werden ServiceNow Anwendung auf Azure AD.
4. Navigieren zu **Alle** > **System-Webservices** > **REST API-Zugriffsrichtlinien** Zum Überprüfen der Details zu den REST API-Zugriffsrichtlinien.
5. Klicken Sie auf der Seite API-Zugriffsrichtlinie auf **SCIM-API-Richtlinie** Datensatz.
6. Verifizieren Sie **SCIMAPIOAuthOnly** Datensatz ist in den Abschnitten Authentifizierungsprofile verfügbar.
7. Überprüfen Sie, ob **OAuth-Entität** Feld ist mit angegeben **SCIM-API** Datensatz, der zuvor als Anwendungsregistrierung konfiguriert oder verifiziert wurde.
8. Erstellen Sie die erforderlichen Konfigurationen am Ende des Anbieters

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Testen Sie die Verbindung, um sicherzustellen, dass der Anbieter eine Verbindung zu herstellen kann ServiceNow.

Hinweis: Wenn die Verbindung fehlschlägt, stellen Sie sicher, dass Ihr ServiceNow Account verfügt über Administratorberechtigungen, und versuchen Sie es erneut.

SCIM-Problembehandlung

Häufige Fehlerszenarien bei der Integration mit SCIM.

Ungültige Rest-API-URL

Aktion: Geben Sie eine gültige API-URL ein. Könnte die REST-API-URL in abgleichen **REST API-Explorer** .

In ist keine Umleitungs-URL festgelegt ServiceNow Instanz

Aktion: Geben Sie eine gültige Umleitungs-URL für die SCIM-OAuth-Entität in ein ServiceNow. Geben Sie die Umleitungs-URL ein, während Sie die OAuth-Entität in konfigurieren ServiceNow.

Wenn sich die Umleitungs-URL von der Anforderung unterscheidet

Aktion: „ **Redirect_url** „ Bereitgestellt in „ **Autorisierungsendpunkt“** Muss mit der in konfigurierten OAuth-Entität identisch sein ServiceNow.

Hinweis:

Dieser Fehler tritt auf, wenn eine Diskrepanz zwischen Azure „Autorisierungsendpunkt“ und besteht ServiceNow„Umleitungs-URL“

Wenn ein ungültiges geheimes Clientgeheimnis übergeben wird

Aktion: Der in „geheimer Client“ eingegebene Wert muss mit der in konfigurierten OAuth-Entität übereinstimmen ServiceNow.

Wenn eine ungültige „clientId“ in Azure „Autorisierungsendpunkt“ übergeben wurde

Aktion: Der für den Parameter „Client_ID“ in „Autorisierungsendpunkt“ eingegebene Wert muss mit der in konfigurierten OAuth-Entität übereinstimmen ServiceNow.

SCIM-Anpassung

Passen Sie SCIM-Protokolle für Ihr Identitätsmanagement an.

Mit der SCIM-Anpassung können Sie Folgendes tun:

- Unterstützen Sie anwenderdefinierte Felder in den Tabellen „sys_user“ und „sys_user_Group“ durch die dynamische Generierung des Erweiterungsschemas.
- Bieten Sie die Möglichkeit, die standardmäßigen SCIM-Zuordnungen zu überschreiben.

Ein SCIM-Administrator kann anwenderdefinierte Erweiterungsschemata für Anwender- und Gruppenressourcen definieren. Die im anwenderdefinierten Erweiterungsschema definierten Attribute können Feldern in den Tabellen „sys_user“ oder „sys_user_Group“ zugeordnet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationen für die SCIM-Anpassung

Für die SCIM-Anpassung sollten Sie die folgenden Aufgaben ausführen:

- Definieren Sie ein anwenderdefiniertes Erweiterungsschema für Anwender und Gruppen in der SCIM-Erweiterungsschematabelle. #Weitere Informationen finden Sie unter . Erstellen Sie ein SCIM-Erweiterungsschema.
- Erstellen Sie Entitäten in einer ETL-Definition für anwenderdefinierte Schemaattribute. Die Entitäten werden für die Zieltabelle erstellt, die entweder den Attributen „sys_user“ oder „sys_user_Group“ zugeordnet ist. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-ETL-Definition.
- Erstellen Sie eine RTE-Zuordnung zwischen diesen beiden Entitäten. #Weitere Informationen finden Sie unter Schritt 5 In Erstellen Sie eine SCIM-ETL-Definition.
- Senden Sie anwenderdefinierte Schemaattribute mit Daten in der Nutzlast der SCIM-API-Anforderung.

Die SCIM-API ruft die RTE-Engine mit der definierten Zuordnung auf. Die Daten werden in den entsprechenden Feldern in der Zieltabelle gespeichert, wie in der Zuordnung definiert.

SCIM-Anpassungseigenschaften und -Schemas

Die SCIM-Anpassung umfasst die folgenden Eigenschaften, unterstützte Schemas und nicht unterstützte Schemas.

Eigenschaften

Die SCIM-Anpassung fügt die folgenden Systemeigenschaften hinzu.

Eigenschaften

Name	Beschreibung
com.snc.integration.scim2.max.member.count	Die maximale SCIM-Mitgliederanzahl.
com.snc.integration.scim2.resolve.external.id.scim.filter	Lösen Sie SCIM-Ressourcen basierend auf der Quelldefinition des anfordernden Clients auf, wenn mehrere Ressourcen mit einem externen ID-SCIM-Filter gefunden werden. **Hinweis:** Wenn die Bereitstellung aus mehreren Quellen erfolgt, müssen die Quellen als Voraussetzung in der SCIM-Quelldefinitionstabelle definiert werden. Wenn Quellen nicht definiert sind oder diese Eigenschaft inaktiv ist, werden alle übereinstimmenden Ressourcen mit einer externen ID-Filterantwort zurückgegeben.
com.snc.integration.scim2.user.etl.definition.id	Die ETL-Definitions-ID des SCIM-Anwenders.
com.snc.integration.scim2.group.etl.definition.id	Die ETL-Definitions-ID der SCIM-Gruppe.
com.snc.integration.scim2.rte.verbose.logging	Aktivieren Sie ausführliche Protokollierung für SCIM-Anwender- und Gruppen-RTE-Definitionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften (Fortsetzung)

Name	Beschreibung
com.snc.integration.scim2.string.field.length.validation.enabled	Die Länge wird für Felder validiert. Diese Eigenschaft ermöglicht die Validierung, anstatt das Feld zu kürzen und zu speichern.
com.snc.integration.scim2.provider.customizer.id	Die ID der Skriptintegration zum Anpassen der SCIM-Antworten.

Unterstützte Schemas

Die SCIM-Anpassung fügt die folgenden unterstützten Schemas hinzu.

Unterstützte Schemas

Schemen	Beschreibung	Präfix	Beispiel
urn:ietf:params:scim:schemas:core:2.0:User	Enthält Kernattribute, die sich auf die Ressourcen.		Name.Mittelname
urn:ietf:params:scim:schemas:extension:servicenow:2.0:User	Enthält Attribute, die sich auf beziehen ServiceNow.		servicenow.Manager.Wert
urn:ietf:params:scim:schemas:extension:custom:2.0:User	Enthält anwenderdefinierte Attribute, die nicht als Teil der Core-Erweiterung oder#der zugeordnet sind ServiceNow Erweiterungsschema.	anwenderdefiniert	Anwenderdefiniert.socialId

Nicht unterstütztes Schema

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: Enthält Attribute, die häufig zur Darstellung von Anwendern verwendet werden, die einem Unternehmen oder Unternehmen angehören oder im Namen eines Unternehmens handeln.

Hinweis: Enterprise-Schema ist ein gültiges Schema, seine Attribute sind jedoch einer beliebigen Tabelle zugeordnet. Da die Datenbankpersistenz nicht unterstützt wird, wird kein Fehler angezeigt, wenn ein Enterprise-Schema im Anforderungstext enthalten ist.

Erstellen Sie ein SCIM-Erweiterungsschema

Erstellen Sie anwenderdefinierte Attribute, um Feldern zuzuordnen, die nicht als Teil des Kernschemas oder des zugeordnet sind ServiceNow Erweiterungsschema.

Vorbereitungen
Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie dieser Rolle sorgfältig. Die Rolle „scim_admin“ entspricht der Zuweisung der Administratorrolle, wobei die Rolle „scmin_admin“ neue Datensätze in die Tabellen einfügen kann, die Geschäftslogik oder ACL-Schutz umgehen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

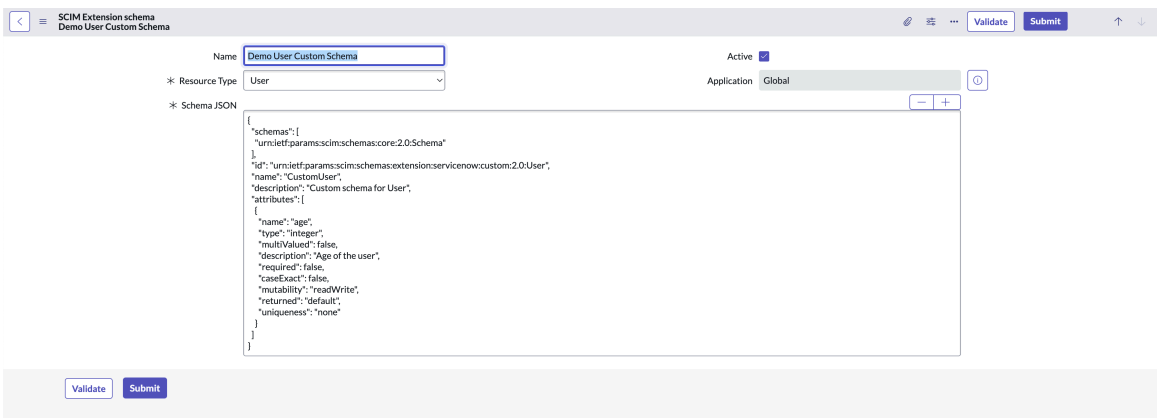
Prozedur

1. Navigieren zu **Alle** > **SCIM** > **SCIM-Erweiterungsschemas**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

> **Hinweis:** Nur ein Erweiterungsschema kann dem zugeordnet werden **Ressourcentyp** Feld. Beispielsweise kann Anwender als Ressourcentyp einem Anwendererweiterungsschema zugeordnet werden.

SCIM-Erweiterungsschema

Feld	Beschreibung
Name	Name des Erweiterungsschemas.
Aktiv	Option zum Aktivieren des Schemas. Wählen Sie dieses Feld aus, wenn der Datensatz als anwenderdefiniertes Erweiterungsschema betrachtet werden muss. Für einen bestimmten Ressourcentyp kann jeweils nur ein anwenderdefinierter Erweiterungsschema-Datensatz aktiv sein, unabhängig davon, ob es sich um den Anwender- oder Gruppentyp handelt.
Ressourcentyp	Ressourcentyp, der dem Erweiterungsschema zugeordnet werden muss. Die folgenden Optionen sind verfügbar: ○ **Benutzer** ○ **Gruppe**
Anwendung	Anwendungsbereich für diesen Datensatz
Schema-JSON	Details in den JSON-Schemas. Weitere Informationen zum Definieren des Erweiterungsschemas mit Attributen finden Sie unter Datenracker .



4. Validieren Sie die Attribute, indem Sie auf klicken **Validieren** .
5. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Das Erweiterungsschema mit anwenderdefinierten Attributen im Zusammenhang mit dem Ressourcentyp „Anwender“ oder „Gruppe“ wird erstellt. Verwenden Sie die SCIM-ETL-Definitionen, um die Ressourcen basierend auf dem Erweiterungsschema in der Tabelle „sys_user“ und „sys_user_Group“ zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-ETL-Definition.

Erstellen Sie eine SCIM-ETL-Definition

Verwenden Sie die SCIM ETL-Definitionen, um die anwenderdefinierten Attribute den Tabellen „sys_user“ oder „sys_user_Group“ zuzuordnen.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie dieser Rolle sorgfältig. Die Rolle „scim_admin“ entspricht der Zuweisung der Administratorrolle, wobei die Rolle „scmin_admin“ neue Datensätze in die Tabellen einfügen kann, die Geschäftslogik oder ACL-Schutz umgehen können.

Hinweis:

- SCIM-Gruppen- und SCIM-Anwender-ETL-Definitionen sind Teil des Basissystems für die Ressourcenzuordnung. Sie können dieselben Ressourcenzuordnungen verwenden und die Kriterien nach Bedarf ändern, oder Sie können neue Ressourcenzuordnungen erstellen.
- Es gibt keine Unterstützung für [*] Felder über RTE in der SCIM-Zuordnung.

Prozedur

1. Befolgen Sie die Anweisungen in Erstellen Sie ETL-Definitionen (Extract Transform Load) .
2. Öffnen Sie den neu erstellten Datensatz, und zeigen Sie die Details an.
3. Erstellen Sie im Abschnitt „ETL-Entitäten“ eine Entität, indem Sie auf klicken **Neu** .
   Sie müssen Entitäten für die folgenden Anwender erstellen:
   - scim-user: Für die Felder, die aus SCIM stammen.
   - Tabelle „Anwender“ (sys_user) oder „Gruppe“ (sys_user_Group): Für die Felder, die Sie aus der Datenbanktabelle mit SCIM zuordnen möchten. Zum Anpassen von Anwenderdetails über SCIM können Sie beispielsweise die Tabelle sys_user verwenden.

   a. Füllen Sie im Formular die Felder aus.

ETL-Entitätsformular

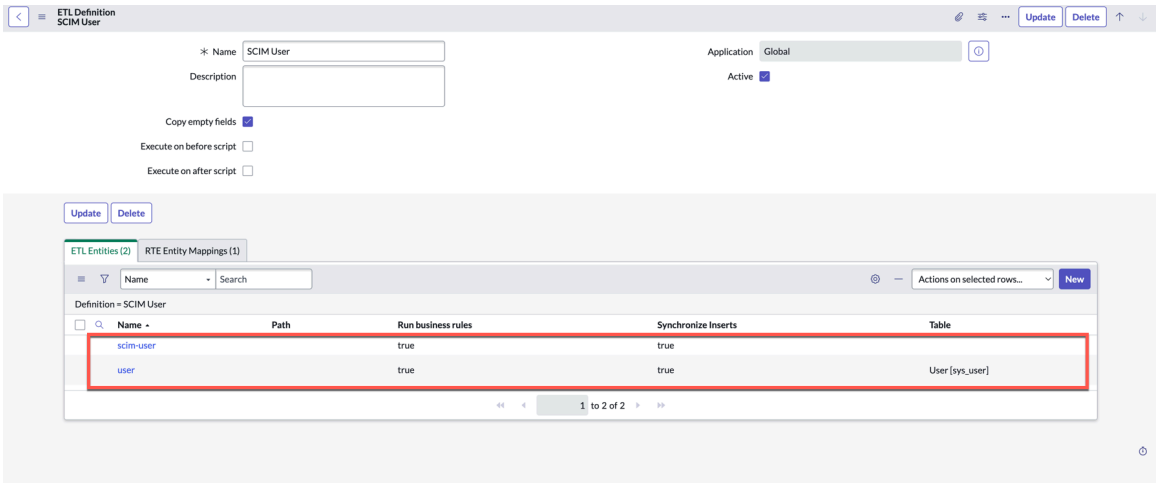
Feld	Beschreibung
Name	Name der ETL-Entität.
Anwendung	Anwendungsbereich für diesen Datensatz
Tabelle	Zieltabelle für die ETL-Entität.
Definition	Ausgewählte ETL-Entität.
Pfad	Eindeutiger Pfad für diese Entität. Geben Sie keinen Pfad für die Entität an, die die Importsatztabelle darstellt. Wenn eine Entität eine Sammlung darstellt, muss der Pfad mit einem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sternchen [*] enden. Diese Anforderung gilt für Zwischeneinträge und die Zieltabellenentität.
Einfügungen synchronisieren	Option, um durch Synchronisieren von Datensatzeinfügungen nur einen Datensatz mit eindeutigen zusammengefügten Feldwerten zu garantieren.
Business-Regeln ausführen	Option zum Ausführen von Business-Regeln.

b. Klicken Sie auf **Absenden**.

Die ETL-Entitäten werden für scim-Anwender- und Anwendertabellen erstellt. Sie müssen ETL-Entitätsfelder innerhalb dieser ETL-Entitäten erstellen und beide Entitäten zuordnen, indem Sie eine RTE-Entitätszuordnung erstellen.



4. Erstellen Sie die Entitäten, und ordnen Sie sie zu.

a. Öffnen Sie den übermittelten Datensatz (scim-user und user).

b. Fügen Sie in den ETL-Entitätsfeldern die Felder hinzu, indem Sie auf klicken **Neu** .

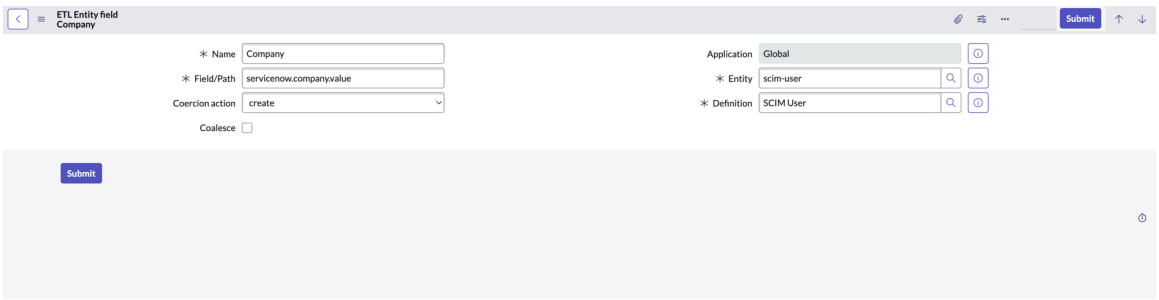
c. Füllen Sie im Formular die Felder aus.

ETL-Entitätsformular

Feld	Beschreibung
Name	Name der ETL-Entitätsfelddefinition.
Anwendung	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Feld/Pfad	Dieses Feld ist entweder eine Spalte oder ein Pfad. ▪ Das Feld ist ein Spaltenname, wenn die Entität die Import- oder Zieltabelle ist. ▪ Das Feld ist ein Pfad, wenn das Feld über geschachtelte Strukturen verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

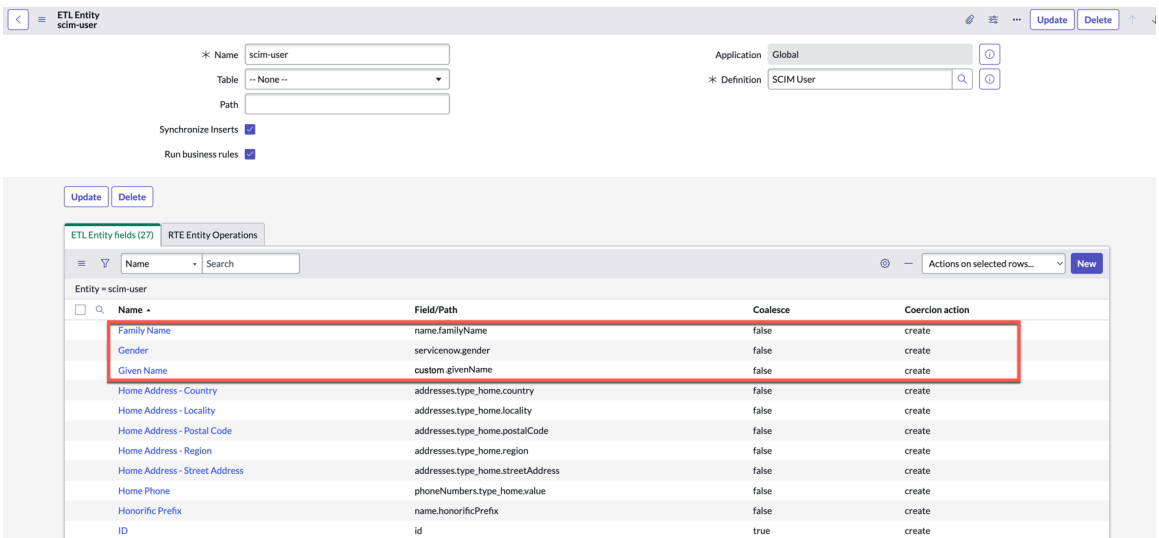
Feld	Beschreibung
Entität	Entität, für die dieser Vorgang gilt. Wählen Sie die Entität mithilfe des Suchsymbols aus.
Zwangsaktion	Was das System tun soll, wenn eine Referenz oder Auswahl nicht gefunden werden konnte. Die Optionen sind wie folgt: ▪ **Erstellen** : Erstellen Sie eine neue Referenz oder Auswahl. Weisen Sie dem aktuellen Datensatz die Referenz oder Auswahl zu. ▪ **Ablehnen** : Speichern Sie nicht den gesamten Datensatz in der Datenbank. ▪ **Ignorieren** : Legen Sie den aktuellen Wert als leer fest.
Definition	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Zusammenfügen	Option zum Abfragen der vorhandenen Datensätze.



d. Übermitteln Sie die Einträge, indem Sie auf klicken **Übermitteln** .

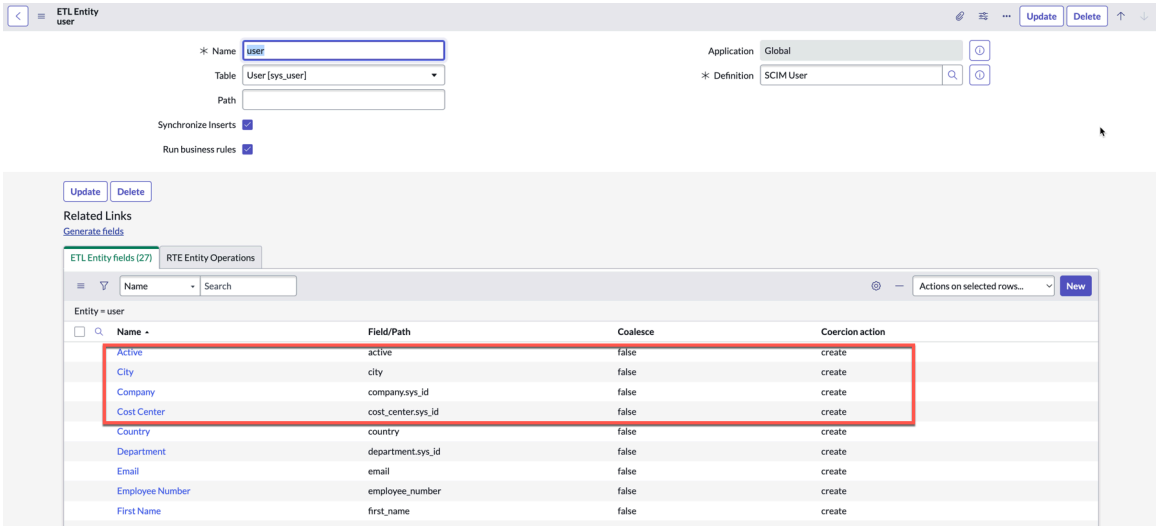
Sie können je nach Anforderung mehrere Einträge als ETL-Entitätsfeld hinzufügen.

Die ETL-Entität scim-user kann Entitäten mit der Kernerweiterung (Anwender) haben ServiceNow Erweiterung oder anwenderdefinierte Erweiterung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anwender-ETL-Entität kann Entitäten aus der Datenbanktabelle haben. Beispiel: Tabelle sys_user.



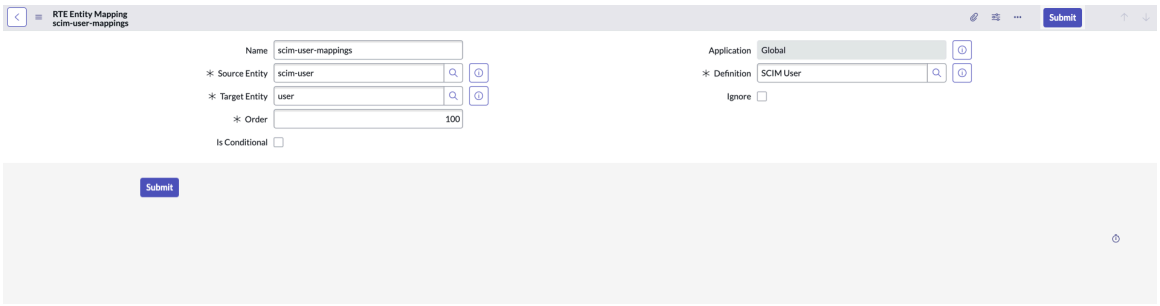
Hinweis: Um einen Filter in den Feldern für eingehende SCIM hinzuzufügen, verwenden Sie einen Unterstrich (`_`). Dieser Unterstrich wird in einen EQ-Filter übersetzt. Zum Beispiel das Attribut *`email.type_work.value`*Wendet den SCIM-Filter der E-Mail an *`[type eq “work”].value`*.

Nachdem die Felder sowohl in den Datensätzen „scim-user“ als auch „Anwender-ETL-Entitätszuordnung“ erstellt wurden, müssen Sie einen RTE-Entitätszuordnungsdatensatz erstellen. Sie müssen dann die Quell- und Zieldefinition angeben, um beide Felder zuzuordnen.

5. Erstellen Sie im Abschnitt „RTE-Entitätszuordnungen“ eine Entitätszuordnung, indem Sie auf klicken **Neu**
6. Füllen Sie die Felder im Formular aus.

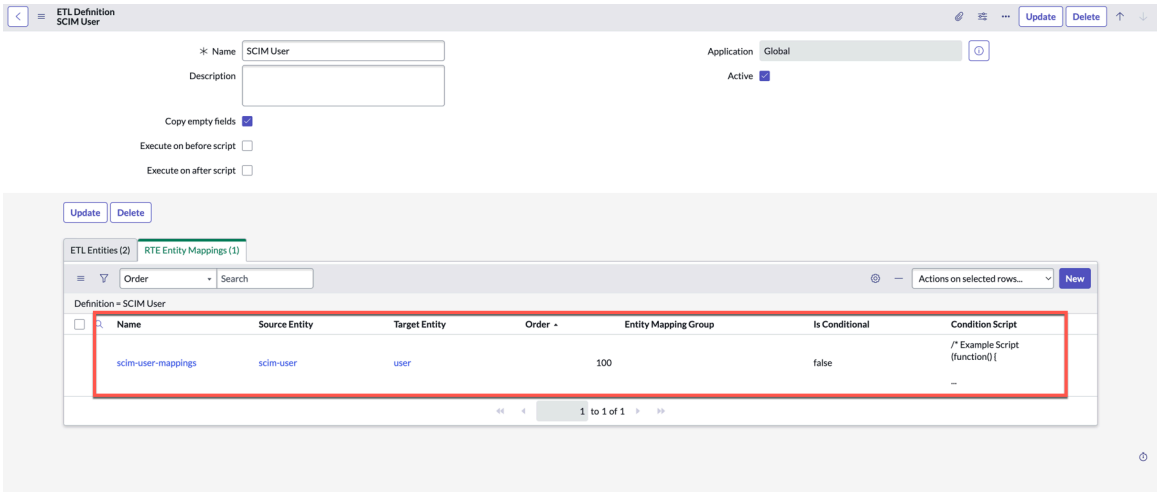
Feld	Beschreibung
Name	Name der Feldzuordnung.
Quellentität	Quellentität für die Zuordnung.
Zielentität	Zielentität für die Zuordnung.
Reihenfolge	Reihenfolge, in der die Zuordnung verarbeitet werden soll.
Ist bedingt	Option, um die Zuordnung als bedingt festzulegen.
Bedingungsskript	Skript, das die Bedingungen definiert, die für die Zuordnung erfüllt sein müssen.
Anwendung	Anwendungsbereich für diesen Datensatz
Definition	Ausgewählte ETL-Entität, zu der diese Zuordnung gehört.
Ignorieren	Option zum Festlegen, ob diese ETL-Entitätszuordnung ignoriert werden soll, wenn Datenintegrationen mit der robusten Importsatztransformation (RTE) durchgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Absenden**.

   Das folgende Beispiel zeigt einen Datensatz, der für die Zuordnung der Datensätze scim-user und Anwender-ETL-Entität erstellt wurde.



8. Öffnen Sie den übermittelten Datensatz (scim-user-Mappings), und erstellen Sie eine Zuordnung zwischen den Datensätzen der scim-user- und ETL-Entität des Anwenders.

   a. Klicken Sie im Abschnitt RTE-Feldzuordnungen auf **Neu** .

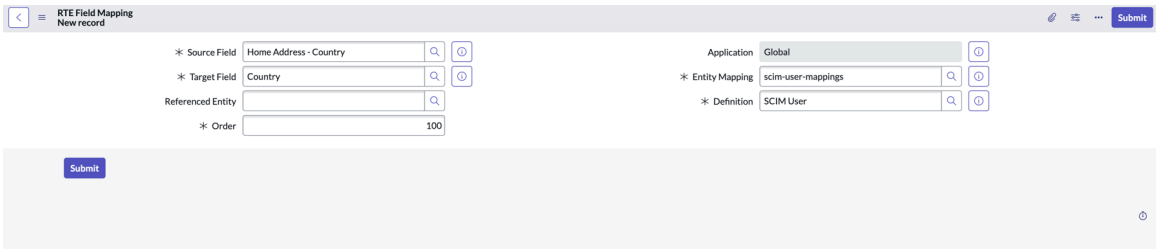
   b. Füllen Sie im Formular die Felder aus.

ETL-Entitätsfelder

Feld	Beschreibung
Quellfeld	Anwendungsbereich für diesen Datensatz
Anwendung	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Zielfeld	Feld „ETL-Ausgabe“ für den Vorgang, wenn der Vorgang eine einzelne Ausgabe verwendet.
Entitätszuordnung	Entitätszuordnung, für die dieser Vorgang gilt.
Referenzierte Entität	Entität, auf die verwiesen wird, und der Vorgang, für den sie gilt.
Definition	Ausgewählte ETL-Entität, zu der diese Felddefinition gehört.
Reihenfolge	Reihenfolge, in der der Vorgang für die Entität ausgeführt wird.

Automatische Übersetzung

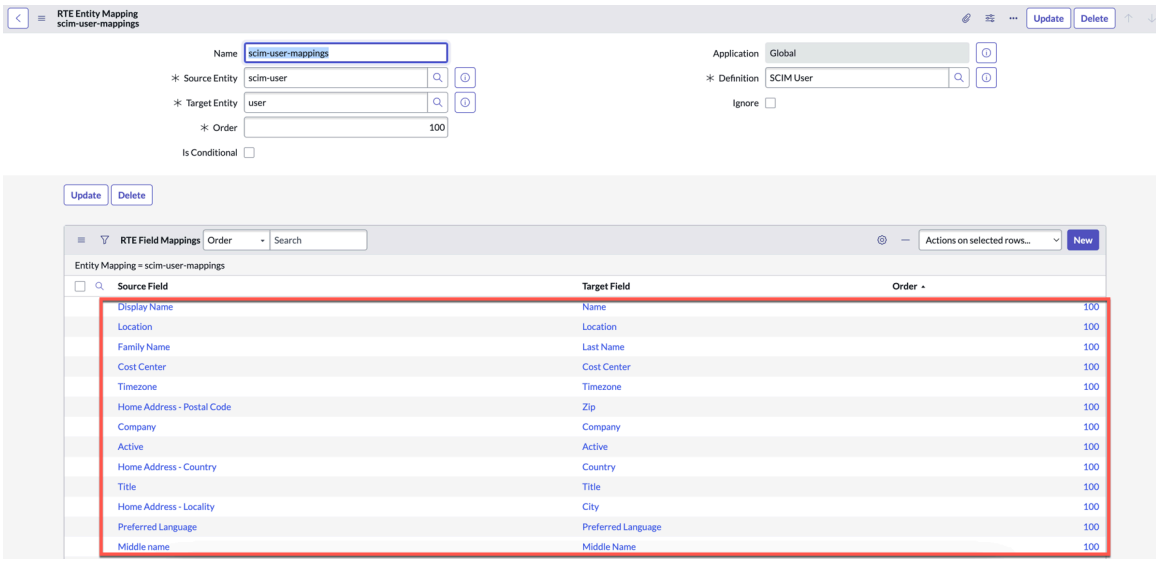
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Quellfeld **Privatadresse: Land** (scim-user ETL-Entität) ordnet das Zielfeld zu **Land** (Anwender-ETL-Entität).

c. Übermitteln Sie die Einträge, indem Sie auf klicken **Übermitteln** .

Sie können je nach Anforderung mehrere Einträge als RTE-Entitätszuordnungen hinzufügen.



Die Quellfelder und Zielfelder werden wie konfiguriert zugeordnet. Wenn Sie CRUD-Vorgänge mit SCIM ausführen, werden die anwenderdefinierten Werte in der entsprechenden Tabelle aktualisiert.

Ergebnis

Mit diesen ETL-Definitionen und -Zuordnungen können Sie Daten aus einer Quelltabelle extrahieren, die Daten nach Bedarf umwandeln und die Daten in eine Zieltabelle laden.

Zugehörige Informationen

Erstellen Sie ETL-Definitionen (Extract Transform Load)

Verarbeitung nicht zugeordneter Felder

Sie können nicht zugeordnete Felder in der SCIM-Anpassung auf verschiedene Weise behandeln.

Während der SCIM-Anpassung können die Felder, die nicht Teil der Tabellen „sys_user“ und „sys_user_Group“ sind, durch Ausführen der folgenden Funktionen zugeordnet werden.

SCIM anpassen (Erstellen oder Aktualisieren)

Sie können den SCIM-Client erstellen oder aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der SCIM-Administrator kann anwenderdefinierte Skripts in hinzufügen *onBefore*Und *onAfter*Skripts für Felder, die nicht in der ETL-Definition oder RTE zugeordnet sind.
- Der SCIM-Administrator kann RTE-Zuordnungen überschreiben, indem er anwenderdefinierte Skripts in hinzufügt *onBefore*Und *onAfter*Skripts.
- Sie können eine skriptfähige API in der RTE aufrufen *onBefore*Oder *onAfter*Skripts für den Zugriff auf eingehende Anforderungen und die Durchführung von Transformationen für andere Tabellen, Listen und nicht zugeordnete Attribute.
- Sie können verwenden *sn_auth.SCIM2Util.getScimProviderCustomizationContext()*Methode zum Bereitstellen des SCIM-Anforderungskontexts, der enthält *scimResource*Objekt. Die *scimResource*In Kontext stellt in jedem Vorgang Folgendes dar:
  - **VERÖFFENTLICHEN** : Die in der Anforderungsnutzlast gesendete SCIM-Ressource.
  - **PLATZIEREN** : Die aktuelle SCIM-Ressource aus der Datenbank wurde durch die SCIM-Ressource ersetzt, die in der Anforderungsnutzlast gesendet wurde.
  - **PATCH** : Die aktuelle SCIM-Ressource aus der Datenbank nach der Ausführung der Patch-Vorgänge.

Im Folgenden finden Sie ein Beispiel für *onAfter*Skript.

```
(function onAfter(source, target, importLog) {

   var ctx = sn_auth.SCIM2Util.getScimProviderCustomizationContext();
   gs.info("scim context ee: " + JSON.stringify(ctx.scimResource));

   var roles = ctx.scimResource.roles;
   if(roles) {
      var removingRolesGR = new GlideRecord("sys_user_has_role");
      removingRolesGR.addQuery("user", target.sys_user[0].sys_id);
      removingRolesGR.query();
      removingRolesGR.deleteMultiple();

   for (var i = 0; i < roles.length; i++) {
      var addingRolesGR = new GlideRecord("sys_user_has_role");
      addingRolesGR.setValue("user", target.sys_user[0].sys_id);
      addingRolesGR.setValue("role", roles[i].value);
      addingRolesGR.setValue("state", "active");
      addingRolesGR.insert();
      }
      }
      var customUserExtn = new
global.SCIMProviderCustomization().getCustomExtensionUrn('User');
      var salary = ctx.scimResource[customUserExtn].salary;
      if (salary) {
         var gr = new GlideRecord("u_user_salary");
         gr.addQuery("user", target.sys_user[0].sys_id);
         gr.query();
         if (gr.next()) {
            gr.setValue("salary", salary);
            gs.info("scim update: " + gr.update());
         } else {
         gr.setValue("salary", salary);
         gr.setValue("user", target.sys_user[0].sys_id);
         gr.insert();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        }
       }

})(source, target, importLog);
```

Passen Sie die SCIM-Antwort an

Für die GET-API-Aufrufe kann jede Antwort zurück an den SCIM-Client mithilfe des Skripts angepasst werden, indem erweitert wird *`SCIMProviderCustomization`*Skript.

Beim erweitern des Skripts kann der Autor den überschreiben *`customizeUserResponse`*Und *`customizeGroupResponse`*Methoden zum Ändern der Antworten für Anwender- und Gruppenressourcen.

Die *`com.snc.integration.scim2.provider.customization.script.id`*Mit der Eigenschaft kann das SCIM-Plugin das Skript verwenden, das für die Anpassung der Antwort verwendet werden soll.

Im Folgenden finden Sie ein Beispiel für die Erweiterung des Basisskripts.

```
var SCIMCustomizationScript = Class.create();
SCIMCustomizationScript.prototype = Object.extendsObject(SCIMProviderCustomization, {
   initialize: function() {
      SCIMProviderCustomization.prototype.initialize.call(this);
   },
   customizeUserResponse: function(context) {
      try {
         var rolesGR = new GlideRecord("sys_user_has_role");
         rolesGR.addQuery("user", context.scimResource.id);
         rolesGR.query();
         var i = 0;
         context.scimResource.roles = [];
         while (rolesGR.next()) {
            context.scimResource.roles[i] = {
               display: rolesGR.getElement('role.name').getValue(),
               value: rolesGR.getElement('role.sys_id').getValue()
            };
            i++;
         }
         var userGR = new GlideRecord("u_user_salary");
         userGR.addQuery("user", context.scimResource.id);
         userGR.query();
         if (userGR.next()) {
            var salary = userGR.getValue("salary");
            if (salary) {
               var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
context);
               customExtensionValue.salary = salary;
               SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this,
"User", context, customExtensionValue);
            }
         }
      } catch (ex) {
         gs.error("err: " + ex);
      }
      return context;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    },
    customizeGroupResponse: function(context) {
        return context;
    },
    type: 'SCIMCustomizationScript'
});
```

Hinweis:

- Der Parameter, der *customizeUserResponse*Und *customizeGroupResponse*„Methoden enthalten“ ist ein Kontextobjekt mit einem Attribut namens *scimResource*. Dieses Attribut hat alle Attribute eines Anwender- oder Gruppenressourcenobjekts.
- Eine anwenderdefinierte Skripteinbindung kann nur vom Administrator erstellt und angezeigt werden.
- Wenn eine Anwender- oder Gruppenressource geändert wird, müssen Sie den Kontext zurückgeben.
- Wenn keine Änderung eines Attributs im Ressourcenobjekt erfolgt, legen Sie fest *com.snc.integration.scim2.provider.customization.script.id*Leer oder als Null zurückgeben.
- Wenn bestimmte Attribute über beibehalten werden *onAfter*Skript, müssen sie mit Datenbankwerten in ausgefüllt werden *scimResource*Objekt im anwenderdefinierten Skript. Diese Aktion ist erforderlich, damit das System Folgendes ausführen kann:
  - Um die richtige zu erhalten *scimResource*Objekt in *onAfter*Skripts während des PUT- und PATCH-Vorgangs.
  - Um die Attribute einzubeziehen, die über beibehalten wurden *onAfter*Skript in der Antwort zurück an den Client.

Hilfsfunktionen

Im Folgenden finden Sie einige der Hilfsfunktionen für die SCIM-Anpassung. Mit diesen Funktionen können Sie verschiedene Arten von Informationen abrufen oder festlegen.

Hilfsfunktionen

Funktion	Zweck
SCIMProviderCustomization.prototype.getCustomExtensionModel.call(this, "User");	Rufen Sie den Wert des anwenderdefinierten Erweiterungsschemas ab.
SCIMProviderCustomization.prototype.getServiceNowExtensionModel.call(this, "User");	Rufen Sie den Wert des ServiceNow Erweiterungsschema.
SCIMProviderCustomization.prototype.getCustomExtensionModelValue.call(this, "User", context);	Rufen Sie den Wert des anwenderdefinierten Schemas aus der Antwort ab.
SCIMProviderCustomization.prototype.getServiceNowExtensionModelValue.call(this, "User", context);	Rufen Sie den Wert des ServiceNow Schemas aus der Antwort
SCIMProviderCustomization.prototype.setCustomExtensionModelValue.call(this, "User", context, customExtensionValue);	Legen Sie den Wert des anwenderdefinierten Schemas in der Antwort fest.

Im Folgenden finden Sie ein Beispiel für die Verwendung der Hilfefunktion:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var customExtensionUrn =
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");
var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
 context);
customExtensionValue.age = "18";
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue call(this, "User", context,
 customExtensionValue);
```

Hinweis: RTE unterstützt das Festlegen von Daten in anderen Tabellen als den Tabellen „sys_user“ und „sys_user_Group“.

Erstellen einer Quelldefinition

Erstellen Sie eine Quelldefinition, um Informationen darüber zu erfassen, aus welcher Identitätsquelle eine Ressource bereitgestellt wird.

Vorbereitungen

Erforderliche Rolle: scim_admin

Warnung: Gewähren Sie dieser Rolle sorgfältig. Die Rolle „scim_admin“ bedeutet, dem Anwender die Administratorrolle zu geben, in der der SCmin_admin personenbezogene Informationen (PII) hinzufügen oder aktualisieren kann.

Warum und wann dieser Vorgang ausgeführt wird

Mithilfe einer Quelldefinition kann die Quelle der Bereitstellungsidentität einer OAuth-Entität zugeordnet werden, mit der sie sich während der Bereitstellung authentifiziert.

Nachdem eine Quelldefinition erstellt wurde, werden alle Ressourcen, die aus dieser Identitätsquelle bereitgestellt werden, der entsprechenden Quelldefinitions-ID zugeordnet.

Die Quelldefinition erfasst die erforderlichen Quellinformationen, z. B. indem Sie Folgendes ausführen:

- Gibt den SCIM-Client an, von dem die Ressource bereitgestellt wird.
- Löst doppelte Informationen auf, die von der externen ID bereitgestellt werden:
  - Wenn mehrere Identitätsquellen Bereitstellungsressourcen sind, können zwei oder mehr Ressourcen denselben externen ID-Wert haben, da die externe ID nur für die Identitätsquelle eindeutig ist.
  - Wenn mehrere Ressourcen mit einem externen ID-SCIM-Filter zurückgegeben werden, können die Ressourcen basierend auf der Quelldefinition der anfordernden Identitätsquelle aufgelöst werden.

Hinweis: Eine Quelldefinition kann nur für die Identitätsquelle erstellt werden, die eine OAuth-Authentifizierungsmethode verwendet.

Prozedur

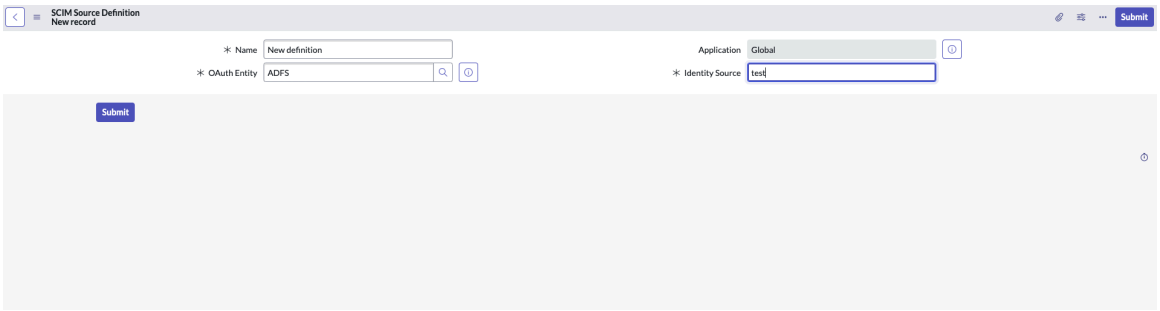
1. Navigieren zu **Alle** > **SCIM** > **Quellendefinition**an.
2. Klicken Sie auf der Seite „SCIM-Quelldefinitionen“ auf **Neu** .
3. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Quellendefinition

Feld	Beschreibung
Name	Name der Quelldefinition.
Anwendung	Anwendungsbereich für diesen Datensatz
OAuth-Entität	Die OAuth-Entität des Integrationsanwenders. Die Entität wird für die Bereitstellung des Anwenders durch den Identitätsquellenanbieter verwendet.
Identitätsquelle	Der Name des Identitätsquellanbieters. Zum Beispiel Azure AD, Okta usw.

Hinweis: Aktivieren Sie `com.snc.integration.scim2.resolve.externalid.conflict`Eigenschaft, um nur SCIM-Ressourcen zurückzugeben, die von der anfordernden Identitätsquelle erstellt wurden. Standardmäßig werden alle übereinstimmenden Ressourcen mit einem externen ID-Filter zurückgegeben.



4. Klicken Sie auf **Absenden**.

Ergebnis

Die SCIM-Quelldefinition wird erstellt. Verwenden Sie die SCIM-ETL-Definitionen, um die Ressourcen basierend auf dem Erweiterungsschema in der Tabelle „sys_user“ und „sys_user_Group“ zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-ETL-Definition.

SCIM-Client

Der SCIM-Client erleichtert die Bereitstellung und Aktualisierung von Identitätsressourcen durch CRUD-Vorgänge, die vom SCIM-Endpunkt auf einem externen System bereitgestellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Untersuchen



Erfahren Sie mehr über SCIM-Client.

Aktivieren



Aktivieren Sie den SCIM-Client.

Eigenschaften des SCIM-Clients



Rufen Sie Details zur Anpassung von SCIM ab.

Problembehandlung



Erfahren Sie mehr über die Quelldefinition für SCIM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCIM-Client erkunden

Der SCIM-Client erleichtert die Bereitstellung und Aktualisierung von Identitätsressourcen durch CRUD-Vorgänge, die vom SCIM-Endpunkt auf einem externen System bereitgestellt werden.

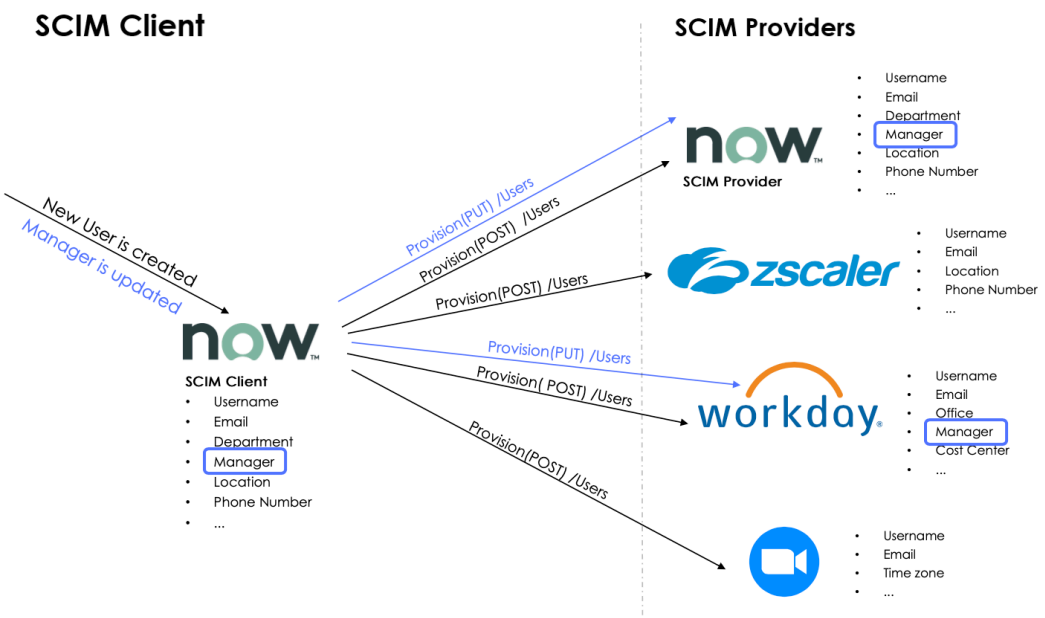
Der SCIM-Client wird zum Erstellen, Aktualisieren und Löschen von Identitätsressourcen in einem System verwendet, das SCIM-konforme REST-Anforderungen unterstützt. Der Client wird für die Verwaltung des Identitätslebenszyklus und für die Synchronisierung von Identitätsattributen über verwendet ServiceNow Instanzen oder zwischen ServiceNow Und andere SCIM-Anbieter.

Da die APIs vom Client verfügbar gemacht werden, können Sie den Prozess zum Erstellen, Aktualisieren oder Löschen von Ressourcen für einen einzelnen oder mehrere SCIM-Anbieter automatisieren. Wenn beispielsweise ein Entwickler der Organisation Beitritt, müssen Sie Zugriff auf Git, Arbeitsplatz usw. gewähren.

Mit dem SCIM-Client können Sie die folgenden Aktionen ausführen:

- Stellen Sie Identitäten und Zugriff für Anwender- oder Gruppenmitgliedschaft bereit.
- Synchronisieren Sie Identität und zugehörige Ressourcen mit SCIM-konformen Systemen.
- Integrieren Sie einen beliebigen SCIM-Anbieter in ServiceNow®.
- Aufheben der Bereitstellung von Identitäten und Zugriff.

Der SCIM-Client stellt skriptfähige APIs bereit, mit denen der Integrationsentwickler Workflows oder Automatisierungen für die Ausführung bestimmter Aufgaben erstellen kann. Weitere Informationen zur skriptfähigen API finden Sie unter SCIM2Client-API .



Konfigurationen für SCIM-Client

Führen Sie die folgenden Aufgaben aus, um den SCIM-Client zu konfigurieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie eine REST-Nachricht für alle ausgehenden Anrufe für einen bestimmten SCIM-Anbieter. Weitere Informationen finden Sie unter REST-Nachrichten erstellen.
- Erstellen Sie einen SCIM-Provider, um Ressourcentypen und Schemadaten vom SCIM-Provider mit der REST-Nachricht abzurufen. Aktivieren Sie die Konfiguration der HTTP-Methode (PUT oder PATCH), um eine Ressource im SCIM-Provider zu aktualisieren. Weitere Informationen finden Sie unter Erstellen Sie einen SCIM-Provider.
- Erstellen Sie die Zuordnungen von SCIM-Attributen zu ServiceNow Attribute für einen bestimmten Ressourcentyp und SCIM-Anbieter. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Provider-Ressourcenzuordnung.
- Führen Sie die Zuordnung des SCIM-Felds mit der Datenbanktabelle und dem Feldnamen durch. Übergeben Sie den Standardwert, oder schreiben Sie ein Skript, um den Wert abzurufen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Attributzuordnung.

Aktivieren Sie das Plugin „SCIM-Client“

Installieren Sie für die SCIM-Client-Aktivierung SCIM v2 – ServiceNow Plugin „Identity Management Client“ (com.snc.integration.scim2.client) für domänenübergreifende Identitätsverwaltung.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach SCIM v2 – ServiceNow Domain-übergreifendes Identity Management Client-Plugin (com.snc.integration.scim2.client) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach dem Plugin anhand seines Namens oder seiner ID suchen. Wenn Sie kein Plugin finden können, müssen Sie es möglicherweise von einem Mitarbeiter von ServiceNow anfordern.
3. Wählen Sie **Installieren**, um den Installationsprozess zu starten.

   Hinweis: Wenn die Domain Separation und der delegierte Administrator in einer Instanz aktiviert sind, muss sich der Administrator in der **globalen** Domäne befinden. Andernfalls wird der folgende Fehler angezeigt: Die Anwendungsinstallation ist nicht verfügbar, da ein anderer Vorgang ausgeführt wird: Plugin-Aktivierung für <Plugin-Name>.

   Nach Abschluss der Installation wird eine Meldung angezeigt. Informationen zu den mit einem Plugin installierten Komponenten finden Sie unter Suchen Sie Komponenten, die mit einer Anwendung installiert sind .

SCIM-Client-Eigenschaften, Tabellen, skriptfähige APIs und Protokolle

SCIM v2 – ServiceNow Das Plugin „Identity Management Client“ (com.snc.integration.scim2.client) enthält die folgenden Systemeigenschaften, Tabellen, skriptfähige APIs und Protokolle.

Eigenschaften

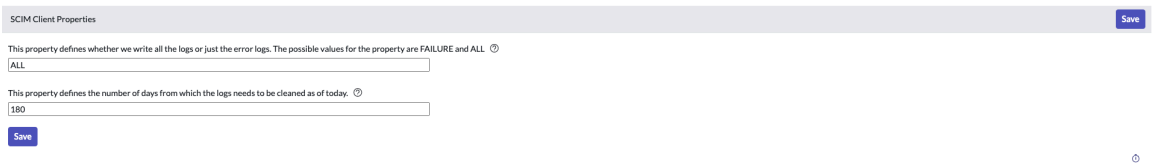
SCIM-Client fügt die folgenden Systemeigenschaften hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften

Name	Beschreibung
com.snc.integration.scim2.client.log.mode	Diese Eigenschaft bestimmt, ob alle Protokolldatensätze oder nur die Fehlerprotokolldatensätze geschrieben werden sollen. Die möglichen Werte sind **FEHLER** Oder **ALLE** . Standardwert: **ALLE**
com.snc.integration.scim2.client.log.clean.duration	Diese Eigenschaft bestimmt die Anzahl der Tage zum Löschen der Protokolle. Standardwert: **180**

Um die Eigenschaften festzulegen, navigieren Sie zu **Alle** > **SCIM** > **Eigenschaften des SCIM-Clients**an.



Tabellen

Der SCIM-Client fügt die folgenden Tabellen hinzu.

Tabellen

Name	Beschreibung
SCIM-Anbieter (sys_scim_Provider)	Speichert Daten für jeden SCIM-Anbieter, z. B. Name, REST-Nachrichtenressourcendefinitionen usw.
Ressourcenzuordnung des SCIM-Anbieters (sys_scim_Provider_resource_Mapping)	Speichert die Informationen der primären Tabelle für jeden Provider und Ressourcennamen.
SCIM-Attributzuordnung (sys_scim_Attribute_Mapping)	Speichert die Quelldetails, aus denen jeder SCIM-Attributwert stammen soll, z. B. Tabellenfeld, Skript usw.
SCIM-Clientprotokoll (sys_scim_Client_Logs)	Speichert die Status jedes Anrufs, der beim SCIM-Anbieter ausgelöst wurde.

Skriptfähige API

Die SCIM2Client-API ruft den SCIM-Provider (System for Domain Identity Management) (Serverrolle) auf, um Daten in einem Service Provider (SP) zu erstellen, zu aktualisieren oder zu löschen. Die skriptfähige API des SCIM-Clients sollte in den Skripts verwendet werden, die im Systemkontext oder von einem Systemadministratoranwender ausgeführt werden.

Sie können beispielsweise das Skript verwenden, während Sie den Integrations-Hub-Workflow als Systemanwender ausführen, während Sie die geplanten Aufgaben ausführen usw.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden finden Sie einige der Anwendungsfälle für die Verwendung der skriptfähigen APIs:

- Stellen Sie als Administrator Identitätsinformationen aus Hintergrundskripts, Geschäftsregeln, Skripteinbindungsaufrufen, Workflows usw. bereit.
- Führen Sie als Administrator eine geplante Aufgabe oder eine Aufgabe bei Bedarf für die Identitätsbereitstellung aus.
- Führen Sie einen Workflow oder einen Subworkflow mit dem Skriptschritt mithilfe des API-Aufrufs „Bereitstellung skriptfähig“ aus.
- Fügen Sie das Bereitstellungsskript direkt in einer Business-Regel oder Skripteinbindung hinzu. Das Skript kann von nicht-Administratoranwendern ausgelöst werden. Dieser Anwendungsfall funktioniert in den folgenden Situationen:
  - Der Anwender hat Zugriff auf das Token, d. h. der Anwender hat die Rolle, das Token aus der REST-Vorlage zu generieren.
  - Der Anwender hat Zugriff, um die SCIM-Attributwerte aus den zugeordneten Tabellen abzurufen.

Weitere Informationen zur skriptfähigen API finden Sie unter SCIM2Client-API .

SCIM-Clientprotokolle

Die SCIM-Clientprotokolle zeigen den Bereitstellungsstatus der SCIM-APIs an. Um den Bereitstellungsstatus anzuzeigen, navigieren Sie zu **Alle** > **SCIM** > **SCIM-Clientprotokolle**an.

REST-Nachrichten erstellen

Konfigurieren Sie eine REST-Nachricht für alle ausgehenden Anrufe für einen bestimmten SCIM-Provider.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **Ausgehend** > **REST-Nachricht**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

SCIM-Anbieter

Feld	Beschreibung
Name	Beschreibender Name für diese Nachricht.
Endpunkt	Basis-URL des SCIM-Anbieters. Beispiel: `https://example.service-now.com/api/now/scim` .
Authentifizierungstyp	Typ der Authentifizierung, die für die Verbindung mit dem externen SCIM-Anbieter verwendet werden soll. Weitere Informationen finden Sie unter . Ausgehende REST-Authentifizierung .
REST-Nachrichtenheader	Der Inhaltstyp, der vom externen SCIM-Anbieter erwartet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Beispielsweise ist Headername der Inhaltstyp im folgenden API-Anforderungstext: Inhaltstyp: Application/scim+JSON

4. ##Klicken Sie in der zugehörigen Liste HTTP-Methoden au**Neu** .
5. Konfigurieren Sie die folgenden HTTP-Methoden.

Hinweis: Die URLs haben Variablen, die Sie ersetzen müssen.

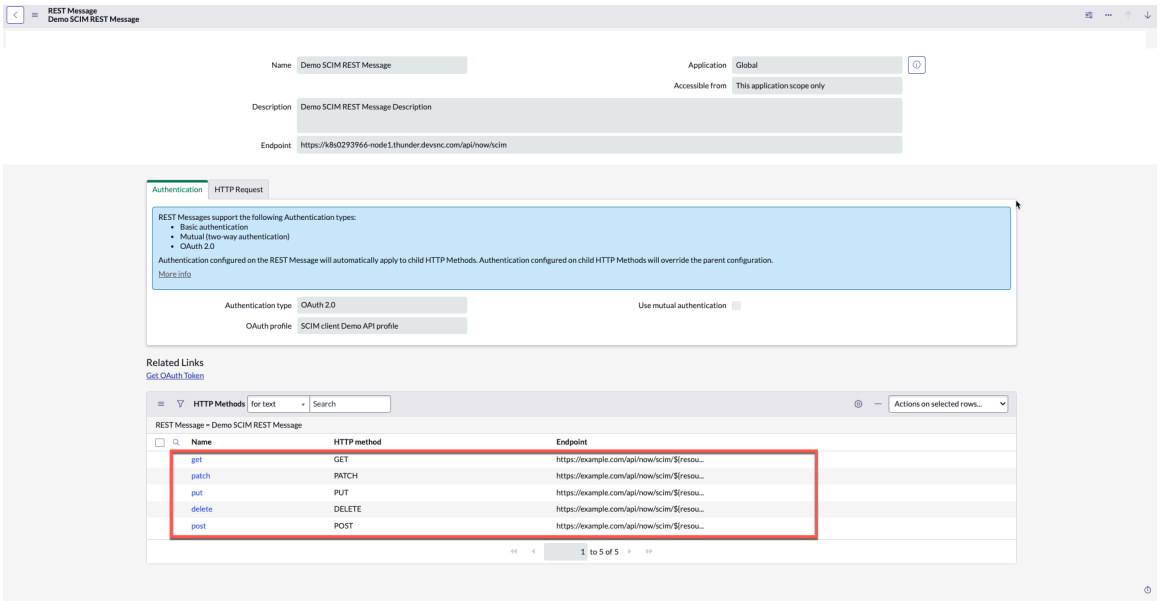
HTTP-Methoden

REST-Nachrichtenfunktionen	Beispiel-URL
GET	https://example.com/api/now/scim/${resourceName}
PATCH	https://example.com/api/now/scim/${resourceName}/${resourceId}
PUT	https://example.com/api/now/scim/${resourceName}/${resourceId}
LÖSCHEN	https://example.com/api/now/scim/${resourceName}/${resourceId}
VERÖFFENTLICHEN	https://example.com/api/now/scim/${resourceName}/${resourceId}

Hinweis:

- Sie müssen alle HTTP-Methoden für den Betrieb des SCIM-Clients erstellen.
- Eine Beispiel-REST-Nachricht wird vom Basissystem gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie auf **Absenden**.

Ergebnis
Der REST-Nachrichtendatensatz wird erstellt.

Nächste Maßnahme
Verwenden Sie die REST-Nachricht, um einen SCIM-Provider zu erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen SCIM-Provider.

Weitere Informationen zum Erstellen einer REST-Nachricht finden Sie unter Erstellen Sie eine REST-Nachricht .

Erstellen Sie einen SCIM-Provider

Erstellen Sie einen SCIM-Provider, um Ressourcentypen und Schemadaten vom SCIM-Provider mit der REST-Nachricht abzurufen. Aktivieren Sie die Konfiguration der HTTP-Methode (PUT oder PATCH), um eine Ressource im SCIM-Provider zu aktualisieren.

Vorbereitungen
Hinweis: Ein Beispiel für einen SCIM-Anbieter ist Teil des Basissystems. Sie können basierend auf Ihren Anforderungen verwenden und konfigurieren oder einen neuen Datensatz erstellen.

Erforderliche Rollen: administrator

Prozedur
1. Navigieren zu **Alle** > **SCIM-Client** > **SCIM-Anbieter**an.
2. Klicken Sie auf der Seite „SCIM-Anbieter“ auf **Neu** .
3. Füllen Sie im Formular die Felder aus.

Formular „SCIM-Anbieter“

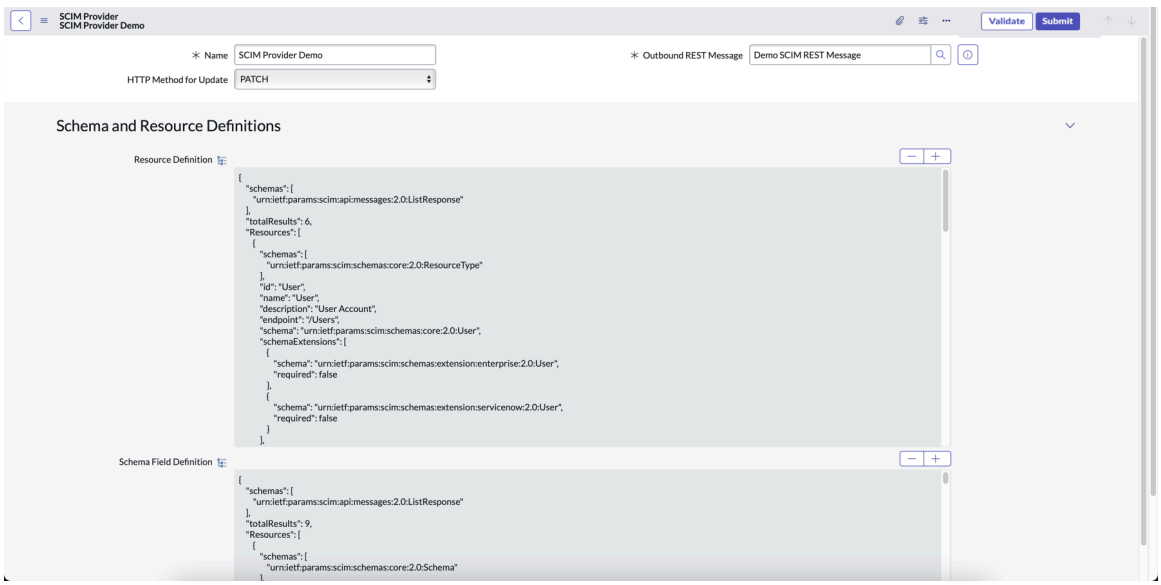
Feld	Beschreibung
Name	Name des SCIM-Anbieters

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ausgehende REST-Nachricht	Nachricht, die zum Aufrufen der API des SCIM-Anbieters verwendet wird. Weitere Informationen finden Sie unter REST-Nachrichten erstellen.
HTTP-Methode für Aktualisierung	Typ der HTTPS-Methode, die zum Aktualisieren der Ressourcenzuordnung verwendet wird. Die PATCH- oder PUT-Methode kann vom Client beim Aktualisieren der Identitätsressource während der Bereitstellung einer bereits vorhandenen Ressource verwendet werden.

Hinweis:

- Die **Ressourcendefinition** Und **Schemafelddefinition** Felder werden aus abgerufen */ResourceTypes*Und */Schemas*Öffentliche Endpunkte des SCIM-Anbieters. Diese Felder werden automatisch ausgefüllt, nachdem die Rest-Nachricht ausgewählt wurde.
- Wenn die REST-Nachricht, die Schemas oder die Ressourcentypen im SCIM-Provider aktualisiert werden, klicken Sie auf **Aktualisieren** Und dann **Aktualisieren** Um zu aktualisieren **Ressourcendefinition** Und **Schemafelddefinition** Felder.



4. Klicken Sie auf **Absenden**.

Ergebnis

Die SCIM-Anbieterdetails wurden erfolgreich erstellt. Verwenden Sie die Ressourcenzuordnung des SCIM-Anbieters, um die SCIM-Anbieterdetails den Ressourcen wie Anwendern oder Gruppen zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Provider-Ressourcenzuordnung.

Erstellen Sie eine SCIM-Provider-Ressourcenzuordnung

Definieren Sie die Zuordnungen von SCIM-Attributen zu ServiceNow Attribute für einen bestimmten Ressourcentyp und SCIM-Anbieter.

Vorbereitungen

Erforderliche Rollen: administrator

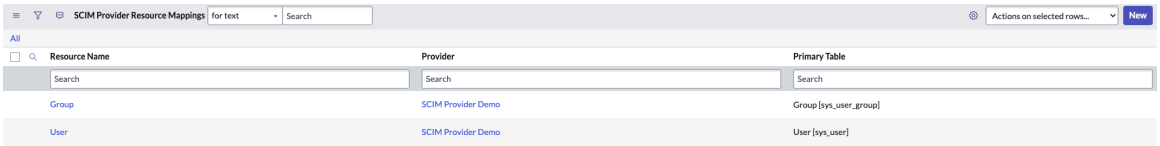
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **SCIM-Client** > **Ressourcenzuordnung des SCIM-Anbieters**an.

   Die SCIM-Provider-Ressourcenzuordnung wird standardmäßig mit der Anwender- und Gruppenzuordnung geliefert.

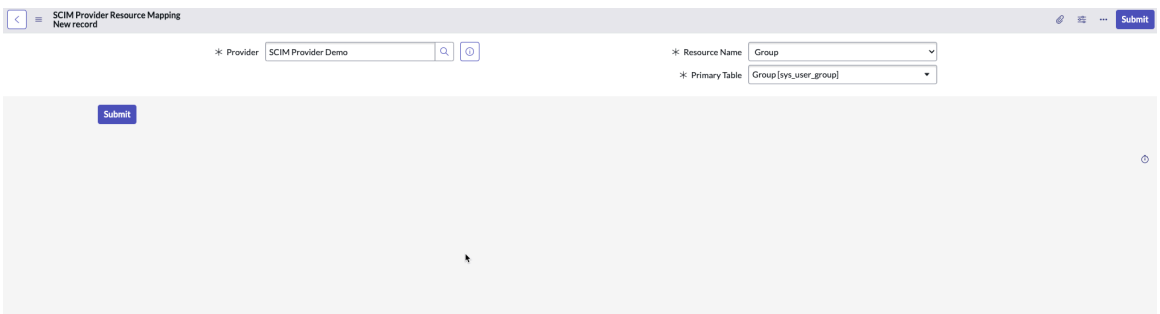
   Hinweis: Die Anwender- oder Gruppenzuordnungen enthalten Beispielzuordnungen, die Sie als Referenz verwenden können. Sie können auch eine Zuordnung basierend auf den Anwender- oder Gruppenressourcen erstellen.



2. Erstellen Sie eine Ressourcenzuordnung, indem Sie auf klicken **Neu** .
3. Füllen Sie im Formular die Felder aus.

Ressourcenzuordnung

Felder	Beschreibung
Anbieter	Name des SCIM-Anbieters. Beachten Sie beim Erstellen eines SCIM-Anbieters den Namen des konfigurierten Anbieters.
Ressourcenname	Ressource, für die die Zuordnung definiert werden muss.
Primäre Tabelle	Die Tabelle, die die sys_ID der zugeordneten Ressource enthält.



4. Klicken Sie auf **Absenden**.

Ergebnis

Der Datensatz wird erstellt und auf der Seite „SCIM-Provider-Ressourcenzuordnung“ angezeigt. Verwenden Sie die SCIM-Attributzuordnungen, um die Attribute aus Schemas weiter zuzuordnen. Weitere Informationen finden Sie unter Erstellen Sie eine SCIM-Attributzuordnung.

Erstellen Sie eine SCIM-Attributzuordnung

Erstellen Sie eine SCIM-Attributzuordnung, und verwenden Sie sie als einzelne Ressource für ServiceNow Tabellenfelder.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rollen: administrator

Warum und wann dieser Vorgang ausgeführt wird

Im Folgenden finden Sie die Attributzuordnungstypen und ihre Beschreibungen.

Attributzuordnungstypen

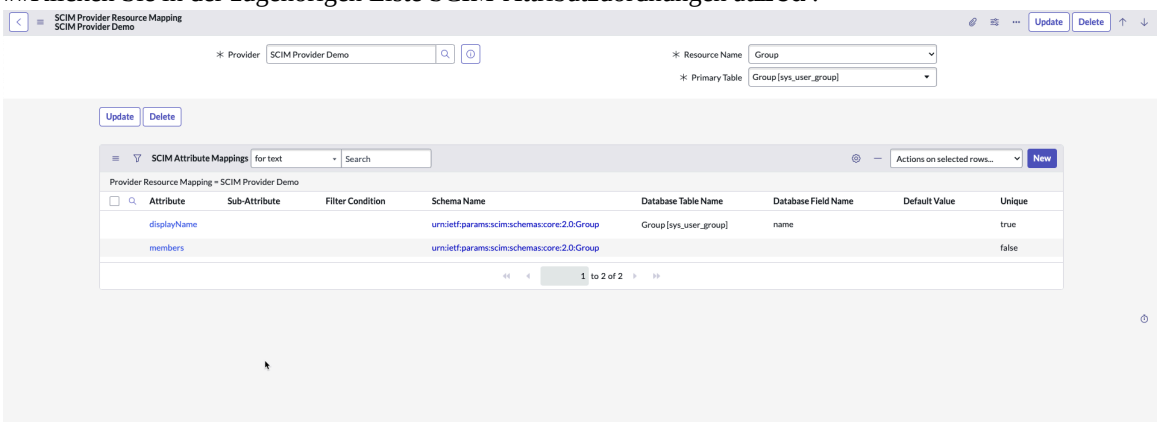
Attributzuordnungstyp	Beschreibung
Direkt	Das SCIM-Attribut wird mithilfe von ausgefüllt **Name Der Datenbanktabelle** Und **Datenbankfeldname** Felder.
Konstante	Das SCIM-Attribut wird mithilfe eines angegebenen Standardwerts ausgefüllt.
Skript/Anwenderdefiniert	Das SCIM-Attribut wird mithilfe des Rückgabewerts eines Skripts ausgefüllt. Dieses Attribut erfordert die Aktivierung der Option „Skript ausführen“.

Hinweis:

- Das Passwortattribut wird nicht unterstützt
- Eine Beispielattribute-Zuordnung für die Anwender- und Gruppenressourcen ist Teil des Basissystems. Sie können die Zuordnungen basierend auf Ihren Anforderungen verwenden und konfigurieren oder einen neuen Datensatz erstellen.

Prozedur

1. Navigieren zu **Alle** > **SCIM-Client** > **Ressourcenzuordnung des SCIM-Anbieters**an.
2. Hat die SCIM-Ressourcenzuordnung ausgewählt, die für die Konfiguration erstellt wird.
3. ##Klicken Sie in der zugehörigen Liste SCIM-Attributzuordnungen au**Neu** .



4. Füllen Sie im Formular die Felder aus.

Formular „SCIM-Attributzuordnungen“

Felder	Beschreibung
Ressourcenzuordnung des Anbieters	Attributzuordnung für eine Kombination aus Provider und Ressource.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Wenn dieses Feld nicht automatisch ausgefüllt wird, verwenden Sie die Suchoption. Wählen Sie den Datensatz „Anbieterressourcenzuordnung“ aus.
Schemaname	Schemaname des SCIM-Attributs, für das die Zuordnung definiert werden muss. Zum Beispiel *urn:ietf:params:scim:schemas:core:2.0:User*.
Attribut	Attribut Für die die Zuordnung definiert werden muss. Zum Beispiel *userName*.
Unterattribut	Unterattribut (Falls vorhanden), für die die Zuordnung definiert werden muss. Beispiel: Wenn ein komplexes Typattribut wie vorhanden ist *name.familyName*, Dann ist das Attribut **Name** Und das Unterattribut ist **FAMILYNAME** .
Feldtyp	Der Datentyp des SCIM-Attributs. Dieses Feld wird automatisch aus den vom SCIM-Provider definierten Schemas ausgefüllt. Beispiel: **boolescher wert** .
Mehrwertig	Mehrere Werte, die dem Attribut zugewiesen sind. Ein Attribut kann mehrere Werte wie geschäftliche E-Mail-Adresse, private E-Mail-Adresse oder eine andere E-Mail-Adresse haben. Zum Beispiel *emails*. Dieses Feld wird mit den vom SCIM-Provider definierten Schemas ausgefüllt.
Filterbedingung	Einige Attribute mit mehreren Werten können zusätzliche Informationen enthalten, die mithilfe von angegeben werden können Filterbedingung . Die Auswahlmöglichkeiten der Filterbedingung werden mit den vom SCIM-Provider definierten Schemas ausgefüllt. Zum Beispiel die *phoneNumbers*Attribut hat mehrere Typen wie „Arbeit“, „Mobilgerät“, „Startseite“ usw.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
Eindeutig	Option zur eindeutigen Identifizierung einer Ressource zwischen dem SCIM-Client und dem SCIM-Provider-System. Attribute mit mehreren Werten können nicht als eindeutig markiert werden. Beispiel: Für eine Anwenderressource die *username*Attribut kann eindeutig gemacht werden.
Name der Datenbanktabelle	Verwenden Sie dieses Feld, um den Attributtabellennamen zu zuordnen ServiceNow Tabellenname. Wenn Sie die direkte Attributzuordnung wählen, müssen Sie dieses Feld definieren. Zum Beispiel die *username*Das SCIM-Attribut kann dem zugeordnet werden **Anwender** Feld in **Name Der Datenbanktabelle** Feld.
Name des Datenbankfelds	Die Datenbankfeldname Feld Zuordnungen Das SCIM-Attribut für ServiceNow Feldname, der dem SCIM-Attribut zugeordnet werden soll. Wenn Sie die direkte Attributzuordnung wählen, müssen Sie dieses Feld definieren. Zum Beispiel die *username*Das SCIM-Attribut kann dem zugeordnet werden **Anwender-ID** Feld in **Datenbankfeldname** Feld.
Standardwert	Details zum Standardwert Der an den SCIM-Anbieter übergeben wird. Kann verwendet werden ich f die direkte Attributzuordnung von Feld Gibt null zurück oder ob der Standard verwendet werden kann, um einen hartcodierten Wert zurückzugeben. Im Falle eines hartcodierten Werts müssen der Name der Datenbanktabelle und der Feldname lauten **Keine** . Beispielsweise kann der primäre Unterattribut-Wert der geschäftlichen E-Mail hartcodiert werden als **Wahr** .
Skript ausführen	Option zum Abrufen des Attributs über ein Skript.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Diese Option ist für die Attribute mit mehreren Werten erforderlich, die keine Filterbedingung enthalten. Für einen komplexen Attributtyp kann ein Skript den Wert auf einer Attribut- oder Unterattributebene bereitstellen. Zum Beispiel die **Mitglieder** Attribut der Gruppenressource hat keine Filterbedingung. Daher sollte die Skriptoption auf der übergeordneten Attributebene von definiert werden **Mitglieder** Attribut.
Skript	Skript, das zum Abrufen des Attributwerts verwendet wird. Der Rückgabetyp des Skripts muss eine Zeichenfolge oder eine als Zeichenfolge konvertierte JSON sein. Die Ausgabe des Skripts muss im richtigen Format vorliegen, wie vom Anbieter für dieses Attribut erwartet.

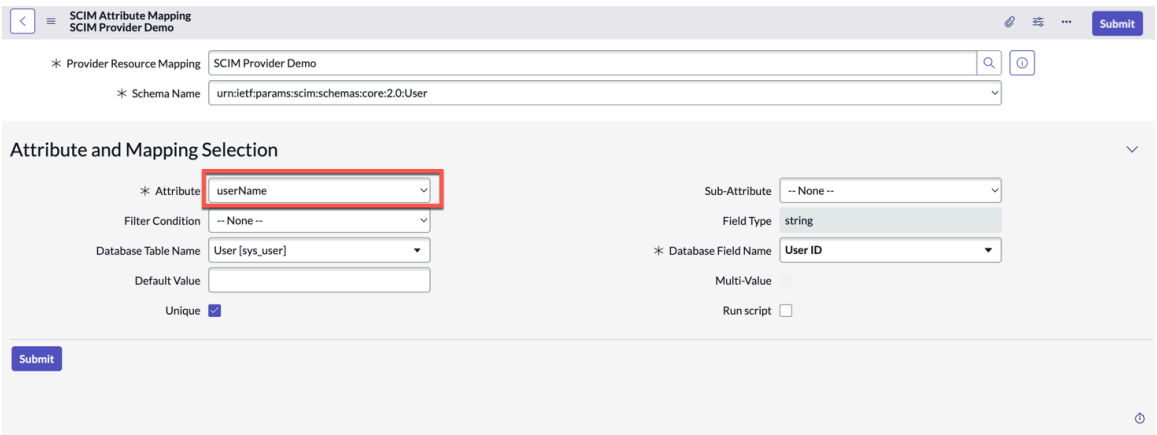
5. Klicken Sie auf **Absenden**.

Attributzuordnungsreferenzen

Mit den Attributzuordnungen können Sie die Attribute als eine einzelne Ressource für verwenden ServiceNow Tabellenfelder.

Attribut

Das Attribut, für das die Zuordnung definiert werden muss. Zum Beispiel *`userName`*.



Unterattribut

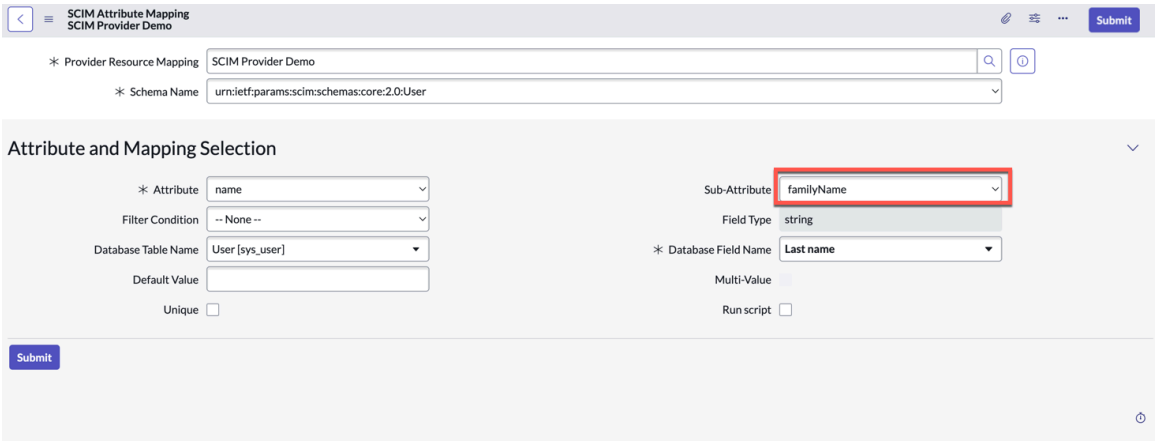
Wählen Sie gegebenenfalls das Unterattribut aus, für das eine Zuordnung definiert werden muss.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Wenn ein komplexes Typattribut wie vorhanden ist *`name.familyName`*, Dann ist das Attribut *`name`*Und das Unterattribut ist *`familyName`*.

Für einfache Attribute wie Anwendername, die **Unterattribut** Wert wäre **Keine** .

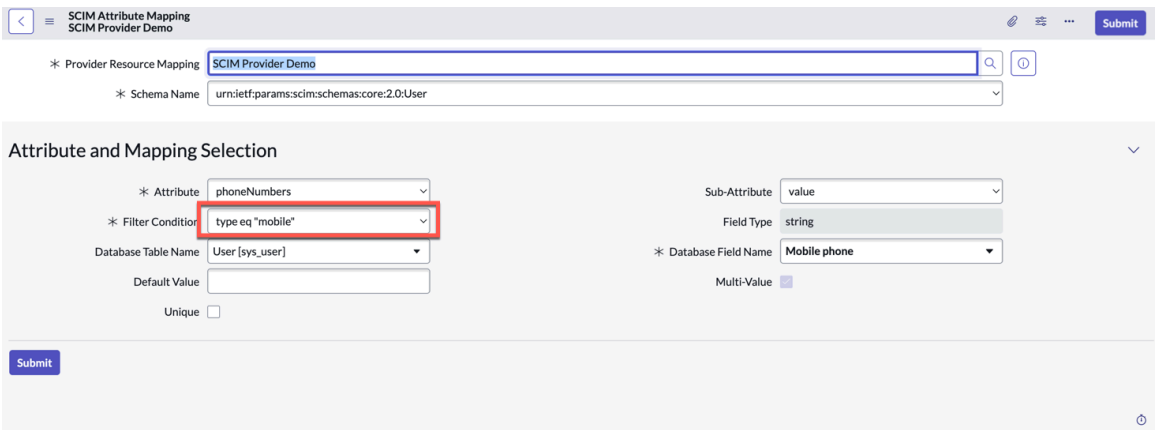


Filterbedingung

Ein Attribut mit mehreren Werten kann zusätzliche Informationen enthalten, die mithilfe einer Filterbedingung angegeben werden können. Die Auswahlmöglichkeiten für die Filterbedingung werden mit den vom SCIM-Provider definierten Schemas ausgefüllt.

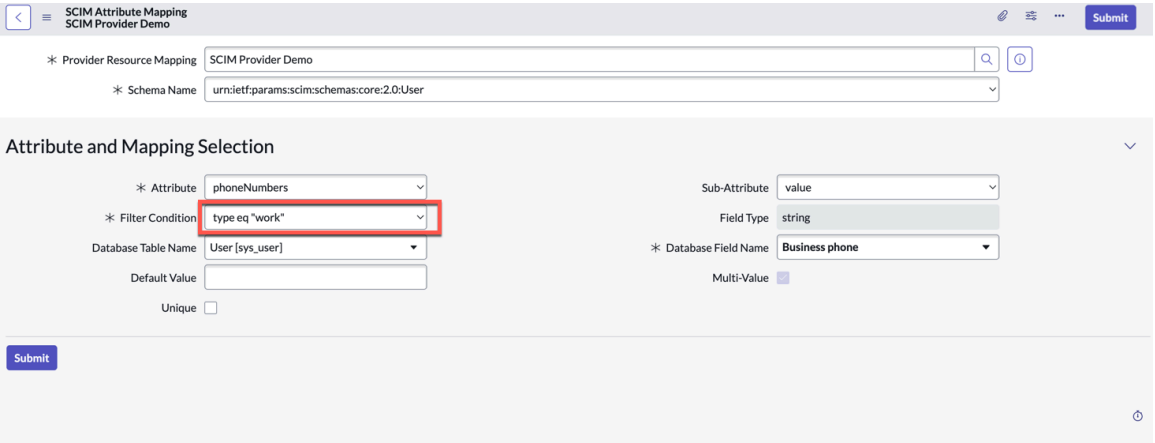
Zum Beispiel die *`phoneNumbers`*Attribut hat mehrere Typen wie „Arbeit“, „Mobilgerät“, „Startseite“ usw.

Sie können eine Filterbedingung aus einer Reihe möglicher Werte angeben. Zum Beispiel die *`phoneNumber`*Das Attribut kann die Filterbedingung als haben **Typ eq „mobil“** .



Die *`phoneNumber`*Attribut kann stattdessen eine Filterbedingung als haben **Typ eq „Arbeit“** .

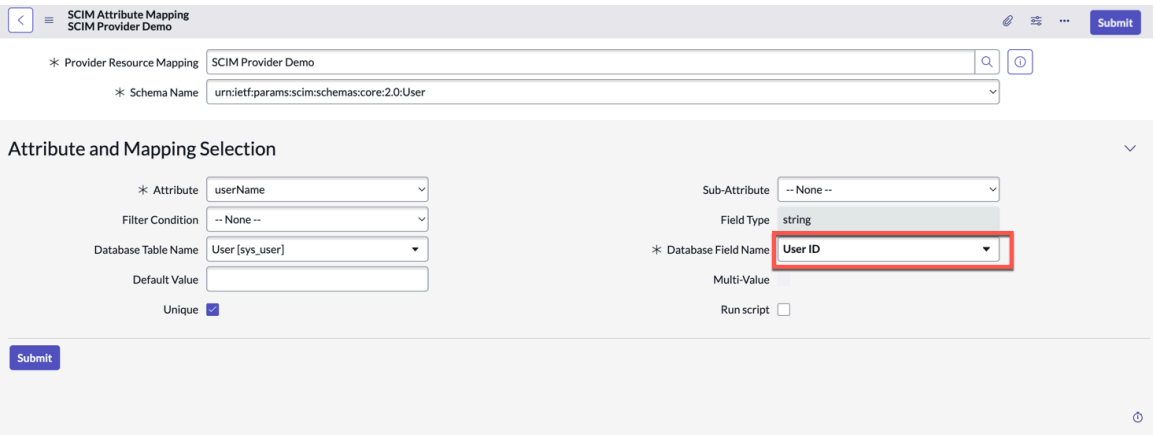
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



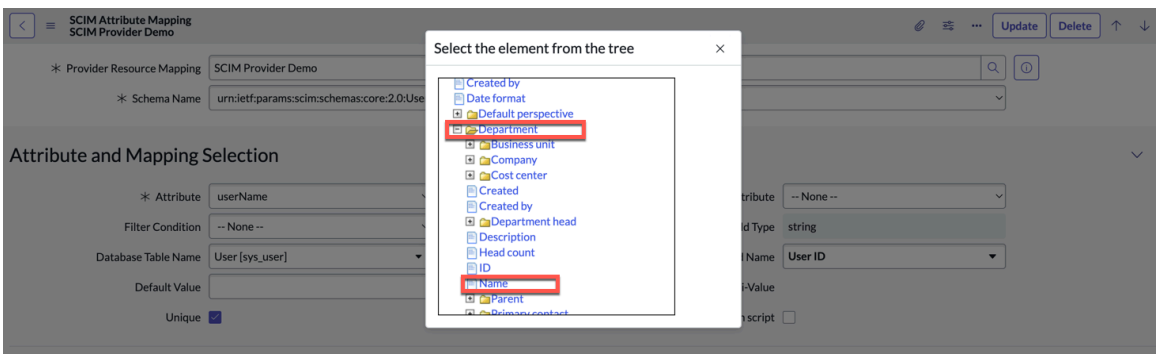
Name des Datenbankfelds

Wenn die Option „direkte Attributzuordnung“ ausgewählt ist, muss dieses Attribut definiert werden. Die **Datenbankfeldname** Feld stellt dar ServiceNow Feldname, der dem SCIM-Attribut zugeordnet ist.

Zum Beispiel die *username*Das SCIM-Attribut kann einem Anwender als zugeordnet werden **Name Der Datenbanktabelle** Und in das Feld Anwender-ID als **Datenbankfeldname** Feld.

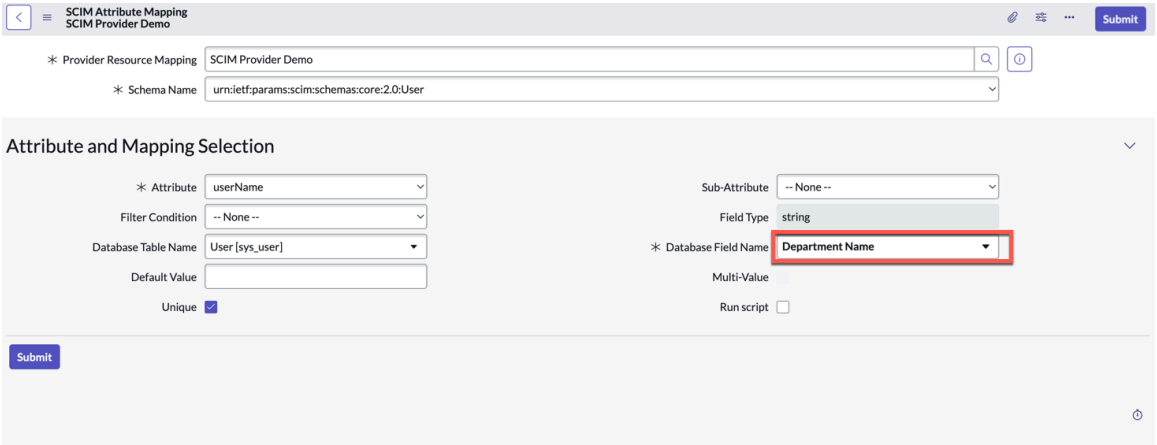


Sie können auch Dot-Walking mit durchführen **Datenbankfeldname** . Zum Beispiel die **Abteilung** Das SCIM-Attribut kann dem zugeordnet werden **Abteilungsname** Feld.



Hier ist die Datenbanktabelle **Anwender** Und der Name des Datenbankfelds ist **Abteilungsname** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

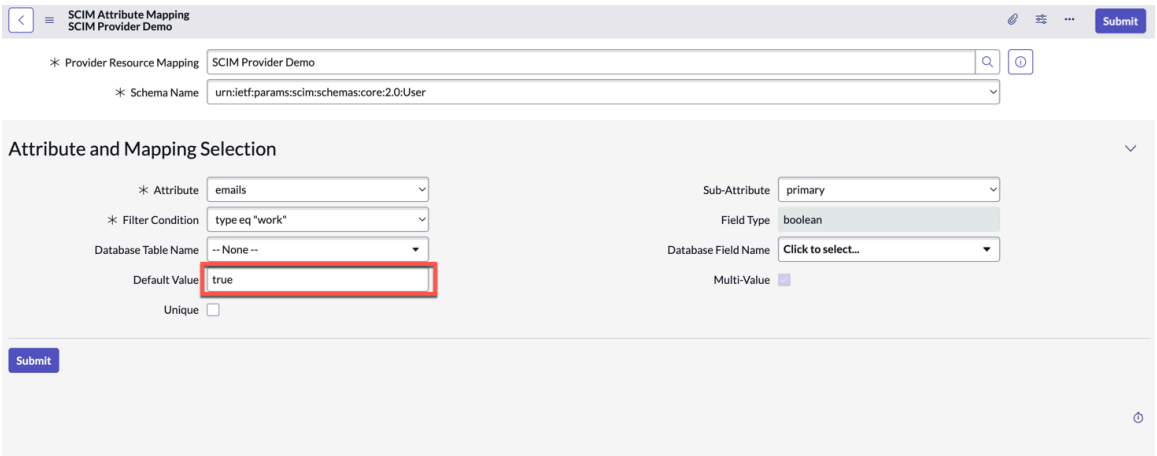


Standardwert

Der Standardwert wird an den SCIM-Anbieter übergeben, wenn die direkte Attributzuordnung dieses Felds null zurückgibt. Der Standardwert kann auch verwendet werden, um einen hartcodierten Wert zurückzugeben.

Im Falle eines hartcodierten Werts müssen der Name der Datenbanktabelle und der Feldname lauten **Keine** .

Beispielsweise kann der primäre Unterattribut-Wert der geschäftlichen E-Mail hartcodiert werden als **Wahr** .

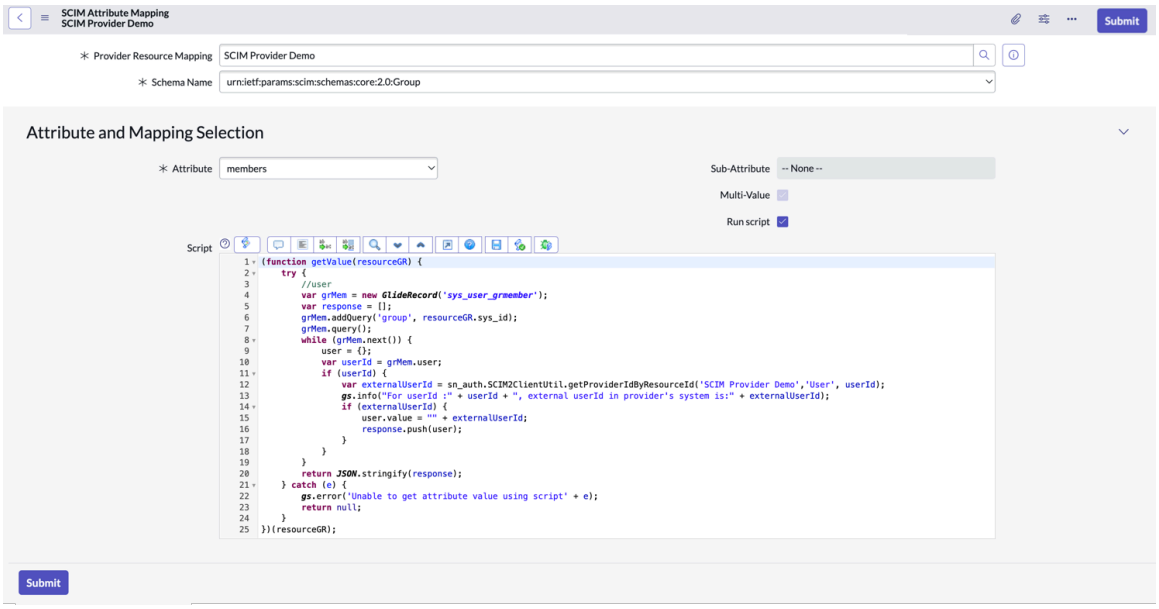


Skript

Das Skript wird verwendet, um den Attributwert abzurufen. Der Rückgabetyp des Skripts muss immer eine Zeichenfolge oder eine als Zeichenfolge konvertierte JSON sein. Die Ausgabe des Skripts muss im richtigen Format vorliegen, wie vom Anbieter für dieses Attribut erwartet.

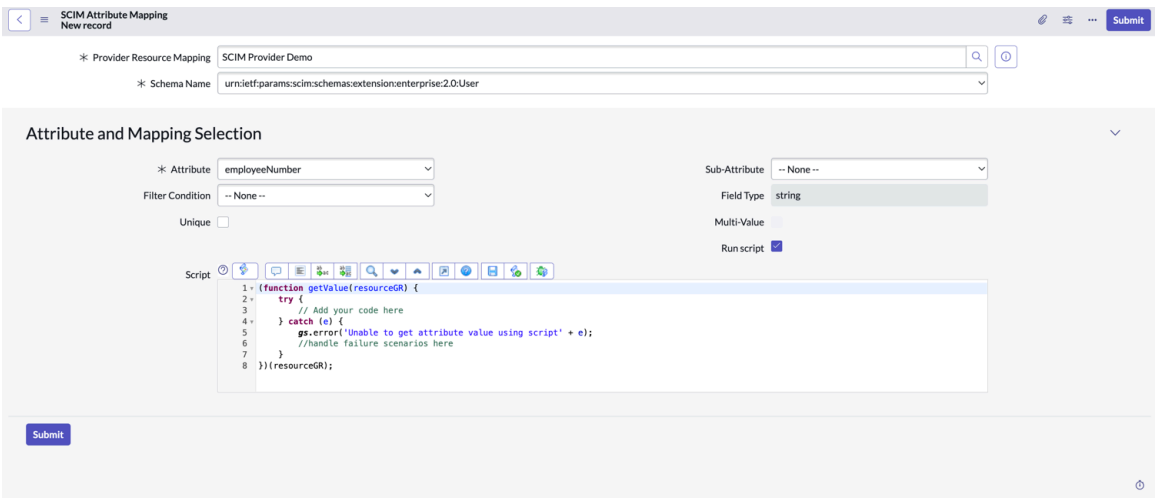
Im Folgenden finden Sie ein Beispielskript für ein Attribut mit mehreren Werten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Ausgabe des Skripts muss ein JSON-Array mit Zeichenfolgen aufweisen.

Im Folgenden finden Sie ein Beispielskript eines Attributs mit einem einfachen Wert.



Die Ausgabe des Skripts muss eine Zeichenfolge sein.

Fehlerbehebung für SCIM-Client

Problembehebungsaktionen können bei der Lösung häufiger Probleme beim Einrichten oder Ausführen des SCIM-Clients helfen.

Problembehandlung

Problem	Aktion
Antwort enthält die folgende Nachricht: “message":"Unable to access the table core_company with id: 0c441abbc6112275000025157c651c89, Please cross check the Access control rules"	Die Nachricht wird angezeigt, wenn die API in einem Anwenderkontext aufgerufen wird und der Anwender keinen Zugriff auf die Tabelle hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung (Fortsetzung)

Problem	Aktion
	Sie müssen sicherstellen, dass die skriptfähige API im Systemkontext aufgerufen wird.
Antwort enthält die folgende Nachricht: `{"message":"User Not Authenticated","detail":" Required to provide Auth information"}`	• Stellen Sie sicher, dass das Token über die entsprechende REST-Nachricht generiert wird und gültig ist. • Stellen Sie sicher, dass die skriptfähige API im Systemkontext aufgerufen wird.
Antwort enthält die folgende Nachricht: `Script execution failed, the reason is: Cannot cast java.lang.Integer to java.lang.String`	Wenn in der SCIM-Attributzuordnung das Feld so definiert ist, dass es aus einem Skript mit diesem Problem abgerufen wird, stellen Sie sicher, dass der Rückgabetyp immer eine Zeichenfolge sein muss.
Antwort enthält die folgende Nachricht: `"status": "400", "scimType": "invalidValue", "detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"`	Für jedes SCIM-Attribut, das die ID erwartet, ist diese ID immer vom Anbietersystem. Stellen Sie sicher, dass die in der Nutzlast übergebene ID im Anbietersystem gültig ist.

Bereiche, die auf Problembehandlung überprüft werden sollen

Im Folgenden sind einige der Bereiche aufgeführt, die bei der Verwendung des SCIM-Clients auf Fehlerbehebungsfehler überprüft werden können:

- Wenn beim Ausführen einer der skriptfähigen APIs ein Problem gefunden wird, lesen Sie den Abschnitt „SCIM-Clientprotokolle“.

Protokollfelder

Feld	Beschreibung
Anforderungs-ID	Eindeutige ID, die eine aufgerufene skriptfähige API darstellt.
SCIM-Anbieter	Anbietername, für den die API aufgerufen wird.
Ressource	Name der Ressource, für die die API aufgerufen wird.
Ressourcen-ID	Die ID, für die die API aufgerufen wird. Zum Löschen stellt die ID die Ressourcen-ID im Anbietersystem dar, und die ID befindet sich im Clientsystem.
Aktion	API, die aufgerufen wird
Status	Status des Protokolls als Erfolg oder Fehler

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Nachricht	Erfolgs- oder Fehlermeldung. Die Fehlermeldung kann vom SCIM-Anbieter oder aufgrund von Konfigurationsproblemen im SCIM-Client stammen.

- Überprüfen Sie den Anforderungstext, indem Sie ausgehende Anrufe konfigurieren und anzeigen. Weitere Informationen finden Sie unter Protokollierung ausgehender Webservices .
- Aktualisieren Sie die Protokollebenen, indem Sie den Inhaltstyp hinzufügen, das Beispiel testen und in der REST-Nachricht des entsprechenden Providers zum entsprechenden HTTP-Methodenformular navigieren.
- Wenn der Anforderungstext gekürzt ist, erhöhen Sie den Grenzwert mithilfe der Systemeigenschaft `glide.outbound_http.content.max_limit`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

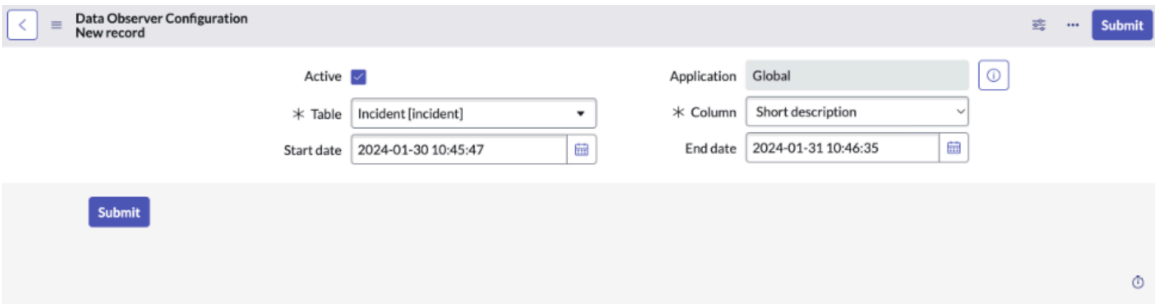
Zugriffsbeobachter

Verwenden Sie Access Observer, um Zugriffsdaten für Personen und Prozesse in Ihrer Instanz zu verstehen.

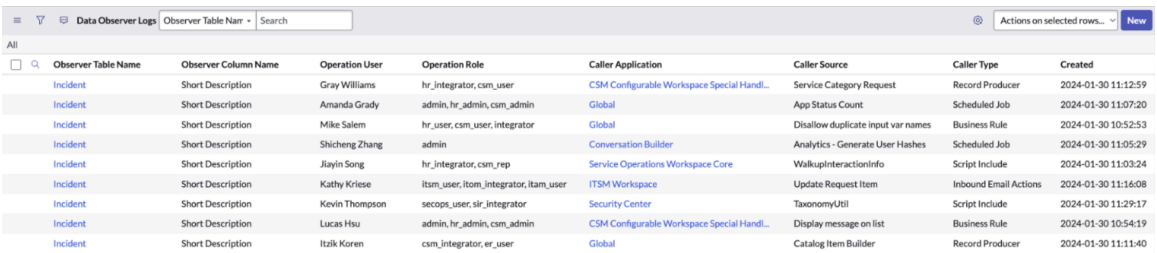
Mit Access Observer können Sicherheitsadministratoren:

- Verstehen Sie, welche Entitäten wie Anwender, Rollen, bereichsbezogene Apps und Skripts auf Ihre Daten zugreifen.
- Verwenden Sie dieses Vorwissen, um zu erfahren, wie Sie Sicherheit am besten anwenden können, um unnötigen Zugriff auf Ihre Daten zu beschränken und gleichzeitig diejenigen zu bestätigen, die Zugriff benötigen und weiterhin normal funktionieren.
- Vermeiden Sie eine fehlerhafte Automatisierung, indem Sie einen klaren Überblick darüber erhalten, wie auf Ihre Daten zugegriffen wird, bevor Sie Sicherheitsänderungen vornehmen.
- Beheben Sie die Notwendigkeit, Informationen darüber bereitzustellen, wie die Verschlüsselung auf Ihre Instanz angewendet wird.

Konfigurieren Sie Access Observer, indem Sie Access Observer-Konfigurationsdatensätze erstellen. In diesen Datensätzen definieren Sie eine bestimmte Tabelle und Spalte, die beobachtet werden soll, sowie die Zeit, in der die Spalte beobachtet wird.



Suchen Sie die Ergebnisse Ihrer Beobachtungen in der Datensatztabelle des Zugriffsüberwachungsprotokolls. In dieser Tabelle wird jedes Mal, wenn auf die angegebene Spalte zugegriffen wird, ein Datensatz angezeigt.



Konfigurieren Sie die Zugriffsbeobachtung

Erstellen Sie einen Zugriffsbeobachtungsdatensatz, um den Zugriff auf eine Datenspalte während eines angegebenen Zeitfensters zu überprüfen.

Vorbereitungen
Erforderliche Rolle: security_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Zugriffsüberwachung** > **Zugriffsüberwachung – Konfiguration**an.
2. Wählen Sie **Neu**, um einen Datensatz zu erstellen.
3. Füllen Sie im Formular die Felder aus.

Greifen Sie auf Konfigurationsfelder des Beobachters zu

Feld	Beschreibung
Aktiv	Ob der Datensatz aktiv ist Ihr Datensatz wird während des Beobachtungszeitraums automatisch als aktiv markiert und andernfalls inaktiv.
Anwendung	Die bereichsbezogene Anwendung für den Datensatz. Dieses Feld ist schreibgeschützt.
Tabelle	Tabelle, die die zu beobachtende Spalte enthält
Spalte	Die Spalte in der ausgewählten Tabelle, die beobachtet werden soll.
Aufgabe sofort starten	Wenn diese Option ausgewählt ist, beginnt die Beobachtung, sobald der Datensatz erstellt wurde.
Enddatum und -zeit	Der Zeitpunkt, zu dem die Beobachtung endet.
Startdatum und -uhrzeit	Der Zeitpunkt, zu dem die Beobachtung beginnt. Dieses Feld ist nur sichtbar, wenn **Auftrag sofort starten** Ist nicht ausgewählt.

4. Wählen Sie Aus **Übermitteln** Zum Speichern des Datensatzes.

Nächste Maßnahme

Sobald das von Ihnen definierte Beobachtungsfenster gestartet wurde, können Sie jede Instanz, auf die auf die Spalte zugegriffen wurde, detailliert in den Datensätzen in der Tabelle „Zugriffsüberwachungsprotokoll“ [sys_Data_ob_log] anzeigen.

Überprüfen Sie die Protokolle des Zugriffsüberwachungsservers

Verwenden Sie Informationen in den Zugriffsüberwachungsprotokolldatensätzen, um Einblicke in den Zugriff auf Ihre Daten zu erhalten.

Sobald Sie einen oder mehrere Zugriffsbeobachtungsdatensätze konfiguriert haben, beginnt Ihre Instanz mit der Erstellung von Zugriffsbeobachtungsprotokolldatensätzen mit Details zum Zugriff auf die von Ihnen ausgewählten Spalten. Sie finden diese Datensätze in Ihrer Instanz unter **Alle** > **Zugriffsüberwachung** > **Zugriffsüberwachung – Protokoll**an.

Zugriff auf Beobachterprotokollergebnisse

Verwenden Sie die folgende Tabelle, um die Informationen in den Protokollen zu verstehen.

Zugriff auf Beobachtungsprotokollfelder

Feld	Beschreibung
Name der Beobachter-Tabelle	Die Tabelle, die im Zugriffsbeobachtungsdatensatz ausgewählt wurde, der diesen Datensatz generiert hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf Beobachtungsprotokollfelder (Fortsetzung)

Feld	Beschreibung
Name der Beobachter-Spalte	Die im Zugriffsbeobachtungsdatensatz ausgewählte Spalte, die diesen Datensatz generiert hat.
Vorgangsanwender	Anwender, der auf die Spalte zugegriffen hat
Vorgangsrolle	Rollen für den Anwender, der auf die Spalte zugegriffen hat
Aufruferanwendung	Die bereichsbezogene Anwendung, von der aus auf die Daten zugegriffen wurde.
Aufrufertyp	Der Typ des Elements, das auf die Spalte zugegriffen hat, z. B. Datensatzersteller, geplante Aufgabe oder Business-Regel.
Dokument-ID der Aufruferquelle	
Aufruferquelle	Element, das auf die Spalte zugegriffen hat. Wird entlang des verwendet **Anrufertyp** Feld, um anzuzeigen, was speziell auf die Spalte zugegriffen hat. Zum Beispiel, wenn der Anrufertyp ist `Business-Regel` , Die Anruferquelle ist der Name der Business-Regel, die auf die Spalte zugegriffen hat.
Primärer Hash	
Wiederholungsanzahl	
Java-Stack	
JavaScript-Stapel	
Sitzungs-ID	ID der Sitzung, in der auf die Spalte zugegriffen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Ressourcen für Plattformsicherheitsprodukte und -Lösungen

Wenn Sie nach Best Practices für Plattformsicherheit, Problembehandlung oder anderen Implementierungsrichtlinien suchen, wählen Sie einen zu erkennenden Funktions- oder Ressourcentyp aus ServiceNow Ressourcen auf anderen relevanten Websites.

Hinweis: Viele Ressourcen in dieser Tabelle erfordern, dass Sie sich bei Websites wie anmelden ServiceNow Universität, Now Create oder ServiceNow Community. Wenn die erwartete Ressource nicht geladen wird, melden Sie sich an, und versuchen Sie erneut, auf die Ressource zuzugreifen.

Ressourcen-Links

Plattformsicherheitsfunktionen oder -Produkte	Ressourcentyp	Ressourcen
Sicherheitscenter	Erste Schritte	ServiceNow-Sicherheitszentrum
Sicherheitscenter	Best Practices	• Best Practices – Sicherheitscenter • BEST Practices für Security Center-Härtung
Sicherheitscenter	Häufig gestellte Fragen	ServiceNow-Sicherheitshärtung: Sicherheitszentrum
Codesignatur	Erste Schritte	• Codesignatur für verbesserte Tiefenverteidigung • Codesignatur und Circle of Trust (Cot): Einführung
Datenschutz	Tipps und Beispiele	[Washington-Release] Minimierung des Risikos der unbeabsichtigten Offenlegung vertraulicher Daten durch Datenschutz
Feldverschlüsselung	Tipps und Beispiele	Verschlüsselung auf Feldebene in ServiceNow
Feldverschlüsselung Enterprise	Erste Schritte	Unterschiede zwischen Verschlüsselung auf Feldebene und Verschlüsselung auf Plattformebene
Feldverschlüsselung	Problembehandlung	• Warum wird die Verschlüsselung auf Feldebene nicht auf Felder des Datentyps „Telefonnummer“ angewendet • Wir verschlüsseln die Feldebene im Fall „Mitarbeiterbeziehungen“ • Anhänge mit „Verschlüsselung auf Feldebene“ verschlüsseln • Verschlüsselte Feldkonfiguration kann nicht gelöscht werden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen-Links (Fortsetzung)

Plattformsicherheitsfunktionen oder -Produkte	Ressourcentyp	Ressourcen
		• Falltabelle ist in der Konfiguration verschlüsselter Felder nicht verfügbar • Das Abfragen des verschlüsselten Felds gibt keine konsistenten Ergebnisse in geplanten Aufgaben zurück
Feldverschlüsselung Enterprise	Problembehandlung	• Verschlüsselung Auf Feldebene Enterprise: Ersteinrichtung • Verschlüsselung auf Feldebene Enterprise: Einschränkungen und Überlegungen • Verschlüsselung Auf Feldebene Enterprise: Administration
Edge Encryption	Problembehandlung	• Edge Encryption in ServiceNow – Übersicht • Edge Encryption: Ersteinrichtung • Edge Encryption-Regeln • Edge Encryption: Einschränkungen • Edge Encryption: Administration
Edge Encryption	Tipps und Beispiele	• Edge Encryption-Ressourcen • Edge Encryption-Proxy-Protokolle • Benachrichtigung Über Ablauf Des Edge Encryption-Zertifikats
Edge Encryption	Problembehandlung	• Edge Encryption-Leistungsdiagramme • Edge Encryption Erweitert Die Feldlänge
Datenbankverschlüsselung	Tipps und Beispiele	Datenbankverschlüsselung in ServiceNow: TSE/DBE mit CCS
Zugriffsverwaltung	Tipps und Beispiele	Identitäts- und Zugriffsmanagement mit ServiceNow
Zero Trust-Zugriff	Problembehandlung	Hilfe bei Zugriffsanalyse, Zero Trust-Zugriff und adaptiver Authentifizierung in ServiceNow
Domänentrennung für Service Provider	Problembehandlung	ServiceNow-Domänentrennung für Service Provider
Datenfilterung	Erste Schritte	Verständnis des Plugins „Datenfiltration“
Sicherheitsrollen	Tipps und Beispiele	Wie funktionieren Sicherheitsrollen?

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen-Links (Fortsetzung)

Plattformsicherheitsfunktionen oder -Produkte	Ressourcentyp	Ressourcen
Verbindung und Anmeldeinformationen	Erste Schritte	Übersicht über Verbindungen und Anmeldeinformationen: Lernen Sie Integrationen im kennen ServiceNow AI Platform
ServiceNow Zugriffssteuerungen	Tipps und Beispiele	Zugriffssteuerungen: Der Einfache Weg
Sicherheitscenter	Best Practices	Best Practices – Sicherheitscenter
Platform-Sicherheit	Best Practices	• Leitfaden für Best Practices für ServiceNow-Sicherheit • Sicherung der ServiceNow KI-Plattform

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.