Yokohama 플랫폼 보안

마지막 업데이트 날짜: 2025년4월22일

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

servicenow

해당 자료는 사용자 편의를 위해 번역 소프트웨어를 사용하여 번역되었습니다. 정확한 번역을 제공하기 위해 합당한 노력을 기울였지만, 사람이 직접 번역하는 것을 대체할 수 있는 기계 번역은 없습니다. 번역은 "기계 번역 결과 그대로" 제공됩니다. 다른 언어로 번역한 내용의 정확성, 신뢰성 또는 무결성에 대해서 명시적이든 묵시적이든 어떠한 보증도 하지 않습니다. 일부 콘텐츠는 번역 소프트웨어의 한계로 인해 정확하게 번역되지 않을 수 있습니다. 해당 자료의 공식 언어는 영어입니다. 번역에서 발생한 불일치 또는 차이점은 구속력이 없으며 규정 준수나 시행을 위한 법적 효력이 없습니다.

여기에 표시된 일부 예와 그래픽은 설명을 위해서만 제공됩니다.
ServiceNow 제품 또는 서비스와의 실제 연관 또는 연결을 의도하지 않았으며 그렇게 유추해서는 안 됩니다.

ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다. 기타 회사 및 제품 이름은 관련된 해당 회사의 상표일 수 있습니다.

다음 사이트에서 ServiceNow 웹 사이트 이용 약관을 읽어보십시오.
www.servicenow.com/terms-of-use.html

기계번역

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

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목차

인스턴스 보호 10
ServiceNow Vault 12
플랫폼 보안 15
보안 센터 16
보안 센터 방문 18
보안 구성 콘솔 19
보안 모니터링 콘솔 48
보안 태세 콘솔 60
보안 학습 69
보안 배너 공지 69
인스턴스 보안 센터 70
마이그레이션으로 ServiceNow 보안 센터 인스턴스 보안 센터 78
보안 이벤트 모니터링 80
일일 준수 점수를 확인하고 보안 속성 설정을 구성합니다. 85
잘못된 보안 정의 스캔 94
인스턴스 메트릭 모니터링 95
ISC 가상 에이전트 인터페이스 활성화 106
강화 설정 107
강화 설정 기준선 109
접근 통제 163
API 및 웹 서비스 221
아키텍처, 설계 및 위협 모델링 234
인증 244
비즈니스 논리 273
커뮤니케이션 275
구성 281
데이터 보호 291
오류 처리 및 로깅 294
파일 및 자원 303
악성 코드 311
세션 관리 312
저장된 암호화 327
확인, 삭제 및 인코딩 329
로그 익스포트 서비스 (레즈) 363
탐색 로그 익스포트 서비스 (LES) 364
관리 로그 익스포트 서비스 (LES) 367
구성 로그 익스포트 서비스 (LES) 369
사용 로그 익스포트 서비스 (LES) 380
로그 익스포트 서비스 (LES) 참조 382

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그 항목 383
시스템 로그 384
로깅, 감사 및 오류 397
비밀 관리 398
비밀 관리 탐색 399
클라이언트 접근 가능한 비밀 구성 403
비밀 관리 대시보드 419
코드 서명 429
코드 서명 탐색 432
코드 서명 구성 435
코드 서명 사용 455
코드 서명 참조 469
바이러스 백신 검사 475
바이러스 백신 검사 탐색 476
바이러스 백신 검사 구성 478
격리된 파일 검토 479
바이러스 백신 활동 검토 480
의 딕셔너리 속성에 대해 알아보기 바이러스 백신 검사 480
HTML 위생 검사 482
HTML 위생 검사 살펴보기 483
HTML 위생 검사 구성 486
HTML 위생 검사 사용 487
개별 필드에서 정리 사용 487
HTML 위생 검사 로깅 사용 488
스타일 유효성 검사 사용 488
감사 489
감사 살펴보기 490
테이블에 대한 감사 구성 492
테이블에 대한 포함 목록 감사 사용 493
감사 대상에서 필드 제외(제외 목록) 493
감사에 테이블 필드 포함(포함 목록) 494
시스템 테이블에 대한 감사 사용 494
시스템 감사 및 감사 관계 보기 변경 테이블 495
감사 관계 변경(sys_audit_relation) 테이블의 작동 방식 495
히스토리 세트에 대한 지식 496
감사와 이력 세트의 차이점 497
이력에 대한 접근 제어 498
이력 항목 수 변경 498
이력 목록 498
이력 달력 500
이력 타임라인 502
참조 필드의 변경 내용 추적 505

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

삽입 추적 505
CI 관계 추적 506
높은 보안 설정 507
높은 보안 설정 탐색 508
스크립트 샌드박스 속성 구성 517
높은 보안 설정 활성화 520
VPN(가상 사설망) 524
VPN(가상 사설망) 살펴보기 525
VPN 서비스 활성화 527
VPN 통신을 위한 주소 구성 527
플랫폼 개인정보 보호 529
데이터 개인정보 보호 530
데이터 개인정보 보호 살펴보기 531
도메인 분리 및 데이터 개인정보 보호 532
익명화를 지원하는 필드 유형 532
데이터 개인정보 보호 역할 534
데이터 개인정보 보호(클래식) 535
Data Privacy 545
데이터 개인정보 보호용 Now Assist 549
데이터 디스커버리 552
데이터 디스커버리 탐색 554
데이터 디스커버리 활성화 555
찾기 페이지에서 데이터 디스커버리 데이터 분류 556
데이터 디스커버리 작업 556
데이터 디스커버리 역할 563
데이터 디스커버리 작업 결과 566
데이터 디스커버리 지원되는 데이터 유형 567
세분화된 구성으로 스캔 568
데이터 분류 570
데이터 분류 탐색 571
플러그인 데모 데이터 설치 데이터 분류 중 572
데이터 분류 생성 574
딕셔너리 항목에 데이터 분류 지정 575
개요 대시보드를 사용하여 데이터 분류 분석 575
도메인 분리 및 데이터 분류 577
데이터 익명화 578
익명화 기술 생성 578
익명화 정책 생성 581
익명화 작업 생성 585
데이터 익명화를 위한 병렬 작업 활성화 588
암호화 589
Key Management Framework 589

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 관리 프레임워크 탐색 591
키 관리 프레임워크 구성 597
핵심 관리 프레임워크 참조 610
키 관리 작업 620
웹 서비스에서 키 임포트 623
핵심 관리 프레임워크 상태 626
GlideEncrypter 사용 중단을 위한 인스턴스 준비 627
키 관리 프레임워크 자원 교환 630
인프라 보안 636
Key Management Framework(KMF)를 사용한 Password2 암호화 638
인증서 641
인증서 탐색 642
LDAP 클라이언트 인증서 생성 643
인스턴스에 인증서 업로드 645
필드 암호화 646
필드 암호화 탐색 648
필드 암호화 구성 650
필드 암호화 사용 671
필드 암호화 엔터프라이즈 697
클라우드 암호화 키 관리 포함 701
키 관리 운영 702
Quorum 통제 정책 709
키 관리 트랜잭션 713
클라우드 암호화 로깅 715
변조 탐지 717
전체 디스크 암호화 720
에지 암호화 규칙 720
에지 암호화 규칙 탐색 722
에지 암호화 규칙 계획 733
에지 암호화 규칙 설치 741
에지 암호화 규칙 업그레이드 787
에지 암호화 규칙 구성 794
데이터베이스 암호화 847
데이터베이스 암호화 탐색 848
데이터베이스 키 회전 요청 849
고객 통제 스위치를 사용한 데이터베이스 암호화 850
접근 관리 852
제로 트러스트 액세스 853
제로 트러스트 액세스 탐색 854
제로 트러스트 액세스 활성화 856
세션 액세스 역할 구성 856
제로 트러스트 액세스 시스템 속성 858

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자습서: 제로 트러스트 액세스 사용 860
모바일용 제로 트러스트 액세스 864
연속 인증 866
서비스 제공자용 도메인 분리 893
도메인 분리 탐색 895
도메인 분리를 위한 애플리케이션 지원 911
서비스 제공자를 위한 도메인 분리 권장 방법 919
도메인 분리 도움말 956
도메인 분리 설정 및 관리 957
도메인 분리 센터 988
인증 994
적응형 인증 997
API 인증 1049
API 접근 정책 1060
인증서 기반 인증 1083
인스턴스에 Custom URL 연결 1090
설치 종료 1097
IP 범위 기반 인증 1100
LDAP 통합 1102
동시 세션 제한 1160
로컬 인증 1164
다단계 인증(MFA) 1188
다중 제공자 1회 사용자 인증(SSO) 1252
OAuth 인바운드 및 아웃바운드 인증 1330
인스턴스에 자체 등록 ServiceNow 1366
토큰 기반 인증(사용자 로그인) 1376
웹 서비스 보안 1389
접근 제어 목록 규칙 1394
접근 제어 목록 탐색 1395
ACL 규칙 구성 1411
상황별 보안 관리자 1416
고급 ACL 구성 1421
보안 속성 1432
보안 속성 기본 1433
보안 속성 생성 1433
보안 속성 범위 1436
필드 쿼리 역할 및 제한 사항 1436
필드 쿼리 역할 구성 1437
필드 쿼리 제한 구성 1437
데이터 필터링(레거시) 1438
데이터 필터링 탐색 1439
데이터 필터링 활성화 1441

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 필터링 규칙 생성 1441
제목 기준 생성 1444
데이터 필터링 디버깅 1447
데이터 필터 베스트 프랙티스 1448
보안 데이터 필터 1448
보안 데이터 필터 생성 1451
기본 보안 필터 1452
보안 역할 1453
명시적 역할 1454
상승된 권한 역할 1461
연결 및 자격 증명 1463
자격 증명, 연결 및 별칭 탐색 1465
연결 시작하기 1479
자격 증명으로 시작 1489
인증 알고리즘 1565
ServiceNow® 접근 제어 1575
접근 제어 살펴보기 ServiceNow® 1577
접근 통제 활성화 ServiceNow® 1579
접근 제어 구성 ServiceNow® 1581
감사 로깅 1582
신원 1583
액세스 분석기 1584
액세스 분석기 살펴보기 1585
액세스 분석기 사용 1586
권한 평가 1605
자주 묻는 질문 1606
액세스 시뮬레이터 1611
액세스 인사이트 1625
전역 ID 1629
페더레이션 ID 탐색 1630
페더레이션 ID 기준 액세스 1631
ID 필드 업데이트 1632
ID 센터 1633
ID 센터 탐색 1635
ID 센터 활성화 1635
사용자를 위한 ID 센터 1635
관리자용 ID 메트릭 1638
SCIM(교차 도메인 ID 관리 시스템) 1638
SCIM 제공자 1639
SCIM 클라이언트 1657
ID 및 액세스 감사 1674

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

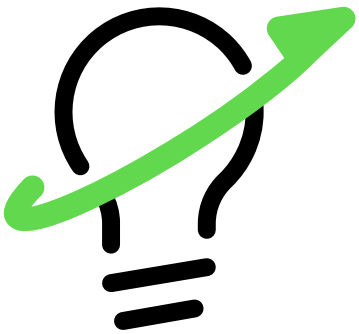
ID 및 액세스 감사 탐색 1675
ID 감사 결과 1676
보안 감사 가능 필드 1680
ID 액세스 및 감사에 대해 지원되는 필드와 지원되지 않는 필드 1683
접근 관찰자 1685
접근 관찰 구성 1685
접근 관찰자 로그 검토 1686
플랫폼 보안 제품 및 솔루션에 대한 추가 자원 1688

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스 보호

플랫폼 보안은 인스턴스를 보호하는 기능을 제공합니다.

ServiceNow Vault



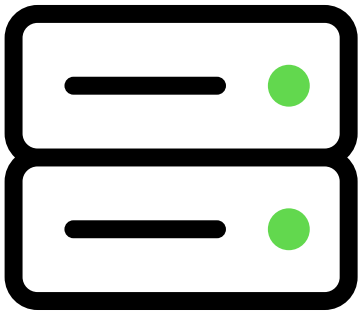
전체 수명주기 동안 무단 액세스, 손상 또는 도난으로부터 중요한 정보를 보호하는 ServiceNow Vault 제품 데이터 보안 도구 세트를 사용합니다.

플랫폼 보안



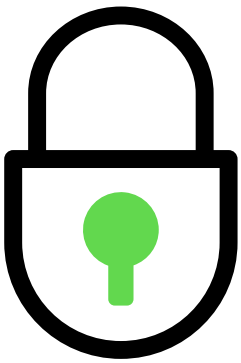
플랫폼 보안은 인스턴스를 보호하는 기능을 제공합니다.

플랫폼 개인정보 보호



플랫폼 개인정보 보호를 사용하면 인스턴스의 민감한 날짜를 마스킹할 수 있습니다.

암호화



민감한 데이터를 보호하고 규제 요구사항 및 표준을 준수하십시오.

접근 관리



액세스 관리를 사용하면 ServiceNow 인스턴스에 안전하게 액세스할 수 있습니다.

신원



인스턴스의 ID에 대해 자세히 알아봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플랫폼 보안 제품 및
솔루션에 대한 추가 자원



학습을 위한 추가 플랫폼
보안 자원을 살펴봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow Vault

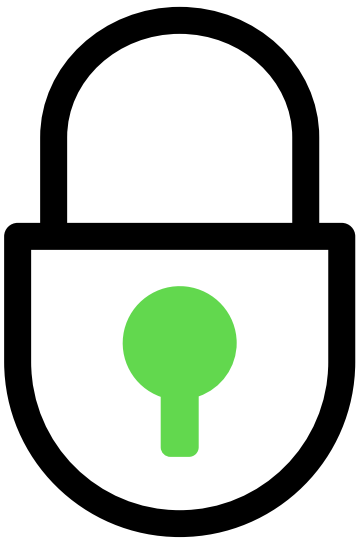
전체 수명주기 동안 무단 액세스, 손상 또는 도난으로부터 중요한 정보를 보호하는 데이터 보안 도구 세트인 ServiceNow 볼트 제품을 사용합니다. 중요한 정보의 수정과 감사를 위해 암호화, 비밀 관리 및 데이터 개인정보 보호와 같은 보호를 적용합니다. ServiceNow 볼트 홈페이지를 통해 한 곳에서 시각적으로 ServiceNow 볼트 데이터 보안 제품을 찾고 탐색할 수 있습니다.

ServiceNow 볼트 는 프로덕션 인스턴스에서 담당자가 활성화해야 하는 ServiceNow 유료 플러그인입니다. ServiceNow 볼트 여기에는 여기에 나열된 구성요소가 포함됩니다.

구독을 구매하려면 ServiceNow 계정 관리자에게 문의하십시오. 구독을 구매하면 특정 플러그인이 자동으로 활성화됩니다. 유료 플러그인이 자동으로 활성화되지 않은 경우, 인스턴스의 모든 애플리케이션 목록에서 수동으로 활성화할 수 있습니다.

ServiceNow 볼트 구성요소

암호화



키 관리 및 필드 암호화는 고도로 구성 가능한 암호화 모듈 제품군입니다.

비밀 관리

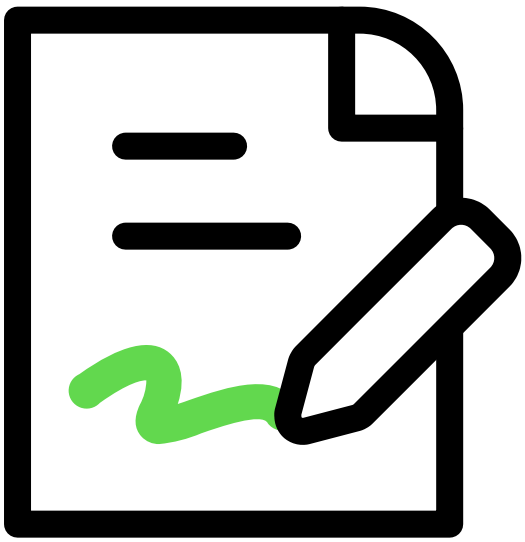


플랫폼에서 암호, 인증서 및 API 키와 같은 하드 코딩된 비밀을 비밀의 고객 관리인으로 대체하는 솔루션입니다.

기계번역

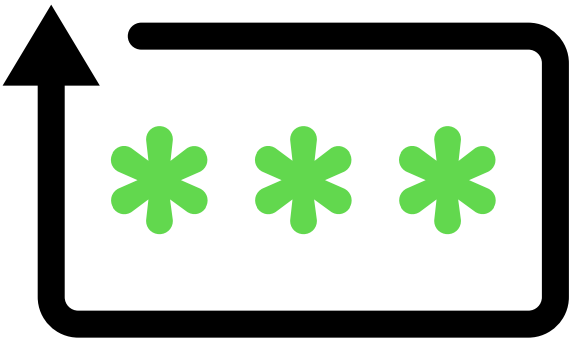
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

코드 서명



민감한 애플리케이션 구성 데이터 및 스크립트를 사용하기 전에 확인하여 보안을 강화할 수 있습니다.

데이터 개인정보 보호



프로덕션 인스턴스에서 비프로덕션 인스턴스로 마이그레이션할 때 사용자 데이터에서 PII(개인 식별 정보)를 제거하려면 데이터 개인정보 보호 플러그인을 사용합니다.

데이터 디스커버리



데이터 디스커버리 플러그인을 사용하면 사용자 데이터에서 PII(개인 식별 정보)를 찾을 수 있습니다. 그런 다음 추가 보안 조치를 위해 데이터를 분류할 수 있습니다.

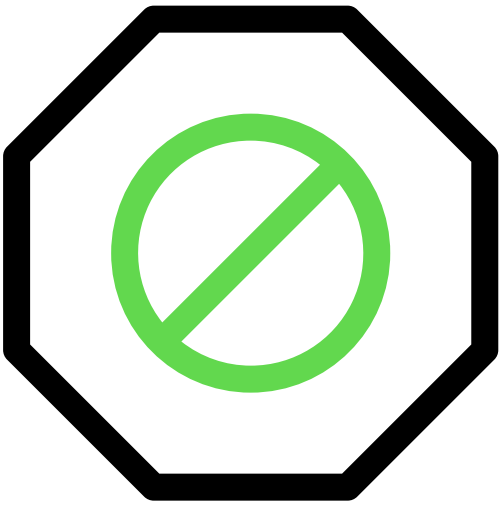
로그 항목



로그 익스포트 서비스를 사용하여 ServiceNow 로그 데이터를 엔터프라이즈 로그 분석으로 임포트 하여 보안, 성능 및 사용자 경험을 개선합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제로 트러스트 액세스



ServiceNow 세션 액세스를 사용하면 조직이 웹 세션에서 사용자 권한을 동적으로 줄일 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플랫폼 보안

플랫폼 보안은 인스턴스를 보호하는 기능을 제공합니다.

보안 센터



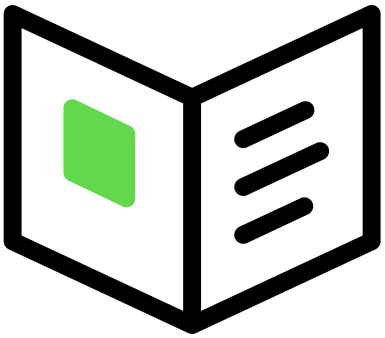
관리자가 최고 수준의 보안 태세를 지속적으로 유지하고 안전하지 않은 이벤트 및 동작을 쉽게 모니터링할 수 있습니다.

로그 익스포트 서비스



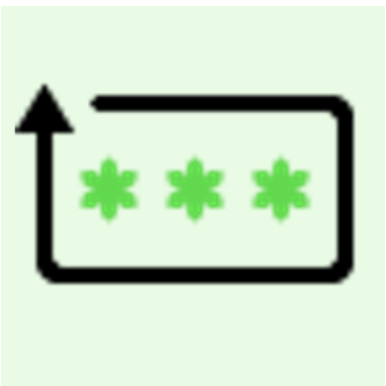
로그 익스포트 서비스(LES)를 사용하면 인스턴스 시스템 및 애플리케이션 로그를 엔터프라이즈 보안 분석 도구로 원활하게 내보낼 수 있습니다. 이 서비스는 확장성이 뛰어나고 분석 도구와의 실시간에 가까운 통합을 제공하여 설정 및 유지 관리가 쉽습니다.

로그 항목



로그 모듈은 인스턴스 내에서 발생하는 트랜잭션 및 이벤트 문제를 해결하고 디버그하는 데 사용할 수 있는 다양한 로그를 제공합니다.

비밀 관리



Secrets Management를 사용하여 ServiceNow 비즈니스 요구에 맞게 암호에 대한 액세스를 세부적으로 관리할 수 있습니다.

코드 서명



코드 서명은 나중에 데이터의 진위 및 무결성을 확인하기 위해 확인된 데이터에 대한 디지털 서명을 생성합니다.

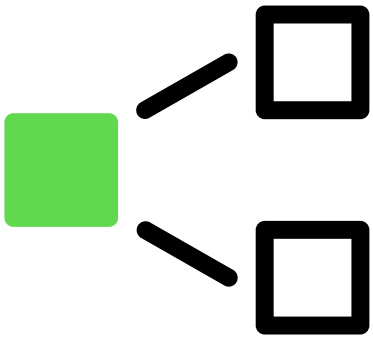
바이러스 백신 검사 역량



인시던트, 문제, 스토리와 같은 시스템 기록에 파일 첨부 파일로 인해 발생할 수 있는 바이러스 감염으로부터 인스턴스를 보호하는 데 사용합니다 바이러스 백신 검사 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

HTML 위생 검사



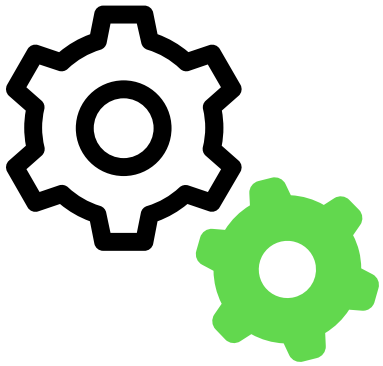
HTML 필드와 번역된 HTML 필드에서 HTML 마크업을 삭제하여 불필요한 코드를 제거하고 교차 사이트 스크립팅 공격과 같은 보안 문제로부터 보호합니다.

감사



감사 지원 테이블에서 기록 변경 내용을 추적합니다. 기본적으로 이 시스템은 인시던트, 변경 및 문제 테이블에 대한 변경 내용을 추적합니다.

높은 보안 설정



높은 보안 설정은 인스턴스에서 사용할 수 있는 여러 보안 옵션을 참조합니다.

VPN(가상 사설망)



VPN(가상 사설망)을 사용하여 인터넷을 통해 인스턴스를 외부 데이터 소스와 통합합니다.

강화 설정

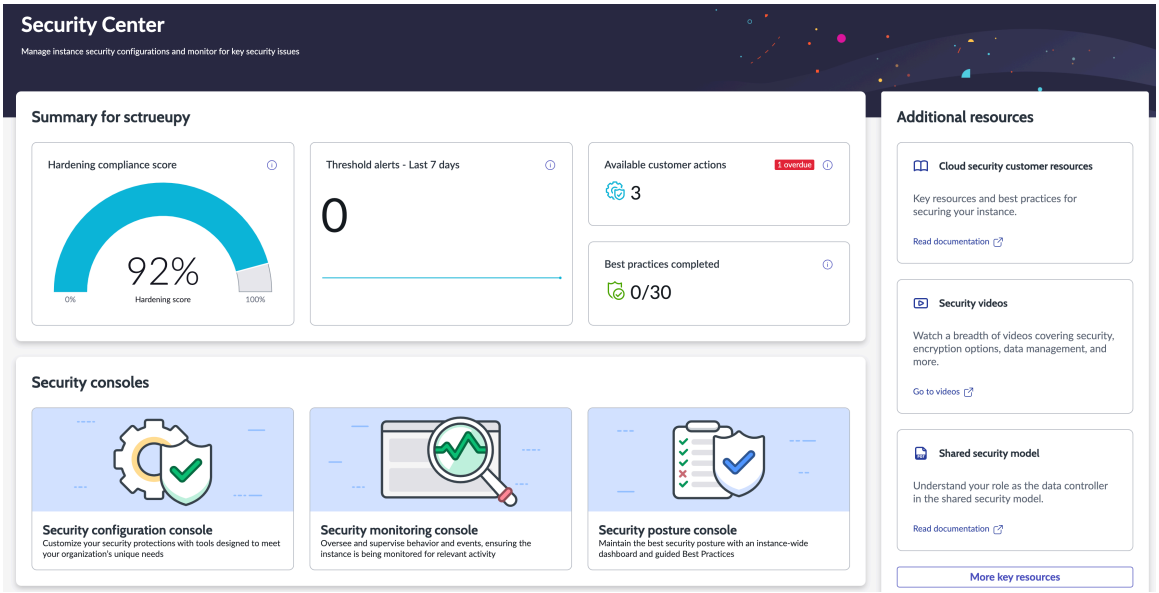


Security Center(SSC) 강화 설정 콘텐츠에 대한 자세한 설명 및 규정 준수 값 찾기

보안 센터

ServiceNow는 조직에서 ServiceNow 배포 시 보안을 유지관리하는 데 도움이 되도록 설계된 도구 세트로 구성된 애플리케이션입니다. Security Center를 사용하면 원활한 사용자 환경을 통해 보안 태세를 개선하고 규정 준수 수준을 강화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



Security Center는 관리자가 ServiceNow Store에서 다운로드할 수 있는 무료 애플리케이션입니다. Vancouver 릴리스부터 기본적으로 설치됩니다. 또한 새로운 기능을 더욱 빠르게 도입할 수 있도록 분기마다 제품군 릴리스 사이에 ServiceNow Store에 제공됩니다.

중요사항:

인스턴스 보안 센터(ISC)는 2024년 9월 현재 판매가 종료되었으며 더 이상 지원되지 않거나 활성화할 수 없습니다.

SSC(보안 센터)는 앞으로 권장되는 솔루션입니다. 자세한 내용은 마이그레이션으로 ServiceNow 보안 센터 인스턴스 보안 센터 문서를 참조하십시오.

시작

보안 센터 방문



보안 센터 방문 페이지를 사용하여 인스턴스를 보호하는 데 필요한 정보와 도구를 찾습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 구성 콘솔



보안 구성 콘솔을 사용하여 개요 페이지에서 인스턴스의 보안 태세에 대한 간략한 개요를 확인합니다.

보안 모니터링 콘솔



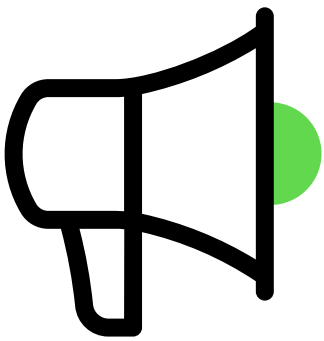
보안 알림 및 메트릭을 감독하여 인스턴스에 대한 잠재적인 보안 위험에 대한 정보를 지속적으로 받습니다.

보안 태세 콘솔



포괄적인 가시성과 단계별 지침으로 보안 태세를 개선합니다.

보안 배너 공지



보안 알림 및 메트릭을 감독하여 인스턴스에 대한 잠재적인 보안 위험에 대한 정보를 지속적으로 받습니다.

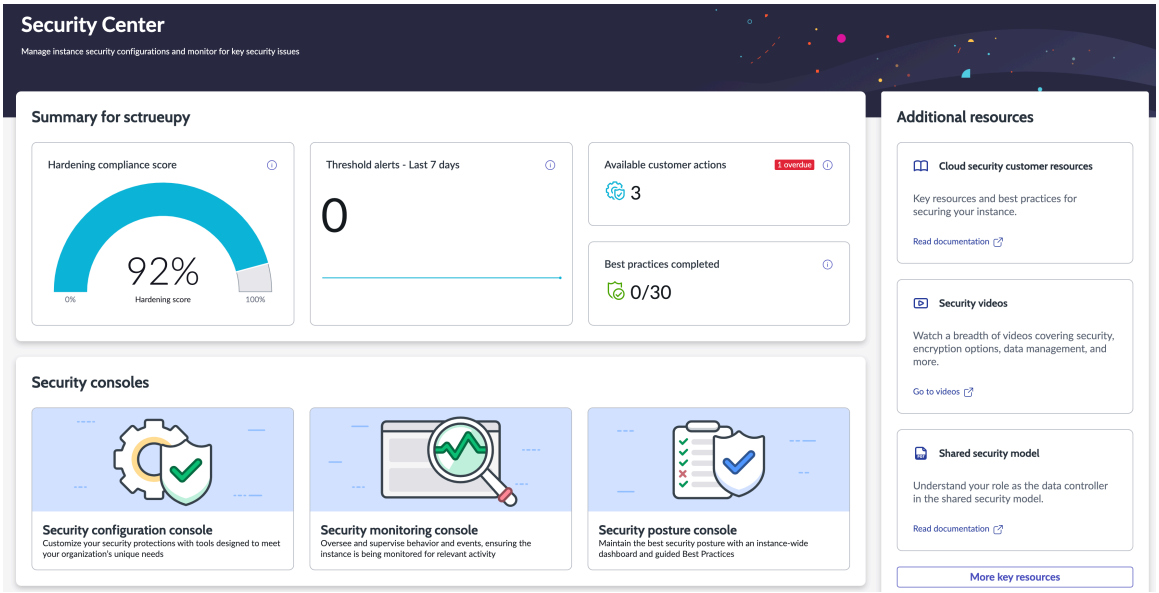
문제 해결 및 도움 받기

- 질문하고 다음에 대한 다른 자원을 살펴보십시오. 보안 센터 보안 운영 섹션의 ServiceNow 커뮤니티 .
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

보안 센터 방문

보안 센터 방문 페이지를 사용하여 인스턴스를 보호하는 데 필요한 정보와 도구를 찾습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



인스턴스 요약

인스턴스 요약은 인스턴스의 보안 상태에 대한 개략적인 개요를 표시합니다. 카드에서 정보(ⓘ) 아이콘을 선택하면 각 카드가 무엇을 나타내는지에 대한 자세한 내용을 볼 수 있습니다. 카드를 선택하여 Security Center의 관련 영역으로 이동할 수도 있습니다.

보안 콘솔

보안 콘솔 섹션 내에서 카드를 선택하여 세 가지 보안 콘솔 중 하나로 이동합니다.

- 보안 구성 콘솔
- 보안 모니터링 콘솔
- 보안 태세 콘솔

도구

도구 섹션을 사용하여 인스턴스 보안을 관리하는 데 필요한 도구로 이동합니다. 이러한 도구는 섹션 상단에 표시되는 세 개의 탭으로 구성됩니다. 카드를 선택하여 선택한 도구로 이동합니다.

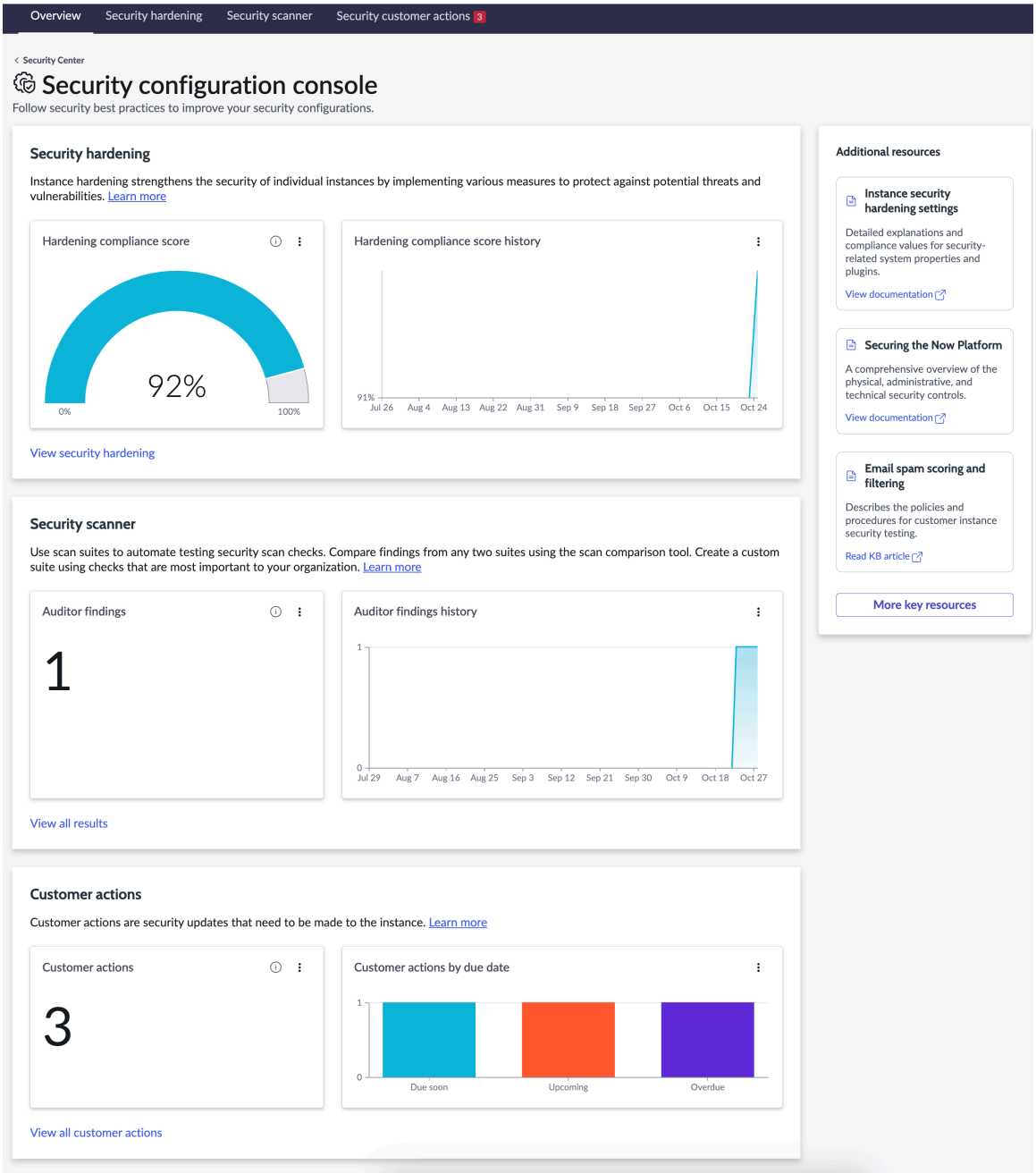
추가 자원

화면 가장자리의 추가 자원 섹션을 사용하여 학습 보안 센터와 관련된 설명서 및 비디오와 인스턴스 보안 관리에 대한 정보로 이동합니다.

보안 구성 콘솔

보안 구성 페이지를 사용하여 인스턴스의 보안 태세에 대한 개요를 확인합니다. 강화 준수 점수를 보고, 그래픽 추세를 검색하고, 상위 미준수 강화 설정을 분석하고, 보안 검사 결과를 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



탐색 모음

페이지 맨 위에 있는 막대를 사용하여 이 페이지와 Security Center의 보안 강화, 보안 스캐너 또는 보안 고객 작업 섹션 사이를 이동합니다.

보안 강화

보안 강화 섹션에서 규정 준수 강화에 대한 자세한 내용을 확인하십시오. 이 섹션에서 카드를 선택하여 페이지로 이동합니다 보안 강화 .

강화 준수 점수는 보안 설정이 권장 설정과 얼마나 밀접하게 일치하는지를 보여 주는 백분율입니다. 보안 강화 섹션에는 이 백분율과 함께 시간의 경과에 따른 인스턴스 점수 기록이 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 스캐너

보안 스캐너 섹션을 사용하여 자동화된 보안 스캔 검사 결과를 검토합니다. 이러한 검사는 보안 취약성, 비효율성 및 규정 준수 문제를 찾는 데 도움이 됩니다.

이 섹션에 있는 카드를 선택하여 보안 스캐너 페이지로 이동합니다.

고객 작업

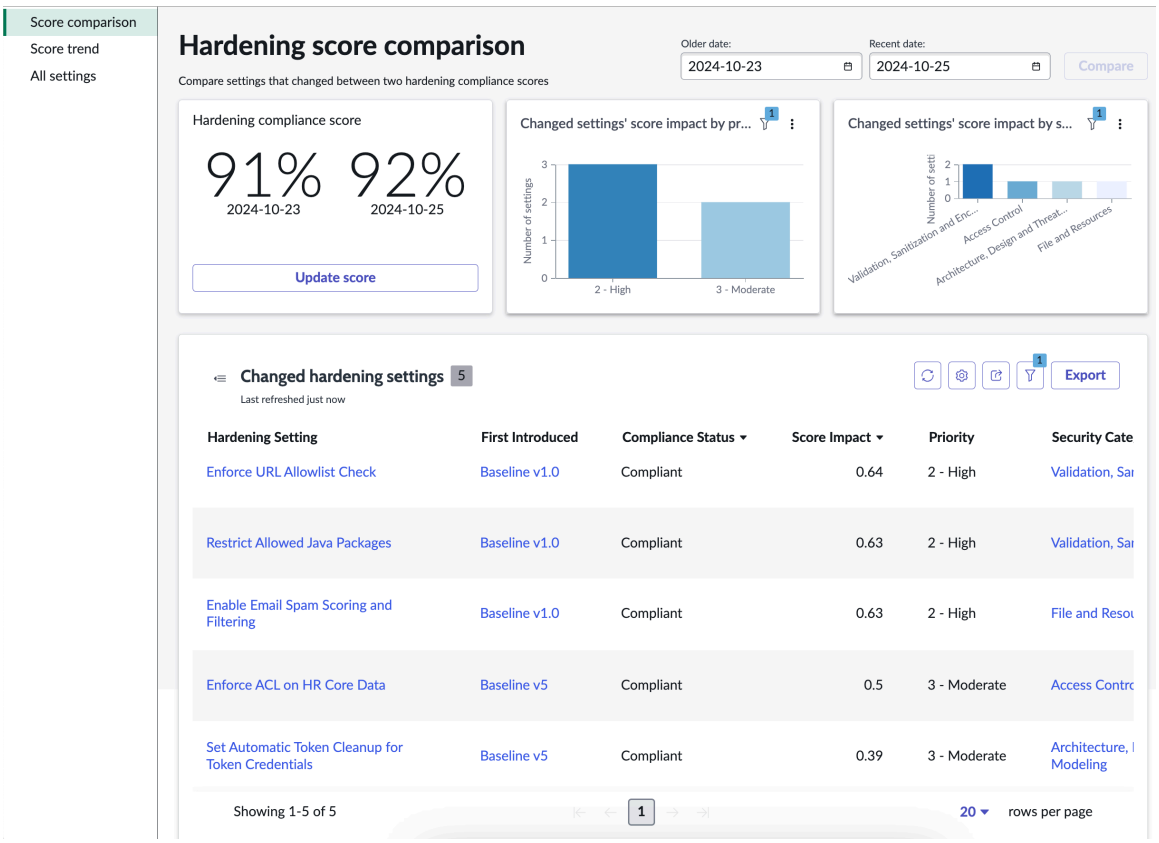
고객 작업 섹션에서 인스턴스에 적용할 수 있는 보안 업데이트를 찾아보십시오. 이 섹션에는 사용 가능한 작업 수와 이러한 작업의 기한을 나타내는 차트가 표시됩니다. 이 섹션의 카드를 선택하여 고객 작업 페이지로 이동합니다.

추가 자원

화면 가장자리의 추가 자원 섹션을 사용하여 학습 보안 센터와 관련된 설명서 및 비디오와 인스턴스 보안 관리에 대한 정보로 이동합니다.

보안 강화

보안 강화 페이지에서 강화 준수 점수를 보고, 이전 점수와 비교하고, 설정을 변경하여 준수 점수와 보안 태세를 개선합니다.



강화 설정 Now Platform의 보안 관련 속성 및 플러그인에 권장되는 값을 지정합니다. 강화 도구는 강화 설정 준수 점수를 백분율로 계산합니다. 이 숫자는 인스턴스가 보안 센터 강화 설정을 얼마나 준수하는지를 나타냅니다.

강화 준수 점수를 계산하는 수식은 다음과 같습니다.

- 각 강화 설정의 위험 점수는 0-10 사이입니다. 모든 설정 섹션에서 개별 설정 값을 볼 수 있습니다.
- 점수는 모든 규정 준수 위험 점수의 합계를 모든 위험 점수의 합계로 나눈 값과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어, 모든 규정 준수 위험 점수의 합계는 25.4이고 모든 위험 점수의 합계는 34.9입니다. 이 합계에 대한 규정 준수 점수는 (25.4 /34.9) × 100으로 72.7과 같습니다. 이 소수는 가장 가까운 정수로 반올림되므로 73이 됩니다.

이 계산은 매월 1일 또는 Security Center를 ServiceNow 설치하거나 다시 설치한 후에 자동으로 수행됩니다. 이 페이지의 점수 업데이트 버튼을 사용하여 언제든지 재계산을 트리거할 수 있습니다.

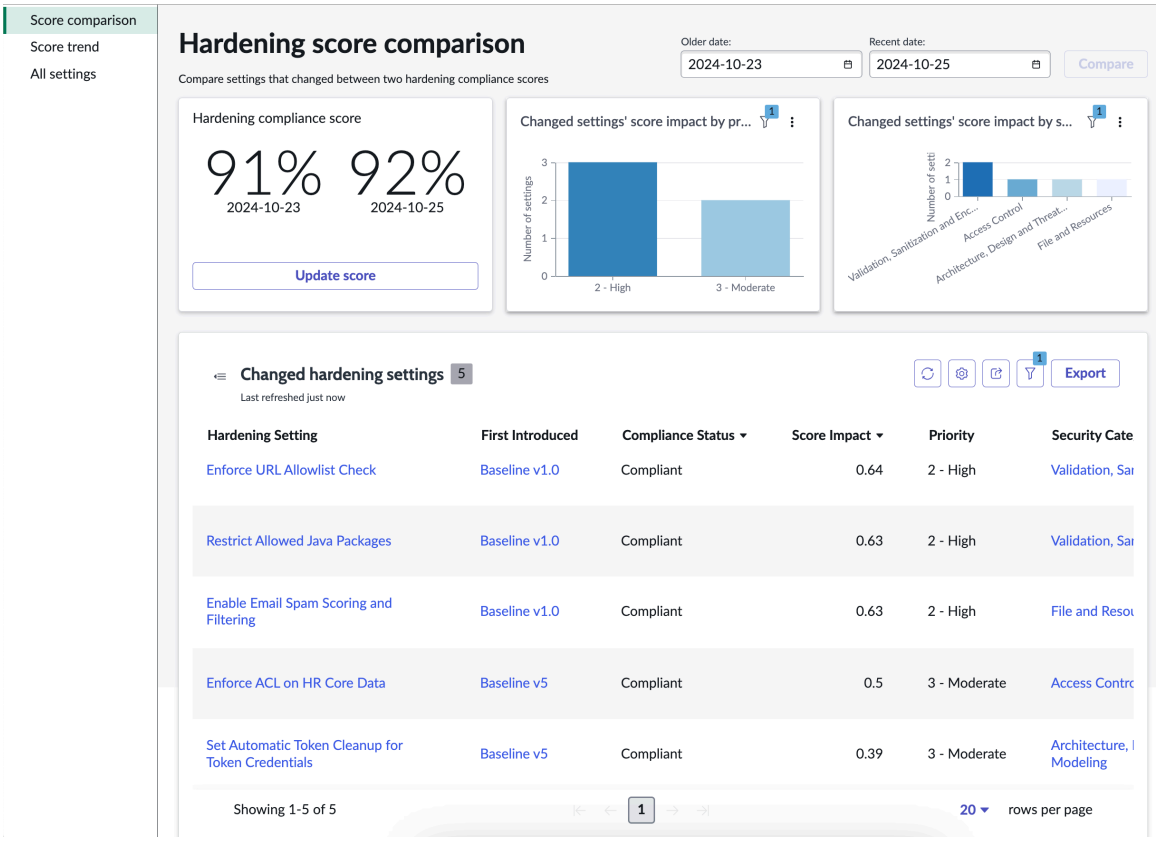
보안 강화 하위 섹션

보안 강화 섹션에는 화면 왼쪽 가장자리에서 선택할 수 있는 세 개의 하위 섹션이 있습니다.

- 강화 점수 비교
- 강화 준수 점수 추세
- 모든 설정

강화 점수 비교

강화 설정의 상태에 대한 가시성을 확보하고 이 데이터를 사용하여 인스턴스의 보안 태세를 개선합니다.



이 페이지에는 강화 준수에 대한 요약과 이 점수에 영향을 미치는 인스턴스에 대한 변경 내용이 표시됩니다.

강화 점수 비교 페이지에는 이전 날짜 와 최근 날짜 필드에서 선택한 날짜 간의 준수 상태가 변경된 강화 설정이 표시됩니다. 이 정보를 사용하여 강화 준수 점수에 어떤 영향을 미쳤는지 확인할 수 있습니다.

강화 준수 점수

카드는 선택한 날짜에 인스턴스의 준수 점수를 백분율로 비교합니다.

우선순위별 변경된 설정의 점수 영향

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

마지막 점수 업데이트 이후 준수 상태를 변경한 강화 설정 수를 우선순위 값별로 구성하여 표시합니다.

보안 영역별 변경된 설정의 점수 영향

선택한 두 날짜 사이에 준수 상태를 변경한 강화 설정 수를 보안 영역별로 구성하여 표시합니다.

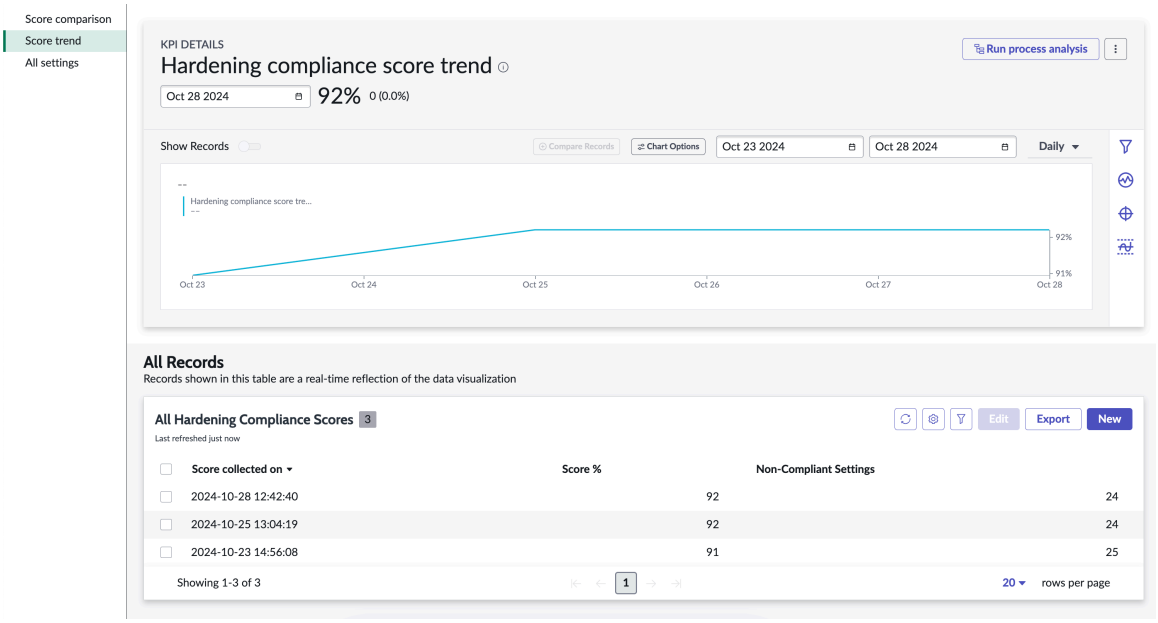
변경된 강화 설정

선택한 날짜 사이에 준수 상태를 변경한 강화 설정 목록을 표시합니다. 미준수가 되고 강화 비교 점수가 감소한 설정을 검토하여 점수를 높일 수 있는 기회를 확인합니다. 강화 준수 점수 증가 문서를 참조하십시오.

강화 준수 점수 추세

차트나 표에서 시간 경과에 따른 강화 준수 점수의 추세를 봅니다.

시간 경과에 따른 준수 점수의 추세를 확인합니다. 날짜 선택기를 사용하여 분석할 시간 범위를 선택하고 대상, 임계치 및 KPI와 같은 퍼포먼스 분석 기능을 적용하여 데이터에 대한 통찰력을 얻습니다.



규정 준수 점수 차트

차트 옵션 단추를 사용하여 분석할 정보와 정보를 표시하는 방법을 지정합니다.

분석

옵션 목록에서 선택합니다. 선택한 차트 유형에 따라 일부 옵션을 사용하지 못할 수 있습니다.

대상

조직에서 달성하고자 하는 목표입니다. 퍼포먼스 분석 대상 문서를 참조하십시오.

임계치

표시기에 대한 점수의 정상 범위를 정의하고 특정 이벤트가 발생할 때 사용자에게 경고합니다. 퍼포먼스 분석 임계값 문서를 참조하십시오.

예측

과거 동작을 기반으로 미래 점수를 예측하는 기능을 설명합니다. 퍼포먼스 분석 점수 예측 문서를 참조하십시오.

추세

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하나 이상의 항목 값이 시간이 지남에 따라 어떻게 변하는지 보여줍니다.

설명

개별 데이터 포인트에 대한 주석을 표시합니다.

레이블

시각화와 관련된 점수를 표시합니다.

통계

준수 점수와 관련된 통계를 표시합니다.

시계열

차트에 표시할 메트릭을 선택합니다.

점수

핵심성과지표(KPI)의 점수입니다.

변경

이 표시기의 점수 변경입니다.

백분율 변경

점수의 백분율로 나타낸 변경

차트 유형

차트 유형을 선택하여 선택한 정보를 시각화하는 방법을 제어합니다. 시계열 시각화 유형 사용 사례 문서를 참조하십시오.

모든 기록 테이블

모든 기록 테이블에는 준수 점수가 수집된 날짜, 점수 백분율 및 미준수 설정 수가 표시됩니다. 이 테이블을 또 다른 옵션으로 사용하여 시간 경과에 따른 인스턴스의 보안 태세를 분석할 수 있습니다.

강화 준수 점수 증가

강화 설정이 시스템의 권장 사항을 준수하도록 하여 강화 준수 점수를 높입니다.

시작하기 전에

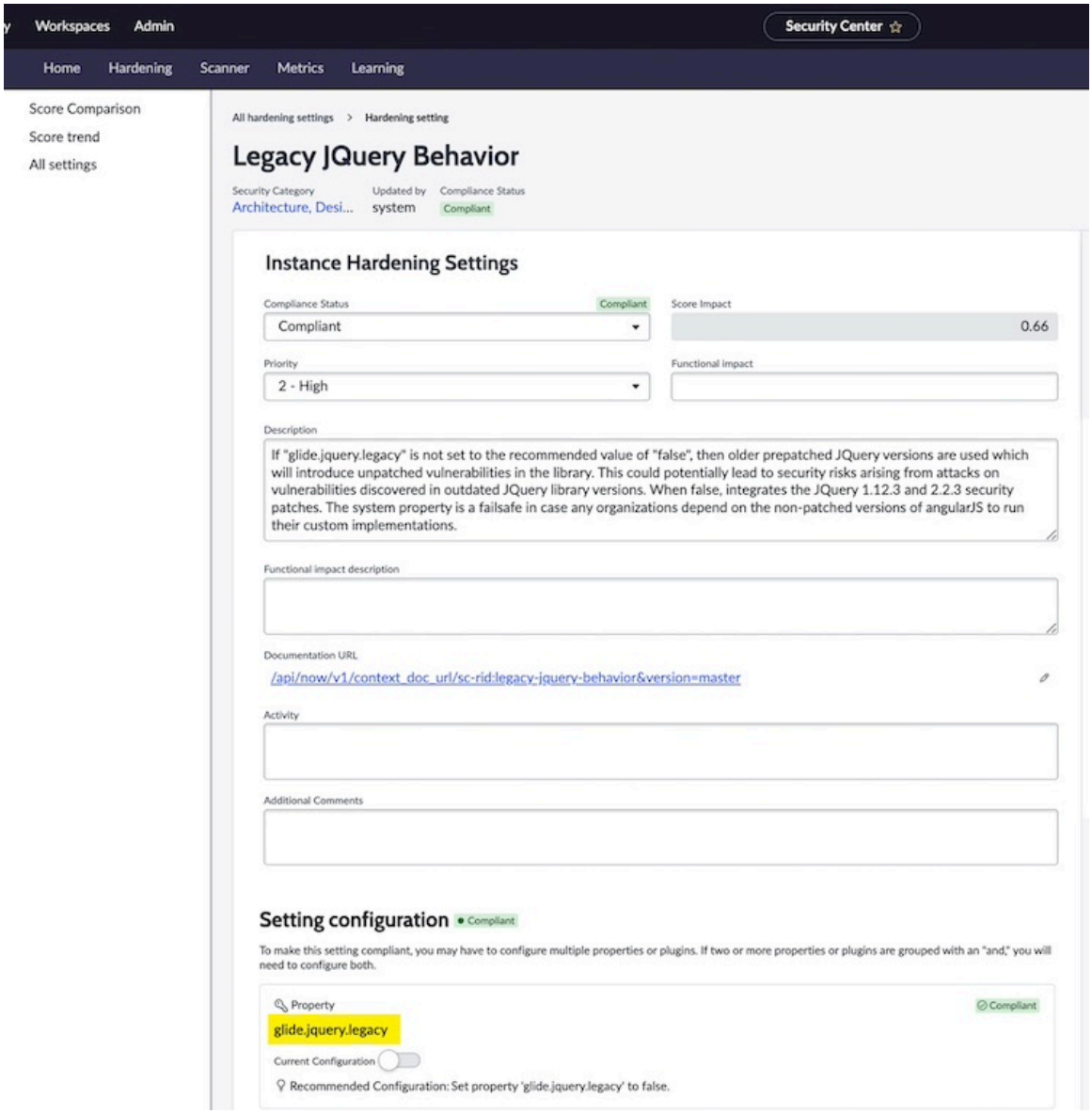
필요한 역할: 관리자

인스턴스에 점수 영향이 가장 큰 미준수 강화 설정을 식별합니다. 이를 검토하여 전반적인 준수 점수를 높일 수 있도록 시스템 권장 사항을 준수할 수 있는지 확인합니다.

프로시저

1. 다음으로 이동 강화 > 모든 설정.
2. 규정 미준수 강화 설정만 보려면 규정 준수 상태 열을 필터링합니다.
3. 점수 영향을 선택하여 가장 큰 것부터 가장 작은 것 순으로 정렬합니다.
4. 설정을 선택하고 설정 상세 정보를 검토하여 권장 사항을 준수할지 여부를 결정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 강화 설정을 준수하도록 합니다.

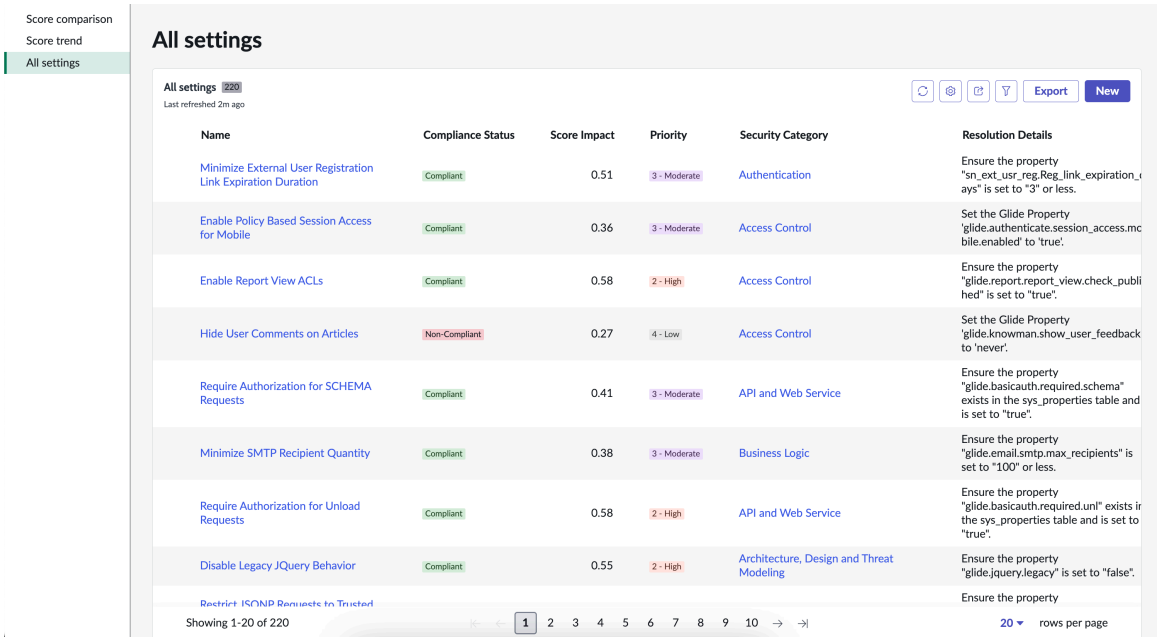
6. 규정 미준수 강화 점수를 업데이트하여 규정을 준수하도록 하는 경우 홈페이지로 이동하고 점수 업데이트를 선택하여 최신 점수를 확인합니다.
강화 점수는 반올림됩니다. 86.75%의 점수는 최대 87점으로 반올림됩니다.

모든 설정

단일 페이지에서 사용 가능한 모든 인스턴스 강화 설정을 검토합니다.

모든 설정 페이지에는 모든 인스턴스 강화 설정에 대한 정보가 표시됩니다. 오른쪽 위에 있는 버튼을 사용하여 이 정보를 새로 고치고, 필터링하고, 익스포트합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



강화 설정에 대한 다음 정보는 목록에서 찾을 수 있습니다.

이름

강화 설정의 이름입니다.

준수 상태

설정이 시스템의 권장 사항에 따라 올바르게 구성되었는지(준수) 또는 반드시 구성되어야 하는지(미준수) 여부

점수 영향

이 강화 설정이 보안 태세에 미치는 영향(백분율로 표시)입니다. 모든 점수 영향의 합은 100%입니다.

우선순위

설정의 중요도는 중요, 높음, 보통 및 낮음입니다. 점수가 높을수록 영향과 우선순위가 더 크다는 것을 나타냅니다.

보안 범주

속성의 보안 범주입니다. 상세 정보를 보려면 범주를 선택합니다.

해결 정보

강화 설정의 보안 취약성을 정정하는 단계에 대한 설명입니다.

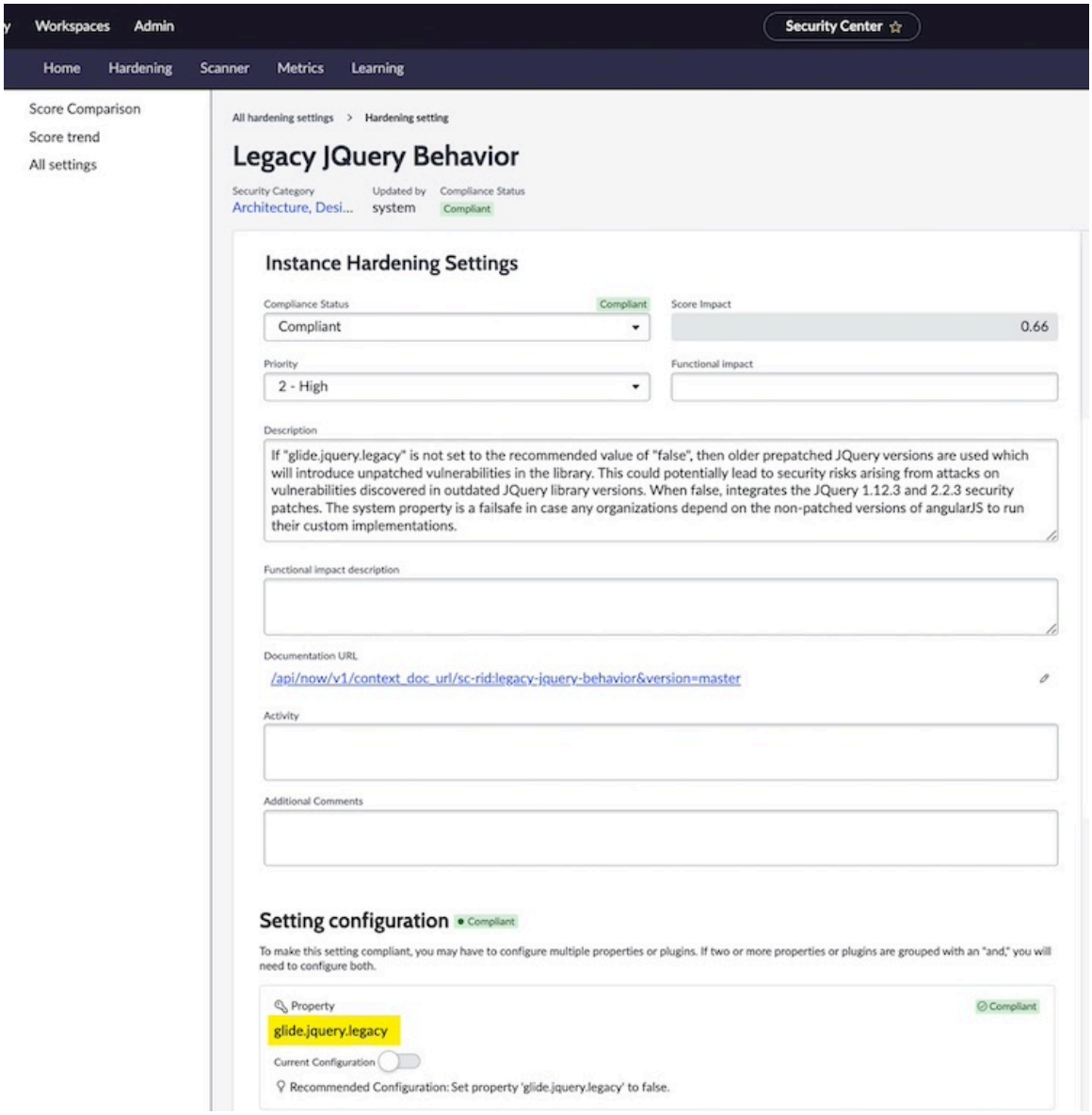
속성 강화 설정을 구성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 강화 준수 점수 증가.

강화 설정 상세 정보

Security Center 앱 내에서 해당 링크를 선택하여 강화 설정의 세부 정보를 분석합니다.

다음으로 이동 강화 > 모든 설정을 클릭한 다음 보안 관련 정보를 표시하는 강화 설정 도구 내의 페이지로 리디렉션할 강화 설정을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



강화 설정 구성 상세 정보

구성 속성	설명
준수 상태	강화 설정이 규격인지 여부를 나타냅니다.
점수 영향	이 강화 설정이 보안 태세에 미치는 영향을 나타내는 백분율입니다.
우선순위	1-4 범위 내의 숫자로, 1의 가중치는 이 강화 설정이 보안 태세에 미치는 영향의 강도를 나타냅니다.
기능적 영향	이 강화 설정이 인스턴스 운영에 미치는 영향입니다.
설명	강화 설정에 대한 일반 개요입니다.
문서 URL	강화 설정에 대한 설명서 링크입니다.
활동	강화 설정과 관련된 업데이트 알림입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

강화 설정 구성 상세 정보

구성 속성	설명
설정 구성	강화 설정의 준수 상태와 관련된 상세 정보와 규정을 준수하도록 하는 방법에 대한 지침입니다. 주: 일부 강화 설정의 경우 규정을 준수하도록 여러 속성과 플러그인을 구성해야 할 수 있습니다.

필터 강화 설정

필터를 사용하여 강화 검토 프로세스를 단순화합니다. 이러한 필터는 검토할 강화 설정의 작업 목록을 만들 수 있으며, 나중에 사용할 수 있도록 복원되고 다른 사용자와 공유할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 보안 센터.
2. **Security** Consoles(보안 콘솔) 섹션에서 **Security configuration** console(보안 구성 콘솔)을 선택합니다.
3. 보안 강화 탭을 선택합니다.
4. 모든 설정을 선택합니다.
5. 필터 패널 표시 단추( )를 선택합니다.
6. 필터 창에서 고급 보기를 선택합니다.
7. 검토하려는 강화 설정만 표시하는 필터를 생성합니다.
8. 필터가 완료되면 필터 저장을 선택합니다.
9. 필터 이름을 입력하고 저장을 선택합니다.

주: 권한을 모든 사람 또는 특정 그룹과 공유할 그룹으로 설정하여 이 목록을 다른 사용자가 사용할 수 있도록 할 수도 있습니다. 이러한 사용자에게는 Security Center를 사용할 수 있는 권한도 있어야 합니다.

다음에 수행할 작업
필터를 저장한 후 기존 필터 사용 단추를 사용하여 고급 뷰에서 로드할 수 있습니다.

사용자 지정 인스턴스 보안 강화 제품군 생성

조직의 보안 관행에 맞게 조정된 사용자 지정 강화 설정 제품군을 생성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
인스턴스와 함께 제공되는 기본 인스턴스 보안 강화 제품군은 수정할 수 없습니다. 그러나 조직의 보안 관행에 맞게 검사를 추가, 제거 또는 편집하려는 경우 이 도구 모음을 복제할 수 있습니다. 인스턴스 보안 강화 제품군을 복사하면 이를 사용자 지정하고 기본 제품군을 기반으로 새 제품군을 만들 수 있습니다. 다음 단계에서는 기본 제품군을 복제하여 조직의 요구사항에 맞게 조정하는 방법을 보여줍니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > **Instance Scan** > 도구 모음.
2. 새로 만들기를 선택하고 선택적 설명과 함께 제품군의 이름을 입력합니다.
3. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
4. 스캔에 필요한 검사를 추가합니다.

   a. 검사 탭에서 편집을 선택합니다.

   b. 조건을 추가합니다.
   예를 들어 스캔 검사를 추가하려면 다음 필드, 연산자, 값 및 조건을 적용합니다.

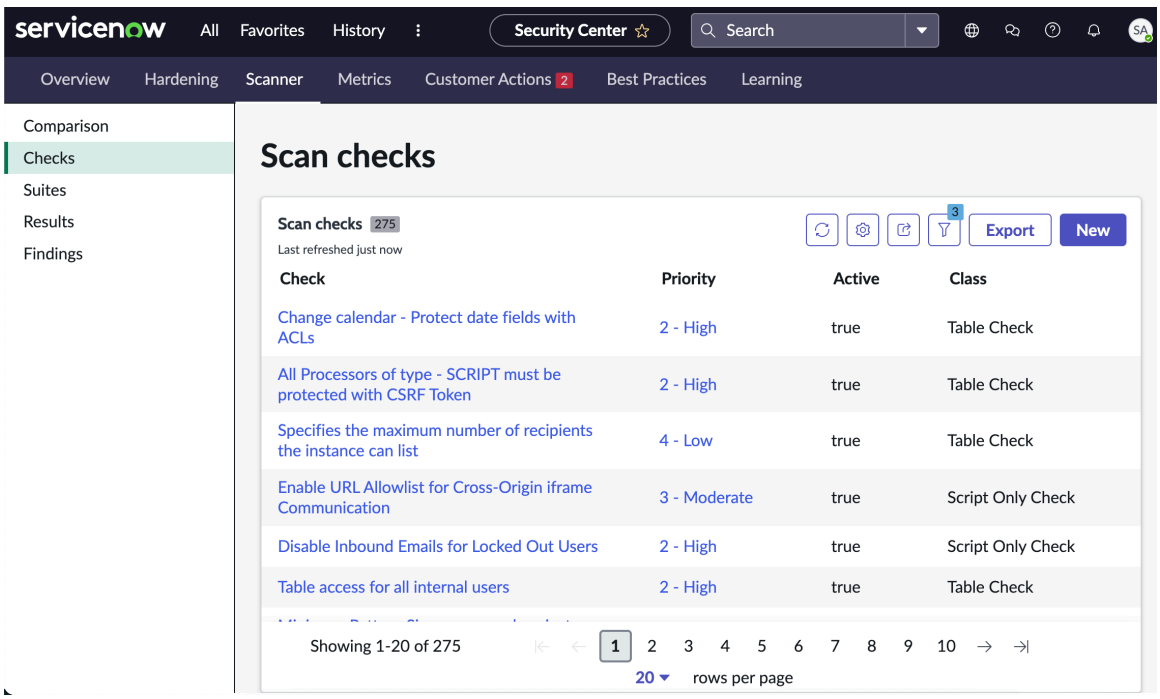
   〔카테고리〕〔는〕〔보안〕 **AND** 〔애플리케이션〕**[is]**〔전역〕

   예를 들어 다음과 같이 표시됩니다. `### #### ####### #####`.

5. 필터 실행을 선택합니다.
6. 컬렉션 목록에서 검사 목록에 추가할 검사 검사를 선택한 다음 추가(>) 단추를 선택합니다.
7. 저장을 선택합니다.
   사용자 지정 검사가 추가된 제품군이 생성되었습니다.
8. 도구 모음 스캔 실행을 선택합니다.

보안 스캐너

잘못된 구성을 식별하기 위해 일련의 보안 검사에 대해 인스턴스를 검사합니다. 스캐너 도구는 시간이 지남에 따라 결과를 분석할 수 있도록 다양한 사용 사례에 대해 서로 다른 검사 도구 모음을 만드는 프로세스를 단순화합니다.



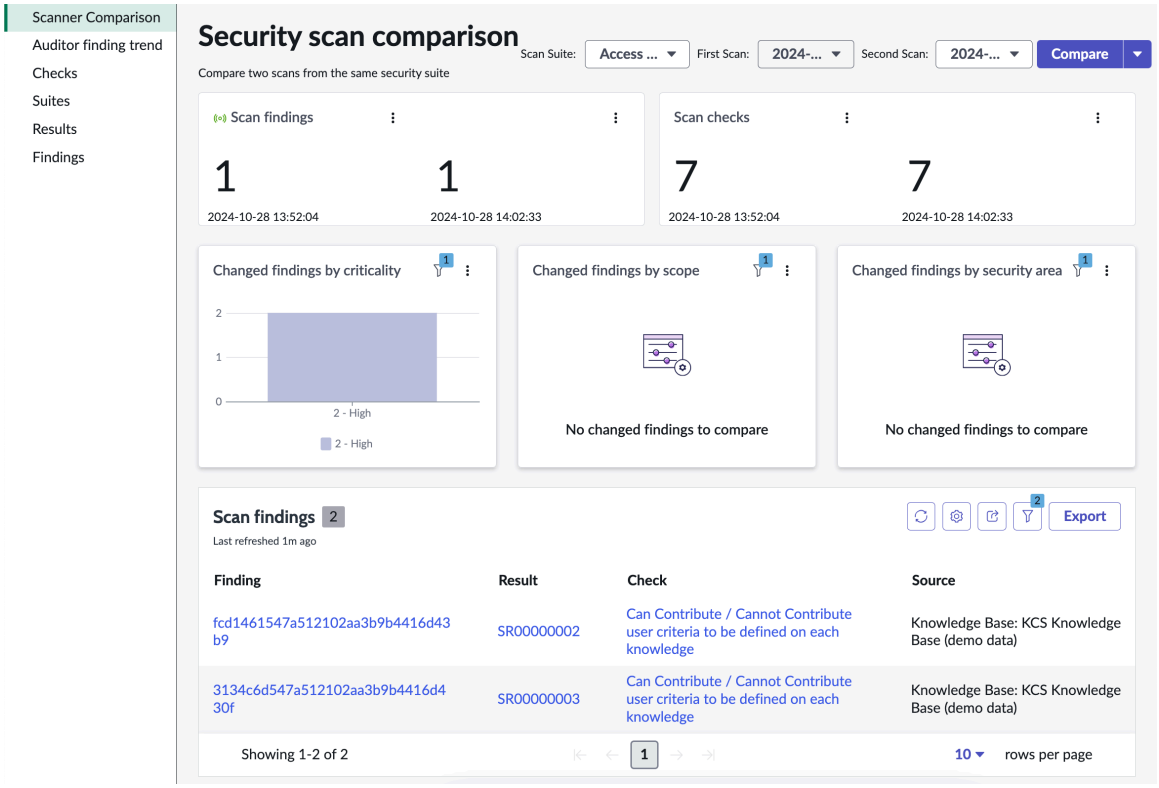
보안 검사는 인스턴스에서 보안 상태 문제를 나타내는 구성을 조사하는 방법입니다. 이를 통해 조직에 대한 보안 권장 사항을 구현할 수 있는 기회를 식별할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스캐너 도구에 액세스할 때 두 개 이상의 제품군 스캔 결과와 비교할 제품군을 선택할 때까지 비교할 수 없습니다. 기본 도구 모음 및 검사를 사용하거나 사용자 지정 검사 및 도구 모음을 직접 만들 수 있습니다.

보안 스캔 비교

동일한 보안 제품군의 두 스캔을 비교하여 강화 설정의 상태를 파악하고 인스턴스의 보안 태세를 개선합니다.



중요사항: 비교할 동일한 스캔의 인스턴스가 두 개 이상 없는 경우 이 페이지는 비어 있습니다. 이 페이지를 비교하려면 검사를 두 번 이상 실행합니다.

스캔 도구 모음 목록에서 스캔을 선택한 다음 첫 번째 스캔과 두 번째 스캔을 선택하여 비교를 시작합니다.

보안 검색 비교 페이지에는 첫 번째 검색과 두 번째 검색 사이의 강화 설정의 보안 변경 내용이 표시됩니다. 다음은 각 카드에 대한 설명입니다.

스캔 결과
: 선택한 각 날짜에 선택한 스캔의 결과 수입니다.

스캔 검사
: 선택한 각 날짜에 선택한 스캔에서 수행된 스캔 검사 수입니다.

중요도별 변경된 결과
: 중요도별로 구성된 모든 결과를 표시하는 차트입니다.

범위별 변경된 결과
: 조직화된 모든 결과를 표시하는 차트입니다.

보안 영역별 변경된 결과
: 모든 결과를 표시하는 차트, 조직된 보안 영역.

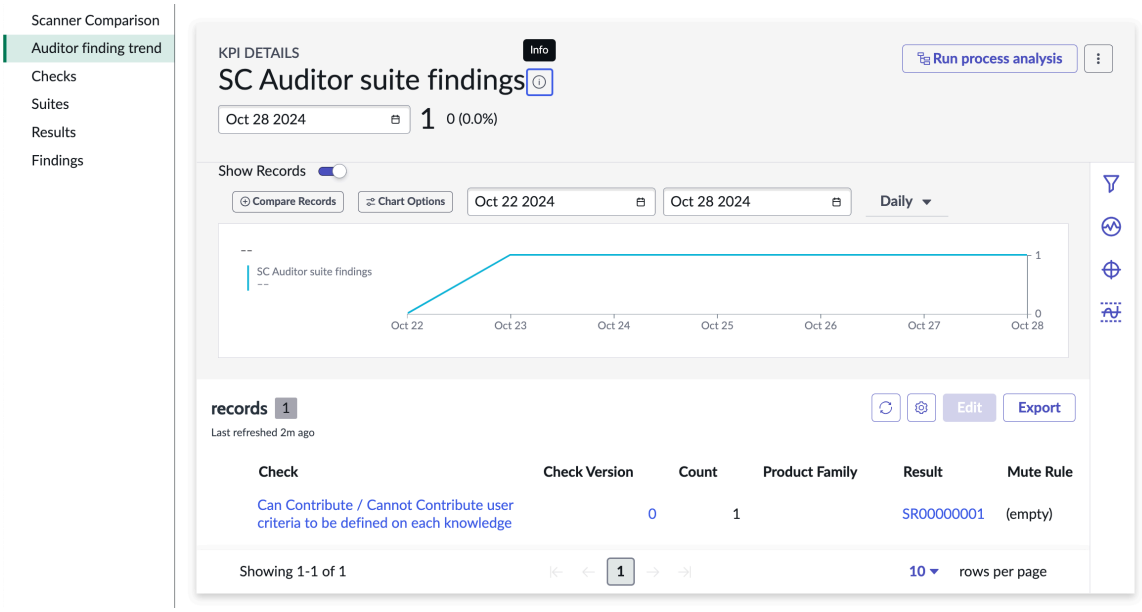
스캔 결과

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 스캔 결과의 목록입니다. 찾은 결과, 스캔 결과 또는 검사를 선택하여 관련 기록을 보고 추가 상세 정보를 찾습니다. 오른쪽 상단의 하단을 사용하여 목록을 필터링, 새로 고침 또는 익스포트할 수 있습니다.

SC 감사자 제품군 결과

시간 경과에 따른 보안 센터 감사자 제품군 결과를 검토합니다.



SC 감사자 제품군 결과 차트

이 페이지에는 선택한 두 날짜 간에 비교된 SC 감사자 제품군 결과가 표시됩니다. 차트 옵션 단추를 사용하여 분석할 정보와 정보를 표시하는 방법을 지정합니다.

분석

옵션 목록에서 선택합니다. 선택한 차트 유형에 따라 일부 옵션을 사용하지 못할 수 있습니다.

대상

조직에서 달성하고자 하는 목표입니다. 퍼포먼스 분석 대상 문서를 참조하십시오.

임계치

표시기에 대한 점수의 정상 범위를 정의하고 특정 이벤트가 발생할 때 사용자에게 경고합니다. 퍼포먼스 분석 임계값 문서를 참조하십시오.

예측

과거 동작을 기반으로 미래 점수를 예측하는 기능을 설명합니다. 퍼포먼스 분석 점수 예측 문서를 참조하십시오.

추세

하나 이상의 항목 값이 시간이 지남에 따라 어떻게 변하는지 보여줍니다.

설명

개별 데이터 포인트에 대한 주석을 표시합니다.

레이블

시각화와 관련된 점수를 표시합니다.

통계

준수 점수와 관련된 통계를 표시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시계열

차트에 표시할 메트릭을 선택합니다.

점수

핵심성과지표(KPI)의 점수입니다.

변경

이 표시기의 점수 변경입니다.

백분율 변경

점수의 백분율로 나타낸 변경

차트 유형

차트 유형을 선택하여 선택한 정보를 시각화하는 방법을 제어합니다. 시계열 시각화 유형 사용 사례 문서를 참조하십시오.

기록 목록

제품군의 일부로 수행된 검사를 나열합니다.

스캔 검사

검사를 사용하여 테이블, 기록 또는 메타데이터에 대해 실행되는 인스턴스 내의 예외를 탐지합니다.

검사는 인스턴스 내의 예외를 탐지하기 위해 설계된 규칙입니다. 목록에서 검사를 선택하여 검사 평가 대상과 검사 결과가 반환될 경우 문제를 해결할 수 있는 단계를 포함한 상세 정보를 봅니다.

검사는 문제를 식별하고 조직에 대한 보안 권장 사항을 구현하기 위해 테이블 검사, 열 유형 검사, 스크립트 전용 검사 및 린터 검사의 네 가지 클래스로 나뉩니다.

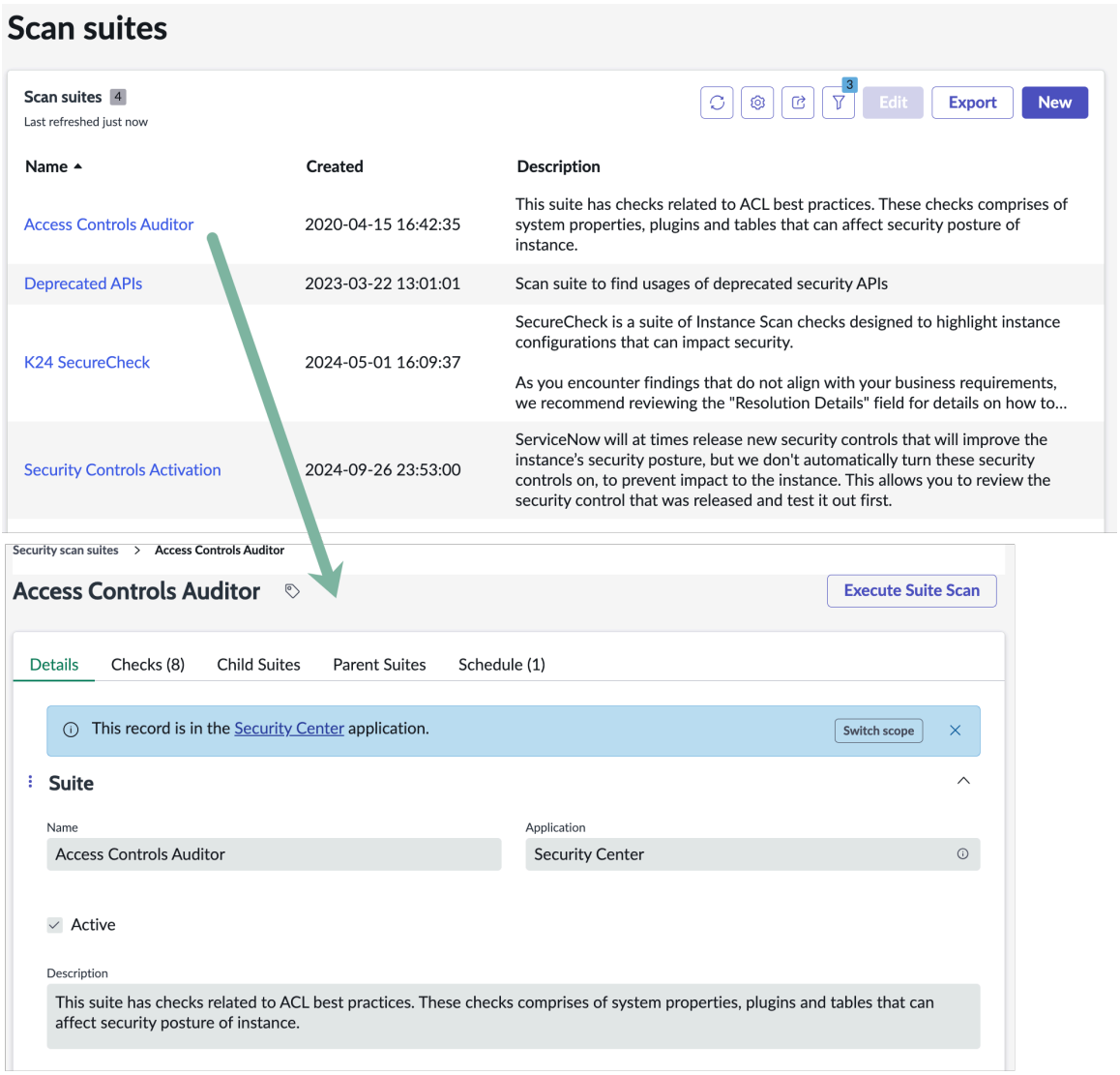
클래스 확인

클래스 확인	설명
테이블 검사	테스트하려는 특정 테이블과 검사를 알고 있는 경우 이를 사용합니다.
열 검사	이를 사용하여 대상 열 필드 유형과 일치하는 모든 기록을 반복하기 위해 생성한 규칙을 구현합니다.
스크립트 검사	이를 사용하여 메타 데이터, 구성을 확인하고 자체 검사를 작성하여 복잡한 검사를 실행합니다.
린터 검사	스크립트에서 문제를 식별하는 데 사용합니다. 레코드에 대해 린터 검사가 실행되면 코드 문제를 분석하는 데 사용할 수 있는 코드에 대한 추상 구문 트리가 생성됩니다.

스캔 도구 모음

인스턴스에서 사용할 수 있는 스캔 도구 모음에 대한 상세 정보를 검토합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



스캔 도구 모음은 함께 실행되는 보안 센터 검사의 컬렉션입니다. bcase 시스템 제품군을 사용하거나 기존 제품군을 복제하고 복제본에서 수행된 검사를 업데이트하여 직접 만들 수 있습니다. 자세한 내용은 스캔 도구 모음 생성 문서를 참조하십시오.

스캔 도구 모음 페이지에는 인스턴스에서 사용할 수 있는 스캔 도구 모음에 대한 상세 정보가 나와 있습니다. 도구 모음을 선택하여 탭 인터페이스에서 도구 모음의 상세 정보를 봅니다. 탭 페이지에서 다음 정보를 찾을 수 있습니다.

세부사항

제품군에 대한 상세 정보에는 이름, 애플리케이션 및 설명이 포함됩니다.

검사

이 도구 모음에 포함된 검사 목록입니다. 개별 검사에 대한 상세 정보는 에 있는 스캔 검사것과 동일합니다.

하위 도구 모음

이 도구 모음과 연결된 하위 도구 모음의 목록입니다. 이 도구 모음을 실행하면 모든 하위 도구 모음도 실행됩니다.

상위 도구 모음

이 제품군이 하위 제품군인 제품군 목록입니다. 상위 도구 모음을 실행하면 이 도구 모음도 실행됩니다.

일정

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 도구 모음의 예약된 실행에 대한 상세 정보입니다.

접근 제어 감사자 확인

기본 접근 제어 감사자 제품군에서 사용할 수 있는 검사, 검사가 평가하는 기준, 인스턴스의 보안을 향상하는 데 사용할 수 있는 방법에 대해 알아보십시오.

ACL(접근 제어 목록) 규칙은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 액세스를 제한합니다. 접근 제어 감사자 검사는 다음 표에 나열된 8가지 기준에 따라 인스턴스를 평가합니다. 이러한 검사의 결과를 사용하여 인스턴스의 보안을 강화합니다.

접근 제어 감사자 확인

검사 이름	검사 기준	설명
유형의 모든 프로세서 - 스크립트는 CSRF 토큰으로 보호되어야 합니다.	CSRF 토큰으로 보호되지 않는 **SCRIPT** 유형의 프로세서를 확인합니다.	**SCRIPT** 유형의 모든 프로세서는 CSRF(교차 사이트 요청 위조) 토큰으로 보호되어야 합니다. 이러한 프로세서에는 CSRF 옵션이 선택되어 있어야 하며, 인스턴스가 CSRF 토큰을 사용하지 않는 한 프로세서가 실행되지 않습니다.
기고할 수 있음/기고할 수 없음 사용자 기준은 각 지식에 대해 정의될 수 있습니다.	기고할 수 있음 또는 기고할 수 없음 사용자 기준이 정의되지 않은 지식베이스 기록을 확인합니다.	각 지식베이스에는 기고할 수 있음 또는 기고할 수 없음 사용자 기준이 정의되어야 합니다. 그렇지 않으면 모든 사용자가 참가 기준이 정의되지 않은 지식베이스에 콘텐츠를 기고할 수 있습니다.
빈 ACL	보안 속성, 역할 또는 공용 역할이 없는 ACL(접근 제어 목록) 기록을 확인합니다.	ACL을 비워 두거나 공용 역할을 사용하면 이 ACL로 보호되는 모든 콘텐츠에 대한 공개 액세스가 제공될 수 있습니다.
클라이언트 호출 가능 스크립트 포함에 대한 접근 통제	ACL로 보호되지 않는 클라이언트 호출 가능 스크립트 포함을 확인합니다.	모든 클라이언트 호출 가능 스크립트 포함은 필수 역할을 사용하는 ACL로 보호되어야 합니다.
UI 페이지의 액세스 통제	ACL로 보호되지 않는 UI 페이지가 있는지 확인합니다.	UI 페이지에 대한 액세스를 보호하는 ACL이 없으면 로그인한 모든 내부 사용자가 해당 UI 페이지에 액세스할 수 있습니다. 제한 없이 로그인한 사용자는 잠재적으로 무단 변경을 수행할 수 있습니다.
테이블의 액세스 통제	ACL이 없는 테이블 검사	테이블은 ACL로 보호해야 합니다. 테이블에 저장된 데이터에 대한 액세스는 필요한 사용자로만 제한되어야 합니다.
사용자 계정에 내부 및 외부 역할이 모두 있을 수 없습니다.	내부 및 외부 역할이 모두 할당된 사용자 기록 확인	내부 사용자 역할은 회사 내 사용자를 위한 것입니다. 외부 사용자 역할은 고객 및 파트너와 같은 외부 직원을 위한 것입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 제어 감사자 확인

검사 이름	검사 기준	설명
공개적으로 접근 가능한 지식베이스 및 문서	공개적으로 접근 가능한 지식베이스 및 지식베이스 문서를 확인합니다.	공개적으로 접근 가능한 지식베이스와 문서는 인스턴스의 모든 사용자가 볼 수 있습니다. 지식베이스와 문서를 필요로 하는 특정 청중으로 제한하여 보안을 강화합니다.

감사자 확인

SecureCheck에 감사자 제품군을 사용하여 인스턴스의 보안 태세에 영향을 줄 수 있는 잘못된 구성을 탐지합니다.

감사자 제품군은 업데이트 세트로 제공됩니다. 내에서 이 도구 모음 보안 센터을 사용할 수 있습니다. Utah 또는 이전 버전을 사용하는 경우 인스턴스에서 Security Center가 활성화되어 있는지 확인합니다.

업데이트 세트 임포트

관리자는 다음 링크를 https://support.servicenow.com/sys_attachment.do?sys_id=821e1e724732969077748d01426d4393 사용하여 support.servicenow.com 에서 업데이트 세트를 다운로드할 수 있습니다.

에 설명된 업데이트 세트 커밋 단계를 사용하여 업데이트 세트를 커밋합니다.

업데이트 세트가 커밋되면 다음 위치에서 감사자 제품군에 액세스할 수 있습니다. 모두 > 보안 센터 > 스캐너 > 도구 모음.

정보 확인

접근 제어 감사자 확인

검사 이름	설명	스캔 찾기 유형
오래된 스토어 앱 식별	인스턴스에서 활성화된 앱 중 업데이트된 버전을 사용할 수 있는지 식별합니다. 잠재적인 보안 문제에 대한 수정 사항을 포함할 수 있는 최신 버전의 스토어 애플리케이션을 실행하고 있는지 확인합니다.	권장 해결
안전하지 않은 GlideRecord 호출	최종 사용자가 직접 호출할 수 없는 스크립트 식별(예: 클라이언트 호출 가능 스크립트 포함, 위젯, 프로세서, REST 엔드포인트) 이러한 스크립트는 ACL을 준수하고 GlideRecordSecure 또는 GlideRecord를 canRead, canWrite, canCreate, canDelete와 함께 사용해야 합니다.	권장 해결
허용된 JavaScript 라이브러리 검토	특정 외부 공급업체 JavaScript 라이브러리를 허용하거나 거부하는 데 JavaScript 콘텐츠 접근 제어가 사용되는 스크립트를 식별합니다.	권장 해결

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 제어 감사자 확인

검사 이름	설명	스캔 찾기 유형
	접근을 차단하기 전에 인스턴스 사용자 지정을 검토하여 라이브러리가 사용 중이 아닌지 확인합니다. JavaScript 컨텐츠 제공자 액세스 추적 [sys_js_content_provider_access_tracking] 테이블을 검토하여 라이브러리에 액세스한 마지막 날짜를 확인할 수 있습니다. 주: Tokyo 이상에서 처음 프로비저닝된 인스턴스에서는 이 검사를 무시할 수 있습니다. 연결된 테이블의 기록에는 기본적으로 거부 규칙이 설정되어 있습니다. Tokyo 이전에 처음 프로비저닝된 인스턴스의 경우 JavaScript 접근 제어 테이블에 허용 규칙이 있을 수 있습니다.	
해당 ACL이 없는 클라이언트 호출 가능 스크립트 포함 검토	해당 ACL이 없는 클라이언트 호출 가능 스크립트 포함을 식별합니다. 이러한 스크립트는 기본 ("*") 클라이언트 호출 가능 스크립트 포함 ACL을 사용합니다. 이러한 스크립트의 경우 예상되는 사용자만 제공된 기능과 상호작용할 수 있도록 적절한 접근 기준을 정의하는 ACL을 생성합니다.	권장 해결
기록 생성자가 있고 비즈니스 규칙이 없는 사용자 지정 테이블 검토	추가 서버 쪽 확인이 없는 기록 생성자를 식별합니다. 이 검사는 기록 생성자가 있지만 연결된 비즈니스 규칙이 없는 사용자 지정 테이블을 식별합니다. 이로 인해 사용자가 예기치 않은 데이터를 관련 테이블로 제출할 수 있습니다.	권장 해결
빈 ACL 검토	스크립트, 조건, 보안 속성, 역할이 없는 ACL 기록이나 공용 역할의 ACL을 식별합니다. ACL을 비워 두거나 **public** 역할을 사용하면 이 ACL로 보호되는 모든 콘텐츠에 대한 공개 액세스가 제공됩니다.	권장 해결
HTML 위생이 비활성화된 필드 검토	HTML 위생화가 비활성 상태인 HTML 필드를 식별합니다. HTML 위생은 HTML 코드 내에서 잠재적으로 유해한 요소와 속성을 제거하거나 대체합니다. 위생이 비활성 상태인 HTML 필드를 검토하여 이 구성이 필요한지 확인합니다.	권장 해결

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 제어 감사자 확인

검사 이름	설명	스캔 찾기 유형
비활성 보안 기능 플러그인 검토	구성 가능한 추가 보안 제어를 제공하는 활성화되지 않은 플러그인을 식별합니다. 이 검사에서 생성된 결과는 정보 제공의 목적으로 제공됩니다. 식별된 플러그인 중 하나를 활성화하기 전에 플러그인이 사용 사례 또는 요구 사항을 충족하는지 확인하십시오. 식별된 사용 사례가 없는 경우 이러한 결과를 음소거할 수 있습니다.	알림
허용되는 큰 IP 주소 범위 검토	많은 수의 IP 주소를 포함하는 IP 주소 액세스 제어 범위를 식별합니다. 주: 많은 수의 가양성이 표시되는 경우 특정 비즈니스 요구 사항에 맞게 largestExpectedCIDRBlock 변수를 조정하는 것이 좋습니다. CIDR(Classless Inter-Domain Routing) 블록에는 IP 주소가 감소할수록 더 많은 양의 IP 주소가 포함됩니다. 예를 들어, CIDR 블록 크기 8은 CIDR 블록 크기 16보다 큽니다(더 많은 IP 주소 포함). 검토하고 현재 구성이 비즈니스 요구에 맞는지 확인합니다.	검토 및 결정
공개 GraphQL 스키마 검토	GraphQL API [sys_graphql_schema] 테이블에서 공용 GraphQL 스키마를 식별합니다. 이러한 스키마는 인증 없이 사용할 수 있도록 구성할 수 있습니다. 엔드포인트의 기능에 따라 인증되지 않은 사용자가 예기치 않은 작업을 수행하거나 예기치 않은 데이터와 상호 작용할 수 있습니다.	검토 및 결정
공개 지식베이스 문서 검토	지식베이스 및 지식베이스 식별인증되지 않은 사용자가 액세스할 수 있도록 구성된 문서입니다. 검토하고 현재 구성이 비즈니스 요구에 맞는지 확인합니다.	검토 및 결정
공용 REST API 엔드포인트 검토	인증 없이 사용할 수 있도록 구성된 스크립팅된 REST 자원[sys_ws_operation] 테이블에서 REST API 엔드포인트를 식별합니다.	검토 및 결정

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 제어 감사자 확인

검사 이름	설명	스캔 찾기 유형
	엔드포인트의 기능에 따라 인증되지 않은 사용자가 예기치 않은 작업을 수행하거나 예기치 않은 데이터와 상호 작용할 수 있습니다.	
공용 서비스 포털 페이지 검토	공개된 서비스 포털 페이지를 식별합니다. "공개" 필드를 "true"로 설정하면 인증되지 않은 사용자가 서비스 포털 페이지를 사용할 수 있습니다. 검토하고 현재 구성이 비즈니스 요구에 맞는지 확인합니다.	검토 및 결정
공개 UI 페이지 검토	공개된 UI 페이지를 식별합니다. [sys_public] 페이지를 사용하여 인증되지 않은 사용자에게 UI 페이지를 제공할 수 있습니다. 검토하고 현재 구성이 비즈니스 요구에 맞는지 확인합니다.	검토 및 결정
"admin" 역할이 포함된 역할 검토	관리자 역할을 포함하는 역할 (역할 [sys_user_role] 테이블)을 식별합니다. 관리자 역할은 사용자에게 관리 권한을 부여하며 필요한 경우에만 사용해야 합니다. 검토하고 현재 구성이 비즈니스 요구에 맞는지 확인합니다. 의도적인 구성인 경우 이 검사를 음소거할 수 있습니다.	검토 및 결정
해당 ACL 없이 UI 페이지 검토	해당 UI 페이지에 대한 ACL이 없는 UI 페이지를 식별합니다. 특정 ACL이 없는 UI 페이지는 기본적으로 일반 UI 페이지 ACL 로 설정되어 의도하지 않은 사용자에게 액세스 권한을 부여할 수 있습니다.	권장 해결
유효한 로컬 암호를 사용하는 사용자 검토	로컬에서 설정된 암호로 사용자를 식별합니다. 로컬 암호를 사용하는 사용자는 로컬 로그인이 허용되지 않아도 로컬 자격 증명을 사용하여 API를 통해 인스턴스와 상호작용할 수 있습니다. 이 암호 구성은 통합 사용자 계정이 올바르게 작동하는 데 필요합니다. 이러한 사용자 계정을 검토하여 의도한 사용자 (예: 통합 계정)만 로컬 인증을 사용하여 인증할 수 있는지 확인합니다.	검토 및 결정
오래된 해싱 알고리즘으로 저장된 비밀번호 순환	이전 버전의 Now Platform에서 생성된 암호로 사용자 계정을 식별합니다. 이 암호는 현재	권장 해결

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 제어 감사자 확인

검사 이름	설명	스캔 찾기 유형
	레거시 또는 오래된 해싱 알고리즘으로 간주되는 것을 사용했을 수 있습니다. 암호를 순환하지 않은 이전 플랫폼 버전에서 생성된 계정에는 레거시 해싱 알고리즘으로 저장된 암호가 여전히 있을 수 있습니다. 생성된 식별된 계정을 검토하고 암호 재설정을 고려합니다.	
기록 생성자 확보 중	안전하지 않은 기록 생성자를 식별합니다. 적절한 역할에 할당되지 않은 경우 권한 없는 사용자가 액세스하여 중요한 정보가 노출될 수 있습니다. 기록 생성자에 적절한 역할을 할당하여 필요한 사용자만 액세스할 수 있도록 합니다.	권장 해결
UI 작업 표시 여부	테이블에 대한 읽기 권한이 없는 역할이 없는 사용자가 액세스할 수 있는 UI 작업을 식별합니다. 이러한 사용자는 이러한 UI 작업을 통해 액세스할 수 없는 테이블의 데이터를 변경할 수 있습니다. UI 작업은 영향을 받는 테이블에 액세스할 수 있는 사용자만 사용할 수 있는지 확인합니다.	권장 해결

스캔 도구 모음 생성

조직의 인스턴스 보안을 분석할 수 있도록 사용자 지정 도구 모음을 만들고 예약합니다.

시작하기 전에
필요한 역할: admin 또는 sn_vsc.security_center_viewer

도구 모음은 검사에 사용할 수 있는 검사의 모음입니다. 다음으로 이동하여 테이블에 구성된 스캔 도구 모음 목록을 봅니다. 스캐너 > 도구 모음. 사용자 고유의 도구 모음을 만들거나 기본 도구 모음인 감사자를 사용합니다. 감사자는 보안 베스트 프랙티스에 대한 검사를 포함하는 기본 시스템 제품군입니다. 이러한 검사는 인스턴스의 보안 태세에 영향을 줄 수 있는 시스템 속성, 플러그인 및 테이블로 구성됩니다. 다음 단계에서는 구성에 사용할 수 있는 몇 가지 옵션과 함께 제품군을 만드는 방법을 보여줍니다.

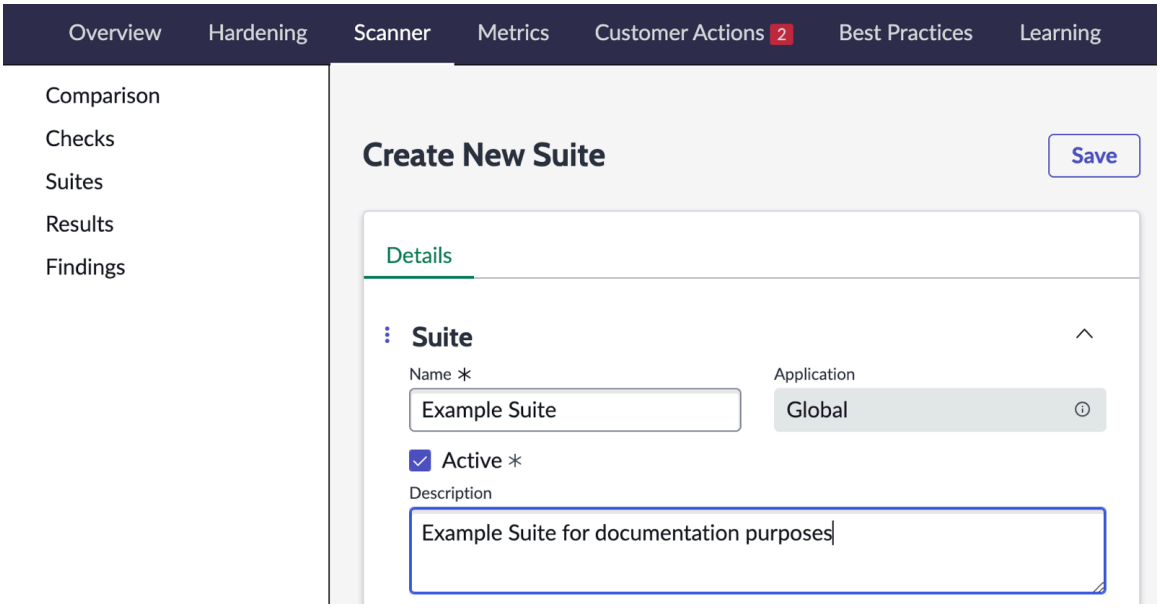
프로시저

1. Security Center에서 스캐너 탭을 선택한 다음, 화면 왼쪽의 패널에서 도구 모음 을 선택합니다.

2. 스캔 도구 모음 페이지에서 새로 만들기 단추를 선택합니다.

3. 제품군 이름과설명을 입력한 다음 저장을 선택합니다

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



저장을 선택하면 제품군에 대한 구성 옵션이 탭 인터페이스에 표시됩니다.

4. 검사 탭을 선택합니다.
   이 탭을 사용하여 도구 모음에 검사를 추가합니다.
   a. 편집을 선택합니다.
   b. 추가할 검사를 선택한 다음 추가(>)를 선택하여 제품군에 배치합니다.
   c. 저장합니다.
5. 하위 도구 모음 탭을 선택합니다.
   이 탭을 사용하여 하위 도구 모음을 추가합니다. 이 도구 모음이 스캔에 사용될 때 하위 도구 모음으로 추가된 도구 모음도 실행됩니다.
   a. 편집을 선택합니다.
   b. 추가할 자식 도구 모음을 선택한 다음 추가(>)를 선택하여 자식 도구 모음에 배치합니다.
   c. 저장합니다.
6. 상위 도구 모음 탭을 선택합니다.
   이 탭을 사용하여 상위 도구 모음을 추가합니다. 스캔에서 실행되는 상위 도구 모음도 이 도구 모음을 실행합니다.
   a. 편집을 선택합니다.
   b. 추가할 자식 도구 모음을 선택한 다음, 추가(>)를 선택하여 부모 도구 모음에 배치합니다.
   c. 저장합니다.
7. 일정 탭을 선택합니다.
   이 탭을 사용하여 도구 모음이 실행되는 시간을 설정합니다.
   a. 새로 만들기를 선택합니다.
   b. 예약된 스캔의 상세 정보를 입력합니다.
      시간 필드의 형식은 시간:분:초입니다.
   c. 저장합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 제어 감사자 제품군 복제

인스턴스에서 기본 접근 제어 감사자 제품군을 클론하고 사용자 지정하여 조직의 보안 관행에 맞는 새 제품군을 생성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
인스턴스와 함께 제공되는 기본 접근 제어 감사자 도구 모음은 수정할 수 없습니다. 그러나 조직의 보안 관행에 맞게 검사를 추가, 제거 또는 편집하려는 경우 접근 제어 감사자 제품군을 복제할 수 있습니다. 접근 제어 감사자 도구 모음을 복사하면 이를 사용자 지정하고 기본 도구 모음을 기반으로 새 도구 모음을 만들 수 있습니다. 접근 제어 감사자 제품군에는 보안 베스트 프랙티스와 관련된 검사가 포함되어 있으며, 인스턴스의 보안 태세에 영향을 주는 시스템 속성, 플러그인 및 테이블을 다룹니다. 다음 단계에서는 기본 접근 제어 감사자 제품군을 복제하여 조직의 요구사항에 맞게 조정하는 방법을 보여줍니다.

프로시저

1. 다음으로 이동 모두 > **Instance Scan** > 도구 모음.
2. 새로 만들기를 선택하고 선택적 설명과 함께 제품군의 이름을 입력합니다.
3. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
4. 스캔에 필요한 검사를 추가합니다.

   a. 검사 탭에서 편집을 선택합니다.

   b. 조건을 추가합니다.
   예를 들어 스캔 검사를 추가하려면 다음 필드, 연산자, 값 및 조건을 적용합니다.

   〔카테고리〕〔는〕〔보안〕 **AND** 〔애플리케이션〕**[is]**〔전역〕

   예를 들어 다음과 같이 표시됩니다. `### #### ####### #####.`

5. 필터 실행을 선택합니다.
6. 컬렉션 목록에서 검사 목록에 추가할 검사 검사를 선택한 다음 추가(>) 단추를 선택합니다.
7. 저장을 선택합니다.
   사용자 지정 검사가 추가된 제품군이 생성되었습니다.
8. 도구 모음 스캔 실행을 선택합니다.

접근 제어 감사자 제품군 보기

기본 접근 제어 감사자 도구 모음에서 사용할 수 있는 검사를 보고 이 도구 모음을 실행할 때 어떤 검사가 실행되는지 파악합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
ServiceNow 인스턴스 내에서 기본 접근 제어 감사자 제품군에 액세스하기 위해 완료해야 하는 단계입니다.

프로시저

1. Security Center에서 스캐너 탭을 선택한 다음 왼쪽 패널에서 도구 모음 을 선택합니다.
2. 스캔 도구 모음 페이지의 목록에서 감사자를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 도구 모음 검사를 검토하려면 검사 탭을 선택합니다.
   제품군에 사용할 수 있는 8개의 검사 목록이 표시됩니다.
4. 분석할 검사의 이름을 선택합니다.
5. 검사와 연결된 필드를 분석합니다.

이름	설명
이름	검사의 이름입니다.
애플리케이션	검사가 속한 애플리케이션(보안 센터)입니다.
범주	검사와 연결된 범주입니다.
우선순위	긴급도 수준입니다.
버전	검사의 버전 번호입니다.
활성	검사의 상태(예: 활성 또는 비활성)입니다.
간단한 설명	검사에 대한 간략한 요약입니다.
설명	검사에 대한 보다 포괄적인 요약입니다.
해결 정보	잠재적인 보안 인시던트를 완화했습니다.
문서 URL	제품 설명서 또는 지식베이스(KB) 문서의 관련 문서에 대한 링크입니다.
조건 실행	검사 시작을 트리거하는 조건입니다.
테이블	검사가 속한 테이블입니다.
조건	검사에 적용되는 조건부 논리입니다.
고급	고급 구성 옵션.

스캔 도구 모음 일정 조정

필요에 맞게 스캔 도구 모음의 일정을 변경합니다.

시작하기 전에

필요한 역할: admin, sn_vsc.security_center_viewer

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 보안 센터.
2. 도구 섹션에서 보안 스캐너를 선택합니다.
3. 화면 왼쪽 가장자리의 메뉴에서 도구 모음 을 선택합니다.
4. 일정을 조정하려는 제품군을 엽니다.
5. 일정 탭을 선택합니다.
6. 기존 일정을 선택하거나 새로 만들기를 선택하여 새 일정을 만듭니다.
7. 예약된 스캔 양식에서 필요에 따라 필드에 내용을 입력합니다.

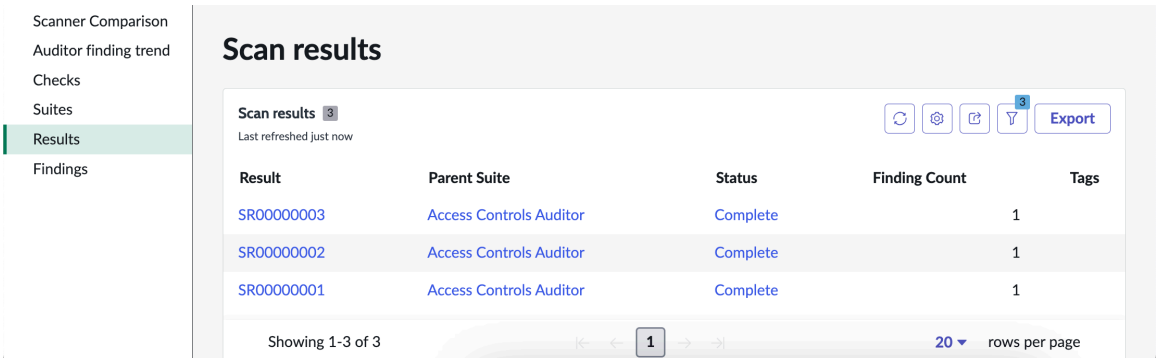
필드	설명
이름	스캔 일정의 이름
실행	제품군의 실행 빈도를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 일정을 정의하는 데 도움이 되는 추가 필드가 표시됩니다. 이러한 필드는 선택 사항에 따라 달라집니다.
활성	일정이 활성 상태인지 여부입니다. 비활성 일정은 실행되지 않습니다.
조건부	일정에 대해 스크립팅된 조건을 정의할 수 있는 조건 필드를 활성화하려면 선택합니다.
조건	일정에 대해 스크립팅된 조건입니다. 스크립트가 `#`로 평가될 때만 제품군이 실행됩니다.
tz로 실행	실행 시기를 결정할 때 일정에서 사용하는 시간대입니다.

스캔 결과

단일 뷰에서 스캔 결과와 관련된 데이터를 봅니다.



스캔 결과는 스캔의 상태와 유형을 보고합니다. 검사의 일부로 실행된 모든 검사와 오류 및 검사 로그와 같은 검사와 관련된 기타 모든 정보도 볼 수 있습니다.

Security Center에서 스캐너 탭을 선택한 다음 왼쪽 패널에서 결과를 선택하여 검사 결과 대시보드를 찾을 수 있습니다. 스캔 결과는 스캔 결과 목록 아래에 나열됩니다. 탭 섹션으로 구분된 상세 정보를 드릴인하고 볼 결과를 선택합니다.

세부사항
: 상태, 유형 및 실행 시간(초)을 포함한 스캔 결과의 개요입니다.

찾은 결과 스캔
: 검사를 실행하는 동안 발견한 결과입니다.

도구 모음
: 이 스캔의 일부로 실행된 도구 모음을 표시합니다.

검사
: 이 검사의 일부로 실행된 검사를 표시합니다.

실패
: 검사 실행 중에 실패한 검사와 실패 원인을 오류 메시지 형식으로 표시합니다.

스캔 로그
: 스캔 중에 출력되는 메시지를 표시합니다.

스캔 통계
: 스캔과 관련된 통계를 표시합니다.

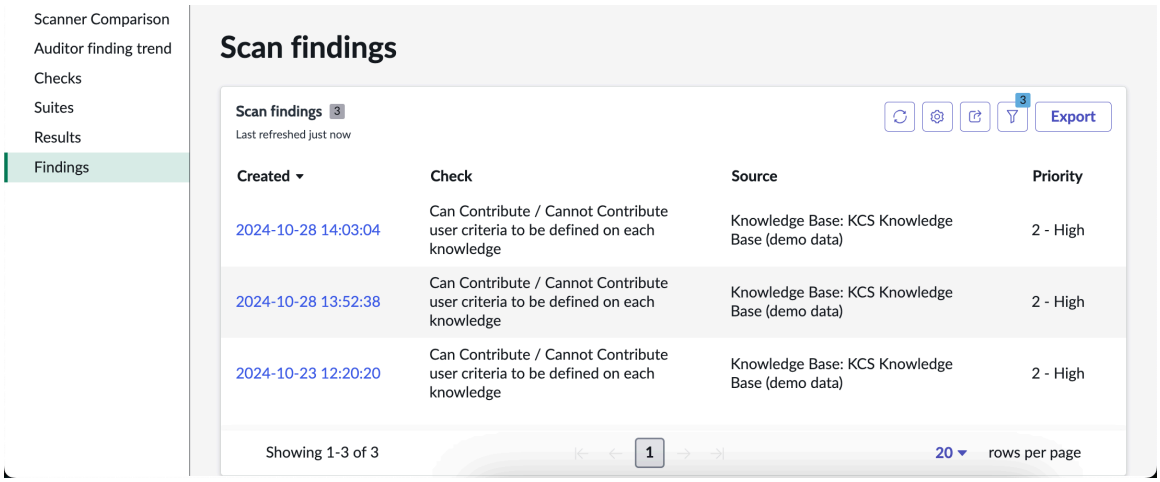
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대상

검사가 실행된 모든 대상을 표시합니다.

스캔 결과

발견 사항 은 인스턴스에 대한 검사를 통해 규칙을 위반한 것으로 파악된 기록에 대한 참조입니다. 소스 기록과 해당 기록이 지정된 검사의 규칙을 트리거한 횟수를 확인할 수 있습니다.



스캔 결과 내에서 스캔 결과 탭으로 이동하여 스캔 결과 목록을 봅니다. 생성된 열 아래의 링크를 선택하여 결과와 관련된 상세 정보를 드릴다운하고 봅니다.

확인

검사와 관련된 검사 목록입니다.

범주

검사와 연결된 보안 범주입니다. 예를 들어 접근 제어 또는 악성 코드가 있습니다.

카운트

기록이 검사 규칙을 위반한 횟수입니다.

우선순위

보안 위험의 심각도: 1은 가장 높은 우선순위이고 4는 가장 낮은 우선순위입니다.

결과

스캔의 상태 및 유형입니다.

버전 검사

검사 버전입니다.

소스 테이블

검사의 규칙을 위반한 기록입니다.

음소거 이유

찾기를 음소거하는 이유입니다.

소스

찾기가 생성된 날짜입니다.

작업

스캔과 연결된 작업 기록입니다. 기록 찾기에서 작업 할당을 용이하게 하는 데 사용됩니다.

도메인

검사가 적용되는 도메인입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

간단한 설명

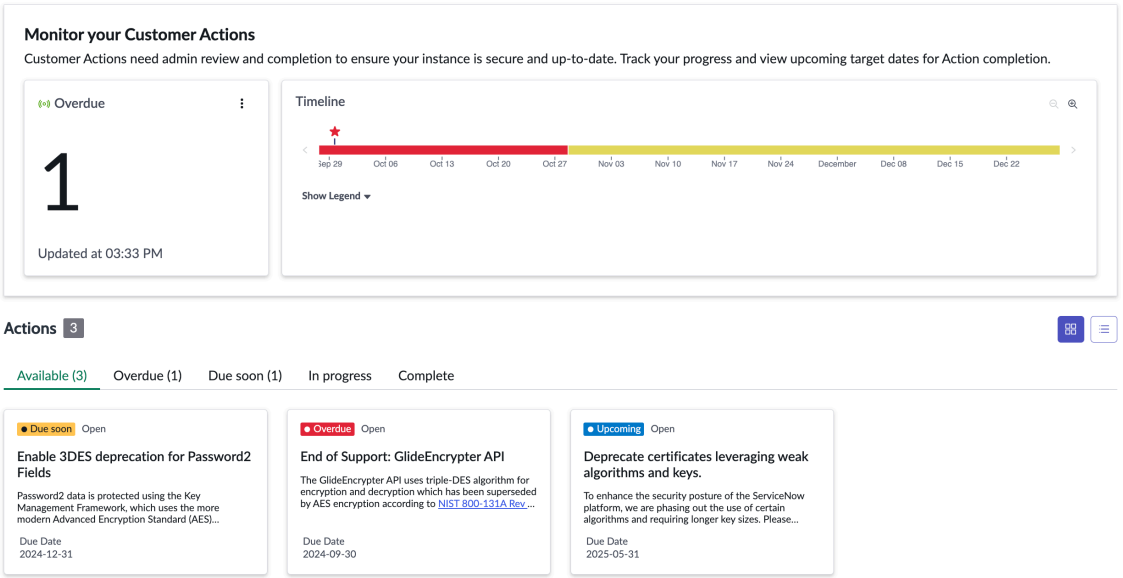
검사에 대한 간략한 설명입니다.

해결 정보

검사에서 보고된 문제를 해결하는 방법에 대한 지침입니다.

고객 작업

고객 작업 도구를 사용하여 인스턴스와 플러그인 구성을 기반으로 중요한 보안 업데이트를 구현합니다.



고객 작업은 보안 관련 변경의 중요성을 이해하는 데 도움을 주는 데 중점을 둔 인스턴스에 대한 권장 변경 사항입니다. 수동으로 구현된 고객 작업은 제품군 릴리스 또는 패치를 통해 인스턴스에서 ServiceNow 코드 또는 기능에 맞게 렌더링되는 자동 업데이트와는 다릅니다. 인스턴스의 커스터마이제이션을 방해하지 않도록 고객 작업을 구현합니다.

고객 작업 홈페이지에서 고객 작업의 타임라인을 볼 수 있으므로 단계를 구현할 시기의 우선순위를 지정할 수 있습니다. 위 예시의 타임라인은 지연된 고객 작업과 곧 만료되는 고객 작업을 보여줍니다. 또한 업데이트 레이블에서 고객 작업의 진행 상황을 추적할 수 있습니다. 탭을 선택하여 사용 가능, 지연, 곧 마감, 진행 중 또는 완료된 고객 작업을 확인할 수 있습니다.

시작:

- 보안 센터 내의 고객 작업으로 이동하여 이 도구에 액세스합니다.
- 고객 작업은 Washington DC부터 Security Center 앱에 포함됩니다.

고객 작업을 위한 단계 구현

인스턴스에 고객 작업을 구현하여 보안 태세를 강화하는 방법에 대해 알아봅니다.

시작하기 전에

필요한 역할: 관리자

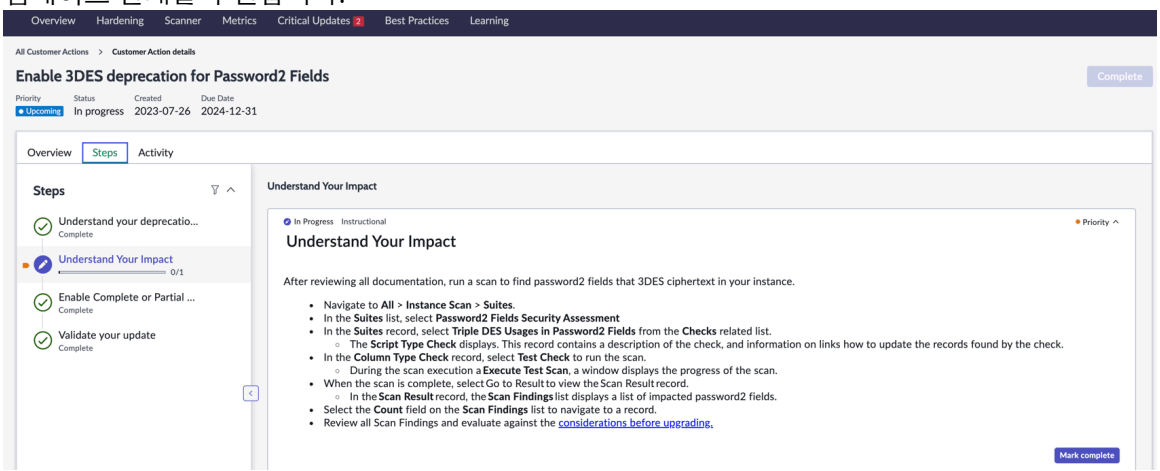
이 태스크 정보

고객 작업 (CA) 은 보안 태세를 강화하기 위해 인스턴스에 변경 사항을 구현하는 방법에 대한 단계별 지침을 제공합니다. CA는 제품 문서에서 관련 콘텐츠를 가져와 구현 프로세스의 각 단계를 안내합니다. 고객 작업을 구현하는 방법을 알아보려면 아래 단계를 따르십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 고객 작업 앱으로 이동합니다.
2. 구현할 고객 작업을 클릭합니다.
   업데이트 섹션의 사용 가능 탭에는 인스턴스에 대한 모든 고객 작업이 나열됩니다. 지침을 보려면 이 탭에서 고객 작업을 클릭하십시오.
3. 개요를 읽고 고객 작업이 필요한 이유를 알아보고 단계 구현을 준비합니다.
   다음 단계로 이동을 클릭하여 구현 세부 정보로 진행합니다.
4. 업데이트 단계를 구현합니다.



   a. 각 지침 그룹을 읽고 인스턴스 내에서 구현합니다.
   b. 일련의 지침이 완료되면 완료 표시를 클릭합니다.
   c. 모든 업데이트 단계를 완료할 때까지 단계 a-b를 반복합니다.
   d. 완료를 클릭합니다.
   고객 작업 홈페이지의 업데이트 섹션에서 고객 작업을 더 이상 사용할 수 없습니다.

고객 작업의 활동 보기

고객 작업과 관련된 모든 활동에 대한 상세 정보를 확인합니다.

시작하기 전에
필요한 역할: 관리자

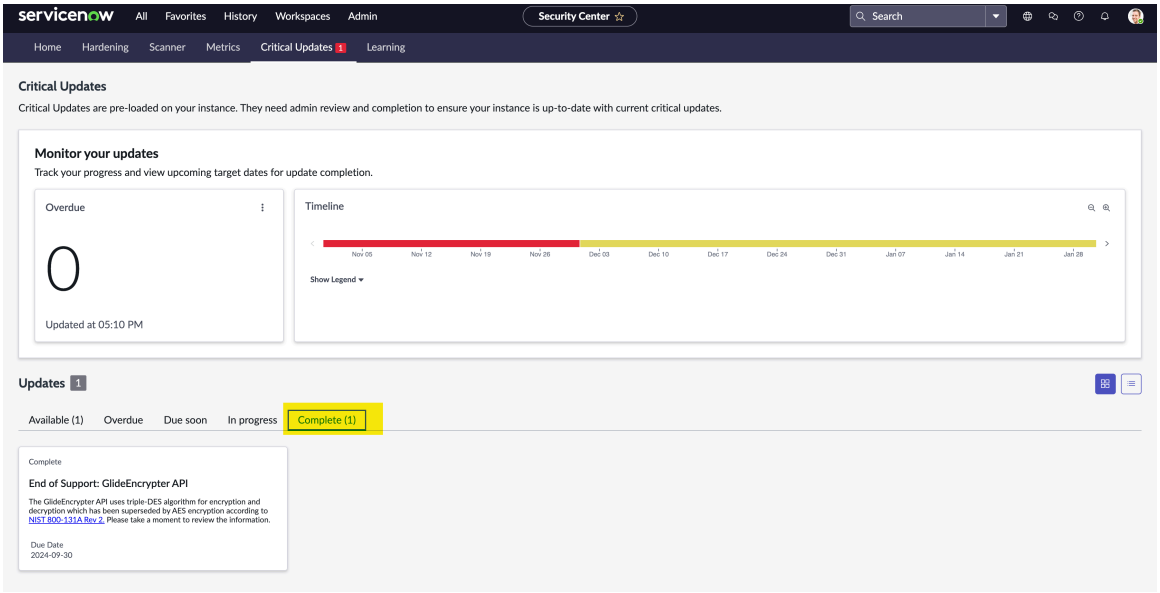
이 태스크 정보
가장 최근의 활동을 먼저 분석할 수 있도록 최신 활동부터 가장 오래된 활동까지 나열됩니다. 활동에 대한 각 업데이트에는 타임스탬프가 지정되며 검색 및 필터를 사용하여 특정 정보를 쿼리할 수 있습니다.

프로시저

1. 보안 센터 내에서 고객 작업 앱으로 이동합니다.
2. 고객 작업의 업데이트 레이블 로 이동합니다.
3. 상태를 클릭한 다음 해당 상태에서 고객 작업을 선택합니다.

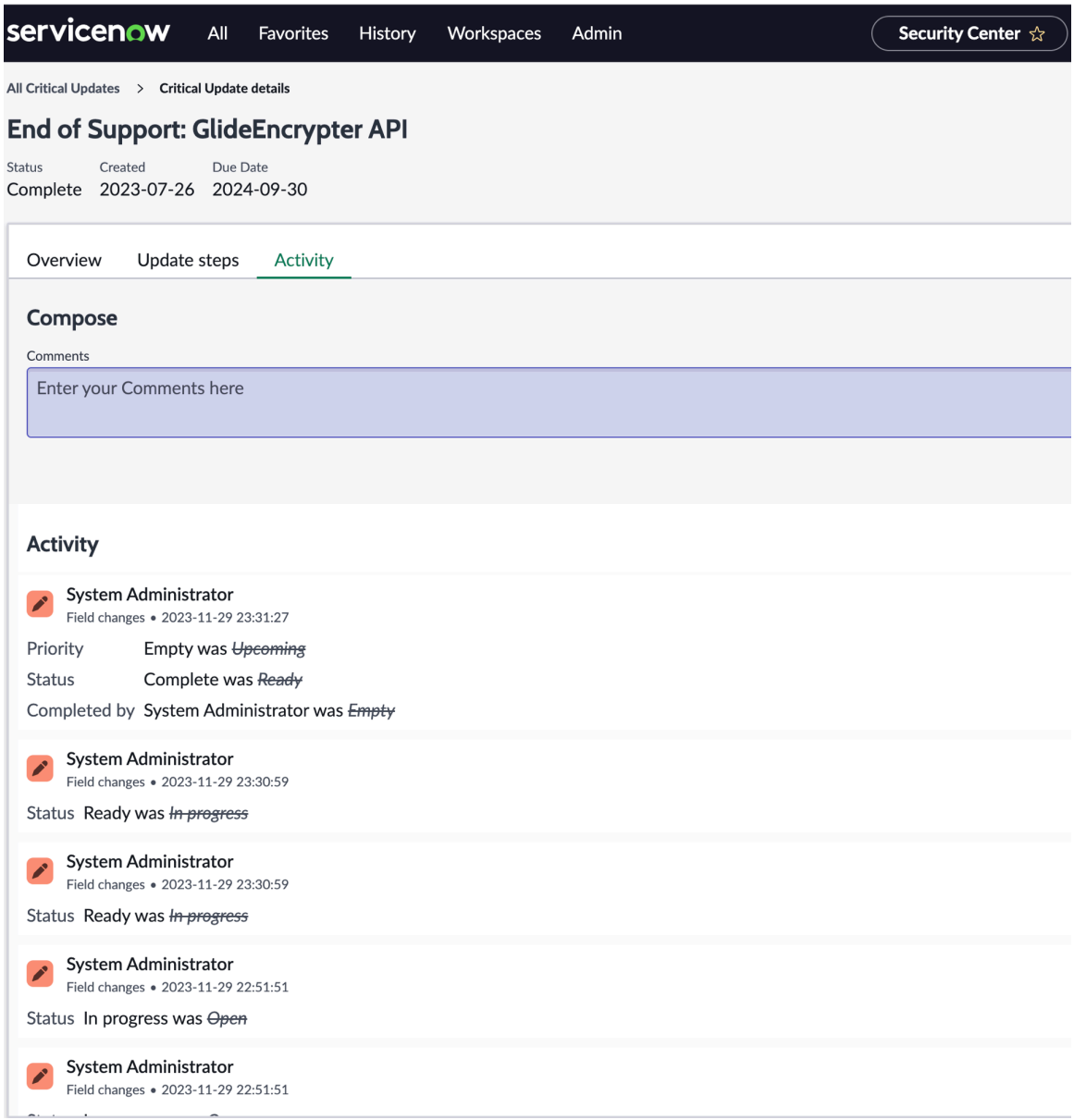
   아래 예에서는 완료 상태가 선택된 다음 지원 종료: **GlideEncrypter** API에 대한 고객 작업이 선택됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 고객 작업의 활동을 봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

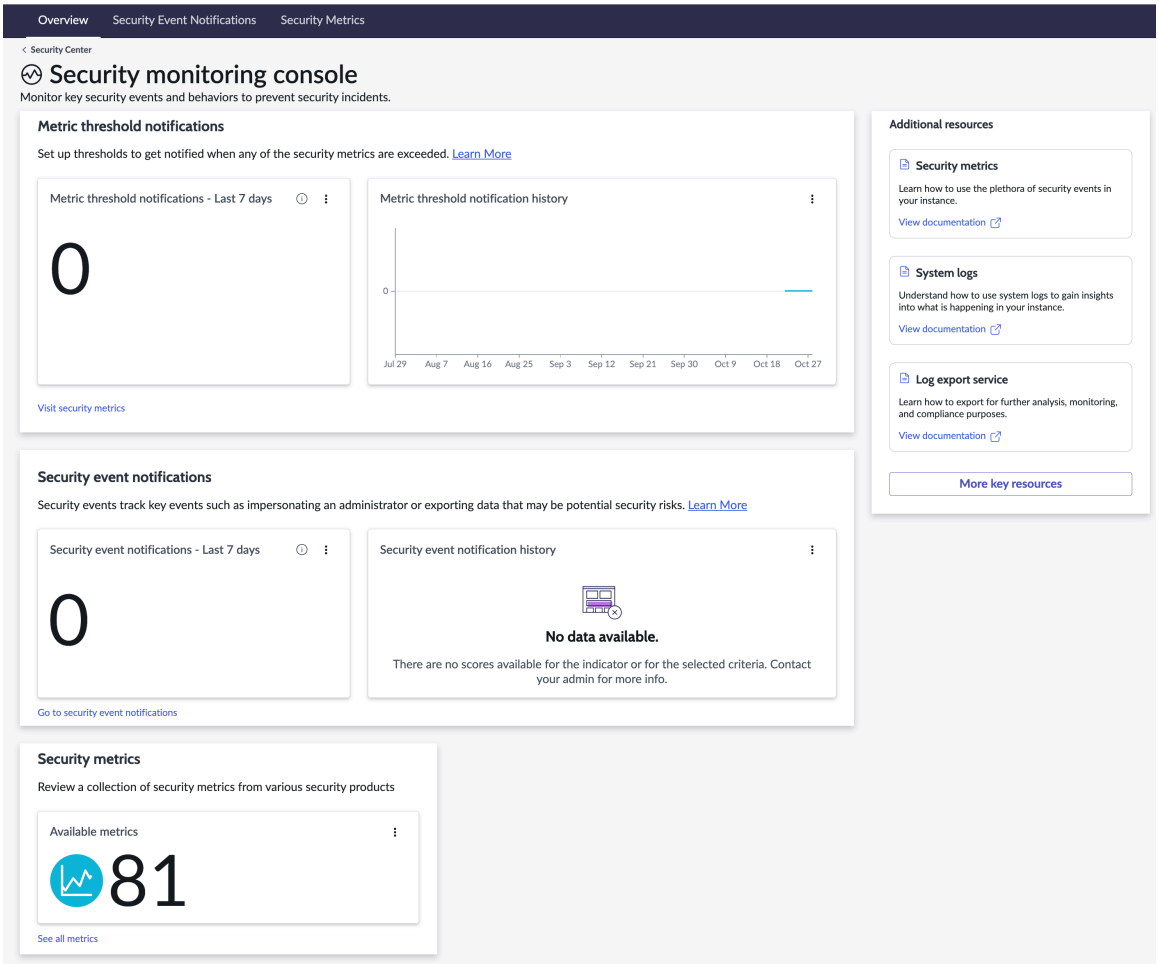


고객 작업과 관련된 모든 활동이 자동으로 기록됩니다. 또한 활동에 코멘트를 추가할 수 있습니다.

보안 모니터링 콘솔

보안 알림 및 메트릭을 감독하여 인스턴스에 대한 잠재적인 보안 위험에 대한 정보를 지속적으로 받습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 모니터링 콘솔은 섹션으로 구성되며, 각 섹션에는 보안 모니터링의 특정 측면에 대한 정보가 포함된 카드가 있습니다. 카드에서 정보(ⓘ) 아이콘을 선택하면 각 카드가 무엇을 나타내는지에 대한 자세한 내용을 볼 수 있습니다.

탐색 모음

페이지 상단의 막대를 사용하여 보안 모니터링 콘솔 섹션 사이를 이동합니다.

메트릭 임계치 알림

메트릭 임계치 알림 패널에서 인스턴스의 메트릭 임계치 알림에 대해 알아봅니다. 임계치는 표시기에 대한 점수의 정상 범위를 정의하고 점수가 사상 최고치에 도달하는 경우와 같은 특정 이벤트가 발생할 때 사용자에게 알립니다. 이 패널에는 지난 7일 동안의 임계치 알림 수와 시간 경과에 따른 임계치 수를 보여주는 차트가 표시됩니다.

두 카드 중 하나를 선택하여 보안 메트릭 탭을 열고 이러한 알림에 대한 자세한 내용을 확인합니다.

보안 이벤트 알림

보안 이벤트 알림 섹션에서 가장 또는 데이터 익스포트와 같은 보안 이벤트를 추적합니다. 이 패널에는 지난 7일 동안의 보안 이벤트 수와 시간 경과에 따른 개수를 보여 주는 차트가 표시됩니다.

두 카드 중 하나를 선택하여 보안 메트릭 탭을 열고 이러한 알림에 대한 자세한 내용을 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 메트릭

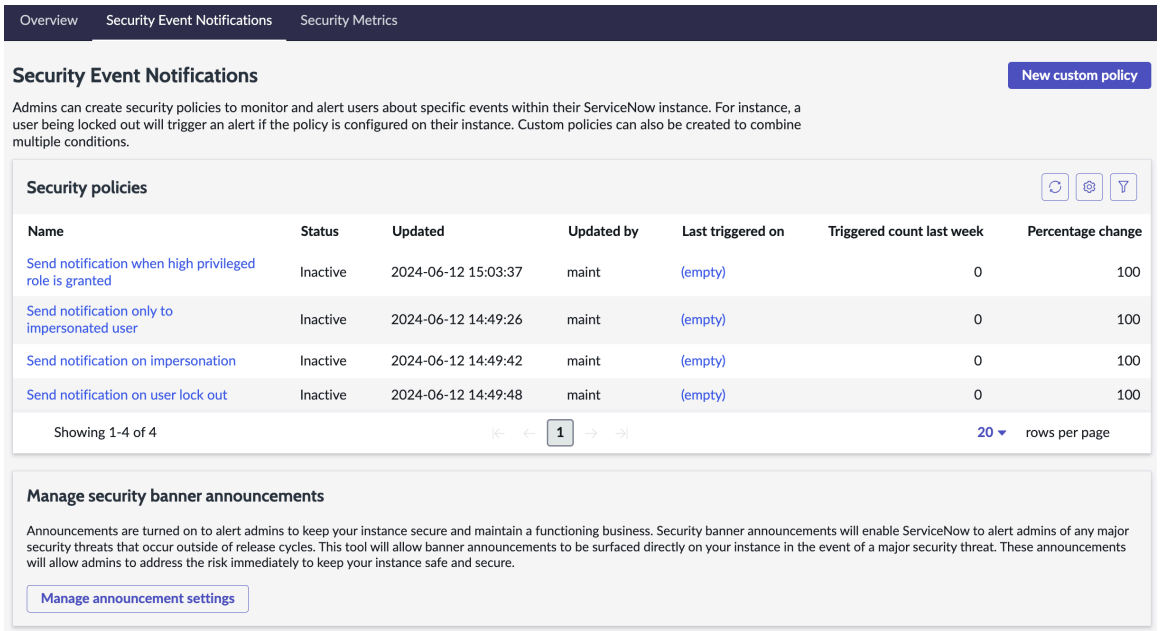
이 섹션에는 인스턴스에서 사용할 수 있는 보안 메트릭의 수가 표시됩니다. 다양한 보안 제품의 보안 메트릭 컬렉션을 검토합니다.

추가 자원

화면 가장자리의 추가 자원 섹션을 사용하여 학습 보안 센터와 관련된 설명서 및 비디오와 인스턴스 보안 관리에 대한 정보로 이동합니다.

보안 이벤트 알림

ServiceNow 인스턴스에서 기본 보안 이벤트 알림 정책을 확인, 관리 및 분석하고 사용자 지정 정책을 생성하는 기능에 액세스합니다.



사용자가 Now Platform에서 안전하지 않거나 관리자 모니터링이 필요할 수 있는 작업을 수행할 때 이메일 알림을 트리거하는 알림 정책을 사용자 지정하고 생성합니다.

관리자는 기본 정책의 값을 사용자 지정하고, 기본 정책을 복제 및 편집하거나, 고유한 사용자 지정 정책을 만들 수 있습니다.

보안 정책

보안 이벤트 알림 콘솔에는 인스턴스의 보안 정책과 관련된 중요한 정보가 표시됩니다. 이 테이블에는 다음을 표시하는 열이 포함됩니다.

레이블	설명
이름	보안 이벤트 알림 정책의 이름입니다.
상태	정책 상태는 활성 또는 비활성일 수 있습니다.
업데이트됨	정책이 마지막으로 업데이트된 날짜 및 시간입니다.
업데이트한 사람	정책을 업데이트한 사용자입니다.
마지막으로 트리거된 날짜	정책이 마지막으로 실행된 날짜 및 시간입니다.
지난 주 트리거된 수	지난 7일 동안 정책에서 생성된 트리거 수입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

레이블	설명
백분율 변경	백분율로 계산되는 주간 트리거의 변경률입니다. 주: 예를 들어 이 정책이 주당 평균 5개의 알림을 트리거하고 지난주에 10번 트리거한 경우 백분율은 100% 증가합니다.

개요, 설정 및 알림 이력을 포함한 자세한 내용을 보려면 테이블에서 정책을 선택합니다. 새 사용자 지정 정책 버튼을 선택하여 조직의 사용 사례에 맞는 사용자 지정 정책을 생성합니다.

보안 배너 공지 관리

공지 설정 관리를 선택하여 관리자가 이 인스턴스에서 배너 알림을 수신할지 여부를 제어합니다. 이러한 공지에 대한 자세한 내용은 문서를 참조하십시오 보안 배너 공지.

사용자 지정 보안 이벤트 알림 정책 생성

조직의 필요에 따라 사용자 지정 보안 이벤트 알림을 만드는 방법에 대해 알아봅니다. 이를 통해 인스턴스에서 사용자와 그룹이 수행한 작업을 모니터링하고 잠재적인 보안 위험에 대한 알림을 생성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. Security Center 앱으로 이동하여 다음을 선택합니다. 알림.
2. 새 사용자 지정 정책을 선택합니다.
3. 정책 시작을 트리거하는 세 가지 이벤트 유형 중 하나를 선택하고 만들기를 선택합니다.
4. 정책을 구성합니다.
   새 사용자 지정 보안 이벤트 알림 정책을 구성하는 방법에 대한 자세한 내용을 참조하십시오 보안 이벤트 알림 정책의 기본 설정 구성 .

보안 이벤트 알림 정책 수정

보안 이벤트 알림 정책의 설정을 수정하는 방법에 대해 알아봅니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 보안 이벤트 알림 홈페이지로 이동하여 수정하려는 정책을 선택합니다.

   주: 기본 정책의 트리거 또는 조건 논리는 수정할 수 없습니다. 이러한 설정을 수정하려면 먼저 업데이트 옆에 있는 아래쪽 화살표를 선택한 다음 복제를 선택하여 수행할 수 있는 정책을 복제해야 합니다.

2. 정책 설정을 선택하여 설정을 변경합니다.
3. 업데이트를 선택하여 변경 내용을 저장합니다.
4. 옵션: 알림 트리거를 시작할 준비가 될 때까지 비활성화 를 선택합니다.
5. 옵션: 활성화를 선택하여 알림 트리거를 시작합니다.
   새 사용자 지정 보안 이벤트 알림 정책을 구성하는 방법에 대한 자세한 내용을 참조하십시오 보안 이벤트 알림 정책의 기본 설정 구성 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 이벤트 알림 정책의 기본 설정 구성

조직의 보안 센터 특정 요구 사항에 맞게 보안 이벤트 알림 정책을 사용자 지정하는 방법을 알아보십시오.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
정책 설정 페이지에서는 보안 이벤트 알림 정책에 대한 설정을 사용자 지정할 수 있습니다. 여기에서 정책이 실행되는 시기, 조건부 논리 및 전송되는 알림과 관련된 옵션을 조정할 수 있습니다.

프로시저

1. Security Center에서 알림을 선택합니다.
2. 보안 정책 테이블에서 구성할 보안 이벤트 알림 정책을 선택합니다.
   예를 들어 높은 권한의 역할이 부여되면 알림을 보냅니다.
3. 정책 설정을 선택합니다.
4. 정책 설정을 구성합니다.

정책 설정 구성 옵션

레이블	구성할 항목
실행 시기	트리거: 정책을 시작하는 이벤트입니다.
조건	정책에 적용할 조건부 논리 및 조건입니다. ◦ 조건 논리: 두 가지 옵션 ▪ 이 정책을 트리거하려면 모든 조건이 충족되어야 합니다. 알림을 보내려면 정책이 모두 유효해야 합니다. ▪ 이 정책을 트리거하려면 조건 중 하나라도 충족되어야 합니다. 조건 중 하나라도 유효하면 알림이 전송됩니다. ◦ 조건 추가: 조건 추가를 선택하고 적절한 값을 제공합니다. 조건 제거를 선택하여 조건을 제거할 수 있습니다.
알림	이메일 본문 및 이메일 수신자는 다음을 수행합니다. ◦ 알림: 미리 정의된 알림 템플릿 중 하나를 선택합니다. 자세한 내용은 보안 이벤트 알림을 위한 사용자 지정 이메일 만들기 문서를 참조하십시오. ◦ 알림 추가: 알림 추가를 선택합니다. ◦ 그룹: 알림을 받을 그룹을 선택합니다. ◦ 사용자: 알림을 받을 사용자를 선택합니다. 알림 제거를 선택하여 알림을 제거할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 정책을 비활성화하려면 비활성화를 선택합니다. 정책을 복제하려면 업데이트 (

.) 버튼 옆에 있는 아래쪽 화살표를 선택합니다.

5. 업데이트를 선택하여 설정을 저장합니다.

보안 이벤트 알림을 위한 사용자 지정 이메일 만들기

새 알림을 구성하고, 트리거를 설정하고, 수신자를 정의하고, 동적 이벤트 필드로 이메일 콘텐츠를 만들어 보안 이벤트 알림에 대한 사용자 지정 이메일을 만드는 방법에 대해 알아봅니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 선택 시스템 알림 > 알림.

2. 새로 만들기를 선택합니다.

3. 알림 필드의 이름을 입력합니다.

4. 테이블 옆의 필드를 선택하고 보안 정책 알림(*sn_vsc_security_policy*)을 입력합니다.

5. 새 기록을 구성합니다.
기록 내에는 보낼 시기, 받을 사람, 포함될 항목 등 세 개의 탭을 구성해야 합니다.

탭	설명
보낼 시기	레이블 전송 시기 옆에 있는 필드를 선택하고 트리거됨을 선택합니다.
수신인	◦ 필드의 사용자/그룹 옆에 있는 로컬 아이콘을 선택하고 사용자와그룹을 모두 선택합니다. 항목 추가(>) 아이콘을 선택하여 필드를 선택됨 텍스트 필드로 이동합니다. ◦ 기록 헤더 배너를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.)

포함될 항목	이메일 템플릿을 생성합니다.
	
	자세한 내용은 이메일 템플릿 생성 문서를 참조하십시오.
	
	이벤트의 필드를 메시지 **HTML**에 입력합니다. `# ### ${event_id.FIELD_NAME}`을 사용하여 수행할 수 있습니다. 예를 들면 다음과 같습니다.
	
	`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}`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탭	설명
	`Security Center Notification: ${execution.policy.name}`

6. 제출을 선택합니다.
7. 보안 이벤트 알림의 이메일 템플릿에 사용자 지정 알림을 추가합니다.
   a. 보안 센터에서 알림 > 정책 설정.
   b. 알림 레이블로 이동합니다.
   c. 알림 필드에 생성한 사용자 지정 알림의 이름을 입력합니다.

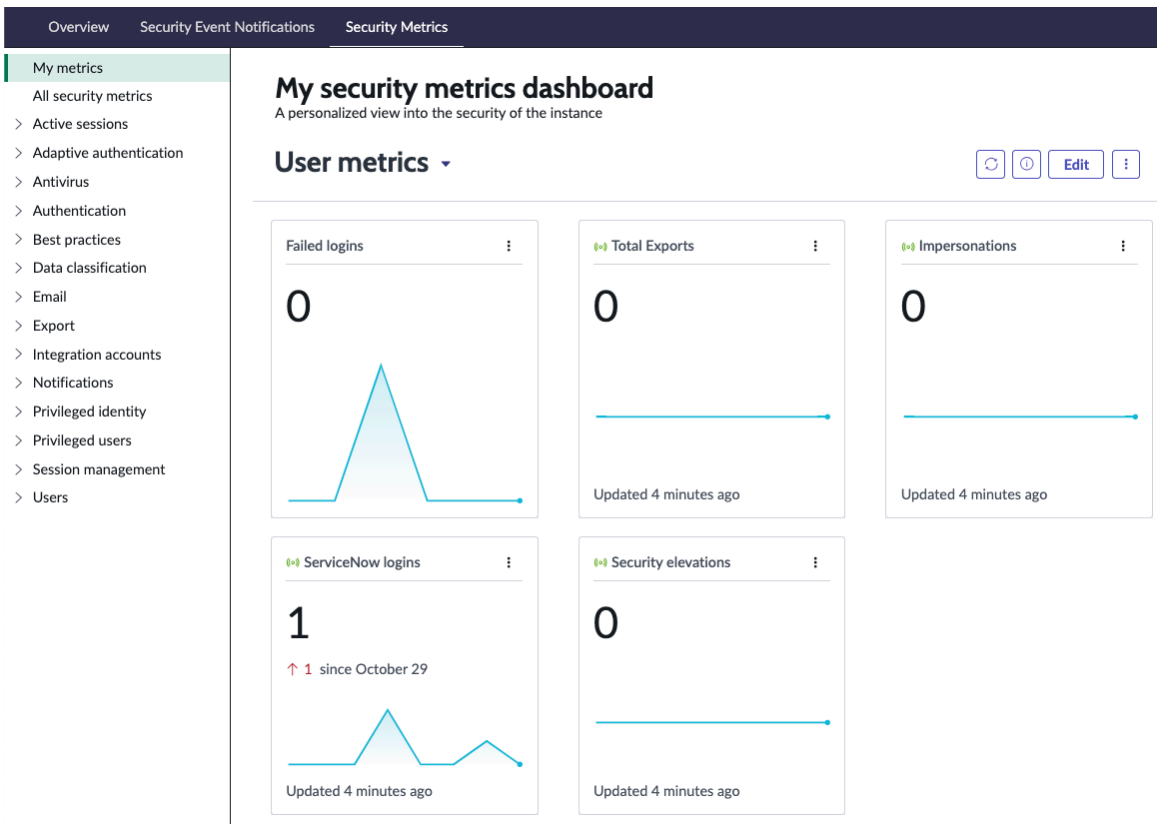
보안 이벤트 알림 이력

인스턴스에 대한 보안 이벤트 알림의 전체 이력을 탐색합니다.

알림 페이지에서는 인스턴스의 모든 보안 이벤트 알림 정책에 대한 알림 이력의 개요를 제공합니다. 차트에서 데이터를 보고 그래픽으로 표시하고 대상, 임계치 및 KPI 신호와 같은 퍼포먼스 분석 기능을 적용할 수 있습니다. 또는 검색, 정렬, 필터링 및 쿼리와 같은 표준 기능을 활용할 수 있는 테이블 형식으로 데이터를 볼 수 있습니다.

보안 메트릭

50개 이상의 다양한 보안 메트릭을 모니터링하여 잠재적인 보안 위협 또는 안전하지 않은 동작을 식별합니다. 이메일 알림에 대한 임계치를 설정하고, 여러 가지 방법으로 데이터를 시각화 및 분석합니다. 데이터를 익스포트하거나 조직에 가장 중요한 메트릭으로 대시보드를 생성합니다.



내 보안 메트릭 대시보드

이 대시보드를 사용하여 실패한 로그인, 익스포트 및 가장과 같은 메트릭을 봅니다. 편집을 선택하여 시각화, 필터, 제목, 이미지, 서식 있는 텍스트 및 목록을 추가하여 대시보드를 사용자 지정합니다.

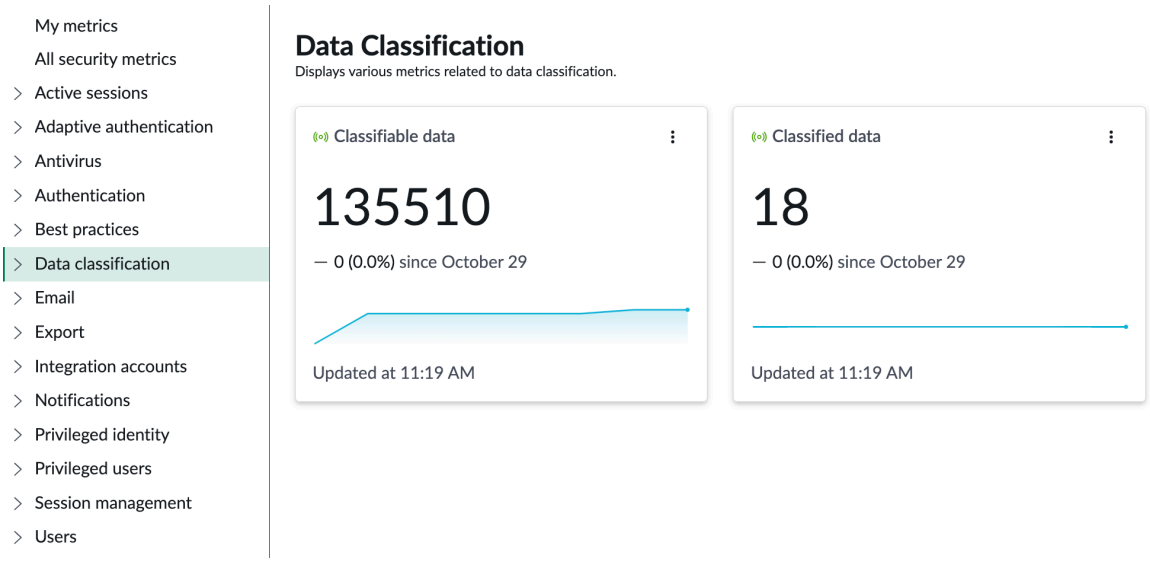
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대시보드를 사용자 지정할 수 있는 다양한 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 의 대시보드 플랫폼 분석 .

메트릭 탐색 창

화면 가장자리의 탐색 창에 인스턴스 메트릭이 표시됩니다. 모든 보안 메트릭을 선택하여 단일 목록의 모든 메트릭을 보거나 그 후 항목을 선택하여 범주별로 구성된 메트릭을 찾아봅니다.

각 범주에는 보안 메트릭 페이지의 보안 메트릭 대시보드와 비슷한 대시보드가 해당 범주의 메트릭에 대한 카드와 함께 표시됩니다.



보안 메트릭 대시보드 사용자 지정

그래프 및 차트와 같은 다양한 소스의 메트릭을 사용하여 사용자 지정할 수 있는 보안 메트릭 대시보드의 유연성을 살펴보십시오. 조직의 특정 요구사항에 맞게 대시보드를 조정합니다.

시작하기 전에

보안 메트릭 대시보드를 사용자 지정하려면 Security Center 애플리케이션 범위 내에 있는지 확인합니다. 이 범위로 전환하려면 애플리케이션 선택기 > 애플리케이션 범위을 클릭하고 보안 센터를 입력합니다.

필요한 역할: 관리자

이 태스크 정보

Security Center 대시보드를 사용하여 보안 메트릭을 구현하고 사용자 지정합니다. 보고서에서 생성된 그래프 및 차트와 같은 다양한 소스의 메트릭과 콘텐츠를 대시보드에 추가합니다. 조직의 필요에 맞게 사용자 지정할 수 있도록 보안 메트릭 대시보드에 탭을 추가하는 데 필요한 단계를 알아봅니다.

프로시저

1. Security Center 앱에서 메트릭을 선택하여 보안 메트릭 대시보드로 이동합니다.
2. 편집을 선택하여 편집 모드를 시작합니다.
3. +탭 추가를 선택하여 탭을 만듭니다.

   주: 기존 탭 옆에 있는 더하기**(+)** 아이콘을 선택하여 새 탭을 추가할 수도 있습니다.

4. 연필 아이콘을 선택하고 이름을 입력하여 새로 만든 탭의 제목을 편집합니다.
5. 새 요소 추가를 선택하여 탭에 요소를 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 저장을 선택합니다.
7. 옵션: 조직의 사용자, 그룹 및 역할과 대시보드를 공유하려면 다음을 선택합니다. 추가 작업 메뉴 > 공유.
   a. 접근 권한을 부여할 사용자의 이름을 입력합니다.
   b. 확인을 선택합니다.

임계치가 트리거되면 이메일을 보내도록 보안 메트릭 구성

임계치가 트리거될 때 인스턴스가 이메일 알림을 생성하도록 보안 메트릭을 구성하는 방법에 대해 알아봅니다.

시작하기 전에
필요한 역할: 관리자

프로시저
1. 보안 센터에서 메트릭으로 이동합니다.
2. 조직에서 임계치를 설정하려는 메트릭을 선택합니다.

   Example
   실패한 로그인을 관리하기 위해 임계값을 설정할 수 있습니다. 실패한 로그인 수가 이 임계값에 도달하면 조직의 관리자 또는 보안 전문가에게 알립니다. 이 경우 대상으로 삼기에 적합한 보안 메트릭은 다음과 같습니다. 사용자 > 실패한 로그인.
3. 임계치 아이콘을 선택합니다.
4. 임계치 패널에서 더하기**(+)** 아이콘을 선택하여 양식을 구성합니다.
   사용 가능한 옵션은 가시성, 임계치 유형 및 임계치 값을 설정하는 것입니다.

   a. 가시성의 경우 모든 사람이 알림을 받도록 하려면 모두를 선택하고, 알림만 받으려면 나용을 선택합니다.

   b. 임계치 유형에서 모든 시간 높음을 선택합니다.
   이 필드는 임계치 알림을 트리거합니다.

   > 주: 임계치 유형이보다 작 거나 보다 큼으로 설정된 경우에만 임계치 값을 입력해야 합니다.

5. 저장을 선택하여 임계치를 생성합니다.
   다음으로 알림을 설정해야 합니다.
6. 모두 선택하고 시스템 알림을 입력합니다.
7. 다음으로 이동 이메일 > 알림.
8. 이름 열에 `*pa thre`를 입력합니다.
   임계치 알림은 이벤트 기반이며 PA 임계치 알림 테이블에서 설정됩니다.
9. **PA** 임계치 알림을 선택합니다.
   결과에는 세 개의 탭이 있습니다.
   - 보내는 시기: 이메일 알림을 보내기 위해 수행해야 하는 조건을 지정합니다. 이 예에서는 이전에 설정한 임계치에 도달하면 이메일이 트리거됩니다.
   - 수신인: 알림을 받을 사용자를 지정합니다. 사용자 및 그룹을 추가할 수 있습니다.
   - 포함될 내용: 사용자와 그룹이 수신할 메시지를 사용자 지정하기 위해 사용자가 수정할 수 있는 스크립트 작업을 지정합니다. 스크립트 동작 생성에 대한 자세한 내용은 문서를 참조하십시오 스크립트 작업 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모든 보안 메트릭

모든 보안 메트릭으로 이동하여 인스턴스의 보안 메트릭과 관련된 데이터가 있는 테이블을 봅니다.

활성 세션

에서 Now Platform활성 사용자의 추세선을 봅니다.

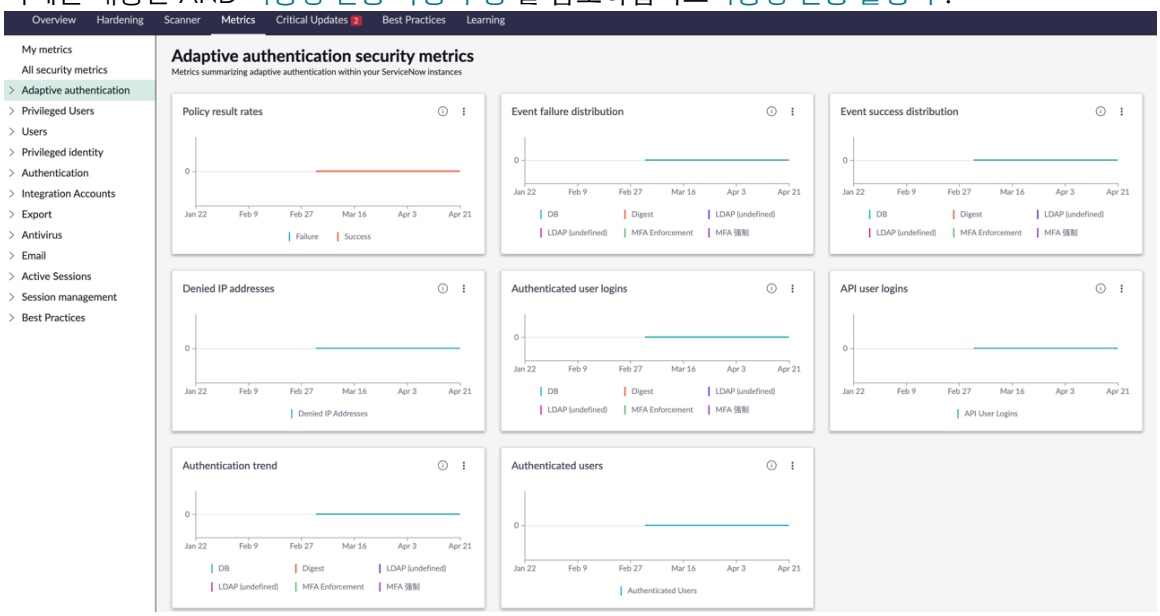
추세선은 다음 메트릭에 대해 볼 수 있습니다.

- 사용자 세션: 인스턴스의 활성 사용자 세션과 관련된 메트릭입니다.
- 권한 있는 사용자 세션: 권한 있는 사용자 또는 추가 역할이 할당된 사용자와 관련된 메트릭입니다.

적응형 인증 보안 메트릭

인증 정책을 사용하여 인증 요청을 평가하고 지정된 정책 조건에 따라 인스턴스에 대한 액세스를 거부하거나 허용합니다.

적응형 인증 메트릭을 사용하면 인스턴스에서 적응형 인증이 사용되는 방식을 모니터링할 수 있습니다. 적응형 인증에 대한 모든 메트릭, 개별 메트릭(예: 정책 결과 비율 또는 거부된 IP 주소)의 요약을 봅니다. 이 페이지를 사용하려면 인스턴스에서 적응형 인증을 위한 적응형 인증() *com.snc.adaptive_authentication* 플러그인을 사용할 수 있어야 합니다. 메트릭을 보려면 인증 정책을 활성화해야 합니다. 자세한 내용은 AND 적응형 인증 속성 구성 를 참조하십시오적응형 인증 활성화 .



주: 이 기능은 버전 1.2에서 릴리스되었습니다.

- 정책 결과 비율: 모든 성공 및 실패한 적응형 인증 이벤트입니다.
- 이벤트 장애 분포: 각 이벤트 유형에 대해 실패한 모든 이벤트입니다.
- 이벤트 성공 분포: 모든 이벤트 유형과 연결된 성공 이벤트입니다.
- 거부된 IP 주소: 연관된 데이터와 함께 인스턴스에 의해 차단된 IP 주소의 수입니다.
- 인증된 사용자 로그인: 사전 로그인 이벤트를 제외하고, 각 이벤트 유형에 대해 계산되는 이벤트 수입니다.
- API 사용자 로그인: 각 이벤트 유형에 대해 API 인증 정책과 연결된 이벤트 수입니다.
- 인증 추세: 기록된 총 이벤트 수입니다.
- 인증된 사용자: 사전 로그인 이벤트를 제외하고 각 이벤트 유형에 대해 계산되는 사용자 수입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

바이러스 백신

잠재적으로 감염된 파일에서 이벤트가 발생하는 추세를 표시합니다. 검색, 격리, 복원 또는 삭제 시기를 확인합니다.

- 격리된 파일: 잠재적으로 맬웨어를 포함할 수 있는 파일 수입니다.
- 다운로드된 파일: 다운로드된 파일 수입니다.
- 복원된 파일: 복원된 파일 수입니다.
- 삭제된 파일: 삭제된 파일 수입니다.

데이터 분류

ServiceNow 인스턴스에서 데이터 분류를 위한 보안 메트릭에 액세스합니다.

데이터 분류를 사용하면 데이터 분류 레이블을 테이블의 기존 딕셔너리 항목에 적용할 수 있습니다. 이러한 레이블은 인스턴스에서 호스팅되는 데이터 유형에 대한 가시성을 제공하는 데 도움이 됩니다. 이러한 분류를 사용하여 개인정보 보호법을 준수하고 업계 규정 요구 사항을 충족합니다.

자세한 내용은 데이터 분류 를 참조하세요.

- 분류 가능한 데이터: 분류할 수 있는 테이블 또는 열입니다.
- 분류된 데이터: 분류된 딕셔너리 항목, 테이블 또는 열입니다.

데이터는 대상 설정, 임계치, 추세, 통계 또는 예측과 같은 자세한 분석을 제공하는 사용자 지정 가능한 차트에 그래픽으로 표시됩니다. 데이터는 테이블의 기록으로도 구성됩니다. 자세한 내용은 분석 허브 문서를 참조하십시오.

인증 메트릭

대시보드에서 인스턴스의 인증과 관련된 메트릭을 봅니다.

MFA 사용량, 웹 서비스 계정 및 생체 인식 스캐너 사용과 같은 인증 체계와 관련된 메트릭에 대한 데이터를 표시합니다.

- MFA에 등록된 사용자: MFA를 사용하기 위해 등록된 총 사용자 수입니다.
- MFA 바이패스를 사용하는 사용자: 다단계 인증을 바이패스하는 총 사용자 수입니다.
- 높은 권한의 비 MFA 사용자: MFA를 사용하지 않는 높은 권한의 총 사용자 수입니다.
- 활성 MFA 사용자: 인스턴스에서 활성 상태인 총 MFA 사용자 수입니다.
- 잠긴 MFA 사용자: 인스턴스에서 잠긴 MFA 사용자의 총 수입니다.
- 웹 서비스 계정 사용자: 웹 서비스 계정만 있는 총 사용자 수입니다.
- X509 인증서 만료 예정: 향후 30일 이내에 만료되는 X509 인증서의 총 수입니다.
- 생체 인식 스캐너/하드웨어 키 사용자: 생체 인식 스캐너 또는 하드웨어 키로 로그인한 총 사용자 수입니다.
- REST API의 액세스 정책 없음: REST API의 액세스 정책 없이 로그인한 총 사용자 수입니다.
- 웹 서비스 액세스 전용 플래그가 없는 통합 계정 사용: 통합 계정 없이 로그인하는 총 사용자 수 웹 서비스 액세스 전용 플래그가 활성화되었습니다.

이메일

외부에서 수신 중인 스팸 이메일과 관련된 데이터를 표시합니다.

스팸 이메일 은 하루에 수신되는 정크 메일 수를 나타냅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

익스포트

일반적으로 익스포트하는 데이터와 익스포트하는 사용자를 검색합니다.

- 총 익스포트: 사용자가 익스포트한 총 테이블 기록 수입니다.
- 분류된 익스포트: 익스포트된 테이블 기록의 총 수로, 할당된 데이터 분류로 요약됩니다.

통합 계정

에서 Now Platform생성된 통합 계정에 대한 추세를 봅니다.

통합 계정 대시보드에는 에서 Now Platform생성된 통합 계정에 대한 추세가 표시됩니다.

다음은 통합 계정의 메트릭에 대한 설명입니다.

- 총 통합 계정: 인스턴스의 통합 계정과 관련된 추세입니다.
- 활성 통합 계정: 인스턴스의 활성 통합 계정과 관련된 추세입니다.
- 비활성 통합 계정: 인스턴스에서 비활성 상태인 통합 계정의 총 수에 대한 추세입니다.

권한 있는 **ID**

권한 있는 ID가 있는 사용자의 메트릭과 관련된 데이터를 분석합니다.

이 대시보드는 권한 있는 ID 사용자와 관련된 데이터와 인스턴스에서의 활동을 표시합니다.

- 관리자 로그인: 관리자 역할의 사용자에 대한 총 로그인 횟수입니다.
- 가장: 가장자 역할을 가진 사용자가 수행한 총 가장 수입니다.
- 권한 상승: security_admin 역할을 가진 사용자가 수행한 총 보안 수준 상승 수입니다.
- ServiceNow 로그인: ServiceNow 직원의 총 로그인 횟수입니다.
- 관리자 사용자 추가됨: 관리자 역할이 부여된 총 사용자 수입니다.

권한 있는 사용자

권한 Now Platform있는 사용자(활성 및 비활성)의 추세선과 해당 활동을 .

권한 있는 사용자 개요 섹션에는 권한 있는 사용자(활성 및 비활성)와 그들의 활동에 Now Platform대한 추세선이 . 권한 사용자는 높은 보안 설정, 임포트 및 포털 사용자와 같은 기능에 액세스하기 위해 추가 역할을 할당받은 사용자입니다.

다음은 권한 있는 사용자에 대한 설명입니다.

- 총 사용자 수: 인스턴스의 총 사용자 수입니다.
- 활성 사용자: 인스턴스에서 세션을 시작한 총 사용자 수입니다.
- 비활성 사용자: 최근에 인스턴스에 로그인하지 않은 사용자입니다.
- 잠김 상태가 아닌 비활성 사용자: 최근에 로그인하지 않았지만 계정에 접근할 수 있는 사용자입니다.
- 잠긴 사용자: 계정에 인증할 수 없는 사용자입니다.
- 새 사용자: 최근에 인스턴스에 추가된 사용자입니다.
- 성공 로그인: 성공적으로 로그인한 사용자입니다.
- 실패한 로그인: 실패한 로그인 시도입니다.
- MFA의 보호를 받지 않는 로컬 로그인: MFA 없이 로그인한 사용자입니다.
- 사용자가 로그인하지 않음: 인스턴스에 로그인한 적이 없는 사용자입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 사용자가 지난 달 이후로 로그인하지 않음: 지난 30일 동안 로그인하지 않은 사용자입니다.
- 사용자가 지난 6개월간 로그인하지 않음: 지난 6개월간 로그인하지 않은 사용자입니다.
- 사용자가 지난 1년간 로그인하지 않음: 지난 1년 동안 로그인하지 않은 사용자입니다.
- 암호 재설정 필요: 암호를 재설정해야 하는 사용자입니다.
- 사용자의 암호 재설정 실패: 사용자당 암호 실패 횟수입니다.

세션 관리

사용자 세션과 관련된 메트릭과 세션의 잠금 빈도를 봅니다.

사용자

에서 총 사용자(활성 및 비활성)와 해당 활동에 Now Platform대한 추세선을 봅니다.

사용자 개요 섹션에는 총 사용자(활성 및 비활성)와 해당 활동에 Now Platform대한 추세선이 표시됩니다.

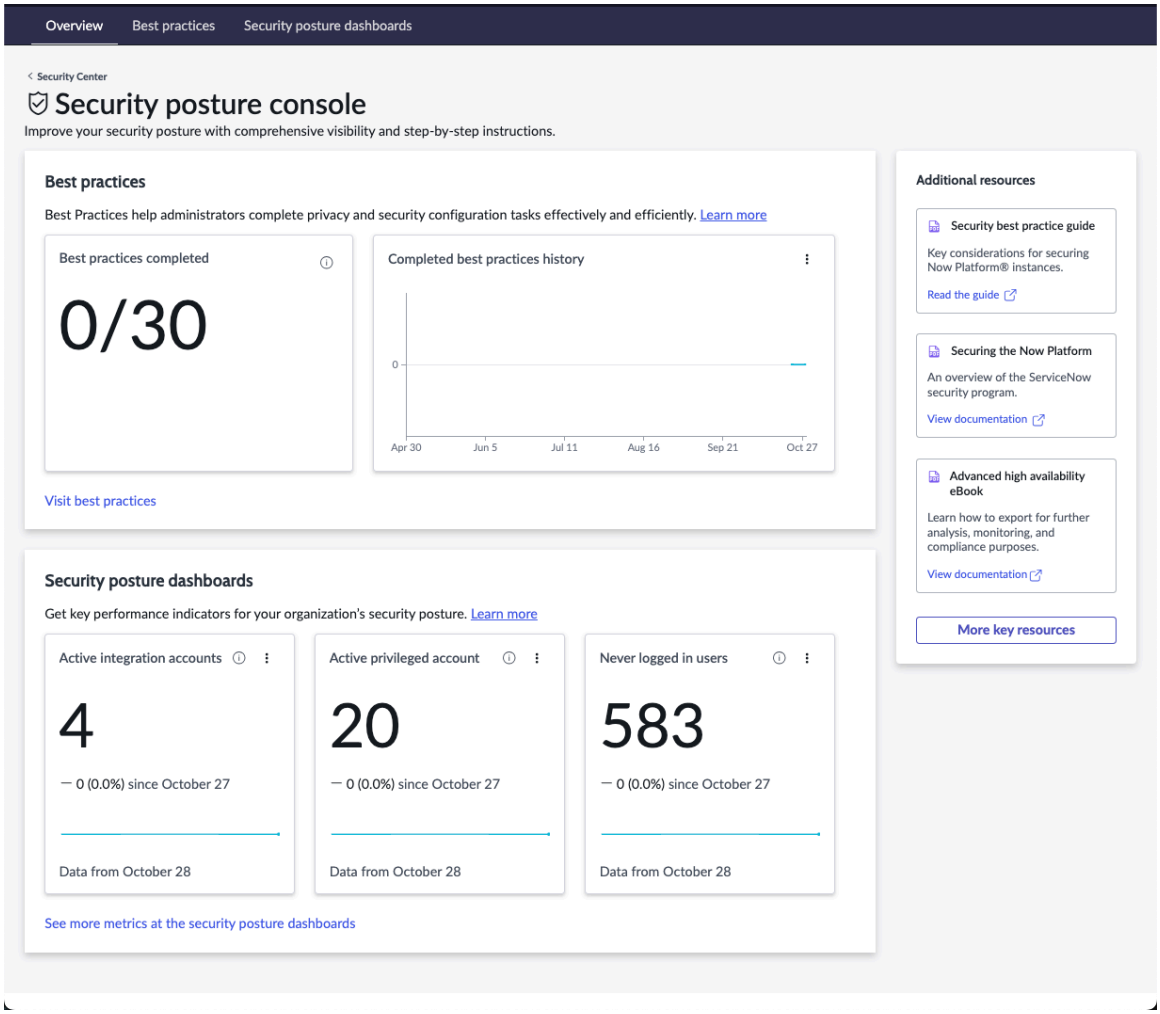
다음은 사용자 유형에 대한 설명입니다.

- 총 사용자 수: 인스턴스의 총 사용자 수입니다.
- 활성 사용자: 인스턴스에서 세션을 시작한 총 사용자 수입니다.
- 비활성 사용자: 최근에 인스턴스에 로그인하지 않은 사용자입니다.
- 잠김 상태가 아닌 비활성 사용자: 최근에 로그인하지 않았지만 계정에 접근할 수 있는 사용자입니다.
- 새 사용자: 최근에 인스턴스에 추가된 사용자입니다.
- 성공 로그인: 성공적으로 로그인한 사용자입니다.
- 실패한 로그인: 실패한 로그인 시도입니다.
- 외부 로그인: 외부 공급업체를 사용하는 인증입니다.
- MFA의 보호를 받지 않는 로컬 로그인: MFA를 사용하지 않는 로그인입니다.
- 사용자가 지난 달 이후로 로그인하지 않음: 지난 30일 동안 로그인하지 않은 사용자입니다.
- 사용자가 지난 6개월간 로그인하지 않음: 지난 6개월간 로그인하지 않은 사용자입니다.
- 사용자가 지난 1년간 로그인하지 않음: 지난 1년 동안 로그인하지 않은 사용자입니다.
- 암호 재설정 필요: 암호를 재설정해야 하는 사용자입니다.
- 사용자의 암호 재설정 실패: 사용자당 암호 실패 횟수입니다.

보안 태세 콘솔

포괄적인 가시성과 단계별 지침을 통해 보안 위협을 식별, 대응 및 복구하는 능력을 향상시킵니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 태세 콘솔은 베스트 프랙티스 및 보안 태세 대시보드에 대한 정보를 제공하는 섹션으로 나뉩니다. 이 섹션에서 카드를 선택하여 추가 상세 정보를 찾습니다. 페이지 맨 위에 있는 막대를 사용하여 이 페이지와 Security Center의 모범 사례 및 보안 태세 대시보드 섹션 사이를 이동할 수도 있습니다.

베스트 프랙티스

이 섹션에는 베스트 프랙티스 개수와 인스턴스에 적용한 개수가 표시됩니다. 시간 경과에 따라 완료된 베스트 프랙티스를 보여 주는 차트를 볼 수 있습니다.

보안 태세 대시보드

이 섹션에는 활성 통합 계정, 활성 권한 있는 계정 및 로그인한 적이 없는 사용자 수가 표시됩니다.

활성 통합 계정

통합 계정은 인스턴스와 외부 공급업체 애플리케이션 간의 통합을 관리하는 사용자 계정입니다.

활성 권한 있는 계정

권한 사용자는 높은 보안 설정, 임포트 및 포털 사용자와 같은 기능에 액세스하기 위해 추가 역할을 할당받은 사용자입니다.

로그인 기록이 없는 사용자

인스턴스에 로그인한 적이 없는 사용자 계정입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 자원

화면 가장자리의 추가 자원 섹션을 사용하여 학습 보안 센터와 관련된 설명서 및 비디오와 인스턴스 보안 관리에 대한 정보로 이동합니다.

보안 베스트 프랙티스

보안 베스트 프랙티스를 사용하여 ServiceNow 인스턴스에서 개인정보 보호 및 보안 구성 작업을 구현합니다.

보안 베스트 프랙티스를 사용하여 ServiceNow의 보안 제안을 검토하고, 보안 태세를 가장 잘 개선할 수 있는 제안을 식별하고, 구현 방법에 대한 단계별 지침을 따르십시오.

보안 베스트 프랙티스는 다음을 제공합니다.

- 홈페이지에는 보안 베스트 프랙티스 구현 진행 상황에 대한 개요가 표시됩니다. 조직의 목표에 따라 보안 베스트 프랙티스 목록을 구성하고 관리할 수도 있습니다.
- 개요 페이지에서는 각 보안 베스트 프랙티스에 대한 상세 정보, 구현 단계, 모든 활동 기록과 의견을 제공합니다.
- 작업 단계 페이지에서는 보안 베스트 프랙티스를 구현하는 방법에 대한 지침을 제공합니다.
- 활동 페이지에서는 보안 베스트 프랙티스와 관련된 사용자 및 시스템 작업의 이력을 추적합니다.

보안 베스트 프랙티스 홈페이지

홈페이지에는 전체적으로 완료된 보안 베스트 프랙티스의 총 수, 성숙 단계별로 완료된 베스트 프랙티스 수, 사용 가능한 모든 보안 베스트 프랙티스가 포함된 테이블을 나타내는 그래프가 포함되어 있습니다.

테이블을 사용하면 필터링된 목록을 정렬하고 저장할 수 있도록 필터를 적용할 수 있으며, 이를 다양한 사용 사례 또는 역할에 대한 작업 목록으로 사용할 수 있습니다. 자세한 내용은 필터링된 목록 저장을 참조하십시오.

다음은 보안 베스트 프랙티스 테이블과 관련된 필드에 대한 설명입니다.

보안 베스트 프랙티스 테이블에 사용되는 필드 요약

이름	설명
이름	보안 베스트 프랙티스를 식별하는 데 사용되는 단어입니다.
성숙 단계	측정 가능한 결과를 제공하기 위해 영향 순서에 따라 정렬된 애플리케이션 및 기능입니다. 성숙 단계 값은 다음과 같습니다. • 기초 빌드 • 사용자 환경 개선 • 기능 최적화 • 고급 기능 추가 이러한 단계는 기어가기, 걷기, 달리기, 날기 단계로 생각할 수도 있습니다.
상태	보안 베스트 프랙티스의 현재 상태:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 베스트 프랙티스 테이블에 사용되는 필드 요약

이름	설명
	• 오픈 • 진행 중 • 완료됨
우선순위	조직에서 보안 베스트 프랙티스를 구현하기 위한 중요도는 다음과 같습니다. • 즉시 • 나중에 • 해당 사항 없음
목표	보안 베스트 프랙티스가 해결하는 보안 범주: • 초기 보안 구성 해결 • 보안 이메일 • 모니터링 로그 • 접근 통제 관리 • 암호화로 보호 • 인스턴스를 최신 상태로 유지
최초 도입됨	보안 베스트 프랙티스가 도입된 Security Center 버전입니다.
변경됨	보안 베스트 프랙티스가 마지막으로 변경된 보안 센터 버전입니다.
제거됨	보안 베스트 프랙티스가 제거된 Security Center 버전입니다.

보안 베스트 프랙티스 개요 페이지

보안 베스트 프랙티스 테이블에서 보안 베스트 프랙티스를 선택하면 개요, 작업 단계 및 활동과 같은 하위 탭이 있는 페이지로 이동합니다.

개요 페이지 상단에서 우선순위, 성숙도 및 상태를 포함한 보안 베스트 프랙티스에 대한 일반 정보를 볼 수 있습니다.

우선순위 드롭다운 메뉴를 사용하면 현재 사용자에게 중요하지만 적용되지 않는 보안 베스트 프랙티스를 지정할 수 있습니다.

상세 정보 섹션은 보안 베스트 프랙티스와 관련된 기능에 대한 컨텐츠를 제공하며, 설명서 섹션은 추가 정보를 찾을 수 있는 하나 이상의 링크를 제공합니다.

오른쪽의 진행률 카드에는 완료된 단계 수와 포함된 총 단계 수가 표시됩니다. 완료되지 않은 다음 단계로 이동하려면 다음 단계로 이동을 선택합니다.

베스트 프랙티스 업데이트 이력 카드는 베스트 프랙티스에 대한 릴리스 정보의 스냅샷을 제공합니다. 보안 베스트 프랙티스가 릴리스된 ServiceNow Security Center 버전과 이후에 마지막으로 업데이트된 버전을 추적할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 베스트 프랙티스 작업 단계 페이지

하위 탭 작업 단계를 선택하면 보안 베스트 프랙티스를 구현하는 방법에 대한 단계별 지침을 제공하는 페이지로 이동합니다. 자세한 내용은 보안 베스트 프랙티스 완료를 참조하십시오.

보안 베스트 프랙티스 활동 페이지

활동은 가장 최근의 활동을 먼저 분석할 수 있도록 최신 활동부터 가장 오래된 것 순으로 나열됩니다. 활동에 대한 각 업데이트에는 타임스탬프가 지정되며 검색 및 필터를 사용하여 정보를 쿼리할 수 있습니다. 자세한 내용은 보안 베스트 프랙티스 테이블에 필터 적용을 참조하십시오.

보안 베스트 프랙티스 완료

ServiceNow 인스턴스에서 보안 베스트 프랙티스를 완료하는 방법에 대해 알아봅니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
ServiceNow 인스턴스에 보안 베스트 프랙티스를 구현하려면 다음 단계를 완료하십시오.

프로시저

1. ServiceNow 인스턴스에서 모두를 선택한 다음 베스트 프랙티스를 입력하여 보안 베스트 프랙티스에 액세스합니다.
2. 구현을 위한 보안 베스트 프랙티스를 보려면 필터를 적용합니다.
   a. UI에서 베스트 프랙티스 테이블로 이동합니다.
   b. 케밥 메뉴를 선택하거나 상태 열에 세 개의 세로 점(⋮)이 있는 항목을 선택합니다.
   c. 열기 및 진행 중 옵션을 선택한 다음, 적용을 선택합니다.
3. 구현할 보안 베스트 프랙티스의 이름을 선택합니다.
4. 다음 단계로 이동을 선택합니다.
5. 작업 단계 목록에서 작업 단계를 선택합니다.
6. 아래쪽 캐럿(v) 아이콘을 선택하여 해당 단계에 대한 구현 지침을 봅니다.
7. 지침을 읽은 다음 ServiceNow 인스턴스에 구현하십시오.
8. 작업이 완료되면 단계 완료 표시를 선택합니다.

   주: 나중에 다시 돌아오려고 하거나 조직의 목표에 적용되지 않는 경우 작업을 건너뛸 수 있습니다. 또한 작업 단계를 선택한 다음 단계 다시 시작을 선택하여 완료된 작업 단계를 다시 열 수 있습니다.

9. 베스트 프랙티스 완료를 선택합니다.

   언제든지 보안 베스트 프랙티스를 완료할 수 있습니다. 모든 단계를 완료할 필요는 없으며 건너뛰어도 괜찮습니다. 그러나 감사 참조에 대한 모든 단계를 완료하지 않은 경우에는 보안 베스트 프랙티스를 완료할 때 활동 하위 탭에 설명을 삽입하는 것이 좋습니다.

베스트 프랙티스의 활동 보기

활동을 시작한 사용자와 함께 ServiceNow 인스턴스에서 완료 중인 보안 베스트 프랙티스와 관련된 시간순 및 타임스탬프 기록을 추적합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. ServiceNow 인스턴스에서 모두를 선택한 다음 베스트 프랙티스를 입력하여 보안 베스트 프랙티스 관리자에 액세스합니다.
2. 베스트 프랙티스 테이블의 이름 열에서 활동을 보려는 보안 베스트 프랙티스를 선택합니다.
3. 활동 탭을 선택합니다.

   확인할 수 있는 활동의 예로는 보안 베스트 프랙티스의 상태가 '미결'에서 '완료'로 변경된 경우 또는 작업 단계가 완료되거나 건너뛰는 경우와 같은 필드 변경 내용이 있습니다. 또한 텍스트 상자에 설명을 입력하여 활동과 관련된 추가 정보를 입력할 수 있습니다.

완료된 베스트 프랙티스의 데이터 보기

완료된 베스트 프랙티스의 총량을 시각적으로 표현하거나 성숙 단계별로 분할합니다.

이 태스크 정보
작업을 완료하여 전반적으로 완료된 보안 베스트 프랙티스와 성숙 수준별로 시각적 추세를 제공하는 차트를 확인합니다.

프로시저

1. Security Center 앱에 액세스하고 모범 사례 탭으로 이동합니다.
2. 베스트 프랙티스 관리 카드에서 완료됨 전체 차트를 선택합니다.
3. 차트를 보고 완료된 보안 베스트 프랙티스 구성에 대한 추세를 확인합니다.
4. 성숙 단계별로 완료 됨을 선택하면 성숙 단계별로 완료된 베스트 프랙티스의 추세를 표시하는 차트가 표시됩니다.

보안 베스트 프랙티스 테이블에 필터 적용

필터를 적용하여 보안 베스트 프랙티스에 대해 더 관련성 높은 결과를 반환합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. ServiceNow 인스턴스에서 모두를 선택하고 베스트 프랙티스를 입력하여 Security Best Practices Manager에 액세스합니다.
2. 베스트 프랙티스 테이블로 이동하고 케밥 메뉴를 선택하여 필터를 적용할 필드를 선택하거나 세 개의 세로 점(⋮)이 있는 필드를 선택합니다.

필드	필터
이름	조건부 연산자를 텍스트 문자열과 결합하여 입력한 이름과 일치하는 보안 베스트 프랙티스를 반환합니다.
성숙 단계	필터를 적용하여 다음 성숙 단계 중 하나 이상과 일치하는 보안 베스트 프랙티스를 반환합니다. ◦ 기초 빌드 ◦ 사용자 환경 개선 ◦ 기능 최적화 ◦ 고급 기능 추가

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	필터
상태	필터를 적용하여 다음 상태 중 하나 이상과 일치하는 보안 베스트 프랙티스를 반환합니다. ◦ 비어 있음 ◦ 오픈 ◦ 진행 중 ◦ 완료됨
우선순위	필터를 적용하여 다음 우선순위와 일치하는 보안 베스트 프랙티스를 반환합니다. ◦ 비어 있음 ◦ 즉시 ◦ 나중에 ◦ 해당 사항 없음
목표	필터를 적용하여 다음 목표 중 하나 이상과 일치하는 보안 베스트 프랙티스를 반환합니다. ◦ 초기 보안 구성 해결 ◦ 인스턴스를 최신 상태로 유지 ◦ 접근 통제 관리 ◦ 모니터링 로그 ◦ 암호화로 보호 ◦ 보안 이메일 참고: 고급 필터는 기본적으로 목표에 적용됩니다. 수정하려면 다음을 선택하십시오. 변경 사항 적용 > 고급 뷰 > 필드 목표 선택 그런 다음, 나머지 조건을 작성하고 업데이트를 선택합니다.
최초 도입됨	조건부 연산자를 텍스트 문자열과 결합하여 입력한 버전과 함께 처음 도입된 베스트 프랙티스를 반환합니다.
변경됨	조건부 연산자를 텍스트 문자열과 결합하여 입력한 버전에서 변경된 보안 베스트 프랙티스를 반환합니다.
제거됨	조건부 연산자를 텍스트 문자열과 결합하여 입력한 버전에서 제거된 보안 베스트 프랙티스를 반환합니다.

나중에 사용할 수 있도록 필터 저장

나중에 재사용할 수 있도록 보안 베스트 프랙티스에서 필터를 저장하는 단계를 알아보십시오.

시작하기 전에

필요한 역할: 없음

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

보안 베스트 프랙티스 테이블에서 필터를 생성한 후 다음에 인스턴스에 인증할 때 사용할 수 있도록 저장할 수 있습니다. 만들 수 있는 필터 유형에 더 많은 유연성을 원하는 경우 고급 필터를 적용할 수 있습니다.

프로시저

1. 필터 표시(필터) 패널 아이콘을 선택합니다.
2. 필터 대화 상자 패널에서 아래로 스크롤하여 고급 보기를 선택합니다.
3. 필드, 연산자 및 값을 포함하는 조건을 추가하여 필터를 구성합니다.
4. 필터 저장을 선택합니다.
5. 필터 이름을 입력합니다.
6. 사용 권한을 선택합니다.
7. 저장을 선택합니다.
8. 업데이트를 선택하여 저장된 필터를 보안 베스트 프랙티스 테이블에 적용합니다.

저장된 필터 사용

보안 베스트 프랙티스를 위해 저장한 필터를 사용하는 단계를 살펴봅니다.

시작하기 전에

필요한 역할: 없음

이 태스크 정보

인스턴스에서 로그아웃하면 필터가 기본 설정으로 재설정됩니다. 다음 단계에서는 저장된 필터를 검색하여 보안 모범 사례 테이블에 다시 적용하는 방법을 보여 줍니다.

프로시저

1. 필터 패널 표시( ) 아이콘을 선택합니다.
2. 필터 대화 상자에서 아래로 스크롤하여 고급 보기를 선택합니다.
3. 기존 필터 사용을 선택한 다음, 드롭다운 목록에서 저장된 필터를 선택합니다.
4. 업데이트를 선택하여 저장된 필터를 적용합니다.

보안 태세 대시보드

사용자 지정 가능한 단일 및 멀티 인스턴스 보안 태세 대시보드를 사용하여 보안 KPI를 모니터링합니다. 이러한 대시보드는 인스턴스의 보안과 관련된 중요한 정보를 단일 위치에 통합하며 여러 기본 시스템 대시보드 위젯을 포함합니다.

보안 태세 대시보드에 액세스

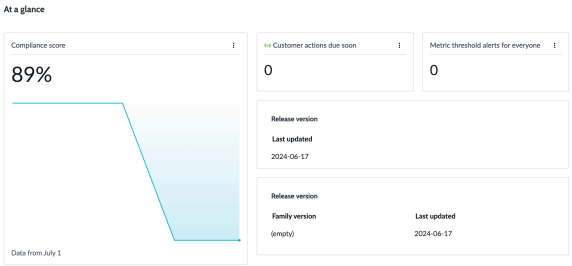
다음으로 이동하여 보안 태세 대시보드에 액세스합니다. 모두 > 보안 센터. 보안 태세 대시보드 콘텐츠는 개요 탭에 있습니다.

대시보드 구성요소

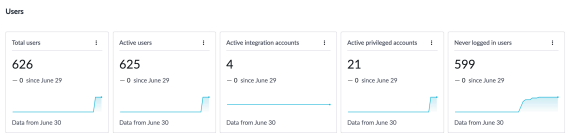
대시보드는 인스턴스 보안의 측면과 관련된 위젯을 포함하는 여러 섹션으로 나뉩니다. 대시보드에서 위젯을 선택하여 인스턴스 보안의 이 측면에 대한 자세한 내용을 봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

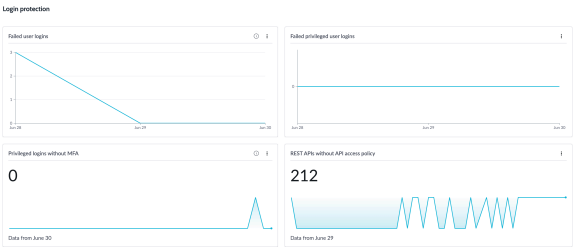
개요 섹션에는 준수 점수, 기한 고객 작업, 인스턴스에 대한 업데이트 및 릴리스 정보 등 인스턴스의 보안에 대한 개요가 표시됩니다.



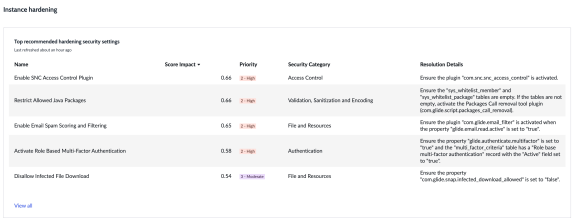
사용자 섹션은 인스턴스의 사용자에 대한 정보를 제공합니다. 이 섹션의 위젯에는 사용자 정보와 시간이 지남에 따라 이 정보의 변경 내용을 보여주는 선 그래프가 표시됩니다. 자세한 내용을 보려면 위젯을 선택하십시오.



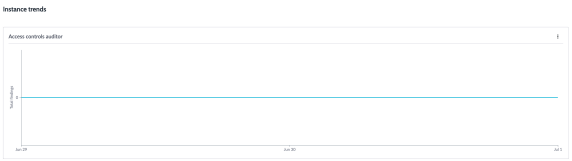
로그인 보호 섹션에는 권한 있는 사용자에 대한 실패한 로그인 시도를 포함하여 실패한 로그인에 대한 정보가 포함되어 있습니다.



인스턴스 강화 섹션에는 인스턴스 보안을 개선하기 위해 변경할 수 있는 권장 강화 보안 설정이 포함되어 있습니다. 이 섹션을 사용하여 이러한 변경의 우선순위와 잠재적 영향을 확인합니다.



인스턴스 추세 대시보드에는 접근 제어 감사자 스캔 도구 모음의 결과가 표시됩니다.

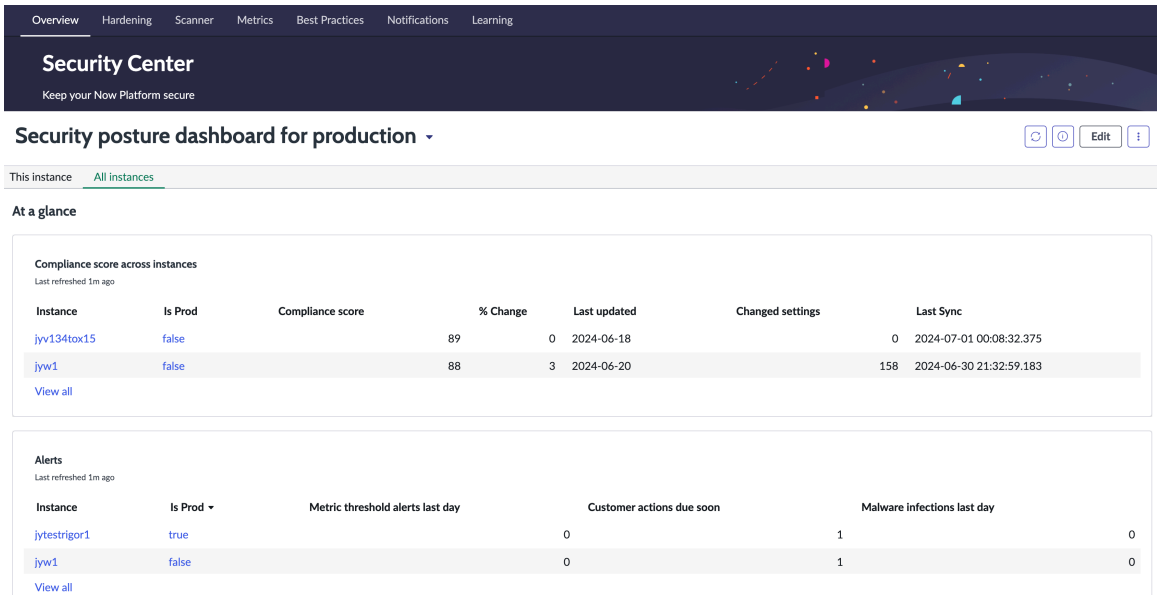


데이터 보호 섹션을 사용하여 PII(개인 식별 정보)와 같은 분류된 데이터에 대한 개요를 확인합니다. 대시보드는 또한 분류된 데이터의 내보내기를 추적합니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

여러 인스턴스 검토



대시보드 맨 위에 있는 모든 인스턴스 탭을 사용하여 프로덕션 인스턴스에서 나가지 않고도 비프로덕션 인스턴스의 보안 상태를 확인합니다. 모든 인스턴스 탭에는 이 인스턴스 탭과 동일한 정보의 요약 버전이 표시되지만, 모든 비프로덕션 인스턴스의 데이터도 포함됩니다.

기본적으로 모든 인스턴스 탭에는 로그인한 프로덕션 인스턴스와 모든 프로덕션 환경의 모든 비프로덕션 인스턴스에 대한 정보가 표시됩니다.

신뢰 구성을 수정하여 이 대시보드에 나타나는 인스턴스를 추가하거나 제거할 수 있습니다. 인스턴스 간에 데이터 가시성을 제공하면 인스턴스 간에 인스턴스를 대시보드에 표시할 수 있습니다. 이 프로세스에 대한 자세한 내용은 데이터 동기화 애플리케이션에 대한 기본 신뢰 구성 문서를 참조하십시오.

대시보드 커스터마이제이션

인스턴스 보안 태세 대시보드는 사용자 지정할 수 없지만 추가 작업 (추가 ⋮) 아이콘을 선택하고 복제를 선택하여 대시보드를 복제할 수 있습니다. 중복 대시보드를 변경할 수 있습니다.

보안 학습

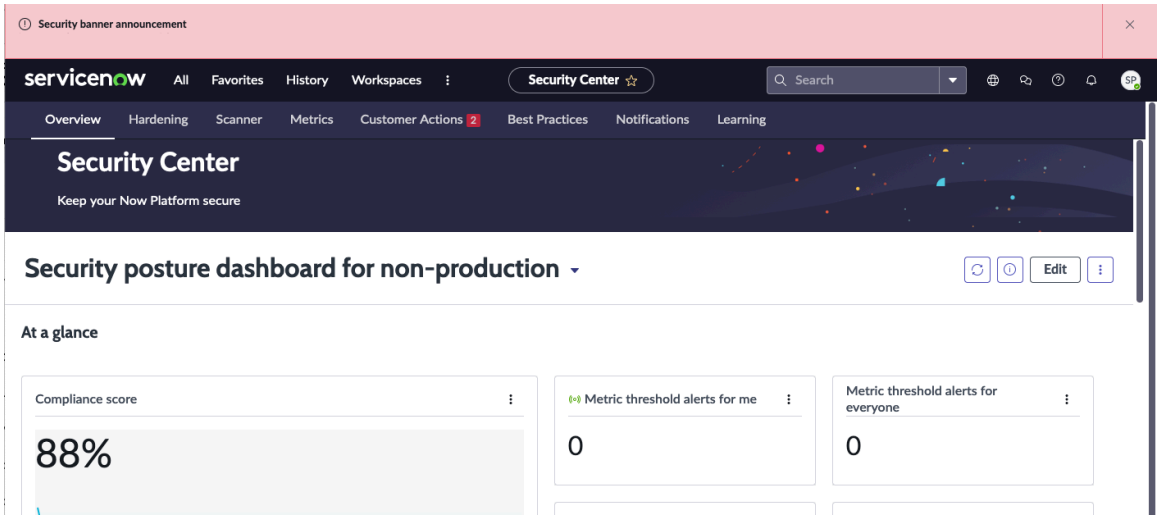
단일 페이지에서 보안 학습 자료에 액세스합니다.

학습으로 이동하여 통합 뷰에서 보안 백서, 전자책, 지식베이스(KB) 문서, 제품 설명서 및 커뮤니티 토론 내용을 읽을 수 있습니다. 콘텐츠는 제목과 설명이 포함된 UI 카드로 구성되어 있어 올바른 자원을 빠르게 찾아낼 수 있습니다.

보안 배너 공지

인스턴스 UI 내에서 관리자가 볼 수 있는 가시성이 높은 배너를 사용하여 보안 배너 공지를 활성화하여 긴급하고 중요한 보안 경보에 대한 정보를 지속적으로 받습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

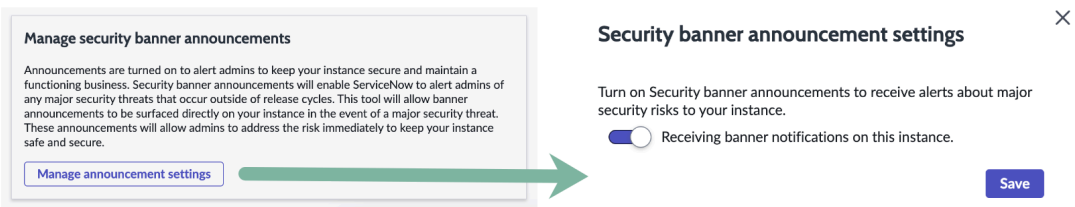


보안 배너 공지는 최근에 발견된 잠재적인 보안 위협에 대한 수정 사항을 지속적으로 알려 주기 위해 ServiceNow고객 관리자에게 표시되는 공지입니다. 이러한 경보에는 보안 위험에 대한 요약과 더불어 인스턴스에 대해 자세히 알아보고 조치를 취할 수 있는 링크가 포함되어 있습니다.

관리자는 닫기(x) 버튼을 선택하여 배너를 해제할 수 있지만 배너 만료 날짜가 지날 때까지 새 세션이 있을 때마다 배너가 다시 나타납니다. 관리자는 sn_vsc.configure_customer_push_action 시스템 속성 값을 false로 설정하여 배너 공지를 비활성화할 수 있습니다.

보안 배너 공지 사용 또는 사용 안 함

보안 배너 기능은 기본적으로 사용하도록 설정됩니다. 보안 배너 공지를 활성화하거나 비활성화하려면 다음으로 이동하십시오. 시스템 보안 > 보안 센터 > 알림. 이 페이지에서 공지 설정 관리 버튼을 선택합니다.



인스턴스 보안 센터

인스턴스 보안 센터 내에서 인스턴스 보안 통제의 준수 수준을 모니터링하고, 보안 이벤트 모니터링 메트릭을 보고, 인스턴스 보안 설정을 구성하고 유지관리합니다. Instance Security Center는 여러 주요 보안 구성요소를 단일 통제 콘솔에 통합하여 인스턴스 기반 보안 이벤트를 탐지, 보호하고 그에 대응하는 데 도움이 됩니다.

인스턴스 보안 센터 개요

중요사항:

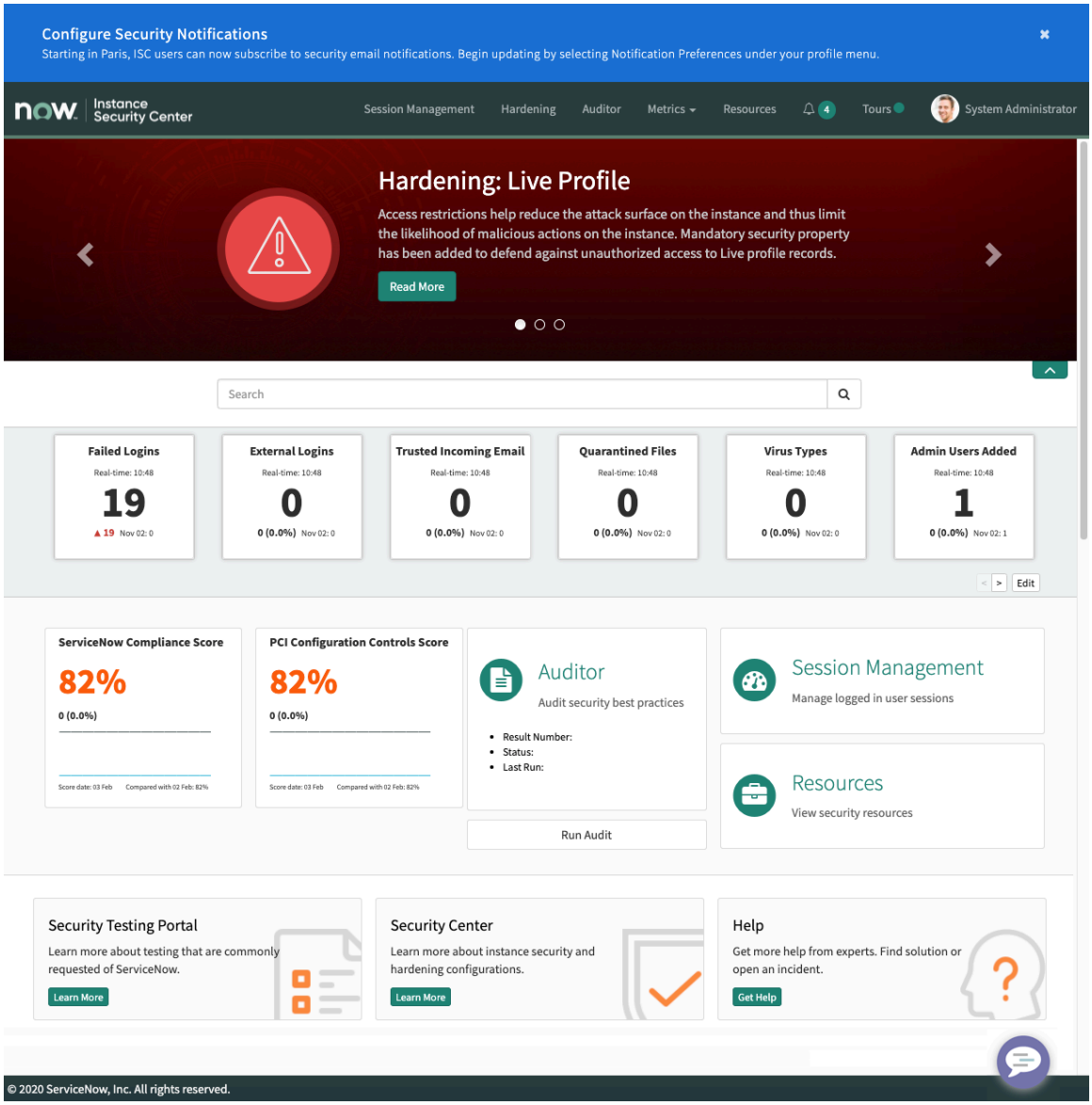
인스턴스 보안 센터(ISC)는 2024년 9월 현재 판매가 종료되었으며 더 이상 지원되지 않으며 새로운 활성화에 사용할 수 없습니다.

ServiceNow SSC(보안 센터)는 앞으로 권장되는 솔루션입니다. 자세한 내용은 마이그레이션으로 ServiceNow 보안 센터 인스턴스 보안 센터 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스 보안 센터 구성요소

인스턴스 보안 센터에 접근하려면 다음으로 이동하십시오. 시스템 보안 > 인스턴스 보안 센터 또는 시스템 관리 홈페이지를 참조하십시오.



인스턴스 보안 센터 홈페이지에는 다음과 같은 보안 구성요소가 포함되어 있습니다.

- 관리자 메시지
- 보안 배너 회전
- 검색
- 보안 이벤트 리본
- 일일 준수 점수
- PCI 구성 통제 점수
- 세션 관리
- 강화
- 감사자
- 메트릭(사용자, 이메일 및 바이러스 백신)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 자원
- 보안 알림
- 둘러보기
- 보안 테스트 포털
- 보안 센터
- 도움말
- 가상 에이전트 액세스

인스턴스 보안 센터 홈페이지에서 인스턴스의 보안 준수 점수를 확인하고 전반적인 보안 상태를 모니터링할 수 있습니다. 그런 다음 인스턴스 보안과 관련된 시스템 속성이 보안 요구 사항을 준수하도록 구성하거나 업데이트할 수 있습니다.

주: 인스턴스 보안 센터에서는 도메인 분리를 지원하지 않습니다.

사용자 역할

인스턴스 보안 센터를 사용하려면 관리자 또는 security_dashboard_user 역할이 있어야 합니다.

사용자별 구독 관리에 대한 자세한 내용은 계정 담당자에게 문의하여 에서 사용자별 구독 관리 구독 관리 문의하십시오.

역할

필요한 역할	사용자	복지
관리자	관리자는 ACL(접근 제어 목록) 규칙을 재정의하고 모든 역할 검사를 통과할 수 있기 때문에 이 역할은 모든 시스템 기능, 함수 및 데이터에 액세스할 수 있습니다. 더 많은 대상 역할을 사용할 수 있는 경우 사용자에게 이 역할을 할당하지 마십시오.	도구를 활용하여 보안 센터 인스턴스 보안 태세를 개선하고 보안 관련 동작을 모니터링합니다.
sn_vsc.보안_센터_뷰어	이 역할을 사용하면 관리자가 아닌 사용자도 도구의 정보를 보안 센터 볼 수 있지만 도구를 사용하여 보안 센터 인스턴스 구성을 변경하거나 변경할 수는 없습니다보안 센터. 예를 들어 플랫폼 소유자, 보안 운영 분석가 또는 규정 준수 이해 관계자는 에서 보안 센터사용할 수 있는 일부 보안 KPI, 보안 인사이트 및 보안 학습 자료를 보기를 원하거나 볼 필요가 있을 수 있습니다.	인스턴스 보안 태세를 모니터링하고 보안 동작을 모니터링하는 도구에 대한 보안 센터 가시성을 확보합니다.

경고: 인스턴스 보안 센터가 모든 업그레이드와 함께 최신 보안 정보를 받을 수 있도록 하려면 이 모듈을 사용자 지정하지 마십시오. 인스턴스의 보안 설정을 변경하는 경우 먼저 비프로덕션 환경에서 테스트해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관리자 메시지

주로 관리자를 위한 메시지와 미리 알림은 회전하는 보안 배너 위에 표시됩니다.

예를 들어 ## ## ## 메시지가 나타나 관리자가 보안 알림의 기본 설정을 구성하지 않은 경우 이를 상기시킵니다. 또한 그렇게 할 수 있는 적절한 페이지를 알려줍니다.

주: 관리자가 아닌 사용자의 경우 또는 관리자 사용자에 대한 실행 가능한 항목이 없는 경우 관리자 메시지 배너가 표시되지 않습니다.

보안 배너 회전

인스턴스의 보안 상태를 모니터링하는 데 도움이 되도록 중요한 인스턴스 보안 메시지가 회전하는 배너에 표시됩니다.

- 일반적으로 2-3개의 보안 메시지가 정기적으로 순환됩니다.
- 배너 아래쪽의 점은 현재 보안 메시지의 총 수를 보여 줍니다.
- 탐색하려면 점을 선택하거나 메시지의 양쪽에 나타나는 화살표를 선택합니다.

배너 배경색은 메시지의 상대적 심각도를 나타냅니다.

색상	설명
적색	적시에 응답해야 하는 중요한 보안 상황 또는 중요한 보안 이벤트를 보호하거나 이에 대응하는 방법에 대한 권장 사항.
진한 회색	중요하지 않은 경고 메시지입니다.
파랑	일반 정보 메시지입니다.

배너의 텍스트 컨텐츠를 축소하거나 최소화하려면 선택합니다 . 텍스트 콘텐츠를 최대화하려면 다시 선택합니다.

- 인스턴스 보안 센터를 다시 사용하면 이전 세션에서 사용한 방식에 따라 텍스트 콘텐츠가 축소되거나 확장된 상태로 나타납니다.
- 텍스트 내용 자체가 변경되면 모든 사용자에게 최대화된 것으로 나타납니다.

검색

검색 창을 사용하여 전체 인스턴스 보안 센터에서 보안 문제를 이해하고 해결하는 데 도움이 되는 보안 자원을 검색합니다. 다음 보안 관련 자원을 검색할 수 있습니다.

- Now Support 지식베이스 기사
- 인스턴스 보안 센터 페이지
- 외부 Now Support 링크
- 일일 준수 점수 및 외부 수신 이메일과 같은 PA 보안 위젯
- 배너 컨텐츠

이벤트 리본

이벤트 리본을 사용하여 현재 인스턴스에 대한 주요 보안 이벤트 모니터링 메트릭을 봅니다.

- 메트릭을 수동으로 스크롤하려면 오른쪽 또는 왼쪽 화살표 키를 선택합니다.
- 이벤트 리본을 구성하려면 편집을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이벤트 리본 및 이를 구성하는 방법에 대한 자세한 내용은 및 보안 이벤트 리본 구성을 참조하십시오보안 이벤트 모니터링.

일일 준수 점수

일일 준수 점수 섹션에는 일일 준수 점수, 세션 관리, 강화,감사자 및 자원 타일이 포함되어 있습니다.

일일 준수 점수를 사용하여 보안 관점에서 인스턴스가 얼마나 정상인지 측정할 수 있습니다.

일일 준수 점수는 백분율 점수입니다. 이는 인스턴스 보안 속성의 현재 설정이 에 게시된 강화 설정준수 값을 얼마나 준수하는지를 기반으로 합니다.

- 일일 준수 점수 계산 및 강화 설정이 미치는 영향에 대한 자세한 내용은 문서를 참조하십시오 일일 준수 점수를 확인하고 보안 속성 설정을 구성합니다..
- 새로 고침 버튼을 사용하면 관리자가 일일 준수 점수를 즉시 다시 계산할 수 있습니다. 자세한 내용은 일일 준수 점수, 추세 및 그래프 데이터를 새로 고치는 방법 문서를 참조하십시오.

강화

이 프로세스를 사용하여 일일 준수 점수에 영향을 주는 특정 보안 구성 속성을 조정합니다.

1. 강화 규정 준수 구성 페이지에 액세스하여 인스턴스 보안 강화를 수행하려면 일일 규정 준수 점수 타일 또는 강화 링크를 선택합니다.
2. 모든 보안 통제를 볼지 아니면 권장되는 보안 통제만 볼지 지정합니다. 그런 다음 작업하려는 범주를 선택합니다.
3. 선택한 범주에서 각 보안 구성 속성을 설정합니다. 속성에 대한 자세한 정보를 보려면 추가 정보를 클릭하십시오.

규정 준수를 더욱 강화하기 위해 보안 구성 속성을 강화하고 최적화하는 방법에 대한 자세한 내용은 문서를 참조하십시오 규정 준수를 강화하기 위해 인스턴스 보안 설정 조정.

추세 및 그래프 데이터를 새로 고치는 방법에 대한 자세한 내용은 을 참조하십시오 일일 준수 점수, 추세 및 그래프 데이터를 새로 고치는 방법.

감사자

감사자를 실행하여 인스턴스를 스캔하고 잘못된 보안 정의를 찾습니다. 인스턴스의 보안 태세를 개선하는 데 도움이 되도록 수정할 수 있는 결과를 제공합니다.

감사자 페이지에 액세스하려면 감사자 타일 또는 감사자 링크를 선택합니다. 자세한 내용은 잘못된 보안 정의 스캔 문서를 참조하십시오.

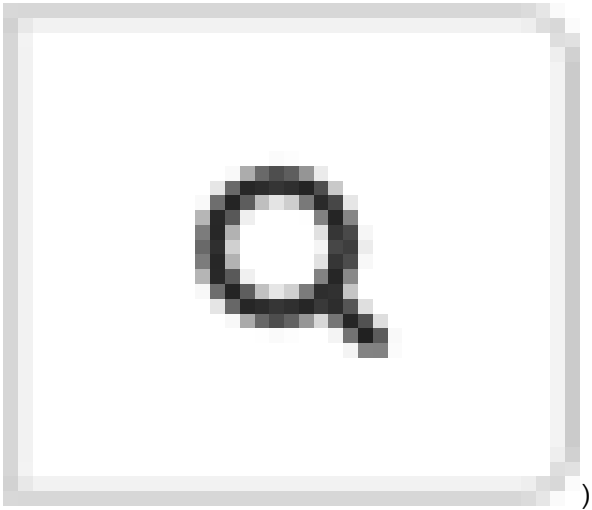
세션 관리

세션 관리를 사용하여 다음을 수행합니다.

- 사용자 로그인 세션을 보고 관리합니다.
- 연결된 현재 노드의 사용자 로그인 세션을 확인합니다.
- 사용자 이름 및 IP 주소와 같은 각 세션에 대한 자세한 정보를 참조하십시오.
- 보안 위험을 초래하는 특정 사용자 세션을 격리하고 잠급니다.

세션 관리 페이지에 액세스하려면 세션 관리 타일 또는 링크를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
사용자	이 로그인 세션과 연결된 사용자의 이름입니다. • 특정 사용자 세션을 찾으려면 스포트라이트 검색 아이콘()을 선택하여 사용자, 사용자 에이전트 키워드 또는 IP 주소로 검색합니다. 예를 들어, 특정 유형의 브라우저에서 모든 현재 로그인을 찾으려면 사용자 에이전트 필드에 브라우저 이름을 키워드로 입력합니다. • 사용자 이름을 클릭하여 사용자 프로파일 기록에 액세스합니다. 할당된 관리자 역할이 있는 경우에만 사용자 프로파일을 수정할 수 있습니다. 주: 사용자 프로필에 대한 자세한 내용은 사용자 만들기를 참조하세요.
MFA	로그인한 사용자에 대해 MFA(다단계 인증)가 활성화되어 있는지 여부를 나타내는 확인란입니다. MFA에 대한 자세한 내용은 다음 문서를 참조하십시오 다단계 인증(MFA).
활성	로그인한 사용자가 활성 상태인지 또는 비활성 상태인지를 나타내는 확인란입니다.
사용자 에이전트	사용자 로그인 세션의 브라우저 및 장치 운영 체제 유형입니다.
IP 주소	로그인한 사용자의 IP 주소입니다.
마지막 접근	이 사용자 세션이 마지막으로 인스턴스에 액세스한 날짜 및 시간입니다. 주: 특정 로그인 세션에 대한 자세한 정보를 보거나 세션 자체를 잠그려면 사용자 에이전트, **IP** 주소 또는 마지막으로 액세스 한 필드를 선택합니다.

메트릭

다음 유형의 메트릭에 대한 상세 정보를 봅니다.

메트릭 유형	설명
사용자	인스턴스의 사용자 활동과 연결된 보안 메트릭입니다. 사용자 메트릭 페이지에 액세스하려면 메트릭 링크를 선택한 다음, 사용자 메트릭을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

메트릭 유형	설명
익스포트	인스턴스에서 익스포트한 데이터와 연결된 보안 메트릭입니다. 메트릭 내보내기 페이지에 액세스하려면 메트릭 링크를 선택한 다음, 메트릭 내보내기를 선택합니다.
인증	자주 사용하지 않는 IP 주소, 실패한 로그인, 사용자가 사용하는 인증 체계 유형 등 인증과 연결된 보안 메트릭 메트릭 내보내기 페이지에 액세스하려면 메트릭 링크를 선택한 다음, 인증 메트릭을 선택합니다.
이메일	인스턴스로 들어오는 이메일과 관련된 예외 동작과 관련된 보안 메트릭입니다. 이메일 메트릭 페이지에 액세스하려면 메트릭 링크를 선택한 다음 이메일 메트릭을 선택합니다.
바이러스 백신	인스턴스의 바이러스 백신 이벤트 활동과 연결된 보안 메트릭입니다. 바이러스 백신 메트릭 페이지에 액세스하려면 바이러스 백신 타일을 선택하거나 메트릭 링크를 선택한 다음 바이러스 백신을 선택합니다.

주: 각 메트릭 유형을 모니터링하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 인스턴스 메트릭 모니터링.

자원

인스턴스 보안과 관련된 문서, 자원 및 블로그에 액세스합니다 Now Support 지식베이스 . 이러한 자원에는 보안 설정, 코딩, 규정 준수, 수정 사항 및 관련 주제가 포함됩니다. 자원 페이지에 액세스하려면 다음을 수행합니다.

1. 자원 타일 또는 링크를 클릭합니다.
2. 자원 페이지에서 범주를 선택합니다.

범주	설명
권장 지침	및 보안 코딩 가이드 [KB0623354] 문서를 포함한 강화 설정 권장 보안 지침에 액세스합니다.
보안 자원	를 포함한 보안 관련 자원 지식베이스에 대한 액세스: ◦ 고객 인스턴스 보안 테스트 ◦ 클라우드 보안, 신뢰 및 준수 센터 KB 문서

보안 알림

알림 벨 아이콘( )이 인스턴스 보안 센터에 표시되며 읽지 않은 보안 알림의 총 개수가 표시됩니다. 알림은 지속되며 읽음으로 표시할 때까지 이 개수에 포함됩니다.

1. 종 모양 아이콘을 클릭하면 읽지 않은 처음 5개의 보안 알림을 볼 수 있습니다.

   관리자 로그인, 관리자 잠금 해제, 실패한 로그인, 높은 권한 역할, 가장, 보안 상승 및 주간 다이제스트 이벤트가 인스턴스에서 발생할 때 알림이 나타납니다. 이러한 보안 이벤트에 대한 자세한 내용은 다음 문서를 참조하십시오 보안 이벤트 모니터링.

2. 특정 보안 이벤트에 대한 자세한 정보를 보려면 알림을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어, 높은 권한 역할 알림을 선택하면 역할(sys_user_role) 테이블을 볼 수 있습니다. 이 테이블을 사용하여 해당 날짜에 권한 있는 역할이 할당된 사용자를 확인합니다. 이 이력을 사용하면 역할이 제대로 할당되었는지 확인할 수 있습니다.

3. 읽지 않은 알림이 5개를 초과하는 경우 모든 알림 보기를 선택하여 읽지 않은 모든 알림 목록이 있는 모든 알림 페이지에 액세스합니다.
   - 특정 보안 이벤트에 대한 자세한 정보를 보려면 알림을 선택합니다.
   - 나열된 모든 알림을 읽음으로 표시하려면 모두 읽음으로 표시를 선택합니다.

주: 관리자는 각 보안 이벤트 유형에 대해 특정 유형의 알림을 보내는 기본 설정을 구성할 수도 있습니다. 자세한 내용은 보안 이벤트 알림에 대한 기본 설정 지정 문서를 참조하십시오.

둘러보기

둘러보기 링크를 클릭하여 인스턴스 보안 센터의 가이드가 있는 시각적 둘러보기를 봅니다.

- 가이드가 있는 둘러보기에는 홈페이지에 나열된 보안 모니터링 기능만 포함됩니다.
- 홈페이지에서 타일이나 링크를 선택할 때 액세스하는 보안 기능은 포함되지 않습니다.

보안 테스트 포털, 보안 센터 및 도움말

인스턴스는 Now Support 서비스 포털 인스턴스, 작업 및 계정을 관리하는 데 사용하는 중앙 자원입니다. 인스턴스의 보안 및 기술 문제를 진단하고 해결하는 데 사용할 수 있는 유용한 자원에 액세스할 수도 있습니다.

이러한 자원에 액세스하려면 다음 타일에서 자세히 알아보기 또는 도움 받기 를 선택합니다.

타일	설명
보안 테스트 포털	보안 테스트 포털에서 보안 대시보드에 Now Support 액세스합니다.
보안 센터	보안 포털에서 보안 규정 준수 Now Support 에 액세스.
도움말	보안 포털에서 다음 도움말 자원에 액세스합니다.Now Support • 전문가에게 질문하여 일반적인 질문에 대한 답변을 찾아보십시오. • 케이스를 열어 문제 또는 중단 ServiceNow 을 전역 기술 지원에 보고합니다. • 다음을 포함한 셀프 서비스 지원 자원: ◦ 비디오 ◦ 설명서 ◦ ServiceNow 커뮤니티 ◦ 지식베이스 ◦ 알려진 오류 포털 ◦ 보안 RFX 데이터베이스 • ServiceNow 커뮤니티 사용하는 것이 권장되는 질문입니다.

가상 에이전트 액세스

메시징 가상 에이전트 인터페이스 내에서 대화를 통해 사용자 지원을 제공하는 플랫폼입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연결된 플러그인이 설치되면, 관리자는 가상 에이전트 아이콘을 선택해 AND 자연어 이해 (NLU) 기능에 접근할 가상 에이전트 수 있습니다.



이를 통해 다음 작업을 수행할 수 있습니다.

- 보안 관련 질문을 한 다음, 빠른 요약 답변과 참조 링크를 받아 자세히 알아보십시오.
- 다음과 같은 프로세스와 관련된 답변을 얻을 수 있습니다.
  - 인스턴스 보안 센터
  - 플랫폼 보안
  - ServiceNow 보안 정책
  - 신뢰, 거버넌스 및 위험
- 보안 포털의 Now Support 주제와 같은 지식베이스 보안 관련 자원을 검색합니다.

주: 를 가상 에이전트사용하고 활성화하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 가상 에이전트
- ISC 가상 에이전트 인터페이스 활성화

마이그레이션으로 **ServiceNow** 보안 센터 인스턴스 보안 센터

인스턴스 보안 센터(ISC)에서 (SSC)로 마이그레이션할 때의 ServiceNow 보안 센터 주요 차이점에 대해 알아봅니다.

중요사항:

Instance Security Center는 2024년 9월까지 판매가 종료되는 레거시 제품입니다. ServiceNow Security Center는 고객이 향후 채택할 것을 권장하는 솔루션입니다. 자세한 내용은 Now Support 지식베이스의 사용 중단 프로세스 문서(KB0867184)를 참조하십시오.

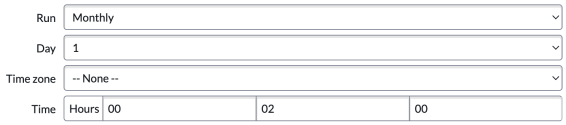
ServiceNow 보안 센터 (SSC)는 조직이 배포의 ServiceNow 보안을 유지관리할 수 있도록 설계된 특수 목적의 도구 세트로 구성된 보안 애플리케이션입니다. SSC를 사용하여 조직은 보안 태세를 개선하고 규정 준수 수준을 강화하며 원활한 사용자 경험을 통해 이를 수행할 수 있습니다.

이 문서를 사용하여 SSC의 기능 향상에 대해 알아보고 이전에 ISC에서 수행했던 작업을 SSC에서 실행하는 방법에 대해 알아봅니다.

보안 강화

기능 개선 사항	**ISC** 대 **SSC**
사용자 상호작용 업데이트	• 개요 또는 강화 비교 페이지로 이동하여 최신 점수를 검토합니다. • 개요로 이동하고 점수 업데이트를 선택하여 최신 점수를 수동으로 업데이트합니다. • 다음 페이지에서 설정 이름 링크를 선택하여 설정 구성을 변경한 다음 설정 상세 페이지에서 편집합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기능 개선 사항	ISC 대 SSC
	◦ 개요 ◦ 강화 > 모든 설정 ◦ 강화 > 비교
규정 준수 점수를 다시 계산하기 위한 일정 설정	SSC를 사용하면 시스템이 준수 점수의 새로 고침을 트리거하는 시기를 설정할 수 있습니다. **1.** 예약된 스크립트 실행 [sysauto_script] 테이블로 이동합니다. **2.** `SC - ## ## ##` 기록을 찾아서 엽니다. **3.** 실행, 요일, 시간대 및 시간 필드를 사용하여 원하는 일정을 설정합니다.  **4.** 업데이트를 선택하여 변경 내용을 저장합니다.

보안 **KPI** 및 메트릭

기능 개선 사항	ISC 대 SSC
KPI 개선 사항	SSC를 사용하여 다음을 수행할 수 있습니다. • 시간 경과에 따른 점수 추세를 확인합니다. • 동일한 인터페이스 및 분석 기능을 사용하여 모든 KPI와 메트릭을 모니터링합니다.
메트릭 개선 사항	SSC에는 다음과 같은 메트릭 개선 사항이 포함되어 있습니다. • 65개 이상의 지표가 추가되었습니다. • 단일 사용자 인터페이스에서 KPI와 메트릭을 모니터링하고 분석합니다. • 메트릭의 대상 및 임계치를 생성합니다.
사용자 상호작용 업데이트	다음으로 이동하여 SSC의 메트릭에 액세스 개요 > 메트릭을 클릭한 다음 탐색 메뉴에서 메트릭을 선택합니다. 또는 모든 메트릭으로 이동할 수 있습니다.

보안 스캐너

기능 개선 사항	ISC 대 SSC
새 기능	SSC에는 다음과 같은 기능이 포함되어 있습니다. • 스캔을 수동으로 실행하거나 특정 시간에 실행되도록 예약합니다. • 스캔 검사를 직접 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기능 개선 사항	ISC 대 SSC
	• 스캔 도구 모음을 직접 만듭니다. • 두 스캔의 결과를 비교합니다.
향상된 이메일 기능	이메일 알림을 설정하여 인스턴스의 보안 이벤트에 대한 최신 정보를 받습니다.
사용자 상호작용 업데이트	• 다음으로 이동하여 감사자 스캔을 실행합니다. 개요 > 스캔 > 도구 모음을 클릭하고 목록에서 감사자 제품군 을 선택합니다. • (으)로 이동하여 스캔 결과를 확인하십시오. 개요 > 스캔 > 결과.

추가 보안 기능

기능 개선 사항	ISC 대 SSC
세션 기능 모니터링	• 를 사용하여 세션 활동을 시각화합니다 분석 허브 . • 로 이동하여 세션 활동 모니터링 메트릭 > 세션.
자원 찾기	에서 단일 페이지의 모든 학습 자원에 액세스 개요 > 학습.

기능 옵트아웃 보안 센터

인스턴스에서 기능을 비활성화 보안 센터 하려면 KB1702514: 인스턴스 보안 센터 구성요소를 비활성화하기 위한 지침(보안 센터를 사용하는 동안) 에 제공된 단계를 따르십시오.

보안 이벤트 모니터링

인스턴스의 이벤트 메트릭을 분석하여 잠재적인 보안 이벤트를 식별하고 방지할 수 있습니다.

중요사항:

인스턴스 보안 센터(ISC)는 2024년 9월 현재 판매가 종료되었으며 더 이상 지원되지 않으며 새로운 활성화에 사용할 수 없습니다.

ServiceNow SSC(보안 센터)는 앞으로 권장되는 솔루션입니다. 자세한 내용은 마이그레이션으로 ServiceNow 보안 센터 인스턴스 보안 센터 문서를 참조하십시오.

인스턴스 보안 홈페이지에 있는 이벤트 리본에서 이러한 메트릭과 수반되는 상세 정보를 분석하여 인스턴스의 잠재적인 보안 이벤트를 식별할 수 있습니다.

- 각 이벤트 메트릭에 대해 실시간 단일 점수 수가 나타나며, 이 인스턴스에서는 하루 동안 이벤트가 발생한 횟수를 나타냅니다. 이러한 단일 점수 보고서는 해당 이벤트가 발생할 때 자동으로 업데이트됩니다.
- 각 이벤트 메트릭에는 날짜 범위에 대한 규정 준수 추세 및 그래프 정보도 포함됩니다. 이 정보는 퍼포먼스 분석 작업을 실행할 때 매일 업데이트됩니다. 자세한 내용은 이벤트 추세 세부 정보 분석 섹션을 참조하세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이벤트 유형

다음 이벤트 유형 중 6개 이상을 모니터링할 수 있습니다. 이벤트가 6개 이상인 경우 이벤트 리본 아래의 왼쪽 또는 오른쪽 화살표를 사용하여 이벤트를 스크롤합니다. 이벤트 리본을 구성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 보안 이벤트 리본 구성.

알림 기본 설정	설명
관리자 로그인	이 인스턴스에서 할당된 관리자 역할이 있는 사용자가 하루 동안 시도한 로그인 횟수입니다.
관리자 사용자가 추가됨	달력 하루 동안 이 인스턴스에 추가된 관리자 역할을 가진 사용자 수입니다. 예를 들어 카운트가 10이지만 관리자 역할이 할당된 사용자 4명인 경우 인스턴스에 보안 문제가 있을 수 있습니다.
외부 수신 이메일	자세한 내용은 이메일 메트릭 문서를 참조하십시오.
외부 로그인	하루 동안 이 인스턴스에 로그인한 할당된 snc_external 역할을 가진 사용자 수입니다. 이러한 로그인은 일반적으로 유지관리, 지원, 컨설팅 또는 감사 목적으로 수행됩니다. 이 메트릭을 모니터링하면 외부 로그인 시도가 합법적이며 잠재적인 보안 문제가 아닌지 확인할 수 있습니다. 외부 사용자 역할 할당에 대한 자세한 내용은 다음 문서를 참조하십시오 명시적 역할.
실패한 로그인	하루 동안 이 인스턴스에서 실패한 로그인 시도 횟수입니다. 이 메트릭은 로그인하여 인스턴스 보안을 손상시키려는 시도가 이루어지고 있음을 나타낼 수 있습니다.
가장 정보	달력 하루 동안 이 인스턴스의 가장 로그인 수입니다. 사용자 가장에 대한 자세한 내용은 사용자 가장을 참조하십시오.
격리된 파일	하루 동안 이 인스턴스에서 실행 바이러스 백신 검사 했을 때 격리된 파일 수입니다. 격리된 파일 및 바이러스 백신 검사에 대한 자세한 내용은 및 바이러스 백신 검사를 참조하십시오바이러스 백신 메트릭.
보안 상승	보안 관리자가 하루 동안 할당된 사용자 역할을 높은 권한의 보안 역할로 변경하여 표준 사용자에 대한 보안을 상승시킨 횟수입니다. 이러한 높은 권한 보안 역할에는 oauth_admin, 관리자, security_admin 및 가장자가 포함됩니다. • 이 메트릭은 누군가가 권한 없는 사용자의 보안을 강화하려고 시도했을 수 있음을 나타냅니다. 이 메트릭만 사용하여 특정 보안 손상을 탐지하지 마십시오. 대신 이

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

알림 기본 설정	설명
	메트릭을 다른 메트릭을 확인하여 보안 손상이 발생했는지 확인해야 한다는 표시로 취급합니다. • 사용자 보안 향상에 대한 자세한 내용은 해당 상승된 권한 역할문서를 참조하십시오권한 있는 역할로 상승.
SNC 로그인	고객 서비스 및 지원 달력 하루 동안 하이홉 기술을 사용하여 이 인스턴스에 로그인한 직원 수입니다. 이러한 로그인은 일반적으로 유지관리, 지원, 컨설팅 또는 감사 목적으로 수행됩니다. 회사 직원 액세스를 제어하는 ServiceNow 방법에 대한 자세한 내용은 ServiceNow 액세스 제어를 참조하십시오.
스팸	자세한 내용은 이메일 메트릭 문서를 참조하십시오.
신뢰할 수 있는 수신 이메일	자세한 내용은 이메일 메트릭 문서를 참조하십시오.
신뢰할 수 없는 수신 이메일	자세한 내용은 이메일 메트릭 문서를 참조하십시오.
바이러스 유형	하루 동안 이 인스턴스에서 발생한 다양한 유형의 바이러스 백신 이벤트 수입니다. 바이러스 백신 이벤트 유형에 대한 자세한 내용은 바이러스 백신 메트릭을 참조하세요.

이벤트 추세 상세 정보 분석

이벤트 메트릭의 추세 상세 정보를 보려면 이벤트 수를 클릭하여 분석 허브 페이지에 액세스합니다. 인스턴스에 대해 표시되는 상세 정보는 메트릭 유형에 따라 다릅니다.

예를 들어 보안 대시보드 이벤트 로그 페이지에서 실패한 각 시도의 목록을 보려면 다음을 수행합니다.

- 실패한 로그인 메트릭을 선택합니다.
- 분석 허브 페이지에서 기록 표시를 클릭합니다.
- 실패한 로그인 시도 중 하나를 클릭합니다.
- 상세 정보에는 로그인을 시도한 사용자의 이름, IP 주소 및 액세스를 시도한 테이블 이름이 포함됩니다.

에서 이벤트 임계치 트리거 코어 UI 분석 허브 를 설정하거나 표시기의 점수 범위 내에서 특정 이벤트가 발생할 때 경보를 제공할 수 있습니다.플랫폼 분석 KPI 세부 정보 원하는 점수와 이벤트의 실제 점수 간의 차이를 시각화할 수 있는 대상을 설정할 수도 있습니다.

예를 들어 실패한 로그인 메트릭에 대해 임계치를 `10`으로 설정할 수 있습니다. 하루에 로그인 시도가 10회 이상 실패하면 특정 보안 담당자에게 경고가 전송됩니다. 하루에 10번의 로그인 실패가 분석 허브 발생하는 경우 시각적 강조 표시를 제공하는 유사한 대상을 설정할 수도 있습니다.

이벤트 리본 타일에 분석 허브 나타나는 추세 데이터와 그래프는 현지 시간으로 오전 2:00에 퍼포먼스 분석 작업이 실행된 후에 업데이트됩니다. 자세한 내용은 일일 준수 점수, 추세 및 그래프 데이터를 새로 고치는 방법 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

인스턴스 보안 센터

Now Intelligence

분석 허브

퍼포먼스 분석 대상 및 임계치

보안 이벤트 리본 구성

인스턴스 보안 추적과 관련된 이벤트만 운영에 포함하도록 인스턴스 보안 센터 홈페이지에서 보안 이벤트 리본을 구성합니다. 보안 이벤트 타일이 리본에 표시되는 순서를 변경할 수도 있습니다.

시작하기 전에

필요한 역할: security_dashboard_user 또는 admin

이 태스크 정보

보안 이벤트 리본은 처음에 전체 표준 보안 이벤트 집합으로 채워집니다. 조직과 관련이 없는 이벤트를 제거하여 사용자 지정할 수 있습니다.

- 예를 들어, 보안 문제가 내부 직원의 작업으로 인해 발생한 것으로 의심되는 경우 관리자 로그인, 추가된 관리자 사용자 및 보안 상승 이벤트 표시기를 포함합니다.
- 이러한 표시기는 관리자 역할이 있는 사용자가 로그인을 시도한 횟수와 관리자 사용자가 추가된 경우 보안 역할을 상승시키려고 시도한 횟수를 모니터링합니다.

주: 이벤트 리본에 나타나는 보안 이벤트 유형에 대한 자세한 내용은 문서를 참조하십시오 보안 이벤트 모니터링.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 인스턴스 보안 센터.
2. 이벤트 리본에서 편집 (< > Edit)을 클릭합니다.
   이벤트 편집 양식의 선택됨 열에는 이미 나열된 이벤트가 포함되어 있습니다.
3. 이벤트 리본에 보안 이벤트를 추가하려면 사용 가능 열에서 선택됨 열로 보안 이벤트를 이동합니다.
   이벤트가 리본에 나타나는 순서를 변경하려면 이벤트를 선택한 다음 위쪽 또는 아래쪽 화살표를 클릭하여 올바른 위치로 이동합니다.
   - 인스턴스 보안 센터 이벤트 리본에 나타나는 것과 동일한 순서로 이벤트를 배치합니다.
   - 사용 가능 열의 맨 위에 배치한 이벤트는 인스턴스 보안 센터 이벤트 리본의 왼쪽에서 시작하여 순차적으로 나타납니다. 열 아래쪽에 배치된 이벤트가 이벤트 리본의 오른쪽에 나타납니다.
4. 이벤트 리본에서 보안 이벤트를 제거하려면 다음을 수행합니다.
   - 선택됨 열의 이벤트 리본에서 제거할 보안 이벤트를 선택합니다.
   - 선택됨 열에서 사용 가능 열로 이동합니다.
5. 저장을 클릭합니다.

관련 정보

인스턴스 보안 센터

보안 이벤트 알림에 대한 기본 설정 지정

특정 보안 이벤트가 발생할 때 받을 알림 유형에 대한 기본 설정을 구성합니다. 각 유형에 대해 이메일, 푸시 알림 Now Mobile또는 또는 또는 Microsoft Teams와 같은 Slack 외부 공급업체 메시징 애플리케이션에서 알림을 받을지 여부를 지정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
외부 공급업체 메시징 애플리케이션이 보안 이벤트 알림을 보낼 수 있도록 하려면 메시징 알림(com.glide.notification.messaging) 플러그인을 활성화해야 합니다. 개별 사용자는 자신의 설정을 구성해야 합니다. 자세한 내용은 메시징 애플리케이션의 알림을 참조하십시오.

필요한 역할: admin.

프로시저

1. 인스턴스 보안 센터 홈페이지에서 프로파일 메뉴를 클릭한 다음 알림 기본 설정을 클릭합니다.

알림 기본 설정

알림 기본 설정	설명
관리자 로그인	할당된 관리자 역할을 가진 다른 사용자가 다른 IP 주소에서 이 인스턴스에 로그인할 때마다 선택한 유형의 알림을 보냅니다.
관리자 잠금 해제	높은 권한의 사용자에 대한 계정이 잠금 해제될 때마다 선택한 알림 유형을 보냅니다.
실패한 로그인	다른 사용자가 속성에 정의된 *glide.user.max_unlock_attempts* 시도 횟수보다 적게 이 인스턴스에 로그인하지 못할 때마다 선택한 유형의 알림을 보냅니다. 이 속성을 구성하지 않으면 기본값은 5입니다. 이 속성에 대한 자세한 내용은 다음 문서를 참조하십시오 실패한 로그인 시도에 대한 잠금 지정.
HP 역할 추가됨	다른 사용자에게 높은 권한 보안 역할(oauth_admin, 관리자, security_admin 및 가장자 역할 포함)이 부여될 때마다 선택한 유형의 알림을 보냅니다. 사용자 보안 향상에 대한 자세한 내용은 해당 상승된 권한 역할문서를 참조하십시오권한 있는 역할로 상승.
가장	다른 사용자가 사용자를 가장할 때마다 선택한 알림 유형을 보냅니다. 사용자 가장에 대한 자세한 내용은 사용자 가장을 참조하십시오.
보안 상승	이 인스턴스에서 다른 사용자가 보안 관리자 역할로 상승할 때마다 선택한 알림 유형을 보냅니다.
주간 다이제스트	선택한 알림 유형에 대한 주간 다이제스트를 보냅니다. 여기에는 다음이 포함됩니다. ◦ 일주일 동안 이 인스턴스에서 발생한 모든 보안 활동에 대한 요약입니다. ◦ 인스턴스의 현재 일일 준수 점수입니다.

2. 각 보안 이벤트 유형에 대해 적절한 확인란을 선택하여 보낼 알림 유형을 지정합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

각각에 대해 여러 알림 방법을 선택할 수 있습니다.

확인란	설명
이메일	이 유형의 보안 이벤트에 대한 이메일을 보냅니다.
여유 시간	를 통해 Slack이러한 유형의 보안 이벤트에 대한 알림을 전송합니다. 주: 이 열은 에 Now Platform대한 통합을 설정한 Slack 경우에만 나타납니다.
팀	를 통해 Microsoft Teams이 보안 이벤트에 대한 알림을 전송합니다. 주: 이 열은 에 Now Platform대한 통합을 설정한 Microsoft Teams 경우에만 나타납니다.
푸시	이 유형의 보안 이벤트에 대해 푸시 알림을 보냅니다 Now Mobile . 주: 이 열은 에 처음 로그인하는 Now Mobile경우에만 나타납니다.
모두 저장	모든 유형의 보안 이벤트에 대해 특정 유형의 알림을 선택합니다. 예를 들어 각 보안 이벤트 유형에 대한 이메일 알림을 받으려면 이메일 위에 있는 모두 선택을 클릭합니다.

3. 저장을 클릭합니다.

일일 준수 점수를 확인하고 보안 속성 설정을 구성합니다.

일일 준수 점수 메트릭 및 보안 구성 속성을 검토하여 인스턴스가 제안된 보안 요구 사항을 준수하는지 확인합니다. 강화 준수 구성 페이지에서 미준수 보안 속성을 업데이트하여 일일 준수 점수에 영향을 줄 수 있습니다.

중요사항:

인스턴스 보안 센터(ISC)는 2024년 9월 현재 판매가 종료되었으며 더 이상 지원되지 않으며 새로운 활성화에 사용할 수 없습니다.

ServiceNow SSC(보안 센터)는 앞으로 권장되는 솔루션입니다. 자세한 내용은 마이그레이션으로 ServiceNow 보안 센터 인스턴스 보안 센터 문서를 참조하십시오.

일일 준수 점수는 백분율 점수입니다. 이는 인스턴스 보안 속성의 현재 설정이 에 게시된 강화 설정준수 값을 얼마나 준수하는지를 기반으로 합니다.

인스턴스의 일일 준수 점수를 정기적으로 검토합니다. 일일 준수 점수를 평가할 때 다음 지침을 따르십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 90%보다 크거나 같으면 인스턴스가 중요한 보안 제어를 준수함을 나타냅니다.
- 50%보다 크거나 같고 90% 미만이면 보안 준수 수준이 보통임을 나타냅니다.
- 50% 미만은 낮은 수준의 보안 준수를 나타냅니다.

규정 준수를 강화하기 위해 인스턴스 보안 설정 조정

강화 준수 구성 페이지를 사용하여 인스턴스의 일일 준수 점수에 영향을 주는 미준수 보안 속성을 강화하고 최적화합니다. 이를 사용하면 인스턴스가 게시된 보안 강화 표준을 준수하는 동시에 회사의 보안 요구 사항을 이행할 수 있습니다.

시작하기 전에

필요한 역할: security_dashboard_user 또는 admin

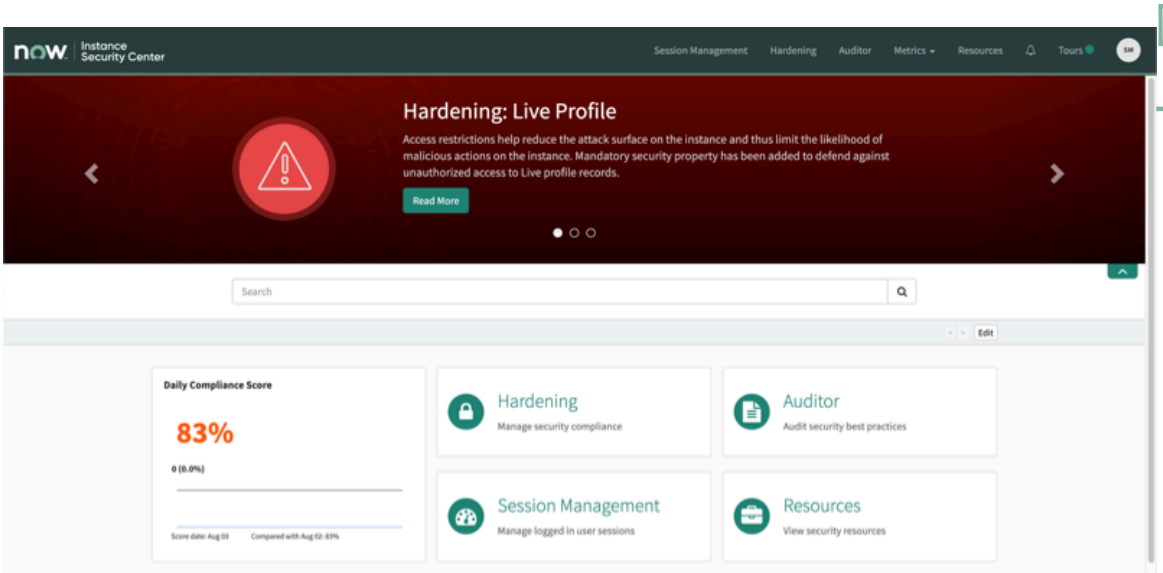
보안 관련 시스템 속성 및 플러그인에 대한 자세한 설명과 준수 값은 컨텐츠를 Now Platform참조하십시오강화 설정.

- 일부 준수 값이 인스턴스에 적합하지 않더라도 보안 관련 속성을 설정하거나 업데이트할 때마다 인스턴스 보안 강화 설정을 참조하십시오.
- 이러한 속성을 업데이트할 때 인스턴스가 계속해서 예상대로 작동하는지 확인합니다. 보안 영향을 결정할 수 있는 전문 지식을 갖춘 적절한 내부 직원과 상의하십시오.

주: 관리자 역할이 있는 경우 보안 제어를 보고 편집할 수 있습니다. security_dashboard_user 역할이 있는 경우 보안 제어를 볼 수 있지만 편집할 수는 없습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 인스턴스 보안 센터.
2. 일일 준수 점수 타일 또는 강화 링크를 클릭하여 강화 준수 구성 페이지에 액세스합니다.

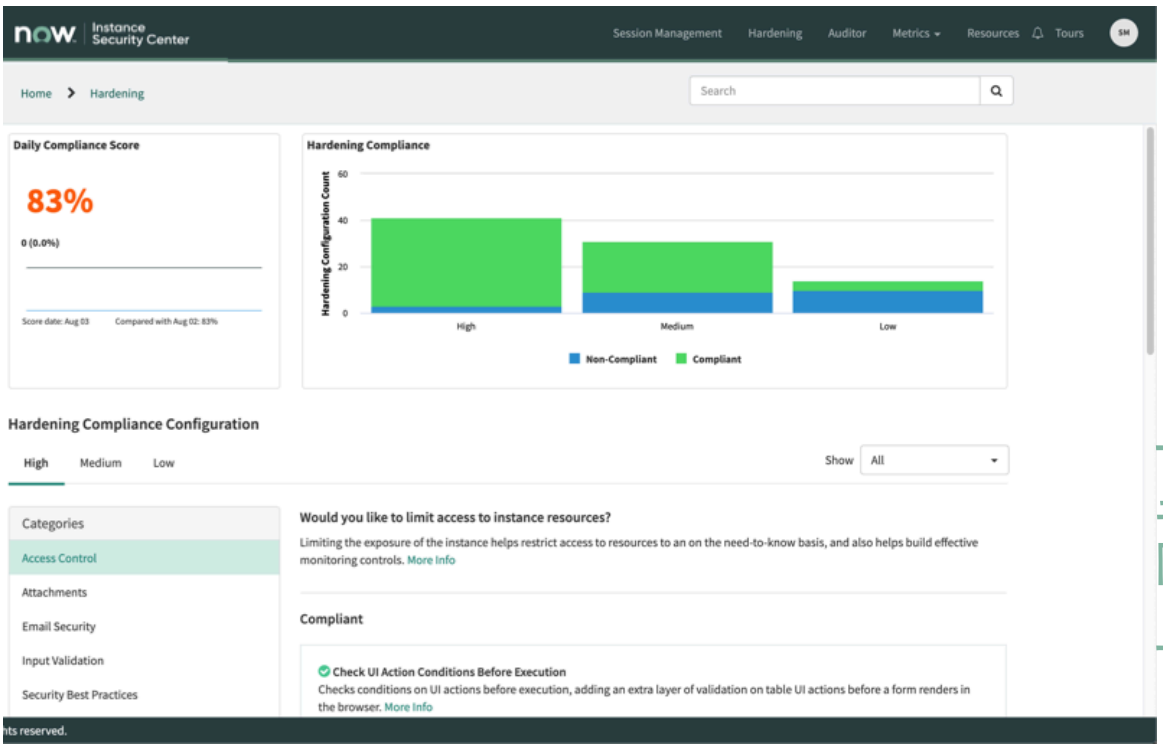


3. 강화 준수 차트에서 준수 및 미준수 보안 구성 속성에 대한 통계를 봅니다.

옵션	설명
규정 준수	인스턴스 보안 강화 설정의 준수 값을 준수하는 보안 구성 속성 수입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	주: 강화 준수 구성에서 준수 보안 속성에 대한 설정을 변경할 수 없습니다. 이렇게 하려면 시스템 속성에서 업데이트해야 합니다. 자세한 내용은 시스템 속성 추가를 참조하십시오.
비준수	인스턴스 보안 강화 설정의 준수 값을 준수하지 않는 보안 구성 속성 수입니다. 미준수 속성에 대한 설정을 업데이트할 수 있습니다.



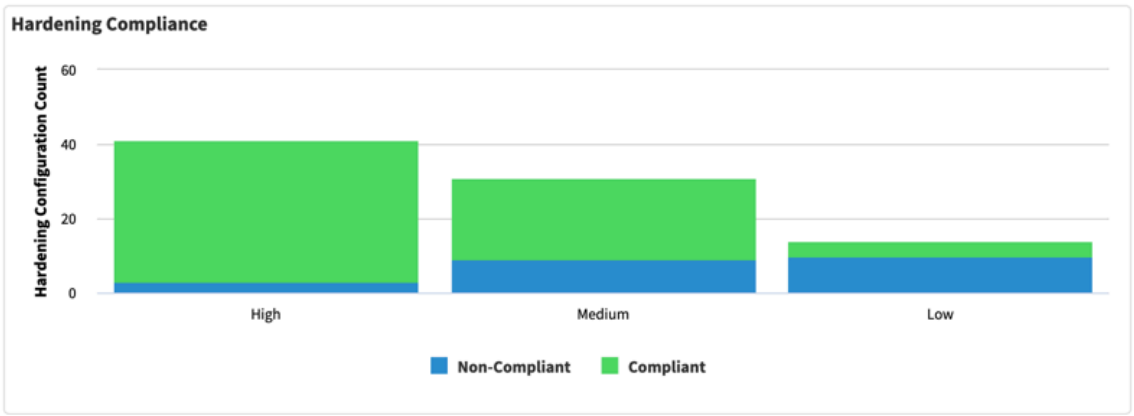
주: 날짜 범위에 대한 규정 준수 또는 비준수 보안 점수 수를 보려면 일일 규정 준수 점수 아래의 슬라이더에서 파란색 점을 이동합니다.

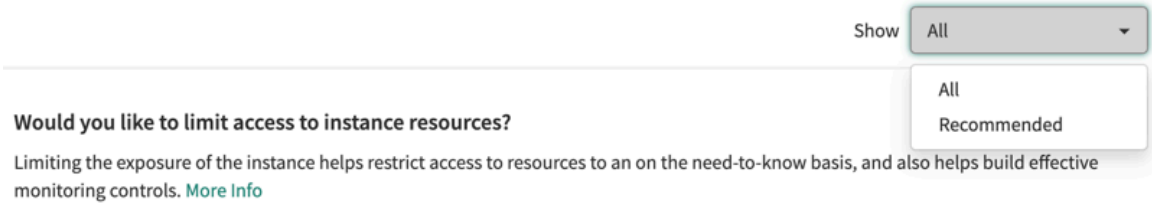
4. 차트 아래의 표시 목록에서 모든 보안 구성 속성에 액세스할지 또는 권장 속성에만 액세스할지 지정합니다.

옵션	설명
모두	(기본값) 선택한 각 범주의 모든 준수 및 미준수 보안 구성 속성입니다.
권장	선택한 각 범주에는 권장되는 보안 구성 속성만 표시됩니다. 이러한 보안 구성 속성은 보안을 유지하는 Now Platform에 사용되는 가장 중요한 속성의 선택된 하위 세트입니다. 이러한 보안 구성 속성은 보안을 Now Platform유지하기 위해 설정해야 하는 최소한의 설정 수로 간주합니다.

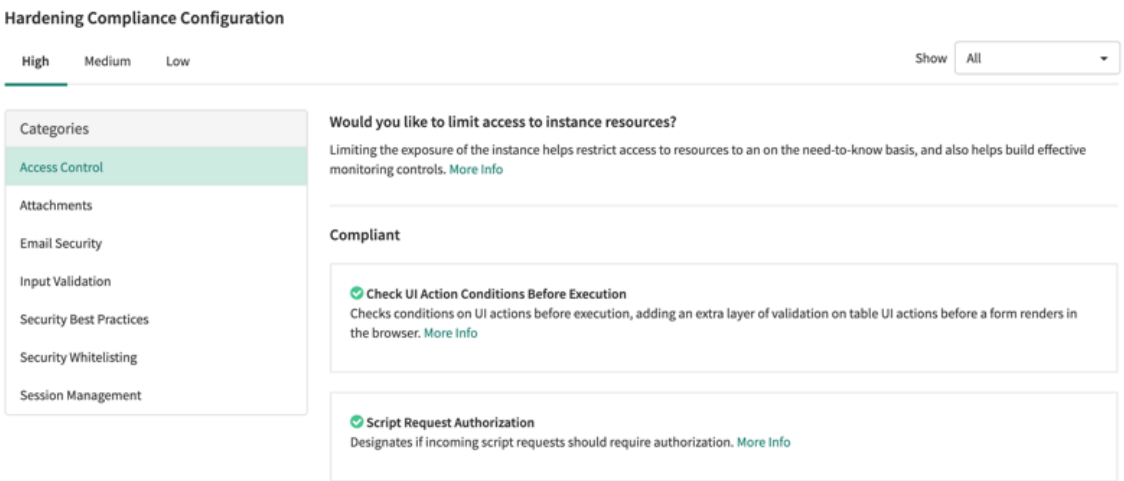
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	주: 인스턴스를 완벽하게 보호하려면 모두 옵션을 사용하십시오. 권장되는 모든 보안 구성 속성도 포함됩니다.





5. 범주에서 액세스하려는 보안 구성 속성이 포함된 범주를 선택합니다.



옵션	설명
접근 제어	접근 제어는 해당 자원을 사용할 수 있는 사용자에 따라 특정 자원에 대한 사용자 접근 권한을 부여할지 또는 거부할지를 결정합니다. 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 접근 통제 .
첨부 파일	첨부 파일 보안 제어를 사용하면 수신 첨부 파일을 확인하여 공격자가 보낸 악성 파일로부터

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	인스턴스를 보호할 수 있습니다. 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 AttachmentCreator SOAP Web Service에서 파일 MIME 형식 확인[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨〕.
이메일 보안	이메일 보안에는 관리자가 모든 인바운드 이메일에 대해 적절한 보안 정책이 마련되어 있는지 확인하기 위해 구성할 수 있는 보안 구성 속성이 포함됩니다. 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 전자 메일 스팸 점수 매기기 및 필터링 사용 [Security Center 1.3에서 업데이트됨〕.
입력 유효성 확인	입력 유효성 검사에는 소스에 관계없이 잘못된 형식의 데이터 항목을 최소화하도록 관리자가 구성할 수 있는 보안 관련 속성이 포함됩니다. 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 확인, 삭제 및 인코딩 .
보안 통신	보안 통신 속성은 관리자가 HTTP 트래픽의 전송을 보호하기 위해 구성할 수 있는 속성입니다. 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 커뮤니케이션 .
보안 베스트 프랙티스	보안 베스트 프랙티스는 관리자가 특정 시간 간격 내에 주기적으로 수행해야 하는 보안 작업을 포함하며 관련 구성 속성을 포함합니다. 자세한 내용은 강화 설정 문서를 참조하십시오.
보안 포함 목록	보안 포함 목록에는 관리자가 알려진 포함 목록으로 동작을 제한하도록 구성할 수 있는 보안 관련 속성이 포함됩니다.자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오.확인, 삭제 및 인코딩
세션 관리	세션 관리에는 관리자가 에서 보안 세션 관리를 Now Platform보장하기 위해 구성할 수 있는 보안 관련 속성이 포함됩니다.자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오.세션 관리

6. 선택한 범주에서 규정 미준수 보안 속성을 구성합니다.
   - 달리 지정하지 않는 한 스위치를 켜면 보안 속성이 권장 설정으로 설정됩니다. 예를 들어 대부분의 컨트롤은 true 또는 false로 설정하지만 일부 컨트롤은 값 또는 값을 입력해야 합니다(예: 쉼표로 구분된 값 목록).
   - 보안 제어에 대한 전용 인스턴스 보안 강화 설정 주제에 액세스하고 자세히 알아보려면 **[More Info**〕를 클릭하십시오.

결과
일일 준수 점수는 비준수 보안 제어 설정에 대한 변경 내용에 따라 증가하거나 감소합니다.

관련 정보

인스턴스 보안 센터

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일일 준수 점수, 추세 및 그래프 데이터를 새로 고치는 방법

인스턴스 보안 센터의 추세 및 그래프 데이터는 현지 시간으로 오전 2:00에 퍼포먼스 분석 작업이 실행된 후에 업데이트됩니다. 일일 준수 점수 타일, 이벤트 리본 타일, 분석 허브 이벤트 타일 중 하나를 클릭할 때 페이지 상세 정보에 나타납니다.

[AppSec] 일일 데이터 관리 작업은 야간에 실행되고 다음 작업을 수행하는 정기적으로 예약된 작업입니다.

1. 처음 예약할 때 유효한 사용자가 [AppSec] 일일 데이터 관리 및 [PA AppSec] 일일 데이터 수집 작업에 할당되었는지 확인합니다.
   - 실행 필드에 유효한 사용자를 입력한 경우 작업은 처리를 계속합니다. 유효한 사용자는 인스턴스에서 잠기지 않고 할당된 관리자 역할이 있는 사용자입니다.
   - 잘못된 사용자를 입력한 경우 인스턴스 보안 센터에서 회전하는 보안 배너 위에 오류 메시지가 나타납니다.

   주: 예약된 작업을 실행할 때 할당된 사용자를 업데이트하는 방법에 대한 자세한 내용은 데이터 수집 작업 만들기 또는 예약을 참조하십시오.

2. 강화 준수 구성 페이지에서 구성한 보안 속성의 준수 상태를 설정하는 비즈니스 논리를 실행합니다. 자세한 내용은 일일 준수 점수를 확인하고 보안 속성 설정을 구성합니다. 문서를 참조하십시오.
3. [PA AppSec] 일일 데이터 수집 퍼포먼스 분석 작업을 실행하여 준수 데이터를 수집하고 일일 준수 점수를 업데이트합니다.

일일 준수 점수를 수동으로 새로 고침

또는 할당된 관리자 역할이 있는 경우 새로 고침을 클릭하여 언제든지 일일 준수 점수를 새로 고치고 다시 계산할 수 있습니다.

주: 할당된 security_dashboard_user 역할이 있는 사용자에게는 새로 고침 버튼이 표시되지 않습니다.

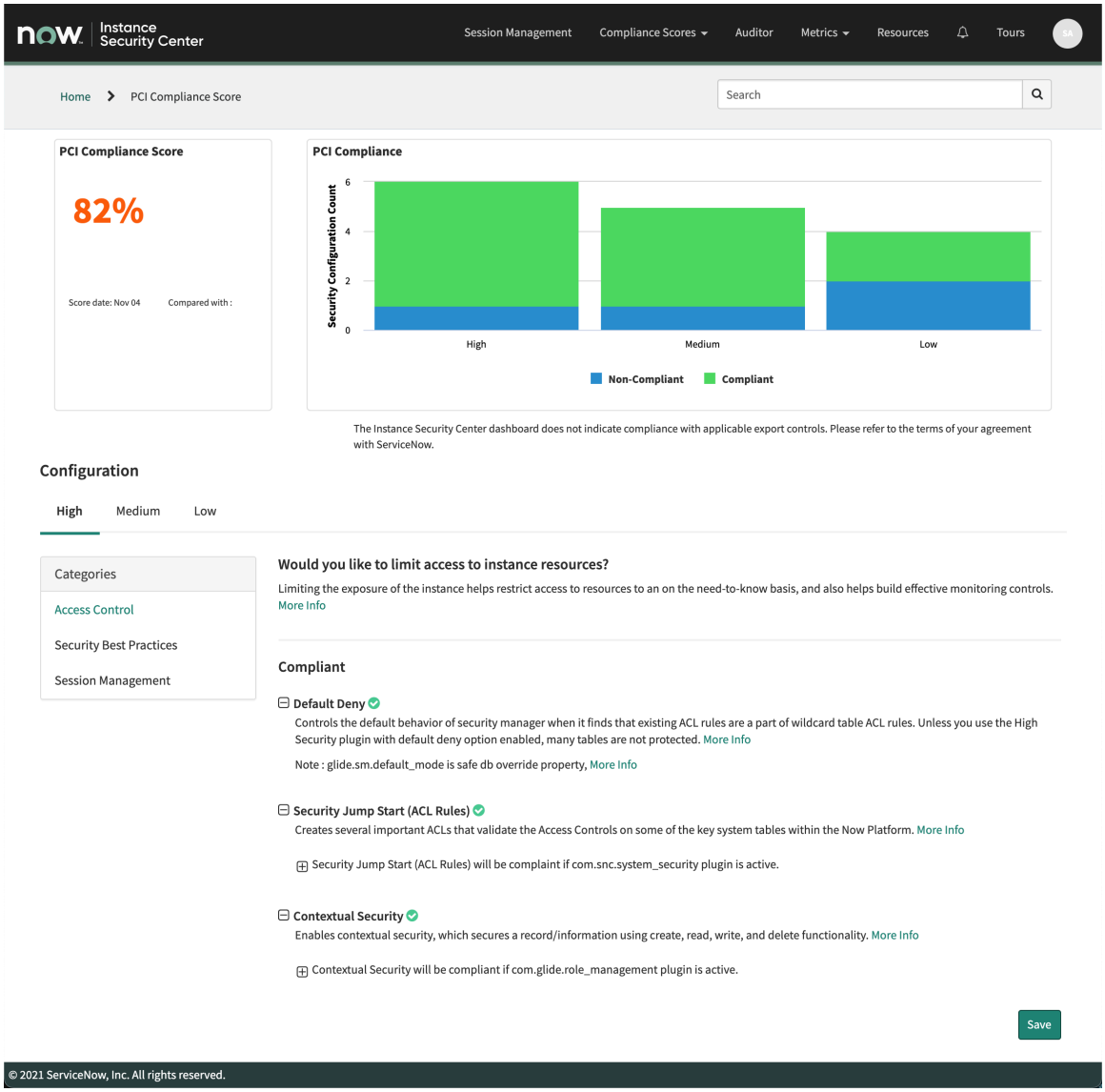
- 새로 고침 기능은 일별 데이터 수집 퍼포먼스 분석 작업과 동일한 작업을 수행하지만 배치 프로세스가 아닌 실시간으로 수행합니다.
- 일반적으로 일일 준수 점수에 대한 업데이트를 수행하여 인스턴스 보안 활동의 영향을 즉시 확인하려는 경우에 사용합니다.
- 업데이트된 점수가 표시되기까지 약간의 지연이 있을 수 있습니다.

주: 업그레이드(예: 에서 London 로 Yokohama)를 수행하면 인스턴스 보안 센터(ISC) 플러그인이 자동으로 활성화됩니다. 제공된 수정 스크립트는 할당된 역할 없이 사용자 지정 사용자를 자동으로 할당합니다.

PCI 규정 준수 점수 대시보드

PCI 규정 준수 점수 대시보드는 인스턴스가 PCI(Payment Card Industry) 보안 표준을 준수하는 방법을 보여줍니다. 대시보드를 사용하여 준수 점수를 보고 구성을 수정하여 보안을 향상합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



필요한 **Now Platform** 역할

PCI 준수 점수 대시보드를 보는 데 필요한 security_dashboard_user 또는 관리자.

PCI 규정 준수 점수 대시보드에 액세스

대시보드를 열려면 다음으로 이동합니다. 시스템 보안 > 인스턴스 보안 센터. 인스턴스 보안 센터의 헤더에서 규정 준수 점수를 클릭한 다음 **PCI** 규정 준수 점수를 선택합니다.

사용 케이스

조직 내 다른 사람이 이 대시보드를 사용하는 방법의 예시는 다음 사용 사례를 참조합니다.

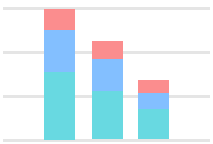
사용자	대시보드 사용
보안 대시보드 사용자 (security_dashboard_user)	인스턴스 보안 준수를 지속적으로 모니터링하고 관리합니다.
관리자(admin)	인스턴스 보안 준수를 지속적으로 모니터링하여 보안 위협을 감지하고 대응합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표시기

표시기	설명
PCI 준수 점수	인스턴스의 준수 점수를 백분율로 표시합니다. 이 백분율은 준수 표준을 충족하는 인스턴스의 보안 구성 백분율을 나타냅니다. 또한 이 표시기에는 규정 준수 점수가 계산된 날짜와 이전에 계산된 점수와의 비교 내용이 표시됩니다.

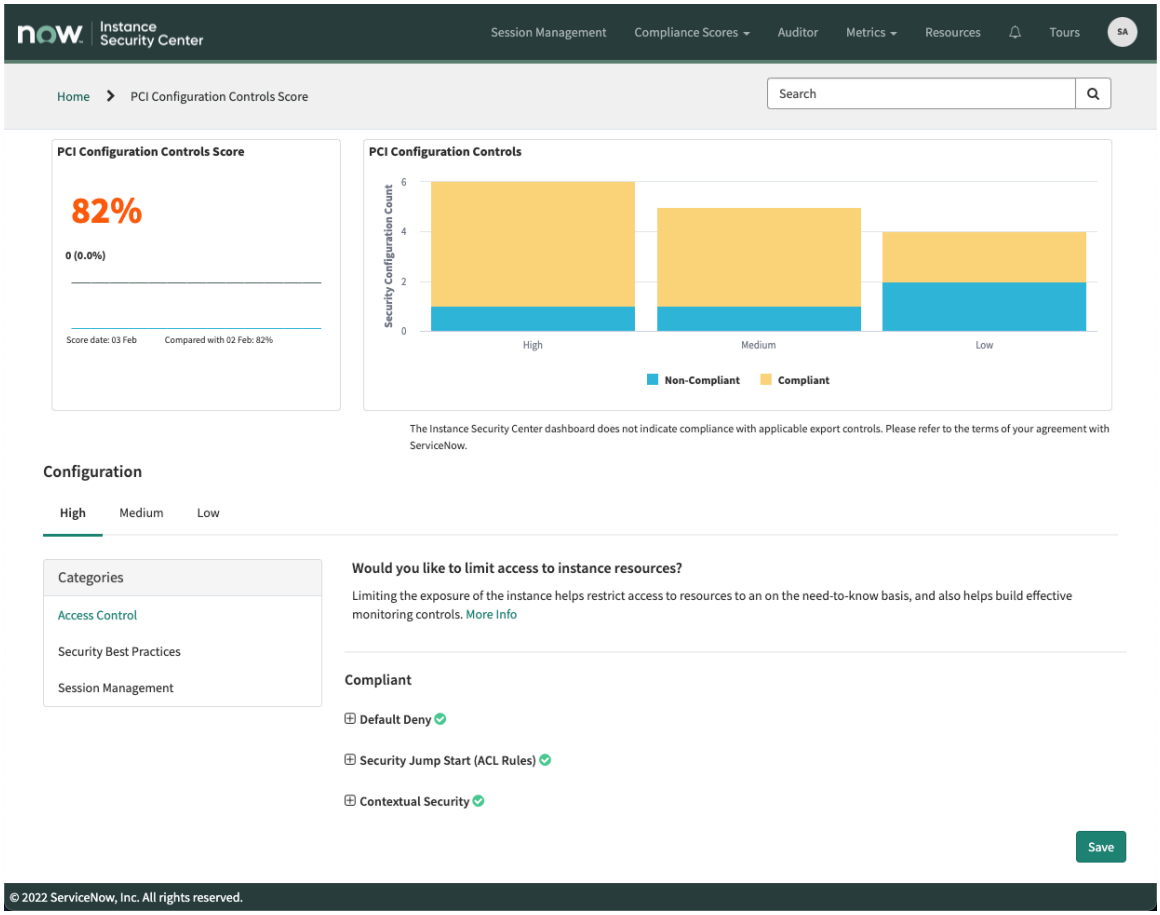
데이터 시각화

제목	유형	소스 테이블	설명
PCI 준수	 누적 막대 그래프	보안 구성 [isc_security_configuration]	준수 및 미준수 보안 구성을 높음, 중간 및 낮음 범주로 표시합니다. 보고서에서 일치하는 보안 구성을 표시하려면 영역의 영역을 클릭합니다.

PCI 구성 통제 점수 대시보드

PCI 구성 통제 점수 대시보드를 사용하여 PCI 구성을 검토하고 어떤 보안 검사가 미준수 검사인지 확인합니다. 인스턴스 보안 센터에서 미준수 보안 검사의 구성을 변경할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



필요한 **Now Platform** 역할

PCI 준수 점수 대시보드를 보려면 security_dashboard_user 또는 관리자 역할이 필요합니다.

PCI 구성 통제 점수 대시보드에 액세스

대시보드를 열려면 다음으로 이동합니다. 시스템 보안 > 인스턴스 보안 센터. 인스턴스 보안 센터의 헤더에서 규정 준수 점수를 클릭한 다음 **PCI** 구성 통제 점수를 선택합니다.

사용 케이스

조직 내 다른 사람이 이 대시보드를 사용하는 방법의 예시는 다음 사용 사례를 참조합니다.

사용자	대시보드 사용
보안 대시보드 사용자 (security_dashboard_user)	인스턴스에 대한 PCI 구성 통제 준수를 지속적으로 모니터링하고 관리합니다. PCI 구성을 수정하여 규정 준수를 보장하고 인스턴스 보안을 강화합니다.
관리자(admin)	PCI 구성 통제 준수를 지속적으로 모니터링하여 잠재적인 보안 위협을 감지하고 대응합니다.

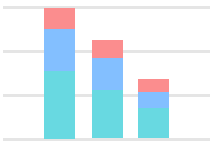
표시기

PCI 구성 통제 점수

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스의 PCI 구성 통제 점수를 백분율로 표시합니다. 이 백분율은 준수 표준을 충족하는 인스턴스의 보안 PCI 제어 구성 백분율을 나타냅니다. 또한 이 표시기에는 규정 준수 점수가 계산된 날짜와 이전에 계산된 점수와의 비교 내용이 표시됩니다.

데이터 시각화

제목	유형	소스 테이블	설명
PCI 구성 통제	 누적 막대 그래프	보안 구성 [isc_security_configurations]	호환 및 미준수 PCI 제어 구성을 높음, 중간 및 낮음 범주로 표시합니다. 보고서에서 일치하는 보안 구성을 표시하려면 영역의 영역을 클릭합니다.

잘못된 보안 정의 스캔

감사자를 실행하여 인스턴스를 스캔하고 잘못된 보안 정의를 찾습니다. 인스턴스의 보안 태세를 개선하는 데 도움이 되도록 수정할 수 있는 결과를 제공합니다.

중요사항:

인스턴스 보안 센터(ISC)는 2024년 9월 현재 판매가 종료되었으며 더 이상 지원되지 않으며 새로운 활성화에 사용할 수 없습니다.

ServiceNow SSC(보안 센터)는 앞으로 권장되는 솔루션입니다. 자세한 내용은 마이그레이션으로 ServiceNow 보안 센터 인스턴스 보안 센터 문서를 참조하십시오.

감사자는 시스템 구성을 분석하는 인스턴스 상태에 대한 "전체" 평가를 수행합니다. 보안 검사의 경우 현재 보안 구성을 베스트 프랙티스 정의 및 보안 속성 준수 값과 비교합니다.

인스턴스 보안 관점에서 계속 해야 하는 것과 개선할 수 있는 부분에 대한 인사이트와 권장 사항을 제공합니다. 이러한 인사이트와 권장 사항은 다음 질문에 답하는 데 도움이 됩니다.

- 적절한 보안 관련 속성이 설정되어 있습니까?
- 높은 보안 플러그인이 활성화되어 있습니까?
- 올바른 접근 제어 규칙이 있습니까?

감사자 실행 및 스캔 결과 분석

1. 감사자를 실행하려면 인스턴스 보안 센터 홈페이지에서 감사 를 클릭합니다.
2. 완료되면 스캔 결과를 열어 보안 결과를 검토하고 분석합니다.
3. 특정 스캔 결과에 대한 상세 정보를 검토하려면 결과 번호를 두 번 클릭합니다. 이 정보에는 상태, 스캔 유형, 실행 시간 및 오류 메시지가 포함됩니다.
4. 각 감사자 결과에는 해결 상세 정보 및 이를 해결하는 방법에 대한 제품 콘텐츠의 URL이 포함되어 있습니다. 문서화된 가이드라인에 따라 각 결과의 문제를 해결합니다.

관련 정보

강화 설정

높은 보안 플러그인 사용 〔보안 센터 1.3에서 업데이트됨〕

접근 제어 목록 규칙

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스 메트릭 모니터링

인스턴스의 사용자, 익스포트, 인증, 이메일 및 바이러스 백신 메트릭을 모니터링합니다. 예를 들어, 인스턴스에 대해 신뢰할 수 없는 도메인과 신뢰할 수 있는 도메인에서 보낸 스팸, 외부 이메일 및 인바운드 이메일에 대한 메트릭을 확인하여 이메일 보안을 모니터링할 수 있습니다. 이러한 메트릭을 분석하여 인스턴스에서 발생하는 활동과 관련된 비정상적인 보안 동작을 찾습니다.

중요사항:

인스턴스 보안 센터(ISC)는 2024년 9월 현재 판매가 종료되었으며 더 이상 지원되지 않으며 새로운 활성화에 사용할 수 없습니다.

ServiceNow SSC(보안 센터)는 앞으로 권장되는 솔루션입니다. 자세한 내용은 마이그레이션으로 ServiceNow 보안 센터 인스턴스 보안 센터 문서를 참조하십시오.

사용자 메트릭

사용자 메트릭을 분석하여 인스턴스의 특정 유형의 사용자 활동과 관련된 예외 동작을 찾습니다.

지난 달/지난 6개월/작년에 로그인하지 않음

지난달, 지난 6개월 및 지난 1년 내에 인스턴스에 로그인하지 않은 사용자 수를 나타냅니다. 특정 메트릭에 대한 사용자 상세 정보를 보려면 다음을 수행합니다.

- 메트릭을 클릭하면 표시된 기간 동안 인스턴스에 로그인하지 않은 사용자 목록을 볼 수 있습니다.
- 해당 사용자에 대한 자세한 내용을 보려면 사용자 이름을 클릭하십시오.

높은 권한 역할의 사용자

다음과 같은 높은 권한 역할 유형을 가진 사용자 수를 나타냅니다.

사용자 역할	설명
관리자	보안 제약 조건에 관계없이 모든 시스템 기능, 데이터에 액세스할 수 있는 기본 관리자 역할입니다.
ais_high_security_admin	사용자가 의 높은 보안 설정에 AI 검색접근할 수 있게 해 주는 상승된 권한 역할입니다. 자세한 내용은 다음을 참조하십시오. 다음에 역할 할당 AI 검색 관리자 및 사용자 .
password_reset_admin	사용자가 암호 재설정 활동의 상태를 보고, 잠재적인 보안 위협을 식별하고, 암호 보안 정책의 준수 여부를 모니터링할 수 있는 관리자 역할입니다. 자세한 내용은 다음을 참조하십시오. 암호 재설정 암호 변경 보고서 및 로그 .
script_include_admin	스크립트 포함에도 액세스할 수 있는 관리자 역할입니다.
security_admin	사용자가 접근 제어 및 높은 보안 설정을 만들고 변경할 수 있는 상승된 권한 역할입니다. 자세한 내용은 Security_admin 역할 문서를 참조하십시오.
user_admin	사용자, 역할, 사용자 그룹, 역할 및 부서 할당을 관리할 수도 있는 관리자 역할입니다.

주: 이러한 관리 역할 유형에 대한 자세한 내용은 특수 관리 역할을 참조하세요.

특정 사용자 역할 메트릭에 대한 사용자 상세 정보를 보려면 다음과 같이 하십시오.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 사용자 수 역할 메트릭을 클릭하여 해당 높은 권한 역할 유형의 사용자 목록을 봅니다.
- 해당 사용자에 대한 자세한 내용을 보려면 사용자 이름을 클릭하십시오. 그런 다음 보안에 중요한 역할이 적절한 담당자에게 할당되었는지 확인할 수 있습니다.

사용자 추세

다음 유형의 사용자에 대한 기간 동안의 카운트 추세 정보를 표시합니다.

카운트 유형	설명
활성 사용자	인스턴스에서 활성으로 표시된 사용자의 수입니다.
비활성 사용자	인스턴스에서 비활성으로 표시된 사용자의 수입니다.
잠겨 있음	인스턴스가 잠겨 있는 사용자 수입니다.

특정 사용자 수에 대한 사용자 상세 정보(예: 잠긴 사용자)를 보려면 다음을 수행합니다.

- 잠긴 사용자 메트릭을 클릭합니다.
- 분석 허브 페이지에서 기록 표시를 클릭합니다.
- 해당 사용자에 대한 자세한 내용을 보려면 사용자 이름을 클릭하십시오. 그런 다음 이 사람이 잠겨 있는 이유가 있는지 확인하고 상황을 해결할 수 있습니다.

이벤트 추세

기간에 걸친 특정 유형의 이벤트에 대한 카운트 추세 정보 표시:

이벤트 유형	설명
관리자 로그인	특정 날짜에 로그인한 높은 권한의 관리자 사용자 역할을 가진 사용자 수입니다.
외부 로그인	하루 동안 이 인스턴스에 로그인한 할당된 snc_external 역할을 가진 사용자 수입니다. 이러한 로그인은 일반적으로 유지관리, 지원, 컨설팅 또는 감사 목적으로 수행됩니다. 이 메트릭을 모니터링하면 외부 로그인 시도가 합법적이며 잠재적인 보안 문제가 아닌지 확인할 수 있습니다.
실패한 로그인	특정 날짜에 실패한 로그인 시도 횟수입니다.
가장	특정 날짜에 로그인하여 다른 사용자를 가장하는 사용자 수입니다.
보안 상승	보안 관리자가 하루 동안 할당된 사용자 역할을 높은 권한의 보안 역할로 변경하여 표준 사용자에 대한 보안을 상승시킨 횟수입니다. 이러한 높은 권한 보안 역할에는 oauth_admin, 관리자, security_admin 및 가장자가 포함됩니다.
SNC 로그인	고객 서비스 및 지원 특정 날짜에 하이호핑 기술을 사용하여 이 인스턴스에 로그인한 사용자 수입니다.

특정 이벤트 수(예: 가장)에 대한 사용자 상세 정보를 보려면 다음과 같이 하십시오.

- 사용자 수 메트릭을 클릭합니다. 보안 대시보드 이벤트 로그 페이지에는 해당 유형의 이벤트에 대한 이벤트 로그가 나열됩니다.
- 해당 이벤트에 대한 자세한 내용을 보려면 사용자 이름을 클릭하십시오.

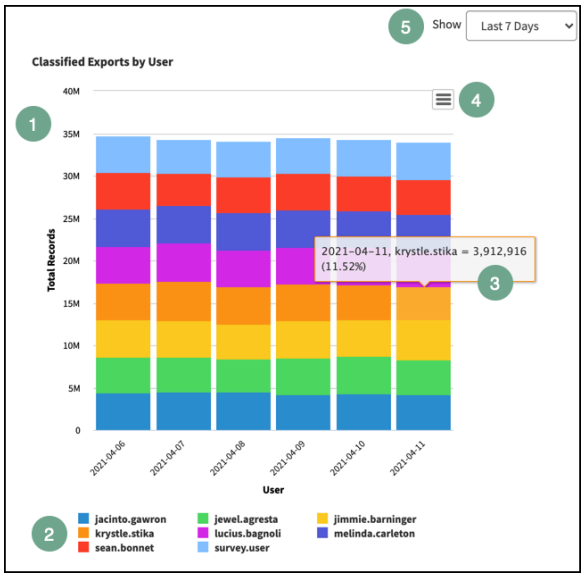
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

분석 허브

메트릭 익스포트

익스포트 메트릭을 분석하여 가장 일반적으로 익스포트되는 데이터와 가장 많은 데이터를 익스포트하는 사용자를 확인합니다.



1. 차트 내보내기

   각 보고서는 익스포트를 수행한 사용자를 나타내는 색상 코드 키를 사용하여 날짜별 익스포트 이벤트 수를 표시합니다. 열의 색상이 지정된 섹션을 클릭하면 해당 항목과 일치하는 익스포트 이벤트 [isc_export_event] 기록 목록을 볼 수 있습니다.

2. 보고서 키

   보고서 하단의 키는 사용자 또는 테이블을 식별하는 색을 나타냅니다.

3. 미리보기 팝업

   차트의 항목을 가리키면 팝업 미리 보기가 표시됩니다. 이 미리 보기에는 사용자 또는 테이블 이름뿐만 아니라 익스포트 수와 해당 열의 합계 백분율이 표시됩니다.

4. 이미지 내보내기

   아이콘을 클릭하여 보고서를 이미지로 저장합니다. 보고서를 PNG 또는 JPEG 형식으로 저장할 수 있습니다.

5. 보고서 날짜 범위

   목록 표시를 사용하여 지난 24시간 이내 또는 지난 7일 이내의 익스포트를 표시합니다.

메트릭 보고서 익스포트

지표 내보내기 페이지에는 4개의 보고서가 표시됩니다.

사용자별 익스포트

사용자별 내보내기 보고서를 사용하여 가장 많은 데이터를 내보내는 사용자를 확인합니다.

사용자별 분류된 익스포트

사용자별 분류된 내보내기 보고서를 사용하여 기밀, 제한된 또는 개인 정보와 같은 분류와 가장 일치하는 데이터를 내보내는 사용자를 확인합니다. 관리자는 설정 탭에서 이 보고서가 사용하는 분류를 정의할 수 있습니다.

테이블을 통해 내보내기

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블별 내보내기 보고서를 사용하여 가장 자주 내보내는 테이블을 확인할 수 있습니다.

테이블별 분류된 익스포트

테이블별 분류된 내보내기 보고서를 사용하여 기밀, 제한 또는 개인 정보와 같은 분류와 일치하는 가장 자주 익스포트되는 테이블을 확인합니다. 관리자는 설정 탭에서 이 보고서가 사용하는 분류를 정의할 수 있습니다.

주: 익스포트 메트릭 보고서는 익스포트 이벤트만 추적합니다. REST API 또는 워크플로우와 같은 다른 소스에서의 익스포트는 이 기능의 일부로 추적되지 않습니다.

메트릭 설정 익스포트

설정 탭의 구성 옵션을 사용하여 보고 결과의 범위를 좁힙니다.

설정 탭을 클릭하여 익스포트 메트릭에 대한 설정에 액세스합니다.

설정 구성 필드

메트릭 구성 익스포트

구성	설명
메트릭에 대한 분류	이 필드에 분류를 추가하거나 제거하여 사용자별 분류된 내보내기 및 테이블별 분류된 내보내기 보고서에 포함되는 내보내기를 결정합니다. 이러한 보고서는 다음 분류를 지원합니다. • 개인 식별 정보 • 기밀 • 제한함 • 내부 • 공개 데이터 분류에 대한 자세한 내용은 데이터 분류 섹션을 참조하세요.
경보에 대한 분류	이 필드에 분류를 추가하거나 제거하여 인스턴스 보안 알림을 트리거하는 익스포트를 결정합니다. 메트릭 분류 필드에서 지원되는 분류가 여기에서 지원됩니다. 이러한 경고에 대한 자세한 내용은 페이지의 보안 알림 섹션을 인스턴스 보안 센터 참조하세요. 기록 임계치 필드는 인스턴스가 트리거되고 경보가 발생하기 전에 익스포트하는 기록 수를 정의합니다.
기록 임계치	경보를 트리거하기 위해 사용자가 익스포트해야 하는 기록 수입니다. 경보를 트리거하려면 이러한 기록이 경보에 대한 분류 필드에 나열된 분류와도 일치해야 합니다.

저장**(⌘ + s)** 버튼을 사용하여 설정을 저장합니다.

인증 메트릭

인증 메트릭을 분석하여 자주 사용하지 않는 IP 주소, 실패한 로그인, 사용자가 사용하는 인증 체계 유형 등 인증과 관련된 정보를 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인증 메트릭 페이지를 사용하여 인증 구성과 관련된 보고서를 봅니다. 이 탭에는 다음과 같은 보고서가 표시됩니다.

주: 인증 메트릭 페이지에는 **REST API Access Policy** 플러그인 (com.glide.rest.policy)이 필요합니다. 이 기능에 대한 자세한 내용은 REST API 액세스 정책을 참조하세요.

인증 정책이 없는 API

액세스 정책 없이 모든 API의 실시간 카운트를 표시합니다.

강화: 계정 복구 플로우

강화: 역할 기반 MFA 기능 관련 설정

웹 서비스 액세스 전용 계정

[sys_user] 테이블에서 웹 서비스 접근 옵션을 사용할 *User* 수 있는 모든 사용자 기록의 수를 표시합니다.

X509 인증서가 30일 후 만료됩니다.

30일 후 만료되는 [sys_certificate] 테이블의 모든 X.509 인증서 *X.509 Certificates* 수를 표시합니다.

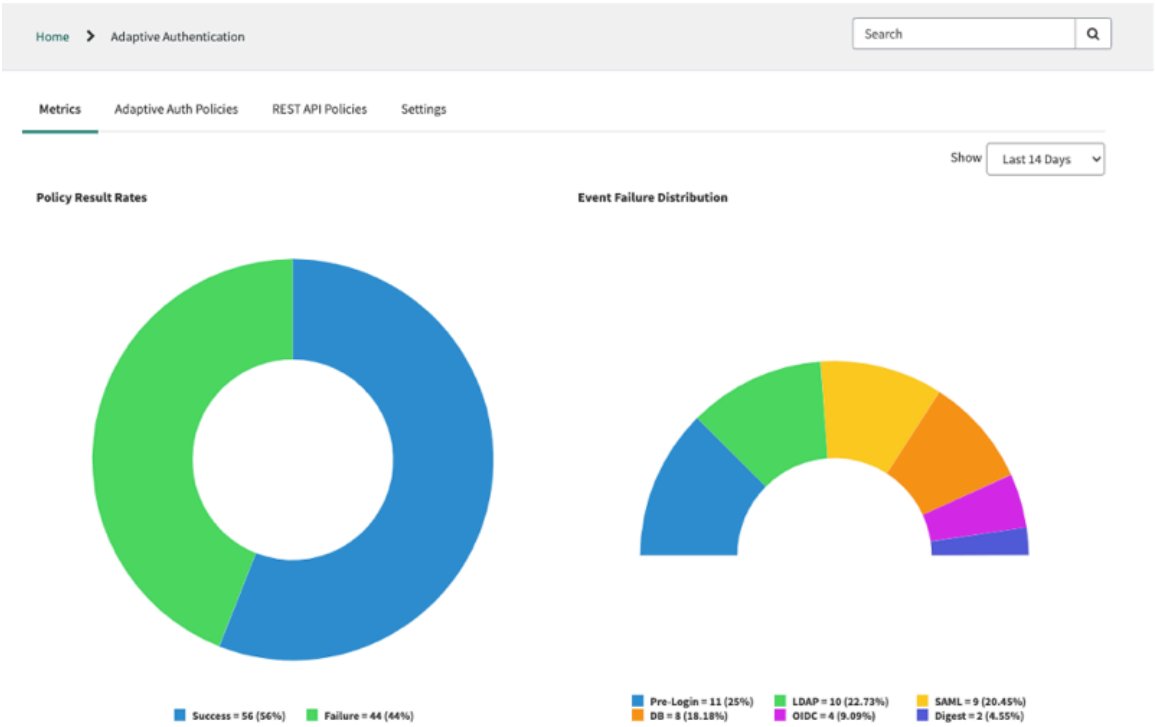
적응형 인증 메트릭

적응형 인증 메트릭을 분석하여 인스턴스에서 적응형 인증이 사용되는 방식을 모니터링하고 인사이트를 추가합니다.

적응형 인증 메트릭 페이지를 사용하여 해당 위치에서 적응형 인증과 관련된 보고서, 설정 및 정책을 봅니다. 보안 관리자는 보고서를 사용하여 적응형 인증 정책의 결과를 모니터링할 수 있습니다. 이 데이터를 사용하여 인사이트를 얻고 정책을 조정하여 성과를 개선합니다.

주: 적응형 인증 메트릭 페이지에는 적응형 인증 (com.snc.adaptive_authentication) 플러그인이 필요합니다. 이 기능에 대한 자세한 내용은 적응형 인증을 참조하세요.

메트릭



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

메트릭 탭을 사용하여 적응형 인증 구성과 관련된 보고서를 봅니다. 이 탭에는 다음과 같은 보고서가 표시됩니다.

- 정책 결과 비율
- 이벤트 장애 분포
- 이벤트 성공 배포
- 거부된 IP 주소
- 인증 사용자 로그인
- API 사용자 로그인
- 인증 추세

표시 목록을 사용하여 표시된 보고서의 시간 범위를 선택합니다

적응형 인증 정책

적응형 인증 정책 탭을 사용하여 인스턴스의 적응형 인증 정책 및 정책 컨텍스트를 봅니다. 연결된 기록을 보려면 해당 목록의 항목을 클릭합니다. 이러한 레코드에 대한 자세한 내용은 적응형 인증을 참조하십시오.

설정

설정 탭을 사용하여 적응형 인증 시스템 속성을 보고 구성합니다. 이러한 속성에 대한 자세한 내용은 적응형 인증 속성 구성을 참조하십시오.

이메일 메트릭

이메일 메트릭을 분석하여 인스턴스로 들어오는 이메일과 관련된 예외 동작을 찾습니다. 예를 들어, 메트릭이 특정 도메인에서 보낸 스팸 이메일의 급증을 나타내는 경우, 인스턴스로의 전송을 차단하는 인바운드 작업을 정의할 수 있습니다.

각 이메일 메트릭의 경우, 해당 날짜 동안 인스턴스로 배달되거나 전송된 각 이메일 유형에 대한 개수가 나타납니다.

알림 기본 설정	설명
외부 수신 이메일	해당 날짜에 외부 이메일 도메인에서 인스턴스로 전송된 수신 이메일 수입니다. 주: 외부 이메일 도메인은 내부 이메일 도메인만 추적하므로 시스템 속성에 나열 *security.list.internal.domains* 되지 않은 도메인입니다. 이 속성에 대한 자세한 내용은 사용 가능한 시스템 속성을 참조하십시오.
스팸	인스턴스로 전송되고 스팸으로 표시된 해당 날짜의 수신 이메일 수입니다. 숫자가 기록 추세와 일치하지 않으면 인스턴스 보안을 손상시키려는 시도가 있었음을 나타낼 수 있습니다.
신뢰할 수 있는 수신 이메일	신뢰할 수 있는 것으로 지정된 이메일 도메인에서 해당 날짜에 인스턴스로 수신되는 이메일 수입니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

알림 기본 설정	설명
신뢰할 수 없는 수신 이메일	신뢰할 수 없음으로 지정된 이메일 도메인에서 해당 날짜에 인스턴스로 수신되는 이메일 수입니다. 신뢰할 수 없는 도메인과 신뢰할 수 있는 도메인 양식에서 신뢰할 수 없는 이메일 도메인이나 신뢰할 수 있는 이메일 도메인을 지정하여 해당 도메인에서 보내는 인바운드 이메일을 추적할 수 있습니다. 신뢰할 수 없거나 신뢰할 수 있는 전자 메일 도메인을 지정하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 이메일 도메인을 신뢰할 수 없음 또는 신뢰할 수 있음으로 지정.

이메일 메트릭을 클릭한 후 다음 중 하나를 클릭하여 인스턴스에서 발생할 수 있는 이메일 보안 문제에 대해 알아볼 수 있습니다.

명령	설명
차트	선택한 이메일 유형(스팸, 외부 수신, 신뢰할 수 없음 또는 신뢰할 수 있음)에 대한 수신 이메일 수 및 시간 경과에 따른 추세 수입니다.
기록	선택한 이메일 유형의 일일 카운트를 손상시키는 개별 이메일 기록입니다.
추가 정보	선택한 이메일 유형에 대한 추가 정보입니다.

주: 이메일 메트릭은 인스턴스로 들어오는 이메일에만 적용됩니다. 메트릭은 전사적 이메일 서버를 통해 처리되는 일반 트래픽에는 적용되지 않습니다. 인바운드 작업을 정의하고 인바운드 이메일 처리에 미치는 영향에 대해 알아보려면 인바운드 이메일 작업을 참조하십시오.

이메일 도메인을 신뢰할 수 없음 또는 신뢰할 수 있음으로 지정

인스턴스에서 이러한 소스로부터 수신되는 이메일의 메트릭을 모니터링할 수 있도록 특정 이메일 도메인을 신뢰할 수 없음 또는 신뢰할 수 있는 것으로 지정합니다.

시작하기 전에
필요한 역할: security_dashboard_user 또는 admin

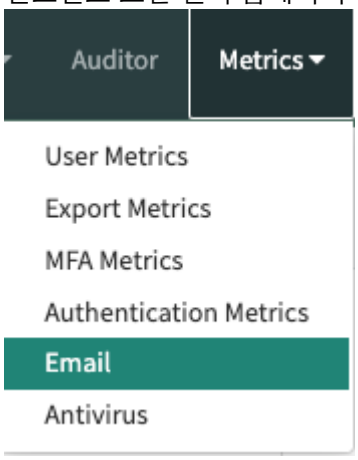
이 태스크 정보
신뢰할 수 없거나 신뢰할 수 있는 도메인이 인스턴스에 이메일을 보내면 이메일 페이지의 신뢰할 수 없는 수신 이메일 또는 신뢰할 수 있는 수신 이메일 메트릭에 일일 개수가 표시됩니다. 그런 다음 이러한 도메인의 이메일 활동을 추적하고 이메일 로그를 사용하여 특정 수신 이메일을 볼 수 있습니다. 또한 신뢰할 수 없거나 신뢰할 수 있는 도메인에서 활동이 발생할 때마다 알림을 받을 사용자(일반적으로 관리자 또는 보안 분석가)를 지정할 수 있습니다.

주: 이메일 도메인을 신뢰할 수 없음으로 지정하는 것은 보안 추적 목적으로만 사용됩니다. 관리자는 신뢰할 수 없는 도메인의 이메일을 무시하도록 시스템 주소 필터를 설정할 수도 있습니다. 전자 메일을 필터링하여 배달을 차단하는 방법에 대한 자세한 내용은 시스템 주소 필터를 참조하세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 인스턴스 보안 센터.
2. 인스턴스 보안 센터 홈페이지의 메트릭 메뉴에서 이메일을 선택합니다.

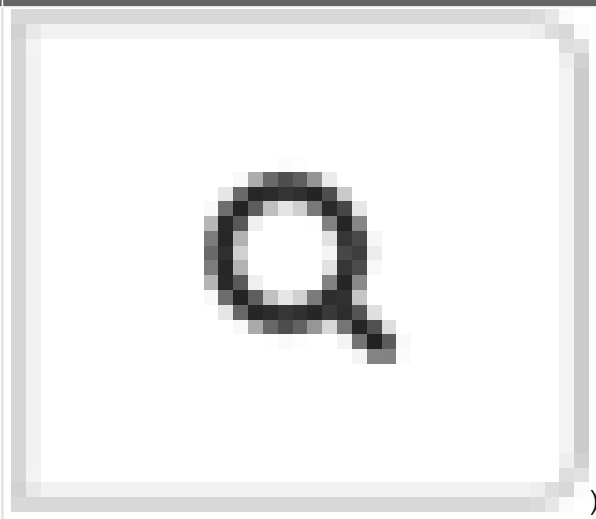


3. Email(이메일) 페이지의 Untrusted And Trusted Domains(신뢰할 수 없는 도메인과 신뢰할 수 없는 도메인) 섹션에서 New(새로 만들기)를 클릭합니다.
4. 양식의 필드에 내용을 입력합니다.

신뢰할 수 없는 도메인과 신뢰할 수 있는 도메인 양식

필드	설명
도메인	신뢰할 수 없음 또는 신뢰할 수 있음으로 지정할 이메일 도메인의 이름입니다. 예를 들어 `servicenow.com` 입력하여 신뢰할 수 있는 이메일을 인스턴스에 보낼 수 있는 직원을 지정합니다 ServiceNow .
범주	이메일 도메인을 신뢰할 수 없는지, 신뢰할 수 있는지를 나타내는 범주: 신뢰할 수 없음 해당 이메일 도메인을 신뢰할 수 없는 것으로 지정합니다. 이를 사용하여 인스턴스에 잠재적인 보안 위협을 제기하는 의심스러운 이메일 또는 의심스러운 이메일을 보내는 도메인을 식별합니다. 신뢰할 수 있음 이메일 도메인을 신뢰할 수 있는 도메인으로 지정합니다. 메트릭에서 들어오는 이메일이 보안 위협을 제기하지 않는 것으로 나타날 때 도메인을 식별하는 데 사용합니다. 도메인을 신뢰할 수 있는 도메인으로 지정하면 시간이 지남에 따라 인바운드 이메일 활동을 추적할 수 있습니다.
활성	지정된 이메일 도메인에 대해 지정된 신뢰할 수 없거나 신뢰할 수 있는 상태를 활성화하거나 비활성화하는 확인란입니다.
Notify	신뢰할 수 없거나 신뢰할 수 있는 도메인에서 활동이 발생할 때 이메일로 알릴 사용자의 이름입니다. 스포트라이트 검색 아이콘(

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	)을 클릭하여 사용자의 이름을 검색합니다. 알림 전송을 원하지 않으면 알림 필드를 비워 둡니다.

5. 저장을 선택합니다.

결과
신뢰할 수 없거나 신뢰할 수 있는 전자 메일 도메인 정보는 전자 메일 페이지의 신뢰할 수 없는 도메인과 신뢰할 수 있는 도메인 목록에도 추가됩니다.

관련 정보

- 인스턴스 보안 센터
- 이메일 메트릭

바이러스 백신 메트릭

플러그인이 바이러스 백신 검사 활성화된 경우 인스턴스에서 바이러스 백신 검사 실행되어 첨부 파일로 인한 바이러스 감염으로부터 플러그인을 보호할 수 있습니다.

다음 메트릭은 지난 60일 동안의 활동에 대해 표시되며, 이를 통해 기능의 효과를 바이러스 백신 검사 평가할 수 있습니다.

바이러스 백신 이벤트

바이러스 백신 이벤트는 인스턴스에 있는 바이러스 백신 이벤트의 수를 날짜별로 나타냅니다. 바이러스 백신 이벤트에 액세스하려면 다음으로 이동하십시오. 시스템 보안 > 인스턴스 보안 센터 을 클릭하고 메트릭 탭을 선택합니다. 색으로 구분된 그래프 선은 다음과 같은 유형의 바이러스 백신 이벤트를 나타냅니다.

색상	설명
파랑	표시된 날짜 동안 이 인스턴스에서 격리된 바이러스 백신 검사 파일 수입니다.
녹색	인스턴스에 다운로드된 후 지정된 날짜 동안 격리된 감염된 파일 수입니다. 이러한 파일은 주로 바이러스 또는 루즈 코드가 포함된 이메일 첨부 파일입니다.
황색	지정된 날짜 동안 삭제된 인스턴스의 격리된 파일 수입니다.
주황	지정된 날짜 동안 재개된 인스턴스의 격리된 파일 수입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

색상	설명
	주: 실행 후 바이러스 백신 검사 긍정 오류를 찾으면 격리된 파일을 복원하고 인스턴스에서 액세스할 수 있도록 할 수 있습니다.

- 페이지에 액세스하여 분석 허브 특정 날짜에 대한 자세한 점수 카드 및 분석 정보를 보려면 바이러스 백신 이벤트 그래프에서 색상이 지정된 선을 클릭합니다. 예를 들어 파란색 그래픽 선을 클릭하여 특정 날짜에 대해 격리된 파일에 대한 분석 정보를 볼 수 있습니다.
- 페이지에서 다음 세부 항목을 분석 허브 보려면 ☰을 클릭한 후 다음을 클릭합니다.

세부 항목	설명
AppSec - 바이러스 백신 이벤트 소스	바이러스 백신 이벤트의 소스입니다. ◦ 업로드 시: 감염된 파일(일반적으로 첨부 파일)의 업로드로 인해 발생했습니다. ◦ 검역소에서: 감염된 파일(일반적으로 첨부 파일)의 격리로 인해 발생했습니다. ◦ 다운로드 시: 감염된 파일(일반적으로 첨부 파일)의 다운로드로 인해 발생했습니다. ◦ 기록에서: 테이블의 기록이 감염되어 발생했습니다.
AppSec - 바이러스 백신 이벤트 유형	바이러스 백신 이벤트의 유형입니다. ◦ 격리: 파일(일반적으로 첨부 파일)의 격리로 인해 발생했습니다. ◦ 다운로드: 파일(일반적으로 첨부 파일)의 다운로드로 인해 발생했습니다. ◦ 복원: 격리된 파일의 복원으로 인해 발생했습니다. ◦ 삭제: 격리된 파일을 삭제하여 발생했습니다.
AppSec - 바이러스 백신 업로더	애플리케이션에서 탐지 바이러스 백신 검사 한 바이러스 감염의 근원지인 파일을 업로드한 로그인한 사용자의 이름입니다.

격리된 파일

격리된 바이러스 백신 검사인스턴스에서 감염된 파일을 나열합니다.

필드	설명
파일 이름	감염된 파일의 이름입니다.
콘텐츠 유형	파일에서 감염된 콘텐츠의 유형입니다. 예를 들어 **application/x-dosexec** 는 감염된 애플리케이션 또는 DOS 실행 파일이고 **text/plain** 은 감염된 .txt 파일입니다.
테이블	감염된 파일이 들어 있는 테이블의 이름입니다. 예를 들어 인시던트 는 인시던트 파일 기록에 대해 나타납니다.
바이러스	에 의해 바이러스 백신 검사격리된 파일의 이름입니다.
탐지됨	감염된 파일이 탐지된 날짜 및 시간입니다.
작성자	감염된 파일을 격리 보관한 사용자의 이름입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
작성됨	격리 파일 기록이 만들어진 날짜 및 시간입니다.
테이블 시스템 ID	격리 파일 기록에 할당된 테이블 시스템 식별자입니다.

주: 검역소에 보관된 파일 및 바이러스 유형 타일을 이벤트 리본에 추가할 수도 있습니다. 자세한 내용은 및 보안 이벤트 리본 구성를 참조하십시오보안 이벤트 모니터링.

관련 정보

- 바이러스 백신 검사
- 바이러스 백신 검사 구성
- 격리된 파일 검토
- 바이러스 백신 활동 검토
- 분석 허브
- 퍼포먼스 분석 세부 항목
- Analytics, Intelligence, and Reporting

MFA 메트릭 대시보드

MFA 메트릭 대시보드에는 인스턴스 다단계 인증 구성에 대한 정보가 표시됩니다. 대시보드를 사용하여 MFA 구성이 보안 표준을 충족하는지 확인합니다.

필요한 **Now Platform** 역할

PCI 준수 점수 대시보드를 보는 데 필요한 security_dashboard_user 또는 관리자.

MFA 메트릭 대시보드에 액세스

대시보드를 열려면 다음으로 이동합니다. 시스템 보안 > 인스턴스 보안 센터. 인스턴스 보안 센터의 헤더에서 메트릭을 클릭한 다음 **MFA** 메트릭을 선택합니다.

사용 케이스

조직 내 다른 사람이 이 대시보드를 사용하는 방법의 예시는 다음 사용 사례를 참조합니다.

사용자	대시보드 사용
보안 대시보드 사용자 (security_dashboard_user)	인스턴스 보안 준수를 지속적으로 모니터링하고 관리합니다.
관리자(admin)	인스턴스 보안 준수를 지속적으로 모니터링하여 보안 위협을 감지하고 대응합니다.

표시기

MFA에 등록된 사용자

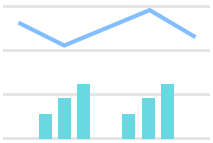
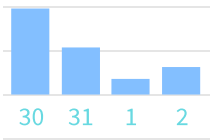
MFA 에 등록된 인스턴스의 총 사용자 수를 표시합니다. 자세한 내용을 보려면 클릭하여 분석 허브를 엽니다.

MFA 바이패스를 사용하는 사용자

MFA 바이패스 를 사용하는 총 사용자 수를 표시합니다. 자세한 내용을 보려면 클릭하여 분석 허브를 엽니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 시각화

제목	유형	소스 테이블	설명
높은 권한 MFA 사용자	막대 		
MFA 사용자 동향	 추세		

ISC 가상 에이전트 인터페이스 활성화

관리자 역할이 있는 경우에는 ISC 가상 에이전트 대화 플러그인(com.glide.isc_virtualagent)을 활성화할 수 있습니다. 이 플러그인을 활성화하면 인스턴스 보안 센터에서 액세스할 수 있는 가상 에이전트 및 자연어 이해 (NLU 콘텐츠 팩이 가상 에이전트 설치됩니다.

시작하기 전에

중요사항:

인스턴스 보안 센터(ISC)는 2024년 9월 현재 판매가 종료되었으며 더 이상 지원되지 않으며 새로운 활성화에 사용할 수 없습니다.

ServiceNow SSC(보안 센터)는 앞으로 권장되는 솔루션입니다. 자세한 내용은 마이그레이션으로 ServiceNow 보안 센터 인스턴스 보안 센터 문서를 참조하십시오.

가상 에이전트 인스턴스 보안 센터의 인터페이스는 유료 가상 에이전트 구독 사용자 및 Glide 가상 에이전트(com.glide.cs.chatbot) 플러그인을 활성화한 사용자만 사용할 수 있습니다. 자세한 내용은 가상 에이전트 활성화 를 참조하십시오.

필요한 역할: admin.

이 태스크 정보

ISC 가상 에이전트 인터페이스를 사용하여 다음 작업을 수행할 수 있습니다.

- 보안 관련 질문을 한 다음, 빠른 요약 답변과 참조 링크를 받아 자세히 알아보십시오.
- 인스턴스 보안 센터, 플랫폼 보안, ServiceNow 보안 정책, 신뢰, 거버넌스, 위험 및 기타 프로세스와 관련된 답변을 확인합니다.
- Now Support 보안 포털에서 지식베이스 주제와 같은 보안 관련 자원을 검색합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ISC용 플러그인 가상 에이전트

플러그인	설명
ISC 가상 에이전트 대화 [com.glide.isc_virtualagent]	인스턴스 보안 센터용 ISC 가상 에이전트 대화 콘텐츠 팩을 활성화합니다.
대화용 가상 에이전트 ISC NLU 모델 [com.glide.isc_nlu]	인스턴스 보안 센터의 (NLU) 컨텐츠 팩을 활성화합니다 자연어 이해 .

주: com.glide.isc_virtualagent 플러그인을 활성화하면 com.glide.isc_nlu 자동으로 활성화됩니다. 그러나 com.glide.isc_nlu 플러그인을 먼저 활성화하는 경우 com.glide.isc_virtualagent도 수동으로 활성화해야 합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 조건과 검색 창을 사용하여 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

강화 설정

보안 센터(SSC) 강화 설정 컨텐츠에는 ServiceNow 보안 관련 시스템 속성 및 플러그인에 대한 자세한 설명과 준수 값이 포함되어 있습니다 Now Platform. 보안 센터의 강화 설정 앱을 사용하여 이러한 속성을 설정할 수 있습니다.

개요 및 목적

Security Center는 현재 인스턴스 보안 설정이 Security Center 강화 설정의 규정 준수 값을 얼마나 준수하는지에 따라 백분율로 표시되는 일일 규정 준수 점수를 계산합니다.

인스턴스 점수에 영향을 줄 수 있는 특정 보안 구성 설정을 보안 센터에서 직접 관리할 수 있습니다.

강화 설정 구성은 표에 설명된 몇 가지 속성과 함께 설명됩니다.

강화 설정 구성 상세 정보

구성 속성	설명
개요	권장 사항에 대한 개략적인 개요를 제공합니다.
구성 이름	속성 또는 플러그인 이름입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

강화 설정 구성 상세 정보

구성 속성	설명
구성 유형	시스템 속성(*sys_properties_list.do*)에서와 같이 보안 센터 외부에서 속성을 구성할 수 있는 위치를 설명합니다.
데이터 유형	구성에 필요한 값의 유형을 설명합니다. 예를 들어 참/거짓 부울, 설치, 플러그인, 문자열 등이 있습니다.
권장 값	인스턴스의 보안 준수를 강화하기 위해 보안 센터에서 권장하는 값입니다.
기본값	기본 시스템에서 구성이 설정된 값입니다.
범주	강화 설정의 범주에 대한 이름 및 링크입니다.
보안 위험	심각도 점수: 점수는 취약성이 악용될 가능성에 따라 인스턴스에 대한 잠재적인 보안 위험을 나타냅니다. 보안 취약성은 **0.0** 에서 **10.0** 사이의 척도에서 CVSS(공통 취약성 평가 시스템) 점수를 사용하여 개별적으로 고려되고 점수가 매겨집니다. 자세한 내용은 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator 문서를 참조하십시오.
	CVSS 점수당 심각도 등급: • 중요: 9.0-10.0 • 높음: 7.0-8.9 • 중간: 4.0-6.9 • 낮음: .01-3.9 • 없음: 0.0
	보안 위험 상세 정보: 설정 구성의 중요성과 권장 구성을 활용하지 않을 경우의 위험에 대해 설명합니다.
의존성 및 필수 구성요소	강화 구성 이전 또는 강화 구성과 함께 필요한 관련 설정 또는 구성입니다.
기능적 영향	이 강화 설정이 인스턴스 운영에 미치는 영향입니다.
참조	구성 문서 또는 기타 유용한 정보에 대한 링크입니다.

주: 일부 구성은 완료해야 고객 서비스 및 지원 만 완료할 수 있으며 그에 따라 표시됩니다.

인스턴스가 강화 요구 사항을 충족하는지 확인하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 보안 강화.

기타 자원

사용자 참조를 위해 제품 Now Platform 설명서에서 광범위한 구성 기능 정보를 유지합니다. 에 있는 링크를 사용하여 대부분의 보안 콘텐츠에 액세스할 수 있습니다 인스턴스 보호. 또한 다음을 참조하십시오.

- 사용 가능한 시스템 속성
- 일반 보안 설정 속성
- 높은 보안 설정

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

강화 설정 기준선

강화 설정의 기준 버전이 제품군 및 스토어 릴리스에 어떻게 부합하는지 살펴보세요.

보안 센터 는 인스턴스에서 시스템 속성의 하위 집합을 수집하고 앱 내 규정 미준수가 보안에 미치는 영향과 함께 구성 상세 정보를 표시하는 방식으로 작동합니다. 기준은 Security Center 앱의 각 릴리스와 함께 수집되는 시스템 속성의 참조점 역할을 합니다.

강화 설정 기준선 개요

보안 센터 버전	강화 설정 기준선 버전	지원 대상 가정	스토어 릴리스 날짜	기본적으로 와 함께 설치됨
SSC v1.1	기준 v1.0	유타, 밴쿠버	2023년 5월	밴쿠버 가족
SSC v1.2	기준 v1.0	유타, 밴쿠버	2023년 8월	스토어 전용
SSC v1.3	기준선 v2.0	밴쿠버, 워싱턴 DC	2023년 11월	워싱턴 가족
SSC v1.5	기준 v4.0	워싱턴 D.C., 제나두	2024년 5월	Xanadu
SSC v1.6	기준 v4.0	워싱턴 D.C., 제나두	2024년 8월	스토어 전용
SSC 버전 2.0	기준 v5.0	제너두, 요코하마	2024년 11월	Yokohama

새 강화 설정

새 강화 설정은 베이스라인 릴리스별로 세분화됩니다.

베이스라인 버전 5.0에 대한 새로운 강화 설정

Security Center 기준 버전 5.0에서 새로운 강화 설정이 릴리스되었습니다.

- HR 수명 주기 이벤트 데이터에 ACL 강제 적용[Security Center 2.0의 새로운 기능]
- 번역된 모든 HTML 필드 삭제 [Security Center 2.0의 새로운 기능]
- 서비스 포털 위젯 허용 목록 구성[Security Center 2.0의 새로운 기능]
- HR Core 데이터에 ACL 강제 적용[Security Center 2.0의 새로운 기능]
- HR 가상 에이전트 데이터에 ACL 강제 적용[Security Center 2.0의 새로운 기능]
- 서비스 포털 위젯 허용 목록 구성[Security Center 2.0의 새로운 기능]
- 서비스 응용 프로그램 정보에 대한 보안 범위 적용[Security Center 2.0의 새로운 기능]
- 빈 ACL 생성 방지[Security Center 2.0의 새로운 기능]
- 가상 에이전트가 포함된 웹 클라이언트에 대한 인증되지 않은 접근 방지
- 토큰 자격 증명에 대한 자동 토큰 정리 설정[Security Center 2.0의 새로운 기능]
- 역할별로 전역 앱 개발 제한[Security Center 2.0의 새로운 기능]
- 단순 목록 위젯에서 인코딩된 쿼리에 ACL 사용 [Security Center 2.0의 새로운 기능]
- OAuth 토큰 만료 후 세션 무효화[Security Center 2.0의 새로운 기능]
- 허용된 MIME 하위 유형 설정[Security Center 2.0의 새로운 기능]
- 관리자로의 가장 제한[Security Center 2.0의 새로운 기능]

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

베이스라인 버전 4.0에 대한 새로운 강화 설정

Security Center 기준 버전 4.0에서 새 강화 설정이 릴리스되었습니다.

- 불필요한 명시적 역할 액세스 제어 조건 검토[Security Center 1.5에서 제거됨]
- 서비스 조직에 대한 작업 주문 관리 쿼리 규칙 사용 [Security Center 1.5의 새로운 기능 및 2.0에서 업데이트됨]
- 플로우 컨텍스트 읽기 액세스 제한[Security Center 1.5의 새로운 기능]
- 정책 기반 세션 액세스 모바일 새로 고침 토큰 간격 제한 [Security Center 1.5의 새로운 기능]
- 모바일에 대한 정책 기반 세션 액세스 사용 [Security Center 1.5의 새로운 기능]
- 비활성 사용자의 로그인 방지 [Security Center 1.5의 새로운 기능]
- 이벤트 관리 할당 그룹 관리자 역할 구성[Security Center 1.5의 새로운 기능]
- HR 케이스 관리용 에이전트 작업 공간의 보안 범위 적용 [Security Center 1.5의 새로운 기능 및 2.0에서 업데이트됨]
- 보안 범위 라이센스 및 허가 플레이북 적용 [Security Center 1.5의 새로운 기능 및 2.0에서 업데이트됨]

기준선 버전 2.0에 대한 새로운 강화 설정

Security Center 기준 버전 2.0에서 새로운 강화 설정이 릴리스되었습니다.

- 보관 테이블 ACL이 선택되어 있는지 확인 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 애플리케이션 범위 제한 적용[Security Center 1.3의 새로운 기능 및 1.5에서 제거됨]
- 강화된 Java 보안 관리자 사용 [Security Center 1.3의 새로운 기능]
- 인증서 해지 확인 [Security Center 1.3의 새로운 기능]
- 모바일 애플리케이션을 백그라운드로 지정할 때 붙여 넣기 보드 지우기 필요 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 보호된 테이블 플러그인 사용 [Security Center 1.3의 새로운 기능]
- 엄격한 권한 상승 적용 [Security Center 1.3의 새로운 기능]
- 통합의 활성 세션 수명 제한 [Security Center 1.3의 새로운 기능]
- 비활성 세션을 사전 예방적으로 무효화 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]
- MID 감사 로그 사용[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 임포트 세트 API 내에서 보안 삽입 다중 작업 사용[Security Center 1.3의 새로운 기능]
- 네트워크 오류에 OCSP 검사 강제 적용 [Security Center 1.3의 새로운 기능 및 2.0에서 업데이트됨]
- 공유 대시보드에 보안 규칙 적용[Security Center 1.3의 새로운 기능]
- OAuth 매개 변수를 POST 본문으로 제한 [Security Center 1.3의 새로운 기능]
- GraphQL 엔드포인트에 대한 교육 및 예측 흐름에서 첨부 파일 크기 제한[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- GlideRecord 범위 펜싱 레거시 동작 사용 안 함[Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]
- 자격 증명 별칭 사용 적용[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 필요한 jms 연결 팩토리 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 학습 및 예측 흐름에서 첨부 파일 크기 제한 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 세션 감사 이벤트 기록[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 서비스 카탈로그 항목 추가 페이지에 액세스하려면 쓰기 권한 필요[Security Center 1.3의 새로운 기능]
- 활성 세션 시간 제한 예외 역할 정의[Security Center 1.3의 새로운 기능]
- 인증서 기반 인증이 적용되지 않음 [Security Center 1.3의 새로운 기능]
- 정보 요청 플레이북에 대한 범위 지정 ACL 액세스 강제 적용 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 문서에 대한 사용자 주석 숨기기 [Security Center 1.3의 새로운 기능]
- 대시보드 생성/삭제에 액세스 확인이 필요한지 확인 [Security Center 1.3의 새로운 기능 및 2.0에서 업데이트됨]
- 장치 암호화 및 암호 요구 사항 강제 적용 [Security Center 1.3의 새로운 기능]
- AttachmentCreator SOAP Web Service에서 파일 MIME 형식 확인[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 인증서 해지 확인 [Security Center 1.3의 새로운 기능]
- HR 앱에서 ACL 평가에 대한 가장 확인[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 고객 서비스 애플리케이션에서 게스트 워크업 경험에 대해 captcha 필요[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- 이벤트 관리 HTTP 프로세서에서 인증 필요[Security Center 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨]
- 게스트의 활성 세션 수명 제한 [Security Center 1.3의 새로운 기능]
- 대상 복제 사용 안 함[Security Center 1.3의 새로운 기능]
- svg 파일에 대한 안전한 콘텐츠 보안 정책 설정 [Security Center 1.3의 새로운 기능]
- 안티-CSRF 토큰 유효성 검사 시간 [Security Center 1.3의 새로운 기능]
- 기술 자료 액세스 제한[Security Center 1.3의 새로운 기능]
- 공공 부문 디지털 서비스에 범위 보안 적용[Security Center 1.3의 새로운 기능]
- 개인 이메일에서 HR 케이스 업데이트 제한 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]
- UI 활성 세션 수명 제한 [Security Center 1.3의 새로운 기능]
- 보안 참조 정책 적용[Security Center 1.3의 새로운 기능]

업데이트된 강화 설정

업데이트된 강화 설정은 각 베이스라인 릴리스에 대해 세분화됩니다.

베이스라인 버전 5.0에 대한 업데이트된 강화 설정

일부 강화 설정은 Security Center 기준 버전 5.0 릴리스로 업데이트되었습니다.

베이스라인 버전 5에는 기록 간 스타일과 일관성을 위한 간단한 설명에 대한 몇 가지 업데이트가 포함되어 있습니다. 또한 속성이 sys_property 테이블에서 제거된 경우 기본값의 정확도를 개선하기 위해 많은 속성 관련 스크립트가 업데이트되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
SOAP 요청에 대해 권한 부여 필요 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.basicauth.required.soap* 존재하고 true 값으로 설정되어 있는지 확인합니다. 또는 속성 glide.soap.require_ws_security true로 설정하고 제품 문서에 따라 WS 보안 프로파일을 구성하여 WS 보안에 대한 인스턴스를 구성하십시오. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.basicauth.required.soap* true 값으로 설정되어 있는지 확인합니다. 또는 속성을 *glide.soap.require_ws_security* 예로 설정하고 제품 설명서에 따라 WS 보안 프로파일을 구성하여 WS 보안에 대한 인스턴스를 구성하십시오.
네트워크 오류에 OCSP 검사 강제 적용 [Security Center 1.3의 새로운 기능 및 2.0에서 업데이트됨]	• 새 정정: 속성이 *com.glide.communications.httpclient.ocsp_allow_* 존재하고 false로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *com.glide.communications.httpclient.ocsp_allow_* false로 설정되어 있는지 확인합니다.
외부 콘텐츠 URL 사용 안 함[Security Center 2.0에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.ui.url.external.content* 존재하고 false 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.ui.url.external.content* false로 설정되어 있는지 확인합니다. • 새로운 CVSS 점수: 7.2 • 이전 CVSS 점수: 8.1 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.xml.entity.whitelist* 존재하고 "http://java.sun.com/j2ee/dtds/"로 설정되어 있는지, Glide 속성이 *glide.xml.entity.whitelist.enabled* 존재하고 true 값으로 설정되어 있는지

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.xml.entity.whitelist* "http://java.sun.com/j2ee/dtds/" 으로 설정되고 속성이 *glide.xml.entity.whitelist.enabled* 예로 설정되어 있는지 확인합니다.
인증되지 않은 게시된 보고서 사용 안 함[Security Center 2.0에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.report.published_reports.enabled* 존재하고 false 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.report.published_reports.enabled* false로 설정되어 있는지 확인합니다.
암호 재설정 정책 검사 사용 [Security Center 2.0에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.enable.password_policy* 존재하고 true 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.enable.password_policy* 예로 설정되어 있는지 확인합니다.
GlideXMLUtil 스크립트에 대한 엔터티 확장 임계치 최소화[Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새 정정: 속성이 *glide.xmlutil.max_entity_expansion* 3000 이하로 설정되어 있는지 확인합니다. 인스턴스가 Washington 이상이고 sys_properties 레코드가 없으면 기본 암시적 값은 3000입니다. 인스턴스가 Washington 이하인 경우 인스턴스 관리자가 이름과 *glide.xmlutil.max_entity_expansion* 값이 3000인 sys_properties 레코드를 생성하는 것이 좋습니다. • 이전 정정: 속성이 *glide.xmlutil.max_entity_expansion* 3000 이하로 설정되어 있는지 확인합니다.
아웃바운드 SSLv2/SSLv3 연결 사용 안 함 [Security Center 1.3에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.outbound.sslv3.disabled* 존재하고 true 값으로 설정되어 있는지

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.outbound.sslv3.disabled* 예로 설정되어 있는지 확인합니다. **중요사항:** 속성 값은 *glide.outbound.sslv3.disabled* 안전한 재정의이며 변경 후에는 변경할 수 없습니다.
GlideRecord 범위 펜싱 레거시 동작 사용 안 함 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: GlideRecord 범위 펜싱 레거시 동작 사용 안 함 • 이전의 간단한 설명: GlideRecord 범위 펜싱 레거시 동작 사용
업로드된 MIME 유형 제한 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새 정정: 속성이 *glide.security.file.mime_type.validation* 존재하고 true로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.security.file.mime_type.validation* 예로 설정되어 있는지 확인합니다.
중첩 식에 대해 Jelly JS 보간 보호 사용 [Security Center 2.0에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.ui.jelly.js_interpolation.protect_nested_* 존재하고 true 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.ui.jelly.js_interpolation.protect_nested_* 예로 설정되어 있는지 확인합니다.
LDAP 인증에서 SSL 사용[Security Center 1.5 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
UserCookie 버전 3.1 사용 [Security Center 2.0에서 업데이트됨]	• 새로운 설명 : UserCookie v3는 속성이 *glide.ui.secure.cookies.use_kmf is disabled* 다음과 같은 경우에만 생성됩니다. UserCookie v3는 HMAC에 대한 비밀 키를 소스 코드에 저장하고 모든 고객에게 동일하기 때문에 안전하지 않습니다. 이를 통해 악의적인 행위자가 사용자 세션을 하이재킹하려는 시도에 이 하나의 비밀 키를 사용할 수 있습니다. 속성을 *glide.ui.secure.cookies.use_kmf* true로 설정하면 UserCookie v3.1이 사용되며

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	비밀 키가 KMF와 같은 보안 스토리지에 저장됩니다. • 이전 설명: UserCookie v3는 속성이 *glide.ui.secure.cookies.use_kmf* 비활성화된 경우에만 생성됩니다. UserCookie v3는 HMAC에 대한 비밀 키를 소스 코드에 저장하고 모든 고객에게 동일하기 때문에 안전하지 않습니다. 이를 통해 악의적인 행위자가 사용자 세션을 하이재킹하려는 시도에 이 하나의 비밀 키를 사용할 수 있습니다. • 새 정정: 속성이 *glide.ui.secure.cookies.use_kmf* 존재하고 true로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.ui.secure.cookies.use_kmf* 예로 설정되어 있는지 확인합니다. 즉, UserCookie v3.1이 사용되며 비밀 키가 KMF와 같은 보안 저장소에 저장됩니다.
12시간 이하로 암호 재설정 OTP 수명 설정 [Security Center 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
사용자 가장 기록 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새 정정: 속성이 *glide.sys.log_impersonation* 존재하고 true로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 속성이 *glide.sys.log_impersonation* 예로 설정되어 있는지 확인합니다.
필요한 jms 연결 팩토리 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
대시보드 생성/삭제에 액세스 확인이 필요한지 확인 [Security Center 1.3의 새로운 기능 및 2.0에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.processors.check_access_before_process* 존재하고 true 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: 값이 *glide.processors.check_access_before_process* 항상 예인지 확인합니다.
비활성 세션을 사전 예방적으로 무효화 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]	• 새 정정: Glide 속성이 *glide.active.session.timeout.invalidate.session* 존재하고 true 값으로 설정되어 있는지

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다. • 이전 정정: Glide 속성을 *glide.active.session.timeout.invalidate.session* true로 설정합니다.
HR 케이스 관리용 에이전트 작업 공간의 보안 범위 적용 [Security Center 1.5의 새로운 기능 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
보안 범위 라이센스 및 허가 플레이북 적용 [Security Center 1.5의 새로운 기능 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
다운로드 가능한 MIME 유형 제한 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새로운 설명: 속성이 *glide.ui.attachment.force_download_all_mime_type* 예 *glide.ui.attachment.download_mime_types* 로 설정되면 속성이 재정의되어 모든 MIME 유형이 브라우저에서 렌더링되지 않고 다운로드됩니다. 예를 들어, 텍스트/html을 다운로드하면 HTML 파일이 브라우저에서 인라인으로 표시되지 않고 파일로 클라이언트에 다운로드되어 XSS 공격을 방지합니다. XSS는 더 많은 횡적 이동이 가능한 관리자와 같은 더 높은 역할로 쉽게 얻을 수 있는 권한 에스컬레이션으로 이어질 수 있습니다. • 이전 설명: 속성이 *glide.ui.attachment.force_download_all_mime_type* 예로 설정되지 않은 경우 *glide.ui.attachment.download_mime_types* 속성이 재정의되어 모든 MIME 유형이 브라우저에서 렌더링되지 않고 다운로드됩니다. 예를 들어, 텍스트/html을 다운로드하면 HTML 파일이 브라우저에서 인라인으로 표시되지 않고 파일로 클라이언트에 다운로드되어 XSS 공격을 방지합니다. XSS를 사용할 수 있는 기능은 더 많은 측면 이동을 수행할 수 있는 관리자와 같은 더 높은 역할로 쉽게 얻을 수 있는 권한 에스컬레이션으로 이어질 수 있습니다. • 새 정정: 속성이 *glide.ui.attachment.force_download_all_mime_type* true로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 없는 경우 기본값은 false입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 이전 정정: 속성이 *glide.ui.attachment.force_download_all_mime_typ* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
제한된 다운로드 가능한 MIME 유형 정의 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
감염된 파일 다운로드 사용 안 함[Security Center 1.5 및 2.0에서 업데이트됨]	• 새로운 설명: 속성이 *com.glide.snap.infected_download_allowed* 예로 설정되면 바이러스 백신 서비스가 다운되거나 연결할 수 없는 경우 사용자가 검사되지 않은 첨부 파일을 계속 다운로드할 수 있습니다. 즉, 사용자가 악성 파일을 다운로드하여 사용자의 데스크톱을 감염시킬 위험이 있습니다(장치에 다른 엔드포인트 보호가 없는 경우). • 이전 설명: *com.glide.snap.infected_download_allowed* 권장 값인 False로 설정하지 않으면 검사되지 않은 악성 파일을 다운로드하여 사용자의 데스크톱을 감염시킬 위험이 있습니다. • 새 정정: 속성이 *com.glide.snap.infected_download_allowed* false로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *com.glide.snap.infected_download_allowed* False로 설정되어 있는지 확인합니다.
GlideSystemUserSession 스크립팅 가능한 API에 대한 접근 제한 [보안 센터 1.3 및 2.0에서 업데이트됨]	• 새로운 설명: *gs.addErrorMessageNoSanitizationMessaging()* 및 *gs.addInfoMessageNoSanitization()* 은 로깅 및 알림에 스크립팅 환경 내에서 사용됩니다. 이 속성이 권장 값인 false로 설정되지 않은 경우 샌드박스에서 이 두 가지를 모두 사용할 수 있습니다. 샌드박스는 인증되지 않은 역할 사용자가 사용할 수 있는 권한이 낮은 스크립팅 환경입니다. 이 두 가지 방법 모두 사용자에게 삭제되지 않은 입력을 표시하는 데 사용할 수 있습니다. 삭제되지 않은 입력에 사용자의 브라우저에서 실행되는 위험한 코드가 포함될 수 있으므로 사용자에게 삭제되지 않은 입력을 표시하는 것은 위험합니다. 이는 기존의 반사된 XSS 공격에 활용될 수 있습니다. 반영된 XSS 공격은 세션 하이재킹을 비롯한 여러 시나리오에서 사용될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 이전 설명: Glide 스크립팅 샌드박스 내의 메시징은 로깅 목적으로 사용됩니다. 이 삭제되지 않은 오류 함수를 호출하면 플랫폼이 반영된 XSS 공격에 노출됩니다. XSS 공격은 다른 사람의 세션 쿠키를 훔쳐 쉽게 권한 에스컬레이션을 허용할 수 있습니다. 권장 값인 false로 설정되지 않은 경우 *glide.sandbox.usersession.allow_unsanitized_mes* 삭제되지 않은 오류 메시징 함수 *addErrorMessageNoSanitization* 및 *addInfoMessageNoSanitization* 을 스크립트에 사용할 수 있습니다.
서비스 조직에 대한 작업 주문 관리 쿼리 규칙 사용 [Security Center 1.5의 새로운 기능 및 2.0에서 업데이트됨]	• 새로운 설명: 예로 설정될 경우 sn_query_rule 테이블의 규칙/필터는 쿼리 비즈니스 규칙과 읽기 ACL을 통해 로그인한 사용자에게 현장 서비스 관리 관련 테이블(작업 주문 및 작업 주문 작업)에 대한 읽기 권한을 결정하는 데 사용됩니다. 아니요인 경우 쿼리 규칙에 따라 기록이 필터링되지 않습니다. 쿼리 비즈니스 규칙은 보안 확인을 추가합니다. 특히 이 속성은 할당된 영역 또는 영역 구성원 자격에 따라 에이전트, 한정자 및 디스패처에 대한 기록을 필터링합니다. 기록을 읽을 때는 최소 권한의 원칙을 따르는 것이 가장 좋습니다. 이 속성을 예로 설정하지 않으면 현장 서비스 관리 테이블에서 데이터 노출 위험이 증가할 수 있습니다. • 이전 설명: 예로 설정되면 sn_query_rule 테이블의 규칙/필터는 쿼리 비즈니스 규칙 및 읽기 ACL을 통해 로그인한 사용자에게 현장 서비스 관리 관련 테이블(작업 주문 및 작업 주문 작업)에 대한 읽기 권한을 결정하는 데 사용됩니다. 아니요인 경우 쿼리 규칙에 따라 기록이 필터링되지 않습니다. 쿼리 비즈니스 규칙은 보안 확인을 추가합니다. 특히 이 속성은 할당된 영역 또는 영역 구성원 자격에 따라 에이전트, 한정자 및 디스패처에 대한 기록을 필터링합니다. 기록을 읽을 때는 최소 권한의 원칙을 따르는 것이 가장 좋습니다.
외부 사용자 등록을 위한 전자 메일 도메인 제한 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로운 설명: 이 *sn_ext_usr_reg.allowed_email_domains* 속성은 ServiceNow 인스턴스에 직접 등록할 수 있는 이메일 주소를 정의합니다. 형식은 domain1.com,domain2.com 같은 허용 가능한 이메일 도메인의 쉼표로 구분된 목록이어야 하며 example@domain2.com 와 같은 이메일이 허용됩니다. 이 허용 가능한 도메인 목록으로 설정되지 않은 경우 *sn_ext_usr_reg.allowed_email_domains* 이메일 주소가 있는 사용자는 인스턴스에

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	계정을 등록할 수 있습니다. 정의되지 않은 경우 악의적인 행위자는 원치 않는 도메인의 이메일 주소를 사용해 등록을 수행하여 인스턴스에 대한 인증된 액세스 권한을 얻을 수 있습니다. • 이전 설명: 이 *sn_ext_usr_reg.allowed_email_domains* 속성은 ServiceNow 인스턴스에 직접 등록할 수 있는 이메일 주소를 정의합니다. 이 허용 가능한 도메인 목록으로 설정되지 않은 경우 *sn_ext_usr_reg.allowed_email_domains* 이메일 주소가 있는 사용자는 인스턴스에 계정을 등록할 수 있습니다. 정의되지 않은 경우 악의적인 행위자는 원치 않는 도메인의 이메일 주소를 사용해 등록을 수행하여 인스턴스에 대한 인증된 액세스 권한을 얻을 수 있습니다.
닷워킹 필드에 도메인 분리 적용 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새 설명: 이 속성은 닷워킹 필드에 도메인 분리 기능을 적용하기 위해 조인 쿼리에 도메인 분리 조건이 부여되는지 여부를 통제합니다. *glide.sys.domain.include_domain_condition_on_jo* 가 도메인 분리를 사용하는 인스턴스에서 권장 값인 true로 설정되지 않은 경우 특정 도메인과 공유할 수 없는 중요한 정보가 공개될 수 있습니다. 구성요소가 안전하지 않은 교차 도메인 쿼리에 의존하는 경우 인스턴스에 보통 정도의 기능적 영향이 있을 수 있습니다. 인스턴스는 활성화하기 전에 하위 프로덕션 환경에서 테스트해야 합니다. • 이전 설명: 이 속성은 닷워킹 필드에 도메인 분리 기능을 적용하기 위해 조인 쿼리에 도메인 분리 조건이 부여되는지 여부를 통제합니다. *glide.sys.domain.include_domain_condition_on_jo* 가 도메인 분리를 사용하는 인스턴스에서 권장 값인 true로 설정되지 않은 경우 특정 도메인과 공유할 수 없는 중요한 정보가 공개될 수 있습니다.
URL 허용 목록 검사 강제 적용[Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로 정정: 속성이 *glide.security.url.whitelist.strict_check* true로 설정되어 있는지 또는 속성이 *glide.security.url.whitelist* 값으로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.security.url.whitelist.strict_check* "예"로 설정되고 속성이 *glide.security.url.whitelist* 값으로 설정되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
SOAP 요청의 게스트 사용자 설정[Security Center 1.3 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
백그라운드 스크립트에 대한 액세스 제한 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새 설명: 이 속성에는 스크립트 백그라운드 모듈에 액세스하는 데 필요한 역할이 있습니다. 가 admin의 권장 값 및 기본 값으로 설정되지 않은 경우 *glide.script_processor.admin* 권한이 더 낮은 사용자가 인스턴스에서 백그라운드 스크립트를 실행할 수 있습니다. 이렇게 하면 ACL 시스템을 완전히 바이패스하여 테이블에 대한 전체 액세스가 허용됩니다. • 이전 설명: 이 속성에는 스크립트 백그라운드 모듈에 액세스하는 데 필요한 역할이 있습니다. 가 권장 값인 admin, security_admin 또는 maint로 설정되지 않은 경우 *glide.script_processor.admin* 권한이 더 낮은 사용자가 인스턴스에서 백그라운드 스크립트를 실행할 수 있습니다. 이렇게 하면 ACL 시스템을 완전히 바이패스하여 테이블에 대한 전체 액세스가 허용됩니다. • 새 정정: 속성이 *glide.script_processor.admin* 관리자로 설정되어 있는지 확인합니다. 이 값은 인스턴스의 기본값입니다. • 이전 정정: 속성이 *glide.script_processor.admin* 관리자, security_admin 또는 유지관리 역할로 설정되어 있는지 확인합니다.
인증서 체인 및 호스트 이름 확인 [Security Center 1.3의 새로운 기능 및 2.0에서 업데이트됨]	• 새로운 설명: Glide 속성이 *com.glide.communications.httpclient.verify_host* 보안 값인 예로 설정되지 않은 경우 ServiceNow 인스턴스에서 시작된 TLS 연결 중에 원격 호스트가 제공하는 호스트 이름 및 인증서 체인의 유효성이 확인되지 않습니다. 이로 인해 TLS 연결의 보안이 손상되고 두 당사자 간의 통신을 가로채는 중간자 공격이 허용될 수 있습니다. 이로 인해 민감한 데이터가 공개될 수 있습니다. • 이전 설명: 예로 설정되지 않은 경우 *com.glide.communications.httpclient.verify_host* 두 당사자 간의 통신을 가로채는 중간자 공격이 허용될 수 있습니다. 이 속성을 안전하지 않은 값으로 설정하면 해지 상태 확인을 통해 인증서 체인의 모든 인증을 평가하는 인증서 검증 프로세스를 사용할 수 없습니다. http 클라이언트가 잠재적으로 유해한 호스트 이름에 연결하지 못하도록 하려면 이 속성을 예로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
잘못된 암호 재설정 시도에 대한 잠금 시간 제어 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: *Control Lockout Time for Invalid Password Reset Attempts* • 이전 간단한 설명: *Minimize Reset Password Request Max Attempts Window Duration* • 새로운 설명: 이 *password_reset.request.max_attempt_window* 속성은 사용자가 로 설정된 최대 실패 시도 횟수를 초과한 후 암호를 재설정하거나 변경하기 위해 기다려야 하는 시간(분) *password_reset.request.max_attempt property*을 정의합니다. 속성에 대한 *password_reset.request.max_attempt_window* 시간(분)이 짧으면 암호 재설정을 더 많이 시도할 수 있으므로 무차별 암호 대입이 성공할 위험이 높아집니다. 기본값은 1440분입니다. • 이전 설명: *password_reset.request.max_attempt_window* 권장 값인 1440 이하로 설정되지 않은 경우 최대 잘못된 인증 시도 횟수 후에 계정이 잠기지 않으므로 계정 무차별 암호 대입을 수행할 수 있습니다. • 새 정정: 속성이 *password_reset.request.max_attempt_window* 1440 이상으로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *password_reset.request.max_attempt_window* 1440 이하로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
GlideRecord 범위 펜싱 레거시 동작 사용 안 함 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: *Disable GlideRecord Scope Fencing Legacy Behavior* • 이전 간단한 설명: *Enable GlideRecord Scope Fencing Legacy Behavior* • 새 정정: Glide 속성을 *glide.record.legacy_cross_scope_access_policy_i* false로 설정합니다. sys_properties 테이블에 없는 경우 기본값은 true입니다. • 이전 정정: Glide 속성을 *glide.record.legacy_cross_scope_access_policy_i* false로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
잘못된 암호 재설정 시도 제한 [Security Center 1.3에서 업데이트되고 2.0에서 업데이트됨]	• 새로운 간단한 설명: *Limit Invalid Password Reset Attempts* • 이전 간단한 설명: *Minimize Reset Password Request Max Attempt Allowance*

베이스라인 버전 4.0에 대한 업데이트된 강화 설정

베이스라인 버전 4.0 릴리스 보안 센터 에서 일부 강화 설정이 업데이트되었습니다.

베이스라인 버전 4.0에는 기록 간의 스타일과 일관성을 위한 간단한 설명에 대한 몇 가지 업데이트가 포함되어 있습니다. 또한 속성이 sys_property 테이블에서 제거된 케이스에 대한 기본값의 정확도를 개선하기 위해 많은 속성 관련 스크립트도 업데이트되었습니다.

설명서	업데이트
SOAP 요청에 대해 권한 부여 필요 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새 기술 구성 이름: *glide.basicauth.required.soap, glide.soap.require_ws_security* • 이전 기술 구성 이름: *glide.basicauth.required.soap* • 새로운 설명: Glide 속성은 *glide.basicauth.required.soap* 인스턴스에 SOAP를 요청하는 데 기본 인증이 필요한지 여부를 제어합니다. 권장 값인 true로 설정되지 않은 경우 *glide.basicauth.required.soap* SOAP 작업을 수행하는 인증되지 않은 사용자는 soap.guest 사용자에 매핑됩니다. 이렇게 하면 미인증 사용자가 인스턴스에 로그인한 사용자인 것처럼 인스턴스에서 작업을 수행할 수 있습니다. 내에서 *com.glide.soap.guest_user* 정의한 사용자에게 추가 역할이 할당되면 추가적인 영향이 있을 수 있습니다. • 이전 설명: Glide 속성은 *glide.basicauth.required.soap* 인스턴스에 SOAP를 요청하는 데 인증이 필요한지 여부를 제어합니다. *glide.basicauth.required.soap* 가 권장 값인 true로 설정되지 않은 경우 인스턴스의 SOAP 요청에 대해 인증이 비활성화됩니다. 관리자 또는 유지 관리 수준 작업에 대한 인증되지 않은 액세스를 허용합니다. 인스턴스 내의 보안 제어를 무효화합니다. • 새 정정: 속성이 *glide.basicauth.required.soap* true 값으로 설정되어 있는지 확인합니다. 또는 속성을 *glide.soap.require_ws_security*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	예로 설정하고 제품 설명서에 따라 WS 보안 프로파일을 구성하여 WS 보안에 대한 인스턴스를 구성하십시오. • 이전 정정: 속성이 *glide.basicauth.required.soap* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
이스케이프 Jelly 스크립트[Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 설명: 이 속성은 출력 스트림에 기록되기 전에 포함된 모든 JS 및 HTML 문자열을 이스케이프하여 여러 XSS 문제가 발생하지 않도록 합니다. *glide.ui.escape_all_script* 권장 값인 true로 설정되지 않은 경우 Jelly에 주입된 스크립트의 이스케이프가 비활성화됩니다. 이러한 완화가 없으면 플랫폼은 다양한 스크립트 삽입 공격에 널리 개방됩니다. 공격자는 인스턴스에서 임의의 Rhino 스크립트를 실행할 수 있습니다. • 이전 설명: 다음 속성은 〈j:jelly〉에 포함된 모든 JS 및 HTML 문자열을 이스케이프합니다. </j:jelly> 출력 스트림에 기록되기 전에 여러 XSS 문제가 발생하지 않도록 합니다. 권장 값인 "예"로 설정되지 않은 경우 *glide.ui.escape_all_script* Jelly에 주입된 스크립트의 이스케이프가 비활성화됩니다. 이러한 완화가 없으면 플랫폼은 다양한 스크립트 삽입 공격에 널리 개방됩니다. 공격자는 인스턴스에서 임의의 Rhino 스크립트를 실행할 수 있습니다.
사용자가 CSRF 유효성 검사를 바이패스하기 위한 경고를 수락하지 못하도록 방지 〔보안 센터 1.3 및 1.5에서 업데이트됨〕	• 새로운 간단한 설명: 사용자가 CSRF 유효성 확인을 바이패스하기 위해 경고를 수락하지 못하도록 방지 • 이전 간단한 설명: CSRF 토큰 엄격한 유효성 확인 강제 적용 • 새 설명: 이 속성은 사용자가 잠재적으로 악의적인 요청을 인스턴스로 보낼 수 있는 경고를 수락할 수 없도록 합니다. 이 경고는 피해자의 다른 활성 세션 중 하나에 속하는 안티-CSRF 토큰이 일치하지 않아 POST 요청이 실패할 때 나타납니다. 권장 값인 true로 설정되지 않은 경우 *glide.security.csrf.strict.validation.mode* 공격자는 피해자에게 속한 다른 활성 세션에서 유출된 안티-CSRF 토큰을 사용하여 CSRF 공격을 공식화할 수 있습니다. 인스턴스에 대한 POST 요청에는 사용자의 현재 세션과 일치하는 sysparm_ck 또는 X-UserToken

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	내에 안티-CSRF 토큰이 포함되어 있습니다. 안티-CSRF 토큰이 사용자의 다른 활성 세션 중 하나에 대신 연결된 경우 POST 요청은 이 속성이 false로 설정된 경우 사용자가 사용할 수 있는 계속 단추를 사용하여 security_interceptor.do에 대한 302 리디렉션을 반환합니다. 이 단추를 클릭하면 인스턴스에 요청을 다시 제출합니다(단, 이제 유효한 안티-CSRF 토큰이 있는 경우는 제외). 이 특성을 예로 설정하면 security_interceptor.do 페이지로의 302 리디렉션에 계속 단추가 표시되지 않으며 사용자가 요청을 다시 제출할 수 없습니다. CSRF 공격이 성공하면 공격자는 피해자가 수행할 수 있는 모든 작업을 효과적으로 수행할 수 있습니다. • 이전 설명: 이 속성을 사용하면 CSRF 토큰의 재사용을 방지하는 CSRF 토큰의 엄격한 유효성 검사를 사용할 수 있습니다. *glide.security.csrf.strict.validation.mode* 권장 값인 true로 설정되지 않은 경우 CSRF 토큰을 다시 사용할 수 있으므로 CSRF 공격에 노출될 수 있습니다. • 새로운 CVSS 점수: 3.7 • 이전 CVSS 점수: 3.1
이벤트 관리 HTTP 프로세서에서 인증 필요 [Security Center 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨]	• 새로운 짧은 설명: 이벤트 관리 HTTP 프로세서에서 인증 필요 • 이전 간단한 설명: 이벤트 관리 HTTP 프로세서에서 인증 필요
안티-CSRF 토큰 사용[Security Center 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨]	• 새로운 설명: CSRF(교차 사이트 요청 위조)는 인증된 사용자가 현재 인증된 웹 응용 프로그램에 요청을 제출하도록 강제하는 공격입니다. CSRF 공격은 웹 응용 프로그램이 인증된 사용자에 대해 가지고 있는 신뢰를 악용합니다. 이 속성을 사용하면 보안 토큰 사용을 식별하고 수신 요청을 확인할 수 있습니다. 이 토큰은 교차 사이트 요청 위조 공격을 방지하는 데 사용됩니다. *glide.security.use_csrf_token* 권장 값인 true로 설정되지 않은 경우 CSRF를 사용할 수 있습니다. • 이전 설명: CSRF(교차 사이트 요청 위조)는 인증된 사용자가 현재 인증된 웹 애플리케이션에 요청을 제출하도록 강제하는 공격입니다. CSRF 공격은 웹 응용 프로그램이 인증된 사용자에 대해 가지고 있는 신뢰를 악용합니다. 이 속성을 사용하면 보안 토큰 사용을 식별하고 수신 요청을 확인할 수 있습니다. 이 토큰은 교차 사이트

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	요청 위조 공격을 방지하는 데 사용됩니다. *glide.security.use_csrf_token* 권장 값인 true로 설정되지 않은 경우 CSRF를 사용할 수 있습니다.
가상 에이전트 내에서 HTML 위생 검사 사용 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 가상 에이전트 내에서 HTML 위생 검사 사용 • 이전 간단한 설명: HTML 위생 검사 사용 • 새로운 설명: 이 속성은 HtmlSanitizerService의 사용 여부를 제어합니다. *com.glide.cs.html.sanitizer.enabled* true로 설정되지 않은 경우 VA 웹 클라이언트에 저장된 XSS(교차 사이트 스크립팅) 공격이 가능합니다. • 이전 설명: 이 속성은 HTMLSanitezerService의 사용 여부를 제어합니다. *com.glide.cs.html.sanitizer.enabled* true로 설정되지 않은 경우 VA 웹 클라이언트에 저장된 XSS(교차 사이트 스크립팅) 공격이 가능합니다.
명시적 외부 역할에 대한 내부 액세스 거부 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새 기술 구성 이름: *glide.security.explicit_roles.enable_internal_u* • 이전 기술 구성 이름: *glide.security.explicit_roles.enable_internal_u* • 새 설명: 이 속성은 외부 사용자에게 snc_internal 역할을 할당하지 못하게 합니다. *glide.security.explicit_roles.enable_internal_u* 권장 값 true로 설정된 경우 신뢰할 수 없는 사용자 클래스 목록에 snc_external 역할을 할당하는 maint-protected *glide.security.explicit_roles.internal_user_bla* *property* 매개변수를 적용합니다. 값이 false *glide.security.explicit_roles.internal_user_bla* 로 설정되면 속성이 무시됩니다. 이 속성을 잘못 구성하면 외부 사용자 계정이 내부 정보에 대한 액세스 권한을 얻을 위험이 높아집니다. • 이전 설명: 이렇게 하면 외부 사용자에게 snc_internal 역할이 할당되지 않습니다. 가 권장 값인 true로 설정되지 않고 *glide.security.explicit_roles.internal_user_bla* 속성이 신뢰할 수 없는 사용자 클래스 목록으로 설정되지 않은 경우 *glide.security.explicit_roles.enable_internal_u* 지정된 역할에 snc_external 역할 대신 snc_internal 역할을 할당할 수 있습니다. 목록이 비어 있으면 기본적으로 모든 사용자에게 snc_internal 역할이

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	할당됩니다. 속성에는 최소한 기본 역할 csm_consumer_user, customer_contact이 포함되어야 합니다. 이러한 속성을 잘못 구성하면 외부 사용자 계정이 내부 정보에 액세스할 위험이 높아집니다. • 새 정정: 속성이 *glide.security.explicit_roles.enable_internal_u* true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.security.explicit_roles.enable_internal_u* true로 설정되어 있고 속성에 *glide.security.explicit_roles.internal_user_bla* 위험한 항목 csm_consumer_user customer_contact이 포함되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
WSDL 요청에 대해 인증 필요 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 설명: *glide.basicauth.required.wsdl* 권장 값인 예로 설정되지 않은 경우 WSDL 요청에 대한 기본 인증이 비활성화됩니다. WSDL은 인스턴스 테이블 스키마와 같은 웹 서비스를 설명하는 데 사용되는 프로토콜이며 테이블 내에서 데이터를 공유하기 위한 메커니즘이 아닙니다. 이 속성을 예로 설정하면 미인증 사용자에게 테이블 스키마를 공개할 수 있습니다. • 이전 설명: *glide.basicauth.required.wsdl* 권장 값인 예로 설정되지 않은 경우 WSDL 요청에 대한 기본 인증이 비활성화됩니다. 이로 인해 인증되지 않은 사용자에게 정보가 공개될 수 있습니다. • 새로운 CVSS 점수: 5.3 • 이전 CVSS 점수: 4.3
URL 허용 목록 검사 강제 적용[Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
제한된 다운로드 가능한 MIME 유형 정의 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로운 짧은 설명: 제한된 다운로드 가능한 MIME 유형 정의 • 이전 간단한 설명: 다운로드 가능한 MIME 유형 제한 • 새로운 설명: text/html,image/svg,image/svg+xml,application/xml과 같은 위험한 항목이 포함된 경우

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	glide.ui.attachment.download_mime_types 브라우저에서 위험한 파일을 인라인으로 렌더링하여 XSS(Cross Sitte Scripting) 공격으로 이어질 수 있습니다. 이 속성은 브라우저에서 인라인으로 렌더링되지 않는 쉼표로 구분된 첨부 파일 MIME 유형의 목록입니다. 예를 들어 text/html을 포함하면 HTML 파일이 브라우저에서 인라인으로 표시되지 않고 첨부 파일로 클라이언트에 다운로드됩니다. 이 목록을 제대로 유지하면 교차 사이트 스크립팅 공격을 방지할 수 있습니다. • 이전 설명: text/html,image/svg,image/svg+xml,application/xml과 같은 위험한 항목이 포함된 경우 *glide.ui.attachment.download_mime_types* 브라우저에서 위험한 파일을 인라인으로 렌더링하여 XSS(Cross Sitte Scripting) 공격으로 이어질 수 있습니다. 이 속성은 브라우저에서 인라인으로 렌더링되지 않는 쉼표로 구분된 첨부 파일 MIME 유형의 목록입니다. 예를 들어 text/html을 포함하면 html 파일이 브라우저에서 인라인으로 표시되지 않고 첨부 파일로 클라이언트에 다운로드됩니다. 이 목록을 제대로 유지하면 교차 사이트 스크립팅 공격을 방지할 수 있습니다.
목록 뷰에서 HTML 이스케이프 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새 설명: 이 속성은 HTML 필드가 표시되는 목록 뷰를 정리하는 데 도움이 됩니다. 권장 값인 true로 설정되지 않은 경우 *glide.ui.escape_html_list_field* 악의적인 사용자가 양식 필드 내에 HTML 코드를 삽입하여 다른 클라이언트/사용자 세션에서 원치 않는 스크립트를 실행할 수 있습니다. 이는 공격자가 세션 정보와 중요한 데이터를 훔치는 데 활용할 수 있습니다. • 이전 설명: 다음 속성은 HTML 필드가 표시되는 목록 뷰를 정리하는 데 도움이 됩니다. 권장 값인 true로 설정되지 않은 경우 *glide.ui.escape_html_list_field* 악의적인 사용자가 양식 필드 내에 HTML 코드를 삽입하여 다른 클라이언트/사용자 세션에서 원치 않는 스크립트를 실행할 수 있습니다. 이는 공격자가 세션 정보와 중요한 데이터를 훔치는 데 활용할 수 있습니다.
외부 사용자 등록을 위한 전자 메일 도메인 제한 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: 외부 사용자 등록을 위한 이메일 도메인 제한 • 이전의 간단한 설명: 외부 사용자 등록을 위한 이메일 도메인 제한(플러그인 적용 가능성: 외부 사용자 등록)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 새로운 설명: 이 *sn_ext_usr_reg.allowed_email_domains* 속성은 ServiceNow 인스턴스에 셀프 등록할 수 있는 이메일 주소를 정의합니다. 이 허용 가능한 도메인 목록으로 설정되지 않은 경우 *sn_ext_usr_reg.allowed_email_domains* 이메일 주소가 있는 사용자는 인스턴스에 계정을 등록할 수 있습니다. 정의되지 않은 경우 악의적인 행위자는 원치 않는 도메인의 이메일 주소를 사용해 등록을 수행하여 인스턴스에 대한 인증된 액세스 권한을 얻을 수 있습니다. • 이전 설명: 허용 가능한 도메인의 허용 목록으로 설정되지 않은 경우 *sn_ext_usr_reg.allowed_email_domains* 악의적인 행위자가 원치 않는 도메인의 이메일 주소를 사용하여 등록을 수행할 수 있습니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
외부 사용자 등록에 Captcha 사용 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 외부 사용자 등록에 Captcha 사용 • 이전 간단한 설명: 외부 사용자 등록에 Captcha 사용(플러그인 적용 가능성: 외부 사용자 등록) • 규칙 스크립트: 탐지 정확도를 개선하기 위해 스크립트가 업데이트되었습니다.
외부 사용자 등록 링크 만료 기간 최소화 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 외부 사용자 등록 링크 만료 기간 최소화 • 이전의 간단한 설명: 외부 사용자 등록 링크 만료 기간 최소화(플러그인 적용 가능성: 외부 사용자 등록) • 규칙 스크립트: 탐지 정확도를 개선하기 위해 스크립트가 업데이트되었습니다.
감염된 파일 다운로드 사용 안 함[Security Center 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: Disallow Infected File Download • 오래된 간단한 설명: 감염된 파일 다운로드 사용 안 함 • 새 정정: 속성이 *com.glide.snap.infected_download_allowed* False로 설정되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 이전 정정: 속성이 *com.glide.snap.infected_download_allowed* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
AttachmentCreator SOAP Web Service에서 파일 MIME 형식 확인[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 설명: *glide.attachment.enforce_security_validation* 권장 값인 예로 설정되지 않은 경우 첨부 파일 MIME 유형에 대한 확인이 수행되지 않으며 잘못된 파일 확장자를 사용하여 위험한 파일이 시스템에 업로드될 수 있습니다. 이 속성을 true로 설정하면 파일이 올바른 파일 형식 확장자로 업로드됩니다. 최소한 MIME 형식 유효성 검사를 사용하여 파일 업로드의 유효성을 검사하는 것이 보안 베스트 프랙티스입니다. • 이전 설명: *glide.attachment.enforce_security_validation* 권장 값인 예로 설정하지 않으면 첨부 파일 MIME 유형에 대한 확인이 수행되지 않으며 잘못된 파일 확장자를 사용하여 위험한 파일이 시스템에 업로드될 수 있습니다. 이 속성을 true로 설정하면 파일이 올바른 파일 형식 확장자로 업로드됩니다. 최소한 MIME 형식 유효성 검사를 사용하여 파일 업로드의 유효성을 검사하는 것이 보안 베스트 프랙티스입니다. • 새 정정: 속성이 *glide.attachment.enforce_security_validation* true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.attachment.enforce_security_validation* 예로 설정되어 있는지 확인합니다.
MultiSSO 디버깅 사용 안 함[Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: MultiSSO 디버깅 사용 안 함 • 이전 간단한 설명: MultiSSO 디버깅 사용 안 함(플러그인 적용 가능성: 다중 제공자 SSO(Single Sign-On))
허용된 ServiceNow 내부 IP 주소 정의 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새 기술 구성 이름: *glide.ip.authenticate.strict* • 이전 기술 구성 이름: *glide.ip.authenticate.strict,glide.ip.authentic* • 새로운 설명: *glide.ip.authenticate.strict* 예로 설정되면 내부 ServiceNow 담당자와

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	시스템은 필수 IP 범위에서 인스턴스에 대한 인바운드 연결만 만들 수 있습니다. 이러한 제한으로 인해 ServiceNow는 필수 내부 인프라에 대한 인스턴스를 볼 수 있으며 기업 네트워크를 통해 지원 및 영업 직원과 같은 광범위한 ServiceNow 담당자가 액세스할 수 없게 됩니다. "예"로 설정하면 이 *glide.ip.authenticate.allow* 속성은 내부 ServiceNow 인바운드 연결을 부여하는 데 사용됩니다. true로 설정되지 않은 경우 정의된 *glide.ip.authenticate.allow* 더 광범위한 ServiceNow 내부 IP 범위를 사용하여 내부 ServiceNow 인바운드 연결을 부여합니다. • 이전 설명: 예로 설정된 경우 *glide.ip.authenticate.strict* 다음에 *glide.ip.authenticate.allow.secured* 지정된 IP 범위만 인스턴스에 대한 인바운드 연결을 만들 수 있습니다. 이 속성에는 필수 ServiceNow 내부 IP 범위(보안 VPN, DC) 목록만 포함되어 있습니다. *glide.ip.authenticate.allow.secured* 권장 값 또는 순열 "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" 또는 최신 값 목록 "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" IPv6 localhost를 Utah에 추가하는 경우 SN DataCenter 외부의 신뢰할 수 없는 소스를 허용하고 보안 VPN이 중요한 정보에 액세스하도록 허용할 수 있습니다. 인스턴스의 엔드포인트를 모니터링합니다. • 새 정정: 속성에 *glide.ip.authenticate.allow.secured* 신뢰할 수 있는 값만 포함되어 있고 속성이 *glide.ip.authenticate.strict* true로 설정되어 있는지 확인합니다. • 이전 정정: 속성에 *glide.ip.authenticate.allow.secured* "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"의 값만 포함되어 있고 속성이 *glide.ip.authenticate.strict* true로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
XMLDocument2 스트리밍 파서 내에서 엔터티 확장 사용 안 함 [Security Center 1.5에서 업데이트됨]	• 새로운 간단한 설명: XMLDocument2 스트리밍 파서 내에서 엔터티 확장 사용 안 함 • 이전 간단한 설명: 엔터티 확장 사용 안 함 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
닷워킹 필드에 도메인 분리 적용 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: 닷워킹 필드에 도메인 분리 적용 • 이전의 간단한 설명: 닷워킹 필드에 도메인 분리 적용(플러그인 적용 가능성: 도메인 분리) • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
CMDB 모델에 대한 권한 제한 [Security Center 1.3 및 1.5에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
모바일 애플리케이션을 백그라운드로 지정할 때 붙여 넣기 보드 지우기 필요 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 설명: 이 *glide.sg.clear_pasteboard_when_backgrounded* 속성은 앱이 백그라운드 모드가 된 후 ServiceNow 모바일 앱에서 복사한 텍스트가 클립보드 및 붙여넣기 보드에 보관되는지 여부를 제어합니다. 권장 값인 true로 설정되지 않은 경우 중요한 정보가 Android 또는 iOS 클립보드에 공개되어 디바이스의 다른 애플리케이션에 노출될 수 있습니다. • 이전 설명: 이 속성은 *glide.sg.clear_pasteboard_when_backgrounded* 앱에 포커스가 더 이상 없으면 ServiceNow 모바일 앱에서 복사한 텍스트가 클립보드/붙여넣기 보드에 보관되는지 여부를 제어합니다. 권장 값인 true로 설정되지 않은 경우 중요한 정보가 Android 또는 iOS 클립보드에 공개되어 디바이스의 다른 애플리케이션에 노출될 수 있습니다.
계정 복구 사용 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 계정 복구 사용 • 이전의 간단한 설명: 계정 복구 사용 (플러그인 적용 가능성: 복수 제공자 SSO(Single Sign-On))
SQL 오류 메시지 사용 안 함 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 설명: *glide.db.loguser* 권장 값인 false로 설정되지 않은 경우 최종 사용자에게 중요한 서버 측 오류 메시지가 표시될 수 있습니다. 오류 메시지에는 스택 추적 및 데이터베이스 구조에 대한 정보가 포함될 수 있으며, 이러한 정보는 전제 조건이 있는 경우 공격자에게 성공적인 SQL 주입을 수행하는

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	데 필요한 지식을 제공할 수 있습니다. 심층 방어로서 이러한 오류 메시지는 최종 사용자에게 표시되지 않아야 합니다. • 이전 설명: *glide.db.loguser* 권장 값인 false로 설정하지 않으면 최종 사용자에게 중요한 서버 측 오류 메시지가 표시될 수 있습니다.
상대 링크 적용[Security Center 1.3 및 1.5에서 업데이트됨]	• 새 설명: 이 *glide.cms.catalog_uri_relative* 속성은 /ess/catalog.do의 URI 매개변수에서 상대 링크를 적용합니다. *glide.cms.catalog_uri_relative* 권장 값인 true로 설정되지 않은 경우 URL은 enforceRelativeURL(url) 함수로 삭제되지 않습니다. 절대 URL은 매개변수 또는 필드 값의 일부로 사용될 때 보안 위험을 초래할 수 있으므로 소스 페이지를 상대방이 통제하는 웹 사이트로 리디렉션합니다. 이 속성은 서비스 포털로 대체된 레거시 CMS(콘텐츠 관리 시스템)에 영향을 미칩니다. • 이전 설명: 이 *glide.cms.catalog_uri_relative* 속성은 /ess/catalog.do의 URI 매개변수에서 상대 링크를 적용합니다. *glide.cms.catalog_uri_relative* 권장 값인 true로 설정되지 않은 경우 URL은 enforceRelativeURL(url) 함수로 삭제되지 않습니다. 절대 URL은 매개변수 또는 필드 값의 일부로 사용될 때 보안 위험을 초래할 수 있으므로 소스 페이지를 상대방이 통제하는 웹 사이트로 리디렉션합니다.
GlideXMLUtil 스크립트에 대한 엔터티 확장 임계치 최소화[Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: GlideXMLUtil 스크립트에 대한 엔터티 확장 임계치 최소화 • 이전의 간단한 설명: 엔터티 확장 임계치 최소화 • 새로운 설명: 이 속성은 XML 파서 내에서 엔터티 확장의 최대 양을 제어합니다. *glide.xmlutil.max_entity_expansion* 권장 값인 3,000 이하로 설정하지 않으면 GlideXMLUtil 구문 분석 스크립트가 서비스 거부 공격에 취약할 수 있습니다. • 이전 설명: 이 속성은 XML 파서 내에서 엔터티 확장의 최대 양을 제어합니다. *glide.xmlutil.max_entity_expansion* 권장 값인 3000 이하로 설정하지 않으면

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	XML 파서가 서비스 거부 공격에 취약할 수 있습니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
GlideRecord 범위 펜싱 레거시 동작 사용 안 함[Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]	• 새 설명: GlideRecord는 해당 액세스 수준으로 구성되지 않은 테이블에 대한 교차 범위 생성/업데이트 액세스 권한을 제공했습니다. 이 범위가 지정된 액세스 동작에 패치가 적용되었을 때 고객이 응용 프로그램이 중단되는 것을 방지하기 위해 속성이 *glide.record.legacy_cross_scope_access_policy_i* 작성되었습니다. 예일 때는 교차 범위 액세스가 레거시 동작(안전하지 않음)으로 대체됩니다. 이 속성은 범위 펜싱을 비활성화하여 범위가 지정된 앱이 전역 스크립트 인터페이스에 액세스할 수 있도록 허용합니다. 범위 펜싱 제한을 시행하는 것이 가장 좋습니다. 범위 지정은 애플리케이션이 최소 권한 원칙에 따라 명시적 액세스 권한이 있거나 범위 내에 있는 자원에만 액세스할 수 있도록 합니다. 이 기능을 비활성화하면 기밀성, 가용성 및 무결성에 영향을 미칠 수 있습니다. • 이전 설명: 레거시 동작으로 인해 허용되지 않는 테이블에 대한 작성/업데이트 접근 권한이 제공되었습니다. 이 범위가 지정된 액세스 동작에 패치가 적용되었을 때 레거시 고객의 애플리케이션이 중단되는 것을 방지하기 위해 속성이 *glide.record.legacy_cross_scope_access_policy_i* 작성되었습니다. 예일 때는 교차 범위 액세스가 레거시 동작(안전하지 않음)으로 대체됩니다. 이 속성은 범위 펜싱을 비활성화하여 범위가 지정된 앱이 전역 스크립트 인터페이스에 액세스할 수 있도록 허용합니다. 범위 펜싱 제한을 시행하는 것이 가장 좋습니다. 범위 지정은 애플리케이션이 최소 권한 원칙에 따라 명시적 액세스 권한이 있거나 범위 내에 있는 자원에만 액세스할 수 있도록 합니다. 이 기능을 비활성화하면 기밀성, 가용성 및 무결성에 영향을 미칠 수 있습니다.
업데이트된 버전의 MultiSSO 플러그인 사용[보안 센터 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 복수 SSO 플러그인의 업데이트된 버전 사용 • 이전 간단한 설명: 복수 SSO 플러그인의 업데이트된 버전 사용(플러그인 적용 가능성: 복수 제공자 SSO(Single Sign-On))
LDAP 인증에서 SSL 사용[Security Center 1.5 및 2.0에서 업데이트됨]	탐지 정확도를 개선하기 위해 스크립트가 업데이트되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
API 요청에 암호 재설정 강제 적용[Security Center 1.5에서 업데이트됨]	탐지 정확도를 개선하기 위해 스크립트가 업데이트되었습니다.
로그인 시 암호 정책 적용 안 함[Security Center 1.5에서 업데이트되고 2.0에서 제거됨]	• 새로운 설명: 속성을 *glide.apply.password_policy.on_login* False로 설정하면 로그인 시 암호 복잡도가 적용되지 않습니다. 속성을 True로 설정하면 암호 복잡성이 적용되고 조직 정책 준수 문제가 발생합니다. ASVS 4.03 v2.1.9 권장 사항에 따라: 허용되는 문자 유형을 제한하는 암호 작성 규칙이 없는지 확인합니다. 대문자나 소문자 또는 숫자 또는 특수 문자는 필요하지 않습니다. (C6) 암호 복잡성을 적용하는 대신 ASVS 권장 사항은 암호 길이에 대해 최소 12자의 길이를 적용하는 것입니다. 참조: OWASP ASVS v4.0 인증 • 이전 설명: 속성을 *glide.apply.password_policy.on_login* False로 설정하면 로그인 시 암호 복잡도가 적용되지 않습니다. 속성을 예로 설정하면 암호 복잡성이 적용되고 조직 정책 준수 문제가 발생합니다. ASVS 4.03 v2.1.9 권장 사항에 따라: 허용되는 문자 유형을 제한하는 암호 작성 규칙이 없는지 확인합니다. 대문자나 소문자 또는 숫자 또는 특수 문자는 필요하지 않습니다. (다6) 암호 복잡성을 적용하는 대신 ASVS 권장 사항은 암호 길이에 대해 최소 12자의 길이를 적용하는 것입니다. 참조: OWASP ASVS v4.0 인증
활성 SAML 구성에 데모 인증서 사용 금지[Security Center 1.5에서 업데이트됨]	• 새로운 간단한 설명: 활성 SAML 구성에 데모 인증 사용 금지 • 이전의 간단한 설명: 활성 SAML 구성에 데모 인증 사용 금지(플러그인 적용 가능성: 다중 제공자 SSO)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
SAML notBefore 또는 notOnOrAfter 제약 조건 기간 최소화[Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: SAML "notBefore" 또는 "notOnOrAfter" 제약 조건 기간 최소화 • 이전의 간단한 설명: SAML "notBefore" 또는 "notOnOrAfter" 제약 조건 기간 최소화 (플러그인 적용 가능성: 다중 제공자 SSO)
만료된 안티-CSRF 토큰 차단 [Security Center 1.5에서 업데이트됨]	• 새로운 간단한 설명: 만료된 안티-CSRF 토큰 차단 • 이전 간단한 설명: 만료된 CSRF 토큰 차단
고객 서비스 애플리케이션에서 게스트 워크업 경험에 대해 captcha 필요[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 고객 서비스 애플리케이션에서 게스트 워크업 경험에 대해 Captcha 필요 • 이전의 간단한 설명: 고객 서비스 애플리케이션에서 게스트 워크업 경험에 대해 Captcha 필요(플러그인 적용 가능성: 고객 서비스용 게스트 워크업 경험)
HR 앱에서 ACL 평가에 대한 가장 확인[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: HR 앱에서 ACL 평가에 대한 가장 확인 • 이전 간단한 설명: HR 앱에서 ACL 평가에 대한 가장 확인(플러그인 적용 가능성: Human Resources Scoped App)
개인 이메일에서 HR 케이스 업데이트 제한 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 개인 이메일에서 HR 케이스 업데이트 제한 • 이전 간단한 설명: 개인 이메일에서 HR 케이스 업데이트 제한(플러그인 적용 가능성: Human Resources Scoped App) • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
MID 감사 로그 사용[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: MID 감사 로그 사용 • 이전의 간단한 설명: MID 감사 로그 사용 (플러그인 적용 가능성: MID 서버)
자격 증명 별칭 사용 적용[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 자격 증명 별칭 사용 강제 적용 • 이전의 간단한 설명: 자격 증명 별칭 사용 적용 (플러그인 적용 가능성: MID 서버)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
필요한 jms 연결 팩토리 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: JMS 연결 팩토리 필요 • 이전 간단한 설명: 필수 JMS 연결 팩토리 (플러그인 적용 가능성: MID 서버) • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
학습 및 예측 흐름에서 첨부 파일 크기 제한 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 교육 및 예측 플로우에서 첨부 파일 크기 제한 • 이전의 간단한 설명: 교육 및 예측 플로우에서 첨부 파일 크기 제한(플러그인 적용 가능성: 플랫폼 문서 인텔리전스)
보관 테이블 ACL이 선택되어 있는지 확인 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
세션 감사 이벤트 기록[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 설명: Glide 속성이 *glide.authenticate.session_access.log_audit_eve* 예로 설정되면 sys_session_access_audit 테이블에 세션 감사 이벤트가 생성됩니다. 악의적인 액터 조사를 지원하기 위해 세션에 액세스한 사람에 대한 정보를 기록하는 것이 베스트 프랙티스입니다. 로그되는 정보에는 사용자, 세션 ID(중요하지 않음), IP 주소, 역할 및 정책이 포함됩니다. • 이전 설명: Glide 속성이 *glide.authenticate.session_access.log_audit_eve* 예로 설정되면 sys_session_access_audit 테이블에 세션 감사 이벤트가 생성됩니다. 악의적인 액터 조사를 지원하기 위해 세션 액세스에 대한 일반 정보를 기록하는 것이 가장 좋습니다. 로그되는 정보에는 사용자, 세션 ID(중요하지 않음), IP 주소, 역할 및 정책이 포함됩니다.
정보 요청 플레이북에 대한 범위 지정 ACL 액세스 강제 적용 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: Information Request 플레이북에 대한 범위 지정 ACL 접근 강제 적용 • 이전의 간단한 설명: Information Request 플레이북에 대한 범위 지정 ACL 접근 강제 적용 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
비활성 세션을 사전 예방적으로 무효화 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]	• 새로운 설명: Glide 속성은 *glide.active.session.timeout.invalidate.session* Tomcat 컨테이너가 세션을 무효화하기 전에 시간 초과된 세션을 사전에 무효화할지 여부를

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	제어합니다. 이 속성이 true로 설정되지 않으면 시간 초과된 세션이 무효화되지 않는 짧은 시간 간격이 있을 수 있습니다(큐 크기에 따라 60+초). 세션이 하이재킹되면 공격자는 이 짧은 시간 동안 세션을 사용할 수 있습니다. • 이전 설명: Glide 속성은 *glide.active.session.timeout.invalidate.session* Tomcat 컨테이너 전에 시간 제한 세션이 사전에 무효화되는지 여부를 제어합니다. 이 속성이 true로 설정되지 않으면 시간 초과된 세션이 무효화되지 않는 짧은 시간 간격이 있을 수 있습니다(큐 크기에 따라 60+초). 세션이 하이재킹되면 공격자는 이 짧은 시간 동안 세션을 사용할 수 있습니다.
HTTP 응답 본문 크기 제한[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: HTTP 응답 본문 크기 제한 • 오래된 간단한 설명: HTTP 응답이 응답 본문 크기로 인해 OutofMemory 예외를 트리거하지 않는지 확인

베이스라인 버전 2.0에 대한 업데이트된 강화 설정

베이스라인 버전 2.0 릴리스 보안 센터 에서 일부 강화 설정이 업데이트되었습니다.

설명서	업데이트
동시 대화형 세션 수량 최소화[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 동시 대화형 세션 수량 최소화 • 이전의 간단한 설명: Glide 인증 최대 동시 대화형 세션
인증서 신뢰 적용[Security Center 1.3에서 업데이트 되고 2.0에서 제거됨]	• 새로운 간단한 설명: 인증서 신뢰 강제 적용 • 이전 간단한 설명: 인증서 신뢰
암호 SMS 복잡성 재설정 최대화[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 암호 SMS 복잡성 재설정 최대화 • 이전 간단한 설명: 암호 SMS 복잡성 재설정
높은 보안 플러그인 사용 〔보안 센터 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 높은 보안 플러그인 사용 • 이전 간단한 설명: 높은 보안 플러그인
세션 쿠키의 엄격한 보안 적용[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 세션 쿠키의 엄격한 보안 강제 적용 • 오래된 간단한 설명: 보안 세션 쿠키

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
활성 SAML 구성에 데모 인증서 사용 금지 [Security Center 1.5에서 업데이트됨]	• 새로운 간단한 설명: 활성 SAML 구성에 데모 인증 사용 금지(플러그인 적용 가능성: 다중 제공자 SSO) • 이전의 간단한 설명: 활성 SAML 구성에 데모 인증 사용 금지
XMLDocument2 스트리밍 파서 내에서 엔터티 확장 사용 안 함 [Security Center 1.5에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
허용된 Java 패키지 제한 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 허용된 Java 패키지 제한 • 이전 간단한 설명: Java 패키지 허용 목록
모바일 앱 UI 난독화 필요[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 모바일 앱 UI 난독화 필요 • 이전의 간단한 설명: 모바일 앱 UI 난독화
즐겨찾기에 공개 액세스 사용 안 함[Security Center 1.3 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: 즐겨찾기에 공개 접근 사용 안 함 • 이전 간단한 설명: 즐겨찾기에 공개 접근
이스케이프 JavaScript [Security Center 1.3에서 업데이트됨]	• 새로운 설명: 글라이드 속성은 *glide.html.escape_script* HTML 필드를 삭제하는 데 도움이 됩니다. *glide.html.escape_script* 권장 값인 예로 설정되지 않은 경우 포함된 JavaScript를 제거하여 백엔드 Java 컨텍스트에서 HTML 필드(출력 인코딩)에 대한 입력이 삭제되지 않습니다. HTML 필드의 JavaScript는 XSS를 저장하고 반영할 수 있습니다. XSS를 사용할 수 있는 기능은 더 많은 측면 이동을 수행할 수 있는 관리자와 같은 더 높은 역할로 쉽게 얻을 수 있는 권한 에스컬레이션으로 이어질 수 있습니다. • 이전 설명: 글라이드 속성은 *glide.html.escape_script* html 필드를 삭제하는 데 도움이 됩니다. *glide.html.escape_script*권장 값인 예로 설정되지 않은 경우 포함된 JavaScript를 제거하여 백엔드 Java 컨텍스트에서 HTML 필드(출력 인코딩)에 대한 입력이 삭제되지 않습니다. HTML 필드의 JavaScript는 XSS를 저장하고 반영할 수 있습니다. XSS를 사용할 수 있는 기능은 더 많은 측면 이동을 수행할 수 있는 관리자와 같은 더 높은 역할로 쉽게 얻을 수 있는 권한 에스컬레이션으로 이어질 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
외부 공급업체 웹 사이트 포함을 방지하기 위해 Xframe 옵션 설정 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 외부 공급업체 웹 사이트 포함을 방지하기 위해 Xframe 옵션 설정 • 오래 된 간단한 설명: Xframe 옵션 • 새 설명: 권장 값인 DENY 또는 SAMEORIGIN으로 설정되지 않은 경우 *com.glide.cs.embed.xframe_options* 웹 애플리케이션의 컨텐츠는 ALLOW-FROM URI를 사용하여 타사 사이트에 포함될 수 있습니다. 신뢰할 수 없는 타사 사이트를 허용하면 클릭재킹과 같은 공격이 가능해질 수 있습니다. • 이전 설명: *com.glide.cs.embed.xframe_options* 권장 값인 DENY 또는 SAMEORIGIN으로 설정되지 않은 경우 웹 애플리케이션의 컨텐츠는 ALLOW-FROM URI를 사용하여 타사 사이트에 포함될 수 있습니다. 신뢰할 수 없는 타사 사이트를 허용하면 클릭재킹과 같은 공격이 가능해질 수 있습니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
목록 뷰에서 HTML 이스케이프 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 목록 뷰에서 HTML 이스케이프 • 오래된 간단한 설명: 이스케이프 HTML
클래식 모바일 앱 UI 난독화 필요[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 클래식 모바일 앱 UI 난독화 필요 • 이전 간단한 설명: 클래식 모바일 앱 UI 난독화
빈 ACL을 사용하여 기본적으로 거부 [보안 센터 1.3에서 업데이트됨]	• 새로운 간단한 설명: 빈 ACL을 사용하여 기본적으로 거부 • 이전 간단한 설명: 보안 관리자 기본 거부 • 새로운 설명: *glide.sm.default_mode* 권장 값인 거부로 설정되지 않은 경우 해당 자원에 대해 정의된 ACL이 없을 때 인스턴스의 레거시 보안 관리자가 자원에 대한 액세스를 허용합니다. 또는 와일드카드 테이블 수준 ACL만 허용합니다. 명시적 ACL 세트가 없는 모든 것을 허용하도록 설정하면 조작에 취약합니다. • 이전 설명: *glide.sm.default_mode* 권장 값인 거부로 설정되지 않은 경우 해당 자원에 대해 정의된 ACL이 없을 때 레거시 보안 관리자가 자원에 액세스할 수 있도록 허용합니다. 또는 와일드카드 테이블 수준

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	ACL만 허용합니다. 명시적 ACL 세트가 없는 모든 것을 허용하도록 설정하면 조작에 취약합니다.
암호 요청 재시도 기간 재설정 최대화 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 암호 요청 재시도 기간 재설정 최대화 • 이전 간단한 설명: 암호 재설정 요청 재시도 창
XSD 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: XSD 요청에 대해 인증 필요 • 이전 간단한 설명: XSD 요청 권한 • 새 정정: 속성이 *glide.basicauth.required.xsd* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.xsd* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
이스케이프 Jelly 스크립트[Security Center 1.3 및 1.5에서 업데이트됨]	• 신규 간단한 설명: 이스케이프 Jelly 스크립트 • 오래 된 간단한 설명: 이스케이프 Jelly
인바운드 트랜잭션 다시 확인 [Security Center 1.3에서 업데이트됨]	• 새 정정: 속성이 *glide.security.strict.updates* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.security.strict.updates* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
정적 콘텐츠에서 다운로드 가능한 파일 형식 제한 [Security Center 1.3에서 업데이트됨]	• 신규 간단한 설명: 정적 컨텐츠에서 다운로드 가능한 파일 형식 제한 • 오래 된 간단한 설명: 파일 형식 정적 컨텐츠에서 제한 다운로드
PDF 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: PDF 요청에 대해 인증 필요 • 이전 간단한 설명: PDF 요청 권한 • 새 정정: 속성이 *glide.basicauth.required.pdf*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.pdf*예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
업로드된 MIME 유형 제한 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: 업로드된 MIME 유형 제한 • 이전 간단한 설명: MIME 유형 제한 업로드 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
레거시 JQuery 동작 사용 안 함[보안 센터 1.3에서 업데이트됨]	• 새로운 간단한 설명: 레거시 JQuery 동작 사용 안 함 • 이전 간단한 설명: 레거시 JQuery 동작
암호 요청 잠금 해제 기간 재설정 최대화[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 암호 요청 잠금 해제 기간 재설정 최대화 • 이전 간단한 설명: 암호 재설정 잠금 해제 창 요청
MultiSSO 디버깅 사용 안 함[Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: MultiSSO 디버깅 사용 안 함(플러그인 적용 가능성: 다중 제공자 SSO(Single Sign-On)) • 이전 간단한 설명: MultiSSO 디버깅 사용 안 함 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
프로덕션 인스턴스 동작 적용[Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 프로덕션 인스턴스 동작 강제 적용 • 이전 간단한 설명: 프로덕션 인스턴스 동작
잘못된 암호 재설정 시도 제한 [Security Center 1.3에서 업데이트되고 2.0에서 업데이트됨]	• 새로운 간단한 설명: 암호 요청 최대 시도 허용 재설정 최소화 • 이전 간단한 설명: 암호 재설정 요청 최대 시도 횟수
csv 요청에 대해 권한 부여 필요[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: CSV 요청에 대해 인증 필요 • 이전 간단한 설명: CSV 요청 권한

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 새 정정: 속성이 *glide.basicauth.required.csv* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.csv* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
암호 요청 성공 기간 재설정 최소화 〔보안 센터 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 암호 요청 성공 기간 재설정 최소화 • 이전 간단한 설명: 암호 재설정 요청 성공 창
SOAP 요청 엄격한 보안 적용[Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: SOAP 요청 엄격한 보안 강제 적용 • 이전 간단한 설명: SOAP 요청 엄격한 보안
SOAP 요청에 대해 권한 부여 필요 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨〕	• 새로운 간단한 설명: SOAP 요청에 대해 인증 필요 • 이전 간단한 설명: SOAP 요청 승인 • 새로운 설명: Glide 속성은 *glide.basicauth.required.soap* 인스턴스에 SOAP를 요청하는 데 인증이 필요한지 여부를 제어합니다. *glide.basicauth.required.soap* 가 권장 값인 true로 설정되지 않은 경우 인스턴스의 SOAP 요청에 대해 인증이 비활성화됩니다. 관리자 또는 유지 관리 수준 작업에 대한 인증되지 않은 액세스를 허용합니다. 인스턴스 내의 보안 제어를 무효화합니다. • 이전 설명: Glide 속성은 *glide.basicauth.required.soap* 인스턴스에 SOAP를 요청하기 위해 인증이 필요한지 여부를 제어합니다. glide.basicauth.required.soap가 권장 값인 예로 설정되지 않은 경우 인스턴스의 SOAP 요청에 대해 인증이 비활성화됩니다. 관리자 또는 유지 관리 수준 작업에 대한 인증되지 않은 액세스를 허용합니다. 인스턴스 내의 모든 보안 통제를 무효화합니다. • 새 정정: 속성이 *glide.basicauth.required.soap* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 이전 정정: 속성이 *glide.basicauth.required.soap* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
allowlistDisable 엔터티 확장으로 XMLdoc2 엔터티 유효성 검사 필요[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: allowlistDisable 엔터티 확장으로 XMLdoc2 엔터티 유효성 검사 필요 • 이전 간단한 설명: allowlistDisable 엔터티 확장을 사용한 XMLdoc2 엔터티 유효성 검사
닷워킹 필드에 도메인 분리 적용 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: 닷워킹 필드에 도메인 분리 적용(플러그인 적용 가능성: 도메인 분리 • 이전의 간단한 설명: 도메인 분리 적용 • 새 설명: 이 속성은 닷워킹 필드에 도메인 분리 기능을 적용하기 위해 조인 쿼리에 도메인 분리 조건이 부여되는지 여부를 통제합니다. *glide.sys.domain.include_domain_condition_on_jo* 가 도메인 분리를 사용하는 인스턴스에서 권장 값인 true로 설정되지 않은 경우 특정 도메인과 공유할 수 없는 중요한 정보가 공개될 수 있습니다. • 이전 설명: 이 속성은 닷워킹 필드에 도메인 분리 기능을 적용하기 위해 조인 쿼리에 도메인 분리 조건이 부여되는지 여부를 통제합니다. *glide.sys.domain.include_domain_condition_on_jo* 권장 값인 true로 설정되지 않은 경우 특정 도메인과 공유할 수 없는 중요한 정보가 공개될 수 있습니다. • 새 정정: 도메인 분리 플러그인이 활성 상태인 경우 속성이 *glide.sys.domain.include_domain_condition_on_jo* 예로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.sys.domain.include_domain_condition_on_jo* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
JSONP 요청을 신뢰할 수 있는 URL로 제한 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: JSONP 요청을 신뢰할 수 있는 URL로 제한 • 이전 간단한 설명: JSONP 요청 포함 목록 • 새 설명: 이 속성은 angularJS $http 서비스의 신뢰할 수 있는 URL을 지정하여 JSONP 요청을 허용/거부합니다. 속성은 고객의 변경 사항을 위반할 가능성이 있으므로 신뢰할 수 있는 URL을 추가할 방법이 필요합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	권장 값인 "true"로 설정되지 않은 경우 *angular.jsonp.inclusion_list.enabled* JSONP 요청은 모든 URL에 허용됩니다. • 이전 설명: 이 속성은 angularJS $http 서비스의 신뢰할 수 있는 URL을 지정하여 JSONP 요청을 허용/거부합니다. 속성은 고객의 변경 사항을 위반할 가능성이 있으므로 신뢰할 수 있는 URL을 추가할 방법이 필요합니다. *angular.jsonp.inclusion_list.enabled*)가 권장 값인 true로 설정되지 않은 경우 jsonp 요청은 모든 URL에 허용됩니다.
일별 암호 최대 SMS 재설정 최소화 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 일별 암호 최대 SMS 재설정 최소화 • 이전 간단한 설명: 암호 재설정 하루 최대 SMS
암호 확인 지연 기간 재설정 최대화[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 암호 검증 지연 기간 재설정 최대화 • 이전 간단한 설명: 암호 검증 지연 재설정 • 새로운 설명: *password_reset.verification.delay* 권장 값인 1000 이상으로 설정하지 않으면 로그인이 무차별 공격에 더 취약해집니다. 이 지연 시간(밀리초)은 자동화 도구("봇")를 사용하여 악의적인 액터가 사용자 식별 또는 확인 세부 정보를 추측하는 기능을 제한합니다. • 이전 설명: *password_reset.verification.delay* 권장 값인 1000 이상으로 설정하지 않으면 로그인이 무차별 공격에 더 취약해집니다. 이 지연 시간(밀리초)은 해커가 자동화 도구("봇")를 사용하여 사용자 식별 또는 확인 세부 정보를 추측하는 능력을 제한합니다.
데이터 브로커 REST API에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 데이터 브로커 REST API에 대해 인증 필요 • 이전 간단한 설명: 데이터 브로커 REST API 인증 • 신규 설명: *glide.basicauth.required.databrokerrestapiproce* 권장 값인 예로 설정되지 않은 경우 모든 인바운드 데이터 브로커 REST API 요청에 기본 인증이 필요하지 않습니다. 이로 인해 인스턴스에서 미인증 정보 공개가 발생할 수 있습니다. • 이전 설명: Utah 릴리스부터 권장 값인 "예"로 설정되지 않은 경우

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	glide.basicauth.required.databrokerrestapiproce 모든 인바운드 데이터 브로커 REST API 요청에 기본 인증이 필요하지 않습니다. 이로 인해 인스턴스에서 미인증 정보 공개가 발생할 수 있습니다. • 새 정정: 속성이 *glide.basicauth.required.databrokerrestapiproce* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: Utah 릴리스 이후를 실행하는 인스턴스에서 속성이 *glide.basicauth.required.databrokerrestapiproce* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
JSONv2 요청에 대해 권한 부여 필요[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: JSONv2 요청에 대해 인증 필요 • 이전 간단한 설명: JSONv2 요청 권한 • 새 정정: 속성이 *glide.basicauth.required.jsonv2* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.jsonv2* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
임베디드 HTML에 JavaScript 태그 사용 안 함[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 임베디드 HTML에 JavaScript 태그 사용 안 함 • 이전 간단한 설명: 임베디드 HTML에 Javascript 태그 허용 • 새 정정: 속성이 *glide.ui.security.codetag.allow_script* sys_properties 테이블에 있고 false로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.ui.security.codetag.allow_script* false로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
보안 점프 시작 플러그인(ACL 규칙) 사용 〔보안 센터 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 보안 점프 시작 플러그인(ACL 규칙) 사용 • 이전 간단한 설명: 보안 점프 시작 플러그인(ACL 규칙)
SOAP 요청의 게스트 사용자 설정[Security Center 1.3 및 2.0에서 업데이트됨〕	• 새로운 간단한 설명: SOAP 요청의 게스트 사용자 설정 • 이전 간단한 설명: SOAP 요청의 게스트 사용자
스크립트 샌드박스 사용[Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 클라이언트 작성 스크립트 샌드박스 강제 적용 • 이전 간단한 설명: 클라이언트 작성 스크립트 샌드박스
XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨〕	• 새로운 간단한 설명: XML 외부 엔터티 제한 • 이전 간단한 설명: XML 엔터티 확인 URL 허용 목록
컨트롤 라이브 프로파일 상세 정보에 ACL 사용 [Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 컨트롤 라이브 프로파일 상세 정보에 ACL 사용 • 이전 간단한 설명: ACL을 사용하여 라이브 프로파일 상세 정보 제어
사용자 지정 저널 항목에 대한 액세스 제한 [Security Center 1.3에서 업데이트되고 2.0에서 제거됨〕	• 새로운 간단한 설명: 사용자 지정 저널 항목에 접근 제한 • 이전의 간단한 설명: 보안 사용자 지정 저널 항목 • 새 설명: *glide.live_feed.custom_journal.acl_check_enable* 권장 값인 true로 설정되지 않은 경우 모든 사용자가 라이프 피드 기능 내의 모든 저널 항목을 볼 수 있습니다. 속성을 예로 설정하면 사용자 지정 저널 필드의 ACL이 적용되므로 기능이 있으면 좋습니다. • 이전 설명: *glide.live_feed.custom_journal.acl_check_enable* 권장 값인 true로 설정되지 않은 경우 모든 사용자가 모든 저널 항목을 볼 수 있습니다. 속성을 예로 설정하면 사용자 지정 저널 필드의 ACL이 적용되므로 기능이 있으면 좋습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
12시간 이하로 암호 재설정 OTP 수명 설정 [Security Center 2.0에서 업데이트됨]	• 새 설명: 이 속성을 사용하면 암호 재설정 이메일의 링크가 해당 이메일 *glide.pwd_reset.onetime.token.validity* 에 지정된 시간 수 후에 만료될 수 있습니다 *glide.pwd_reset.onetime.token.validity property*. 암호 재설정 토큰의 유효 시간은 일반 사용자 경험에 따라 가능한 한 짧게 유지되어야 합니다. 암호 재설정 토큰의 유효 시간이 길면 악의적인 액터가 계정 인수를 수행하는 데 도움이 될 수 있습니다. • 이전 설명: 이 속성을 *glide.pwd_reset.onetime.token.validity* 사용하면 암호 재설정 이메일의 링크가 해당 *glide.pwd_reset.onetime.token.validity* 속성에 지정된 시간 수 후에 만료됩니다. 암호 재설정 토큰의 유효 시간은 일반 사용자 경험에 따라 가능한 한 짧게 유지되어야 합니다. 암호 재설정 토큰의 유효 시간이 길면 해커가 계정 탈취를 수행하는 데 도움이 될 수 있습니다.
위임된 개발자의 읽기 권한 제한[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 위임된 개발자의 읽기 권한 제한 • 이전 간단한 설명: 위임된 개발자 읽기 액세스 허용 목록
허용된 ServiceNow 내부 IP 주소 정의 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 허용된 ServiceNow 내부 IP 주소 정의 • 이전 간단한 설명: IP 주소 액세스 허용 목록
SOAP 콘텐츠 형식 확인[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: SOAP 콘텐츠 유형 확인 • 오래된 간단한 설명: SOAP 콘텐츠 유형 검사 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
Excel 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: Excel 요청에 대해 인증 필요 • 이전 간단한 설명: Excel 요청 권한 • 새 정정: 속성이 *glide.basicauth.required.excel* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 이전 정정: 속성이 *glide.basicauth.required.excel* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
API 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: API 요청에 대해 인증 필요 • 이전 간단한 설명: API 요청 승인 • 새 정정: 속성이 *glide.basicauth.required.api* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.api* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
GlideXMLUtil 스크립트에 대한 엔터티 확장 임계치 최소화[Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: 엔터티 확장 임계치 최소화 • 이전 간단한 설명: 엔터티 확장 임계치 설정
암호 재설정/변경 프로세스 중에 사용자에게 알림 [Security Center 1.5에서 제거됨]	• 새로운 간단한 설명: 암호 재설정/변경 프로세스 중에 사용자에게 알림 • 이전 간단한 설명: 암호 재설정/변경 알림 프로세스 • 새 정정: 암호 재설정 프로세스가 암호 변경 또는 재설정 시 사용자에게 알리는지 확인합니다. • 이전 정정: 암호 재설정 프로세스가 암호 변경 또는 재설정 시 사용자에게 알리는지 확인합니다.
레거시 AngularJS 동작 사용 안 함[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 레거시 AngularJS 동작 사용 안 함 • 이전 간단한 설명: 레거시 AngularJS 동작
실패한 로그인 잠금 해제 시간 제한 기간 최대화 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 실패한 로그인 잠금 해제 시간 제한 기간 최대화 • 이전의 간단한 설명: 로그인 실패 후 잠금 해제 시간 제한 관리

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
HTTP 쿠키 전용 플래그 사용[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: HTTP 쿠키 전용 플래그 사용 • 오래된 간단한 설명: HTTP 전용 쿠키 플래그 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
범위가 지정된 관리자 애플리케이션 ACL 사용 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 범위가 지정된 관리자 애플리케이션 ACL 사용 • 이전의 간단한 설명: 범위가 지정된 관리자 애플리케이션 ACL 관리 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
UserCookie 버전 3.1 사용 [Security Center 2.0에서 업데이트됨]	• 새로운 설명 : UserCookie v3는 속성이 *glide.ui.secure.cookies.use_kmf* 비활성화 된 경우에만 생성됩니다. UserCookie v3는 HMAC에 대한 비밀 키를 소스 코드에 저장하고 모든 고객에게 동일하기 때문에 안전하지 않습니다. 이를 통해 악의적인 행위자가 사용자 세션을 하이재킹하려는 시도에 이 하나의 비밀 키를 사용할 수 있습니다. • 이전 설명: UserCookie v3은 속성 glide.ui.secure.cookies.use_kmf 사용하지 않도록 설정된 경우에만 생성됩니다. UserCookie v3는 HMAC에 대한 비밀 키를 소스 코드에 저장하고 모든 고객에게 동일하기 때문에 안전하지 않습니다. 이를 통해 해커는 사용자 세션을 하이재킹하려는 시도에 이 하나의 비밀 키를 사용할 수 있습니다.
XML 요청에 대해 권한 부여 필요[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: XML 요청에 대해 인증 필요 • 이전 간단한 설명: XML 요청 승인 • 새 정정: 속성이 *glide.basicauth.required.xml* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.xml* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
외부 사용자 등록 링크 만료 기간 최소화 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 외부 사용자 등록 링크 만료 기간 최소화 • 이전의 간단한 설명: 외부 사용자 등록 링크 만료
인바운드 전자 메일 이미지를 첨부 파일로 변환 [Security Center 1.3에서 업데이트 되고 1.5에서 제거됨]	• 새로운 간단한 설명: 인바운드 이메일 이미지를 첨부 파일로 변환 • 이전 간단한 설명: 변환 인바운드 이메일 HTML
SMTP 받는 사람 수량 최소화 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: SMTP 수신자 수량 최소화 • 이전의 간단한 설명: 최대 SMTP 받는 사람
업데이트된 버전의 MultiSSO 플러그인 사용 [보안 센터 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 복수 SSO 플러그인의 업데이트된 버전 사용(플러그인 적용 가능성: 복수 제공자 SSO) • 이전 간단한 설명: 복수 SSO 플러그인의 업데이트된 버전을 사용할 수 있습니다. • 새로운 CVSS 점수: 7.1 • 이전 CVSS 점수: 5
원시 데이터베이스 쿼리 실행 사용 안 함[Security Center 1.3에서 업데이트되고 2.0에서 제거됨]	• 새로운 간단한 설명: 원시 데이터베이스 쿼리 실행 사용 안 함 • 이전 간단한 설명: 운영 수준 접근 제어 요구 사항 • 신규 설명: 이 속성을 사용하면 사용자가 데이터베이스에서 원시 SQL 쿼리를 수행할 수 있으며, 이를 통해 GlideRecord 제한을 벗어난 테이블 및 데이터에 액세스할 수 있습니다. *glide.db.allow_unsafe_dbi_execute_sql* 권장 값인 false로 설정되지 않은 경우 Glide Scriptable에서 *dbi.executeStatement()*를 호출할 수 있습니다. • 이전 설명: 이 속성을 사용하면 사용자가 데이터베이스에서 원시 SQL 쿼리를 수행할 수 있으며, 이를 통해 GlideRecord 제한을 벗어난 테이블 및 데이터에 액세스할 수 있습니다. *glide.db.allow_unsafe_dbi_execute_sql* 권장 값인 false로 설정되지 않은 경우 Glide Scriptable에서 *dbi.executeStatement()*를 호출할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
이스케이프 XML 마크업 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 이스케이프 XML 마크업 • 이전 간단한 설명: 이스케이프 XML • 새 정정: 속성이 *glide.ui.escape_text* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.ui.escape_text* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
RSS 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: RSS 요청에 대해 인증 필요 • 이전 간단한 설명: RSS 요청 권한 • 새 정정: 속성이 *glide.basicauth.required.rss* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.rss* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
허용된 첨부 파일 크기 최소화 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 허용된 첨부 파일 크기 최소화 • 이전 간단한 설명: 허용되는 최대 첨부 파일 크기
상대 링크 적용[Security Center 1.3 및 1.5에서 업데이트됨]	• 새 설명: 이 *glide.cms.catalog_uri_relative* 속성은 /ess/catalog.do의 URI 매개변수에서 상대 링크를 적용합니다. *glide.cms.catalog_uri_relative* 권장 값인 true로 설정되지 않은 경우 URL은 enforceRelativeURL(url) 함수로 삭제되지 않습니다. 절대 URL은 매개변수 또는 필드 값의 일부로 사용될 때 보안 위험을 초래할 수 있으므로 소스 페이지를 상대방이 통제하는 웹 사이트로 리디렉션합니다. • 이전 설명: 이 속성을 사용하여 *glide.cms.catalog_uri_relative* / ess/catalog.do의 URI 매개변수에서 상대 링크를 적용합니다. *glide.cms.catalog_uri_relative*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	권장 값인 true로 설정되지 않은 경우 enforceRelativeURL(url) 함수를 사용하여 URL을 삭제하지 않을 수 있습니다.
등록 및 확인을 위한 SMS 코드 알림 사용 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 등록 및 검증을 위한 SMS 코드 알림 사용 • 이전 간단한 설명: 등록 및 검증을 위한 SMS 코드 알림
Cache-Control HTTP 헤더 값 [Security Center 1.3에서 업데이트되고 1.5에서 제거됨]	• 새로운 짧은 설명: Cache-Control HTTP 헤더 값 • 오래된 간단한 설명: 캐시 제어 HTTP 헤더 값 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
명시적 외부 역할에 대한 내부 액세스 거부 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 명시적 외부 역할에 대한 내부 액세스 거부 • 이전의 간단한 설명: 명시적 역할 내부 거부 목록 활성화 • 새 기술 구성 이름: glide.security.explicit_roles.enable_internal_user_blacklist,gl • 이전 기술 구성 이름: glide.security.explicit_roles.enable_internal_user_blacklist • 새 설명: 이렇게 하면 외부 사용자에게 snc_internal 역할이 할당되는 것을 방지할 수 있습니다. 가 권장 값인 true로 설정되지 않고 *glide.security.explicit_roles.internal_user_bla* 속성이 신뢰할 수 없는 사용자 클래스 목록으로 설정되지 않은 경우 *glide.security.explicit_roles.enable_internal_u* 지정된 역할에 snc_external 역할 대신 snc_internal 역할을 할당할 수 있습니다. 목록이 비어 있으면 기본적으로 모든 사용자에게 snc_internal 역할이 할당됩니다. 속성에는 최소한 기본 역할 csm_consumer_user,customer_contact이 포함되어야 합니다. 이러한 속성을 잘못 구성하면 외부 사용자 계정이 내부 정보에 액세스할 위험이 높아집니다. • 이전 설명: 이 속성은 외부 사용자에게 snc_internal 역할이 할당되는 것을 방지합니다. 가 권장 값인 true로 설정된 경우 *glide.security.explicit_roles.enable_internal_u* snc_external *glide.security.explicit_roles.internal_user_bla property* 역할을 할당할 수 있습니다. 값이 false로 설정되면 속성이 비활성화됩니다 *glide.security.explicit_roles.internal_user_bla*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 새 정정: 속성이 *glide.security.explicit_roles.enable_internal_u* true로 설정되어 있고 속성에 *glide.security.explicit_roles.internal_user_bla* 위험한 항목 csm_consumer_user, customer_contact이 포함되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.security.explicit_roles.enable_internal_u* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
일회성 대역 외 검증자 수명 기간 최소화 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 일회성 대역 외 검증자 수명 기간 최소화 • 오래된 간단한 설명: 짧은 일회성 대역 외 검증자 수명
스크립트 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 스크립트 요청에 대해 인증 필요 • 이전 간단한 설명: 스크립트 요청 권한 • 새 정정: 속성이 *glide.basicauth.required.scriptedprocessor* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.scriptedprocessor* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
동시 대화형 세션 제한[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 동시 대화형 세션 제한 • 이전 간단한 설명: Glide 인증 동시 대화형 세션 제한 • 새로운 설명: 이 속성은 동시 세션 제한 ()*com.glide.limit.concurrent.sessions* 플러그인과 함께 사용되도록 되어 있습니다. 플러그인이 활성 상태이고 속성이 false로 설정되면 사용자는 인스턴스에서 동시 대화형 세션을 가질 수 있습니다. 오픈 세션이 많을수록 세션 하이재킹이 발생할 가능성이 큽니다. • 이전 설명: 이 속성은 동시 세션 제한 ()*com.glide.limit.concurrent.sessions* 플러그인과 함께 사용하기 위한 것입니다. 플러그인이 활성 상태이고 속성이 false로 설정되면 사용자는 인스턴스에서 동시

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	대화형 세션을 가질 수 있습니다. 오픈 세션이 많을수록 세션 하이재킹이 발생할 가능성이 큽니다.
사용자가 CSRF 유효성 검사를 바이패스하기 위한 경고를 수락하지 못하도록 방지 〔보안 센터 1.3 및 1.5에서 업데이트됨〕	• 새로운 간단한 설명: CSRF 토큰 엄격한 유효성 확인 강제 적용 • 이전 간단한 설명: CSRF 엄격한 유효성 확인 • 새로운 설명: 이 속성은 CSRF 토큰의 재사용을 방지하는 CSRF 토큰의 엄격한 유효성 검사를 사용합니다. *glide.security.csrf.strict.validation.mode* 권장 값인 true로 설정되지 않은 경우 CSRF 토큰을 다시 사용할 수 있으므로 CSRF 공격에 노출될 수 있습니다. • 이전 설명: 이 속성을 사용하면 CSRF 토큰의 재사용을 방지하는 CSRF 토큰의 엄격한 유효성 검사를 사용할 수 있습니다. 권장 값인 예로 설정되지 않은 경우 *glide.security.csrf.strict.validation.mode* CSRF 토큰을 재사용하여 CSRF 공격에 대한 문을 열 수 있습니다.
세션 활동 시간 제한 기간 최소화 [Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 세션 활동 시간 제한 기간 최소화 • 이전 간단한 설명: 세션 활동 시간 제한
HTML 위생 검사 사용 [Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: HTML 위생 검사 사용 • 오래된 간단한 설명: HTML 위생 검사
백그라운드 스크립트에 대한 액세스 제한 [Security Center 1.3 및 2.0에서 업데이트됨〕	• 새 설명: 이 속성에는 스크립트 백그라운드 모듈에 액세스하는 데 필요한 역할이 있습니다. 가 권장 값인 admin, security_admin 또는 maint로 설정되지 않은 경우 *glide.script_processor.admin* 권한이 더 낮은 사용자가 인스턴스에서 백그라운드 스크립트를 실행할 수 있습니다. 이렇게 하면 ACL 시스템을 완전히 바이패스하여 테이블에 대한 전체 액세스가 허용됩니다. • 이전 설명: 이 속성에는 스크립트 백그라운드 모듈에 액세스하는 데 필요한 역할이 있습니다. 권장 값인 관리자로 설정되지 않은 경우 *glide.script_processor.admin* 권한이 낮은 역할을 가진 모든 사용자가 인스턴스에서 백그라운드 스크립트를 실행할 수 있습니다. 이렇게 하면 ACL 시스템을 완전히 바이패스하여 테이블에 대한 전체 액세스가 허용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 새 정정: 속성이 *glide.script_processor.admin* 관리자, security_admin 또는 유지관리 역할로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.script_processor.admin* 관리자로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
내장된 HTML 코드 사용 안 함[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 내장된 HTML 코드 사용 안 함 • 오래된 간단한 설명: 포함된 HTML 코드
절대 세션 시간 제한 기간 최소화[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 절대 세션 시간 제한 기간 최소화 • 이전 간단한 설명: 절대 세션 시간 제한
클라이언트 호출 가능 스크립트 포함에 대해 기본적으로 인증 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 짧은 설명: 클라이언트 호출 가능 스크립트 포함에 대해 기본적으로 인증 필요 • 이전 간단한 설명: 클라이언트 호출 가능 스크립트 포함에 대한 개인정보 보호
GlideSystemUserSession 스크립팅 가능한 API에 대한 접근 제한 [보안 센터 1.3 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: GlideSystemUserSession 스크립팅 가능한 API에 접근 제한 • 이전의 간단한 설명: Access to GlideSystemUserSession 스크립팅 가능한 API
HTML 위생화 강제 적용[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: HTML 위생화 강제 적용 • 오래된 간단한 설명: Check Unsanitized HTML • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
절대 세션 시간 제한 기간 최소화[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 절대 세션 시간 제한 기간 최소화 • 이전 간단한 설명: 절대 세션 시간 제한
역할 기반 다단계 인증 사용[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 역할 기반 다단계 인증 활성화 • 이전의 간단한 설명: 역할 기반 다단계 인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
SAML notBefore 또는 notOnOrAfter 제약 조건 기간 최소화[Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: SAML "notBefore" 또는 "notOnOrAfter" 제약 조건 기간 최소화 (플러그인 적용 가능성: 다중 제공자 SSO) • 이전의 간단한 설명: SAML "notBefore" 또는 "notOnOrAfter" 제약 조건 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
외부 사용자 등록을 위한 전자 메일 도메인 제한 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: 외부 사용자 등록을 위한 이메일 도메인 제한(플러그인 적용 가능성: 외부 사용자 등록) • 이전의 간단한 설명: 외부 사용자 레지스트리 이메일 도메인 허용 목록 • 새로 정정: 속성이 *sn_ext_usr_reg.allowed_email_domains* 빈 값으로 설정되지 않았는지 확인합니다. • 이전 정정: 속성이 *sn_ext_usr_reg.allowed_email_domains* 빈 값으로 설정되지 않았는지 확인합니다.
암호 SMS 일시 중지 기간 재설정 최대화 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 암호 SMS 중지 기간 재설정 최대화 • 이전 간단한 설명: 암호 SMS 중지 창 재설정 • 새 정정: 속성이 *password_reset.sms.pause_window* 2 이상으로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *password_reset.sms.pause_window* 2로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
아웃바운드 SSLv2/SSLv3 연결 사용 안 함 [Security Center 1.3에서 업데이트됨]	• 새로운 짧은 설명: 아웃바운드 SSLv2/SSLv3 연결 사용 안 함 • 이전 간단한 설명: SSLv2/SSLv3 사용 안 함
언로드 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 언로드 요청에 대해 인증 필요 • 오래된 간단한 설명: 요청 인증 언로드 • 새 정정: 속성이 *glide.basicauth.required.unl* sys_properties_table에 있고 true로 설정되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 이전 정정: 속성이 *glide.basicauth.required.unl* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
전자 메일 스팸 점수 매기기 및 필터링 사용 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 이메일 스팸 점수 매기기 및 필터링 사용 • 이전 간단한 설명: 이메일 스팸 점수 매기기 및 필터링
LDAP 초기 고유 이름 설정 해제 [Security Center 1.3에서 업데이트되고 2.0에서 제거됨]	• 새로운 간단한 설명: LDAP 초기 고유 이름 설정 해제 • 이전 간단한 설명: LDAP 초기 고유 이름
안티-CSRF 토큰 사용[Security Center 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨]	• 새로운 짧은 설명: 안티-CSRF 토큰 사용 • 이전 짧은 설명: 안티-CSRF 토큰
AJAXGlideRecord ACL 검사 필요[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: AJAXGlideRecord ACL 검사 필요 • 이전 간단한 설명: AJAXGlideRecord ACL 검사 사용
사용자 가장 기록 [Security Center 1.3 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다. 탐지 정확도를 개선하기 위해 스크립트가 업데이트되었습니다.
감염된 파일 다운로드 사용 안 함[Security Center 1.5 및 2.0에서 업데이트됨]	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
외부 사용자 등록에 Captcha 사용 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 외부 사용자 등록에 Captcha 사용(플러그인 적용 가능성: 외부 사용자 등록) • 이전의 간단한 설명: 외부 사용자 등록에 Captcha 사용
SQL 오류 메시지 사용 안 함 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: SQL 오류 메시지 사용 안 함 • 이전 간단한 설명: SQL 오류 메시지 사용 안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
암호 요청 만료 기간 재설정 최소화[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 암호 요청 만료 기간 재설정 최소화 • 이전 간단한 설명: 암호 재설정 요청 만료 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
잘못된 암호 재설정 시도에 대한 잠금 시간 제어 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새로운 간단한 설명: 암호 요청 최대 시도 기간 재설정 최소화 • 이전 간단한 설명: 암호 재설정 요청 최대 시도 창
다운로드 가능한 MIME 유형 제한 [Security Center 1.3 및 2.0에서 업데이트됨]	• 새로운 짧은 설명: 다운로드 가능한 MIME 유형 제한 • 이전 간단한 설명: 다운로드 가능한 MIME 유형 거부 목록
이스케이프 Excel 수식 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 이스케이프 Excel 수식 • 이전 간단한 설명: 이스케이프 Excel 수식
상황별 보안 플러그인 사용[보안 센터 1.3에서 업데이트됨]	• 새로운 간단한 설명: 상황별 보안 플러그인 사용 • 이전 간단한 설명: 상황별 보안 플러그인
계정 복구 사용 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: 계정 복구 사용 (플러그인 적용 가능성: 복수 제공자 SSO(Single Sign-On)) • 이전 간단한 설명: 계정 복구 • 새로운 설명: 이 속성은 1회 사용자 인증(SSO)을 바이패스하는 기능을 특별히 지정된 관리자에게 바인딩하는 계정 복구 기능을 제어합니다. *glide.sso.acr.enabled* 권장 값인 예로 설정되지 않은 경우 인스턴스에서 1회 사용자 인증(SSO)을 사용할 때 로컬 대화형 로그인(사용자 이름 또는 암호 기반)이 활성화된 상태로 유지됩니다. 로컬 대화형 로그인을 제거하면 인스턴스에 대한 무단 액세스 가능성이 줄어듭니다. • 이전 설명: 이 속성은 계정 복구 기능을 제어합니다. *glide.sso.acr.enabled*권장 값인 true로 설정되지 않은 경우 userId로 계정 복구가 불가능합니다. • 새로운 CVSS 점수: 6.5

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 이전 CVSS 점수: 9.1 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
임포트 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 임포트 요청에 대해 인증 필요 • 이전의 간단한 설명: 요청 인증 임포트 • 새 정정: 속성이 *glide.basicauth.required.importprocessor* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.importprocessor* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
SNC 액세스 제어 플러그인 사용 [보안 센터 1.3에서 업데이트됨]	• 새로운 간단한 설명: SNC 접근 통제 플러그인 사용 • 이전 간단한 설명: SNC 접근 통제 플러그인
모든 노드에서 동시 세션 제한 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 동시 세션 제한 모든 노드간 • 이전의 간단한 설명: Glide 인증 동시 세션 제한 모든 노드간
XML 출력 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 짧은 설명: XML 출력 요청에 대해 인증 필요 • 이전 간단한 설명: XML 출력 승인 • 새 정정: 속성이 *glide.basicauth.required.xmloutputprocessor* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.xmloutputprocessor* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
스크래치패드의 이스케이프 스크립트[Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 스크래치패드의 이스케이프 스크립트 • 오래 된 간단한 설명: 스크래치패드 이스케이프

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	• 새로운 설명: 스크래치패드는 브라우저에서 액세스할 수 있는 서버의 정보를 쉽게 설정할 수 있는 방법입니다. 관리자는 임의 기록의 임의 데이터를 포함하여 무엇이든 스크립트로 작성할 수 있습니다. *glide.ui.escape_scratchpad* 권장 값인 true로 설정되지 않은 경우 교차 사이트 스크립팅 취약성과 같은 악의적인 스크립트를 실행할 수 있습니다. • 이전 설명: 스크래치패드는 브라우저에서 액세스할 수 있는 서버의 정보를 쉽게 설정할 수 있는 방법입니다. 관리자는 임의 기록의 임의 데이터를 포함하여 무엇이든 스크립트로 작성할 수 있습니다. *glide.ui.escape_scratchpad* 권장 값인 true로 설정되지 않은 경우 교차 사이트 스크립팅 취약성과 같은 악의적인 스크립트를 실행할 수 있습니다.
WSDL 요청에 대해 인증 필요 [Security Center 1.3 및 1.5에서 업데이트됨]	• 새로운 간단한 설명: WSDL 요청에 대해 인증 필요 • 이전 간단한 설명: WSDL 요청 승인 • 새 정정: 속성이 *glide.basicauth.required.wsdl* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.wsdl* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
SCHEMA 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]	• 새로운 간단한 설명: 스키마 요청에 대해 인증 필요 • 이전 간단한 설명: SCHEMA 권한 요청 • 새 정정: 속성이 *glide.basicauth.required.schema* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.basicauth.required.schema* 예로 설정되어 있는지 확인합니다. • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
다운로드 가능한 MIME 유형 제한 [Security Center 1.3 및 2.0에서 업데이트됨〕	• 새로운 짧은 설명: 다운로드 가능한 MIME 유형 제한 • 이전 간단한 설명: 다운로드 가능한 MIME 유형
스크립트 샌드박스에서 낮은 권한 사용자에 대한 로거 사용 안 함[Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 스크립트 샌드박스에서 낮은 권한 사용자에 대한 로거 사용 안 함 • 이전 간단한 설명: Glide 보안 로거 샌드박스에 대한 Loggining 없음 • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
x-frame-options 구현: SAMEORIGIN 보안 헤더 [Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: X-Frame-Options 구현: SAMEORIGIN 보안 헤더 • 이전 간단한 설명: X-Frame-Options: SAMEORIGIN • 규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
성능 모니터링 액세스 제한 [Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 성과 모니터링 접근 제한 • 이전 간단한 설명: 성과 모니터링 ACL
가져오기 프로세서에 자세한 SQL 오류 메시지 끄기[Security Center 1.3에서 업데이트됨〕	규칙 스크립트: 탐지 정확도를 향상하기 위해 스크립트가 업데이트되었습니다.
암호 SMS 만료 기간 재설정 최소화 [Security Center 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 암호 SMS 만료 기간 재설정 최소화 • 이전 간단한 설명: 암호 SMS 만료 재설정
수신 전자 메일에서 사용자 만들기 사용 안 함〔보안 센터 1.3에서 업데이트됨〕	• 새로운 간단한 설명: 수신 이메일에서 사용자 생성 사용 안 함 • 이전 간단한 설명: 도메인별 이메일 제한 • 새로운 설명: 관리자는 이메일 속성을 설정하여 수신 이메일에서 사용자를 자동으로 만들 수 있습니다. 이 속성을 안전하지 않은 값으로 설정하면 인스턴스가 수신 이메일에서 사용자를 자동으로 작성합니다. 생성된 각 사용자에게는 동일한 하드코딩된 기본 암호가 적용되므로 무차별 암호 대입을 통한 인증 우회가 더 쉬워집니다. • 이전 설명: 관리자는 수신 이메일에서 사용자를 자동으로 만들도록 이메일 속성을 설정할 수 있습니다. 이 속성을 안전하지 않은 값으로 설정하면 인스턴스가 수신 이메일에서 사용자를 자동으로 작성합니다. 생성된 각 사용자에게는 동일한 하드코딩된 기본 암호가

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설명서	업데이트
	적용되므로 무차별 암호 대입을 통한 인증 우회가 더 쉬워집니다. • 새 정정: 속성이 *glide.pop3readerjob.create_caller* false로 설정되어 있는지 확인합니다. • 이전 정정: 속성이 *glide.pop3readerjob.create_caller* false로 설정되어 있는지 확인

삭제된 강화 설정

일부 강화 설정은 Security Center 기준에서 제거됩니다.

베이스라인 버전 5.0에 대한 강화 설정 삭제

일부 강화 설정은 Security Center 기준 버전 5.0 릴리스에서 제거되었습니다.

- 이벤트 관리 HTTP 프로세서에서 인증 필요
- 사용자 지정 저널 항목에 접근 제한
- 로그인 시 암호 정책을 적용하지 않음
- 원시 데이터베이스 쿼리 실행 사용 안 함
- 로그 HTML 위생화
- 안티-CSRF 토큰 사용
- 인증서 신뢰 강제 적용
- LDAP 초기 고유 이름 설정 해제
- 최소 암호 길이 설정

베이스라인 버전 4.0에 대한 강화 설정 삭제

베이스라인 버전 4.0 릴리스 보안 센터 와 함께 일부 강화 설정이 제거되었습니다.

- LDAP 초기 암호
- 모바일 오프라인 역할
- 제로 트러스트 액세스 정책을 통해 중요 데이터에 대한 액세스 제한(플러그인 적용 가능성: Adaptive Authentication)
- 읽기 전용 테이블 쓰기 허용 목록
- 허용된 JDBC 프로브 작업(플러그인 적용 가능성: MID 서버)
- 수신 이메일에서 사용자를 작성하는 허용 도메인 설정
- 복잡한 "기본" 암호 설정
- GraphQL 허용 목록에서 접근 가능한 속성
- 교차 원본 메시징 허용 목록
- GraphQL 엔드포인트에 대한 교육 및 예측 플로우에서 첨부 파일 크기 제한(플러그인 적용 가능성: 플랫폼 문서 인텔리전스)
- 컨텐츠 역할 편집 허용 목록(플러그인 적용 가능성: 커뮤니티)
- 데이터베이스 쿼리가 쿼리 크기로 인해 OutofMemory 예외를 트리거하지 않도록 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 스크립트 실행을 위한 역할 허용 목록
- 다운로드 가능한 파일 형식 허용 목록
- 읽기 전용 테이블 삭제 허용 목록
- 역할 없는 ACL에 인증 강제 적용
- LDAP 일회성 토큰 만료 시간 최소화
- 인증에 신뢰할 수 있는 IP 주소만 허용
- 모바일 암호 재설정 URL 설정
- 서비스 계정의 암호 복잡성(플러그인 적용 가능성: Service Bridge)
- 암호 재설정/변경 프로세스 중 사용자에게 알림
- 애플리케이션 범위 제한 적용
- 접근 제어 요구사항(플러그인 적용 가능성: 커뮤니티)
- 기록 이력 접근 역할 허용 목록
- 첨부 파일에 대한 역할 접근 제한
- 신뢰할 수 있는 URL의 미리 정의된 목록에 있는 PDF만 허용
- LDAP 서버 중단 시 일회용 암호 이메일 전송 방지
- 인바운드 이메일 이미지를 첨부 파일로 변환
- 관련 없는 명시적 역할 접근 제어 조건 검토

베이스라인 버전 2.0에 대한 강화 설정 삭제

베이스라인 버전 2.0 릴리스 보안 센터 와 함께 일부 강화 설정이 제거되었습니다.

- 애플리케이션 구성 데이터 및 스크립트에 대한 코드 서명 사용
- Glide KMF 암호화기 사용
- 인스턴스 수준 암호화기 사용 사용 안 함
- 명시적 역할 내부 거부 목록 사용
- 코드 서명 요구 사항으로 인해 MID ECC 큐에 직접 삽입 차단
- 모든 아웃바운드 HTTP 요청 필드 로깅

접근 통제

접근 제어 범주는 권한 모델을 기반으로 요청을 부여하고 거부하여 무단 접근으로부터 자원을 보호하는 프로세스를 감사합니다. 여기에는 리소스에 액세스하는 엔터티가 유효한 자격 증명을 보유하도록 하고, 잘 정의된 역할 또는 권한 집합을 생성 및 보호하고, 역할 또는 권한 제어가 재생 및 변조로부터 보호되도록 하는 것이 포함됩니다.

접근 제어는 특정 자원에 대한 접근을 허가할지 또는 거부할지를 결정합니다. 사용 권한이 있는 사용자에게만 리소스에 대한 액세스를 허용합니다.

안티-**CSRF** 토큰 유효성 검사 시간 **[Security Center** 1.3의 새로운 기능]

이 *glide.security.csrf_previous.time_limit* 속성은 보안 토큰이 만료되는 시간(초)을 지정합니다.

사용자 세션이 만료될 때 만료된 토큰의 재사용 허용 허용 속성이 사용되어 있지 않으면 보안 토큰도 만료되고 이 속성이 이 속성에서 설명한 시간 프레임 내에 있습니다. 이 토큰은 교차 사이트 요청 위조 공격을 방지하는 데 사용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.security.csrf_previous.time_limit*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	86400초 또는 1일
기본값	86400초 또는 1일
범주	접근 통제
보안 위험	• 심각도 점수: 5.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값으로 설정하지 않으면 교차 사이트 요청 위조 공격을 방지하는 데 사용되는 토큰 유효성 검사가 비활성화됩니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성은 보안 토큰이 유효한 상태로 유지되는 기간(초)을 결정합니다. 만료된 토큰의 재사용 허용 속성이 사용이고 토큰이 이 속성에 지정된 시간 프레임 내에 있지 않으면 사용자 세션이 만료될 때 보안 토큰이 만료됩니다. 이 토큰은 교차 사이트 요청 위조 공격을 방지합니다. 기본값은 86400초 또는 1일입니다.

닷워킹 필드에 도메인 분리 적용 **[Security Center 1.3, 1.5** 및 2.0에서 업데이트됨〕

이 *glide.sys.domain.include_domain_condition_on_join* 속성은 닷워킹 필드에 도메인 분리 기능을 적용하기 위해 조인 쿼리에 도메인 분리 조건이 부여되는지 여부를 제어합니다.

이 속성은 닷워킹 필드에 도메인 분리 기능을 적용하기 위해 조인 쿼리에 도메인 분리 조건이 부여되는지 여부를 통제합니다. *glide.sys.domain.include_domain_condition_on_join*가 도메인 분리를 사용하는 인스턴스에서 권장 값인 true로 설정되지 않은 경우 특정 도메인과 공유할 수 없는 중요한 정보가 공개될 수 있습니다. 구성요소가 안전하지 않은 교차 도메인 쿼리에 의존하는 경우 인스턴스에 보통 정도의 기능적 영향이 있을 수 있습니다. 인스턴스는 활성화하기 전에 하위 프로덕션 환경에서 테스트해야 합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.sys.domain.include_domain_condition_on_join*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	도메인 분리가 설치되면 True이고, 그렇지 않으면 속성이 존재하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기본값	거짓
범주	접근 통제
목적	닷워킹 필드에 도메인 분리 기능을 적용하기 위해 조인 쿼리에 도메인 분리 조건이 부여되는지 여부를 통제합니다.
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: *glide.sys.domain.include_domain_condition_on_join* 권장 값인 **true**로 설정되지 않은 경우 특정 도메인과 공유할 수 없는 중요한 정보가 공개될 수 있습니다.
참조	서비스 제공자용 도메인 분리

범위가 지정된 관리자 애플리케이션 **ACL** 사용**[Security Center** 1.3에서 업데이트됨]

애플리케이션 *glide.security.scoped_administration.honor_global_acl* 관리 앱이 ACL(전역 접근 제어 목록) 규칙을 상속할 수 있는지 여부를 결정합니다.

이 속성은 기록 범위에 대해 정의된 범위 관리자 애플리케이션 ACL이 없을 때 특히 유용합니다.

애플리케이션에 대한 권한이 낮은 사용자가 중요한 기록에 잠재적으로 액세스할 수 없도록 하려면 예로 설정합니다 *glide.security.scoped_administration.honor_global_acl*.

추가 정보

속성	설명
속성 이름	*glide.security.scoped_administration.honor_global_acl*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	범위가 지정된 관리자 애플리케이션의 ACL 접근 규칙을 통제합니다.
권장 값	예
기본값	예
구성 유형	부울
보안 위험	(낮음) 속성 값이 예이고 기록 범위에 대해 정의된 범위가 지정된 관리자 애플리케이션 ACL이 없는 경우 전역 ACL이 허용됩니다. 기록 범위에 대해 정의된 범위가 지정된 관리자 애플리케이션 ACL이 없는 false로 설정하면 ACL 검사가 무시됩니다.
보안 위험 등급	3.8
참조	애플리케이션 관리 앱의 접근 제어 규칙

플러그인 활성화에 대한 자세한 내용은 다음을 참조하십시오. 플러그인 활성화

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

서비스 조직에 대한 작업 주문 관리 쿼리 규칙 사용 **[Security Center** 1.5의 새로운 기능 및 2.0에서 업데이트됨]

이 *sn_fsm.use_query_rules* 속성을 사용하여 현장 서비스 관리 테이블에 규칙과 필터를 적용합니다.

예로 설정되면 sn_query_rule 테이블의 규칙/필터는 쿼리 비즈니스 규칙 및 읽기 ACL을 통해 로그인한 사용자에게 현장 서비스 관리 관련 테이블(작업 주문 및 작업 주문 작업)에 대한 읽기 권한을 결정하는 데 사용됩니다. 아니요인 경우 쿼리 규칙에 따라 기록이 필터링되지 않습니다. 쿼리 비즈니스 규칙은 보안 확인을 추가합니다. 특히 이 속성은 할당된 영역 또는 영역 구성원 자격에 따라 에이전트, 한정자 및 디스패처에 대한 기록을 필터링합니다. 기록을 읽을 때는 최소 권한의 원칙을 따르는 것이 가장 좋습니다. 이 속성을 예로 설정하지 않으면 현장 서비스 관리 테이블에서 데이터 노출 위험이 증가할 수 있습니다.

추가 정보

속성	설명
구성 이름	*sn_fsm.use_query_rules*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 세부 정보: 이 속성을 예로 설정하면 sn_query_rule의 규칙과 필터를 사용하여 최소 권한 원칙을 구현하는 현장 서비스 관리 테이블에 대한 읽기 권한을 결정합니다. 아니오로 설정하면 쿼리 비즈니스 규칙에 따라 기록이 필터링되지 않으며 현장 서비스 관리 테이블에서 데이터가 노출될 위험이 증가할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	예로 설정하면 sn_query_rule 테이블의 규칙/필터를 사용하여 현장 서비스 관리 관련 테이블에 대한 읽기 권한을 결정합니다. 예를 들어, 쿼리 비즈니스 규칙과 읽기 ACl를 통해 로그인한 사용자에게 작업 주문(WO) 및 작업 주문 테이블(WOT)을 제공할 수 있습니다. 아니요인 경우 쿼리 규칙에 따라 기록이 필터링되지 않습니다. 이 속성을 활성화하면 데이터가 보호되며 모든 데이터(wm_task 및 wm_order)는 사용자에게 표시되지 않습니다.
참조	현장 서비스 관리 참조

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

위임된 개발자의 접근 차단

이 구성은 스크립트를 통해 사용자 역할을 업데이트하는 위임된 개발자의 액세스에 영향을 미칩니다. 구성이 준수되면 개발자는 user_admin 역할이 없으면 sys_user_has_role 테이블에 기록을 업데이트하거나 삽입할 수 없습니다.

이 속성의 값은 위임된 개발자가 인스턴스의 기능에 대한 예기치 않은 액세스 권한을 부여하거나 받을 수 있는지 여부에 영향을 줍니다. 속성에 역할이 포함되어 있으면 해당 역할만 스크립트 모듈을 실행할 수 있습니다.

추가 정보

속성	설명
속성 이름	*com.glide.sys.security.delegateddev.block_grant_roles*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	이 속성의 값은 위임된 개발자가 인스턴스의 기능에 대한 예기치 않은 액세스 권한을 부여하거나 받을 수 있는지 여부에 영향을 줍니다.
유형	토글 스위치
기본값	예
권장 값	예
보안 의존성	안 함
보안 위험 등급	6.7
기능적 영향	delegated_developer 역할이 있는 사용자가 sys_user_has_role 테이블의 기록을 수정하려고 시도할 때 이 속성을 사용하면 작업에 대한 추가 보안 검사를 수행할 수 있습니다. 추가 보안 검사는 사용자가 sys_user_has_role 테이블을 만들거나 업데이트하려는 경우 사용자에게 user_admin 역할이 부여되었는지 확인합니다. user_admin 역할이 없는 경우 액세스가 거부됩니다. 속성이 false이면 이러한 추가 검사의 유효성이 확인되지 않습니다.
보안 위험	(보통) 적절한 권한이 없으면 권한 없는 사용자가 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다.
참조	접근 통제

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

만료된 안티-**CSRF** 토큰 차단 **[Security Center** 1.5에서 업데이트됨]

만료된 CSRF 토큰을 차단하여 교차 사이트 요청 위조 공격을 방지합니다.

개요

교차 사이트 요청 위조는 인증된 사용자를 대신하여 무단 명령이 수행되는 악의적인 익스플로잇의 한 유형입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 상세 정보

속성	설명
개요	수신 요청을 식별하고 유효성을 검사하기 위해 만료된 보안 토큰 사용을 제어합니다. 이전에 만료된 토큰이 수신 요청을 확인하지 못하도록 하려면 **false** 로 설정합니다.
구성 이름	*glide.security.csrf_previous.allow*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	**false**
기본값	**true**
범주	접근 통제
보안 위험	심각도 점수: 6.5
	CVSS 점수당 심각도 등급: 중간
	보안 위험 상세 정보: 강력한 안티-CSRF 메커니즘을 적용하여 인증된 기능을 보호하고, 효과적인 안티-자동화 또는 안티-CSRF는 인증되지 않은 기능을 보호합니다.
의존성 및 필수 구성요소	안 함
참조	안티-CSRF 토큰 사용[Security Center 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨], 교차 사이트 요청 위조.

실행 전 **UI** 작업 조건 확인

이 *glide.security.strict.actions* 속성을 사용하면 UI 작업을 실행하기 전에 양식과 목록에서 UI 작업 조건을 검사할 수 있습니다. 이 속성을 true로 설정하면 테이블 UI 작업이 실행되기 전에 확인 레이어가 추가됩니다.

추가 정보

속성	설명
속성 이름	*glide.security.strict.actions*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	테이블 UI 작업이 실행되기 전에 추가 확인 계층을 보장합니다.
데이터 유형	부울
권장 값	예
기본값	예
보안 위험 등급	3.3
기능적 영향	이렇게 정정하면 인스턴스의 대상 테이블/페이지에서 UI 작업을 확인하기 위한 추가 유효성 확인 계층만 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	고객 인스턴스에 접근 제어가 적절히 설정되어 있기만 하면 여기에 영향을 미치지 않아야 합니다.
보안 위험	(낮음) 두 영역 간에 트랜잭션이 발생할 때 액세스 요청이 항상 확인됩니다. 이 작업은 양식이 최종 사용자에게 렌더링되기 전에 UI 작업의 유효성을 검사합니다.
참조	높은 보안 플러그인

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

이벤트 관리 할당 그룹 관리자 역할 구성[Security Center 1.5의 새로운 기능]

이 *evt_mgmt.connector_assignment_group_admin_roles* 속성을 사용하여 커넥터 인스턴스의 할당 그룹 필드에 대해 관리자 액세스 권한이 부여되는 역할을 설정합니다.

이 *evt_mgmt.connector_assignment_group_admin_roles* 속성에는 커넥터 인스턴스의 할당 그룹 필드에 대한 관리자 액세스 권한이 있는 역할 이름을 나타내는 쉼표로 구분된 문자열이 포함되어 있습니다. 이 목록의 기본 역할을 변경하면 권한 없는 사용자가 인스턴스의 이벤트 통합을 변경할 수 있습니다. 역할에 대한 무단 액세스를 방지하려면 admin,evt_mgmt_admin,sn_sow_srm.srm_admin 값으로 설정합니다 *evt_mgmt.connector_assignment_group_admin_roles*. 권장 값 문자열에서 추가 역할을 검토하여 역할을 포함해야 하는지 확인합니다.

추가 정보

속성	설명
구성 이름	*evt_mgmt.connector_assignment_group_admin_roles*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	admin,evt_mgmt_admin,sn_sow_srm.srm_admin
기본값	admin,evt_mgmt_admin,sn_sow_srm.srm_admin
범주	접근 통제
보안 위험	• 심각도 점수: 3.1 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 기본 역할을 변경하면 권한 없는 사용자가 인스턴스의 이벤트 통합을 변경할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	그룹 생성

서비스 포털 위젯 허용 목록 구성[Security Center 2.0의 새로운 기능]

테이블의 ACL(접근 제어 목록)이 중요한 정보를 노출하지 않도록 glide.service_portal.widget.allow_list 속성을 안전하게 구성하는 방법에 대해 알아봅니다.

이 *glide.service_portal.widget.allow_list* 속성은 인스턴스 내의 모든 테이블에 액세스할 수 있는 위젯을 식별합니다. 그러나 이러한 테이블의 접근 제어 목록(ACL)은 계속

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

적용됩니다. ACL이 잘못 구성되었거나 없는 경우 이 목록의 위젯이 이러한 테이블에 대한 액세스를 활성화하여 중요한 정보를 노출할 수 있습니다. 이 속성은 위젯이 SNCACLWidgetUtil을 사용하고 *glide.service_portal.widget.enforce_public_check* 속성이 사용 가능(예로 설정)된 경우에만 유효합니다.

추가 정보

속성	설명
구성 이름	*glide.service_portal.widget.allow_list*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	배열
권장 값	비어 있음
기본값	비어 있음 - 일부 고객의 케이스에는 몇 가지 값이 있을 수 있습니다.
범주	접근 통제
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 권장 값으로 구성하지 않으면 위젯이 인스턴스 내의 모든 테이블에 액세스할 수 있습니다.
의존성 및 필수 구성요소	*glide.service_portal.widget.allow_list* 설정을 적용할 *glide.service_portal.widget.enforce_public_check* 수 있으려면 속성을 true로 설정해야 합니다.
기능적 영향	이 속성을 사용하면 위젯이 공개로 설정되어 있고 속성 값에 포함된 경우 고객이 테이블 정보에 액세스할 수 있습니다.

서비스 포털 위젯 허용 목록 구성**[Security Center** 2.0의 새로운 기능)

추가 검사 및 특정 Glide 속성 설정에 따라 서비스 포털 위젯을 통해 인증되지 않은 사용자가 액세스할 수 있는 테이블을 나열하여 속성이 보안을 강화하는 방법에 *glide.service_portal.widget.table_allow_list* 대해 알아봅니다.

이 *glide.service_portal.widget.table_allow_list* 속성에는 인증되지 않은 사용자가 SNCACLWidgetUtil 스크립트의 추가 보안 검사를 활용하는 서비스 포털 위젯을 통해 액세스할 수 있는 테이블 목록이 포함되어 있습니다. 이 속성은 Glide 속성이 *glide.service_portal.widget.enforce_public_check* true로 설정된 경우에만 적용됩니다. 이 속성에 불필요한 테이블을 포함하면 중요한 정보가 공개될 수 있습니다. 그럼에도 불구하고 테이블 ACL은 이전과 마찬가지로 계속 평가됩니다.

추가 정보

속성	설명
구성 이름	*glide.service_portal.widget.table_allow_list*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	부울
권장 값	예
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 보안 값으로 설정하지 않으면 불필요한 테이블이 포함될 수 있으며, 이로 인해 중요한 정보가 공개될 수 있습니다.
의존성 및 필수 구성요소	*glide.service_portal.widget.enforce_public_check* 설정을 적용하려면 속성을 true *glide.service_portal.widget.table_allow_list* 로 설정해야 합니다.
기능적 영향	테이블 목록은 위젯이 데이터를 검색할 수 있는 테이블에 대한 액세스를 제어합니다.

명시적 외부 역할에 대한 내부 액세스 거부 **[Security Center 1.3** 및 1.5에서 업데이트됨]

여러 속성이 함께 명시적 역할 사용 내부 거부 목록 강화 설정에 대한 구성을 구성합니다. 이 *glide.security.explicit_roles.enable_internal_user_blacklist* 속성은 외부 사용자에게 snc_internal 역할이 할당되는 것을 방지하며 속성이 snc_external 역할을 할당할 수 있도록 합니다 *glide.security.explicit_roles.internal_user_blacklist*.

Glide.security.explicit_roles.enable_internal_user_blacklist

Glide.security.explicit_roles.enable_internal_user_blacklist 및 **Glide.security.explicit_roles.internal_user_blacklist** 시스템 속성을 사용하여 외부 사용자 계정이 내부 정보에 액세스할 수 있는 위험을 줄입니다. **glide.security.explicit_roles.enable_internal_user_blacklist** 시스템 속성은 외부 사용자에게 snc_internal 역할을 할당하지 못하게 합니다.

maint로 보호되는 **glide.security.explicit_roles.internal_user_blacklist** 속성의 매개변수를 적용하려면 **Glide.security.explicit_roles.enable_internal_user_blacklist**를 예로 설정합니다. 이 속성은 신뢰할 수 없는 사용자 클래스 목록에 **snc_external** 역할을 할당합니다.

값이 **false**로 설정되면 **glide.security.explicit_roles.internal_user_blacklist** 속성이 무시됩니다. 이 속성을 잘못 구성하면 외부 사용자 계정이 내부 정보에 대한 액세스 권한을 얻을 위험이 높아집니다.

주: 명시적 역할이 설치되지 않은 인스턴스는 영향을 받지 않습니다. 릴리스부터 Paris 명시적 역할을 새로 설치하면 기본값이 true인 속성을 가져옵니다.

추가 정보

속성	설명
속성 이름	*glide.security.explicit_roles.enable_internal_user_black*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
범주	접근 통제
목적	지정된 사용자 클래스를 **snc_internal** 역할 대신 **snc_external** 역할에 할당할 수 있습니다.
권장 값	예
기본값	예
구성 유형	부울
보안 위험	(보통) 속성을 사용하지 않도록 설정하면 기본 역할 할당이 부적절해질 수 있습니다.
보안 위험 등급	5.4
참조	CSM의 명시적 역할

Glide.security.explicit_roles.internal_user_blacklist

이 *glide.security.explicit_roles.internal_user_blacklist* 값은 snc_internal 역할 대신 snc_external 역할을 할당해야 하는 사용자 클래스(sys_user 확장하는 테이블)를 결정합니다. 기본값 csm_consumer_user customer_contact은 고객 서비스 관리 플러그인의 사용 사례에 맞게 정의됩니다.

속성 값은 snc_internal 역할 대신 기본적으로 snc_external 역할을 할당해야 하는 추가 또는 다른 사용자 클래스가 있는 경우에만 변경해야 합니다. 이러한 값을 변경하려면 지원 서비스에 문의하십시오.

속성	설명
속성 이름	*glide.security.explicit_roles.internal_user_blacklist*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	snc_internal 역할 대신 기본적으로 snc_external 역할을 할당할 수 있습니다.
권장 값	*csm_consumer_user*, *customer_contact*
구성 유형	문자열
보안 위험	(보통) 속성을 사용하지 않도록 설정하면 기본 역할 할당이 부적절해질 수 있습니다.
보안 위험 등급	5.4
참조	명시적 역할, 외부 사용자 역할 할당 수정

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

요청 항목에 대한 무단 액세스 거부[Security Center 1.3에서 업데이트됨]

이 *glide.sc.req_for.roles.default* 속성은 `retrieveAddress` API에 대한 기본 동작을 정의합니다.

이 속성은 값이 없는 경우에만 *glide.sc.req_for.roles* 작동합니다. 값이 있는 경우 *glide.sc.req_for.roles* 이 속성은 중요하지 않으며 정의된 역할만 있는 사용자에게 API에 대한 액세스 권한이 부여됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.sc.req_for.roles.default*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	속성에 지정된 역할이 없는 경우 클라이언트 호출 가능 스크립트 포함 *ScriptServiceCatalogGetLocation* 은 권한이 없는 로그인한 사용자가 호출할 수 있으며 시스템의 다른 사용자 주소를 검색할 수 있습니다. 이 속성은 이 API가 권한이 없는 사용자에게 노출되도록 보호합니다.
권장 값	거부
기본값	거부
구성 유형	선택 목록(허용 | 거부)
보안 위험	(보통) 가 권장 값인 거부(허용)로 설정되지 않고 *glide.sc.req_for.roles* 값이 비어 있으면 *glide.sc.req_for.roles.default* 모든 사용자가 다른 사용자에게 무단 자원 액세스를 허용하는 항목을 요청할 수 있습니다.
참조	클라이언트 호출 가능 스크립트 포함

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

안티-**CSRF** 토큰 사용**[Security Center** 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨〕

이 *glide.security.use_csrf_token* 속성을 사용하여 보안 토큰을 사용하여 들어오는 요청을 식별하고 유효성을 검사하며, 이는 이러한 공격을 방지하는 데 사용됩니다.

CSRF(교차 사이트 요청 위조)는 인증된 사용자가 현재 인증된 웹 응용 프로그램에 요청을 제출하도록 강제하는 공격입니다. CSRF 공격은 웹 응용 프로그램이 인증된 사용자에 대해 가지고 있는 신뢰를 악용합니다. 이 속성을 사용하면 보안 토큰 사용을 식별하고 수신 요청을 확인할 수 있습니다. 이 토큰은 교차 사이트 요청 위조 공격을 방지하는 데 사용됩니다. *glide.security.use_csrf_token* 권장 값인 true로 설정되지 않은 경우 CSRF를 사용할 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.security.use_csrf_token*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	잠재적인 CSRF 공격으로부터 애플리케이션을 보호합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 위험 등급	8.1
권장 값	예
기본값	예
기능적 영향	이렇게 정정하면 인스턴스 사용자가 인스턴스에 쓰기 요청을 제출하기 전에 추가 확인 단계가 활성화됩니다. 모든 쓰기 요청에는 CSRF 토큰(즉, 사용자 세션에 연결된 유효성 검사/CSRF ID)이 포함됩니다. 사용자 세션이 만료되면 보안 토큰도 함께 만료됩니다.
보안 위험	(높음) 교차 사이트 요청 위조는 인스턴스 데이터의 무결성을 침해하는 중요한 보안 위험입니다. 공격자는 인스턴스 사용자의 신뢰를 악용하여 CSRF 공격을 시작할 수 있습니다. 소셜 엔지니어링 공격을 통해 사용자는 인스턴스에서 공격자를 대신하여 잘못된 형식의 요청을 제출할 수 있습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

보관 테이블 ACL이 선택되어 있는지 확인 **[Security Center** 1.3의 새로운 기능 및 1.5에서 업데이트됨]

이 *glide.security.enable_archive_table_acls* 속성은 원래 테이블, 즉 보관 테이블이 생성된 테이블의 ACL(접근 제어 목록)이 false로 평가되는지 여부를 제어합니다.

glide.security.enable_archive_table_acls 원래 테이블의 ACL은 값에 관계없이 평가되므로 속성을 아니오로 설정해서는 안 됩니다. ACL을 추가하지 않으면 보관 테이블에 대한 추가 ACL을 피할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.security.enable_archive_table_acls*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 3 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 속성을 false로 설정하면 보관된 테이블에 추가된 ACL이 무시되며, 이는 직관적이지 않은 작업이므로 권한 부여 바이패스로 이어질 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성을 예로 설정하면 보관 테이블의 활성 읽기 ACL이 모두 허용됩니다. 활성 읽기 ACL이 없거나 속성이 false로 설정된 경우 원본 테이블(데이터가 보관된 테이블)이 보관 테이블에 적용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	주: 보관 테이블에서는 읽기 ACL만 지원됩니다. 보관 테이블에 대한 다른 작업은 액세스 핸들러를 통해 내부적으로 관리됩니다.

HR 수명 주기 이벤트 데이터에 ACL 강제 적용[Security Center 2.0의 새로운 기능]

가 *glide.enforce_security_scope.sn_hr_le property* 보안 값으로 설정되어 있는지 확인하여 인사 관리 수명주기 이벤트 애플리케이션의 데이터에 대한 무단 액세스를 방지하는 방법에 대해 알아봅니다.

이 *glide.enforce_security_scope.sn_hr_le* 속성은 "sn_hr_le" 범위만 고려되도록 여러 HR 테이블의 ACL(접근 제어 목록)을 제한합니다. 권장 값인 true로 설정되지 않은 경우 *glide.enforce_security_scope.sn_hr_le* Human Resources: 수명주기 이벤트 애플리케이션의 데이터가 다른 모든 범위의 ACL에 노출되어 권한이 없는 사용자가 중요한 데이터에 액세스할 수 있습니다. 예를 들어 IT 관리자가 HR 데이터에 액세스할 수 있습니다.

경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.enforce_security_scope.sn_hr_le*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 true 값으로 설정하지 않으면 Human Resources: 수명주기 이벤트 애플리케이션 데이터가 다른 모든 범위의 ACL에 노출될 수 있습니다. 이로 인해 권한이 없는 사용자가 민감한 데이터에 액세스할 수 있습니다.
의존성 및 필수 구성요소	안 함

애플리케이션 데이터에만 애플리케이션별 ACL 적용

애플리케이션 데이터에만 애플리케이션별 ACL(접근 제어 목록)을 적용하여 애플리케이션 데이터에 대한 무단 또는 원치 않는 액세스를 방지합니다.

애플리케이션 외부의 마스터 테이블에 상주하는 애플리케이션 데이터의 동작을 제어합니다. 이러한 속성의 값이 **true**이면 이러한 테이블에 있는 애플리케이션 데이터에 대한 액세스 여부는 애플리케이션별 ACL만 평가됩니다. 일부 애플리케이션은 이 구성에서 작동하도록 설계되거나 이 용도로 시스템 속성 [sys_properties] 레코드를 사용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 시스템 속성은 **glide.enforce_security_scope.<scope>** 명명 형식을 사용합니다. 예를 들어 sn_hr_sp(직원 센터 코어) 범위에 **glide.enforce_security_scope.sn_hr_sp** 속성을 사용합니다. 다음 애플리케이션 범위에 이 속성이 포함됩니다.

- 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_awa
- sn_hr_core
- sn_hr_ef
- sn_hr_er
- sn_hr_gen_ai
- sn_hr_hc
- sn_hr_le
- sn_hr_mii_base
- 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_uni_req
- sn_uni_task

추가 정보

속성	설명
기술 구성 이름	glide.enforce_security_scope.<scope>
플러그인 적용 가능성	안 함
보안 위험	이러한 속성의 **true** 값이 없는 경우 마스터 테이블의 ACL에 대한 액세스 평가가 계속 진행되므로 애플리케이션 데이터에 대한 무단 또는 원치 않는 액세스가 허용될 수 있습니다.
CVSS(공통 취약성 평가 시스템) 점수	5.5
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	현재 응용 프로그램을 사용하지 않는 사용자와 같은 사용자는 범위 마스터 테이블에 있는 응용 프로그램 데이터에 액세스하지 못할 수 있습니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	예
폴백 값	거짓
권장 값	예

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

상황별 보안 플러그인 사용(보안 센터 1.3에서 업데이트됨)

상황별 보안 플러그인(*com.glide.role_management*) 플러그인을 활성화하면 작성, 읽기, 쓰기 및 삭제 기능을 사용하여 기록/정보를 보호하는 상황별 보안을 사용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설치 및 활성화 후에는 사전 역할(단순 보안 관리자가 생성)이 더 이상 테스트되지 않습니다. Now Platform 대신 필드와 테이블에서 ACL 규칙을 찾습니다. 단순 보안 관리자가 구현하는 기존의 역할 기반 딕셔너리 규칙 대신 ACL 규칙을 사용하여 데이터를 보호합니다. 딕셔너리 양식을 구성하고 딕셔너리 항목에 역할을 추가해도 권한은 변경되지 않습니다.

추가 정보

속성	설명
플러그인 ID	*com.glide.role_management*
구성 유형	시스템 정의 > 플러그인
범주	접근 통제
목적	단순 보안 관리자와 달리 상황별 보안 관리자는 시스템 테이블 계층 구조를 인식합니다. 계층 구조에서 나타나는 위치에 따라 필드에 대해 다른 보안 규칙을 가질 수 있습니다.
권장 값	활성
기본값	이는 Glide 속성이 아닌 플러그인이므로 기본값이 없습니다.
보안 위험 등급	8.1
기능적 영향	이렇게 정정하면 접근 통제의 기능 수준이 적용되므로 애플리케이션에서 ACL 테이블만을 기준으로 접근 제한을 결정할 수 있습니다.
보안 위험	(높음) CRUD 작업을 실행하기 전에 서버 측에서 기능 수준 액세스 제어를 적용하여 인스턴스 사용자에 대한 적절한 수준의 액세스 권한을 보장해야 합니다.
참조	상황별 보안 관리자

보안 범위 라이센스 및 허가 플레이북 적용 **[Security Center** 1.5의 새로운 기능 및 2.0에서 업데이트됨]

이 속성을 사용하여 라이선스 및 허가 플러그인 내의 ACL(접근 제어 목록)만 범위에 대한 액세스를 결정하는 데 사용되는지 또는 모든 범위의 ACL을 고려할지 결정합니다.

glide.enforce_security_scope.sn_gsm_lic_prmt 속성이 권장 값인 true로 설정되면 License and Permit 플러그인 내의 ACL만 범위에 대한 액세스를 결정하는 데 사용됩니다. 이 설정이 false로 구성되면 모든 범위의 ACL에 액세스 권한이 부여되기 때문에 범위 마스터 테이블의 라이센스 및 허가 플레이북 데이터가 노출됩니다. 데이터 노출을 줄이려면 권장 값인 true로 설정합니다 *glide.enforce_security_scope.sn_gsm_lic_prmt*.

추가 정보

속성	설명
구성 이름	*glide.enforce_security_scope.sn_gsm_lic_prmt*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 2.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 설정을 권장 값인 true로 구성하면 액세스 권한을 부여할 범위의 ACL *sn_gsm_lic_prmt* 만 고려하여 범위 마스터 테이블의 라이센스 및 허가 플레이북 데이터를 보호합니다. 이를 아니오로 설정하면 액세스 권한을 부여하기 위해 모든 범위의 ACL을 고려하여 범위 마스터 테이블의 라이센스 및 허가 플레이북 데이터가 노출됩니다. 예를 들어, 이 설정이 false인 경우 IT 관리자는 라이센스 및 허가 플레이북 데이터에 액세스할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	• 라이센스 및 허가 플레이북 사용 • 애플리케이션 범위

HR 케이스 관리용 에이전트 작업 공간의 보안 범위 적용 [Security Center 1.5의 새로운 기능 및 2.0에서 업데이트됨]

범위 마스터 테이블의 데이터에 올바른 권한이 있는 사용자만 액세스할 수 있도록 HR 케이스 관리용 에이전트 작업 공간 플러그인을 구성하여 최소 권한 원칙을 적용합니다.

플러그인이 *glide.enforce_security_scope.sn_hr_agent_ws* 권장 값인 true로 구성되면 HR 케이스 관리용 에이전트 작업 공간 플러그인 내의 ACL(접근 제어 목록)만 자원에 대한 액세스를 결정하는 데 사용됩니다. 이 설정이 false로 설정되면 모든 범위의 ACL에 액세스 권한이 부여되므로 범위 마스터 테이블의 HR 케이스 관리용 에이전트 작업 공간 데이터가 노출됩니다.예를 들어 이 설정이 false로 설정된 경우 IT 관리자가 HR 케이스 관리용 에이전트 작업 공간 데이터에 액세스할 수 있습니다. 이러한 일이 발생하지 않도록 하려면 사용자가 권한이 있는 자원에만 액세스할 수 있으므로 최소 권한 원칙이 존재하도록 권장 값인 true로 설정합니다 *glide.enforce_security_scope.sn_hr_agent_ws*.

추가 정보

속성	설명
구성 이름	*glide.enforce_security_scope.sn_hr_agent_ws*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 2.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 설정을 false로 구성하면 모든 범위의 ACL에 액세스 권한이 부여되므로 범위 마스터 테이블의 HR 케이스 관리용 에이전트 작업 공간 데이터가 노출됩니다.
의존성 및 필수 구성요소	HR 케이스 관리용 에이전트 작업 공간
기능적 영향	이 설정을 예로 구성하면 범위가 지정된 ACL이 없는 경우 테이블에 대해 전역 ACL이 실행됩니다.
참조	• https://owasp.org/www-project-proactive-controls/#div-numbering • 에 구성요소 추가 에이전트 작업 공간

사용자가 **CSRF** 유효성 검사를 바이패스하기 위한 경고를 수락하지 못하도록 방지〔보안 센터 **1.3** 및 1.5에서 업데이트됨〕

glide.security.csrf.strict.validation.mode 속성을 사용하여 CSRF 토큰 엄격한 확인을 활성화합니다. CSRF 토큰이 일치하지 않으면 요청을 다시 제출할 수 없습니다.

이 속성은 사용자가 잠재적으로 악의적인 요청을 인스턴스로 보낼 수 있는 경고를 수락할 수 없도록 합니다. 이 경고는 피해자의 다른 활성 세션 중 하나에 속하는 안티-CSRF 토큰이 일치하지 않아 POST 요청이 실패할 때 나타납니다. 권장 값인 true로 설정되지 않은 경우 *glide.security.csrf.strict.validation.mode* 공격자는 피해자에게 속한 다른 활성 세션에서 유출된 안티-CSRF 토큰을 사용하여 CSRF 공격을 공식화할 수 있습니다. 인스턴스에 대한 POST 요청에는 사용자의 현재 세션과 일치하는 "sysparm_ck" 또는 "X-UserToken" 내에 안티-CSRF 토큰이 포함되어 있습니다.

안티-CSRF 토큰이 사용자의 다른 활성 세션 중 하나에 대신 연결된 경우 POST 요청은 이 속성이 false로 설정된 경우 사용자가 사용할 수 있는 계속 단추를 사용하여 security_interceptor.do에 대한 302 리디렉션을 반환합니다. 이 단추를 클릭하면 인스턴스에 요청을 다시 제출합니다(단, 이제 유효한 안티-CSRF 토큰이 있는 경우는 제외). 이 특성을 예로 설정하면 security_interceptor.do 페이지로의 302 리디렉션에 계속 단추가 표시되지 않으며 사용자가 요청을 다시 제출할 수 없습니다. CSRF 공격이 성공하면 공격자는 피해자가 수행할 수 있는 모든 작업을 효과적으로 수행할 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.security.csrf.strict.validation.mode*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	CSRF 토큰의 엄격한 유효성 검사를 적용하고 재사용을 방지합니다.
데이터 유형	부울
권장 값	예

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기본값	예
보안 위험 등급	(중간) 교차 사이트 요청 위조는 인스턴스 데이터의 무결성을 침해하는 중요한 보안 위험입니다. 공격자는 인스턴스 사용자의 신뢰를 악용하여 모든 인스턴스 사용자에 대해 CSRF 공격을 시작할 수 있습니다. 소셜 엔지니어링 공격을 통해 사용자는 공격자 대신 인스턴스에 잘못된 형식의 요청을 제출할 수 있습니다.
보안 위험 등급	3.7
기능적 영향	이렇게 정정하면 인스턴스 사용자가 인스턴스에 쓰기 요청을 제출하기 전에 추가 확인 단계가 활성화됩니다. 현재 CSRF 토큰이 이전에 사용되었는지 여부를 확인합니다. 예일 경우 추가 쓰기 요청이 제출되지 않습니다.
보안 위험	(중간) 교차 사이트 요청 위조는 인스턴스 데이터의 무결성을 침해하는 중요한 보안 위험입니다. 공격자는 인스턴스 사용자의 신뢰를 악용하여 모든 인스턴스 사용자에 대해 CSRF 공격을 시작할 수 있습니다. 소셜 엔지니어링 공격을 통해 사용자는 공격자 대신 인스턴스에 잘못된 형식의 요청을 제출할 수 있습니다.

래핑된 키를 업로드하려면 돌아가기 고객 공급 키 구성 및 업로드

HR Core 데이터에 ACL 강제 적용[Security Center 2.0의 새로운 기능]

인사 관리 범위 지정 앱: Core(com.sn_hr_core) 플러그인이 다른 모든 범위의 접근 제어 목록(ACL)에 중요한 데이터를 노출하지 않도록 속성을 구성하는 *glide.enforce_security_scope.sn_hr_core* 방법에 대해 알아봅니다.

이 *glide.enforce_security_scope.sn_hr_core* 속성은 sn_hr_core 범위만 고려하도록 sys_attachment 및 sys_email와 같은 여러 전역 데이터 테이블의 ACL(접근 제어 목록)을 제한합니다. 이 속성을 권장 값인 예로 설정하지 않으면 인사 관리 범위 지정 앱: Core 플러그인의 데이터가 다른 모든 범위의 ACL에 노출됩니다. 예를 들어 IT 관리자가 인사 관리 데이터에 접근하는 상황이 발생할 수 있습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.enforce_security_scope.sn_hr_core*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 보안 값인 예로 설정하지 않으면 인사 관리 범위 지정 앱: Core 플러그인의 데이터가 다른 모든 범위의 ACL에 노출됩니다.
의존성 및 필수 구성요소	안 함
참조	Case and Knowledge Management 활성화

HR 가상 에이전트 데이터에 ACL 강제 적용[Security Center 2.0의 새로운 기능]

속성을 안전한 값으로 설정하여 *glide.enforce_security_scope.sn_hr_va* 가상 에이전트 대화 범위가 지정된 애플리케이션에서 데이터 유출을 방지하는 방법을 알아봅니다.

이 *glide.enforce_security_scope.sn_hr_va* 속성은 여러 HR(인사 관리) 테이블의 ACL(접근 제어 목록)이 sn_hr_va 범위만 고려하도록 제한합니다. 이 속성을 권장 값인 true로 설정하지 않으면 인사 관리: 가상 에이전트 대화 범위가 지정된 애플리케이션의 데이터가 다른 모든 범위의 ACL에 노출됩니다. 예를 들어 IT 관리자가 HR 데이터에 액세스할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.enforce_security_scope.sn_hr_va*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 보안 값 예로 설정하지 않으면 인사 관리: 가상 에이전트 대화 범위가 지정된 애플리케이션의 데이터가 다른 모든 범위의 ACL에 노출될 수 있습니다.
의존성 및 필수 구성요소	안 함

서비스 응용 프로그램 정보에 대한 보안 범위 적용[Security Center 2.0의 새로운 기능]

속성을 *glide.enforce_security_scope.sn_svc_appl* 사용하여 마스터 범위 테이블의 데이터가 보호되도록 합니다.

glide.enforce_security_scope.sn_svc_appl_info 속성이 true로 설정되면 범위 내의 자원에 대한 액세스는 서비스 sn_svc_appl_info(애플리케이션 정보 플러그인)의 ACL(접근 제어

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

목록)에 의해서만 결정됩니다. 이렇게 하면 sn_svc_appl_info 범위 내에 정의된 권한으로 액세스 권한을 제한하여 마스터 범위 테이블의 데이터 보안을 보장할 수 있습니다.

안전하지 않은 값인 false로 설정하면 sys_attachment와 같은 마스터 범위 테이블의 데이터에 대한 액세스 권한을 부여할 때 모든 범위의 ACL이 고려됩니다. 이로 인해 서비스 애플리케이션 정보 데이터에 대한 권한이 없는 사용자가 중요한 정보에 무단으로 액세스할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.enforce_security_scope.sn_svc_appl_info*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 안전하지 않은 값인 false로 설정하면 서비스 애플리케이션 정보 데이터에 대한 권한이 없는 사용자가 중요한 데이터에 무단으로 액세스할 수 있습니다.
의존성 및 필수 구성요소	속성을 적용하려면 서비스 신청자 정보 플러그인(*com.sn_svc_appl_info*을 *glide.enforce_security_scope.sn_svc_appl_info* 활성화해야 합니다.

위임된 개발자의 읽기 권한 제한**[Security Center** 1.3에서 업데이트됨〕

권장 값인 wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget 및 sp_page가 포함되지 않은 경우 *com.glide.dd_allow_global_access_tables* 위임된 개발자가 해당 테이블을 읽을 수 있습니다. 이렇게 하면 위임된 개발자에게 중요한 정보에 대한 읽기 권한이 제공될 수 있습니다.

추가 정보

속성	설명
속성 이름	*com.glide.dd_allow_global_access_tables*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본값	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget, sp_page
범주	접근 통제
보안 위험	• 심각도 점수: 2.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget sp_page로 설정되어 있는지 확인합니다 *com.glide.dd_allow_global_access_tables*.

잠긴 사용자에 인바운드 이메일 사용 안 함

이 *glide.pop3.process_locked_out* 속성을 사용하여 잠겨 있는 활성 사용자에 대한 인바운드 이메일 작업을 제어합니다.

잠긴 사용자에 대해 인바운드 이메일을 사용하지 않으려면 이 속성을 아니오 로 설정합니다.

주: 신뢰할 수 없는 도메인의 사용자를 허용하는 것이 보안에 미치는 영향과 해당 사용자가 잠긴 이유를 고려한 후 해당 사용자의 이메일이 인바운드 이메일 작업을 트리거하도록 허용합니다.

추가 정보

속성	설명
속성 이름	*glide.pop3.process_locked_out*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	이 속성은 잠긴 사용자에 대한 인바운드 이메일 작업을 제어합니다.
데이터 유형	부울
권장 값	거짓
기본값	거짓
보안 위험	(높음) 이 속성을 예 로 설정하면 잠긴 계정을 가진 사용자가 인바운드 이메일을 수신하므로 정보 공개가 있을 수 있습니다.
보안 위험 등급	7.5

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가.

높은 위험 **UI** 페이지에 대한 권장 사항 표시

위험도가 높은 UI 페이지에 대한 권장 사항을 표시하여 권한 부여 오류 및 의도하지 않은 정보 공개 가능성을 줄입니다.

다음과 같은 경우 **glide.script.ui_page.customer_scoped.security_msgs_enabled** 시스템 속성을 사용하여 UI 페이지를 구성하는 사용자에게 보안 권장 사항을 표시할지 여부를 결정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- ACL이 없습니다.
- GlideRecordSecure 대신 GlideRecord/GlideDBQuery API가 사용됩니다.
- 페이지는 "sys_public" 테이블에서 공개로 구성됩니다.

속성을 활성화하면 이전 조건이 충족될 때 권장 사항이 적용되어 권한 부여 오류가 발생할 가능성이 줄어들고 의도하지 않은 정보 공개를 방지할 수 있습니다.

이러한 권장 사항을 표시하려면 시스템 속성 **glide.script.ui_page.customer_scoped.security_msgs_enabled** 를 **true** 로 설정합니다.

추가 정보

속성	설명
기술 구성 이름	glide.script.ui_page.customer_scoped.security_msgs_enabled
플러그인 적용 가능성	안 함
보안 위험	이 시스템 속성을 **false** 로 설정하면 권한 부여 오류 및 의도하지 않은 정보 공개 가능성이 높아집니다.
CVSS(공통 취약성 평가 시스템) 점수	5.3
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	UI 페이지를 구성하는 사용자에게 보안 권장 사항을 표시합니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	예
폴백 값	예
권장 값	예

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

인바운드 트랜잭션 다시 확인 **[Security Center** 1.3에서 업데이트됨〕

이 *glide.security.strict.updates* 속성을 사용하여 양식을 제출하는 동안 인바운드 트랜잭션의 보안을 두 번 검사할 수 있습니다. 이 속성을 **true**로 설정하면 양식이 브라우저에서 렌더링되기 전에 테이블 유효성 검사 레이어가 추가됩니다.

속성이 *glide.security.strict.updates* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
속성 이름	*glide.security.strict.updates*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	브라우저에 양식을 표시하기 전에 사용자 권한에 대한 추가 검증 계층을 보장하기 위해
데이터 유형	부울
권장 값	예
기본값	예
보안 위험 등급	8.1
기능적 영향	이렇게 정정하면 인스턴스의 대상 테이블/페이지에서 사용자 권한을 확인하기 위한 추가 유효성 확인 계층을 추가합니다. 고객 인스턴스에 접근 제어가 적절히 설정되어 있기만 하면 영향은 없습니다.
보안 위험	(높음) 두 영역 간에 트랜잭션이 발생하는 경우 항상 액세스 요청을 확인해야 합니다. 이 작업은 양식이 요청될 때와 양식 렌더링이 발생하기 전에 권한을 확인합니다.
참조	

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

컨트롤 라이브 프로파일 상세 정보에 **ACL** 사용 **[Security Center** 1.3에서 업데이트됨]

이 *glide.live_profile.details* 속성을 사용하여 사용자가 라이브 프로파일에서 회사 이름 및 전화번호와 같은 모든 상세 필드를 볼 수 있어야 하는지 여부를 지정합니다.

속성의 설정에 *glide.live_profile.details* 따라 다음과 같은 상황이 발생합니다.

- 값을 표시로 설정하면 사용자 프로파일에 대해 만들어진 ACL에 관계없이 라이브 프로파일 정보에 대한 액세스 권한이 부여됩니다.
- 값을 ACL로 설정하면 사용자 프로파일에 대해 생성된 ACL에 따라 라이브 프로파일 정보에 대한 액세스가 제한됩니다.
- 값을 숨기기로 설정하면 사용자 프로파일에 대해 생성된 ACL에 관계없이 라이브 프로파일 정보에 대한 액세스가 제한됩니다.

추가 정보

속성	설명
속성 이름	*glide.live_profile.details*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	목적은 권한이 있는 사용자만 라이브 프로필의 세부 정보(예: 회사 이름, 전화 번호)에 액세스할 수 있도록 하는 것입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	선택 목록
권장 값	ACL
기본값	ACL
보안 위험 등급	4.3
기능적 영향	속성이 활성화되지 않은 경우 권한 없는 사용자는 다른 모든 사용자의 라이브 프로파일 상세 정보에 액세스할 수 있습니다.
보안 위험	(보통) API 요청은 항상 테이블 ACL을 사용해야 합니다. 권한이 없는 사용자가 라이브 프로파일의 세부 사항에 액세스하지 못하도록 제한을 적용해야 합니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

단순 목록 위젯에서 인코딩된 쿼리에 **ACL** 사용 **[Security Center** 2.0의 새로운 기능]

사용자가 단순 목록 위젯의 쿼리 조건에 대한 접근 제어 목록 (ACL) 평가를 바이패스하지 못하도록 속성을 보안 값으로 설정하는 *glide.service_portal.enable_acls_for_encoded_query_in_list* 방법에 대해 알아봅니다.

glide.service_portal.enable_acls_for_encoded_query_in_list 속성이 보안 값인 true로 설정되지 않은 경우 사용자는 단순 목록 위젯의 쿼리 조건에 대한 ACL(접근 제어 목록) 평가를 바이패스할 수 있습니다. 속성이 false로 설정되면 이전 동작으로 되돌아가고, enforce_acl 확인란 값을 기반으로 인코딩된 쿼리에 대한 ACL 검사를 적용합니다.

쿼리 내에서 ACL을 평가하여 사용자가 쿼리 중인 필드에 액세스할 수 있도록 하여 무단 데이터 유출을 방지하는 것이 가장 좋습니다.

Glide 속성이 *glide.service_portal.enable_acls_for_encoded_query_in_list* true로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 없는 경우 기본값은 true입니다.

추가 정보

속성	설명
구성 이름	*com.glide.script.fencing.cross_scope_access.shared_table_*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값인 예로 설정하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
의존성 및 필수 구성요소	안 함
기능적 영향	단순 목록 위젯은 사용자의 역할과 기본 ACL에 따라 데이터를 표시하지 않을 수 있습니다. 또한 단순 목록 쿼리에 현재 사용자가 액세스할 수 없는 속성이 있는 필터 조건이 포함되어 있는 경우 보안 경고가 발생할 수 있습니다.

iframe 간의 교차 원본 통신에 URL 허용 목록 사용

이 *glide.ui.concourse.onmessage_enforce_same_origin* 속성을 사용하여 `iframe` 간의 교차 출처 통신을 활성화합니다.

`OpenFrame` 은 속성에 지정된 신뢰 도메인의 메시지만 처리할 수 있습니다 *glide.ui.concourse.onmessage_enforce_same_origin_whitelist*. 자세한 내용은 iframe 간의 교차 원본 통신에 URL 허용 목록 사용 문서를 참조하십시오.

추가 정보

속성	설명
속성 이름	*glide.ui.concourse.onmessage_enforce_same_origin*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
범주	접근 통제
목적	OpenFrame의 iframe 간에 통신할 수 있도록 신뢰할 수 있는 도메인의 포함 목록을 활성화합니다.
권장 값	예
기본값	예
보안 위험 등급	4.2
기능적 영향	원하는 도메인을 포함 목록에 추가하지 않으면 인스턴스 내에 Now Platform 다른 페이지를 포함하는 기능이 제한될 수 있습니다.
보안 위험	(높음) 웹 페이지에 적절한 원본 유효성 검사를 수행하지 않는 이벤트 처리기가 포함된 경우 모든 원본의 웹 페이지 또는 스크립트가 해당 처리기와 통신할 수 있습니다. 또한 이벤트 처리기에서 수행하는 모든 기능을 시작할 수도 있습니다.
참조	OpenFrame 개요

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

애플리케이션 범위 제한 적용[Security Center 1.3의 새로운 기능 및 1.5에서 제거됨]

이 *glide.record.legacy_cross_scope_access_policy_in_script* 속성을 사용하여 범위가 지정된 앱의 권한을 제어합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

glide.record.legacy_cross_scope_access_policy_in_script 속성이 true로 설정된 경우 범위가 지정된 앱은 전역 앱에서만 사용할 수 있어야 하는 API를 호출할 수 있습니다. 이 속성은 범위가 지정된 앱에 대한 개발자를 만들고 업데이트하기 위해 의도된 접근 제어를 바이패스합니다.

추가 정보

속성	설명
구성 이름	*glide.record.legacy_cross_scope_access_policy_in_script*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	false
기본값	true(속성이 sys_properties 테이블에 없는 경우)
범주	접근 통제
보안 위험	• 심각도 점수: 3.5 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성이 권장 값으로 설정되지 않은 경우 범위가 지정된 앱 및 해당 범위가 지정된 앱에 대해 위임된 개발자는 인시던트와 같은 전역 테이블에서 기록을 만들고 업데이트할 수 있습니다.
의존성 및 필수 구성요소	안 함

로그인 시 현재 암호 정책 준수 요구 사항 강제 적용

로그인 시 현재 암호 정책 준수 요구 사항을 적용하여 무차별 암호 대입 계정 로그인의 위험을 줄입니다.

대화형 사용자가 **glide.apply.password_policy.on_login** 시스템 속성을 사용하여 현재 관리자 요구 사항을 충족하지 않는 암호로 인스턴스에 로그인하지 못하도록 합니다.

glide.apply.password_policy.on_login 시스템 속성을 **true**로 설정하여 현재 암호 정책 준수 요구 사항을 적용합니다. 이 속성이 시스템 속성 [sys_properties] 테이블에 없는 경우 기본값은 **false**입니다.

추가 정보

속성	설명
기술 구성 이름	glide.apply.password_policy.on_login
플러그인 적용 가능성	안 함
보안 위험	대화형 사용자는 현재 관리자 요구 사항을 충족하지 않는 암호로 인스턴스에 계속 로그인할 수 있습니다. 이는 사용자가 최신 보안 요구 사항을 충족하지 않는 약한 암호를 가지고 있음을 의미할 수 있으며, 이는 악의적인 사용자의 무차별 암호 대입 계정 로그인 위험을 증가시킬 수 있습니다.
CVSS(공통 취약성 평가 시스템) 점수	4.4

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	기존 암호가 현재 암호 정책을 준수하지 않는 경우 이 속성을 활성화하면 사용자가 다음에 로그인할 때 암호를 변경해야 합니다. 이 속성은 **false**로 자동 설정됩니다. 값을 **true** 로 설정하면 로그인하는 동안 암호 정책이 적용됩니다. 주: 이 속성을 사용하도록 설정하면 새 암호 정책을 준수하지 않는 많은 수의 사용자가 암호를 변경해야 할 수 있습니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	거짓
폴백 값	거짓
권장 값	예

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

공유 대시보드에 보안 규칙 적용[**Security Center** 1.3의 새로운 기능]

이 *glide.cms.dashboards.sharing_with_secure_search* 속성을 사용하여 사용자가 대시보드를 공유할 수 있는지 여부를 제어합니다.

속성이 *glide.cms.dashboards.sharing_with_secure_search***true**로 설정되지 않은 경우 사용자는 액세스할 수 없는 대시보드 그룹 및 역할을 공유할 수 있습니다. 이 속성을 활성화하면 대시보드 공유 프로세스 중에 sys_user, sys_user_role 및 sys_user_group 테이블을 검색할 때 ACL(접근 제어 목록)이 적용됩니다. 대시보드를 과도하게 공유하면 사용자, 그룹 또는 역할이 볼 수 있는 권한이 없어야 하는 데이터에 액세스하여 중요한 정보가 손상될 수 있습니다. 따라서 대시보드가 적절한 권한이 있는 사용자와만 공유되도록 true로 설정하는 *glide.cms.dashboards.sharing_with_secure_search* 것이 좋습니다.

추가 정보

속성	설명
구성 이름	*glide.cms.dashboards.sharing_with_secure_search*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 3.5 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 권장 값인 예로 설정하지 않으면 sys_user, sys_user_role 및 sys_user_group

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	테이블을 검색할 때 접근 제어 목록이 적용되지 않습니다. 이로 인해 대시보드가 권한이 없는 사용자와 공유되어 중요한 정보가 노출될 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	접근 통제
기능적 영향	이 속성은 대시보드를 공유할 때 표시되는 사용자, 사용자 그룹 및 역할 목록에 보안 규칙을 적용합니다.

공공 부문 디지털 서비스에 범위 보안 적용**[Security Center** 1.3의 새로운 기능]

이 *glide.enforce_security_scope.sn_gsm* 속성을 사용하여 공공 부문 디지털 서비스 애플리케이션의 애플리케이션 데이터에 액세스하는 방법을 제어합니다.

이 ServiceNow 공공 부문 디지털 서비스 애플리케이션을 사용하면 구성원, 기업 및 기관에 디지털 서비스를 제공하는 공공 부문 애플리케이션을 개발할 수 있습니다.

glide.enforce_security_scope.sn_gsm false로 설정되면 공공 부문 디지털 서비스 앱의 전역 테이블 내에 있는 애플리케이션 데이터에 대한 액세스는 해당 전역 테이블의 접근 제어 목록(ACL)을 기반으로 접근할 수 있습니다. 이 속성을 예로 설정하면 전역 테이블에 상주하는 데이터에 대한 액세스는 공공 부문 디지털 서비스 앱에서 직접 제공된 ACL을 기준으로만 평가됩니다. 이 속성을 아니오로 설정하면 허용 ACL을 통해 정보가 공개될 수 있습니다.

이 보안 위험을 정정하려면 true로 설정합니다 *glide.enforce_security_scope.sn_gsm*.

추가 정보

속성	설명
구성 이름	*glide.enforce_security_scope.sn_gsm*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 4.2 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값으로 설정하지 않으면 허용 ACL을 통해 정보 공개가 발생할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	공공 부문 디지털 서비스 구성

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정보 요청 플레이북에 대한 범위 지정 **ACL** 액세스 강제 적용 **[Security Center** 1.3의 새로운 기능 및 1.5에서 업데이트됨〕

이 *glide.enforce_security_scope.sn_gsm_info_req* 속성을 사용하여 Information Request Playbook 기능의 플레이북 데이터에 대한 액세스를 제어합니다.

이 Information Request Playbook 애플리케이션을 통해 공공 부문 최종 사용자는 공용 기록 요청을 제출하고 추적할 수 있으며 정부 에이전트에게는 이러한 요청을 처리하고 해결하기 위한 미리 정의된 프로세스가 제공됩니다. true로 설정되지 않은 경우 *glide.enforce_security_scope.sn_gsm_info_req* Information Request 플레이북 애플리케이션의 플레이북 데이터에 대한 예기치 않은 액세스 권한이 부여될 수 있습니다. 액세스 권한을 부여할 때 sn_gsm_info_req 범위의 ACL만 고려하려면 이 속성을 예로 설정합니다.

추가 정보

속성	설명
구성 이름	*glide.enforce_security_scope.sn_gsm_info_req*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성이 false로 설정되면 범위 마스터 테이블의 플레이북 데이터에 대한 액세스 권한을 부여할 때 모든 범위의 ACL이 고려됩니다. 이는 정보 요청 플레이북 데이터를 노출할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	• Information Request Playbook 사용 • 정보 요청 서비스 채널 구성

엄격한 권한 상승 적용 **[Security Center** 1.3의 새로운 기능〕

이 *glide.security.strict_elevate_privilege* 속성을 사용하여 사용자에게 역할의 기능을 부여하기 위해 권한 있는 것으로 표시된 역할을 수동으로 상승시켜야 하는지 여부를 제어합니다.

권한 있는 사용자가 역할을 상승시킬 때 보안 확인 계층을 추가하려면 이 속성을 예로 설정합니다.

추가 정보

속성	설명
구성 이름	*glide.security.strict_elevate_privilege*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 6.7 • CVSS 점수: 중간 • 보안 위험 상세 정보: *glide.security.strict_elevate_privilege* false로 설정하면 권한 있는 것으로 표시된 역할이 관리자 사용자 새 세션에서 자동으로 상승되며 수동으로 상승시킬 필요가 없습니다(security_admin 제외).
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성은 필요한 경우 권한을 상승시키기 위해 관리자 역할 사용자가 필요합니다.

AJAXGlideRecord ACL 검사 필요[Security Center 1.3에서 업데이트됨]

*glide.script.secure.ajaxglideRecord*이 속성을 사용하여 테이블과 같은 서버 측 기록이 클라이언트 스크립트 내의 GlideAjax API를 사용하여 액세스할 때 접근 통제 규칙(ACL) 확인을 수행합니다.

클라이언트 스크립트에서 AJAXGlideRecord(GlideAjax - 클라이언트) API를 사용하여 서버 측 Glide 기록과 같은 구문을 사용할 수 있습니다. 많은 배포에서 강력하고 유용한 도구입니다.

GlideAjax API 호출에 ACL(접근 제어 목록)을 적용하기로 선택한 경우 현재 연결된 사용자가 액세스할 수 있는 데이터만 쿼리할 수 있습니다. 예를 들어 cmn_location 테이블을 읽을 권한이 없는 ESS 사용자가 로그인한 경우 해당 테이블에 대한 GlideAjax API 호출이 실패합니다.

Now Platform GlideAjax ACL 호출 검사 없이 실행 중인 경우 API는 현재 로그인한 사용자가 액세스할 수 없는 정보를 반환할 수 있습니다.

데이터를 쿼리할 때 GlideRecordSecure를 사용하여 최고 수준의 보안을 보장합니다. GlideRecord는 구성을 통한 ACL 시행에 의존하는 반면 GlideRecordSecure는 더 엄격한 보안 통제를 적용합니다. GlideRecordSecure는 중요한 데이터를 처리하기 위한 보다 안전하고 즉시 사용 가능한 솔루션을 제공합니다.

경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.script.secure.ajaxglideRecord*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
목적	클라이언트 측 API를 통해 기록에 액세스하는 경우에도 보안 ACL을 확인하고 유효성을 검사해야 합니다.
권장 값	예
기본값	예
보안 위험 등급	8.1
기능적 영향	이렇게 하면 AJAXGlideRecord API 호출을 사용하여 요청이 이루어질 때 서버 측 기록과 ACL 관계가 적용됩니다. ACL 컨피그레이션이 제대로 구성되지 않은 경우 잠재적인 영향이 있습니다. 영향 및 식별 방법에 대한 자세한 내용은 에서 클라이언트 측 GlideRecord(AJAXGlideRecord) 트랜잭션 감사 및 검토 [KB0550828] 문서를 참조하십시오HI 지식베이스 .
보안 위험	(높음) 클라이언트 스크립트를 통해 GlideAjax API를 통해 서버에서 임의의 데이터를 쿼리할 수 있습니다. 서버 측 자원은 적절한 권한 부여 없이도 액세스할 수 있으므로 ACL 유효성 검사를 사용하면 애플리케이션이 구성된 권한 부여를 기반으로 요청을 확인하는 데 도움이 됩니다.
임시 해결책	적절한 권한 부여 하에 실행되도록 GlideAjax(AJAXGlideRecord) API에서 사용하는 스크립트 포함, 프로세서 및 기타 엔터티에 대해 적절한 ACL이 생성되었는지 확인합니다. GlideRecord를 사용하여 테이블 기록에 액세스하기 전에 사용자 인증을 수행하는 `canRead(),canWrite(),canCreate(),canDelete()`와 같은 메서드를 구현합니다. 또 다른 방법은 GlideRecordSecure를 사용하는 것입니다. 클래스는 GlideRecord와 동일한 기능을 수행하고 ACL을 적용하는 GlideRecord 서버에서 상속됩니다.
참조	AJAXGlideRecord에 ACL 적용(클라이언트 측 Glide 기록) 이 속성은 클라이언트에서 시작된 스크립트 실행을 보호하고 제한하는 동일한 속성 제품군에 속합니다. • *glide.script.use.sandbox*: 클라이언트 작성 스크립트 샌드박스를 참조하십시오. • *glide.script.allow.ajaxevaluate*: AJAXEvaluate 사용을 참조하십시오.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

GlideRecordSandbox에 필드 수준 **ACL** 강제 적용

인스턴스의 GlideRecordSandbox에서 필드 수준 ACL을 관리합니다.

이*glide.sandbox.fields.check_acl* 속성을 사용하여 GlideRecordSandbox에서 필드 수준 ACL을 적용합니다. 이 속성이 적용되는 예는 에서와 같이 *sysparm_query*사용자가 스크립트를 제공할 수 있는 경우입니다. 이 속성을 권장 값인 **true**로 설정하지 않으면 ACL 제한을 바이패스할 수 있으므로 권한이 없는 사용자의 민감한 데이터와 같은 *sys_user.user_password*데이터가 손상될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

⚠ 경고: 이 속성의 값은 DB 재정의가 없습니다. 변경하거나 재정의할 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.sandbox.fields.check_acl*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 7.5 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하면 중요한 데이터를 노출할 수 있는 ACL 제한을 바이패스할 수 있습니다.
의존성 및 필수 구성요소	안 함

자격 증명 별칭 사용 적용**[Security Center** 1.3의 새로운 기능 및 1.5에서 업데이트됨**]**

MID 서버 속성을 구성하여 자격 증명이 무단으로 사용되지 않도록 보호하는 방법에 대해 알아봅니다.

MID(관리, 계측 및 검색) 서버는 로컬 네트워크에서 Windows 서비스 또는 UNIX 디먼으로 실행되는 Java 애플리케이션입니다. MID 서버 속성이 [ecc_agent_property] 테이블에 나열됩니다. 인스턴스로 이동하여 해당 정보에 액세스할 수 있습니다. **MID** 서버 > 속성. 자격 증명 별칭을 사용하면 관리자가 Discovery 일정에서 특정 자격 증명을 사용할 수 있습니다. 자격 증명 별칭을 사용하면 검색 테이블에서 사용할 자격 증명을 보다 세부적으로 제어할 수 있습니다. 이 보안 취약성을 정정하려면 상승된 권한으로 자격 증명이 불필요하게 노출되지 않도록 엄격으로 설정하십시오 *alias_filtering_behavior*. 자세한 내용은 MID 서버 속성 문서를 참조하십시오.

추가 정보

속성	설명
구성 이름	*alias_filtering_behavior*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	엄격한
기본값	헐렁하다
범주	접근 통제

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 2 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 강화 설정이 엄격으로 설정되지 않으면 검색 테이블의 별칭에 관계없이 모든 자격 증명이 사용되므로 무단 액세스 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함
참조	• MID 서버 • 검색에 대한 자격 증명 별칭

그룹별 **ACL** 강제 적용

groupby 열에서 ACL 검사를 수행하도록 인스턴스를 구성합니다.

이 속성을 사용하여 groupby 열에서 ACL 검사를 수행하도록 인스턴스를 구성합니다. 이 속성이 권장 값인 **true**로 설정되면 테이블의 *groupby_acl_check* 속성이 그룹 기준 ACL을 승인하도록 설정됩니다. 속성이 **false**로 설정되면 테이블의 groupby 열에 대한 ACL 검사가 수행되지 않으므로 정보가 유출될 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.security.groupby_acl_check*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하면 groupby 열에 대한 ACL 검사가 비활성화되어 정보 유출로 이어질 수 있습니다.
의존성 및 필수 구성요소	안 함

대시보드 생성/삭제에 액세스 확인이 필요한지 확인 **[Security Center** 1.3의 새로운 기능 및 2.0에서 업데이트됨]

이 *glide.processors.check_access_before_process* 속성을 사용하면 사용자가 로그인할 때 대시보드를 생성하거나 삭제하기 위한 ACL(접근 제어 목록) 적용을 사용할 수 있습니다.

Glide 속성이 *glide.processors.check_access_before_process* 존재하고 true 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.processors.check_access_before_process*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 6.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 아니오로 설정하여 사용하지 않도록 설정하면 대시보드에서 ACL 바이패스가 활성화됩니다. 이렇게 하면 권한이 낮고 인증된 모든 사용자가 대시보드를 삭제하고 추가할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성은 사용자에게 필요한 액세스 권한이 없는 경우 새 sys_dashboards 만들고 기존 대시보드를 삭제하는 기능을 통제합니다. 이 값을 false로 설정하면 부적절한 역할을 가진 사용자가 sys_dashboard 항목을 추가하고 삭제할 수 있습니다(GlideRecord 계층에서 기존 ACL을 다시 확인해야 함). true 값은 필요한 액세스 권한이 없는 사용자에 대한 추가 및 삭제 작업을 제한합니다.

OAuth 상태 매개변수 유효성 검사 강제 적용

glide.oauth.state.parameter.required 인스턴스가 CSRF(교차 사이트 요청 위조) 공격으로부터 보호되도록 이 속성을 구성합니다.

이 *glide.oauth.state.parameter.required* 속성을 사용하면 인증 코드 플로우에 대한 OAuth 요청에 상태 매개변수가 필요할 수 있습니다. State 매개변수는 특수 문자를 포함하거나 비워둘 수 없는 문자열 값입니다. 이 속성을 예 로 설정하면 공격자가 인증 중에 CSRF(교차 사이트 요청 위조) 공격을 수행할 수 없으므로 가장된 사용자의 공격으로부터 인스턴스를 보호할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.oauth.state.parameter.required*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 4.2 • CVSS 점수: 중간 • 보안 위험 상세 정보: CSRF 공격을 방지하려면 이 속성을 예 로 설정합니다.
의존성 및 필수 구성요소	안 함

엄격한 사용자 이미지 업로드 강제 적용

이 *glide.security.strict.user_image_upload*속성을 사용하여 사용자 기록에서 수행할 때 프로파일 사진의 업로드/업데이트에 대한 접근 통제를 활성화합니다.

이 설정을 사용하면 권한이 없는 사용자가 다른 사용자의 프로파일에 이미지를 업로드할 수 있습니다.

- 이 속성을 예로 설정하면 사진을 업로드할 때 테이블 ACL이 적용되며 권한 있는 사용자만 이미지를 업로드할 수 있습니다.
- **false**로 설정하면 사진 필드에 이미지 업로드에 ACL이 적용되지 않습니다.

추가 정보

속성	설명
속성 이름	*glide.security.strict.user_image_upload*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	권한이 있는 사용자에게만 사용자 이미지 업로드를 제한합니다.
권장 값	예
보안 위험 등급	3.7
기능적 영향	권한이 있는 사용자는 여전히 사용자 프로파일에 이미지를 업로드할 수 있으므로 기능에 영향을 미치지 않습니다.
보안 위험	(낮음) 이 속성을 **false**로 설정하면 인증된 사용자가 권한 부여 없이 다른 사용자의 계정에 이미지를 업로드할 수 있습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

외부 사용자 등록을 위한 전자 메일 도메인 제한 **[Security Center 1.3, 1.5** 및 2.0에서 업데이트됨]

속성을 *sn_ext_usr_reg.allowed_email_domains* 사용하여 허용되는 외부 이메일 도메인을 나열합니다.

sn_ext_usr_reg.allowed_email_domains 시스템 속성은 인스턴스에 직접 등록할 ServiceNow 수 있는 이메일 주소를 정의합니다. 형식은 `domain1.com`, `domain2.com` 와 같은 허용 가능한 이메일 도메인의 쉼표로 구분된 목록이어야 하며, `example@domain2.com` 등의 이메일이 허용됩니다. 허용 가능한 도메인 목록으로 **sn_ext_usr_reg.allowed_email_domains** 가 설정되지 않은 경우 이메일 주소가 있는 사용자는 인스턴스에 계정을 등록할 수 있습니다. 정의되지 않은 경우 악의적인 행위자는

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

원치 않는 도메인의 이메일 주소를 사용해 등록을 수행하여 인스턴스에 대한 인증된 액세스 권한을 얻을 수 있습니다.

추가 정보

속성	설명
속성 이름	*sn_ext_usr_reg.allowed_email_domains*
구성 유형	시스템 속성(/sys_properties_list.do), 커뮤니티 속성
범주	접근 통제
목적	사용자 등록에 이메일을 허용할 이메일 도메인을 나열합니다.
권장 값	비어 있지 않은 값으로 설정
구성 유형	문자열
보안 위험	(높음) 악의적인 행위자는 원치 않는 도메인의 이메일 주소를 사용하여 등록을 수행할 수 있습니다. **sn_ext_usr_reg.allowed_email_domains**가 빈 값으로 설정되지 않았는지 확인합니다.
보안 위험 등급	7.5
참조	Communities

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

높은 보안 플러그인 사용 〔보안 센터 1.3에서 업데이트됨〕

High Security 플러그인을 사용하면 수백 가지의 다른 구성이 생성 또는 업데이트되어 인스턴스 보안 수준을 통제합니다. 이러한 구성은 엄격한 액세스 제어, 입력 유효성 검사 및 출력 인코딩을 사용하도록 설정하여 많은 최상위 OWASP 공격을 완화합니다.

이러한 구성에는 다음이 포함됩니다.

- 접근 통제
- 비즈니스 규칙
- 시스템 속성
- UI 정책 작업
- 스크립트 작업
- 스크립트 포함

예제

다음 속성에 대한 예시를 참조하십시오.

속성	주제
glide.ui.escape_all_script	이스케이프 Jelly 스크립트[Security Center 1.3 및 1.5에서 업데이트됨〕
glide.security.strict.actions	실행 전 UI 작업 조건 확인

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	주제
glide.security.csrf_previous.허용	안티-CSRF 토큰 사용[Security Center 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨]
glide.security.csrf.strict.validation.mode	사용자가 CSRF 유효성 검사를 바이패스하기 위한 경고를 수락하지 못하도록 방지 [보안 센터 1.3 및 1.5에서 업데이트됨]

추가 정보

속성	설명
플러그인 이름	com.glide.high_security
구성 유형	시스템 정의 > 플러그인 - 개발
범주	접근 통제
목적	이 플러그인을 활성화해야 합니다. 인스턴스의 보안 수준을 높여 CSRF, XSS, 세션 쿠키 보안 및 파일 업로드를 포함한 owasp 상위 10개 공격을 완화하여 공격 노출 영역을 줄입니다.
권장 값	활성
보안 위험 등급	9.8
기능적 영향	이 플러그인을 사용하면 UI와 기능에도 영향을 줄 수 있는 여러 시스템 보안 구성을 사용할 수 있습니다.
보안 위험	(높음) 많은 보안 구성이 의도치 않게 열려 있어 일부 중요한 취약점에 대한 문이 열릴 수 있습니다.
참조	높은 보안 설정 활성화 높은 보안 설정

플러그인 활성화에 대한 자세한 내용은 다음을 참조하십시오. 플러그인 활성화

관리자 재정의 **ACL** 인식

이 *glide.security.admin.override.accessterm* 속성은 재정의가 적용되어야 하는 위치에서도 관리자가 ACL 평가를 재정의할 수 없도록 통제합니다.

추가 정보

속성	설명
속성 이름	*glide.security.admin.override.accessterm*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	관리자가 ACL 평가를 재정의할 수 없도록 통제합니다.
데이터 유형	부울
권장 값	예

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기본값	예
보안 위험	(낮음) ACL은 누적 평가됩니다. 지정된 필드에 ACL 수가 있고 그 중 하나에서 Admin Overrides(관리자 재정의) 옵션이 false(선택되지 않음)인 경우 모든 ACL에 대한 유효한 관리자 재정의는 false로 간주됩니다.
보안 위험 등급	3.8
참조	접근 제어 목록 규칙

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

비활성 사용자의 로그인 방지 [Security Center 1.5의 새로운 기능]

비활성 사용자가 인스턴스에서 인증할 수 있는지 여부를 제어하려면 이 속성을 구성합니다.

속성 값을 예(권장)로 *glide.authenticate.only.allow.active.user.login* 설정하면 비활성으로 표시된 sys_user 테이블의 사용자가 인스턴스에 로그인할 수 없으며 잠깁니다.

설정이 false로 구성된 경우 사용자는 이전에 액세스할 수 있었던 인스턴스와 데이터에 계속 액세스할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.only.allow.active.user.login*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 7.5 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 권장 값인 예로 설정하지 않으면 해고된 직원과 같은 비활성 사용자가 인스턴스 및 데이터에 계속 액세스할 수 있습니다.
의존성 및 필수 구성요소	안 함

가상 에이전트가 포함된 웹 클라이언트에 대한 인증되지 않은 접근 방지

인증되지 않은 사용자가 포함된 웹 클라이언트에 액세스하지 못하도록 테이블을 구성하는 *sn_va_web_client_app_embed* 방법을 알아봅니다.

포함된 가상 에이전트용 웹 클라이언트인 UI 페이지에는 *sn_va_web_client_app_embed* 바로 사용 가능한 sys_public 테이블에서 true로 표시된 접근 제어 목록(ACL)이 포함되어 있습니다. 공개 접근성이 필요한 사용 사례가 있는 것으로 확인되었지만 이는 기본적으로 공개 접근성으로 설정하는 표준이 아닙니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

미인증 사용자에게 포함된 웹 클라이언트가 필요하지 않은 경우 공용 페이지 [sys_public] 테이블에서 기록(sys_id `04b1905473222300e985658b4cf6a7ef`)을 열고 *sn_va_web_client_app_embed*활성 필드를 선택 취소하여 페이지를 비활성화합니다.

추가 정보

속성	설명
구성 이름	**sn_va_web_client_app_embed**
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	테이블
권장 값	**sn_va_web_client_app_embed** 공용 페이지 [sys_public] (sys_id `04b1905473222300e985658b4cf6a7ef`)이 없거나 활성 상태가 아닙니다.
기본값	사용할 수 없음(테이블 값)
범주	접근 통제
보안 위험	• 심각도 점수: 7.5 • CVSS 점수: 높음 • 보안 위험 상세 정보: 미인증 사용자에게 포함된 웹 클라이언트가 필요하지 않은 경우 UI 페이지를 *sn_va_web_client_app_embed*비활성화하는 것이 좋습니다.
의존성 및 필수 구성요소	안 함

JSONP 요청을 신뢰할 수 있는 URL로 제한[Security Center 1.3에서 업데이트됨]

AngularJS $http 서비스에 신뢰할 수 있는 URL을 지정하여 JSONP 요청을 허용하거나 거부합니다.

이 *angular.jsonp.inclusion_list.enabled*속성은 angularJS $http 서비스에서 JSONP 요청을 허용 및/또는 거부할 신뢰할 수 있는 URL을 지정합니다. 이 속성은 고객의 변경 사항을 위반할 가능성이 있으므로 신뢰할 수 있는 URL을 추가할 방법이 필요하므로 이 속성이 필요합니다. 이 속성이 권장 값인 true로 설정되지 않은 경우 JSONP 요청은 모든 URL에 허용됩니다.

추가 정보

속성	설명
구성 이름	*angular.jsonp.inclusion_list.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 중간 • CVSS 점수: 5.4 • 보안 위험 상세 정보: 이 속성을 **false** 로 설정하면 모든 URL에 대한 JSONP 요청을 사용할 수 있습니다.
의존성 및 필수 구성요소	안 함

원시 데이터베이스 쿼리 실행 사용 안 함**[Security Center** 1.3에서 업데이트되고 2.0에서 제거됨〕

사용자가 데이터베이스에서 원시 SQL 쿼리를 수행할 수 있는지 여부를 제어합니다.

이*glide.db.allow_unsafe_dbi_execute_sql* 속성을 사용하면 사용자가 데이터베이스에서 원시 SQL 쿼리를 수행할 수 있으며, 이를 통해 GlideRecord 제한을 벗어난 테이블 및 데이터에 액세스할 수 있습니다. 이 속성이 권장 값인 *false*로 설정되지 않은 경우 Glide 스크립트에서 호출할 *dbi.executeStatement()* 수 있으며, 이로 인해 악성 SQL 문이 실행될 수 있습니다.

⚠ 경고: 이 속성은 안전하며 db 재정의가 없습니다.

추가 정보

속성	설명
구성 이름	*glide.db.allow_unsafe_dbi_execute_sql*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 7.2 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하지 않으면 Glide 스크립트에서 호출할 *dbi.executeStatement()* 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	접근 제어 목록 규칙

문서에 대한 사용자 주석 숨기기 **[Security Center** 1.3의 새로운 기능〕

이 속성을 사용하여 피드백 의견의 *glide.knowman.show_user_feedback* 표시 여부를 제어합니다.

안 함으로 설정되지 않은 경우 *glide.knowman.show_user_feedback* KB(지식베이스) 문서에 대한 피드백 의견이 Glide 속성, *glide.knowman.show_user_feedback.roles*에 정의된 역할을 가진 사용자에게 표시됩니다. 피드백 의견에는 중요한 정보가 포함될 수 있으므로 피드백이

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표시되는 것을 원하지 않을 수 있습니다. 이 속성이 never로 설정되지 않으면 중요한 정보가 피드백에 공개될 경우 기밀성에 영향을 미칠 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.knowman.show_user_feedback*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	선택 목록
권장 값	절대
기본값	온로드
범주	접근 통제
보안 위험	• 심각도 점수: 3.5 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 절대 설정하지 않으면 피드백 주석에 중요한 정보가 공개될 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	구성에 언급된 선택사항에 따라 KB 문서에 대한 사용자 의견을 표시합니다.

클라이언트 호출 가능 스크립트 포함에 대해 기본적으로 인증 필요 **[Security Center 1.3에서 업데이트됨]**

기본적으로 가시성을 명시적으로 설정하지 않는 클라이언트 호출 가능 스크립트 포함은 공개입니다. 필요한 경우 공용 페이지에서 접근한 모든 클라이언트 호출 가능 스크립트 포함에 대한 개인정보 통제를 *glide.script.ccsi.ispublic* 활성화하려면 속성을 추가하십시오.

이 속성을 추가할 때 해당 값을 **false**로 설정해야 하며, 이는 모든 클라이언트 호출 가능 스크립트 포함이 비공개임을 지정하고 공용 페이지에서의 가시성을 변경합니다.

주: **true** 값을 가진 속성을 추가하거나 **false** 값을 **true** 로 변경할 수 없습니다. 이렇게 하려고 하면 오류 메시지가 나타납니다.

필요한 경우 `isPublic()` 함수를 추가하여 개별 클라이언트 호출 가능 스크립트 포함에 대한 개인정보 설정을 변경할 수 있습니다.

- `isPublic()` 설정이 속성보다 *glide.script.ccsi.ispublic* 우선합니다.
- 예를 들어, 개별 스크립트에서 `isPublic()` 을 **true** 로 설정하면 public으로 설정되며, 이는 다른 모든 클라이언트 호출 가능 스크립트 포함을 비공개로 만드는 속성을 재정의 *glide.script.ccsi.ispublic* 합니다.

경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.script.ccsi.ispublic*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	클라이언트 호출 가능 스크립트 포함을 비공개로 설정하면 공용 페이지에 액세스하는 게스트가 클라이언트 호출 가능 스크립트 포함에 액세스할 수 없습니다. 로그인하지 않은 사용자는 비공개 스크립트를 실행할 수 없습니다.
권장 값	거짓
기본값	거짓
보안 위험 등급	7.5
기능적 영향	클라이언트 호출 가능 스크립트 포함이 공용으로 지정된 경우(즉, 이 속성이 누락된 경우) 인증되지 않은 사용자가 클라이언트 스크립트를 실행할 수 있습니다. 속성을 추가하면 로그인하지 않은 사용자의 스크립트 실행이 제한됩니다.
보안 위험	(높음) 이 속성을 추가하지 않으면 클라이언트 측 스크립트에 우회 ACL이 포함되어 의도하지 않은 공용 기능이 발생할 수 있습니다. 클라이언트 스크립트가 기밀 정보를 제공하는 경우 잠재적인 보안 위험에 악영향을 미칠 수 있습니다.
임시 해결책	*glide.script.ccsi.ispublic* 속성을 **false**로 설정하면 모든 클라이언트 호출 가능 스크립트 포함이 비공개로 설정됩니다. `isPublic()` 함수를 추가하여 개별 클라이언트 호출 가능 스크립트 포함에 대한 개인 정보 설정을 변경할 수 있습니다. `isPublic` 함수는 속성보다 *glide.script.ccsi.ispublic* 우선합니다. 스크립트 포함에 다음 구문을 추가합니다. `isPublic:function(){##[#/##];},`

프로덕션 인스턴스 동작 적용**[Security Center 1.3 및 1.5**에서 업데이트됨〕

인스턴스를 프로덕션 또는 비프로덕션 인스턴스처럼 처리할지 여부를 구성합니다.

속성이 권장 값인 **true**로 설정되지 않은 경우 인스턴스는 프로덕션 인스턴스로 처리되지 않으므로 zboot 및 기타 잠재적으로 위험한 스크립트를 실행할 수 있습니다. *glide.installation.production* 프로덕션 인스턴스를 비프로덕션 인스턴스로 평가하도록 설정하면 정보 유출 또는 DoS(서비스 거부) 공격으로 이어질 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.installation.production*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 6.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성 값을 **false** 로 설정하면 인스턴스가 비프로덕션 인스턴스로 처리되어 zboot 및 기타 잠재적으로 위험한 스크립트가 실행될 수 있습니다.
의존성 및 필수 구성요소	안 함

백그라운드 스크립트에 대한 액세스 제한 **[Security Center 1.3** 및 2.0에서 업데이트됨)

스크립트 백그라운드 모듈에 액세스하는 데 필요한 역할을 설정하도록 속성을 *glide.script_processor.admin* 구성합니다.

이 속성에는 스크립트 백그라운드 모듈에 액세스하는 데 필요한 역할이 있습니다. 가 admin의 권장 값 및 기본 값으로 설정되지 않은 경우 *glide.script_processor.admin* 권한이 더 낮은 사용자가 인스턴스에서 백그라운드 스크립트를 실행할 수 있습니다. 이렇게 하면 ACL 시스템을 완전히 바이패스하여 테이블에 대한 전체 액세스가 허용됩니다.

속성이 *glide.script_processor.admin* 관리자로 설정되어 있는지 확인합니다. 이 값은 인스턴스의 기본값입니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.script_processor.admin*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	관리자
기본값	관리자
범주	접근 통제

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 8.8 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 권장 값인 관리자로 설정하지 않으면 모든 사용자가 인스턴스에서 백그라운드 스크립트를 실행할 수 있습니다.
의존성 및 필수 구성요소	안 함

빈 대상 테이블이 있는 이메일에 접근 제한

glide.email.email_with_no_target_visible_to_all 이메일을 보낸 사람이거나 관리자 역할이 있는 사람이 아닌 경우 속성을 활성화하여 이메일에 대한 사용자 액세스를 제한합니다.

권한 없는 사용자는 대상 기록이 없는 sys_email_list 테이블의 이메일에 액세스할 수 있습니다. 이 속성은 이메일 항목에 ACL을 적용하는 대신 이메일 보낸 사람과 관리자 역할을 가진 사용자로만 액세스를 제한합니다.

주: 인스턴스와 주고받은 이메일은 sys_email_list 테이블에 표시됩니다. 그러나 오류 및 무시됨 상태로 표시된 수신된 이메일에만 빈 대상 테이블이 있어야 합니다.

추가 정보

속성	설명
속성 이름	*glide.email.email_with_no_target_visible_to_all*
구성 유형	시스템 속성(/sys_properties_list.do)
구성	접근 통제
목적	사용자가 액세스 권한을 부여하지 않은 경우 이메일 클라이언트가 이메일을 표시하지 못하도록 차단합니다.
권장 값	거짓
기본값	예
보안 위험 등급	6.5
기능적 영향	사용자가 관리자가 아니거나 이메일의 발신자가 아닌 경우 대상 테이블이 비어 있는 이메일을 더 이상 볼 수 없습니다.
보안 위험	(보통) 이 속성이 활성화되지 않은 경우 권한 없는 사용자는 target_table 필드가 비어 있는 모든 이메일에 액세스할 수 있습니다.
참조	고급 이메일 속성 https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특정 IP 범위 플러그인에 대한 액세스 제한〔보안 센터 1.3에서 업데이트됨〕

com.snc.ipauthenticator 플러그인을 사용하여 특정 IP 범위에 대한 액세스를 제한합니다. 인스턴스에 대한 공용 액세스를 의도한 게 아니라면 관리자는 할당된 IP 네트워크 블록에 대한 액세스를 제한해야 합니다.

필수 구성요소

이 플러그인은 예로 설정되면 특정 IP 범위에 대한 액세스를 제한합니다. 인스턴스에 대한 공용 액세스를 의도한 게 아니라면 관리자는 할당된 IP 네트워크 블록에 대한 액세스를 제한해야 합니다. IP 주소 액세스 제어(ip_access_list.do)를 통해 IP 주소의 제외 목록(거부) 또는 포함 목록(허용)을 만들 수 있습니다.

이 속성을 설정하기 전에 IP 범위 기반 인증 (com.snc.ipauthenticator) *com.snc.ipauthenticator* 플러그인을 활성화해야 합니다. 자세한 내용은 구성 단계 섹션(아래)을 참조하십시오 IP 범위 기반 인증 .

플러그인 *com.snc.ipauthenticator* 이 활성화되어 있고 테이블 ip_access에 하나 이상의 활성 IP 액세스 정책이 있는지 확인합니다.

추가 정보

속성	설명
플러그인 이름	• com.snc.ipauthenticator • ip_access
구성 유형	시스템 보안 > IP 주소 접근 제어
범주	접근 통제
목적	인스턴스에 액세스할 수 있거나 액세스할 수 없는 IP 주소 범위를 신뢰할 수 있는 도메인 및 신뢰할 수 없는 도메인 목록에 추가합니다.
권장 값	활성
기본값	없음. 이것은 Glide 속성이 아닌 플러그인입니다. 따라서 기본값은 없습니다.
보안 위험 등급	5.3
기능적 영향	고객 거부 IP 범위는 이 정정 항목에 사용됩니다. 고객이 대상 목록을 정의하므로 영향이 없습니다.
보안 위험	(낮음) 인터넷의 대상 인스턴스에 대한 불필요한 노출은 IP 접근 제어 기능을 사용하여 제한해야 합니다.
참조	IP 범위 기반 인증

구성 단계

1. com.snc.ipauthenticator 플러그인이 활성 상태인지 확인합니다.

2. 다음으로 이동 시스템 보안 > **IP** 주소 접근 통제.

3. 새로 만들기를 클릭하여 IP 주소의 제외 목록(거부) 또는 포함 목록(허용)을 만듭니다.

4. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기술 자료 액세스 제한[Security Center 1.3의 새로운 기능]

이 *glide.knowman.block_access_with_no_user_criteria* 속성은 지식 기반 문서에 대한 사용자의 읽기/쓰기 액세스를 제어하는 데 사용됩니다.

추가 정보

속성	설명
구성 이름	*glide.knowman.block_access_with_no_user_criteria*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 9.1 • CVSS 점수: 심각 • 보안 위험 상세 정보: 이 속성을 권장 값인 true로 설정하지 않으면 모든 사용자가 KB를 읽고 기고할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	읽기 가능 또는 참가 가능이 지정되지 않은 경우 지식베이스에 대한 접근을 거부합니다.

CMDB 모델에 대한 권한 제한 [Security Center 1.3 및 1.5에서 업데이트됨]

csm_cmdb_model.customer_visible_flag 시스템 속성을 사용하여 CMDB 모델에 대한 추가 접근 제어로서 제품 모델 테이블의 데이터에 대한 고객 접근을 제한합니다.

csm_cmdb_model.customer_visible_flag 아래 나열된 테이블에 대해 고객에게 표시 필드를 사용하려면 속성을 예로 설정합니다.

- 제품 모델 테이블 [cmdb_model]
- 소프트웨어 모델 테이블 [cmdb_software_product_model]
- 애플리케이션 모델 테이블 [cmdb_application_product_model]
- 소비재 모델 테이블 [cmdb_consumable_product_model]
- 시설 모델 테이블 [cmdb_facility_product_model]
- 하드웨어 모델 테이블 [cmdb_hardware_product_model]

이 속성을 **true** 로 설정하면 기본적으로 모든 cmdb_model 값이 숨겨집니다.

cmdb_model 테이블의 customer_visible 열/속성을 고려하지 않고 sn_esm_user에 액세스할 수 있는 기본 cmdb_model ACL에 의존하려면 속성을 아니오로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*csm_cmdb_model.customer_visible_flag*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	**tue true**로 설정하면 시스템은 고객 표시 필드의 설정을 사용하여 고객 서비스 포털의 제품 모델 데이터에 대한 액세스를 결정합니다.
권장 값	예
기본값	거짓
구성 유형	부울
보안 위험	(보통) sn_esm_user 역할과 바로 사용 가능한 ACL을 가진 모든 사용자는 CMDB 모델에 대한 권한을 가질 수 있습니다. 주: 이 역할은 외부 사용자에게 부여되는 경향이 있습니다. 외부 사용자에게 CMDB 모델에 대한 권한을 마지못해 부여할 수 있습니다.
참조	고객 서비스 포털에서 제품 모델 데이터에 대한 액세스 제한

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

첨부 파일에 인증되지 않은 접근 제한

이 *glide.image_provider.security_enabled* 속성을 사용하여 이미지의 보안 설정을 제어합니다. **true**로 설정하면 인증된 사용자와 권한이 있는 사용자에게만 이미지가 표시됩니다. **false**로 설정하면 첨부 파일에 대한 URL이 있는 모든 사용자에게 이미지가 표시됩니다.

인스턴스의 이미지를 보호하여 중요한 정보 유출을 방지합니다. 인스턴스의 이미지는 `.iix`로 끝나는 URL을 통해 액세스할 수 있습니다.

이러한 URL을 통해 이미지에 액세스하지 못하도록 하려면 **glide.image_provider.security_enabled** 시스템 속성을 **true** 로 설정합니다.

주:

원본 테이블이 다음 중 하나인 경우 첨부 파일 테이블의 이미지에 대해 이 속성이 적용되지 않습니다.

- 문구류 [sysevent_email_style]
- 시작 페이지 섹션 [sys_home]
- 시스템 속성 [sys_properties]

일부 첨부 파일에는 중요한 정보가 포함될 수 있으므로 인증되지 않은 사용자에 대해서는 제한을 적용해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.image_provider.security_enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	*.iix* 형식을 사용하여 렌더링할 때 첨부 파일에 대한 인증되지 않은 액세스를 방지합니다.
권장 값	예
기본값	거짓
기능적 영향	기능에 큰 영향을 미치지 않습니다. 이전에 .iix에 직접 액세스한 사용자는 인증을 거쳐야 하기 때문에 사용자 경험이 약간 영향을 받을 수 있습니다.
보안 위험	(높음) 일부 첨부 파일에 중요한 정보가 포함될 수 있으므로 인증되지 않은 사용자에 대해서는 제한을 적용해야 합니다.
참조	첨부 파일 관리 사용 가능한 시스템 속성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

사용자 지정 저널 항목에 대한 액세스 제한 **[Security Center** 1.3에서 업데이트되고 2.0에서 제거됨〕

이 *glide.live_feed.custom_journal.acl_check_enabled*속성을 사용하여 사용자 지정 저널 필드의 ACL을 적용합니다.

권장 값인 true로 설정되지 않은 경우 *glide.live_feed.custom_journal.acl_check_enabled*모든 사용자가 라이프 피드 기능 내의 모든 저널 항목을 볼 수 있습니다. 속성을 예로 설정하면 사용자 지정 저널 필드의 ACL이 적용되므로 기능이 있으면 좋습니다.

추가 정보

속성	설명
속성 이름	*glide.live_feed.custom_journal.acl_check_enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	ACL을 기반으로 저널 항목을 볼 수 있는 사용자를 제어합니다.
권장 값	예
기본값	예
구성 유형	부울.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	(보통) 예로 설정하면 ACL을 통과하는 사용자 지정 저널 항목만 라이브 피드에 표시되고, 그렇지 않으면 모든 사용자가 모든 저널 항목을 볼 수 있습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

플로우 컨텍스트 읽기 액세스 제한[Security Center 1.5의 새로운 기능]

com.snc.process_flow.reporting.require_flow_access 사용자가 플로우 검사를 읽는 데 추가 액세스 검사가 필요한 경우 속성을 사용하여 적용합니다.

com.snc.process_flow.reporting.require_flow_access 속성이 권장 값인 true로 설정되면 플로우 컨텍스트를 읽으려는 사용자에 대한 추가 액세스 검사가 수행됩니다. 이 속성이 아니오로 설정된 경우 사소한 정보가 공개될 수 있습니다.

추가 정보

속성	설명
구성 이름	*com.snc.process_flow.reporting.require_flow_access*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 2.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 false로 설정하면 기존 동작이 유지됩니다. 이 속성을 true로 설정하면 읽기 액세스의 추가 보안 계층이 적용됩니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성을 사용하면 플로우 컨텍스트 기록을 읽기 위한 보안이 강화됩니다. 이 인스턴스는 플로우 컨텍스트를 읽으려는 사용자에게 상위 플로우에 대한 읽기 권한도 부여하도록 적용합니다.

관리자로의 가장 제한[Security Center 2.0의 새로운 기능]

이 *glide.sys.permissive.impersonate* 속성은 관리자가 아닌 역할이 다른 사용자를 가장하지 못하도록 하는 데 사용할 수 있습니다.

glide.sys.permissive.impersonate 속성이 false로 설정되면 admin 역할이 있는 사용자만 다른 사용자를 가장할 수 있습니다. 이 속성을 true로 설정하면 사용자가 가장 API를 노출하는 애플리케이션 구성 요소를 사용하여 더 높은 권한의 사용자를 가장할 수 있습니다. 관리자가 아닌 사용자는 가장 기능에 액세스할 수 있기 때문에 이러한 애플리케이션 구성요소가 잘못 구성된 경우 무단 액세스가 발생할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관리자가 아닌 사용자가 다른 사용자를 가장할 수 있어야 하는 경우 속성을 기본값이 아닌 값으로 설정할 수 있습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.sys.permissive.impersonate*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 6.7 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값인 아니오로 설정하지 않으면 관리자가 아닌 사용자가 API를 노출하는 애플리케이션 구성 요소를 활용하여 더 높은 권한을 가진 사용자를 가장할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	관리자가 아닌 사용자는 다른 스크립트 및 UI 페이지에 대한 일부 사용자 지정을 통해 가장 기능에 액세스할 수 있습니다. 그러나 올바른 사용자에게만 이러한 기능에 대한 액세스 권한이 부여되도록 하는 것이 중요합니다.

보안 점프 시작 플러그인(ACL 규칙) 사용(보안 센터 1.3에서 업데이트됨)

보안 점프 시작(ACL 규칙)(com.snc.system_security*com.snc.system_security*) 플러그인을 활성화하여 내의 Now Platform일부 주요 시스템 테이블에서 액세스 통제를 확인하는 몇 가지 중요한 ACL을 만듭니다.

이러한 규칙을 사용하면 여러 시스템 테이블의 보안을 더욱 쉽게 확보할 수 있으므로 조직에서 인스턴스를 프로덕션으로 쉽게 전환할 수 있습니다. 보안 점프 시작(ACL 규칙) 플러그인은 모든 새 인스턴스에 자동으로 설치됩니다.

추가 정보

속성	설명
플러그인 ID	*com.snc.system_security*
구성 유형	시스템 정의 > 플러그인
범주	접근 통제
목적	보안 점프 시작(ACL 규칙) 플러그인을 활성화하여 적절한 보안 준수를 달성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	인스턴스의 기본 프로비저닝과 함께 제공되는 각 시스템 테이블을 수동으로 생성하는 대신 애초에 시스템 테이블을 보호하는 몇 가지 기본 ACL을 제공합니다. 이러한 ACL은 새로 생성된 인스턴스를 프로덕션으로 신속하게 이동해야 할 때 유용합니다.
권장 값	활성
기본값	없음. 이는 Glide 속성이 아닌 플러그인이므로 기본값이 없습니다. 플러그인은 zBoot(재설정)에 기본적으로 설치됩니다.
보안 위험 등급	8.1
기능적 영향	인스턴스에 있는 기존 ACL을 감사하지 않고 이 플러그인을 설치하면 기능에 상당한 영향을 미칩니다. 정정이 발생하기 전에 고객 지원 및 정의가 필요합니다.
보안 위험	(높음) 인스턴스에 대한 의도하지 않은 액세스를 잠그려면 접근 제어를 적용해야 합니다. ACL 빠르게 시작하기 규칙은 조직이 보다 쉽고 신속하게 프로덕션에 들어갈 수 있도록 많은 시스템 테이블을 보호하는 시작점을 제공하기 위해 만들어졌습니다.
참조	보안 점프 시작 - ACL 규칙

구성 단계

이 플러그인이 인스턴스에 활성화되어 있지 않으면 지원 센터에 문의하십시오 ServiceNow . 이때 플러그인을 활성화하면 프로덕션 환경에서 이미 사용 중인 테이블에 대한 보안 액세스가 수정될 수 있습니다. 관리자가 플러그인이 제공하는 새로운 ACL 규칙에 관심이 있는 경우, 필요한 경우 기존 인스턴스에 하나 이상의 규칙을 수동으로 생성할 수 있습니다. 이 경우 이 ACL 목록을 지침으로 사용할 수 있습니다.

임포트 세트 **API** 내에서 보안 삽입 다중 작업 사용**[Security Center** 1.3의 새로운 기능)

이 *com.glide.import_set_api.insert_multiple_optimize* 속성을 사용하여 임포트 세트 API 내에서 다중 삽입 작업에 *GlideRecordSecure* 또는 *GlideRecord*를 사용할지 여부를 제어합니다.

com.glide.import_set_api.insert_multiple_optimize 권장 값인 false로 설정된 경우 *GlideRecordSecure*를 사용하여 기록을 삽입하고 테이블 수준 ACL(접근 제어 목록)을 평가합니다. 이 속성을 예로 설정하면 *GlideRecord*가 기록을 삽입하는 데 사용되며 테이블 수준 ACL은 평가되지 않습니다. 또한 임포트 세트 API 삽입 다중 REST 엔드포인트 ACL(sys_id: 3101b770ff2211105cf343d0653bf182)이 활성 상태이고 사용자에게 import_transformer 역할이 있는지 확인해야 합니다.

추가 정보

속성	설명
구성 이름	*com.glide.import_set_api.insert_multiple_optimize*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	거짓
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성이 false로 설정되지 않은 경우 권한이 낮은 사용자가 권한 있는 역할의 범위를 벗어난 테이블에 데이터를 삽입할 수 있습니다.
되돌릴 수 있는 동작	안전한 재정의 및 DB 재정의 없음.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성은 GlideRecord를 사용하여 데이터를 저장함으로써 임포트 세트 API 성능을 최적화합니다. 매개변수가 설정되면 통합 사용자에게 API에 액세스할 수 있는 import_transformer 역할이 필요합니다.
참조	https://developer.servicenow.com/blog.do?p=/post/gliderecord-vs-gliderecordsecure

SOAP 요청 엄격한 보안 적용[Security Center 1.3에서 업데이트됨]

이 *glide.soap.strict_security* 속성을 사용하여 웹 서비스 보안을 적용합니다.

이 속성은 다음의 조합을 사용합니다.

- HTTP 프로토콜을 통한 기본 인증 문제/응답 및
- 의 시스템 수준 액세스 제어.보안 점프 시작 플러그인(ACL 규칙) 사용[보안 센터 1.3에서 업데이트됨]

이 속성을 **true**로 설정하면 다음 작업이 수행됩니다.

- 사용자에게 작업을 수행할 수 있는 적절한 역할이 있는 경우 유효성을 검사할 역할 인증에 대한 수신 SOAP 요청을 확인합니다. CREATE, READ, UPDATE 또는 DELETE 작업을 수행할 때 테이블에 대한 Now Platform SOAP 웹 서비스 호출/요청 중에 발생합니다.
- 테이블에서 SOAP 데이터 형식으로 데이터를 검색하는 동안 시스템 수준 ACL을 확인합니다.
- 테이블 필드에 대해 수행된 CRUD 작업에 대한 필드 수준 ACL을 확인합니다.

ACL 검사는 웹 서비스가 아닌 표준 테이블 API 호출에 대해서만 완료됩니다.

추가 정보

속성	설명
속성 이름	*glide.soap.strict_security*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
기본값	예

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	예
기능적 영향	이렇게 정정하면 인스턴스의 SOAP 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 시스템 수준 액세스 통제를 적용합니다. 현재 이 데이터에 액세스하는 사용자가 있는 경우 ACL 규칙에 따라 데이터에 대한 액세스가 제한/허용됩니다. SOAP 데이터에 액세스할 수 있는 기본 역할에 대해서는 다음 문서를 참조하십시오 SOAP Web Service .
보안 위험	(보통) 수신 SOAP 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다.
참조	인바운드 SOAP에 엄격한 보안 강제 적용 SOAP Web Service

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

필요한 **jms** 연결 팩토리 **[Security Center** 1.3의 새로운 기능 및 **1.5** 및 2.0에서 업데이트됨]

이 *mid.property.jms.command.allowed_factory_names* 속성은 MID 서버에서 사용할 수 있는 JMS(Java 메시징 서비스) 연결 팩토리를 제어합니다.

JMS 활동 또는 작업을 위한 플러그인에 필요한 몇 가지 선별된 팩토리를 위한 것입니다. 추가 공장을 포함하는 것은 공격자가 허용된 공장에서 활용할 수 있는 기능에 의존하는 JDNI 삽입과 같은 취약성에 대한 공격 체인의 단계가 될 수 있습니다. 레버리지 취약성의 가능성을 방지하려면 필요한 채무 불이행을 초과하는 공장을 포함하지 마십시오.

이 보안 위험을 정정하려면 MID 속성에 *mid.property.jms.command.allowed_factory_names*제공된 이름 목록을 검토하십시오. 기본값인 connectionFactory, queueConnectionFactory 및 topicConnectionFactory 이외의 추가 Java 팩토리 이름이 필요한지 확인하십시오.

추가 정보

속성	설명
구성 이름	*mid.property.jms.command.allowed_factory_names*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
기본값	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
권장 값	*connectionFactory*, *queueConnectionFactory*, *topicConnectionFactory*
범주	접근 통제
보안 위험	• 심각도 점수: 4.1 • CVSS 점수: 중간

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	• 보안 위험 상세 정보: MID 서버()*com.glideapp.agent* 플러그인이 활성 상태인 경우 MID 속성에 *mid.property.jms.command.allowed_factory_names*제공된 이름 목록을 검토합니다. 기본값인 connectionFactory, queueConnectionFactory 및 topicConnectionFactory 이외의 추가 팩토리 이름이 필요한지 확인합니다.
의존성 및 필수 구성요소	안 함

역할별로 전역 앱 개발 제한**[Security Center** 2.0의 새로운 기능)

이 *sn_g_app_creator.allow_global* 속성을 사용하면 가이드 애플리케이션 생성자를 사용하여 전역 범위에서 애플리케이션을 생성할 수 있는 사용자를 제어할 수 있습니다.

가 권장 값인 false로 설정된 경우 *sn_g_app_creator.allow_global* 사용자는 전역 범위에서 애플리케이션을 만들 수 있는 *sn_g_app_creator.global* 역할이 필요합니다. 반대로 안전하지 않은 값인 true로 설정하면 기본 sn_g_app_creator.app_creator 역할이 있는 모든 사용자가 전역 애플리케이션을 만들 수 있습니다. 전역 애플리케이션에는 범위 보호가 부족하여 개발자가 특정 범위를 넘어서는 광범위한 기능에 액세스할 수 있습니다. 추가 역할이 있는 사용자로 전역 애플리케이션 개발을 제한하는 것은 최소 권한 원칙을 준수하는 것입니다.

주: 이 속성은 인스턴스에 미리 구성되어 있지 않습니다. 조직의 필요에 따라 이 속성을 수동으로 만들고 구성해야 합니다.

추가 정보

속성	설명
구성 이름	*sn_g_app_creator.allow_global*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	접근 통제
보안 위험	• 심각도 점수: 3.3 • CVSS 점수: 낮음 • 보안 위험 세부 정보: 이 속성을 권장 값으로 설정하지 않으면 s*n_g_app_creator.app_creator* 역할을 가진 모든 사용자가 최소 권한 원칙을 준수하지 않는 전역 애플리케이션을 만들 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	전역 애플리케이션 ACL 및 속성 생성을 확인하도록 API(/api/now/templates)가 개선되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

불필요한 명시적 역할 액세스 제어 조건 검토[Security Center 1.5에서 제거됨]

Explicit Roles 플러그인은 모든 사용자가 내부 자원에 액세스할 수 있는 snc_internal 역할 또는 외부 자원에 액세스할 수 있는 snc_external 역할을 갖도록 명령하는 데 권장됩니다.

이 플러그인을 설치하면 기존의 모든 사용자에게 snc_internal 역할이 할당되고 기존 ACL(접근 제어 목록)이 역할 조건으로 채워집니다. 자동화 논리 또는 인스턴스 관리자의 개입으로 인해 더 엄격한 역할 요구 사항이 이미 포함되어 있는 ACL에 snc_internal 또는 snc_external 역할이 잘못 추가될 수 있습니다. ACL에 매핑된 역할이 포함된 모든 사용자에 대해 ACL 역할 평가가 통과되므로 snc_internal 또는 snc_external의 추가가 ACL의 의도된 목적에 비해 너무 광범위할 수 있습니다. ACL을 통해 권한이 낮은 사용자에게 액세스 권한이 부여되는 경우 데이터 유출이 발생할 수 있습니다.

예를 들어, snc_internal 역할과 관리자 역할을 테이블 내의 동일한 ACL에 매핑할 필요가 없습니다. ACL은 관리자에게 액세스 권한을 부여하기 위한 것으로, 이 경우 snc_internal 역할은 실수입니다. 또는 ACL이 모든 snc_internal 사용자에게 액세스 권한을 부여하기 위한 것이므로 관리자 역할이 필요하지 않습니다. Explicit Roles 플러그인이 설치되면 snc_internal 또는 snc_external에 대한 역할 조건과 다른 역할에 대한 조건도 포함하는 ACL을 검토합니다. 역할이 특정 사용 사례에 작동할 수 있는 경우 발견 사항을 주기적으로 검토해야 합니다.

중요사항: 이 강화 설정은 다음 Security Center v1.5 스토어 패치 릴리스 및 이후 버전에서 제거됩니다. "명시적 역할 ACL 구성 검사 도구 모음"이라는 인스턴스 스캔 도구 모음을 Washington 릴리스에서 사용할 수 있습니다. 이 새로운 Instance Scan의 결과를 검토하는 것이 좋습니다.

SOAP 요청의 게스트 사용자 설정[Security Center 1.3 및 2.0에서 업데이트됨]

이 속성을 구성하여 미인증 SOAP 요청의 접근 수준을 제어합니다.

이 속성은 미인증 SOAP 요청의 액세스 수준을 제어합니다. 권장 값인 *soap.guest*로 설정되지 않았거나 제한된 권한이 있는 사용자로 설정된 경우 SOAP 요청은 사용자를 대신하여 실행됩니다. 이 속성이 비어 있으면 관리자에 대한 인증되지 않은 접근 또는 인스턴스 내의 모든 보안 통제를 무효화하는 유지관리 수준 운영이 활성화됩니다.

추가 정보

속성	설명
구성 이름	*com.glide.soap.guest_user*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	soap.guest
기본값	soap.guest
범주	접근 통제
보안 위험	• 심각도 점수: 8.1 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 공백으로 설정하면 관리자 또는 유지관리 수준 운영에 대한 인증되지 않은 액세스가 가능합니다.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

즐겨찾기에 공개 액세스 사용 안 함**[Security Center 1.3** 및 2.0에서 업데이트됨〕

이 옵션을 *glide.ui.magellan.favorites.allow_public* 사용하여 인증되지 않은 사용자가 네비게이터에서 즐겨찾기 를 볼 수 있는지 여부를 지정합니다.

아니오로 설정된 경우 *glide.ui.magellan.favorites.allow_public* 즐겨찾기에 대한 공개 액세스가 준수됩니다.

추가 정보

속성	설명
속성 이름	*glide.ui.magellan.favorites.allow_public*
구성 유형	시스템 속성(/sys_properties_list.do)
인스턴스 보안 센터에서 구성	예
목적	인증되지 않은 사용자가 네비게이터에서 즐겨찾기 를 볼 수 있는지 여부를 제어합니다.
유형	예/아니요
권장 값	*false*
보안 의존성	**false**로 설정합니다*glide.ui.magellan.favorites.allow_public*.
기능적 영향	(중간) 이 속성을 활성화하면 권한이 없는 사용자에 대한 보호 계층 역할을 합니다.
보안 위험	(중간) 이 속성을 사용하도록 설정하지 않으면 중요한 데이터에 무단으로 액세스할 위험이 있습니다.
참조	즐겨찾기 관리

SNC 액세스 제어 플러그인 사용〔보안 센터 1.3에서 업데이트됨〕

SNC 접근 제어(com.snc.snc_access_control) 플러그인을 활성화하여 직원이 인스턴스에 대한 접근을 통제합니다 고객 서비스 및 지원 .

SNC 접근 제어(com.snc.snc_access_control) 플러그인을 활성화하여 고객 서비스 및 지원 담당자가 사용자의 명시적 허가 없이 인스턴스에 액세스하지 못하게 합니다 ServiceNow . 인스턴스에 대한 모든 액세스가 감사되지만 이 액세스를 제어하는 것이 좋습니다. 이 액세스 방법은 완전히 감사 및 추적이 가능합니다.

> **주:** 제품을 지원하고 관리할 수 있는 기타 공인 ServiceNow 운영 담당자는 기본 인프라에 대한 관리 작업을 수행해야 합니다. 이 플러그인을 사용하도록 설정하면 지원 서비스 수준 및 가용성 SLA에 영향을 줄 수 있습니다. 그런 다음 가용성 SLA는 지원 담당자가 인스턴스에 대한 액세스 권한을 부여받은 시간부터 측정됩니다.

SNC 접근 제어(com.snc.snc_access_control) 플러그인을 활성화하여 명시적 허가 없이 인스턴스에 대한 액세스를 제한합니다. 이 기능에 대한 자세한 내용은 다음 문서를 참조하십시오 ServiceNow 접근 제어. 활성화 정보는 다음을 참조하십시오. 접근 통제 활성화 ServiceNow

추가 정보

속성	설명
플러그인 이름	*com.snc.snc_access_control*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
구성 유형	시스템 정의 > 플러그인
범주	접근 통제
목적	직원이 인스턴스에 액세스하는 것을 금지합니다 고객 서비스 및 지원 .
권장 값	활성
기본값	없음. 이는 Glide 속성이 아닌 플러그인이므로 기본값이 없습니다. 플러그인은 기본적으로 설치되지 않습니다.
필요한 역할	고객 관리자는 이 플러그인을 활성화할 수 없습니다. 플러그인을 활성화하려면 높은 권한이 필요하므로 명시적으로 요청해야 합니다.
보안 위험 등급	3.3
기능적 영향	이 플러그인이 비활성화된 경우 모든 고객 서비스 및 지원 직원이 고객의 인스턴스에 액세스할 수 있습니다. 플러그인을 활성화하면 고객이 인증된 고객 서비스 및 지원 직원으로만 액세스를 제한할 수 있습니다.
보안 위험	(높음) 더 많은 사람들에게 인스턴스 액세스가 불필요하게 노출됩니다.
참조	ServiceNow 접근 제어

구성 단계

1. 플러그인을 요청하려면 다음 접근 통제 활성화 ServiceNow의 단계를 수행합니다. 고객은 HI에서 SNC 접근 제어 플러그인(com.snc.snc_access_control)을 요청해야 합니다.
2. SNC 액세스 제어를 사용하려면 다음 접근 제어 구성 ServiceNow의 단계를 수행합니다. 인스턴스에 로그인할 수 있는 권한을 가진 한 명 이상의 고객 서비스 및 지원 직원을 지정하도록 접근 제어 기록을 구성합니다.

사용자가 **CSRF** 유효성 확인을 바이패스하기 위한 경고를 수락하지 못하도록 방지

사용자가 CSRF 확인을 바이패스하기 위해 경고를 수락하지 못하도록 하여 CSRF(교차 사이트 요청 위조)의 위험을 줄입니다.

CSRF 공격을 허용할 수 있는 CSRF(교차 사이트 요청 위조) 토큰이 재사용되지 않도록 CSRF 토큰 엄격한 확인을 활성화합니다.

CSRF 토큰 엄격한 확인을 사용하려면 **glide.security.csrf.strict.validation.mode** 시스템 속성 값을 예 로 설정합니다. 이 속성이 시스템 속성 [sys_properties] 테이블에 없는 경우 기본값은 Xanadu부터 **true** 입니다.

추가 정보

속성	설명
기술 구성 이름	glide.security.csrf.strict.validation.mode
플러그인 적용 가능성	안 함
보안 위험	교차 사이트 요청 위조는 인스턴스 데이터의 무결성을 침해하는 중대한 보안 위험입니다. 공격자는 인스턴스 사용자의 신뢰를 악용하여 모든 인스턴스 사용자에 대해 CSRF 공격을 시작할 수

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	있습니다. 소셜 엔지니어링 공격을 통해 사용자는 공격자 대신 인스턴스에 잘못된 형식의 요청을 제출할 수 있습니다.
CVSS(공통 취약성 평가 시스템) 점수	3.7
CVSS(공통 취약성 평가 시스템) 등급	낮음
기능적 영향	이렇게 정정하면 사용자가 인스턴스에 쓰기 요청을 제출하기 전에 추가 확인 단계가 활성화됩니다. 현재 CSRF 토큰이 이전에 사용되었는지 여부를 확인합니다. 있는 경우 추가 쓰기 요청이 제출되지 않습니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	예
폴백 값	예
권장 값	예

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

다른 사용자로 가장이 애플리케이션 데이터를 볼 수 없도록 방지

시스템 속성을 사용하여 다른 사용자로 전환한 사용자가 애플리케이션 데이터를 볼 수 없도록 합니다.

계정을 가장할 때 관리자 수준이 해당 사용자에게 속한 애플리케이션 특정 데이터에 액세스하지 못하도록 합니다. 이 권한은 애플리케이션과 관련된 시스템 속성을 만들어 애플리케이션 수준에서 설정할 수 있습니다.

이러한 시스템 속성은 **<scope>.impersonateCheck** 명명 형식을 사용합니다(예: **sn_hr_core.impersonateCheck**). true 값을 사용하여 시스템 속성을 생성하여 사용자가 계정을 가장할 때 다른 사용자에게 속한 애플리케이션 관련 데이터에 액세스하지 못하도록 합니다.

주: 일부 애플리케이션은 이 구성에서 작동하도록 설계되었거나 이 목적을 위한 시스템 속성 [sys_properties] 기록이 없습니다. 다음 범위가 이 속성과 함께 작동하도록 구성됩니다.

- sn_opp_market
- sn_jny
- sn_imt_vaccine
- sn_imt_health_test
- sn_hr_core
- sn_egd_goals
- sn_egd_core
- sn_egd_act

추가 정보

속성	설명
기술 구성 이름	<scope>.impersonateCheck

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
플러그인 적용 가능성	안 함
보안 위험	이러한 속성 값이 **False** 이면 관리자 수준 사용자가 다른 사용자를 가장하고 가장한 사용자의 액세스 권한으로 애플리케이션 데이터에 액세스할 수 있습니다. 이는 바람직하지 않거나 특정 애플리케이션 컨텍스트에서 무단 데이터 액세스를 허용할 수 있습니다.
CVSS(공통 취약성 평가 시스템) 점수	4.4
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	관리자 수준 사용자는 다른 사용자를 가장하여 특정 애플리케이션 컨텍스트에서 해당 사용자의 데이터를 볼 수 없습니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	거짓
폴백 값	거짓
권장 값	예

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

API 및 웹 서비스

API 및 웹 서비스 범주는 애플리케이션이 적절한 인증, 권한 부여 및 세션 관리를 수행하고, 신뢰 경계를 트래버스하는 모든 입력의 유효성을 검사하고, 모든 API 유형에 대한 보안 제어를 포함하는지 확인합니다.

이 범주의 특정 통제는 SOAP 웹 서비스에 대한 XDS 스키마 유효성 검사 또는 graphQL API에 대한 서비스 거부 보호와 같은 서비스 유형별 입력 유효성 검사를 처리합니다.

SOAP 콘텐츠 형식 확인[Security Center 1.3에서 업데이트됨]

이 *glide.soap.require_content_type_xml* 속성을 사용하여 콘텐츠 유형을 text/xml로 확인하고 잘못된 SOAP 요청으로부터 보호할 수 있습니다.

- **true**로 설정하면 콘텐츠 Now Platform 형식이 text/xml로 확인되고 잘못된 SOAP 요청으로부터 보호됩니다.
- **false**로 설정하면 모든 content-type 값이 허용됩니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.soap.require_content_type_xml*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
범주	API 및 웹 서비스
목적	잘못된 SOAP 요청으로부터 보호
권장 값	예
기본값	예
보안 위험 등급	8.8
기능적 영향	이렇게 정정하면 모든 인바운드 SOAP 요청에 대해 SOAP 콘텐츠 유형을 확인할 수 있습니다. • 인바운드 요청에 text/xml 이외의 콘텐츠 유형을 사용하는 경우 SOAP 트랜잭션이 실패할 수 있습니다. • 올바른 MIME 유형을 사용하지 않는 경우 타사 통합이 중단될 수 있습니다.
보안 위험	(보통) 인바운드 SOAP 요청을 수락할 때 적절한 유효성 검사가 수행되어 관련 콘텐츠 형식이 요청의 일부로 정의되고 있는지 확인합니다. 보안 위험으로 볼 수 있는 잘못된 SOAP 응답을 제한합니다.
참조	컨텐츠 유형

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

PDF 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]

이 *glide.basicauth.required.pdf* 속성을 사용하여 수신하는 PDF 요청에 기본 인증을 요구해야 하는지 여부를 지정합니다.

속성이 *glide.basicauth.required.pdf* sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.pdf*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	PDF 요청에 기본 인증을 적용합니다.
권장 값	예
기본값	예
보안 위험 등급	7.5
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	• 인스턴스의 PDF 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다. 자세한 내용은 웹 서비스 가져오기 집합을 참조하십시오.
보안 위험	(높음) 수신 PDF 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

이벤트 관리 **HTTP** 프로세서에서 인증 필요**[Security Center** 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨〕

이벤트 관리 플러그인()*com.glideapp.itom.snac*이 활성화된 경우 인바운드 Amazon Simple Notification Service(SNS) 요청에 대해 안전한 기본 인증을 설정하는 방법에 대해 알아봅니다.

*glide.basicauth.required.evtmgmthttpprocessor*속성이 권장 값인 **true**로 설정되지 않고 이벤트 관리 플러그인()*com.glideapp.itom.snac*이 활성 상태인 경우 모든 인바운드 Amazon Simple Notification Service(SNS) 요청에 기본 인증이 필요하지 않습니다. 이로 인해 인스턴스 데이터에 대한 인증되지 않은 액세스가 발생할 수 있습니다.

이 보안 위험을 정정하려면**true***glide.basicauth.required.evtmgmthttpprocessor*로 설정되고 *com.glideapp.itom.snac* 활성 상태인지 확인합니다.

추가 정보

속성	설명
구성 이름	*glide.basicauth.required.evtmgmthttpprocessor*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	API 및 웹 서비스
보안 위험	• 심각도 점수: 7 • CVSS 점수: 높음 • 보안 위험 상세 정보: 권장 값인 true로 설정하지*glide.basicauth.required.evtmgmthttpprocessor* 않고 플러그인을 활성화 *com.glideapp.itom.snac* 하지 않으면 인바운드 SNS 요청에 대해 기본 인증이 활성화되지 않습니다. 이로 인해 인스턴스 데이터에 대한 인증되지 않은 액세스가 발생할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
의존성 및 필수 구성요소	안 함
참조	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • 접근 통제
기능적 영향	*glide.basicauth.required.evtmgmthttpprocessor* 권장 값인 True로 설정되지 않고 이벤트 관리 플러그인(com.glideapp.itom.snac)이 활성 상태인 경우 모든 인바운드 Amazon 웹 서비스 SNS 요청에 기본 인증이 필요하지 않습니다. 이로 인해 인스턴스 데이터에 대한 인증되지 않은 액세스가 발생할 수 있습니다.

SOAP 요청에 대해 권한 부여 필요 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]

이 *glide.basicauth.required.soap* 속성을 사용하여 수신하는 SOAP 요청에 기본 권한을 부여해야 하는지 여부를 지정합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.soapglide.soap.require_ws_securi*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	SOAP 요청 권한 부여를 적용하기 위해
권장 값	예
보안 위험 등급	8.1
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다. • 인스턴스의 SOAP 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. • 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 통제 권한이 있는 계정을 생성합니다. 자세한 내용은 SOAP 웹 서비스 및 MID 서버 인증 자격 증명과 SOAP 요청을 참조하십시오.
보안 위험	(중간) SOAP 요청 데이터 소스에 적절한 권한이 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
참조	Authentication

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

언로드 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]

(useUnloadFormat) 속성을 사용하여 수신되는 *glide.basicauth.required.unl* 언로드 요청에 기본 인증이 필요한지 여부를 지정합니다.

추가 정보

속성	설명
속성 이름	*glide.basicauth.required.unl*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	언로드 요청에 기본 인증을 적용하기 위해
권장 값	예
보안 위험 등급	7.5
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다. 인스턴스에서 데이터를 언로드하는 형태로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다.
보안 위험	(높음) 데이터 소스 언로드 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다. sys_properties_table *glide.basicauth.required.unl* 에 있고 true로 설정되어 있는지 확인합니다.
참조	Authentication

csv 요청에 대해 권한 부여 필요[Security Center 1.3에서 업데이트됨]

glide.basicauth.required.csv 이 속성을 사용하여 수신되는 CSV(쉼표로 구분된 값) 요청에 기본 인증이 필요한지를 지정합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.csv*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	CSV 요청에 기본 인증을 적용하기 위해.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	예
보안 위험 등급	7.5
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다. • 인스턴스의 CSV 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다. 자세한 내용은 CSV 형식의 파일에서 데이터 검색을 참조하세요.
보안 위험	(높음) 수신 CSV 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 콘텐츠 및 데이터에 액세스할 수 있습니다. sys_properties *glide.basicauth.required.csv* 테이블에 있고 true로 설정되어 있는지 확인합니다.
참조	웹 서비스 보안

Excel 요청에 대해 권한 부여 필요 **[Security Center** 1.3에서 업데이트됨〕

이 *glide.basicauth.required.excel* 속성을 사용하여 수신하는 Excel 요청에 기본 인증을 요구해야 하는지 여부를 지정합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.excel*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	Excel 요청에 기본 인증을 적용합니다.
권장 값	예
보안 위험 등급	7.5
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	• 인스턴스의 Excel 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다.
보안 위험	(높음) 수신 Excel 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 콘텐츠/데이터에 액세스할 수 있습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

임포트 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]

이 *glide.basicauth.required.importprocessor* 속성을 사용하여 수신하는 임포트 요청에 기본 인증을 요구해야 하는지 여부를 지정합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.importprocessor*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	임포트 요청에 기본 인증을 적용하기 위해
권장 값	예
보안 위험 등급	5.3
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다. • 데이터 소스를 인스턴스 테이블/페이지로 임포트하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다. 자세한 내용은 CSV 형식의 파일에서 데이터 검색을 참조하세요.
보안 위험	(보통) 데이터 소스 임포트 요청에 적절한 권한이 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다.
참조	SOAP 웹 서비스 보안 SOAP 웹 서비스

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

JSONv2 요청에 대해 권한 부여 필요[Security Center 1.3에서 업데이트됨]

이 *glide.basicauth.required.jsonv2* 속성을 사용하여 수신하는 JSONv2 요청에 기본 권한을 부여해야 하는지 여부를 지정합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.jsonv2*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	JSONv2 요청 권한 부여를 적용하기 위해.
보안 위험 등급	7.5
권장 값	예
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다. • 인스턴스의 JSON 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. • 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 통제 권한이 있는 계정을 생성합니다. 자세한 내용은 JSONv2 웹 서비스 JSONv2 웹 서비스를 참조하세요.
보안 위험	(높음) 데이터 소스 JSON 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다.
참조	Authentication 수신 JSONv2 요청에 대해 기본 인증 요구

WSDL 요청에 대해 인증 필요 [Security Center 1.3 및 1.5에서 업데이트됨]

glide.basicauth.required.wsdl 이 속성을 사용하여 수신하는 WSDL(Web Services Description Language) 요청에 기본 인증을 요구해야 하는지 여부를 지정합니다.

glide.basicauth.required.wsdl 이 권장 값인 예로 설정되지 않은 경우 WSDL 요청에 대한 기본 인증이 비활성화됩니다. WSDL은 인스턴스 테이블 스키마와 같은 웹 서비스를 설명하는 데 사용되는 프로토콜이며 테이블 내에서 데이터를 공유하기 위한 메커니즘이 아닙니다. 이 속성을 예로 설정하면 미인증 사용자에게 테이블 스키마를 공개할 수 있습니다.

ⓘ 주: 들어오는 WSDL 요청에 대해 기본 인증을 요구하지 않기로 할 경우 접근 제어(ACL) 규칙을 수정하여 게스트 사용자도 WSDL 컨텐츠를 이용할 수 있게 해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.wsdl*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	WSDL 요청에 기본 인증을 적용하기 위해
권장 값	예
보안 위험 등급	5.3
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다. • 인스턴스의 WSDL 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다.
보안 위험	(중간) WSDL 웹 서비스에 적절한 권한이 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 WSDL 컨텐츠/데이터에 액세스할 수 있습니다.
참조	웹 서비스 보안

XML 요청에 대해 권한 부여 필요[Security Center 1.3에서 업데이트됨]

glide.basicauth.required.xml 이 속성을 사용하여 수신하는 XML 요청에 기본 인증을 요구해야 하는지 여부를 지정합니다.

추가 정보

경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.xml*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	XML 요청에 기본 인증을 적용하기 위해
보안 위험 등급	7.5
권장 값	예
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	• 인스턴스의 XML 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다. 자세한 내용은 XML 파서 단계를 참조하십시오.
보안 위험	(높음) 수신 XML 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다.
참조	Authentication

XML 출력 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]

모든 인바운드 XMLOutputProcessor 요청에 기본 권한 부여가 필요하도록 이 특성을 구성하십시오.

glide.basicauth.required.xmloutputprocessor 특성이 권장 값인 **true**로 설정되지 않은 경우, 인바운드 XMLOutputProcessor 요청에 기본 인증이 필요하지 않으므로 인스턴스에서 인증되지 않은 정보 공개가 발생할 수 있습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.basicauth.required.xmloutputprocessor*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	API 및 웹 서비스
보안 위험	• 심각도 점수: 7.5 • CVSS 점수: 높음 • 보안 위험 상세 정보: 속성을 권장 값인 예 로 설정하지 않으면 인스턴스에서 중요한 정보가 유출될 수 있습니다.
의존성 및 필수 구성요소	안 함

XSD 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]

*glide.basicauth.required.xsd*이 속성을 사용하여 수신하는 XSD(XML 스키마 정의) 요청에 기본 인증을 요구해야 하는지 여부를 지정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성이 *glide.basicauth.required.xsd*sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	glide.basicauth.required.xsd*glide.basicauth.required.xsd*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	XSD 요청에 기본 인증을 적용하기 위해
권장 값	예
보안 위험 등급	5.3
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다. • 인스턴스의 XSD 데이터 형식으로 테이블/페이지에서 데이터를 검색하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다. 자세한 내용은 비대화형 세션을 참조하세요.
보안 위험	(보통) 수신 XSD 요청에 적절한 권한 부여가 구성되지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스할 수 있습니다.
참조	Authentication

스크립트 요청에 대해 인증 필요 **[Security Center** 1.3에서 업데이트됨〕

이 *glide.basicauth.required.scriptedprocessor*속성을 사용하여 수신하는 스크립트 요청에 기본 인증을 요구해야 하는지 여부를 지정합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.scriptedprocessor*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	스크립트 요청에 기본 인증을 적용하기 위해

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	예
보안 위험 등급	7.2
기능적 영향	이렇게 정정하면 기본 인증의 형태로 인증을 적용합니다. • 인스턴스에서 스크립트 요청을 처리하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다.
보안 위험	(높음) 수신 스크립트 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 컨텐츠/데이터에 액세스합니다.
참조	Authentication

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

SCHEMA 요청에 대해 권한 부여 필요 **[Security Center** 1.3에서 업데이트됨]

이 *glide.basicauth.required.schema* 속성을 사용하여 모든 인바운드 테이블 스키마 프로세서 요청에 대해 기본 인증을 요구합니다.

인바운드 테이블 Schebma 프로세서는 플랫폼에 대해 들어오는 스키마 요청을 처리합니다.

모든 인바운드 테이블 스키마 프로세서 요청에 대해 기본 인증을 요구하려면 권장 값인 **true**로 설정합니다*glide.basicauth.required.schema*. 모든 인바운드 테이블 스키마 프로세서 요청에 대해 기본 인증을 요구하지 않으려면 값을 **false** 로 설정합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.basicauth.required.schema*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	모든 인바운드 테이블 스키마 프로세서 요청에 대해 기본 권한 부여를 요구합니다.
권장 값	True(기본값)입니다.
구성 유형	부울
보안 위험	(보통) 이 프로세서에서 인증을 생략하면 인스턴스 데이터에 대한 인증되지 않은 액세스가 발생할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

RSS 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]

glide.basicauth.required.rss 이 속성을 사용하여 수신하는 RSS 요청에 기본 인증이 필요한지를 지정합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*glide.basicauth.required.rss*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	RSS 요청에 기본 인증을 적용하기 위해
권장 값	예
보안 위험 등급	7.5
기능적 영향	이렇게 정정하면 기본 인증과 시스템 수준 접근 통제의 형태로 인증 방법의 조합을 적용합니다. • 인스턴스에서 RSS 요청을 처리하는 동안 이 인증을 수행합니다. • 현재 이 데이터에 액세스하는 게스트 사용자를 제한합니다. 해당하는 경우 이 콘텐츠에 액세스해야 하는 사용자를 위해 필요한 액세스 제어 권한을 사용하여 새 계정을 만들어야 할 수 있습니다. 자세한 내용은 RSS 피드 생성기 를 참조하세요.
보안 위험	(높음) 수신 RSS 요청에 적절한 권한 부여가 구성되어 있지 않으면 권한 없는 사용자가 대상 인스턴스의 중요한 콘텐츠/데이터에 액세스할 수 있습니다.
참조	RSS 기본 인증

API 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]

이 *glide.basicauth.required.api* 속성을 사용하여 수신 REST 요청에 대한 기본 인증에 대한 보안을 강화합니다.

glide.basicauth.required.api 모든 REST 요청에 대해 인증을 요구하려면 속성을 예로 설정합니다. 모든 REST 요청에 대한 권한 부여를 바이패스하려면 속성을 **false** 로 설정합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.basicauth.required.api*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
구성 유형	시스템 속성(/sys_properties_list.do)
범주	API 및 웹 서비스
목적	수신 REST 요청에 대한 기본 권한 부여.
권장 값	True(기본값)
구성 유형	문자열
보안 위험	(높음) "glide.basicauth.required.api"가 권장 값인 "예"로 설정되지 않은 경우 API 요청에서 기본 인증이 비활성화되고 인스턴스 데이터에 대한 미인증 액세스로 이어질 수 있습니다.
보안 위험 등급	8.6

아키텍처, 설계 및 위협 모델링

이 광범위한 제어는 보안 응용 프로그램을 구현하기 위한 높은 수준의 디자인 고려 사항과 핵심 요소를 다룹니다. 여기에는 가용성, 기밀성, 처리 무결성, 부인 방지 및 개인 정보 보호의 테넌트가 포함됩니다. 또한 보안 소프트웨어 개발 수명 주기의 요소가 포함됩니다.

인증서 기반 인증이 적용되지 않음 **[Security Center** 1.3의 새로운 기능**]**

이 *glide.authenticate.mutual.enabled*속성을 사용하면 에서 REST 및 SOAP API에 대한 인바운드 REST 연결에 대한 상호 인증 유형인 인증서 기반 인증을 사용할 수 Now Platform있습니다.

상호 인증은 신뢰할 수 있는 인증 기관을 통해 인증서의 유효성을 검사하기 위해 SSL(Secure Socket Layer) 인증서를 교환하여 서버와 클라이언트 간에 신뢰를 설정합니다. 이를 통해 신뢰할 수 있는 소스가 에 연결되어 있는지 확인할 수 있습니다 Now Platform. 이 인스턴스가 권장 값인 true로 설정되지 않은 경우 인스턴스가 MitM(메시지 가로채기) 공격에 취약할 수 있습니다.

이 보안 위협을 해결하려면 인바운드 웹 서비스에 대해 상호 인증을 활성화합니다. 인증서 기반 인증 플러그인(*com.glide.auth.mutual)* 의 경우 Now Platform)을 처음 설치하는 경우 지침을 따릅니다 인증서 기반 인증 설정 . 또한 *glide.authenticate.mutual.enabled*플러그인을 활성화하려면 속성을 true로 설정해야 합니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.mutual.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	아키텍처, 설계 및 위협 모델링
보안 위험	• 심각도 점수: 5.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성이 권장 값인 예로 설정되지 않은 경우 인증서 기반 인증은 신뢰할 수 있는 인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	기관을 통해 인증서를 확인하지 않습니다. 이렇게 하면 악의적인 액터가 MitM 공격을 사용하여 인스턴스를 공격할 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함
참조	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • 인증서 기반 인증 • 상호 인증 구성

HR 앱에서 ACL 평가에 대한 가장 확인[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]

이 *sn_hr_core.impersonateCheck* 속성을 사용하여 사용자가 다른 사용자를 가장하고 HR 정보에 액세스하지 못하도록 합니다.

보안 설정은 가장을 사용하는 동안 관리자가 다른 사용자의 HR 정보를 볼 수 없도록 합니다. 이 속성의 안전하지 않은 설정을 사용하면 관리자가 사용자를 가장하고 가장한 사용자의 액세스 권한으로 설문 조사 결과 또는 감사 기록과 같은 HR 데이터에 액세스할 수 있습니다. 이메일처럼 사용자 자신만 사용할 수 있는 정보와 같은 이러한 유형의 데이터는 특성상 권장되지 않습니다. 예로 설정하면 *sn_hr_core.impersonateCheck* 사용자가 다른 사람을 가장하지 않을 때만 HR 정보에 액세스할 수 있습니다.

추가 정보

속성	설명
구성 이름	*sn_hr_core.impersonateCheck*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	아키텍처, 설계 및 위협 모델링
보안 위험	• 심각도 점수: 2.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성의 안전하지 않은 설정을 사용하면 관리자가 사용자를 가장하고 가장한 사용자의 액세스 권한으로 설문 조사 결과 또는 감사 기록과 같은 HR 데이터에 액세스할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성을 예로 설정하면 가장을 사용하는 동안 관리자가 다른 사용자의 HR 정보를 볼 수 없도록 합니다. false로 설정하면 관리자가 사용자를 가장하고 가장한 사용자의 액세스 권한으로 설문 조사 결과 또는 감사 기록과 같은 HR

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	데이터에 액세스할 수 있습니다. 이메일처럼 사용자 자신만 사용할 수 있는 정보와 같은 이러한 유형의 데이터는 특성상 권장되지 않습니다. sn_hr_core.impersonateCheck를 true로 설정하면 사용자가 다른 사람을 가장하지 않을 때만 HR 정보에 액세스할 수 있습니다.

1회 사용자 인증(SSO)이 활성화된 사용자에 대해 로컬 로그인 사용 안 함

1회 사용자 인증(SSO)이 활성화된 사용자에 대해 로컬 로그인을 사용하지 않도록 사용자 기록을 업데이트합니다.

SSO 인증을 사용하도록 구성된 사용자는 사용자 [sys_user] 기록의 **user_password** 필드에 저장된 로컬 자격 증명을 사용하여 인스턴스 또는 인스턴스의 일부에 계속 액세스할 수 있습니다. 이 액세스는 대화형 액세스와 비대화형 액세스 모두에 적용됩니다. SSO로 구성된 사용자가 로컬 자격 증명을 사용하지 못하도록 하여 악의적인 사용자가 유효한 로컬 로그인 자격 증명을 도난당해 사용할 가능성을 줄일 수 있습니다.

SSO가 활성화된 인스턴스에서 로컬 로그인이 여전히 활성화된 계정을 식별하고 주소를 지정하는 방법에 대한 지침은 Now Support 지식베이스 문서 KB1649420 검토하십시오.

추가 정보

속성	설명
보안 위험	로컬 자격 증명을 사용하는 사용자는 유효한 로컬 로그인 자격 증명을 도난당하여 악의적인 사용자가 사용할 수 있는 위험을 만들 수 있습니다.
CVSS(공통 취약성 평가 시스템) 점수	5.9
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	SSO 구성 사용자는 로컬 자격 증명으로 로그인할 수 있습니다.
의존성 및 필수 구성요소	1회 사용자 인증(SSO)을 활성화해야 합니다(**glide.authenticate.multisso.enabled** 시스템 속성이 예로 설정됨).
데이터 유형	해당 사항 없음
기본 시스템 값	해당 사항 없음
폴백 값	해당 사항 없음
권장 값	해당 사항 없음

인증되지 않은 게시된 보고서 사용 안 함**[Security Center** 2.0에서 업데이트됨)

사용자가 보고서를 게시하거나 액세스할 수 없도록 하려면 이 속성을 비활성화합니다. 이 속성은 보고에서 게시된 보고서 기능을 비활성화합니다.

를 *glide.report.published_reports.enabled***true**로 설정하여 보고서 게시를 활성화합니다.

Glide 속성이 *glide.report.published_reports.enabled*존재하고 false 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.report.published_reports.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	아키텍처, 설계 및 위협 모델링
목적	보고에서 게시된 보고서 기능을 비활성화합니다.
유형	예 | 아니요
권장 값	**false**
보안 위험 등급	6.5
기능적 영향	사용자가 보고서를 게시할 수 없습니다.
보안 위험	(보통) 이 속성을 사용하지 않으면 사용자가 중요한 데이터를 노출하는 보고서에 액세스하거나 이를 게시할 수 있습니다. 보고서를 게시하면 사용자가 아닌 사용자를 포함하여 모든 사용자가 보고서에 액세스하는 데 사용할 수 있는 URL이 생성됩니다. 누군가 URL로 이동하면 인스턴스의 현재 데이터를 사용하여 보고서가 생성됩니다.
참조	보고서 게시

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

인바운드 쿼리 요청에 필드 **ACL** 강제 적용

인스턴스에서 수신 쿼리의 유효성을 검사하는 방법을 관리합니다.

*glide.report.report_view.check_published*이 속성을 사용하여 인스턴스에서 수신 쿼리의 유효성을 검사하는 방법을 확인합니다. 속성이 권장 값인 예로 설정된 경우 수신 쿼리에 대해 필드 ACL을 확인하고 사용자가 승인되지 않은 경우 거부됩니다. 속성이 **false**로 설정되면 수신 쿼리에 대해 ACL이 검사되지 않고 계속 실행되므로 권한이 없는 당사자에게 정보가 공개될 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.export.query.enforce_field_acl*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	아키텍처, 설계 및 위협 모델링

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 4.4 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 **false**로 설정하면 수신 쿼리에 대해 ACL이 검사되지 않으므로 정보 공개로 이어질 수 있습니다.
의존성 및 필수 구성요소	안 함

보고서 보기에 읽기 **ACL** 강제 적용

인스턴스에 읽기 ACL이 적용되는 방법을 관리합니다.

glide.report.report_view.read_acl 테이블 또는 필드에 보고서 뷰 ACL이 없는 경우 속성을 사용하여 보고 기능에 대한 읽기 ACL(테이블 수준)을 적용합니다. 이 속성을 적용하도록 설정하지 않으면 ACL을 바이패스하여 중요한 정보가 유출될 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.report.report_view.read_acl*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	적용
기본값	적용
범주	아키텍처, 설계 및 위협 모델링
보안 위험	• 심각도 점수: 7.1 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 적용 하도록 설정하지 않으면 ACL이 바이패스될 수 있습니다.
의존성 및 필수 구성요소	안 함

허용된 **ServiceNow** 내부 **IP** 주소 정의 **[Security Center 1.3** 및 **1.5**에서 업데이트됨]

이 *glide.ip.authenticate.strict* 속성을 사용하여 인스턴스에서 인바운드 연결을 만들 수 있는 IP 범위를 지정합니다.

glide.ip.authenticate.strict 및 **glide.ip.authenticate.allow.secured** 시스템 속성을 사용하여 광범위한 사용자 그룹에 대한 인스턴스 액세스의 불필요한 노출을 방지합니다.

glide.ip.authenticate.strict 시스템 속성이 예로 설정되면 내부 ServiceNow 직원과 시스템은 필수 IP 범위에서 인스턴스에 대한 인바운드 연결만 만들 수 있습니다. 이렇게 하면 인스턴스의 필수 내부 인프라에 대한 가시성이 제한 ServiceNow되고, 지원 및 영업 직원과 같은 광범위한 ServiceNow 직원이 회사 네트워크를 통해 액세스할 수 없게 됩니다. **glide.ip.authenticate.allow.secured** 시스템 속성은 일반 인증된 액세스 및 인증되지 않은 진단 페이지를 포함하여 내부 ServiceNow 인바운드 연결을 허용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예로 설정되지 않은 경우 **glide.ip.authenticate.allow** 속성에 정의된 더 ServiceNow 광범위한 내부 IP 범위가 이러한 내부 ServiceNow 인바운드 연결을 부여하는 데 사용됩니다.

glide.ip.authenticate.allow.secured 시스템 속성에 신뢰할 수 있는 값만 포함되어 있고 **glide.ip.authenticate.strict** 속성이 예로 설정되어 있는지 확인합니다.

⚠ 경고: 이 속성의 값은 DB 재정의가 없습니다. 변경하거나 재정의할 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.ip.authenticate.strict*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	아키텍처, 설계 및 위협 모델링
목적	ServiceNow 직원이 보안 IP 범위 세트를 통해서만 인스턴스에 액세스할 수 있도록 허용합니다.
권장 값	예
보안 위험 등급	4.3
기능적 영향	(낮음) 이 속성을 활성화하지 않으면 ServiceNow 직원은 모든 IP 범위를 통해 고객의 인스턴스에 액세스할 수 있습니다. 속성을 사용하도록 설정하면 보안 IP 범위 집합(보안 VPN, DC)에 대한 액세스가 제한됩니다. ⓘ 주: 이 속성을 #Now Platform로 설정하면 인스턴스에 액세스할 수 있는 IP 범위 세트에 대해 성능 모니터링 IP 제한 ()*glide.ip.authenticate.allow.secured* 속성 대신 더 제한 *glide.ip.authenticate.allow.secured*적인 속성을 사용합니다.
보안 위험	(낮음) 더 많은 사람들에게 인스턴스 액세스가 불필요하게 노출됩니다.
참조	IP 범위 기반 인증

ⓘ 주: IP 액세스 제어에 추가되지 않은 IP로부터의 액세스를 제한하려면 모두 거부 규칙을 IP 액세스 제어에 추가해야 합니다. 그런 다음 필요한 모든 허용 IP를 IP 액세스 제어에 추가해야 합니다.

레거시 **JQuery** 동작 사용 안 함(보안 센터 1.3에서 업데이트됨)

이 *glide.jquery.legacy*방법은 사전 패치된 이전 JQuery 버전이 사용되지 않도록 하여 라이브러리에 패치되지 않은 취약점을 도입하는 데 사용됩니다.

라이브러리에 패치되지 않은 취약점을 발생시키는 사전 패치된 이전 JQuery 버전이 사용되지 않도록 하려면 권장 값인 **false**로 설정합니다*glide.jquery.legacy*. 사전 패치된 JQuery 버전을 허용하려면 값을 **true** 로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.jquery.legacy*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	아키텍처, 설계 및 위협 모델링
목적	오래된 JQuery 라이브러리 버전에서 발견된 취약성에 대한 공격으로 인해 발생할 수 있는 잠재적인 보안 위험을 방지합니다.
권장 값	아니요
구성 유형	부울
보안 위험	(높음) 라이브러리에 패치되지 않은 취약점을 발생시키는 사전 패치된 이전 JQuery 버전이 사용되지 않도록 합니다. 시스템 속성은 모든 조직이 패치되지 않은 AngularJS 버전에 의존하여 사용자 지정 구현을 실행하는 경우 안전 장치입니다.
보안 위험 등급	7.1

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

GlideRecord 범위 펜싱 레거시 동작 사용 안 함**[Security Center** 1.3의 새로운 기능 및 **1.5** 및 2.0에서 업데이트됨〕

이 *glide.record.legacy_cross_scope_access_policy_in_script* 속성은 범위가 지정된 앱이 전역 스크립트 인터페이스에 액세스할 수 있도록 범위 펜싱을 비활성화합니다. 이는 GlideRecord의 교차 범위 접근에 대한 패치로 만들어졌습니다.

GlideRecord는 해당 액세스 수준으로 구성되지 않은 테이블에 대한 교차 범위 생성/업데이트 액세스 권한을 제공했습니다. 이 범위가 지정된 액세스 동작에 패치가 적용되었을 때 고객이 응용 프로그램이 중단되는 것을 방지하기 위해 속성이 *glide.record.legacy_cross_scope_access_policy_in_script* 작성되었습니다. 예일 때는 교차 범위 액세스가 레거시 동작(안전하지 않음)으로 대체됩니다. 이 속성은 범위 펜싱을 비활성화하여 범위가 지정된 앱이 전역 스크립트 인터페이스에 액세스할 수 있도록 허용합니다.

범위 펜싱 제한을 시행하는 것이 가장 좋습니다. 범위 지정은 애플리케이션이 최소 권한 원칙에 따라 명시적 액세스 권한이 있거나 범위 내에 있는 자원에만 액세스할 수 있도록 합니다. 이 기능을 비활성화하면 기밀성, 가용성 및 무결성에 영향을 미칠 수 있습니다.

Glide 속성을 *glide.record.legacy_cross_scope_access_policy_in_script* false로 설정합니다. sys_properties 테이블에 없는 경우 기본값은 true입니다.

추가 정보

속성	설명
구성 이름	*glide.record.legacy_cross_scope_access_policy_in_script*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기본값	true(속성이 sys_properties 테이블에 없는 경우)
범주	아키텍처, 설계 및 위협 모델링
보안 위험	• 심각도 점수: 5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 범위 지정은 애플리케이션이 최소 권한 원칙에 따라 명시적 액세스 권한이 있거나 범위 내에서만 리소스에 액세스할 수 있도록 합니다. 이 기능을 비활성화하면 기밀성, 가용성 및 무결성에 영향을 미칠 수 있습니다.
의존성 및 필수 구성요소	안 함

레거시 **AngularJS** 동작 사용 안 함**[Security Center** 1.3에서 업데이트됨〕

이 *glide.angular.legacy* 속성을 사용하여 오래된 AngularJS 라이브러리 버전에서 발견된 취약성에 대한 공격으로 인해 발생하는 잠재적인 보안 위험으로부터 보호합니다.

사전 배치된 이전 angularJS 버전이 사용되지 않도록 하려면 권장 값인 **false**로 설정합니다*glide.angular.legacy*. 이전의 사전 배치된 AngularJS 버전을 사용하려면 속성을 **true** 로 설정합니다.

추가 정보

속성	설명
속성 이름	*glide.angular.legacy*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	아키텍처, 설계 및 위협 모델링
목적	시스템 속성은 모든 조직이 패치되지 않은 AngularJS 버전에 의존하여 사용자 지정 구현을 실행하는 경우 안전 장치입니다.
권장 값	아니요
구성 유형	부울
보안 위험	(높음) 이전 버전의 AngularJS를 사용하면 오래된 AngularJS 라이브러리 버전에서 발견된 취약성에 대한 공격으로 인해 보안 위험이 발생할 수 있습니다.
보안 위험 등급	7.1

데이터 브로커 **REST** API에 대해 인증 필요 **[Security Center** 1.3에서 업데이트됨〕

이 *glide.basicauth.required.databrokerrestapiprocessor* 속성을 사용하여 모든 인바운드 데이터 브로커 REST API 요청에 대해 기본 인증을 요구합니다.

이 속성을 **true**로 설정하면 권한 부여가 적용됩니다. **false**로 설정된 경우 인증이 사용되지 않으므로 인스턴스에서 중요한 정보가 유출될 수 있습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.basicauth.required.databrokerrestapiprocessor*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	아키텍처, 설계 및 위협 모델링
보안 위험	• 심각도 점수: 8.6 • CVSS 점수: 높음 • 보안 위험 상세 정보: 속성이 **false**로 설정된 경우 API 인증이 적용되지 않으므로 악의적인 행위자가 중요한 데이터에 액세스할 수 있습니다.
의존성 및 필수 구성요소	안 함

빈 ACL을 사용하여 기본적으로 거부 〔보안 센터 1.3에서 업데이트됨〕

기존 ACL(접근 제어 목록) 규칙이 와일드카드 테이블 ACL 규칙의 일부임을 발견한 보안 관리자의 기본 동작을 제어하려면 이 *glide.sm.default_mode* 속성을 사용합니다.

해당 자원에 대해 정의된 ACL이 없거나 와일드카드 테이블 수준 ACL(예: `incident.*`)만 있는 경우 인스턴스의 레거시 보안 관리자가 자원에 대한 액세스를 허용하지 못하도록 합니다. 기본적으로 액세스가 허용되면 명시적 ACL 세트가 없는 모든 항목은 조작에 취약합니다.

정의 ACL 규칙이 없거나 와일드카드 테이블 수준 ACL만 있는 경우 액세스를 허용하지 않으려면 **glide.sm.default_mode** 시스템 속성 값을 거부 로 설정합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.sm.default_mode*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	아키텍처, 설계 및 위협 모델링
목적	가장 좋은 보안 방법은 권한이 없는 사용자의 테이블 액세스를 제한하는 것입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	• 테이블에 대한 ACL 규칙이 없는 경우 이 속성은 테이블/필드에서 수행되는 모든 CRUD 작업에 대해 최소한 와일드카드 ACL이 확인되도록 합니다. • 이러한 규칙은 사용자에게 관리자 역할이 있거나 다른 테이블 ACL 규칙의 요구 사항을 충족하지 않는 한 모든 테이블에서 읽기, 쓰기, 생성 및 삭제 작업을 제한합니다.
권장 값	거부
기능적 영향	이 속성을 허용으로 설정하면 와일드카드 테이블 ACL 규칙을 통해 해당 작업을 제한하는 특정 테이블 ACL 규칙이 없는 한 모든 테이블에서 CRUD 작업을 허용합니다. 주: 프로덕션 환경에서 이미 사용 중인 테이블에 대한 보안 액세스를 수정할 수 있으므로 이 플러그인은 기존 인스턴스를 위한 것이 아닙니다.
보안 위험	6.3
참조	기본 거부 속성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

토큰 자격 증명에 대한 자동 토큰 정리 설정[Security Center 2.0의 새로운 기능]

이 *com.snc.platform.security.token.auth.cleanup* 속성을 사용하여 만료된 API 키와 HMAC 암호가 삭제되도록 하여 토큰 재사용 가능성을 제한합니다.

com.snc.platform.security.token.auth.cleanup 속성이 안전하지 않은 값인 false로 설정된 경우 만료된 API 키 및 HMAC 암호가 삭제되지 않으므로 토큰을 다시 사용할 수 있습니다. 토큰이 유출 또는 손상으로 인해 만료된 경우 재사용으로 인해 유출된 토큰을 소유한 모든 사람에게 인스턴스가 노출될 수 있습니다.

만료된 토큰은 및 로 정의된 *com.snc.platform.security.token.auth.days.expired.hmac_secret.is.kept* 일수 동안 보존됩니다 *com.snc.platform.security.token.auth.days.expired.api_key.is.kept*. 이러한 설정에 유효한 값은 0 이상의 정수입니다. 값이 0이면 만료된 토큰이 같은 날 삭제되고, 일수가 높을수록 노출 기간이 늘어납니다. 기본값은 7일 이하로 설정하는 것이 좋습니다.

추가 정보

속성	설명
구성 이름	*com.snc.platform.security.token.auth.cleanup*, *com.snc.platform.security.token.auth.days.expired.hmac_se*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	권장 값은 true이며 7보다 작거나 같은 정수입니다.
기본값	7
범주	아키텍처, 설계 및 위협 모델링

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 5.1 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값인 예로 구성하지 않으면 만료된 API 키 및 HMAC 암호가 삭제되지 않아 토큰 재사용 가능성이 높아질 수 있습니다.
의존성 및 필수 구성요소	안 함

인증

인증 범주는 엔터티와 해당 클레임이 정통하고 정확하며 가장에 저항하고 암호 가로채기를 방지하는 최신 인증의 주요 요소를 다룹니다.

ASVS 표준은 이 섹션의 NIST 800-63b(https://pages.nist.gov/800-63-3/sp800-63b.html) 사양을 기반으로 합니다.

인증에는 암호 정책, 통제 및 스토리지, 인증자의 적절한 구현 및 대역 외 또는 일회성 검증기의 적절한 구현이 포함됩니다.

역할 기반 다단계 인증 활성화**[Security Center** 1.3에서 업데이트됨〕

이 *glide.authenticate.multifactor* 속성을 사용하여 특정 역할에 할당된 모든 사용자에 대해 역할 기반 MFA(다단계 인증)를 적용합니다.

사용자에게 할당된 역할에 따라 다단계 인증을 적용합니다. 사용자가 다단계 역할 목록에서 "관리자", "security_admin" 또는 "user_admin" 역할을 할당받은 경우 MFA가 적용됩니다.

- 특정 역할에 할당된 모든 사용자에 대해 역할 기반 다단계 인증을 적용하려면 이 속성을 **true** 로 설정합니다.
- 특정 역할에 할당된 모든 사용자에 대해 역할 기반 다단계 인증을 사용하지 않으려면 이 속성을 아니오 로 설정합니다.

추가 정보

속성	설명
속성 이름	*glide.authenticate.multifactor*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	특정 역할에 할당된 모든 사용자에 대해 역할 기반의 다단계 인증을 적용합니다.
유형	예/아니요
권장 값	*true*
보안 의존성	다중요인 기준 테이블 내에서 역할 기반 다단계 인증을 사용합니다.
보안 위험 등급	7.2

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기능적 영향	이 속성을 활성화하면 사용자 경험이 개선됩니다. 손상된 자격 증명에 대한 추가 보호 및 보안 계층 역할을 합니다.
보안 위험	(보통) 이 속성을 사용하도록 설정하지 않으면 중요한 데이터에 무단으로 액세스할 위험이 있습니다.
참조	역할 기반 다중요인 기준 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

계정 복구 사용 [Security Center 1.3 및 1.5에서 업데이트됨]

이 *glide.sso.acr.enabled* 속성은 계정 복구 기능을 제어합니다.

가능한 사용자 ID로 계정 복구를 허용하려면 권장 값인 예로 설정합니다 *glide.sso.acr.enabled*. 사용자 ID로 계정 복구를 허용하지 않으려면 값을 아니오 로 설정합니다.

추가 정보

속성	설명
속성 이름	*glide.sso.acr.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	사용자 ID별 계정 복구 기능을 통제합니다.
권장 값	True(기본값)
구성 유형	부울
보안 위험	중요(이 속성을 사용하지 않으면 사용자는 사용자 ID로 계정을 복구할 수 없습니다.
보안 위험 등급	9.1
참조	자세한 내용은 계정 복구(ACR) 를 참조하세요.

클래식 모바일 앱 UI 난독화 필요[Security Center 1.3에서 업데이트됨]

glide.ui.m.blur_ui_when_backgrounded 백그라운드 프로세스 중에 이미지가 저장될 때 이 속성을 사용하여 스냅샷의 모든 필드를 난독 처리합니다.

Android 장치에서 Android 운영 체제는 애플리케이션이 백그라운드로 전송될 때 최근 작업 메뉴에서 사용할 스크린샷을 찍습니다. 사용자는 장치에 공개적으로 저장된 응용 프로그램의 수동 스크린샷을 찍을 수도 있습니다.

iOS 디바이스에서 iOS 운영 체제를 사용하면 애플리케이션이 이미지 파일을 저장할 수도 있습니다. 이 파일은 애플리케이션이 백그라운드로 전송될 때 사용자가 본 마지막 화면을 나타냅니다. 더 나은 사용자 경험을 제공하기 위한 것이지만 이미지가 PNG 이미지 파일로 저장되기 때문에 보안 위험이 발생할 수도 있습니다.

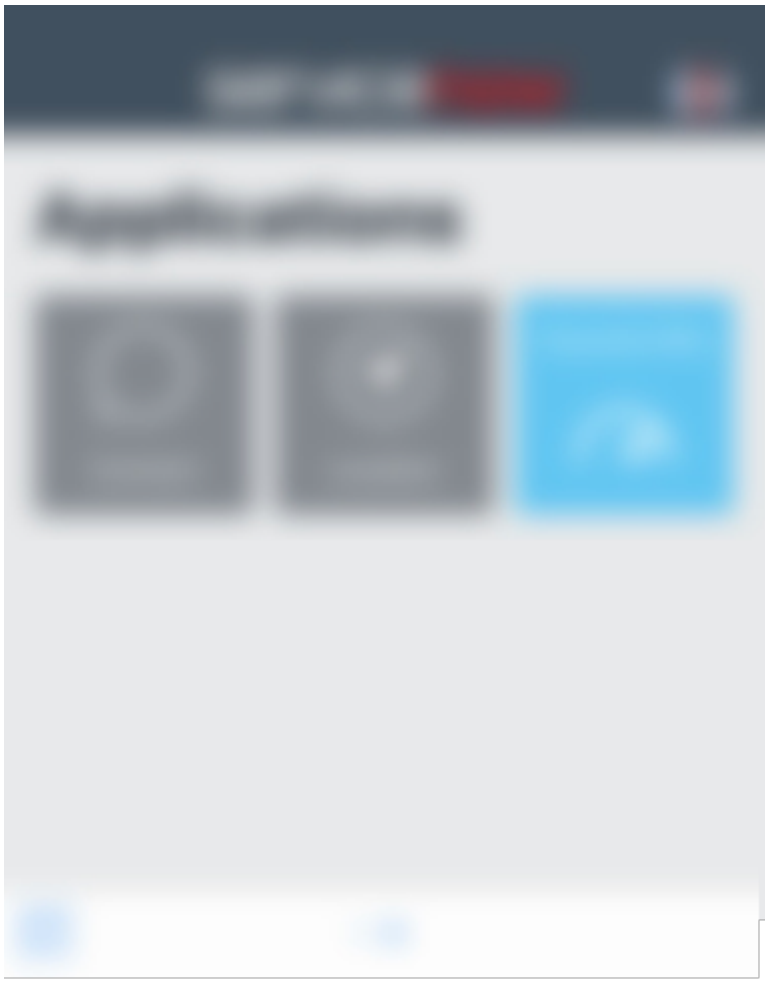
주: 이 설정 또는 구성은 인스턴스를 기준으로 이루어지므로 사용자는 속성이 구성된 인스턴스에 연결해야 합니다.

ServiceNow 클래식 앱의 스냅샷에서 모든 필드를 난독 처리하려면 다음을 참조하십시오. 흐 리게 앱 옵션을 구성하여 보안 향상 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예제

이 속성을 true로 설정하면 background 애플리케이션이 iOS 장치에 대해 난독화되고 Android iOS 장치에 대해 블랙아웃됩니다.



추가 정보

속성	설명
속성/플러그인 이름	*glide.ui.m.blur_ui_when_backgrounded*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	백그라운드 프로세스 중에 이미지가 저장될 때 스냅샷의 모든 필드를 난독 처리합니다.
권장 값	예
보안 위험 등급	2.4
기능적 영향	*glide.ui.m.blur_ui_when_backgrounded*속성이 true로 설정된 경우 네이티브 앱은 서버에 정의된 매개 변수를 사용하여 앱이 백그라운드로 들어갈 때 화면을 흐리게 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	• 앱이 백그라운드에 들어갈 때 iOS 및 Android에서 찍은 스크린샷을 흐리게 처리합니다. • 앱이 백그라운드로 전송될 때 콘텐츠를 볼 수 없기 때문에 사용자 환경에 부정적인 영향을 줄 수 있습니다.
보안 위험	(중간) 손상된(탈옥된) 디바이스를 통해 공격자는 파일 시스템에 대한 전체 액세스 권한을 가질 수 있으며, 중요한 정보가 포함된 해당 파일/스냅샷에 액세스할 수 있습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

암호 없는 인증 사용 안 함

이 *glide.login.no_blank_password* 속성을 사용하면 사용자가 빈 암호로 Now Platform에 로그인하거나 암호 필드를 비워 둘 수 없습니다.

관리자가 의도적으로 사용자 기록에 빈 값 또는 빈 암호를 할당한 경우에도 사용자는 암호 필드에 값을 입력하지 않으면 로그인할 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.login.no_blank_password*
구성 유형	시스템 속성(/sys_properties_list.do)
인스턴스 보안 센터에서 구성	예
목적	강력한 인증을 보장하기 위해 조직 내에서 사용자 이름을 쉽게 추측할 수 있는 경우가 있습니다.
권장 값	예
기능적 영향	작업에서는 심각한 보안 위험으로 간주되므로 빈 암호를 사용해서는 안 됩니다. 그러나 이러한 사용에 대한 유효한 사례가 있는 경우 중단될 가능성이 있습니다. 암호가 비어 있는 사용자는 인스턴스에 로그인할 수 없습니다.
보안 위험	(높음) 공격자는 기본 사용자 이름을 사용하거나 암호 없이 특정 개인/그룹(일반적으로 이름.성)으로 인스턴스에 로그인할 수 있습니다. 이렇게 하면 공용 사용자가 인스턴스 데이터의 기밀성과 무결성을 위반할 수 있으므로 심각한 보안 위험으로 간주됩니다.

로그인 시 암호 정책 적용 안 함 **[Security Center** 1.5에서 업데이트되고 2.0에서 제거됨]

인스턴스에서 암호 복잡도가 처리되는 방식을 관리합니다.

속성을 *glide.apply.password_policy.on_login* false로 설정하면 로그인 시 암호 복잡도가 적용되지 않습니다. 속성을 true로 설정하면 암호 복잡성이 적용되고 조직 정책 준수 문제가 발생합니다.

ASVS 4.03 v2.1.9 권장 사항에 따라:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

"허용되는 문자 유형을 제한하는 암호 구성 규칙이 없는지 확인합니다. 대문자나 소문자 또는 숫자 또는 특수 문자는 필요하지 않습니다. (C6)"

암호 복잡성을 적용하는 대신 ASVS 권장 사항은 암호 길이에 대해 최소 12자의 길이를 적용하는 것입니다.

OWASP ASVS v4.0 인증을 참조하십시오.

추가 정보

속성	설명
구성 이름	*glide.apply.password_policy.on_login*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	인증
보안 위험	• 심각도 점수: 4.4 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 예 로 설정하면 암호 복잡성이 적용되고 조직 규정 준수 문제가 발생할 수 있습니다.
의존성 및 필수 구성요소	안 함

거부 목록 암호 확인 검사 사용

제외된 암호 테이블에서 거부 목록 암호를 관리합니다.

이 *glide.enable.blacklist_password*속성을 사용하여 거부 목록 암호를 모니터링합니다. 속성이 **True**로 설정되면 사용자의 암호를 거부 목록 암호 목록과 비교하여 사용자가 위반된 암호 집합의 암호를 사용하지 못하도록 합니다. 관리자는 제외된 암호 테이블에 암호를 삽입하여 목록을 유지할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.enable.blacklist_password*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	인증
의존성 및 필수 구성요소	안 함
참조	인스턴스의 암호 정책을 통한 암호 제외

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

외부 사용자 등록에 **Captcha** 사용 **[Security Center 1.3** 및 1.5에서 업데이트됨]

외부 사용자 등록을 위해 CAPTCHA의 유효성을 검사할지 여부를 통제합니다 *sn_ext_usr_reg.captchaEnabled*.

외부 사용자 등록에 CAPTCHA를 요구하는 자동 계정 생성 공격을 방지하려면 권장 값인 예로 설정합니다*sn_ext_usr_reg.captchaEnabled*. 외부 사용자 등록에 CAPTCHA가 필요하지 않도록 값을 **false** 로 설정합니다.

추가 정보

속성	설명
속성 이름	*sn_ext_usr_reg.captchaEnabled*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	이 속성은 CSP, 커뮤니티와 같은 포털에서 외부 사용자 등록을 수행하는 동안 CAPTCHA 확인을 활성화하거나 비활성화하는 데 사용됩니다. 이는 VAM 및 CSM 게스트 워크업과 같은 스토어 앱에서 captcha를 활성화/비활성화하는 데도 사용됩니다.
권장 값	예
구성 유형	부울
보안 위험	(낮음) 이 속성은 외부 사용자 등록에서 CAPTCHA 활성화를 제어합니다. 비이상적인 값은 보안 취약성을 초래할 수 있습니다.
보안 위험 등급	3.7

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

고객 등록에 **CAPTCHA** 사용

고객 등록에 CAPTCHA를 활성화하여 악의적인 봇의 요청 위험을 줄입니다.

고객 서비스 관리 포털에서 고객 등록에 CAPTCHA 확인을 사용할 수 있는지 확인하려면 **sn_customerservice.captchaEnabled** 시스템 속성을 사용하십시오. CAPTCHA 확인을 사용하여 잠재적으로 악의적인 봇이 애플리케이션에 대한 요청을 자동으로 제출하지 못하도록 합니다.

CAPTCHA 확인을 사용하려면 시스템 속성 **sn_customerservice.captchaEnabled** 를 **true** 로 설정합니다. 속성이 시스템 속성 [sys_properties] 테이블에 없는 경우 기본값은 **true**입니다.

추가 정보

속성	설명
기술 구성 이름	sn_customerservice.captcha활성화됨
플러그인 적용 가능성	고객 서비스 관리
보안 위험	CAPTCHA 검증은 잠재적으로 악의적인 봇이 애플리케이션에 대한 요청을 자동으로 제출하는 것을 방지하는 데 도움이 됩니다.
CVSS(공통 취약성 평가 시스템) 점수	3.7

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
CVSS(공통 취약성 평가 시스템) 등급	낮음
기능적 영향	등록하는 사용자는 CAPTCHA 확인을 통과해야 하므로 부정적인 경험을 할 수 있습니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	**true**
폴백 값	**true**
권장 값	**true**

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

암호 재설정에 **CAPTCHA** 사용

이 *password_reset.captcha.ignore* 속성을 사용하여 사용자가 암호를 재설정할 때 CAPTCHA 질문 요구를 활성화하거나 비활성화합니다.

사용자가 암호를 재설정할 수 있도록 CAPTCHA 챌린지를 요구하려면 권장 값인 **false**로 설정합니다*password_reset.captcha.ignore*. 암호 재설정에 대한 CAPTCHA 옵션을 무시하려면 값을 **true** 로 설정합니다.

CAPTCHA는 자동화된 시스템에서 쉽게 응답할 수 없는 과제 대응을 사용자에게 요청하여 자동화 공격을 방지하는 데 도움이 됩니다. CAPTCHA가 비활성화된 경우 공격자는 암호 재설정 기능에 대한 자동 공격 중에 더 성공할 수 있습니다.

주: 이 속성은 암호 재설정 자동화에만 사용됩니다.

추가 정보

속성	설명
속성 이름	*password_reset.captcha.ignore*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	이 속성은 암호 재설정 중에 CAPTCHA 확인을 활성화하거나 비활성화하는 데 사용됩니다.
권장 값	거짓
구성 유형	부울
보안 위험	(보통) 비이상적인 값은 보안 취약성을 초래할 수 있습니다.
보안 위험 등급	5.5

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

다단계 인증용 이메일 **OTP** 사용

인스턴스에 2단계 인증을 적용하는 방법을 관리합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이*glide.authenticate.multifactor.email.otp.enabled*속성을 사용하여 2단계 인증을 위한 토큰의 이메일 사용 여부를 제어합니다. 이메일은 공격자가 MFA를 우회하기 위해 액세스 권한을 얻을 가능성이 높은 약한 MFA 요소로 간주됩니다. 이 속성을 **false**로 설정하면 공격자가 사용자의 암호를 손상시킬 때 MFA를 우회할 위험이 줄어듭니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.multifactor.email.otp.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	예
범주	인증
보안 위험	• 심각도 점수: 3.1 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하면 악의적인 액터가 2단계 인증을 바이패스할 위험이 줄어듭니다.
의존성 및 필수 구성요소	안 함
참조	이메일을 사용한 다단계 인증

암호 재설정 정책 검사 사용 **[Security Center** 2.0에서 업데이트됨〕

glide.enable.password_policy 속성을 사용하면 사용자가 사용자 인터페이스를 사용하여 암호를 변경할 때마다 암호 정책 검사를 활성화할 수 있습니다.

이 속성을 활성화한 후 사용할 암호 정책을 정의하려면 다음 문서를 참조하십시오 인스턴스에서 암호 정책 사용. Glide 속성이 *glide.enable.password_policy* 존재하고 true 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다.

주: 관리자가 암호를 변경하거나 스크립트를 통해 사용자를 추가하는 경우에는 **glide.enable.password_policy** 적용되지 않습니다.

경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.enable.password_policy*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	암호 변경 시 암호 정책을 적용하기 위해.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	true(강도가 높은 암호의 경우)
보안 위험 등급	7.4
기능적 영향	속성을 예로 설정하면 사용자가 암호를 재설정할 때 암호 정책 검사가 켜집니다.
보안 위험	(보통) 암호 정책이 없으면 사용자가 취약한 암호를 생성하여 악의적 사용자가 인스턴스에 액세스할 가능성을 높일 수 있습니다.

구성 단계

인스턴스 보안 센터의 강화 준수 구성 페이지에서 이 설정을 구성하는 경우:

1. 중간에서 세션 관리를 선택합니다.
2. 암호 재설정 정책 검사 사용 설정에서 중간 강도의 암호에 대해 보통을 선택하고, 더 강력하고 강도가 높은 암호에 대해 강함을 선택합니다. 이러한 옵션 중 하나를 선택하면 **glide.enable.password_policy** 속성이 true로 설정되고 암호 정책을 자동으로 업데이트하는 워크플로우가 시작됩니다.

또한 로그인 시 암호 정책 검사를 사용하도록 시스템 속성을 설정할 *glide.apply.password_policy.on_login* 수 있습니다.

모바일에 대한 정책 기반 세션 액세스 사용 **[Security Center** 1.5의 새로운 기능]

Zero Trust- Policy Based Session Access 플러그인을 사용하여 모바일 앱을 통해 인증하는 사용자의 역할이 축소되는지 여부를 제어합니다.

Zero Trust- Policy Based Session Access 플러그인을 사용하면 보안 관리자가 적응형 인증 정책으로 IP 주소, 위치, ID 제공자 속성 및 사용자 속성과 같은 매개변수를 기반으로 세션에서 사용자 액세스를 줄일 수 있습니다. 이 플러그인을 사용하거나 true로 설정하면 모바일 장치를 통해 인증하는 사용자의 역할이 플러그인 정책에 따라 제한됩니다. 인스턴스 관리자는 사용자가 모바일 장치를 통해 인증할 때 중요한 작업에 안전하지 않은 환경을 나타낼 수 있으므로 높은 권한의 액세스를 제한할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.session_access.mobile.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	접근 통제
보안 위험	• 심각도 점수: 4.7 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 강화 설정을 true로 설정하면 모바일 로그인을 위해 인스턴스에 정책 기반 세션 액세스가 적용되고 신뢰할 수 있는 환경에서 오지 않거나 신뢰할 수 있는 장치를 사용하지 않는 사용자는 권한이

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	감소된 역할을 갖게 됩니다. 보안 설정은 True입니다. 이 설정을 false로 구성하면 정책 기반 세션 액세스가 비활성화되고 사용자는 항상 관리자와 같은 높은 권한 있는 역할을 포함하여 전체 역할을 계속 사용할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	관리자가 인스턴스에서 세션 액세스 정책을 구성한 경우, 사용자가 신뢰할 수 있는 환경에서 오지 않거나 신뢰할 수 있는 장치를 사용하지 않는 경우 모바일 로그인 후 사용자의 역할이 줄어듭니다.
참조	적응형 인증

SAML 요청에서 릴레이 상태를 활성화하여 재생 공격 방지

SAML 요청에서 릴레이 상태를 활성화하여 재생 공격을 방지함으로써 재생 공격의 위험을 줄입니다.

glide.authenticate.sso.saml2.enable_relay_state_with_id 시스템 속성을 사용하여 SAML 재생 공격으로부터 보호합니다. 이 속성을 **true**로 설정하면 릴레이 상태 매개변수에 릴레이 상태 URL이 리디렉션되는 MultiSSO 요청 매개변수[multisso_request_parameter] 테이블의 기록 sys_id 포함됩니다.

시스템 속성 **glide.authenticate.sso.saml2.enable_relay_state_with_idtrue**로 설정합니다. 이렇게 하면 SAML 요청에 대한 액세스 권한을 얻은 공격자가 유효한 요청을 다시 제출하여 인스턴스에 액세스하는 것을 방지할 수 있습니다.

추가 정보

속성	설명
기술 구성 이름	glide.authenticate.sso.saml2.enable_relay_state_with_id
플러그인 적용 가능성	복수 제공자 SSO 플러그인 (com.snc.integration.sso.multi.installer)
보안 위험	이 시스템 속성에서 활성화한 릴레이 상태는 재생 공격으로부터 인스턴스를 보호하는 데 도움이 됩니다. 속성을 활성화하면 SAML 요청에 대한 액세스 권한을 얻은 공격자가 유효한 요청을 다시 제출하여 인스턴스에 액세스하는 것을 방지할 수 있습니다.
CVSS(공통 취약성 평가 시스템) 점수	3.8
CVSS(공통 취약성 평가 시스템) 등급	낮음
기능적 영향	이 속성이 true로 설정되면 SAML 요청의 릴레이 상태에 리디렉션할 릴레이 상태 URL을 포함하는 MultiSSO 요청 매개변수 [multisso_request_parameter] 테이블의 기록 sys_id 포함됩니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기본 시스템 값	예
폴백 값	거짓
권장 값	예

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

LDAP 인증에서 SSL 사용[Security Center 1.5 및 2.0에서 업데이트됨]

인스턴스에서 LDAP 인증 요청의 암호화를 관리합니다.

glide.ldap.use.ssl 이 속성을 사용하여 네트워크를 통해 전송되는 LDAP 인증 요청에 대해 TLS 암호화를 사용하거나 사용하지 않도록 설정합니다. 이 속성을 권장 값인 **true**로 설정하지 않으면 LDAP 인증이 메시지 가로채기(man-in-the-middle) 공격에 취약해집니다.

추가 정보

속성	설명
구성 이름	*glide.ldap.use.ssl*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	인증
보안 위험	• 심각도 점수: 8.1 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 아니오로 설정하면 LDAP 인증이 메시지 가로채기(man-in-the-middle) 공격에 취약해집니다.
의존성 및 필수 구성요소	안 함
참조	LDAP 통합

외부 사용자 등록 링크 만료 기간 최소화 [Security Center 1.3 및 1.5에서 업데이트됨]

등록 링크에 액세스할 수 있는 일 수를 관리합니다.

이 *sn_ext_usr_reg.Reg_link_expiration_days* 속성을 사용하여 등록 링크에 액세스할 수 있는 사용자를 관리합니다. 링크가 권장 값인 **3**으로 설정되어 있으면 나중에 링크가 검색될 때 의도한 사용자 이외의 사람이 등록 링크를 사용할 수 있습니다.

추가 정보

속성	설명
구성 이름	*sn_ext_usr_reg.Reg_link_expiration_days*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	3
기본값	3
범주	인증
보안 위험	• 심각도 점수: 중간 • CVSS 점수: 6.6 • 보안 위험 상세 정보: 이 속성을 정수 3으로 설정하지 않으면 의도하지 않은 사용자가 등록 링크를 사용할 수 있습니다.
의존성 및 필수 구성요소	안 함

로그인 실패 후 잠금 해제 시간 제한 관리[**Security Center** 1.3에서 업데이트됨]

사이트 관리자가 에서 잠기기 Now Platform전에 사용자가 잘못된 암호를 제공할 수 있는 횟수를 관리할 수 있는 두 가지 스크립트 작업을 사용할 수 있습니다. 이러한 스크립트 작업 중 하나를 활성화하여 실패한 로그인 시도를 관리할 수 있습니다.

추가 정보

속성	설명
속성/플러그인 이름	해당 사항 없음
구성 유형	시스템 정책 > 스크립트 작업
범주	인증
목적	자격 증명의 무차별 강제 적용을 방지하기 위해 실패한 로그인 시도에 대해 엄격한 정책을 적용합니다.
권장 값	활성
보안 위험 등급	7.3
기능적 영향	이러한 정정을 통해 인스턴스 관리자는 악의적인 사용자 액세스를 모니터링하고 보고할 수 있습니다. 기능에는 영향을 미치지 않으며 사용자 경험만 변경됩니다.
보안 위험	(보통) 의심스러운 활동을 적시에 식별하고 조치를 취할 수 있도록 정의된 로깅 및 감사 전략을 적용합니다.

구성 단계

1. 다음으로 이동 시스템 정책 > 스크립트 작업.
2. 이름을 *`*SNC User`*검색합니다.
3. 실패한 로그인 시도를 관리하려면 OR *`SNC User Lockout Check`* 스크립트 작업의 활성 상태를 *`SNC User Lockout Check with Auto Unlock`***false**에서 **true**로 변경합니다.
4. 로그인에 성공한 후 실패한 로그인 카운터를 *`SNC User Clear`* 재설정하려면 스크립트 작업을 활성화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실패한 로그인 잠금 해제 시간 제한 기간 최대화[Security Center 1.3에서 업데이트됨]

사이트 관리자가 에서 잠기기 Now Platform전에 사용자가 잘못된 암호를 제공할 수 있는 횟수를 관리할 수 있는 두 가지 스크립트 작업을 사용할 수 있습니다. 이러한 스크립트 작업 중 하나를 활성화하여 실패한 로그인 시도를 관리할 수 있습니다.

사용자가 잠긴 후 로그인을 시도할 수 없는 기간을 정의하여 무차별 암호 대입 공격으로부터 인스턴스를 보호할 수 있습니다. **glide.user.unlock_timeout_in_mins** 시스템 속성은 해당 값에 지정된 기간 후에 사용자 계정의 잠금을 해제합니다. 값을 지정하지 않으면 인스턴스가 기본 기간인 15분 후에 사용자 계정의 잠금을 해제합니다.

glide.user.unlock_timeout_in_mins 시스템 속성 값을 최소 **15**로 설정합니다.
glide.user.unlock_timeout_in_mins 없으면 기본 잠금 시간이 15분으로 설정됩니다.

SNC 사용자 잠금 해제 및 자동 잠금 해제 확인 스크립트 작업(스크립트 작업 [sysevent_script_action] 테이블에 있음)이 존재하고 활성 상태인지 확인합니다. 자동 잠금 해제로 **SNC** 사용자 잠금 확인 스크립트 작업은 com.glide.high_security(높은 보안 설정) 플러그인과 함께 설치됩니다.

추가 정보

속성	설명
구성 이름	• glide.user.unlock_timeout_in_mins(시스템 속성) • sysevent_script_action(스크립트 작업)
구성 유형	시스템 정책 > 스크립트 작업
범주	인증
목적	자격 증명의 무차별 강제 적용을 방지하기 위해 실패한 로그인 시도에 대해 엄격한 정책을 적용합니다.
권장 값	• **glide.user.unlock_timeout_in_mins** 시스템 속성의 경우 **15** • 자동 잠금 해제로 **SNC** 사용자 잠금 확인 스크립트 작업에 대해 활성화됩니다.
기능적 영향	이러한 정정을 통해 인스턴스 관리자는 악의적인 사용자 액세스를 모니터링하고 보고할 수 있습니다. 기능에는 영향을 미치지 않으며 사용자 경험만 변경됩니다.
보안 위험	(보통) 의심스러운 활동을 적시에 식별하고 조치를 취할 수 있도록 정의된 로깅 및 감사 전략을 적용합니다.

구성 단계

1. 다음으로 이동 시스템 정책 > 스크립트 작업.
2. 이름을 *`*SNC User`*검색합니다.
3. 실패한 로그인 시도를 관리하려면 OR *`SNC User Lockout Check`* 스크립트 작업의 활성 상태를 *`SNC User Lockout Check with Auto Unlock`***false**에서 **true**로 변경합니다.
4. 로그인에 성공한 후 실패한 로그인 카운터를 *`SNC User Clear`* 재설정하려면 스크립트 작업을 활성화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모바일 앱 UI 난독화 필요[Security Center 1.3에서 업데이트됨]

*glide.sg.blur_ui_when_backgrounded*앱이 백그라운드에서 실행 중일 때 앱의 UI가 흐리게 표시되도록 속성을 구성합니다.

이 속성을 권장 값인 **true**로 설정하지 않으면 앱 전환기에서 볼 때 모바일 앱의 사용자 인터페이스가 표시됩니다. 앱이 백그라운드에서 실행되는 경우에도 UI가 계속 표시되어 최종 사용자에게 낮은 수준의 보안과 기밀성을 제공합니다.

추가 정보

속성	설명
구성 이름	*glide.sg.blur_ui_when_backgrounded*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	파일 및 자원
보안 위험	• 심각도 점수: 2.4 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 값을 **true** 로 설정하면 앱이 백그라운드에서 실행 중일 때 UI를 흐리게 하여 로컬 장치에서 더 높은 수준의 기밀성과 개인정보 보호를 제공합니다.
의존성 및 필수 구성요소	안 함
참조	클래식 모바일 앱 UI 난독화 필요[Security Center 1.3에서 업데이트됨]

암호 재설정/변경 프로세스 중에 사용자에게 알림 [Security Center 1.5에서 제거됨]

이속성을 사용하면 최종 사용자가 셀프 서비스 프로세스를 통해 암호를 재설정하거나 변경할 수 있습니다.

이 속성을 사용하면 최종 사용자가 셀프 서비스 프로세스를 사용하여 암호를 재설정하거나 변경할 수 있습니다. 또는 조직에서 서비스 데스크 에이전트가 최종 사용자의 암호를 재설정하도록 요구하는 프로세스를 구현할 수 있습니다. 암호 변경 및/또는 재설정 프로세스가 암호 업데이트에 대해 사용자에게 알리지 않는 경우 악의적인 행위자는 사용자 모르게 해당 사용자를 계정에서 잠글 수 있습니다. 이렇게 하면 악의적인 행위자가 악의적인 활동을 수행할 수 있는 더 많은 시간을 확보할 수 있습니다. 암호 재설정 프로세스가 암호 변경 또는 재설정 시 사용자에게 알리는지 확인합니다.

추가 정보

속성	설명
구성 이름	*pwd_process.change, pwd_process.reset*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	부울
권장 값	예
기본값	예
범주	인증
보안 위험	• 심각도 점수: 8.1 • CVSS 점수: 높음 • 보안 위험 세부 정보: 암호 변경이 재설정될 때 알림이 전송되지 않으면 악의적인 행위자가 사용자 모르게 계정에서 사용자를 잠글 수 있습니다.
의존성 및 필수 구성요소	안 함

소개 페이지에서 자격 증명 제거

시작 페이지의 기본 컨텐츠를 수정하여 기본 자격 증명을 제거합니다.

두 개의 로그인 방법 기록이 CMS 플러그인에 대한 데모 데이터의 일부로 설치됩니다.

주: 인스턴스에 대한 데모 데이터를 설치하지 않으면 이러한 기록이 존재하지 않습니다. 이 경우 구성은 권장 보안 관행에 따라 보안 준수로 간주됩니다.

추가 정보

속성	설명
이름	*How to login*
구성 유형	테이블: sys_home
범주	인증
목적	데모 데이터와 함께 추가된 기본 자격 증명을 시작 페이지에서 제거합니다.
권장 값	데모 데이터가 사용되지 않은 경우 False 또는 null입니다.
기본값	없음. 이는 Glide 속성이 아닌 테이블 구성입니다. 따라서 기본값에 대한 값은 없습니다.
구성 유형	부울
보안 위험	(보통) CMS 플러그인에 대한 데모 데이터가 제공되며, 여기에는 시작 페이지에 포함된 두 개의 기본 암호가 포함됩니다. 이를 제거하지 않으면 권한 없는 공격자가 인스턴스에 액세스할 수 있습니다.
참조	https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107 시작 페이지

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호 요청 만료 기간 재설정 최소화[Security Center 1.3에서 업데이트됨]

사용자가 *password_reset.request.expiry* 암호 재설정 프로세스를 수행해야 하는 기간(분)을 나타냅니다.

주: 이 속성의 설정은 *password_reset.request.expiry* 기본값이 12시간인 속성의 설정 *glide.pwd_reset.onetime.token.validity*보다 우선합니다.

추가 정보

속성	설명
속성 이름	*password_reset.request.expiry*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	사용자가 암호 재설정 프로세스를 수행해야 하는 기간(분)을 나타냅니다.
권장 값	**10** 이하의 정수로 설정합니다. 기본값은 10입니다.
구성 유형	정수 값
보안 위험	(보통) 속성이 권장 값인 10 이하로 설정되지 않은 경우 다른 사람이 요청을 추측하여 사용하고 암호 재설정을 시도할 수 있는 기회가 증가합니다.
보안 위험 등급	4.2
참조	암호 재설정 속성 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

잘못된 암호 재설정 시도 제한 [Security Center 1.3에서 업데이트되고 2.0에서 업데이트됨]

이 *password_reset.request.max_attempt* 옵션은 사용자가 지정된 기간 동안 잠기기 전에 암호를 재설정하거나 변경할 수 있는 최대 실패 시도 횟수를 제어하는 데 사용됩니다.

추가 정보

속성	설명
속성 이름	*password_reset.request.max_attempt*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	사용자가 암호 재설정 프로세스에서 잠기기 전에 수행할 수 있는 실패한 암호 재설정 시도의 최대 수를 나타냅니다. 잠금 기간은 의 *password_reset.request.max_attempt_window*값에 따라 결정됩니다.
권장 값	3보다 작은 양의 정수 값으로 설정합니다. 기본값은 **3**입니다. 속성의 상한 범위에 대한 제한을 결정할 때는 사용자가 수행하는 작업을 고려합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
구성 유형	양의 정수 값
보안 위험	(높음) 속성이 권장 값인 "**3**" 또는 기타 합당한 작은 값으로 설정되지 않은 경우 암호 재설정 프로세스에 대해 무차별 암호 대입 공격을 수행할 수 있습니다.
보안 위험 등급	7.5
참조	암호 재설정 속성 구성

잘못된 암호 재설정 시도에 대한 잠금 시간 제어 **[Security Center 1.3** 및 2.0에서 업데이트됨]

이 *password_reset.request.max_attempt_window* 속성은 사용자가 속성으로 설정된 실패한 최대 시도 횟수를 초과한 후 암호를 재설정하거나 변경하기 위해 기다려야 하는 시간(분)을 *password_reset.request.max_attempt* 제어합니다.

이 *password_reset.request.max_attempt_window* 속성은 사용자가 로 설정된 *password_reset.request.max_attempt_property* 실패한 최대 시도 횟수를 초과한 후 암호를 재설정하거나 변경하기 위해 기다려야 하는 시간(분)을 정의합니다. 속성에 대한 *password_reset.request.max_attempt_window* 시간(분)이 짧으면 암호 재설정을 더 많이 시도할 수 있으므로 무차별 암호 대입이 성공할 위험이 높아집니다. 기본값은 1440분입니다.

속성이 *password_reset.request.max_attempt_window* 1440 이상으로 설정되어 있는지 확인합니다.

추가 정보

속성	설명
속성 이름	*password_reset.request.max_attempt_window*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	실패한 암호 재설정 시도의 최대 횟수가 충족된 후의 잠금 기간(분)을 나타냅니다.
권장 값	1440
기본값	1440
구성 유형	양의 정수 값
보안 위험	(높음) 속성이 권장 값인 1440 이하로 설정되지 않은 경우 최대 수의 잘못된 인증 시도 후에도 계정이 잠기지 않으므로 계정 무차별 암호 대입을 수행할 수 있습니다.
보안 위험 등급	7.5
참조	암호 재설정 속성 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

암호 요청 재시도 기간 재설정 최대화 **[Security Center** 1.3에서 업데이트됨]

이 *password_reset.request.retry_window* 속성은 암호 재설정 시도 횟수가 새로 고침되기 전의 시간(분)을 제어합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*password_reset.request.retry_window*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	재시도 횟수가 0으로 재설정되기 전에 마지막 요청에서 암호 시도 횟수가 새로 고침되기 전의 시간(분)을 나타냅니다.
권장 값	**1440** 이상의 양의 정수 값으로 설정합니다. 기본값은 **1440** 분입니다.
구성 유형	양의 정수 값입니다.
보안 위험	(높음) 속성이 권장 값인 1440 이상으로 설정되지 않은 경우 암호 재설정 프로세스에 대해 계정 무차별 암호 대입 공격을 수행할 수 있습니다.
보안 위험 등급	7.5
참조	암호 재설정 속성 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

암호 요청 잠금 해제 기간 재설정 최대화**[Security Center** 1.3에서 업데이트됨〕

이 *password_reset.request.unlock_window* 속성은 사용자가 마지막으로 성공한 계정 잠금 해제 작업 후 재설정 요청을 시작하기 위해 기다려야 하는 시간(분)을 제어합니다.

이 속성은 사용자가 마지막으로 성공한 계정 잠금 해제 후 재설정 요청을 시작하기 위해 기다려야 하는 시간(분)을 제어합니다. 권장 값인 1440 이상으로 설정되지 않은 경우 *password_reset.request.unlock_window* 악의적인 액터가 자동화된 도구를 사용하여 사용자의 암호를 강제로 강제 적용할 수 있는 기회가 증가합니다.

추가 정보

속성	설명
속성 이름	*password_reset.request.unlock_window*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	사용자가 암호를 성공적으로 재설정한 후 암호를 다시 재설정하기 위해 기다려야 하는 기간(분)을 나타냅니다.
권장 값	1440
기본값	1440
구성 유형	양의 정수 값
보안 위험	(높음) 속성이 권장 값인 1440 이상으로 설정되지 않은 경우 악의적인 액터가 자동 도구를 사용하여 암호 대입 권한을 강제할 수 있는 기회가 증가합니다.
보안 위험 등급	5.9

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
참조	암호 재설정 속성 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

암호 SMS 복잡성 재설정 최대화[Security Center 1.3에서 업데이트됨]

이 *password_reset.sms.default_complexity* 속성은 암호 재설정 중에 필요한 최소 필수 SMS 코드 검증 크기를 제어합니다.

추가 정보

속성	설명
속성 이름	*password_reset.sms.default_complexity*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	암호 재설정 중에 필요한 SMS 코드 검증 크기를 나타냅니다.
권장 값	6
기본값	4
구성 유형	0보다 큰 정수 값
보안 위험	(낮음) 속성이 권장 값으로 설정되지 않은 경우 약한 SMS 확인 토큰이 사용됩니다. 이는 계정 탈취로 이어질 수 있는 토큰 추측의 가능성을 높입니다.
보안 위험 등급	3.8

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

암호 SMS 일시 중지 기간 재설정 최대화 [Security Center 1.3에서 업데이트됨]

사용자가 새 암호 재설정 코드를 요청하기 전에 기다려야 하는 시간(분)을 관리합니다.

이 속성을 권장 값인 **2** 분 이상으로 설정하지 않으면 악의적인 사용자가 짧은 시간 내에 많은 암호 재설정 코드를 시작할 수 있습니다. 이렇게 하면 악의적인 행위자가 SMS 재설정 코드를 예측할 가능성이 높아집니다.

추가 정보

속성	설명
구성 이름	*password_reset.sms.pause_window*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	2
기본값	2
범주	인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 4.8 • CVSS 점수: 중간 • 보안 위험 상세 정보: 2 *password_reset.sms.pause_window* 이상의 값으로 설정되어 있는지 확인합니다.
의존성 및 필수 구성요소	안 함

암호 확인 지연 기간 재설정 최대화 **[Security Center** 1.3에서 업데이트됨]

사용자가 새 암호 재설정 요청을 제출하기 전에 기다려야 하는 지연 시간(밀리초)을 구성합니다.

악의적인 행위자는 암호 검증 지연 속성 재설정 이 방어하는 데 도움이 되는 봇과 같은 자동화 도구를 사용하여 무차별 암호 대입 로그인 자격 증명을 시도할 수 있습니다. 속성 값은 사용자가 암호 재설정 요청을 하기 전에 기다려야 하는 지연 시간(밀리초)을 나타냅니다. 이 속성을 권장 값인 **1,000** 이상으로 설정하지 않으면 로그인이 무차별 암호 대입 공격에 더 취약해집니다.

추가 정보

속성	설명
구성 이름	*password_reset.verification.delay*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	1000
기본값	1000
범주	인증
보안 위험	• 심각도 점수: 5.9 • CVSS 점수: 중간 • 보안 위험 상세 정보: 속성 값을 1000 미만으로 설정하면 로그인이 무차별 암호 대입 공격에 더 취약해집니다.
의존성 및 필수 구성요소	안 함
참조	사용자에 대한 암호 구성

높은 보증 세션에 대한 실패한 로그인 시도 최소화

높은 보증 세션에 대한 로그인 시도 실패를 최소화하여 무차별 암호 대입 공격의 가능성을 줄입니다.

glide.zta.high_assurance.session.max.login.failed_attempts 시스템 속성을 사용하여 연속 인증을 통해 재인증할 때 사용자가 로그아웃되기 전에 허용되는 인증 실패 시도 횟수를 제한합니다.

이 시스템 속성의 값을 낮은 값(예: 5)으로 설정하여 무차별 암호 대입 공격의 가능성을 줄입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
기술 구성 이름	glide.zta.high_assurance.session.max.로그인.실패_시도
플러그인 적용 가능성	제로 트러스트 - 연속 인증 (com.snc.zero_trust_continuous_authentication)
보안 위험	허용되는 인증 시도 횟수가 많을수록 무차별 암호 대입 공격의 가능성이 높아집니다.
CVSS(공통 취약성 평가 시스템) 점수	3.3
CVSS(공통 취약성 평가 시스템) 등급	낮음
기능적 영향	사용자는 속성에서 인증 실패 횟수가 선택된 후 세션에서 로그아웃됩니다.
의존성 및 필수 구성요소	안 함
데이터 유형	정수
기본 시스템 값	5
폴백 값	5
권장 값	5

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

일별 암호 최대 **SMS** 재설정 최소화 **[Security Center** 1.3에서 업데이트됨〕

사용자가 매일 검증용으로 전송하는 최대 SMS 코드 수를 관리합니다.

이*password_reset.sms.max_per_day*속성은 사용자가 매일 확인을 위해 보낼 수 있는 최대 SMS 코드 수를 나타냅니다.

추가 정보

속성	설명
구성 이름	*password_reset.sms.max_per_day*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	10
기본값	10
범주	인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 5.9 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성이 권장 값인 **10** 이하로 설정되지 않은 경우 SMS 코드를 강제로 적용하는 것이 더 쉽습니다.
의존성 및 필수 구성요소	안 함

암호 요청 성공 기간 재설정 최소화 [보안 센터 1.3에서 업데이트됨]

이 *password_reset.request.success_window* 속성은 사용자가 암호를 성공적으로 재설정한 후 암호를 재설정하거나 다시 변경하기 위해 기다려야 하는 시간(분)을 제어합니다. 사용자가 지정된 기간 동안 암호를 다시 재설정할 수 없도록 차단됩니다.

추가 정보

속성	설명
속성 이름	*password_reset.request.success_window*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
목적	사용자가 암호를 성공적으로 재설정한 후 암호를 다시 재설정하기 위해 기다려야 하는 기간(분)을 나타냅니다.
권장 값	1440
기본값	1440
구성 유형	양의 정수 값
보안 위험	(높음) 속성이 권장 값인 1440 이하로 설정되지 않은 경우 다른 사람이 암호 재설정 기능을 남용하여 사용자 계정에 무단으로 액세스할 수 있는 기회가 증가합니다.
보안 위험 등급	4.9
참조	암호 재설정 속성 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

암호 **SMS** 만료 기간 재설정 최소화 **[Security Center** 1.3에서 업데이트됨]

SMS 코드가 만료되기 전 남은 시간(분)을 제어합니다.

이 *password_reset.sms.expiry* 속성은 SMS 코드가 만료되기까지 남은 시간(분)을 나타냅니다.

추가 정보

속성	설명
구성 이름	*password_reset.sms.expiry*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	정수
권장 값	5
기본값	5
범주	인증
보안 위험	• 심각도 점수: 5.6 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값인 **5** 이하로 설정하지 않으면 악의적인 액터가 SMS 코드를 추측하고 사용하여 암호를 재설정할 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함

SAML notBefore 또는 notOnOrAfter 제약 조건 기간 최소화[Security Center 1.3 및 1.5에서 업데이트됨]

SAML 요청 및 응답이 유효한 것으로 간주되는 유예 기간을 추가하려면 이 속성을 구성합니다.

이 속성은 SAML 요청 및 응답이 유효한 것으로 간주되는 유예 기간을 추가합니다. 속성 값은 IdP(ID 제공자) 클럭과 SP(서비스 제공자) 클럭 간의 시간 차이를 처리하기 위해 AND *NotOnOrAfter* 제약 조건에 추가할 *NotBefore* 시간(초)을 나타냅니다. 이러한 제약 조건은 지정된 시간 프레임 내에 이루어지지 않은 요청을 거부하여 재생 공격을 방어합니다. IdP 및 SP 클럭이 크게 다른 경우 네트워크 대기 시간으로 인해 SAML 요청이 무단으로 처리될 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.sso.saml2.clockskew*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	60 미만
기본값	180
범주	인증
보안 위험	• 심각도 점수: 7.5 • CVSS 점수: 높음 • 보안 위험 세부 정보: 속성을 60 이상의 값으로 설정하면 제약 조건이 재생 공격을 방어하지 못할 수 있습니다.
의존성 및 필수 구성요소	안 함

수신 전자 메일에서 사용자 만들기 사용 안 함 [보안 센터 1.3에서 업데이트됨]

이 *glide.user.trusted_domain* 속성을 사용하여 수신 이메일에서 사용자를 만드는 데 사용되는 신뢰할 수 있는 도메인의 목록을 쉼표로 구분하여 지정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관리자는 수신 이메일에서 사용자를 자동으로 만들도록 이메일 속성을 설정할 수 있습니다. 이 속성을 안전하지 않은 값으로 설정하면 인스턴스가 수신 이메일에서 사용자를 자동으로 작성합니다. 생성된 각 사용자에게는 동일한 하드 코딩된 기본 암호가 적용되므로 무차별 암호 대입을 통한 인증 우회가 더 쉬워집니다.

추가 정보

속성	설명
속성 이름	*glide.pop3readerjob.create_caller*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증
권장 값	거짓
기본값	거짓
보안 위험 등급	5.4
기능적 영향	이 속성이 구성되면 인스턴스는 신뢰할 수 있는 도메인의 이메일만 수락합니다. 신뢰할 수 있는 목록에 도메인을 포함하지 않으면 계정이 자동으로 생성되기 때문에 게스트 사용자에게 영향이 있습니다.
보안 위험	(보통) 속성을 사용하도록 설정하지 않으면 공격자는 전자 메일 스푸핑/스팸 캠페인을 사용하여 여러 전자 메일을 보내 불필요한 게스트 사용자를 더 많이 만들 수 있습니다.
참조	인바운드 메일 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

역할 기반 다단계 인증 사용**[Security Center** 1.3에서 업데이트됨〕

이 *glide.authenticate.multifactor* 속성을 사용하여 특정 역할에 할당된 모든 사용자에 대해 역할 기반 MFA(다단계 인증)를 적용합니다.

사용자에게 할당된 역할에 따라 다단계 인증을 적용합니다. 사용자가 다단계 역할 목록에서 "관리자", "security_admin" 또는 "user_admin" 역할을 할당받은 경우 MFA가 적용됩니다.

- 특정 역할에 할당된 모든 사용자에 대해 역할 기반 다단계 인증을 적용하려면 이 속성을 **true** 로 설정합니다.
- 특정 역할에 할당된 모든 사용자에 대해 역할 기반 다단계 인증을 사용하지 않으려면 이 속성을 아니오 로 설정합니다.

추가 정보

속성	설명
속성 이름	*glide.authenticate.multifactor*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
목적	특정 역할에 할당된 모든 사용자에 대해 역할 기반의 다단계 인증을 적용합니다.
유형	부울
권장 값	`true`
기본값	거짓
보안 의존성	다중요인 기준 테이블 내에서 역할 기반 다단계 인증을 사용합니다.
보안 위험 등급	7.2
기능적 영향	이 속성을 활성화하면 사용자 경험이 개선됩니다. 손상된 자격 증명에 대한 추가 보호 및 보안 계층 역할을 합니다.
보안 위험	(보통) 이 속성을 사용하도록 설정하지 않으면 중요한 데이터에 무단으로 액세스할 위험이 있습니다.
참조	역할 기반 다중요인 기준 구성

Multifactor Setup에 허용되는 바이패스 감소

Multifactor 설정에 허용되는 바이패스를 줄여 계정이 손상 위험에 처할 수 있는 기간을 줄입니다.

사용자가 다단계 암호 설정 요구 사항을 건너뛸 수 있는 횟수를 줄여 계정이 손상될 위험이 있는 기간을 줄입니다. MFA(사용자 다단계 인증)는 추가 형태의 검증을 요구하여 암호 관련 공격이나 취약한 암호로부터 보호합니다. 사용자가 이 설정을 건너뛸 수 있는 시간을 줄이면 이러한 취약성을 줄일 수 있습니다.

glide.authenticate.multifactor.setup.bypass.count 시스템 속성을 **0**으로 설정하여 사용자가 다단계 암호 설정을 건너뛰지 못하게 합니다.

추가 정보

속성	설명
기술 구성 이름	glide.authenticate.multifactor.setup.bypass.count
플러그인 적용 가능성	없음.
보안 위험	Multifactor Authentication은 추가 형태의 검증을 요구하여 암호 관련 공격이나 취약한 암호로부터 보호합니다. 허용된 다단계 설정 바이패스가 많으면 계정이 다단계로 보호되지 않으므로 계정 손상 위험이 높아집니다. 허용된 바이패스 수가 적으면 이 시간이 줄어듭니다.
CVSS(공통 취약성 평가 시스템) 점수	3.9
CVSS(공통 취약성 평가 시스템) 등급	낮음
기능적 영향	사용자가 속성에 지정된 로그인 수를 초과하는 경우 MFA를 설정하지 않고 인스턴스에 로그인할 수 없습니다.
의존성 및 필수 구성요소	안 함
데이터 유형	정수

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기본 시스템 값	0
폴백 값	0
권장 값	0

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

최소 암호 길이 설정 [Security Center 2.0에서 제거됨, 2.1에 추가됨]

규정 준수 문제를 방지하고 무차별 암호 대입 공격의 성공 위험을 줄이기 위해 최소 암호 길이를 설정합니다.

규정 준수 문제를 방지하고 무차별 암호 대입 공격의 성공 위험을 줄이기 위해 최소 암호 길이를 12자 이상으로 적용합니다.

인스턴스에서 사용 중인 모든 사용된 암호 자격 증명 스토어에 대해 암호 재설정 자격 증명 스토어 [pwd_cred_store] 테이블의 관련 기록에서 암호 정책 사용 필드를 선택하여 암호 정책이 적용되고 있는지 확인합니다.

그런 다음 암호 정책 [password_policy] 기록 테이블에서 기록을 열고 최소 암호 길이 필드를 **12** 이상으로 설정합니다. 암호 재설정 자격 증명 스토어 [pwd_cred_store] 기록의 암호 정책 필드에서 연결된 암호 정책 기록을 찾을 수 있습니다.

암호 정책 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 인스턴스에서 암호 정책 사용.

추가 정보

속성	설명
기술 구성 이름	암호 재설정 자격 증명 스토어[pwd_cred_store] 및 암호 정책 [password_policy] 테이블의 기록입니다.
플러그인 적용 가능성	안 함
보안 위험	최소 암호 길이 정책 [password_policy] 레코드의 값을 12 미만으로 설정하면 규정 준수 문제가 발생할 수 있으며 공격자가 무차별 암호 대입에 성공할 위험이 높아집니다.
CVSS(공통 취약성 평가 시스템) 점수	5.9
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	인스턴스는 최소 암호 길이 12로 인한 영향을 받지 않습니다.
의존성 및 필수 구성요소	안 함
데이터 유형	정수
기본 시스템 값	8
폴백 값	8
권장 값	12

12시간 이하로 암호 재설정 OTP 수명 설정 [Security Center 2.0에서 업데이트됨]

암호 재설정 이메일의 링크 지속 시간을 제어합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 속성은 속성에 지정된 시간이 경과한 후 암호 재설정 이메일의 링크가 만료되게 합니다. 암호 재설정 토큰의 유효 시간은 일반적인 사용자 경험을 방해하지 않으면서 가능한 한 짧게 유지되어야 합니다.

추가 정보

속성	설명
구성 이름	*glide.pwd_reset.onetime.token.validity*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	12
기본값	12
범주	인증
보안 위험	• 심각도 점수: 5.6 • CVSS 점수: 중간 • 보안 위험 세부 정보: 암호 재설정 토큰의 유효 시간이 길면 악의적인 행위자가 계정 인수를 수행할 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함

일회성 대역 외 검증자 수명 기간 최소화 **[Security Center** 1.3에서 업데이트됨〕

대역 외 검증기의 기간을 관리합니다.

대역 외 검증기는 일회성 코드 상황에 대한 대체 전달 방법입니다. 예를 들어 다단계 토큰을 재설정할 수 있습니다. 플러그인에서 다단계 인증(MFA) 관리자가 이 방법을 활성화하면 일회용 코드가 이메일로 전달됩니다. 유효 기간을 제한하기 위해 일회성 대역 외 검증기가 10분 후에 만료되도록 설정합니다. 기간이 길수록 피싱, 소셜 엔지니어링 또는 숄더 서핑 공격과 같은 불법적인 수단을 통해 코드가 손상될 수 있는 시간이 더 많아집니다.

추가 정보

속성	설명
구성 이름	*glide.multifactor.onetime.code.validity*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	10
기본값	10
범주	인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 3.9 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 일회성 대역 외 검증기가 10분 후에 만료되도록 설정합니다. 더 이상 코드가 악의적인 행위자에 의해 손상될 위험이 증가합니다.
의존성 및 필수 구성요소	다단계 인증(MFA)
참조	다단계 인증 기준

장치 암호화 및 암호 요구 사항 강제 적용 **[Security Center** 1.3의 새로운 기능**]**

이 *glide.sg.device_encryption_enabled*속성은 FIPS 140-2(Federal Information Processing Standard) 암호화를 적용합니다. 모바일 장치 암호화 및 암호는 장치를 물리적으로 가져온 경우에도 권한이 없는 사용자가 장치의 콘텐츠에 액세스할 수 없도록 합니다.

예로 설정되면 *glide.sg.device_encryption_enabled*ServiceNow 모바일 앱에서 장치 암호화 및 장치 암호가 사용되는지 확인합니다.

추가 정보

속성	설명
구성 이름	*glide.sg.device_encryption_enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	인증
보안 위험	• 심각도 점수: 4.2 • CVSS 점수: 중간 • 보안 위험 상세 정보: 암호화 또는 암호가 활성화되지 않은 경우 사용자는 모바일에서 인스턴스에 로그인할 수 없습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성을 true로 설정하면 모바일 앱에서 장치 암호화가 사용되는지 확인합니다. 암호화를 사용할 수 없는 경우 사용자는 모바일에서 현재 인스턴스에 로그인할 수 없습니다.

고객 서비스 애플리케이션에서 게스트 워크업 경험에 대해 **captcha** 필요**[Security Center** 1.3의 새로운 기능 및 1.5에서 업데이트됨**]**

게스트 워크업 경험용 captcha는 사용자에게 captcha 확인을 완료하도록 요구하여 인증되지 않은 게스트 사용자가 예약을 생성하지 못하도록 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
구성 이름	*sn_guest_walkup_cs.captcha.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	인증
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: captcha가 활성화되지 않은 경우 스팸 약속이 자동으로 생성되어 시스템에 과부하가 발생하거나 사용 가능한 모든 예약 스팟을 채워 DoS(서비스 거부) 공격을 생성할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성은 CSM 게스트 워크업 체크인 위젯에서 captcha를 활성화하거나 비활성화합니다. 기본적으로 true로 설정됩니다.

등록 및 확인을 위한 **SMS** 코드 알림 사용**[Security Center** 1.3에서 업데이트됨〕

이*password_reset.sms.use_notify*속성은 암호 재설정을 위한 SMS 코드 알림 사용을 제어합니다.

*password_reset.sms.use_notify*속성이 권장 값인 **true**로 설정되면 사용자에게 이메일보다 더 안전한 SMS 검증 및 새 장치 등록을 사용하여 암호 재설정을 수행하라는 알림이 표시됩니다.

추가 정보

속성	설명
구성 이름	*password_reset.sms.use_notify*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부엘란
권장 값	예
기본값	예
범주	인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을**false** 로 설정하면 이메일이 SMS보다 덜 안전한 암호 복구의 기본 방법이 됩니다.
의존성 및 필수 구성요소	안 함

비즈니스 논리

이 범주에서는 일반적인 보안 원칙을 사용하여 각 애플리케이션에 고유한 논리와 플로우를 살펴봅니다. 특히 의도한 일련의 비즈니스 논리 플로우가 바이패스될 수 없고, 자동화된 공격을 탐지 및 방지하기 위한 제한이 존재하며, 스푸핑, 변조, 정보 공개 및 권한 공격 상승에 대한 보호가 존재하는지 확인합니다.

다음은 Now Platform 내의 중요한 엔터티에 대한 무단 액세스를 제한하기 위해 관리자가 구성할 수 있는 몇 가지 보안 제어입니다.

일별 사용자당 최대 댓글 제한

sn_kb_social_qa.max_comments_per_user_daily 하루에 QA 코멘트 수를 제한하도록 속성을 구성합니다.

이 속성을 권장 값인 **500** 개 이하로 설정하지 않으면 자원 소모로 이어질 수 있는 일별 QA 코멘트 수에 제한이 없습니다.

추가 정보

속성	설명
구성 이름	*sn_kb_social_qa.max_comments_per_user_daily*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	500
기본값	500
범주	비즈니스 논리
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성의 권장 값을 500 이하로 설정하지 않으면 일별 QA 의견에 제한이 없으므로 자원이 고갈될 수 있습니다.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일별 사용자당 최대 구독 제한

사용자가 하루에 구독할 수 있는 최대 구독 수를 제한하도록 속성을 *sn_kb_social_qa.max_subscriptions_per_user_daily* 구성합니다.

이 속성을 권장 값인 **500** 개 이하로 설정하지 않으면 사용자가 하루에 구독할 수 있는 Q&A 질문의 최대 수에 제한이 없습니다. 이 제한 없음은 자원 고갈로 이어질 수 있으며 인스턴스 가용성에 영향을 줄 수 있습니다.

추가 정보

속성	설명
구성 이름	*sn_kb_social_qa.max_subscriptions_per_user_daily*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	500
기본값	500
범주	비즈니스 논리
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 자원 고갈을 방지하려면 속성 값을 500 이하로 설정합니다.
의존성 및 필수 구성요소	안 함

SMTP 받는 사람 수량 최소화 [Security Center 1.3에서 업데이트됨]

단일 *glide.email.smtp.max_recipients* 이메일 알림에 대해 인스턴스가 **To:** 라인에 나열할 수 있는 최대 수신자 수를 지정합니다.

권장 값 **100** 이하로 설정합니다*glide.email.smtp.max_recipients*. 이 한도를 초과하는 알림은 대신 수신자 목록의 하위 집합에 주소가 지정된 중복 이메일 알림을 작성합니다. 각 이메일 알림의 최대 수신자 수는 동일합니다.

추가 정보

속성	설명
속성 이름	*glide.email.smtp.max_recipients*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	비즈니스 논리
목적	이 속성이 기본값 100보다 안전하지 않은 값으로 설정된 경우 인스턴스에서 서비스 거부가 발생할 수 있습니다.
권장 값	100
기본값	100
구성 유형	정수

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	(보통) 이 한도를 초과하는 알림은 대신 수신자 목록의 하위 집합에 주소가 지정된 중복 이메일 알림을 작성합니다.
보안 위험 등급	4.9

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

원격 호스트의 유효성 확인

잘못된 액터가 네트워크에서 내부 포트 검사를 사용하지 못하도록 속성을 true로 설정합니다.

glide.update_set.remote.check_host 속성이 권장 값인 **true**로 설정되지 않은 경우 팀 개발 원격 인스턴스 테스트 기능은 악의적인 행위자가 네트워크의 취약성을 검색하는 데 사용할 수 있는 방법인 내부 포트 검사를 허용합니다. 그런 다음 지정된 호스트의 모든 열린 포트를 열거할 수 있으며, 경우에 따라 정보 유출 또는 무단 데이터 액세스로 이어질 수 있는 응답 데이터를 가져올 수 있습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.update_set.remote.check_host*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	비즈니스 논리
보안 위험	• 심각도 점수: 6.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 속성을 권장 값인 **true** 로 설정하지 않으면 악의적인 행위자가 내부 포트 검사를 사용하여 무단 데이터에 액세스할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132 원격 인스턴스 정의

커뮤니케이션

이 제어는 강력한 알고리즘과 암호를 사용하여 적절한 암호화를 보장합니다. 여기에는 클라이언트 연결에 권장되는 버전의 TLS 사용, 강력한 암호 도구 모음 사용, 신뢰할 수 있는 인증서 및 서명된 인증서 사용, 구성 요소 간 연결 암호화 및 연결 실패 로깅이 포함됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인증서 신뢰 적용**[Security Center** 1.3에서 업데이트 되고 2.0에서 제거됨**]**

기본적으로 속성은 *com.glide.communications.trustmanager_trust_all***false**로 설정됩니다. Now Platform JVM 인증서 저장소에 대해 확인할 수 있는 유일한 신뢰 인증서입니다. 자체 서명 및 엔터프라이즈 서명 인증서는 신뢰할 수 없습니다.

주: 이러한 속성의 값은 변경 후 변경할 수 없습니다(되돌릴 수 없음). 보안상의 이유로 이 속성 값을 변경하지 마십시오. 추가 질문이 있는 경우 로 문의하십시오 고객 서비스 및 지원.

추가 정보

속성	설명
속성 이름	*com.glide.communications.trustmanager_trust_all*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	커뮤니케이션
목적	발신 요청에 대해 인증서 확인을 적용합니다.
권장 값	거짓
보안 위험 등급	6.6
기능적 영향	이렇게 정정하면 인증서 CA(인증 기관) 필드에 엄격한 유효성 검사가 적용됩니다. 신뢰할 수 있는 엔터티(CA)가 인증서를 발급한 경우 인스턴스는 나중에 사용할 수 있도록 인증서를 수락합니다.
보안 위험	(중간) 기밀성 및 무결성을 위해 애플리케이션은 트랜잭션 작업에 인증서를 사용하기 전에 인증서의 CA를 확인해야 합니다.
참조	인증서 인증서 체인 및 호스트 이름 확인 [Security Center 1.3의 새로운 기능 및 2.0에서 업데이트됨]

사용되지 않는 **TLS** 버전 사용 안 함

사용되지 않는 TLS 버전을 비활성화하여 민감한 데이터의 손실 또는 유출을 방지합니다.

약한 TLS 1 및 TLS 1.1 프로토콜 버전을 통한 데이터 전송을 방지하기 위해 인스턴스가 다른 서버와 통신할 때 전송 계층 보안(TLS) 버전 1.2를 통한 통신에 대해서만 협상하는지 확인합니다.

TLS 버전 1.2 이상만 사용하려면 **com.glide.communications.disable.deprecated.tls** 를 예 로 설정합니다.

추가 정보

속성	설명
기술 구성 이름	com.glide.communications.disable.deprecated.tls
플러그인 적용 가능성	안 함
보안 위험	오래되고 지원되지 않는 TLS 버전을 사용하면 중요한 데이터가 손실되고 유출될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
CVSS(공통 취약성 평가 시스템) 점수	4.4
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	이 속성을 **true**로 설정하면 약한 TLS 1 또는 1.1 프로토콜이 필요한 안전하지 않은 이전 서버가 인스턴스와 통신할 수 없습니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	예
폴백 값	예
권장 값	예

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

아웃바운드 **SSLv2/SSLv3** 연결 사용 안 함**[Security Center** 1.3에서 업데이트됨**]**

REST 및 SOAP 요청과 같은 아웃바운드 연결을 만들 때 MID 서버가 TLS를 사용하도록 강제 실행하려면 이 *glide.outbound.sslv3.disabled*속성을 사용합니다. 일반적으로, 인스턴스의 아웃바운드 연결에 SSL 대신 TLS를 사용하도록 강제 적용됩니다.

추가 정보

속성	설명
속성 이름	*glide.outbound.sslv3.disabled*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	커뮤니케이션
목적	ServiceNow 인스턴스의 모든 아웃바운드 연결 중에 if TLS를 사용하도록 적용합니다.
권장 값	예
기본값	거짓 중요사항: 속성 값은 *glide.outbound.sslv3.disabled*안전한 재정의이며 변경 후에는 변경할 수 없습니다.
보안 위험 등급	6.5
기능적 영향	이렇게 정정하면 HTTPS에서 통신할 때 TLS 프로토콜 버전 사용이 적용됩니다. 인스턴스의 고객/사용자가 사용하고 있는 장치 중 TLS 통신을 지원하지 않는 장치가 있는 경우 서비스가 중단될 가능성이 있습니다.
보안 위험	(보통) SSL의 레거시 버전은 BEAST 및 SSL heart-bleed를 포함한 클라이언트 측 공격으로 인해 HTTP 보안 셸 구현에 사용될 때 안전하지 않은 것으로 입증되었습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

활성 **SAML** 구성에 데모 인증서 사용 금지 **[Security Center** 1.5에서 업데이트됨〕

프로덕션 SAML 구성에서 데모 인증서를 사용할지 여부를 제어합니다.

ServiceNow에서 제공하는 데모 인증서는 알려진 암호가 있는 모든 인스턴스에서 공통적이므로 프로덕션 SAML 구성에 사용해서는 안 됩니다. 인증서 키 스토어를 사용하는 SAML 속성 중 하나가 활성(*require_signed_authnrequest*, *require_signed_logoutrequest*또는 *encrypt_assertion*)인 경우 데모 데이터를 사용하면 안 됩니다. 데모 데이터는 모든 인스턴스 간에 공유되므로 공유 인증서로 서명된 요청의 무결성이 보장되지 않습니다. 따라서 IDP에서 암호화한 모든 메시지는 가로채면 악의적인 행위자가 해독할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.sso.saml2.keystore*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	사용자 지정 키 스토어 sys_id
기본값	빈 문자열
범주	커뮤니케이션
보안 위험	• 심각도 점수: 3.9 • CVSS 점수: 낮음
의존성 및 필수 구성요소	안 함

네트워크 오류에 **OCSP** 검사 강제 적용 **[Security Center** 1.3의 새로운 기능 및 2.0에서 업데이트됨〕

악의적인 행위자가 OCSP(온라인 인증서 상태 프로토콜) 검사를 바이패스하지 못하도록 속성을 구성하는 *com.glide.communications.httpclient.ocsp_allow_network_error*방법을 알아봅니다.

*com.glide.communications.httpclient.ocsp_allow_network_error*권장 값인 false로 설정되지 않고 OCSP(온라인 인증 상태 프로토콜) 검사에서 네트워크 오류(예: 시간 초과 또는 해지 정보를 가져오는 문제)가 발생하면 OCSP 보안 검사를 바이패스하고 성공한 것으로 간주합니다. 이렇게 하면 해지된 인증서를 가진 공격자가 웹의 기반이 되는 PKI(공개 키 인프라) 및 디지털 인증서 신뢰를 깨뜨릴 수 있습니다. 해지된 인증서의 사용은 서버가 동기화되지 않은 경우가 아닌 한 악의적인 활동의 지표가 되는 경우가 많습니다.

속성이 *com.glide.communications.httpclient.ocsp_allow_network_error*존재하고 false로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다.

추가 정보

속성	설명
구성 이름	*com.glide.communications.httpclient.ocsp_allow_network_e*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	부울
권장 값	거짓
기본값	예
범주	커뮤니케이션
보안 위험	• 심각도 점수: 5.9 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 아니오로 설정하지 않으면 잘못된 액터가 OCSP 보안 검사를 바이패스할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성은 연결 또는 시간 초과 오류 발생 시 AIA(발급자 정보 접근) OCSP(온라인 인증 상태 프로토콜) URI에 대한 요청이 통과 또는 실패 결과를 초래하는지 여부를 판별합니다. false로 설정하면 제공된 서버 인증서의 해지 상태를 확인할 수 없으며 해당 엔드포인트와의 통신이 실패합니다. 속성이 기본값인 true로 설정된 경우 네트워크 오류가 발생하면 인증서는 해지 관점에서 유효한 것으로 처리됩니다.

인증서 체인 및 호스트 이름 확인 **[Security Center** 1.3의 새로운 기능 및 2.0에서 업데이트됨]

com.glide.communications.httpclient.verify_hostname 인증 검증 프로세스가 실행되도록 하여 메시지 가로채기(man-in-the-middle) 공격을 방지하도록 속성을 구성합니다.

Glide 속성이 *com.glide.communications.httpclient.verify_hostname* 보안 값 true로 설정되지 않은 경우 ServiceNow 인스턴스에서 시작된 TLS 연결 중에 원격 호스트가 제공하는 호스트 이름 및 인증서 체인의 유효성이 확인되지 않습니다. 이로 인해 TLS 연결의 보안이 손상되고 두 당사자 간의 통신을 가로채는 중간자 공격이 허용될 수 있습니다. 이로 인해 민감한 데이터가 공개될 수 있습니다.

추가 정보

속성	설명
구성 이름	*com.glide.communications.httpclient.verify_hostname*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	커뮤니케이션
보안 위험	• 심각도 점수: 높음 • CVSS 점수: 7.4

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	• 보안 위험 상세 정보: 권장 값인 true로 설정하지 *com.glide.communications.httpclient.verify_hostname* 않으면 인스턴스가 메시지 가로채기(man-in-the-middle) 공격에 취약해질 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	원격 SSL(Secure Socket Layer) 호스트가 제공하는 호스트 이름 및 인증서 체인을 확인합니다. MITM(중간자) 공격으로부터 보호하려면 이 속성을 예로 설정합니다. 주: 이 속성은 , 속성을 재정의합니다 *com.glide.communications.trustmanager_trust_all*.

인증서 해지 확인 [Security Center 1.3의 새로운 기능]

이 *com.glide.communications.httpclient.verify_revoked_certificate* 속성은 TLS(전송 계층 보안) 핸드셰이크 중 인증서 해지를 검사하여 보안 검사가 바이패스되지 않도록 합니다.

권장 값인 **true**로 설정되지 않은 경우 *com.glide.communications.httpclient.verify_revoked_certificate* TLS 핸드셰이크 중에 인증서 해지가 확인되지 않습니다. TLS는 인터넷을 통해 전송되는 데이터를 암호화하여 악의적인 행위자가 암호 또는 신용 카드 번호와 같은 민감한 정보를 볼 수 없도록 합니다. TLS 핸드셰이크를 우회하는 것은 해지된 인증서를 가진 공격자가 유효한 인증서 제공을 무시하고 PKI(공개 키 인프라) 및 디지털 인증서 신뢰를 깨뜨릴 수 있기 때문에 보안 위험이 있습니다.

추가 정보

속성	설명
구성 이름	*com.glide.communications.httpclient.verify_revoked_certi*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	커뮤니케이션
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 권장 값인 true로 설정하지 *com.glide.communications.httpclient.verify_revoked_cert* 않으면 TLS 핸드셰이크 중에 인증서 해지가 확인되지 않습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	TLS(전송 계층 보안) 세션이 인증된 엔드포인트로 시작되도록 하려면 이 속성을 true로 설정해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	이 속성이 false로 설정되면 인증서가 검사되지 않으므로 인스턴스의 보안이 손상될 수 있습니다.

구성

구성 범주는 애플리케이션에 보안 빌드 환경과 강화된 외부 공급업체 라이브러리 구성요소가 있는지 확인합니다. 특히 빌드 및 배포 파이프라인을 반복할 수 있도록 하고 자동화된 테스트를 포함하며 알려진 보안 문제가 배포되는 것을 방지합니다. 여기에는 종속성을 최신 상태로 유지하고 알려진 취약성으로부터 보호하는 것이 포함됩니다.

자동 콘텐츠 유형 설정 옵션**[Security Center** 1.3.3에서 제거됨〕

MIME 혼선 공격을 방지하기 위해 인스턴스에서 콘텐츠 유형 옵션 자동 설정 속성을 구성합니다.

이 속성을 사용하여 X-Content-Type-Options 응답 HTTP 헤더를 제어합니다. X-Content-Type-Options 응답 HTTP 헤더는 Content-Type 헤더에 광고되는 MIME 유형을 따라야 함을 나타내기 위해 서버에서 사용됩니다. 이 속성이 false로 설정된 경우 공격자가 MIME 혼동 공격을 수행할 수 있습니다. if true로 설정되면이 헤더는 브라우저가 파일을 HTTP 헤더의 콘텐츠 유형 이외의 것으로 해석하지 못하게합니다.

⚠ 경고: 이 속성의 값은 DB 재정의가 없습니다. 변경하거나 재정의할 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.security.header.auto_set_x_content_type_options*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	구성
보안 위험	• 심각도 점수: 7.3 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 **false** 로 설정하면 공격자가 MIME 혼동 공격을 수행할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	시스템 속성 추가

Cache-Control HTTP 헤더 값 **[Security Center** 1.3에서 업데이트되고 1.5에서 제거됨〕

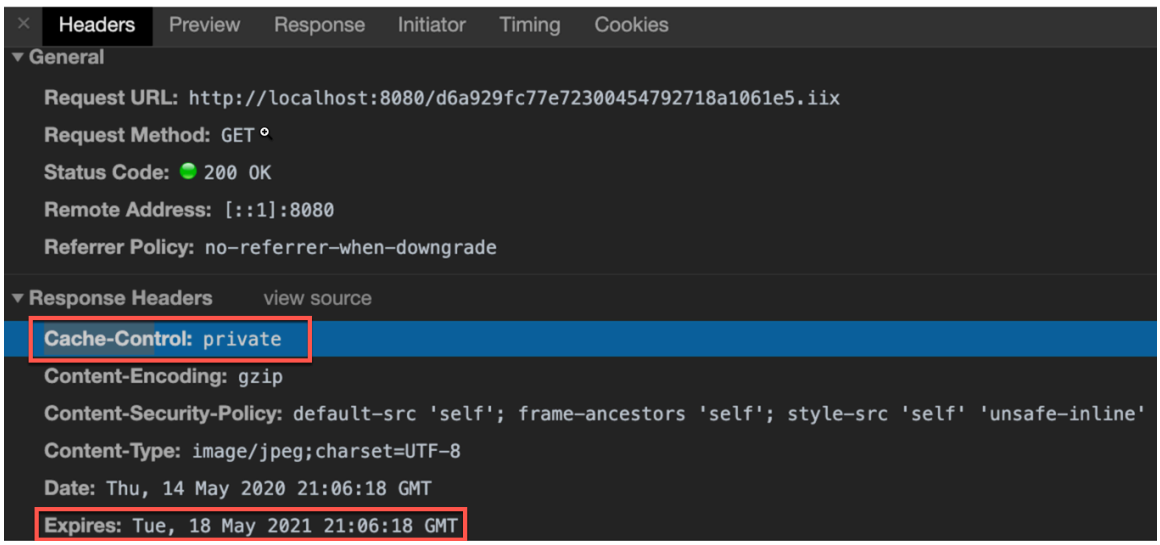
이 *glide.http.cache_control* 속성을 사용하여 페이지에 대한 정적 컨텐츠 데이터를 요청할 때 전송하는 HTTP 응답 헤더 Now Platform 에서 기본 cache-control 값을 설정합니다. 정적 콘텐츠의 예로는 페이지에 대해 내부에서 렌더링된 이미지, CSS 및 JavaScript가 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 *glide.http.cache_control* 속성은 HTTP 응답 헤더의 기본 Cache-Control 값을 **private** 또는 **public**으로 설정합니다. 기본값은 **private**입니다.

값	설명
개인	정적 콘텐츠는 브라우저(클라이언트) 수준에서 캐시할 수 있지만 프록시 서버 수준에서는 캐시할 수 없습니다.
공개	정적 콘텐츠는 브라우저(클라이언트) 수준과 프록시 서버 수준에서 캐시할 수 있습니다.

HTTP 응답 헤더의 Expires 값은 정적 컨텐츠가 만료되는 시기를 제어하며 기본값은 369일입니다. 기본값을 수동으로 재정의하려면 이 *glide.http.expire.days* 속성을 사용합니다.



주: HTTP 응답 헤더에서 *glide.http.cache* Cache-Control 및 Expires 값의 설정을 활성화할지 또는 비활성화할지 여부를 지정하는 속성을 사용할 수 있습니다. 기본값은 **true**이며 다음을 설정할 수 있습니다.

- 속성을 사용하는 Cache-Control 값 기본값입니다 *glide.http.cache_control*.
- 만료값 기본값(속성 사용).*glide.http.expire.days*

추가 정보

속성	설명
속성 이름	*glide.http.cache_control*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	구성
목적	정적 콘텐츠에 대한 Cache-Control HTTP 응답 헤더 값을 구성하기 위해
권장 값	개인
기본값	개인
보안 위험 등급	4.3
기능적 영향	HTTP 응답 헤더에서 기본 Cache-Control 값을 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	(높음) 이 속성을 **public**으로 설정하면 CDN/프록시가 있는 인스턴스가 정적 콘텐츠를 캐시하고 인증 없이 렌더링할 수 있습니다. • **private** 은 CDN/프록시 설정이 있는 인스턴스에 더 적합한 설정입니다. • 인스턴스에 CDN/프록시 설정이 없는 경우 두 값 모두 괜찮습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

채팅 서버 디버깅 사용 안 함

이 속성을 구성하여 인스턴스의 시스템 로그를 활성화하거나 비활성화합니다.

이*glide.cs.debug*속성을 사용하여 인스턴스가 시스템 로그를 처리하는 방법을 관리합니다. 속성이 권장 값인 **false**로 설정된 경우 시스템 로그가 활성화되지 않습니다. **true**로 설정하면 시스템 로그가 활성화됩니다. 문제를 해결하려는 경우에만 속성을 **true** 로 설정하고 완료되면 비활성화합니다. 시스템 로그를 사용하도록 설정하면 많은 메시지가 생성되어 시스템 로그에 과부하가 걸릴 수 있습니다. 로그 메시지가 실수로 중요한 정보를 노출할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.cs.debug*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	구성
보안 위험	• 심각도 점수: 2.3 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 시스템 로그를 활성화하면 많은 메시지가 생성되어 실수로 중요한 정보를 노출하는 로그 메시지로 시스템에 과부하가 걸릴 수 있습니다.
의존성 및 필수 구성요소	안 함

레거시 **JQuery UI** 사용 사용 안 함

레거시 JQuery UI 사용을 사용하지 않도록 설정하여 패치되지 않은 취약성이 라이브러리에 발생하지 않도록 합니다.

라이브러리에 패치되지 않은 취약점을 발생시키는 사전 패치된 이전 JQuery UI 버전의 사용을 방지합니다. 이전 버전을 사용하면 오래된 JQuery UI 라이브러리 버전에서 발견된 취약성에 대한 공격으로 인해 보안 위험이 발생할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이전 사전 패치된 JQuery UI 버전이 사용되지 않도록 **glide.jquery_ui.legacy** 시스템 속성이 **false** 로 설정되어 있는지 확인합니다. 이 시스템 속성은 조직이 패치되지 않은 버전에 의존하여 사용자 지정 구현을 실행하는 경우 페일세이프입니다.

추가 정보

속성	설명
기술 구성 이름	glide.jquery_ui.레거시
플러그인 적용 가능성	안 함
보안 위험	이전 사전 패치된 JQuery UI 버전이 사용되지 않도록 하면 라이브러리에 패치되지 않은 취약점이 발생할 수 있습니다.
CVSS(공통 취약성 평가 시스템) 점수	3.9
CVSS(공통 취약성 평가 시스템) 등급	낮음
기능적 영향	이 시스템 속성은 조직이 패치되지 않은 버전에 의존하여 사용자 지정 구현을 실행하는 경우 페일세이프입니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	거짓
폴백 값	예
권장 값	거짓

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

잠긴 양식 요소 디버깅 사용 안 함

에 대한 *glide.security.explain.write.locks*설명은 다음과 같습니다.

잠긴 양식 요소의 설명이 표시되지 않도록 하려면 권장 값인 아니오로 설정하십시오*glide.security.explain.write.locks*. 잠긴 폼 팩터에 대한 설명을 표시하려면 값을 **true** 로 설정합니다.

추가 정보

속성	설명
속성 이름	*glide.security.explain.write.locks*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	구성
목적	다른 속성에 의존하지 않고 SecurityDebugger의 표시 동작을 제한합니다.
권장 값	거짓
기본값	거짓
구성 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	(낮음) 잠긴 양식 요소에 설명이 표시되지 않습니다. 이렇게 하면 보안 디버거에서 제공하는 정보가 줄어들기 때문에 응용 프로그램의 보안이 약간 더 높아집니다.
보안 위험 등급	3.5

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

MultiSSO 디버깅 사용 안 함[Security Center 1.3 및 1.5에서 업데이트됨]

이 *glide.authenticate.multisso.debug* 속성은 다중 SSO에 대한 디버그 로깅을 제어합니다.

추가 정보

속성	설명
속성 이름	*glide.authenticate.multisso.debug*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	구성
목적	다중 SSO 디버그를 비활성화합니다.
권장 값	거짓
기본값	거짓
구성 유형	부울
보안 위험	(높음) 속성을 권장 값인 "아니오"로 설정합니다. 그렇지 않으면 MultiSSO 디버그가 활성화되어 의도하지 않은 민감한 정보가 유출될 수 있습니다.
보안 위험 등급	4.0
참조	복수 제공자 SSO 속성, 테이블 및 스크립트

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

대상 복제 사용 안 함[Security Center 1.3의 새로운 기능]

glide.db.clone.allow_clone_target 인스턴스가 복제 대상으로 사용되지 않도록 속성을 구성합니다.

glide.db.clone.allow_clone_target 시스템 속성을 **false**로 설정하여 인스턴스가 클론 대상으로 사용되지 않도록 보호합니다. 시스템 클론은 데이터베이스의 모든 것을 소스 인스턴스에서 대상 인스턴스로 복사합니다. 대상 인스턴스의 인스턴스 데이터베이스가 복제 프로세스에서 덮어쓰여져 데이터 손실 및 데이터 무결성 부족으로 이어지기 때문에 보안상 위험합니다.

인스턴스를 클론 대상으로 선택하지 않으려면 **glide.db.clone.allow_clone_target** 시스템 속성을 **false** 로 설정합니다.

추가 정보

속성	설명
구성 이름	*glide.db.clone.allow_clone_target*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	예
범주	구성
보안 위험	• 심각도 점수: 5.9 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값인 아니오로 설정하지 않으면 인스턴스가 클론 대상으로 사용될 수 있습니다. 이는 복제 프로세스에서 인스턴스 데이터베이스를 덮어쓸 수 있기 때문에 보안상 위험합니다.
의존성 및 필수 구성요소	안 함
참조	• 시스템 클론 • 클론 대상을 작성
기능적 영향	이 속성은 프로덕션 인스턴스가 클론되는 것을 방지하는 추가 보호 기능을 제공합니다. 프로덕션 인스턴스의 기본값은 false이고 dev 또는 qa와 같은 하위 프로덕션 인스턴스의 기본값은 true입니다. 인스턴스를 클론 대상으로 사용하려면 이 속성을 예로 설정합니다.

SOAP 오류 스택 추적 표시 사용 안 함

인스턴스에 스택 추적이 표시되는 방식을 관리합니다.

이 *glide.soapfault.display_stack_trace*속성을 사용하여 인스턴스에서 스택 추적을 관리합니다. 이 속성이 **false**로 구성되면 중요한 정보가 유출될 수 있습니다. **true**로 설정하면 스택 추적이 표시되지 않습니다.

추가 정보

속성	설명
구성 이름	*glide.soapfault.display_stack_trace*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	구성

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하면 스택 추적에서 중요한 정보가 노출될 수 있습니다.
의존성 및 필수 구성요소	안 함

성능 모니터링 액세스 제한 **[Security Center** 1.3에서 업데이트됨〕

이 *glide.security.diag_txns_acl* 속성을 사용하여 인증되지 않은 연결에서 stats.do, threads.do, thread_pool_stats 및 replication.do 액세스를 제어합니다.

이 속성을 **true**로 설정하면 속성은 *glide.security.diag_txns_acl* 관리자 계정에서 다음 항목에만 액세스할 수 있도록 허용합니다.

- 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

이 설정을 활성화하지 않아도 인증되지 않은 연결에서 이러한 자원에 액세스할 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.security.diag_txns_acl*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	구성
목적	구성 페이지에 대한 접근을 관리자 계정으로만 제한
권장 값	예
기본값	예
보안 위험 등급	5.3
기능적 영향	이렇게 정정하면 로깅 및 문제 해결을 위해 관리자 계정만 애플리케이션에 민감한 데이터에 액세스할 수 있게 됩니다.
보안 위험	(보통) 서버 세부 정보, 스레드 및 서버에서 실행된 프로세스와 같은 중요한 데이터는 적절한 권한 없이 최종 사용자에게 표시되거나 액세스되어서는 안 됩니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

업데이트된 버전의 **MultiSSO** 플러그인 사용〔보안 센터 **1.3** 및 **1.5**에서 업데이트됨〕

MultiSSO 플러그인 v2를 사용하고 있으며 보안 취약성을 줄이기 위해 true로 설정되어 있는지 확인합니다.

인스턴스에서 다중 SSO 플러그인이 활성화된 경우 v2 버전이 활성화되어 있는지 확인하여 보안 취약성을 줄입니다. 최신 버전은 보안을 강화하고 어설션 암호화 지원 및 IDP 시작 단일 로그아웃

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

(SLO)과 같은 더 많은 기능을 제공합니다. 최신 버전을 사용할 수 없는 경우 새 보안 기능을 사용할 수 없으며 인스턴스는 더 이상 사용되지 않는 플러그인을 사용할 위험이 있습니다.

KB0756504 의 단계에 따라 최신 버전으로 업그레이드합니다. 이 프로세스에는 커스터마이제이션 관련 변경 내용을 확인하고 마이그레이션한 후 버전을 업그레이드하는 작업이 포함됩니다. 완료되면 **glide.authenticate.multissov2_feature.enabled** 시스템 속성이 자동으로 **true**로 설정됩니다.

추가 정보

속성	설명
구성 이름	glide.authenticate.multissov2_feature.활성화됨
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	구성
보안 위험	최신 버전이 활성화되어 있지 않으면 새 보안 기능을 사용할 수 없으며 인스턴스가 더 이상 사용되지 않는 플러그인을 사용할 위험이 있습니다.
의존성 및 필수 구성요소	안 함
참조	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

보안 참조 정책 적용**[Security Center** 1.3의 새로운 기능〕

이 *com.glide.security.referrerpolicy* 속성을 사용하여 Referrer-Policy HTTP 헤더가 데이터 유출을 방지하기 위해 각 ServiceNow® 페이지에 적절한 수준의 데이터를 전송하도록 합니다.

com.glide.security.referrerpolicy 속성을 default로 설정하면 Referrer-Policy HTTP 헤더가 요청 페이지에 맞게 Now Platform® 특별히 조정된 적절한 수준의 정보를 사용하여 관리됩니다. 이렇게 하면 경로 및 쿼리 문자열과 같은 전체 URL의 다른 부분에서 액세스할 수 있는 무단 데이터 유출을 방지할 수 있습니다.

추가 정보

속성	설명
구성 이름	*com.glide.security.referrerpolicy*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	default
기본값	기본값
범주	구성

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 권한이 없는 데이터의 유출을 방지하기 위해 속성이 기본값으로 설정되어 있는지 *com.glide.security.referrerpolicy* 확인합니다.
의존성 및 필수 구성요소	안 함
참조	referrer-policy
기능적 영향	이 속성은 페이지에서 요청을 보낼 때 레퍼러 헤더를 통해 전송되는 정보의 양을 제어합니다. • 기본값: 인스턴스가 참조자 헤더를 처리합니다. • same-origin: 인스턴스/동일 도메인 내에서 전체 리퍼러 URL을 전송하고 외부 오리진에는 리퍼러 없음 • origin: 원본 내부 및 외부에서 리퍼러로 원본만 전송합니다. • origin-when-cross-origin: 인스턴스/동일 도메인 내에서 전체 리퍼러 URL과 원본 외부의 원본만 전송

x-frame-options 구현: SAMEORIGIN 보안 헤더 [Security Center 1.3에서 업데이트됨]

이 *glide.set_x_frame_options* 속성을 사용하여 모든 UI 페이지에 대해 X-Frame-Options 응답 헤더를 SAMEORIGIN으로 설정합니다.

X-Frame-Options HTTP 응답 헤더를 사용하여 브라우저에서 또는 로 페이지를 `<frame><iframe>`렌더링하도록 허용해야 하는지 여부를 나타냅니다. 사이트는 이 기능을 사용하여 콘텐츠가 다른 사이트에 포함되지 않도록 함으로써 클릭재킹 공격을 방지할 수 있습니다. 공격자는 페이지를 자신의 페이지에 삽입하고 페이지 요소가 악의적으로 작동하도록 할 수 있습니다. 최종 사용자는 페이지가 귀하의 페이지와 유사하기 때문에 페이지가 합법적이라고 생각할 수 있습니다. 최종 사용자는 악성 스크립트나 요소를 실행하기 위해서만 평소와 같이 요소를 클릭할 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.set_x_frame_options*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	구성
목적	ClickJacking 공격을 완화합니다.
권장 값	예
기본값	예
보안 위험 등급	5.9
기능적 영향	이렇게 정정하면 타사 애플리케이션에서 애플리케이션을 iFrame 형태로 렌더링 Now Platform 하는 것에 제한이

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	적용됩니다. 이러한 통합이 있는 경우 애플리케이션은 사용자 지정된 외부 공급업체 앱에서 렌더링되지 않습니다.
보안 위험	(중간) 동일 원본 정책을 사용하면 도메인이 다른 도메인에서 스크립트나 자원을 검색하지 못하도록 제한할 수 있습니다. 모든 최신 브라우저는 이 기능을 지원합니다. 정책은 프로토콜, 포트 및 호스트를 기반으로 연결의 유효성을 검사합니다. CORS(교차 원본 요청)는 헤더 값의 일부로 명시적으로 언급된 경우 다른 도메인의 자원/스크립트에 액세스할 수 있도록 하는 동일 원본 정책의 수정 사항입니다. • 이 경우 X-Frame-Options 헤더는 타사 웹 사이트에서 애플리케이션을 렌더링할 수 있는지 여부를 Now Platform 제어합니다. • 속성 값이 **SAMEORIGIN** 으로 설정되면 렌더링이 발생하지 않으므로 민감한 노출이 줄어듭니다.
참조	사용 가능한 시스템 속성 iFrame 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

서비스 카탈로그 항목 추가 페이지에 액세스하려면 쓰기 권한 필요**[Security Center 1.3의 새로운 기능]**

glide.sc.request.add_item_write_access 이 속성을 사용하여 카탈로그 항목에 대해 무단 작업이 수행되지 않도록 합니다.

추가 정보

속성	설명
구성 이름	*glide.sc.request.add_item_write_access*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	구성
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: *glide.sc.request.add_item_write_access* 속성이 false로 설정되면 로그인한 모든 사용자가 카탈로그 항목 추가 UI 페이지에 액세스할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	이로 인해 카탈로그 항목에 대해 무단 작업이 수행될 수 있습니다. 이 보안 위험을 정정하려면 이 속성을 true로 설정합니다.
의존성 및 필수 구성요소	안 함
기능적 영향	속성이 true이면 사용자는 UI 페이지의 컨텍스트에서 기록에 대한 쓰기 권한이 있어야 합니다.

외부 공급업체 웹 사이트 포함을 방지하기 위해 **Xframe** 옵션 설정 **[Security Center** 1.3에서 업데이트됨]

웹 애플리케이션의 컨텐츠가 외부 공급업체 사이트에 포함되지 않도록 하려면 이 속성을 구성합니다.

권장 값인 DENY 또는 SAMEORIGIN으로 설정되지 않은 경우 *com.glide.cs.embed.xframe_options* 웹 애플리케이션의 콘텐츠는 ALLOW-FROM URI를 사용하여 타사 사이트에 포함될 수 있습니다. 신뢰할 수 없는 타사 사이트를 허용하면 클릭재킹과 같은 공격이 가능해질 수 있습니다.

추가 정보

속성	설명
구성 이름	*com.glide.cs.embed.xframe_options*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	sameorigin
기본값	sameorigin
범주	구성
보안 위험	• 심각도 점수: 3.1 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 권장 값으로 설정하지 않으면 웹 애플리케이션의 콘텐츠가 타사 사이트에 포함되어 클릭재킹과 같은 공격을 사용할 수 있습니다.
의존성 및 필수 구성요소	안 함

데이터 보호

데이터 보호 범주는 데이터의 기밀성, 무결성 및 가용성(CIA) 요소를 다룹니다.

CIA 구성요소는 다음과 같습니다.

- 기밀성: 데이터는 전송 중 및 저장 중 무단 액세스로부터 보호됩니다.
- 무결성: 데이터는 무단 생성, 삭제 또는 변경으로부터 보호됩니다.
- 가용성: 필요한 경우 데이터에 액세스할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

내용 저장하기 제거

로그인 정보가 캐시되지 않도록 하려면 이 *glide.ui.forgetme* 속성을 사용하여 로그인 페이지에서 사용자 기억 확인란을 제거합니다.

추가 정보

속성	설명
속성 이름	*glide.ui.forgetme*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	데이터 보호
목적	인증 정보가 캐시되지 않도록 합니다.
보안 위험 등급	3.5
권장 값	예
기본값	예
기능적 영향	이렇게 정정하면 세션이 만료될 때 인스턴스에서 자동으로 로그아웃하는 방식으로 사용자 경험을 변경합니다. 세션 만료는 에 사용자 세션 관리 설명된 대로 시스템 속성에 설정된 값에 따라서만 달라집니다.
보안 위험	(낮음) 로그인 시 메일 주소 저장 확인란을 선택하면 추가 쿠키가 사용자의 컴퓨터에 저장됩니다. • 그 목적은 로그인한 사용자의 후속 방문을 위해 세션을 자동으로 다시 설정하는 것입니다. • 사용자가 의도적으로 로그아웃할 때까지 사용자 세션이 활성 상태로 유지될 수 있으므로 보안 위험이 있습니다. 이 시나리오의 공격 가능성은 최종 사용자가 브라우저를 방치했거나 다른 공격으로 인해 손상된 경우 증가합니다.
참조	메일 주소 저장 확인란 제거

시스템 속성 추가 또는 생성에 대한 자세한 내용은 시스템 속성 추가

모바일 애플리케이션을 백그라운드로 지정할 때 붙여 넣기 보드 지우기 필요 **[Security Center** 1.3의 새로운 기능 및 1.5에서 업데이트됨〕

이 *glide.sg.clear_pasteboard_when_backgrounded* 속성은 앱이 백그라운드 모드가 된 후 ServiceNow 모바일 앱에서 복사한 텍스트가 클립보드 및 붙여넣기 보드에 보관되는지 여부를 제어합니다. 권장 값인 true로 설정되지 않은 경우 중요한 정보가 Android 또는 iOS 클립보드에 공개되어 디바이스의 다른 애플리케이션에 노출될 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.sg.clear_pasteboard_when_backgrounded*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	예
기본값	거짓
범주	데이터 보호
보안 위험	• 심각도 점수: 3.5 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 권장 값인 true로 설정하지 않으면 중요한 정보가 Android 또는 iOS 클립보드에 공개되어 디바이스의 다른 애플리케이션에 노출될 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성은 ServiceNow 앱이 백그라운드에서 실행되면 복사 및 붙여넣기 클립보드를 지웁니다.

개인 이메일에서 **HR** 케이스 업데이트 제한 **[Security Center** 1.3의 새로운 기능 및 1.5에서 업데이트됨**]**

이*sn_hr_core.restrict_guest_email* 속성을 사용하여 사용자가 개인 이메일로 HR 케이스에 회신할 수 있는지 여부를 제어합니다.

sn_hr_core.restrict_guest_email 속성이 true로 설정되지 않은 경우 사용자는 작업 메모에 포함할 HR 케이스를 참조하는 개인 계정에서 이메일을 보낼 수 있습니다. 이로 인해 개인 이메일이 손상되거나 불안정한 통신이 이루어지는 경우 사소한 기밀성 또는 무결성 문제가 발생할 수 있습니다. 관리자는 개인 이메일 계정에 액세스하는 사용자를 전적으로 신뢰할 수 없으므로 사용자가 개인 이메일에서 HR 케이스에 응답하는 기능을 제한할 수 있습니다.

추가 정보

속성	설명
구성 이름	*sn_hr_core.restrict_guest_email*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	데이터 보호
보안 위험	• 심각도 점수: 3.5 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 예로 설정하지 않으면 개인 이메일이 손상되거나 불안정한 통신이 이루어지는 경우 사소한 기밀성 또는 무결성 문제가 발생할 수 있습니다.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기능적 영향	이 속성은 개인 이메일 주소를 통한 회신으로 HR 케이스를 업데이트할지 여부를 통제합니다. true로 설정하면 개인 이메일을 통해 오는 모든 회신이 케이스 메모에 추가됩니다. false인 경우 케이스와 메모가 업데이트되지 않습니다.

OAuth 매개 변수를 POST 본문으로 제한 [Security Center 1.3의 새로운 기능]

이 *glide.oauth.allow.parameters.in.post.body.only* 속성은 인바운드 OAuth 인증의 액세스 토큰 수락을 제어합니다. 액세스 토큰은 중요하며 POST 요청 본문 내에 있는 경우에만 허용되어야 합니다.

추가 정보

속성	설명
구성 이름	*glide.oauth.allow.parameters.in.post.body.only*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	데이터 보호
보안 위험	• 심각도 점수: 4.2 • CVSS 점수: 중간 • 보안 위험 세부 정보: 권장 값인 true로 설정되지 않은 경우 *glide.oauth.allow.parameters.in.post.body.only* 액세스 토큰은 클라이언트 인프라 로그에 남아 해당 로그가 유출될 경우 계정 탈취로 이어질 수 있는 GET 요청 매개 변수에 있을 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	• OAuth 2.0 • OAuth 토큰 관리
기능적 영향	지원되는 모든 권한 유형에 대해 게시 본문 매개변수만 oauth_token.do 프로세서에 입력되도록 합니다.

오류 처리 및 로깅

오류 처리 및 로깅 범주는 이해 관계자에게 노출되는 로깅된 정보의 품질과 상세 정보를 다룹니다.

여기에는 로그 및 오류 메시지가 중요한 정보를 수집하지 않고 분류에 따라 데이터를 올바르게 보호하며 수명이 적절한지 확인하는 것이 포함됩니다. 또한 이 범주는 적절한 오류 처리와 관련이 있으며 보안에 영향을 미치는 처리되지 않은 예외에 대한 자세한 스택 추적과 같은 중요한 오류를 최종 사용자에게 공개하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트 샌드박스에서 낮은 권한 사용자에 대한 로거 사용 안 함**[Security Center 1.3에서 업데이트됨]**

샌드박스 환경에서 실행 중인 스크립트를 기록하는 Glide 시스템의 기능을 관리합니다.

이 *glide.security.sandbox_no_logging* 속성을 사용하여 샌드박스 환경에서 실행 중인 스크립트를 기록하는 Glide 시스템의 기능을 제어합니다. *glide.security.sandbox_no_logging* **false**로 설정되면 샌드박스 스크립트를 사용하여 권한이 낮은 사용자가 로깅을 사용할 수 있습니다. 이는 권한이 낮은 사용자가 로그를 삽입하여 악의적인 행위자가 공격을 난독 처리할 수 있기 때문에 잠재적인 보안 취약점입니다. 샌드박스 스크립트를 사용하는 권한이 낮은 사용자가 로깅 기능을 사용할 수 없도록 속성을 예 로 구성합니다.

추가 정보

속성	설명
구성 이름	*glide.security.sandbox_no_logging*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 2.2 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하면 권한이 낮은 사용자에 대한 로깅이 활성화되어 악의적인 액터가 공격을 난독 처리할 수 있습니다.
의존성 및 필수 구성요소	안 함

보안 쿠키 디버깅 사용 안 함

인스턴스의 쿠키와 관련된 로그 메시지를 관리합니다.

이*glide.secure_cookie.debug* 속성을 사용하여 쿠키와 관련된 로그 메시지를 관리합니다. 이 속성을 **false**로 설정하면 로그 메시지가 표시되지 않습니다. **true**로 설정하면 `SecureUserCookie` 및 `Cookie` 클래스의 메시지가 기록됩니다. 이로 인해 중요한 정보가 인스턴스에 노출될 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.secure_cookie.debug*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 4.2 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 예 로 구성하면 중요한 정보가 노출될 수 있습니다.
의존성 및 필수 구성요소	안 함

SQL 오류 메시지 사용 안 함 [Security Center 1.3 및 1.5에서 업데이트됨]

이 *glide.db.loguser* 속성을 사용하여 브라우저에서 SQL 오류 메시지가 렌더링되지 않도록 설정합니다.

권장 값인 false로 설정되지 않은 경우 *glide.db.loguser* 최종 사용자에게 중요한 서버 측 오류 메시지가 표시될 수 있습니다. 오류 메시지에는 스택 추적 및 데이터베이스 구조에 대한 정보가 포함될 수 있으며, 이러한 정보는 전제 조건이 있는 경우 공격자에게 성공적인 SQL 주입을 수행하는 데 필요한 지식을 제공할 수 있습니다. 심층 방어로서 이러한 오류 메시지는 최종 사용자에게 표시되지 않아야 합니다.

추가 정보

속성	설명
속성 이름	*glide.db.loguser*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	오류 처리 및 로깅
목적	SQL 오류 메시지가 브라우저에 표시되지 않도록 설정합니다.
유형	부울
권장 값	거짓
기본값	예
보안 위험 등급	3.1
기능적 영향	이렇게 정정하면 SQL 오류 메시지의 렌더링이 비활성화됩니다. 기능에는 영향을 주지 않습니다.
보안 위험	(중간) 공격자에게 도움이 될 수 있는 중요한 SQL 정보가 웹 페이지에 오류 메시지의 일부로 표시되어서는 안 됩니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

MID 감사 로그 사용[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]

MID 서버 명령 감사 로그는 명령 이름, 명령 해시, 사용된 자격 증명 이름 및 실행 상태와 같은 상세 정보를 기록합니다.

감사 로그를 활성화하면 ecc_agent_command_audit_log 테이블에 agent_security_admin 역할이 있는 사용자가 보거나 **Mid Server** > 명령 감사 로그.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MID 서버에서 실행하는 명령에 대한 감사를 설정하려면 MID 서버 속성 [ecc_agent_property] 테이블에서 예로 설정합니다 *mid.log.command_audit.enable*.

추가 정보

속성	설명
구성 이름	*mid.log.command_audit.enable*
구성 유형	MID 서버 속성 [ecc_agent_property] 기록
데이터 유형	부울
권장 값	예
기본값	거짓
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 2.2 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 보안 조사 시 인시던트 응답 팀은 이 테이블을 사용하여 MID 서버에서 실행되는 명령을 감사할 수 있습니다. 이 로그가 없으면 무단 계정 사용과 같은 상황에 대응하기에 충분한 세부 정보가 없을 수 있습니다.
의존성 및 필수 구성요소	안 함

보호된 테이블 플러그인 사용 **[Security Center** 1.3의 새로운 기능)

이 속성을 사용하여 더 높은 권한의 *com.glide.security.protected_table.enabled* 사용자가 로그 테이블을 변조하지 못하도록 합니다.

*com.glide.security.protected_table.enabled*속성을 예로 설정하면 인스턴스에서 더 높은 권한의 사용자가 로그 테이블을 변조하지 못하도록 보호된 테이블 플러그인이 사용됩니다. 이 속성이 **true**로 설정된 경우 다음 로그 테이블은 특별한 보호를 받습니다.

- syslog(DB 재정의 없음)
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- protected_table_configuration(DB 재정의 없음)

로그의 무결성은 고객 관리자가 인스턴스에서 악의적인 활동을 확인하는 데 중요합니다.

추가 정보

속성	설명
구성 이름	*com.glide.security.protected_table.enabled*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 4.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 권장 값인 예로 설정하지 않으면 인스턴스에서 권한이 높은 사용자가 로그 테이블을 변조할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	시스템 로그

모든 아웃바운드 **http** 요청 필드 기록**[Security Center** v1.3.2에서 제거됨〕

glide.outbound_http.security.log.allow.all.fields 중요한 아웃바운드 HTTP 필드가 일반 텍스트로 기록되지 않도록 속성을 아니오로 구성합니다.

이 속성이 권장 값인 **false**로 설정되지 않은 경우 중요한 아웃바운드 HTTP 필드가 일반 텍스트로 기록될 수 있습니다. 이렇게 하면 중요한 데이터 및 자격 증명이 포함된 아웃바운드 요청을 암호화되지 않은 일반 텍스트로 기록할 수 있고 권한이 낮은 사용자가 볼 수 있으므로 엔터프라이즈 네트워크의 보안 태세가 저하될 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.outbound_http.security.log.allow.all.fields*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	30
기본값	30
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 6.8 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하지 않으면 중요한 아웃바운드 필드가 일반 텍스트로 기록될 가능성이 높아져 보안 위험이 있습니다.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그 **html** 정리 **[Security Center** 2.0에서 제거됨]

HTML 위생 이벤트를 인스턴스에 기록할지 여부를 결정하는 속성을 구성합니다 *glide.html_sanitize.discarded_log.enable*.

이 속성을 권장 값인 **true**로 설정하지 않으면 HTML 정리 이벤트가 테이블에 기록 *sys_log* 되지 않습니다. 로깅이 부족하면 인스턴스 자동 보안 탐지 및 조사 기능에 부정적인 영향을 미칠 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.html_sanitize.discarded_log.enable*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 2.4 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 속성을 권장 값인 예로 설정하지 않으면 HTML 정리 이벤트가 테이블에 기록 *sys_log* 되지 않으므로 자동화된 보안 탐지 및 조사 역량에 영향을 줄 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	HTML 위생 검사 사용

세션 감사 이벤트 기록**[Security Center** 1.3의 새로운 기능 및 1.5에서 업데이트됨]

glide.authenticate.session_access.log_audit_event 속성을 예로 설정하면 테이블에 세션 감사 이벤트가 생성됩니다*sys_session_access_audit*.

Glide 속성이 *glide.authenticate.session_access.log_audit_event* 예로 설정되면 sys_session_access_audit 테이블에 세션 감사 이벤트가 생성됩니다. 악의적인 액터 조사를 지원하기 위해 세션에 액세스한 사람에 대한 정보를 기록하는 것이 베스트 프랙티스입니다. 로그되는 정보에는 사용자, 세션 ID(중요하지 않음), IP 주소, 역할 및 정책이 포함됩니다.

주: *glide.authenticate.session_access.log_audit_event* 시스템 속성은 제로 트러스트 액세스에만 해당됩니다. 자세한 내용은 제로 트러스트 액세스 문서를 참조하십시오.

추가 정보

속성	설명
구성 이름	*glide.authenticate.session_access.log_audit_event*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	예
기본값	예
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 6.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값인 예로 설정하지 않으면 이벤트가 기록되지 않습니다. 이렇게 하면 사이버 공격이 발생할 경우 악의적인 행위자를 찾을 수 없습니다.
의존성 및 필수 구성요소	안 함

사용자 가장 기록 **[Security Center 1.3** 및 2.0에서 업데이트됨]

사용자 가장 이벤트가 인스턴스에 기록되는지 여부를 제어하도록 구성합니다 *glide.sys.log_impersonation*.

이 속성을 권장 값인 **true**로 설정하지 않으면 사용자 사칭 이벤트가 더 이상 기록되지 않습니다. 로깅이 없으면 인스턴스의 자동화된 보안 탐지 및 조사 역량에 영향을 줄 수 있습니다. 속성이 *glide.sys.log_impersonation* 존재하고 true로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다.

추가 정보

속성	설명
구성 이름	*glide.sys.log_impersonation*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 6.4 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 예로 설정하지 않으면 사용자 가장 이벤트가 더 이상 기록되지 않으므로 인스턴스의 보안 탐지 및 조사 역량에 영향을 줄 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	사용자 가장 중

자세한 **HTTP** 요청 로깅 방지

자세한 HTTP 요청 로깅을 줄여 중요한 정보에 대한 액세스를 방지할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

권한 부여 헤더 또는 쿠키와 같은 중요한 정보에 대한 액세스를 방지할 수 있도록 아웃바운드 HTTP 요청에 대한 로깅 수준을 제어합니다. 이 정보는 요청된 자원에 액세스하기 위한 자격 증명처럼 사용할 수 있습니다.

이러한 요청에 대한 로깅 수준은 **glide.outbound_http_log.override** 및 **glide.outbound_http_log.override.level** 속성에 의해 제어됩니다. **glide.outbound_http_log.override**가 **true**로 설정되면 요청 및 응답에 대한 로그 수준은 **glide.outbound_http_log.override.level** 속성에 의해 제어됩니다. **glide.outbound_http_log.override.level**이 **all** 또는 **elevated**로 설정된 경우 요청 및 응답 헤더가 로깅됩니다.

glide.outbound_http_log.override를**false**로 설정하고 **glide.outbound_http_log.override.level**을 **basic**으로 설정합니다. 이러한 속성이 시스템 속성 [sys_properties] 테이블에 표시되지 않으면 기본적으로 보안 상태입니다.

추가 정보

속성	설명
기술 구성 이름	• glide.outbound_http_log.재정의 • glide.outbound_http_log.재정의.수준
플러그인 적용 가능성	안 함
보안 위험	자세한 정보 표시 설정으로 기록된 아웃바운드 HTTP 요청 헤더에는 권한 부여 헤더 또는 쿠키와 같은 중요한 정보가 포함될 수 있습니다. 이 정보는 요청된 자원에 액세스하기 위한 자격 증명처럼 사용할 수 있습니다. 아웃바운드 HTTP 로그 [sys_outbound_http_log] 테이블에 액세스할 수 있는 사용자는 이 정보를 볼 수 있습니다. 아웃바운드 요청의 유형에 따라 심각도가 달라집니다.
CVSS(공통 취약성 평가 시스템) 점수	5
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	**glide.outbound_http_log.override** 시스템 속성을 사용하면 아웃바운드 http 요청 로그 수준을 재정의할 수 있습니다. **False** 값은 기본적으로 로그 수준이 기본으로 설정됩니다. **glide.outbound_http_log.override**가 **true**로 설정된 경우 로깅 수준은 **glide.outbound_http_log.override.level** 속성 값에 의해 결정됩니다. 이 값은 기본, 상승 또는 모두일 수 있습니다. 3 개 모두 문자열 / 텍스트 기반 값입니다. 이 값 이외의 값은 **basic**으로 해석됩니다. 자세한 내용은 아웃바운드 로깅 구성 문서를 참조하십시오.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	• 부울 • 문자열
기본 시스템 값	• 거짓 • 〈공백〉
폴백 값	• 거짓 • 〈공백〉
권장 값	• 거짓 • 기본

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

가져오기 프로세서에 자세한 **SQL** 오류 메시지 끄기**[Security Center** 1.3에서 업데이트됨〕

자세한 SQL 오류 메시지를 표시할지 여부를 제어하려면 이 속성을 구성합니다.

속성이 **false**로 설정되면 중요한 정보가 유출될 수 있는 자세한 SQL 오류 메시지가 표시됩니다. 이를 방지하려면 속성을 **true** 로 설정하여 일반 메시지를 표시합니다.

추가 정보

속성	설명
구성 이름	*glide.import.error_message.generic*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	오류 처리 및 로깅
보안 위험	• 심각도 점수: 3.1 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 속성을 **false** 로 설정하면 자세한 SQL 메시지가 표시되어 정보 유출로 이어질 수 있습니다.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

파일 및 자원

파일 및 리소스 범주를 사용하면 애플리케이션이 신뢰할 수 없는 파일 데이터를 안전하게 처리하고 신뢰할 수 없는 원본의 신뢰할 수 없는 데이터를 적절한 위치에 제한된 권한으로 저장할 수 있습니다.

여기에는 크거나 예기치 않은 파일 형식을 통한 서비스 거부 방지, 파일 형식 유효성 검사 및 경로 통과 방지와 같은 제어가 포함됩니다.

감염된 파일 다운로드 사용 안 함**[Security Center 1.5** 및 2.0에서 업데이트됨〕

스택 추적을 인스턴스에 표시할지 여부를 제어하려면 이 속성을 관리합니다.

*com.glide.snap.infected_download_allowed*속성이 true로 설정되면 바이러스 백신 서비스가 다운되거나 연결할 수 없는 경우 사용자가 검사되지 않은 첨부 파일을 계속 다운로드할 수 있습니다. 이 상황에서는 사용자가 악성 파일을 다운로드할 위험에 노출될 수 있으므로 특히 장치에 다른 끝점 보호가 설치되어 있지 않은 경우 데스크톱이 감염될 위험이 있습니다.

속성이 *com.glide.snap.infected_download_allowed*false로 설정되어 있는지 확인합니다.

추가 정보

속성	설명
구성 이름	*com.glide.snap.infected_download_allowed*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	파일 및 자원
보안 위험	• 심각도 점수: 6.7 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값인 아니오로 설정하지 않으면 인스턴스가 악성 파일 다운로드에 노출될 수 있습니다.
의존성 및 필수 구성요소	안 함

전자 메일 스팸 점수 매기기 및 필터링 사용 **[Security Center** 1.3에서 업데이트됨〕

이메일 필터()*com.glide.email_filter*플러그인을 설치하여 인스턴스 내에 이메일 필터링을 설치합니다. 이 필터링은 기존 헤더를 식별하므로 연결된 헤더를 기반으로 이메일로 수행할 작업을 결정할 수 있습니다. 또는 false로 설정합니다 *com.glide.email_filter*.

이메일 서버를 통해 Now Platform 전송되는 모든 메시지는 스팸일 가능성이 평가됩니다.

주: 인스턴스에서 개인 이메일 서버를 사용하는 경우에는 이 주제가 적용되지 않습니다. 자세한 내용은 전자 메일 스팸 점수 매기기 및 필터링을 참조하십시오.

필수 구성요소

이 속성을 설정하기 전에 다음을 수행하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

glide.email.read.active 속성을 True로 설정합니다. 자세한 내용은 자체 POP3 서버 사용 사용을 참조하십시오.

추가 정보

속성	설명
플러그인 이름	com.glide.email_filter, glide.email.read.active
구성 유형	시스템 정의 > 플러그인
범주	파일 및 자원
목적	이메일 스팸을 방지하기 위해 필터링을 적용합니다.
권장 값	다음 중 하나입니다. • **glide.email.read.active** 속성을 **false**로 설정 • **glide.email.read.active** 속성을 **true**로 설정하고 이메일 필터(com.glide.email_filter) 플러그인을 활성화합니다. 활성
기본값	없음. 이는 Glide 속성이 아닌 플러그인이므로 기본값이 없습니다.
보안 위험 등급	8.1
기능적 영향	이메일은 스팸 점수 매기기의 일부로 인스턴스에서 필터링, 차단 또는 격리되지 않습니다. 점수만 매기고 인스턴스로 보냅니다. 모든 필터링은 이메일 필터 플러그인을 사용하여 인스턴스 내에서 수행됩니다.
보안 위험	(보통) 이메일 필터를 사용하면 관리자가 조건 작성기 또는 조건부 스크립트를 사용하여 알려진/알 수 없는 보낸 사람으로부터 받은 악성 수신 이메일을 무시할 시기를 지정할 수 있습니다.
참조	이메일 필터 https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

플러그인 활성화에 대한 자세한 내용은 다음 문서를 참조하십시오 플러그인 활성화 .

바이러스 스캔 사용

이 *com.glide.snap.enable_scan* 속성은 바이러스 백신 검사 기능을 활성화합니다.

바이러스 백신 검사를 사용하려면 권장 값인 **true**로 설정합니다*com.glide.snap.enable_scan*.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*com.glide.snap.enable_scan*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
구성 유형	시스템 속성(/sys_properties_list.do)
범주	파일 및 자원
목적	특정 인스턴스에서 바이러스 백신 검사를 사용하거나 사용하지 않도록 설정합니다.
권장 값	예
기본값	예
데이터 유형	부울
보안 위험	(높음) 바이러스 백신 검사는 인시던트, 문제, 스토리와 같은 시스템 기록에 파일 첨부 파일로 인해 발생할 수 있는 바이러스 감염으로부터 인스턴스를 보호하는 데 도움이 됩니다.
보안 위험 등급	7.7

정적 콘텐츠에서 다운로드 가능한 파일 형식 제한 **[Security Center** 1.3에서 업데이트됨]

이 *glide.ui.strict_customer_uploaded_static_content* 속성을 사용하여 파일 업로드 기능을 사용하여 업로드되었을 때 다운로드할 수 있는 파일 형식에 대한 제한을 활성화합니다.

이 속성을 속성과 함께 *glide.ui.strict_customer_uploaded_content_types* 사용하면 쉼표로 구분된 제한된 다운로드 가능한 파일 형식 목록이 만들어집니다.

⚠ 경고: 이 속성의 값은 DB 재정의가 없습니다. 변경하거나 재정의할 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.strict_customer_uploaded_static_content*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	파일 및 자원
목적	애플리케이션에서 안전한 파일 형식을 다운로드할 수 있도록 합니다.
권장 값	예
기본값	예
보안 위험 등급	3.1
기능적 영향	이렇게 정정하면 속성에 지정된 *glide.ui.strict_customer_uploaded_content_types* 값에 따라 파일 다운로드를 제한합니다.
보안 위험	(낮음) 신뢰할 수 없는 사용자 입력 소스에는 파일 다운로드 제한이 적용되어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

GraphQL 엔드포인트에 대한 교육 및 예측 흐름에서 첨부 파일 크기 제한[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]

이 *glide.platform_ml_di.max_attachment_size_graphql* 속성은 교육 또는 예측 플로우의 GraphQL 엔드포인트에서 첨부 파일을 반환하기 위해 허용되는 최대 크기 제한을 제어합니다.

추가 정보

속성	설명
구성 이름	*glide.platform_ml_di.max_attachment_size_graphql*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	5,242,880
기본값	5,242,880
범주	파일 및 자원
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성이 권장 값인 5,242,880 이하로 설정되지 않은 경우 큰 파일을 반환하면 DoS(서비스 거부)가 발생할 수 있습니다.
의존성 및 필수 구성요소	안 함

학습 및 예측 흐름에서 첨부 파일 크기 제한 [Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]

이 *glide.platform_ml_di.max_attachment_size* 속성은 교육 및 예측 플로우에서 첨부 파일을 반환하기 위해 허용되는 최대 크기 제한을 제어합니다.

추가 정보

속성	설명
구성 이름	*glide.platform_ml_di.max_attachment_size*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	4,000,000
기본값	4,000,000
범주	파일 및 자원
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 권장 값인 4,000,000개 이하로 설정하지 않은 경우

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	glide.platform_ml_di.max_attachment_size 큰 파일을 반환하면 DoS(서비스 거부) 공격이 발생할 수 있습니다.
의존성 및 필수 구성요소	안 함

HTTP 응답 본문 크기 제한[Security Center 1.3의 새로운 기능 및 1.5에서 업데이트됨]

glide.http.response.get_body.limit.enabled and *glide.http.response.get_body.limit* 속성을 *#### OutOfMemoryExceptions*로부터 인스턴스를 보호합니다.

glide.http.response.get_body.limit.enabled 및 **glide.http.response.get_body.limit** 시스템 속성을 사용하여 요청 응답 본문이 너무 커서 발생할 수 있는 `OutOfMemoryExceptions`를 방지합니다. 이러한 예외로 인해 DOS(서비스 거부) 공격뿐만 아니라 공격자가 인스턴스를 손상시키는 데 도움이 될 수 있는 기타 문제가 발생할 수 있습니다. 이러한 속성을 권장 값으로 설정하지 않으면 인스턴스가 OutOfMemoryExceptions 및 서비스 거부 공격에 취약해질 수 있습니다.

이러한 보안 취약성으로부터 인스턴스를 보호하려면 다음을 수행합니다.

- **glide.http.response.get_body.limit.enabled** 시스템 속성을 **true**로 설정합니다.
- **glide.http.response.get_body.limit** 시스템 속성이 524,288,000메가바이트(500MB) 이하로 설정되어 있는지 확인합니다.

추가 정보

속성	설명
구성 이름	• **glide.http.response.get_body.limit.enabled** • glide.http.response.get_body.제한
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	파일 및 자원
보안 위험	• 심각도 점수: 3.1 • 보안 위험 세부 정보: 이러한 속성을 권장 값으로 설정하지 않으면 인스턴스가 *OutOfMemoryExceptions* 및 서비스 거부 공격에 취약해질 수 있습니다.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기능적 영향	이 속성은 고객이 실수로 큰 파일을 메모리에 로드하여 *OutOfMemoryException* 이 발생할 가능성을 줄여줍니다.

이메일의 최대 첨부 파일 개수 제한

인스턴스에서 인바운드 이메일 첨부 파일의 개수를 구성합니다.

이*glide.email.inbound.max_attachment_count* 속성은 인스턴스에서 인바운드 이메일 첨부 파일의 최대 수를 제어합니다. 이 속성을 권장 값 **30** 이하로 설정하지 않으면 인바운드 이메일이 인스턴스 성능 저하를 일으킬 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.email.inbound.max_attachment_count*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	30
기본값	30
범주	파일 및 자원
보안 위험	• 심각도 점수: 5.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 속성 값을 30보다 크게 설정하면 성능 저하 문제가 발생할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	이메일 속성

허용된 첨부 파일 크기 최소화 **[Security Center** 1.3에서 업데이트됨]

업로드된 *com.glide.attachment.max_size* 첨부 파일에 허용되는 최대 크기(MB)를 제어하도록 속성을 구성합니다.

이 속성은 업로드된 첨부 파일의 최대 크기(MB)를 제어합니다. 이 속성이 권장 값인 **1024** 이하로 설정되지 않은 경우 플랫폼은 스토리지를 채우고 DoS(서비스 거부) 공격으로 이어질 수 있는 큰 파일을 수락할 수 있습니다.

주: 실제 첨부 파일 크기는 1024에 속성 값을 곱하여 계산됩니다. 속성 값이 **1024**이면 첨부 파일에 허용되는 최대 크기는 1GB입니다.

추가 정보

속성	설명
구성 이름	*com.glide.attachment.max_size*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	1024
기본값	4096
범주	파일 및 자원
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성이 **1024** 이하로 설정되지 않은 경우 플랫폼은 DoS 공격으로 이어질 수 있는 큰 파일을 수락할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	첨부 파일 제한 속성

허용된 **MIME** 하위 유형 설정**[Security Center** 2.0의 새로운 기능**]**

파일 형식이 MIME(Multipurpose Internet Mail Extensions) 형식 검사를 통과하지 않도록 속성을 보안 설정으로 구성하는 *glide.security.mime.type.allowed_child_types* 방법을 알아봅니다. 이렇게 하면 업로드된 파일에서 코드를 원격으로 실행할 위험이 줄어듭니다.

이 *glide.security.mime.type.allowed_child_types* 속성은 업로드된 파일 내의 데이터와 일치하지 않는 파일 확장자를 가질 수 있는 MIME 파일 유형을 정의합니다. 이렇게 하면 이러한 파일 형식이 MIME 형식 검사를 무시할 수 있습니다. 이 속성은 와 같이 *application/zip=application/java-archive*쉼표로 구분된 파일 형식 쌍의 목록을 허용합니다. 이 예제에서 속성이 이러한 값으로 설정된 경우 기술적으로 `.jar` 파일인 `.zip` 확장명을 가진 파일은 불일치에도 불구하고 MIME 형식 검사를 통과할 수 있습니다. 제대로 설정되지 않은 경우 이 바이패스는 업로드된 파일의 원격 코드 실행으로 이어질 수 있습니다. 따라서 유효한 사용 사례가 발생하지 않는 한 항상 빈 문자열("")로 설정해야 합니다. 예를 들어 특정 MIME 유형이 다른 파일 확장자로 허용되어야 하고 Tika 구성에 따라 유효한 경우 해당 키-값 쌍은 이 속성 값의 일부로 업데이트됩니다.

추가 정보

속성	설명
구성 이름	*glide.security.mime.type.allowed_child_types*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	""
기본값	""
범주	파일 및 자원

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 4.6 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 보안 값으로 설정하지 않으면 잘못된 구성의 파일이 업로드된 파일의 원격 코드 실행으로 이어질 수 있습니다.
의존성 및 필수 구성요소	예, 예로 설정될 경우 *glide.security.mime.type.detection.allow_child_types* 이 속성의 값을 사용하여 허용되는 MIME 하위 유형의 구성된 목록과 비교하여 유효성을 검사합니다.
기능적 영향	파일 확장자가 파일의 내용과 일치하지 않지만 의 *tika-mimetypes.xml*Tika 하위 유형 구성에 따라 유효한 MIME 유형을 지원하려면 .

AttachmentCreator SOAP Web Service에서 파일 **MIME** 형식 확인**[Security Center** 1.3의 새로운 기능 및 1.5에서 업데이트됨〕

이 *glide.attachment.enforce_security_validation* 속성은 MIME(Multipurpose Internet Mail Extensions) 파일의 유효성 검사 여부를 결정합니다.

첨부 파일에 대해 MIME 유형의 유효성을 검사하여 잘못된 파일 확장자를 사용하여 인스턴스에 위험한 파일이 업로드되는 것을 방지해야 합니다.

glide.attachment.enforce_security_validation 시스템 속성을 **true**로 설정합니다. **true**로 설정하면 파일이 올바른 파일 형식 확장자로 업로드됩니다.

추가 정보

속성	설명
구성 이름	*glide.attachment.enforce_security_validation*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	파일 및 자원
보안 위험	• 심각도 점수: 6.7 • CVSS 점수: 중간 • 보안 위험 세부정보: 속성이 false로 설정된 경우 업로드 중에 MIME 파일에 대한 유효성 검사가 수행되지 않습니다. 이렇게 하면 파일 확장자를 변경하여 악성 파일을 위장할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기능적 영향	업로드된 첨부 파일에서 MIME 형식 및 파일 확장명 확인을 실행하려면 이 강화 설정을 예로 설정합니다. 이 속성이 false로 설정된 경우 확인이 실행되지 않습니다. 이 속성은 기본적으로 true로 설정됩니다.

악성 코드

악성 코드 범주를 사용하면 코드에 취약성 및 원치 않는 기능이 없는지 확인하기 위해 최선을 다할 수 있습니다.

여기에는 악의적인 활동에 대한 안전하고 적절한 처리, 시간 기반 공격 없음, 신뢰할 수 없는 대상에 대한 아웃바운드 통신, 무단 또는 공격자 통제 코드가 포함되지 않는 것이 포함됩니다. 이 범주에는 애플리케이션 코드베이스의 감사 또는 외부 공급업체 라이브러리가 포함됩니다.

루트 또는 탈옥 모바일 장치 차단

탈옥된 장치의 무단 액세스를 방지하여 인스턴스를 보호합니다.

이 *glide.sg.allow_rooted_jailbroken_device* 속성을 사용하여 탈옥된 장치의 무단 액세스로부터 인스턴스를 보호합니다. 이 속성이 **false**로 설정되어 있는 동안 사용자가 모바일 앱을 사용하여 인스턴스에 인증하려고 하면 다음과 같은 경고가 표시됩니다. `# ### ### ### ### # ##### ##### # ### # ####. ServiceNow ##### ######.` 경고 메시지가 표시되는 동안 앱이 정지되며, 이 메시지를 해제하는 유일한 방법은 로그아웃을 선택하는 것입니다. 이 속성이 예 로 설정되면 사용자는 탈옥된 장치를 사용하여 인스턴스에 인증합니다.

추가 정보

속성	설명
구성 이름	*glide.sg.allow_rooted_jailbroken_device*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	악성 코드
보안 위험	• 심각도 점수: 4.5 • CVSS 점수: 중간 • 보안 위험 세부 정보: 탈옥된 장치에 대한 보안 부족으로 인해 악의적인 행위자의 주요 표적이 됩니다. 권한이 없는 엔터티가 회사 데이터에 액세스하도록 하면 회사 네트워크의 보안 태세가 약화될 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	접근 통제

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 구성 데이터 및 스크립트에 대해 코드 서명 사용[Security Center 1.3에서 제거됨]

인스턴스의 애플리케이션 구성 데이터 및 스크립트에 대한 코드 서명을 관리합니다.

코드 서명은 민감한 애플리케이션 구성 데이터 및 스크립트를 사용하기 전에 유효성을 검사하여 보안을 개선하는 데 도움이 될 수 있습니다. 코드 서명은 나중에 데이터의 진위 및 무결성을 확인하기 위해 확인된 데이터에 대한 디지털 서명을 생성합니다. 이 검증은 악성 데이터나 스크립트가 인스턴스에서 사용되는 것을 방지하여 인스턴스를 완전히 손상시킬 수 있습니다.

이 *com.snc.kmf.signature.validation.flag* 속성을 사용하여 애플리케이션 구성 데이터 및 스크립트에 대한 코드 서명을 관리합니다. 이 속성을 **true**로 설정하면 애플리케이션 구성 데이터 및 스크립트에 대해 코드 서명이 활성화됩니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*com.snc.kmf.signature.validation.flag*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	악성 코드
보안 위험	• 심각도 점수: 6 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 **true** 로 설정하면 코드 서명이 활성화되어 중요한 애플리케이션 구성 데이터 및 스크립트를 확인하여 보안을 향상시킬 수 있습니다.
의존성 및 필수 구성요소	안 함

세션 관리

이 범주는 사용자에 대한 애플리케이션 상태의 보안을 확인합니다. 세션은 각 개인에게 고유해야 하며, 추측하거나 공유할 수 없어야 하며, 일정 기간 동안 활동이 없거나 필요하지 않은 경우 무효화되어야 합니다. 여기에는 쿠키 기반 세션에 대한 쿠키 속성, 세션 토큰 생성, 페더레이션 재인증에 대한 스토리지 및 요구 사항과 같은 요소가 포함됩니다.

모바일 세션에 연속 인증 정책 적용

모바일 세션에 지속적인 인증 정책을 적용하여 세션 하이재킹 위험을 줄입니다.

glide.zta.high_assurance.mobile.session.allowed 시스템 속성을 **false**로 설정하여 모바일 사용자가 Zero Trust - Continuous Authentication 플러그인의 높은 보증 세션 기능을 사용하고 있는지 확인합니다. 모바일 세션에 대한 연속 인증 정책을 바이패스하려면 이 속성을 **true**로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

glide.zta.high_assurance.mobile.session.allowed 시스템 속성을 **false**로 설정합니다. 이 작업은 세션이 손상될 경우 세션 하이재킹 및 지속적인 액세스의 위험을 줄입니다. 이 속성이 시스템 속성 [sys_properties] 테이블에 표시되지 않는 경우 기본값은 **false**입니다.

추가 정보

속성	설명
기술 구성 이름	glide.zta.high_assurance.mobile.session.allowed
플러그인 적용 가능성	제로 트러스트 - 연속 인증 (com.snc.zero_trust_continuous_authentication)
보안 위험	이 시스템 속성이 **true**로 설정되면 높은 보증 세션 기능이 모바일 세션에 적용되지 않습니다. 재인증은 상위 역할 세션에 대한 정책에 정의된 대로 발생하지 않습니다. 이렇게 하면 세션이 손상될 경우 세션 하이재킹 및 지속적인 액세스의 위험이 증가합니다.
CVSS(공통 취약성 평가 시스템) 점수	3.9
CVSS(공통 취약성 평가 시스템) 등급	낮음
기능적 영향	**true**로 설정하면 높은 보증 세션 기능이 모바일 세션에 적용되지 않으므로 세션이 손상될 경우 세션 하이재킹 및 지속적인 액세스의 위험이 증가합니다.
의존성 및 필수 구성요소	안 함
데이터 유형	부울
기본 시스템 값	거짓
폴백 값	거짓
권장 값	거짓

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

절대 세션 시간 제한 기간 최소화**[Security Center** 1.3에서 업데이트됨〕

이 *glide.ui.user_cookie.max_life_span_in_days* 속성을 사용하여 사용자가 내 주소 저장 확인란을 선택한 상태로 로그인할 때 작성되는 사용자 쿠키의 최대 수명을 설정합니다. 쿠키가 만료되면 사용자 기억 확인란을 선택한 사용자는 강제로 인스턴스에 다시 인증해야 합니다.

쿠키를 사용하면 쿠키가 처음 발급된 시점부터 지정된 기간(일) 동안 사용자 쿠키가 유효할 수 있습니다. 기본값은 30일이고 최대 한도는 365일입니다.

주: 활성 사용자 세션에 최대 세션 시간을 적용하려면 문서를 참조하십시오 사용자 세션 관리 .

추가 정보

속성	설명
속성 이름	*glide.ui.user_cookie.max_life_span_in_days*
구성 유형	시스템 속성(/sys_properties_list.do)

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
범주	세션 관리
목적	사용자 기억 확인란을 선택한 사용자가 특정 날짜 이후에 다시 인증하도록 강제합니다.
권장 값	30 이하.
기본값	30일
기능적 영향	이 속성은 지정된 시간 범위 후에 모든 종류의 쿠키 회전을 방지하여 필수 재로그인을 적용합니다.
보안 위험 등급	4.2
보안 위험	(중간) 무기한 활성 상태인 사용자 쿠키는 보안 위험이며 시간 기반 구성에서 만료되어야 합니다.
참조	사용 가능한 시스템 속성 메일 주소 저장

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

활성 세션 시간 제한 예외 역할 정의[**Security Center** 1.3의 새로운 기능]

이 *glide.active.session.timeout.exception.roles* 속성은 활성 세션 시간 제한 제한에서 제외되는 역할을 제어합니다.

활성 세션 시간 제한은 인증 정보를 다시 제공하지 않고 하이재킹된 세션을 무기한 사용할 수 없도록 합니다. 이 보안 위험을 정정하려면 속성이 **edge_encryption, mid_server**로 설정되어 있는지 *glide.active.session.timeout.exception.roles* 확인합니다.

추가 정보

속성	설명
구성 이름	*glide.active.session.timeout.exception.roles*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	edge_encryption, mid_server
기본값	edge_encryption, mid_server
범주	세션 관리
보안 위험	• 심각도 점수: 6.4 • CVSS 점수: 중간 • 보안 위험 상세 정보: 내부 통합 계정 역할에 대한 활성 세션 시간 제한 예외만 고려합니다. 역할에 세션 시간 제한에 대한 예외가 지정되고 세션 하이재킹 공격의 희생자인 사용자에게 해당 역할이 부여되는 경우 공격자는 해당 세션에 무기한 인증할 수 있습니다. 이렇게 하면 공격자가 하이재킹된 계정을 사용할 수 있는 시간이 더 많아져 보안 인시던트의 영향이 증가할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
의존성 및 필수 구성요소	안 함

UserCookie 버전 3.1 사용 [Security Center 2.0에서 업데이트됨]

소스 코드에서 비밀 키의 저장을 보호하기 위해 인스턴스에서 사용할 수 있는 UserCookie의 버전을 관리합니다.

UserCookie v3는 속성이 *glide.ui.secure.cookies.use_kmf is disabled*있는 경우에만 생성됩니다. UserCookie v3는 HMAC에 대한 비밀 키를 소스 코드에 저장하고 모든 고객에게 동일하기 때문에 안전하지 않습니다. 이를 통해 악의적인 행위자가 사용자 세션을 하이재킹하려는 시도에 이 하나의 비밀 키를 사용할 수 있습니다. 속성을 *glide.ui.secure.cookies.use_kmf* true로 설정하면 UserCookie v3.1이 사용되며 비밀 키가 KMF와 같은 보안 스토리지에 저장됩니다.

추가 정보

속성	설명
구성 이름	*glide.ui.secure.cookies.use_kmf*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	세션 관리
보안 위험	• 심각도 점수: 7.1 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이를 **false** 로 설정하면 소스 코드에 저장되는 HMAC(해시 기반 메시지 인증 코드)의 비밀 키로 인한 보안 취약점이 발생합니다.
의존성 및 필수 구성요소	안 함

API 요청에 암호 재설정 강제 적용[Security Center 1.5에서 업데이트됨]

인스턴스에서 암호 재설정 기능이 작동하는 방식을 관리합니다.

사용자가 암호 재설정 필요로 표시되면 다음 인증 시도 시 새 암호를 제공해야 합니다. 이 속성은 API를 호출하기 전 암호 재설정이 필수인지 여부를 제어합니다. 이 속성이 권장 값인 **true**로 설정되지 않은 경우 암호 재설정 필요 로 표시된 사용자 계정은 기본 인증을 통해 테이블 API를 쿼리하여 작업을 수행할 수 있습니다. 이 보안 취약성은 비활성 계정이 손상된 경우 정보 유출을 유발할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.api.user.reset_password.mandatory*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	예
기본값	거짓
범주	세션 관리
보안 위험	• 심각도 점수: 8.1 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하면 비활성 계정이 손상될 경우 정보 유출이 발생할 수 있습니다.
의존성 및 필수 구성요소	안 함

HTTP 쿠키 전용 플래그 사용[Security Center 1.3에서 업데이트됨]

이 *glide.cookies.http_only* 속성을 사용하여 중요한 쿠키에 대해 HTTPOnly 속성을 활성화합니다.

HTTPOnly 속성은 JavaScript와 같은 클라이언트 측 스크립트를 사용하여 쿠키에 대한 액세스를 허용하지 않으므로 사이트 간 스크립팅과 같은 공격을 방지합니다. 교차 사이트 스크립팅 위험을 제거하지는 않지만 일부 악용 벡터를 제거합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.cookies.http_only*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	세션 관리
목적	보호된 쿠키에 액세스하는 클라이언트 측 스크립트의 위험을 완화하기 위해
권장 값	예
기본값	예
보안 위험 등급	8
기능적 영향	이렇게 정정하면 세션 쿠키에 추가 HTTPOnly 플래그가 추가되어 도난당하지 않도록 보호됩니다. • 사용자의 쿠키에 액세스하기 위해 JavaScript가 필요한 사용자 지정 기능이 있는 경우 해당 기능이 중단됩니다. 정상적인 상황에서는 그렇지 않아야 합니다. • Now Platform 세션 관리를 처리하며 사용자 지정 스크립트가 사용자의 쿠키에 액세스할 이유가 없어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	(보통) 응용 프로그램의 세션 쿠키는 최종 사용자를 인증하고 응용 프로그램에 대한 암시적 액세스 권한을 제공합니다. 즉, 도난당하거나 수출되지 않도록 보호할 필요가 있습니다. HTTP 전용 플래그는 JavaScript 주입 또는 교차 사이트 스크립팅 취약성으로부터 세션 쿠키를 보호합니다.
참조	사용 가능한 시스템 속성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

OAuth 토큰 만료 후 세션 무효화[Security Center 2.0의 새로운 기능]

glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled 세션을 생성하는 데 사용된 OAuth 토큰이 만료된 후에도 사용자가 쿠키를 통해 세션을 계속 사용하지 못하도록 속성을 안전한 값으로 구성합니다.

glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled 속성이 보안 값인 예로 설정되지 않은 경우 사용자는 세션을 생성하는 데 사용된 OAuth 토큰이 만료된 후에도 쿠키를 통해 세션을 계속 사용할 수 있습니다. 이렇게 하면 쿠키가 유출되고 악의적인 사용자가 세션을 하이재킹하여 승인되지 않은 리소스에 액세스할 위험이 높아집니다. glide property *glide.authenticate.oauth.post.token.expiration.cookie_auth.disabled*가 true로 설정되어 있는지 확인하십시오. sys_properties 테이블에 기록이 없는 경우 기본값은 false입니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.oauth.post.token.expiration.cookie_au*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	zboot 인스턴스의 경우 이 속성은 true입니다. 업데이트 인스턴스의 경우 이 속성은 기본적으로 false입니다.
범주	세션 관리
보안 위험	• 심각도 점수: 5.4 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 보안 값 예로 설정하지 않으면 세션을 생성하는 데 사용된 OAuth 토큰이 만료된 후에도 사용자가 세션을 계속 사용할 수 있으므로 악의적인 사용자가 세션을 하이재킹할 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함
기능적 영향	True: OAuth 액세스 토큰이 만료될 때까지만 쿠키 인증이 적용됩니다. 만료 후에는 인증이 적용되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	False: OAuth 액세스 토큰이 만료된 후에도 쿠키 인증이 적용됩니다.

동시 대화형 세션 수량 최소화 **[Security Center** 1.3에서 업데이트됨〕

이 속성을 동시 세션 제한 플러그인과 함께 사용하여 사용자가 열 수 있는 활성 세션 수를 제어합니다.

동시 세션 제한(*com.glide.limit.concurrent.sessions* 플러그인과 함께 **Glide** 인증 최대 동시 대화형 세션 속성을 사용하여 사용자에 대해 열리는 활성 세션 수를 제어합니다. 권장되는 값은 **1**이며, 이 경우 열리는 세션 수가 줄어듭니다(숫자가 클수록 세션이 하이재킹될 가능성이 높아짐).

추가 정보

속성	설명
구성 이름	*glide.authenticate.max.concurrent.interactive.sessions*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	1
기본값	1
범주	세션 관리
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 속성의 기본값을 1보다 크게 설정하면 세션이 하이재킹될 가능성이 높아집니다.
의존성 및 필수 구성요소	동시 대화형 세션(*com.glide.limit.concurrent.sessions* 플러그인이 활성 상태여야 합니다.
참조	동시 세션 제한

모든 노드에서 동시 세션 제한 **[Security Center** 1.3에서 업데이트됨〕

이 *glide.authenticate.limit.concurrent.sessions.across.all.nodes* 속성을 동시 세션 제한 플러그인과 함께 사용하여 모든 노드에서 추적되는 세션 수를 관리합니다.

플러그인이 동시 세션 제한 활성화되면 사용자당 오픈 세션 수를 제한할 수 있습니다. 이 플러그인이 활성화되면 (**Glide** 인증은 모든 노드에서 동시 세션 제한) 속성이 예 로 설정되어 단일 애플리케이션 노드 대신 모든 노드에서 오픈 세션 수가 추적되도록 합니다. 이 속성이 아니오로 설정되면 여러 노드에서 여러 세션을 열 수 있으므로 세션이 하이재킹될 가능성이 높아집니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.limit.concurrent.sessions.across.all.*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	부울
권장 값	예
기본값	예
범주	세션 관리
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 동시 세션 제한 플러그인을 사용할 때 이 속성을 아니오 로 설정하면 여러 노드에서 여러 세션이 열릴 수 있으므로 세션 하이재킹과 같은 보안 취약성이 발생할 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함
참조	동시 세션 제한

동시 세션 제한 플러그인

인스턴스에서 세션 하이재킹 가능성을 줄이도록 com.glide.limit.concurrent.sessions 플러그인을 구성합니다.

이 플러그인을 사용하면 관리자가 사용자 및/또는 역할당 활성 세션 수를 제한할 수 있습니다. 세션 하이재킹 가능성을 줄이기 위해 이 플러그인을 사용하도록 설정하고 구성하는 것이 좋습니다. 이 플러그인이 활성화되고 구성된 경우 하이재킹할 수 있는 오픈 세션 수에 제한이 있습니다.

추가 정보

속성	설명
구성 이름	*com.glide.limit.concurrent.sessions*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	플러그인
권장 값	com.glide.limit.concurrent.sessions 활성화 및 구성됨
기본값	com.glide.limit.concurrent.sessions 활성화 및 구성됨
범주	세션 관리
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 이 플러그인이 활성화되어 있지 않으면 세션이 하이재킹될 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함

게스트의 활성 세션 수명 제한 **[Security Center** 1.3의 새로운 기능]

이 *glide.guest.active.session.life_span* 속성을 사용하여 활성 게스트의 HTTP 세션 기간을 제어합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 *glide.guest.active.session.life_span* 속성은 세션 비활성 또는 세션 시간이 초과되어 닫히기 전에 사용자가 비활성 상태인 시간에 관계없이 활성 게스트 HTTP 세션에 최대 수명을 적용합니다. 구성된 값은 분 단위입니다. 값이 0이면 활성 세션의 시간 초과가 비활성화됩니다. 값이 클수록 공격자는 도난당한 세션에 더 오래 머물 수 있으므로 보안 인시던트가 발생할 가능성이 높아집니다. 이 속성은 인스턴스에 대한 낮은 권한을 가진 게스트 사용자로 제한됩니다.

이 보안 취약성을 정정하려면 0보다 크고 720 이하의 값으로 설정하십시오 *glide.guest.active.session.life_span*.

추가 정보

속성	설명
구성 이름	*glide.guest.active.session.life_span*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	1-720(분)
기본값	0
범주	세션 관리
보안 위험	• 심각도 점수: 4.2 • CVSS 점수: 중간 • 보안 위험 상세 정보: 최대 수명을 큰 값으로 설정하면 악의적인 액터가 세션을 훔칠 경우 인스턴스 내에서 더 많은 시간을 확보할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 구성은 비활성 시간 제한에 관계없이 활성 게스트 HTTP 세션에 최대 수명 범위를 적용합니다. 구성된 값은 분 단위입니다. 값이 0이면 활성 세션의 시간 초과가 비활성화됩니다. 최대 수명은 비활성 시간 제한 *glide.guest.session_timeout* (기본값 30분)보다 길어야 합니다.

동시 대화형 세션 제한**[Security Center** 1.3에서 업데이트됨〕

인스턴스에서 대화형 세션 수를 관리합니다.

이 속성은 동시 세션 제한() *com.glide.limit.concurrent.sessions* 플러그인과 함께 사용되도록 되어 있습니다. 플러그인이 활성 상태이고 속성이 false로 설정되면 사용자는 인스턴스에서 동시 대화형 세션을 가질 수 있습니다. 오픈 세션이 많을수록 세션 하이재킹이 발생할 가능성이 큽니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.limit.concurrent.interactive.sessions*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
권장 값	예
기본값	거짓
범주	세션 관리
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 플러그인이 활성 상태이고 속성이 **false**로 설정된 경우 사용자는 동시 대화형 세션을 가질 수 있으므로 세션이 하이재킹될 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함
참조	동시 대화형 세션 제한[Security Center 1.3에서 업데이트됨]

통합의 활성 세션 수명 제한 [Security Center 1.3의 새로운 기능]

이 *glide.integrations.active.session.life_span* 속성은 비활성 시간 제한에 관계없이 활성 게스트 HTTP 세션에 최대 수명을 적용합니다. 구성된 값은 분 단위입니다. 값이 0이면 활성 세션의 시간 초과가 비활성화됩니다.

추가 정보

속성	설명
구성 이름	*glide.integrations.active.session.life_span*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	0에서 720
기본값	0
범주	세션 관리
보안 위험	• 심각도 점수: 4.2 • CVSS 점수: 중간 • 보안 위험 상세 정보: 최대 수명이 길수록 공격자가 도난당한 세션에 더 오래 머물 수 있으므로 보안 인시던트의 범위가 늘어날 수 있습니다. 이 속성은 인스턴스에 대한 낮은 액세스 권한이 있는 통합으로 제한됩니다. glide 속성을 *glide.integrations.active.session.life_span* 값 0, 720 이하로 설정합니다.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정책 기반 세션 액세스 모바일 새로 고침 토큰 간격 제한 [Security Center 1.5의 새로운 기능]

이 *glide.authenticate.session_access.mobile.refresh_token_interval* 속성을 사용하여 모바일 장치 사용자가 강제로 재인증을 받아야 하기 전에 경과해야 하는 시간을 관리합니다.

관리자가 세션 정책에서 ID 제공자 속성을 구성하고(속성은 로그인마다 다를 수 있음) 사용자가 SSO(Single Sign On)를 사용하여 인증하는 경우에만 사용자에게 다시 인증하라는 메시지가 표시됩니다. 기본값은 사용자가 재인증을 받기 전의 시간(초)을 나타냅니다. 기본값이 클수록 세션 하이재킹이 발생할 경우 잘못된 액터에 세션 액세스 시간이 더 많이 제공됩니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.session_access.mobile.refresh_token_i*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	1800(초)
기본값	1800(초)
범주	세션 관리
보안 위험	• 심각도 점수: 4.3 • CVSS 점수: 중간 • 보안 위험 상세 정보: 인스턴스에서 ZTA 정책이 활성화된 경우 모바일 로그인 중에 SSO를 사용하는 사용자는 기본값인 1800초(30분)가 지난 후 강제로 로그아웃했다가 다시 로그인해야 합니다. 더 높은 값을 사용하면 사용자는 경과된 시간을 기다려야 합니다.
의존성 및 필수 구성요소	제로 트러스트 - 정책 기반 세션 액세스
기능적 영향	이 설정은 로그인 후 시간(초)을 제어하며, 사용자가 Single Sign On을 사용하여 인증하고 관리자가 세션 액세스 정책에서 ID 제공자 속성을 구성한 경우 모바일 장치에서 강제로 로그아웃해야 합니다.

높은 보증 세션에 대한 세션 길이 제한

세션 길이를 제한하여 높은 보증 세션에서 계정 탈취 위험 감소

세션 길이를 제한하여 높은 보증 세션에서 계정 탈취 위험을 줄입니다. 지정된 시간이 지나면 최종 사용자가 다시 인증해야 합니다.

glide.zta.high_assurance.session.timeout 시스템 속성을 사용하여 사용자가 다시 인증해야 하는 시간(분)을 설정합니다. 이 속성의 값은 1분에서 480분 사이여야 합니다. 계정 탈취 위험을 줄이려면 이 값을 30 이하로 제한하는 것이 좋습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
기술 구성 이름	glide.zta.high_assurance.session.timeout
플러그인 적용 가능성	제로 트러스트 - 연속 인증 (com.snc.zero_trust_continuous_authentication)
보안 위험	세션 길이가 짧을수록 사용자가 재인증을 받도록 강제하여 계정 탈취의 위험을 줄일 수 있습니다.
CVSS(공통 취약성 평가 시스템) 점수	3.3
CVSS(공통 취약성 평가 시스템) 등급	낮음
기능적 영향	높은 보증 세션의 사용자는 이 속성에서 설정한 간격으로 다시 인증해야 합니다.
의존성 및 필수 구성요소	안 함
데이터 유형	정수
기본 시스템 값	30
폴백 값	30
권장 값	30 이하

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

UI 활성 세션 수명 제한 [Security Center 1.3의 새로운 기능]

이 *glide.ui.active.session.life_span* 속성은 비활성 시간 제한에 관계없이 활성 인증된 HTTP 세션에 최대 수명을 적용합니다.

활성 HTTP 세션의 수명을 줄여 잠재적인 보안 인시던트의 범위를 줄입니다. **glide.ui.active.session.life_span** 시스템 속성은 비활성 시간 제한에 관계없이 활성 HTTP 세션에 최대 수명을 적용합니다. 최대 수명이 길수록 공격자는 도난당한 세션을 더 오랫동안 사용할 수 있으므로 보안 인시던트의 범위가 늘어날 수 있습니다. 기본값 **0** 은 활성 세션의 시간 제한을 비활성화합니다.

glide.ui.active.session.life_span 1에서 720 사이의 값으로 설정합니다. 이 값은 HTTP 세션이 활성 상태로 유지될 수 있는 시간(분)을 나타냅니다.

주: **glide.ui.active.session.life_span**는 UI 세션 시간 제한으로 제한됩니다.

추가 정보

속성	설명
구성 이름	*glide.ui.active.session.life_span*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	1-720
기본값	0

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
범주	세션 관리
보안 위험	• 심각도 점수: 4.2 • CVSS 점수: 중간 • 보안 위험 상세 정보: 최대 수명이 길수록 공격자가 도난당한 세션에 더 오래 머물 수 있으므로 보안 인시던트의 가능성이 높아질 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	비활성 시간 제한에 관계없이 활성 인증된 HTTP 세션에 최대 수명 범위를 적용합니다. 구성된 값은 분 단위입니다. 값이 0이면 활성 세션의 시간 초과가 비활성화됩니다. 최대 수명은 비활성 시간 제한 glide.ui.session_timeout(기본값 30분)보다 길어야 합니다.

비활성 세션을 사전 예방적으로 무효화 [Security Center 1.3의 새로운 기능 및 1.5 및 2.0에서 업데이트됨]

이 *glide.active.session.timeout.invalidate.session* 속성은 시간 제한 세션이 Tomcat 서버보다 먼저 사전에 무효화되는지 여부를 제어합니다.

가 **true**로 설정되지 않은 경우 *glide.active.session.timeout.invalidate.session* 시간 초과된 세션이 무효화되지 않는 짧은 시간 간격이 있을 수 있습니다(큐 크기에 따라 60초 이상). 세션이 하이재킹되면 공격자는 이 짧은 시간 동안 세션을 사용할 수 있습니다. 이 보안 위험을 정정하려면 **true**로 설정합니다*glide.active.session.timeout.invalidate.session*.

추가 정보

속성	설명
구성 이름	*glide.active.session.timeout.invalidate.session*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	세션 관리
보안 위험	• 심각도 점수: 4.6 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 권장 값인 예로 설정하지 않으면 시간 초과된 세션의 유효성이 확인되지 않을 수 있습니다. 이렇게 하면 악의적인 행위자가 세션을 하이재킹할 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

HTTP 세션 식별자 교대

glide.ui.rotate_sessions 이 속성을 사용하여 HTTP 세션 식별자 순환을 활성화하여 보안 취약성을 줄입니다.

인증 후에도 인증되지 않은 사용자의 세션 ID가 변경되지 않으면 웹 애플리케이션이 세션 고정 공격 에 취약해집니다. 악의적인 사용자가 인증되지 않은 세션을 시작하고 연결된 세션 ID를 피해자에게 제공할 수 있습니다. 피해자가 인증되면 악의적인 사용자는 이제 인증된 세션을 공유합니다.

추가 정보

속성	설명
속성 이름	*glide.ui.rotate_sessions*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	세션 관리
목적	보다 안전한 세션 인증을 달성하기 위해.
권장 값	예
기본값	예
보안 위험 등급	8.8
기능적 영향	이 정정하면 사용자가 인증되지 않은 페이지에서 인증된 페이지로 이동할 때 SessionID를 수정합니다. • 사용자가 처음 로그인할 때 또는 어떤 목적으로든 프록시를 사용하거나 SessionID를 하드 코딩하는 경우 잠재적인 기능에 영향이 있을 수 있습니다. • 1회 사용자 인증(SSO)에 SAML 2.0 플러그인을 사용하는 경우, 인스턴스와 ID 제공자 간의 세션 정보 공유에 방해가 될 수 있습니다. 이 경우 이 속성을 false로 설정할 수 있습니다.
보안 위험	(보통) SessionID는 브라우저에서 세션 상태를 유지 관리하여 인스턴스 사용자를 처리하고 인증하는 데 사용됩니다. 따라서 SessionID는 중요한 데이터로 간주되며 기본적으로 안전해야 합니다. 세션 교대는 사용자가 인증되지 않은 페이지에서 페이지를 인증하기 위해 탐색할 때마다 sessionID의 변경을 적용하는 보안 제어입니다.
참조	SAML을 사용한 인증

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

동시 대화형 세션 수량 최소화[Security Center 1.3에서 업데이트됨]

이 속성을 동시 세션 제한 플러그인과 함께 사용하여 사용자가 열 수 있는 활성 세션 수를 제어합니다.

동시 세션 제한(*com.glide.limit.concurrent.sessions* 플러그인과 함께 **Glide** 인증 최대 동시 대화형 세션 속성을 사용하여 사용자에 대해 열리는 활성 세션 수를 제어합니다. 권장되는 값은 **1**이며, 이 경우 열리는 세션 수가 줄어듭니다(숫자가 클수록 세션이 하이재킹될 가능성이 높아짐).

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.authenticate.max.concurrent.interactive.sessions*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	정수
권장 값	1
기본값	1
범주	세션 관리
보안 위험	• 심각도 점수: 3.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 속성의 기본값을 1보다 크게 설정하면 세션이 하이재킹될 가능성이 높아집니다.
의존성 및 필수 구성요소	동시 대화형 세션()*com.glide.limit.concurrent.sessions* 플러그인이 활성 상태여야 합니다.
참조	동시 세션 제한

세션 활동 시간 제한 기간 최소화 **[Security Center** 1.3에서 업데이트됨〕

이 *glide.ui.session_timeout* 속성을 사용하여 활동 시간 제한 값을 분 단위로 지정합니다.

이 속성을 설정하면 여러 가지 기능에 영향을 미칩니다.

- 지정된 세션 제한 시간이 길수록 처리 세션 중에 더 많은 양의 메모리가 사용됩니다. 기본 시스템에서는 기본 Apache Tomcat 시간 제한 기간인 30분을 사용합니다.
- Now Platform 여전히 사용자는 '메일 주소 저장'을 사용하여 로그아웃합니다. 애플리케이션에서 30분 동안 활동이 없으면 로그인 페이지에서 사용자 이름 저장 확인란을 선택하지 않으면 플랫폼에서 사용자를 자동으로 로그아웃합니다. 다른 점은 계속하기 위해 다시 로그인하지 않는다는 것입니다.
- 사용자의 홈페이지에 자동으로 새로 고침되는 게이지 또는 컨텐츠가 있는 경우 이 시간 제한에 도달하지 못할 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.session_timeout*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	세션 관리
목적	세션 시간 제한을 적용하기 위해.
권장 값	사용자 지정 시간 제한(분)입니다. 60분이 권장되는 값이지만 이 값은 기능 및 보안 요구 사항에 따라 다를 수 있습니다. 이 값을 1일 이상으로 설정하지 마십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험 등급	7.5
기능적 영향	이렇게 정정하면 사용자 계정이 적시에 만료됩니다. 기능에는 영향을 주지 않지만 사용자 경험이 변경됩니다.
보안 위험	(높음) 사용자 세션이 무기한 활성 상태인 것은 보안상 위험하며 시간 기반 구성에서 만료되어야 합니다.
참조	사용자 세션 관리

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

세션 시간 제한 기간 최소화[Security Center 1.3에서 업데이트됨]

이 *glide.ui.user_cookie.life_span_in_days* 속성을 사용하여 내 정보 기억 쿠키의 만료 기간을 설정합니다. 기본값은 15일이고 최대 한도는 30일입니다.

추가 정보

속성	설명
속성 이름	*glide.ui.user_cookie.life_span_in_days*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	세션 관리
목적	내 정보 기억 쿠키의 기본 만료를 사용하도록 설정합니다.
데이터 유형	정수
권장 값	15
기본값	15
보안 위험 등급	4.9
기능적 영향	최종 사용자가 로그인 페이지에서 메일 주소 저장 확인란을 선택하고 에 로그인 Now Platform하면 최종 사용자가 이 속성을 활성화합니다.
보안 위험	(보통) 무기한 활성 상태인 사용자 쿠키는 보안 위험이며 시간 기반 구성에서 만료되어야 합니다.
참조	사용 가능한 시스템 속성 메일 주소 저장

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

저장된 암호화

이 범주는 저장된 데이터의 암호화에 중점을 둡니다. 여기에는 확립된 알고리즘 및 암호화 모듈 사용, 의사 난수 값의 적절한 생성 보장, 데이터 분류에 따른 암호화 구현, 주요 자료를 안전하게 저장 및 격리하는 것과 같은 몇 가지 주요 측면이 포함됩니다.

Glide KMF 암호화기 사용 [Security Center 1.3.2에서 제거됨]

인스턴스에서 Password2 필드에 사용되는 암호화기를 관리합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이*glide.kmf.encrypter.enabled*속성을 사용하여 KMF 암호화를 Password2 필드의 기본 암호화기로 설정합니다. 이 속성은 레거시 암호화기 대신 강력하고 규정을 준수하는 암호화 표준이 사용되도록 합니다. 레거시 암호화기 대신 KMF 암호화기가 사용되도록 하려면 이 속성을 **true**로 설정합니다.

추가 정보

속성	설명
구성 이름	*glide.kmf.encrypter.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	저장된 암호화
보안 위험	• 심각도 점수: 4.9 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 **true** 로 설정하면 레거시 암호화기 대신 KMF 암호화기가 사용됩니다.
참조	Key Management Framework(KMF)를 사용한 Password2 암호화

TripleDES/3DES 암호화 알고리즘 사용 안 함

TripleDES/3DES 암호화 알고리즘의 사용을 사용하지 않도록 설정하여 오래된 암호화 방법으로 인한 보안 위험을 방지합니다.

민감한 정보의 손실 및 유출을 초래할 수 있으므로 더 이상 사용되지 않는 레거시 3DES 또는 Triple-DES(Triple Data Encryption Standard)의 사용을 비활성화합니다.

NIST(National Institute of Standards and Technology)는 3DES(Triple DES)를 사용하여 데이터를 암호화하지 말 것을 권고했습니다. 자세한 내용은 NIST 800-131A Rev 2를 참조하십시오. 3DES는 현재 연방 시스템에서 암호화가 금지되어 있습니다. 앞으로 TDES는 이전 메시지 암호 해독, 키 래핑 해제 및 MAC 확인과 같은 기록 목적으로만 사용할 수 있습니다.

glide.security.3des.encryption.allow 시스템 속성은 인스턴스에서 3DES 암호화가 활성화되었는지 여부를 제어하지만, 인스턴스를 사용 중지할 준비가 되었는지 확인하기 위해 수행해야 할 몇 가지 단계가 있습니다. 이 속성을 설정하기 전에 사용 중단 프로세스에 대한 자세한 내용은 KB1704481 검토하십시오.

추가 정보

속성	설명
기술 구성 이름	glide.security.3des.encryption.allow
플러그인 적용 가능성	안 함
보안 위험	3DES와 같이 오래되고 약한 암호화를 사용하면 민감한 정보가 손실되거나 유출될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
CVSS(공통 취약성 평가 시스템) 점수	4.2
CVSS(공통 취약성 평가 시스템) 등급	보통
기능적 영향	이 속성을 아니오 로 설정하면 인스턴스가 오래되고 약한 암호화를 사용하는 것을 방지할 수 있습니다. 이는 Password2 데이터가 저장되는 방식에 영향을 줍니다. 3DES 사용 중단의 기능적 영향에 대한 자세한 내용은 KB1704481 검토하십시오.
의존성 및 필수 구성요소	이 속성의 값을 변경하기 전에 KB1704481 설명된 작업을 수행합니다.
데이터 유형	부울
기본 시스템 값	거짓
폴백 값	거짓
권장 값	거짓

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

확인, 삭제 및 인코딩

유효성 검사, 삭제 및 인코딩은 XSS(교차 사이트 스크립팅), SQL 주입 및 기타 공격과 같은 취약성을 방지하기 위한 입력 유효성 검사를 해결합니다.

이 제어를 통해 입력 유효성 검사 및 출력 인코딩이 제대로 구성됩니다(예: 인코딩 또는 출력 데이터 이스케이프). 이 범주에는 객체의 해제, 필요한 경우 샌드박싱, 허용 목록을 통한 양수 확인과 같은 항목에 대한 검사도 포함됩니다.

GlideSystemUserSession 스크립팅 가능한 API에 대한 접근 제한 〔보안 센터 **1.3** 및 2.0에서 업데이트됨〕

클라이언트 호출 가능 GlideSystemUserSessionSandbox 스크립트 가능 API는 GlideSystemUserSession의 addErrorMessageNoSanitization 및 addInfoMessageNoSanitization 메서드를 JavaScript 샌드박스에 노출합니다. 이렇게 하면 모든 사용자가 스크립트를 통해 이 메서드를 호출할 수 있습니다.

`gs.addErrorMessageNoSanitizationMessaging()` 및 *`gs.addInfoMessageNoSanitization()`* 은 스크립팅 환경 내에서 로깅 및 알림에 사용됩니다. 이 속성이 권장 값인 false로 설정되지 않은 경우 샌드박스에서 이 두 가지를 모두 사용할 수 있습니다. 샌드박스는 인증되지 않은 역할 사용자가 사용할 수 있는 권한이 낮은 스크립팅 환경입니다. 이 두 가지 방법 모두 사용자에게 삭제되지 않은 입력을 표시하는 데 사용할 수 있습니다. 삭제되지 않은 입력에 사용자의 브라우저에서 실행되는 위험한 코드가 포함될 수 있으므로 사용자에게 삭제되지 않은 입력을 표시하는 것은 위험합니다. 이는 기존의 반사된 XSS 공격에 활용될 수 있습니다. 반영된 XSS 공격은 세션 하이재킹을 비롯한 여러 시나리오에서 사용될 수 있습니다.

시스템 속성을 **false**로 설정합니다**glide.sandbox.usersession.allow_unsanitized_messages**. 시스템 속성 [sys_properties] 테이블에 이 속성에 대한 기록이 없으면 기록을 하나 만듭니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.sandbox.usersession.allow_unsanitized_messages*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	접근 통제
목적	이 속성은 샌드박스 사용자 세션에서 삭제되지 않은 정보 또는 오류 메시지가 호출되지 않도록 제한합니다.
유형	부울
권장 값	거짓
기본값	예
보안 위험 등급	8.1
기능적 영향	false 값으로 속성을 설정하면 해당 함수가 호출되어도 메시지가 생성되거나 로깅되지 않습니다.
보안 위험	(높음) 적절한 정리가 없으면 잠재적으로 위험한 콘텐츠에 액세스할 수 있으며 삭제되지 않은 오류 함수를 스크립트에 사용할 수 있습니다.
참조	접근 통제

임베디드 HTML에 **JavaScript** 태그 사용 안 함**[Security Center** 1.3에서 업데이트됨**]**

이 *glide.ui.security.codetag.allow_script* 속성을 사용하여 [code] 태그를 사용하여 만든 HTML JavaScript 코드를 포함하기 위한 지원을 비활성화합니다.

이스 Now Platform 케이프 및 인코딩 기술을 구현하여 많은 삽입 및 교차 사이트 공격을 완화합니다. 따라서 사용자는 저널 필드에 대한 HTML 형식의 입력을 쓰고 제출할 수 없습니다. 그러나 저널 필드는 코드 태그로 묶인 텍스트를 HTML로 렌더링할 수 있습니다. *glide.ui.security.codetag.allow_script* 속성이 sys_properties 테이블에 있고 false로 설정되어 있는지 확인합니다.

- 그러나 이와 관련된 보안 위험이 있습니다. **true**로 설정하면 악의적인 사용자가 저널 필드를 렌더링한 후 다른 클라이언트 브라우저에서 실행될 수 있는 유해한 HTML JavaScript 코드를 작성할 수 있습니다.
- 관리자가 `[code]` 태그에 대한 지원을 사용하지 않도록 설정하여 저널 필드에서 HTML JavaScript 코드를 렌더링하지 못하도록 하려면 이 속성을 **false**로 설정합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.security.codetag.allow_script*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
목적	사이트 간 스크립팅 및 악의적인 스크립트 실행으로부터 보호
권장 값	거짓
기본값	거짓
보안 위험 등급	8.8
기능적 영향	이렇게 정정하면 UI에 JavaScript 이스케이핑이 적용되고 인코딩된 결과를 사용자에게 렌더링합니다. 결과 데이터에 대한 인스턴스 사용자의 상호작용에 따라 기능에 영향을 미칠 수 있습니다.
보안 위험	(높음) 교차 사이트 스크립팅 공격을 방어하기 위해 애플리케이션에서 입력 유효성 검사가 수행되어야 합니다. 이러한 공격을 통해 외부 스크립트가 로그인된 브라우저의 컨텍스트에서 사용자 세션에서 실행될 수 있습니다. 공격자는 이를 사용하여 세션 정보와 중요한 데이터를 훔칠 수 있습니다.
참조	저널 필드의 코드 태그 제한 저널 필드 항목을 HTML로 렌더링 높은 보안 설정

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

강화된 **Java** 보안 관리자 사용 **[Security Center** 1.3의 새로운 기능**]**

이 *glide.security.manager* 특성은 현재 Java 보안 관리자의 Java 클래스 이름을 포함합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.security.manager*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	*com.glide.sys.security.ContextualSecurityManager*
기본값	*com.glide.sys.security.ContextualSecurityManager*
범주	확인, 삭제 및 인코딩
보안 위험	• 심각도 점수: 7.2 • CVSS 점수: 높음 • 보안 위험 상세 정보: *glide.security.manager* 권장 값인 *com.glide.sys.security.ContextualSecurityManager*로 설정되지 않은 경우 인스턴스가 예상 강화 정책이 누락된

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	오래된 Java 보안 관리자를 사용 중일 수 있습니다. 이 강화가 없으면 스크립트 실행 액세스 권한이 있는 악의적인 액터가 인스턴스에서 원격 코드를 실행할 수 있습니다.
의존성 및 필수 구성요소	안 함

HTML 위생화 강제 적용[Security Center 1.3에서 업데이트됨]

이 *com.glide.security.check_unsanitized_html* 속성을 사용하여 필드 할당을 위해 전역 수준에서 translated_html 필드의 정리 동작을 적용합니다.

HTML은 딕셔너리 필드에 할당할 수 있는 유형 중 하나입니다. 필드 유형에 HTML 필드를 할당하면 HTML 태그(예: `<p>`, `<a href>`, , `<font><b>`,)`<img>`를 사용하여 내용의 서식을 지정하는 기능이 제공됩니다. 악의적인 활동을 방지하기 위해 차단 목록을 사용하여 특정 HTML 태그를 허용하지 않을 수 있습니다. 이 속성은 허용되지 않는 태그가 인스턴스의 translated_html 필드에 사용되는 것을 방지합니다.

- translated_html 필드의 위생 동작을 적용하려면 이 속성을 강제로 설정합니다.
- translated_html 필드에서 차단된 html 태그를 허용하도록 html 정리를 끄려면 속성을 비활성화 로 설정합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*com.glide.security.check_unsanitized_html*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	안전하지 않은 HTML 태그의 사용을 차단하여 교차 사이트 스크립팅과 같은 공격으로부터 보호합니다.
유형	문자열
권장 값	적용
기본값	적용
보안 위험 등급	7.3
기능적 영향	이렇게 정정하면 UI에서 HTML 정리를 수행하고 번역된 html 필드를 사용자에게 렌더링합니다. 가독성과 서식에 영향을 줄 수 있습니다.
보안 위험	(높음) 교차 사이트 스크립팅 공격을 방어하기 위해 애플리케이션에서 입력 유효성 검사가 수행되어야 합니다. 이러한 공격을 통해 외부 스크립트가 로그인된 브라우저의 컨텍스트에서 사용자 세션에서 실행될 수 있습니다. 공격자는 이를 사용하여 세션 정보와 중요한 데이터를 훔칠 수 있습니다.
참조	HTML 위생 검사

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트 샌드박스 사용[Security Center 1.3에서 업데이트됨]

glide.script.use.sandbox 이 속성을 사용하여 스크립트 샌드박스를 활성화합니다.

스크립트 샌드박스 기능을 활성화하여 권한이 없거나 인증되지 않은 사용자가 인스턴스에서 권한 있는 스크립트를 실행하지 못하도록 합니다. 스크립트 샌드박스는 권한이 제한된 "샌드박스" 환경에서 쿼리 조건 및 GlideAjax 표현식과 같은 클라이언트 작성 스크립트를 실행하는 데 사용됩니다.

스크립트 샌드박스가 없으면 인증되지 않은/인증되지 않은 사용자가 인스턴스에서 권한 있는 스크립트를 실행할 수 있습니다. 이는 인스턴스의 모든 데이터에 대한 잠재적인 악의적인 액세스를 포함하되 이에 국한되지 않는 모든 영역의 보안에 영향을 줄 수 있습니다.

glide.script.use.sandbox 시스템 속성을 **true**로 설정하여 인스턴스에서 스크립트 샌드박스 기능을 활성화합니다.

클라이언트가 평가를 위해 서버에 스크립트를 보낼 수 있도록 하는 두 가지 경우가 Now Platform 있습니다.

필터 또는 쿼리

`assigned_to=JavaScript:getMyGroups()`와 같은 필터를 서버에 보내는 것은 합법적입니다.

시스템 API

API 호출을 사용하면 클라이언트가 서버에서 임의의 스크립트를 실행하고 응답을 받을 수 있습니다.

스크립트 샌드박스를 사용하도록 설정하면 이 두 엔트리포인트 중 하나에서 평가되는 스크립트가 샌드박스에서 축소된 권한으로 실행되며 다음과 같은 특징이 있습니다.

- 클라이언트 호출 가능으로 표시된 비즈니스 규칙만 샌드박스 내에서 사용할 수 있습니다.
- 클라이언트 호출 가능으로 표시된 스크립트 포함만 샌드박스 내에서 사용할 수 있습니다.
- 특정 API 호출(전부는 아니지만 직접 DB 액세스를 처리하는 호출로 제한되는 호출은 허용되지 않습니다.)
- 샌드박스 내에서 데이터를 삽입, 업데이트 또는 삭제할 수 없습니다. 예를 들어, `current.update()`에 대한 모든 호출은 무시됩니다. 스크립트 샌드박스를 활성화하지 않고 실행하면 Now Platform 이러한 제한 사항이 적용되지 않습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.script.use.sandbox*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	플랫폼에 대해 실행되는 클라이언트 측 JavaScript 쿼리에 대한 유효성 검사를 적용합니다.
권장 값	예
기본값	예
보안 위험 등급	10

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기능적 영향	이렇게 정정하면 에 Now Platform대해 실행되는 클라이언트 측 JavaScript 쿼리에 대한 유효성 검사가 수행됩니다. 고객이 CRUD 작업을 수행하기 위해 하드 코딩된 JavaScript 쿼리를 포함하는 사용자 지정을 하는 경우 잠재적인 영향이 있습니다.
보안 위험	(중요) JavaScript Now Platform 쿼리를 통해 다양한 기능을 제공합니다. 그러나 적절한 권한 부여 및 유효성 검사가 없으면 공격자가 플랫폼에 대해 무단 작업을 수행할 가능성이 있습니다.
참조	스크립트 샌드박스 속성 구성 *glide.script.use.sandbox* 클라이언트에서 시작된 스크립트 실행을 보호하고 제한하는 동일한 속성 제품군에 속합니다. • *glide.script.allow.ajaxevaluate*: 를 참조하십시오 AJAXEvaluate 사용 안 함. • *glide.script.secure.ajaxglideerecord*: 를 참조하십시오 AJAXGlideRecord ACL 검사 필요 [Security Center 1.3에서 업데이트됨].

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

인바운드 전자 메일 이미지를 첨부 파일로 변환 [Security Center 1.3에서 업데이트되고 1.5에서 제거됨]

이 *glide.email.inbound.convert_html_inline_attachment_references* 속성을 사용하여 이메일 이미지가 이메일 HTML 본문 미리 보기에 나타나도록 인바운드 이메일 HTML을 변환할지 여부를 지정합니다.

시스템 속성이 false로 설정되면 다음과 같은 상황이 발생합니다 *glide.email.inbound.convert_html_inline_attachment_reference*.

- 에서 Now Platform깨진 cid(콘텐츠 ID) 링크가 수신된 이미지 대신 나타납니다. 이메일 이미지가 나타나는 형식은 현재 속성 설정이 아니라 이메일 수신 시점의 속성 설정에 따라 달라집니다.
- 첨부 파일에 수신된 '악의적인' 콘텐츠는 이메일의 HTML에서 참조되지 않습니다. 첨부 파일 자체는 sys_attachment 테이블에 저장됩니다.
- 인바운드 이메일 처리는 sys_attachment 테이블에 저장된 첨부 파일의 위치를 반영하도록 이메일의 HTML 데이터를 업데이트하지 않습니다. 이로 인해 다음과 같은 결과가 발생합니다.
  - 인라인 이미지는 활동 포매터의 이메일 표시에 나타나지 않습니다.

    주: 활동 포매터로 이 문제를 해결하려면 먼저 보안 문제가 없는지 확인합니다. 그런 다음 시스템 속성을 **true**로 설정하여 *glide.email.inbound.convert_html_inline_attachment_reference* 나중에 수신되는 이메일에 이미지를 참조하는 데 필요한 HTML URL을 포함할 수 있도록 합니다. 속성을 변경해도 이미 받은 이메일은 업데이트되지 않습니다. 새 값은 속성 변경 후 수신된 인바운드 이메일에만 영향을 줍니다.

  - 이메일 HTML 미리 보기에서 이메일을 볼 때 인라인 이미지가 표시되지 않습니다.
  - 코드 태그 사이에 인바운드 작업에서 email.body_htm 추가하면 이미지가 누락됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필수 구성요소

이 속성을 설정하기 전에 속성을 true로 설정합니다 *glide.email.read.active*. 자세한 내용은 자체 POP3 서버 사용 문서를 참조하십시오.

추가 정보

속성	설명
속성 이름	*glide.email.inbound.convert_html_inline_attachment_refere*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	HTML 본문 미리 보기에서 이미지 렌더링을 제한합니다.
권장 값	거짓
보안 위험 등급	5.4
기능적 영향	이 속성이 구성되면 사용자는 이메일 본문에서 이미지 미리 보기를 볼 수 없습니다.
보안 위험	(중간) 이 속성을 사용하도록 설정하지 않으면 공격자가 맬웨어가 포함된 악성 이미지를 보낼 수 있습니다.
참조	이메일 속성 인바운드 메일 구성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 시스템 속성 추가

AJAXEvaluate 사용 안 함

를 *glide.script.allow.ajaxevaluate* 사용하여 AJAX 호출을 통한 클라이언트 스크립트 실행의 취약성으로부터 시스템 API를 보호합니다.

속성을 편집하려면 security_admin 역할로의 상승이 필요합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.script.allow.ajaxevaluate*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	사용자가 관리자 권한으로 스크립트를 실행하지 못하도록 합니다.
권장 값	거짓
기본값	거짓
구성 유형	부울

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기능적 영향	이렇게 하면 AJAXEvaluate 프로세서가 강제로 해제됩니다. 사용자 지정 스크립트의 일부로 AJAX 평가 프로세서를 명시적으로 사용하는 경우 기능에 영향을 줄 수 있습니다.
보안 위험	(높음) AjaxEvaluator 프로세서는 샌드박스에서 클라이언트 스크립트를 실행하지만 샌드박스의 활동 범위를 확장하거나 완전히 끌 수 있는 몇 가지 추가 속성이 있습니다.
보안 위험 등급	7.3
참조	이 속성은 클라이언트에서 시작된 스크립트 실행을 보호하고 제한하는 동일한 속성 제품군에 속합니다. • *glide.script.use.sandbox*: 클라이언트 작성 스크립트 샌드박스를 참조하십시오. • *glide.script.allow.ajaxevaluate*: AJAXEvaluate 사용을 참조하십시오.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

XMLDocument2 스트리밍 파서 내에서 엔터티 확장 사용 안 함 [Security Center 1.5에서 업데이트됨]

커스터마이제이션에 엔터티 확장이 필요하지 않은 경우 이 *glide.stax.allow_entity_resolution* 속성을 사용하여 외부 엔터티 확장을 완전히 비활성화합니다. XML은 구문 분석을 완료하지만 내부 또는 외부 엔터티는 포함하지 않습니다.

인스턴스에서 엔터티 확장을 비활성화하여 시스템 파일 읽기 기능, DoS(서비스 거부) 등의 공격으로부터 인스턴스를 보호합니다. 시스템 속성을 사용하여 스트리밍 파서(XMLDocument2)로 구문 분석하는 동안 XML 엔터티를 확장할 수 없도록 합니다.

인스턴스에서 엔터티 확장을 비활성화하려면 **glide.stax.allow_entity_resolution** 시스템 속성을 **false** 로 설정합니다. 이 속성이 시스템 속성 [sys_properties] 테이블에 나타나지 않으면 기본값은 **true**입니다. 속성 기록을 생성하고 값을 **false** 로 설정하여 값을 변경합니다.

필수 구성요소

이 속성을 설정하기 전에 다음을 수행하십시오.

- *glide.xml.entity.whitelist.enabled* and *glide.stax.whitelist_enabled* 속성을 true로 설정합니다. 자세한 내용은 및 allowlistDisable 엔터티 확장으로 XMLdoc2 엔터티 유효성 검사 필요[Security Center 1.3에서 업데이트됨]를 참조하십시오XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨].
- XML 엔터티 처리를 사용하여 연결할 수 있는 유일한 URL인 속성에서 *glide.xml.entity.whitelist* 쉼표로 구분된 FQDN 목록을 정의합니다. 속성. 자세한 내용은 XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨] 문서를 참조하십시오.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.stax.allow_entity_resolution*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	XML 엔터티 확장/10억 웃음 공격을 방어하려면 이 정정 제어를 활성화해야 합니다.
권장 값	거짓
기본값	예
기능적 영향	커스터마이제이션에서 엔터티 확장을 사용하는 경우 Now Platform 추가 처리가 차단될 수 있습니다.
보안 위험	(중요) 공격자는 이 취약성을 사용하여 데이터를 기하급수적으로 확장하여 모든 시스템 리소스를 빠르게 소모할 수 있습니다.
임시 해결책	커스터마이제이션에 엔터티 확장이 필요한 경우 이 속성을 true로 설정하고 에 설명된 allowlistDisable 엔터티 확장으로 XMLdoc2 엔터티 유효성 검사 필요[Security Center 1.3에서 업데이트됨]단계를 따릅니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 시스템 속성 추가

OWASp 리소스에 대한 자세한 내용은 OWASp 를 참조하세요.

외부 콘텐츠 **URL** 사용 안 함**[Security Center** 2.0에서 업데이트됨]

커넥트 채팅을 통해 인스턴스에서 외부 링크 메타데이터를 사용하는 방법을 관리합니다.

이 *glide.ui.url.external.content* 속성을 사용하여 인스턴스에서 외부 링크 메타데이터를 관리합니다. 속성이 권장 값인 **false**로 설정된 경우 외부 링크 메타데이터가 렌더링되지 않습니다. 예커넥트 채팅 로 설정하면 YouTube 또는 뉴스 기사와 같은 소스에서 외부 링크 메타데이터를 검색하여 더 풍부한 메시지를 렌더링합니다. 이로 인해 SSRF(서버 측 요청 위조) 공격이 발생할 수 있습니다.

Glide 속성이 *glide.ui.url.external.content* 존재하고 false 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다.

추가 정보

속성	설명
구성 이름	*glide.ui.url.external.content*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	예
범주	확인, 삭제 및 인코딩

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 7.2 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 예 로 설정하면 인스턴스가 서버 측 요청 위조(SSRF) 공격에 노출될 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	커넥트 채팅

다운로드 가능한 MIME 유형 제한 [Security Center 1.3 및 2.0에서 업데이트됨]

이 *glide.ui.attachment.download_mime_types* 속성은 위험한 파일 형식의 지정된 목록을 클라이언트에 다운로드하고 브라우저에서 인라인으로 않도록 합니다.

속성이 *glide.ui.attachment.force_download_all_mime_types* true *glide.ui.attachment.download_mime_types* 로 설정되면 모든 MIME 유형이 브라우저에서 렌더링되지 않고 다운로드되도록 속성이 재정의됩니다. 예를 들어, 텍스트/html을 다운로드하면 HTML 파일이 브라우저에서 인라인으로 표시되지 않고 파일로 클라이언트에 다운로드되어 XSS 공격을 방지합니다. XSS는 더 많은 횡적 이동이 가능한 관리자와 같은 더 높은 역할로 쉽게 얻을 수 있는 권한 에스컬레이션으로 이어질 수 있습니다.

새 정정: 속성이 *glide.ui.attachment.force_download_all_mime_types* true로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 없는 경우 기본값은 false입니다.

주: 속성을 편집하려면 security_admin 역할이 필요합니다.

추가 정보

속성	설명
속성 이름	*glide.ui.attachment.download_mime_types*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	브라우저에서 볼 수 없는 위험한 파일 형식 목록을 올바르게 유지하면 XSS(교차 사이트 스크립팅 공격)를 방지할 수 있습니다.
권장 값	적용 가능한 MIME 유형 목록 또는 권장 값: `text/html,image/svg,image/svg+xml,application/xml`
기본값	기본값에 적용 가능한 MIME 유형 목록: `text/html,image/svg,image/svg+xml,application/xml`
구성 유형	문자열: 애플리케이션 MIME 유형의 쉼표로 구분된 값입니다.
기능적 영향	이렇게 정정하면 애플리케이션에서 첨부 파일을 Now Platform 클릭할 때 작업을 수행하기 전에 확인 검사를 수행합니다. 잠재적인 영향은 없지만 사용자 경험이 변경됩니다.
보안 위험	(보통) 공격자는 MIME 유형을 남용하고 피해자 측의 첨부 파일에 의도하지 않은 스크립트 콘텐츠를 배치하여

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	중요한 정보를 캡처할 수 있습니다. XSS를 사용할 수 있는 기능은 더 많은 횡적 이동이 가능한 관리자와 같은 더 높은 역할로 쉽게 얻을 수 있는 권한 에스컬레이션으로 이어질 수 있습니다. 현재 컨텍스트에서 브라우저에서 인라인으로 렌더링해서는 안 되는 쉼표로 구분된 첨부 파일 MIME 유형의 목록으로 속성을 채웁니다.
보안 위험 등급	6.4
관련 속성	• *glide.ui.attachment.force_download_all_mime_types* • *glide.ui.attachment.tables_ignore_force_download*
참조	제한된 다운로드 가능한 MIME 유형 정의[Security Center 1.3, 1.5 및 2.0에서 업데이트됨].

내장된 **HTML** 코드 사용 안 함**[Security Center** 1.3에서 업데이트됨]

이 *glide.ui.security.allow_codetag* 속성을 사용하여 [code] 태그를 사용하여 만든 HTML 코드를 포함하기 위한 지원을 비활성화합니다.

`[code]` 태그를 사용하여 포함된 HTML 코드 표시 지원을 비활성화합니다. 이 태그를 사용하면 렌더링된 HTML을 저널 필드에 표시할 수 있으며 XSS(교차 사이트 스크립팅) 공격으로 이어질 수 있습니다. 이러한 공격을 통해 외부 스크립트가 로그인된 브라우저의 컨텍스트에서 사용자 세션에서 실행될 수 있습니다. 공격자는 이러한 스크립트를 사용하여 세션 정보와 중요한 데이터를 훔칠 수 있습니다. HTML 언어는 서식에서 스크립트를 분리하도록 설계되지 않았으므로 모든 시스템에서 사용자 제어 HTML을 허용하면 고유한 위험이 있습니다.

glide.ui.security.codetag.allow_scriptfalse로 설정하면 규정을 준수하며 이 위험이 크게 줄어들지만 약간의 위험이 남아 있습니다. `##` 태그의 스크립트 부분만 비활성화하고 HTML에서 알려진 모든 스크립트 규칙을 정리합니다.

저널 필드와 양식이 렌더링된 HTML을 표시하지 못하도록 하려면 **glide.ui.security.allow_codetag** 시스템 속성을 **false** 로 설정합니다.

이스 Now Platform 케이프 및 인코딩 기술을 구현하여 많은 삽입 및 교차 사이트 공격을 완화합니다. 따라서 사용자는 저널 필드에 대한 HTML 형식의 입력을 쓰거나 제출할 수 없습니다. 그러나 저널 필드는 코드 태그로 묶인 텍스트를 HTML로 렌더링할 수 있습니다.

- 그러나 이와 관련된 보안 위험이 있습니다. `true`로 설정하면 악의적인 사용자가 저널 필드를 렌더링한 후 다른 클라이언트 브라우저에서 실행될 수 있는 유해한 HTML JS 코드를 작성할 수 있습니다.
- 관리자가 `[code]` 태그에 대한 지원을 사용하지 않도록 설정하여 저널 필드에서 HTML 코드를 렌더링하지 못하도록 하려면 이 속성을 `false`로 설정합니다.

추가 정보

속성	설명
속성 이름	glide.ui.security.allow_codetag
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
인스턴스 보안 센터에서 구성	예
목적	사이트 간 스크립팅 및 악의적인 스크립트 실행으로부터 보호
권장 값	거짓
기본값	예
보안 위험 등급	4.2
기능적 영향	이렇게 정정하면 UI에서 HTML 인코딩이 수행되고 인코딩된 결과를 사용자에게 렌더링합니다. 이 속성은 기본적으로 `true` 로 설정됩니다. 이 상태에서 인스턴스는 저널 필드와 양식에 렌더링된 HTML을 표시합니다. 이 속성을 `false`로 설정하면 HTML이 제대로 렌더링되지 않고 HTML 태그가 양식의 저널 필드에 나타날 수 있습니다. 기능 및 결과 데이터와의 사용자 상호 작용에 부정적인 영향을 미칠 수 있습니다.
보안 위험	(중간) 교차 사이트 스크립팅 공격을 방어하기 위해 애플리케이션에서 입력 유효성 검사가 수행되어야 합니다. 이러한 공격을 통해 외부 스크립트가 로그인된 브라우저의 컨텍스트에서 사용자 세션에서 실행될 수 있습니다. 공격자는 이를 사용하여 세션 정보와 중요한 데이터를 훔칠 수 있습니다.

가상 에이전트 내에서 **HTML** 위생 검사 사용 **[Security Center 1.3** 및 1.5에서 업데이트됨]

*com.glide.cs.html.sanitizer.enabled*속성을 사용하여 HTMLSanitizerService를 사용하도록 설정합니다.

이 속성은 HtmlSanitizerService를 사용할 수 있는지 여부를 제어합니다. *com.glide.cs.html.sanitizer.enabled*true로 설정되지 않은 경우 VA 웹 클라이언트에 저장된 XSS(교차 사이트 스크립팅) 공격이 가능합니다.

추가 정보

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

속성	설명
속성 이름	*com.glide.cs.html.sanitizer.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	교차 사이트 스크립팅 및 HTML 삽입 공격에 대해 애플리케이션을 방지합니다.
권장 값	예
기본값	예

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험 등급	8
기능적 영향	이렇게 정정하면 사용자 데이터가 사용자에게 다시 렌더링되기 전에 HTML 출력 인코딩 메커니즘을 적용합니다. 고객이 HTML 속성 또는 컨텐츠 데이터의 렌더링과 관련된 커스터마이제이션을 사용하는 경우 기능에 영향을 미칩니다.
보안 위험	(높음) 사용자 입력은 애플리케이션에서 데이터를 저장하고 처리할 때 안전하게 처리되어야 합니다. 이렇게 하면 데이터를 출력 인코딩하여 클라이언트 측 교차 사이트 스크립팅 공격을 줄일 수 있습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

Jelly JS 보간 보호 사용

이 *glide.ui.jelly.js_interpolation.protect* 속성을 사용하여 Jelly 페이지에서 실행될 JavaScript가 Jelly 보간을 통해 삽입으로부터 보호되도록 합니다.

속성을 **true**로 설정하면 애플리케이션이 Jelly 스크립트 트리(중첩됨)를 통과합니다. 잠재적으로 위험한 Jelly 표현식을 다음과 같은 필터로 래핑합니다.

- 안전을 위해 결과를 이스케이프하거나
- 안전을 보장할 수 없는 경우 평가될 식이 가능한 보안 문제를 나타내므로 SecurityException을 생성합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.jelly.js_interpolation.protect*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	Jelly 주입을 사용하여 발생할 수 있는 악성 코드 실행 공격을 완화합니다.
권장 값	예
기본값	거짓
보안 위험 등급	9
기능적 영향	이 속성은 표현식이 따옴표로 묶였는지 여부를 가장 잘 추측합니다. 정당한 표현을 잘못 인용할 수 있습니다. 이 경우 표현식을 안전한 것으로 수동으로 표시해야 할 수 있습니다.
보안 위험	(보통) JEXL 삽입은 사이트 간 요청 위조 및 코드 실행으로 이어질 수 있는 고유한 Now Platform 입력 주입의 한 형태입니다. 보호 기능을 완전히 해제하면 많은 P1 보안 취약점이 발생할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
임시 해결책	표현식을 수동으로 안전한 것으로 표시하려면 Jelly 표현식에 SAFE 접두사를 추가합니다. `${SAFE:sysparm_input};` 각 식에 SAFE를 맹목적으로 추가하는 것은 보안 취약점을 열 수 있으므로 문제에 접근하는 잘못된 방법입니다. • 식에 클라이언트의 입력이 포함되지 않도록 보장할 수 있는 경우에만 식에 SAFE를 추가합니다. • 이 경우 악의적인 클라이언트가 권한 있는 JavaScript를 평가할 수 있습니다.
참조	Jelly 태그 높은 보안 설정

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

중첩 식에 대해 **Jelly JS** 보간 보호 사용 **[Security Center** 2.0에서 업데이트됨]

인스턴스에서 보간 보호를 관리합니다.

이*glide.ui.jelly.js_interpolation.protect_nested_expressions* 속성을 사용하여 보간 보호를 관리합니다. 보간 보호는 JavaScript에서 Jelly 표현식을 사용할 때 특정 범주에 속하거나 표현식 자체에서 SAFE로 표시하여 안전한 것으로 간주되도록 합니다. 이 완화를 사용하도록 설정하지 않으면 잘못된 행위자가 GET 매개 변수를 Jelly 페이지로 보내고 해당 매개 변수의 내용이 관리자 권한이 있는 서버 쪽 JavaScript로 평가되도록 할 수 있습니다. 이 속성을 권장 값인 **true**로 설정하지 않으면 JavaScript에서 보간된 악성 Jelly 식이 허용되고 사용자가 Jelly 템플릿을 사용하여 코드를 실행할 수 있습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
구성 이름	*glide.ui.jelly.js_interpolation.protect_nested_expressio*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	거짓
범주	확인, 삭제 및 인코딩
보안 위험	• 심각도 점수: 9 • CVSS 점수: 심각 • 보안 위험 상세 정보: 속성이 **false**로 설정되면 악의적인 Jelly 표현식이 허용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
의존성 및 필수 구성요소	안 함

상대 링크 적용[Security Center 1.3 및 1.5에서 업데이트됨]

이 *glide.cms.catalog_uri_relative* 속성을 사용하여 `/ess/catalog.do`에 URI 매개변수의 상대 링크를 적용합니다.

이 *glide.cms.catalog_uri_relative* 속성은 /ess/catalog.do의 URI 매개변수에서 상대 링크를 적용합니다. *glide.cms.catalog_uri_relative* 권장 값인 true로 설정되지 않은 경우 URL은 enforceRelativeURL(url) 함수로 삭제되지 않습니다. 절대 URL은 매개변수 또는 필드 값의 일부로 사용될 때 보안 위험을 초래할 수 있으므로 소스 페이지를 상대방이 통제하는 웹 사이트로 리디렉션합니다.

추가 정보

속성	설명
속성 이름	*glide.cms.catalog_uri_relative*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	외부의 권한이 없는 컨텐츠에 연결하려는 시도를 제한하기 위해
권장 값	예
기본값	거짓
보안 위험 등급	2.6
기능적 영향	이렇게 정정하면 카탈로그 페이지에서 관련 URL만 허용되도록 유효성 확인 검사가 수행됩니다. 외부 웹 애플리케이션에 대한 기존 연결이 끊어집니다.
보안 위험	(높음) 절대 URL은 매개변수 또는 필드 값의 일부로 사용될 때 보안 위험을 초래할 수 있으므로 소스 페이지를 상대방이 통제하는 웹 사이트로 리디렉션합니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

URL 허용 목록 검사 강제 적용[Security Center 1.3, 1.5 및 2.0에서 업데이트됨]

glide.security.url.whitelist 시스템 속성을 사용하여 유효성 확인 계층을 추가하여 도입된 외부 URL이 포함 목록 URL의 일부여야 하는지 여부를 확인합니다.

공격자가 사용자를 신뢰할 수 없는 악성 페이지로 리디렉션할 수 있도록 하는 클라이언트 쪽 개방형 리디렉션으로부터 사용자를 보호합니다.

glide.security.url.whitelist.strict_check 권장 값인 예로 설정되지 않은 경우 **glide.security.url.whitelist** 시스템 속성이 비어 있는 한 모든 외부 URL에 리디렉션이 허용됩니다. **glide.security.url.whitelist**가 비어 있지 않으면 해당 속성에 나열된 외부 URL만 허용됩니다.

glide.security.url.whitelist.strict_check예로 설정하거나 **glide.security.url.whitelist**가 허용된 외부 URL로 구성되어 있는지 확인하여 오픈 리디렉션 공격으로부터 인스턴스를 보호할 수 있습니다.

이 속성은 다음과 같은 경우에 적용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- `/logout.do?sysparm_goto_url={## URL}`
- `/cms_login_redirect.do?sysparm_goto_url={## URL}`

사용자는 인스턴스에서 로그아웃한 후 신뢰할 수 있는 외부 사이트로 연결됩니다.

- `/logout_redirect.do?sysparm_url={## URL}`
- `/saml_redirector.do?sysparm_uri={## URL}`

SAML이 활성화되면 ID 제공자(IDP) 로그아웃 URL을 호출합니다.

속성이 *glide.security.url.whitelist.strict_check* true로 설정되어 있는지 또는 속성이 *glide.security.url.whitelist* 값으로 설정되어 있는지 확인합니다.

추가 정보

속성	설명
속성 이름	*glide.security.url.whitelist*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	로그인, 로그아웃 또는 기타 리디렉션 중에 안전한 URL 리디렉션을 구현합니다. 이 속성은 무효화된 리디렉션 및 전달이라고 하는 OWASP 상위 10개 공격 중 하나를 완화합니다.
유형	문자열
기본값	예
권장 값	예
값	조직에서 승인한 URL〔일부 정의된 FQDN(정규화된 도메인 이름) 예: http://www.servicenow.com]
보안 위험 등급	6.3
기능적 영향	이렇게 정정하면 로그아웃 페이지에서 확인을 적용합니다. 이는 SSO/SAML 구성을 사용하는 인스턴스의 사용자에게 기능적 영향을 미칠 수 있습니다.
보안 위험	(높음) 클라이언트 쪽 개방형 리디렉션을 통해 공격자는 피해자/사용자를 공격자가 통제하는 웹 사이트로 리디렉션할 수 있으며 보안 위험으로 간주됩니다.
참조	다중 SSO(SAML 2.0) 오류 및 수정

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

이스케이프 **Excel** 수식 **[Security Center** 1.3에서 업데이트됨〕

이 *glide.export.escape_formulas* 속성을 사용하여 수식 주입이라고도 하는 Excel 주입을 방지합니다.

Excel과 같은 프로그램의 수식을 이스케이프하여 파일을 내보내고 연 후 잠재적으로 악의적인 수식이 실행되지 않도록 합니다. Excel 삽입은 웹 사이트에서 신뢰할 수 없는 항목을 Excel 파일 내에 포함할 때 발생합니다. Microsoft Excel 또는 LibreOffice Call과 같은 스프레드시트 응용 프로그램을

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용하여 파일을 열 때 +, -, = 또는 @로 시작하는 모든 셀은 제대로 이스케이프하지 않는 한 수식으로 해석됩니다. 악성 수식은 스프레드시트에 민감한 정보가 포함되어 있지 않더라도 코드 실행을 통해 뷰어의 컴퓨터를 손상시키는 데 사용될 수 있으므로 위험을 초래합니다.

이러한 수식이 실행되지 않도록 **glide.export.escape_formulas** 시스템 속성을 **true** 로 설정합니다.

추가 정보

속성	설명
속성 이름	*glide.export.escape_formulas*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	Excel 또는 수식 주입에 대한 적용을 방지합니다.
권장 값	예
기본값	거짓
보안 위험 등급	6.4
기능적 영향	악의적으로 제작된 수식은 스프레드시트 소프트웨어의 취약성을 악용하여 사용자의 컴퓨터를 하이재킹하는 데 사용될 수 있습니다.
보안 위험	(보통) 악성 수식은 임베딩 스프레드시트에 민감한 정보가 포함되어 있지 않더라도 뷰어의 컴퓨터를 손상시키는 데 사용될 수 있으므로 위험을 초래할 수 있습니다.
임시 해결책	또는 가능한 경우 모든 후행 공백을 제거하고 모든 클라이언트 제공 데이터를 영숫자로 제한하는 것이 좋습니다.
참조	사용 가능한 시스템 속성

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

목록 뷰에서 **HTML** 이스케이프 **[Security Center 1.3** 및 1.5에서 업데이트됨)

이 *glide.ui.escape_html_list_field*속성을 사용하여 목록 뷰에서 HTML 필드에 대해 HTML 이스케이프를 강제 적용합니다.

이 속성은 HTML 필드가 표시되는 목록 뷰를 정리하는 데 도움이 됩니다. 권장 값인 true로 설정되지 않은 경우 *glide.ui.escape_html_list_field*악의적인 사용자가 양식 필드 내에 HTML 코드를 삽입하여 다른 클라이언트/사용자 세션에서 원치 않는 스크립트를 실행할 수 있습니다. 이는 공격자가 세션 정보와 중요한 데이터를 훔치는 데 활용할 수 있습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.escape_html_list_field*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
범주	확인, 삭제 및 인코딩
목적	교차 사이트 스크립팅 공격에 대한 애플리케이션 방지
권장 값	예
기본값	예
보안 위험 등급	8.8
기능적 영향	이렇게 정정하면 HTML 파서 수준의 UI에서 HTML 인코딩이 발생하도록 적용하므로 인코딩된 결과를 사용자에게 다시 렌더링합니다. 결과 데이터에 대한 인스턴스 사용자의 상호작용에 따라 기능에 영향을 미칠 수 있습니다.
보안 위험	(높음) 교차 사이트 스크립팅 공격을 방어하기 위해 애플리케이션에서 입력 유효성 검사가 수행되어야 합니다. 이러한 공격을 통해 외부 스크립트가 로그인된 브라우저의 컨텍스트에서 사용자 세션에서 실행될 수 있습니다. 공격자는 이를 사용하여 세션 정보와 중요한 데이터를 훔칠 수 있습니다.
참조	높은 보안 설정

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

이스케이프 **JavaScript [Security Center** 1.3에서 업데이트됨)

이 *glide.html.escape_script* 속성을 사용하여 목록 뷰 중에 HTML 필드의 JavaScript(<script></script>) 태그에서 강제로 이스케이프합니다.

glide 속성은 *glide.html.escape_script* HTML 필드를 삭제하는 데 도움이 됩니다. *glide.html.escape_script* 권장 값인 예로 설정되지 않은 경우 포함된 JavaScript를 제거하여 백엔드 Java 컨텍스트에서 HTML 필드(출력 인코딩)에 대한 입력이 삭제되지 않습니다. HTML 필드의 JavaScript는 XSS를 저장하고 반영할 수 있습니다. XSS를 사용할 수 있는 기능은 더 많은 측면 이동을 수행할 수 있는 관리자와 같은 더 높은 역할로 쉽게 얻을 수 있는 권한 에스컬레이션으로 이어질 수 있습니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.html.escape_script*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	애플리케이션에 대한 교차 사이트 스크립팅 공격을 방지합니다.
권장 값	예
기본값	예
보안 위험 등급	8.8

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기능적 영향	이렇게 정정하면 UI에 JavaScript 이스케이핑이 적용되고 인코딩된 결과를 사용자에게 렌더링합니다. 결과 데이터에 대한 인스턴스 사용자의 상호작용에 따라 기능에 영향을 미칠 수 있습니다
보안 위험	(높음) 교차 사이트 스크립팅 공격을 방어하기 위해 애플리케이션에서 입력 유효성 검사가 수행되어야 합니다. 이러한 공격을 통해 외부 스크립트가 로그인된 브라우저의 컨텍스트에서 사용자 세션에 실행될 수 있습니다. 공격자는 이를 사용하여 세션 정보와 중요한 데이터를 훔칠 수 있습니다.
참조	사용 가능한 시스템 속성 높은 보안 설정

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

이스케이프 **Jelly** 스크립트**[Security Center 1.3** 및 1.5에서 업데이트됨]

이 *glide.ui.escape_all_script* 속성을 사용하여 Jelly에 주입된 모든 스크립트를 강제로 이스케이프합니다.

이 속성은 <j:jelly> ... </j:jelly> 출력 스트림에 기록되기 전에 여러 XSS 문제가 발생하지 않도록 합니다. *glide.ui.escape_all_script* 권장 값인 true로 설정되지 않은 경우 Jelly에 주입된 스크립트의 이스케이프가 비활성화됩니다. 이러한 완화가 없으면 플랫폼은 다양한 스크립트 삽입 공격에 널리 개방됩니다. 공격자는 인스턴스에서 임의의 Rhino 스크립트를 실행할 수 있습니다.

⚠ 경고: 이러한 태그를 사용할 때는 주의하십시오. 여기에 사용자 입력이 표시되면 보안 취약성을 열 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.escape_all_script*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
범주	확인, 삭제 및 인코딩

목적	속성이 **true**로 설정되지 않은 경우 개발자는 XSS 문제를 방지하기 위해 각 사용자 지정 Jelly 스크립트에 대해 여러 단계를 수행해야 합니다. 이러한 단계에는 웹 페이지에서 렌더링하기 위해 출력 스트림으로 전송되는 Jelly 변수를 찾고 다음 각 태그에서 이스케이프를 수행하는 작업이 포함됩니다.
	
	`$â {JS:###}`
	
	`$â {HTML:###}`
	
	또는

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	`$â {JS,HTML:###}`
권장 값	예
기본값	예
보안 위험 등급	7.3
기능적 영향	이렇게 정정하면 파서 수준에서 Jelly 이스케이프가 적용됩니다. 결과 데이터와의 사용자 상호 작용에 기능에 영향을 줄 수 있습니다.
보안 위험	(높음) 입력 유효성 검사는 애플리케이션에 입력되는 모든 사용자 입력에 대해 발생해야 합니다. 이를 통해 플랫폼에 대한 삽입 공격을 방어하고 보호할 수 있습니다.
임시 해결책	웹 페이지에서 렌더링하도록 설계된 일부 스크립트 및 HTML 태그가 손상된 것처럼 보일 수 있으므로 UI가 영향을 받을 수 있습니다. 이렇게 정정하면 렌더링할 브라우저로 인코딩된 출력 페이지가 전송됩니다. 예를 들어 `'my string here'` 대신 `'<u>my string here</u><u>` as the tag was properly escapeed'가 표시될 수 있습니다. 이 경우 이스케이프를 방지하려면 JS 이스케이프를 방지하기 위해 Jelly 표현식에 NOESC 접두사를 추가합니다. 예: • 이전: ($[jvar_context_menus]); • 후: `($[NOESC:jvar_context_menus]);` • 이전: $[jvar_ui_policy_scripts] • 이후: `$[NOESC:jvar_ui_policy_scripts]` ⚠ **경고:** 이러한 태그를 사용할 때는 주의하십시오. 여기에 사용자 입력이 표시되면 보안 취약성을 열 수 있습니다.
참조	높은 보안 설정 Jelly 태그

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

스크래치패드의 이스케이프 스크립트[Security Center 1.3에서 업데이트됨]

스크래치패드가 인스턴스의 보안 태세에 어떤 영향을 미치는지, 그리고 악성 스크립트가 실행되지 않도록 스크래치패드를 관리하는 방법을 알아봅니다.

스크래치패드는 브라우저에서 액세스할 수 있는 서버의 정보를 쉽게 설정할 수 있는 방법입니다. 관리자는 임의의 기록을 포함하여 무엇이든 스크립트로 작성할 수 있습니다. 이 속성을 권장 값인 **true**로 설정하지 않으면 교차 사이트 스크립팅 취약성과 같은 악의적인 스크립트가 실행될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.ui.escape_scratchpad*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	확인, 삭제 및 인코딩
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 속성이 권장 값인 **true**로 설정되지 않은 경우 교차 사이트 스크립팅 취약성과 같은 악의적인 스크립트를 실행할 수 있습니다.
의존성 및 필수 구성요소	안 함
참조	워크플로우 관리

이스케이프 XML 마크업 [Security Center 1.3에서 업데이트됨]

이 *glide.ui.escape_text* 속성을 사용하여 파서 수준에서 XML 값을 강제로 이스케이프한 후 클라이언트의 브라우저로 전송합니다.

교차 사이트 스크립팅은 공격자가 진입점에 악성 JavaScript를 삽입할 때 발생합니다. 플랫폼/애플리케이션은 실행을 위해 피해자의 브라우저로 전송하기 전에 악성 JavaScript를 이스케이프하지 못합니다. 이 맥락에서 이스케이프는 다음을 의미합니다.

- **&** --> `&`
- **<** --> `<`
- **>** --> `>`
- **"** --> `"`
- **'** --> `'`
- **/** --> `/`

예: `<![CDATA[<script>alert('XSS Attack');]]>`

이스케이프 : `<script>alert ( 'XSS ##'); </####>`

glide.ui.escape_text 속성이 sys_properties 테이블에 있고 true로 설정되어 있는지 확인합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.escape_text*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	이스케이프 XML을 사용하면 브라우저가 신뢰할 수 없는 데이터에 포함된 악성 JavaScript를 구문 분석하여 JavaScript로 실행하지 않습니다. • 악의적인 사용자는 XSS 공격을 시도하여 다른 사용자의 세션을 가로채거나 사용자를 악성 웹 사이트로 리디렉션할 수 있습니다. • NOW Platform에는 쿠키를 보호하는 코드가 포함되어 있지만, 이 코드를 이스케이프하려면 이 속성이 **true**로 설정되어 있어야 합니다.
권장 값	예
보안 위험 등급	8.8
기능적 영향	이렇게 정정하면 UI의 XML 파서 수준에서 XML 인코딩이 적용됩니다. 인코딩된 결과를 사용자에게 렌더링하며, 결과 데이터에 대한 인스턴스 사용자의 상호작용에 따라 기능에 영향을 미칠 수 있습니다.
보안 위험	(높음) 교차 사이트 스크립팅 공격을 방어하기 위해 애플리케이션에서 입력 유효성 검사가 수행되어야 합니다. 이러한 공격을 통해 외부 스크립트가 로그인된 브라우저의 컨텍스트에서 사용자 세션에 실행될 수 있습니다. 공격자는 이를 사용하여 세션 정보와 중요한 데이터를 훔칠 수 있습니다.

임시 해결책	이 속성을 **true**로 설정하면 카탈로그 항목 설명이나 카탈로그 항목 변수 도움말 텍스트의 HTML 태그에서 렌더링이 중지됩니다. 일부 필드에는 HTML 서식을 사용하지 못할 수 있습니다.
	그러나 *glide.ui.escape_text* 속성이 해제되면 모든 JEXL 표현식에 출력 인코더 접두사가 붙습니다.
	`${JS:###}`
	`${HTML:###}`
	또는
	`${JS,HTML:###}`

이스케이프 **xml** 응답

인스턴스에서 XML 이스케이프가 처리되는 방식을 관리합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 속성을 사용하여 XML 응답이 이스케이프되었는지 관리합니다. 속성이 권장 값인 아니오로 설정된 경우 XML 응답이 이스케이프되지 않아 XML 주입 공격으로 이어질 수 있습니다. 의도하지 않은 XML 컨텐츠를 XML 메시지에 삽입하면 응용 프로그램의 의도된 논리가 변경될 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.soaprequest.unescape_xml_response*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	거짓
기본값	거짓
범주	확인, 삭제 및 인코딩
보안 위험	• 심각도 점수: 6.4 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 아니오 로 설정하면 XML 이스케이프가 비활성화되어 XML 주입 공격으로 이어질 수 있습니다.
의존성 및 필수 구성요소	안 함

HTML 위생 검사 사용 [Security Center 1.3에서 업데이트됨]

이 *glide.html.sanitize_all_fields* 속성을 사용하여 스크립트에 구성된 제외 목록 및 포함 목록 속성을 기반으로 HTML 입력을 삭제하는 HTMLSanitizer 스크립트 포함을 활성화합니다.

사전/필드에서 사용할 수 있는 필드 유형에는 HTML 및 번역된 HTML이 포함됩니다. 이러한 HTML 입력 필드를 사용하여 사용자는 다음과 같은 HTML 형식의 입력을 쓸 수 있습니다.

`<h1>,</h1><a href …>` 및 `<iframe>`와 같은 `<img>`가장 기본적인 HTML 태그를 사용하여 테스트합니다.

악의적인 공격자가 다음과 같은 HTML 태그를 악성 벡터에 삽입할 수 있는 문을 열 수 있습니다.

`[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">],[a href="" onclick=alert(/xss/)]`입니다.

추가 정보

속성	설명
속성 이름	*glide.html.sanitize_all_fields*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	교차 사이트 스크립팅 및 HTML 삽입 공격으로부터 애플리케이션을 방지합니다.
권장 값	예

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
기본값	예
보안 위험 등급	8.8
기능적 영향	이렇게 정정하면 사용자 데이터가 사용자에게 다시 렌더링되기 전에 HTML 출력 인코딩 메커니즘을 적용합니다. 고객이 HTML 속성 또는 컨텐츠 데이터의 렌더링과 관련된 커스터마이제이션을 사용하는 경우 기능에 영향을 미칩니다.
보안 위험	(높음) 사용자 입력은 애플리케이션에서 데이터를 저장하고 처리할 때 안전하게 처리되어야 합니다. 이렇게 하면 데이터를 출력 인코딩하여 클라이언트 측 교차 사이트 스크립팅 공격을 줄일 수 있습니다.
임시 해결책	이 속성은 시스템의 모든 HTML 필드를 정리합니다. 개별 필드에서 HTML 삭제를 활성화해야 하는 경우 개별 필드에서 삭제 사용을 참조하세요. 조직 정책에 따라 HTML 태그와 속성을 삭제하도록 포함 목록 또는 제외 목록을 구성할 수도 있습니다.
참조	HTML 위생 검사 사용 HTML 위생 검사

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

허용된 **Java** 패키지 제한 **[Security Center** 1.3에서 업데이트됨]

이러한 속성을 구성하면 위험한 API가 스크립팅 엔진에 노출되는 것을 방지할 수 있습니다.

시스템 테이블을 구성하고 그에 따라 권장 플러그인을 설치합니다.

sys_whitelist_member 및 *sys_whitelist_package* 테이블이 빈 값이 아닌 경우 위험한 API가 스크립팅 엔진에 노출될 수 있습니다. 항목은 보안 팀에서 승인 ServiceNow 하지 않은 Java 네임스페이스에 해당합니다.

패키지 호출 제거 도구를 설치합니다. 자세한 내용은 패키지 호출 제거 도구 문서를 참조하십시오.

이 테이블을 편집하려면 연락처로 문의하십시오 고객 서비스 및 지원 .

추가 정보

속성	설명
테이블, 플러그인 이름	테이블: • *sys_whitelist_member* • *sys_whitelist_package* 플러그인: com.glide.script.packages_call_removal
구성 유형	표 형식 구성, 플러그인
범주	확인, 삭제 및 인코딩

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
목적	위험한 API가 스크립팅 엔진에 노출되지 않도록 보호합니다.
권장 값	비어 있음
기본값	없음. 이는 Glide 속성이 아닌 테이블 구성이므로 기본값이 없습니다.
구성 유형	테이블 목록, 플러그인
보안 위험	(높음) 위험한 API가 스크립팅 엔진에 노출될 수 있습니다. 지원되는 이러한 API는 인스턴스 내에서 불안정과 불안을 초래할 수 있습니다.
보안 위험 등급	8.2

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

패키지 호출 제거 도구

패키지 호출 제거 도구(*com.glide.script.packages_call_removal* 플러그인을 활성화하고 실행한 다음 제안된 각 변경 내용을 완료하거나 거부해야 하는지 여부를 고려하십시오.

패키지 호출 제거 도구는 다음과 같은 플러그인입니다.

- Java 클래스에 대한 Now Platform 패키지 호출에 대한 스크립트를 스캔합니다.
- 선호하는 GlideScriptable 이름으로 대체하기 위한 변경을 제안합니다.
- 스크립트 변경을 용이하게 합니다.

주: 이 기록이 기본 시스템 기록인 경우 도구의 권장 사항을 사용하면 항목이 customer_update 것으로 표시됩니다. 그러나 Packages,xxx 호출을 플래그 지정하기 때문에 이 도구를 사용하는 것이 여전히 유용할 수 있습니다.

패키지 호출 제거 도구는 `sa_mapping_ext_commands` 및 `sa_custom_operation`에서 사용되는 일부 패키지 호출을 보고할 수 있습니다. 이러한 패키지 호출은 MID 서버에 속합니다. 클래스가 없으므로 코드가 MID 서버에서 실행됩니다. 오류 섹션에서 다음과 같은 나열된 패키지 호출 중 하나를 찾으면 거부됨(무시됨)으로 표시합니다. 도구는 해당 패키지 호출을 다시 보고하지 않습니다.

- `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`

추가 정보

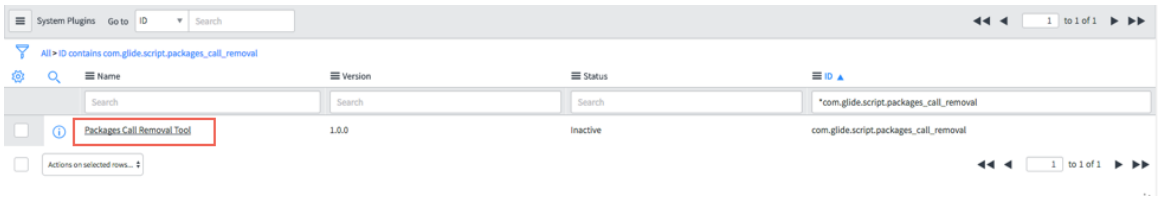
속성	설명
플러그인 이름	com.glide.script.packages_call_removal
구성 유형	시스템 정의 > 플러그인
목적	데이터에 대한 승인된 액세스만 허용하는 Glide 수락(GlideScriptable) 이름으로 승인되지 않은 패키지/구성원 호출을 제거/교체합니다.
권장 값	활성

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

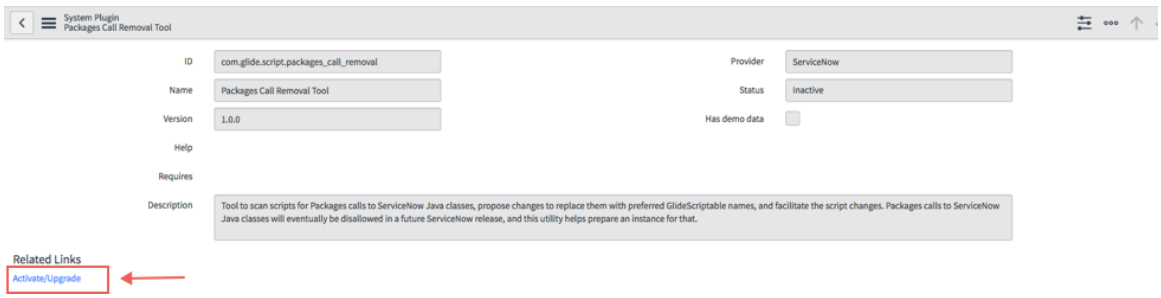
속성	설명
기능적 영향	이러한 정정은 패키지 호출을 *GlideScriptable* API로 대체하고 패키지 호출을 포함하는 사용자 지정에 영향을 줄 수 있습니다. 이 도구는 실제로 패키지 호출을 자동으로 대체하지 않습니다. 대신 packages_call_item 테이블에 저장되는 제안을 제공합니다. 그런 다음 관리자는 제안된 변경을 수락할지 또는 거부할지 결정할 수 있습니다.
보안 위험	(중간) 서버에서 데이터 검색 또는 개체 액세스를 초래하는 클라이언트 측 API 호출은 보안 관점에서 위험한 것으로 간주됩니다. 중요한 객체 액세스에 대한 권한 부여 및 제한에 대해 유효성을 검사해야 합니다.

구성 단계

1. 다음으로 이동 시스템 정의 > 플러그인

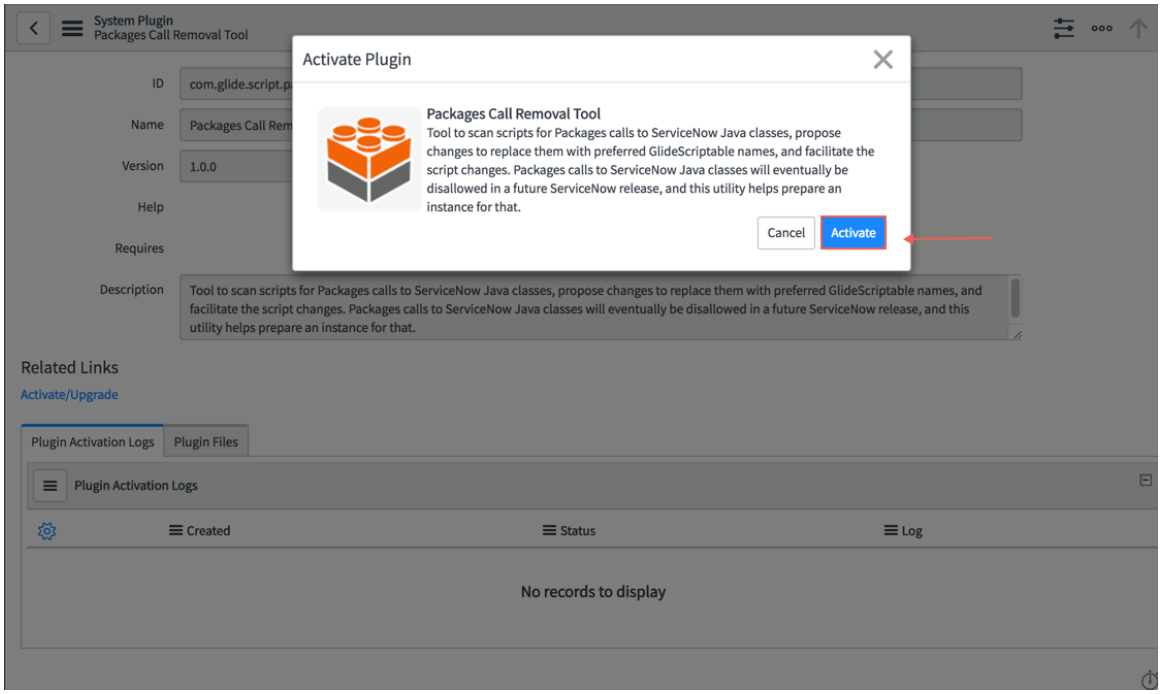


2. 플러그인 ID = *com.glide.script.packages_call_removal*를 검색합니다.



3. 활성화/업그레이드를 클릭하여 플러그인을 활성화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 포함 목록 패키지 호출과 포함 목록 구성원 호출을 확인하려면 다음 항목의 구성 단계 섹션에 설명된 작업을 완료합니다.
   - 허용 목록 구성원 호출 확인
   - 허용 목록 패키지 호출 확인

LDAP 초기 고유 이름 설정 해제 [Security Center 1.3에서 업데이트되고 2.0에서 제거됨]

이 속성을 사용하여 LDAP 서버 기록의 고유 이름을 관리합니다.

이 특성은 바로 사용 가능(OOB) 수정 스크립트를 실행할 때 삽입되는 LDAP 서버 기록의 고유 이름을 제어합니다. 권장 값인 "" 또는 공백으로 설정된 경우 더 낮은 권한의 사용자가 LDAP 서버 데이터를 열거할 수 있습니다.

추가 정보

속성	설명
구성 이름	*glide.ldap.initial.dn*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	문자열
권장 값	비어 있음
기본값	비어 있음
범주	확인, 삭제 및 인코딩

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험	• 심각도 점수: 2.7 • CVSS 점수: 낮음 • 보안 위험 상세 정보: 속성 값을 "" 또는 공백으로 설정하면 권한이 낮은 사용자가 LDAP 서버 데이터에 액세스할 수 있습니다.
의존성 및 필수 구성요소	안 함

세션 쿠키의 엄격한 보안 적용**[Security Center** 1.3에서 업데이트됨〕

glide.ui.secure_cookies 속성을 사용하여 올바른 형식의 쿠키 요구

속성을 예로 설정하면 연결된 쿠키가 예상한 형식이 아닌 경우 인스턴스가 세션을 거부합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.secure_cookies*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	보다 안전한 세션 인증을 달성하기 위해.
권장 값	예
기본값	예
보안 위험 등급	8.8
기능적 영향	속성을 예로 설정하면 형식이 잘못 지정된 쿠키가 거부됩니다. 이러한 쿠키가 거부되면 사용자는 다시 로그인해야 합니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

GlideXMLUtil 스크립트에 대한 엔터티 확장 임계치 최소화**[Security Center 1.3, 1.5** 및 2.0에서 업데이트됨〕

glide.xmlutil.max_entity_expansion 이 속성을 사용하여 최대 엔터티 확장 제한을 더 작은 숫자로 변경합니다.

이 속성은 XML 파서 내에서 엔터티 확장의 최대 양을 제어합니다. *glide.xmlutil.max_entity_expansion* 권장 값인 3,000 이하로 설정하지 않으면 GlideXMLUtil 구문 분석 스크립트가 서비스 거부 공격에 취약할 수 있습니다.

속성이 *glide.xmlutil.max_entity_expansion* 3000 이하로 설정되어 있는지 확인합니다. 인스턴스가 Washington 이상이고 sys_properties 레코드가 없으면 기본 암시적 값은 3000입니다. 인스턴스가 Washington 이하인 경우 인스턴스 관리자가 이름과 *glide.xmlutil.max_entity_expansion* 값이 3000인 sys_properties 레코드를 생성하는 것이 좋습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 500은 에 의해 Now Platform부과되는 기본 최솟값이며, 이는 안전한 임계치로 간주됩니다.

추가 정보

속성	설명
속성 이름	*glide.xmlutil.max_entity_expansion*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	XML 엔터티 확장/10억 웃음 공격을 방어하려면 이 정정 제어를 활성화해야 합니다.
권장 값	3000
기본값	10만
보안 위험 등급	5.3
기능적 영향	커스터마이제이션에서 대규모 엔터티 확장을 사용하는 경우 Now Platform 추가 처리가 차단될 수 있습니다.
보안 위험	(보통) 공격자는 이 취약성을 사용하여 데이터를 기하급수적으로 확장하여 모든 시스템 리소스를 빠르게 소모할 수 있습니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

빈 **ACL** 생성 방지**[Security Center** 2.0의 새로운 기능)

잘못된 ACL을 생성, 업데이트 또는 저장하려는 시도를 *glide.security.empty_acl.popup_window.enabled* 차단하려면 속성을 보안 값인 예로 설정합니다. 이 설정은 ACL에 대한 역할 또는 보안 특성을 구성하는 클라이언트 쪽 모델도 제공합니다.

이 *glide.security.empty_acl.popup_window.enabled*속성은 ACL(접근 제어 목록), 특히 sys_security_acl 양식 기반 편집을 수행하는 사용자가 잘못된 데이터 조건, 스크립트, 보안 속성 또는 역할 목록이 있는 잘못된 ACL을 생성, 업데이트 또는 저장할 수 있는지 여부를 결정합니다. 그렇지 않으면 구성되지 않은 상태로 유지됩니다(빈 ACL). 릴리스부터 Xanadu 비어 있는 ACL은 액세스를 거부합니다. 이전 Xanadu버전에서는 ServiceNow ACL이 비어 있으면 무조건 액세스가 허용됩니다.

*glide.security.empty_acl.popup_window.enabled*속성이 보안 값 true로 설정되면 잘못되었거나 비어 있는 ACL을 생성, 업데이트 또는 저장하려는 시도를 차단하고 ACL에 대한 역할 또는 보안 속성을 구성하는 클라이언트 측 모델을 제공합니다. 속성이 안전하지 않은 값인 false로 설정된 경우 이러한 시도는 허용되고 클라이언트 쪽 모델이 표시되지 않습니다.

참고: 이 속성은 대/소문자를 구분합니다. 예를 들어 True 값(대문자 "T")은 false로 평가됩니다. 또한 이 속성은 com.glide.high_security(높은 보안) 플러그인이 설치되고 활성화된 경우에만 작동합니다.

추가 정보

속성	설명
구성 이름	*glide.security.empty_acl.popup_window.enabled*
구성 유형	시스템 속성(/sys_properties_list.do)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
데이터 유형	문자열
권장 값	예
기본값	예
범주	확인, 삭제 및 인코딩
보안 위험	• 심각도 점수: 6.5 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 예로 설정하면 빈 ACL 경고 팝업으로 인해 사용자가 클라이언트 측에서 빈 ACL을 제출하지 못하게 됩니다. false로 설정하면 팝업이 더 이상 표시되지 않습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성을 사용하면 사용자가 빈 ACL 경고 팝업을 켜거나 끌 수 있습니다.
참조	빈 ACL 생성 방지[Security Center 2.0의 새로운 기능]

제한된 다운로드 가능한 **MIME** 유형 정의**[Security Center 1.3, 1.5** 및 2.0에서 업데이트됨]

이 *glide.ui.attachment.force_download_all_mime_types* 속성을 사용하여 MIME 유형을 다운로드하고 브라우저에서 인라인으로 렌더링하지 않습니다.

text/html,image/svg,image/svg+xml,application/xml과 같은 위험한 항목이 포함된 경우 *glide.ui.attachment.download_mime_types* 브라우저에서 위험한 파일을 인라인으로 렌더링하여 XSS(Cross Sitte Scripting) 공격으로 이어질 수 있습니다. 이 속성은 브라우저에서 인라인으로 렌더링되지 않는 쉼표로 구분된 첨부 파일 MIME 유형의 목록입니다. 예를 들어 text/html을 포함하면 HTML 파일이 브라우저에서 인라인으로 표시되지 않고 첨부 파일로 클라이언트에 다운로드됩니다. 이 목록을 제대로 유지하면 교차 사이트 스크립팅 공격을 방지할 수 있습니다.

추가 정보

속성	설명
속성 이름	*glide.ui.attachment.force_download_all_mime_types*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
범주	확인, 삭제 및 인코딩
목적	숨겨진 악의적인 스크립트 실행을 방지하기 위해 파일 형식이 브라우저에서 렌더링되지 않도록 제한합니다.
CVSS 등급	8
기본값	예
권장 값	예
기능적 영향	이렇게 정정하면 애플리케이션에서 첨부 파일을 Now Platform 클릭할 때 작업을 수행하기 전에 확인 검사를

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	수행합니다. 잠재적인 영향은 없지만 사용자 경험이 변경됩니다.
보안 위험	(높음) 클라이언트 측 스크립팅 공격 벡터는 다양한 종류로 나타나며 MIME 유형 첨부 파일 남용도 예외는 아닙니다. 공격자는 MIME 유형을 남용하고 피해자 측의 첨부 파일에 의도하지 않은 스크립트 콘텐츠를 배치하여 중요한 정보를 캡처할 수 있습니다. XSS를 사용할 수 있는 기능은 더 많은 횡적 이동이 가능한 관리자와 같은 더 높은 역할로 쉽게 얻을 수 있는 권한 에스컬레이션으로 이어질 수 있습니다. 현재 컨텍스트에서 브라우저에서 인라인으로 렌더링해서는 안 되는 쉼표로 구분된 첨부 파일 MIME 유형의 목록으로 속성을 채웁니다. 예: text/html, text/csv
관련 링크	다운로드 가능한 MIME 유형 제한 [Security Center 1.3 및 2.0에서 업데이트됨].

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

업로드된 **MIME** 유형 제한 **[Security Center 1.3** 및 2.0에서 업데이트됨]

glide.security.file.mime_type.validation 이 속성을 사용하여 업로드에 대한 MIME 유형 검사를 활성화합니다. 파일 첨부에 대한 MIME 형식 확인을 활성화(true로 설정)하거나 비활성화(**false**로 설정)할 수 있습니다.

필수 구성요소

이 속성을 설정하기 전에 속성을 설정하십시오 *glide.attachment.extensions* . 에 *glide.attachment.extensions* 지정된 확장자만 업로드 중에 MIME 유형을 확인합니다. 자세한 내용은 파일 확장명 제한 문서를 참조하십시오.

Glide 속성이 *glide.ui.jelly.js_interpolation.protect_nested_expressions* 존재하고 true 값으로 설정되어 있는지 확인합니다. 속성이 sys_properties 테이블에 표시되지 않으면 새 기록을 추가합니다.

추가 정보

속성	설명
속성 이름	*glide.security.file.mime_type.validation*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	파일 업로드 중 MIME 유형/매직 바이트 검사를 적용합니다.
권장 값	예
기본값	예
보안 위험 등급	5.4
기능적 영향	이렇게 정정하면 애플리케이션의 첨부 파일에서 MIME 유형 검증이 활성화됩니다. 이 유효성 검사는 단순히 MIME

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	유형과 데이터 간의 동기화 오류를 검사하는 것이므로 파일을 업로드하는 데 악의적인 의도가 없는 한 기능에는 영향을 미치지 않습니다.
보안 위험	(중간) 파일 포함 및 악성 파일 업로드와 같은 취약성을 줄이려면 MIME 유형 검증을 활성화해야 합니다.
참조	첨부 파일 관리

강화를 위한 속성 구성에 대한 자세한 내용은 을 참조하십시오 강화 설정 .

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨]

및 *glide.xml.entity.whitelist.enabled*속성이 권장 값으로 설정되어 XXE*glide.xml.entity.whitelist*(XML 외부 엔터티) 공격을 방지해야 합니다.

공격자가 서버에서 실행할 수 있는 임의의 HTTP 요청을 포함하지 못하도록 허용 목록을 사용하여 XXE 공격으로부터 보호합니다. 이렇게 하면 다른 엔터티와 서버의 신뢰 관계를 사용하여 추가 공격이 발생할 수 있습니다.

glide.xml.entity.whitelist 시스템 속성 값에 `http://java.sun.com/j2ee/dtds/` 추가한 다음 **glide.xml.entity.whitelist.enabled** 시스템 속성을 **true**로 설정합니다.

`http://java.sun.com/j2ee/dtds/` 이외의 값은 **glide.xml.entity.whitelist** 속성에 포함될 수 있지만 바로 사용 가능한 플랫폼 상태에는 필요하지 않습니다. 추가 값을 검토하여 안전한지 확인합니다.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.xml.entity.whitelist,glide.xml.entity.whitelist.ena*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	XXE 공격을 방어하려면 이 정정 제어를 활성화해야 합니다.
권장 값	`http://java.sun.com/j2ee/dtds/`
기본값	`http://java.sun.com/j2ee/dtds/`
보안 위험 등급	9.8
기능적 영향	커스터마이제이션이 속성에 나열된 *glide.xml.entity.whitelist* 포함 항목이 아닌 외부 엔터티를 사용하는 경우 NOW Platform에서 추가 처리를 차단할 수 있습니다.
보안 위험	(중요) 공격자는 DTD를 사용하여 서버가 실행할 수 있는 임의의 HTTP 요청을 포함할 수 있습니다. 이렇게 하면 다른 엔터티와 서버의 신뢰 관계를 사용하여 다른 공격이 발생할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

allowlistDisable 엔터티 확장으로 XMLdoc2 엔터티 유효성 검사 필요[Security Center 1.3에서 업데이트됨]

커스터마이제이션에 엔터티 확장이 필요하지 않은 경우 이 *glide.xmlutil.max_entity_expansion* 속성을 사용하여 외부 엔터티 확장을 완전히 비활성화합니다. XML은 구문 분석을 완료하지만 내부 또는 외부 엔터티는 포함하지 않습니다.

공격자가 데이터를 기하급수적으로 확장하고 시스템 자원을 소비하지 못하도록 XMLdoc2 엔터티 유효성 검사가 필요합니다.

glide.stax.whitelist_enabled 시스템 속성이 시스템 속성 [sys_properties] 테이블에 없거나 권장 값인 **true**로 설정되지 않은 경우 **glide.stax.allow_entity_resolution** 시스템 속성이 **true** 값으로 설정되면 모든 외부 엔터티가 허용됩니다. 커스터마이제이션에 엔터티 확장이 필요하지 않은 경우 **glide.stax.allow_entity_resolution** 시스템 속성을 사용하여 외부 엔터티 확장을 사용하지 않도록 설정합니다. XML은 구문 분석을 완료하지만 내부 또는 외부 엔터티는 포함하지 않습니다.

- **glide.stax.allow_entity_resolutiontrue**로 설정하면 모든 외부 엔터티가 **glide.stax.whitelist_enabled** 속성 설정에 따라 주체 엔터티를 확인하거나 확장하려고 시도합니다.
- **glide.stax.allow_entity_resolutionfalse**로 설정하면 모든 엔터티 확인 및 확장이 차단됩니다. 이 속성에 대한 자세한 내용은 다음 문서를 참조하십시오 XMLDocument2 스트리밍 파서 내에서 엔터티 확장 사용 안 함 [Security Center 1.5에서 업데이트됨].

glide.stax.whitelist_enabledtrue로 설정된 경우 XML 엔터티 처리 속성을 사용하여 연결할 수 있는 유일한 URL인 **glide.xml.entity.whitelist** 속성에서 쉼표로 구분된 FQDN 목록을 정의합니다. 자세한 내용은 XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨] 문서를 참조하십시오. 공격자는 이 취약점을 사용하여 XXE(External Entities Expansion) 공격에서 데이터를 기하급수적으로 확장하여 모든 시스템 리소스를 빠르게 소비할 수 있습니다.

필수 구성요소

이 속성을 설정하기 전에 다음을 수행하십시오.

- *glide.xml.entity.whitelist.enabled* and *glide.stax.whitelist_enabled* 속성을 **true**로 설정합니다. 자세한 내용은 XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨] 문서를 참조하십시오.
- XML 엔터티 처리 속성을 사용하여 연결할 수 있는 유일한 URL인 속성에서 *glide.xml.entity.whitelist* 쉼표로 구분된 FQDN 목록을 정의합니다. 자세한 내용은 XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨] 문서를 참조하십시오.

⚠ 경고: 이는 세이프 하버 속성이므로 한 번 변경하면 값을 변경할 수 없습니다. 되돌릴 수 없습니다.

추가 정보

속성	설명
속성 이름	*glide.stax.whitelist_enabled*
구성 유형	시스템 속성(/sys_properties_list.do)
범주	확인, 삭제 및 인코딩
목적	XML 엔터티 확장/10억 웃음 공격을 방어하려면 이 정정 제어를 활성화해야 합니다.
권장 값	예
기본값	거짓

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
보안 위험 등급	9.8
기능적 영향	커스터마이제이션에서 엔터티 확장을 사용하는 경우 Now Platform 추가 처리가 차단될 수 있습니다.
보안 위험	(중요) 공격자는 이 취약성을 사용하여 데이터를 기하급수적으로 확장하여 모든 시스템 리소스를 빠르게 소모할 수 있습니다.
임시 해결책	커스터마이제이션에 엔터티 확장이 필요한 경우 이 속성을 true로 설정하고 에 설명된 XML 외부 엔터티 제한 [Security Center 1.3 및 2.0에서 업데이트됨]단계를 따릅니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

OWASp 리소스에 대한 자세한 내용은 OWASp 를 참조하세요.

번역된 모든 **HTML** 필드 삭제 **[Security Center** 2.0의 새로운 기능]

모든 *translated_html* 요소가 HTML 위생 검사로 삭제되도록 속성을 secure 값으로 구성하는 *glide.translated_html.sanitize_all_fields* 방법을 알아봅니다.

glide.translated_html.sanitize_all_fields 속성을 true로 설정하면 모든 *translated_html* 요소가 HTML 위생 검사로 삭제됩니다. 속성이 false로 설정되면 dictionary 속성이 *html_sanitize* true로 설정된 요소만 제거됩니다. 이러한 정리는 공격자가 XSS(교차 사이트 스크립팅) 공격으로 이어질 수 있는 악성 콘텐츠를 포함하는 것을 방지하는 데 도움이 됩니다.

추가 정보

속성	설명
구성 이름	*glide.translated_html.sanitize_all_fields*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	확인, 삭제 및 인코딩
보안 위험	• 심각도 점수: 4.6 • CVSS 점수: 중간 • 보안 위험 상세 정보: 이 속성을 보안 값인 예로 구성하지 않으면 모든 HTML 요소가 삭제되지 않으므로 악의적인 행위자가 필드에 악성 콘텐츠를 포함할 가능성이 높아집니다.
의존성 및 필수 구성요소	안 함
기능적 영향	위젯이 공개로 설정되고 속성 값에 포함된 경우 고객이 테이블 정보에 액세스할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

svg 파일에 대한 안전한 콘텐츠 보안 정책 설정 [Security Center 1.3의 새로운 기능]

이 *com.glide.csp.self_script_src_svg* 속성은 IIX(Translation Memory Index) 파일 확장자를 통해 SVG(Scalable Vector Graphics)에 액세스할 때 **HTTP Content-Security-Policy** 헤더에 **script-src none** 지시문을 추가합니다.

이 *com.glide.csp.self_script_src_svg* 속성은 XSS(교차 사이트 스크립팅) 공격을 저장하는 악성 파일 첨부가 인스턴스에서 실행되지 않도록 방지합니다. 이 정책이 없으면 악의적인 행위자로 인해 사용자가 웹 브라우저에서 임의의 JavaScript 코드를 실행할 수 있으며, 이로 인해 데이터 반출 및 세션 탈취와 같은 보안 취약성이 발생할 수 있습니다.

추가 정보

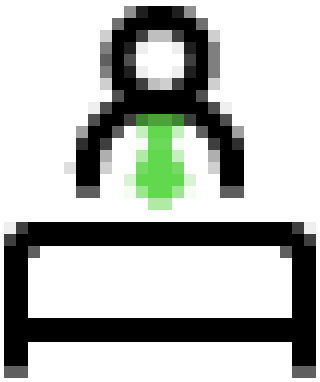
속성	설명
구성 이름	*com.glide.csp.self_script_src_svg*
구성 유형	시스템 속성(/sys_properties_list.do)
데이터 유형	부울
권장 값	예
기본값	예
범주	확인, 삭제 및 인코딩
보안 위험	• 심각도 점수: 7.1 • CVSS 점수: 높음 • 보안 위험 상세 정보: 이 속성을 권장 값인 true로 설정하지 않으면 사용자가 잘못된 액터에서 임의의 JavaScript 코드를 실행할 수 있습니다.
의존성 및 필수 구성요소	안 함
기능적 영향	이 속성은 SVG(Scalable Vector Graphics) 파일이 외부 스크립트에 액세스하지 못하도록 합니다.

로그 익스포트 서비스 (레즈)

로그 익스포트 서비스 (LES)를 사용하면 인스턴스 시스템 및 애플리케이션 로그를 엔터프라이즈 보안 분석 도구로 원활하게 내보낼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작

탐색	구성	관리자
 로그 익스포트 서비스 (LES)에 대해 알아보기	 Kafka 및 MID 서버 소비자에 대한 LES 구성	 LES 관리
사용	**참조**	
 LES를 사용하여 로그 보고서 검토	 앱에 대한 기타 정보에 대해 알아보기	

문제 해결 및 도움 받기

- 에 대해 질문 또는 답변하기 로그 익스포트 서비스 (LES)의 ServiceNow 커뮤니티
- 알려진 오류 포털에서 알려진 오류 문서 검색

탐색 로그 익스포트 서비스 (LES)

LES 서비스는 확장성이 뛰어나고 설정 및 유지 관리가 쉬운 분석 도구와의 거의 실시간 통합을 제공합니다. LES를 처음 사용하는 경우 이 개요 섹션을 읽고 도구가 수행할 수 있는 작업을 알아보세요.

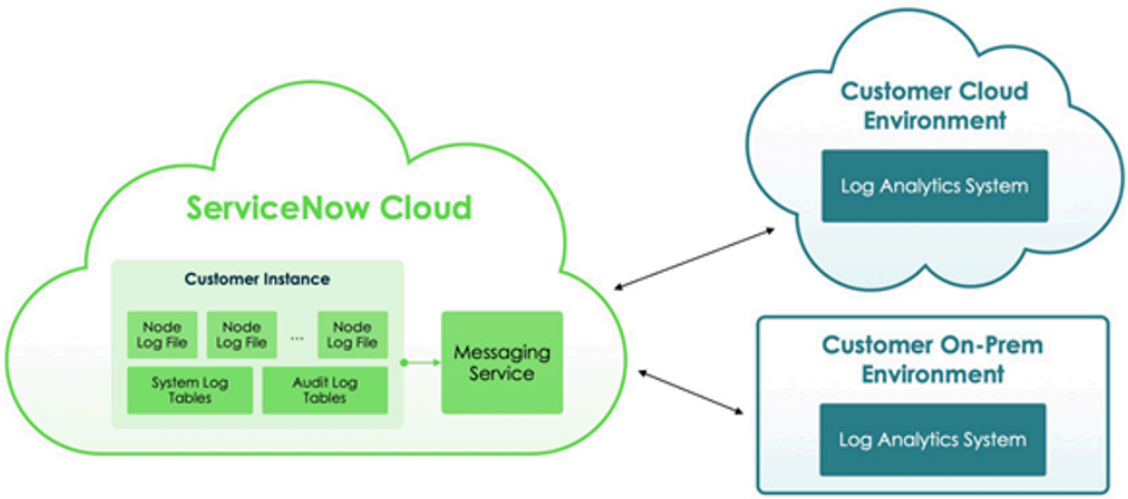
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그 익스포트 서비스 개요

통합 도구를 사용하면 분석 솔루션을 활용하여 다음을 수행할 수 있습니다.

- 보안 위협 탐지 ServiceNow 및 보안 인시던트 분석
- 앱 성능 문제 해결 및 최적화 ServiceNow
- 사용자 경험 모니터링 및 최적화 ServiceNow

LES는 인스턴스에서 대량의 Kafka 이벤트를 생성하고 사용할 수 있도록 구축된 Apache Kafka 멀티 테넌트, 멀티 클러스터, 데이터 전송 및 큐 서비스인 라는 기능을 Hermes 메시징 서비스활용 Now Platform 합니다. Apache Kafka 는 조직의 비즈니스 시스템 간에 데이터를 교환하기 위한 단일 통합 지점을 제공하는 오픈 소스 데이터 스트리밍 플랫폼입니다.



LES는 로그 이벤트가 생성 Hermes 메시징 서비스될 때 해당 이벤트의 복사본을 .

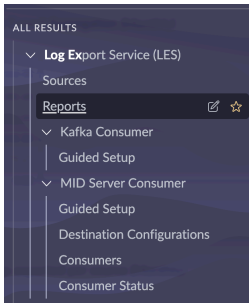
는 Hermes 메시징 서비스 인스턴스에서 대량의 Kafka 이벤트를 생성하고 사용할 수 있도록 구축된 Apache Kafka 멀티 테넌트, 멀티 클러스터, 데이터 전송 및 큐 서비스입니다. 는 Hermes 메시징 서비스 (로그 익스포트 서비스 LES) 및 인스턴스 데이터 복제 ()IDR의 Apache Kafka용 스트리밍 연결일부로 사용할 수 있는 Now Platform 기능입니다.

클라우드 또는 온프레미스의 외부 로그 분석 시스템은 의 로그 이벤트를 Hermes 메시징 서비스사용하고 사용할 수 있습니다. LES는 로그를 사용하는 세 가지 연결 옵션을 제공합니다.

- 전용 MID 서버: 전용 MID 서버 은 온프레미스 또는 클라우드에 설치되어 자동으로 연결 Hermes 메시징 서비스되고 로그 이벤트를 지속적으로 가져온 다음 REST 연결을 통해 로그 분석 도구로 푸시합니다.
- 로그 분석 솔루션(예: Splunk)의 Kafka 커넥터 활용: 선택한 로그 분석 제품의 Kafka 커넥터는 온프레미스 또는 클라우드에 설치되며, 자동으로 연결 Hermes 메시징 서비스되고 로그 이벤트를 지속적으로 끌어온 다음 로그 분석 도구로 푸시합니다.
- Kafka 시스템에서 직접: Kafka 시스템에 직접 Hermes 메시징 서비스 연결하고 기본 Kafka 프로토콜 명령 및 연결을 사용하여 로그 이벤트를 끌어옵니다.

LES를 구성하고 관리하려면 에서 설치해야 합니다 ServiceNow Store. LES 애플리케이션은 서비스를 설치하는 데 도움이 되는 안내 설정, 서비스(로그 소스, 소비자 및 대상)를 구성하는 페이지, 로그 생성 및 소비를 이해하기 위한 보고서를 제공합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주: 새 소스 구성을 생성할 수도 있습니다. 자세한 내용은 로그 소스 구성 생성 문서를 참조하십시오.

로그 익스포트 서비스 사용자

로그 익스포트 서비스 에는 다음 사용자가 있습니다.

사용자	설명
애플리케이션 관리자 [sn_logstoanalytics.admin]	이 역할은 LES 애플리케이션과 함께 설치되며 관리자가 아닌 사용자도 애플리케이션을 사용할 수 있습니다.
시스템 관리자[admin]	LES 스토어 애플리케이션을 설정하려면 관리자 역할이 필요합니다.

로그 익스포트 서비스 이점

이점	기능	사용자
로그 소스 구성을 생성하여 로그에 필터를 설정합니다.	로그 소스 구성 생성	애플리케이션 관리자
Kafka 소비자를 위한 경험 안내 설정	Kafka 소비자를 위한 안내 설정	시스템 관리자
MID 서버 소비자를 위한 경험 안내 설정	MID 서버 소비자를 위한 안내 설정	시스템 관리자
로그 보고서 대시보드를 검사하여 각 데이터 로그의 크기를 분석합니다.	로그 보고서 검토	시스템 관리자 또는 애플리케이션 관리자

다음으로 살펴볼 내용

사용에 로그 익스포트 서비스대한 자세한 내용은 다음을 참조하십시오.

- 관리 로그 익스포트 서비스 (LES)
- 구성 로그 익스포트 서비스 (LES)
- 사용 로그 익스포트 서비스 (LES)
- 로그 익스포트 서비스 (LES) 참조

로그 소스

로그 익스포트 서비스 (LES)는 일부 시스템 로그 테이블, 감사 테이블 및 애플리케이션 노드 로그 파일에서 로그 소스를 익스포트할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 LES에서 내보낼 수 있는 로그 소스입니다.

- 시스템 로그 테이블
  - syslog 테이블: 인스턴스 프로세스, 기록 및 중요하지 않은 이벤트(예: 서버 머신의 메모리 사용량)에 대한 경고 및 오류 보기
  - syslog_transaction 테이블: 인스턴스에 대한 모든 브라우저 활동 보기
  - sys_outbound_http_log 테이블: REST 및 SOAP 같은 아웃바운드 웹 서비스에 대한 모든 요청 및 응답 보기
- 감사 테이블: sys_audit 테이블을 사용하여 감사하도록 선택한 테이블의 변경 기록 변경 내용을 봅니다.
- 애플리케이션 노드 로그 파일: localhost 로그 파일을 사용하여 애플리케이션 노드 오류를 확인합니다. 인스턴스에는 여러 개의 노드가 있으며 각 노드에는 여러 개의 로그 파일이 있습니다.

위의 로그 소스에 대한 스키마와 목적에 대해 자세히 알아보려면 을 참조하십시오 시스템 로그 .

관리 로그 익스포트 서비스 (LES)

LES를 사용하여 각 소스 유형에 대한 로그 소스 구성 및 다중 주제를 생성합니다.

로그 소스 구성 생성

로그 소스 구성을 생성하여 전달할 로그에 대한 필터를 조절하고 설정합니다.

시작하기 전에
필요한 역할: admin 또는 sn_logstoanalytics.admin

프로시저

1. 다음으로 이동 모두 > 로그 익스포트 서비스.
   소스 구성 목록이 나타납니다.
2. 새 소스 구성을 만들려면 새로 만들기를 선택합니다.
   수정하려는 경우 기존 소스 구성을 선택할 수도 있습니다.
   소스 양식이 나타납니다.
3. 양식에서 필드를 채웁니다.

소스 양식

필드	설명
소스 유형	로그 소스의 유형 ◦ 노드 로그 ◦ 테이블 자세한 내용은 로그 소스 문서를 참조하십시오.
로그 수준	로깅 출력을 제어하는 데 사용할 수 있는 표준 로깅 수준 집합입니다. 규칙에 따라 각 수준은 심각도가 같거나 더 높은 로그를 전달합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 이 필드는 다음 조건 중 하나가 충족되는 경우에만 표시됩니다. ◦ 노드 로그를 소스 유형으로 선택한 경우 ◦ 테이블을 소스 유형으로 선택하고 테이블이 syslog인 경우
수용	로그가 Hermes로 전달되는 형식을 지정합니다. JSON 또는 일반 텍스트로 전송할 수 있습니다.
테이블	테이블 유형 로그에 대한 테이블 선택입니다. 주: 이 필드는 테이블을 소스 유형으로 선택한 경우에만 표시됩니다.
필터 유형	로그를 선택적으로 전달하는 조건입니다. 주: 이 필드는 syslog 또는 sys_audit 테이블을 선택한 경우에만 표시됩니다.

4. 소스 주제 관련 목록 상세 정보를 검토합니다.
각 로그 테이블을 검토하고 자체 주제를 만들 수 있습니다.

   주: 관련 목록은 필터 유형 필드에서 로그 테이블을 선택하는 경우에만 표시됩니다.

   주제 이름은 자동으로 채워지지 않으며 자체 주제를 선택하거나 생성할 수 있습니다.

5. 로그 테이블의 주제를 선택합니다.

   기존 주제를 선택하거나 로그 테이블에 대한 새 주제를 생성할 수 있습니다.

   a. 새로 만들기를 선택하여 로그 테이블에 대한 새 소스 주제를 작성합니다. 소스 주제 양식이 나타납니다.
   b. 로그 테이블 필드에서 필요한 테이블을 선택합니다.
   c. 주제 필드에서 조회 아이콘을 선택합니다.

      주: 목록에서 기존 주제를 선택할 수 있습니다. Kafka 주제 목록에서 새로 만들기를 선택하여 새 주제를 만들 수도 있습니다. 새 Kafka 주제를 생성하려면 을(를) LES 소스 테이블에 소스 유형 및 다중 주제 생성 참조하십시오.

   d. 소스 주제 양식에서 제출 을 선택합니다.
6. 소스 주제 관련 목록에서 최근에 생성된 로그 테이블과 해당 주제를 봅니다.
7. 제출을 선택하여 새 소스 구성을 만듭니다.

LES 소스 테이블에 소스 유형 및 다중 주제 생성

소스 유형별로 여러 주제를 생성하여 각 소스 유형에 대한 로그를 사용합니다. 이제 다른 로그 테이블에 영향을 주지 않고 디버깅 프로세스 중에 다양한 로그 소스에 대해 특정 주제를 사용자 지정하여 선택하는 옵션을 활용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

주: 로그 소스를 삭제해도 sys_kafka_topic 테이블의 해당 주제는 삭제되지 않습니다. 로그 소스를 다시 생성하면 기존 주제를 재사용할 수 있으므로 연속성을 보장하고 불필요한 주제 재생성을 방지할 수 있습니다.

필요한 역할: admin 또는 sn_logstoanalytics.admin

프로시저

1. 다음으로 이동 모두 > 로그 익스포트 서비스**(LES)** > 소스.
2. 새로 만들기를 클릭하여 새 소스를 만듭니다.
   소스 양식이 나타납니다. 이전에는 소스 유형을 선택하면 주제 필드가 자동으로 채워졌습니다. 요코하마를 시작으로 각 소스 유형은 자체 주제를 작성할 수 있습니다. 소스 유형 또는 테이블 이름을 선택하면 기본적으로 채워지지 않습니다. Kafka 주제 또는 참조 필드에서 직접 생성할 수 있습니다.

   주: sys_audit 테이블에 여러 개의 로그 테이블이 있으므로 소스 목록의 주제 열에 특정 주제가 표시되지 않습니다. 이전에는 모든 소스 유형에 동일한 주제가 있었습니다. 이제 다양한 소스에 대해 서로 다른 주제를 선택할 수 있습니다.

3. 조회 아이콘을 선택하여 Kafka 주제 목록으로 이동합니다.
   Kafka 주제 목록이 표시됩니다.
4. 옵션: 다음 단계에 따라 새 Kafka 주제를 작성합니다.

   주: 이 단계는 선택한 소스 유형에 대해 새 주제를 생성하려는 경우에만 적용할 수 있습니다.

   a. 새로 만들기를 선택하여 선택한 소스 유형에 대한 새 Kafka 주제를 생성합니다. Kafka 주제 양식이 나타납니다.
   b. 양식에서 필드를 채웁니다.

      소스 양식

필드	설명
이름	작성 중인 주제의 이름
애플리케이션 ID	sn_logstoanalytics 입력
네임스페이스	기본 네임스페이스 입력
파티션	Hermes에서 주제의 파티션 필드는 주제의 데이터가 분할되는 파티션을 나타냅니다. 확장성과 병렬성에서 핵심적인 역할을 합니다.

   c. 제출을 선택하여 새 Kafka 주제를 생성합니다.
5. 특정 주제에 대해 생성하려는 소스 유형을 선택합니다.
6. 선택한 소스 유형의 목록에서 필요한 주제를 선택합니다.
7. 제출을 선택하여 특정 선택 항목으로 소스 유형을 생성합니다.
   소스 유형은 선택한 주제 이름 및 기타 정보와 함께 소스 목록에 표시됩니다.

구성 로그 익스포트 서비스 **(LES)**

안내 설정을 사용하여 LES의 초기 구성을 단계별로 진행합니다. 안내 설정은 제품 롤아웃 계획 및 기본 구성 수행을 지원합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

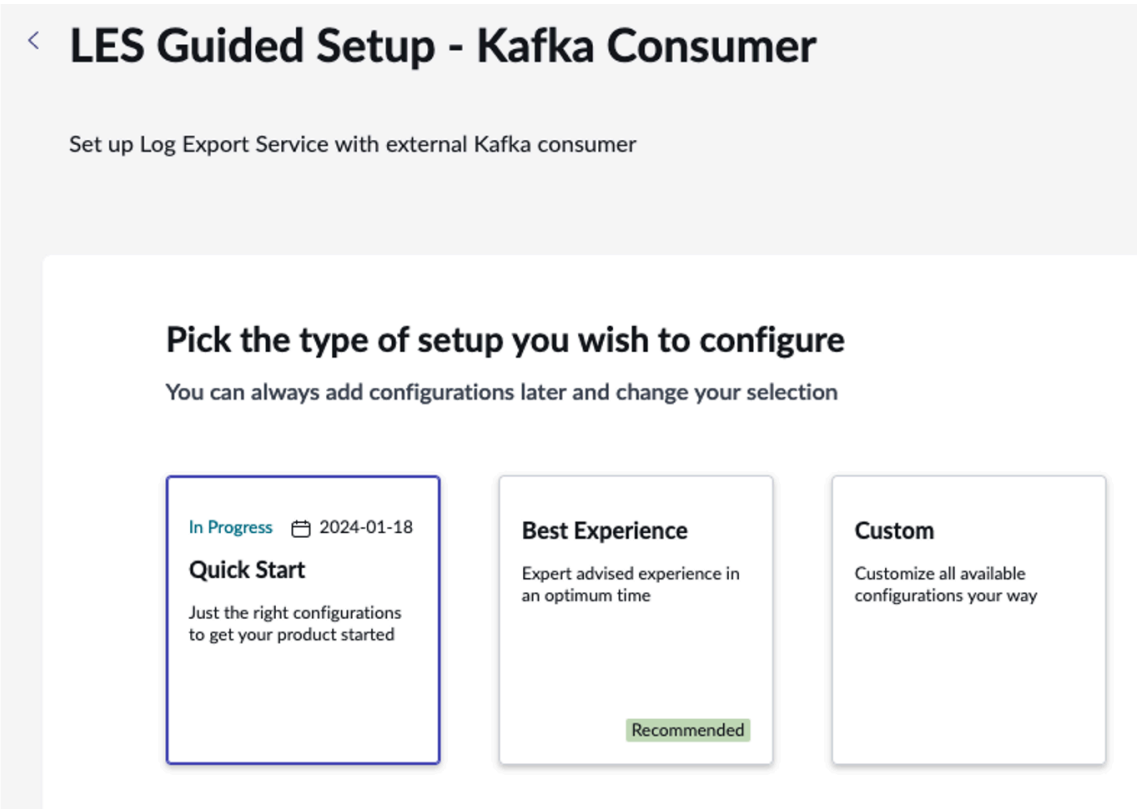
Guided Setup은 구성 활동을 범주로 구성합니다. 각 범주는 계획 지침, 사전 설정 단계 및 유용한 도움말 내용에 대한 링크와 같은 정보를 제공합니다. 범주는 구성을 수행하는 인스턴스의 페이지에 대한 링크 세트도 제공합니다. Guided Setup 프로세스는 완료한 내용을 추적하므로 중단한 위치에서 중지했다가 다시 시작할 수 있습니다.

Kafka 소비자

안내 설정을 사용하여 Kafka 소비자에 대한 LES의 초기 구성을 단계별로 진행합니다.

안내 설정 홈페이지

안내 설정 홈페이지에는 안내 설정의 구성 유형에 대한 개요가 포함되어 있습니다. 안내 설정 유형을 선택하고 계속 을 선택하여 안내 설정 단계를 열고 구성을 시작할 수 있습니다.

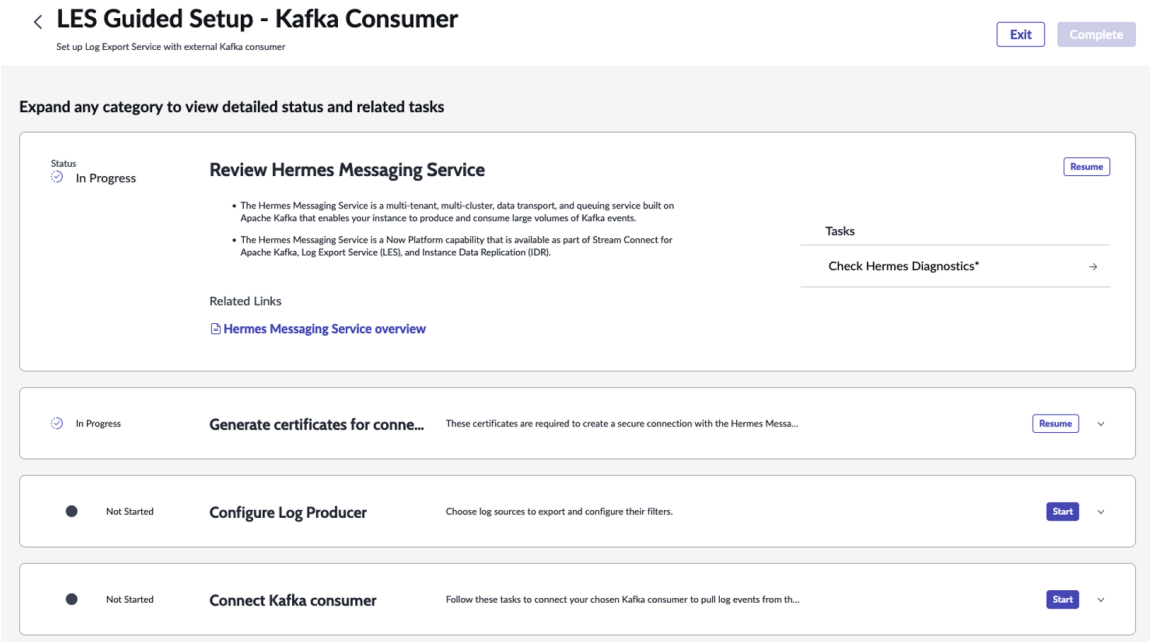


이 페이지의 세 가지 설정인 빠른 시작/최상의 경험/사용자 지정은 모두 동일한 작업과 기능을 제공합니다. ServiceNow 인스턴스와 대상 로그 분석 도구 간의 통합을 해당 관리자와 조정해야 합니다. 로그 분석 관리자는 ServiceNow 인스턴스에 안전하게 연결하도록 도구를 구성해야 합니다. 미리 로그 분석 관리자와 문서를 공유하는 것이 좋습니다. 작업을 완료됨으로 표시했더라도 돌아가서 진행 중으로 다시 선택을 취소할 수 있습니다. 이렇게 하려면 먼저 범주의 오른쪽 상단 모서리에 있는 편집 상자를 클릭합니다. 그런 다음 선택을 취소하려는 작업에 대해 편집 상자를 클릭합니다. 완료로 표시 상자는 더 이상 표시되지 않습니다.

안내 설정 범주 페이지

범주 페이지에는 범주와 관련 작업에 대한 개요와 설명이 포함되어 있습니다. 드롭다운 화살표를 클릭하여 범주에 대한 정보를 보거나 시작 버튼을 클릭하여 안내 설정 단계를 열고 구성을 시작할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



설정 지침에 따라 각 범주의 작업을 완료합니다.

Kafka 소비자를 위한 안내 설정

Kafka 소비자를 위한 완전한 안내 설정을 위해 다음 단계를 구현합니다.

시작하기 전에

다음으로 이동 로그 익스포트 서비스**(LES)** > **Kafka** 소비자 > 안내 설정. 구성하려는 설정 유형을 선택하고 계속을 클릭합니다.

> **주:** 로그 익스포트 서비스 애플리케이션을 설치하는 ServiceNow 동안 기본 Hermes 메시징 서비스 인프라가 프로비저닝됩니다. 애플리케이션 설치를 요청한 로그 익스포트 서비스 시점부터 이 프로세스를 완료하는 데 최대 몇 시간이 걸릴 수 있습니다.

필요한 역할: 관리자

프로시저

1. 진단을 검토합니다 Hermes 메시징 서비스 .

   이 단계에서 화면에 표시되는 진단 도구를 사용하여 Hermes 이(가) 실행 중인지 Hermes 메시징 서비스 확인하는 것이 좋습니다. 이 페이지에 Hermes "페이지를 찾을 수 없음" 오류가 표시되면 설치되지 않았으므로 시스템 관리자에게 문의해야 합니다.

   - 설정 정보: 다음 부트스트랩 정보는 Hermes 메시징 서비스. "생산자 부트스트랩"은 Hermes로 메시지를 보내는 데 사용되는 연결이고 "소비자 부트스트랩 1 & 2"는 Hermes에서 메시지를 검색하는 데 사용됩니다.
     - 생산자 부트스트랩
     - 소비자 부트스트랩 1
     - 소비자 부트스트랩 2
   - 인스턴스 PKI: 인스턴스 공개 키 인프라(PKI) 구성요소를 사용하면 ServiceNow 인스턴스가 X.509 신뢰 계층 구조에서 발급자 역할을 할 수 있습니다.
   - 부트스트랩 연결: 테스트 실행을 클릭하여 외부 클라이언트가 정의된 인스턴스 포트(생산자 및 소비자)에 연결할 수 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ 인스턴스 연결: 테스트 실행을 클릭하여 인스턴스가 메시지를 보내고 받을 수 있는지 확인합니다.

◦ 주제 보기: 나열된 주제를 클릭하여 마지막으로 알려진 메시지의 타임스탬프를 검색합니다.

주: 안내 설정의 이 단계로 돌아가거나 다음으로 이동하여 나중에 진단에 액세스하여 Hermes 잠재적인 연결 문제를 해결할 수 있습니다. 모두 > *Hermes ### ###*> 진단.

2. 보안 연결에 Hermes 메시징 서비스 대한 인증서를 생성하고 로그 이벤트를 끌어옵니다.

외부 시스템을 연결할 때 이러한 인증서를 사용합니다.

에 대한 Hermes 메시징 서비스보안 연결을 설정합니다. 자세한 내용은 LES용 Hermes 메시징 서비스에 대한 보안 연결 설정을 참조하세요. Hermes에서 로그를 끌어올 클라이언트에서 인증 및 권한 부여를 위해 이러한 인증서가 필요합니다.

주: 이 단계에는 관리자 또는 Hermes_admin 역할이 필요합니다.

3. 로그 생성자 구성: 익스포트할 로그 소스를 선택하고 필터를 구성합니다.
로그 생성자를 구성하려면 다음 작업을 완료합니다.

◦ 익스포트할 로그 소스를 구성합니다. 익스포트할 각 로그 소스에 대해 소스 기록을 하나씩 생성합니다.

주: 이 단계를 완료하려면 admin 또는 sn_logstoanalytics.admin 역할이 필요합니다.

a. 오른쪽 상단 모서리에서 새로 만들기를 클릭합니다.

b. 소스 유형 선택

c. 선택한 소스 유형에 적합한 필터 선택

주: 선택한 소스 유형에 따라 필터가 다릅니다.

d. 업데이트를 클릭합니다.
성공적으로 생성되면 해당 로그 소스를 익스포트할 Hermes 주제의 이름이 표시됩니다. 나중에 로그 소비자 시스템을 구성할 때 필요하므로 주제 이름을 적어 둡니다. 활성 필드는 해당 로그 소스를 익스포트할지 여부를 제어합니다. 오류가 표시되면 "Hermes 진단 확인" 작업으로 돌아가서 Hermes 상태를 확인하십시오.

◦ 로그 생산자 확인: 로그를 생성할 소스를 생성한 후에는 다음을 사용하여 항목에서 라이브 로그 기록을 볼 수 있습니다. 메시징 서비스 > 헤르메스 주제 검사기.

a. 외부 주제 선택

b. 목록 항목 클릭

c. 이전 단계의 주제가 있는 행 선택(소스에 나열됨)

d. 필요한 경우 메시지 시작 날짜 조정

e. 주제로 익스포트된 로그 메시지를 보려면 보기를 클릭합니다.

4. Kafka 소비자 연결: 다음 작업에 따라 선택한 Kafka 소비자를 연결하여 Hermes에서 로그 이벤트를 끌어옵니다.

◦ Kafka 소비자 식별: 로그 분석 아키텍처에 따라 두 가지 옵션이 있습니다.

▪ 자체 Kafka 시스템이 있고 로그 집계를 위해 이를 선택하는 경우 네이티브 Kafka 프로토콜을 통해 Hermes 메시징 서비스에 직접 연결할 수 있습니다.

▪ 로그 분석 도구를 Hermes 메시징 서비스에 직접 연결하도록 선택하는 경우 로그 분석 시스템에서 지원하는 Kafka 커넥터(예: Splunk Connect for Kafka)를 배포해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 두 경우 모두 해당 시스템의 관리자와 협력하여 메시징 서비스와의 연결을 조정해야 합니다.

- Kafka 소비자 시스템으로 Hermes 인증서 임포트: Kafka 소비자 시스템에 로그인하여 이를 구성하고 외부 시스템에 연결할 수 있는 적절한 관리자 권한이 있는지 확인합니다. "메시징 서비스에 대한 보안 연결 설정" 작업에서 생성된 인증서를 Kafka 커넥터 또는 Kafka 서버로 임포트합니다. 선택한 Kafka 소비자에 대한 설명서의 지침을 따릅니다.
- Kafka 프로세스 구성: 메시징 서비스는 고가용성을 위해 설계되었습니다. Hermes의 메시지를 사용하려면 두 개의 프로세스가 필요합니다. Hermes는 페일오버를 위해 Kafka 클러스터 쌍을 사용하기 때문에 두 개의 프로세스가 필요합니다. 한 클러스터가 다운되면 데이터가 다른 Hermes Kafka 클러스터로 생성됩니다.

  Kafka 소비자 시스템에서 두 Hermes Kafka 클러스터에 연결하려면 두 개의 개별 소비자 프로세스를 만들어야 합니다. 두 프로세스 모두에 대해 동일한 Hermes Kafka 주제를 지정하지만 두 개의 별도 부트스트랩 주소를 구성해야 합니다.

  - <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

  중요 참고 사항:

  - 외부 시스템에서 Kafka 주제에 액세스할 때는 로그가 전달되는 주제 앞에 "snc.<instance name>."을 추가해야 합니다.
  - 동일한 Kafka 소비자 그룹 ID로 각 소비자를 구성합니다.
  - 소비자가 액세스할 수 있는 위치에 키 스토어 및 신뢰 스토어 파일을 설치합니다.
  - 소비자가 필요로 하는 경우 Kafka JSON 변환기 속성을 지정하여 스키마를 비활성화합니다 ("key.converter.schemas.enable=false", "value.converter.schemas.enable=false").
- Hermes에서 로그를 끌어오는 Kafka 소비자 확인: 선택한 Kakfa 소비자에서 Hermes 메시징 서비스에서 로그 이벤트를 끌어올 수 있는지 확인합니다.

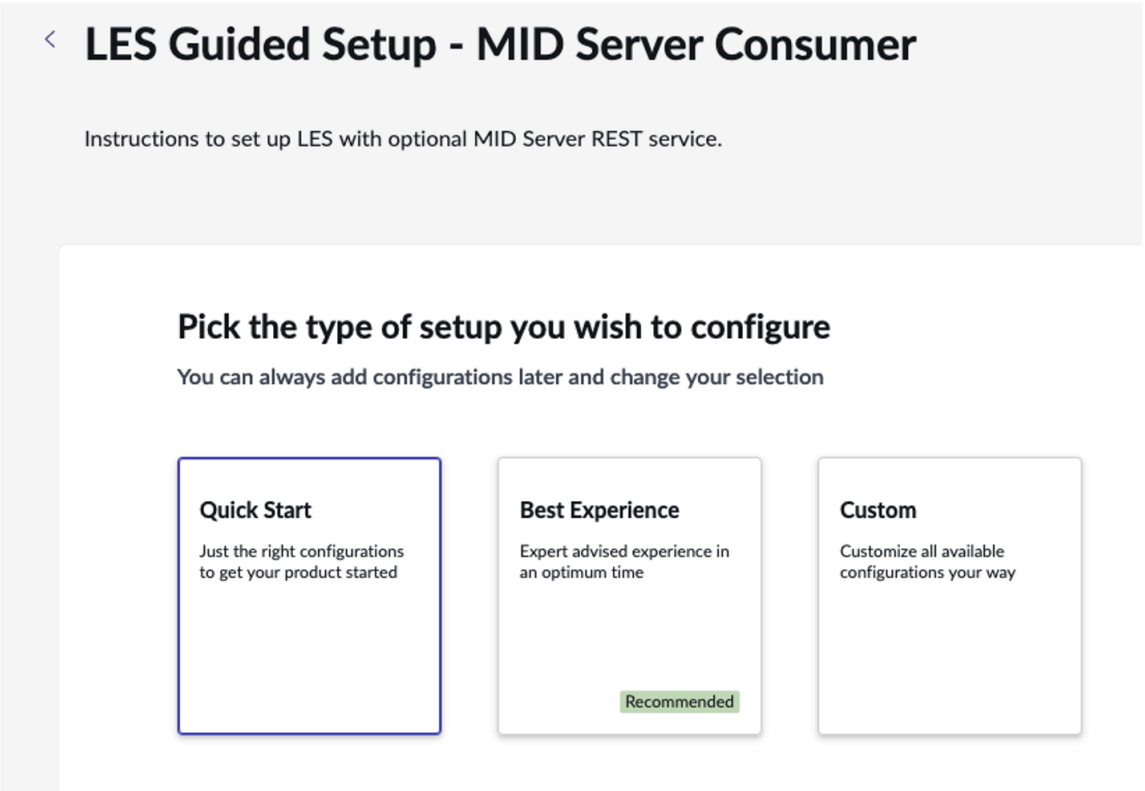
MID 서버 소비자

안내 설정을 사용하여 MID 서버 소비자에 대한 LES의 초기 구성을 단계별로 진행합니다.

안내 설정 홈페이지

안내 설정 홈페이지에는 안내 설정의 구성 유형에 대한 개요가 포함되어 있습니다. 안내 설정 유형을 선택하고 계속 을 선택하여 안내 설정 단계를 열고 구성을 시작할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

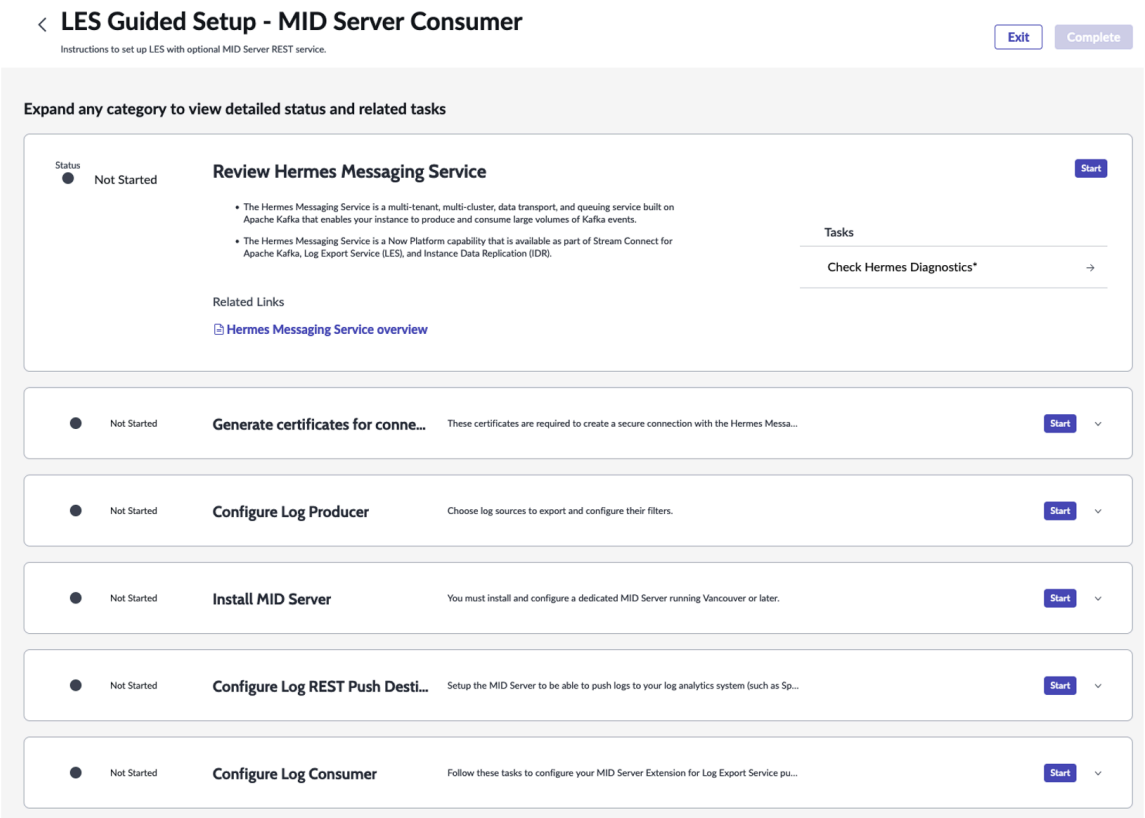


이 페이지의 세 가지 설정인 빠른 시작/최상의 경험/사용자 지정은 모두 동일한 작업과 기능을 제공합니다. 인스턴스에서 로그 분석 시스템으로 로그를 지속적으로 스트리밍하려면 전용 MID 서버가 필요합니다. 메시징 서비스에 대한 보안 연결을 설정하려면 MID 서버를 일회성 설정이 필요합니다. 작업을 완료됨으로 표시했더라도 돌아가서 진행 중으로 다시 선택을 취소할 수 있습니다. 이렇게 하려면 먼저 범주의 오른쪽 상단 모서리에 있는 편집 상자를 클릭합니다. 그런 다음 선택을 취소하려는 작업에 대해 편집 상자를 클릭합니다. 완료로 표시 상자는 더 이상 표시되지 않습니다.

안내 설정 범주 페이지

범주 페이지에는 범주와 관련 작업에 대한 개요와 설명이 포함되어 있습니다. 드롭다운 화살표를 클릭하여 범주에 대한 정보를 보거나 시작을 클릭하여 안내 설정 단계를 열고 구성을 시작할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



설정 지침에 따라 각 범주의 작업을 완료합니다.

MID 서버 소비자를 위한 안내 설정

MID 서버 소비자를 위한 완전한 안내 설정을 위해 다음 단계를 구현합니다.

시작하기 전에

다음으로 이동 로그 익스포트 서비스**(LES)** > **MID** 서버 소비자 > 안내 설정. 구성하려는 설정 유형을 선택하고 계속을 클릭합니다.

주: 로그 익스포트 서비스 애플리케이션을 설치하는 ServiceNow 동안 기본 Hermes 메시징 서비스 인프라가 프로비저닝됩니다. 애플리케이션 설치를 요청한 로그 익스포트 서비스 시점부터 이 프로세스를 완료하는 데 최대 몇 시간이 걸릴 수 있습니다.

필요한 역할: 관리자

프로시저

1. 진단을 검토합니다 Hermes 메시징 서비스 .

   이 단계에서 화면에 표시되는 진단 도구를 사용하여 Hermes 이(가) 실행 중인지 Hermes 메시징 서비스 확인하는 것이 좋습니다. 이 페이지에 Hermes "페이지를 찾을 수 없음" 오류가 표시되면 설치되지 않았으므로 시스템 관리자에게 문의해야 합니다.

   - 설정 정보: 다음 부트스트랩 정보는 메시징 서비스에 연결하는 데 사용됩니다. "생산자 부트스트랩"은 Hermes로 메시지를 보내는 데 사용되는 연결이고 "소비자 부트스트랩 1 & 2"는 Hermes에서 메시지를 검색하는 데 사용됩니다.
     - 생산자 부트스트랩
     - 소비자 부트스트랩 1
     - 소비자 부트스트랩 2

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인스턴스 PKI: 인스턴스 공개 키 인프라(PKI) 구성요소를 사용하면 ServiceNow 인스턴스가 X.509 신뢰 계층 구조에서 발급자 역할을 할 수 있습니다.
- 부트스트랩 연결: 테스트 실행을 클릭하여 외부 클라이언트가 정의된 인스턴스 포트(생산자 및 소비자)에 연결할 수 있는지 확인합니다.
- 인스턴스 연결: 테스트 실행을 클릭하여 인스턴스가 메시지를 보내고 받을 수 있는지 확인합니다.
- 주제 보기: 나열된 주제를 클릭하여 마지막으로 알려진 메시지의 타임스탬프를 검색합니다.

주: 안내 설정의 이 단계로 돌아가거나 다음으로 이동하여 나중에 진단에 액세스하여 Hermes 잠재적인 연결 문제를 해결할 수 있습니다. 모두 > *Hermes ### ###*> 진단.

2. 메시징 서비스에 대한 보안 연결을 위한 인증서를 생성하고 로그 이벤트를 끌어옵니다.

메시징 서비스에 대한 보안 연결을 설정합니다. 자세한 내용은 LES용 Hermes 메시징 서비스에 대한 보안 연결 설정을 참조하세요. Hermes에서 로그를 끌어올 클라이언트에서 인증 및 권한 부여를 위해 이러한 인증서가 필요합니다.

주: 이 단계에는 관리자 또는 Hermes_admin 역할이 필요합니다.

3. 로그 생성자 구성: 익스포트할 로그 소스를 선택하고 필터를 구성합니다.
로그 생성자를 구성하려면 다음 작업을 완료합니다.

- 익스포트할 로그 소스를 구성합니다. 익스포트할 각 로그 소스에 대해 소스 기록을 하나씩 생성합니다.

  주: 이 단계를 완료하려면 admin 또는 sn_logstoanalytics.admin 역할이 필요합니다.

  a. 오른쪽 상단 모서리에서 새로 만들기를 클릭합니다.

  b. 소스 유형 선택

  c. 선택한 소스 유형에 적합한 필터 선택

  주: 선택한 소스 유형에 따라 필터가 다릅니다.

  d. 업데이트를 클릭합니다.
  성공적으로 생성되면 해당 로그 소스를 익스포트할 Hermes 주제의 이름이 표시됩니다. 나중에 로그 소비자 시스템을 구성할 때 필요하므로 주제 이름을 적어 둡니다. 활성 필드는 해당 로그 소스를 익스포트할지 여부를 제어합니다. 오류가 표시되면 Hermes 진단 확인 작업으로 돌아가서 Hermes 상태를 확인합니다.

- 로그 생산자 확인: 로그를 생성할 소스를 생성한 후에는 다음을 사용하여 항목에서 라이브 로그 기록을 볼 수 있습니다. 메시징 서비스 > 헤르메스 주제 검사기.

  a. 외부 주제 선택

  b. 목록 항목 클릭

  c. 이전 단계의 주제가 있는 행 선택(소스에 나열됨)

  d. 필요한 경우 메시지 시작 날짜 조정

  e. 주제로 익스포트된 로그 메시지를 보려면 보기를 클릭합니다.

4. MID 서버 설치: Vancouver 이상을 실행하는 전용 MID 서버를 설치하고 구성해야 합니다.
다음 작업을 완료하여 MID 서버를 설치합니다.

- 전용 MID 서버 설치: 로그 익스포트 서비스에서 사용하는 MID 서버는 이 용도로만 전용이어야 하며 다른 프로세스를 실행할 것으로 기대해서는 안 됩니다. 이는 익스포트된 로그 메시지를 REST 엔드포인트에 적시에 전달하는 데 중요합니다. 를 사용하거나 MID 서버 안내 설정 사용

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수동으로 설치하여 새 MID 서버를 설치할 수 있습니다. 수동 설치의 경우 먼저 설명서를 따른 다음 MID Server 설치 설명서를 따르십시오MID Server 네트워크 연결 구성 .

- MID 서버 확인: MID 서버에서 자동화 작업을 실행할 수 있도록 MID 서버가 설치된 후 수동으로 MID 서버를 확인해야 합니다. LES 전용으로 사용할 MID 서버를 확인하려면 다음을 참조하십시오. MID 서버 확인

5. 로그 REST 푸시 대상 구성: 로그 분석 시스템(예: Splunk)에 로그를 푸시할 수 있도록 MID 서버를 설정합니다.
로그 REST 푸시 대상을 구성하려면 다음 작업을 완료합니다.
   - MID 속성 추가: Hermes에 연결할 수 있도록 MID 서버 속성을 추가해야 합니다. **MID** 서버 >속성으로 이동하여 아래에 나열된 각 속성에 대해 적절한 값을 설정합니다.

이름	값
mid.les.kafka.ssl.truststore.password	〈암호〉
mid.les.kafka.ssl.keystore.password	〈암호〉
mid.les.kafka.ssl.key.password	〈암호〉
mid.les.kafka.ssl.truststore.location	<your_path>/〈신뢰 저장소>.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>
mid.les.kafka.set2.bootstrap.servers	<instance_name>.servicenow.com:4200,<instance_name>

위의 값 중 일부를 가져오는 방법에 대한 다음 참고 사항

- 〈password〉는 키 저장소 및 신뢰 저장소에 대해 설정한 암호입니다.
- 〈your_path〉은 다운로드한 키 저장소 및 신뢰 저장소 파일을 보관하는 디렉터리의 파일 경로입니다. 인증서는 MID를 실행 중인 서버에 있어야 합니다.
- ServiceNow 인스턴스의 이름은 〈instance_name〉입니다. 확실하지 않은 경우 sys_properties 테이블에서 찾을 수 있습니다.
- Hermes 진단 페이지에서 mid.les.kafka.bootstrap.servers 및 mid.les.kafka.set2.bootstrap.servers의 값을 모두 얻을 수 있습니다. 다음으로 이동 메시징 서비스 > 진단 그리고 Consumer Bootstrap 1 및 Consumer Bootstrap 2 아래의 문자열을 각각 복사합니다.

   - 대상 구성: 이 확장이 로그를 전달할 REST 엔드포인트를 정의하는 새 대상 구성 기록을 만듭니다.

     주: 이 단계를 완료하려면 admin 또는 sn_logstoanalytics.admin 역할이 필요합니다.

     a. 다음으로 이동 로그 익스포트 서비스**(LES)** > 대상 구성
     b. 새 구성 기록 생성
     c. 익스포트한 로그 소스에 대해 원하는 엔드포인트의 URL을 지정합니다

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 엔드포인트에 연결하기 위한 새 자격 증명을 검색하거나 생성합니다. 엔드포인트에 대한 자격 증명을 만들 때 LES에는 기본 인증, OAuth, API 키 자격 증명 유형만 유효하다는 점에 유의하십시오

e. 새 변환 스크립트를 검색하거나 작성합니다. 미리 작성된 스크립트인 **SplunkTransform** for Splunk와 함께 제공됩니다

6. 로그 소비자 구성: 로그 익스포트 서비스를 위해 MID 서버 확장을 구성하려면 다음 작업을 따르십시오.

- LES 소비자 컨텍스트 구성: 이 단계에서는 LES 소비자 기록을 업데이트하여 로그 익스포트 서비스를 위해 방금 설치한 전용 MID 서버에서 실행합니다. 다음으로 이동 **MID** 서버 > 확장명 > **LES** 소비자 컨텍스트 및 다음 필드를 설정하여 LES 소비자 기록을 업데이트합니다.
  - "LES Consumer"를 클릭하여 MID Server 컨텍스트 기록을 엽니다.
  - "실행 날짜" 필드에 대해 특정 MID 서버를 선택합니다.
  - "MID 서버" 필드에 이전 단계에서 확인한 MID의 이름을 입력합니다.

  업데이트를 클릭하여 저장합니다.

  > 주: 우리는 미리 빌드된 컨텍스트와 함께 배송합니다. 두 번째 것을 만들지 마십시오. 이는 의도하지 않은 결과를 초래할 수 있습니다.

- 소비자 구성: 로그 익스포트 서비스 MID 서버 확장의 일부인 프로세스를 나타내는 새 소비자 기록을 만듭니다. 다음으로 이동 로그 익스포트 서비스**(LES)** > 소비자 로그 메시지를 검색할 Hermes 주제와 로그 메시지를 릴레이할 대상을 지정하는 새 구성 기록을 생성합니다. 소비자 모듈을 선택하면 소비자 이름 및 대상 구성에 대한 정보가 표시됩니다.

  a. 새 소비자 기록 생성

  b. 드롭다운에서 소스 주제 선택

  c. 대상 구성 선택

  d. 소비자 시작

- MID 서버 통합 확인: 다음으로 이동 로그 익스포트 서비스**(LES)** > 소비자 상태 그리고 정의된 기록의 상태 및 상태 세부 정보 필드를 봅니다. 이러한 필드의 정보는 REST 엔드포인트로 메시지를 릴레이하는 동안 발생할 수 있는 오류를 포함하여 MID 서버에서 실행 중인 프로세스의 현재 상태를 보고합니다. 이것은 상태 보기 페이지입니다. 다음으로 이동 로그 익스포트 서비스**(LES)** > 소비자 새 소비자 기록을 생성하려는 경우. #소비자상태가 프로세스가 시작되었음을 나타내는 경우 엔드포인트를 검사하여 릴레이된 로그를 볼 수 있어야 합니다. 또한 MID 서버에서 로그를 확인하여 발생할 수 있는 오류에 대한 추가 세부 정보가 있는지 확인할 수 있습니다. 필요한 경우 MID 서버에서 디버그 로깅을 활성화하여 추가 정보를 얻을 수도 있습니다.

  > 주: 소비자 기록 중 하나를 변경하면 소비자 상태 뷰 페이지에 표시됩니다. 소비자 상태 목록에서 소비자 기록 이름을 선택하면 선택한 기록에 대한 소비자 양식이 열립니다. 그런 다음 선택한 기록의 이름 및 대상 구성을 업데이트할 수 있습니다.

LES용 **Hermes** 메시징 서비스에 대한 보안 연결 설정

인스턴스에 서명된 인증서를 생성하여 ServiceNow® Kafka 주제를 보호합니다.

시작하기 전에

설정하려면 Hermes 메시징 서비스 네트워크 관리자 및 Kafka 관리자와의 조정이 필요합니다. 네트워크 관리자와 협력하여 필요한 보안 인증서를 확보하고 필요한 포트를 엽니다. Kafka 관리자와 협력하여 Kafka 환경이 올바르게 구성되어 있고 애플리케이션이 표준 Kafka 프로토콜을 사용하여 연결할 Hermes 메시징 서비스 수 있는지 확인합니다.

다음 설정이 제대로 되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 이(가 Hermes 메시징 서비스) 활성화됩니다. Hermes 메시징 서비스 활성화 문서를 참조하십시오.
- Key Management Framework 플러그인(com.glide.kmf.global)이 활성화됩니다.
- 인증서 [sys_kmf_certificate] 테이블에는 인스턴스 루트 CA 인증서가 포함되어 ServiceNow 있습니다.

필요한 역할: hermes_admin, sn_kmf.cryptographic_manager 또는 admin

KMF 역할 할당에 대한 자세한 내용은 문서를 참조하십시오 키 관리 프레임워크와 함께 설치되는 역할.

프로시저

1. 다음으로 이동 모두 > 인증서 생성기 > 인스턴스 **PKI** 인증서 생성기.
2. 제한된 호출자 접근을 승인합니다.
   a. 제한된 호출자 접근 승인에 대한 메시지에서 기록 보기를 선택합니다.
   b. 제한된 호출자 접근 권한 기록 양식에서 상태 필드를 승인됨으로 변경합니다.
   c. 저장을 선택합니다.
3. 옵션: 네임스페이스 또는 주제 수준에서 ACL(접근 제어 목록)을 구성하여 주제에 대한 액세스를 제어합니다.

옵션	설명
네임스페이스에 ACL 적용	a. **ACL** 구성을 선택합니다. b. 주제 ACL 대화 상자에서 네임스페이스를 선택합니다. c. 구성할 네임스페이스를 입력합니다. d. 읽기 전용 또는 읽기/쓰기를 선택하여 권한 수준을 설정합니다. e. 추가를 선택합니다.
정의된 주제에 ACL 적용	a. **ACL** 구성을 선택합니다. b. 주제 ACL 대화 상자에서 정의된 주제를 선택합니다. c. 구성하려는 기존 주제를 입력합니다. d. 읽기 전용 또는 읽기/쓰기를 선택하여 권한 수준을 설정합니다. e. 추가를 선택합니다.

   인증서 전달자에게는 네임스페이스의 주제 또는 선택한 기존 주제에 대한 읽기 또는 읽기/쓰기 권한이 부여됩니다.
4. 에 Hermes 메시징 서비스대한 보안을 설정합니다.
   a. 인스턴스 PKI 인증서 생성기 페이지로 되돌아갑니다.
   b. 인증서 암호 필드에 키 저장소 암호를 입력합니다.
   c. 생성을 선택합니다.
   시스템은 인증서 [sys_kmf_certificate] 테이블에서 인스턴스 서명 인증서를 생성하고, 키 스토어를 생성하고, 신뢰 스토어를 생성합니다.
5. 키 저장소 다운로드를 선택하여 키 저장소의 사본을 저장합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 신뢰 저장소 다운로드를 선택하여 신뢰 저장소의 복사본을 저장합니다.
7. 키 저장소 및 신뢰 저장소 파일을 에 연결할 Hermes 메시징 서비스각 생성자 및 소비자 클라이언트에 복사합니다.

결과
이제 에 대한 보안 연결을 만들 수 있습니다 Hermes 메시징 서비스.

주: 에 연결하려면 Hermes인스턴스 PKI 인증서 생성기를 사용하여 생성한 키 스토어를 사용해야 합니다. 설명서에 따라 생성되지 않은 사용자 지정 생성 키 스토어는 ServiceNow 지원되지 않습니다.

사용 로그 익스포트 서비스 (LES)

LES를 사용하여 로그 보고서 대시보드를 검토합니다.

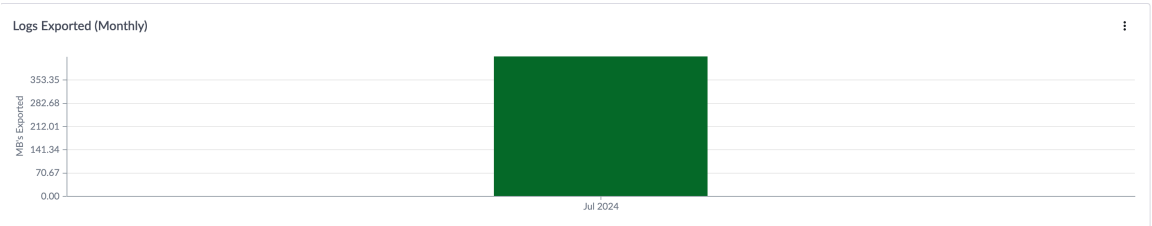
로그 보고서 검토

로그 보고서 대시보드를 검토하여 각 데이터 로그의 크기를 분석합니다.

시작하기 전에
필요한 역할: admin 또는 sn_logstoanalytics.admin

프로시저

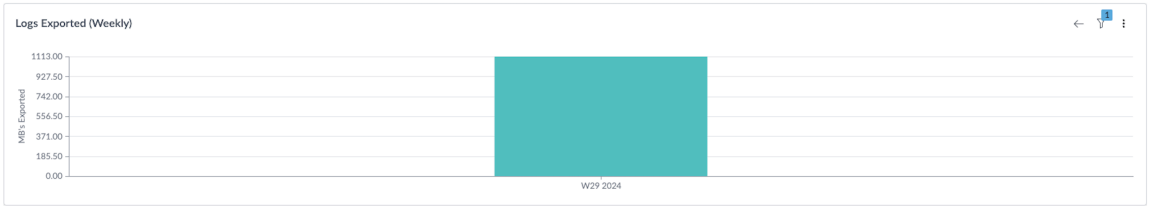
1. 다음으로 이동 모두 > 로그 익스포트 서비스 > 보고서.
2. 다음 위젯에서 로그 데이터를 검토합니다.
   - 로그 익스포트됨(월별): 초기 뷰에 월별 익스포트된 메가바이트가 표시됩니다. 그래프를 드릴다운하여 매주 또는 일별 데이터에 대한 데이터를 볼 수 있습니다. 지난 395일 동안의 데이터를 볼 수 있습니다.



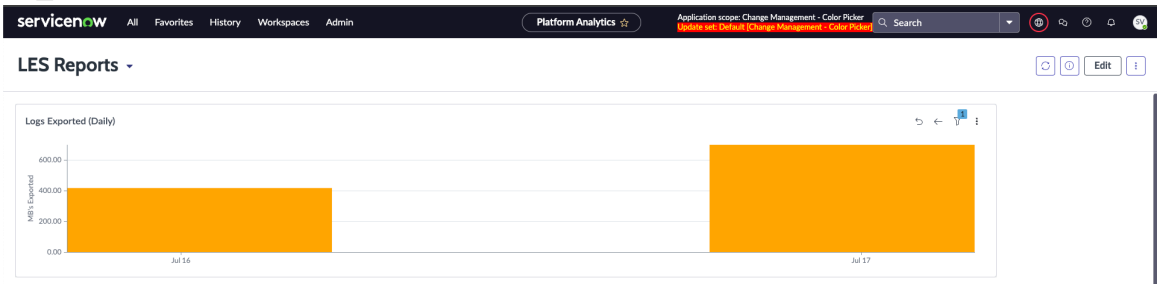
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 위젯의 오른쪽 위 모서리에 있는 화살표를 클릭하여 데이터를 드릴다운합니다. 상위 데이터로 다시 이동할 수도 있습니다.

주별:

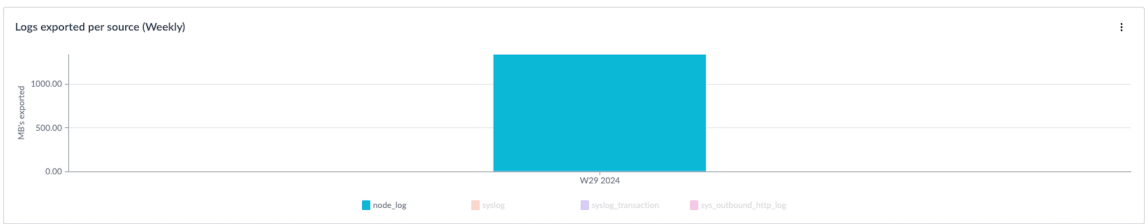


일별:

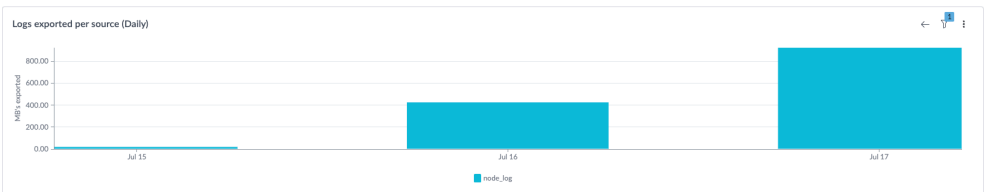


이 보고서의 데이터는 4시간 전에 수집된 정보를 반영합니다.

◦ 소스당 익스포트된 로그(주별): 이 위젯은 매주 익스포트된 로그의 종류를 보여줍니다. 드릴다운하여 일일 로그 데이터를 볼 수도 있습니다. 지난 32일 동안의 데이터를 볼 수 있습니다.

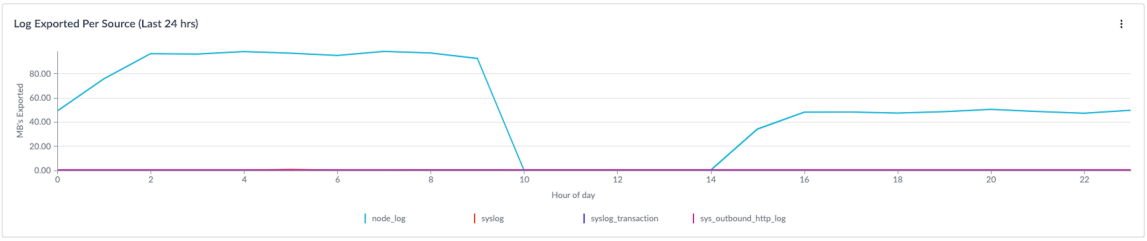


주: 데이터를 보려는 소스를 선택하거나 선택을 취소할 수 있습니다. 로그를 볼 수 있는 소스는 node_log, syslog, syslog_transaction 및 sys_outbound_http_log입니다.



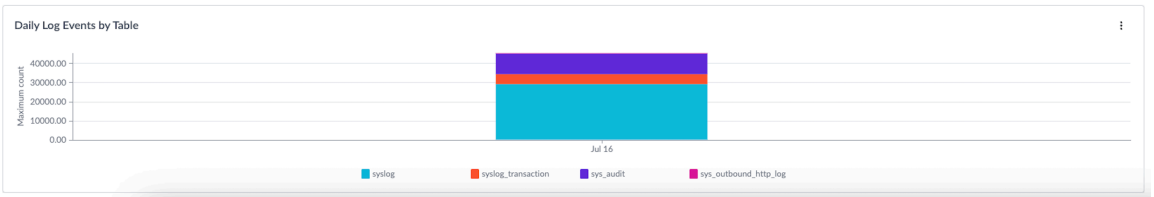
◦ 소스당 로그 익스포트됨(최근 24시간): 지난 24시간 동안의 데이터를 보여줍니다. 그래프는 24시간 척도에서 왼쪽에서 오른쪽으로 시간순으로 진행되며, 가장 오래된 데이터(24시간)는 보고서의 오른쪽에 배치되고 최신 데이터는 보고서의 왼쪽에 배치됩니다. 데이터를 보려는 소스를 선택하거나 선택을 취소할 수 있습니다. 로그를 볼 수 있는 소스는 node_log, syslog, syslog_transaction 및 sys_outbound_http_log입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주: 이 데이터를 확인하는 시간에 따라 위젯이 동적으로 업데이트되어 지난 24시간을 정확하게 반영합니다.

- 테이블별 일일 로그 이벤트: 각 로그 테이블에서 하루에 생성된 로그 이벤트를 표시합니다. 데이터를 보려는 테이블을 선택하거나 선택을 취소할 수 있습니다.



주: 로그 이벤트를 볼 수 있는 테이블은 syslog, syslog_transaction, sys_audit 및 sys_outbound_http_log입니다.

로그 익스포트 서비스 (LES) 참조

참조 섹션에서 LES에 대한 모든 기타 정보를 찾으십시오.

로그 익스포트 서비스 역할

로그 익스포트 서비스 이 다음 역할과 함께 설치됩니다.

애플리케이션 관리자 [sn_logstoanalytics.admin]

사용자별 구독 관리에 대한 자세한 내용은 계정 담당자에게 문의하여 에서 사용자별 구독 관리 구독 관리 문의하십시오.

이 역할은 LES 애플리케이션과 함께 설치되며 관리자가 아닌 사용자도 애플리케이션을 사용할 수 있습니다.

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

상승함

역할이 상승된 역할인지 여부 상승된 역할은 사용자 또는 그룹에 할당되지 않으며 권한 상승에서 사용해야 합니다. 자세한 내용은 단원을 참조하십시오권한 있는 역할로 상승.

번호

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특별 고려 사항

없음.

시스템 관리자 **[admin]**

사용자별 구독 관리에 대한 자세한 내용은 계정 담당자에게 문의하여 에서 사용자별 구독 관리 구독 관리 문의하십시오.

LES 스토어 애플리케이션을 설정하려면 관리자 역할이 필요합니다.

역할 포함

역할에 포함된 역할 목록입니다.

- sn_templated_snip.template_snippet_admin
- sn_employee.admin
- taxonomy_admin
- sn_ace.ace_user
- sn_hr_sp.esc_admin

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

상승함

역할이 상승된 역할인지 여부 상승된 역할은 사용자 또는 그룹에 할당되지 않으며 권한 상승에서 사용해야 합니다. 자세한 내용은 권한 있는 역할로 상승 문서를 참조하십시오.

번호

특별 고려 사항

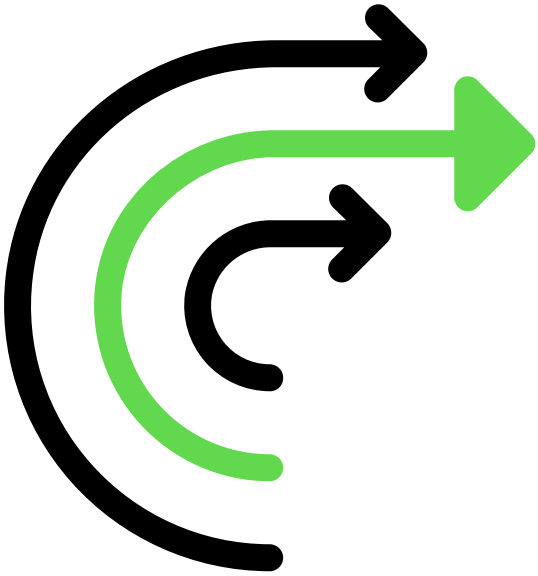
없음.

로그 항목

로그 모듈은 인스턴스 내에서 발생하는 트랜잭션 및 이벤트 문제를 해결하고 디버그하는 데 사용할 수 있는 다양한 로그를 제공합니다.

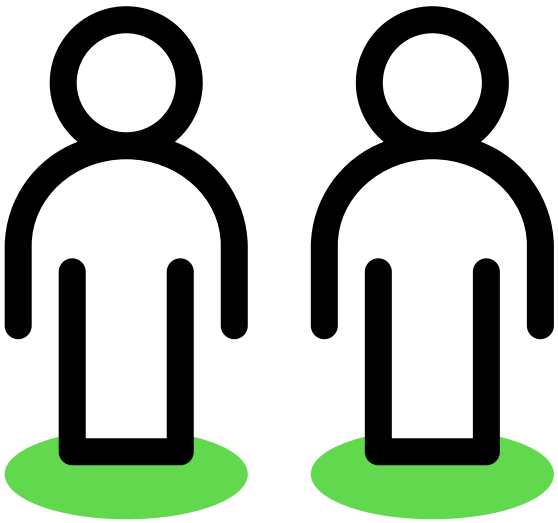
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 로그



시스템 로그 모듈은 인스턴스 내에서 발생하는 트랜잭션 및 이벤트 문제를 해결하고 디버그하는 데 사용할 수 있는 다양한 로그를 제공합니다.

로깅, 감사 및 오류



의심스러운 활동을 적시에 식별하고 조치를 취할 수 있도록 로깅 및 감사 전략을 적용합니다.

시스템 로그

시스템 로그 모듈은 인스턴스 내에서 발생하는 트랜잭션 및 이벤트 문제를 해결하고 디버그하는 데 사용할 수 있는 다양한 로그를 제공합니다.

시스템 로그 모듈에서 다음 로그에 액세스합니다.

로그	설명
트랜잭션	인스턴스에 대한 모든 애플리케이션 활동입니다.
이메일 및 푸시	시스템 내의 전체 인스턴스에서 보낸 모든 이메일 알림 및 푸시 메시지입니다.
이벤트 로그	시스템 내에서 발생하는 모든 시스템 이벤트입니다.
임포트	플랫폼 내 데이터 임포트 활동입니다.
테이블 변경	시스템의 모든 테이블에 대한 변경.
아웃바운드 웹 서비스 로깅	REST 및 SOAP 요청과 같은 모든 아웃바운드 웹 서비스 요청입니다.
서명 이미지	HR 서명 패드의 전자 서명입니다.
시스템	인스턴스 프로세스, 기록 및 중요하지 않은 이벤트(예: 서버 머신의 메모리 사용량)에 대한 경고 및 오류입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그 파일 브라우저를 사용하여 로그를 검색하고 다운로드합니다. 로그 기록에서 보관된 로그를 검색할 수도 있습니다.

기타 로그

인스턴스는 시스템 로그 모듈에 있는 로그 외에 다른 로그를 제공합니다. 예를 들어 시스템 진단 모듈는 업그레이드 기록 및 느린 쿼리 로그를 제공하며, 쿼리를 사용하여 쿼리가 플랫폼 성능에 미치는 영향에 대한 인사이트를 얻을 수 있습니다. 고객 업데이트 테이블 시스템에서 수행된 모든 변경 내용을 기록합니다.

시스템 로그

인스턴스 프로세스, 기록 및 중요하지 않은 이벤트(예: 서버 머신의 메모리 사용량)에 대한 경고 및 오류를 봅니다.

시스템 로그에서 추적되는 정보는 다음과 같습니다.

- 워크플로우
- 구성
- 채팅 세션
- 네트워크, 서버 및 브라우저에 대한 로드 시간을 포함하여 시스템에 있는 각 페이지의 각 뷰에 대한 트랜잭션
- 인바운드 및 아웃바운드 이메일
- 시스템에서 트리거된 이벤트
- 임포트 및 통합
- 시스템 경고, 오류 및 스크립트 로그
- 플러그인 활성화, 업데이트 세트 또는 시스템 업그레이드에 대한 업그레이드 정보

로그 항목은 현재 날짜에 대해서만 표시됩니다. 다른 로그 파일을 보려면 로그 파일 브라우저를 사용하십시오. 이 로그는 모든 항목에 대해 다음 정보를 제공합니다.

시스템 로그

필드	설명
작성됨	인스턴스를 실행하는 머신의 로캘에 대한 로깅 활동의 날짜 및 시간입니다.
수준	메시지 유형입니다. 수준은 디버그, 오류, 경고 및 정보입니다. • 경고는 처리 및 복구된 오류입니다. • 오류는 수정해야 하는 것입니다.
메시지	발생의 특성과 관련하여 시스템에서 생성된 메시지입니다.
소스	발생의 영향을 받는 프로세스 또는 영역의 이름입니다. 예를 들어 발생 소스는 이메일 또는 메모리일 수 있습니다.
소스 패키지	발생과 연관된 애플리케이션 패키지의 이름입니다. 이름을 클릭하면 이 패키지에 대한 스토어 애플리케이션 [sys_store_app] 기록을 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

워크플로우 로깅

- 다음을 포함하여 실행된 각 활동은 다음과 같습니다.
  - 시작된 날짜 및 시간
  - 종료된 날짜 및 시간
  - 상태(예: 완료됨, 취소됨, 시간 초과됨, 오류)
  - 결과
  - 오류가 발생한 경우 결함 설명
- 다음을 포함한 전환 이력:
  - 전환 시간
  - 활동 전환됨 위치
  - 활동이 다음으로 전환됨
  - 트리거된 전환
- 워크플로우에 추가된 모든 로그 문을 포함한 워크플로우 로그

구성 정보

- 삽입, 업데이트 및 삭제를 포함하여 수행된 작업
- 변경 범주
- 변경과 함께 기록된 설명
- 변경 이름
- 변경의 XML 차이
- 변경이 관련된 업데이트 세트
- 변경 날짜 및 시간
- 변경한 사용자
- 변경이 이루어진 테이블
- 변경 중인 객체의 이름
- 변경 중인 객체의 유형
- 양식 또는 목록의 변경 내용에 대한 변경 내용 보기

트랜잭션 로그

트랜잭션 로그는 인스턴스에 대한 모든 브라우저 활동을 기록합니다. 시스템 문제의 디버깅을 돕기 위해 애플리케이션 범위별로 트랜잭션 로그를 필터링하여 특정 범위에서 시작된 트랜잭션에만 나타나는 트랜잭션을 제한할 수 있습니다.

다음으로 이동하여 트랜잭션 로그에 액세스합니다. 모두 > 시스템 로그 > 거래. 트랜잭션 로그는 모든 작업에 대해 다음 정보를 제공합니다.

필드	설명
작성됨	인스턴스를 실행하는 머신의 로캘에 대한 애플리케이션 작업의 날짜 및 시간입니다.
유형	기록된 트랜잭션의 유형입니다.
작성자	이 활동을 작성한 사용자입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
원본 애플리케이션	트랜잭션이 시작된 애플리케이션 범위입니다. 트랜잭션이 전역 범위에서 시작된 경우 전역이 표시됩니다.
응답시간	애플리케이션 요청에 대한 왕복 응답시간(밀리초)입니다.
네트워크 시간	애플리케이션 요청이 이루어진 후 네트워크 응답의 대기 시간(밀리초)입니다.
출력 길이	인스턴스에서 애플리케이션으로 보낸 출력 문자열의 크기(바이트)입니다.
SQL 수	이 활동에 대해 실행된 SQL Server 명령의 수입니다.
비즈니스 규칙 수	이 활동에 대해 실행된 비즈니스 규칙의 수입니다.
비즈니스 규칙 시간	이 활동에 대한 비즈니스 규칙을 실행하기 위한 경과 시간입니다.
URL	클라이언트 애플리케이션에서 연결한 애플리케이션 또는 모듈입니다.
시스템 ID	요청을 하는 클라이언트 인스턴스의 시스템 생성 식별자입니다. 이 ID는 여러 인스턴스(노드)가 데이터베이스와 통신하는 클러스터 환경에 사용됩니다.
IP 주소	요청을 하는 클라이언트의 IP 주소입니다.
GZip됨	응용 프로그램에서 압축된 웹 페이지를 요청했는지 여부를 나타냅니다.
프로토콜	이 인스턴스의 애플리케이션에서 사용하는 HTTP 프로토콜입니다.

클라이언트 트랜잭션 타이밍

클라이언트 트랜잭션 타이밍 플러그인은 클라이언트와 서버 간에 발생하는 트랜잭션 기간에 대한 추가 정보를 제공하여 시스템 로그를 향상시킵니다.

시간이 소비되는 위치와 트랜잭션 중에 소요된 시간을 확인하여 성능 문제를 원본으로 추적할 수 있습니다.

이 플러그인을 사용하려면 응답시간 표시기 응답시간 표시기 를 활성화해야 하며 다음 브라우저에서 정보를 수집합니다.

- Firefox
- Internet Explorer
- Chrome

클라이언트 트랜잭션 정보

플러그인을 설치하면 클라이언트 트랜잭션 모듈이 시스템 로그 애플리케이션에 추가됩니다. 마지막 날 동안 클라이언트와 서버 간에 기록된 모든 트랜잭션 목록을 제공합니다.

클라이언트 트랜잭션 정보

필드	설명
작성됨	트랜잭션이 기록된 순간입니다.
응답시간	서버가 트랜잭션을 이행하는 데 소비한 ms입니다.
비즈니스 규칙 시간	트랜잭션에 의해 트리거된 비즈니스 규칙에 의해 소요된 ms입니다.
SQL 시간	SQL 데이터베이스에서 소비한 ms입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라이언트 트랜잭션 정보

필드	설명
클라이언트 응답시간	(Load_completion_time) - (start_time). 여기에는 서버 시간이 포함됩니다.
클라이언트 네트워크 시간	클라이언트가 연결하는 네트워크에서 소비한 ms입니다.
브라우저 시간	트랜잭션 중 브라우저에서 소비한 ms의 수입니다.
클라이언트 스크립트 시간	클라이언트 스크립트 실행에 소요된 ms 수입니다.
UI 정책 시간	UI 정책을 실행하는 데 소요된 ms 수입니다.
유형	트랜잭션 유형: • 양식 • 목록 • 기타
테이블	나타난 테이블의 이름입니다. 예: 인시던트 change_request.
뷰	이 양식/목록에 대한 뷰입니다.

클라이언트 상세 정보

모든 양식 렌더링(목록 렌더링 제외)에 대한 클라이언트 타이밍에 대한 자세한 세부 항목도 추적됩니다. 상세 정보를 보려면 특정 클라이언트 트랜잭션 기록을 드릴다운하고 화면 하단에서 관련 목록을 확인합니다.

클라이언트 상세 정보

필드	설명
순서	이 작업이 발생한 로드 중의 순서입니다.
유형	운영 유형입니다.
이름	이 특정 작업의 설명이 포함된 이름
지속 시간	이 작업을 완료하는 데 걸린 시간(밀리초)입니다.

푸시 로그

푸시 로그를 참조하여 시스템에서 보내기 위해 대기 중인 푸시 알림의 상태를 추적합니다.

푸시 로그를 보려면 다음으로 이동하십시오. 시스템 로그 > 푸시 알림. 사용자가 푸시 로그를 보려면 push_admin 또는 관리자 역할이 필요합니다.

푸시 로그 필드

필드	설명
클레임	푸시 알림을 보내는 예약된 작업에서 생성되는 식별 번호입니다. 이 숫자는 여러 푸시 예약된 작업에서 일관성을 보장하기 위해 클레임 필드에 적용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

푸시 로그 필드

필드	설명
페이로드	푸시 알림의 내용입니다.
큐 수	시스템에서 푸시 알림 전송을 시도한 횟수입니다. 푸시 알림의 상태는 큐 수와 관련되어 있습니다. • 큐 수가 예상보다 오래 0이면 푸시 알림을 보내려는 예약된 작업이 없는 것입니다. • 큐 수가 0보다 크고 유형이성공인 경우 시스템이 최종적으로 전송하기 전에 푸시 알림 전송을 시도한 횟수임을 유추할 수 있습니다. • 큐 수가 10에 도달하면 시스템은 푸시 알림 전송 시도를 중지합니다. 유형이실패로 변경됩니다.
요청 ID	푸시 알림의 고유 식별 번호입니다. 이메일의 메시지 ID와 마찬가지로 요청 ID는 푸시 알림의 상관관계 토큰으로 사용됩니다.
유형	푸시 알림이 전송되었는지 여부를 나타내는 상태입니다. 유형 열은 다음 값을 가질 수 있습니다. • 실패: 메시지를 보낼 수 없습니다. • **pending**: 메시지가 처리를 위해 대기 중입니다. • **success**: 메시지가 성공적으로 전송되었지만 모바일 장치에서 수신되지 않을 수도 있습니다.

관련 정보

예약된 작업

시스템 이메일 로그 및 사서함

시스템 이메일 로그는 인스턴스가 생성하거나 수신하는 모든 이메일을 기록합니다. 시스템 사서함은 이 로그의 필터링된 뷰입니다.

인스턴스가 생성하거나 수신하는 모든 알림 이메일은 이메일 [sys_email] 기록에 기록됩니다. 다음에서 이러한 기록의 로그로 이동할 수 있습니다. 시스템 로그 > 이메일.

시스템 사서함은 이메일 [sys_email] 테이블의 필터링된 뷰입니다. 인스턴스는 유형 및 상태 필드의 값에 따라 시스템 사서함에 이메일 기록을 할당합니다. 자세한 내용은 시스템 사서함 을 참조하십시오.

다음 필드는 시스템 로그의 레이아웃과 시스템 사서함에 포함될 수 있습니다.

이메일 로그

필드	설명
사서함	이 이메일 기록을 나열하는 시스템 사서함입니다. 인스턴스는 유형 및 상태 필드의 값에 따라 이 필드의 값을 설정합니다.
상태	이메일의 현재 상태(오류, 무시됨, 처리됨 또는 준비됨)입니다.
수신 유형	인바운드 이메일의 유형(없음, 전달, 신규 또는 회신)입니다.
유형	이메일의 상태입니다. 선택 항목은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 로그

필드	설명
	• 수신됨: 서버에서 이 이메일을 수신했습니다. • 수신 - 무시됨: 서버에서 이 이메일을 수신했지만 인바운드 이메일 작업을 위해 인스턴스에서 무시되었습니다. 일반적으로 이러한 이메일은 스팸 또는 자동 회신입니다. 자세한 내용은 오류 문자열 필드를 참조하십시오. • send - failed: 서버에서 이메일 전송을 시도했지만 실패했습니다. 자세한 내용은 오류 문자열 필드를 참조하십시오. • 보내기 - 무시됨: 서버에서 이 이메일 보내기를 건너뛰었습니다. 일반적으로 생성되었지만 수신자 이메일 주소가 없거나 중복된 이메일에 대한 것입니다. 자세한 내용은 오류 문자열 필드를 참조하십시오. • send - ready: 이메일을 보낼 준비가 되었지만 메일 서버에서 보내지 않았습니다. 일반적으로 이메일은 잠시 동안만 이 상태로 유지됩니다. • send - translation - ready: 이메일 번역 중에 이메일이 생성되어 전송됩니다. 일반적으로 이메일은 잠시 동안만 이 상태로 유지됩니다. • sent: 오류나 문제 없이 인스턴스에서 이메일을 보냈습니다.
대상	특정 기록의 삽입, 업데이트 또는 삭제에 의해 이메일이 작성되는 경우 기록에 대한 문서 ID 참조.
사용자	이메일 알림이 전송된 인스턴스의 사용자 기록에서 사용자의 이름입니다. 주: 문자열 필드입니다.
알림 유형	알림의 유형입니다. 선택 항목은 다음과 같습니다. • 없음 • SMS • SMTP
UID	서버에 저장된 이메일의 고유 ID입니다.
작성됨	인스턴스를 실행하는 머신의 로캘에 대한 이메일 활동의 날짜 및 시간입니다.
삭제됨	인바운드 이메일의 경우 이메일이 이메일 서버에서 삭제되었는지 여부를 나타냅니다.
가중치	같은 테이블의 다른 알림을 기준으로 전송 우선순위를 결정하는 이메일의 가중치입니다.
중요도	이메일이 긴급과 같이 중요도 수준이 변경된 상태로 전송되었음을 나타냅니다.
이벤트 및 알림 시작	알림으로 생성된 이메일의 경우 이메일을 생성한 이벤트와 알림을 저장하는 포함된 목록입니다.
제목	이메일 제목입니다. 알림의 경우 시스템 통보 > 이메일 > 알림.
오류 문자열	이메일이 전송되지 않은 이유를 확인하기 위해 이메일 서버에서 캡처한 오류 문자열입니다. 이는 이메일 전송이 실패한 경우에만 기록됩니다.
수신자	수신자의 이메일 주소입니다.
본문	원시 HTML 마크업으로 표시되는 이메일의 본문입니다. 관련 링크인 HTML 본문 미리 보기를 사용하여 본문 텍스트를 렌더링된 HTML로 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일 로그

필드	설명
컨텐츠 유형	이메일 콘텐츠 유형입니다.
머리글	이메일에 포함된 모든 헤더

이벤트 로그

이벤트 로그는 내에서 Now Platform발생하는 모든 시스템 이벤트를 기록합니다.

이 로그는 발생하는 모든 이벤트에 대해 다음 정보를 제공합니다.

이벤트 로그

필드	설명
작성됨	인스턴스를 실행하는 머신의 로캘에 대한 이벤트의 날짜 및 시간입니다.
이름	이벤트 레지스트리에 나열된 이벤트 이름입니다.
URI	이벤트를 생성한 HTTP 쿼리입니다.
매개변수 1	이벤트 및 수신자에 따라 달라지는 이벤트별 값입니다.
매개변수 2	이벤트 및 수신자에 따라 달라지는 이벤트별 값입니다.
테이블	이 이벤트에 대해 조치를 취한 데이터베이스 테이블입니다.
처리됨	이벤트 처리가 시작된 날짜 및 시간입니다. 이 시간은 인스턴스를 실행하는 머신의 로캘을 반영합니다.
처리 시간	이 이벤트를 처리하는 데 걸린 시간(밀리초)입니다.
큐	프로세서 큐 이름입니다.

임포트 로그

임포트 로그에는 플랫폼 내의 데이터 임포트 활동에 대한 정보가 자세한 형식으로 표시됩니다.

특정 로그를 생성한 임포트 세트에 대한 자세한 내용은 다음을 참조하십시오. 임포트 세트 > 변환 이력.

이 로그는 모든 임포트에 대해 다음 정보를 제공합니다.

임포트 로그

필드	설명
작성됨	인스턴스를 실행하는 머신의 로캘에 대한 임포트 날짜 및 시간입니다.
수준	표시되는 메시지의 유형입니다. 가져오기 파일의 경우 수준은 정보입니다.
메시지	임포트 상태와 관련하여 시스템에서 생성된 메시지입니다.
소스	통합과 같은 임포트의 외부 소스의 이름입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 진단 모듈

System Diagnostics 애플리케이션은 플랫폼과 관련된 로그를 제공합니다.

다음과 같은 로그를 사용할 수 있습니다.

업그레이드 이력

인스턴스에 대한 모든 업그레이드를 추적합니다.

느린 쿼리

쿼리가 플랫폼 성능에 미치는 영향에 대한 인사이트을 제공합니다. 느린 쿼리 로그 사용을 참조하세요.

고객 업데이트 테이블

시스템에서 변경한 내용은 고객 업데이트 `[sys_update_xml]` 테이블에 시간순으로 기록됩니다. 아래에 설명된 것처럼 몇 가지 예외가 있습니다.

이 테이블로 이동하려면 탐색 필터에 `sys_update_xml.list` 를 입력합니다. 업데이트 세트에 대한 자세한 내용은 시스템 업데이트 세트를 참조하십시오.

각 업데이트에 대해 다음 정보가 저장됩니다.

고객 업데이트 테이블

필드	설명
이름	업데이트된 기록을 식별하는 이름입니다.
작성됨	고객 업데이트 기록이 생성된 날짜 및 시간입니다.
작성자	변경을 수행한 사용자입니다.
유형	업데이트의 유형입니다.
업데이트됨	고객 업데이트 기록이 업데이트된 날짜 및 시간입니다.
업데이트한 사람	업데이트를 수행한 사용자입니다.
업데이트	기록이 업데이트된 횟수입니다.
대상 이름	변경된 요소의 이름입니다.
뷰	양식 레이아웃 변경인 경우 변경된 양식의 뷰입니다.
페이로드	변경 후 기록의 XML 내용입니다.
원격 업데이트 세트	원격 업데이트 세트에서 변경이 수행된 경우 해당 업데이트 세트에 대한 참조입니다.
로컬 업데이트 세트	변경과 연결된 업데이트 세트입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 일부 애플리케이션 변경 사항은 고객 업데이트 기록(sys_update_xml)에 표시되지 않습니다. 예:

- updateSynch = false인 메타데이터 유형
- 표시 이름 변경과 같은 테이블 및 필드의 계단식 변경
- 다른 애플리케이션의 해결되지 않은 메타데이터 참조(요소에 "표시 값"이 없음)
- 병합 파일의 변경 내용 sys_id
- sys_documentation 발생할 수 있는 플로우/플로우 작업의 변경
- 테이블 생성 시 생성된 ua_table_license_config 기록
- 자연어 처리와 같이 백그라운드에서 실행되는 작업
- sys_update_xml 수동으로 수정하거나 제거하는 케이스

자세한 내용은 변경 내용 커밋을 참조하세요.

로그 이력

시스템은 테이블 교대와 테이블 확장을 사용하여 오래된 로그를 보관합니다.

기본적으로 시스템은 다음 일정을 사용하여 공통 로그를 보관합니다.

일반 로그 보관 일정

테이블	일정 보관	교대	유형
이벤트 [ecc_event]	매일	7	교대
큐 [ecc_queue]	매일	7	교대
이벤트 [sysevent]	매일	7	교대
로그 [syslog]	매주	8	교대
트랜잭션 로그 [syslog_transaction]	매주	8	교대
이메일 [sys_email]	30일 마다	8	확장명

로그 파일 브라우저 사용

인스턴스는 로그 파일 브라우저와 로그 파일 다운로드 유틸리티를 제공합니다.

사용 시스템 로그 > 공공 서비스 > 노드 로그 파일 브라우저 시스템 로그 항목을 볼 수 있습니다. 다음 필터를 사용하여 로그 파일을 검색할 수 있습니다.

로그 파일 브라우저

필드	설명
시작 시간	인스턴스를 실행하는 컴퓨터의 로캘에 대해 검색하려는 범위의 시작 날짜 및 시간입니다.
세션 ID	로그 항목을 생성한 세션을 식별하는 시스템에서 생성된 16진수 문자열입니다.
종료 시간	인스턴스를 실행하는 컴퓨터의 로캘에 대해 검색하려는 범위의 종료 날짜 및 시간입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그 파일 브라우저

필드	설명
메시지	발생에 대해 시스템에서 생성된 설명입니다.
수준	표시되는 메시지의 유형입니다. 수준은 디버그, 오류, 경고 및 정보입니다. 경고는 처리 및 복구된 오류입니다. 오류는 수정해야 하는 것입니다.
스레드 이름	로그 파일을 만든 스레드의 시스템 생성 식별자입니다.
최대 행 수	특정 필터에 대해 반환되는 최대 기록 수입니다.

이 인스턴스는 2일마다 시스템 로그의 압축된 아카이브를 생성하고 21일이 지나면 로그 아카이브를 제거합니다.

중요사항: 노드가 폐기되면 노드의 로그 파일이 즉시 제거되므로 추가로 21일 동안 보관되지 않습니다.

로그 파일 아카이브를 다운로드하여 다음을 사용하여 볼 수 있습니다. 시스템 로그 > 공공 서비스 > 노드 로그 파일 다운로드. 목록에서 로그 보관 파일을 선택한 다음 관련 링크 아래에서 로그 다운로드를 클릭하여 보관 파일을 열거나 저장합니다.

주: 로그 파일은 현재 로그인한 노드에서만 사용할 수 있습니다. 현재 로그인된 노드를 보려면 다음으로 이동하십시오. 시스템 진단 > 통계.

트랜잭션 및 활성 트랜잭션 양식에서 새로운 **Show Syslog Records** 버튼을 사용하여 트랜잭션 실행 중에 생성된 시스템 로그 항목을 봅니다. 트랜잭션에는 syslog 항목 수가 제한 없이 있을 수 있습니다. 모든 트랜잭션에 대한 여러 syslog 항목을 사용하면 트랜잭션을 해당 syslog 항목과 상호 연결하기가 어렵습니다. 시스템 로그 기록 표시 UI 작업은 시스템 로그 테이블을 쿼리하는 URL을 작성하여 활성 트랜잭션과 완료된 트랜잭션을 해당 시스템 로그 항목에 상호 연결하는 데 도움이 됩니다. 특정 트랜잭션에 대한 올바른 syslog 항목을 식별하면 보안 문제를 디버깅하고 해결하는 데 도움이 됩니다.

향상된 로깅 보안

노드 로그 라인의 속성 필드를 탐색하여 로그 메시지를 생성한 스크립트 또는 구성요소를 식별합니다. 트랜잭션 시작 라인에는 수행된 요청 유형을 식별하는 새 필드가 포함됩니다.

새로운 개선 사항을 사용하여 다음을 수행할 수 있습니다.

- 각 로그 라인의 소스 송신자 추적
- 송신자 정보를 사용할 수 없는 경우 Java 클래스 이름과 속성을 인쇄하십시오.
- 각 트랜잭션 라인의 시작 부분에는 트랜잭션 ID와 트랜잭션 유형이 포함됩니다.

각 로그 라인의 트랜잭션 ID를 사용하여 각 로그 라인에 제공된 정보를 이해합니다. 트랜잭션 유형을 식별하면 각 로그 라인의 송신자 정보를 가져옵니다. 각 로그 라인의 트랜잭션 유형과 송신자 정보는 각 노드 로그 라인에 필요한 소스 정보를 제공합니다.

주: 속성에서 SYS_UI_MACRO 및 SERVICE_PORTAL_WIDGET 스크립트 유형은 보고되지 않습니다.

트랜잭션 유형

다음은 트랜잭션 유형 목록입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 목록
- 양식
- XMLHttp
- 보고서
- SOAP
- 익스포트
- 스케줄러
- 텍스트 검색
- 기타
- REST
- JSON
- AMB
- 보관
- 배치 REST
- Instance Scan

시스템 속성

다음은 기능에 필요한 시스템 속성입니다.

- Glide.log.append.attribution: 이 속성은 기본적으로 활성화되어 있습니다. 각 노드 라인의 속성 정보를 켜거나 끕니다.
- Glide.db.log.append.classname.attribution: 이 속성은 기본적으로 활성화되어 있습니다. Java 클래스 이름 속성 로깅을 켜고 끕니다.

로그 변조 방지

시스템 로그 테이블 보호 규칙을 구성하여 애플리케이션 로그 기록의 수정 및 삭제 범위를 제한합니다. 규칙을 사용하면 이러한 테이블에서 변경 내용의 로깅 또는 변경 시도를 결정할 수 있습니다.

security_admin인 경우 플랫폼에서 다음 시스템 로그 테이블에 대한 업데이트, 삽입 및 삭제 작업을 제한할 수 있는 보호된 테이블 플러그인(com.glide.protected_tables)을 활성화합니다.

- Syslog
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- syslog_app_scope
- protected_table_configuration(구성을 수정할 수 없음)

> **주:** com.glide.protected_tables 플러그인은 위에서 언급한 시스템 로그 테이블에만 보호 기능을 제공합니다. 레코드를 업데이트, 삽입 또는 삭제하려고 하면 protected_table_log 테이블에 메시지가 로깅됩니다.

자세한 내용은 로그 보호 플러그인 설치 및 구성을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

각 시스템 로그 테이블에 대해 다음 로그 보호 수준 중 하나를 지정할 수 있습니다.

- 시도 차단 및 기록: 수정을 차단하고 시도를 기록합니다.
- 시도만 차단: 수정을 차단하고 시도를 기록하지 않습니다.
- 시도만 기록: 수정을 차단하지는 않지만 시도를 기록합니다.
- 시도를 차단하지 않고 기록하지 않음: 수정을 차단하지 않고 시도를 기록하지 않습니다

Platform은 각 시스템 로그 테이블에 지정된 로그 보호 수준을 사용하여 처음 만든 후 레코드를 수정하려는 시도를 차단 및/또는 로깅합니다.

주: security_admin인 경우 각 시스템 로그 테이블의 기본 로그 보호 수준을 재정의하여 인스턴스의 사용자 지정 사항에 맞게 조정할 수 있습니다.

시스템 로그 테이블을 수정하려는 시도가 있으면 protected_table_log 테이블에 로그됩니다.

주: 테이블에 대한 보호 수준이 지정되지 않은 경우 수정 시도는 protected_table_log 테이블에 기록되지 않습니다.

관리자 패널의 테이블에서 플러그인 작업을 비활성화하려면 com.glide.security.protected_table.enabled 속성을 false로 설정합니다. 자세한 내용은 로그 보호 속성 만들기를 참조하세요.

로그 보호 플러그인 구성

각 테이블 및 운영에 대한 보호 규칙을 구성하여 로그 보호 플러그인의 구성을 완료합니다.

시작하기 전에

필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 보호된 테이블 > 로그 보호.
   관리 패널 페이지가 표시됩니다.

   주: Utah 릴리스부터 보호된 테이블 플러그인이 기본적으로 설치되지만 사용하지 않도록 설정됩니다.

2. 플러그인을 계속 구성하려면 역할을 security_admin로 승격합니다.

   a. 시스템 관리자를 선택합니다.

   b. 역할 상승을 선택합니다.
   역할 상승 모달이 나타납니다.

   c. security_admin 옵션을 선택하여 역할을 승격하고 업데이트를 선택합니다.

3. 각 테이블 및 운영에 대한 보호 규칙을 구성합니다. 보호 규칙은 업데이트, 삽입 및 삭제에 적용됩니다. 일부 테이블의 경우 보호 수준을 변경할 수 없습니다. syslog 및 syslog_app_scope 테이블에는 업데이트 및 삭제 보호에 대한 고정 값이 있습니다. protected_table_configuration 테이블에는 세 가지 작업 모두에 대한 고정 보호 값이 있습니다.

   주: sysevent 테이블의 경우 삽입 보호를 차단으로 설정할 수 없습니다.

   이전 릴리스에서 syslog에 대해 하위 테이블에 적용을 켠 경우 Utah 릴리스로 업그레이드할 때 하위 테이블이 syslog와 동일한 보호 규칙을 사용하여 로그 보호에 추가됩니다. 이는 syslog에 대해서만 발생하며 다른 테이블에는 발생하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 로그 보호 사용 토글을 선택하여 기능을 사용하도록 설정합니다.

   주: sys_properties 테이블에서 com.glide.security.protected_table.enabled 속성을 변경해야만 이 플러그인을 비활성화할 수 있습니다.

로그 보호 속성 생성

로그 변조 위험을 방지하기 위해 로그 보호 속성을 생성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. *com.glide.security.protected_table.enabled* 속성이 시스템 속성 목록에 없으면 새로 만들기를 선택합니다.
   새 시스템 속성 양식이 나타납니다.
2. 양식에 상세 정보를 입력합니다

필드	설명
이름	속성 이름 com.glide.security.protected_table.enabled
애플리케이션	속성이 있는 애플리케이션입니다.
설명	속성 설명
선택	
유형	값 유형 - true 또는 false
값	속성의 실제 값
캐시 무시	캐시 내용을 무시하는 옵션
프라이빗	속성을 비공개로 만드는 옵션 ◦ 읽기 역할 ◦ 쓰기 역할

3. 제출을 선택하여 속성을 만듭니다.

로깅, 감사 및 오류(인스턴스 보안 강화)

의심스러운 활동을 적시에 식별하고 조치를 취할 수 있도록 로깅 및 감사 전략을 적용합니다.

인스턴스에 기록할 수 있는 항목에 대한 자세한 내용은 다음 문서를 참조하십시오 시스템 로그. 를 사용하여 로그인 및 실패한 로그인과 같은 시스템 이벤트를 모니터링하는 일정이 있는지 확인합니다 시스템 로그 > 이벤트.

SQL 오류 메시지 비활성화(인스턴스 보안 강화)

이 *glide.db.loguser* 속성을 사용하여 브라우저에서 SQL 오류 메시지가 렌더링되지 않도록 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 정보

속성	설명
속성 이름	glide.db.loguser
구성 유형	시스템 속성(/sys_properties_list.do)
인스턴스 보안 센터에서 구성 가능	아니요
목적	SQL 오류 메시지가 브라우저에 표시되지 않도록 설정합니다.
유형	true | false
권장 값	거짓
기능적 영향	(낮음) 이렇게 정정하면 SQL 오류 메시지의 렌더링이 비활성화됩니다. 기능에는 영향을 주지 않습니다.
보안 위험	(중간) 공격자에게 도움이 될 수 있는 중요한 SQL 정보가 웹 페이지에 오류 메시지의 일부로 표시되어서는 안 됩니다.

시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

비밀 관리

Secrets Management를 사용하여 ServiceNow 비즈니스 요구에 맞게 암호에 대한 액세스를 세부적으로 관리할 수 있습니다.

탐색



비밀 관리의 주요 기능과 비즈니스 가치를 알아봅니다.

분석



비밀 관리 대시보드에 대해 자세히 알아보십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성	
	
코어 구성을 계획합니다.	

비밀 관리 탐색

Secrets Management를 사용하여 ServiceNow 비즈니스 요구에 맞게 암호에 대한 액세스를 세부적으로 관리할 수 있습니다.

중요사항: 관리자는 비밀 관리와 관련된 모듈 및 기록을 볼 수 있는 역할이 있어야 합니다. 비밀 관리 역할 정보는 다음 문서를 참조하십시오 비밀 관리 역할.

비밀 관리의 코어 및 엔터프라이즈 버전 중에서 선택

비즈니스 요구에 따라 Secrets Management Core 및 Secrets Management Enterprise 중에서 선택합니다.

비밀 관리 코어	비밀 관리 엔터프라이즈
Secrets Management Core는 추가 비용 없이 인스턴스에서 활성화할 수 있습니다. 이 플러그인은 애플리케이션 엔지니어링 팀에서 생성한 ServiceNow 플랫폼에 제공된 ServiceNow 사용자 지정이 아닌 테이블의 기준에 따라 비밀 그룹을 사용하는 기능을 제공합니다.	비밀 관리 엔터프라이즈에는 관리자가 비밀 그룹을 만들고 관리하는 데 도움이 되는 추가 기능이 포함되어 있습니다. Enterprise는 Core에 나열된 기능 외에도 다음과 같은 기능을 제공합니다. • 세분화된 액세스 제어를 사용하여 이러한 기준에 따라 비밀 그룹을 생성합니다. ◦ 범위 ◦ 테이블 ◦ 열 ◦ 기록

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

비밀 관리 코어	비밀 관리 엔터프라이즈
	• 액세스할 수 없는 자체 키를 ServiceNow 사용하여 암호화된 클라이언트 접근 가능한 비밀을 생성합니다. • 비밀 관리 대시보드를 사용하여 인스턴스에 구성된 비밀 그룹을 검토하고 잠재적인 보안 문제에 대해 알아봅니다. 주: Secrets Management Enterprise는 직원이 프로덕션 인스턴스에서 활성화해야 하는 ServiceNow 유료 플러그인입니다.

비밀 그룹을 사용하여 비밀 구성

비밀 관리를 사용하여 보안 암호를 그룹으로 구성한 다음 그룹 수준에서 해당 보안 암호에 액세스 정책을 적용합니다.

기본 비밀 그룹

이러한 그룹은 범위 내의 모든 비밀에 적용됩니다. 이러한 비밀은 공통 암호화 모듈 및 모듈 액세스 정책에 의해 해독됩니다.

기준이 있는 비밀 그룹

기준이 있는 비밀 그룹은 기본 비밀 그룹과 동일하게 작동하지만 기준을 사용하여 포함된 항목을 더 구체화합니다. 이러한 기준은 다음과 같습니다.

- 애플리케이션 범위
- 패키지
- 테이블
- 비밀 열
- 기록 필터링

두 가지 유형의 비밀 그룹을 인스턴스에 접근하거나 클라이언트에 접근하도록 만들 수 있습니다.

인스턴스 측 비밀 그룹

인스턴스 측 보안 그룹에는 인스턴스에서 해독할 수 있는 보안 암호가 포함되어 있습니다.

클라이언트 측 비밀 그룹

클라이언트 측 비밀 그룹은 공개 및 개인 키 쌍을 사용하여 클라이언트에서만 암호를 해독할 수 있도록 합니다. 클라이언트가 액세스할 수 있는 비밀 그룹을 만들 때 공개 키를 인스턴스에 업로드하고 MID 서버에 개인 키를 유지합니다. 인스턴스는 공개 키를 사용하여 보안 암호를 암호화하지만 개인 키를 사용해야만 암호를 해독할 수 있습니다.

주: 이러한 그룹 유형에 대한 자세한 내용은 다음 문서를 참조하십시오 클라이언트 측 이해 비밀 관리.

보다 세분화된 제어를 위해 비밀 그룹 사용

password2는 플랫폼에서 사용할 수 있지만 Secrets Management는 ServiceNow 다음과 같은 추가 기능을 제공합니다.

세분화된 접근 제어	암호 2

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

	password2를 사용하면 관리자가 애플리케이션 범위에 대한 액세스를 제어할 수 있지만 범위 내의 요소에 대한 액세스는 제한할 수 없습니다. 비밀 관리 Secrets Management를 사용하면 관리자가 정의한 기준에 따라 액세스를 제한할 수 있습니다. 기준 유형은 패키지, 테이블 또는 열과 같은 기준을 기반으로 할 수 있습니다.
보안 스토리지	클라이언트 측 비밀 그룹의 경우 비밀 관리는 새로운 암호화 체계를 사용합니다. 이 암호화 체계 ServiceNow 에서는 암호화 키를 저장하지 않습니다. 이러한 이유로 데이터의 보안은 보안에 의존 ServiceNow 하지 않습니다.

그룹에 모듈 액세스 정책 적용

보안 암호를 보안 그룹으로 그룹화한 후 그룹 수준에서 해당 보안 암호에 액세스할 수 있는 방법을 결정하는 정책을 적용할 수 있습니다. 모듈 액세스 정책은 암호화 키에 대한 유효 시간 프레임과 같은 인스턴스 수준 제어를 정의하기 위해 암호화 모듈에 적용하는 액세스 제어 메커니즘입니다. 모듈 액세스 정책에 대한 자세한 내용은 모듈 액세스 정책 개요를 참조하세요.

비밀 관리와 함께 설치되는 테이블

비밀 관리는 이러한 테이블을 추가하거나 수정합니다.

새 테이블	
[sn_sm_secret_group]	비밀 그룹 저장
[sn_sm_secret_group_criteria]	기준 비밀 그룹 저장
[sn_sm_secret]	래핑된 비밀 저장
[sn_sm_identity_group]	ID 그룹을 공용 키에 매핑하기 위한 ID 그룹을 정의합니다.
[sys_kmf_wrapped_module_key]	래핑된 대칭 암호화 키를 저장합니다.
수정된 테이블	
[sys_kmf_crypto_module]	암호화 모듈 유형이 추가되었습니다. (ID 암호화 모듈 또는 비밀 그룹 암호화 모듈)
[sys_kmf_module_key]	• 개념적 비밀 암호화 키를 저장합니다(키 자료 없음). • ID 공개 키를 저장합니다.
[sys_kmf_crypto_caller_policy]	새 모듈 접근 정책 유형이 추가되었습니다.

비밀 관리 사용 사례 예시

안전한 ITOM 디스커버리 보장

이 인포그래픽에서는 조직에서 IT Operations Management(ITOM) 디스커버리를 배포할 수 있는 방법에 ServiceNow 대한 간단한 참조 아키텍처를 보여줍니다. 인포그래픽에서 볼 수 있듯이 여러 Windows 및 Linux 서버가 MID 서버에 연결되고 여러 MID 서버 에이전트가 검색 프로세스를 활성화하여 CMDB를 업데이트합니다. 모든 MID Server 트랜잭션에는 보안 인증이 필요하므로 보안 관점에서 인증 자격 증명을 관리하는 것이 중요합니다.

Integration Hub와의 안전한 워크플로우 연결 가속화

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 통합 허브를 사용하여 ServiceNow자동화된 API(애플리케이션 프로그래밍 인터페이스)를 사용하여 다른 시스템에 연결합니다. Integration Hub가 API를 사용하여 시스템에 연결할 때마다 연결을 설정하려면 인증 자격 증명이 필요합니다. 연결을 위한 다양한 애플리케이션과 API를 관리하려면 비밀 관리 솔루션이 필요합니다.

비밀 관리는 조직의 사이버 보안을 보장하는 데 있어 핵심적인 부분입니다. 암호화 키, API 토큰 및 암호와 같은 디지털 자격 증명의 생성, 저장, 전송 및 관리와 관련된 모든 프로세스와 도구를 다룹니다. 보안 암호를 안전하고 효과적으로 관리하기 위해 보안 암호 수명 주기의 모든 단계에 대한 표준 규칙 및 절차를 설정하는 핵심 보안 암호 관리 정책을 빌드할 수 있습니다.

클라이언트 측 이해 비밀 관리

비밀 및 그룹에 대한 액세스를 관리하는 데 사용하는 비밀 관리 방법을 알아봅니다.

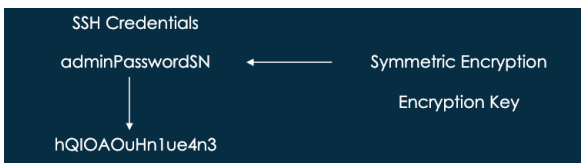
용어

클라이언트 측 비밀 관리는 프록시를 사용하지 않고 암호 해독된 데이터에 대한 액세스 권한을 부여 ServiceNow 하지 않고 비밀을 관리하는 방법을 제공하도록 설계되었습니다. 이 프로세스를 이해하려면 다음 암호화 용어로 시작합니다.

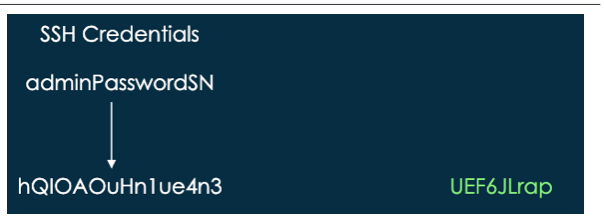
용어	설명
대칭 암호화	대칭 암호화는 동일한 단일 키를 사용하여 데이터를 암호화하고 해독합니다. 데이터가 대칭 키로 암호화된 경우 이 키만 있으면 암호를 해독할 수 있습니다.
대칭 키	대칭 키는 비밀을 암호화하여 일반 텍스트 암호를 읽을 수 없는 암호 텍스트로 변환합니다.
비대칭 암호화	비대칭 암호화는 두 개의 키를 사용하는데, 하나는 암호화하고 다른 하나는 해독합니다.
공개 키	공개 키는 비대칭 키 쌍의 절반입니다. 이 키는 인스턴스에 저장되며 이 키를 사용하여 대칭 키를 암호화합니다. 이 암호화된 대칭 키는 개인 키와 페어링된 경우에만 해독할 수 있습니다.
개인 키	개인 키는 비대칭 키 쌍의 절반입니다. 이 키는 MID Server의 키 스토어에 저장됩니다. ServiceNow 은(는) 이 키에 액세스할 수 없습니다. 공개 키와 결합된 비대칭 키 페어는 보안 암호를 해독하는 데 사용됩니다.

클라이언트 측 암호화 프로세스

대칭 키는 자격 증명(이 경우 관리자 암호)을 암호화하여 읽을 수 있는 일반 텍스트에서 암호화된 암호 텍스트로 변경합니다.



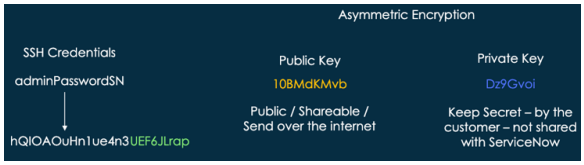
대칭 키(녹색으로 표시)를 자격 증명에 적용하여 암호화하거나 해독할 수 있습니다.



기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 시점에서 비대칭 암호화는 공개(노란색) 및 개인 키(파란색) 키를 사용하여 시작됩니다.



공개 키는 대칭 키와 함께 자격 증명을 암호화합니다. 이제 대칭 키가 보호되므로 자격 증명을 해독하는 데 사용할 수 없습니다. 공개 키는 이 암호화를 수행할 수 있지만 단독으로 사용하여 암호를 해독할 수는 없습니다.



공개 키로 암호화된 후 자격 증명을 해독하려면 개인 키가 필요합니다. 고객만 이 키를 가지고 있기 때문에 암호화된 자격 증명에 액세스할 수 있는 유일한 사람입니다.



클라이언트 접근 가능한 비밀 구성

클라이언트 접근 가능한 비밀을 사용하도록 인스턴스를 구성하는 방법에 대해 알아봅니다.

이 예제 구현을 사용하여 프록시를 사용하지 않고 구성 비밀 관리 하거나 암호 해독된 데이터에 대한 액세스 권한을 부여 ServiceNow 할 수 있습니다.

클라이언트 측 비밀 관리 을 사용하여 암호 및 그룹에 대한 액세스를 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 클라이언트 측 이해 비밀 관리.

이 지침에서는 로컬 네트워크에 MID 서버가 구성되어 있다고 가정합니다. 이 프로세스에 대한 자세한 내용은 문서를 참조하십시오 MID 서버 .

프로세스 개요

1. 암호화 키 및 인증서 생성

   로컬 환경에서 터미널 명령을 사용하여 암호화 키와 인증서를 생성합니다.

2. ServiceNow 신뢰할 수 있는 키 저장소에 인증서 추가

   신뢰할 수 있는 키 스토어에 ServiceNow 키와 인증서를 업로드합니다.

3. 기준을 사용하여 비밀 그룹 생성

   비밀에 대한 그룹을 생성합니다. 비밀 그룹을 사용하여 비밀을 그룹으로 구성합니다. 이러한 그룹을 사용하면 그룹 수준에서 해당 보안 암호에 액세스 정책을 적용할 수 있습니다. 그런 다음 비밀 그룹을 ID 그룹에 연결하고 MID 서버를 해당 ID 그룹에 추가합니다.

4. 공개/개인 키 페어를 MID 서버에 업로드

   공개/개인 키 페어를 MID 서버에 업로드합니다. 이 키 쌍을 사용하여 MID 서버가 인스턴스의 인증 요청을 처리할 수 있습니다.

5. 자격 증명 생성 및 자격 증명 암호화 테스트

   타사 시스템에 인증하기 위한 자격 증명을 생성하고 자격 증명에 액세스할 수 없는 ServiceNow 테스트를 수행합니다.

6. 통합을 관리하도록 플로우 디자이너 구성

   인스턴스에서 로컬 네트워크와 인스턴스 간의 통합을 관리하는 데 사용합니다 플로우 디자이너 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 엔드 투 엔드 클라이언트 측 암호화된 비밀 통합 테스트

   통합을 테스트하고 실행 상세 정보를 검토하여 구성이 작동하는지 확인합니다.

암호화 키 및 인증서 생성

로컬 환경에서 터미널 명령을 사용하여 암호화 키와 인증서를 생성합니다.

시작하기 전에

필요한 역할: 없음

프로시저

1. 로컬 환경에서 터미널(Mac 또는 Linux) 또는 명령줄(Windows)을 엽니다.
2. 터미널을 사용하여 `cd` 를 사용하여 암호화 키를 저장할 폴더로 이동합니다.
3. 터미널을 사용하여 다음을 입력합니다.

```
openssl req -newkey rsa:4096 -nodes -keyout sm_private_key.pem -x509
 -days 365 -out sm_public_cert.pem
```

   주: 이 예제에서는 OpenSSL을 사용하여 키와 인증서를 생성합니다. 요구 사항에 따라 다른 유사한 도구를 대체할 수 있습니다.

   이 명령은 개인 키와 공용 인증서(일치하는 공개 키 포함)를 생성합니다. "국가 이름"으로 시작하는 필수 정보를 묻는 일련의 프롬프트가 이어집니다.

4. 요청된 정보로 프롬프트를 채웁니다.
   다음과 같은 프롬프트가 나타납니다.
   - 국가 이름
   - 시/도 이름
   - 구/군/시 이름(예: 도시)
   - 조직 이름(예: 회사)
   - 조직 단위 이름(예: 섹션)
   - 일반 이름(예: 정규화된 호스트 이름)
   - 이메일 주소

   보안 팀과 협력하여 올바른 인증서 정보를 입력하도록 합니다.

```
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
```

5. 2단계에서 선택한 폴더를 확인하여 개인 키와 공용 인증서가 생성되었는지 확인합니다.
   3단계 예제와 동일한 파일 이름을 사용한 경우 다음 파일이 표시됩니다.
   - sm_private_key.pem
   - sm_public_cert.pem
6. 같은 폴더에서 다음 명령을 사용합니다.

   중요사항: 사용할 특정 명령은 운영 체제에 따라 다릅니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Linux의 경우:	`cat sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`
Windows의 경우:	`sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`

이 명령은 이후 단계에서 MID Server에 로드할 개인 키와 공개 인증서를 단일 파일로 묶습니다.

7. 폴더를 다시 확인하여 개인 키(sm_keypair_bundle.pem) 및 공용 인증서가 포함된 새 파일이 생성되었는지 확인합니다.

ServiceNow 신뢰할 수 있는 키 저장소에 인증서 추가

신뢰할 수 있는 키 스토어에 ServiceNow 키와 인증서를 업로드합니다.

시작하기 전에

필요한 역할: 관리자

이 예제에서 만든 공용 인증서는 "자체 서명된" 인증서로 간주됩니다(신뢰할 수 있는 루트 기관에서 제공되지 않았음을 의미). 인증서를 사용하려면 신뢰할 수 있는 키 스토어에 ServiceNow 인증서를 추가해야 합니다. 인증 기관에서 온 인증서를 사용하는 경우 이 단계를 완료할 필요가 없습니다.

프로시저

1. 로컬 환경에서 터미널(Mac 또는 Linux) 또는 명령줄(Windows)을 엽니다.
2. 터미널을 사용하여 `cd` 를 사용하여 암호화 키를 만든 폴더로 이동합니다.
3. 터미널에서 다음 명령을 입력합니다.

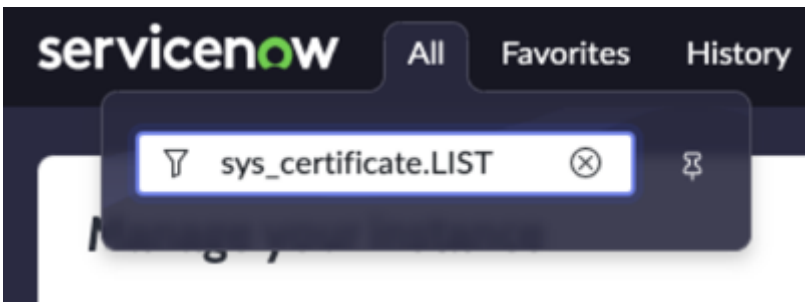
```
cat sm_public_cert.pem
```

신뢰할 수 있는 키 저장소에 복사하려면 공용 인증서의 내용을 확인해야 합니다. 이 `cat` 명령은 인증서를 표시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 인증서 정보를 클립보드에 복사합니다.
`-----BEGIN CERTIFICATE-----` 줄로 시작하고 `-----END CERTIFICATE-----` 줄로 끝나고 포함합니다.
5. ServiceNow 인스턴스에서 sys_certificate를 입력하여 **X.509** 인증서 목록으로 이동합니다. `LIST`를 입력합니다.



6. 새로 만들기를 선택하여 **X.509** 인증서 기록을 만듭니다.
7. 양식의 다음 필드에 내용을 입력합니다.

X.509 인증서 필드

필드	값
이름	인증서의 이름입니다. 이 이름은 선택한 이름이 될 수 있습니다.
형식	**PEM** 선택

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	값
	주: PEM(Privacy Enhanced Mail) 파일은 키 및 인증서에 사용되는 PKI(공개 키 인프라) 파일의 유형입니다. 이전 단계에서 생성한 기록은 이 파일 형식입니다.
유형	신뢰할 수 있는 스토어 인증서 선택
간단한 설명	인증서에 대한 설명입니다. 이 인증서의 용도를 알 수 있는 값을 입력합니다.
PEM 인증서	4단계에서 복사한 인증서 정보를 붙여넣습니다.

8. 제출을 선택하여 기록을 저장합니다.

기준을 사용하여 비밀 그룹 생성

비밀에 대한 그룹을 생성합니다. 비밀 그룹을 사용하여 비밀을 그룹으로 구성하고 그룹 수준에서 해당 비밀에 액세스 정책을 적용할 수 있습니다. 그런 다음 비밀 그룹을 ID 그룹에 연결하고 MID 서버를 해당 ID 그룹에 추가합니다.

시작하기 전에

필요한 역할: admin, KMF_admin, sn_secrets.secret_manager 및 sn_kmf.cryptographic_manager

프로시저

1. 다음으로 이동 모두 > 비밀 관리 > 기준이 있는 비밀 그룹.

2. 새로 만들기를 선택하여 기준 기록이 있는 비밀 그룹을 작성합니다.

3. 양식의 다음 필드에 내용을 입력합니다.

기준 필드가 있는 비밀 그룹

필드	값
그룹 이름	비밀 그룹의 이름입니다. 이 이름은 선택한 이름이 될 수 있습니다.
비밀 유형	클라이언트 접근 가능 선택
자동 작성 모듈	상자 선택
간단한 설명	비밀 그룹에 대한 설명입니다. 이 그룹의 용도를 나타내는 값을 입력합니다.
기준 유형	대상 테이블 선택
대상 테이블	**SSH** 자격 증명 선택 **[ssh_credentials]**

4. 양식 헤더를 길게 누르거나 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 저장을 선택하여 기록을 저장합니다.

5. 활성 확인란이 선택되어 있지 않은지 확인합니다.

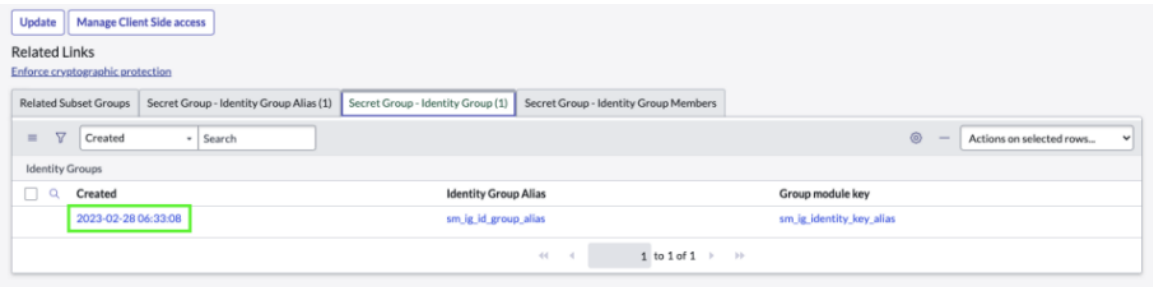
6. 클라이언트 쪽 액세스 관리 버튼을 선택하여 ID 그룹을 생성합니다.
ID 그룹 별칭 창이 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 새로 만들기 버튼을 선택합니다.
8. **ID** 그룹 별칭 필드 옆에 있는 참조 아이콘( )을 선택합니다.
9. 그룹 별칭 이름 필드에 값을 입력합니다.
   이 이름은 원하는 값이 될 수 있습니다.
10. 9단계에서 고유한 이름을 선택한 경우 제출을 선택합니다.
11. **ID** 키 업로드 단추를 선택합니다.
    ID 공개 키 인증서 가져오기 창이 표시됩니다.
12. **ID** 키 별칭 필드에 값을 입력합니다.

> **중요사항:** 이 값은 원하는 모든 것이 될 수 있지만 이후 단계에서 MID 서버에 삽입하는 값과 정확히 일치해야 합니다.

13. 임포트를 선택합니다.
    첨부 파일 창이 표시됩니다.
14. 파일 선택을 선택합니다.
15. 이전 단계에서 만든 공용 인증서를 선택합니다.
    이 인증서는 `sm_public_cert.pem` 파일이어야 합니다.
16. X 아이콘을 선택하여 창을 닫습니다.
17. 확인을 선택하여 **ID** 공개 키 인증서 가져오기 창을 닫습니다.
    파란색 키와 인증서가 인스턴스로 성공적으로 임포트되고, 임포트가 성공적으로 완료되었음을 확인하는 배너가 표시됩니다.
18. 제출을 선택합니다.
    ID 그룹 목록이 표시됩니다.
19. 목록에서 ID 그룹 기록 왼쪽에 있는 확인란을 선택합니다.
20. 비밀 그룹 연결 버튼을 선택합니다.
    기준 기록이 있는 비밀 그룹으로 돌아갑니다. 비밀 그룹 **- ID** 그룹 별칭" 및 비밀 그룹 **- ID** 그룹 관련 목록이 표시됩니다. 이러한 관련 목록에는 이전 단계에서 생성한 기록이 표시됩니다.
21. 비밀 그룹 **- ID** 그룹 관련 목록에서 해당 목록의 기록에 대해 생성된 필드를 선택합니다.



   ID 그룹 레코드가 표시됩니다.
22. **ID** 그룹 구성원 관련 목록에서 새로 만들기 버튼을 선택합니다.
    ID 그룹 구성원 기록이 표시됩니다.
23. 구성원 테이블 필드에서 **MID** 서버 (ecc_agent)를 선택합니다.
24. **ID** 그룹 구성원 기록 필드 옆에 있는 참조 아이콘( )을 선택하고 MID 서버를 선택합니다.

> **주:** 모든 기록 포함 확인란을 선택하면 인스턴스에 연결된 모든 MID 서버가 ID 그룹에 추가됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

25. 확인을 선택하여 문서 선택 창을 닫습니다.
26. 제출을 선택합니다.
27. (으)로 다시 이동 모두 > 비밀 관리 > 기준이 있는 비밀 그룹으로 클릭하고 2단계에서 생성한 기록을 엽니다.
28. 활성 필드를 활성화합니다.
29. 업데이트를 선택하여 기록을 저장합니다.

공개/개인 키 페어를 **MID** 서버에 업로드

공개/개인 키 페어를 MID 서버에 업로드합니다. 이 키 쌍을 사용하여 MID 서버가 인스턴스의 인증 요청을 처리할 수 있습니다.

시작하기 전에
필요한 역할: 없음

프라이빗 키에 대한 액세스 권한이 부족하기 때문에 ServiceNow 공개 키와 페어링하여 대칭 키를 해독한 다음 자격 증명을 해독할 수 없습니다. MID 서버가 이 암호화된 자격 증명을 사용하려고 하면 개인 키에 액세스하지 않으면 인증을 위해 자격 증명을 해독할 수 없습니다.

이 단계에서는 개인 키를 MID 서버에 업로드하여 퍼블릭/프라이빗 키 체인을 완성합니다. 이 업로드는 액세스 권한을 부여 ServiceNow 하지 않고 MID 서버 액세스 권한을 부여합니다.

MID 서버에 개인 키에 대한 액세스 권한을 부여하려면 Powershell에서 관리자 권한으로 실행할 명령을 구성해야 합니다. 이 예에서 명령은 Azure Windows 가상 머신에 대한 것입니다.

> **중요사항:**
>
> 이러한 단계를 수행하는 시스템이 MID 서버와 키 쌍 파일 모두에 액세스할 수 있는지 확인합니다.

프로시저

1. 로컬 환경에서 단계에서 키 쌍 암호화 키 및 인증서 생성 을 만든 폴더를 찾습니다.
2. `manage-certificates.bat` 파일의 전체 경로를 찾아 복사합니다.

   > **주:** 이 파일은 MID Server 폴더에 있습니다. MID 서버 폴더를 저장한 위치에 따라 경로는 다음 예와 같을 수 있습니다.

   ```
   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. 텍스트 파일을 만들고 경로를 파일에 붙여넣습니다.
4. 텍스트 파일에서 경로 뒤에 다음을 추가합니다.
   `-your_identity_key_alias`

   `your_identity_key_alias` 공용 인증서를 업로드할 때 생성한 ID 키 별칭의 이름으로 바꿉니다.
5. 키 쌍 파일의 전체 경로를 찾아 복사합니다.

   > **주:** 이러한 단계에서 이름을 사용한 경우 해당 파일의 이름은 `sm_keypair_bundle.pem`입니다.

6. 텍스트 파일에서 이 경로를 줄 끝에 추가하고 이 경로와 이전 정보 사이에 공백을 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

텍스트 파일 내의 텍스트는 다음 예제와 유사해야 합니다.

```
C:
\Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2
022__patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\sc
ripts\manage-certificates.bat -a your_identity_key_alias
 C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
```

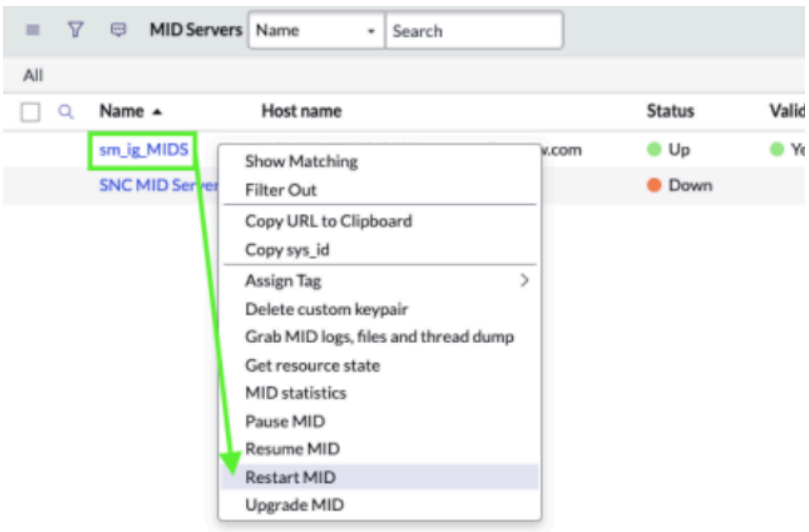
주: 이 예제에서는 `sm_keypair_bundle.pem` 파일이 바탕 화면에 있어 경로를 더 짧게 만듭니다.

7. 텍스트 파일의 전체 텍스트를 클립보드에 복사합니다.
8. 시스템에서 Powershell을 찾고 관리자 권한으로 실행 옵션을 선택합니다.
9. 텍스트 파일의 텍스트를 Powershell에 붙여넣고 Enter 키를 누릅니다.
   성공하면 다음 메시지가 표시됩니다.

```
Installed certificate with alias: <your_identity_key_alias> into the
 MID keystore.
```

팁: 이 메시지가 표시되지 않으면 명령에 오류, 공백 또는 불필요한 따옴표가 없는지 확인합니다. 전체 경로를 올바르게 입력했는지 확인하십시오.

10. MID 서버 기록으로 이동하여 기록을 마우스 오른쪽 버튼으로 클릭하고 **MID** 다시 시작을 선택하여 MID 서버를 다시 시작합니다.



MID 서버를 다시 시작하면 MID 키 스토어에 업로드된 키 쌍이 작업에 사용할 수 있도록 동기화됩니다. 계속하기 전에 **MID** 서버가 다시 시작될 때까지 기다렸다가 상태가 Up이고 확인된 값이 **Yes** 입니다.

자격 증명 생성 및 자격 증명 암호화 테스트

타사 시스템에 인증하기 위한 자격 증명을 생성합니다.

시작하기 전에
필요한 역할: admin, KMF_admin, sn_secrets.secret_manager 및 sn_kmf.cryptographic_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항: MID 서버에 로그인한 사용자는 admin, KMF_admin, sn_secrets.secret_manager 및 sn_kmf.cryptographic_manager 역할도 있어야 합니다.

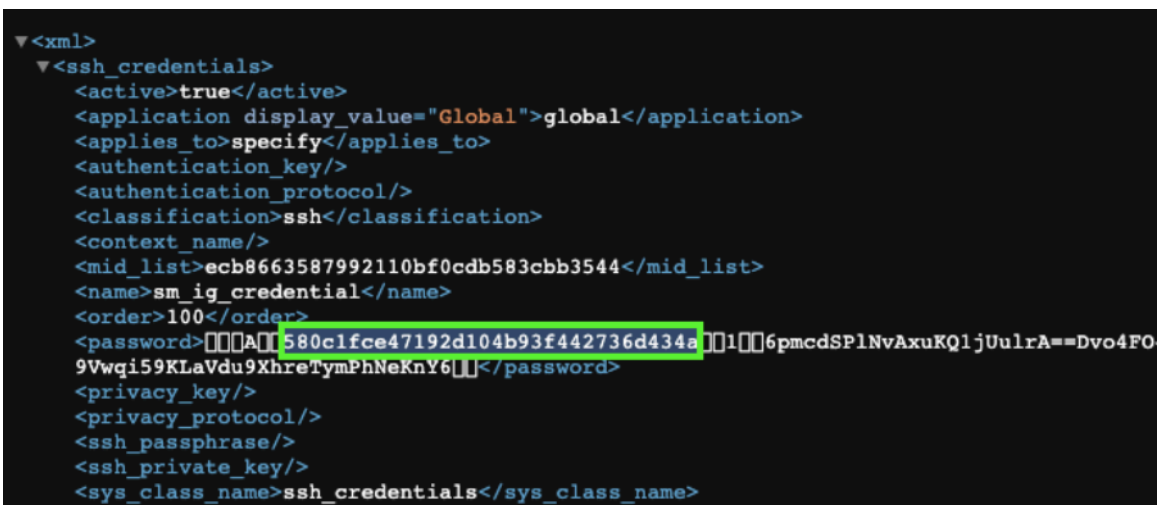
프로시저

1. 탐색 필터에 `ssh_credentials.list`를 입력하여 **SSH** 자격 증명 목록으로 이동합니다.
2. 새로 만들기를 선택하여 **SSH** 자격 증명 기록을 생성합니다.
3. 양식의 다음 필드에 내용을 입력합니다.

SSH 자격 증명 양식

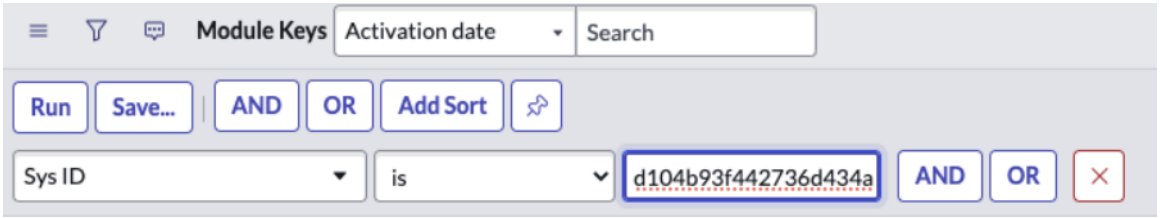
필드	값
이름	자격 증명 기록의 이름을 입력합니다. 이 이름은 원하는 값이 될 수 있습니다.
적용 대상	특정 **MID** 서버 선택
MID 서버	MID 서버를 선택합니다.
사용자 이름	사용자 이름을 입력합니다.
암호	사용자 이름 필드에 사용자와 관련된 암호를 입력합니다.

4. 자격 증명 별칭 필드 옆에 있는 잠금 아이콘(잠금)을 선택합니다.
5. 참조 아이콘( )을 선택하여 연결 및 자격 증명 별칭 목록을 엽니다.
6. 새로 만들기를 선택하여 연결 및 자격 증명 별칭 기록을 생성합니다.
7. 이름 필드에 이름을 입력합니다.
8. 유형 필드에서 자격 증명을 선택합니다.
9. 제출을 선택합니다.
   SSH 자격 증명 기록으로 돌아갑니다. 다음 단계에서는 자격 증명이 암호화되었는지 테스트합니다.
10. 양식 헤더를 길게 누르거나 마우스 오른쪽 단추로 클릭하고 **XML** 표시를 선택합니다.
11. XML에서 `<password>` XML 태그를 찾습니다.
12. 이 `<password>` 태그 내의 sys_id 클립보드에 복사합니다.
    sys_id는 이 자격 증명을 암호화하는 데 사용되는 대칭 키를 나타내는 32자 코드입니다. SSH 자격 증명 테이블에 입력한 암호화된 암호는 같은 줄에 있는 두 상자 집합 중 오른쪽에 있습니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

13. 탐색 필터에 `sys_kmf_module_key.list`를 입력하여 모듈 키 목록으로 이동합니다.
14. 시스템 **ID** 필드가 12단계에서 복사한 sys_id와 일치하는 기록에 대한 목록을 필터링하고 실행을 선택합니다.



검색에서 단일 모듈 키 기록이 반환되어야 합니다. 이 기록은 대칭 키를 성공적으로 생성했으며 사용하고 있음을 보여줍니다.

15. 탐색 필터에 `sys_kmf_wrapped_module_key.list`를 입력하여 래핑된 모듈 키 목록으로 이동합니다.
16. 암호화 모듈 필드가 이전 단계에서 작성한 암호화 모듈과 일치하는 기록에 대한 목록을 필터링하고 실행을 선택하십시오.
검색에서 단일 래핑된 모듈 키 레코드가 반환되어야 합니다. 이 목록에서 다음을 확인할 수 있습니다.
    - 래핑된 키 자료 열은 SSH 자격 증명을 암호화하는 데 사용되는 암호화 모듈 내의 대칭 키가 ID 그룹에 업로드한 공개 키로 암호화되었음을 보여줍니다.
    - 래핑된 키 시스템 **ID** 필드에는 래핑 키 시스템 **ID**(ID 그룹에 업로드된 공개 키)에 의해 암호화되는 키(암호화 모듈 대칭 키)가 표시됩니다.

이전 필드가 기본적으로 목록에 없는 경우 목록 개인화 아이콘( )을 선택하여 목록에 추가할 수 있습니다.

주: 인스턴스는 10분마다 정리 작업을 실행하여 분리된 키를 제거하고 자격 증명을 업데이트한 후 연결되지 않은 키의 확산을 방지합니다.

통합을 관리하도록 플로우 디자이너 구성

인스턴스에서 로컬 네트워크와 인스턴스 간의 통합을 관리하는 데 사용합니다 플로우 디자이너 .

시작하기 전에

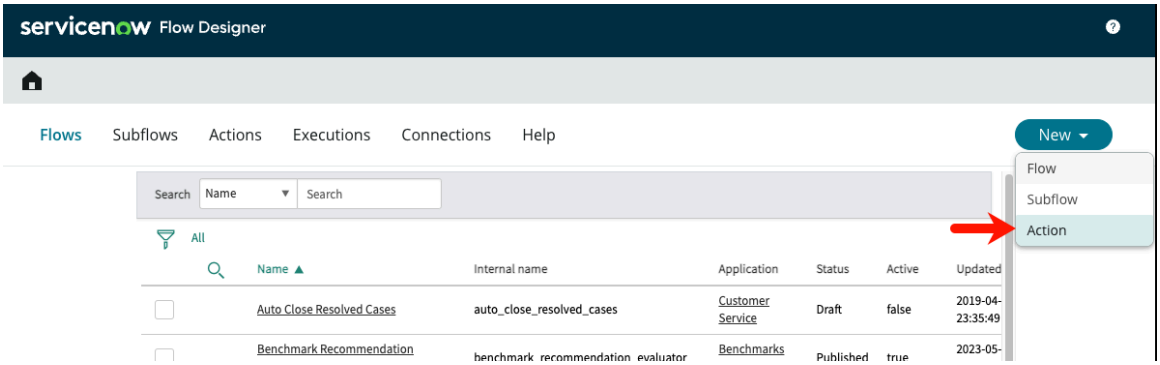
필요한 역할: admin, KMF_admin, sn_secrets.secret_manager 및 sn_kmf.cryptographic_manager

이 단계에서는 워크플로우를 플로우 디자이너 생성하여 로컬 시스템에 텍스트 파일을 생성합니다.

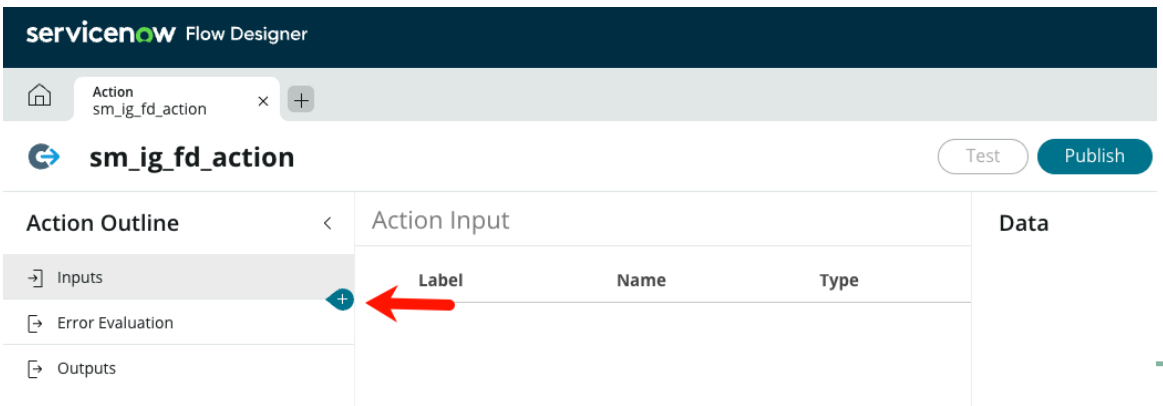
프로시저

1. 인스턴스에서 다음으로 이동합니다. 모두 > 프로세스 자동화 > 플로우 디자이너.
2. 새로 만들기를 선택하고 작업을 선택하여 작업을 ServiceNow 만듭니다.

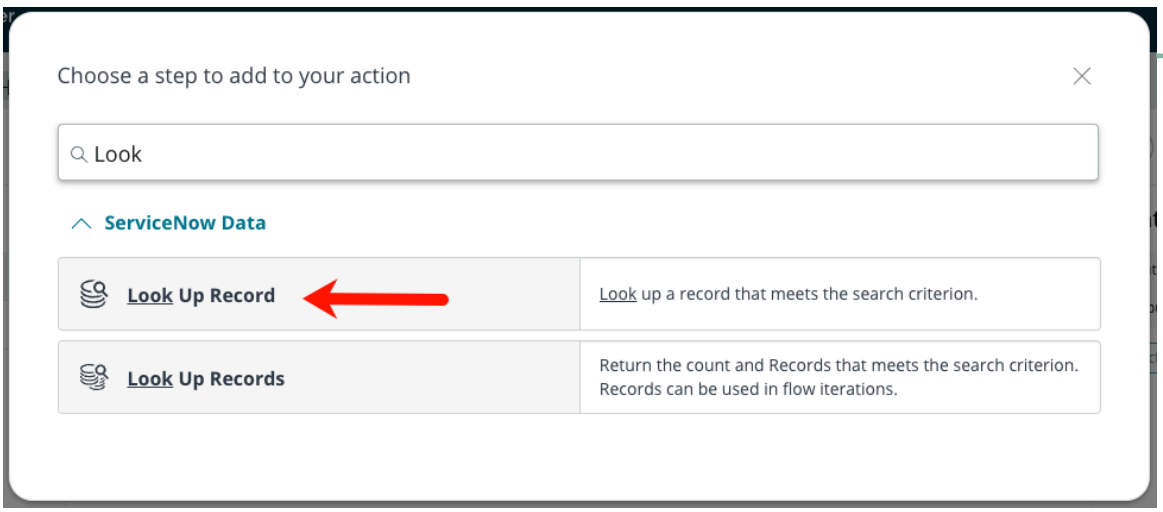
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 작업 이름 필드에 이름을 입력하고 제출을 선택합니다.
4. 작업 개요에서 입력과 오류 평가 사이의 더하기 기호를 선택하여 단계를 생성합니다.



5. 작업에 추가할 단계 선택 창에서 기록 조회를 선택합니다.



6. 기록 조회 단계 섹션의 테이블 필드에서 **MID** 서버 **[ecc_agent]**를 선택합니다.
7. 기록 조회 단계 아래에서 더하기 기호를 선택하여 다른 단계를 생성합니다.
8. 작업에 추가할 단계 선택 창에서 **SSH**를 선택합니다.

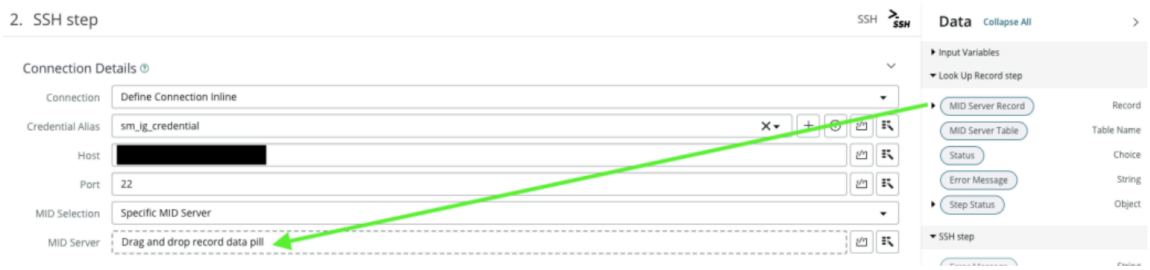
   주: **SSH** 옵션이 표시되지 않으면 필요한 플러그인을 활성화해야 합니다.

9. **SSH** 단계 섹션에서 다음 정보를 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	값
연결	연결 인라인 정의 선택
자격 증명 별칭	이전 단계에서 생성된 SSH 자격 증명에 대한 자격 증명 별칭을 선택합니다.
호스트	SSH를 통해 연결하는 호스트의 IP 주소를 입력합니다.
포트	`22# #####.`
MID 선택	특정 **MID** 서버를 선택합니다.

10. **MID** 서버 필드를 채우려면 데이터 섹션에서 **MID** 서버 기록 알약을 필드로 끌어옵니다.



⚠ 경고: 알약을 필드로 끌 때 알약 옆에 있는 검은색 화살표가 아닌 알약을 선택합니다.

11. **SSH** 구성 섹션에서 명령 필드에 다음 값을 입력합니다.

```
/bin/date > sm_ig_text_file.txt
```

이 명령은 MID 서버에서 암호가 해제된 비밀을 사용하여 로컬 시스템에 텍스트 파일을 만듭니다. MID 서버는 인스턴스에 암호 해독된 비밀에 대한 액세스 권한을 부여 ServiceNow 하지 않고 (를 통해플로우 디자이너) 인스턴스에 대한 액세스 ServiceNow 권한을 부여합니다.

💡 팁: `/bin/date` 명령은 생성된 텍스트 파일에 현재 날짜/시간을 삽입합니다. 이 명령은 텍스트 파일이 생성된 시기와 비교하여 현재 날짜/시간을 기준으로 통합이 실시간으로 수행되고 있음을 보여줍니다.

12. 저장 버튼을 선택하여 워크플로우를 저장합니다.

엔드 투 엔드 클라이언트 측 암호화된 비밀 통합 테스트

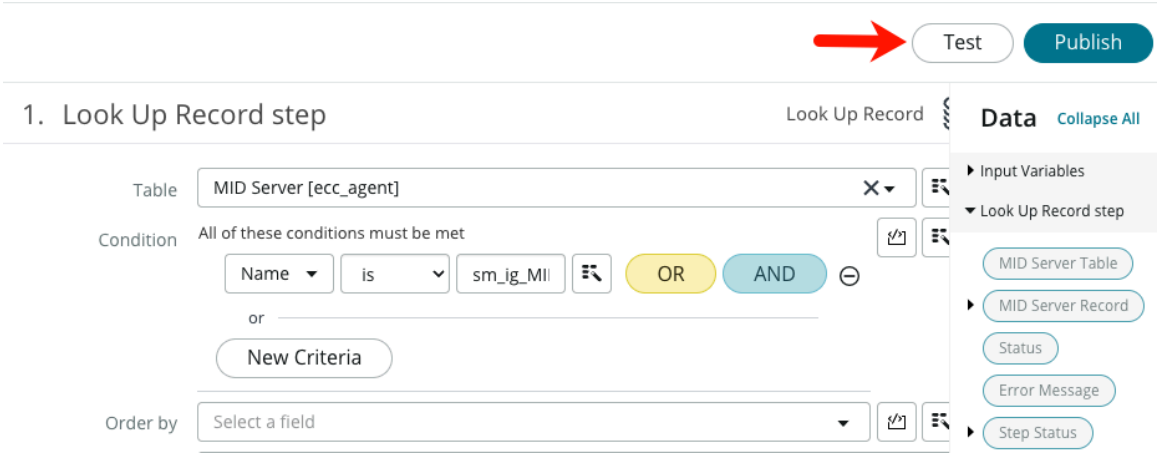
통합을 테스트하고 실행 상세 정보를 검토하여 구성이 작동하는지 확인합니다.

시작하기 전에
필요한 역할: admin, KMF_admin, sn_secrets.secret_manager 및 sn_kmf.cryptographic_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 에서 플로우 디자이너 화면 오른쪽 상단 모서리에 있는 테스트 버튼을 선택합니다.



2. 테스트 작업 창에서 테스트 실행을 선택합니다.
3. 테스트 실행이 완료되었습니다를 선택합니다 . 작업 실행 상세 정보를 봅니다.
4. 화면 오른쪽 상단에 테스트 실행 – 완료 됨이 표시될 때까지 화면을 새로 고칩니다.
5. 화면 왼쪽 아래에 있는 단계 화살표를 선택합니다.
6. 다음 성공 메시지와 함께 단계 출력 데이터 제목이 표시될 때까지 아래로 스크롤합니다.

```
{"Step Status";{"code";0,"message";"Success"}}
```

7. 에서 플로우 디자이너이 메시지를 본 후 텍스트 파일이 로컬 시스템에 생성되었는지 확인합니다.

비밀 관리로 암호화된 **Windows Management Instrumentation** 자격 증명 테스트

WMI(Windows Management Instrumentation) 자격 증명이 비밀 관리로 암호화되었는지 확인하고 통합 허브 워크플로우를 사용하여 엔드 투 엔드 테스트를 완료합니다.

시작하기 전에
필요한 역할: admin, KMF_admin, sn_secrets.secret_manager 및 sn_kmf.cryptographic_manager

- Integration Hub Enterprise가 인스턴스에서 활성 상태여야 합니다. 자세한 내용은 통합 허브 플러그인 요청 문서를 참조하십시오.
- 인스턴스에 구성된 비밀 그룹이 있어야 합니다. 에 나열된 클라이언트 접근 가능한 비밀 구성1-3단계를 참조하십시오.
- 비밀 관리로 암호화된 구성 자격 증명이 있어야 합니다. 에 나열된 자격 증명 생성 및 자격 증명 암호화 테스트1-9단계를 참조하십시오.

프로시저

1. 원하는 MID 서버가 비밀 그룹과 연결되어 있는지 확인합니다.
   기준 〔sn_sm_criteria_secret_group〕로 비밀 그룹을 열고 비밀 그룹 **- ID** 그룹 구성원 목록에서 MID 서버를 찾습니다. MID 서버가 그룹과 연결되어 있지 않은 경우 문서를 참조하십시오 기준을 사용하여 비밀 그룹 생성.
2. 자격 증명이 비밀 관리를 사용하여 암호화되었는지 확인합니다.

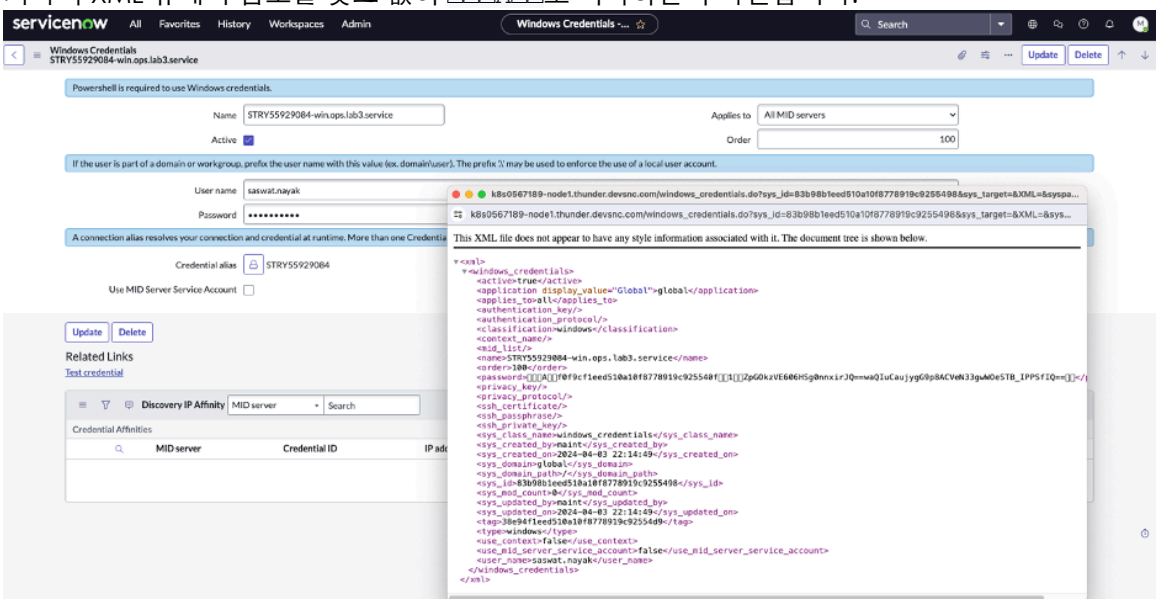
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 모두 > 통합 허브 > 연결 및 자격 증명 > 자격 증명.

b. 자격 증명 기록을 엽니다.
자격 증명 별칭 필드에 자격 증명 별칭이 나열되어 있는지 확인합니다. 아직 생성하지 않은 경우 문서를 참조하십시오 연결 및 자격 증명 별칭 생성.

c. 자격 증명 기록의 헤더를 길게 누르거나 마우스 오른쪽 버튼으로 클릭하고 목록에서 **XML** 표시를 선택합니다.

d. 기록의 XML 뷰에서 암호를 찾고 값이 □□□A□□로 시작하는지 확인합니다.



3. 워크플로우 스튜디오에서 테스트 워크플로우 생성

a. 다음으로 이동 모두 > 프로세스 자동화 > 워크플로우 스튜디오.

b. 새로 만들기를 선택한 다음, 목록에서 작업을 선택합니다.

c. 작업 이름 필드에 이름을 입력합니다.
애플리케이션 필드를 전역으로 설정된 상태로 둡니다.

d. 빌드 작업 버튼을 선택합니다.

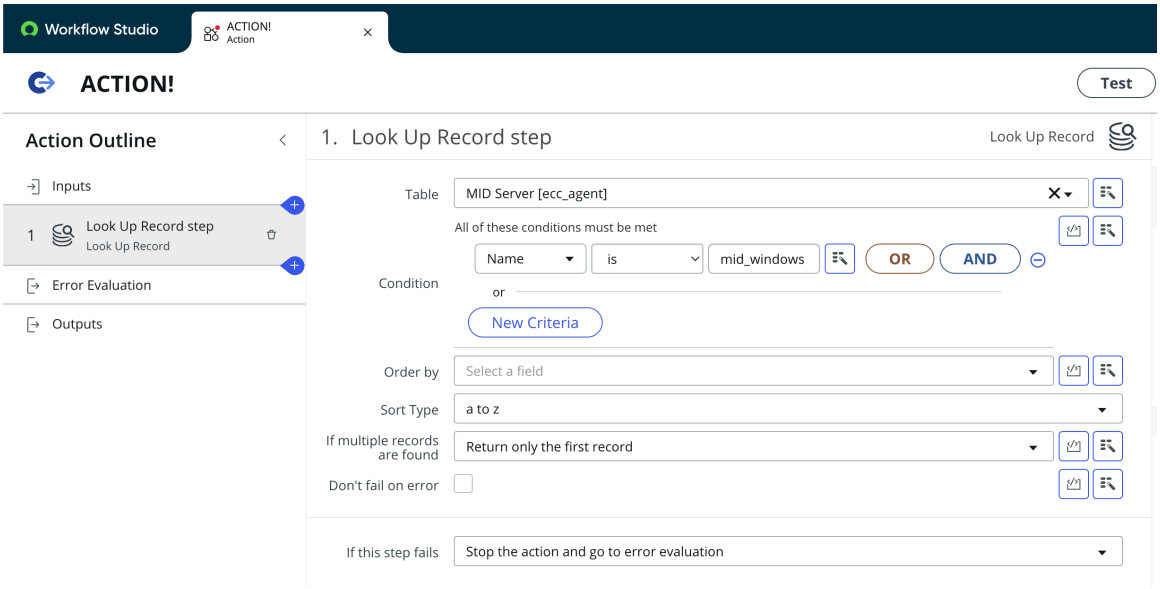
4. 워크플로우 스튜디오에서 기록 조회 단계를 구성합니다.

a. 작업 개요에서 더하기 버튼을 선택하여 새 단계를 추가합니다.
기록 조회 단계 유형을 찾아 선택합니다.

b. 테이블 필드에서 **MID** 서버 (ecc_agent)를 선택합니다.

c. 조건으로 이름, MID 서버 이름을 차례로 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



중요사항: 선택한 MID 서버가 비밀 그룹에 연결된 서버와 동일한지 확인합니다.

5. 워크플로우 스튜디오에서 기록 조회 단계를 구성합니다.

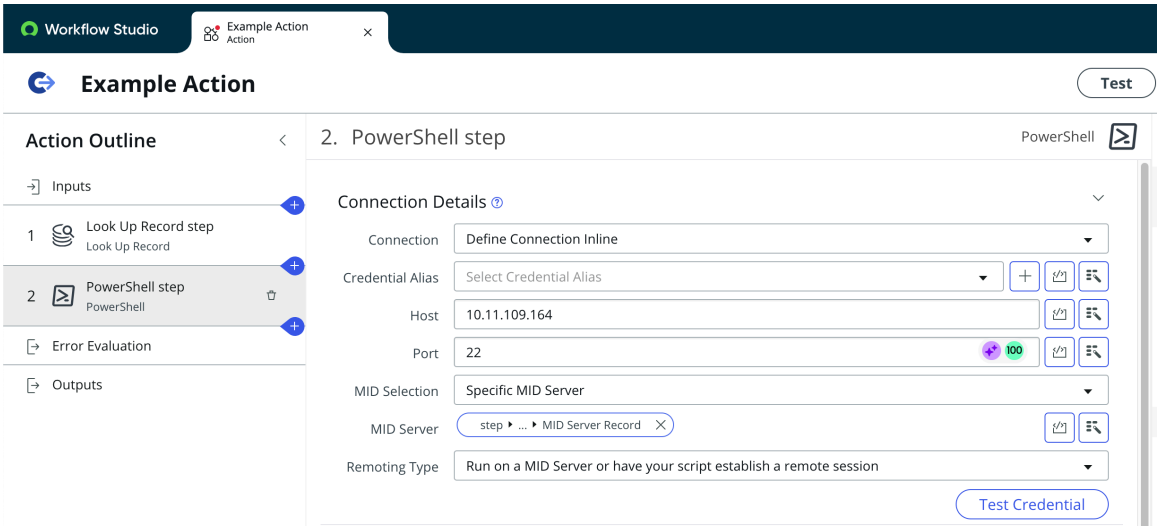
a. 작업 개요에서 더하기 버튼을 선택하여 기록 조회 단계 아래에 새 단계를 추가합니다. **PowerShell** 단계 유형을 찾아 선택합니다.

b. PowerShell 단계 양식에서 필요에 따라 필드에 내용을 입력합니다.

PowerShell 단계 필드

필드	값
연결	연결 인라인 정의 선택
자격 증명 별칭	자격 증명 별칭 선택
호스트	대상 Windows Server의 IP 주소 입력
포트	아직 기본값이 아닌 경우 22 를 입력합니다.
MID 선택	특정 **MID** 서버 선택
MID 서버	데이터 패널에서 **MID** 서버 기록 정제를 끌어옵니다 이 데이터 알약은 화면 오른쪽 가장자리의 데이터 패널에서 기록 조회 단계 아래에 표시됩니다.
원격 유형	**MID** 서버에서 실행을 선택하거나 스크립트에서 원격 세션을 설정하도록 하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 테스트 작업에 대한 스크립트를 생성합니다.

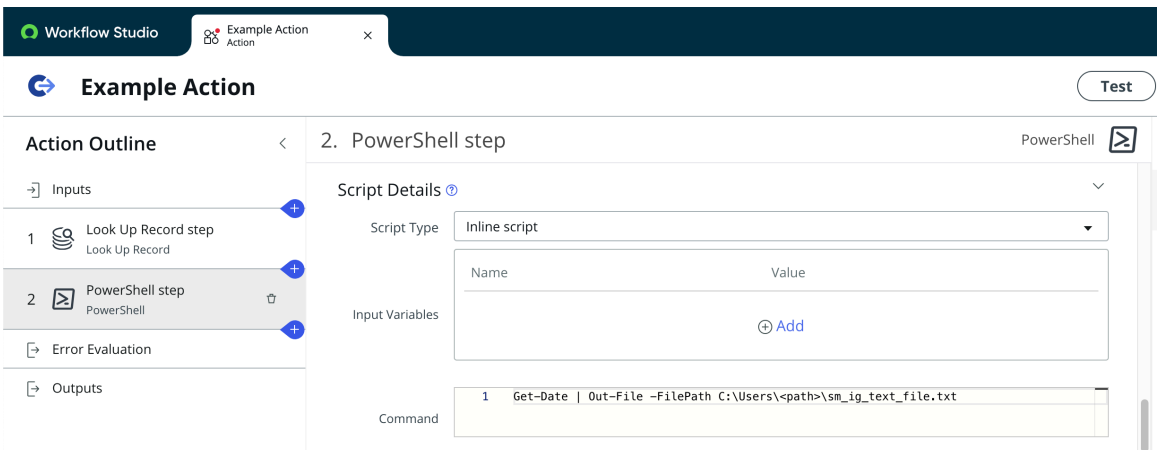
   a. 스크립트 유형 필드에서 인라인 스크립트를 선택합니다.

   b. 다음 스크립트를 사용하여 예시 경로를 테스트 호스트의 경로로 바꿉니다.

```
Get-Date | Out-File -FilePath C:\Users\<path>\sm_ig_text_file.txt
```

   주: 원격 호스트 구성에 적합한 스크립트를 직접 실행할 수도 있습니다. SM 암호화 값을 사용하여 연결이 설정되었는지 확인하는 것이 중요합니다.

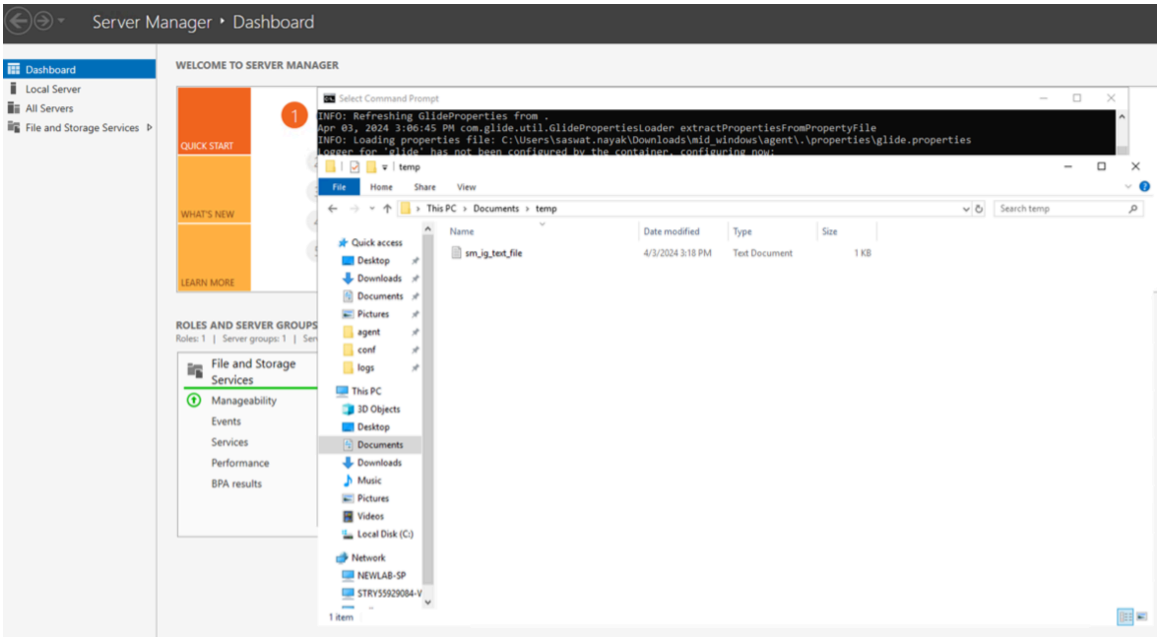
   c. 저장 버튼을 선택하여 작업을 저장합니다.



7. 테스트 버튼을 선택하여 작업을 테스트합니다.
8. 출력 로그에서 오류 메시지를 검토합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 스크립트에 제공한 파일 경로의 호스트 서버에서 테스트 파일이 생성되었는지 확인합니다.



복제 및 비밀 관리

클론 후 비밀 그룹 및 클라이언트 비밀 그룹을 재구성하는 방법을 알아봅니다.

인스턴스를 복제한 후 비밀 그룹과 클라이언트 비밀 그룹이 예상대로 작동하도록 재구성해야 할 수 있습니다.

비밀 그룹 원본	클론 후 동작
원본 인스턴스 비밀 대상 인스턴스의 그룹	누락된 암호화 모듈을 수동으로 임포트한 후 예상대로 작동합니다. XML을 통해 데이터 내보내기 및 가져오기 문서를 참조하십시오.
대상 인스턴스의 원래 클라이언트 비밀 그룹	누락된 암호화 모듈을 수동으로 임포트한 후 예상대로 작동합니다. XML을 통해 데이터 내보내기 및 가져오기 문서를 참조하십시오.
소스 인스턴스에서 복제된 인스턴스 비밀 그룹	수동으로 설정하지 않으면 작동하지 않습니다.
소스 인스턴스에서 복제된 클라이언트 비밀 그룹	SG/ID 그룹/별칭/MID를 수동으로 구성하는 경우 작업

비밀 관리 대시보드

비밀 관리 대시보드를 사용하여 인스턴스에 구성된 비밀 그룹을 검토하고 보안 문제에 대해 알아봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

비밀 그룹 개요



비밀 그룹 개요 탭에는 구성된 비밀 그룹에 대한 정보가 표시됩니다. 이 탭을 사용하여 인스턴스에 구성된 비밀 그룹에 대한 정보를 볼 수 있습니다.

유형별 비밀 그룹

인스턴스에 설치된 비밀 그룹을 비밀 유형(클라이언트 측의 인스턴스 측)별로 그룹화하여 보여 주는 원형 차트를 표시합니다.

기준 유형별 비밀 그룹

사용된 기준 유형별로 인스턴스에 구성된 기준이 있는 비밀 그룹을 보여 주는 원형 차트를 표시합니다.

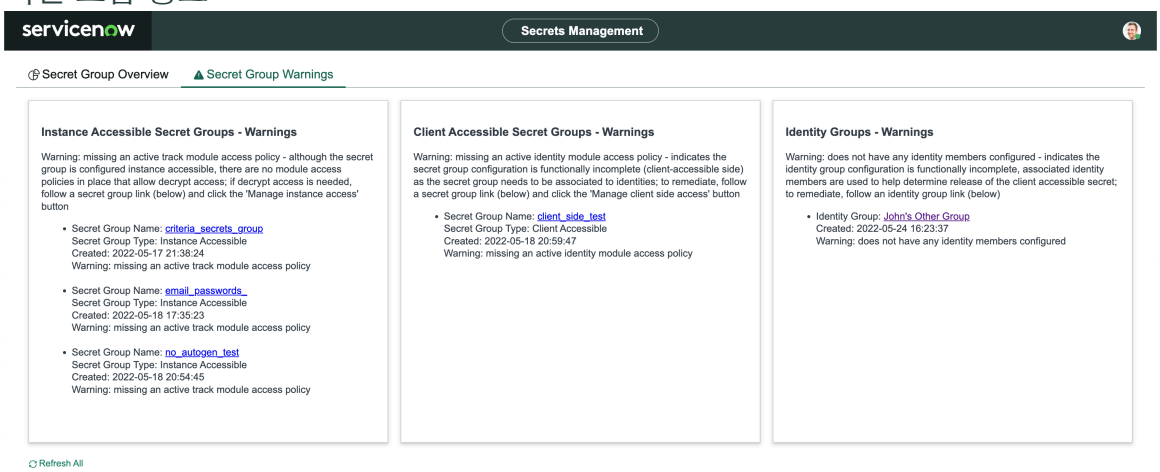
비활성 비밀 그룹 수

인스턴스에 구성된 비활성 비밀 그룹의 수를 표시합니다.

전용 비밀 수

기본 비밀 그룹 내의 비밀 수를 표시합니다.

비밀 그룹 경고



Secret Group Warnings(비밀 그룹 경고) 탭에는 비밀 그룹 및 ID 그룹과 관련된 경고가 표시됩니다.

인스턴스 접근 가능 비밀 그룹 - 경고

이 카드는 활성 액세스 정책이 없는 비밀 그룹이 있는 경우 경고를 표시합니다. 해당 기록을 보려면 비밀 그룹 이름을 선택합니다.

클라이언트 접근 가능 비밀 그룹 - 경고

이 카드는 활성 MAP(ID 모듈 액세스 정책)이 없는 클라이언트 접근 가능한 비밀 그룹이 있는 경우 경고를 표시합니다. 해당 기록을 보려면 비밀 그룹 이름을 선택합니다.

ID 그룹 - 경고

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 카드는 그룹 구성원이 구성되지 않은 ID 그룹이 있는 경우 경고를 표시합니다. 기록을 보려면 ID 그룹 이름을 선택합니다.

주: Secrets Management 대시보드는 Secrets Management Enterprise의 일부입니다. Secrets Management Enterprise는 직원이 프로덕션 인스턴스에서 활성화해야 하는 ServiceNow 유료 플러그인입니다.

비밀 관리 역할

비밀 관리는 이러한 역할을 추가합니다.

비밀 관리자 **[sn_secrets.admin]**

관리자가 아닌 비밀 역할을 다른 사용자에게 할당합니다. 비밀 관리자는 비밀 관리자 및 최종 사용자와 동일한 권한을 갖습니다.

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

중요사항: 보다 전문적인 역할을 사용할 수 있는 경우 관리자 역할을 부여하지 마십시오.

- 사용자에게 sn_secret.admin 역할을 할당하려면 admin 역할과 security_admin 역할이 모두 있어야 합니다.
- 더 많은 대상 역할을 사용할 수 있는 경우 관리자 역할을 부여하지 마십시오.

비밀 관리자 **[sn_secrets.manager]**

다음 기능을 수행할 수 있어야 하는 사용자에게 이 역할을 부여합니다.

- 비밀 및 비밀 그룹 기록 보기
- 접근 이력 및 기타 사용 활동 정보 보기
- 비밀 그룹 및 필터 생성
- 비밀 제공자 생성
- 비밀 그룹 간에 비밀 이동
- 비밀 그룹 및 비밀 제공자 설정 변경

역할 포함

역할에 포함된 역할 목록입니다.

없음.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

중요사항: 비밀 관리자는 일반 텍스트의 비밀을 볼 수 없습니다.

비밀 뷰어 **[sn_secrets.viewer]**
비밀 및 비밀 그룹 기록을 볼 수 있어야 하는 사용자에게 이 역할을 부여합니다.

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

없음.

비밀 그룹 암호화 모듈 작성

암호화 및 암호 해독을 수행할 비밀 그룹 암호화 모듈을 생성합니다.

시작하기 전에

필요한 역할:

- 관리자
- sn_secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_manager
- sn_kmf.admin

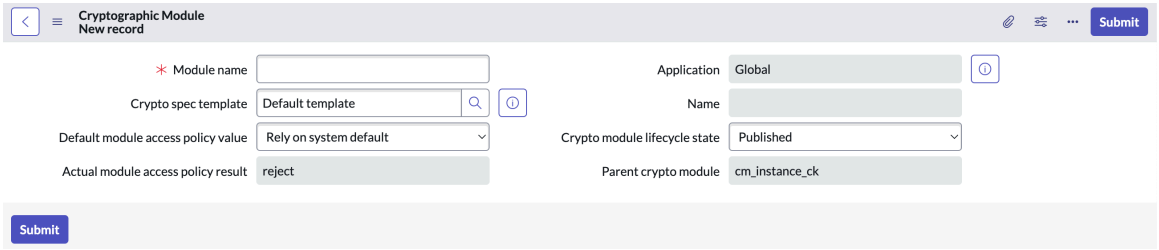
프로시저

1. 다음으로 이동 모두 > 비밀 관리 > 비밀 그룹 암호화 모듈 작성.
2. 작성하려는 그룹 암호화 모듈의 유형을 선택합니다.

암호화 모듈 유형	설명
인스턴스 접근 가능한 비밀 암호화 모듈 작성	인스턴스에서 해독할 수 있는 인스턴스 접근 가능한 비밀을 생성합니다.
클라이언트 접근 가능한 비밀 암호화 모듈 작성	액세스할 수 없는 사용자 고유의 키를 ServiceNow 사용하여 암호화된 클라이언트 접근 가능한 비밀을 만듭니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 암호화 모듈 양식의 필드에 내용을 입력합니다.



필드	설명
모듈 이름	모듈을 설명하는 이름입니다
애플리케이션	모듈을 포함하는 애플리케이션 범위입니다. 이 필드는 자동으로 현재 모듈로 채워집니다.
암호화 사양 템플릿	기본 템플릿 이 기본적으로 선택됩니다.
이름	모듈의 이름입니다. 이 이름은 애플리케이션 및 모듈 이름에 따라 자동으로 생성됩니다.
기본 모듈 접근 정책 값	◦ 시스템 기본값 사용 ◦ 거부 ◦ 트랙
암호화 모듈 수명 주기 상태	모듈이 초안 상태인지 게시됨 상태인지 여부입니다.
실제 모듈 접근 정책 결과	이 필드는 정보 제공을 목적으로 하며 읽기 전용입니다.
상위 암호화 모듈	상위 암호화 모듈로, 이전 단계에서 선택한 암호화 모듈 유형에 따라 결정됩니다. 이 필드는 읽기 전용입니다.

4. 제출을 선택합니다.

기본 비밀 그룹 생성

기준에 관계없이 비밀을 그룹화할 기본 비밀 그룹을 만듭니다.

시작하기 전에
필요한 역할: 관리자

기본 비밀 그룹에는 테이블, 범위 또는 애플리케이션에 관계없이 추가하는 모든 비밀이 포함될 수 있습니다. 생성한 후 그룹에 수동으로 비밀을 추가합니다. 이와 같은 공통 속성을 공유하는 모든 비밀에 대한 그룹을 생성하려면 의 기준을 사용하여 비밀 그룹 생성지침을 사용하여 기준이 있는 비밀 그룹을 생성합니다.

프로시저

1. 다음으로 이동 모두 > 비밀 관리 > 비밀 그룹.
2. 새로 만들기를 선택합니다.
3. 어떤 유형의 비밀 그룹을 작성하시겠습니까?에서 기본 비밀 그룹을 선택합니다.
4. 비밀 그룹 양식의 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

비밀 그룹 필드

필드	설명
그룹 이름	그룹의 이름입니다 주: 비밀 그룹 이름에는 소문자, 숫자 및 밑줄(_)만 사용할 수 있습니다.
비밀 유형	그룹이 인스턴스 접근 가능 한지 또는 클라이언트 접근 가능한지 여부입니다.
자동 작성 모듈	이 비밀 그룹에 대한 새 암호화 모듈을 작성합니다. 이 모듈은 데이터를 암호화하고 해독합니다. 이 필드는 기본적으로 활성화됩니다.
애플리케이션	이 기록에 대해 범위가 지정된 애플리케이션입니다. 이 읽기 전용 필드는 현재 범위로 자동으로 채워집니다.
간단한 설명	그룹의 설명
암호화 모듈	이 그룹에 사용할 암호화 모듈을 선택하십시오. 이 모듈은 데이터를 암호화하고 해독합니다. 이 필드는 자동 작성 모듈을 선택하지 않은 경우에만 표시됩니다. 모듈 액세스 정책에 대한 자세한 내용은 모듈 액세스 정책 개요를 참조하십시오. 주: 인스턴스 액세스 관리 버튼을 사용하여 보안 그룹과 관련된 모듈 액세스 정책을 검토할 수 있습니다.

5. 제출을 클릭합니다.

주: 비밀 그룹을 만들면 기본적으로 비활성 상태가 됩니다. 그룹 기록으로 돌아가 활성 을 선택하여 그룹을 활성화합니다.

기준을 사용하여 비밀 그룹 생성

테이블이 테이블, 범위 또는 애플리케이션과 같은 공통 기준을 공유할 때 Password2 필드에 입력된 비밀을 자동으로 구성하려면 기준을 사용하여 비밀 그룹을 생성합니다.

시작하기 전에

필요한 역할: admin, KMF_admin, sn_secrets.secret_manager 및 sn_kmf.cryptographic_manager

이 유형의 비밀 그룹 내의 비밀은 모두 공통 기준을 공유해야 합니다. 이 제한이 없는 그룹의 경우 기본 비밀 그룹을 만드는 것이 좋습니다. 에서 기본 비밀 그룹 생성기본 비밀 그룹을 만드는 방법에 대해 알아봅니다.

프로시저

1. 다음으로 이동 모두 > 비밀 관리 > 비밀 그룹.

2. 새로 만들기를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 어떤 유형의 비밀 그룹을 작성하시겠습니까? prompr에서 기준이 있는 비밀 그룹을 선택합니다.
4. 비밀 그룹 양식의 필드에 내용을 입력합니다.

비밀 그룹 필드

필드	설명
그룹 이름	그룹의 이름입니다 주: 비밀 그룹 이름에는 소문자, 숫자 및 밑줄(_)만 사용할 수 있습니다.
비밀 유형	그룹이 인스턴스 접근 가능 한지 또는 클라이언트 접근 가능한지 여부입니다.
자동 작성 모듈	이 비밀 그룹에 대한 새 암호화 모듈을 작성합니다. 이 모듈은 데이터를 암호화하고 해독합니다. 이 필드는 기본적으로 활성화됩니다.
애플리케이션	이 기록에 대해 범위가 지정된 애플리케이션입니다. 이 읽기 전용 필드는 현재 범위로 자동으로 채워집니다.
간단한 설명	그룹의 설명
기준 유형	이 그룹의 비밀이 공유하는 기준입니다. ◦ 범위 ◦ 패키지 ◦ 대상 테이블 ◦ 비밀 열 ◦ 기록 필터링
암호화 모듈	이 그룹에 사용할 암호화 모듈을 선택하십시오. 이 모듈은 데이터를 암호화하고 해독합니다. 이 필드는 자동 작성 모듈을 선택하지 않은 경우에만 표시됩니다. 모듈 액세스 정책에 대한 자세한 내용은 모듈 액세스 정책 개요를 참조하십시오. 주: 인스턴스 액세스 관리 버튼을 사용하여 보안 그룹과 관련된 모듈 액세스 정책을 검토할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 구성에 따라 암호화 모듈은 자동으로 선택된 값을 사용할 수 있습니다.

기준 유형 필드가 #### 설정되고 자동 작성 모듈 필드가 선택된 경우:	암호화 모듈 필드가 비어 있으며 읽기 전용입니다. 기존 Password2 서브모듈이 사용됩니다. Password2 하위 모듈을 찾을 수 없는 경우 인스턴스 수준 Glide Encrypter 모듈이 사용됩니다.
기준 유형 필드가 #### 설정되고 자동 작성 모듈 필드가 선택 취소된 경우: (자동 작성 모듈 필드는 엔터프라이즈 사용자만 선택 취소할 수 있음)	암호화 모듈 필드는 편집 가능하며, 관리자는 사용할 암호화 모듈을 선택할 수 있습니다.

5. 양식 헤더를 길게 누르거나 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.

주: 비밀 그룹을 만들면 기본적으로 비활성 상태가 됩니다.

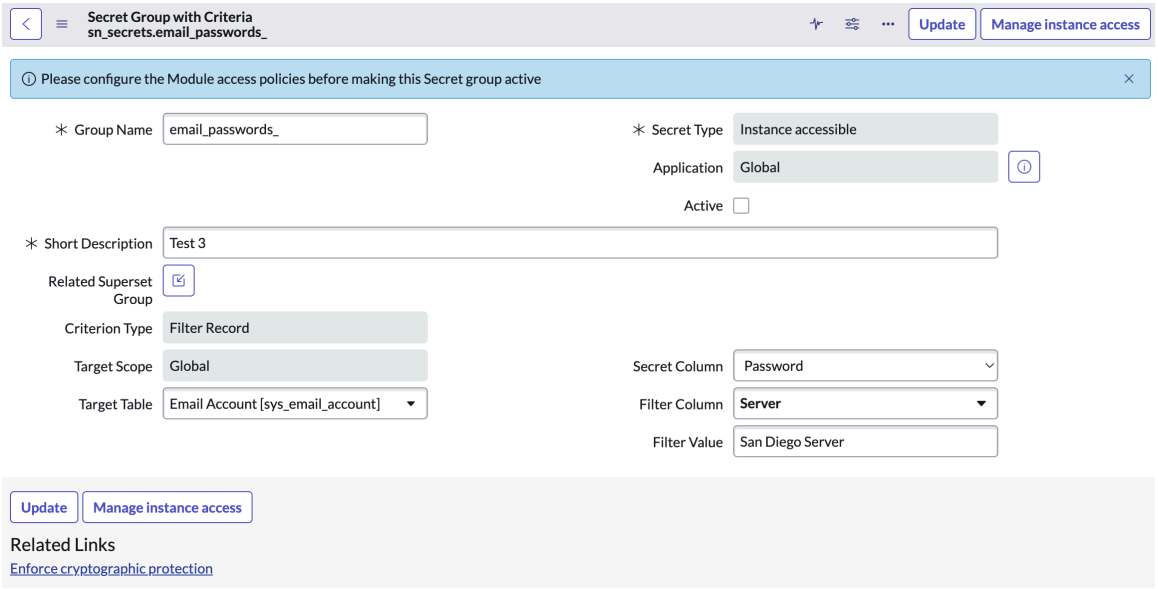
6. 기록을 저장한 후 그룹을 구성한 방법에 따라 추가 필드가 나타날 수 있습니다.

추가 비밀 그룹 필드

필드	설명
대상 범위	이 그룹에 할당할 비밀이 공유하는 범위입니다. 이 필드는 기준 유형 필드에서 ### 선택한 경우에만 사용할 수 있습니다.
대상 패키지	이 그룹에 할당할 비밀에서 공유하는 패키지입니다. 이 필드는 기준 유형 필드에서 #### 선택한 경우에만 사용할 수 있습니다.
대상 테이블	이 그룹에 할당할 비밀이 공유하는 테이블입니다. 이 필드는 기준 유형 필드에서 ### 또는 ## ## 선택한 경우에만 사용할 수 있습니다.
대상 범위	대상 테이블 필드에서 선택한 테이블의 애플리케이션 범위입니다. 이 필드는 기준 유형 필드에서 ###, ## # 또는 ## ## 선택한 경우에만 표시됩니다.
비밀 열	이 그룹에 포함하는 pasword2 비밀이 들어있는 테이블 열입니다. 이 목록에서 사용할 수 있는 필드는 대상 테이블 필드에서 선택한 테이블에 따라 결정됩니다. 주: 선택 테이블에 비밀이 포함된 열이 없는 경우 이 필드는 - ## - 만 선택 항목으로 표시됩니다.
필터 열	필터로 사용할 대상 테이블에서 선택한 테이블의 열입니다. 이 필드는 Password2 필드일 수 없습니다.
필터 값	필터로 사용할 값입니다. 이 필터는 필터 열 필드에서 선택한 필드에 적용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example: 이메일 서버의 모든 이메일 계정 암호를 포함하는 인스턴스 접근 가능한 그룹



다음에 수행할 작업

그룹을 생성하면 기준과 일치하는 새 기록이 모두 암호화됩니다. 이 그룹의 암호화 모듈을 사용하여 기존 기록을 암호화하려면 보안 작업을 실행해야 합니다. 자세한 내용은 비밀 관리 보안 작업 실행 문서를 참조하십시오.

클라이언트 액세스 가능 그룹은 비밀을 암호화하기 위해 고객이 제공한 공개 키가 필요합니다. 이 키를 업로드하는 단계는 문서를 참조하십시오 비밀 관리를 위한 공개 키 업로드.

비밀 관리를 위한 공개 키 업로드

비밀을 암호화하기 위한 공개 키를 업로드합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 비밀 관리 > 비밀 그룹을 클릭하고 비밀 그룹 기록을 엽니다.
2. 기록에서 클라이언트 쪽 액세스 관리 버튼을 선택합니다.
   새 ID 그룹 레코드가 열립니다.
3. **ID** 키 업로드 단추를 선택합니다.
   ID 공개 키 인증서 가져오기 창이 표시됩니다.
4. **ID** 키 별칭 필드에 키의 별칭을 입력합니다.
5. 임포트 단추를 선택하여 로컬 환경에서 키를 업로드합니다.
6. **OK** 버튼을 선택합니다.
   그룹 모듈 키 필드는 ID 키 별칭 이름을 사용합니다.
7. 제출을 선택하여 ID 그룹 기록을 저장합니다.

비밀 관리 보안 작업 실행

인스턴스의 비밀 필드에 대한 암호화 작업을 수행하도록 비밀 관리 작업을 예약합니다.

시작하기 전에

필요한 역할: sn_kmf.admin, security_admin, sn_secrets.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 단계를 수행하려면 security_admin 역할로 승격해야 합니다. 이 프로세스에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 보안 작업 > 새로 작성.
2. 어떤 유형의 보안 작업을 생성하시겠습니까? 프롬프트에서 비밀 관리 작업을 선택합니다.
3. 양식의 필드에 내용을 입력합니다.

비밀 관리 작업 양식

필드	설명
이름	보안 작업의 이름
상태	초기 작업 상태는 신규입니다. 작업이 예정대로 실행되면 상태가 그에 따라 업데이트됩니다.
기간 시작	24시간 형식의 작업 시작 시간입니다. 선택한 시간에 작업이 실행을 시작합니다.
기간 종료	24시간 형식의 작업 종료 시간입니다. 이 시간까지 작업이 완료되지 않으면 작업이 완료될 때까지 지정된 다음 처리 기간 동안 작업이 계속됩니다.
시행 수준	작업이 모든 테이블 또는 특정 테이블이나 필드 선택에 영향을 미치는지 여부 다음 중에서 선택합니다. ◦ 모든 테이블 ◦ 특정 테이블 ◦ 특정 필드 ◦ 특정 패키지 ⚠ 경고: 모든 테이블 옵션을 선택하면 인스턴스 성능에 영향을 줄 수 있습니다. 사용량이 많지 않은 시간에 예약하는 것이 좋습니다.
패키지	이 작업에 포함할 패키지입니다. 선택한 패키지에 암호화가 적용됩니다. 이 옵션은 적용 수준 필드가 특정 패키지로 설정된 경우에만 표시됩니다
테이블	이 작업에 포함할 테이블입니다. 암호화는 선택한 테이블 내에서 적용 가능한 모든 필드에 적용됩니다. 이 옵션은 적용 수준이특정 테이블로 설정된 경우에만 표시됩니다.
필드	이 작업에 포함할 테이블입니다. 선택한 모든 필드에 암호화가 적용됩니다. 이 옵션은 적용 수준이특정 필드로 설정된 경우에만 표시됩니다.
작업 모드	다음 중에서 선택합니다. 비밀 관리에 대한 Password2

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	각 그룹의 모듈 액세스 정책에 정의된 암호화 모듈을 사용하여 비밀 그룹 내의 모든 password2 필드를 암호화합니다. Password2에 대한 비밀 관리 password2 암호화를 사용하여 비밀 그룹의 데이터를 다시 암호화합니다. 이 암호화 유형에 대한 자세한 내용은 KMF를 사용한 Password2 암호화를 참조하세요. 비밀 그룹 적용 비밀 그룹 필드에서 선택한 그룹과 일치해야 하는 모든 데이터를 쿼리합니다. 쿼리에서 찾은 모든 데이터가 이미 그룹에 있는 경우 작업은 변경되지 않습니다. 쿼리가 아직 그룹에 없는 데이터를 찾으면 작업은 비밀 그룹 내에서 이 데이터를 다시 암호화합니다. 주: 이 쿼리에서 찾은 데이터가 이미 암호화되어 있고 인스턴스가 해당 데이터를 해독할 수 없는 경우 암호화되지 않고 비밀 그룹에 추가됩니다.
비밀 그룹	암호화할 비밀을 포함하는 비밀 그룹입니다. 이 필드는 작업 모드 필드에서 비밀 그룹을 선택한 경우에만 사용할 수 있습니다.
데이터 키 강제 입력	
요약	작업 진행률에 대한 정보를 표시합니다. 요약에는 작업으로 암호화할 수 없는 기록도 표시됩니다.

4. 제출을 선택합니다.

다음에 수행할 작업
이 작업은 선택한 비밀 그룹과 일치해야 하는 모든 데이터를 쿼리합니다. 쿼리에서 찾은 모든 데이터가 이미 그룹에 있는 경우 작업은 변경되지 않습니다. 쿼리가 아직 그룹에 없는 데이터를 찾으면 작업은 비밀 그룹 내에서 이 데이터를 다시 암호화합니다. (인스턴스가 암호를 해독할 수 있는 경우, 클라이언트 측에서 암호화된 암호의 경우에는 해당되지 않을 수 있음).

코드 서명

코드 서명은 나중에 데이터의 진위 및 무결성을 확인하기 위해 확인된 데이터에 대한 디지털 서명을 생성합니다. 코드 서명은 의 ServiceNow 볼트구성요소로 사용이 허가된 모듈입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

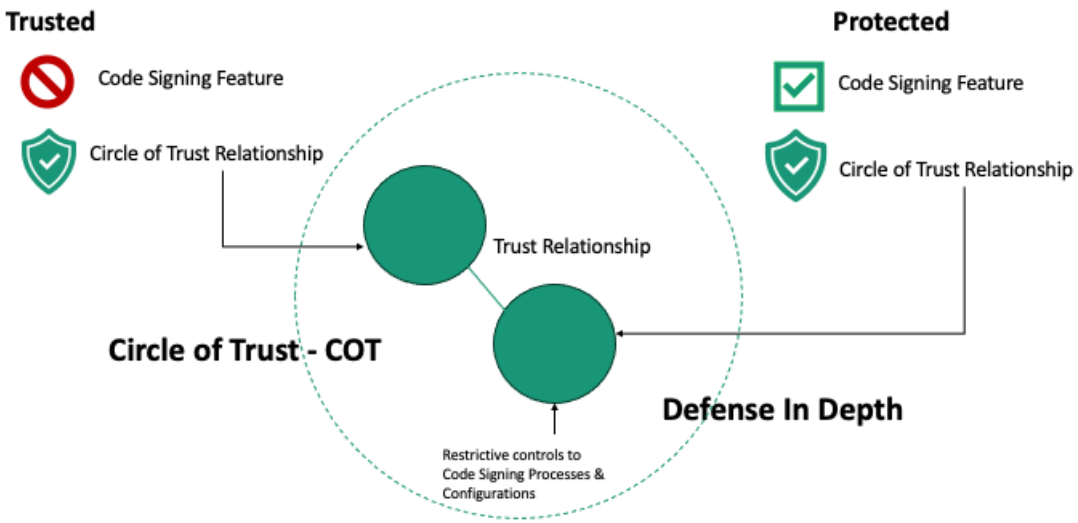
코드 서명 및 **Circle of Trust**

Circle of Trust ()COT는 신뢰할 수 있는 인스턴스와 보호된 인스턴스 간에 보안 통신을 생성하여 권한 있는 사용자만 코드 서명 기능에 액세스할 수 있도록 하는 코드 서명의 필요 조건입니다.

다양한 보안 조치를 통해 보호된 인스턴스가 손상된 경우 악의적인 행위자가 코드 서명을 비활성화하거나 오용하지 못하도록 방지할 수 있습니다. 심층 방어 전략 COT 의 일부로 다음 구성요소를 사용합니다.

- 가장 강력한 관리자 계정도 제한하는 통제가 보호된 인스턴스에 설정되어 코드 서명 프로세스 및 구성을 보호합니다.
- 신뢰할 수 있는 인스턴스는 보호된 인스턴스와 함께 작동하여 관계를 설정해야 합니다 Circle of Trust . 신뢰할 수 있는 인스턴스가 하나 이상 필요하지만 보호된 인스턴스와 공동 작업하도록 신뢰할 수 있는 인스턴스를 여러 개 구성할 수 있습니다.

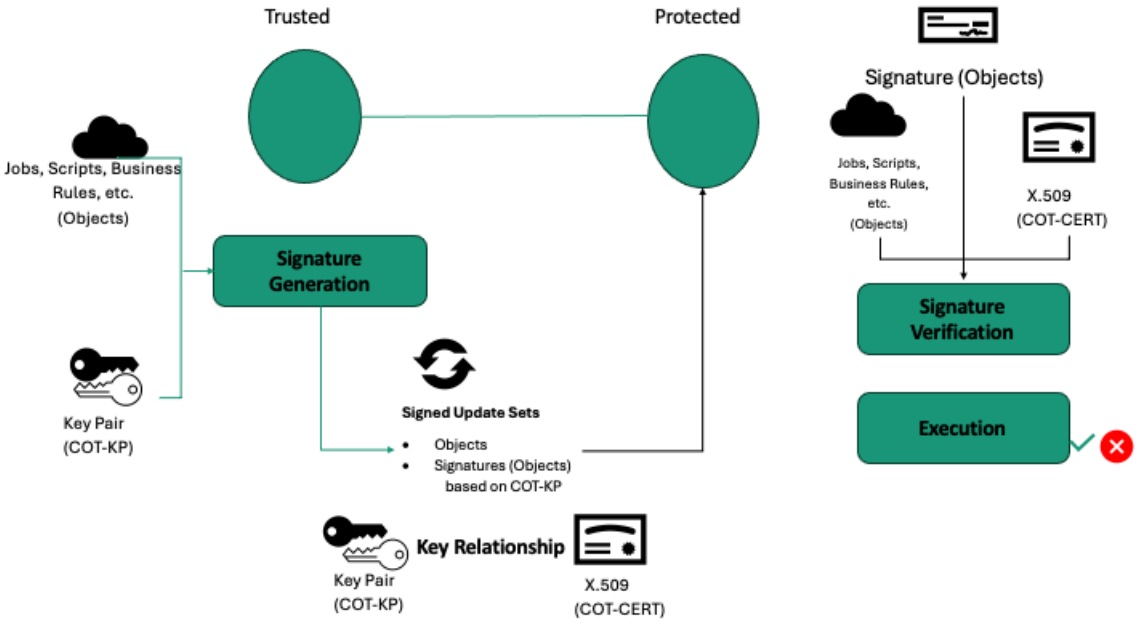
Circle of Trust 개요



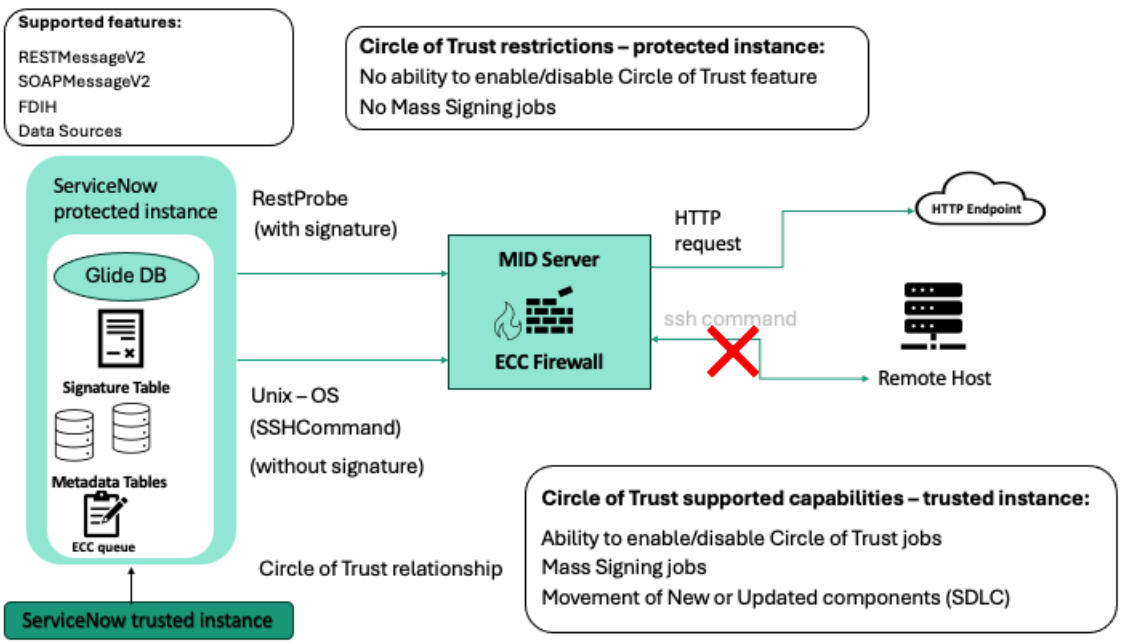
Circle of Trust 키 쌍과 함께 작업, 스크립트 및 비즈니스 규칙을 사용하여 보호된 인스턴스에 업데이트 세트에 서명하는 서명을 작성합니다. 작업이 호출되면 신뢰할 수 있는 인증서와 함께 서명이 확인되어 보호된 인스턴스 업데이트를 실행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Trusted Update Sets 프로세스



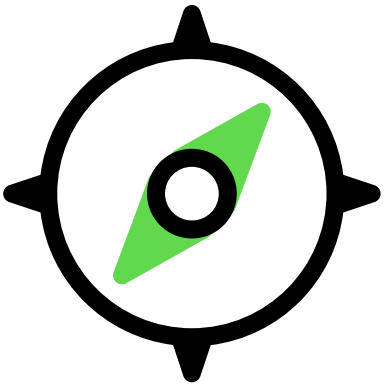
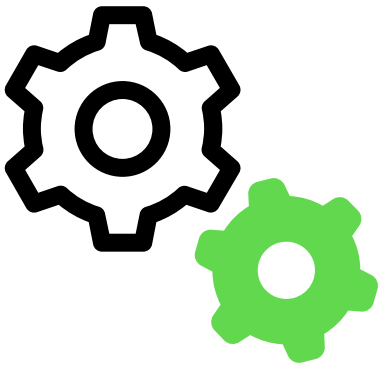
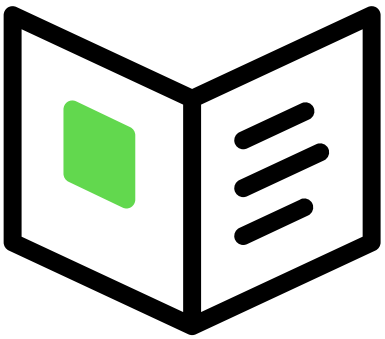
코드 서명 플로우

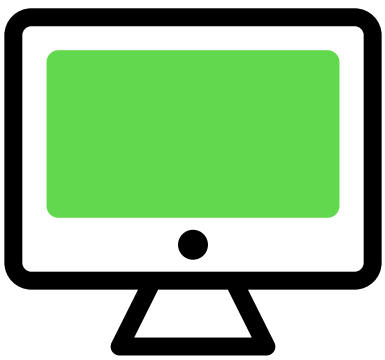


이를 Circle of Trust 위해서는 신뢰할 수 있는 인스턴스와 보호된 인스턴스 간의 초기 신뢰 관계가 필요하며, 이를 통해 권한 부여 수준이 지정된 권한이 없는 사용자가 승인되지 않은 활동에 액세스하지 못하도록 해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작

탐색	구성	참조
		
코드 서명의 주요 기능 및 비즈니스 가치에 대해 알아봅니다.	코드 서명을 활성화하고 구성합니다.	속성 및 문제 해결에 대한 상세 정보 받기

사용

코드 서명을 사용하여 데이터의 진위 및 무결성을 검증하는 방법에 대해 알아봅니다.

문제 해결 및 도움 받기

- https://www.servicenow.com/community/secops/ct-p/security-operations
- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원

코드 서명 탐색

코드 서명은 민감한 애플리케이션 구성 데이터 및 스크립트를 사용하기 전에 유효성을 검사하여 보안을 개선하는 데 도움이 될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

코드 서명은 데이터에 대한 디지털 서명을 생성하며, 나중에 이를 확인하여 데이터의 진위 및 무결성을 확인합니다. 코드 서명은 의 ServiceNow 볼트구성요소로 사용이 허가된 모듈입니다.

주: 팀에서 고객 서비스 및 지원 코드 서명에 대한 액세스 권한을 부여해야 합니다.

코드 서명은 수행 중인 작업의 의도를 선언하고 자원이나 기록이 의도한 목적에 사용될 수 있는지 여부를 확인합니다. 코드 서명을 용이하게 하기 위해 (KMF)는 핵심 관리 프레임워크 디지털 서명에 디지털 인증서와 산업 표준 비대칭 암호화를 사용합니다.

플랫폼 및 인프라 측에서 내부적으로 코드 서명을 사용합니다. 코드 서명은 지정된 메타데이터 테이블에 있는 특정 테이블 또는 기록 하위 집합의 콘텐츠에 서명하는 방법을 제공합니다.



코드 서명은 신뢰할 수 있는 인스턴스와 보호된 인스턴스 사이에 보안 Circle of Trust (COT)을 사용하여 권한이 있고 안전한 인스턴스만 코드 서명 기능에 액세스할 수 있도록 합니다.

주: 코드 서명은 신뢰할 수 있는 인스턴스가 아닌 보호된 인스턴스에서 활성화됩니다.

사용 케이스

다음은 코드 서명에 대한 몇 가지 일반적인 사용 사례입니다.

- 무단 코드 변경 방지: 승인된 스크립트, 통합 및 워크플로우만 인스턴스에 배포되도록 합니다. 이렇게 하면 악의적이거나 우발적인 변경으로부터 인스턴스가 보호되어 운영 위험과 비용이 줄어듭니다.
- 보안 **MID Server** 및 **Integration Hub** 운영: 무단 또는 변조된 ECC 큐 레코드가 MID Server 또는 통합 허브. 이를 통해 ServiceNow와 외부 시스템 간의 보안 통합이 유지됩니다.
- 신뢰서클 구축: 신뢰할 수 있는 인스턴스와 보호된 인스턴스 간에 신뢰서클을 설정합니다. 이렇게 하면 다른 보안 조치가 손상되더라도 보호된 인스턴스에서 실행되는 코드의 무결성은 그대로 유지됩니다.
- 보안 플러그인 배포: 인스턴스에 설치된 플러그인의 진위 여부를 확인하여 외부 공급업체 플러그인에서 악의적이거나 변조된 코드가 유입되지 않도록 방지합니다.
- 보안 소프트웨어 개발 수명 주기**(SDLC):** 코드 서명을 SDLC에 통합하여 서명 및 테스트된 코드만 개발에서 보호된 인스턴스로 이동되도록 합니다.

다음은 Circle of Trust가 악의적인 공격을 방지할 수 있는 방법의 예입니다.

공격자가 레코드 집합에 대한 액세스 권한을 획득하고 고객의 보호된 인스턴스에서 SQL(구조적 쿼리 언어) 문을 수정한다고 가정해 보겠습니다. MID 서버는 데이터 소스 요청을 탐지하고 악의적인 SQL 변경을 실행하여 잠재적으로 상태를 손상시킵니다. 그러나 시스템 관리자는 CoT(Circle of Trust)를 구현하여 다음과 같은 시나리오의 취약성을 효과적으로 완화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 관리자는 신뢰할 수 있는 인스턴스에서 데이터 소스를 업데이트하고 통합 기록에 디지털 서명합니다.
2. 업데이트된 데이터는 신뢰할 수 있는 인스턴스에서 보호된 인스턴스로 안전하게 푸시됩니다.
3. 악의적인 액터가 악성 SQL 쿼리로 보호된 인스턴스를 업데이트하려고 시도합니다.
4. MID 서버가 악성 데이터 소스 요청을 식별합니다.
5. 유효한 디지털 서명이 없어 요청이 거부되었습니다.
6. 고객의 보호된 인스턴스로 다시 전송되어 디지털 서명 문제를 알리고 추가 조치가 필요하지 않음을 확인합니다.

코드 서명 확인 및 작업

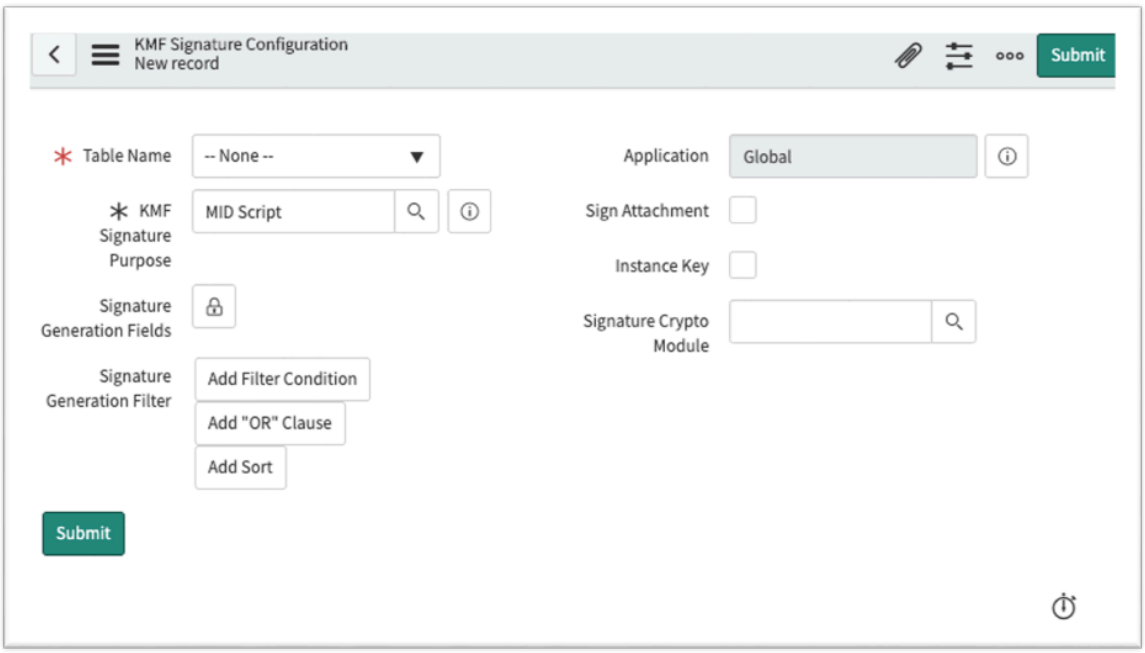
유효한 구성이 있는 모든 메타데이터 테이블은 *com.glide.code_signing*(코드 서명 메타데이터 플러그인)을 사용하여 빌드 시 서명됩니다. 테이블에 서명하도록 선택하면 보안 관리자 역할을 가진 관리 사용자가 코드 서명 암호화 작업에 액세스할 수 있습니다.

- 업데이트 세트에 서명합니다.
- 대량 서명 기록입니다.
- 대량 서명 첨부 파일.

업데이트 세트 서명

이 작업은 업데이트 세트의 서명 구성과 일치하는 기록에 서명합니다. 또한 이 작업은 모든 새 서명 기록과 확인 인증서를 업데이트 세트에 추가합니다.

업데이트 세트에 대한 **KMF** 서명 기록



대량 서명 기록

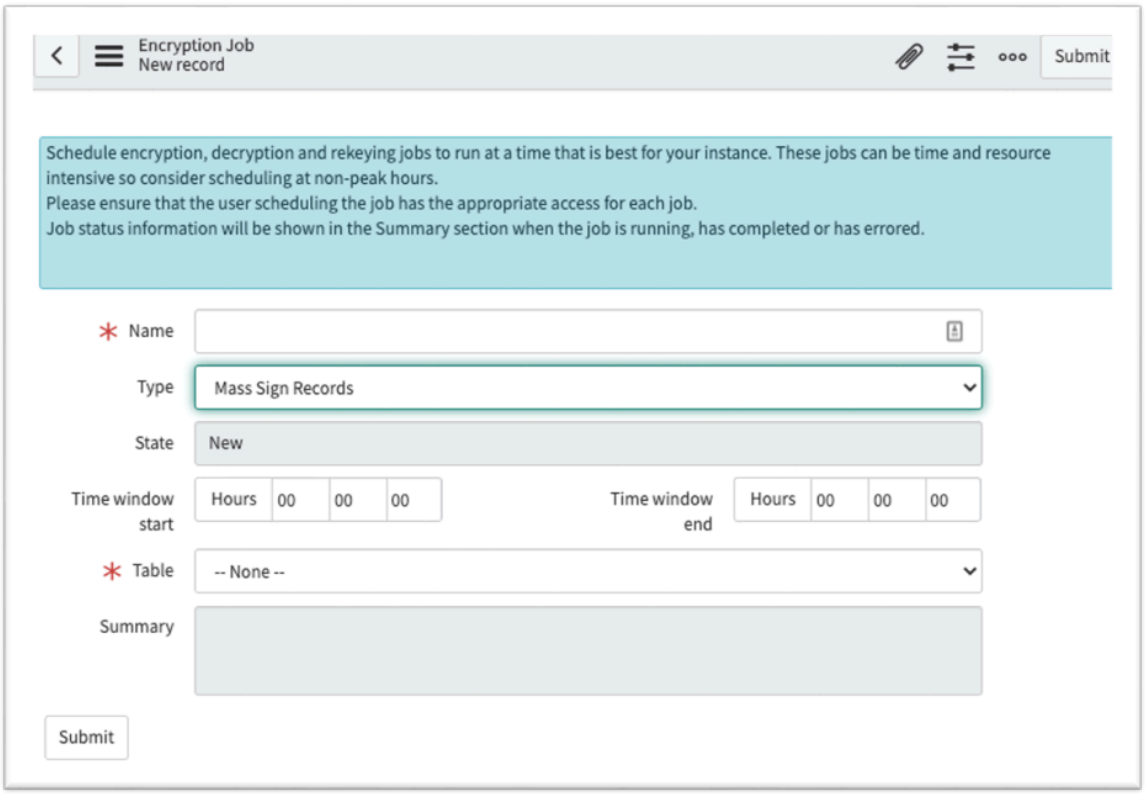
이 작업은 특정 메타데이터 테이블에 적용된 서명 구성과 일치하는 모든 기록에 서명합니다.

첨부 파일에 대량 서명

이 작업은 지정된 서명 구성과 일치하는 테이블에 첨부된 모든 첨부 파일 기록에 서명합니다.

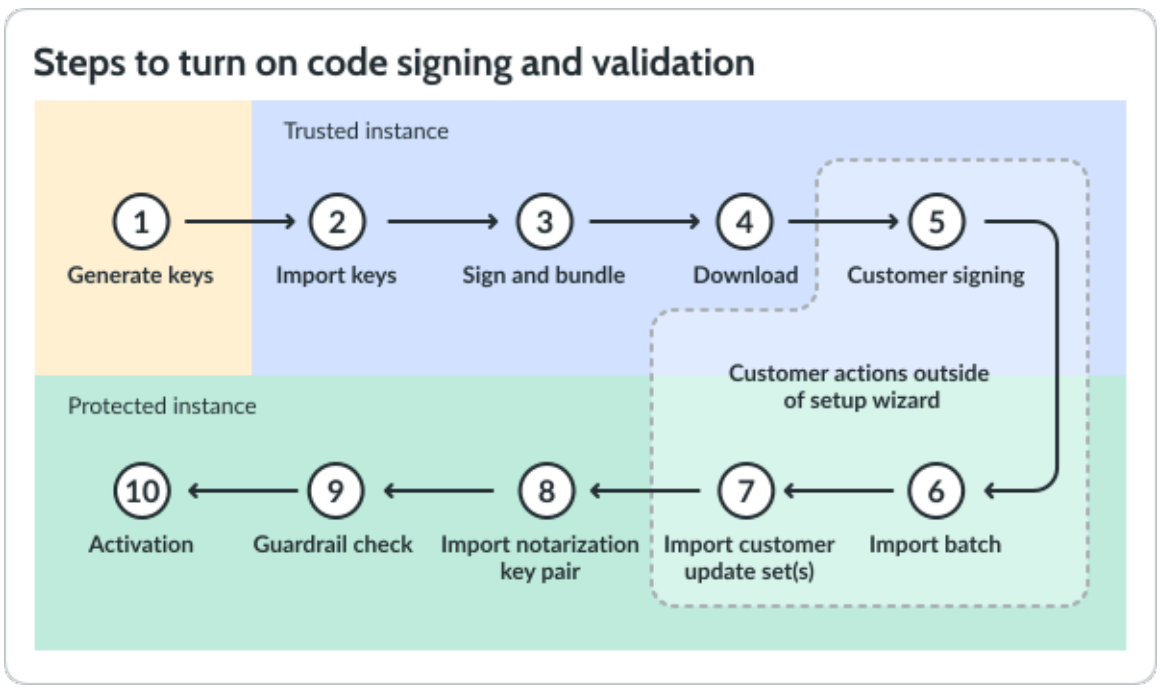
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기록을 대량 서명하기 위한 암호화 작업



코드 서명 구성

코드 서명을 활성화하고 구성하여 데이터의 진위 및 무결성을 확인합니다.



Code Signing Enterprise에는 신뢰할 수 있는 인스턴스와 보호된 인스턴스 간의 초기 신뢰 관계가 필요하며, 이를 통해 권한 부여 수준이 높은 권한이 없는 사용자가 승인되지 않은 활동에 액세스하지 못하도록 할 수 있습니다.

코드 서명 엔터프라이즈를 설정하는 Circle of Trust 구성 단계를 완료하려면 각 주제를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

코드 서명 관리자 역할 할당

코드 서명 관리자 역할을 사용자에게 할당하여 코드 서명 구성 환경에 액세스합니다.

신뢰할 수 있는 인스턴스에 코드 서명 엔터프라이즈 구성

신뢰할 수 있는 인스턴스에서 코드 서명을 켭니다.

보호된 인스턴스에 코드 서명 구성 파일 업로드

신뢰할 수 있는 인스턴스에서 생성된 구성 파일을 업로드합니다.

보호된 인스턴스에서 코드 서명 엔터프라이즈 구성

보호된 인스턴스에서 코드 서명을 켜고 구성합니다.

인증서 확인 켜기

인스턴스에서 인증서 확인을 켭니다.

코드 서명 끄기

보호된 인스턴스에서 코드 서명을 사용하지 않도록 설정합니다.

주: 이 선택적 단계는 코드 서명을 위한 초기 구성의 일부가 아닙니다

코드 서명 관리자 역할 할당

코드 서명 관리자 역할을 사용자에게 할당하여 코드 서명 구성 환경에 액세스합니다.

시작하기 전에

필요한 역할:

- 관리자
- security_admin

중요사항: 코드 서명 관리자 역할이 할당된 사용자는 전역 범위에 있어야 합니다.

프로시저

1. 신뢰할 수 있는 인스턴스를 선택하여 사용합니다.
   신뢰할 수 있는 인스턴스는 보호된 인스턴스에서 서명 확인을 활성화하기 전에 작업을 생성하고, 기록에 서명하고, 기타 필요한 작업을 수행하는 데 사용됩니다.
2. 다음으로 이동 모두 > 코드 서명 > 코드 서명 역할 관리.
3. 사용 가능한 사용자 목록에서 선택한 사용자 목록으로 사용자를 이동하여 사용자에게 코드 서명 관리자 역할을 부여합니다.
4. 저장을 선택합니다.

중요사항: 역할에 할당된 사용자가 코드 서명 작업을 수행하려면 로그아웃했다가 다시 로트인해야 합니다.

결과

선택한 사용자에게 코드 서명 관리자 역할이 있습니다. 이 역할을 가진 사용자는 코드 서명 구성 환경에 액세스하고 사용자에게 다른 코드 서명 역할을 할당할 수 있습니다.

코드 서명 역할에 대한 자세한 내용은 다음 문서를 참조하십시오 코드 서명과 함께 설치되는 역할.

신뢰할 수 있는 인스턴스에 코드 서명 엔터프라이즈 구성

신뢰할 수 있는 인스턴스에서 코드 서명을 켜고 구성합니다.

시작하기 전에

필요한 역할:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 관리자
- security_admin
- codesigning_admin

  주: codesigning_admin 역할은 에 코드 서명 관리자 역할 할당설명된 프로세스를 사용하여 할당할 수 있습니다.

- sn_kmf.cryptographic_manager

고객 서명 및 COT(Circle of Trust) 관리를 위해 하나 이상의 암호화 키 페어 및 인증서(p12 파일 확장명)가 있어야 합니다. 보안을 향상시키려면 고객 서명 및 COT 관리에 별도의 암호화 키 쌍을 사용하는 것이 좋습니다.

경고: 이 프로세스를 완료하면 한 시간 이내에 보호된 인스턴스에 설치해야 하는 구성 파일을 다운로드하게 됩니다. 이 프로세스 이후에 보호된 인스턴스에 구성 파일을 업로드할 시간이 있는지 확인합니다. 해당 프로세스에 대한 자세한 내용은 보호된 인스턴스에 코드 서명 구성 파일 업로드 문서를 참조하십시오.

프로시저

1. 신뢰할 수 있는 인스턴스에서 다음으로 이동합니다. 모두 > 코드 서명 > 코드 서명 구성 을 클릭하여 코드 서명 구성 페이지를 엽니다.
2. 인스턴스 유형 필드에서 신뢰할 수 있는 인스턴스를 선택합니다.
3. 다음 단추를 선택합니다.
4. 수행하려는 작업 선택 아래의 작업 필드에서 코드 서명 켜기를 선택합니다.
5. 고객 서명 키 페어 및 인증서 섹션의 첨부 파일 옆에 있는 +파일 추가를 선택하여 고객 서명에 사용할 암호화 키 페어(p12 파일 확장명)를 업로드합니다.

   팁: +파일 추가 옵션을 사용할 수 없는 경우 전역 범위에 있고 sn_kmf.cryptographic_manager 역할이 있는지 확인합니다.

6. 암호 필드에 업로드된 키 쌍의 암호를 입력합니다.
7. 임포트를 선택합니다.
8. 계속을 선택하여 다음 섹션으로 이동합니다.
9. **COT** 관리 키 쌍 및 인증서 섹션의 첨부 파일 옆에 있는 +파일 추가를 선택하여 고객 서명에 사용할 암호화 키 쌍(p12 파일 확장명)을 업로드합니다.
10. 암호 필드에 업로드된 키 쌍의 암호를 입력합니다.
11. 임포트를 선택합니다.
12. 계속을 선택하여 다음 섹션으로 이동합니다.
13. 신뢰할 수 있는 작업 수행 섹션에서 모든 작업이 완료될 때까지 기다립니다.

    인스턴스가 이러한 작업을 자동으로 생성하고 실행합니다. 릴리스 이전에 Vancouver 코드 서명을 사용한 경우 서명을 업데이트하기 위한 작업이 생성되고 실행됩니다.

    작업이 필요 없는 경우도 있습니다. 이 페이지에는 필요한 작업 없음 이 표시됩니다.

14. 계속을 선택하여 다음 섹션으로 이동합니다.
15. 구성 파일 익스포트 페이지에서 익스포트를 선택하여 보호된 인스턴스에서 코드 서명을 켜는 데 사용되는 구성 파일을 작성하고 다운로드합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

익스포트 프로세스는 XML 파일을 로컬 머신에 다운로드하여 이 단계의 세부 사항 보호된 인스턴스에서 코드 서명 엔터프라이즈 구성에서 사용할 수 있도록 합니다.

주: 코드 서명은 사용자 경험을 개선하기 위해 대규모 업데이트 세트에 제한을 적용합니다. 업데이트 세트의 최대 크기는 10,000개입니다.

보호된 인스턴스에 코드 서명 구성 파일 업로드

신뢰할 수 있는 인스턴스에서 생성된 구성 파일을 업로드합니다.

시작하기 전에
필요한 역할:

- 관리자
- security_admin
- codesigning_admin

주: codesigning_admin 역할은 에 코드 서명 관리자 역할 할당설명된 프로세스를 사용하여 할당할 수 있습니다.

- sn_kmf.cryptographic_manager

에 설명된 신뢰할 수 있는 인스턴스에 코드 서명 엔터프라이즈 구성단계에서 생성된 구성 파일도 필요합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 업데이트 세트 > 검색된 업데이트 세트.
2. 검색된 업데이트 세트 목록 하단에 있는 XML에서 업데이트 세트 임포트를 선택합니다.
3. 파일 선택을 선택하고 구성 파일(xml 파일 확장명)을 선택합니다.
4. 업로드를 선택합니다.
   검색된 업데이트 세트 목록에 **Codesigning** 구성 업데이트 세트가 표시됩니다.
5. **Codesigning** 구성 업데이트 세트를 선택하고 엽니다.
6. 업데이트 세트 배치 미리 보기를 선택합니다.
   미리 보기 중에 충돌이 발생하는 경우 원격 업데이트 허용 또는 알려진 **CS** 충돌 해결을 선택하여 충돌을 해결합니다.
7. 충돌을 해결한 후 업데이트 세트 배치 커밋을 선택합니다.

보호된 인스턴스에서 코드 서명 엔터프라이즈 구성

보호된 인스턴스에서 코드 서명을 켜고 구성합니다.

시작하기 전에
필요한 역할:

- 관리자
- security_admin
- codesigning_admin

주: codesigning_admin 역할은 에 코드 서명 관리자 역할 할당설명된 프로세스를 사용하여 할당할 수 있습니다.

- sn_kmf.cryptographic_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. PPI에서 모두 > 코드 서명 > 코드 서명 구성 을 클릭하여 코드 서명 구성 페이지를 엽니다.
2. 인스턴스 유형 필드에서 보호된 인스턴스를 선택합니다.
3. 다음 단추를 선택합니다.
4. 코드 서명 구성 업데이트 세트를 가져와서 커밋했는지 확인하십시오 확인란을 선택합니다.
5. 다음 단추를 선택합니다.
6. 인증서 설치가 완료될 때까지 기다립니다.
   구성 파일의 항목이 설치 중임을 나타내는 파란색 경고 메시지가 표시됩니다. 설치가 완료되면 경고가 몇 초 후에 사라집니다.
7. 런타임/공증 키 페어 및 인증서 섹션의 첨부 파일 옆에 있는 +파일 추가를 선택하여 런타임/공증 목적으로 사용할 암호화 키 페어(p12 파일 확장명)를 업로드합니다.
   신뢰할 수 있는 인스턴스의 키 쌍을 재사용하거나 이 용도를 위해 특별히 새 키 쌍을 업로드할 수 있습니다.

   팁: +파일 추가 옵션을 사용할 수 없는 경우 전역 범위에 있고 sn_kmf.cryptographic_manager 역할이 있는지 확인합니다.

8. 암호 필드에 업로드된 키 쌍의 암호를 입력합니다.
9. 임포트를 선택합니다.
10. 계속을 선택하여 다음 섹션으로 이동합니다.
11. 인스턴스가 가드레일 검사를 수행하는 동안 기다립니다.
    이 검사는 인스턴스에서 잘못된 서명을 검사하며, 완료하는 데 시간이 걸릴 수 있습니다. 스캔이 완료될 때까지 페이지를 종료하거나 새로 고치지 마십시오.
12. 검사 결과 잘못된 서명이 발견되면 보고서 다운로드를 선택합니다.

    보고서 다운로드를 선택하면 잘못된 서명을 조사하고 수정하는 데 사용할 수 있는 보고서(`scan_report.txt`)가 다운로드됩니다.

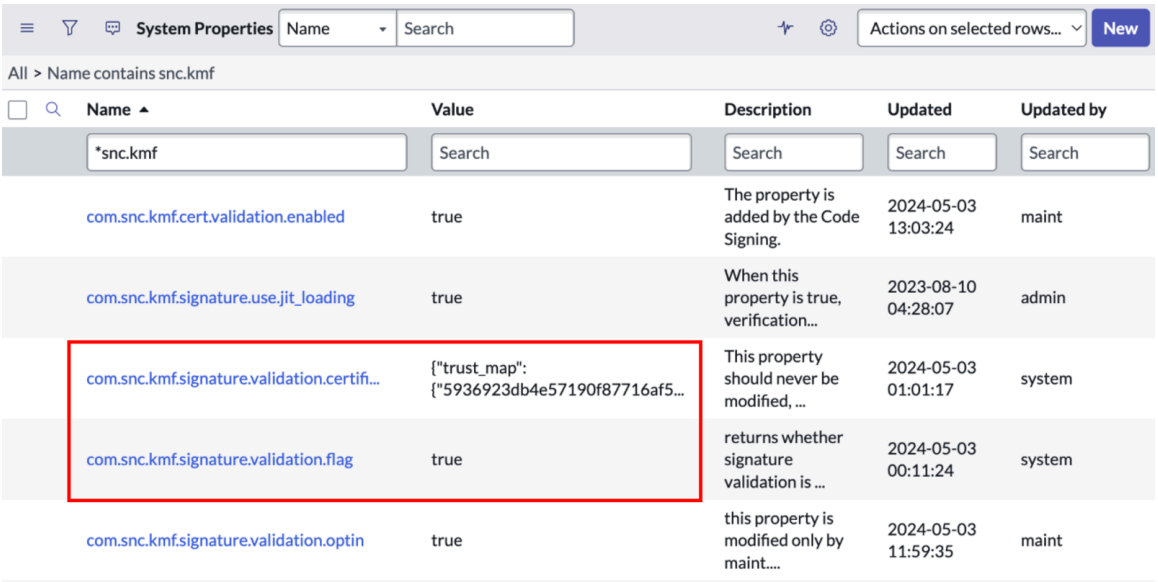
    오류를 해결한 후 페이지를 새로 고쳐 검사를 다시 실행합니다.

13. 오류가 없으면 설정 완료를 선택합니다.
14. 구성 작업이 완료될 때까지 기다립니다.
    인스턴스가 하나 이상의 작업을 실행하여 구성 프로세스를 완료합니다. 작업이 완료될 때까지 페이지를 종료하거나 새로 고치지 마십시오. 완료되면 코드 서명 구성이 성공적으로 완료 되었다는 메시지가 표시됩니다.

결과

이제 프로덕션 인스턴스에 서명 확인이 적용됩니다. 시스템 속성을 확인하여 성공적으로 완료되었는지 확인할 수 있습니다. 시스템 속성 [sys_property] 테이블에서 **com.snc.kmf.signature.validation.flag** 속성을 찾아 **true** 값인지 확인합니다. **com.snc.kmf.signature.validation.certificate_trust** 속성에 빈 값이 없는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



인증서 확인 켜기

인증서 기반 확인으로 인스턴스를 보호합니다.

시작하기 전에

필요한 역할:

- codesigning_admin
- security_admin
- sn_kmf.cryptographic_manager

프로시저

1. 신뢰할 수 있는 인스턴스에서 다음으로 이동합니다. 모두 > 코드 서명 > 코드 서명 구성 을 클릭하여 코드 서명 구성 페이지를 엽니다.
2. 인스턴스 유형 필드에서 신뢰할 수 있는 인스턴스를 선택합니다.
3. 다음 단추를 선택합니다.
4. 수행하려는 작업 선택 아래의 작업 필드에서 인증서 유효성 검사 켜기를 선택합니다.
5. 다음 단추를 선택합니다.
6. 고객 서명 키 페어 및 인증서 섹션의 첨부 파일 옆에 있는 +파일 추가를 선택하여 고객 서명에 사용할 암호화 키 페어(p12 파일 확장명)를 업로드합니다.

   팁: +파일 추가 옵션을 사용할 수 없는 경우 전역 범위에 있고 sn_kmf.cryptographic_manager 역할이 있는지 확인합니다.

7. 암호 필드에 업로드된 키 쌍의 암호를 입력합니다.
8. 임포트를 선택합니다.
9. 계속을 선택하여 다음 섹션으로 이동합니다.
10. **COT** 관리 키 쌍 및 인증서 섹션의 첨부 파일 옆에 있는 +파일 추가를 선택하여 고객 서명에 사용할 암호화 키 쌍(p12 파일 확장명)을 업로드합니다.
11. 암호 필드에 업로드된 키 쌍의 암호를 입력합니다.
12. 임포트를 선택합니다.
13. 계속을 선택하여 다음 섹션으로 이동합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

14. 신뢰할 수 있는 인스턴스 작업 수행 섹션에서 모든 작업이 완료될 때까지 기다립니다.

    인스턴스가 이러한 작업을 자동으로 생성하고 실행합니다. 릴리스 이전에 Vancouver 코드 서명을 사용한 경우 서명을 업데이트하기 위한 작업이 생성되고 실행됩니다.

    작업이 필요 없는 경우도 있습니다. 이 페이지에는 필요한 작업 없음 이 표시됩니다.

15. 계속을 선택하여 다음 섹션으로 이동합니다.
16. 구성 파일 익스포트 페이지에서 익스포트를 선택하여 보호된 인스턴스에서 코드 서명을 켜는 데 사용되는 구성 파일을 작성하고 다운로드합니다.
    익스포트 프로세스는 XML 파일을 로컬 머신에 다운로드하여 다음에 보호된 인스턴스에서 코드 서명 엔터프라이즈 구성설명된 단계에서 사용할 수 있도록 합니다.
17. 보호된 인스턴스에서 다음으로 이동합니다. 모두 > 시스템 업데이트 세트 > 검색된 업데이트 세트.
18. 검색된 업데이트 세트 목록 하단에 있는 XML에서 업데이트 세트 임포트를 선택합니다.
19. 파일 선택을 선택하고 구성 파일(xml 파일 확장명)을 선택합니다.
20. 업로드를 선택합니다.
21. 의 코드 서명 구성 페이지로 돌아갑니다. 모두 > 코드 서명 > 코드 서명 구성.
22. 마법사를 사용하여 구성을 완료하고 인증서 유효성 확인 활성화를 완료하기 위한 옵션을 선택합니다.

코드 서명 끄기

보호된 인스턴스에서 코드 서명을 사용하지 않도록 설정합니다.

시작하기 전에
필요한 역할: admin, codesigning_admin

프로시저

1. 신뢰할 수 있는 인스턴스에서 다음으로 이동합니다. 모두 > 코드 서명 > 코드 서명 구성 을 클릭하여 코드 서명 구성 페이지를 엽니다.
2. 인스턴스 유형 필드에서 신뢰할 수 있는 인스턴스를 선택합니다.
3. 다음 단추를 선택합니다.
4. 수행하려는 작업 선택 아래의 작업 필드에서 코드 서명 해제를 선택합니다.
5. 구성 파일 익스포트 패널에서 익스포트를 선택하여 업데이트 세트를 다운로드합니다.
   익스포트 프로세스는 다음 단계에서 사용할 XML 파일을 로컬 머신에 다운로드합니다.
6. 완료를 선택합니다.
7. 보호된 인스턴스에 로그인합니다.
8. 의 보호된 인스턴스에 코드 서명 구성 파일 업로드단계를 사용하여 구성 파일을 업로드합니다.
9. 다음으로 이동 모두 > 코드 서명 > 코드 서명 구성 을 클릭하여 코드 서명 구성 페이지를 엽니다.
10. 인스턴스 유형 필드에서 보호된 인스턴스를 선택합니다.
11. 다음 단추를 선택합니다.
12. 코드 서명 구성 업데이트 세트를 가져와서 커밋했는지 확인하십시오 확인란을 선택합니다.
13. 다음 단추를 선택합니다.
14. 인증서 설치가 완료될 때까지 기다립니다.
    완료되면 코드 서명 구성이 성공적으로 완료 되었다는 메시지가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
시스템 속성을 확인하여 성공적으로 완료되었는지 확인할 수 있습니다. 시스템 속성 [sys_property] 테이블에서 **com.snc.kmf.signature.validation.flag** 속성을 찾아 값이 **false**인지 확인합니다.

코드 서명에 필요한 키 쌍 및 인증서 로드

코드 서명을 사용하여 지정된 신뢰할 수 있는 인스턴스에서 관계를 설정합니다. 이 첫 번째 단계에서는 신뢰할 수 있는 환경에 두 개의 암호화 키를 로드하여 프로덕션 인스턴스 업데이트에 대한 신뢰할 수 있는 소스를 설정합니다.

시작하기 전에
필요한 역할: security_admin 및 sn_kmf.cryptographic_manager

이 태스크 정보
관계 설정의 첫 단계는 코드 서명을 사용하여 지정된 신뢰할 수 있는 인스턴스에서 신뢰 기반을 설정하는 것입니다. 이 작업을 수행하려면 다음이 필요합니다.

- 코드 서명 암호화 모듈에 로드할 두 개의 4096비트 RSA 공개/개인 키 쌍이 있어야 합니다.
  - cm_code_signing 암호화 모듈용 한 쌍
  - cm_code_attest 암호화 모듈용 한 쌍

  이러한 키에 대한 자세한 내용은 다음 문서를 참조하십시오 코드 서명 키 페어 및 인증서 생성.

  중요사항: 이러한 키 쌍은 공용 인증 기관에서 서명하거나 조직 내부 인증 기관에서 서명해야 합니다. 인증서는 자체 서명할 수 없습니다.

- 리프 및 중간 인증서를 포함하는 공개 키 암호화 표준 #12(.p12) 파일입니다.

프로시저

1. 키 저장소에서 키를 임포트합니다.
   a. 다음으로 이동 모두 > 주요 운영 > 암호화 모듈 > 모두.
   b. `cm_code_signing`라는 암호화 모듈을 찾아 엽니다.
   c. 암호화 사양 목록에서 암호화 사양의 이름을 선택하여 엽니다.
   d. 키 저장소에서 키 가져오기 화면에서 키 가져오기를 선택합니다.
2. 첫 번째 단계를 반복하여 `cm_code_attest`라는 암호화 모듈을 가져옵니다.
3. **Enter Keystore** Password(키 저장소 암호 입력) 필드에 RSA 인증서를 생성할 때 생성한 챌린지 암호를 입력합니다.

   주: 생성한 챌린지 암호를 여기서는 키 저장소 암호라고 합니다. 프로세스의 다른 부분에서는 가져오기 암호 또는 내보내기 암호라고 할 수 있습니다. 모든 경우에 이 암호는 이전 단계에서 만든 것과 동일한 챌린지 암호입니다.

4. **Import Keystore**/Certificate(키 스토어/인증서 가져오기) 옆에 있는 Browse(찾아보기) 버튼을 선택합니다.
5. 배포 인증서가 포함된 공개 키 암호화 표준 #12(.p12) 파일을 선택합니다(이 문서의 맨 위에 있는 시작하기 전에 섹션에 언급됨).
6. 확인을 선택합니다.

   중요사항: 자체 내부 인증 기관을 사용하는 경우 5-6단계의 프로세스를 사용하여 내부 인증 기관의 중간 인증서를 업로드해야 합니다.

   키 및 인증서를 성공적으로 가져오면 확인 메시지가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

X.509 인증서[sys_certificate] 테이블에서 인스턴스에 키와 인증서가 있는지 확인할 수 있습니다. 이러한 기록에는 신뢰할 수 있는 스토어 인증서 유형이 있습니다.

암호화 모듈 [sys_kmf_crypto_module] 테이블에서 키를 확인할 수 있습니다.

다음에 수행할 작업
인증서를 프로덕션으로 익스포트합니다. 자세한 내용은 Circle of Trust 인증서 준비 문서를 참조하십시오.

Circle of Trust 인증서 준비

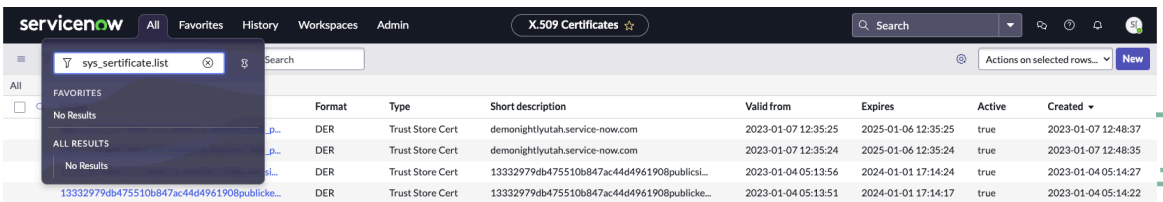
신뢰할 수 있는 환경에서 업데이트 세트를 생성하여 신뢰할 수 있는 인증서를 프로덕션 환경으로 익스포트합니다.

시작하기 전에
필요한 역할: admin, security_admin

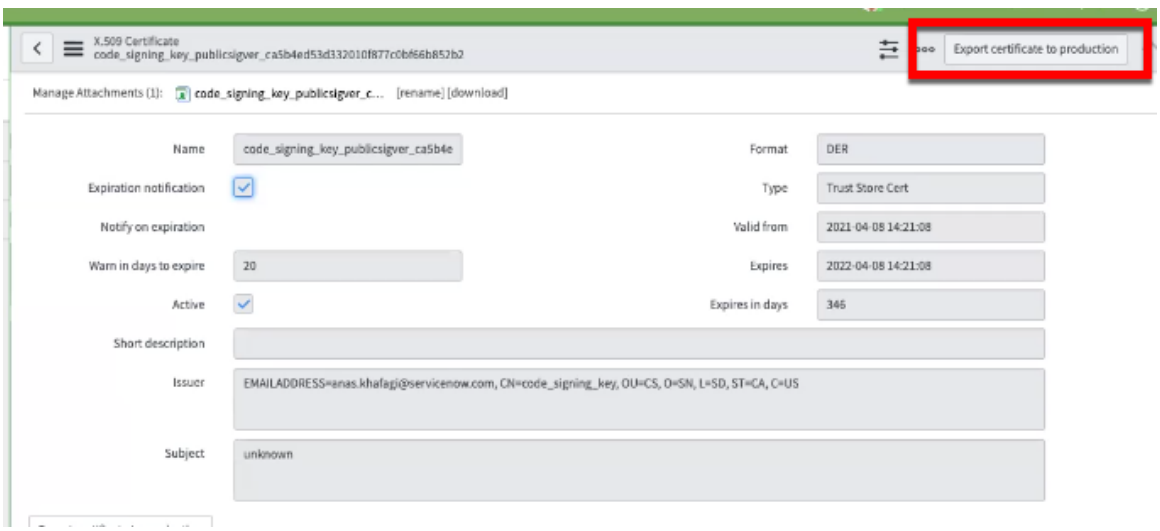
시작하기 전에
신뢰할 수 있는 인스턴스

프로시저

1. 신뢰할 수 있는 환경에서 다음으로 이동합니다. **sys_certificate.list**.



2. 신뢰할 수 있는 저장소 인증서 유형으로 생성된 가장 최근에 작성된 X.509 인증서를 엽니다. 가장 최근 기록을 찾으려면 생성됨 필드를 목록에 추가해야 할 수 있습니다. 개인 목록을 참조하십시오.
3. 프로덕션으로 인증서 내보내기를 선택합니다.



인증서와 함께 서명이 생성됩니다.

4. 다음으로 이동 시스템 업데이트 세트 > 로컬 업데이트 세트.
5. 코드 서명 업데이트를 찾아서 엽니다.

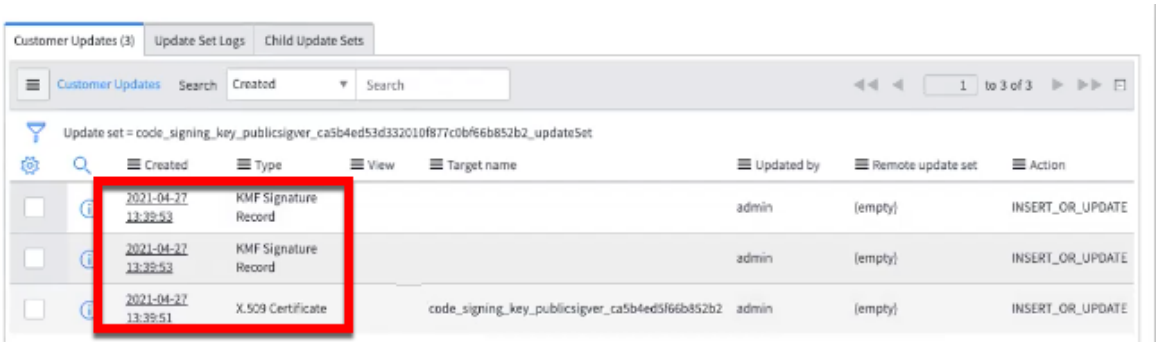
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 업데이트는 `### code_signing_key_publicsigver`로 시작됩니다.

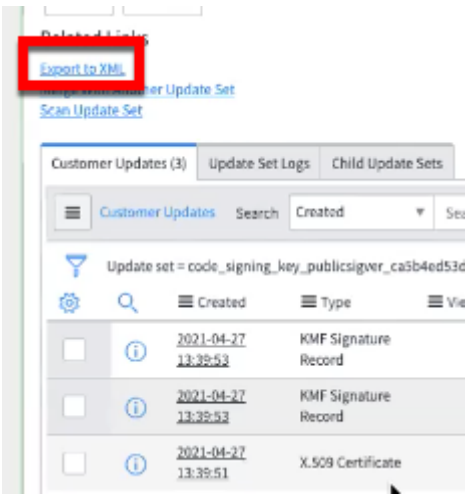
이전 단계에서 새 코드 서명 업데이트 세트 기록이 생성되었습니다. 이 기록을 찾으려면 작성자 필드를 사용하여 목록을 정렬하고 이름 필드에서 있는 기록을 찾습니다.

6. 관련 서명 레코드와 X.509 인증서를 봅니다.

   업데이트 세트에는 테이블의 서명 항목 및 인증서와 함께 서명 기록의 첨부 파일이 포함됩니다.



7. XML로 익스포트 관련 링크를 선택합니다.



8. 프로덕션에서 업데이트 세트를 검색합니다.
   자세한 내용은 업데이트 세트 검색 문서를 참조하십시오.

> **중요사항:** 두 번째 키 쌍에 대해 이 단계를 반복합니다. cm_code_attest 및 cm_code_signing 암호화 모듈 모두에 대한 키가 있음을 기억하십시오.

Circle of Trust에 대한 인증서 임포트 및 설치

프로덕션에서 업데이트 세트를 검색하여 두 인스턴스 간에 신뢰 관계를 설정합니다. 신뢰할 수 있는 인스턴스에서 신뢰를 나타내기 위해 만든 인증서는 보호된 인스턴스에 수락되어야 합니다.

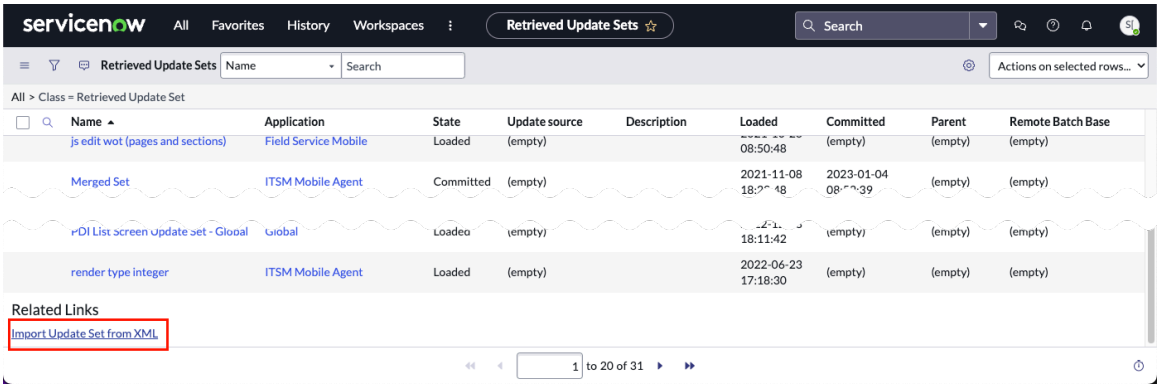
시작하기 전에

필요한 역할: admin, security_admin

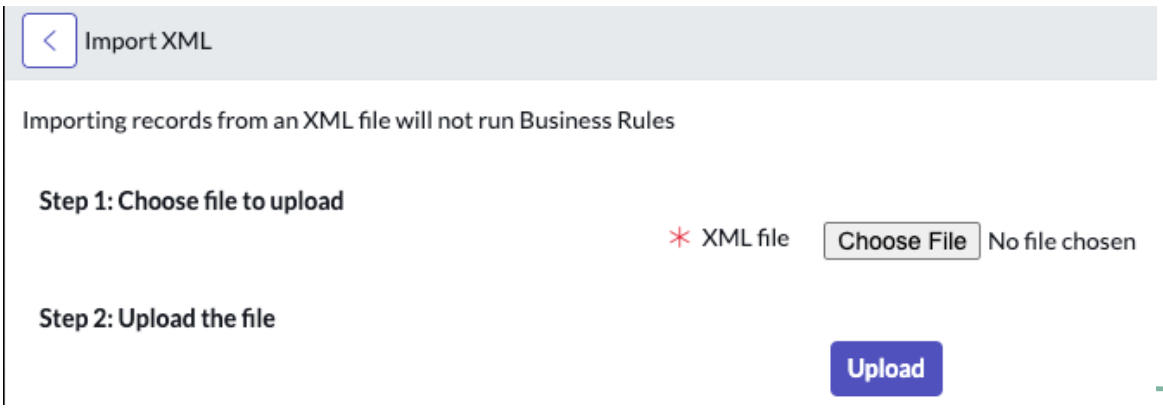
프로시저

1. 보호된 인스턴스에서 다음으로 이동합니다. 시스템 업데이트 세트 > 검색된 업데이트 세트.
2. 화면 왼쪽 아래 모서리에 있는 XML에서 업데이트 세트 임포트 버튼을 선택합니다.

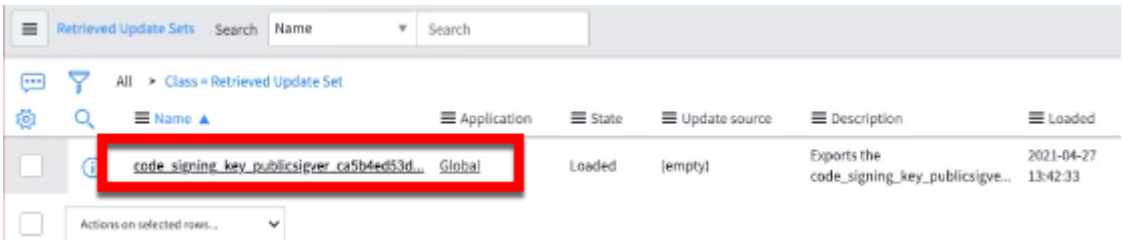
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 파일 선택을 선택하고 에서 익스포트Circle of Trust 인증서 준비한 XML 파일을 찾아 선택합니다.



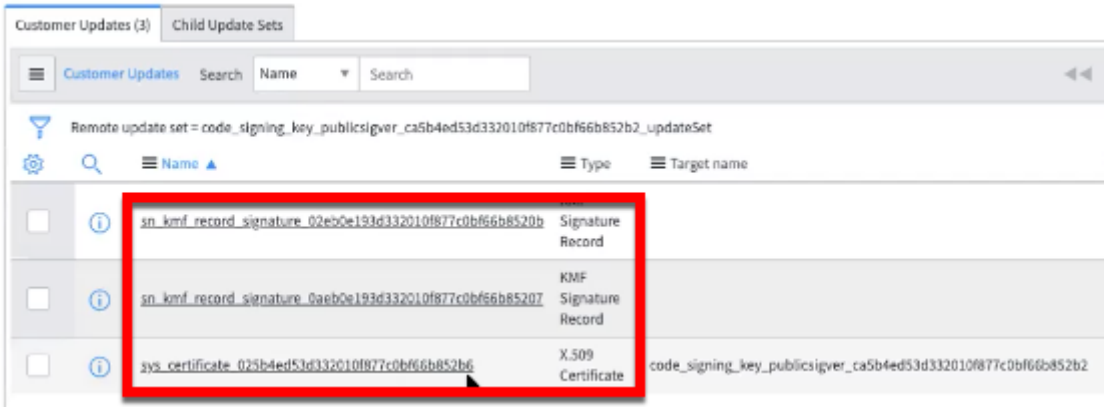
4. 업로드를 선택합니다.
코드 서명 업데이트 세트가 검색된 업데이트 세트 테이블에 추가됩니다.



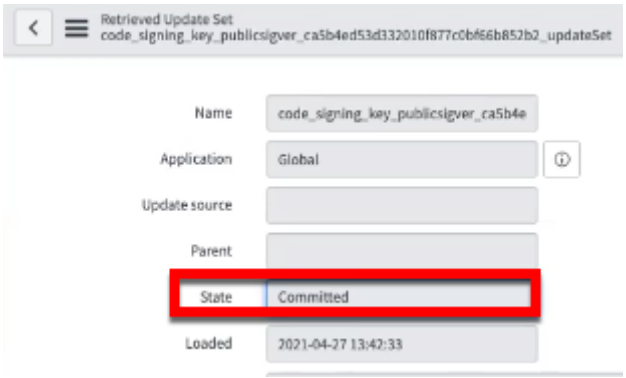
주: 업데이트 세트가 표시되지 않으면 로드됨 상태의 기록으로 목록을 필터링하고 로드됨 필드를 기준으로 목록을 정렬합니다.

5. 업데이트 세트 기록을 열어 고객 업데이트 테이블에 다음 세 개의 기록이 포함되어 있는지 확인합니다.
   - 두 개의 KMF 서명 기록
   - X.509 인증서

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



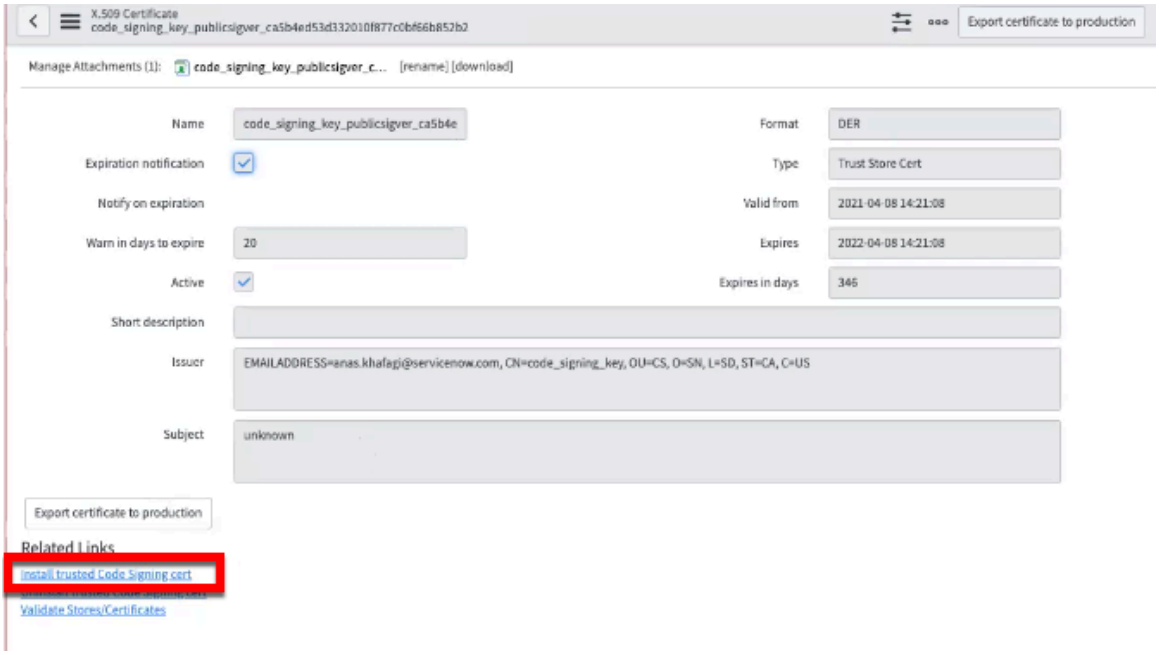
6. 업데이트 세트 미리 보기를 선택합니다.
7. 업데이트 세트 커밋을 선택합니다.



검색된 업데이트 세트 상태가 커밋됨으로 업데이트됩니다.

8. 탐색기에서 `sn_kmf_record_signature.list` 를 입력하여 **KMF** 서명 기록 목록을 엽니다.
9. 두 개의 KMF 서명 기록을 찾습니다.
이러한 기록은 **KMF** 서명 목적 필드 값이 `####`인 가장 최근에 생성된 기록입니다. 생성됨 필드를 목록에 추가하거나 현재 날짜에 생성된 기록을 필터링해야 할 수 있습니다.
10. 탐색기에서 `sys_certificate.list` 를 입력하고 간단한 설명 값이 *`code_signing_key`* 이고 유형 값이 `Trust Store Cert`인 기록을 엽니다.
11. 신뢰할 수 있는 코드 서명 인증서 설치를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



인증서 유형이 *### # ## CodeSigning ###*로 업데이트됩니다.

중요사항: 두 번째 인증서에 대해 이 단계를 반복합니다. cm_code_attest 및 cm_code_signing 암호화 모듈 모두에 대한 인증서가 있음을 기억하십시오.

결과
트러스트 관계는 신뢰할 수 있는 인스턴스와 보호된 인스턴스 간에 설정됩니다. 코드 서명을 활성화할 준비가 되었습니다. 단계를 완료하려면 다음을 참조하십시오 코드 서명 켜기 .

코드 서명 켜기

신뢰할 수 있는 비프로덕션 인스턴스에서 코드 서명을 켜서 프로덕션 인스턴스와 연결된 신뢰할 수 있는 인스턴스를 식별합니다.

시작하기 전에
필요한 역할: security_admin, sn_kmf.crypto_manager 또는 sn_kmf.admin

코드 서명을 활성화하기 전에 팀에 문의하여 고객 서비스 및 지원 코드 서명 엔터프라이즈 [com.glide.code_signing_enterprise] 플러그인을 켜야 합니다. 코드 서명의 사용 사례에 대한 자세한 내용은 문서를 코드 서명 탐색참조하십시오.

이 태스크 정보
서명된 업데이트 세트가 있는 코드 서명 작업은 코드 서명 기능을 켜거나 끄는 데 사용됩니다. 이 기능을 위한 다른 방법은 없습니다. 이 프로세스에는 다음이 포함됩니다.

- 신뢰할 수 있는 인스턴스에 코드 서명 작업을 두 개 생성하는데, 하나는 코드 서명을 설정하는 작업이고 다른 하나는 코드 서명을 끄는 작업입니다.
  - 예약된 작업을 켜면 서명된 코드에 대한 MID 서버 확인 프로세스가 시작됩니다.
  - 예약된 작업 끄기 는 서명된 코드에 대한 MID Server 확인을 중지합니다.

  기본적으로 코드 서명은 모든 MID 서버에 적용됩니다. 그러나 코드 서명을 MID 서버의 특정 하위 집합으로 제한해야 하는 경우 ECC 방화벽을 사용하여 이를 수행할 수 있습니다.

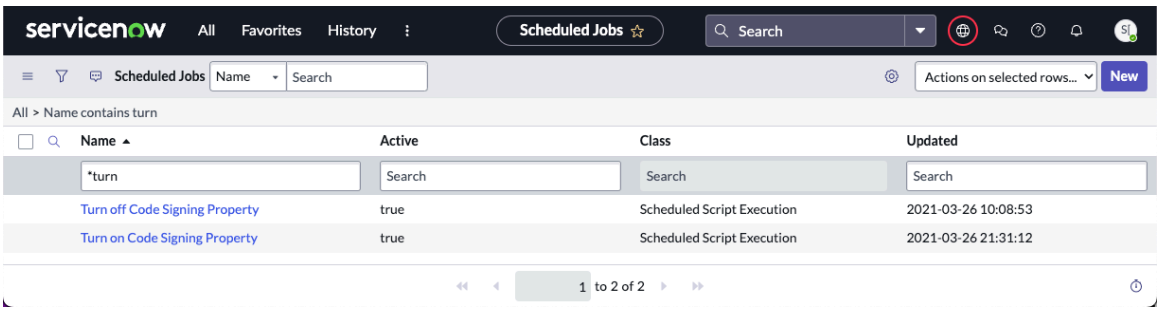
  주: 코드 서명을 끄면 시스템 속성이 **false**로 표시되지만 코드 서명의 신뢰할 수 있는 친구 목록은 계속 사용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

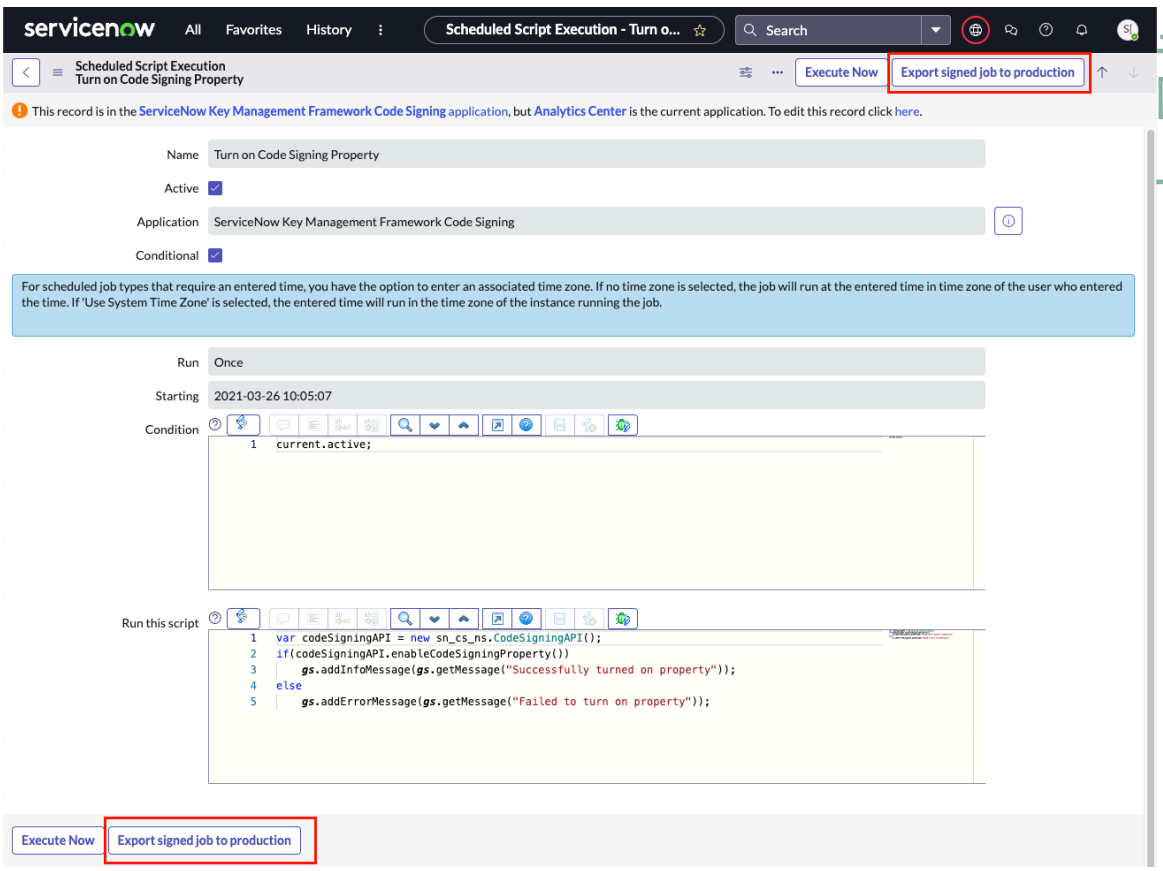
- 코드 서명 속성 켜기 작업을 업데이트 세트에 넣습니다.
- 작업을 프로덕션으로 가져옵니다.
- 서명이 신뢰할 수 있는 인스턴스에서 시작된 것으로 확인된 경우 프로덕션 환경에서 코드 서명 속성 켜기 작업을 사용합니다.

프로시저

1. 신뢰할 수 있는 인스턴스에서 다음으로 이동합니다. 모두 > 시스템 정의 > 예약된 작업.
2. 이름 필드에서 "*Turn"을 검색합니다.
3. 코드 서명 속성 켜기를 선택합니다.



예약된 스크립트 실행 양식이 로드됩니다. 이 양식에는 코드 서명 속성을 활성화하는 정보가 포함되어 있습니다. 작업은 코드 서명 프로세스를 통해 작업과 확인된 서명을 포함하는 업데이트 세트를 만듭니다.

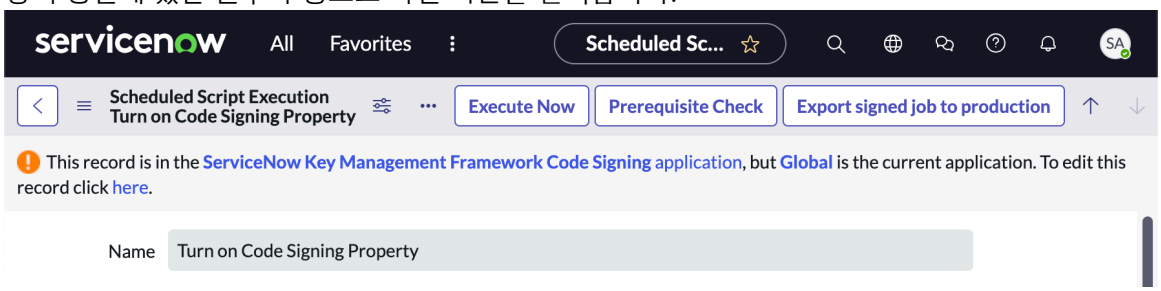


4. 스크립트를 즉시 실행하려면 인증서에 서명하고, 업데이트 세트를 만들고, 서명된 작업을 프로덕션으로 익스포트를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지정된 일정에 따라 실행되도록 스크립트를 구성할 수도 있습니다.

5. 다음으로 이동 시스템 업데이트 세트 > 로컬 업데이트 세트.
6. 각 코드 서명 속성 업데이트 세트를 열고 XML로 익스포트를 선택합니다.
7. 프로덕션 인스턴스에 로그인합니다.
8. 다음으로 이동 시스템 업데이트 세트 > 검색된 업데이트 세트.
9. XML에서 업데이트 세트 임포트 버튼을 선택하고 코드 서명 속성 업데이트 세트를 선택합니다.
10. 파일 선택을 선택하고 업데이트 세트를 업로드하고 커밋합니다.
11. 다음으로 이동하여 예약된 작업 목록으로 돌아갑니다. 모두 > 시스템 정의 > 예약된 작업.
12. 코드 서명 속성 켜기 작업 기록을 엽니다.
13. 양식 상단에 있는 필수 구성요소 확인 버튼을 선택합니다.



14. 필수 구성요소 확인이 완료된 후 지금 실행 버튼을 선택합니다.
코드 서명 속성 켜기 예약된 작업은 서명된 코드의 MID 서버 확인 프로세스를 시작합니다.
15. 탐색기에서 `sn_kmf_record_signature.list` 를 입력하여 **KMF** 서명 기록 목록을 열고 **KMF** 서명 목적 이 `####`인 기록을 필터링합니다.
신뢰 관계로 인해 작업이 이동되었으며 작업이 사용되면 서명 검증 프로세스가 실행됩니다. 작업, 서명 및 인증서가 모두 의 일부인 Circle of Trust경우 를 사용하여 Circle of Trust 코드 서명을 켤 수 있습니다.
16. 탐색기에서 `sys_properties.list` 를 입력하여 시스템 속성 목록을 엽니다.
17. *`com_snc_kmf_signature.validation.flag`* 검색하여 값이 **true**로 설정되어 있는지 확인합니다.
18. 새 속성이 *`com_snc_kmf_signature.validation.certificate`* 테이블에 나열되어 있는지 확인합니다.

시스템 속성

com.snc.kmf.signature.validation.certifi...	{"trust_map": {"025b4ed53d332010f877c0bf6...	string	ServiceNow Key Management Framework
com.snc.kmf.signature.validation.flag	true	true | false	Global

프로덕션에서 Circle of Trust 작업을 사용하여 신뢰 관계를 확인합니다. 프로덕션에서 코드 서명을 시도하는 직접 작업을 실행할 수 없습니다. 구성 옵션에 대한 자세한 내용은 을 참조하십시오 코드 서명 구성 .

코드 서명 키 페어 및 인증서 생성

서명된 인증서에 키 쌍 2개를 생성하여 보호된 인스턴스와 신뢰할 수 있는 인스턴스 간에 신뢰를 설정합니다.

인스턴스 간에 신뢰를 구축하려면 각 `cm_code_attest` 및 `cm_code_signing` 암호화 모듈에 대한 키 페어와 인증서를 생성해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 쌍 및 인증서 생성은 OpenSSL 도구와 같은 로컬 장치에 설치된 암호화 도구를 사용하여 수행됩니다. 이 도구에 대한 자세한 내용은 다음 문서를 참조하십시오 https://www.openssl.org . 조직에서 LibreSSL 또는 GnuTLS와 같은 다른 암호화 도구를 사용하는 경우 해당 제품의 설명서에서 유사한 단계를 참조하십시오.

키 페어 사양

생성하는 키 쌍은 이러한 요구 사항을 충족해야 합니다.

유형	RSA
키 길이	4096
서명 알고리즘	RSASSA_PKCS1_V1_5_SHA_512

인증서 사양

인증서는 공용 인증 기관에서 서명해야 합니다.

ECC 방화벽에서 사용자 지정 규칙 지정

수신 메시지를 선택적으로 허용하거나 거부하고 코드 서명 구성을 재정의하는 사용자 지정 규칙을 지정하여 외부 통신 채널(ECC) 방화벽 MID 서버 을 구성합니다.

보안 관리자는 ECC 방화벽 태그를 사용하여 코드 서명 구성을 재정의하고 에서 특정 작업을 MID 서버허용하거나 거부할 수 있습니다. 이러한 사용자 지정 규칙은 `agent/boot-config.yaml` 에 있는 YAML 파일에 지정해야 합니다.

이러한 태그는 프로토콜에 따라 다릅니다. 상위 태그에 지정된 구성을 하위 태그에 적용할 수 있습니다. 예를 들어 `HTTP` 프로토콜이 허용되는 경우 `REST` 및 `SOAP` 프로토콜도 허용됩니다. 이 테이블에서는 사용 가능한 상위 및 하위 태그를 간략하게 설명합니다.

상위 태그	하위 태그
DNS	
HTTP	• REST • SOAP
DIRECTORY_SERVICES	LDAP
SNMP	
SSH	• SCP • SFTP
시스템 로그	
윈도우	• CIM • POWERSHELL • WMI • 윈름

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상위 태그	하위 태그
자바스크립트	
그루비	
VCS	GIT
데이터베이스	JDBC
DATA_SOURCES	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • 디스커버리 • EVENT_MANAGEMENT • HEALTH_LOG_ANALYTICS • SERVICE_MAPPING
오케스트레이션	

사용자 지정 규칙을 구성하려면 다음을 수행합니다.

1. 에서 MID 서버`boot-config-sample.yaml` 파일을 식별합니다.
2. YAML 파일의 이름을 `boot-config.yaml` 로 바꾸고 파일을 `agent/boot-config.yaml` 위치로 이동합니다.
3. YAML 파일에서 사용자 지정 규칙을 지정하고 변경 내용을 저장합니다. YAML 파일의 예:

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. MID 서버를 다시 시작합니다.

신뢰 루트 구성 변경

ROT(신뢰 루트)를 사용하도록 변경하여 빌드 인증서(기본값)에 의존하는 ServiceNow 대신 자체 인증서를 신뢰하고 사용합니다. ServiceNow 스크립트 포함, 비즈니스 규칙 등과 같은 구성 요소는 빌드 시간 키(확인 인증서는 빌드 인증서임ServiceNow)를 ServiceNow 사용하여 빌드 시 서명됩니다.

신뢰 루트 변경

이러한 레코드 서명에 대한 신뢰 루트를 변경하려면 신뢰 루트 변경 프로세스를 따라야 합니다.

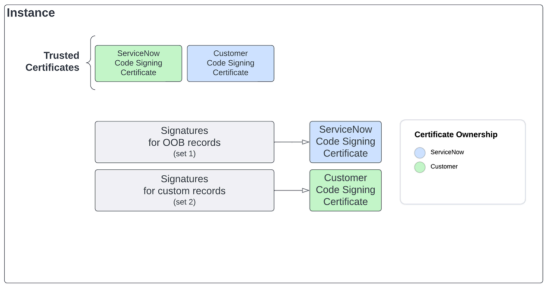
- 제공된 인증서를 사용하여 제공된 모든 구성요소에 대해 새 서명 세트를 생성하고 마이그레이션합니다.
- 예약된 작업을 사용하여 신뢰 루트 속성을 사용하지 않도록 설정합니다.

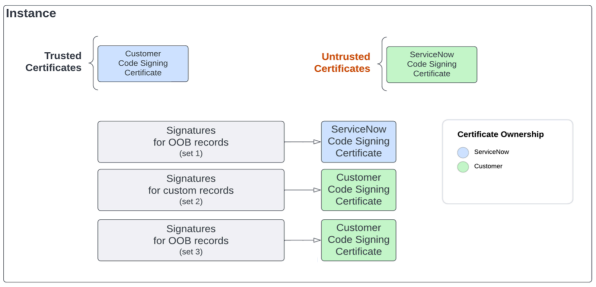
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

및 ServiceNow 신뢰 루트 비활성화에서 이러한 단계에 고객 인증서를 사용하도록 서명 마이그레이션 대해 자세히 알아보십시오.

서명 생성 및 검증 프로세스에 미치는 영향

기본적으로 코드 서명 빌드 인증서는 서명 검증 프로세스 중에 신뢰할 수 있습니다. 이렇게 변경한 후에는 인스턴스가 자체 코드 서명 인증서에서만 서명을 수락합니다.





ROT 속성이 false(기본값)로 설정됨	**ROT** 속성이 true로 설정됨
• 확인할 때 빌드 인증서가 있는 서명을 신뢰할 수 있습니다. • 서명할 때 키를 제공하지 않으면 인스턴스 서명 키가 백업 키로 사용됩니다. • 서명 REST 엔드포인트 *api/sn_kmf/signature/certificates*는 인스턴스에 있는 다른 인증서와 함께 코드 서명 빌드 인증서를 반환합니다 ServiceNow .	• 확인할 때 빌드 인증서가 있는 서명은 신뢰할 수 없습니다. • 서명할 때 키를 제공하지 않으면 서명이 수행되지 않습니다. • 서명 REST 엔드포인트 *api/sn_kmf/signature/certificates*는 빌드 인증서(San Diego, Vancouver PKI, W PKI)를 제외합니다 ServiceNow .

MID 서버에 미치는 영향

ROT 속성이 false로 설정된 경우

ROT 속성을 기본값(false)으로 유지해도 MID 서버에는 영향을 주지 않습니다.

코드 서명이 활성화되고 ROT 속성이 true로 설정된 경우

- *isTrusted()* API는 빌드 인증서가 있는 서명에 대해 `false`를 반환합니다.
- *isTrusted()* API는 인증서와 함께 서명에 대해 `true`를 반환합니다.
- 인증서에 대한 REST API 호출은 빌드 인증서를 제외합니다.
- 로그에 `## ## ##` 메시지와 같은 MID 서버 문제가 표시될 수 있습니다.

고객 인증서를 사용하도록 서명 마이그레이션

서명 작업을 실행하여 서명을 고객 ROT(신뢰 루트)로 마이그레이션합니다.

시작하기 전에
필요한 역할: admin, security_admin, sn_kmf.cryptographic_manager

보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화해야 합니다.
com.snc.kmf.signature.validation.flag 시스템 속성이 `true`로 설정되어 있는지 확인하여 확인할 수 있습니다.

이 절차는 인스턴스에서 고객 ROT(신뢰 루트)를 변경하는 일련의 절차 중 일부입니다. 이 프로세스에 대한 개요는 다음 문서를 참조하십시오 신뢰 루트 구성 변경.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 보호된 인스턴스에 로그인합니다.
2. 다음으로 이동 모두 > 시스템 정의 > 예약된 작업.
3. **ROT -** 기록 업데이트 세트를 찾아서 열어 고객 인증서 예약 작업을 사용하여 서명을 마이그레이션합니다.
4. 양식 하단에서 지금 실행을 선택합니다.
5. 다음으로 이동 모두 > 시스템 보안 > 보안 작업 > 새로 작성.
6. 프롬프트에서 서명 작업을 선택합니다.
7. 서명 작업 양식에서 필요에 따라 필드를 채웁니다.

필드	값
이름	작업에 고유한 이름을 만듭니다.
유형	업데이트 세트 서명을 선택합니다.
테이블	이전 단계에서 생성된 업데이트 세트를 선택합니다. 업데이트 세트의 이름은 `change_root_of_trust_updateSet`로 시작합니다.

8. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택하여 이 기록을 저장합니다.
9. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 익스포트 > XML(이 기록) 을 클릭하여 이 기록을 XML 파일로 익스포트합니다.
10. 신뢰할 수 있는 인스턴스에 로그인합니다.
11. 다음으로 이동 모두 > 시스템 보안 > 보안 작업 > 모두.
12. 목록 헤더를 마우스 오른쪽 버튼으로 클릭하고 **XML** 임포트를 선택합니다.
13. **XML** 임포트 양식에서 파일 선택을 선택하고 이전 단계에서 다운로드한 XML 파일을 선택합니다.
14. 업로드를 선택합니다.
15. 목록에서 임포트한 보안 작업을 엽니다.
16. 코드 서명 작업을 프로덕션으로 익스포트를 선택합니다.
    이 작업은 작업에 서명하고 보호된 인스턴스로 임포트할 수 있는 새 업데이트 세트에 배치합니다.

> **중요사항:** 작업에 서명한 후 10분 이내에 다음 단계를 수행해야 합니다. 이 기간을 초과하면 다음 단계를 사용하여 작업에 다시 서명하여 서명된 다른 업데이트 세트를 만들 수 있습니다.

17. 다음으로 이동 모두 > 시스템 업데이트 세트 > 로컬 업데이트 세트.
18. 이전 단계에서 생성된 업데이트 세트를 찾습니다.
    이름은 `SIGN_UPDATE_SET_updateSet`로 시작합니다.
19. 업데이트 세트를 XML 파일로 익스포트하려면 **XML** 익스포트를 선택합니다.
20. 보호된 인스턴스에 로그인합니다.
21. 다음으로 이동 모두 > 시스템 업데이트 세트 > 검색된 업데이트 세트.
22. 목록 하단에서 XML에서 업데이트 세트 임포트를 선택합니다.
23. **XML** 임포트 양식에서 파일 선택을 선택하고 이전 단계에서 다운로드한 XML 파일을 선택합니다.
24. 업로드를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

25. 다음으로 이동 모두 > 시스템 업데이트 세트 > 검색된 업데이트 세트으로 시작하고 `SIGN_UPDATE_SET_updateSet`로 시작하는 업데이트 세트를 엽니다.
26. 업데이트 세트 미리 보기를 선택합니다.
27. 미리 보기가 완료되면 업데이트 세트 커밋을 선택합니다.
28. 다음으로 이동 모두 > 시스템 보안 > 보안 작업 > 모두.
29. 임포트한 보안 작업을 엽니다.
30. 시작을 선택하여 보안 작업을 실행합니다.

    보안 작업이 완료되면 작업 상태에 대한 정보가 요약 필드에 나타납니다.

    작업이 완료 상태이면 업데이트 세트 기록의 모든 서명은 고객이 제공한 인증서를 검증 인증서로 사용해야 합니다. KMF 서명 기록 [sn_kmf_record_signature] 테이블에서 이를 확인할 수 있습니다.

다음에 수행할 작업

신뢰 루트 구성 프로세스를 계속하려면 문서를 참조하십시오 ServiceNow 신뢰 루트 비활성화.

ServiceNow 신뢰 루트 비활성화

신뢰할 수 있는 인스턴스에서 예약된 작업을 실행하여 신뢰 루트를 비활성화합니다.

시작하기 전에

필요한 역할: admin, security_admin, sn_kmf.cryptographic_manager

보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화해야 합니다. **com.snc.kmf.signature.validation.flag** 시스템 속성이 `true`로 설정되어 있는지 확인하여 확인할 수 있습니다.

이 절차는 인스턴스에서 고객 ROT(신뢰 루트)로 변경하는 일련의 절차 중 일부입니다. 이 프로세스에 대한 개요는 다음 문서를 참조하십시오 신뢰 루트 구성 변경.

프로시저

1. 신뢰할 수 있는 인스턴스에 로그인하십시오.
2. 다음으로 이동 모두 > 시스템 정의 > 예약된 작업.
3. **ServiceNow** 신뢰 루트 사용 안 함 예약된 작업을 엽니다.
4. 서명된 작업을 프로덕션으로 익스포트를 선택합니다.
5. 다음으로 이동 모두 > 시스템 업데이트 세트 > 로컬 업데이트 세트.
6. **ServiceNow** 신뢰 루트 비활성화 업데이트 세트를 찾아서 엽니다.
7. 업데이트 세트를 XML 파일로 익스포트하려면 **XML** 익스포트를 선택합니다.
8. 보호된 인스턴스에 로그인합니다.
9. 다음으로 이동 모두 > 시스템 업데이트 세트 > 검색된 업데이트 세트.
10. 목록 하단에서 XML에서 업데이트 세트 임포트를 선택합니다.
11. **XML** 임포트 양식에서 파일 선택을 선택하고 이전 단계에서 다운로드한 XML 파일을 선택합니다.
12. 업로드를 선택합니다.
13. 다음으로 이동 모두 > 시스템 업데이트 세트 > 검색된 업데이트 세트을 클릭하고 **ServiceNow** 신뢰 루트 사용 안 함 업데이트 세트를 엽니다.
14. 업데이트 세트 미리 보기를 선택합니다.
15. 미리 보기가 완료되면 업데이트 세트 커밋을 선택합니다.
16. 다음으로 이동 모두 > 시스템 정의 > 예약된 작업.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

17. 업데이트 세트에서 임포트한 예약된 작업을 엽니다.
18. 지금 실행 단추를 선택하여 작업을 실행합니다.

결과
예약된 작업을 실행하면 ROT 속성이 true로 설정됩니다. 인스턴스가 고객 신뢰 루트를 사용하도록 구성되었습니다.

코드 서명 사용

데이터의 진위 여부와 무결성을 확인하는 데 도움이 되도록 기록, 메시지 및 첨부 파일에 서명하는 방법에 대해 알아봅니다.

보호된 인스턴스에서 JDBC 데이터 소스 레코드에 서명

업데이트 세트를 사용하여 보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화하여 JDBC 데이터 소스에 서명하고 유효성을 확인합니다.

프로덕션 인스턴스에서 REST 및 SOAP 메시지에 서명

업데이트 세트를 사용하여 보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화함으로써 REST 및 SOAP 메시지에 서명하고 유효성을 확인합니다.

보호된 인스턴스의 플로우, 하위 플로우 및 작업에 서명

업데이트 세트를 사용하면 보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화하여 플로우, 하위 플로우 및 작업에 서명하고 유효성을 검사할 수 있습니다.

특정 기록 또는 첨부 파일에 서명

테이블의 모든 기록이나 첨부 파일이 아닌 특정 기록이나 첨부 파일에 서명하는 보안 작업을 생성합니다.

독립 실행형 서명 도구

독립 실행형 서명 도구를 사용하면 고유한 개인 키를 사용하여 애플리케이션에서 지원되는 기록에 ServiceNow 서명할 수 있습니다.

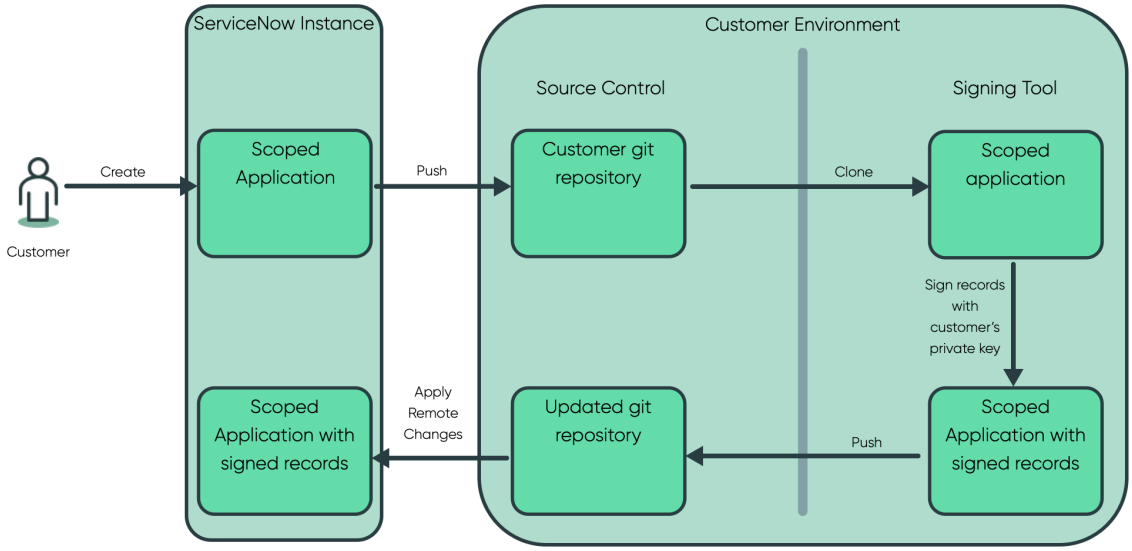
독립 실행형 서명 도구

독립 실행형 서명 도구를 사용하면 고유한 개인 키를 사용하여 애플리케이션에서 지원되는 기록에 ServiceNow 서명할 수 있습니다.

서명 도구를 사용하여 앱에서 레코드에 ServiceNow 서명합니다. 이 도구는 사용자 고유의 개인 키를 사용하여 로컬 환경의 레코드에 대한 서명을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

서명 도구 워크플로우



1. 비즈니스 규칙 또는 스크립트 포함처럼 서명할 기록이 있는 기존 ServiceNow 애플리케이션을 만들거나 선택합니다.
2. 사용자 환경에 있는 Git 리포지토리에 애플리케이션을 푸시합니다.

   주: 소스 통제 통합을 사용하여 Git 리포지토리와 인스턴스 간에 애플리케이션을 동기화할 수 있습니다. 이 통합 구성 및 사용에 대한 자세한 내용은 문서를 참조하십시오 소스 통제 통합 .
3. 로컬 환경에서 애플리케이션을 복제합니다.
4. 서명 도구(로컬 환경에서도 가능)를 사용하여 개인 키를 사용하여 복제된 ServiceNow 애플리케이션에서 지원되는 기록에 서명합니다. 서명 도구는 서명 레코드와 X.509 인증서 [sys_certificate] 레코드를 만듭니다. 서명 도구 사용에 대한 자세한 내용은 을 참조하십시오 서명 도구 사용.
5. 업데이트된 애플리케이션을 Git 리포지토리에 푸시합니다.
6. 해당 인스턴스에 원격 변경 내용을 적용하여 업데이트된 애플리케이션을 임포트합니다.

서명 도구 사용

서명 도구를 사용하여 애플리케이션에서 지원되는 기록에 ServiceNow 서명하는 방법을 알아봅니다.

시작하기 전에
필요한 역할: 관리자

이러한 단계를 수행하려면 다음이 있어야 합니다.

- ServiceNow 서명할 기록이 있는 애플리케이션입니다.
- 레코드 서명을 위한 개인 키입니다.
- 실행 권한이 있는 로컬 환경의 *signRecords.sh* 스크립트입니다.

중요사항: *signRecords.sh* 스크립트는 signing-tool jar 파일의 일부로 포함되며, 이 파일은 다음에서 요청해야 합니다. ServiceNow 고객 지원 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 로컬 환경에서 *signRecords.sh* 스크립트가 포함된 디렉터리로 이동합니다.
2. 다음 명령 형식을 사용하여 기록에 서명합니다.

```
./signRecords.sh -d [Path to the root directory of the ServiceNow
 Application to Sign] -f [Path to the Keystore file]
```

예:

```
./signRecords.sh -d /users/abc/ServiceNow-App-1
 -f /users/abc/codesigning.p12
```

3. 메시지가 표시되면 키 저장소의 암호를 입력합니다.
암호가 없으면 Enter 키를 누릅니다.
4. 출력을 검토하여 서명이 성공했는지 확인합니다.

```
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!
```

앞의 출력 예제에서 서명 도구는 제공된 키 스토어 파일을 사용하여 기록에 서명했습니다. 또한 다음을 확인할 수 있습니다.

- 스크립트가 지원되는 기록 `65e811327702111057416efe7c5a994f` 찾고 서명했습니다.
- ServiceNow-App-1 디렉터리에서 `sys_certificate.xml` 와 `sn_kmf_record_signature.xml`이라는 두 개의 기록이 생성되었습니다.

5. 에서 스튜디오원격 변경 사항을 적용하여 업데이트된 애플리케이션을 다시 인스턴스로 임포트합니다.
자세한 내용은 원격 변경 내용 적용 문서를 참조하십시오.

서명 도구 인수

서명 도구에 사용할 수 있는 인수에 대해 알아봅니다.

명령줄 인수

인수	필수	설명
-d	예	서명할 프로젝트의 루트 디렉터리입니다. 프로젝트 디렉터리 (임의 32자리 영숫자), sn_source_control.properties 파일 및 <project_name>.iml 파일을 포함해야 합니다.
-f	예	키 저장소의 파일 경로입니다.
-a	아니요	키 스토어 내의 특정 항목에 접근하는 데 사용되는 별칭입니다.
-c	아니요	레코드 서명을 하나의 파일로 연결합니다.
-k	아니요	키 스토어 내에 저장된 키에 액세스하기 위한 암호입니다. 인수 대신 메시지가 표시될 때 이 암호를 입력할 수도 있습니다.
-o	아니요	기존 sys_cert 파일 대신 새 인증서로 서명합니다.
-p	아니요	암호가 있는 경우 키 스토어에 액세스하기 위한 암호입니다. 인수 대신 메시지가 표시될 때 이 암호를 입력할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

명령줄 인수

인수	필수	설명
-w	아니요	기존 서명 기록 파일을 모두 지웁니다.
-h	아니요	이 도움말 메시지를 표시하고 종료합니다.

보호된 인스턴스에서 JDBC 데이터 소스 레코드에 서명

업데이트 세트를 사용하여 보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화하여 JDBC 데이터 소스에 서명하고 유효성을 확인합니다.

- 보호된 인스턴스와 신뢰할 수 있는 인스턴스 사이에 설정합니다 Circle of Trust .
- 필요한 역할: security_admin

주:

- MID 서버 는 파일 데이터 원본을 처리하지 않으므로 이러한 데이터 원본은 코드 서명되지 않습니다.
- LDAP 데이터 원본은 코드 서명할 수 없습니다.

JDBC 유형의 기존 데이터 소스에 서명

업데이트 세트를 사용하여 대량 서명 작업을 보호된 인스턴스로 가져올 수 있습니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 신뢰할 수 있는 인스턴스에서 데이터 소스에 서명하도록 KMF 서명 작업을 구성합니다.

   a. 다음으로 이동 시스템 보안 > 보안 작업 > 모두.

   b. 새로 만들기를 클릭합니다.

   c. 양식에서 다음 값을 입력합니다.

필드	설명
이름	기록을 식별하는 이름입니다.
유형	암호화 작업의 유형입니다. 대량 서명 기록을 선택합니다.
테이블	기록에 서명해야 하는 테이블입니다. 데이터 소스를 선택합니다.

   d. 코드 서명 작업을 프로덕션으로 익스포트를 클릭합니다.
   업데이트 세트가 서명되었다는 확인 메시지가 표시됩니다.

   e. 생성된 업데이트 세트를 XML 파일로 익스포트합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 보호된 인스턴스에서 업데이트 세트를 임포트하고 커밋하여 신뢰할 수 있는 인스턴스에서 대량 서명된 작업을 검색합니다.

   a. 다음으로 이동 시스템 보안 > 보안 작업 > 모두.

   b. 신뢰할 수 있는 인스턴스에서 익스포트한 업데이트 세트를 엽니다.

   c. 시작을 클릭합니다.
   기록이 서명되었다는 확인 메시지가 표시됩니다.

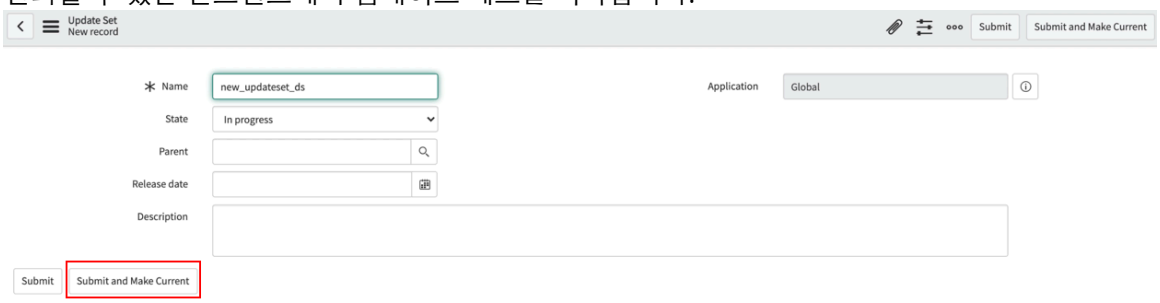
JDBC 유형의 새 데이터 소스 서명

업데이트 세트를 사용하여 서명된 업데이트 세트를 보호된 인스턴스로 가져옵니다.

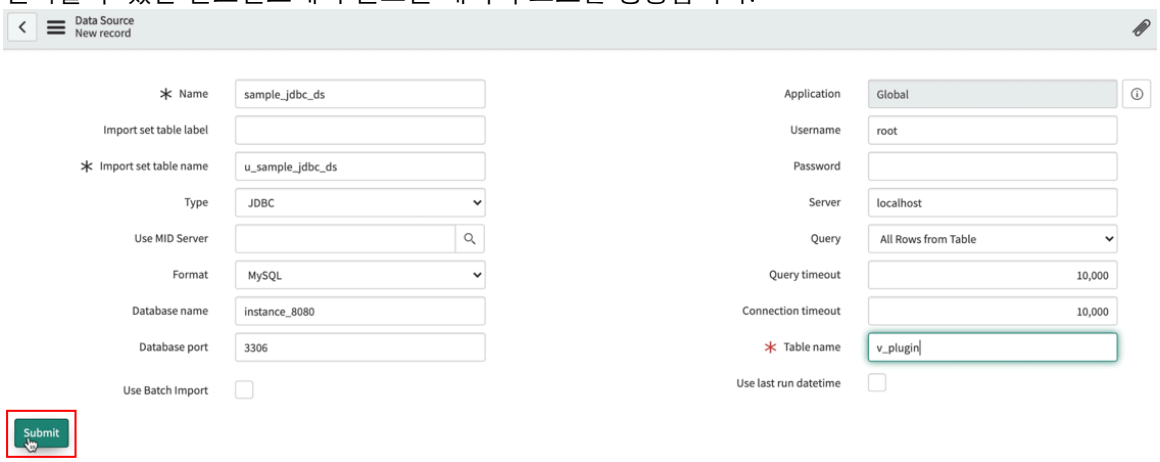
시작하기 전에
필요한 역할: sn_kmf.cryptographic_manager

프로시저

1. 신뢰할 수 있는 인스턴스에서 업데이트 세트를 시작합니다.



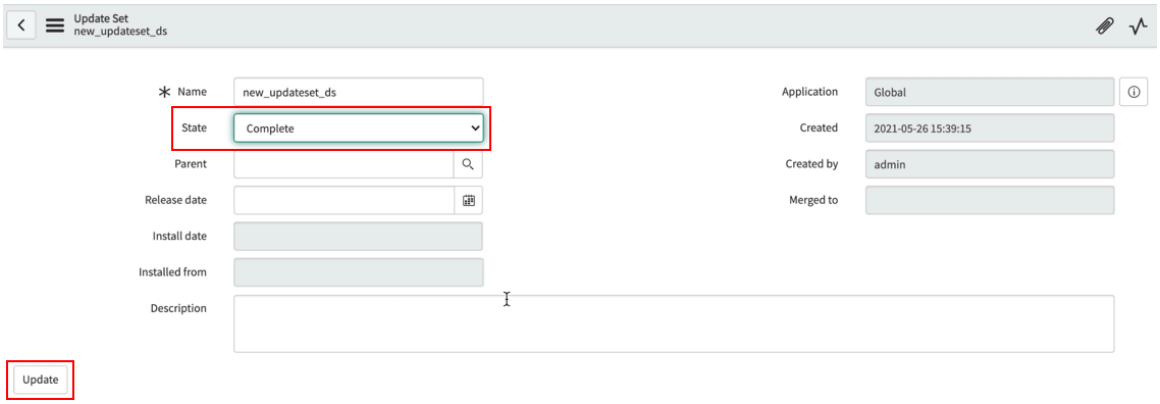
2. 신뢰할 수 있는 인스턴스에서 필요한 데이터 소스를 생성합니다.



   데이터 소스가 업데이트 세트에 추가됩니다.

3. 신뢰할 수 있는 인스턴스에서 업데이트 세트의 상태를 완료 로 변경하고 업데이트를 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



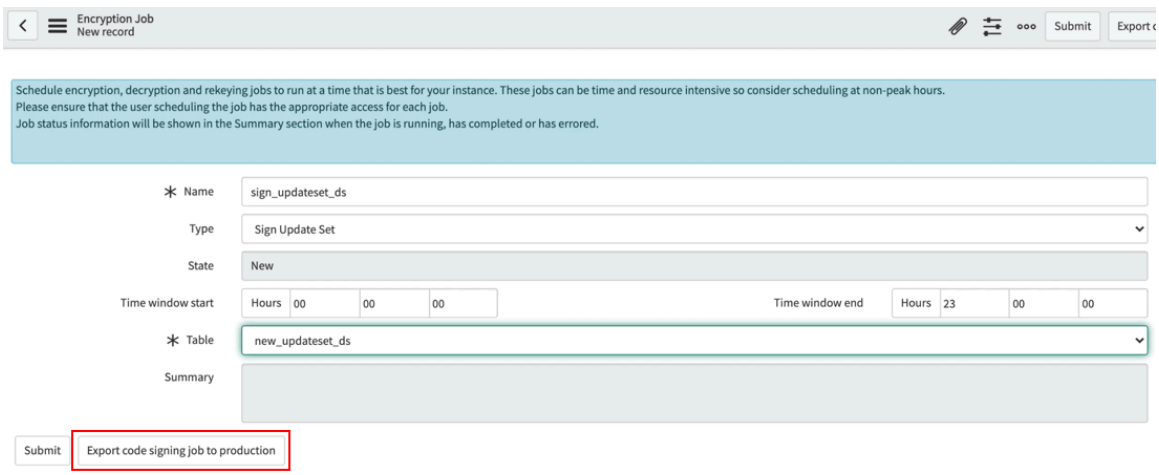
4. 신뢰할 수 있는 인스턴스에서 암호화 작업을 생성하여 업데이트 세트에 서명합니다.

a. 다음으로 이동 시스템 보안 > 보안 작업 > 모두.

b. 새로 만들기를 클릭합니다.

c. 양식에서 다음 값을 입력합니다.

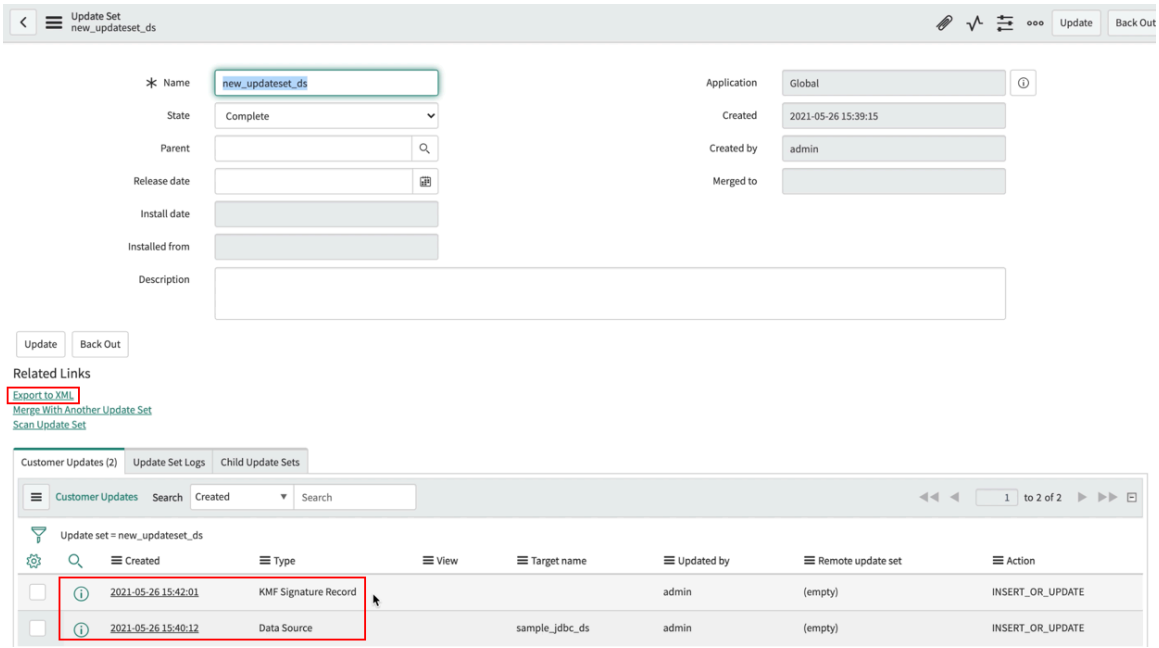
필드	설명
이름	기록을 식별하는 이름입니다.
유형	암호화 작업의 유형입니다. 업데이트 세트 서명을 선택합니다.
테이블	기록에 서명해야 하는 업데이트 세트입니다.



d. 제출을 클릭합니다.

e. 시작을 클릭하여 업데이트 세트에 서명합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



- 기록이 서명되었다는 요약이 업데이트됩니다.
- 업데이트 세트가 업데이트되고 서명이 포함됩니다.

5. 신뢰할 수 있는 인스턴스에서 서명된 업데이트 세트 기록을 열고 XML로 익스포트합니다.

6. 보호된 인스턴스에서 서명된 업데이트 세트를 임포트합니다.

a. 다음으로 이동 시스템 업데이트 세트 > 검색된 업데이트 세트.

b. XML에서 업데이트 세트 임포트 관련 링크를 클릭하여 신뢰할 수 있는 인스턴스에서 익스포트한 업데이트 세트를 임포트합니다.
자세한 내용은 빠른 시작 업데이트 세트 임포트 및 커밋을 참조하십시오.
업데이트 세트가 성공적으로 커밋되었습니다.

프로덕션 인스턴스에서 **REST** 및 **SOAP** 메시지에 서명

업데이트 세트를 사용하여 보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화함으로써 REST 및 SOAP 메시지에 서명하고 유효성을 확인합니다.

시작하기 전에

- 보호된 인스턴스와 신뢰할 수 있는 인스턴스 사이에 설정합니다 Circle of Trust .
- 필요한 역할: security_admin

기존 **REST** 및 **SOAP** 메시지에 서명

보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화하여 기존 REST 및 SOAP 메시지에 서명하고 유효성을 확인합니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 신뢰할 수 있는 인스턴스에서 UI 작업에 서명하도록 KMF 서명 작업을 구성합니다.

   a. KMF 서명 구성으로 이동합니다.

   b. 양식에서 다음 값을 입력합니다.

   KMF 서명 구성 양식

필드	설명
테이블 이름	Glide 테이블 이름입니다. 예를 들어 **UI** 작업 **[sys_ui_action]**을 선택합니다.
KMF 서명용	기록에 서명하는 목적입니다. **ECC** 큐를 선택합니다.
서명 작성 필드	서명할 데이터 소스의 필드입니다. 이러한 필드 중 하나 이상의 값이 변경되면 이전에 생성된 서명이 무효화됩니다. 이름 및 스크립트를 선택합니다.
서명 작성 필터	기록에 서명하기 위해 충족해야 하는 필터 기준입니다.
서명 첨부 파일	Glide 기록의 첨부 파일에 서명하는 옵션입니다.
인스턴스 키	인스턴스 키를 사용하는 옵션입니다.

   c. 양식 헤더를 마우스 오른쪽 단추로 클릭하고 저장을 클릭합니다.

2. 신뢰할 수 있는 인스턴스에서 필요한 기록에 서명합니다.

   a. 다음으로 이동 시스템 보안 > 보안 작업 > 모두.

   b. 새로 만들기를 클릭합니다.

   c. 양식에서 다음 값을 입력합니다.

필드	설명
이름	기록을 식별하는 이름입니다.
유형	암호화 작업의 유형입니다. 대량 서명 기록을 선택합니다.
테이블	기록에 서명해야 하는 테이블입니다. **UI** 작업을 선택합니다.

   d. 코드 서명 작업을 프로덕션으로 익스포트를 클릭합니다.
   로컬에 서명된 업데이트 세트 2개가 생성됩니다.
   - UI 작업 구성에 대한 하나의 업데이트 세트입니다.
   - 코드 서명 작업을 익스포트하기 위한 암호화 작업의 또 다른 업데이트 세트입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 신뢰할 수 있는 인스턴스에서 로컬 업데이트 세트를 XML 파일로 익스포트합니다.
   a. 다음으로 이동 시스템 업데이트 세트 > 로컬 업데이트 세트.
   b. 기록 대량 서명을 위해 생성한 업데이트 세트를 엽니다.
   c. XML로 익스포트 관련 링크를 클릭하고 XML 파일을 저장합니다.
4. 보호된 인스턴스에서 업데이트 세트를 임포트합니다.
   a. 다음으로 이동 시스템 업데이트 세트 > 검색된 업데이트 세트.
   b. XML에서 업데이트 세트 임포트 관련 링크를 클릭하여 신뢰할 수 있는 인스턴스에서 익스포트한 업데이트 세트를 임포트합니다.
   자세한 내용은 빠른 시작 업데이트 세트 임포트 및 커밋을 참조하십시오.
   업데이트 세트가 성공적으로 커밋되었습니다.
5. 보호된 인스턴스에서 시작을 선택하여 신뢰할 수 있는 인스턴스에서 이전에 만든 암호화 작업을 실행합니다.
   기록에 서명되었다는 확인 메시지가 표시됩니다.

새 **REST** 및 **SOAP** 메시지에 서명

보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화하여 신뢰할 수 있는 인스턴스의 새 REST 및 SOAP 메시지에 서명하고 유효성을 확인합니다.

시작하기 전에
필요한 역할: security_admin

프로시저
1. 신뢰할 수 있는 인스턴스에서 업데이트 세트를 시작합니다.
2. 신뢰할 수 있는 인스턴스에서 필요한 REST 또는 SOAP 메시지를 생성합니다.
   메시지가 업데이트 세트에 추가됩니다.
3. 신뢰할 수 있는 인스턴스에서 업데이트 세트의 상태를 완료 로 변경하고 업데이트를 클릭합니다.
4. 신뢰할 수 있는 인스턴스에서 암호화 작업을 생성하여 업데이트 세트에 서명합니다.
   a. 다음으로 이동 시스템 보안 > 보안 작업 > 모두.
   b. 새로 만들기를 클릭합니다.
   c. 양식에서 다음 값을 입력합니다.

필드	설명
이름	기록을 식별하는 이름입니다.
유형	암호화 작업의 유형입니다. 업데이트 세트 서명을 선택합니다.
테이블	기록에 서명해야 하는 업데이트 세트입니다. 새 **REST V2** 업데이트 세트 서명 **- 1**을 선택합니다.

   d. 제출을 클릭합니다.
   e. 시작을 클릭하여 업데이트 세트에 서명합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기록이 서명되었다는 요약이 업데이트됩니다.
- 업데이트 세트가 업데이트되고 서명이 포함됩니다.

5. 신뢰할 수 있는 인스턴스에서 서명된 업데이트 세트 기록을 열고 XML로 익스포트합니다.
6. 보호된 인스턴스에서 업데이트 세트를 임포트합니다.

   a. 다음으로 이동 시스템 업데이트 세트 > 검색된 업데이트 세트.

   b. XML에서 업데이트 세트 임포트 관련 링크를 선택하여 신뢰할 수 있는 인스턴스에서 익스포트한 업데이트 세트를 임포트합니다.
   자세한 내용은 빠른 시작 업데이트 세트 임포트 및 커밋을 참조하십시오.
   업데이트 세트가 성공적으로 커밋되었습니다.

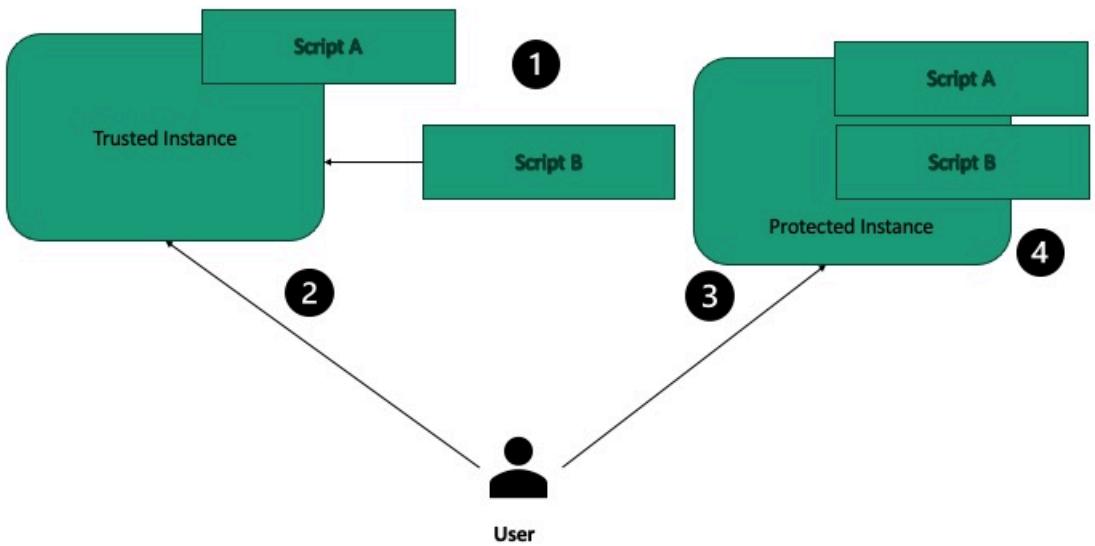
특정 기록 또는 첨부 파일에 서명

테이블의 모든 기록이나 첨부 파일이 아닌 특정 기록이나 첨부 파일에 서명하는 보안 작업을 생성합니다.

릴리스부터 Vancouver 보안 관리자는 보안 작업을 사용하여 테이블의 모든 기록이 아닌 테이블의 특정 기록에 서명할 수 있습니다. 검토되지 않은 코드에 실수로 서명하는 일이 없도록 특정 기록에 서명합니다.

이러한 작업에는 서명 작업이 끝날 때 생성되는 첨부된 로그 파일이 포함됩니다. 이 로그 파일에는 서명된 레코드 및 사용된 서명 구성에 대한 정보가 포함되어 있습니다.

서명 프로세스



이 다이어그램은 서명 프로세스를 사용할 수 있는 방법의 예를 보여줍니다. 이 예에서 `#### B` 라는 레이블이 지정된 스크립트는 보호된 인스턴스에만 존재하며 서명할 신뢰할 수 있는 인스턴스로 가져와야 합니다. `#### A` 가 두 인스턴스에 이미 존재하므로 서명할 필요가 없습니다. 이미 검토 및 서명되었거나, 아직 검토되지 않았으므로 서명해서는 안 됩니다.

1. 신뢰할 수 있는 환경으로 기록을 임포트합니다.
2. 신뢰할 수 있는 인스턴스에서 기록에 서명하는 서명 작업을 생성합니다. 이 프로세스는 에 자세히 설명되어 있습니다 신뢰할 수 있는 인스턴스에서 특정 기록 또는 첨부 파일에 서명하는 작업 만들기.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 업데이트 세트를 사용하여 서명된 서명 작업을 보호된 인스턴스로 임포트합니다.
4. 보호된 인스턴스에서 임포트한 서명 작업을 실행합니다.

신뢰할 수 있는 인스턴스에서 특정 기록 또는 첨부 파일에 서명하는 작업 만들기

신뢰할 수 있는 인스턴스에서 정의한 특정 기록 또는 기록 그룹에 서명합니다.

시작하기 전에

필요한 역할: security_admin 또는 sn_kmf.cryptographic_manager

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 보안 작업 > 새로 작성.
2. 어떤 유형의 보안 작업을 생성하시겠습니까? 프롬프트에서 서명 작업을 선택합니다.
   새 서명 작업 기록이 표시됩니다.
3. 양식의 필요에 따라 필드에 내용을 입력합니다.

서명 작업 필드

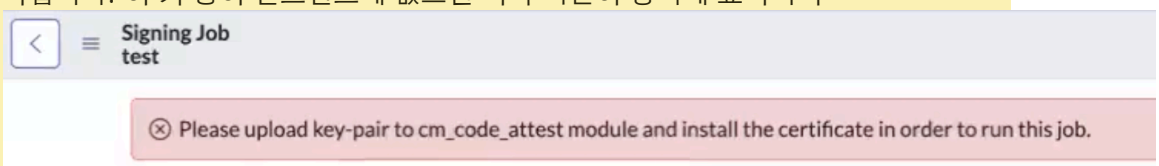
필드	설명
이름	이 작업에 대한 설명이 포함된 이름입니다.
유형	보안 작업의 유형입니다. 특정 레코드에 서명하려면 **[Sign Specific Records**] 옵션을 선택합니다. 특정 첨부 파일에 서명하려면 특정 첨부 파일 서명을 선택합니다.
상태	이 작업의 상태입니다. 이 필드는 신규 값으로 시작합니다. 이 필드는 읽기 전용입니다.
테이블	서명하려는 기록 또는 첨부 파일이 포함된 테이블입니다. 첨부 파일에 서명하는 경우 첨부 파일 [sys_attachment] 테이블이 아니라 첨부 파일이 연결된 기록이 있는 테이블을 선택합니다. **팁:** 키 관리 프레임워크(KMF) 서명 기록 [sn_kmf_record_signature] 테이블을 검사하여 선택한 테이블에 대한 서명이 아직 없는지 확인합니다.
기록 필터링	서명할 기록 선택 테이블에 표시되는 기록을 제한하는 데 사용되는 필터 조건입니다.
서명할 기록 선택	테이블 필드에서 선택한 테이블의 기록 목록으로, 기록 필터 필드에서 생성된 필터로 제한됩니다. 사용 가능 창에서 선택됨 창으로 기록을 이동하여 서명 작업에 포함합니다.
기간 시작	이 작업을 실행할 기간의 시작입니다. 이 필드에 입력한 시간 이후에 작업이 실행됩니다. 유효한 시간 값은 24시간 표기법에 따라 조정된 범용 시간입니다.
기간 종료	이 작업을 실행할 기간의 끝입니다. 이 필드에 입력된 시간 전에 작업이 실행됩니다. 작업이 아직 완료되지 않은 경우 작업이 일시

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	중지되었다가 다음에 시작할 때 다시 시작됩니다. 종료 시간은 시작 시간 이후여야 합니다. 유효한 시간 값은 24시간 표기법에 따라 조정된 범용 시간입니다.
요약	이 작업의 실행에 대한 요약입니다. 이 필드는 읽기 전용입니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
5. 양식 아래쪽에서 프로덕션으로 코드 서명 작업 익스포트를 선택합니다.
   이 작업은 서명 작업에 서명하고 익스포트할 준비가 됩니다.
6. 다음으로 이동 모두 > 시스템 업데이트 세트 > 로컬 업데이트 세트
7. 서명 작업에 대한 업데이트 세트를 찾아서 엽니다.
   고객 업데이트 탭에서 이 업데이트 세트에 서명 작업과 서명 기록이 포함되어 있는 것을 확인할 수 있습니다.
8. XML로 내보내기를 선택합니다.
   이 작업은 로컬 장치에 업데이트 세트를 포함하는 XML 파일을 생성합니다.
9. 프로덕션 인스턴스에서 다음으로 이동합니다. 모두 > 시스템 업데이트 세트 > 검색된 업데이트 세트 > .
10. 페이지 하단에서 XML에서 업데이트 세트 임포트를 선택합니다.
11. 파일 선택 단추를 선택하고 이전 단계에서 만든 XML 파일을 선택합니다.
12. 업로드를 선택합니다.
    업데이트 세트가 로드되고 검색된 업데이트 세트 목록에 나타납니다.
13. 검색된 업데이트 세트 목록에서 임포트한 업데이트 세트의 기록을 엽니다.
14. 업데이트 세트 미리 보기 버튼을 누릅니다.
    미리 보기가 성공적으로 완료되면 업데이트 세트 커밋 버튼이 나타납니다.
15. 업데이트 세트 커밋을 선택합니다.
16. 모두 > 시스템 보안 > 보안 작업 > 모두.
17. 서명 작업을 엽니다.
18. 시작을 선택하여 서명 작업을 실행합니다.

⚠ 경고: 키 페어가 프로덕션 인스턴스에 업로드되지 않은 경우 기록 양식 상단에 경고가 표시됩니다. 이 키 쌍이 인스턴스에 없으면 시작 버튼이 양식에 표시되지 않습니다.



다음에 수행할 작업
완료되면 요약 필드에 작업 결과가 표시됩니다. 서명 작업 기록에 "Mass_Sign_Records-〈sys_id〉"라는 로그 파일도 첨부되어 있습니다. 작업에 대한 자세한 내용과 서명된 각 기록의 sys_ids 목록을 확인하려면 이 기록을 검토하십시오.

보호된 인스턴스의 플로우, 하위 플로우 및 작업에 서명

업데이트 세트를 사용하면 보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화하여 플로우, 하위 플로우 및 작업에 서명하고 유효성을 검사할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 보호된 인스턴스와 신뢰할 수 있는 인스턴스 사이에 설정합니다 Circle of Trust .
- 필요한 역할: security_admin

기존 플로우, 하위 플로우 및 작업에 서명

프로덕션 및 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화하여 기존 플로우, 하위 플로우 및 작업에 서명하고 유효성을 확인합니다.

시작하기 전에
필요한 역할: sn_kmf.cryptographic_manager

프로시저

1. 신뢰할 수 있는 인스턴스에서 단계 인스턴스 테이블의 기록에 서명합니다.

a. 다음으로 이동 시스템 보안 > 보안 작업 > 모두.

b. 새로 만들기를 클릭합니다.

c. 양식에서 다음 값을 입력합니다.

필드	설명
이름	기록을 식별하는 이름입니다.
유형	암호화 작업의 유형입니다. 대량 서명 기록을 선택합니다.
테이블	기록에 서명해야 하는 테이블입니다. 단계 인스턴스를 선택합니다.

d. 코드 서명 작업을 프로덕션으로 익스포트를 클릭합니다.
로컬에 서명된 업데이트 세트 2개가 생성됩니다.
- KMF 서명에 대한 업데이트 세트 1개입니다.
- 코드 서명 작업을 익스포트하기 위한 암호화 작업의 또 다른 업데이트 세트입니다.

2. 신뢰할 수 있는 인스턴스에서 로컬 업데이트 세트를 XML 파일로 익스포트합니다.

a. 다음으로 이동 시스템 업데이트 세트 > 로컬 업데이트 세트.

b. 기록 대량 서명을 위해 생성한 업데이트 세트를 엽니다.

c. XML로 익스포트 관련 링크를 클릭하고 XML 파일을 저장합니다.

3. 보호된 인스턴스에서 XML 파일을 가져옵니다.

a. 다음으로 이동 시스템 업데이트 세트 > 검색된 업데이트 세트.

b. XML에서 업데이트 세트 임포트 관련 링크를 클릭하여 신뢰할 수 있는 인스턴스에서 익스포트한 업데이트 세트를 임포트합니다.
자세한 내용은 빠른 시작 업데이트 세트 임포트 및 커밋을 참조하십시오.
업데이트 세트가 성공적으로 커밋되었습니다.

4. 보호된 인스턴스에서는 신뢰할 수 있는 인스턴스에서 이전에 생성한 암호화 작업을 실행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 시스템 보안 > 보안 작업 > 모두.

b. 신뢰할 수 있는 인스턴스에서 이전에 생성한 암호화 작업을 엽니다.

c. 시작을 클릭하여 작업을 시작합니다.
기록에 서명되었다는 확인 메시지가 표시됩니다.

새 플로우, 하위 플로우 및 작업 서명

보호되고 신뢰할 수 있는 인스턴스에서 코드 서명을 활성화하여 새 플로우, 하위 플로우 및 작업에 서명하고 유효성을 검사합니다.

시작하기 전에
필요한 역할: sn_kmf.cryptographic_manager

프로시저

1. 신뢰할 수 있는 인스턴스에서 업데이트 세트를 시작합니다.
2. 신뢰할 수 있는 인스턴스에서 필요한 플로우, 하위 플로우 또는 작업을 생성하고 게시합니다.
플로우, 하위 플로우 또는 작업이 업데이트 세트에 추가됩니다.
3. 신뢰할 수 있는 인스턴스에서 업데이트 세트의 상태를 완료 로 변경하고 업데이트를 클릭합니다.
4. 신뢰할 수 있는 인스턴스에서 암호화 작업을 생성하여 업데이트 세트에 서명합니다.

a. 다음으로 이동 시스템 보안 > 보안 작업 > 모두.

b. 새로 만들기를 클릭합니다.

c. 양식에서 다음 값을 입력합니다.

필드	설명
이름	기록을 식별하는 이름입니다.
유형	암호화 작업의 유형입니다. 업데이트 세트 서명을 선택합니다.
테이블	기록에 서명해야 하는 업데이트 세트입니다.

d. 제출을 클릭합니다.

e. 시작을 클릭하여 업데이트 세트에 서명합니다.
- 기록이 서명되었다는 요약이 업데이트됩니다.
- 업데이트 세트가 업데이트되고 서명이 포함됩니다.

5. 신뢰할 수 있는 인스턴스에서 서명된 업데이트 세트 기록을 열고 XML로 익스포트합니다.
6. 보호된 인스턴스에서 서명된 업데이트 세트를 임포트합니다.

a. 다음으로 이동 시스템 업데이트 세트 > 검색된 업데이트 세트.

b. XML에서 업데이트 세트 임포트 관련 링크를 선택하여 신뢰할 수 있는 인스턴스에서 익스포트한 업데이트 세트를 임포트합니다.
자세한 내용은 빠른 시작 업데이트 세트 임포트 및 커밋을 참조하십시오.
업데이트 세트가 성공적으로 커밋되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

코드 서명 참조

참조 주제는 코드 서명을 관리하고 문제를 해결하기 위한 추가 정보를 제공합니다.

코드 서명과 함께 설치되는 속성

코드 서명은 다음 속성을 추가합니다.

로그 문제 해결 및 액세스

다양한 로그에 액세스하여 문제를 해결하고 실패 원인을 식별합니다.

코드 서명과 함께 설치되는 속성

코드 서명은 다음 속성을 추가합니다.

속성	유형	설명
com.glide.codesigning.expanded.tracking.enabled	true | false	예인 경우 **com.glide.codesigning.expanded_tracking.topic.list** 속성에 나열된 ecc_queue 주제에 대한 메타 스택의 유효성 확인 길이가 증가합니다. **중요사항:** 이 속성을 수정하려면 높은 보안이 필요합니다.
com.glide.codesigning.expanded.tracking.length	정수	코드 서명을 사용할 때 발생하는 코드 서명 확인 수준입니다. 기본값은 3입니다. **중요사항:** 이 속성을 수정하려면 높은 보안이 필요합니다.
com.glide.codesigning.expanded_tracking.topic.list	문자열	메타 스택 추적을 증가시킬 주제의 쉼표로 구분된 목록입니다. **중요사항:** 이 속성을 수정하려면 높은 보안이 필요합니다.
com.glide.codesigning.tracking.agent.validation.exclusion.list	문자열	코드 서명을 건너뛰어야 하는 ecc_queue 에이전트의 쉼표로 구분된 목록
com.glide.codesigning.tracking.debug	true | false	true인 경우 코드 서명 추적기에 대한 디버그 로깅이 활성화됩니다.
com.glide.codesigning.tracking.enabled	true | false	true일 경우 코드 서명 호출자 추적을 사용합니다. **중요사항:** 이 속성을 수정하려면 높은 보안이 필요합니다.
com.glide.codesigning.tracking.logging.enabled	true | false	true일 경우 코드 서명 추적에 대한 로깅을 활성화합니다.
com.glide.codesigning.tracking.unsupported_script_tracking.enabled	true | false	예인 경우 지원되지 않는 스크립트를 통해 삽입된 ecc_queue 기록(탐지된 경우)은 공증되지 않습니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	유형	설명
		중요사항: 이 속성을 수정하려면 높은 보안이 필요합니다.
com.glide.codesigning.tracking.validation.fail_fast	true | false	예일 때는 모든 스크립트를 검증하는 대신 첫 번째 스크립트 확인 실패 시 코드 서명 검증에 실패합니다. 중요사항: 이 속성을 수정하려면 높은 보안이 필요합니다.
com.glide.event_handler.code_signing.tracking	true | false	코드 서명을 새로 활성화하는 고객이 가능한 한 안전하게 구성되도록 하는 데 도움이 되는 이벤트 핸들러를 정의합니다. 중요사항: 이 속성을 수정하려면 높은 보안이 필요합니다.
com.glide.web_service_outbound.impl.codesigning.tracking	true | false	예일 때는 SOAPMessageV2 코드 서명 추적을 사용합니다. 중요사항: 이 속성을 수정하려면 높은 보안이 필요합니다.
com.snc.csf.servicenow_root_of_trust.비활성화됨	true | false	신뢰 루트 기능이 활성 상태인지 여부입니다. 기본값은 `false`이며, 이는 빌드 인증서를 신뢰할 수 있음을 ServiceNow 의미합니다. 중요사항: 이 속성은 관리자, 보안 관리자 및 KMF 관리자 역할이 있는 사용자의 서명된 예약된 작업을 통해서만 변경할 수 있습니다. 신뢰 루트 변경에 대한 자세한 내용은 을 참조하십시오 신뢰 루트 구성 변경.
com.snc.kmf.signature.validation.optin	true | false	예일 때는 인스턴스에서 코드 서명을 사용합니다. 중요사항: 이 속성은 에 대한 고객 서비스 및 지원요청을 통해서만 변경할 수 있습니다.
glide.jdbcprobeloader.tracking	true | false	JDBC 데이터 소스에 대해 코드 서명을 설정하거나 해제합니다. 중요사항: 이 속성을 수정하려면 높은 보안이 필요합니다.
glide.rest.codesigning.tracking	true | false	예일 때는 RESTMessageV2 코드 서명 추적을 사용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	유형	설명
		중요사항: 이 속성을 수정하려면 높은 보안이 필요합니다.

코드 서명과 함께 설치되는 역할

코드 서명에는 다음 역할이 포함됩니다.

코드 서명 관리자 **[codesigning_admin]**

코드 서명 관리자 역할을 사용하여 codesigning_manager 및 codesigning_auditor 역할을 다른 사용자에게 할당합니다.

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

보다 전문적인 역할을 사용할 수 있는 경우 관리자 역할을 부여하지 마십시오.

코드 서명 관리자 **[codesigning_manager]**

코드 서명 관리자 역할을 사용하여 서명 구성을 생성 및 업데이트하고, 코드 서명 작업을 생성 및 실행합니다.

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

없음.

코드 서명 감사자 **[codesigning_auditor]**

코드 서명 감사자 역할을 사용하여 서명 구성 및 서명 작업을 봅니다. 감사자 역할에는 코드 서명 자산을 만들거나 쓸 수 있는 권한이 없습니다.

역할 포함

역할에 포함된 역할 목록입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

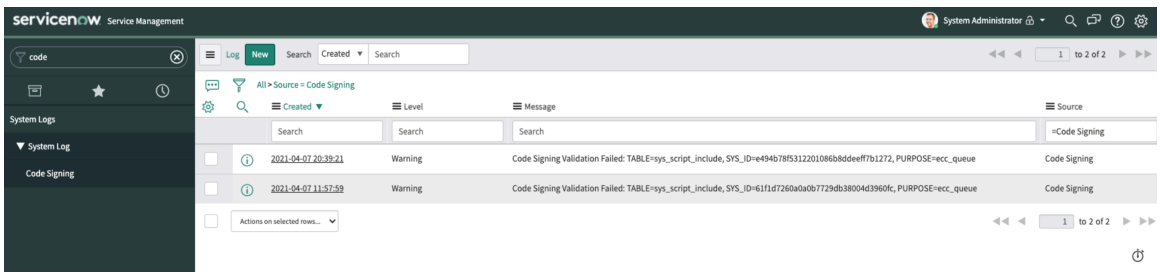
없음.

로그 문제 해결 및 액세스

다양한 로그에 액세스하여 문제를 해결하고 실패 원인을 식별합니다.

코드 서명 로그

ECC 큐 레코드가 코드 서명 추적기 API에 의해 서명되지 않은 경우 서명되지 않은 메시지와 필수 세부 정보가 코드 서명 모듈에 표시됩니다. 다음으로 이동 시스템 로그 > 시스템 로그 > 코드 서명 신뢰할 수 없는 기록 목록에 액세스하기 위해

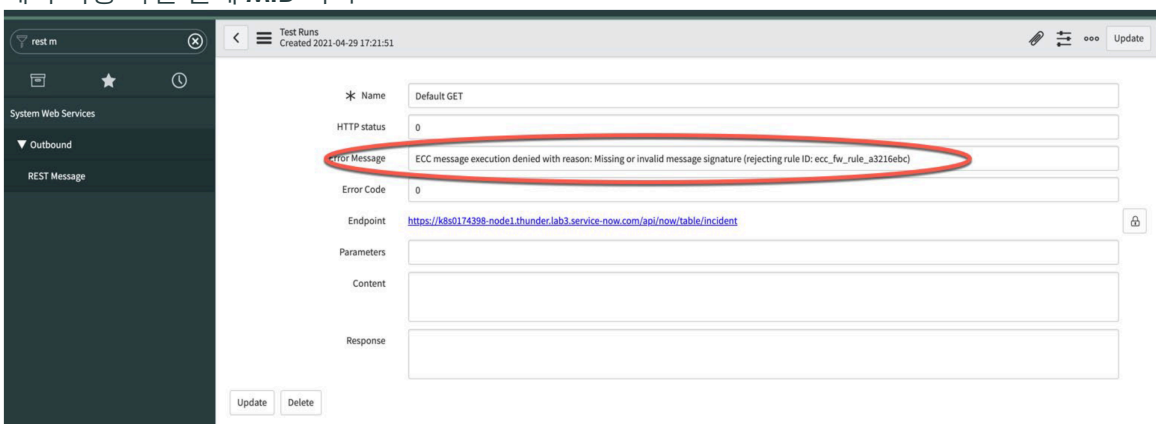


추가 디버그 노드 로그의 경우 해당 값을 활성화 *com.glide.codesigning.tracking.debug* 하고 `true# #####`.

에서 **REST** 메시지 서명 확인 실패 **MID** 서버

다음으로 이동하여 서명 확인 실패 와 관련된 오류 메시지에 액세스합니다. 시스템 웹 서비스 > 아웃바운드 > **REST** 메시지 필요한 REST 메시지 기록을 엽니다.

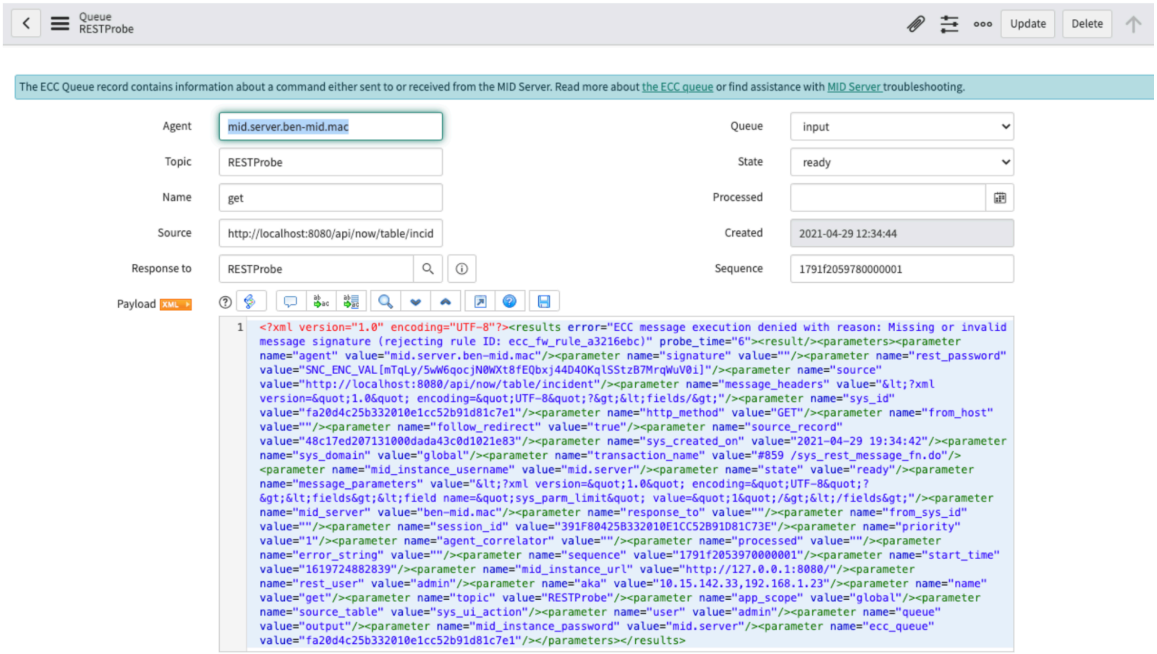
에서 서명 확인 실패 **MID** 서버



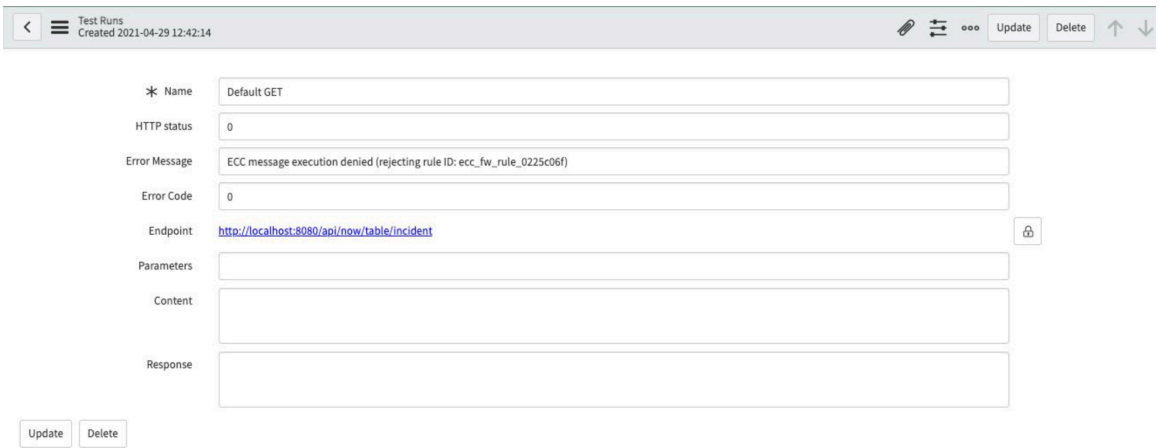
주: ECC 방화벽 거부와 관련된 오류 메시지는 `ECC ### ### ###` 것으로 시작합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에서 서명 확인에 실패할 경우의 **ECC** 큐 **MID** 서버



ECC 메시지가 사용자 규칙에 의해 차단될 때의 오류 메시지



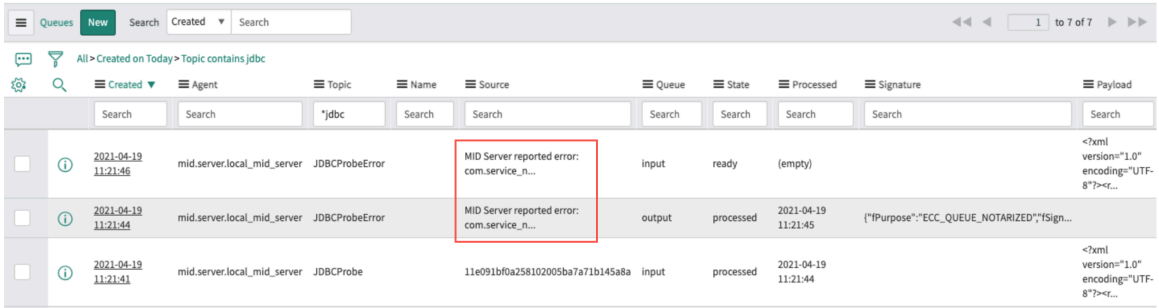
JDBC 프로브

유효하지 않거나 누락된 서명이 있는 JDBC 데이터 소스가 에서 MID 서버실행되면 필요한 세부사항이 포함된 오류 메시지가 표시됩니다.



소스 에는 오류 메시지의 상세 정보도 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



MID 서버 로그

상세 ECC 방화벽 로깅을 사용하려면 MID 서버 구성 매개변수 *mid.log.level*의 값을 TRACE로 설정하여 로그 수준을 높입니다. 자세한 로그는 다음에 대한 정보를 제공합니다.

- 부팅 구성 파일에서 로드된 MID 서버 규칙입니다.
- 규칙의 세분화된 실행 추적입니다.
- ECC 메시지를 수락하거나 거부해야 하는 특정 규칙입니다.

주: `boot-config.xml` 잘못되면 시작되지 MID 서버 않으며 실패 상세 정보가 MID 에이전트 로그에 기록됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

바이러스 백신 검사

바이러스 백신 검사을 사용하면 인시던트, 문제, 스토리와 같은 시스템 기록에 첨부 파일을 통해 유입될 수 있는 바이러스 감염으로부터 인스턴스를 보호할 수 있습니다.

바이러스 백신 검사 살펴보기



바이러스 백신 검사의 가치에 대해 알아보십시오.

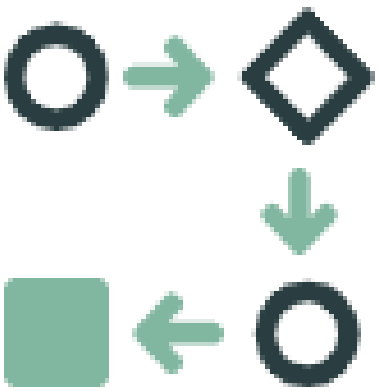
바이러스 백신 보호 구성



바이러스 백신 보호를 구성하는 방법을 이해합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

감염된 파일 해결



감염된 파일로 수행할
작업에 대해 알아봅니다.

바이러스 백신 검사에 대한 참조



바이러스 백신 검사에 대한
사전 속성에 대해 알아봅니다.

바이러스 백신 검사 탐색

바이러스 백신 검사을 사용하면 인시던트, 문제, 스토리와 같은 시스템 기록에 첨부 파일을 통해 유입될 수 있는 바이러스 감염으로부터 인스턴스를 보호할 수 있습니다.

바이러스 백신 검사 에서 첨부 파일 [sys_attachment] 테이블에 저장된 첨부 파일을 검사하여 사용자가 감염된 파일을 업로드 및 다운로드하지 못하도록 보호합니다. 플랫폼에서 지원하는 모든 문서 유형은 바이러스 백신 검사로 검사됩니다.

바이러스 백신 검사 이 옵션을 활성화하면 기본적으로 첨부 파일 테이블 〔sys_attachment.do〕의 모든 첨부 파일이 검사됩니다.

플러그인(com.glide.snap)이 바이러스 백신 보호 활성화되어 인스턴스에서 기본적으로 활성화됩니다. 관리자는 토글을 전환하여 인스턴스 전체에서 기능을 바이러스 백신 검사 비활성화 및 재활성화하고, 구성 옵션을 설정하고, 인스턴스의 바이러스 백신 활동을 검토할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 바이러스 백신 검사 는 GCC(정부 커뮤니티 클라우드) 및 상용 환경의 고객도 사용할 수 있습니다.

  GCC 사용자는 기능 사용을 시작하려면 (com.glide.snap.fed_enable_scan) 속성을 `true` 로 설정해야 합니다.

  상용 사용자는 `true`로 설정해야 *com.glide.snap.enable_scan* 합니다.

- HTTP 및 HTTPS 통신 프로토콜이 지원됩니다.
- 에지 암호화 파일은 이 검사에서 제외됩니다.
- 바이러스 백신 정의는 매일 업데이트됩니다.
- 파일 크기가 100MB를 초과하는 파일은 검사되지 않습니다.

이메일 스캔

인바운드 이메일은 에 의해서바이러스 백신 검사가 아니라 시스템 이메일 필터 에 의해 바이러스 검사를 받습니다.

테이블의 파일 첨부 필드

테이블에 첨부 파일 필드를 추가하면 zz_yy 테이블이 작성됩니다. 이러한 테이블은 동적 테이블과 가상 테이블입니다. 열 유형 **file_attachment** 상위 테이블에 추가될 때 자동으로 생성됩니다.

사용자 테이블에 사용자 사진을 추가하고 양식 뷰에 통합하는 것이 좋습니다. 사진이 기록에 업로드되면 첨부 파일이 sys_attachment 테이블에 자동으로 업로드됩니다. sys_attachment 테이블은 사진을 zz_yyUsers 테이블에 매핑합니다.

기본적으로 zz_yylive_profile 테이블에 첨부된 첨부 파일만 검사됩니다. 열 유형이 있는 다른 테이블을 스캔 **file_attachment** 시스템 속성을 *com.glide.snap.scan.zz_yytables* 생성하고 테이블 이름을 삽입합니다.

예

"zz_yyincident" 및 "zz_yycase" 테이블은 열이 상위 테이블(인시던트 및 케이스)에 추가될 때 작성되는 동적 테이블이므로 속성 값은 다음과 같아 *zz_yyincident,zz_yycase*야 합니다.

이 속성이 설정되면 zz_yyincident 및 zz_yycase 테이블의 첨부 파일이 검색됩니다.

스캔 시나리오

이러한 업로드 및 다운로드 시나리오를 검토하여 시스템이 기록에 첨부된 파일에서 잠재적인 보안 위협을 식별하는 방법을 이해합니다.

시나리오 1 - 파일 업로드

1. 사용자가 자신도 모르게 감염된 파일을 레코드에 업로드합니다.
2. 시스템에서 파일을 검사하여 격리로 옮깁니다.
3. 파일이 사용할 수 없음으로 표시된 첨부 파일 창에 나타납니다.
4. 사용자가 파일을 선택하면 파일 Infected_testing.txt 보안 검사를 통과하지 못했습니다. `## INC0000059## ### #### ## ######.`
5. 시스템은 사용자와 바이러스 백신 관리자에게 이메일 알림을 보냅니다.
6. 사용자가 첨부 파일 창을 닫고 기록으로 돌아갑니다. 감염된 파일이 헤더에 사용할 수 없음으로 표시됩니다. 예: `infected_testing123.txtZ [unavailable].`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시나리오 2 - 파일 다운로드

1. 사용자는 기록을 열어 첨부된 파일을 다운로드합니다.
2. 파일이 감염되었다는 사실을 모르고 사용자는 다운로드하기 위해 파일을 선택합니다.
3. 시스템에서 파일을 검사하여 격리 저장소로 옮기고 다음과 유사한 메시지를 표시합니다. `## infected_testing123.txt ## ### #### ## ##### # ####.`
4. 사용자가 메시지를 닫고 화면을 새로 고쳐 파일을 사용할 수 없음을 알립니다.
5. 시스템은 사용자와 바이러스 백신 관리자에게 이메일 알림을 보냅니다.

시나리오 3 - ZIP 파일 다운로드

1. 사용자가 기록을 열고 첨부된 ZIP 파일을 다운로드합니다.
2. 시스템이 ZIP 파일을 개별적으로 검사합니다.
3. 한 파일이 보안 검사를 통과하지 못하고 사용할 수 없는 것으로 표시됩니다. 나머지 파일은 압축되고 성공적으로 다운로드됩니다.
4. 사용자가 ZIP 파일을 열면 성공적으로 다운로드된 파일 외에 "error.txt" 파일이 표시됩니다. 이 파일에는 검사를 통과하지 못해 ZIP에 포함되지 않은 파일을 지정하는 오류 메시지가 포함되어 있습니다.
5. 사용자가 레코드를 다시 열면 사용할 수 없는 파일이 첨부 파일 창의 잠재적 보안 위험 섹션으로 이동되어 다운로드할 수 없음을 알 수 있습니다.

바이러스 백신 검사 구성

인스턴스 전체와 테이블 수준에서 구성합니다 바이러스 백신 검사 .

시작하기 전에
필요한 역할: antivirus_admin 또는 admin

이 태스크 정보
바이러스 백신 검사 는 인스턴스에서 기본적으로 활성화되어 첨부 파일을 자동으로 검사하여 바이러스에 감염된 파일을 식별합니다. 인스턴스 전체에서 스캔이 활성화되도록 하고 스캔에서 제외할 테이블을 식별하여 기능을 구성합니다.

프로시저
1. 다음으로 이동 모두 > 바이러스 백신 > 구성.
2. 기능을 구성할 때 다음 사항을 고려하십시오.

옵션	설명
바이러스 백신 검색 사용	바이러스 백신 검사가 활성화되어 있고 인스턴스에서 기본적으로 활성화되어 있으며, 토글이 켜짐 위치로 설정되고 녹색으로 나타납니다. 주: 속성을 `false` 로 설정하려면 고객 지원에 문의하십시오.
바이러스 검사 프로그램을 사용할 수 없을 때 첨부 파일을 다운로드할 수 있음	이 옵션을 켜짐 위치로 설정하면 스캐너 시간이 초과되어 응답을 얻을 수 없는 경우 바이러스 백신 검사가 무시됩니다. 이 경우 스캔을

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	완료하지 않고 파일 다운로드가 진행됩니다. 이 옵션을 꺼짐으로 설정하면 검사가 성공적으로 완료될 때까지 파일 다운로드가 금지됩니다.
제외된 테이블 목록	이 목록의 테이블과 연결된 첨부 파일은 바이러스 백신 검사에서 제외됩니다. 시스템이 검사에서 제외할 테이블을 정의하려면 4단계로 진행합니다.

3. 저장을 선택합니다.
4. 제외된 테이블 목록에 테이블을 추가하여 바이러스 백신 검사에서 제외합니다.
   a. 시스템 정의 → 딕셔너리로 이동
   b. 검사에서 제외할 테이블을 검색하고 유형이 수집으로 설정된 테이블을 선택합니다.
   c. 속성 탭에서 새로 만들기를 선택합니다.
   d. 속성 필드에 `Exclude_from_antivirus_scan` 추가하고 값 필드에 `True`를 입력합니다.
   e. 제출을 선택합니다.

결과
바이러스 백신 검사 인스턴스에서 활성화되고 바이러스 백신 구성 페이지에서 제외된 테이블 목록이 검사에서 제외한 모든 테이블로 채워집니다.

격리된 파일 검토

격리된 파일 첨부 파일을 검토하고 필요에 따라 추가 조치를 취합니다.

시작하기 전에
필요한 역할: antivirus_admin 또는 admin

이 태스크 정보
바이러스 백신 격리 페이지에서 격리된 파일 항목을 정기적으로 모니터링하여 다음 작업을 수행합니다.

프로시저

1. 다음으로 이동 모두 > 바이러스 백신 > 격리.
2. 사용 가능한 작업을 수행하려는 각 격리된 항목 옆의 확인란을 선택합니다.
3. 배너에서 선택한 행에 대한 작업 드롭다운을 선택하여 선택한 행의 격리된 항목에서 수행할 작업을 선택합니다.

동작	설명
삭제	사용자에게 더 이상 필요하지 않은 경우 격리된 파일을 삭제하려면 이 작업을 선택합니다.
재개	상태 평가 또는 사용자 요청에 따라 파일을 복원하려면 이 작업을 선택합니다. 그러나 바이러스 위협을 완화하려면 복원하기 전에 타사 바이러스 백신 제품으로 파일을 검사하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

동작	설명
	복원이 완료되면 사용자가 파일을 다운로드할 수 있습니다.
다운로드	추가 스캔 및 분석을 위해 파일을 로컬 시스템에 다운로드하려면 이 작업을 선택합니다.

결과
시스템은 확인을 요청하고 입력에 따라 선택한 작업을 수행합니다.

관련 정보

인스턴스 보안 센터

바이러스 백신 메트릭

바이러스 백신 활동 검토

잠재적으로 감염된 파일에서 발생하는 모든 활동이 검색되어 격리된 시점부터 추적하는 바이러스 백신 활동 로그를 검토합니다.

시작하기 전에
필요한 역할: antivirus_admin 또는 admin

이 태스크 정보
이 로그는 검색, 삭제 및 기타 격리된 파일 이벤트와 같은 바이러스 백신 활동을 캡처하는 보고서 역할을 합니다.

프로시저

1. 다음으로 이동 모두 > 바이러스 백신 > 활동.
2. 격리된 파일의 로그를 검토합니다.
   격리된 각 파일에 대한 이벤트 열에서 수행된 작업을 볼 수 있습니다.

다음에 수행할 작업
삭제, 복원, 다운로드 또는 로그에 보관할 기록을 결정합니다. 격리된 파일 검토를 참조하십시오.

의 딕셔너리 속성에 대해 알아보기 바이러스 백신 검사

딕셔너리 속성은 딕셔너리 레코드가 설명하는 테이블 또는 요소의 동작을 변경합니다. 관리자는 딕셔너리 속성 값을 설정하여 기본 바이러스 백신 검색 구성의 동작을 수정할 수 있습니다.

의 딕셔너리 속성 바이러스 백신 검사

이름	값	대상 요소	설명
Exclude_from_antivirus_scan	예/아니요	모든 테이블	예일 경우 테이블의 첨부 파일이 바이러스 백신 검사에서 제외됩니다. 바이러스 백신 검사 구성 문서를 참조하십시오.
Supress_antivirus_email_notification	예/아니요	모든 테이블	true이면 잠재성에 감염된 파일이 식별되면 플랫폼에서 생성된

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 딕셔너리 속성 바이러스 백신 검사

이름	값	대상 요소	설명
			이메일 알림 전송을 중지합니다.
Suppress_antivirus_ui_notification	예/아니오	모든 테이블	true이면 잠재적으로 감염된 파일이 식별될 때 플랫폼에서 생성된 UI 알림을 중지합니다.

관련 정보

딕셔너리 속성을 사용하여 테이블 및 필드 변경

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

HTML 위생 검사

HTML 필드와 번역된 HTML 필드에서 HTML 마크업을 삭제하여 불필요한 코드를 제거하고 교차 사이트 스크립팅 공격과 같은 보안 문제로부터 보호합니다.

HTML 위생 검사 탐색



HTML 위생 검사의 작동 방식에 대해 알아봅니다.

HTML 위생 검사 구성



HTML 위생 검사를 구성합니다.

HTML 위생 검사 활성화



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

HTML 위생 검사를 사용
설정하는 방법을 알아보세요.

HTML 위생 검사 살펴보기

HTML 필드와 번역된 HTML 필드에서 HTML 마크업을 삭제하여 불필요한 코드를 제거하고 교차 사이트 스크립팅 공격과 같은 보안 문제로부터 보호합니다.

HTML 정리를 사용하여 인스턴스 내의 HTML 콘텐츠에 잠재적으로 유해한 콘텐츠가 포함되어 있지 않도록 합니다. HTML 정리는 인스턴스를 손상시키는 데 사용될 수 있는 HTML 태그(예: `<![CDATA[<script>]]>`) `<link>`또는 `<embed>` 인스턴스에서 원치 않는 스크립트를 실행하거나 사용자를 원치 않는 콘텐츠로 안내하는 데 사용될 수 있는 태그를 제거하는 방식으로 작동합니다. 콘텐츠의 서식을 제어하는 안전한 태그는 유지됩니다. 관리자는 제거되거나 보존되는 콘텐츠를 사용자 지정할 수 있습니다. 또한 위생을 모든 콘텐츠에 적용할지 또는 지정한 필드에만 적용할지를 제어할 수 있습니다.

HTML 위생 검사는 항상 유지하려는 마크업에 대한 기본 제공 포함 목록을 확인하여 작동합니다. 새니타이저는 관리자가 내장 포함 목록을 수정하는 데 사용할 수 있는 *HTMLSanitizerConfig* 스크립트 포함을 제공합니다. 제외 목록에 항목을 추가하여 HTML 마크업을 제거할 수도 있습니다. 제외 목록의 내용이 포함 목록을 재정의합니다.

포함 및 제외 목록에 추가할 수 있는 항목 유형은 다음과 같습니다.

- 전역 속성
- 모든 HTML 요소

주: 기본적으로 `href` 및 `src` 와 같은 URL 속성은 다음 프로토콜만 지원합니다.

- `http`
- `https`
- `mailto`
- `###`

예:

```
<a href="https://community.servicenow.com/community"> ServiceNow 커뮤니티
 </a>
```

주: HTML 위생 검사 사용을 제어하는 속성에 대한 *glide.html.sanitize_all_fields* 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 HTML 위생 검사 사용 [Security Center 1.3에서 업데이트됨] .

urlAttributes 및 프로토콜 구성

HTMLSanitizer 스크립트 포함에서 urlAttributes 및 해당 프로토콜을 구성할 수 있습니다. 예:

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
                 -  -
                 -  -
        }
```

`# #### ##`가 포함 목록에 있기 때문에 이 URL은 삭제되지 않습니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
<a title="Lotus"
 href="Notes://
ABC/X575C90019DE33/ABC594DCB76D86EB4925653E0011C4C1/ZZ90B7E2D33964749257E
EA003456FD">Lotus</a></p>
```

기본 포함 목록

주: 기본 포함 목록은 시스템 목록이며 인스턴스에서 사용자가 액세스할 수 없습니다.

```
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","backg
round","align","no resize","height","width","summary","frame","rules"]},


 th:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowr
ap","height","width","align","valign","char
 off","char","colspan","rowspan"]},


 td:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowr
ap","height","width","align","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"]},

    p:{attribute:["align"]},
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
    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","disa
bled","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:{},
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
   dd:{},    dt:{},    dl:{},  fieldset:{},    legend:{}, figure:{},
tt:{},

   body:{},   caption:{},   head:{},   title:{},  shape:{},},
```

HTML 위생 검사 구성

HTML 위생 검사의 구성을 변경하려면 스크립트 포함을 수정해야 합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 스크립트 포함.
2. **HTMLSanitizerConfig**를 엽니다.
3. 제외 목록에 항목을 추가하려면 HTML_BLACKLIST 클래스를 사용합니다.

   포함 목록에 항목을 추가하려면 HTML_WHITELIST 클래스를 사용합니다.

   다음 형식을 사용합니다.

```
HTML_XXXXLIST :{
        globalAttributes :{

            attribute:[attribute-name1,...],

 attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,
...}

        },<html-element-name>:{// Same as Above},----}
```

   - *globalAttributes* 에는 모든 HTML 요소에 전역적으로 적용 가능한 속성 또는 attributeValuePattern 항목이 포함되어 있습니다.
   - *attribute* 는 쉼표로 구분된 속성 목록입니다.
   - *attributeValuePattern* 속성은 속성-값-정규 표현식 패턴 쌍에 대한 속성 딕셔너리입니다. attribute-value-regex-pattern은 속성 값과 일치해야 하는 정규 표현식입니다.

Example:
다음과 같은 예를 들 수 있습니다.

```
HTML_WHITELIST:{
        globalAttributes:{
            attribute:["id","name"],},
        img:{
            attribute:["style","align"],
            attributeValuePattern:{src:".*jpeg"}},
        iframe:{},}
```

포함 목록에 다음 항목이 추가됩니다.

- 전역 속성 id 및 이름입니다. 모든 요소에 전역으로 적용할 수 있는 문자열 목록입니다.
- 속성이 style 및 align인 img 요소입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 이미지의 source 속성이 .jpeg 확장자를 가진 파일인 img 요소. 다음은 속성 값과 일치하는 정규 표현식 패턴의 예입니다.
- iframe 요소입니다.

HTML 위생 검사 사용

HTML 위생 검사는 시스템의 모든 HTML 필드에 대해 위생 검사를 활성화하거나 비활성화하는 속성을 제공합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
기본적으로 이 속성은 새 인스턴스에 대해 true로 설정됩니다.

프로시저

1. 탐색 필터에 `sys_properties.list`를 입력합니다.
2. 속성 *glide.html.sanitize_all_fields* 및 *glide.translated_html.sanitize_all_fields*를 **true**로 설정합니다.

   주: 이 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 HTML 위생 검사 사용 [Security Center 1.3에서 업데이트됨].

Trouble?

속성이 시스템 속성 테이블에 없는 경우 추가할 수 있습니다.

개별 필드에서 정리 사용

필드 속성을 사용하여 개별 필드에서 위생 검사를 활성화하거나 비활성화할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
먼저 sanitizer 속성을 false로 설정한 다음 모든 양식에 대해 필드별로 sanitizer를 활성화해야 합니다.

프로시저

1. sys_properties 테이블로 이동하여 **false** *glide.html.sanitize_all_fields*로 설정합니다.
   이렇게 하면 시스템의 모든 HTML 필드에 대해 위생 검사가 비활성화됩니다.
2. HTML 필드가 포함된 양식으로 이동합니다.
3. HTML 필드 레이블을 마우스 오른쪽 단추로 클릭하고 딕셔너리 구성을 선택합니다.
   HTML 필드에 대한 딕셔너리 항목 양식이 열립니다.
4. 속성 필드에 다음 중 하나를 입력합니다.
   - 정리를 비활성화하려면 `html_sanitize=false`를 입력합니다.
   - 정리를 활성화하려면 `html_sanitize=true`를 입력합니다.
5. 업데이트를 클릭합니다.
6. 번역된 HTML 필드에 대해 HTML 위생 검사를 사용하려면 속성을 예로 *glide.translated_html.sanitize_all_fields* 설정하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

HTML 위생 검사 로깅 사용

HTML 위생 검사가 요소나 속성을 제거하면 시스템 로그에 추가됩니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
인스턴스 URL에 /syslog_list.do?sysparm_query=source%3DHTMLSanitizer를 추가하여 이러한 삭제된 요소를 검토할 수 있습니다.

프로시저

1. 이러한 삭제된 요소를 검토하려면 인스턴스 URL에 `/syslog_list.do?sysparm_query=source%3DHTMLSanitizer` 를 추가합니다.
2. 로깅을 활성화하거나 비활성화하려면 `### ###` `glide.html_sanitize.discarded_log.enable` 속성을 추가하고 값을 **true** (활성화) 또는 **false** (비활성화)로 설정합니다.
   이 속성은 기본적으로 **true** 입니다.

스타일 유효성 검사 사용

HTML/번역된 HTML 필드에 저장되는 CSS 스타일시트에 사용할 수 있는 도메인 목록을 허용합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Yokohama 및 Xanadu Patch6(아직 출시되지 않음) 시작 관리자는 HTML/번역된 HTML 필드에 저장된 CSS에서 사용할 수 있는 도메인의 허용 목록을 지정할 수 있습니다.

프로시저

1. 탐색 필터에 `sys_properties.list`를 입력합니다.
2. 속성을 *glide.html.css.enable_url_validation* **true**로 설정합니다.

   Trouble?

   속성이 시스템 속성 테이블에 없는 경우 추가할 수 있습니다.

3. 허용되는 도메인 이름의 쉼표로 구분된 목록을 입력하십시오.
   glide.html.css.url_allowed_hosts

결과
가 예일 때는 *glide.html.css.enable_url_validation* HTML/번역된 HTML 필드의 일부인 CSS 컨텐츠에 사용되는 URL이 에 *glide.html.css.url_allowed_hosts*지정된 도메인의 허용 목록에 대해 유효성이 검사됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

감사

감사 지원 테이블에서 기록 변경 내용을 추적합니다. 기본적으로 이 시스템은 인시던트, 변경 및 문제 테이블에 대한 변경 내용을 추적합니다.

탐색



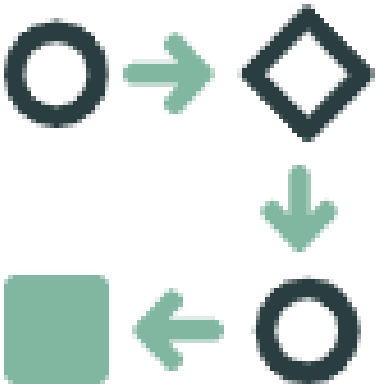
감사의 기능 및 비즈니스 가치에 대해 알아봅니다.

구성



감사 구성 방법을 이해합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

뷰	참조
	
시스템 감사 및 감사 관계 변경 테이블을 검토합니다.	역사 세트에 대해 알고 있습니다.

감사 살펴보기

감사 지원 테이블에서 기록 변경 내용을 추적합니다. 기본적으로 이 시스템은 인시던트, 변경 및 문제 테이블에 대한 변경 내용을 추적합니다.

감사를 활성화하면 테이블에 있는 모든 기록의 생성, 업데이트 및 삭제가 추적됩니다. 테이블의 개별 필드를 감사하려면 딕셔너리 속성을 사용하여 추적하지 않으려는 필드를 숨길 수 있습니다.

감사 정보는 다음 테이블에 보관됩니다.

- 감사 테이블
- 테이블입니다 히스토리 세트에 대한 지식 .

⚠ **경고:** 워크플로우 컨텍스트[wf_context] 또는 이벤트 관리 경보(em_alert)와 같이 많은 양의 트래픽을 수신하는 시스템 테이블을 감사하면 성능에 영향을 줄 수 있습니다. 따라서 em_alert 테이블 전체를 감사할 수 없습니다. 대신, 선택한 관심 분야를 감사하십시오. em_alert 테이블과 선택한 필드 모두에 설정합니다 `audit=true`. 가능한 한 적은 수의 필드를 감사하도록 하십시오.

상위 및 하위 테이블 감사

테이블은 상위 또는 하위 감사 테이블에서 감사 플래그를 파생하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 예를 들어 구성 항목 [cmdb_ci] 테이블에 대한 감사를 사용하도록 설정하면 해당 기본 테이블에 저장된 CI만 감사됩니다.
- 마찬가지로 컴퓨터 [cmdb_ci_computer] 테이블에 대한 감사를 사용하도록 설정하면 구성 항목 [cmdb_ci] 테이블에서 파생된 컴퓨터 [cmdb_ci_computer] 테이블의 필드를 포함하여 컴퓨터 CI 기록만 감사됩니다.

감사 시스템 테이블

기본적으로 시스템은 시스템 테이블에서 기록 삭제를 감사하지 않습니다. 시스템 테이블을 감사하려면 속성 목록의 테이블 *glide.ui.audit_deleted_tables* 목록에 추가합니다.

양식 또는 목록에서 삭제 감사

기본적으로 시스템은 양식에서 개별 기록 삭제를 감사합니다. 감사를 방지하려면 테이블의 딕셔너리 속성을 *no_audit_delete*설정하십시오.

테이블 딕셔너리에서 감사 가 선택되고 테이블이 속성에 나열 *glide.db.audit.ignore.delete* 되지 않은 경우 시스템은 목록에서 삭제를 감사합니다.

주: 기본적으로 이 *glide.db.audit.ignore.delete* 속성은 시스템 속성 [sys_properties] 테이블에 없습니다. 속성 및 관련 값을 변경하려면 먼저 수동으로 추가해야 합니다. 그러나 수동으로 추가하면 다음 기본값을 덮어씁니다.

```
glide.db.audit.ignore.delete =
sys_mutex,sys_db_cache,sys_lucene_block,sys_lucene_file,sys_lucene_directory,sys_use
cmdb_ci_windows_service, cmdb_sam_sw_install, cmdb_software_instance,
cmdb_sam_sw_usage, sam_sw_counter_detail
```

시스템 속성 추가에 대한 자세한 내용은 시스템 속성 추가를 참조하십시오.

기본적으로 감사 삭제는 기록이 양식 보기, 목록 보기 또는 스크립트/예약된 작업을 통해 삭제되는지 여부에 관계없이 활성화됩니다.

정보 감사됨

감사는 다음과 같은 레코드 변경 내용을 추적합니다.

- 변경된 기록의 고유 기록 식별자(sys_id)
- 변경된 필드
- 새 필드 값
- 기존 필드 값
- 이 기록과 필드가 업데이트된 횟수
- 변경이 발생한 날짜 및 시간
- 변경한 사용자
- 변경 이유(변경과 관련된 이유가 있는 경우)
- 기록에 여러 버전이 있는 경우 기록에 대한 내부 검사점 ID입니다.

감사에서 제외된 정보

테이블에 대한 감사를 활성화했음에도 불구하고 일부 업데이트는 감사되지 않습니다. 예를 들어 기록의 이력에는 132개의 업데이트가 표시되지만 감사된 업데이트는 7개만 표시될 수 있습니다.

감사에서 다음 정보는 제외됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 업그레이드에 의해 수행된 업데이트입니다.
- 업데이트는 임포트 세트를 통해 수행됩니다.
- 상위 또는 하위 테이블의 기록입니다.
- no_audit 딕셔너리 속성이 있는 필드입니다.
- 시스템 테이블은 속성 목록에 나열 *glide.ui.audit_deleted_tables* 되지 않습니다.
- sys_class_name 열과 sys_domain_id 열을 제외하고 sys_ 프리픽스로 시작하는 필드(시스템 필드)
- UI 페이지는 경우에 따라 감사 로그를 생성하지 않고 기록에 대한 업데이트를 트리거할 수 있습니다.
- 비활성 모니터가 기록을 터치할 때마다 이로 인해 인시던트에 대해 나열된 수백 개의 업데이트가 표시되지 않으며 노이즈로 인해 유용한 데이터가 익사합니다.
- 점수에 대한 퍼포먼스 분석 수동 변경.

테이블 감사

테이블을 감사하는 방법에 대한 지침은 다음 문서를 테이블에 대한 감사 구성참조하십시오.

기본적으로 시스템은 감사된 테이블의 모든 필드를 추적합니다. 다음 두 가지 방법 중 하나로 테이블의 필드 하위 집합을 감사할 수 있습니다.

- 전체 테이블에 대해 감사를 활성화한 다음 포함하지 않으려는 필드를 제외할 수 있습니다. 전부는 아니지만 대부분의 필드를 감사하려는 경우에 적합하며 제외 목록이라고 합니다. 자세한 내용은 감사 대상에서 필드 제외(제외 목록) 문서를 참조하십시오.
- 테이블에 대한 감사를 활성화할 수 있지만 지정된 필드에 대해서만 활성화할 수 있습니다. 적은 수의 테이블 필드만 감사하려는 경우에 적합하며 포함 목록이라고 합니다. 포함 목록을 사용하여 필드를 포함하는 방법에 대한 자세한 내용은 문서를 참조하십시오 감사에 테이블 필드 포함(포함 목록).

취소할 수 없는 감사 기록

새 기본 설정으로 트랜잭션을 취소할 때 감사 기록이 기록되지 않을 가능성을 줄입니다.

대상 기록 쓰기 작업과 동일한 트랜잭션에서 즉시 기록을 작성하도록 감사가 설정되었습니다. 대상 기록이 삭제되어도 감사는 **NCA** 테스트 감사 삭제 모듈에 계속 생성되고 유지됩니다.

주: 강화된 감사 프로세스는 기본적으로 사용하도록 설정됩니다. `glide.db.audit.lazy` 속성이 `True`로 설정되면 향상된 감사 프로세스가 비활성화됩니다.

Yokohama 릴리스 이전에는 트랜잭션이 취소되면 감사 가능한 특정 작업이 기록되지 않았습니다. 이는 플랫폼이 기록 변경 사이에 일부 작업을 실행하고 감사 생성 전에 취소되기 때문입니다. 그러나 이제 감사는 레코드가 변경된 직후에 생성되므로 감사가 기록되기 전에 취소된 트랜잭션으로 인해 작업이 중단될 가능성이 줄어듭니다.

이제 감사가 트랜잭션과 동일한 스레드에 기록됩니다. 이전 감사는 백그라운드 스레드에서 생성되었습니다. 이 변경은 `glide.db.audit.lazy` 속성의 기본값을 True에서 False로 재정의합니다. 대부분의 인스턴스가 새 기본값과 동작을 사용하기 시작하기 때문에 일반적으로 이 속성은 속성 테이블에 정의되지 않습니다. 일부 인스턴스에서는 이 속성이 이미 존재하고 True로 설정될 수 있으며, 이는 이러한 인스턴스가 이 변경 내용을 사용하여 동작을 감사할 수 없음을 의미합니다.

주: 업데이트를 활용하려면 이 속성을 삭제하는 것이 좋습니다.

테이블에 대한 감사 구성

테이블 감사를 활성화하여 테이블 필드 전체 또는 일부에 대한 변경 내용을 추적할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: admin.

주: 암호화된 필드는 설계에 의해 감사되지 않습니다. 이 동작은 구성할 수 없습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 딕셔너리.
   시스템에 딕셔너리 항목 목록이 표시됩니다. 목록에는 각 테이블에 대한 행과 테이블의 각 열(필드)에 대한 행이 포함됩니다.
2. 딕셔너리 항목 목록에서 감사할 테이블에 해당하는 행을 찾습니다(예: `cmdb_ci_computer`).
   올바른 테이블 이름, 열 이름에 대한 빈 항목 및 컬렉션유형이 있는 행을 찾아 테이블 자체의 행과 테이블의 열에 대한 행을 구분할 수 있습니다.
3. 테이블에 대한 딕셔너리 항목을 선택합니다.
   시스템에 딕셔너리 입력 양식이 표시됩니다.
4. 감사 확인란을 선택합니다.
5. 업데이트를 선택합니다.

다음에 수행할 작업
테이블의 테이블에 대한 포함 목록 감사 사용몇 개의 필드만 감사하려면 다음을 수행합니다.
일부 필드를 제외하고 대부분의 필드를 감사하려면 문서를 감사 대상에서 필드 제외(제외 목록)참조하십시오.

테이블에 대한 포함 목록 감사 사용

명시적으로 지정한 필드만 감사하려면 테이블을 활성화합니다. 이 기능은 감사된 테이블에서 적은 수의 필드만 감사하려는 경우에 유용합니다.

시작하기 전에
필요한 역할: 관리자
감사를 위해 테이블을 활성화해야 합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 딕셔너리.
   시스템에 딕셔너리 항목 목록이 표시됩니다. 목록에는 각 테이블에 대한 행과 테이블의 각 열(필드)에 대한 행이 포함됩니다.
2. 필요한 경우 속성 열을 표시하도록 목록 뷰를 사용자 지정합니다.
3. 딕셔너리 항목 목록에서 감사할 테이블에 해당하는 행을 찾습니다(예: `cmdb_ci_computer`).
   테이블 자체의 행과 테이블의 열에 대한 행은 올바른 테이블 이름, 열 이름에 대한 빈 항목 및 *.collection*
4. 해당 행의 속성 필드에 를 입력합니다 *audit_type=whitelist*.

다음에 수행할 작업
이 테이블에서 감사할 필드를 지정합니다.

감사 대상에서 필드 제외(제외 목록)

감사에서 해당 필드를 제외하여 감사된 테이블의 필드 하위 집합이 추적되지 않도록 합니다 Now Platform .

시작하기 전에
필요한 역할: 관리자
테이블의 필드를 감사에서 제외하려면 먼저 해당 테이블에 대한 감사를 활성화해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
감사 가능한 테이블에 있는 대부분의 필드를 감사하려면 제외 목록에 필드 집합을 추가합니다. 몇 개의 필드만 감사하려면 대신 포함 목록 절차를 따르십시오.

주: 저널 기반 필드에 대한 감사를 비활성화하면 활동 포매터와 같은 기능의 기능에 영향을 줄 수 있습니다. 자세한 내용은 KB0743142 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 딕셔너리.
2. 필요한 경우 속성 열을 표시하도록 목록 뷰를 사용자 지정합니다.
3. 감사에서 제외할 테이블 및 필드(열)에 해당하는 행으로 이동합니다.
4. 해당 행의 속성 열에 `no_audit`를 입력합니다.

감사에 테이블 필드 포함(포함 목록)

필드를 포함 목록에 추가하여 감사된 테이블의 필드 하위 집합을 추적합니다.

시작하기 전에
필요한 역할: 관리자
테이블의 필드를 포함 목록에 추가하려면 먼저 해당 테이블에 대한 감사를 활성화 하고 해당 테이블에 대해 포함 목록 감사를 활성화해야 합니다.

이 태스크 정보
소수의 감사 대상 테이블 필드만 감사하려면 포함 목록에 필드 세트를 추가합니다. 대부분의 필드를 감사해야 하고 몇 개만 제외해야 하는 경우에는 대신 제외 목록 절차를 따르십시오.

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 딕셔너리.
2. 필요한 경우 속성 열 표시를 포함하도록 목록 뷰를 사용자 지정합니다.
3. 포함 목록으로 이동할 테이블과 필드(열)로 이동합니다.
4. 속성 필드에 를 입력합니다*`audit=true`*.

시스템 테이블에 대한 감사 사용

sys_ 접두사가 있는 테이블에서의 삭제는 기본적으로 감사되지 않습니다. 이러한 테이블에서 삭제를 추적하려면 속성에 테이블 이름을 *`glide.ui.audit_deleted_tables`* 추가합니다. 삭제된 기록 재개 플러그인을 활성화하면 이 속성에 몇 가지 기본값이 추가됩니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 속성 > **UI** 속성.
2. 감사 삭제 속성이 있는 시스템 테이블 목록("sys_"로 시작되고, 쉼표로 구분됨)을 찾습니다.
3. 테이블 이름을 추가하거나 제거합니다. 테이블 이름은 공백 없이 쉼표로 구분해야 합니다.
4. 저장을 클릭합니다.

주: 감사에 대한 자세한 내용은 시스템 감사 테이블 이해를 참조하세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 감사 및 감사 관계 보기 변경 테이블

Now Platform 시스템 감사(sys_audit) 및 감사 관계 변경(sys_audit_relation) 테이블에서 감사된 기록에 대한 삽입 및 업데이트를 추적합니다.

Now Platform 감사 테이블을 추적합니다. 테이블을 추적하려면 딕 셔너 리 기록에서 감사 확인란을 선택하여 값을 true로 설정합니다. 기본적으로 업데이트 세트 테이블과 같은 시스템 테이블의 기록은 감사하지 않습니다.

주: 성능 문제와 무한 루프를 방지하기 위해 시스템은 시스템 감사 테이블 삽입에 의해 트리거되는 모든 비즈니스 규칙 또는 워크플로우를 건너뜁니다.

시스템 감사 테이블 열

다음 열이 sys_audit 테이블 기록에 나타납니다.

필드	설명
테이블 이름	감사 기록의 대상 테이블(예: "####")
필드 이름	감사 기록이 포함되어 있는 테이블의 열(예: "assigned_to")
문서 키	감사 기록과 연결된 원래 기록의 Sys_id(고유 기록 식별자)입니다.
사용자	변경을 생성한 사용자의 이름입니다. 주: 일부 자동화된 프로세스는 시스템 또는 게스트 사용자를 사용하여 기록에 변경 사항을 적용하고 추적합니다. 자세한 내용은 시스템 및 게스트 사용자를 참조하세요.
이전 값	이 sys_audit 기록으로 나타내는 필드 변경의 이전 값입니다. • 참조 필드: 변경된 기록의 고유한 sys_id 값입니다. • 날짜 및 시간 필드: 데이터베이스에 저장된 UTC(협정 세계시) 값입니다.
새 값	이 sys_audit 기록으로 나타내는 필드 변경의 새 값입니다. • 참조 필드: 변경된 기록의 고유한 sys_id 값입니다. • 날짜 및 시간 필드: 데이터베이스에 저장된 UTC(협정 세계시) 값입니다.

감사 관계 변경**(sys_audit_relation)** 테이블의 작동 방식

시스템 감사 [sys_audit] 테이블은 감사를 위해 플래그가 지정된 테이블의 참조 필드에 대한 변경 내용을 추적합니다. 이 활동에는 저널 필드 항목 및 이력 세트가 포함됩니다. 감사 관계 변경 [sys_audit_relation] 테이블은 sys_audit 테이블 기록과 감사된 기록이 시작된 소스 테이블 간의 관계 변경을 추적합니다. 또한 기록이 삭제되었을 수 있는 시기를 추적합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

-
- 테이블의 기록을 감사할 때마다 데이터를 기록하는 저장소의 다양한 원래 테이블 간에 관계가 생성됩니다. 이 관계 정보는 sys_history_set, sys_history_line 및 sys_journal 테이블에 저장됩니다.
- 감사된 테이블 기록과 관련된 필드를 삭제하면 sys_audit_relation 테이블에 삭제가 기록됩니다. 즉, 감사된 기록을 변경할 때마다 먼저 이전 요소를 삭제한 다음 새 문서 ID를 사용하여 sys_audit_relation 테이블에 관계를 생성합니다.

히스토리 세트에 대한 지식

사용자가 기록을 만들거나 이력을 볼 때 시스템은 감사 테이블에서 필요한 경우 이력 세트 기록을 자동으로 생성합니다.

기록이 감사 대상 테이블에 있으면 기록이 삽입되거나 사용자가 기록을 볼 때 해당 이력 세트가 생성됩니다.

주: 이력 세트를 사용하여 보고서를 생성하지 마십시오.

목록 뷰에 표시되는 이력 세트 기록에는 여러 정보 필드가 캡처됩니다.

목록 뷰 기록 필드

필드	입력 값
ID	이력이 기록되고 있는 기록의 문서 ID입니다.
테이블	이력이 기록되고 있는 기록에 대한 감사된 테이블입니다.
로드 시간	이력 세트를 생성하는 데 걸린 시간입니다.

감사 이력 기록 필드

필드	입력 값
레이블	변경된 필드의 레이블입니다.
이전	변경 전 값입니다.
신규	변경 후의 값입니다.
유형	항목이 일반 필드, 이메일 기록 또는 관계 변경 기록에 대한 것인지 나타냅니다.
업데이트 번호	이 필드가 변경된 횟수입니다. -1 값은 기록이 작성 또는 삭제된 시기를 나타냅니다.
업데이트 시간	변경 날짜 및 시간입니다. 주: 자동 생성된 이력 라인의 업데이트 시간이 특정 처리 상황에서 기록의 생성됨 또는 업데이트됨 시간과 일치하지 않습니다. 기록의 이력 세트를 처음 보면 초기 이력 라인 기록 세트가 자동으로 생성됩니다. 업그레이드의 파일 변경은 감사되지 않으므로 이 날짜 불일치는 다음과 같은 경우에 발생합니다. • 기록이 변경된 후 이력 세트를 볼 수 있지만 • 향후 업그레이드에서 다른 변경이 이루어지기 전.
사용자 이름	변경을 생성한 사용자의 이름입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

달력 뷰의 이력 세트

이력 세트가 활성화되면 이력 컨텍스트 메뉴 선택은 `sys_audit` 테이블이 아닌 이력 세트의 정보를 사용하여 채워집니다. 사용자의 관점에서는 동일한 사용자 인터페이스에서 동일한 기록 데이터를 사용할 수 있지만 정보가 저장되는 방식은 다릅니다.

이력 뷰는 달력 뷰를 포함하지만 이력 기록을 필터링하고 상호작용하기 위해 일반 목록 인터페이스를 사용하지 않으므로 다음을 수행할 수 있습니다.

- 기록 데이터 검색 및 필터링
- 이력 데이터를 익스포트하는 중입니다.

이력 세트 보기

이력 세트를 보는 방법에는 두 가지가 있으며, 컨텍스트 메뉴 작업 이력을 통해 액세스할 수 있습니다.

감사와 이력 세트의 차이점

감사 [sys_audit], 이력 세트 [sys_history_set] 및 이력 [sys_history_line] 테이블은 동일한 데이터를 저장하지만 용도가 다르고 데이터를 관리하는 방식이 다릅니다.

감사 **[sys_audit]** 테이블

감사 [sys_audit] 테이블은 시스템이 모든 기록에 대한 기록 정보를 저장하는 곳입니다. 이러한 기록은 영구적으로 보관되므로 관리자는 감사 기록의 이력을 항상 추적할 수 있습니다. 시간이 지남에 따라 감사 기록 수가 증가하면 감사 테이블에서 기록 정보를 직접 쿼리하는 것이 더 비효율적입니다. 실제로 기록 정보를 보려는 더 작은 하위 집합 기록에 대해서만 쿼리를 실행하는 것이 훨씬 더 효율적입니다.

이력 세트 **[sys_history_set]** 테이블

이력 세트 [sys_history_set] 테이블은 감사된 테이블에서 이력 정보가 있는 특정 기록을 식별합니다. 이력 [sys_history_line] 테이블에는 발생한 필드 값에 대한 실제 변경 내용이 저장됩니다.

- 사용자가 기록을 만들거나 이력을 요청하면 시스템은 감사 테이블에서 필요한 경우 이력 세트 및 이력 기록을 자동으로 생성합니다.
- 이력 세트 및 이력 기록은 시스템의 모든 변경 내용에 대한 전체 이력을 포함하는 대신 사용자가 이러한 정보를 생성하거나 요청한 기록에 대한 이력 정보의 최근 하위 집합만 포함합니다.
- 감사 데이터 외에도 이력 세트에는 저널 필드 항목을 포함하여 레코드 삽입 중에 설정된 정보도 포함됩니다. 기록을 작성하기 전에 작성하는 저널 필드 항목은 기록 작성 시 작성된 저널 항목과 동일한 방식으로 처리됩니다. 이러한 저널 항목은 관련 기록 자체와 동일한 생성 시간과 데이터에 의해 생성된 이력 세트에 나타납니다.

시스템은 다음을 기준으로 이력 세트와 이력 기록을 제한합니다.

- 테이블 클리너가 30일 동안 업데이트되지 않은 이력 세트 기록을 삭제하도록 합니다.
- 테이블 교대를 사용하여 7일마다 4개의 이력 테이블 사이를 교대합니다. 시스템은 28일이 지난 이력 기록을 삭제합니다.

나중에 누군가 기록 정보가 다시 필요한 경우 시스템은 감사 소스 기록에서 이를 재생성할 수 있습니다.

시스템이 이력 세트 기록을 생성하면 컨텍스트 메뉴 선택 이력 은 감사 기록이 아니라 이력 세트를 사용합니다. 사용자의 관점에서는 동일한 사용자 인터페이스에서 동일한 기록 데이터를 사용할 수 있지만 정보가 저장되는 방식은 다릅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이력에 대한 접근 제어

시스템 속성을 설정하여 감사 이력을 볼 수 있는 액세스 권한을 역할에 부여할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 속성 > 시스템.
2. *glide.history.role* 테이블에서 속성을 선택합니다.
3. 에서 기록에 *List of roles (comma-separated) that can access the history of a record*액세스하려는 사용자 역할을 선택합니다.
4. 저장을 선택합니다.

결과
읽기 권한이 없는 사용자가 기록 기록을 보는 경우 필드에 대한 변경 내용이 생략됩니다.

이력 항목 수 변경

기본적으로 이력에는 최대 250개의 이력 항목이 표시되지만 이 값을 변경할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

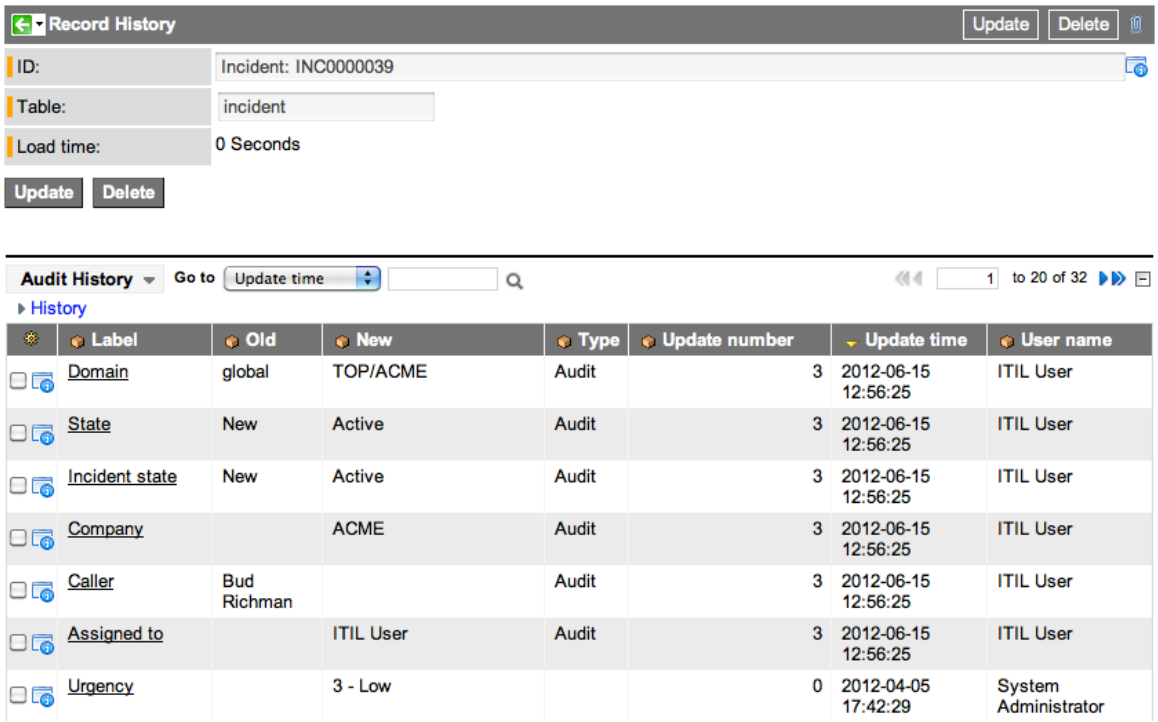
1. 다음으로 이동 모두 > 시스템 속성 > 시스템.
2. *glide.history.max_entries* 속성을 선택합니다.
3. *Maximum number of field entries displayed in record history, default is 250* 표시할 항목의 새 최대 수로 값을 설정합니다.

이력 목록

이력 목록은 변경 목록에서 각 변경 사항을 행으로 표시합니다.

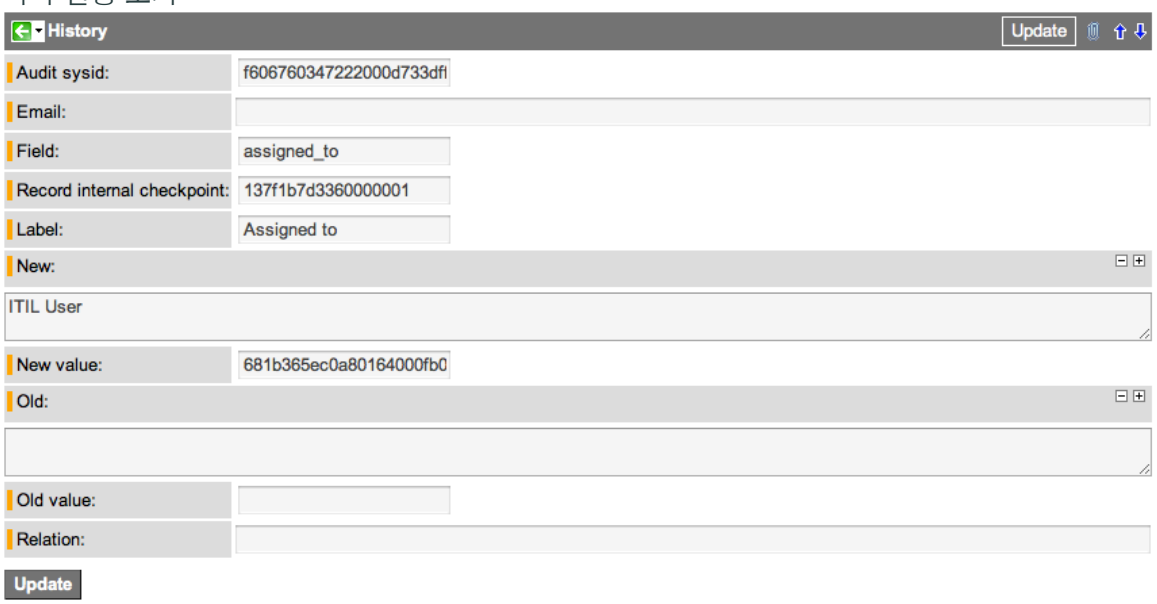
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이력 목록 뷰



변경에 대한 자세한 내용을 보려면 행 항목을 클릭하십시오.

목록 변경 보기



요구 사항

이력 목록을 보려면 다음 요구 사항을 충족해야 합니다.

감사

이력 목록을 보려면 테이블에 대한 감사를 활성화해야 합니다.

ACL

기본적으로 목록 이력 옵션은 관리자 사용자 역할을 가진 사용자만 사용할 수 있습니다. 비관리자가 이 옵션을 사용하도록 설정하려면 기록 이력 [sys_history_set] 테이블에 대한 읽기 권한을 부여하는 사용자 지정 ACL 규칙을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할

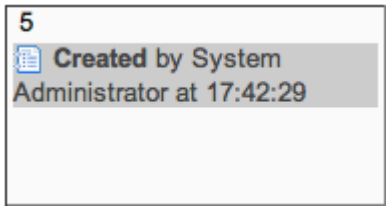
사용자가 가지고 있는 역할 중 하나 이상이 속성에 포함되어야 *glide.history.role* 하며, 여기에는 기본적으로 itil 역할이 포함됩니다.

이력 달력

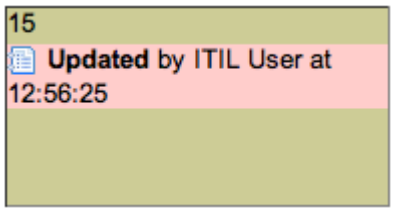
이력 달력에는 기록이 변경된 날, 변경한 사람, 시기가 표시됩니다.

이력 달력은 업데이트 번호별로 정렬됩니다. 각 사용자에게는 색상이 할당되므로 특정 사용자가 기록을 변경한 횟수를 한눈에 알 수 있습니다. 예:

시스템 관리자에 의해 변경



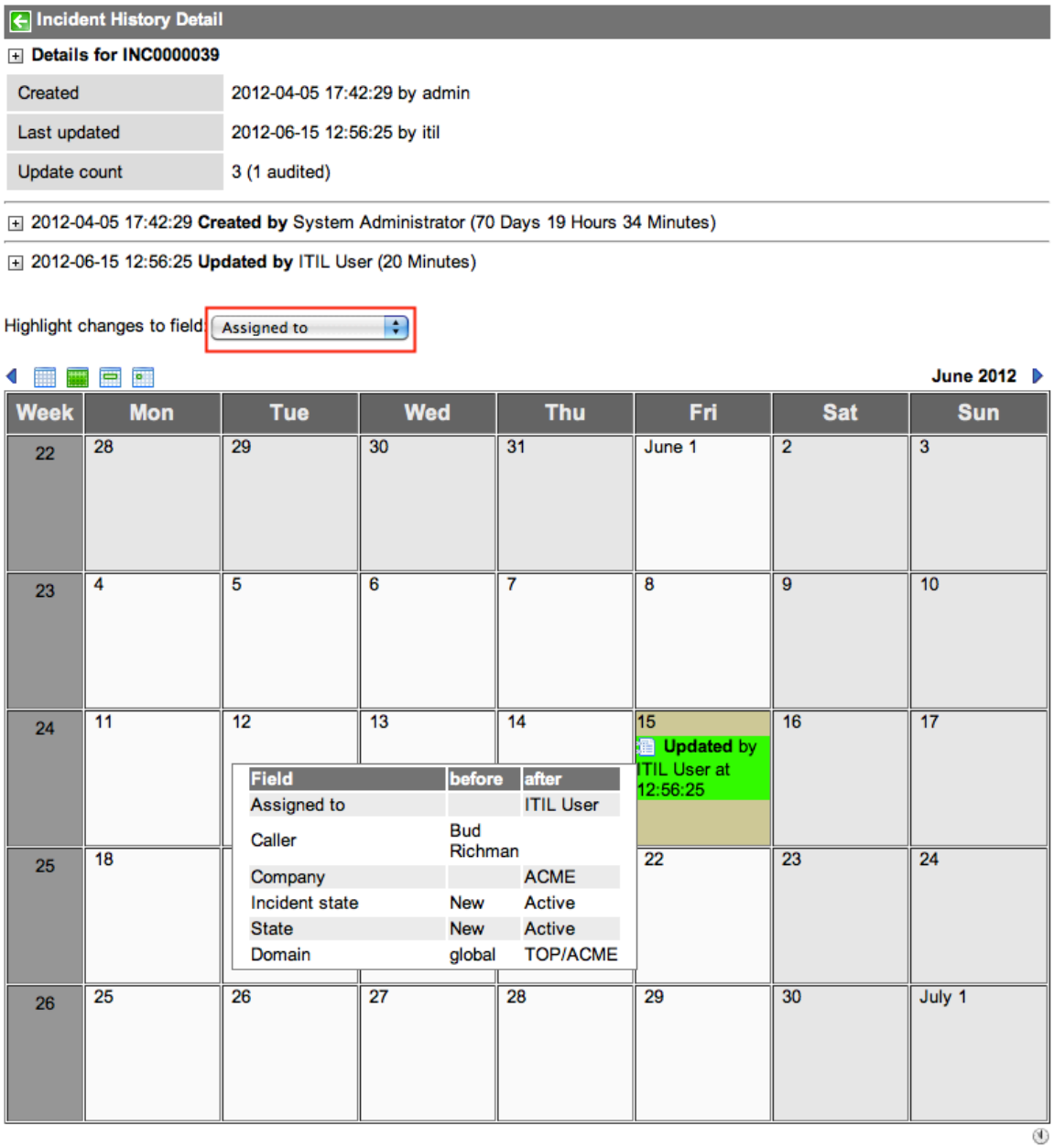
ITIL 사용자에 의한 변경



특정 필드에 대한 변경 내용을 강조 표시하려면 변경 내용 강조 표시 대상 필드 선택 상자에서 필드를 선택합니다. 이 선택 상자에서 필드를 선택하면 달력이 변경되어 필드가 변경된 시간을 강조 표시합니다. 강조 표시된 변경 내용 중 하나의 텍스트 위에 마우스를 올려놓으면 값의 변경 내용을 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

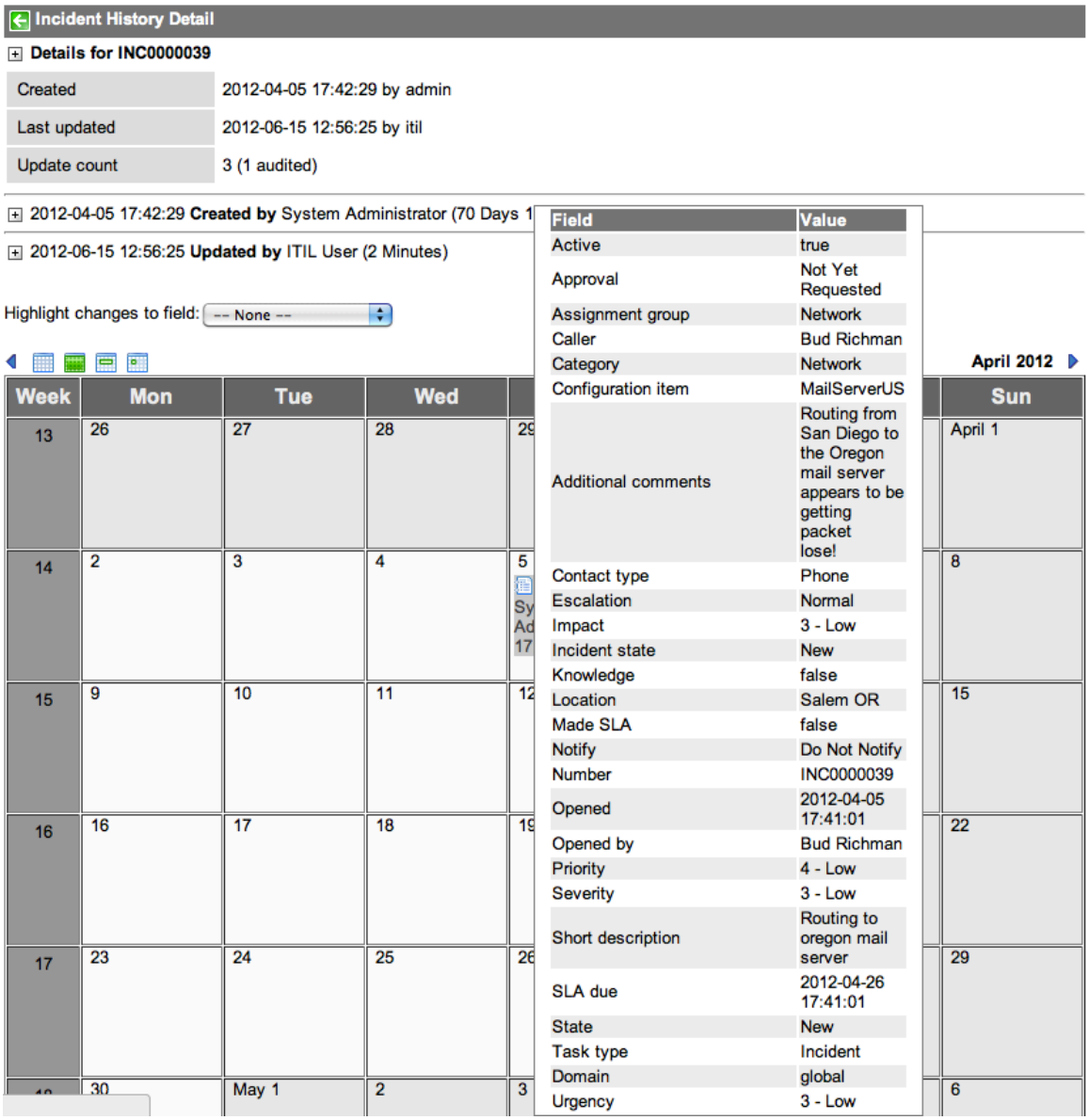
강조 표시된 변경 내용 보기



항목 내의 아이콘 위로 마우스를 가져가면 모든 값 변경 내용이 팝업에 표시됩니다. 이는 양식 윗부분에 표시되는 정보와 동일합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

달력 변경 내용 보기



일 번호를 클릭하면 해당 일의 변경 내용을 볼 수 있습니다. 왼쪽의 주 번호를 클릭하여 주간보기를 볼 수도 있습니다. 월별로 스크롤하여 변경 내용을 볼 수 있습니다.

이력 타임라인

CI 및 CI에 대한 관련 기록, 관계, 기준선 및 제안된 변경 사항에 대한 변경 타임라인을 볼 수 있습니다. 구성 항목 [cmdb_ci] 테이블의 CI 또는 이 테이블의 하위 항목(테이블에 대해 감사가 활성화된 경우)에 대해 타임라인을 사용할 수 있습니다.

필요한 역할: 이 뷰의 ACL은 기본적으로 `itil`로 설정된 시스템 속성에 정의된 *`glide.history.role`* 역할을 기반으로 합니다. 또한 사용자에게는 기본적으로 admin에게 부여되는 이력 세트 [sys_history_set] 테이블에 대한 읽기 권한이 있어야 합니다.

CI 이력을 볼 때 타임라인을 열 수 있습니다. 타임라인에 표시되는 기간, 시간 범위 및 속성을 지정할 수 있습니다. 특정 변경 세트에서 변경된 내용을 보거나 전체 CI를 보고 문제를 보다 잘 해결할 수 있습니다. 또한 CI의 관련 기록에 대한 변경 타임라인을 표시하고 언제든지 CI의 스냅샷을 익스포트 및 비교할 수 있습니다.

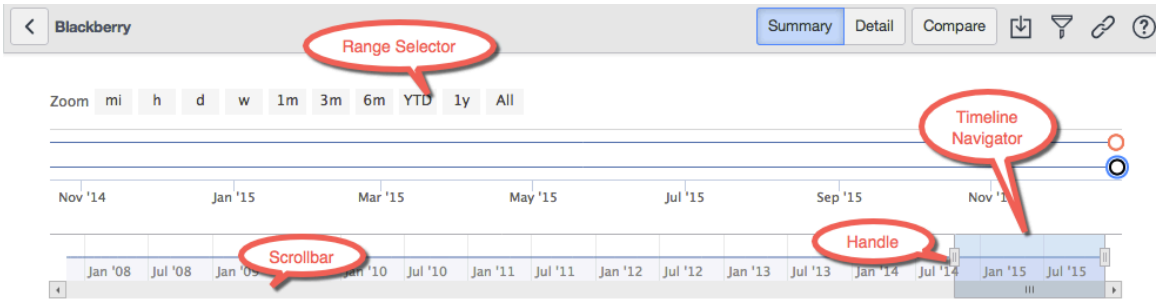
CI 변경 내용은 타임라인을 따라 다양한 모양과 색상의 거품으로 표시됩니다. 각 거품의 모양은 다른 유형의 변경을 나타내며 각 거품의 색은 변경 내용이 유효한지 여부를 지정합니다. CI 기준선은 검은색

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

원으로 표시되며, 그 위에 마우스를 갖다 대면 자세한 정보를 표시할 수 있습니다. 거품형 모양과 색상 정의를 표시하려면 **?** 아이콘을 클릭하고, 거품을 가리키면 변경 세트에 대한 세부 정보가 표시됩니다.

관계에 대한 변경은 변경 관리를 통해 적용된 경우에만 유효한 것으로 간주됩니다. 제안된 변경 프레임워크를 통해 변경이 적용된 경우 유효한 것입니다. 추가 유효성 검사 단계는 다음 문서를 참조하십시오 계획된 확인 스크립트 생성 또는 편집 .

이력 타임라인 뷰



타임라인 거품형



주: 계획된 시작 날짜가 없는 제안된 변경은 향후 시점에 배치됩니다.

타임라인 탐색기

타임라인 탐색기의 양쪽 끝에 있는 핸들을 사용하여 표시되는 기간을 늘리거나 줄입니다.

타임라인 네비게이터의 하단 부분을 클릭한 다음 네비게이터를 왼쪽이나 오른쪽으로 드래그하여 다른 기간으로 스크롤할 수 있습니다.

Zoom

기본적으로 마지막 달의 타임라인이 표시됩니다. 타임라인 위의 확대/축소 레이블 옆에 있는 다른 시간 간격을 선택할 수 있습니다. 분 단위에서 전체 데이터 기간까지 간격을 선택할 수 있습니다.

기간 동안 CI가 많이 변경되면 표시되는 거품이 너무 복잡해질 수 있습니다. 두 방법 중 하나로 거품을 확대하거나 축소하여 퍼뜨릴 수 있습니다.

- 타임라인의 시간 간격을 변경합니다. 시간 간격을 줄이면 확대되고 시간 간격을 늘리면 축소됩니다.
- 확대하려는 타임라인 섹션을 선택합니다.

속성 필터

표시되는 거품을 필터링할 수 있습니다. 기본적으로 모든 거품이 표시되며 이는 CI의 모든 속성에 대한 변경 사항을 나타냅니다. 선택한 속성이 변경된 거품만 표시하도록 뷰를 제한하고 선택하지 않은 속성만 변경된 거품을 제외할 수 있습니다.

상세 정보 및 요약 뷰는 필터 범위 내에서 변경된 속성을 강조 표시합니다. 변경된 속성은 연한 파란색으로 강조 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요약 뷰에서 CI의 모든 속성을 포함하거나 변경된 속성만 포함하도록 선택할 수 있습니다. 요약 뷰에 모든 속성을 표시하도록 선택하면 변경된 속성이 변경되지 않은 속성 앞에 나열됩니다.

요약 뷰

요약 뷰에는 각 거품으로 표시된 CI의 스냅샷이 표시됩니다. 각 스냅샷에는 변경 세트에 따라 CI 필드와 관계에 대한 변경 내용이 표시됩니다. 변경 전후의 이전 값과 새 값, 그리고 추가되거나 삭제된 모든 관계가 표시됩니다.

스냅샷 화면의 양쪽에 있는 **>** 및 **<** 버튼을 사용하여 다음 및 이전 변경 세트 기록을 시간 순서대로 스크롤합니다.

상세 정보 뷰

상세 정보 뷰에는 거품에 해당하는 CI의 스냅샷이 표시됩니다. 각 스냅샷에는 속성 필터 범위 내에 있는 필드가 포함되며, 연한 파란색 배경으로 변경된 속성을 표시합니다. 거품을 클릭하여 CI의 해당 스냅샷을 표시합니다. 표시되는 데이터는 읽기 전용입니다.

양쪽에 있는 **>** 및 **<** 버튼을 사용하여 다음 및 이전 변경 세트 기록을 시간 순서대로 스크롤합니다.

관련 기록에 대한 변경 타임라인 보기

CI 기록의 변경 타임라인에서 CI의 관련 기록에 대한 변경 타임라인을 볼 수도 있습니다.

시작하기 전에

필요한 역할 : admin

- 대상 테이블: CI 기록은 구성 항목 [cmdb_ci] 테이블 또는 이 테이블의 하위 항목에 있어야 합니다.
- 감사: CI가 포함된 테이블에 대해 활성화해야 합니다.

프로시저

1. CI의 타임라인을 엽니다.
2. 관련 기록 아이콘을 선택하고 확인하려는 관련 기록 목록에서 관련 기록을 선택합니다.
   관련 기록 아이콘을 다시 클릭하면 관련 기록 타임라인이 표시됩니다.

결과

CI의 관련 기록에 대한 변경 타임라인은 CI의 타임라인 바로 위에 표시됩니다. 모든 관련 기록을 선택 취소하면 관련 기록 타임라인이 숨겨집니다.

다음에 수행할 작업

관련 기록 타임라인의 변경 거품 위에 마우스를 올려 놓으면 변경된 속성의 날짜 및 수와 같은 변경 관련 상세 정보가 표시됩니다. 포커스 시간 간격을 변경하거나 확대 또는 축소하면 CI 타임라인과 관련 기록 타임라인에 동시에 영향을 줍니다.

CI의 스냅샷 익스포트

CI의 타임라인에서 스냅샷을 익스포트할 수 있습니다.

시작하기 전에

CI는 구성 항목 [cmdb_ci] 테이블 또는 이 테이블의 하위 항목에 있어야 합니다. CI가 포함된 테이블에 대해 감사를 활성화해야 합니다.
필요한 역할: admin.

이 태스크 정보

CI의 스냅샷을 XML, PDF(포털) 또는 PDF(가로) 형식으로 익스포트할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. CI의 타임라인을 엽니다.
2. CI의 스냅샷을 익스포트할 시간을 나타내는 거품을 선택합니다.
3. 익스포트 아이콘()  을 클릭합니다.
4. 내보내기에 사용할 파일 형식을 선택합니다.
   파일을 시스템에 다운로드하여 볼 수 있습니다.

CI 스냅샷 비교

타임라인의 서로 다른 두 지점에서 CI의 속성과 관계를 비교할 수 있습니다.

시작하기 전에
CI는 구성 항목 [cmdb_ci] 테이블 또는 이 테이블의 하위 항목에 있어야 합니다. CI가 포함된 테이블에 대해 감사를 활성화해야 합니다.
필요한 역할: admin.

프로시저

1. CI의 타임라인을 엽니다.
2. 비교를 클릭합니다.
3. 시작 날짜 및 종료 날짜를 선택합니다.
4. 비교를 클릭합니다.

참조 필드의 변경 내용 추적

관리자는 참조 필드 표시 값에 대한 변경 사항을 추적할 수 있습니다.

참조 필드는 ID 값만 저장하므로 시스템은 일반적으로 ID 값이 변경될 때만 변경 사항을 감사할 수 있습니다. 기본적으로 시스템은 참조 필드 표시 값이 변경될 때 변경 사항을 감사하지 않습니다.

다음과 같은 상황을 생각해 볼 수도 있습니다. 사용자가 자신의 이름을 Jane Smith에서 Jane Miller로 변경합니다. 사용자 이름은 사용자 테이블의 표시 값이므로 Jane Smith에 대한 이전 참조는 대신 Jane Miller를 참조합니다. 관리자가 기존 사용자 기록의 이름을 업데이트하기만 하면 감사 및 이력 기록에는 새 이름 Jane Miller만 표시됩니다. 기본적으로 시스템에서는 원래 사용자 이름으로 변경한 내용과 새 사용자 이름으로 변경한 내용을 구분할 수 있는 방법을 제공하지 않습니다.

감사 정책에서 사용자 이름 변경을 추적해야 하는 경우 다음을 수행할 수 있습니다.

- 새 이름에 대한 새 사용자 기록을 생성하고 이전 사용자 기록을 비활성화합니다. 시스템은 이전 사용자 이름에 대한 감사 기록을 보존하고 새 사용자 이름으로 향후 감사 기록을 생성합니다.
- 사용자 지정 필드와 비즈니스 규칙을 만들어 이전 이름과 이름 변경 날짜를 저장합니다. 시스템은 이 정보를 사용하여 감사 및 이력 기록에서 적절한 이름을 구성할 수 있습니다.

삽입 추적

일반적인 인스턴스에서 삽입이 감사 테이블 크기의 80% 이상을 차지할 수 있기 때문에 기본적으로 시스템은 삽입에 대한 감사 레코드를 생성하지 않습니다.

삽입을 추적하지 않으면 성능이 향상되고 감사 테이블이 훨씬 작아집니다. 관리자는 속성을 *true*로 설정하여 삽입 감사를 활성화할 수 있습니다*glide.sys.audit_inserts*.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CI 관계 추적

CI 관계(CI 관계, CI/사용자 관계 또는 CI/그룹 관계)에 대한 변경 사항은 변경이 수동인지 또는 의 결과 디스커버리인지에 관계없이 변경된 관계의 양쪽에 있는 항목의 이력에 나타납니다.

예를 들어 컴퓨터 알파에 컴퓨터 베타와의 CI 관계에서 사용됨이 있는 경우 알파의 기록에는 베타와의 관계가 설정된 시기의 기록이 있으며 마찬가지로 베타의 기록에도 알파와의 관계가 설정된 시기의 기록이 있습니다. 이 예에서는 일부 CI 관계가 설정된 후 관계 중 하나가 제거될 때 표시되는 이력을 보여줍니다.

CI 관계 이력

⊟ 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)

작성된 글머리 기호는 CI, 사용자 또는 그룹이 작성된 날짜를 나타냅니다. 마지막 활동 글머리 기호는 관계가 마지막으로 변경된 시기를 나타냅니다. 일부 또는 모든 CI 관계 유형에 대한 CI 관계 이력을 표시하지 않으려면 CI 관계 테이블(CI 관계 [`cmdb_rel_ci`], CI/사용자 관계 유형 [`cmdb_rel_user_type`] 또는 그룹 관계 [`cmdb_rel_group`])에 대한 감사를 비활성화하여 해제할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

높은 보안 설정

높은 보안 설정은 인스턴스에서 사용할 수 있는 여러 보안 옵션을 참조합니다.

높은 보안 설정 탐색



높은 보안 설정의 기능과 비즈니스 가치를 알아봅니다.

높은 보안 설정 활성화



높은 보안 설정을 활성화합니다.

높은 보안 설정 구성



높은 보안 설정을 구성하는 방법을 이해합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

높은 보안 설정 탐색

높은 보안 설정은 인스턴스에서 사용할 수 있는 여러 보안 옵션을 참조합니다.

높은 보안 설정 모듈은 새 인스턴스에서 기본적으로 활성화되어 있는 높은 보안 설정 플러그인을 통해 활성화됩니다. 인스턴스에서 높은 보안 설정이 활성화되어 있지 않은 경우 높은 보안 설정 요청 활성화를 참조하십시오. 이 플러그인에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 높은 보안 플러그인 사용 〔보안 센터 1.3에서 업데이트됨〕. 다음 유형의 높은 보안 설정에 대한 속성을 사용할 수 있습니다.

- 기본 속성 값: 관리 및 감사를 위해 모든 중요한 보안 설정을 한 위치로 중앙 집중화하여 플랫폼의 보안을 강화합니다.
- 기본 거부 속성: 테이블 접근에 대한 기본 보안 동작을 제어하는 보안 관리자 속성을 제공합니다.
- 보안 관리자 역할: 주요 보안 설정 및 자원의 수정을 방지하는 역할을 제공합니다. 보안 관리자 역할은 관리자 역할에 상속되지 않으며 명시적으로 할당해야 합니다.
- 상승된 권한: 보안 관리자 역할을 가진 사용자가 일반 사용자의 컨텍스트에서 작동하고 필요한 경우 더 높은 보안 역할로 상승할 수 있습니다.
- 속성 접근 제어: 보안 관리자가 속성을 읽고 쓰는 데 필요한 역할을 설정할 수 있습니다.
- 시스템 로그: 읽기 전용입니다.
- 접근 제어 규칙: 사용자가 접근할 수 있는 데이터와 접근 방법을 제어합니다.

주:

- 또한 높은 보안 설정은 상황별 보안 플러그인이 아직 활성화되지 않은 경우 이를 자동으로 활성화합니다. 또한 플랫폼 보안 설정 - 높음은 인스턴스의 보안을 강화하는 컨텍스트에서 설정과 기능을 제공합니다.
- 인스턴스 보안 강화 설정 컨텐츠에는 보안 관련 시스템 속성 및 플러그인에 대한 자세한 설명과 준수 값이 포함되어 있습니다 Now Platform.
- 이러한 각 속성에 대한 자세한 내용은 다음 문서를 참조하십시오 강화 설정.

높은 보안 설정 속성을 설정하거나 변경하는 방법에는 두 가지가 있습니다.

- 다음으로 이동 시스템 보안 > 높은 보안 설정.

  높은 보안 속성 페이지의 옵션은 예 또는 아니오입니다.

- **sys_properties.list**로 이동하여 설정하거나 변경하려는 속성을 검색합니다.

  시스템 속성 테이블 〔sys_properties.list〕의 옵션은 **true** 또는 **false**입니다.

속성 접근 제어

높은 보안 설정이 활성화되면 속성 [sys_properties] 테이블에 두 개의 열이 추가로 작성됩니다.

- **read_roles**: 이 속성의 모든 필드를 읽을 수 있는 역할 이름의 목록이며 콤마로 구분됩니다.
- **write_roles**: 이 속성의 모든 필드를 쓰거나 수정할 수 있는 역할 이름의 목록으로, 쉼표로 구분됩니다.

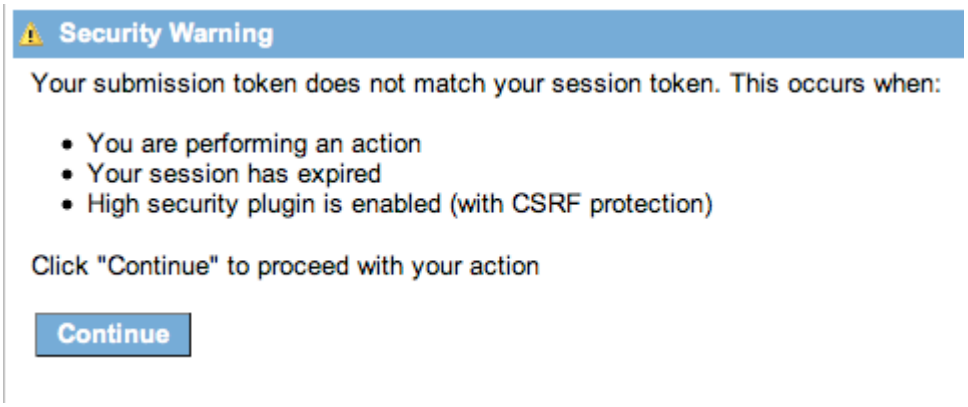
속성 테이블에 나열된 속성에는 admin **read_roles** 와 **security_admin write_roles** 이 있습니다. 관리자 역할을 가진 사용자는 속성 값을 보고 읽을 수 있지만 수정하려면 security_admin 역할로 격상해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

알림

높은 보안 설정을 활성화하면 보안 경고 메시지도 활성화됩니다. 다음은 승인 후 나타나는 메시지의 예입니다.

보안 경고 알림



높은 보안 설정 속성

속성	설명	기본값	인스턴스 보안 강화 설정
glide.ui.escape_text	사용자 인터페이스의 파서 수준으로 XML 값을 이스케이프하십시오. 리플렉션되고 저장된 교차 사이트 스크립팅 공격을 방지합니다. 이 속성은 서비스 포털에서 적용할 수 없습니다. 주: 이 속성은 이후 릴리스에서 Vancouver 기본적으로 **true**로 설정되며 관리자가 변경할 수 없습니다. 속성을 변경해야 하는 사용 사례의 경우 고객 지원에 문의하십시오.	예	이스케이프 XML 마크업 [Security Center 1.3에서 업데이트됨]
glide.ui.escape_all_script	기본적으로 Jelly JavaScript `<![CDATA[<script type="text/javascript">]]>` 태그 내의 모든 표현식을 강제로 이스케이프합니다.	예, 새 인스턴스에서 가능합니다.	이스케이프 Jelly 스크립트[Security Center 1.3 및 1.5에서 업데이트됨]

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명	기본값	인스턴스 보안 강화 설정
	`]]> ###<![CDATA[<script>` type 속성이 비어 있거나 `## text/javascript, text/ecmascript, application/javascript, application/ecmascript` 또는 `application/x-javascript`인 경우에만 이스케이프를 적용합니다.		
glide.ui.rotate_sessions	보안 취약성을 줄이기 위해 HTTP 세션 식별자를 순환합니다. 참조: http://www.owasp.org/index.php/Session_Management#	예 주: 1회 사용자 인증(SSO)에 SAML 2.0 플러그인을 사용하는 경우 이 속성을 아니요로 설정합니다. 그렇지 않으면 인스턴스와 ID 제공자 간에 수행되는 세션 정보 공유에 방해가 됩니다.	HTTP 세션 식별자 교대 fiers .
glide.ui.secure_cookies	보안 세션 쿠키 사용: 추가 쿠키 보안을 사용하도록 설정합니다. 예인 경우 엄격한 세션 쿠키 유효성 검사가 적용됩니다.	예	세션 쿠키의 엄격한 보안 적용[Security Center 1.3에서 업데이트됨]
glide.security.password_reset.uri	모바일 암호 재설정의 경우 사용자가 암호를 잊으셨습니까? 단추를 클릭할 때 이동되는 URL입니다.		안 함
glide.security.strict.updates	양식을 제출하는 동안 인바운드 트랜잭션의 보안을 다시 한 번 확인하십시오 (양식 작성 시 권한을 항상 확인합니다).	예	인바운드 트랜잭션 다시 확인 [Security Center 1.3에서 업데이트됨]

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명	기본값	인스턴스 보안 강화 설정
	주: 이 속성은 이후 릴리스에서 Vancouver 기본적으로 **true**로 설정되며 관리자가 변경할 수 없습니다. 속성을 변경해야 하는 사용 사례의 경우 고객 지원에 문의하십시오.		
glide.security.strict.actions	실행 전에 UI 작업의 조건을 확인합니다. 일반적으로 조건은 양식을 렌더링하는 동안에만 확인됩니다.	예	실행 전 UI 작업 조건 확인
glide.security.use_csrf_token	보안 토큰 사용을 식별하고 수신 요청을 확인할 수 있습니다. 이 토큰은 교차 사이트 요청 위조 공격을 방지하는 데 사용됩니다.	예	안티-CSRF 토큰 사용 [Security Center 1.3의 새로운 기능, 1.5에서 업데이트, 2.0에서 제거됨]
glide.ui.escape_html_list_field	목록 뷰에 HTML 필드용 HTML 이스케이프	예	목록 뷰에서 HTML 이스케이프 [Security Center 1.3 및 1.5에서 업데이트됨]
glide.html.escape_script	HTML 필드에 JavaScript 태그를 이스케이프합니다.	예	이스케이프 JavaScript [Security Center 1.3에서 업데이트됨]
glide.ui.forgetme	로그인 페이지에서 메일 주소 저장 확인란을 제거합니다.	예	내용 저장하기 제거
glide.smtp.auth	사용자 이름 및 암호 속성으로 SMTP 서버에 인증합니다. 주: 이 속성은 더 이상 사용되지 않습니다.	예	
glide.script.use.sandbox	축소된 권한 샌드박스 내에서 클라이언트가 생성한 스크립트 (AJAXEvaluate	예	스크립트 샌드박스 사용[Security Center 1.3에서 업데이트됨]

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명	기본값	인스턴스 보안 강화 설정
	및 쿼리 조건)를 실행합니다. 예인 경우 클라이언트 호출 가능 확인란이 예로 설정된 해당 비즈니스 규칙 및 스크립트 포함만 사용할 수 있으며 일부 백엔드 API 호출은 허용되지 않습니다. 자세한 내용은 스크립트 샌드박스 속성 구성 문서를 참조하십시오.		
glide.soap.strict_security	수신 SOAP 요청에 엄격한 보안을 적용합니다. 수신 SOAP 요청이 테이블과 필드 접근을 위해 보안 관리자를 거쳐야 하며 SOAP 사용자가 웹 서비스 사용을 위한 올바른 역할을 가지고 있는지 확인합니다.	예	SOAP 요청 엄격한 보안 적용[Security Center 1.3에서 업데이트됨]
glide.basicauth.required.wsdl	수신 WSDL 요청에 대해 권한 부여가 필요합니다. 주: 들어오는 WSDL 요청에 인증을 요구하지 않기로 할 경우 접근 제어(ACL) 규칙을 수정하여 게스트 사용자도 WSDL 컨텐츠를 이용할 수 있게 해야 합니다.	예	WSDL 요청에 대해 인증 필요 [Security Center 1.3 및 1.5에서 업데이트됨]
glide.basicauth.required.csv	수신 CSV 요청에 대해 기본 인증 필요 .	예	csv 요청에 대해 권한 부여 필요[Security Center 1.3에서 업데이트됨]
glide.basicauth.required.excel	수신 Excel 요청에 대해 기본적인 권한 부여가 필요합니다.	예	Excel 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명	기본값	인스턴스 보안 강화 설정
glide.basicauth.required.importprocessor	수신 임포트 요청에 대해 기본적인 권한 부여가 필요합니다.	예	임포트 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]
glide.basicauth.required.pdf	수신 PDF 요청에 대해 기본적인 권한 부여가 필요합니다.	예	PDF 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]
glide.basicauth.required.rss	수신 RSS 요청에 대해 기본적인 권한 부여가 필요합니다.	예	RSS 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]
glide.basicauth.required.scriptedprocessor	수신 스크립트 요청에 대해 기본적인 권한 부여가 필요합니다.	예	스크립트 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]
glide.basicauth.required.soap	수신 SOAP 요청에 대해 기본적인 권한 부여가 필요합니다.	예	SOAP 요청에 대해 권한 부여 필요 [Security Center 1.3, 1.5 및 2.0에서 업데이트됨]
glide.basicauth.required.unl	수신 업로드 요청에 대해 기본적인 권한 부여가 필요합니다.	예	언로드 요청에 대해 권한 부여 필요 [Security Center 1.3에서 업데이트됨]
glide.basicauth.required.xml	수신 XML 요청에 대해 기본적인 권한 부여가 필요합니다.	예	XML 요청에 대해 권한 부여 필요[Security Center 1.3에서 업데이트됨]
glide.basicauth.required.xsd	수신 XSD 요청에 대해 기본적인 권한 부여가 필요합니다.	예	XSD 요청에 대해 인증 필요 [Security Center 1.3에서 업데이트됨]
glide.cms.catalog_uri_relative	/ess/catalog.do에 URI 매개변수의 상대 링크를 적용하십시오. 예인 경우, 매개변수를 사용하여 *uri* 상대 URL만 /ess/catalog.do 페이지를 통해 허용됩니다. 아니요인 경우 모든 URL이 허용되어 외부의 권한이 없는 콘텐츠에 링크될 수 있습니다.	예	상대 링크 적용 [Security Center 1.3 및 1.5에서 업데이트됨]
glide.set_x_frame_options	모든 UI 페이지에 대해 X-Frame-	예	x-frame-options 구현: SAMEORIGIN 보안

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명	기본값	인스턴스 보안 강화 설정
	Options 응답 헤더를 SAMEORIGIN으로 설정하려면 이 속성을 활성화합니다. X-Frame-Options HTTP 응답 헤더는 브라우저가 또는 〈iframe〉에서 페이지를 <frame> 렌더링할 수 있도록 허용해야 하는지 여부를 나타내는 데 사용할 수 있습니다. 사이트는 이 속성을 사용하여 콘텐츠가 다른 사이트에 포함되지 않도록 함으로써 클릭재킹 공격을 방지할 수 있습니다. https://developer.mozilla.org/en/the_x-frame-options_response_header		헤더 [Security Center 1.3에서 업데이트됨〕
glide.ui.attachment.download_mime_types	브라우저에서 인라인으로 렌더링되지 않는 쉼표로 구분된 첨부 파일 MIME 유형의 목록입니다. 교차 사이트 스크립팅 공격을 방지합니다. 예를 들어, `text/html` 은 HTML 파일을 브라우저에서 인라인으로 보는 대신 첨부 파일로 클라이언트에 다운로드하도록 강제합니다.	`### / HTML, ### / svg, ### / svg + xml`	다운로드 가능한 MIME 유형 제한 [Security Center 1.3 및 2.0에서 업데이트됨〕
glide.security.groupby_acl_check	이 속성을 사용하면 그룹의 실제 데이터를 기반으로 그룹 이름에 대해 GroupBy 작업에 대한 ACL 검사가 수행됩니다.	예	안 함
glide.security.diag_txns_only	예인 경우 관리자 사용자 또는 허용된 IP 주소의 사용자만 `stats.do`, `threads.do` 및	아니요	성능 모니터링 액세스 제한 [Security Center 1.3에서 업데이트됨〕

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명	기본값	인스턴스 보안 강화 설정
	`replication.do` 에 액세스할 수 있습니다.		
glide.ui.security.codetag.allow_script	임베디드 HTML(〔코드〕 태그 사용)에 JavaScript 태그를 포함시킬 수 있습니다. 주: 이 속성은 이후 릴리스에서 Vancouver 기본적으로 **true**로 설정되며 관리자가 변경할 수 없습니다. 속성을 변경해야 하는 사용 사례의 경우 고객 지원에 문의하십시오.	아니요	내장된 HTML 코드 사용 안 함[Security Center 1.3에서 업데이트됨]
glide.script.allow.ajaxevaluate	AJAXEvaluate 프로세서를 사용하도록 설정합니다. *AJAXEvaluate* API 호출을 사용하면 클라이언트가 서버에서 임의의 스크립트를 보내고 실행할 수 있습니다.	아니요	AJAXEvaluate 사용 안 함
glide.login.autocomplete	브라우저에서 로그인 양식의 암호 필드에 자동 완성 기능을 사용할 수 있습니다.	아니요	

다음 속성은 sys_properties 테이블에 정의되어 있지만 높은 보안 설정 페이지에는 표시되지 않습니다.

속성	설명	기본값	인스턴스 보안 강화 설정
com.glide.communications.httpclient.verify_hostname	원격 SSL 호스트에서 제공하는 호스트 이름 및 인증서 체인을 검증하십시오. MITM(중간자) 공격으로부터 보호합니다. 자세한 내용은 Kubernetes	예	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명	기본값	인스턴스 보안 강화 설정
	스포크 설정을 참조하십시오. 주: 이 속성은 com.glide.communications.trustmanager_trust_all 속성을 재정의합니다.		
glide.basicauth.required.schema	인바운드 테이블 스키마 요청에 대해 기본적인 권한 부여가 필요합니다.	예	안 함
glide.security.csrf_previous.허용	만료된 보안 토큰 사용을 식별하고 수신 요청을 확인할 수 있습니다. 이 토큰은 교차 사이트 요청 위조 공격을 방지하는 데 사용됩니다.	거짓	안 함
glide.security.csrf_previous.time_limit	보안 토큰이 만료되는 시간(초)입니다. 이전 CSRF 토큰이 유효한 기간을 제어할 수 있습니다. 사용자 세션이 만료될 때 속성이 사용되고 이 속성에서 설명한 시간 범위 내에 있지 않으면 *glide.security.csrf_previous.allow* 보안 토큰도 만료됩니다. 이 토큰은 교차 사이트 요청 위조 공격을 방지하는 데 사용됩니다.	86400 주: 초 단위의 값입니다. 1일에 해당합니다.	안 함
glide.security.csrf.strict_validation.mode	CSRF 토큰이 일치하지 않는 경우 사용자가 요청을 다시 제출할 수 없도록 CSRF 토큰에 엄격한 유효성 검사를 적용합니다.	거짓	사용자가 CSRF 유효성 검사를 바이패스하기 위한 경고를 수락하지 못하도록 방지 〔보안 센터 1.3 및 1.5에서 업데이트됨〕
com.glide.security.check_unsanitized_html	필드 할당 및 전역 수준에서 translated_html 필드의 정리 동작을 적용합니다.	적용	안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트 샌드박스 속성 구성

스크립트 샌드박스 속성()*glide.script.use.sandbox*을 사용하여 권한이 제한된 샌드박스 내에서 클라이언트가 작성한 스크립트를 실행합니다.

시스템 내에는 클라이언트가 평가를 위해 서버에 스크립트를 보낼 수 있는 두 가지 경우가 있습니다.

- 필터 및/또는 쿼리: `assigned_to=javascript:getMyGroups()`와 같은 필터를 서버에 보내는 것은 합법적입니다.
- 시스템 API: *`API ## AJAXEvaluate`*를 사용하면 클라이언트가 서버에서 임의의 스크립트를 실행하고 응답을 받을 수 있습니다.

스크립트 샌드박스 속성()*glide.script.use.sandbox*을 활성화하면 이 두 엔트리포인트 중 하나를 통해 평가되는 스크립트가 축소된 권한 샌드박스 내에서 실행되며 다음과 같은 특징이 있습니다.

- 클라이언트 호출 가능으로 표시된 비즈니스 규칙만 샌드박스 내에서 사용할 수 있습니다.
- 클라이언트 호출 가능으로 표시된 스크립트 포함만 샌드박스 내에서 사용할 수 있습니다.
- 특정 API 호출(대부분 직접 DB 액세스를 처리하는 호출에 국한되지 않음)은 허용되지 않습니다.
- 샌드박스 내에서 데이터를 삽입, 업데이트 또는 삭제할 수 없습니다. 예를 들어 *`current.update()`*에 대한 모든 호출은 무시됩니다.

주: 이 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 스크립트 샌드박스 사용[Security Center 1.3에서 업데이트됨] .

스크립트 샌드박싱이 활성화된 경우 이러한 메서드는 클라이언트 작성 스크립트에서 허용되지 않습니다.

제한된 방법

클래스	메서드
GlideRecord	• *`delete##()`* • *`deleteRecord()`* • *`getRowCount()`* • *`##()`* • *`####()`* • *`updateMultiple()`*
GlideSystem(gs)	• *`addErrorMessage()`* • *`addInfoMessage()`* • *`addMessage()`* • *`### # ()`* • *`flushMessages()`* • *`getEscapedProperty()`* • *`getProperty()`* • *`##()`*

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제한된 방법

클래스	메서드
	• *## ##()* • *## ##()* • *setProperty()* • *setRedirect()* • *setReturn()* • *workflowFlush()*
ScopedGlideRecord	• *delete##()* • *deleteRecord()* • *##()* • *####()* • *updateMultiple()*
ScopedGlideSystem(gs)	• *addErrorMessage()* • *addInfoMessage()* • *###()* • *### # ()* • *####Now()* • *getProperty()* • *getSessionToken()* • *##()* • *setRedirect()*
GlideDate Glide날짜/시간 글라이드타임	• *###()* • *addDays()* • *addDaysLocalTime()* • *addDaysUTC()* • *addMonthsLocalTime()* • *addMonths()* • *addSeconds()* • *addWeeks()* • *addYears()* • *compareTo()* • *getByFormat()* • *getDate()* • *getDayOfWeek()*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제한된 방법

클래스	메서드
	• *getDayOfWeekUTC* • *getDayOfWeekLocalTime()* • *getDayOfMonth()* • *getDayOfMonthLocalTime()* • *getDayOfMonthNoTZ()* • *getDayOfWeek()* • *getDayOfWeekLocalTime()* • *getDayOfWeekUTC()* • *getHourOfDayLocalTime()* • *getHourOfDayUTC()* • *getDaysInMonth()* • *getDaysInMonthUTC()* • *getDaysInMonthLocalTime()* • *getDisplayValueInternal ()* • *getDisplayValue()* • *getHourLocalTime()* • *getLocalDate()* • *getLocalTime()* • *getMinutesLocalTime()* • *getMinutesUTC()* • *getMonthLocalTime()* • *getMonthNoTZ()* • *getMonthUTC()* • *getNumericValue()* • *getSeconds()* • *getTime()* • *getTZOffset()* • *getValue()* • *getYear()* • *getUserTimeZone()* • *getWeekOfYearLocalTime()* • *## getWeekOfUTC()* • *getYearUTC()* • *getYearLocalTime()* • *isDST()* • *onOrAfter()*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제한된 방법

클래스	메서드
	• *onOrBefore()* • *setDayOfMonthUTC()* • *setDisplayValue()* • *setMonth()* • *setNumericValue()* • *setTZ()* • *setValue()* • *setValueUTC()* • *##()* • *toString()*
GlideSchedule	• *###()* • *isInSchedule()* • *##()* • *when##()*

주: 시스템 속성을 `false`로 설정하여 스크립트 샌드박스와 함께 GlideSystem(gs) 메서드 *log(), logError()* 및 *logWarning()*을 *glide.security.sandbox_no_logging* 활성화할 수 있습니다.

스크립트 샌드박싱을 활성화하지 않고 시스템을 실행하는 경우 이러한 제한 사항이 적용되지 않습니다.

주: 이 속성은 높은 보안 설정 플러그인을 활성화할 때 기본적으로 활성화됩니다. 플러그인 외부에서 이 속성을 활성화하지 마십시오.

속성	기본값
축소된 오른쪽 "샌드박스"에서 클라이언트가 작성한 스크립트(*AJAXEvaluate* 및 쿼리 조건)를 실행하십시오. 활성화되면 클라이언트 호출 가능 확인란이 true로 설정된 해당 비즈니스 규칙 및 스크립트 포함만 사용할 수 있고 특정 백엔드 API 호출은 허용되지 않습니다.	활성화됨(샌드박스 사용 중).

높은 보안 설정 활성화

높은 보안 설정 플러그인은 모든 새 인스턴스에서 기본적으로 활성화됩니다. 인스턴스에서 활성 상태가 아닌 경우, 플러그인을 요청할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 없음

기존 인스턴스에서 높은 보안 설정을 활성화 하기 전에:

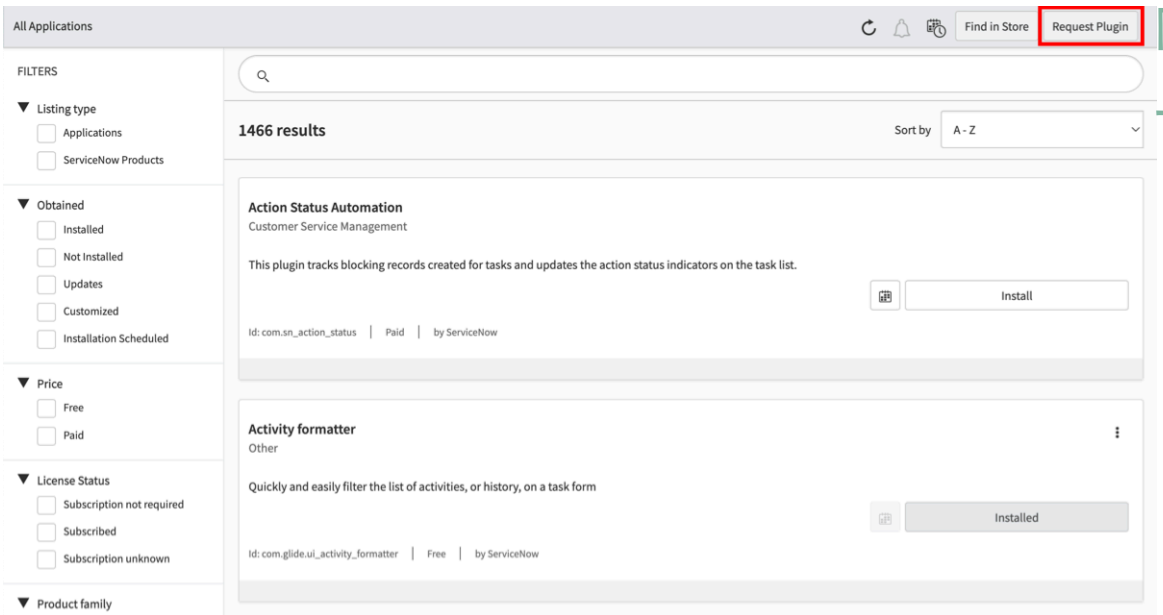
1. 다음 정보를 검토하여 새 동작을 이해하십시오.
   - 접근 제어 목록 규칙
   - 높은 보안 설정
   - 기본 거부 속성
2. 비프로덕션 인스턴스에서 플러그인을 활성화합니다. 최근 프로덕션의 복제가 바람직합니다.
3. 수정된 기능, 특히 추가된 ACL 및 기본 거부 기능을 테스트합니다. 시스템이 예상대로 작동할 때까지 테스트를 계속합니다. 사용자가 예상 자원에 액세스할 수 없는 경우 액세스 권한을 부여하는 적절한 역할과 ACL 규칙이 있는지 확인합니다.
4. 프로덕션에 적용할 수 있도록 필요한 변경 사항의 업데이트 세트를 생성합니다.

주: 이 플러그인에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 높은 보안 플러그인 사용 (보안 센터 1.3에서 업데이트됨) .

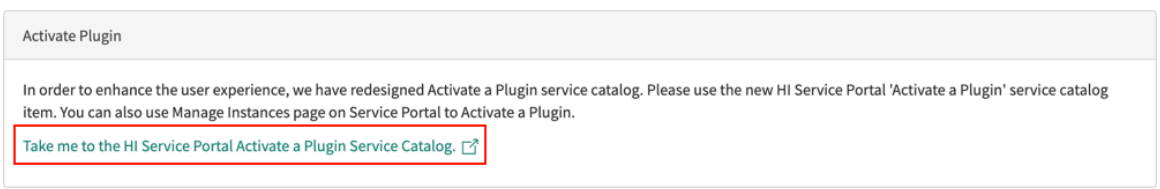
필요한 역할: admin

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 모든 애플리케이션 페이지에서 플러그인 요청을 선택하여 Now Support의 플러그인 활성화 양식을 엽니다.



3. Now Support에서 Now Support 서비스 포털 서비스 카탈로그에 액세스하는 링크를 선택합니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 인스턴스를 선택합니다.
5. 작업 > 플러그인 활성화를 선택합니다.
6. 플러그인 활성화 양식에서 다음 정보를 입력합니다.

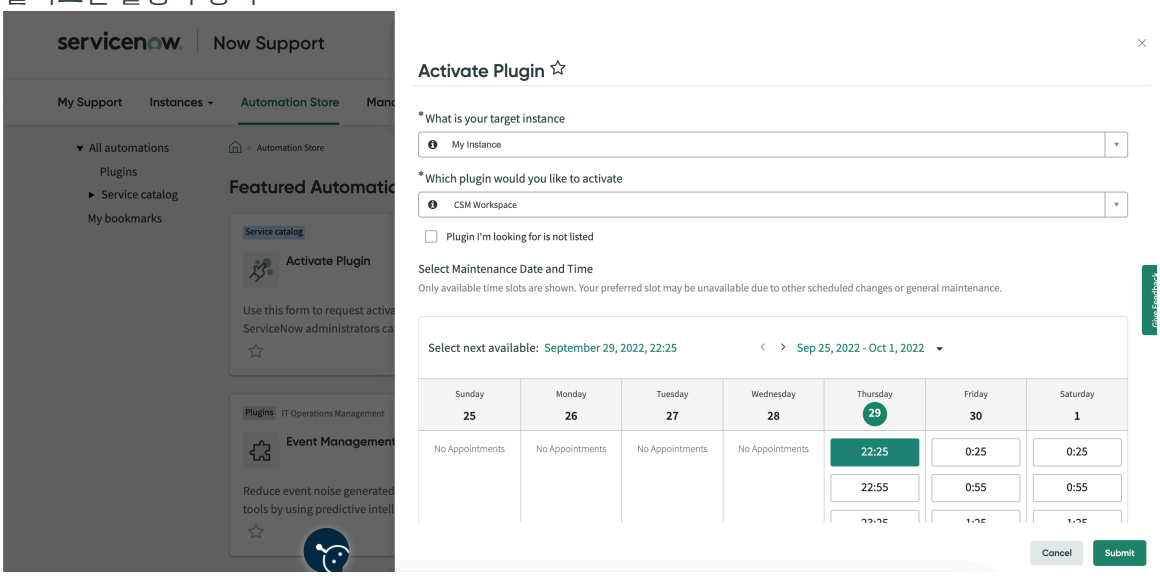
플러그인 활성화 양식

필드	설명
대상 인스턴스는 무엇입니까?	플러그인을 활성화할 인스턴스입니다.
어떤 플러그인을 활성화하시겠습니까?	활성화할 플러그인의 이름입니다. 주: 시스템에서 원하는 플러그인을 나열하지 않거나 OEM 또는 온프레미스 인스턴스에서 플러그인을 활성화하는 경우 찾고 있는 플러그인이 목록에 없음 확인란을 선택한 다음 플러그인 이름을 입력합니다.
유지관리 날짜 및 시간 선택	플러그인을 활성화하는 날짜 및 시간입니다. 주: 플러그인은 미국 태평양 시간대의 모든 영업일에 두 번(오전과 저녁에 각각 한 번씩) 활성화됩니다. 특정 시간에 플러그인을 활성화해야 하는 경우 이유/설명 필드에 요청을 입력합니다.

Example

예를 들어, 내 인스턴스라는 인스턴스에서 CSM Workspace 플러그인을 활성화하는 다음 양식을 참조하십시오.

플러그인 활성화 양식



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 제출을 선택합니다.
   플러그인 요청에 대한 자세한 내용은 다음을 참조하십시오. 의 서비스 카탈로그 [KB0751715] 문서에서 플러그인 요청 Now Support 지식베이스.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VPN(가상 사설망)

VPN(가상 사설망)을 사용하여 인터넷을 통해 인스턴스를 외부 데이터 소스와 통합합니다.

탐색



VPN(가상 사설망)의 기능과 비즈니스 가치를 알아봅니다.

활성화



VPN(가상 사설망)을 활성화합니다.

구성



VPN(가상 사설망)을 구성하는 방법을 이해합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

VPN(가상 사설망) 살펴보기

VPN(가상 사설망)을 사용하여 인터넷을 통해 인스턴스를 외부 데이터 소스와 통합합니다.

내 IP 정보

LDAP(Lightweight Directory Access Protocol) 또는 HTTPS와 같은 암호화된 프로토콜을 사용하는 통합을 구성할 때는 인터넷을 전송 메커니즘으로 사용하는 것이 좋습니다.

그러나 데이터 센터와 비즈니스 네트워크 간에 사이트 간 IPSEC(인터넷 프로토콜 보안) VPN(가상 사설망) 연결을 사용하도록 지시하는 보안 또는 네트워크 아키텍처 요구 사항이 있을 수 있습니다. VPN은 인스턴스와 네트워크 간에 필요한 암호화된 통신을 지원합니다.

⚠ 경고:

VPN 터널이 시작되면 사이트 간 연결로 작동합니다. 즉, 인프라의 엔드포인트가 암호화 도메인이라고 하는 IP 주소를 받습니다. 이 공용 IP는 동일한 데이터 센터 내의 모든 인스턴스에서 액세스할 수 있습니다.

예를 들어 내부 웹 서비스가 있고 VPN 터널을 설정하는 경우 인스턴스는 내부 엔드포인트뿐만 아니라 동일한 데이터 센터의 다른 모든 인스턴스에도 연결할 수 있습니다.

VPN 연결

VPN 인프라는 ServiceNow VPN 종료 지점 역할을 하는 Cisco ASA(Adaptive Security Appliance) 디바이스 쌍을 사용합니다.

인스턴스와 네트워크 간의 VPN은 기존 네트워킹 하드웨어를 활용하여 통신을 지원합니다. 하드웨어를 설치할 필요는 없습니다. 각 고객은 고유한 구성을 가지고 있기 때문에 인스턴스에는 유연한 VPN 솔루션이 있습니다. 인스턴스는 Checkpoint, Juniper, Nortel 및 기타 IPSEC VPN 지원 장치에 대한 터널을 구축했습니다.

인스턴스와 네트워크 간의 VPN 연결은 네트워크로의 암호화된 트래픽 흐름을 지원하기 위해 생성됩니다. VPN을 사용하는 통합에는 기본 프로토콜의 일부로 암호화가 없는 경우가 많습니다. 예를 들어 VPN을 통한 LDAP , 인터넷을 통한 LDAP, VPN을 통한 HTTP, 인터넷을 통한 HTTPS가 있습니다.

네트워크는 VPN 연결을 통과하는 인바운드 - ServiceNow 통합 또는 최종 사용자와 ServiceNow 간 트래픽을 허용하지 않습니다. 이 제한된 통신에는 플랫폼에 대한 최종 사용자 액세스, 플랫폼 관리, 웹 서비스 통합 및 MID Server 를 사용하도록 구성된 기타 통합이 포함됩니다. 인스턴스에 대한 모든 인바운드 통신은 HTTPS를 사용하여 인터넷을 통해 수행되어야 합니다. 이 구성은 암호화된 통신 채널을 제공합니다. IP 액세스 제어와 함께 암호화 채널은 이 트래픽 흐름에 대한 보안 요구 사항을 충족합니다.

VPN 통신을 위한 주소

내부 ServiceNow 네트워크 또는 네트워크의 다른 내부 IP 주소 체계와 충돌하거나 겹치지 않도록 하려면 암호화 도메인의 모든 터널링된 트래픽은 터널의 양쪽에서 RFC-1918이 아닌 주소를 사용해야 합니다.

ServiceNow 는 네트워크에 대한 쿼리 소스의 단일 IP 주소를 제공합니다. 인스턴스와 통합되는 각 호스트에 대해 RFC-1918이 아닌 NAT(네트워크 주소 변환) 주소를 제공해야 합니다. 이러한 공용 주소는 조직에서 소유해야 합니다. 터널 내에서 타사 주소를 사용할 수 없습니다. 또한 암호화 도메인에는 VPN 피어의 IP 주소가 포함되지 않아야 합니다.

중복 터널

터널에 대한 이중화를 구축하는 방법에는 두 가지가 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 두 피어 모두에서 동일한 암호화 도메인을 사용합니다. 이 방법이 선호됩니다.
- 각 피어 뒤에 다른 암호화 도메인을 사용합니다.

첫 번째 방법에서는 각 피어 뒤에 동일한 NAT 주소를 제공하여 해당 주소를 사용하여 서버에 대한 연결 경로를 만들어야 합니다. 서버에 대한 경로는 동일한 물리적 시스템이거나 동일한 서비스를 제공하는 미러일 수 있습니다. 이 방법을 사용하면 인스턴스가 기본 또는 보조 터널이 활성 상태인지 여부에 관계없이 동일한 IP 주소를 사용하여 서버에 연결합니다. 서버가 두 개 이상인 경우 추가 서버에 대해 동일한 구성표를 따릅니다. 이 방법은 사용자에게 가장 투명한 방법을 제공하므로 권장됩니다.

두 번째 방법은 인스턴스에 중복성을 제공하도록 구성해야 합니다. 예를 들어 터널이 LDAP에 사용되는 경우 인스턴스에 중복 LDAP 서버를 제공할 수 있습니다. 이 방법을 사용하려면 인스턴스가 보조 서버에 연결을 시도하기 전에 첫 번째로 구성된 LDAP 서버에 대한 연결이 시간 초과되어야 합니다. 이러한 추가 시간 지연으로 인해 이 솔루션은 첫 번째 옵션을 달성할 수 없는 경우에만 구현해야 합니다. 또한 인스턴스에서 모든 서비스를 중복으로 구성할 수 있는 것은 아닙니다. LDAP 이외의 용도로 VPN 터널을 사용 중이고 중복성이 필요한 경우, 구성이 여러 주소를 지원할 수 있는지 확인하거나 위의 첫 번째 옵션을 참조하십시오.

VPN 사용의 대안

이러한 대안은 인스턴스를 데이터 센터의 자원 ServiceNow 에 연결하는 더 간단한 방법을 제공하고 더 나은 암호화를 제공합니다. 또한 VPN 터널에 문제가 있는 경우 사용자가 인스턴스를 사용할 수 없도록 하는 등 VPN 가동 중단으로 인해 발생할 수 있는 문제를 방지할 수 있습니다.

SSO(Single Sign-On) 및 MID Server

VPN을 사용하여 LDAP 서버를 인스턴스에 연결하는 대신 인증에 SSO(Single Sign-On)를 사용하고 사용자 데이터 동기화를 위해 MID Server를 사용하는 것이 좋습니다. LDAP 이외의 통합의 경우 인증서 기반 암호화 사용을 고려하십시오.

MID 서버에서 LDAP 수신기를 사용하여 거의 실시간으로 사용자 테이블을 동기화할 수 있습니다.

이 접근 방식의 장점은 구성 및 유지 관리할 방화벽 구멍, 경로, VPN 터널 또는 기타 특수 네트워크 설정이 없다는 것입니다. SSO/MID Server 솔루션은 완전한 LDAP 통합을 달성하기 위한 가장 유연하고 안전하며 비용 효율적인 방법입니다.

SSL을 통한 LDAP

VPN 터널을 사용하는 또 다른 방법은 인터넷을 통해 직접 LDAPS(LDAP Over SSL)를 구성하는 것입니다. 읽기 전용 도메인 컨트롤러를 구성하고 인스턴스의 소스 주소와 선택한 대상 포트만 사용하여 DMZ에서 인스턴스를 잠글 수 있습니다. LDAP에 대한 포트는 인스턴스에서 구성할 수 있으므로 원하는 경우 포트 주소 변환(PAT)을 수행할 수 있습니다. LDAPS를 사용하면 암호화된 채널을 통해 인스턴스에 업로드되는 인증서를 제어할 수 있습니다(문서 참조 인스턴스에 인증서 업로드). 인증서 없이는 패킷을 암호화하거나 해독할 수 없습니다.

이 접근 방식의 장점은 더 강력한 암호화 및 암호 해독 메커니즘을 제공한다는 것입니다. VPN은 비밀번호와 유사한 조정된 사전 공유 키를 사용하여 인터넷에 있는 두 피어 간의 트래픽만 암호화하고 해독할 수 있습니다. LDAPS는 응용 프로그램 계층에서 종단 간 더 긴 암호화 경로와 IPSec 터널에서 사용하는 미리 공유된 키보다 훨씬 더 복잡한 인증서를 제공합니다.

VPN 설정

VPN 요청이 제출된 시점부터 VPN 빌드를 완료하는 데 일반적으로 1주일 미만이 소요됩니다. 인스턴스와 조직의 중복 요구 사항을 지원하기 위해 최소 2개 및 최대 4개의 VPN이 프로비저닝됩니다 (활성 사이트에서 활성 사이트로 또는 활성 사이트에서 DR 사이트로 등).

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 도메인은 가능한 한 구체적으로 지정하는 것이 좋습니다. 암호화 도메인에는 통합에 필요한 특정 호스트만 포함하는 것이 가장 좋습니다. 암호화 도메인이 크면 라우팅 불일치(VPN과 인터넷)가 발생할 수 있습니다.

VPN을 생성하기 위해 인스턴스는 다음을 수행합니다.

1. 각 데이터 센터의 VPN 피어 및 호스트 주소를 제공합니다.
2. 두 데이터 센터에서 네트워크로 필요한 VPN 연결을 구축합니다. 이중화 및 재해 복구(DR) 요구 사항을 지원하기 위해 VPN을 두 개의 데이터 센터에서 두 개의 네트워크로 프로비저닝할 수 있습니다.

이 인스턴스는 여러 지리적 리전 또는 자회사에 연결하기 위해 고객 네트워크에 여러 VPN 터널을 구축하는 것을 지원하지 않습니다. 여러 VPN 터널을 사용하는 대신 자체 내부 네트워크 내에서 사이트 간 라우팅, 트래픽 분산 또는 트래픽 셰이핑을 수행해야 합니다.

VPN 서비스 활성화

프로비저닝, 수정 또는 일반적인 질문을 포함하여 모든 VPN 요청의 경우 서비스 카탈로그 VPN 요청 양식을 사용하십시오.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동합니다: https://support.servicenow.com/now?draw=case
2. 자동화 저장소 탭을 선택합니다.
3. 왼쪽의 트리를 사용하여 모든 자동화 > 서비스 카탈로그 > 클라우드 인프라.
4. **VPN** 요청 선택
5. 적절한 VPN 요청 유형을 선택합니다.
6. 질문에 대답합니다.
   질문은 선택한 요청 유형에 따라 다릅니다.
7. 제출을 클릭합니다.

결과
요청이 제출 ServiceNow 되면 네트워크 엔지니어와 협력하여 VPN이 트래픽을 성공적으로 전달하는지 테스트하고 확인합니다. 질문에 적시에 답변할 수 있도록 이 과정에서 VPN 관련 질문에 답하십시오.

VPN 통신을 위한 주소 구성

내부 ServiceNow 네트워크 또는 다른 고객의 내부 IP 주소 체계와의 충돌 또는 겹침을 방지하기 위해 인스턴스는 암호화 도메인의 모든 터널링된 트래픽이 터널의 양쪽에서 비 RFC-1918 주소를 사용하도록 요구합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
인스턴스는 네트워크에 대한 쿼리 소스에 대해 단일 IP 주소를 제공합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

인스턴스와 통합되는 각 호스트에 대해 RFC-1918이 아닌 NAT(네트워크 주소 변환) 주소를 제공합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플랫폼 개인정보 보호

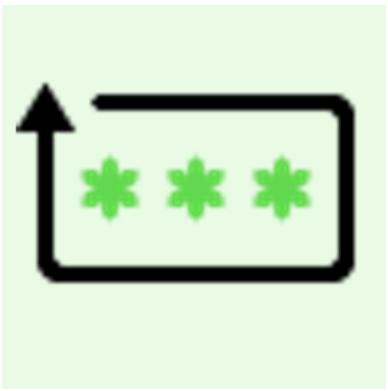
개인정보 보호를 사용하면 인스턴스에서 중요한 데이터를 마스킹할 수 있습니다.

데이터 개인정보 보호



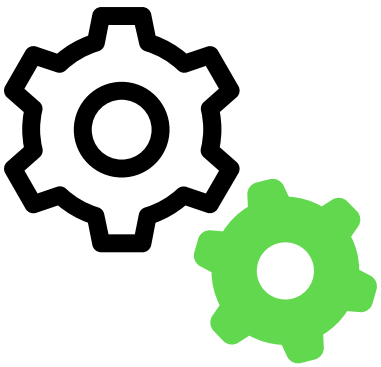
Data Privacy를 사용하면 중요한 데이터를 분류할 수 있으며 프로덕션 인스턴스의 사용자 데이터에서 개인 식별 정보(PII)를 제거하고 비프로덕션 인스턴스의 데이터를 익명화할 수 있습니다.

데이터 디스커버리



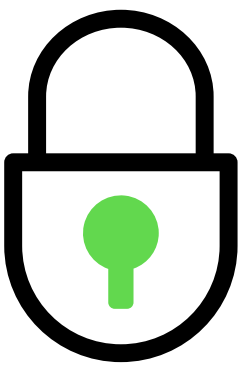
데이터 검색을 사용하여 인스턴스 내에서 분류, 보호 또는 보고할 중요한 데이터를 식별합니다.

데이터 분류



미리 정의되었거나 사용자 정의된 데이터 분류를 사용하여 데이터를 유형별로 그룹화합니다. 할당된 데이터 분류 관리자 또는 감사자 역할이 있는 경우 다양한 데이터 분류를 관리하거나 인스턴스 내에서 각종 데이터의 현재 상태를 시각적으로 분석할 수 있습니다.

데이터 익명화



데이터 익명화는 식별할 수 없으며 데이터 개인정보 보호 규정을 더 준수하도록 데이터를 쉽게 변환할 수 있는 방법을 제공합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 개인정보 보호

Data Privacy를 사용하면 중요한 데이터를 분류할 수 있으며 프로덕션 인스턴스의 사용자 데이터에서 개인 식별 정보(PII)를 제거하고 비프로덕션 인스턴스의 데이터를 익명화할 수 있습니다. 익명화되면 사용자 데이터는 더 이상 규제 대상 비공개 정보로 간주되지 않습니다.

데이터 개인정보 보호 살펴보기



데이터 개인정보 보호에 대해 자세히 알아보십시오.

데이터 개인정보 보호 구성



데이터 개인정보 보호 구성 방법을 알아봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 개인정보 보호 담당 역할



데이터 개인정보 보호의 역할에 대한 자세한 내용을 참조하십시오.

데이터 개인정보 보호 고급 기능



데이터 개인정보 보호의 고급 기능에 대해 알아봅니다.

데이터 개인정보 보호 살펴보기

Data Privacy를 사용하면 중요한 데이터를 분류할 수 있으며 프로덕션 인스턴스의 사용자 데이터에서 개인 식별 정보(PII)를 제거하고 비프로덕션 인스턴스의 데이터를 익명화할 수 있습니다. 익명화되면 사용자 데이터는 더 이상 규제 대상 비공개 정보로 간주되지 않습니다.

데이터 개인정보 보호의 중요성과 분류 및 익명화를 통해 민감한 정보를 보호하기 위해 기업이 취할 수 있는 조치에 대해 설명합니다. 데이터 개인정보 보호 저장소 애플리케이션을 사용하여 기본 대시보드 및 기능에 대한 개요를 제공합니다.

개발자는 비프로덕션 인스턴스의 데이터로 작업하여 구현이 예상대로 작동하는지 확인해야 합니다. 프로덕션 인스턴스에서 데이터를 임포트하는 것은 프로덕션을 시뮬레이션하는 유용한 방법이지만 보안 위험이 있습니다. 관리자는 데이터 개인정보 보호를 사용하여 비프로덕션 환경에서 안전하게 작업할 수 있도록 개발자에게 개인 정보가 포함되지 않은 데이터를 제공할 수 있습니다.

데이터 분류

인스턴스에 있는 데이터 유형의 민감도 수준에 따라 결정되는 미리 정의된 기준에 따라 중요한 데이터를 식별하고 분류합니다. 데이터 민감도 수준은 분류된 각 유형의 데이터를 처리하는 방법을 결정하는 데 도움이 됩니다. 기본 수준 데이터 개인정보 보호와 함께 제공되는 몇 가지 사전 정의된 클래스가 있습니다. 데이터 개인정보 보호의 분류 섹션을 사용하여 인스턴스 내에서 데이터에 레이블을 지정하고 그룹화합니다. 클래스를 추가하고, 데이터 클래스 구조를 보고, 데이터를 분류합니다. 미리 정의되었거나 사용자 정의된 데이터 분류를 사용하여 데이터를 유형별로 그룹화합니다.

데이터 개인정보 보호 스토어 애플리케이션을 사용하여 데이터를 분류하는 방법에 대해 설명합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 데이터 익명화

관리자는 모든 사용자 또는 일부 사용자의 모든 정보를 익명화할지 여부를 정의합니다. 익명화되면 선택한 사용자 기록에 대한 데이터가 임의의 값 또는 사용자가 정의한 값으로 대체됩니다. 값을 대체할 때 다양한 기법을 사용하여 데이터 구조를 보존할 수 있습니다.

데이터 개인정보 보호 저장소 애플리케이션을 사용하여 데이터를 익명화하는 방법에 대해 설명합니다.

데이터 개인정보 보호 옵션

- 데이터 개인정보 보호(클래식): 먼저 데이터 분류 앱을 사용하여 사전 정의되거나 사용자 정의된 데이터 분류를 사용하여 데이터를 유형별로 그룹화합니다. 그런 다음 데이터 개인정보 보호 기술과 작업을 생성하여 PII를 익명화합니다.
- Data Privacy (스토어 앱): 데이터 개인정보 보호 앱 내에서 모든 데이터를 분류하고 익명화합니다.

고려 사항

- 분류된 데이터만 익명화할 수 있습니다. 데이터 클래스 및 분류에 대한 자세한 내용은 데이터 분류(클래식) 또는 데이터 분류 스토어 앱을 참조하세요.
- 로그 및 기타 감사 데이터의 PII는 익명화되지 않습니다.
- 구조화된 데이터만 익명화할 수 있습니다. 저널 필드, 코멘트, 첨부 파일 및 부분 텍스트가 PII를 나타낼 수 있는 기타 필드와 같은 구조화되지 않은 데이터는 익명화되지 않습니다. 자세한 내용은 익명화를 지원하는 필드 유형 문서를 참조하십시오.
- 1회 사용자 인증(SSO) 시스템과 통합하면 정보 소스 시스템에서 사용자 정보를 재동기화할 수 있습니다. sys_user 데이터의 비식별화의 영속성을 보장하는 메커니즘은 없습니다. 사용자 관리 및 sys_users에 대한 자세한 내용은 사용자 관리를 참조하십시오.

도메인 분리 및 데이터 개인정보 보호

도메인 분리는 데이터 개인정보 보호에 대해 지원되지 않습니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 지원 없음

- 도메인 필드가 데이터 테이블에 존재할 수 있지만 데이터를 관리할 비즈니스 논리가 없습니다.
- 이 수준은 도메인으로 구분된 것으로 간주되지 않습니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원을 참조하십시오.

관련 정보

서비스 제공자용 도메인 분리

익명화를 지원하는 필드 유형

데이터를 익명화할 때 지원되는 필드 유형을 확인합니다.

주: 분류된 모든 필드 유형을 익명화에 사용할 수 있는 것은 아닙니다.

일부 고위험 필드 유형은 테이블에 설명된 대로 기본적으로 꺼져 있습니다. 필드에 대한 자세한 내용은 필드 유형을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

익명화를 지원하는 필드 유형

필드 유형	기본적으로 사용 가능
오디오	아니요
조건	아니요
condition_string	아니요
통화	예
10진수	예
due_date	예
부동	예
glide_date	예
glide_date_time	예
glide_duration	아니요
glide_time	예
HTML	아니요
아이콘	아니요
정수	예
ip_addr	아니요
ip_address	아니요
일지	예
journal_input	예
journal_list	예
경도	예
name_values	아니요
percent_complete	아니요
phone_number_e164	예
가격	예
문자열	예
string_full_utf8	예
translated_html	아니요
translated_text	아니요
URL	아니요
user_image	아니요
비디오	아니요
wiki_text	아니요

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 개인정보 보호 역할

데이터 개인정보 보호는 이러한 역할을 추가합니다.

데이터 개인정보 보호 관리자

데이터 개인정보 보호 관리자 역할은 데이터 개인정보 보호 기술 및 정책을 만드는 데 사용되는 관리자 역할입니다.

데이터 개인정보 보호 관리자 **[data_privacy_admin]**

포함하는 역할

안 함

그룹에 할당됨

안 함

구독

아니요

상승함

예

고려 사항

더 많은 대상 역할을 사용할 수 있는 경우 사용자에게 이 역할을 할당하지 마십시오.

"데이터 개인정보 보호 관리자" 역할을 할당하려면 사용자를 보안 관리자 역할로 승격하여 역할을 추가합니다.

데이터 개인정보 보호 감사자

데이터 개인정보 보호 감사자는 데이터 개인정보 보호 기록을 보는 데 사용되는 읽기 전용 역할입니다.

데이터 개인정보 보호 감사자 **[data_privacy_auditor]**

포함하는 역할

안 함

그룹에 할당됨

안 함

구독

아니요

상승함

아니요

고려 사항

안 함

데이터 개인정보 보호 클론 프로세서

데이터 개인정보 클론 프로세서 역할을 가진 사용자는 데이터 클래스 데이터 개인정보 보호 작업을 생성하고 실행할 수 있습니다.

데이터 개인정보 보호 클론 프로세서 **[data_privacy_clone_processor]**

포함하는 역할

안 함

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그룹에 할당됨
안 함
구독
아니요
상승함
예
고려 사항
안 함

데이터 개인정보 보호 프로세서

데이터 개인정보 프로세서 역할을 가진 사용자는 사용자 [sys_user] 테이블에서 데이터 개인정보 보호 작업을 생성하고 실행합니다.

데이터 개인정보 보호 프로세서 **[data_privacy_processor]**

포함하는 역할
안 함
그룹에 할당됨
안 함
구독
아니요
상승함
예
고려 사항
안 함

데이터 개인정보 보호(클래식)

데이터 개인정보 보호(클래식)는 제품군 릴리스로 사용할 수 있습니다. 마지막 제품군 업데이트는 Tokyo 출시에서 릴리스되었습니다.

데이터 개인정보 보호 활성화(클래식)

관리자 역할이 있는 경우 데이터 개인정보 보호 플러그인(com.glide.data_privacy) 플랫폼 보안을 활성화할 수 있습니다. 애플리케이션은 데모 데이터를 포함하며 관련 ServiceNow® Store 애플리케이션 및 플러그인이 아직 설치되어 있지 않으면 이를 설치합니다.

시작하기 전에
데이터 개인정보 보호를 위해서는 나머지 항목과 별도의 구독이 Now Platform®필요합니다.

구독을 구매하려면 ServiceNow 계정 관리자에게 문의하십시오. 구독을 구매하면 특정 플러그인이 자동으로 활성화됩니다. 유료 플러그인이 자동으로 활성화되지 않은 경우, 인스턴스의 모든 애플리케이션 목록에서 수동으로 활성화할 수 있습니다.

> **주:** 구독을 구매하기 전에 30일 평가판 기간으로 데이터 개인정보 보호(클래식) 및 데이터 디스커버리를 평가할 수 있습니다. 평가판이 만료된 후에는 라이선스 없이 더 이상 데이터를 검색하거나 익명화 작업을 실행할 수 없습니다.

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

데이터 개인정보 보호와 함께 다음 항목이 설치됩니다.

- 플러그인
- 역할
- 테이블

자세한 내용은 데이터 개인정보 보호 (클래식)와 함께 설치되는 구성요소 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 데이터 개인정보 보호 플러그인(com.glide.data_privacy)을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

데이터 개인정보 보호 (클래식)와 함께 설치되는 구성요소

데이터 개인정보 보호 플러그인(com.glide.data_privacy)과 함께 설치되는 구성 요소에 대해 알아봅니다.

설치되는 테이블

테이블	설명
데이터 개인정보 보호 연합 작업 [dp_federated_job]	데이터 개인정보 보호를 위한 연합 작업
데이터 개인정보 보호 작업 [dp_job]	데이터 개인정보 보호 작업
데이터 개인정보 보호 작업 [dp_job_summary]	데이터 개인정보 보호 작업 요약
데이터 개인정보 보호 기술 [dp_technique]	데이터 개인정보 보호 기술
기본 참조 링크	기본 참조 링크

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	설명
[dp_primary_reference]	
개인정보 분류 필드 기술 [dp_field_technique]	데이터 개인정보 보호 분류 필드 기술
개인정보 구성 [dp_configuration]	데이터 개인정보 보호 구성
개인정보 기술 구성 [dp_technique_with_params]	데이터 개인정보 보호 기술
개인정보 기술 매개변수 [dp_technique_with_parameter]	매개변수를 사용한 데이터 개인정보 보호 기술
개인정보 기술 매개변수 값 [dp_technique_with_parameter_value]	매개변수가 있는 데이터 개인정보 보호 기술에 사용되는 매개변수 값입니다.

데이터 개인정보 보호(클래식) 구성

데이터 개인정보 보호 기술 및 정책을 생성하는 방법과 데이터 개인정보 보호 작업을 생성하고 실행하는 방법을 알아봅니다.

데이터 개인정보 보호 기술

데이터 개인정보 보호 기술은 데이터를 익명화하는 방법을 결정하기 위해 선택하는 옵션입니다. 데이터 개인정보 보호 작업에서 참조할 데이터 개인정보 보호 기술을 생성해야 합니다. 개인정보 기술을 관련 개인정보 기술 구성에 연결하려면 을(를) 데이터 개인정보 보호 기술 구성 생성 참조하십시오.

데이터 개인정보 보호 정책

데이터를 익명화할 때 사용되는 데이터 개인정보 보호 기술을 지정하도록 데이터 개인정보 보호 정책을 구성합니다. 자세한 내용은 데이터 개인정보 보호 정책 만들기 문서를 참조하십시오.

데이터 개인정보 보호 작업

데이터 개인정보 보호 작업은 이러한 모든 구성요소를 사용하여 데이터를 익명화합니다. 이러한 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 데이터 개인정보 보호 작업 구성.

데이터 개인정보 보호 기술 구성 생성

데이터 개인정보 보호 기술 구성을 생성하여 데이터 개인정보 보호가 데이터를 익명화하는 방법을 사용자 지정합니다.

시작하기 전에
필요한 역할: data_privacy_admin 및 admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. **data_privacy_admin** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.
2. 다음으로 이동 시스템 보안 > 데이터 개인정보 보호 > 개인정보 기술 구성.
3. 새로 만들기를 클릭합니다.
4. 이름 필드에 개인정보 보호 기술 구성의 이름을 입력합니다.
5. 개인정보 기술 필드에서 개인정보 기술을 선택합니다.

데이터 개인정보 보호 기술

기술	설명
작업 없음	이 기술은 자리 표시자입니다. 선택해도 필드는 수정되지 않습니다.
무작위 바꾸기	이 기술은 값을 임의로 생성된 값으로 바꿉니다. 문자열 및 번호 데이터는 이 기술을 사용할 수 있습니다.
선택적 바꾸기	이 기술은 String 데이터를 선택적으로 대체합니다. 입력의 시작과 끝 인덱스 사이의 모든 문자가 선택한 문자로 대체됩니다. 마스킹에서 제외할 문자를 지정할 수 있습니다. ◦ start_index: 기술은 지정된 문자에서 시작하는 데이터를 마스킹합니다. 공백으로 두면 마스킹이 첫 번째 문자로 시작됩니다. ◦ end_index: 기술은 문자열의 시작부터 지정된 문자까지 데이터를 마스킹합니다. 공백으로 두면 마스킹이 마지막 문자로 끝납니다. ◦ exclude_char: 마스킹에서 제외할 문자를 정의합니다. ◦ replacement_char: 마스킹에 사용되는 문자를 정의합니다. 제공되지 않은 경우 별표(*)가 기본적으로 사용됩니다.
정적 바꾸기	이 기술은 값을 정적 값으로 교환합니다. 문자열, 숫자 및 날짜 데이터는 이 기술을 사용할 수 있습니다. ◦ date_time_value: 날짜 값을 이 날짜로 바꿉니다. yyyy-MM-dd HH:mm:ss 형식을 사용합니다. ◦ date_value: 날짜 값을 이 날짜로 바꿉니다. yyyy-MM-dd 형식을 사용합니다. ◦ number_value: 번호 값을 이 숫자로 바꿉니다. ◦ string_value: 문자열 값을 이 텍스트로 바꿉니다.
제거	이 기술은 값을 제거하고 비어 있는(null) 값으로 대체합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 이전에 지원되었던 값 바꾸기 는 더 이상 사용되지 않으며 이름이 **Replace-Deprecated** 이므로 사용해서는 안 됩니다.

6. 머리글을 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 저장을 클릭합니다.
   기록이 저장되면 개인정보 매개변수형 값 목록이 나타납니다.
7. 개인정보 매개변수형 값 목록의 기록을 사용하여 데이터 개인정보 보호 기술 구성을 사용자 지정합니다.
   사용 가능한 매개변수화된 값은 선택한 개인정보 보호 기술에 따라 다릅니다. 작업 없음 및 제거 기술에 대한 매개변수화된 값은 없습니다.

선택적 바꾸기에 대한 개인정보 매개변수형 값

개인정보 기술 매개변수 값	설명	기본값
char_to_replace	선택적 바꾸기를 사용하여 값을 바꿀 때 사용할 문자입니다.	*
end_index	기술은 문자열의 시작부터 지정된 문자까지 데이터를 마스킹합니다. 비워 두면 마스킹이 마지막 문자로 끝납니다.	(비어 있음)
exclude_char	마스킹을 건너뛸 문자입니다. 이 값에는 단일 문자만 사용할 수 있습니다. 두 개 이상 입력하면 첫 번째 문자가 사용됩니다.	(비어 있음)
start_index	기술은 지정된 문자에서 시작하는 데이터를 마스킹합니다.	1

바꾸기에 대한 개인정보 매개변수형 값

개인정보 기술 매개변수 값	설명	기본값
date_time_value	날짜 및 시간 값을 이 날짜로 대체합니다. yyyy-MM-dd HH:mm:ss 형식을 사용합니다.	1988-11-11 10:10:10
date_value	날짜 값을 이 날짜로 대체합니다. yyyy-MM-dd 형식을 사용합니다.	1988-11-11
number_value	번호 값을 이 숫자로 대체합니다.	1234567
preserve_data_length	데이터 길이를 유지하려면 **true** 로 설정합니다. 식별되지 않은 데이터는 원래 데이터와 길이가 같습니다.	예
string_value	문자열 값을 이 텍스트로 대체합니다.	TEXT123
use_random_generated_value	데이터를 임의로 작성된 값으로 바꾸려면 **true** 로 설정합니다. 문자열 및 번호 데이터만	거짓

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개인정보 기술 매개변수 값	설명	기본값
	임의의 값으로 대체할 수 있습니다. 이 옵션은 정적 값을 재정의합니다.	

8. 저장을 클릭합니다.

데이터 개인정보 보호 정책 만들기

데이터를 익명화할 때 사용되는 데이터 개인정보 보호 기술을 지정하도록 데이터 개인정보 보호 정책을 구성합니다.

시작하기 전에

데이터 개인정보 보호 구성은 사용 사례에 따라 테이블, sys_user 및 기타, 식별되지 않은 열을 정의하고 데이터를 익명화하는 동안 사용할 기술의 매개변수화된 유형을 지정합니다.

주: 개인정보 구성을 완료하려면 먼저 데이터 개인정보 보호 기술 구성을 구성해야 합니다. 자세한 내용은 데이터 개인정보 보호 기술 구성 생성 문서를 참조하십시오.

필요한 역할: data_privacy_admin 및 admin

프로시저

1. **data_privacy_admin** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.
2. 다음으로 이동 시스템 보안 > 데이터 개인정보 보호(클래식) > 개인정보 보호 정책 구성.
3. 새로 만들기를 선택합니다.
4. 이름 필드에 개인정보 보호 정책 구성의 이름을 입력합니다.
5. 데이터 클래스 필드에서 이 정책에 사용할 데이터 클래스를 선택합니다.
   데이터 개인정보 보호 정책은 분류된 데이터에만 적용할 수 있으며, 데이터 분류에 대한 자세한 내용은 데이터 분류를 참조하십시오.
   데이터 클래스를 선택하면 개인정보 분류 필드 기술 및 개인정보 기본 참조 링크 목록이 양식에 표시됩니다.
6. 옵션: 선택한 데이터 클래스의 모든 데이터에 익명화를 적용하려면 클래스의 모든 데이터에 적용을 선택합니다.
   이 필드를 선택하지 않으면 데이터 개인정보 보호 프로세서 사용자가 데이터 개인정보 보호 작업을 만들 때 익명화할 사용자를 선택할 수 있습니다. 이 필드를 선택하면 해당 옵션을 사용할 수 없습니다.
   - 복제 시 적용: 이 옵션을 사용할 수 있게 됩니다. 이 옵션을 선택하면 데이터 개인정보 보호 클론 중에 개인정보 구성이 실행됩니다.
   - 애플리케이션 순서: 애플리케이션 순서가 더 높은 Postclone 구성에 대한 데이터 개인정보 보호 작업이 순서가 낮은 다른 작업보다 먼저 시작될 수 있습니다.

   중요사항: 동일한 순서를 가진 사용자에 대한 결과 처리 순서가 일관되지 않으므로 동일한 애플리케이션 순서로 여러 데이터 개인정보 보호 정책을 생성하지 마십시오.
7. 옵션: 데이터 개인정보 보호 작업에서 데이터를 익명화하는 기능을 활성화하려면 롤백 지원을 선택합니다.
   자세한 내용은 데이터 개인정보 보호 작업 롤백 문서를 참조하십시오.
   데이터 개인정보 보호 작업을 만들 때 롤백 지원을 선택하면 작업을 롤백하는 옵션을 사용할 수 있게 됩니다.
8. 개인정보 분류 필드 기술 탭을 선택하여 개인정보 분류 필드 기술 목록을 표시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 테이블 필드에서 항목을 선택하여 각 목록 항목에 대한 개인정보 기술 구성 필드를 엽니다.
   개인정보 분류 필드 기술 목록에는 선택한 데이터 클래스에서 익명화할 모든 데이터가 표시됩니다. 이러한 각 항목에 대해 적용할 개인정보 보호 기술을 선택해야 합니다.
10. 적용할 개인정보 기술 구성을 선택합니다.

> **중요사항:** 항목을 익명화하지 않는 경우 항목을 비워 두는 대신 **DoNothing** 기술을 선택합니다. 개인정보 보호 기술 구성 필드에 빈 값이 있는 정책은 데이터 개인정보 보호 작업에 사용될 때 실행할 수 없습니다.

11. 제출 또는 저장을 선택하여 기록을 저장합니다.

다음에 수행할 작업
데이터 개인정보 보호 작업 구성.

데이터 개인정보 보호 작업 구성

프로덕션 인스턴스에서 데이터 개인정보 보호 작업을 구성하여 비프로덕션 인스턴스에서 익명화된 데이터를 사용자 및 데이터 클래스 작업에 사용합니다.

시작하기 전에
데이터 개인정보 보호 작업은 다음 두 가지 익명화 사용 사례를 지원합니다.

- 특정 sys_users의 민감 데이터
- 특정 데이터 클래스의 중요한 데이터입니다.

필요한 역할: data_privacy_processor 및 admin

프로시저

1. **data_privacy_processor** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.
2. 다음으로 이동 시스템 보안 > 데이터 개인정보 보호 > 데이터 개인정보 보호 작업.
3. 데이터 개인정보 보호 작업 목록에서 새로 만들기를 클릭합니다.
4. 양식에서 필드에 내용을 입력합니다.

데이터 개인정보 보호 작업 필드

필드	설명
이름	작업의 이름입니다.
설명	작업에 대한 설명입니다.
개인정보 구성	이 작업에 사용할 개인정보 보호 정책 구성입니다. 개인정보 보호 정책 구성에 대한 자세한 내용은 문서를 참조하십시오 데이터 개인정보 보호 정책 만들기.
사용자	이 작업에서 익명화할 사용자 또는 사용자 그룹을 선택합니다. 그룹의 사용자를 최대 1,000명까지 처리할 수 있습니다. 주: 이 필드는 선택한 개인정보 보호 정책 조건에 대해 사용자 기록을 선택해야 하는 경우에만 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
시운전	작업을 테스트로 실행합니다. 이 작업을 실행할 때 영향을 받는 기록은 없습니다. 결과는 작업이 실행된 것처럼 요약 필드에 표시됩니다. 주: 롤백이 있는 데이터 개인정보 보호 작업을 구성할 때 시험 실행을 꺼야 합니다. 자세한 내용은 데이터 개인정보 보호 작업 롤백 문서를 참조하십시오.
상태	데이터 개인정보 보호 작업의 상태: ◦ 일정 예약 준비 완료: 새 작업의 기본 상태입니다. ◦ 롤백 진행 중: 익명화를 롤백하도록 작업이 설정되었습니다. ◦ 롤백 완료: 익명화 작업 롤백이 성공적으로 완료되었습니다. 읽기 전용 필드입니다.
추정된 기록 카운트	이 작업이 영향을 주는 예상 기록 수입니다. 읽기 전용 필드입니다.
요약	작업을 실행할 때의 결과를 표시하는 읽기 전용 필드입니다.
기간 시작	이 작업을 실행할 기간의 시작입니다. 이 필드에 입력한 시간 이후에 작업이 실행됩니다. 유효한 시간 값은 24시간 표기법에 따라 조정된 범용 시간으로 표시됩니다.
기간 종료	이 작업을 실행할 기간의 끝입니다. 이 필드에 입력된 시간 전에 작업이 실행됩니다. 작업이 아직 완료되지 않은 경우 작업이 일시 중지되었다가 다음에 시작할 때 다시 시작됩니다. 종료 시간은 시작 시간 이후여야 합니다. 유효한 시간 값은 24시간 표기법에 따라 조정된 범용 시간으로 표시됩니다.

5. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 저장을 선택합니다.
   기록을 저장하면 작업 예약 및 작업 삭제 버튼이 나타납니다.
6. 작업 예약을 클릭하여 작업을 실행합니다.
   작업은 기간 시작 필드와 기간 종료 필드에서 선택한 시간 사이에 실행됩니다. 시작 및 종료 기간 동안 작업이 완료되지 않은 경우 다음 기간 시작 시 작업이 계속됩니다.

   주: 드라이 런을 선택한 경우에도 작업은 한 번만 실행할 수 있습니다. 동일한 작업을 다시 실행하려면 동일한 필드 값을 사용하여 데이터 개인정보 보호 작업을 생성합니다.

7. 옵션: 다음 기능 중 하나를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 작업 취소: 데이터 개인정보 보호 작업을 취소합니다.
- 일시 중지: 롤백을 선택한 경우 작업 및 롤백 기록을 일시 중지합니다. 롤백 컨텍스트에 대한 3일 만료 기간 후에 경고 메시지가 표시됩니다. 자세한 내용은 데이터 개인정보 보호 작업 롤백 문서를 참조하십시오.
- 다시 시작: 일시 중지된 작업을 다시 시작합니다. 일시 중지된 경우 재개된 작업에 대해서는 롤백이 지원되지 않습니다. 작업을 취소하고 데이터 개인정보 보호 작업을 생성합니다. 기록은 만료되지 않은 롤백 컨텍스트를 사용합니다.

데이터 개인정보 보호 작업 롤백

데이터베이스 변경 내용은 작업 및 스크립트와 같은 작업에 대해 캡처되므로 변경 내용을 롤백할 수 있습니다. 인적 오류로 인해 실수로 잘못된 사용자 정보가 익명화되는 경우를 대비하여 데이터 개인정보 보호 작업을 롤백합니다. 롤백은 데이터 개인정보 보호 작업에서 데이터를 익명화합니다.

개요

- 롤백은 새 RollbackType *REDACT*의 구성된 만료 기간에 따라 며칠로 제한됩니다. 데이터 개인정보 보호 작업과 연결된 RollbackContext가 만료되면 해당 작업에 롤백 기능을 더 이상 사용할 수 없습니다.
  - 익명화의 롤백 컨텍스트는 기본적으로 3일 동안 저장됩니다.
  - 기본 만료 시간은 새 **RollbackType** *REDACT.*의 **RollbackContext**에서 데이터 개인 정보 보호 관리자가 1보다 큰 값으로 설정할 수 있습니다 Glide 시스템 속성*glide.rollback.expiration_days_redact*에서 값을 설정합니다 . 복구 롤백 및 삭제 문서를 참조하십시오.

    시스템 속성 추가 또는 생성에 대한 자세한 내용은 문서를 참조하십시오 시스템 속성 추가 .

    자세한 내용은 다음을 참조하십시오.
- 롤백은 완료됨, 취소됨 또는 오류 상태에 있는 데이터 개인정보 보호 작업에 사용할 수 있습니다.
- 롤백 지원이 켜진 데이터 개인정보 보호 정책으로 구성된 성공적인 모든 sys_user 익명화 제거 작업에 대해 롤백 컨텍스트가 생성됩니다. 데이터 개인정보 보호 작업당 최대 하나의 롤백 컨텍스트가 있을 수 있습니다.

데이터 개인정보 보호 작업 롤백

프로덕션 인스턴스의 익명화된 데이터를 사용하는 비프로덕션 인스턴스에서 데이터 클래스 또는 사용자 작업을 식별 해제하기 전의 상태로 데이터 개인정보 보호 작업을 롤백합니다.

시작하기 전에

필요한 역할: data_privacy_admin 또는 data_privacy_processor, admin

프로시저

1. **data_privacy_processor** 또는 **data_privacy_admin** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.
2. 다음으로 이동 모두 > 시스템 보안 > 데이터 개인정보 보호 > 데이터 개인정보 보호 작업.

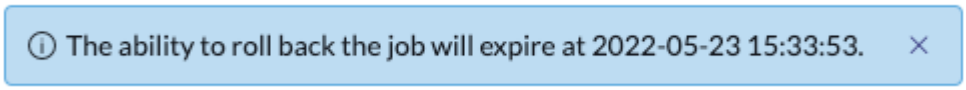
   주: 사전에 롤백을 지원하는 데이터 개인정보 보호 정책 구성을 만들어야 합니다. 데이터 개인정보 보호 정책 만들기입니다.

3. 데이터 개인정보 보호 작업을 생성하고 롤백을 지원하는 개인정보 구성을 선택합니다.
   데이터 개인정보 보호 작업 구성 문서를 참조하십시오.
4. 데이터 익명화를 위해 작업을 예약합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ 작업이 실행된 후 선택한 구성에 대해 데이터가 익명화됩니다.

◦ 만료 시간을 알리는 메시지가 작업에 표시됩니다. 만료 기간 내에 작업을 롤백할 수 있습니다.



5. **data_privacy_processor** 역할로 승격합니다.
6. 롤백할 데이터 개인정보 보호 작업을 엽니다.
7. 롤백을 선택하여 데이터를 익명화합니다.

데이터 개인정보 보호 클론

고객 데이터가 소스에서 대상 인스턴스로, 일반적으로 프로덕션에서 비프로덕션으로 복제되면 대상 인스턴스에서 중요한 데이터가 식별되지 않습니다.

데이터 개인정보 보호 관리자는 복제 후 정책을 구성합니다. 대상 인스턴스에서 복제 후 스크립트가 완료되면 사용자는 식별되지 않은 데이터를 볼 수 있으며 원래 데이터에는 액세스할 수 없습니다. 데이터 개인정보 보호 관리자는 복제 시 대상 인스턴스에 적용할 익명화 정책을 구성하여 대상 인스턴스에 원본 중요한 데이터가 없도록 할 수 있습니다. 실행할 다른 정책을 기준으로 정책에 대한 순서가 지정됩니다.

주: 데이터 개인정보 복제는 자체 호스팅 인스턴스에서는 사용할 수 없습니다.

데이터 개인정보 보호 클론에는 다음과 같은 추가 속성이 있습니다.

- 데이터 개인정보 보호 플러그인은 대상 인스턴스에서 실행할 복제 후 스크립트를 만듭니다.
- PostClone 구성을 위해 생성된 데이터 개인정보 보호 작업은 동일한 테이블을 포함하지 않는 경우 병렬로 실행될 수 있습니다.
- 더 높은 순서의 작업에 다른 하위 작업과 관련된 테이블이 포함되지 않은 경우, 애플리케이션 순서가 더 높은 Postclone 구성에 대한 데이터 개인정보 보호 작업이 더 낮은 순서의 다른 작업보다 먼저 시작될 수 있습니다.
- 데이터 개인정보 보호 플러그인을 사용하면 데이터 개인정보 보호 테이블은 기본적으로 클론 데이터 보관자 테이블 세트에 있습니다.
- 클론 제외 테이블에 데이터 개인정보 보호 테이블(dp_{table})을 추가하려고 하면 경고가 표시되며 해당 테이블을 제외하면 안 됩니다.

데이터 개인정보 보호 클론 요청 구성

데이터 개인정보 보호 클론 통합은 PostClone 스크립트를 사용하여 대상에 구성된 정책에 대한 데이터 개인정보 보호 작업을 생성하고 실행하도록 구성됩니다. 스크립트를 실행한 후 사용자는 식별되지 않은 데이터를 볼 수 있으며 원래 데이터에는 액세스할 수 없습니다.

시작하기 전에

필요한 역할: data_privacy_clone_processor, data_privacy_admin, admin

프로시저

1. 소스 인스턴스에서 데이터 개인정보 보호 플러그인(sn_dp_store_app)을 활성화합니다.
   플러그인 고객 서비스 및 지원은 .
   데이터 개인정보 보호 PostClone 스크립트가 설치되어 있습니다.
2. **data_privacy_admin** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.
3. 다음으로 이동 시스템 보안 > 데이터 개인정보 보호 > 개인정보 보호 정책 구성.
4. 개인정보 보호 정책 구성을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 클래스의 모두에 적용을 선택하고 복제할 때 적용을 선택합니다. 자세한 내용은 데이터 개인정보 보호 정책 만들기 문서를 참조하십시오.

5. 데이터 개인정보 보호 구성을 백업합니다.
6. 데이터 개인정보 보호 관리자로서 복제 요청을 제출합니다.

결과
데이터 개인정보 보호 PostClone 스크립트는 대상 인스턴스에서 실행되고 PostClone 스크립트는 대상 인스턴스에 데이터 개인정보 보호 연합 작업 기록을 생성합니다. 페더레이션 작업은 대상 인스턴스에서 애플리케이션 순서에 따라 각 복제 후 정책에 대한 데이터 개인정보 보호 작업을 생성하고 실행합니다.백업 소스가 대상 인스턴스에 복제됩니다. 데이터 개인정보 보호 PostClone 스크립트는 대상 인스턴스에서 구성된 정책에 대한 데이터 개인정보 보호 작업을 생성하고 실행합니다.

상승된 데이터 개인정보 보호 클론 프로세서는 대상 인스턴스에 로그온하고 dp_federated_job.list 및 dp_job.list에서 클론 후 페더레이션 작업 상태를 모니터링할 수 있습니다.

Data Privacy

데이터 개인정보 보호 스토어 앱은 현대적인 모양과 느낌 및 유용성을 갖춘 데이터 분류 및 데이터 개인정보 보호를 위한 Next Experience 새로고침입니다. 데이터 개인정보 보호 스토어 앱은 Utah 이상에서 지원됩니다.

데이터 개인정보 보호는 개요, 분류 및 익명화의 여러 구성 요소로 구성됩니다.

개요

개요 섹션을 시작점으로 사용하여 데이터 및 데이터 개인정보 보호 준수를 관리합니다. 자세한 내용은 데이터 개인정보 보호 개요 문서를 참조하십시오.

분류

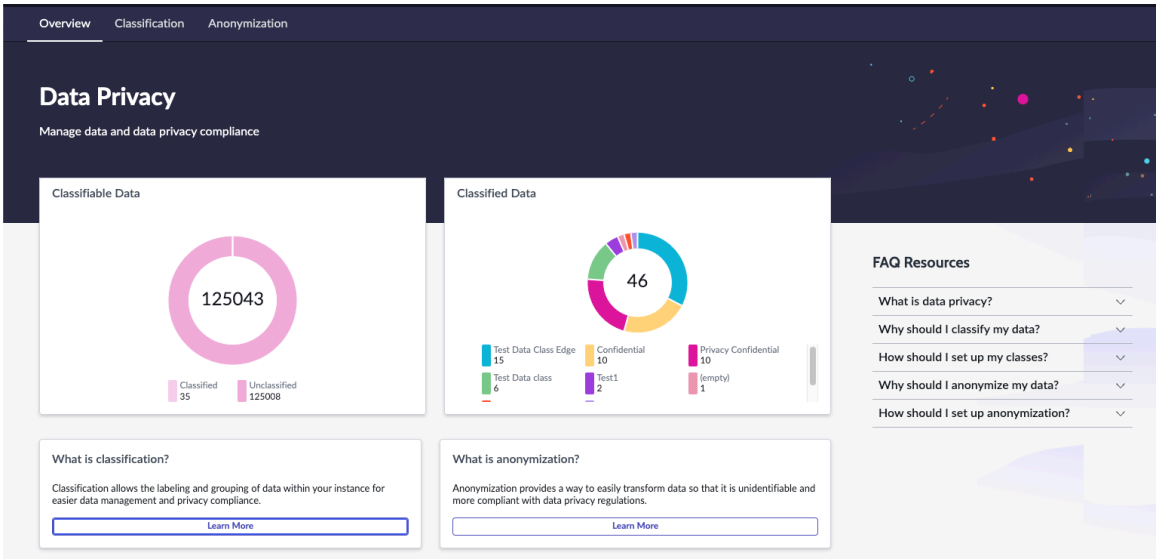
데이터 분류는 나중에 사용할 수 있도록 데이터를 쉽게 검색, 정렬 및 저장할 수 있는 범주로 구성하는 프로세스입니다. 분류 시스템을 사용하면 기밀성 및 보안 정책 요구 사항에 집중할 수 있습니다. 익명화에 사용할 데이터를 분류합니다. 데이터 클래스 및 분류에 대한 자세한 내용은 다음 문서를 참조하십시오 데이터 분류.

데이터 개인정보 보호 개요

개요 홈페이지는 데이터 및 데이터 개인정보 보호 준수를 관리하기 위한 시작점입니다.

개요 대시보드는 인스턴스 내에서 데이터 분류 및 익명화 작업의 현재 상태를 보고합니다. 개요 대시보드에서 데이터를 보고 분류할 수 있는 데이터의 양, 사용 가능한 데이터 클래스, 각 클래스의 데이터 양 및 익명화 작업의 전체 상태를 확인할 수 있습니다. 분류된 데이터는 여러 범주로 나뉩니다. 두 차트 중 하나에서 하위 범주를 선택하면 전체 차트에서 범주가 추가되거나 제거되고 개수가 조정됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



분류 가능한 데이터

분류할 수 있는 인스턴스의 총 데이터 기록 수를 표시합니다. 이 숫자는 분류된 데이터의 총 수와 분류되지 않은 데이터의 총수로 세분화됩니다. 이를 통해 관리자는 잠재적인 분류 기회를 빠르게 볼 수 있습니다.

분류된 데이터

분류된 인스턴스의 총 데이터 기록 수를 표시합니다. 이 숫자는 할당된 각 데이터 클래스에 대해 분류된 총 데이터 수로 세분화됩니다. 이를 통해 각 영역에서 얼마나 많은 데이터가 분류되었는지 빠르게 파악할 수 있습니다.

익명화 작업

사용자 및 데이터 클래스 작업에 대해 비프로덕션 인스턴스에서 완료된 작업을 현재 처리 중인 데이터 개인정보 보호 작업을 표시합니다.

자세히 알아보기

자세히 알아보기 섹션에서는 분류 및 익명화를 이해하기 위한 빠른 보기와 프로세스를 쉽게 시작할 수 있는 방법을 제공합니다.

FAQ 자원

분류 또는 익명화에 대한 제품 학습 자원에 액세스하여 데이터 개인정보 보호를 통해 인스턴스 보안을 시작하는 방법에 대한 자세한 내용을 확인하십시오.

데이터 개인정보 보호 활성화

데이터 개인정보 보호에는 데이터 분류 및 익명화가 포함되며 에서 ServiceNow Store설치됩니다.

시작하기 전에

데이터 익명화를 사용하려면 먼저 데이터 개인정보 보호(클래식)를 권리로 ServiceNow 볼트 활성화해야 합니다. 자세한 내용은 데이터 개인정보 보호 활성화(클래식) 문서를 참조하십시오.

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두 > 데이터 개인정보 보호.
2. 필터 기준 및 검색 창을 사용하여 애플리케이션을 찾습니다.

   애플리케이션 이름 또는 ID로 애플리케이션을 검색할 수 있습니다. 애플리케이션을 찾을 수 없으면 ServiceNow Store에서 요청해야 할 수도 있습니다.

   ServiceNow Store 웹 사이트를 방문하면 사용 가능한 모든 앱을 확인하고 스토어에 요청을 제출하는 방법에 대한 정보를 참조할 수 있습니다. 출시된 모든 앱의 누적 릴리스 정보는 ServiceNow Store 버전 기록 릴리스 정보 를 참조하십시오.
3. 목록에서 버전을 선택하고 설치를 선택합니다.

   표시되는 설치 대화 상자에서 애플리케이션과 함께 설치되는 모든 종속성이 나열됩니다.
4. 프롬프트가 표시되면 ServiceNow Store에 연결되는 해당 링크를 따라 종속성을 위한 모든 추가 권리를 얻습니다.
5. 옵션: 데모 데이터를 사용할 수 있고 이를 설치하려면 데모 데이터 로드 확인란을 선택합니다.

   (Optional) 데모 데이터는 일반적인 사용 사례에 대한 애플리케이션 기능을 설명하는 샘플 기록으로 구성됩니다. 개발 또는 테스트 인스턴스에서 애플리케이션을 처음 설치할 때 데모 데이터를 로드합니다.

   중요사항: 설치 중에 데모 데이터를 로드하지 않으면 나중에 로드할 수 없습니다.
6. 설치를 선택합니다.

데이터 분류

미리 정의되었거나 사용자 정의된 데이터 분류를 사용하여 데이터를 유형별로 그룹화합니다. 할당된 데이터 분류 관리자 또는 감사자 역할이 있는 경우 다양한 데이터 분류를 관리하거나 인스턴스 내에서 각종 데이터의 현재 상태를 시각적으로 분석할 수 있습니다.

데이터 분류 다음에 대한 지원 활성화:

- 인스턴스에 호스팅된 데이터 유형에 대한 Now Platform 가시성
- 개인 정보 보호법을 준수하고 금융 서비스 및 의료 장치 제조와 같은 산업에 대한 규제 요구 사항을 충족합니다.

데이터 분류

데이터 분류는 테이블의 기존 딕셔너리 항목에 데이터 분류를 수동으로 적용하는 독립 실행형 프로세스입니다. 자세한 내용은 데이터 딕셔너리 테이블 문서를 참조하십시오.

- 비즈니스에 적합하다고 판단되는 대로 데이터를 분류하고 필요에 따라 사용 가능한 데이터 클래스를 변경할 수 있습니다.
- 데이터를 분류할 때 미리 정의된 데이터 분류를 사용하거나 직접 생성할 수 있습니다. 사전 정의된 데이터 분류를 사용하는 것은 선택 사항이지만 시작점으로 사용하는 것이 좋습니다. 이러한 사전 정의된 데이터 분류는 인스턴스에 설치할 수 있는 데모 데이터에 포함되어 있습니다.
- 고유한 데이터 분류를 만드는 경우 상위 및 하위 데이터 분류를 사용하여 계층화된 계층 구조 시스템을 디자인할 수도 있습니다.

주: 데이터 분류 은 도메인 분리를 지원하며 data_classification 테이블 자체는 프로세스 분리됩니다. 자세한 내용은 도메인 분리 및 데이터 분류 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용 케이스

GDPR(General Data Protection Regulation)은 개인에게 자신의 개인 데이터에 대한 통제권을 제공하는 것을 목적으로 하는 유럽 연합 규정입니다. 개인 식별 정보와 같은 데이터 분류를 사용하여 인스턴스에서 개인 데이터가 저장되는 위치를 식별할 수 있습니다. 개인 데이터가 유출되지 않도록 보호하기 위해 적절한 보안 메커니즘을 적용함으로써 조직은 GDPR 요구 사항을 충족합니다.

에 고객 정보를 Now Platform저장하는 경우 필요한 경우 PII(개인 식별 정보) 분류 코드를 사용하여 현지 개인정보 보호법의 규제를 받는 데이터를 추적합니다.

SSN(사회 보장 번호)과 같은 중요한 직원 정보를 저장하는 직원 테이블 열에 제한된 데이터 분류를 적용할 수 있습니다. 그러면 관리자와 감사자가 개요 대시보드를 사용하여 올바른 열에 데이터 분류를 할당했는지 확인할 수 있습니다. 또한 제한된 유형의 정보에 대한 분류 상세 정보를 볼 수도 있습니다.

데이터 분류 생성

[data_classification] 테이블에서 사용자 정의 데이터 분류를 생성한 다음 특정 테이블의 특정 열에 할당할 수 있습니다. 새 데이터 클래스를 만들어 분류 프로세스를 시작합니다.

시작하기 전에
필요한 역할: data_classification_admin, admin

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > **Data Privacy** > 분류.
2. +데이터 클래스 추가를 선택합니다.

   주: 기본 시스템에는 여러 데이터 클래스가 포함되어 있습니다.

3. 양식에서 필드에 입력합니다.

필드	설명
클래스 이름	데이터 분류의 이름입니다.
상위 클래스	이 데이터 분류가 종속되는 상위 데이터 분류의 이름입니다. 이 데이터 분류가 상위 데이터 분류의 하위 분류가 아닌 경우 필드를 비워 둡니다.
설명	데이터 분류에 대한 설명입니다.

4. 제출을 클릭합니다.
   새 데이터 클래스가 추가됩니다. 데이터 클래스가 자식이면 왼쪽 탐색 모음의 상위 아래에 나열됩니다.

데이터 분류

미리 정의되었거나 사용자 정의된 데이터 분류를 사용하여 데이터를 유형별로 그룹화합니다. 사전 [sys_dictionary] 테이블의 특정 테이블 열에 데이터 분류를 할당합니다. 데이터 분류를 할당하면 Dictionary-Data Class [m2m_dictionary_dataclass] 테이블에 항목이 생성되어 개요 대시보드에서 검토할 수 있습니다.

시작하기 전에
필요한 역할: data_classification_admin, admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 분류할 테이블의 데이터를 할당하려면 새로 만들기를 선택하십시오.
2. 드롭다운에서 데이터 클래스를 선택합니다.
3. 분류할 테이블과 열을 반영하는 기록을 선택합니다.
   특정 테이블을 간편하게 찾을 수 있도록 테이블의 페이지당 표시할 추가 행을 선택합니다.
4. 데이터 분류를 선택합니다.
   데이터는 분류된 데이터 테이블의 분류 이름 아래에 분류됩니다.
5. 데이터를 보거나 Excel, CSV, JSON 또는 PDF로 익스포트합니다.
   선택한 형식으로 데이터를 다운로드하거나 이메일을 통해 수신하도록 선택합니다.

실시간 익명화

RTA(실시간 익명화) 정책을 사용하여 데이터 항목을 실시간으로 익명화합니다.

RTA 개요

사용자는 익명화 정책 페이지를 통해 RTA 정책을 생성합니다. 대상 테이블의 열을 RTA에 대해 선택할 수 있으며, 이에 따라 활성 데이터 패턴이 사용되고 해당 정책이 RTA 대상 열에 유효한 기록 항목에 적용됩니다. 항목이 활성 데이터 패턴과 일치하면 관련 익명화 기술이 익명화에 사용됩니다.

팁: 익명화 기술을 변경해야 하는 경우 을 참조하십시오 패턴 구성 데이터 디스커버리.

실시간 익명화 실패

RTA 정책이 실패하면 테이블을 사용하여 상태를 검토할 수 있습니다 실시간 익명화 실패 .

실시간 익명화 실패

실시간 익명화(RTA) 실패를 검토합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 데이터 개인정보 보호(클래식).
2. 표에서 RTA 오류를 검토합니다.

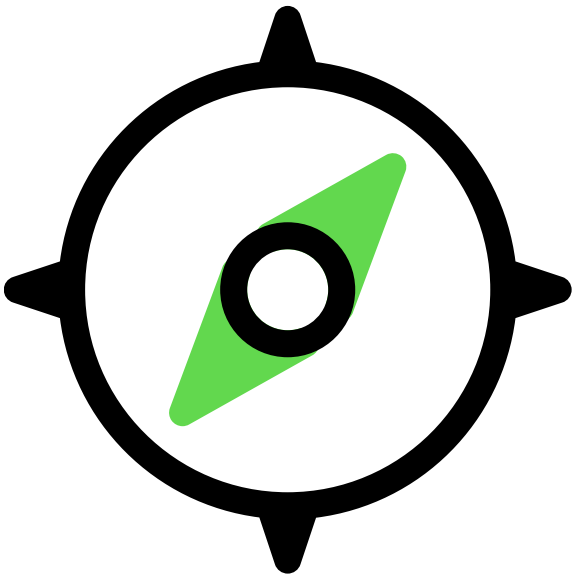
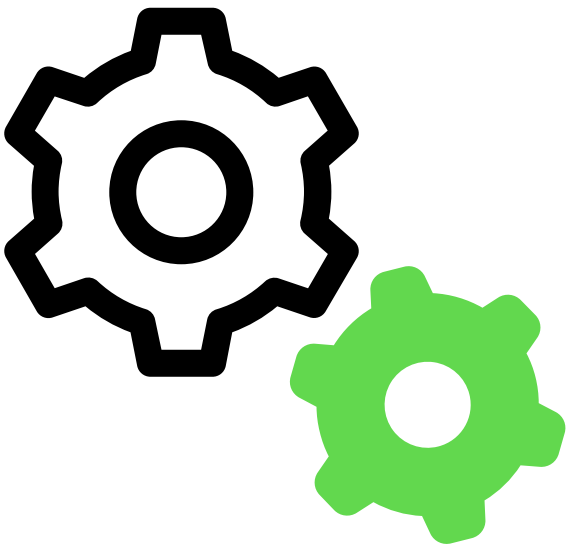
필드 제목	설명
테이블 열	실패가 발생한 테이블 열입니다.
장애 이유	장애 원인의 범주입니다.
장애 이유 상세 정보	실패의 원인을 요약한 간단한 설명입니다.
개인정보 구성	실패한 RTA 개인정보 보호 구성입니다.
기록	실패한 특정 기록입니다.
테이블 이름	오류가 발생한 테이블입니다.
타임스탬프	실패 시간입니다.

데이터 개인정보 보호용 **Now Assist**

Now Assist 생성형 AI 역량으로 민감한 데이터를 익명화하기 위한 것입니다 데이터 개인정보 보호 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작

탐색	구성
	
데이터 개인정보 보호를 위한 Now Assist에 대해 자세히 알아보기	데이터 개인정보 보호를 위한 Now Assist 구성

AI 제한 사항

이 애플리케이션은 데이터의 패턴을 기반으로 예측을 생성하는 빠르게 진화하는 연구 분야인 인공 지능(AI) 및 머신 러닝을 사용합니다. 따라서 이 애플리케이션이 항상 정확하고 완전하거나 적절한 정보를 생성하지 못할 수도 있습니다. 또한 이 애플리케이션이 사용 사례에 대해 완전히 학습되거나 테스트되었다는 보장은 없습니다. 이러한 문제를 완화하기 위해 이 애플리케이션의 사용이 사용 사례에 대한 정확성, 유해성 및 적합성을 테스트 및 평가하고, 출력에 대한 인적 감독을 사용하고, 의사 결정 목적으로 AI 생성 출력에만 의존하지 않는 것은 귀하의 책임입니다. 이는 의료, 재무, 법률, 고용 보안 또는 인프라와 같이 결과적인 영향을 미치는 영역에 이 애플리케이션을 배포하려는 경우 특히 중요합니다. 귀하는 ServiceNow에서 업데이트할 수 있는 ServiceNow의 AI 사용 제한 방침 을 준수하는 데 동의합니다.

데이터 처리

이 애플리케이션을 사용하려면 ServiceNow 고객의 개별 인스턴스에서 사용자의 인스턴스가 있는 지역과 다른 데이터 센터 지역에 있을 수 있는 중앙 집중식 ServiceNow 환경으로 데이터를 전송해야 하며, Microsoft Azure와 같은 외부 공급업체 클라우드 제공자에게 데이터를 전송해야 합니다. 이 데이터는 당사의 CORE Compliance 포털 을 통해 제공되는 당사의 정책을 포함하여 ServiceNow의 내부 정책 및 절차에 따라 처리됩니다.

AI 제한 사항

이 애플리케이션은 데이터의 패턴을 기반으로 예측을 생성하는 빠르게 진화하는 연구 분야인 인공 지능(AI) 및 머신 러닝을 사용합니다. 따라서 이 애플리케이션이 항상 정확하고 완전하거나 적절한 정보를 생성하지 못할 수도 있습니다. 또한 이 애플리케이션이 사용 사례에 대해 완전히 학습되거나 테스트되었다는 보장은 없습니다. 이러한 문제를 완화하기 위해 이 애플리케이션의 사용이 사용 사례에 대한 정확성, 유해성 및 적합성을 테스트 및 평가하고, 출력에 대한 인적 감독을 사용하고,

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의사 결정 목적으로 AI 생성 출력에만 의존하지 않는 것은 귀하의 책임입니다. 이는 의료, 재무, 법률, 고용 보안 또는 인프라와 같이 결과적인 영향을 미치는 영역에 이 애플리케이션을 배포하려는 경우 특히 중요합니다. 귀하는 ServiceNow에서 업데이트할 수 있는 ServiceNow의 AI 사용 제한 방침 을 준수하는 데 동의합니다.

데이터 처리

이 애플리케이션을 사용하려면 ServiceNow 고객의 개별 인스턴스에서 사용자의 인스턴스가 있는 지역과 다른 데이터 센터 지역에 있을 수 있는 중앙 집중식 ServiceNow 환경으로 데이터를 전송해야 하며, Microsoft Azure와 같은 외부 공급업체 클라우드 제공자에게 데이터를 전송해야 합니다. 이 데이터는 당사의 CORE Compliance 포털 을 통해 제공되는 당사의 정책을 포함하여 ServiceNow의 내부 정책 및 절차에 따라 처리됩니다.

데이터 수집

ServiceNow는 이 애플리케이션의 입력, 출력 및 출력 편집 내용을 수집하고 사용하여 ServiceNow 모델 및 AI 제품을 포함한 ServiceNow 기술을 개발하고 개선합니다. 또한 이 애플리케이션은 텍스트 정보. 고객은 Now Assist옵트아웃 페이지 에 설명된 대로 언제든지 향후 데이터 수집을 옵트아웃할 수 있습니다.

데이터 개인정보 보호용 **Now Assist** 탐색

중요한 데이터 개인정보 보호 데이터를 보호하는 능력을 향상시키는 방법에 Now Assist 대해 자세히 알아보십시오.

Now Assist개요용 데이터 개인정보 보호

Now Assist데이터 개인정보 보호 는 생성형 AI 역량을 통해 경험을 향상시킵니다데이터 개인정보 보호. Now Assist 사용자는 패턴을 따르지 않는 기존 데이터 또는 실시간 데이터에서 중요한 데이터를 검색하고 검색된 데이터를 합성 데이터로 식별할 수 있습니다. 구성 상세 정보는 데이터 개인정보 보호 구성 Now Assist 문서를 참조하십시오.

데이터 개인정보 보호 구성 **Now Assist**

생성형 AI 애플리케이션에서 PII(개인 식별 정보)를 비식별화하도록 데이터 개인정보 보호 고급 구성을 구성합니다.

시작하기 전에

인스턴스에 다음 애플리케이션이 설치되어 있어야 합니다.

- 데이터 개인정보 보호 (클래식) [com.glide.data_privacy]
- 데이터 개인정보 보호 [sn_dp_store_app]
- 데이터 디스커버리 [sn_data_discovery]
- 데이터 디스커버리 API[com.glide.data_discovery]

이러한 플러그인은 최신 버전의 생성형 AI 컨트롤러.

필요한 역할: now_assist_data_privacy_admin

프로시저

1. 다음으로 이동 모두 > 데이터 개인정보 보호(클래식) > 개인정보 보호 정책 고급 구성.
   이전에 중요한 데이터 핸들러를 사용하여 생성형 AI의 데이터 익명화를 지원한 경우 개인정보 보호 정책이 이미 구성되어 있을 수 있습니다. 이전에 구성한 정규 표현식이 업그레이드의 일부로 마이그레이션되었습니다. 에 대한 Now Assist데이터 정책이 이미 있는 경우 6단계로 건너뜁니다.
2. 새로 만들기를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 개인정보 보호 정책의 이름을 입력합니다.
4. 데이터 채널 필드에서 사용할 데이터 채널을 선택합니다.

채널	설명
데이터 키트	AI 모델이 평가에 사용하는 데이터는 민감한 데이터를 검색하고 익명화하여 정리됩니다
데이터 추출	데이터는 모델 교육을 위해 전송되기 전에 삭제됩니다.
Now Assist	데이터는 GenAI 컨트롤러로 전송되기 전에 정리됩니다.

5. 활성을`true`로 설정한 다음, 제출을 선택하여 정책 고급 구성을 만듭니다.
   각 데이터 채널에 대한 정책 구성은 한 번에 하나만 활성화할 수 있습니다. 새 정책 고급 구성을 활성화하려면 해당 데이터 채널의 다른 모든 정책 구성에 대해 활성 을 `false` 로 설정해야 합니다.
6. 정책 고급 구성 목록으로 리디렉션된 후 생성한 기록을 엽니다.
   Now Assist 데이터 채널이 이미 있는 경우 이를 사용하여 기존 기록을 엽니다.
7. 식별할 데이터 패턴을 추가하려면 데이터 패턴 선택을 선택합니다.
8. 옵션: 고유한 데이터 패턴을 생성하려면 다음 문서를 참조하십시오 패턴 구성 데이터 디스커버리.
9. 데이터 패턴을 선택한 다음, 저장을 선택합니다.

결과
데이터 패턴에서 선택한 정규 표현식에 의해 포착된 데이터는 생성형 AI 애플리케이션에 대해 식별되지 않습니다.

데이터 디스커버리

인스턴스 내에서 신용 카드 정보, 이메일 또는 주민 등록 번호와 같은 중요한 데이터를 식별하는 데 사용합니다 데이터 디스커버리 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 디스커버리 탐색



데이터 디스커버리에 대해 자세히 알아보십시오.

데이터 디스커버리 구성



데이터 디스커버리 구성에 대한 도움말을 확인합니다.

데이터 디스커버리에서의 역할



데이터 디스커버리의 역할에 대해 알아봅니다.

데이터 디스커버리 결과



데이터 디스커버리 결과를 검토합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 디스커버리 탐색

인스턴스 내에서 신용 카드 정보, 이메일 또는 주민 등록 번호와 같은 중요한 데이터를 식별하는 데 사용합니다 데이터 디스커버리 .

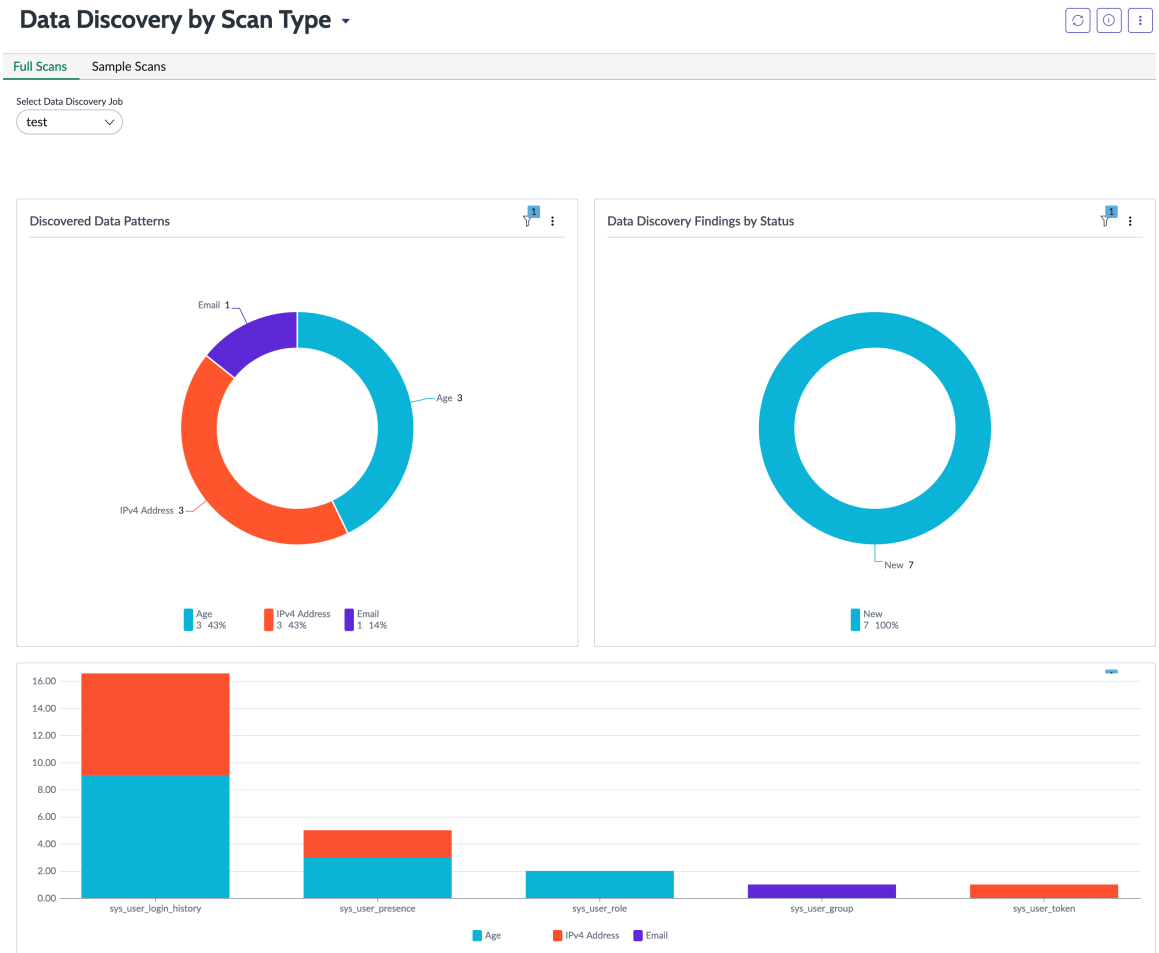
데이터 디스커버리 테이블 세트에서 사용자 정의 작업 세트를 실행합니다. 작업은 대시보드에서 데이터 디스커버리 검토할 중요한 정보를 검색하고 보고합니다. 예약된 작업은 실행될 때 자동으로 모든 활성 데이터 패턴과 대상 테이블을 사용합니다.

데이터 디스커버리 에는 데이터에 대한 다양한 액세스 수준을 가진 사전 할당된 역할도 포함됩니다.

데이터 디스커버리 대시보드에 액세스

다음으로 이동 모두 > 시스템 보안 > 데이터 디스커버리(클래식) > 대시보드 대시보드를 보고 데이터 디스커버리 현재 작업 결과를 검토합니다.

데이터 디스커버리 대시보드



검색된 데이터 패턴

팁: 기록을 선택하여 자세한 정보를 확인하고 결과에 대한 추가 조치를 취합니다. 자세한 내용은 다음을 참조하십시오 데이터 디스커버리 작업 결과 .

검색된 데이터 패턴 차트에는 현재 검색된 데이터 패턴의 수와 백분율이 표시됩니다. 추가 작업을 수행할 섹션을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태별 데이터 디스커버리 결과

데이터 디스커버리 결과 차트는 상태별로 현재 검색된 데이터 패턴의 수와 백분율을 검토합니다.

검색된 테이블

검색된 테이블은 현재 검색된 데이터가 있는 테이블과 해당 데이터 패턴을 강조 표시합니다.

검색된 데이터가 있는 열

검색된 데이터가 있는 열 섹션은 현재 검색된 데이터를 열별로 검토합니다.

데이터 디스커버리 활성화

애플리케이션 및 관련 ServiceNow® Store 애플리케이션 및 플러그인이 아직 설치되지 않은 경우 설치됩니다데이터 디스커버리.

시작하기 전에
데이터 검색에는 나머지 Now Platform항목과 별도의 구독이 필요합니다.

구독을 구매하려면 ServiceNow 계정 관리자에게 문의하십시오. 구독을 구매하면 특정 플러그인이 자동으로 활성화됩니다. 유료 플러그인이 자동으로 활성화되지 않은 경우, 인스턴스의 모든 애플리케이션 목록에서 수동으로 활성화할 수 있습니다.

주:

구독을 구매하기 전에 Now Support 서비스 카탈로그에서 요청하면 무료로 비프로덕션 인스턴스의 기능을 평가할 수 있습니다.

필요한 역할: 관리자

이 태스크 정보
데이터 검색과 함께 다음 항목이 설치됩니다.

- 역할
- 테이블

설치된 역할 및 테이블에 대한 자세한 내용은 해당 기본 데이터 패턴문서를 참조하십시오데이터 디스커버리 역할.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 데이터 디스커버리 플러그인(sn_data_discovery)을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.

3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

찾기 페이지에서 데이터 디스커버리 데이터 분류

결과를 통해 데이터 디스커버리 성공한 모든 작업에서 찾은 민감한 데이터를 분류합니다.

시작하기 전에
필요한 역할: data_discovery_admin

결과 데이터가 분류된 것처럼 보이려면 먼저 작업이 성공적으로 실행되어야 합니다.

이 태스크 정보
데이터 디스커버리 발견 사항 페이지에는 작업에서 찾은 모든 데이터 항목이 표시됩니다. 발견 사항 페이지에서는 항목을 검토하고 분류와 연결할 수 있습니다.

프로시저
1. 다음으로 이동 시스템 보안 > 데이터 디스커버리(클래식) > 데이터 디스커버리 결과.
2. 분류하려는 항목을 선택합니다.
3. 데이터 디스커버리 결과 목록에서 분류를 선택합니다.
4. 테이블 항목과 연결할 데이터 클래스를 선택합니다.
5. 분류를 선택합니다.

데이터 디스커버리 작업

데이터 디스커버리 사용자 정의 데이터 패턴과 대상 테이블을 사용하여 대상 정보를 검토합니다.

데이터 디스커버리 는 먼저 데이터 검색 작업 섹션에서 작업을 예약하여 작동합니다. 예약된 작업이 실행되면 현재 대상 테이블에서 모든 활성 데이터 패턴이 검색됩니다. 작업 생성 및 구성에 데이터 디스커버리 대한 자세한 내용은 다음 문서를 참조하십시오 데이터 디스커버리 작업 구성.

주: 샘플 스캔 작업은 패턴별로 테이블당 최대 10,000개의 기록을 스캔합니다.

경고: 작업이 짧은 시간에 두 번 실행되면 스캔된 행 수가 두 번째 실행에 대해 0을 반환할 수 있습니다.

데이터 디스커버리 데이터 패턴

데이터 패턴 섹션에는 활성 및 비활성의 모든 현재 데이터 패턴이 표시됩니다. 데이터 패턴은 중요한 데이터를 일치시키는 데 사용되는 정규 표현식입니다. 데이터 패턴에 액세스하고 구성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 패턴 구성 데이터 디스커버리. 활성 데이터 패턴 섹션에는 활성 패턴만 표시됩니다. 비활성 패턴은 나타나지 않습니다.

대상 테이블

대상 테이블 섹션에는 작업에 대해 처리할 수 있는 모든 테이블이 나열됩니다. 대상 테이블에 액세스하려면 대상 테이블을 선택하십시오.

다음 테이블은 지원되지 않습니다.

- sr
- 시스엑스
- v
- 쉬$
- Syslog
- 우아

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 사용량 분석
- ECC
- 클론
- jrobin 님
- 파
- sla_repair_log
- 스캔
- GCF
- fm_log
- log
- NP$
- sn_data_discovery
- dp_configuration
- dp_federated_job
- dp_field_technique
- dp_job
- dp_job_summary
- dp_primary_reference
- dp_technique
- data_classification
- m2m_dictionary_dataclass

세분화된 구성

세분화된 구성 도구를 사용하면 테이블에서 중요한 데이터를 검색하기 위해 보다 구체적이고 세부적으로 조정된 제어를 사용할 수 있습니다. 그러나 기존의 데이터 검색 작업과 비교할 때 작동에 중요한 차이점이 있습니다. 세분화된 구성은 디스커버리를 위해 테이블의 지정된 열만 스캔하고 기록으로 결과를 보고합니다. 세분화된 결과라고 하는 세분화된 구성 스캔의 결과에는 기록당 작업이 지정되어 있으며 data_privacy_admin 역할이 익명화되어야 합니다.

데이터 디스커버리 작업 구성

데이터 디스커버리 작업을 구성하고 진행 중인 작업의 상태를 검토합니다. 데이터 디스커버리 작업은 대상 테이블에서 패턴이 실행되는 시기를 정의합니다.

시작하기 전에

필요한 역할: data_discovery_admin

프로시저

1. 다음으로 이동 시스템 보안 > 데이터 디스커버리(클래식) > 데이터 디스커버리 작업.
2. 데이터 디스커버리 작업 목록에서 새로 만들기를 선택합니다.
3. 데이터 디스커버리 작업 필드 양식의 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 디스커버리 작업 필드

필드	설명
이름	작업의 이름입니다.
설명	작업에 대한 설명입니다.
스캔 유형	스캔할 항목 수입니다. 가능한 상태는 다음과 같습니다. ◦ 샘플: 항목 10,000개를 검사합니다. ◦ 전체: 모든 항목을 검색합니다.
첨부 파일 스캔	첨부 파일에 중요한 데이터 패턴이 있는지 검사합니다. .pdf 또는 .doc 파일에 포함된 이미지는 민감한 데이터를 검사하지 않습니다. ⚠ 경고: 이 기능을 사용하려면 데이터를 통제된 ServiceNow 환경으로 보내야 합니다. 활성화하기 전에 이 기능을 사용하는 데 필요한 추가 사용 약관에 동의했는지 확인하십시오.
컨텍스트	스캔한 패턴, 대상 테이블 항목 적중 및 경과 시간에 대한 작업 상세 정보입니다.
상태	데이터 디스커버리 작업의 상태입니다. 가능한 상태는 다음과 같습니다. ◦ 일정 예약 준비 완료: 새 작업의 기본 상태입니다. ◦ 예약됨: 작업이 실행되도록 예약되어 있습니다. ◦ 진행 중: 작업이 활발하게 실행 중입니다. ◦ 완료됨: 작업 실행이 성공적으로 완료되었습니다. ◦ 오류: 오류로 인해 작업 실행이 중지되었습니다. ◦ 취소됨: 작업이 취소되었습니다. ◦ 일시 중지됨: 작업이 일시 중지되었습니다.
요약	작업을 실행한 후의 결과를 표시합니다.
시작 날짜	작업의 시작 날짜를 설정합니다.
기간 시작	이 작업을 실행할 기간의 시작입니다. 이 필드에 입력한 시간 이후에 작업이 실행됩니다. 기간 시작 필드에 입력한 시간은 기간 종료 필드에 입력된 시간 이전이어야 합니다. ⓘ 주: 유효한 시간 값은 24시간 표기법에 따라 조정된 범용 시간입니다.
기간 종료	이 작업을 실행할 기간의 끝입니다. 이 작업은 이 필드에 입력한 시간까지 실행됩니다. 이

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	시간에 작업이 완료되지 않은 경우 작업이 일시 중지되었다가 다음 기간 시작 시 다시 시작됩니다. 기간 종료 필드에 입력한 시간은 기간 시작 필드에 입력한 시간 이후여야 합니다. 주: 유효한 시간 값은 24시간 표기법에 따라 조정된 범용 시간입니다.

4. 제출을 선택합니다.
   작업 예약 및 업데이트 버튼이 나타납니다.
5. 작업을 실행하려면 작업 예약을 선택합니다.
   작업은 기간 시작 필드와 기간 종료 필드에서 선택한 시간 사이에 실행됩니다. 시작 및 종료 기간 동안 작업이 완료되지 않은 경우 다음 기간 시작 시 작업이 계속됩니다.
6. 옵션: 다음 기능 중 하나를 선택합니다.
   - 작업 취소: 작업을 취소합니다.
   - 일시 중지: 작업을 일시 중지합니다.
   - 다시 시작: 일시 중지된 작업을 다시 시작합니다.

패턴 구성 데이터 디스커버리

데이터 디스커버리 패턴을 구성하고 현재 패턴을 검토합니다. 패턴은 데이터 디스커버리 대상 테이블에 대해 데이터를 일치시키는 데 사용되는 정규 표현식을 정의합니다.

시작하기 전에

필요한 역할: data_discovery_admin

프로시저

1. 다음으로 이동 시스템 보안 > 데이터 디스커버리 > 전체 데이터 패턴.
2. 데이터 디스커버리 패턴 목록에서 새로 만들기를 선택합니다.
3. 작업 필드 양식에서 데이터 디스커버리 필드에 내용을 입력합니다.

데이터 디스커버리 작업 필드

필드	설명
내부 범위	패턴의 범위입니다.
설명	작업에 대한 설명입니다.
이름	데이터 패턴의 이름입니다.
애플리케이션	패턴의 적용 범위입니다.
표현식	데이터 패턴을 검색하는 데 사용되는 정규식입니다. 주: 표현식 길이는 1000자 미만이어야 합니다.
키워드(선택 사항)	표현식 주변에서 검색할 특정 단어(또는 쉼표로 구분된 단어)입니다. 키워드 근접성과 함께 사용해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 키워드는 패턴에 대한 추가 컨텍스트를 검색하는 데 사용할 수 있습니다. 예를 들어 키워드를 사용하면 MM/DD/YY 서식이 동일한 경우 생년월일 또는 고용일을 구별하는 데 도움이 될 수 있습니다.
키워드 근접성(선택 사항)	키워드를 검색할 표현식으로부터의 거리입니다. 키워드와 함께 사용해야 합니다. 주: 기본값은 30, 상한은 64입니다.
개인정보 기술 구성	패턴에 사용되는 개인정보 기술
합성 값	패턴을 대체한 값 목록
유형	패턴 유형

4. 제출을 선택합니다.
   - 테스트 버튼을 사용하면 데이터 패턴 목록을 제출하기 전에 정규 표현식을 테스트할 수 있습니다.

예약된 작업에 사용하려면 데이터 패턴을 활성으로 설정해야 합니다.

5. 다음으로 이동 시스템 보안 > 데이터 디스커버리 > 활성 데이터 패턴.
6. Active Pattern(활성 패턴) 데이터 디스커버리 목록에서 Edit(편집)를 선택합니다.
7. 사용 가능한 목록에서 패턴 목록을 선택하고 선택한 목록으로 이동합니다.

기본 데이터 패턴

에 포함된 기본 데이터 패턴 정규 표현식을 데이터 디스커버리검토합니다. 이러한 기본 데이터 패턴을 사용하여 추가 분류를 위해 테이블 항목을 필터링할 수 있습니다.

다음은 데이터 검색에 사용할 수 있는 기본 패턴입니다.

이름	설명	정규 표현식	키워드	예제
기간	0-99세 사이의 사람	\b([0-9]|[1-9][0-9]|1[012][0-9])\b	기간	일치함 24 일치하지 않음 • 103 • -2
생년월일	DD/MM/YYYY 형식을 사용하는 생년월일	\b[0-3]? [0-9]/[0-3]? [0-9]/(?:[0-9]{2})? [0-9]{2}\b	생년월일, 생년월일, 생년월일	일치함 • 06/18/2012 • 1/1/19
이메일	표준 이메일 주소	\b[\w!#$%&'*+/=?'{\|}~^-]+(?:\. [\w!#$%&'*+/=?'{|}~^-]+)*@(?:[a-zA-Z0-9-]+		일치함 • johndoe@emailserver.co • historyprofessor@college

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명	정규 표현식	키워드	예제
		\.)+[a-zA-Z]{2,6}\b		일치하지 않음 • notanemail.com • bademail@.org
차량 식별 번호	차량 식별 번호 (VIN)	\b[A-HJ-NPR-Z0-9]{17}\b		일치함 AHUYA31581L000000
IP 주소	표준 IP 주소	4자리 IP \b(?:(?:25[0-5] | 2[0-4][0-9] | [01]?[0-9][0-9]?)\.){3}(?:25[0-5] | 2[0-4][0-9] | [01]?[0-9][0-9]?)\b 6자리 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}[0-9a-fA-F]{1,4})\b		일치하는 4자리 IP 102.28.46.103 일치하는 6자리 IP 914B:D45A:61EA:6346:59BC
신용 카드 - Visa	Visa 신용 카드 번호	\b4[0-9]{12}(?:[0-9]{3})?\b		일치함 4444434342424242

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명	정규 표현식	키워드	예제
신용 카드 - American Express	American Express 신용 카드 번호	\b3[47][0-9]{13}\b		일치함 378225246366005
신용 카드 - Mastercard	Mastercard 신용 카드 번호	\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		일치함 5555444455554444
신용 카드 - Diners Club	다이너스 클럽 신용카드 번호	\b3(?:0[0-5]|[68][0-9])[0-9]{11}\b		일치함 3056930009020004
신용 카드 - Discover	검색 신용 카드 번호	\b6(?:011|5[0-9]{2})[0-9]{12}\b		일치함 6011025690875424
신용 카드 - CCV	신용 카드 보안 번호	\b[0-9]{3,4}\b	CVV, 검증 코드, 보안 코드	일치함 124
신용 카드 - 만료 날짜	MM/YYYY 형식의 신용 카드 만료	\b(([1-9])|(0[1-9]|1[0-2]))\/?([0-9]{4}|[0-9]{2})\b	만료, 예	일치함 • 02/2027 • 04/23 일치하지 않음 03/9
미국 - 주민등록번호	미국 시민 주민등록번호	\b(?!666|000|9\d{2})\d{3}-(?!00)\d{2}-(?!0{4})\d{4}\b		일치함 001-22-111
미국 - 전화 번호	미국 전화 번호 ⚠ 경고: 미국 전화 코드를 사용하지 않습니다.	\b\(?([0-9]{3})\)?[-.]?([0-9]{3})[-.]?([0-9]{4})\b		일치함 2065550199 일치하지 않음 1 555 238 0199
미국 - 여권 번호	9자리 미국 여권 번호	\b[a-zA-Z0-9]\\d{8}\b		일치함 770022122
미국 - 납세자 ID	미국 납세자 ID 번호	\b(9\d{2})([\-]?)([7]\d|8[0-8])([\-]?)(\d{4})\b		일치함 927 70 5828
미국 - 캘리포니아 주 운전면허 번호	미국 캘리포니아주 운전면허 번호	\b[a-zA-Z]\d{7}\b		일치함 A0002144
미국 - 은행 라우팅 번호	ABA(US Bank Routing) 번호	\b((0[0-9])|(1[0-2])|(2[1-9])|(3[0-2])|		일치함 125210305

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	설명	정규 표현식	키워드	예제
		(6[1-9]) | (7[0-2]) | 80)([0-9]{7})\b		

대상 테이블 구성 데이터 디스커버리

작업에 사용할 데이터 디스커버리 대상 테이블을 추가합니다. 대상 테이블만 데이터 패턴에 대해 스캔됩니다.

시작하기 전에
필요한 역할: data_discovery_admin

이 태스크 정보
데이터 디스커버리 작업이 실행되면 모든 활성 패턴이 있는 모든 대상 테이블에 대해 실행됩니다.

프로시저

1. 선택 시스템 보안 > 데이터 디스커버리(클래식) > 대상 테이블.
2. 새로 만들기를 선택합니다.
3. 테이블 이름 필드에서 대상 테이블을 선택합니다.
4. 제출을 선택합니다.

에 대한 병렬 작업 활성화 데이터 디스커버리

병렬 작업을 사용하여 작업 실행 시간을 줄입니다 데이터 디스커버리 .

시작하기 전에
필요한 역할: 관리자

프로시저
기본적으로 데이터 디스커버리 단일 스레드를 사용하여 작업을 실행합니다. 전체 스캔을 위해 데이터 디스커버리 여러 스레드를 활성화할 수 있습니다.

1. 탐색 필터에 `sys_properties.list`를 입력합니다.
2. `com.glide.data_discovery.max_concurrent_item_workers` 속성 생성
3. 유형이##인지 확인합니다.
4. **중요사항:** 노드당 적은 수의 작업자(2 또는 3)로 시작하는 것이 좋습니다.

   값 필드에 병렬 작업 작업자 수를 최대 5개까지 입력합니다.

데이터 디스커버리 역할

역할을 할당 데이터 디스커버리 하여 특정 데이터 유형에 대한 사용자 액세스를 제한할 수 있습니다.

데이터 검색 관리자 **[sn_data_discovery.data_discovery_admin]**

데이터 패턴 및 관련 작업을 보고, 생성하고, 수정합니다.

- 데이터 패턴:
  - 작성
  - 읽기

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

  - 업데이트
  - 삭제
- 활성 데이터 패턴:
  - 삭제
  - 읽기
- 작업:
  - 작성
  - 읽기
  - 업데이트
  - 삭제
  - 일정
  - 일시 중지
  - 다시 시작
  - 취소
- 대상 테이블:
  - 작성
  - 읽기
  - 쓰기
- 세분화된 구성:
  - 작성
  - 읽기
  - 업데이트
  - 삭제
- 세분화된 결과:
  - 작성
  - 읽기
  - 작업

> **주:** 이 역할을 가진 사용자는 무시 작업만 수행할 수 있습니다

역할 포함

역할에 포함된 역할 목록입니다.

- data_classification_auditor
- data_classification_admin
- sn_data_discovery.data_discovery_api_processor

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특별 고려 사항

제품 설치 시 관리자에게 이 역할이 자동으로 할당됩니다.

주: 보다 전문적인 역할을 사용할 수 있는 경우 관리자 역할을 부여하지 마십시오.

데이터 검색 감사자 **[sn_data_discovery.data_discovery_auditor]**

데이터 패턴과 대상 테이블을 읽습니다.

- 데이터 패턴 읽기
- 활성 데이터 패턴 읽기
- 작업 읽기 데이터 디스커버리
- 대상 테이블 읽기
- 세분화된 구성 검토
- 세분화된 결과 검토

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

없음.

데이터 분류 관리자 **[data_classification_admin]**

활성화된 특정 패턴 찾기가 분류될 때 데이터 패턴, 검색 작업 및 data_classification 테이블을 읽습니다.

역할 포함

데이터 분류 역할에는 data_classification_auditor 역할에 포함된 역할 목록이 포함되어 있습니다.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

주: 데이터 분류 관리자 역할에 대한 자세한 내용은 다음 문서를 참조하십시오 플러그인 데모 데이터 설치 데이터 분류 중.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 디스커버리 작업 결과

데이터 디스커버리 결과 페이지에는 작업에서 찾은 데이터에 대한 상세 정보가 표시됩니다. 발견 사항 페이지를 사용하여 작업 결과를 검토하고 데이터 분류를 시작할 수 있습니다.

데이터 디스커버리 작업을 완료한 후 결과 페이지에 다음 상세 정보가 표시됩니다.

열	설명
딕셔너리 항목	데이터가 있는 대상 테이블의 열
테이블	데이터가 발견된 대상 테이블
데이터 패턴	데이터를 찾는 데 사용되는 데이터 패턴
데이터 패턴 일치 수	데이터 패턴과 일치하는 데이터 항목 수
총 행 스캔 수	작업 중에 스캔된 행의 수
일치하는 행의 백분율	데이터 패턴과 일치하는 대상 테이블의 행 백분율
데이터 디스커버리 직업	대상 테이블에 사용되는 작업
상태	항목의 상태

작업을 실행 데이터 디스커버리 한 후 결과는 New의 상태가 됩니다. 아무 작업도 필요하지 않은 경우 데이터를 그대로 두어도 되며, 이렇게 하면 상태가 자동으로 무시됨으로 설정됩니다. 그렇지 않으면 사용자 정의 데이터 분류를 만드는 등의 방법으로 데이터를 분류하여 도구를 사용하여 데이터 분류 데이터 익명화를 준비할 수 있습니다.

세분화된 결과

사용자는 세분화된 결과 추적 작업을 선택하여 페이지를 사용하여 검색된 특정 기록에 세분화된 결과 대한 작업을 수행할 수 있습니다. 자세한 내용은 세분화된 결과 문서를 참조하십시오.

사용 가능한 보호

사용 가능한 보호 버튼을 선택하여 항목 제어 서비스, 상태, 메모 및 마지막 체크인을 검토합니다. Xanadu 현재 이 기능은 필드 암호화.

Protecton 서비스는 대시보드에서도 액세스할 수 있습니다. 대시보드에 대한 자세한 내용은 을 참조하십시오 데이터 디스커버리.

결과 통합

결과 통합 버튼을 사용하여 작업 결과를 통합할 수 있습니다. 그러면 두 개의 개별 작업 간에 공유된 작업 결과가 가장 최근에 실행된 작업에 통합됩니다.

주: 완료된 전체 스캔 작업만 통합할 수 있습니다.

작업 결과 페이지에서 데이터 데이터 디스커버리 분류

작업의 결과 페이지에서 직접 데이터를 데이터 디스커버리 분류합니다.

시작하기 전에
필요한 역할: data_discovery_admin 및 admin

결과 데이터가 분류된 것처럼 보이려면 먼저 작업이 성공적으로 실행되어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 이동 시스템 보안 > 데이터 디스커버리 > 데이터 디스커버리 작업.
2. 분류하려는 항목을 선택합니다.
3. 데이터 디스커버리 결과 목록에서 분류를 선택합니다.
4. 테이블 항목과 연결할 데이터 분류를 선택합니다.
5. 분류를 선택합니다.

데이터 디스커버리 지원되는 데이터 유형

를 사용할 데이터 디스커버리때 지원되는 필드 유형을 확인합니다.

주: 분류된 모든 필드 유형을 에 사용할 데이터 디스커버리수 있는 것은 아닙니다.

일부 고위험 필드 유형은 테이블에 설명된 대로 기본적으로 꺼져 있습니다. 필드에 대한 자세한 내용은 필드 유형을 참조하십시오.

데이터 디스커버리에 지원되는 필드 유형

필드 유형	기본적으로 사용 가능
오디오	아니요
조건	아니요
condition_string	아니요
통화	예
10진수	예
due_date	예
부동	예
glide_date	예
glide_date_time	예
glide_duration	아니요
glide_time	예
HTML	아니요
아이콘	아니요
정수	예
ip_addr	아니요
ip_address	아니요
일지	예
journal_input	예
journal_list	예
경도	예
name_values	아니요
percent_complete	아니요

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 유형	기본적으로 사용 가능
phone_number_e164	예
가격	예
문자열	예
string_full_utf8	예
translated_html	아니요
translated_text	아니요
URL	아니요
user_image	아니요
비디오	아니요
wiki_text	아니요

세분화된 구성으로 스캔

세분화된 스캔을 사용하여 디스커버리에 대한 특정 테이블 열을 스캔할 수 있습니다. 기존 데이터 디스커버리 작업은 전체 테이블을 스캔하여 데이터를 검색하는 반면, 세분화된 스캔은 테이블의 특정 열을 대상으로 하므로 검색 프로세스를 더 잘 제어할 수 있습니다

시작하기 전에

필요한 역할: admin, sn_data_discovery_admin, data_privacy_admin

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 데이터 디스커버리(클래식) > 세분화된 구성.
2. 세분화된 구성 목록에서 새로 만들기를 선택합니다.
3. 세분화된 구성 필드 양식의 필드에 내용을 입력합니다.

세분화된 구성 필드

필드	설명
딕셔너리 항목	스캔할 열입니다.
테이블	스캔할 테이블입니다.
열 레이블	스캔할 열의 레이블
스캔 시작점	중요한 데이터는 스캔 시작 지점 당일과 그 이후에만 검색됩니다. 주: 스캔 시작점을 비워 두면 열의 모든 항목이 스캔됩니다. 스캔 시작점이 변경되면 새로 구성된 타임스탬프에서 시작하도록 스캔이 재설정됩니다.
활성	세분화된 구성을 활성화하려면 선택합니다.

4. 제출을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성을 위해 확장 가능한 테이블의 하위 항목을 선택할 수 있습니다.

5. 옵션: 상위 테이블에 대한 세분화된 구성을 선택하고 하위 테이블 선택을 선택한 다음 스캔할 하위 테이블을 선택합니다.

결과
대상 테이블의 특정 열은 디스커버리를 위해 스캔됩니다. 세분화된 스캔은 활성 데이터 패턴의 데이터 패턴을 사용합니다. 다음에서 결과를 검토하고 조치를 취할 수 있습니다. 모두 > 시스템 보안 > 데이터 디스커버리(클래식) > 세분화된 결과. 자세한 내용은 세분화된 결과 문서를 참조하십시오.

세분화된 결과

세분화된 결과는 세분화된 결과 도구를 사용하여 검토할 수 있습니다.

세분화된 결과 검토

세분화된 결과는세분화된 구성에서 최대 500개의 결과를 검토하는 데 사용됩니다. 결과가 500개 있는 경우 작업이 수행될 때까지 세분화된 구성 검사가 일시 중지됩니다.

열 레이블	설명
기록	검색된 기록입니다.
테이블	기록의 상위 테이블입니다.
열	중요한 정보가 검색된 기록의 열입니다.
데이터 패턴	기록을 검색하는 데 사용되는 패턴입니다.
동작	결과에 대해 수행할 동작 변경하려면 선택 **중요사항:** 기록에 대한 익명화 작업을 수행하려면 data_privacy_admin 역할이 필요합니다. 검토 기록이 검토 대기 중입니다. 이것은 새로운 세분화된 검색에 할당됩니다. 무시 기록에 대해 아무 작업도 수행되지 않습니다. 익명화 기록이 익명화됩니다.
상태	기록 상태입니다. 신규 처음 보고된 시점의 찾기에 할당된 상태 처리됨 사용자가 선택한 작업이 찾은 결과에 성공적으로 적용된 경우 주: 처리된 결과는 삭제되기 전에 세분화된 결과 테이블에 3일 동안 저장됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

열 레이블	설명
	수동 검토 사용자 선택 작업을 적용할 때 실패했습니다. ⚠ 경고: 수동 검토의 결과는 적절한 조치를 취한 후 사용자가 삭제해야 합니다.

⚠ 경고: 세분화된 결과에서 트리거된 익명화에 대해서는 롤백이 지원되지 않습니다.

데이터 분류

미리 정의되었거나 사용자 정의된 데이터 분류를 사용하여 데이터를 유형별로 그룹화합니다. 할당된 데이터 분류 관리자 또는 감사자 역할이 있는 경우 다양한 데이터 분류를 관리하거나 인스턴스 내에서 각종 데이터의 현재 상태를 시각적으로 분석할 수 있습니다.

데이터 분류 탐색



데이터 분류에 대해 알아봅니다.

데이터 분류 구성



고유한 데이터 클래스를 만들고 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 분류에 대한 참조



데모 데이터를 사용하여 데이터 분류가 작동하는 방식을 알아보십시오.

데이터 분류 분석



데이터 분류를 분석하는 방법을 알아봅니다.

데이터 분류 탐색

데이터 분류에 대해 탐색합니다.

데이터 분류 다음에 대한 지원 활성화:

- 인스턴스에 호스팅된 데이터 유형에 대한 Now Platform 가시성
- 개인 정보 보호법을 준수하고 금융 서비스 및 의료 장치 제조와 같은 산업에 대한 규제 요구 사항을 충족합니다.

데이터 분류

데이터 분류는 테이블의 기존 딕셔너리 항목에 데이터 분류를 수동으로 적용하는 독립 실행형 프로세스입니다. 자세한 내용은 데이터 딕셔너리 테이블 문서를 참조하십시오.

- 비즈니스에 적합하다고 판단되는 대로 데이터를 분류하고 필요에 따라 사용 가능한 데이터 클래스를 변경할 수 있습니다.
- 데이터를 분류할 때 미리 정의된 데이터 분류를 사용하거나 직접 생성할 수 있습니다. 사전 정의된 데이터 분류를 사용하는 것은 선택 사항이지만 시작점으로 사용하는 것이 좋습니다. 이러한 사전 정의된 데이터 분류는 인스턴스에 설치할 수 있는 데모 데이터에 포함되어 있습니다. 자세한 내용은 및 데모 데이터와 함께 데이터 분류 설치되는 구성요소를 참조하십시오플러그인 데모 데이터 설치 데이터 분류 중.
- 고유한 데이터 분류를 만드는 경우 상위 및 하위 데이터 분류를 사용하여 계층화된 계층 구조 시스템을 디자인할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요 대시보드

개요 대시보드를 사용하여 현재 데이터 테이블이 다양한 데이터 분류에 매핑되는 방식을 이해합니다. 또한 전 세계, 지역, 해외 사용자가 데이터 사용 또는 액세스와 관련하여 데이터 분류에 대해 어떻게 다른 접근 방식을 요구할 수 있는지 분석할 수 있습니다. 개요 대시보드 내용과 레이아웃을 필요에 맞게 사용자 지정할 수도 있습니다.

사용 가능한 스크립트 및 REST API를 사용하여 기존 프로세스, 워크플로우 및 애플리케이션 내에서 분류 메타데이터를 적용하는 방법을 알아보려면 다음을 참조하십시오.

- 데이터 분류 - REST API
- DCManager - 전역
- ScopedDCManager - 범위 지정됨

주: 데이터 분류 은 도메인 분리를 지원하며 data_classification 테이블 자체는 프로세스 분리됩니다.

사용 케이스

GDPR(General Data Protection Regulation)은 개인에게 자신의 개인 데이터에 대한 통제권을 제공하는 것을 목적으로 하는 유럽 연합 규정입니다. 개인 식별 정보와 같은 데이터 분류를 사용하여 인스턴스에서 개인 데이터가 저장되는 위치를 식별할 수 있습니다. 개인 데이터가 유출되지 않도록 보호하기 위해 적절한 보안 메커니즘을 적용함으로써 조직은 GDPR 요구 사항을 충족합니다.

에 고객 정보를 Now Platform저장하는 경우 필요한 경우 PII(개인 식별 정보) 분류 코드를 사용하여 현지 개인정보 보호법의 규제를 받는 데이터를 추적합니다. 데모 데이터를 설치하면 이 분류 코드가 사용자 [sys_user] 테이블의 보안에 민감한 특정 필드에 자동으로 적용됩니다. 자세한 내용은 다음을 참조하십시오.

- 데모 데이터와 함께 데이터 분류 설치되는 구성요소
- 딕셔너리 항목에 데이터 분류 지정

SSN(사회 보장 번호)과 같은 중요한 직원 정보를 저장하는 직원 테이블 열에 제한된 데이터 분류를 적용할 수 있습니다. 그러면 관리자와 감사자가 개요 대시보드를 사용하여 올바른 열에 데이터 분류를 할당했는지 확인할 수 있습니다. 또한 제한된 유형의 정보에 대한 분류 상세 정보를 볼 수도 있습니다.

플러그인 데모 데이터 설치 데이터 분류 중

(및 그 이상으로) 데이터 분류 업그레이드하거나 설치하면 Yokohama (com.glide.data_classification) 플러그인이 자동으로 활성화됩니다. 그러나 플러그인과 함께 제공되는 데모 데이터를 수동으로 설치해야 합니다. 여기에는 몇 가지 중요한 사전 정의된 데이터 분류가 포함되며, 그 중 하나를 인스턴스의 특정 사용자[sys_user] 테이블 열에 할당하기도 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
데모 데이터를 설치하는지 여부에 관계없이 활성화된 데이터 분류 플러그인은 인스턴스에 다음 사용자 역할을 추가합니다.

- data_classification_admin: 데이터 분류 설정 및 할당을 포함하여 애플리케이션의 모든 측면을 데이터 분류 관리할 수 있습니다.
- data_classification_auditor: 사용자 테이블 및 열에 대한 코드 할당을 감사 데이터 분류 할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항: 고객의 사용에 관한 고지:

본 애플리케이션 구현과 관련된 모든 결정은 전적으로 고객의 결정에 달려 있습니다. 고객은 애플리케이션 사용이 ServiceNow가 어떠한 법률이나 규제를 준수한다고 말하지 않으며, 애플리케이션 사용 시 제안하는 언어, 필드 또는 분류가 ServiceNow에 의한 법적 조언을 구성하지 않는다는 것을 인정하고 이에 동의합니다.

데이터 보호법, 보안 요구 사항 및 개인정보 보호법을 포함하고 이에 국한되지 않는 적용되는 법률에 따른 고객의 법적 의무사항을 이행할 책임은 전적으로 고객에게 있으며, 고객의 요구사항을 충족하기 위해 템플릿을 포함하되 이에 국한되지 않는 이 애플리케이션을 구성하고 필요한 수정을 수행할 책임은 고객에게 있습니다.

프로시저

1. 다음으로 이동 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 데이터 분류 필터 조건과 검색 창을 사용하여 플러그인을 찾습니다.
   플러그인을 찾으면 ### 메시지가 나타납니다.
3. 세 개의 수직 점이 있는 아이콘을 클릭한 다음 복구를 선택하여 플러그인 활성화 대화창에 액세스합니다.
4. 데모 데이터 로드를 선택한 다음 복구를 클릭합니다.

데모 데이터와 함께 데이터 분류 설치되는 구성요소

(com.glide.data_classification) 플러그인에 데이터 분류 포함된 데모 데이터를 설치하면 여러 유형의 구성요소가 인스턴스에 설치됩니다. 이러한 구성요소에는 특정 사용자[sys_user} 열에 대한 사전 정의된 데이터 분류 및 코드 할당이 포함됩니다.

설치되는 데이터 분류

데이터 분류	설명
기밀	손상될 경우 운영에 부정적인 영향을 미칠 수 있는 민감한 데이터입니다.
내부	공개를 위한 것이 아닌 내부 데이터입니다.
개인 식별 정보	PII라고도 합니다. 특정 개인을 식별하는 데 사용될 수 있는 데이터입니다.
공개	대중에게 자유롭게 공개될 수 있는 데이터.
제한함	손상될 경우 조직이 재정적 또는 법적 위험에 처할 수 있는 매우 민감한 회사 데이터입니다.

데이터 분류 할당

테이블	할당된 열	할당된 데이터 분류
sys_user	우편번호	개인 식별 정보
sys_user	first_name	개인 식별 정보
sys_user	이메일	개인 식별 정보
sys_user	구/군/시	개인 식별 정보
sys_user	middle_name	개인 식별 정보

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블	할당된 열	할당된 데이터 분류
sys_user	주소	개인 식별 정보
sys_user	mobile_phone	개인 식별 정보
sys_user	last_name	개인 식별 정보
sys_user	국가	개인 식별 정보
sys_user	성별	개인 식별 정보
sys_user	이름	개인 식별 정보
sys_user	사진	개인 식별 정보
sys_user	상태	개인 식별 정보
sys_user	home_phone	개인 식별 정보

데이터 분류 생성

[data_classification] 테이블에서 사용자 정의 데이터 분류 데이터 분류 를 생성한 다음 특정 테이블의 특정 열에 할당할 수 있습니다.

시작하기 전에

필요한 역할: data_classification_admin, admin

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 데이터 분류 > 데이터 클래스.
2. 새로 만들기를 선택합니다.
3. 양식에서 필드에 입력합니다.

필드	설명
분류 이름	데이터 분류의 이름입니다.
설명	데이터 분류에 대한 설명입니다.
상위	이 데이터 분류가 종속되는 상위 데이터 분류의 이름입니다. 이 데이터 분류가 상위-하위 데이터 분류가 아닌 경우 필드를 비워두십시오.
애플리케이션	이 데이터 분류에 대한 애플리케이션 범위입니다.

4. 이 데이터 분류가 상위 데이터 분류에서 하위 데이터 분류여야 하는 경우 새로 만들기를 클릭합니다. 하위 데이터 분류를 생성하지 않으려면 이 단계를 건너뜁니다.
5. 양식에서 필드에 입력합니다.

제목

필드	설명
분류 이름	하위 데이터 분류의 이름입니다.
설명	하위 데이터 분류에 대한 설명입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
상위	이 데이터 분류가 종속되는 상위 데이터 분류의 이름입니다. 이 데이터 분류가 상위-하위 데이터 분류가 아닌 경우 필드를 비워두십시오.
애플리케이션	이 하위 데이터 분류에 대한 애플리케이션 범위입니다.

6. 제출을 클릭합니다.

딕셔너리 항목에 데이터 분류 지정

사전 [sys_dictionary] 테이블의 특정 테이블 열에 데이터 분류를 할당합니다. 데이터 분류를 할당하면 Dictionary-Data Class [m2m_dictionary_dataclass] 테이블에 항목이 생성되어 개요 대시보드에서 검토할 수 있습니다.

시작하기 전에
필요한 역할: data_classification_admin 및 admin

프로시저

1. 탐색기 창에서 `sys_dictionary.list#` 입력합니다.
2. 딕셔너리 항목에서 특정 데이터 분류를 할당할 각 요소를 선택합니다.
3. 요소를 선택한 후 선택한 행에 대해 작업을 클릭한 다음 분류를 선택합니다.

   주: 선택한 사전 요소에 대해 이전에 할당된 데이터 분류를 지우려면 분류 지우기를 선택할 수 있습니다.

4. Assign to data class 대화 상자가 나타나면 선택한 사전 요소에 할당할 데이터 분류를 선택한 다음 **Classify**를 클릭합니다.

   경고: 선택한 사전 항목에 대한 모든 기존 분류를 덮어씁니다.

   필요에 따라 여러 데이터 분류를 선택할 수 있습니다.

   자세한 내용은 데이터 딕셔너리 테이블 문서를 참조하십시오.

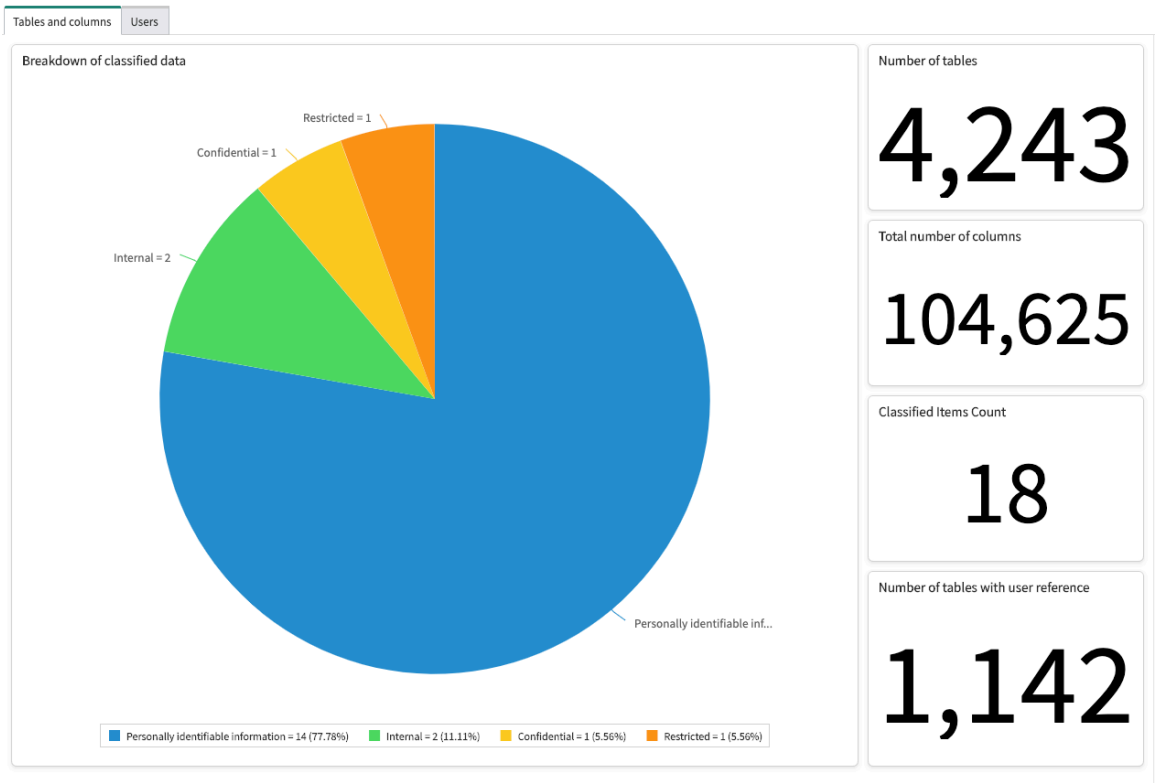
개요 대시보드를 사용하여 데이터 분류 분석

개요 대시보드는 인스턴스 내 데이터 분류의 현재 상태와 사용자들이 위치별로 분포되는 방식을 보고합니다.

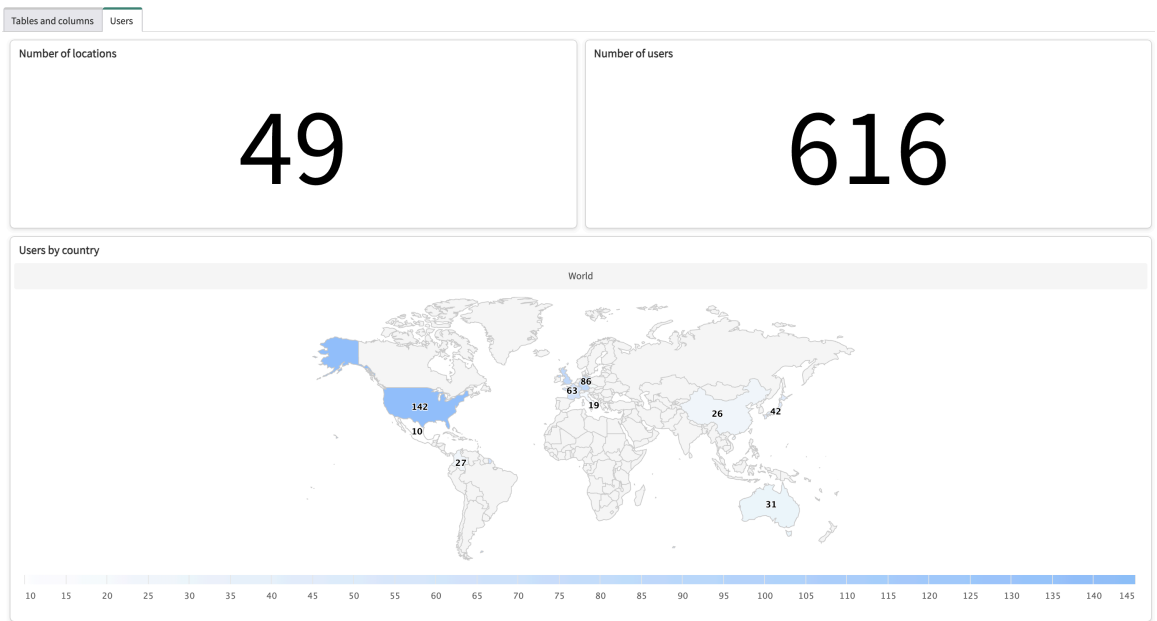
데이터 분류 관리자 또는 감사자 역할이 있는 경우 인스턴스 데이터의 현재 민감도를 시각화하여 보안 및 개인정보 보호법 준수를 강화할 수 있습니다. 관리자는 사용자 기록의 위치 필드를 사용하여 개인정보 보호 규정이 다른 여러 지역에 걸쳐 사용자를 매핑합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블 및 열 탭



사용자 탭



필요한 **Now Platform** 역할

- data_classification_admin: 데이터 분류 설정 및 할당을 포함하여 애플리케이션의 모든 측면을 데이터 분류 관리합니다.
- data_classification_auditor: 코드 할당을 감사합니다 데이터 분류 .

사용 케이스

조직 내 다른 사람이 이 대시보드를 사용하는 방법에 대한 추가 예는 의 데이터 분류사용 사례를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자	대시보드 사용
data_classification_admin	인스턴스의 올바른 필드에 데이터 분류를 할당했는지 확인합니다.
data_classification_auditor	인스턴스에 있는 데이터의 노출성 및 보안을 감사합니다.

보고서

제목	유형	소스 테이블	설명
분류된 데이터의 세부 항목	도넛형 차트	m2m_dictionary_datacls	데이터 클래스별로 인스턴스 데이터 분류에 대한 세부 항목을 제공하며 총계는 중앙에 표시됩니다.
총 테이블	단일 점수	sys_dictionary	전체 사전의 총 데이터 테이블 수입니다.
총 열 수	단일 점수	sys_dictionary	전체 사전에서 분류된 데이터 열의 총 수입니다.
사용자 참조 열	단일 점수	sys_dictionary	사전의 총 사용자 참조 열 수입니다.
사용자 위치 수	단일 점수	sys_user	사용자에 대해 찾은 총 고유 위치 수
사용자 수	단일 점수	sys_user	인스턴스의 총 사용자 기록 수입니다.
국가별 사용자	지도	sys_user	국가별 사용자 기록 세부 항목입니다.

도메인 분리 및 데이터 분류

에 대한 데이터 분류 도메인 분리가 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 강화

- 기본 및 표준 지원 수준의 모든 측면을 포함합니다.
- 서비스 제공자 고객은 데이터 기반 프로세스를 통해 정의된 사용 사례를 기반으로 하는 비즈니스 논리를 수정할 수 있습니다. 이러한 구성은 한 고객의 구성이 다른 고객에 영향을 주지 못하도록 UI 기반 및 페일 세이프로 되어 있습니다.
- 인스턴스 테넌트는 자신을 위한 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성할 수 있어야 합니다. 이 논리와 매개변수는 애플리케이션의 정상적인 기능에 필요합니다.

샘플 사용 사례: 공유 환경의 테넌트 고객이 자신의 도메인 내에서 우선순위를 설정하기 위해 영향, 긴급도, 우선순위 매트릭스를 수정할 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 분류에서 도메인 분리가 작동하는 방식

도메인 분리를 위해 애플리케이션은 [sys_data_classification] 테이블에 대한 프로세스 분리를 데이터 분류 사용합니다. Dictionary-Data Class [m2m_dictionary_dataclass] 테이블의 경우 데이터 분리를 사용합니다. 데이터 및 프로세스 분리에 대한 자세한 내용은 도메인 분리 설명을 참조하십시오.

관련 정보

- 서비스 제공자용 도메인 분리

데이터 익명화

익명화는 식별할 수 없으며 데이터 개인정보 보호 규정을 더 준수하도록 데이터를 쉽게 변환할 수 있는 방법을 제공합니다.

관리자는 프로덕션 및 비프로덕션 인스턴스 모두에서 익명화 프로세스를 수행할 수 있습니다. 데이터 개인정보 보호는 프로덕션 인스턴스에서 사용자 식별을 해제하는 데 사용할 수 있습니다. 데이터 클래스의 익명화는 비프로덕션 인스턴스에서만 사용해야 합니다. 이렇게 보존하면 이메일 주소나 실제 주소와 같은 데이터가 형식이 유사하지만 익명화된 버전으로 대체됩니다.

관리자는 GDPR(General Data Protection Regulation) RTBF(Right to be Forgotten) 프로세스의 일부로 익명화를 사용하여 사용자 정보를 익명화할 수도 있습니다. 자세한 내용은 https://gdpr-info.eu/art-17-gdpr/ 문서를 참조하십시오.

데이터 개인정보 보호의 익명화 섹션을 사용하여 개인정보 보호 정책 및 기술을 생성 및 조회하고 개인정보 대량 할당을 수행합니다. 설명, 사용된 개인 정책 및 상태와 함께 모든 작업을 봅니다. 익명화 섹션에 액세스하려면 관리자는 먼저 data_privacy_admin 및 data_privacy_processor 역할로 격상해야 합니다.

익명화 기술

익명화 기술은 데이터를 익명화하는 방법을 결정하기 위해 선택하는 옵션입니다. 익명화 작업에서 참조할 익명화 기술을 생성해야 합니다. 개인정보 기술을 연관된 익명화 기술 구성에 연결하려면 을(를) 참조하십시오익명화 기술 생성.

익명화 정책

익명화 정책을 구성하여 데이터를 익명화할 때 사용되는 데이터 개인정보 보호 기술을 지정합니다. 자세한 내용은 익명화 정책 생성 다음을 참조하십시오.

익명화 작업

익명화 작업은 이러한 모든 구성요소를 사용하여 데이터를 익명화합니다. 이러한 작업에 대한 자세한 내용은 다음 문서를 참조하십시오 익명화 작업 생성.

익명화 기술 생성

데이터 개인정보 보호 기술 구성을 생성하여 데이터 개인정보 보호가 데이터를 익명화하는 방법을 사용자 지정합니다.

시작하기 전에
필요한 역할: data_privacy_admin 및 admin

프로시저

1. **data_privacy_admin** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 다음으로 이동 시스템 보안 > 데이터 개인정보 보호 > 익명화.
3. 기술 보기를 선택합니다.
   선택할 수 있는 몇 가지 사전 정의된 기술이 있습니다.

기술	설명
선택적 바꾸기	이 기술은 String 데이터를 선택적으로 대체합니다. 입력의 시작과 끝 인덱스 사이의 모든 문자가 선택한 문자로 대체됩니다. 마스킹에서 제외할 문자를 지정할 수 있습니다. ◦ start_index: 기술은 지정된 문자에서 시작하는 데이터를 마스킹합니다. 공백으로 두면 마스킹이 첫 번째 문자로 시작됩니다. ◦ end_index: 기술은 문자열의 시작부터 지정된 문자까지 데이터를 마스킹합니다. 공백으로 두면 마스킹이 마지막 문자로 끝납니다. ◦ exclude_char: 마스킹에서 제외할 문자를 정의합니다. ◦ replacement_char: 마스킹에 사용되는 문자를 정의합니다. 제공되지 않은 경우 별표(*)가 기본적으로 사용됩니다.
정적 바꾸기	이 기술은 값을 정적 값으로 교환합니다. 문자열, 숫자 및 날짜 데이터는 이 기술을 사용할 수 있습니다. ◦ date_time_value: 날짜 값을 이 날짜로 바꿉니다. yyyy-MM-dd HH:mm:ss 형식을 사용합니다. ◦ date_value: 날짜 값을 이 날짜로 바꿉니다. yyyy-MM-dd 형식을 사용합니다. ◦ number_value: 번호 값을 이 숫자로 바꿉니다. ◦ string_value: 문자열 값을 이 텍스트로 바꿉니다. ◦ number_type: 정수를 허용합니다.
무작위 바꾸기	이 기술은 값을 임의로 생성된 값으로 바꿉니다. 문자열 및 번호 데이터는 이 기술을 사용할 수 있습니다.
제거	이 기술은 값을 제거하고 비어 있는(null) 값으로 대체합니다.
작업 없음	이 기술은 자리 표시자입니다. 선택해도 필드는 수정되지 않습니다.
X로 선택적 바꾸기	문자열 데이터를 변환하고 중요한 문자를 문자 X로 선택적으로 대체합니다. 주: 의 데이터 디스커버리 탐색데이터 패턴에 대한 기본 기술입니다.
데이터 패턴 익명화	구조화되지 않은 데이터 필드 내에서 검색된 데이터 패턴만 익명화하며 기본 컨텍스트는 그대로 유지합니다. 주: 이 기술에 대한 설정은 의 데이터 패턴 익명화 기술 설정을 참조합니다 데이터 디스커버리 탐색.

4. 미리 정의된 기술을 사용하지 않는 경우 사용자 지정 기술 추가를 선택합니다.
5. 기술 사용자 지정 양식의 필드에 내용을 입력합니다.

필드1	설명
기본 기술	사용자 지정 기술은 미리 정의된 기술을 기반으로 하므로 미리 정의된 기술을 선택합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드1	설명
기술 이름	기술의 이름을 입력합니다.
기술 설명	기술에 대한 설명을 입력합니다.

6. 다음을 선택합니다.
7. 기술 매개변수를 입력합니다.
   사용 가능한 매개변수화된 값은 선택한 개인정보 보호 기술에 따라 다릅니다. 작업 없음 및 제거 기술에 대한 매개변수화된 값은 없습니다.

기본 기술에 대한 개인정보 매개변수형 값

기본 기술	개인정보 기술 매개변수 값	설명	기본값
선택적 바꾸기	end_index	기술은 문자열의 시작부터 지정된 문자까지 데이터를 마스킹합니다. 비워 두면 마스킹이 마지막 문자로 끝납니다.	(비어 있음)
선택적 바꾸기	exclude_char	마스킹을 건너뛸 문자입니다. 이 값에는 단일 문자만 사용할 수 있습니다. 두 개 이상 입력하면 첫 번째 문자가 사용됩니다.	(비어 있음)
선택적 바꾸기	replacement_char	선택적 바꾸기를 사용하여 값을 바꿀 때 사용할 문자입니다.	다른 값을 입력하지 않으면 별표(*)가 사용됩니다.
선택적 바꾸기	start_index	기술은 지정된 문자에서 시작하는 데이터를 마스킹합니다.	공백으로 두면 마스킹이 첫 번째 문자에서 시작됩니다.
정적 바꾸기	date_time_value	날짜 및 시간 값을 이 날짜로 대체합니다. yyyy-MM-dd HH:mm:ss 형식을 사용합니다.	1988-11-11 10:10:10
정적 바꾸기	date_value	날짜 값을 이 날짜로 대체합니다. yyyy-MM-dd 형식을 사용합니다.	1988-11-11
정적 바꾸기	number_value	번호 값을 이 숫자로 대체합니다.	1234567
정적 바꾸기	string_value	문자열 값을 이 텍스트로 대체합니다.	TEXT123
무작위 바꾸기	preserve_data_length	데이터 길이를 유지하려면 **true** 로 설정합니다. 식별되지	예

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 기술	개인정보 기술 매개변수 값	설명	기본값
		않은 데이터는 원래 데이터와 길이가 같습니다.	

8. 사용자 지정 기술 만들기를 선택합니다.
   사용자 지정 기술이 익명화 기술에 추가됩니다.

다음에 수행할 작업
데이터를 익명화할 때 사용되는 기술을 지정하려면 익명화 정책을 구성하려면 섹션을 참조하십시오 익명화 정책 생성 .

익명화 정책 생성

데이터를 익명화할 때 사용되는 기술을 지정하도록 익명화 정책을 구성합니다.

시작하기 전에
데이터 개인정보 보호 구성은 사용 사례에 따라 테이블, sys_user 및 기타, 식별되지 않은 열을 정의하고 데이터를 익명화하는 동안 사용할 기술의 매개변수화된 유형을 지정합니다.

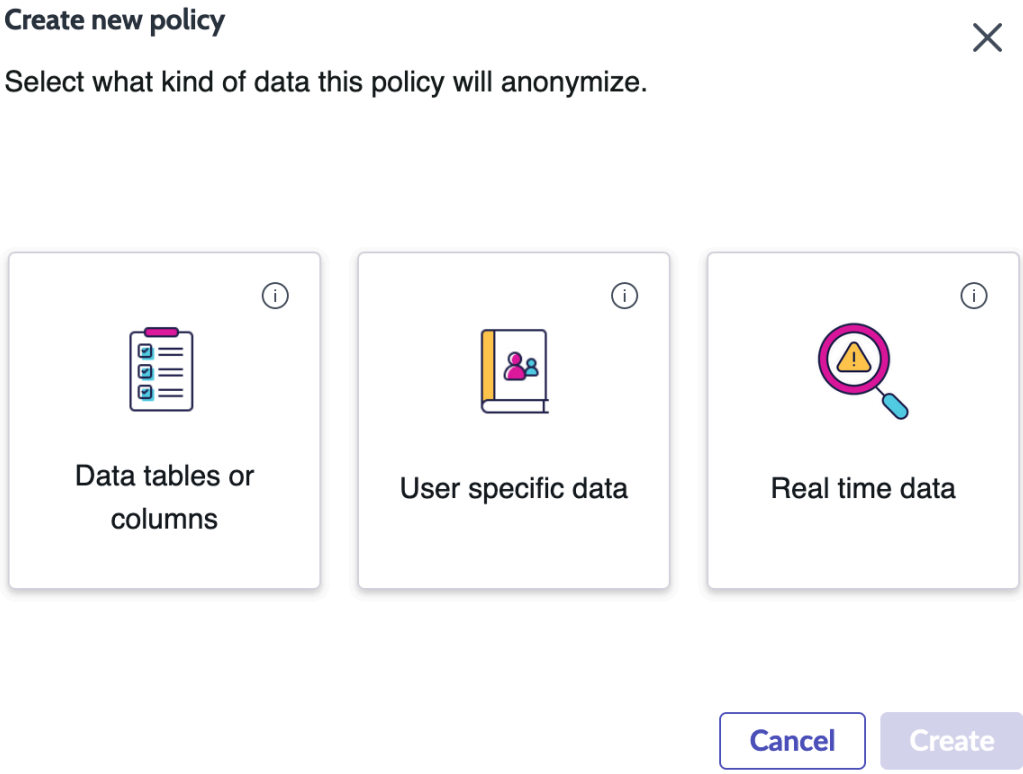
주: 개인정보 구성을 완료하려면 먼저 데이터 개인정보 보호 기술 구성을 구성해야 합니다. 자세한 내용은 익명화 기술 생성 문서를 참조하십시오.

필요한 역할: data_privacy_admin 및 admin

프로시저

1. **data_privacy_admin** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.
2. 다음으로 이동 시스템 보안 > 데이터 개인정보 보호 > 익명화.
   모든 익명화 정책이 표시됩니다. 게시된 정책을 사용하여 익명화 작업을 예약할 수 있습니다.
3. 새 정책 만들기를 선택합니다.
4. 데이터 테이블 또는 열, 사용자별 데이터 또는 실시간 데이터를 익명화하려면 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



데이터 유형	설명
데이터 테이블 또는 열	데이터 정책과 일치하는 기록은 익명화됩니다.
사용자별 데이터	익명화할 사용자 또는 사용자 그룹 세트를 선택합니다.
실시간 데이터	열 세트에 대한 실시간 항목을 익명화합니다.

데이터 개인정보 보호 정책은 분류된 데이터에만 적용할 수 있으며, 데이터 분류에 대한 자세한 내용은 을 참조하십시오 데이터 분류.

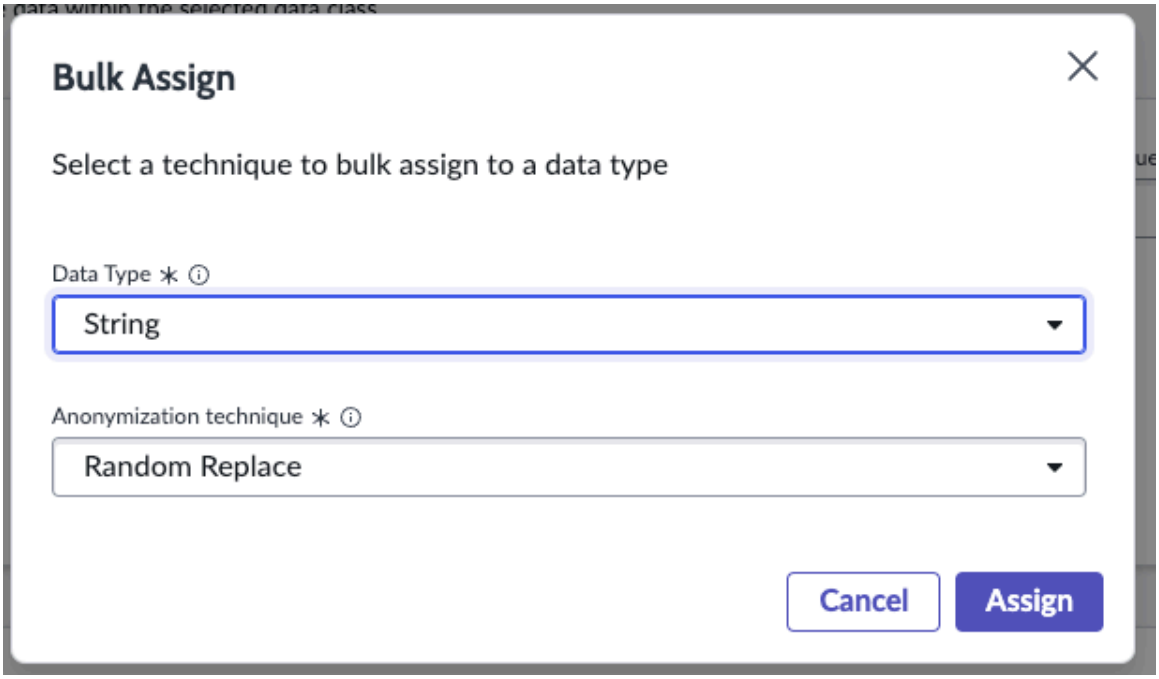
5. 생성을 선택합니다.
정책을 완료하고, 상세 정보를 정의하고, 기술을 할당하는 데 필요한 순차적 단계가 있습니다. 사용자 관련 데이터에 대한 정책을 정의할 때도 사용자 참조 선택이 필요합니다.
6. 새 익명화 정책의 세부 정보를 정의합니다.
   - 이름 필드에 정책 이름을 입력하고 설명 필드에 정책 설명을 입력합니다.
   - 데이터 클래스 필드에서 이 정책에 사용할 데이터 클래스를 선택합니다.

   주: 항목을 익명화하지 않는 경우 항목을 비워 두는 대신 **DoNothing** 기술을 선택합니다. 개인정보 보호 기술 구성 필드에 빈 값이 있는 정책은 데이터 개인정보 보호 작업에 사용될 때 실행할 수 없습니다.

데이터 클래스를 선택하면 정의된 데이터 클래스에 대해 반환된 각 기록에 대해 기술 할당 양식이 표시됩니다.

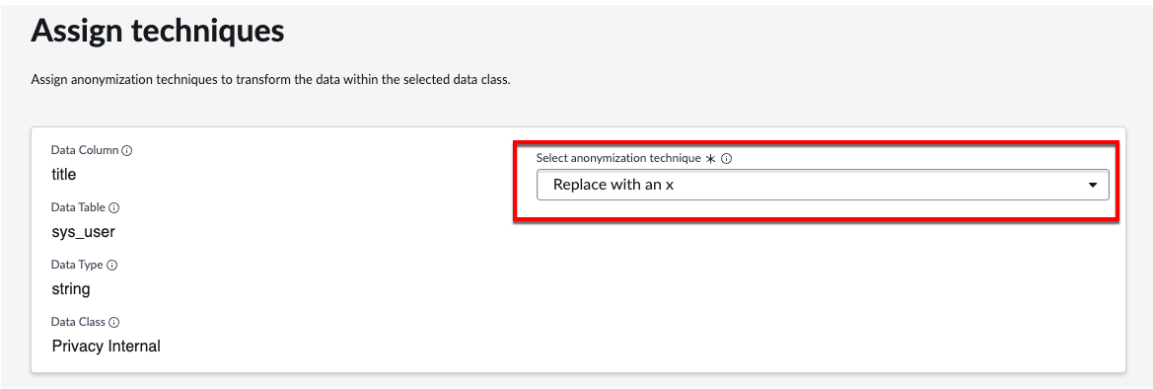
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 선택한 데이터 클래스에 대한 익명화 기술을



할당합니다.

옵션	설명
기술 대량 할당 선택	선택한 데이터 클래스의 모든 데이터 기록에 익명화를 적용합니다. 선택한 데이터 유형의 모든 항목에 적용할 데이터 유형 및 익명화 기술을 선택합니다. 다른 데이터 형식의 추가 대량 할당에 대해 이 단계를 반복합니다. 데이터 유형 목록은 을 참조하십시오 익명화를 지원하는 필드 유형 .
각 데이터 열 기록에 대한 익명화 기술 선택	데이터 개인정보 프로세서 사용자는 데이터 개인정보 보호 작업을 생성할 때 익명화할 기록을 선택할 수 있습니다. 선택한 데이터 클래스의 각 데이터 기록에 익명화를 개별적으로 적용합니다.



8. 옵션: 스캔할 하위 테이블을 입력합니다.
상위 항목의 하위 테이블은 익명화되며, 테이블에 하위 테이블이 없는 경우에는 이 옵션을 사용할 수 없습니다.

⚠ 경고: 하위 작업이 실패하면 상위 작업도 실패합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 옵션: 데이터 패턴 익명화를 선택한 경우 사용할 익명화 기술을 선택합니다.
10. 옵션: 데이터 패턴의 순서를 설정합니다.
11. 옵션:

    팁: 테스트 기능을 사용하여 샘플 입력을 테스트합니다. 스캔 시간, 결과 및 검색된 패턴과 같은 결과에서 메트릭을 검토할 수 있습니다.

    테스트 단추를 선택하여 정책을 테스트합니다.

12. **중요사항:** 모든 테이블에는 올바른 sys_dictionary 항목이 있어야 합니다.

    저장을 선택합니다.
13. 게시를 선택하여 예약에 대한 익명화 정책을 업데이트하고 익명화 정책으로 돌아갑니다.

    주: 게시된 정책만 익명화 작업 예약에 사용할 수 있습니다.

다음에 수행할 작업
익명화 작업 생성.

데이터 익명화 클론 요청 구성

데이터 개인정보 보호 클론 통합은 PostClone 스크립트를 사용하여 대상에 구성된 정책에 대한 데이터 개인정보 보호 작업을 생성하고 실행하도록 구성됩니다. 스크립트를 실행한 후 사용자는 식별되지 않은 데이터를 볼 수 있으며 원래 데이터에는 액세스할 수 없습니다.

시작하기 전에
데이터 개인정보 보호 PostClone 스크립트는 데이터 개인정보 보호 플러그인(sn_dp_store_app)이 활성화되면 설치됩니다. 자세한 내용은 데이터 개인정보 보호 활성화 문서를 참조하십시오.

필요한 역할: data_privacy_clone_processor, data_privacy_admin, admin

프로시저

1. 소스 인스턴스에서 데이터 개인정보 보호 플러그인(sn_dp_store_app)을 활성화합니다.
   데이터 개인정보 보호 PostClone 스크립트가 설치되어 있습니다.
2. **data_privacy_admin** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.
3. 다음으로 이동 시스템 보안 > 데이터 개인정보 보호 > 익명화.
4. 새 정책 만들기를 선택합니다.
   자세한 내용은 익명화 정책 생성 문서를 참조하십시오.
5. 데이터 테이블 또는 열을 선택합니다.
6. 생성을 선택합니다.
7. 이름을 입력하고 데이터 클래스를 선택합니다.
8. 클론 중에 정책을 활성화하려면 선택합니다.
9. 클론 정책이 여러 개인 경우 실행할 정책 순서를 선택합니다.
   더 높은 순서의 작업에 다른 하위 작업과 관련된 테이블이 포함되지 않은 경우, 애플리케이션 순서가 더 높은 Postclone 구성에 대한 데이터 개인정보 보호 작업이 더 낮은 순서의 다른 작업보다 먼저 시작될 수 있습니다.
10. 계속을 선택합니다.
11. 정책 구성을 완료하고 정책을 게시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

12. 데이터 개인정보 보호 구성을 백업합니다.
13. 익명화 작업을 예약합니다.
    자세한 내용은 익명화 작업 생성 문서를 참조하십시오.
14. 데이터 개인정보 보호 관리자로서 복제 요청을 제출합니다.

결과
데이터 개인정보 보호 PostClone 스크립트는 대상 인스턴스에서 실행되고 PostClone 스크립트는 대상 인스턴스에 데이터 개인정보 보호 연합 작업 기록을 생성합니다. 페더레이션 작업은 대상 인스턴스에서 애플리케이션 순서에 따라 각 복제 후 정책에 대한 데이터 개인정보 보호 작업을 생성하고 실행합니다.백업 소스가 대상 인스턴스에 복제됩니다. 데이터 개인정보 보호 PostClone 스크립트는 대상 인스턴스에서 구성된 정책에 대한 데이터 개인정보 보호 작업을 생성하고 실행합니다.

상승된 데이터 개인정보 보호 클론 프로세서는 대상 인스턴스에 로그온하고 dp_federated_job.list 및 dp_job.list에서 클론 후 페더레이션 작업 상태를 모니터링할 수 있습니다.

익명화 작업 생성

프로덕션 인스턴스에서 데이터 개인정보 보호 작업을 구성하여 비프로덕션 인스턴스에서 익명화된 데이터를 사용자 및 데이터 클래스 작업에 사용합니다.

시작하기 전에
데이터 개인정보 보호 작업은 다음 두 가지 익명화 사용 사례를 지원합니다.

- 특정 sys_users의 민감 데이터
- 특정 데이터 클래스의 중요한 데이터입니다.

필요한 역할: data_privacy_processor 및 admin

프로시저

1. **data_privacy_processor** 역할로 승격합니다.
   역할 상승에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하세요.
2. 다음으로 이동 시스템 보안 > 데이터 개인정보 보호 > 익명화.
3. 익명화 정책에서 작업에 사용할 정책에 대해 작업 예약을 선택합니다.
   익명화 작업을 예약하려면 정책이 게시됨 상태여야 합니다.

⚠ 경고: 익명화 작업은 매우 파괴적이며 롤백 시에만 되돌릴 수 있습니다. 작업을 예약하기 전에 처리된 기록, 테이블 등 모든 정보를 다시 한 번 확인하십시오.

4. 양식에서 필드에 내용을 입력합니다.

데이터 개인정보 보호 작업 필드

필드	설명
사용된 정책	이 작업에 사용하기 위해 선택한 개인정보 보호 정책 구성의 읽기 전용 이름입니다. 정책에 대한 추가 정보를 보려면 정책을 편집합니다. 개인정보 보호 정책 구성에 대한 자세한 내용은 문서를 참조하십시오 익명화 정책 생성.
직무 기술서	작업에 대한 설명입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
시작 시간	이 작업을 실행할 시간의 시작(**HH:MM:SS**)입니다.
종료 시간	이 작업을 실행할 기간의 종료(**HH:MM:SS**)입니다. 종료 시간은 시작 시간 이후여야 합니다. 이 필드에 입력된 시간 전에 작업이 실행됩니다. 작업이 아직 완료되지 않은 경우 작업이 일시 중지되었다가 다음에 시작할 때 다시 시작됩니다.
시운전	작업을 테스트로 실행합니다. 이 작업을 실행할 때 영향을 받는 기록은 없습니다. 결과는 작업이 실행된 것처럼 작업 목록에 표시됩니다. 주: 롤백이 있는 데이터 개인정보 보호 작업을 구성할 때 시험 실행을 꺼야 합니다. 자세한 내용은 데이터 개인정보 보호 작업 롤백 문서를 참조하십시오.
사용자 선택 유형	익명화할 사용자 또는 그룹을 선택합니다.
사용자/그룹 선택	이 작업에서 익명화할 특정 사용자 또는 그룹 집합을 선택합니다. 최대 1,000명의 사용자를 지원합니다. 주: 이 필수 필드는 선택한 개인정보 보호 정책 조건에서 사용자 기록을 선택해야 하는 경우에만 표시됩니다.

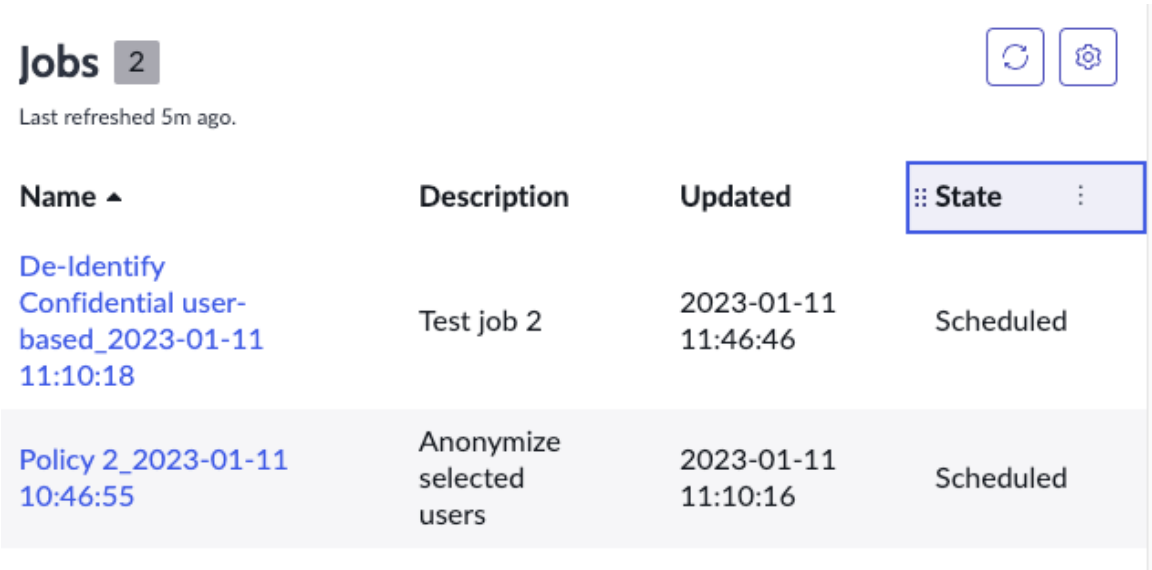
5. 중요사항: 모든 테이블에는 예약 전과 작업 중에 올바른 sys_dictionary 항목이 있어야 합니다.

양식에서 작업 예약을 선택하여 익명화를 작업 큐에 배치합니다.
작업은 시작 시간과종료 시간 필드에서 선택한 시간 사이에 실행됩니다. 시작 및 종료 기간 동안 작업이 완료되지 않은 경우 다음 기간 시작 시 작업이 계속됩니다.

주: 드라이 런을 선택한 경우에도 작업은 한 번만 실행할 수 있습니다. 동일한 정책에 따라 작업을 다시 실행하려면 작업 예약을 선택하고 동일한 필드 값을 사용하여 양식을 작성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

작업이 작업 창에



나열됩니다.

필드	설명
이름	익명화 작업의 이름입니다.
설명	익명화 작업에 대한 설명입니다.
업데이트됨	작업이 마지막으로 업데이트된 날짜 및 시간입니다.
상태	데이터 개인정보 보호 작업의 상태: ◦ 예약됨: 새 작업의 기본 상태입니다. ◦ 완료됨: 작업이 선택한 데이터를 성공적으로 익명화했습니다. ◦ 취소됨: 작업이 수동으로 취소되었습니다. ◦ 오류: 작업을 저장하는 동안 문제가 발생했습니다. 작업 일정을 변경하거나 새 작업을 생성합니다. 오류가 계속되면 구성에 문제가 있을 수 있습니다. ◦ 롤백 진행 중: 익명화를 롤백하도록 작업이 설정되었습니다. ◦ 롤백 완료: 익명화 작업 롤백이 성공적으로 완료되었습니다. 읽기 전용 필드입니다.

6. 작업 창에서 작업을 선택하여 작업 요약을 엽니다.
작업이 예약되면 작업 취소**(Cancel Job**) 및 일시 중지**(Pause**) 버튼이 작업 요약에 나타납니다.

예약된 작업에 대한 추가 필드

필드	설명
추정된 기록 카운트	이 드라이 런 작업이 실행되기 전에 영향을 받는 예상 기록 수입니다. 읽기 전용 필드
처리된 총 데이터 기록	이 작업의 영향을 받는 개별 데이터 기록의 총 수입니다. 읽기 전용 필드입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
처리된 총 데이터 테이블	이 작업에서 처리한 총 데이터 테이블 수입니다. 읽기 전용 필드입니다.
롤백까지 남은 시간	완료된 데이터 익명화 작업을 롤백하고 데이터를 익명화할 수 있는 남은 시간입니다. 읽기 전용 필드입니다.
처리된 총 사용자	이 작업이 영향을 주는 개별 사용자 기록의 총 수입니다. 읽기 전용 필드입니다.
작업 취소	익명화 작업을 취소하려면 선택합니다. 작업 시작 시간 전에 이 항목을 선택해야 합니다. 선택하면 작업 상태가 *##*됨으로 업데이트됩니다.
일시 중지	롤백이 선택된 경우 작업을 일시 중지하고 기록을 롤백하려면 선택합니다. 롤백 컨텍스트에 대한 3일 만료 기간 후에 경고 메시지가 표시됩니다. 작업 시작 시간 후와 작업 종료 시간 전에 선택해야 합니다. 선택하면 작업 상태가 *## ##*됨으로 업데이트됩니다.
다시 시작	일시 중지된 작업을 다시 시작합니다. 일시 중지된 경우 재개된 작업에 대해서는 롤백이 지원되지 않습니다. 작업을 취소하고 데이터 개인정보 보호 작업을 생성합니다. 기록은 만료되지 않은 롤백 컨텍스트를 사용합니다. 선택하면 작업 상태가 *###*으로 업데이트됩니다.
익스포트	데이터 개인정보 보호 작업 상세 정보의 .PDF 파일을 다운로드합니다.

데이터 익명화를 위한 병렬 작업 활성화

병렬 작업을 사용하여 익명화 작업 실행 시간을 줄입니다.

시작하기 전에
필요한 역할: 관리자

프로시저
기본적으로 데이터 클래스 및 사용자 기반 익명화 작업은 단일 스레드를 사용하여 실행됩니다. 데이터 클래스 및 사용자 기반 작업에 대해 다중 스레드를 활성화할 수 있습니다. 또한 복제 중에 사용되는 페더레이션 작업은 기본적으로 작업자가 3개인 병렬 작업을 사용합니다.

1. 탐색 필터에 `sys_properties.list`를 입력합니다.
2. `com.glide.data_privacy.max_parallel_workers` 속성 생성
3. 옵션: 페더레이션 작업 병렬 작업자 수를 조정하려면 `dp.max_concurrent_clone_item_workers` 속성을 편집합니다.
4. 유형이##인지 확인합니다.
5. **중요사항:** 노드당 적은 수의 작업자(2 또는 3)로 시작하는 것이 좋습니다.

   값 필드에 병렬 작업 작업자 수를 최대 5개까지 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화

민감한 데이터를 보호하고 규제 요구사항 및 표준을 준수하십시오.

Key Management Framework



(KMF)를

핵심 관리 프레임워크

사용하여 인스턴스에서 암호화 작업이 수행되는 방식을 완전히 사용자 지정하고 관리합니다.

필드 암호화



사용자 역할에 따라 암호화된 데이터에 대한 접근을 허용하거나 거부하는 데 사용합니다

필드 암호화

.

필드 암호화

암호화 모듈을 사용한 기본 키 관리를 포함합니다.

필드 암호화 엔터프라이즈



사용자 역할에 따라 암호화된 데이터에 대한 접근을 허용하거나 거부하는 데 사용합니다

필드 암호화

.

필드 암호화

암호화 모듈을 사용한 기본 키 관리를 포함합니다.

클라우드 암호화



향상된 키 관리와 함께 블록 암호화를 사용하여 인스턴스 데이터베이스를 암호화합니다.

플랫폼 암호화 권리 번들



무제한 사용

필드 암호화 엔터프라이즈

, 클라우드 암호화 및 데이터베이스 암호화로 업그레이드하십시오.

전체 디스크 암호화**(FDE)**



전체 디스크 암호화는 데이터베이스 서버 내의 전체 스토리지 시스템에만 암호화를 적용합니다. 이것이 유일한 고객 데이터 저장 구성 요소이기 때문입니다.

에지 암호화 규칙



인터넷을 통해 ServiceNow 인스턴스로 데이터를 전송하기 전에 회사 구내에서 중요한 데이터를 암호화합니다 . 데이터는 인스턴스에 저장되어 있을 때 암호화된 상태로 유지됩니다.

인증서



인증서를 사용하여 보안 연결을 설정하고 서명의 유효성을 검사합니다.

데이터베이스 암호화



저장된 모든 데이터를 실시간으로 암호화하여 기능 손실 없이 온라인 및 오프라인 데이터를 보호합니다.

Key Management Framework

(KMF)를 핵심 관리 프레임워크 사용하여 암호화 키를 생성, 교환, 저장, 사용 및 교체합니다. KMF를 사용하면 ServiceNow 인스턴스의 데이터를 보호하는 데 사용되는 키와 작업을 관리할 수 있습니다.

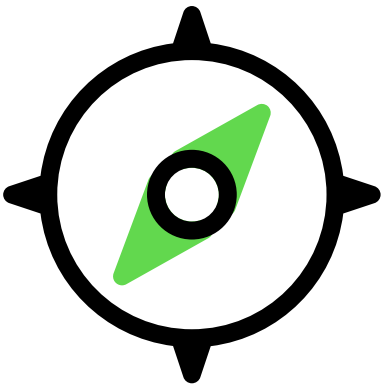
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 관리는 키의 수명 주기 동안 암호화 키 및 관련 보안 매개변수를 처리하는 것과 관련된 활동을 나타냅니다. 키 관리는 NIST(National Institute of Standards and Technology) 800-57 지침을 기반으로 합니다. 이러한 가이드라인에 따라 KMF를 사용하여 다음을 수행할 수 있습니다.

- 암호화 관리 및 운영, 감사 및 통합을 위한 전용 역할을 할당합니다.
- 암호화 모듈을 생성하여 고유한 암호화 목적 및 키 유형에 맞게 암호화 사양을 구성합니다.
  - 대칭 키: 암호화 및 암호 해독, 키 래핑 및 래핑 해제, 인증
  - 비대칭 키: 디지털 서명 생성 및 검증, 암호화 및 암호 해독, 키 래핑 및 래핑 해제
- 여러 키 수명주기 상태 지원을 포함하여 키 수명주기를 관리하여 키를 생성, 회전, 해지 및 일시 중단합니다
- 모듈 액세스 정책(MAP)을 생성하여 액세스 제어를 적용하고 선택한 사용자와 스크립트에만 액세스 권한을 부여합니다.
- FIPS(Federal Information Processing Standard) 140-2-L3 하드웨어 RoT(Root of Trust), PKI(Public Key Infrastructure), 키 계층 구조 및 봉투 암호화를 사용하여 암호화 키를 보호합니다.
- 사용자에게 감사 역할을 할당하면 키 사용 통계와 같은 감사 정보를 볼 수 있습니다.

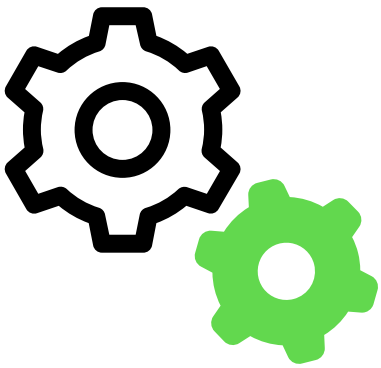
시작

키 관리 프레임워크 탐색



키 관리 프레임워크의 구성요소에 대해 알아보고, 이를 사용하여 인스턴스에서 암호화 작업이 수행되는 방식을 관리하는 방법에 대해 알아보십시오.

키 관리 프레임워크 구성



키 관리 구성요소를 작성하고 유지하여 암호화 작업이 수행되는 방식을 사용자 지정하고 관리합니다.

ServiceNow 인스턴스.

핵심 관리 프레임워크 참조

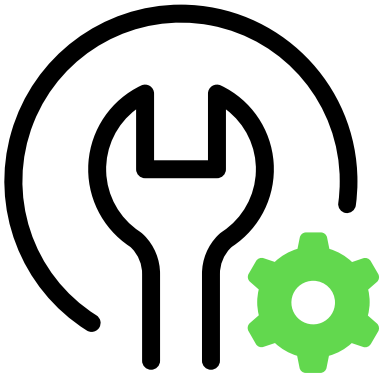


키 관리 구성요소를 작성하고 유지하여 암호화 작업이 수행되는 방식을 사용자 지정하고 관리합니다.

ServiceNow 인스턴스.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주요 관리 프레임워크 작업



KMF 기능을 사용하여 키를 관리, 해지 또는 회전하여 최신 암호화 자료 및 수명 주기 작업으로 중요한 데이터를 보호합니다.

활성화 정보

Platform Encryption 구독 번들은 ServiceNow , 필드 암호화 엔터프라이즈, 클라우드 암호화및 데이터베이스 암호화를 포함하는 핵심 관리 프레임워크그룹 상용 권리입니다.

필드 암호화 엔터프라이즈 의 무제한 라이센스 필드 암호화입니다. 엔터프라이즈 플러그인은 필드 암호화 com.glide.now.platform.encryption 플러그인을 활성화하여 사용할 수 있습니다. 자세한 내용은 암호화 및 키 관리 구독 번들을 참조하십시오.

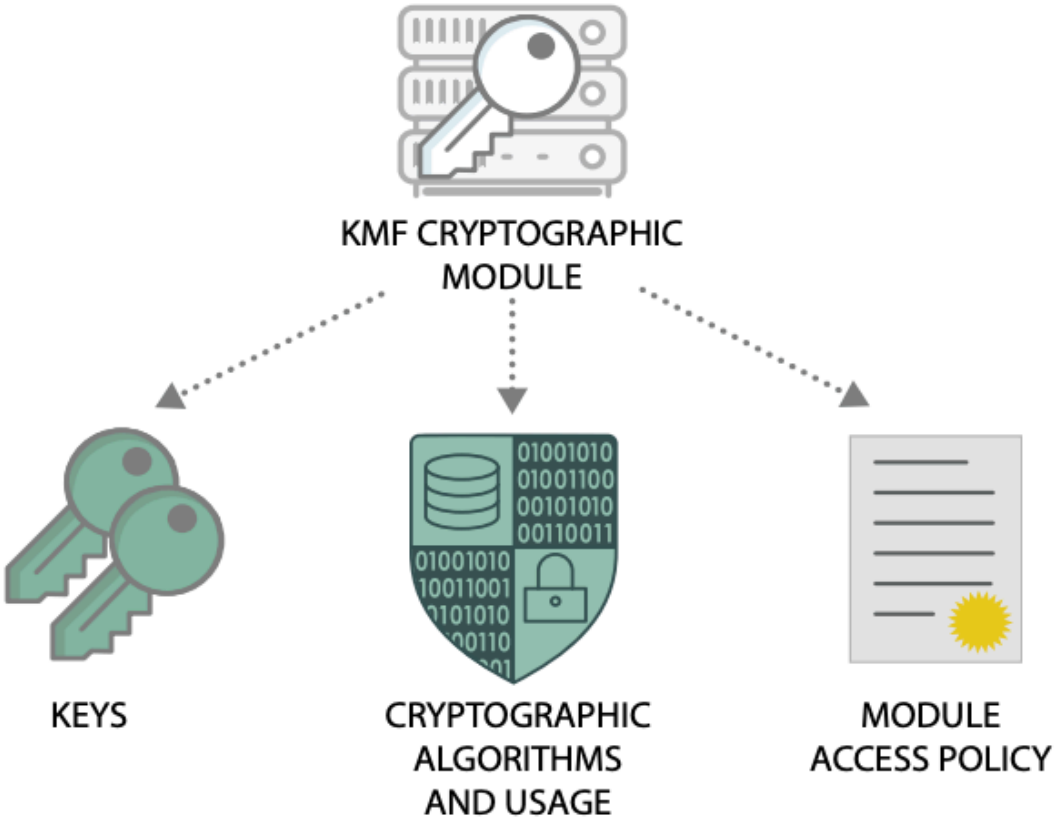
주: KMF는 도메인 분리를 지원하지 않지만 온프레미스 인스턴스와 함께 사용할 수 있습니다.

키 관리 프레임워크 탐색

Key Management Framework(KMF)의 구성요소에 대해 알아보고, 이를 사용하여 인스턴스에서 암호화 작업이 수행되는 방식을 관리하는 방법에 대해 알아봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 관리 프레임워크의 구성요소



이 그래픽에서는 KMF를 구성하는 구성요소를 보여줍니다.

KMF 암호화 모듈

KMF는 암호화 모듈 관리에 중점을 둡니다. 이러한 모듈을 사용하여 암호화되는 인스턴스의 데이터와 사용할 암호화 방법을 정의합니다. 여러 모듈을 사용하면 서로 다른 암호화 사양을 사용하여 인스턴스의 여러 영역을 암호화할 수 있습니다.

예를 들어 256비트 대칭 키가 있는 AES-CBC를 사용하여 인사 관리 애플리케이션의 데이터를 보호하려는 경우 해당 용도로 모듈을 만들 수 있습니다. 이러한 모듈에 대한 자세한 내용은 다음 문서를 참조하십시오 암호화 모듈 개요.

암호화 키

암호화 키는 암호화에 사용되는 문자열입니다. 암호화 알고리즘과 함께 사용하면 데이터를 인코딩하거나 디코딩할 수 있습니다. 이러한 키는 모듈에 할당된 암호화 사양에서 사용됩니다. 에서 ServiceNow생성된 키를 사용하도록 선택하거나 를 사용하여 필드 암호화 엔터프라이즈고유한 키를 업로드할 수 있습니다. 키에 대한 자세한 내용은 다음 문서를 참조하십시오 Key Management Framework의 인스턴스 수준 키.

암호화 사양

암호화 사양은 데이터를 암호화하는 데 사용되는 알고리즘을 정의합니다. 이러한 알고리즘은 암호화 키를 사용하여 데이터를 인코딩하거나 디코딩합니다. 모듈에 암호화 사양을 지정하면 해당 모듈에 할당된 데이터가 암호화되는 방법이 결정됩니다.

모듈 접근 정책

모듈 액세스 정책(MAP)은 암호화 모듈에 적용하는 액세스 제어입니다. 이러한 정책을 사용하여 암호화 모듈로 암호화된 데이터에 액세스할 수 있는 사용자와 스크립트를 결정할 수 있습니다. 자세한 내용은 모듈 접근 정책 개요 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

핵심 관리 프레임워크 워크플로우

1. KMF 역할 할당

   관리자는 먼저 자신에게 sn_kmf.admin 역할을 할당해야 합니다. 이 역할을 통해 KMF 기능을 사용하고 다른 사용자에게 KMF 역할을 할당할 수 있습니다.

2. KMF 설정 구성

   필드 암호화 설정을 구성하여 암호화를 위해 제공된 키 또는 자체 CSK(고객 제공 키)를 선택합니다.

3. 암호화 모듈 생성

   암호화 모듈을 사용하여 암호화할 인스턴스의 데이터 세트를 선택합니다. 이후 단계에서는 암호화 사양을 할당하여 이 데이터를 암호화하는 방법을 결정하고 모듈 액세스 정책을 할당하여 데이터를 해독할 수 있는 사용자를 결정합니다.

4. 암호화 사양 생성

   암호화 사양은 암호화 방법을 정의합니다. 모듈에 할당되면 해당 모듈에 할당된 데이터가 암호화되는 방식을 정의합니다.

5. 모듈 접근 정책 생성

   데이터를 보호하기 위한 모듈을 만든 후에는 모듈 액세스 정책을 생성하여 암호화된 데이터에 액세스할 수 있는 사용자와 스크립트를 제어합니다.

6. 암호화 모듈 수명 주기 정책 만들기

   이러한 정책은 암호화 키가 유효한 기간과 같은 암호화 모듈에 제한을 둡니다. 이러한 정책은 노출을 제한하여 암호화 모듈을 보호할 수 있습니다.

핵심 관리 프레임워크의 이점

혜택	기능	사용자
민감한 독점 데이터를 보호하십시오.	암호화 및 키 관리	모두
NIST 800-57 지침을 준수하도록 유지합니다. 이러한 지침은 네트워크 및 데이터에 대한 사이버 보안 위험을 줄이기 위해 National Institute of Standards and Technology에서 제공합니다.	암호화 및 키 관리	보안 관리자
키 관리 프레임워크를 사용하여 암호화 키를 생성, 업로드, 조회 및 관리할 수 있습니다. 보안 강화를 위해 키의 수동 또는 예약된 회전에 키 회전을 사용합니다.	Key Management Framework	보안 관리자

암호화 모듈 개요

Key Management Framework(KMF)는 암호화 모듈 관리를 중심으로 합니다. 이러한 모듈을 사용하여 암호화 메커니즘을 선택하고 인스턴스에 적용되는 위치를 정의합니다.

암호화 모듈은 의 KMF핵심입니다. 지정된 사용 사례의 암호화 작업에 사용되는 특정 암호화 메커니즘을 정의합니다.

예를 들어 256비트 대칭 키가 있는 AES-CBC를 사용하여 인사 관리 애플리케이션의 데이터를 보호하려고 합니다. 해당 목적을 위한 모듈을 생성할 수 있습니다.

암호화 모듈은 키 수명 주기 관리도 지원합니다. 암호화 키를 생성 및 교체하고 암호화 방법을 정의할 수 있습니다. 암호화 모듈은 다음 구성요소로 구성됩니다.

암호화 사양

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 목적과 사용할 알고리즘을 포함하여 모듈의 여러 측면을 정의합니다.

암호화 키

모듈에서 암호화 데이터를 인코딩하거나 디코딩하는 데 사용하는 키입니다. 이 키는 인스턴스 또는 사용자가 만들고 업로드하는 고객 제공 키에서 생성할 수 있습니다.

모듈 접근 정책

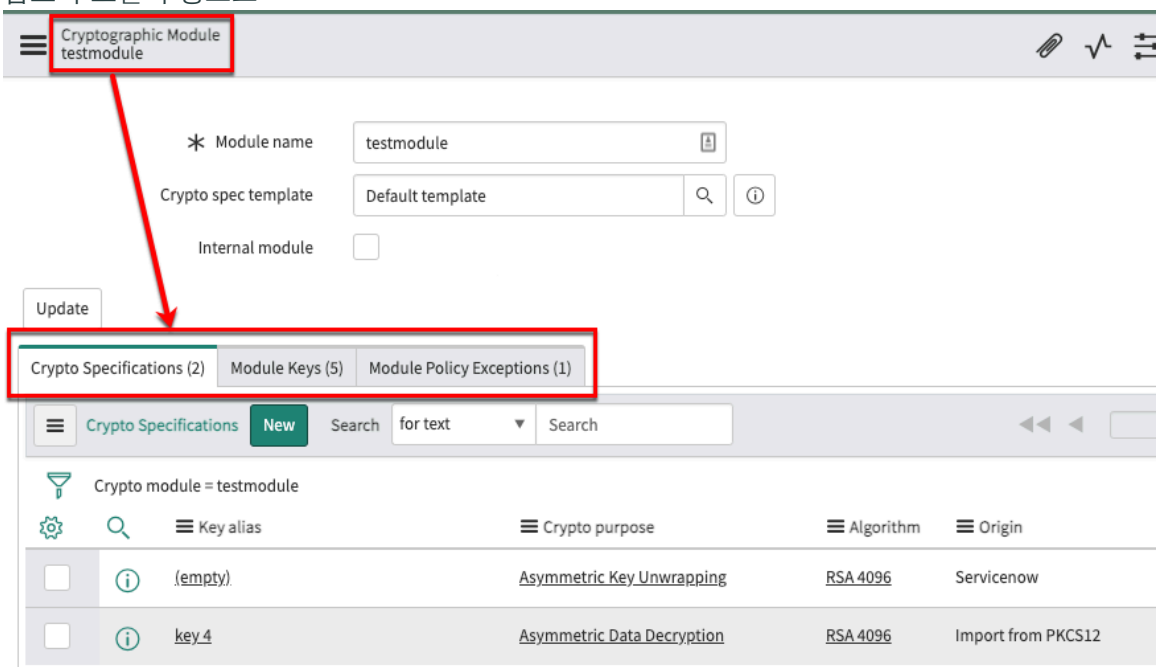
모듈 접근 정책은 데이터를 암호화하거나 해독할 수 있는지 여부를 제한하는 접근 제어 메커니즘입니다.

모듈 정책 예외

모듈 액세스 정책에 대한 예외를 정의하는 통제 메커니즘입니다.

다음 화면은 암호화 모듈에서 이러한 상위 수준 구성요소를 보여줍니다.

암호화 모듈 구성요소



암호화 모듈 생성에 대한 자세한 내용은 다음 문서를 참조하십시오 암호화 모듈 생성.

암호화 사양

암호화 사양은 암호화 목적과 사용할 암호화 알고리즘을 포함하여 암호화 모듈의 여러 측면을 정의하는 구성요소입니다.

암호화 사양은 비대칭 및 대칭 키 기반 암호화 작업을 모두 포함하는 지정된 암호화 목적에 맞게 조정할 수 있습니다. 암호화 목적을 선택하면 지원되는 알고리즘 및 키 길이 구성 집합에 대한 추가 선택이 제공됩니다.

암호화 목적, 알고리즘 및 키 정보

암호화 목적	알고리즘	주요 정보
비대칭 데이터 암호 해독	RSA	비대칭 – 2048비트, 3072비트 및 4096비트 키
비대칭 데이터 암호화	RSA	비대칭 – 2048비트, 3072비트 및 4096비트 키
비대칭 키 래핑 해제	RSA	비대칭 – 2048비트, 3072비트 및 4096비트 키
비대칭 키 래핑	RSA	비대칭 – 2048비트, 3072비트 및 4096비트 키

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 목적, 알고리즘 및 키 정보

암호화 목적	알고리즘	주요 정보
서명 작성	RSA	비대칭 – 2048비트, 3072비트 및 4096비트 키
서명 검증	RSA	비대칭 – 2048비트, 3072비트 및 4096비트 키
대칭적 진위	HMAC	대칭 – 256비트, 384비트 및 512비트 키
대칭 데이터 암호화/암호 해독*	AES-CBC *	대칭 – 128비트, 192비트, 256비트 키
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM **	
대칭 키 래핑/래핑 해제*	AES-CBC *	대칭 – 128비트, 192비트, 256비트 키
	AES-CFB	
	AES-OFB	
	AES-CTR	
	AES-GCM **	

* AES-CBC는 동일성 유지 옵션을 지원합니다. 필드 암호화 엔터프라이즈 AES-CBC를 활용합니다.

** AES-GCM에는 데이터 무결성이 내장되어 있습니다.

이러한 매개변수의 구성은 에서 암호화 모듈 생성다룹니다.

모듈 접근 정책 개요

모듈 액세스 정책(MAP)은 암호화 모듈에 적용하는 액세스 제어입니다. 이러한 액세스 정책을 사용하여 암호화 모듈로 암호화된 데이터에 액세스할 수 있는 사용자와 스크립트를 결정할 수 있습니다.

모듈 접근 정책

주: 이 기능을 활용하려면 구독이 필드 암호화 엔터프라이즈 필요합니다. 에 대한 필드 암호화 엔터프라이즈자세한 내용은 를 참조하십시오필드 암호화 활성화.

모듈 접근 정책은 기본 시스템에서 (KMF)와 핵심 관리 프레임워크 함께 도입됩니다.

모듈 액세스 정책은 암호화 모듈과 함께 제공된 역할 기반 지정을 확장합니다. 모듈 액세스 정책은 다음을 기반으로 할 수 있습니다.

- 기본(범위)
- 역할
- 시스템 사용자
- 스크립트
- 자원 교환

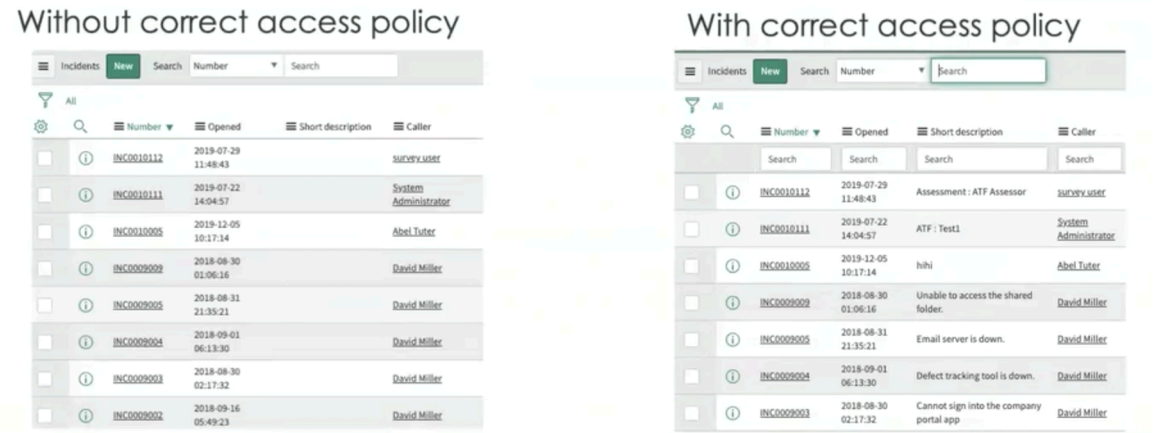
주: 자세한 내용은 키 관리 프레임워크 자원 교환 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 모듈에서는 암호화된 데이터에 대한 액세스를 허용하도록 올바른 모듈 액세스 정책을 구성해야 합니다. 암호화 모듈과 연결된 모듈 액세스 정책이 없으면 암호화된 데이터가 사용자에게 표시되지 않으며 목록의 관련 필드와 열이 비어 있는 상태로 표시됩니다.

이 예에서는 암호화된 간단한 설명 필드에 모듈 액세스 정책이 없으면 인시던트 테이블에 액세스하는 모든 사용자에게 콘텐츠가 숨겨집니다. 모듈 액세스 정책이 적용되면 특정 역할을 가진 사용자만 암호화된 데이터를 볼 수 있습니다.

모듈 접근 정책을 사용하거나 사용하지 않고 암호화된 간단한 설명



주: 또한 열의 데이터는 모듈 액세스 정책에 지정된 올바른 역할이 없는 사용자에게도 비어 있는 것으로 나타납니다.

설정은 참조하십시오 모듈 액세스 정책 생성 .

자동 작성 정책

자동 작성 정책은 지정된 암호화 모듈에 대해 정의된 기본 모듈 접근 정책에 따라 시스템에서 자동으로 생성됩니다. 시스템 또는 스크립트가 지정된 암호화 모듈에 액세스하려고 할 때 정의된 세분화된 수준 정책이 없는 경우 이러한 전역 정책이 생성되고 적용됩니다.

중요사항:

자동 생성 정책 규칙은 예약된 작업 유형 또는 필드 암호화 모듈(상위 모듈이 있는 필드 암호화모듈)에는 적용되지 않습니다.

Key Management Framework의 인스턴스 수준 키

(KMF) 아키텍처는 핵심 관리 프레임워크 보안을 염두에 두고 구축된 키 구조를 도입합니다. HSM KMF (하드웨어 보안 모듈)을 사용하면 봉투 암호화를 사용하여 관리 중인 KMF 모든 플랫폼 키가 키 체인을 통해 보호되도록 합니다. 생성한 KMF 고객 데이터 암호화 키(CDEK)도 포함됩니다.

인스턴스 수준에서, KMF 전반에 걸쳐 Now Platform다양한 암호화 목적을 위해 내부적으로 사용되는 여러 키를 정의합니다.

봉투 암호화는 다른 키를 사용하여 키를 암호화하는 방법입니다. 다음 그림은 봉투 암호화의 예를 제공합니다. 여기서 CDEK는 IKEK에 의해 봉투 암호화되고, 이는 다시 IRK에 의해 봉투 암호화되며, 최종적으로 RK에 의해 봉투 암호화됩니다. IRK는 HSM에서만 액세스할 수 있으므로 암호 해독을 위해 IKEK를 업로드해야 합니다.

이 표에서는 에서 KMF관리하고 보호하는 사용 가능한 고객/앱 키의 하위 집합의 예를 제공합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키	위치	설명
루트 키(RK)	HSM(하드웨어 보안 모델)	IRK의 암호를 해독하는 데 사용되는 루트 키입니다.
인스턴스 루트 키(IRK)	증권 시세 표시기	여러 인스턴스 내부 키를 봉투 암호화하는 데 사용되는 인스턴스 고유의 키입니다.
인스턴스 HMAC 키(IHK)	인스턴스	인스턴스마다 고유한 IHK는 HMAC(해시 기반 메시지 인증 코드) 목적으로 내부적으로 사용됩니다. IHK는 모듈 키의 신뢰성과 무결성을 확인하는 데 도움이 되며 KeySecure 또는 파일 키 저장소에 래핑됩니다.
인스턴스 키 암호화 키(IKEK)	인스턴스	IKEK는 모듈 키를 래핑하고 KeySecure 또는 파일 키 저장소에 래핑됩니다.
인스턴스 비대칭 암호화 키(IAEK)	인스턴스	비대칭 암호화를 위해 내부적으로 사용되는 인스턴스에 고유한 키입니다. IAEK는 소비자 승인 중 키 교환인스턴스 데이터 복제 인스턴스 간에 기밀 메시지를 전송하는 데 사용됩니다.
인스턴스 서명 키(ISK)	인스턴스	서명을 위해 내부적으로 사용되는 인스턴스에 고유한 키입니다.
Password2(PW2)	인스턴스	를 사용하면 KMF필드의 키가 PW2 에 의해 KMF완전히 관리됩니다.
고객 데이터 암호화 키(CDEK)	인스턴스	을 통해 KMF 생성된 암호화 키는 IKEK에 의해 봉투 암호화됩니다.
인스턴스 데이터 복제(IDR) 데이터 암호화 키(DEK)	인스턴스	IDR 프로세스에 사용되는 특정 암호화 키입니다.

키 관리 프레임워크 구성

키 관리 구성요소를 작성하고 유지관리하여 인스턴스에서 암호화 작업이 수행되는 ServiceNow 방법을 사용자 지정하고 관리합니다.

키 유형을 선택하도록 필드 암호화 설정 구성

Now Platform에서 암호화를 위해 제공된 키 또는 자체 CSK(고객 공급 키)를 사용하도록 ServiceNow 필드 암호화 설정을 구성합니다.

시작하기 전에

고객이 제공한 키는 에서만 지원됩니다 필드 암호화 엔터프라이즈.

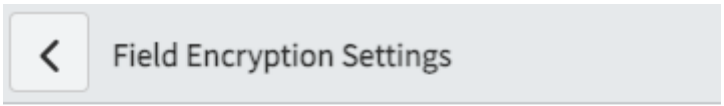
필요한 역할: sn_kmf.cryptographic_manager 및 security_admin

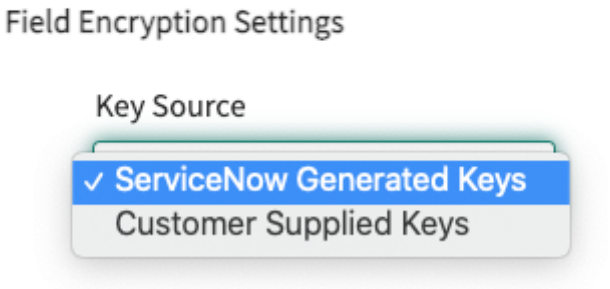
프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 설정.
2. 필드 암호화 설정의 키 소스 목록에서 **ServiceNow** 작성 키 또는 고객 공급 키를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 소스 선택





이 옵션은 `com.glide.encryption.cle_kmf.key_source` 속성을 **ServiceNow** 작성 키 또는 고객 제공 키로 변경합니다.

3. 저장을 선택합니다.

다음에 수행할 작업

- 자체 고객 제공 키를 사용하는 경우 문서를 참조하십시오 와 함께 고객 제공 키 사용 필드 암호화 엔터프라이즈.
- 제공된 키를 사용하는 ServiceNow 경우 암호화 모듈 생성을 시작합니다. 암호화 모듈 생성 문서를 참조하십시오.

암호화 모듈 생성

암호화 모듈을 생성하여 암호화 작업에 사용되는 메커니즘을 정의합니다. 모듈을 만든 후 암호화 사양을 생성하여 암호화 알고리즘을 정의하고 키를 생성합니다.

시작하기 전에

자체 키를 제공하는 경우 로 고객 공급 키 구성 및 업로드이동합니다.

필요한 역할: sn_kmf.cryptographic_manager

이 태스크 정보

이 절차에서는 플랫폼 기본 시스템에서 사용할 수 KMFServiceNow 있는 옵션에 대해 설명합니다. 필드 암호화 엔터프라이즈 기능은 *com.glide.now.platform.encryption* 플러그인이 활성화된 경우에만 사용할 수 있습니다. 를 얻는 필드 암호화 엔터프라이즈방법에 대한 자세한 내용은 를 참조하십시오필드 암호화 활성화. 용 암호화 모듈 생성 필드 암호화 문서를 참조하십시오.

주: 암호화 모듈 [sys_kmf_crypto_module] 기록은 삭제할 수 없습니다.

프로시저

1. 다음으로 이동 모두 > 주요 운영 > 암호화 모듈 > 새로 작성.
2. 양식의 필드에 내용을 입력합니다.

암호화 모듈 필드

필드	설명
모듈 이름	스크립트를 실행할 때 참조할 영숫자 문자열입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
암호화 사양 템플릿	암호화 사양을 위해 지원되는 알고리즘의 매핑이 포함되어 있으므로 암호화 모듈을 생성하는 데 사용할 기본 템플릿을 선택합니다.
기본 모듈 접근 정책 값	◦ 시스템 기본값 사용: ◦ 거부 ◦ 트랙
실제 모듈 접근 정책 결과	기본 정책 값 또는 모듈 액세스 정책을 생성하는 동안 선택한 값에 따라 거부 또는 추적합니다.
이름	애플리케이션 범위 이름이 앞에 추가된 암호화 모듈 이름입니다.
암호화 모듈 수명주기 상태	수명주기는 암호화 모듈의 생성, 사용 및 비활성화를 나타냅니다. 구성 중에 처음에는 초안 으로 설정합니다. 모듈을 사용할 때는 이 필드를 게시됨으로 설정하십시오. 기본 템플릿은 게시됨으로 자동 설정됩니다.

3. 제출을 선택합니다.

⚠ 경고:

레거시 암호화 지원 사용자의 경우:

의 엔터프라이즈가 아닌 버전을 필드 암호화사용하는 경우 모듈은 5개로 제한됩니다. 이 한도를 초과하면 다음과 같은 경고가 표시됩니다.

이 삽입은 구독 제품에 부여된 게시된 모듈 수 제한을 필드 암호화 초과합니다. 추가 모듈에는 Enterprise 구독 필드 암호화 이 필요합니다. 계정 팀에 문의하십시오.

성공적으로 제출하면 암호화 모듈이 암호화 모듈 테이블에 나열됩니다. 시스템은 범위가 지정된 다른 애플리케이션과의 충돌을 피하기 위해 이름 앞에 범위를 추가합니다. 예를 들어 전역 애플리케이션 범위에서 `my_crypto_module` 라는 이름의 모듈을 만든 경우 이름은 `global.my_crypto_module`로 저장됩니다.

다음에 수행할 작업

암호화 사양 작성

.

암호화 사양 작성

암호화 모듈을 만든 후 암호화 사양을 만들어 모듈 알고리즘을 정의합니다.

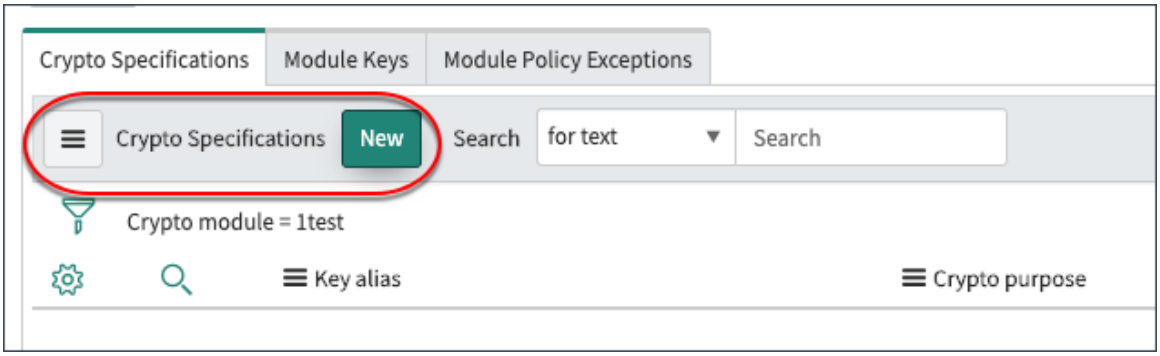
시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager

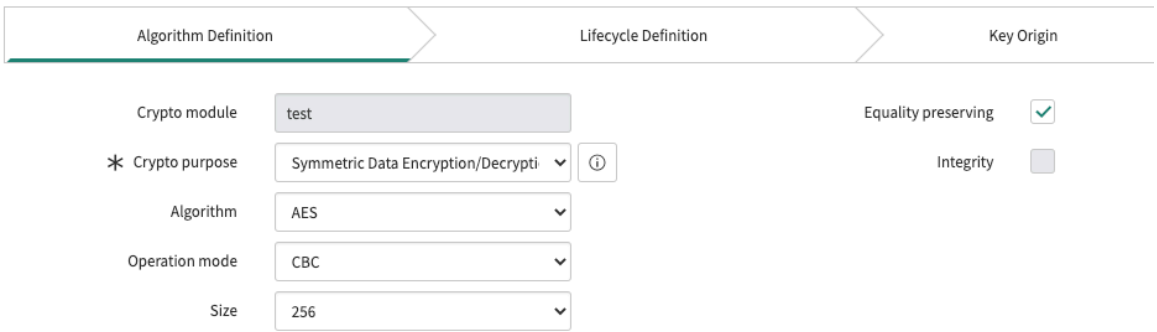
프로시저

1. 다음으로 이동 주요 운영 > 암호화 모듈 > 모두.
2. 정의에 암호화 모듈을 선택하여 구성 옵션을 엽니다.
3. 암호화 사양 탭에서 새로 만들기를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 알고리즘 정의 양식을 작성합니다.
   자세한 내용은 암호화 사양 문서를 참조하십시오.



알고리즘 정의 화면이 열립니다. 키 생성을 위한 옵션을 선택합니다. 이 단계를 반복하여 선택된 암호화 모듈에 대한 다중 키를 생성하십시오.

알고리즘 정의 필드

필드	
암호화 모듈	읽기 전용입니다. 선택한 암호화 모듈의 이름이 표시됩니다.
암호화 목적	이 모듈의 용도를 선택하십시오. 예를 들어 데이터 암호화, 서명 생성 또는 키 래핑에 사용할 수 있습니다. 사용 가능한 알고리즘은 선택한 암호화 목적에 따라 조정됩니다. 자세한 내용은 암호화 사양 문서를 참조하십시오.
알고리즘	암호화 목적을 달성하는 데 사용되는 알고리즘 유형입니다. 이 알고리즘은 키 원점도 제어합니다. 선택한 암호화 목적에 따라 자동으로 조정됩니다. 암호화 사양 자세한 내용은 다음을 참조하십시오.
작동 모드	이 필드는 선택한 암호화 목적에 따라 표시될 수 있습니다.
크기	비트 크기를 선택합니다.
해시	선택한 알고리즘에 따라 이 필드를 사용할 수 있게 됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	
동등 유지	비결정적 암호화를 활성화합니다. 이 옵션은 **AES**를 사용하는 대칭 데이터 암호화/암호 해독**(Symmetric Data Encryption/Decryption** with AES) 및 **CBC(Cipher Block Chaining)** 모드를 선택할 때 나타납니다. 이 옵션을 선택하면 동일한 데이터가 다시 암호화되면 인코딩된 데이터가 매번 동일합니다. 비결정적 암호화는 같음 비교 연산자를 사용하여 암호화된 데이터 목록을 필터링하는 것을 지원하지 않습니다.
무결성	GCM 작동 모드는 무결성을 제공합니다.

5. 다음을 선택합니다.
   암호화 사양은 선택한 알고리즘에 따라 키 수명 주기 테이블에 나열됩니다.

다음에 수행할 작업
다음 작업 중 하나를 수행합니다.

- 키 수명주기 테이블에서 항목을 선택하여 키 수명주기 동작을 정의합니다. 키에 대한 수명주기 정의를 완료하려면 자세한 내용을 참조하십시오 키 수명주기 상태 구성 .
- 다음을 선택하여 암호화 키를 만듭니다. 키 생성을 위해 다음 작업 중 하나를 참조하십시오.
  - ServiceNow 암호화 키 작성.
  - 고객 공급 키의 속성 구성.
  - 키 쌍의 래핑/래핑 해제 임포트.

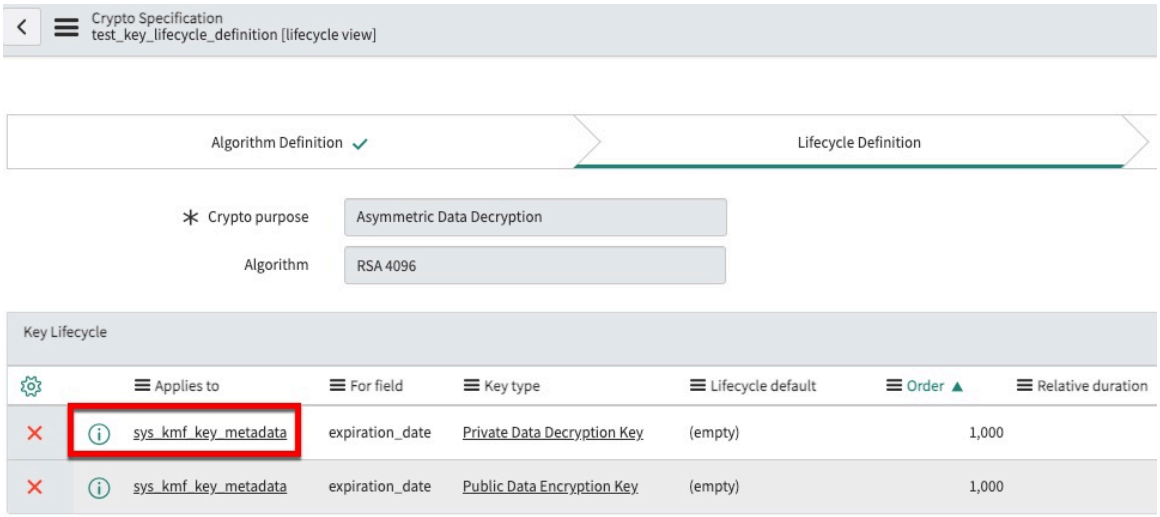
키 수명주기 상태 구성

암호화 사양을 생성한 후 인스턴스의 키에 대한 수명 주기 작업을 구성할 수 있습니다.

시작하기 전에
필요한 역할: sn_kmf.admin

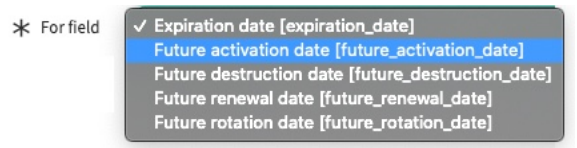
프로시저
1. 다음으로 이동 주요 운영 > 암호화 모듈 > 모두.
2. 암호화 모듈을 선택하여 키의 수명 주기를 구성합니다.
3. 암호화 사양 탭에서 키 별칭을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

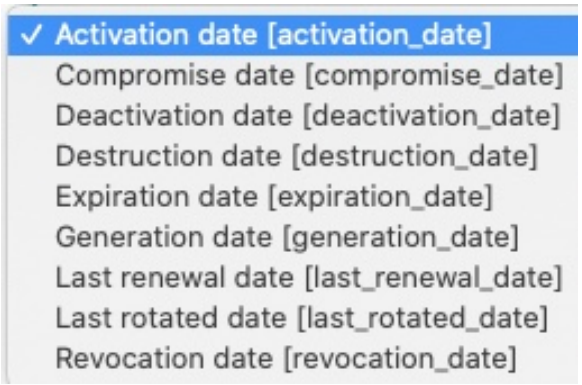


4. 다음을 선택합니다.
   필드 수명 주기 템플릿이 로드됩니다. 기본 키 수명 주기 값은 정의된 암호화 사양에 대해 선택한 알고리즘을 기반으로 만들어집니다.
5. 암호화 사양에 대한 수명주기 정의 단계의 적용 대상 열에서 키 수명주기를 선택합니다.

주요 수명주기 필드

필드	설명
적용 대상	수명주기가 적용되는 선택한 키입니다.
필드용	수명주기가 적용되는 키의 통제 유형을 선택합니다. 키 수명주기 관리 "필드용" 값 
유형	키 수명주기에 대한 평가가 상대 값인지 절대값인지 선택합니다. ◦ 상대: 키 생성, 활성화 및 비활성화와 같은 시스템의 다른 데이터 항목에 따라 달라지는 값을 입력합니다. ◦ 절대: 날짜와 같은 정확한 값을 입력합니다.
수명주기 기본값	읽기 전용입니다. 설정된 경우 값을 표시합니다.
순서	암호화 사양의 키 수명주기 상태를 처리할 순서를 입력합니다.
상대 기간 유형	수명주기 기간: 년, 월 또는 일.
상대 기간	키가 유효한 년, 월 또는 일 수입니다.
상대 작업	이전또는 이후.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
관련 대상	기간이 기준이 되는 필드입니다. 상대 기간 또는 작업을 선택한 경우 표시됩니다. 

ServiceNow 암호화 키 작성

다음 절차에 따라 중요한 데이터를 암호화하도록 암호화 키를 업로드하고 구성합니다 ServiceNow .

시작하기 전에

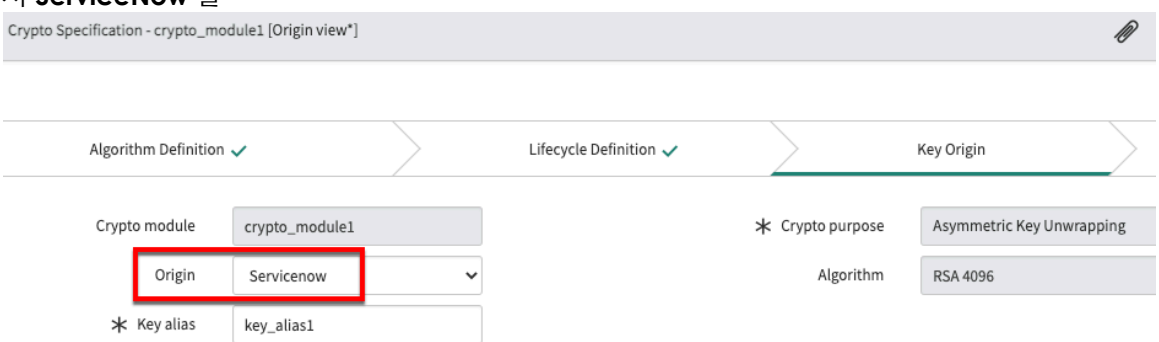
필요한 역할: sn_kmf.cryptographic_manager

이 태스크 정보

암호화 관리자는 암호화를 위해 제공된 키 또는 자체 CSK(고객 제공 키)를 Now Platform 사용할 ServiceNow 수 있습니다필드 암호화 엔터프라이즈. CSK에 대한 자세한 내용은 를 참조하십시오 고객 공급 키의 속성 구성.

프로시저

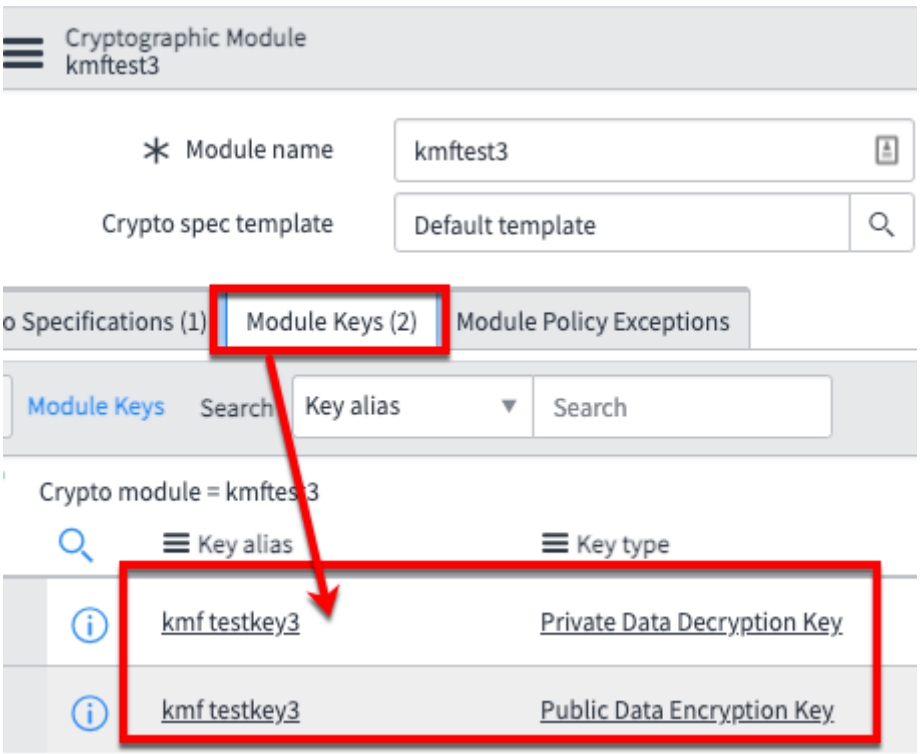
1. ServiceNow 작성 키를 사용하도록 필드 암호화 설정을 지정합니다.
   자세한 내용은 키 유형을 선택하도록 필드 암호화 설정 구성 문서를 참조하십시오.
2. 다음으로 이동 주요 운영 > 암호화 모듈 > 모두.
3. 해당 암호화 모듈을 선택하여 암호화 모듈 상세 정보 페이지를 엽니다.
4. 암호화 사양 탭에서 키 별칭 항목의 행을 선택합니다.
   키가 아직 생성되지 않은 경우 키 별칭 필드가 비어 있습니다.
5. 다음을 선택하여 암호화 사양 구성요소의 키 원본 탭으로 이동합니다.
   수명주기 정의 탭은 키 수명주기 테이블과 함께 표시되며 검토하거나 편집할 수 있습니다. 자세한 내용은 키 수명주기 상태 구성 문서를 참조하십시오.
6. 원본 필드에서 **ServiceNow** 를



선택합니다.
이 필드는 1단계의 필드 암호화 설정과 선택한 알고리즘에 따라 달라집니다. 임포트한 키를 사용하려면 문서를 참조하십시오 키 쌍의 래핑/래핑 해제 임포트. 자체 키를 사용하고 있는지 확인합니다 고객 공급 키의 속성 구성 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 키 별칭에 대한 식별 이름을 입력합니다.
8. 다음을 선택하여 키 만들기 탭으로 이동합니다.
9. 키 생성을 선택합니다.
   키를 생성하면 암호화 모듈 양식이 다시 로드되어 암호화 사양이 표시됩니다.
10. 모듈 키 탭을 선택하여 키를 확인합니다.
    키에 대한 보안 정보는 암호화 사양에 대해 존재하는 키 수와 함께 모듈 키 탭에 저장됩니다.



11. 키 관리 작업을 수행할 키를 선택합니다.
    자세한 내용은 키 관리 작업 문서를 참조하십시오.

모듈 액세스 정책 생성

모듈 액세스 정책을 생성하여 암호화 모듈로 암호화된 데이터에 액세스할 수 있는 사용자와 스크립트를 결정합니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager 또는 sn_kmf.admin

이 태스크 정보

필드 암호화 는 역할 기반 모듈 접근 정책을 지원하며 (CLE_Ent) 기능을 통해 추가 구성 옵션을 사용할 수 있습니다.

- 대칭 작업을 지원하는 암호화 모듈에 대한 모듈 액세스 정책에서 특정 암호화 작업을 구성합니다. 예를 들어 사용자는 데이터를 암호화할 수 있지만 데이터의 해독은 활성화하지 않을 수 있습니다.
- 기본 모듈 액세스 정책 값을 설정하거나 암호화 모듈에 따라 설정합니다.
- 스크립트에 대한 변경 내용을 추적하는 스크립트 버전을 연결하고 스크립트 정책을 무효화하여 스크립트 유형 모듈 액세스 정책에 대한 보안을 강화합니다.

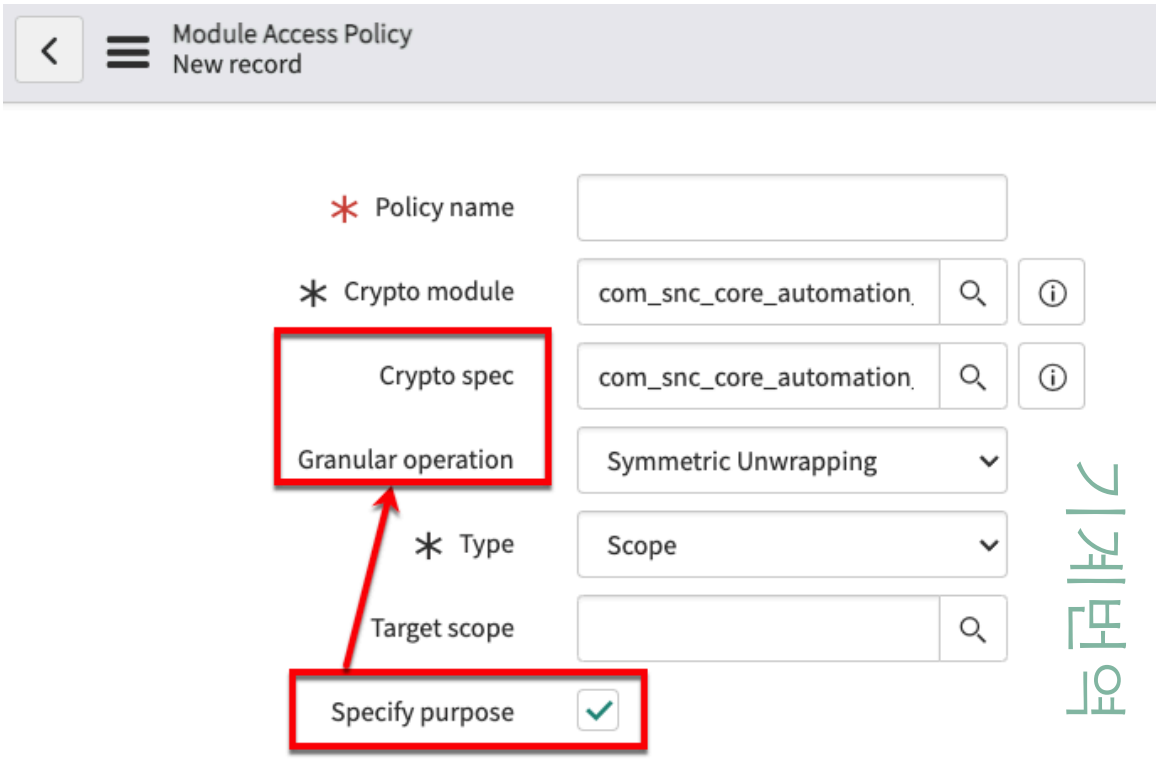
CLE_Ent 유료 구독을 통해 기능을 사용할 수 있습니다. 각 오퍼링에서 사용할 수 있는 지원되는 기능 및 옵션을 참조하십시오. 자세한 내용은 필드 암호화 엔터프라이즈 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: MAP(모듈 액세스 정책)의 기본 동작은 MAP 기록에 명시적으로 선언되지 않는 한 무단 액세스를 방지하기 위해 거부입니다.

프로시저

1. 다음으로 이동 모두 > 주요 운영 > 모듈 접근 정책 > 모두.
   대칭 데이터 암호화/암호 해독을 위해 구성된 암호화 모듈을 생성하지 않으면 자동 생성된 모듈 액세스 정책이 생성되어 테이블에 나열됩니다.
2. 새로 만들기를 선택합니다.
   - 목적 지정을 선택하여 암호화 사양을 선택하고 세분화된 작업을



설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ 대칭 데이터 암호화/암호 해독 및 대칭 래핑/래핑 해제에 대한 암호화 사양을 사용하면 목적 지정 확인란을 선택하면 세분화된 작업 필드를 사용할 수 있습니다.



3. 양식을 작성합니다.

모듈 접근 정책 필드

필드	설명
정책 이름	정책 이름을 입력합니다.
암호화 모듈	검색 아이콘(.)을 선택하여 모듈을 선택합니다.
암호화 사양	모듈 접근 정책을 생성하는 동안 암호화 사양을 선택하거나 생성합니다. 이 필드는 목적 지정 확인란을 선택한 경우에 사용할 수 있게 됩니다.
세분화된 운영	암호화 사양에 대한 암호화 목적을 선택합니다. 사용 가능한 값은 선택한 암호화 스펙의 유형에 따라 다릅니다. 암호화 목적에 대한 자세한 내용은 을 참조하십시오.
유형	◦ 범위: 애플리케이션 범위로 액세스를 제어합니다. ◦ 시스템 사용자: 시스템 사용자가 암호화 모듈에 액세스할 수 있도록 허용합니다. ◦ 스크립트: 스크립트로 액세스를 제어합니다. 자세한 내용은 다음을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	◦ 역할: 사용자 역할로 액세스를 제어합니다. ◦ 자원 교환: 를 자원 교환사용하여 액세스를 제어합니다. 자세한 내용은 문서를 참조하십시오. 주: 에서는 역할 유형만 지원됩니다 필드 암호화. 다른 모든 유형은 와 함께 필드 암호화 엔터프라이즈사용할 수 있습니다.
대상 범위	필드는 범위 유형의 식별자로 표시됩니다. 정책에 대한 기능을 참조합니다. 검색 메뉴에서 애플리케이션을 선택합니다. 주: 대상 범위는 지원되지 않으며 다음을 통해서만 설정할 수 있습니다. 필드 암호화 엔터프라이즈
대상 역할	필드는 역할 유형의 식별자로 표시됩니다. 이 정책이 적용되는 역할입니다.
스크립트 테이블 대상 스크립트	이러한 필드는 스크립트를 유형으로 선택할 때 나타납니다. 필드는 스크립트 유형의 식별자로 표시됩니다. 이 정책이 적용되는 테이블을 선택합니다. 이 정책이 적용되는 문서입니다. 테이블 이름을 선택한 다음 정책의 관련 문서를 선택합니다. 스크립트가 암호화 모듈을 처음 호출하면 모듈에 대한 액세스가 거부되고 개발자에게 오류가 발생합니다. 이 오류를 통해 모듈 소유자는 모듈에 대한 액세스 권한을 부여하거나 거부할 수 있습니다.
자원 교환: ◦ 암호화 사양 ◦ 승인 유형 ◦ 대상 인스턴스 호스트	이러한 옵션은 유형으로 선택할 때 나타납니다. 자원 교환 는 KMF에서 지원되며 상위 모듈이 **column_level_encryption**될 때 지원됩니다. 암호화 사양, 일회성 또는 반복, 대상 인스턴스의 URL을 선택합니다. 자세한 내용은 문서를 참조하십시오.
가장	역할 기반 모듈 액세스 정책에서 사용자는 가장 세션을 사용하여 암호화된 데이터에 액세스할 수 있습니다. 관리자와 같은 사용자가 다른 사용자를 가장하면 이러한 가장 사용 모듈 액세스 정책이 적용됩니다.
목적 지정	암호화 사양 필드를 정책에 사용 가능한 필드로 전환하려면 선택합니다.
활성	정책을 활성화하려면 선택합니다.
결과	다음 중 하나를 선택합니다. ◦ **StrictReject** 는 모든 상황에서 액세스를 거부합니다. ◦ 거부 는 다른 정책에서 액세스 권한을 부여하지 않는 한 대상 역할 또는 대상 범위가 있는 사용자가 이 암호화 모듈에 액세스하지 못하도록 거부합니다. ◦ 모듈의 액세스를 허용하고 사용을 모니터링하기 위한 추적입니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 제출을 선택합니다.

⚠ 경고:

레거시 암호화 지원 사용자의 경우:

의 엔터프라이즈가 아닌 버전을 필드 암호화사용하는 경우 모듈은 5개로 제한됩니다. 이 한도를 초과하면 다음 경고가 표시됩니다.

이 삽입은 구독 제품에 부여된 게시된 필드 암호화 모듈 수를 초과합니다. 추가 모듈에는 Enterprise 구독 필드 암호화 이 필요합니다. 계정 팀에 문의하십시오.

5. 검사할 암호화 모듈과 연결된 정책 이름을 선택합니다.
스크립트 유형 모듈 접근 정책 사용:

모듈 액세스 정책은 스크립트가 실행될 때 기본 액세스 설정에 따라 자동으로 생성됩니다. 모듈 이름 앞에는 `AutoGen-`이 붙습니다. 예를 들어 `Module-TestPolicy` 모듈은 정책 이름 열에 `AutoGen-Module-TestPolicy` 로 나열됩니다.

암호화 호출자 정책 양식에는 선택한 호출자 정책이 나열됩니다. 대상 범위 필드는 모듈을 사용하려는 스크립트의 범위를 지정합니다. 자세한 내용은 을 참조하십시오.

ℹ 주: 에는 필드 암호화최대 5개의 모듈 액세스 정책이 허용됩니다. 구성 옵션에 대해서는 을 참조하십시오.

암호화 모듈 수명 주기 정책 만들기

암호화 모듈 수명주기 정책을 작성하여 암호화 모듈에 키의 유효 기간과 같은 제한을 둡니다. 노출을 제한하여 암호화 모듈을 보호하는 정책을 만듭니다.

시작하기 전에
필요한 역할: sn_kmf.cryptographic_manager

이 태스크 정보
암호화 모듈 수명주기 정책은 인스턴스 수준 정책입니다. 암호화 키에 대한 노출이 많을수록 손상될 가능성이 높아집니다. 키를 사용할 수 있는 기간과 키를 사용할 수 있는 사람을 제한하여 키를 보호합니다.

다음 기능은 암호화 모듈을 관리합니다.

- 인스턴스 정책은 인스턴스의 경계를 설정합니다. 예를 들어, 인스턴스 정책에서 만료 날짜가 활성화 날짜 이후 2년을 넘지 않도록 지정한 경우, 수명 주기 규칙을 사용하여 만료 날짜를 활성화 날짜 5년 후로 설정할 수 없습니다.

- 인스턴스 수명 주기 템플릿을 사용하면 키마다 다른 정책을 설정할 수 있습니다. 템플릿은 암호화 모듈에 대한 기본 수명 주기 규칙을 제공하므로 모든 모듈에 대해 다시 만들 필요가 없습니다. 예를 들어 대칭 데이터 암호화 키에 대해 공개 키 래핑 키와 다른 만료 날짜를 설정할 수 있습니다.

- 수명 주기 규칙은 키에 직접 영향을 줍니다. 예를 들어 수명 주기 규칙에서 만료 날짜가 활성화 날짜 이후 2년이 되도록 지정하면 키는 활성화 날짜 2년 후에 만료됩니다.

프로시저

1. 다음으로 이동 모두 > 주요 운영 > 수명주기 정책 > 인스턴스 정책.
2. 선택 신규.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 양식을 작성합니다.

암호화 수명주기 정책 필드

필드	설명
적용 대상	읽기 전용입니다. 수명주기가 적용되는 키입니다.
활성	정책을 활성화하려면 선택합니다.
정책 조건	암호화 모듈을 활성화, 갱신, 비활성화 및 삭제할 시기를 지정하는 조건문입니다.
결과	**Reject** (거부)를 클릭하여 암호화 모듈에 대한 액세스를 취소하거나, Track(추적)을 클릭하여 액세스를 허용하고 암호화 모듈 사용을 모니터링합니다.

다음에 수행할 작업
모듈 수준에서 이 수명 주기 정책에 예외를 추가하려면 다음 문서를 참조하십시오 모듈 수명주기 정책 예외 작성.

모듈 수명주기 정책 예외 작성

모듈 정책 예외를 생성하여 한 인스턴스의 특정 키에 대해서만 수명 주기 정책을 변경합니다.

시작하기 전에
필요한 역할: sn_kmf.cryptographic_manager 및 sn_kmf.admin

예외는 전체 인스턴스가 아닌 해당 모듈에만 적용됩니다. 예를 들어, 관리자는 인스턴스 수준에서 대칭 키를 1년으로 제한하도록 구성했습니다. 모듈 수준에서 2년으로 예외를 만들 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 주요 운영 > 암호화 모듈 모두.
2. 정책 예외를 사용할 암호화 모듈을 선택하십시오.
3. 암호화 모듈 테이블에서 모듈 정책 예외 탭.
4. 선택 신규.
5. 양식을 작성합니다.

모듈 정책 예외 필드

필드	설명
암호화 모듈	선택한 모듈의 이름입니다. 이 필드는 읽기 전용입니다.
적용 대상	지정된 키가 자동으로 채워집니다.
키 유형	예외 정책과 관련된 키 유형입니다. 주: 단일 키 유형만 선택할 수 있지만 암호화 모듈당 여러 예외 정책을 만들 수 있습니다.
정책 조건	정책 예외가 적용되는 시기를 결정하는 사용자 지정 가능한 조건입니다.
결과	정책 조건 필드의 조건이 충족될 때 발생하는 결과입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	◦ 거부 는 키 사용을 거부합니다. ◦ 트랙을 사용하면 키를 사용할 수 있습니다.

6. 선택 제출 암호화 모듈 테이블로 반환됩니다.

핵심 관리 프레임워크 참조

핵심 관리 프레임워크 (KMF) API/UX를 사용하면 인스턴스에서 암호화 작업이 수행되는 방식을 완전히 사용자 지정하고 관리할 수 있습니다ServiceNow. 인스턴스 ServiceNow 핵심 관리 프레임워크 측 암호화 키 관리 서비스를 위한 안전하고 포괄적인 인터페이스를 제공합니다.

핵심 관리 프레임워크 주요 수명주기 상태

KMF는 허용되는 특정 작업의 적용을 통해 여러 암호화 키 수명 주기 상태를 지원합니다. 예를 들어 활성 상태인 키만 의도한 암호화 목적으로 완전히 사용할 수 있습니다. 다음 표에서는 다양한 키 수명주기 상태에 대해 자세히 설명합니다.

키 관리 프레임워크와 함께 설치되는 역할

(KMF)는 핵심 관리 프레임워크 암호화 모듈 및 키 관리 관련 구성에 대한 특정 역할을 소개합니다.

모듈 액세스 정책 시각화

모듈 액세스 정책 시각화를 사용하여 단일 UI 페이지에서 모든 관련 암호화 모듈 정보를 봅니다.

모듈 접근 정책 디버거

모듈 액세스 정책 디버거를 사용하여 로깅 정보를 검토하고 사용자에게 암호화 컨텍스트에 대한 액세스 권한이 부여되거나 부여되지 않는 이유를 이해합니다.

암호화 및 키 관리 구독 번들

키 관리를 필드 암호화 통해 고도로 구성 가능한 암호화 모듈로 추가 비용 없이 업그레이드됩니다. 무제한 사용 라이선스로 업그레이드할 수도 있습니다. 및 를 포함하는 필드 암호화 엔터프라이즈 새 암호화 권리 번들인 Platform Encryption을 구독합니다 클라우드 암호화.

핵심 관리 프레임워크 주요 수명주기 상태

KMF는 허용되는 특정 작업의 적용을 통해 여러 암호화 키 수명 주기 상태를 지원합니다. 예를 들어 활성 상태인 키만 의도한 암호화 목적으로 완전히 사용할 수 있습니다. 다음 표에서는 다양한 키 수명주기 상태에 대해 자세히 설명합니다.

주요 수명주기 상태 또는 작업	설명
활성	암호화 모듈에는 지정된 암호화 사양에 대한 활성 키가 하나만 있을 수 있습니다.
손상됨	암호화 모듈의 지정된 암호화 사양에서 해지를 위해 손상된 상태로 여러 키가 존재할 수 있습니다. 활성 또는 일시 중단된 키는 손상된 상태로 이동할 수 있습니다. 손상된 키는 암호화 또는 서명과 같은 새 콘텐츠를 생성하는 데 사용할 수 없지만 암호 해독 또는 확인과 같은 기존 콘텐츠의 목적을 식별하는 데 계속 사용할 수 있습니다.
비활성화함	모든 활성 키를 비활성화할 수 있습니다. 암호화 모듈에서 지정된 암호화 사양에 대해 비활성화된 상태의 키가 여러 개 있을 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

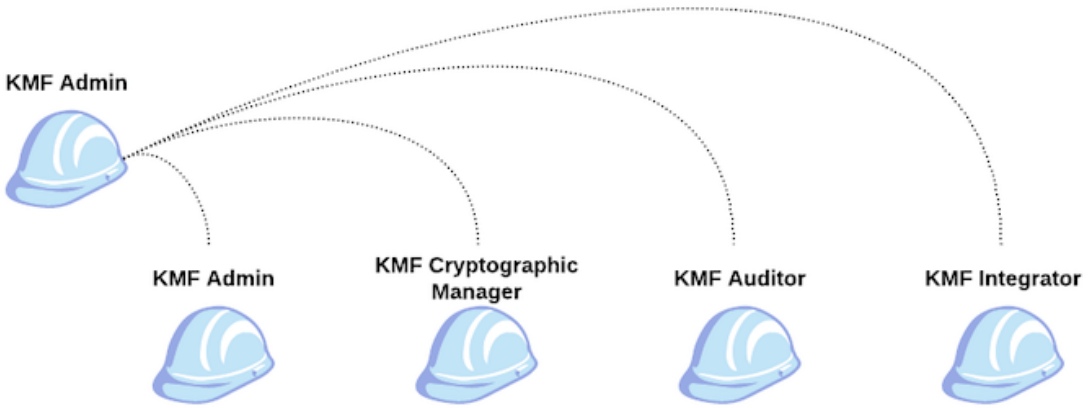
주요 수명주기 상태 또는 작업	설명
	예를 들어 키를 회전하면 현재 활성 키가 비활성화됩니다. 비활성화된 키는 암호화 및 서명과 같은 새 콘텐츠를 생성하는 데 사용할 수 없지만 암호 해독 또는 검증과 같은 기존 콘텐츠의 목적을 식별하는 데는 계속 사용할 수 있습니다. 주: 손상되거나 해지된 키는 비활성화된 키로 처리됩니다.
파괴됨	키가 파괴되면 키 자료가 영구적으로 제거되며 더 이상 암호화 목적으로 사용할 수 없습니다. 비활성화된 키는 구성된 지정된 시간 범위 내에 사용되지 않은 경우 수명주기 자동화를 사용하여 파기할 수 있습니다. 암호화 모듈에서 지정된 암호화 사양에 대해 파괴된 상태의 키가 여러 개 있을 수 있습니다. 경고: 삭제된 키와 관련된 데이터에 더 이상 액세스할 수 없으므로 키 삭제 작업을 수행할 때 각별한 주의를 기울여야 합니다.
작성됨	암호화 모듈에서 지정된 암호화 사양에 대해 생성된 상태에 여러 키가 존재할 수 있습니다. 지정된 암호화 사양에 대한 활성 키가 없는 경우 생성된 키를 활성 상태로 이동할 수 있습니다. 생성된 첫 번째 키는 자동으로 활성으로 설정됩니다. 주: 새 키를 생성하도록 선택하는 경우 지정된 암호화 사양에 대해 생성된 상태의 키가 있더라도 새 키가 생성되고 활성화됩니다.
갱신함	만료 날짜가 있는 활성 키는 키의 수명 주기를 연장하기 위해 여러 번 갱신할 수 있습니다. 주: 활성화 날짜와 만료 날짜 간의 차이가 계산되고 만료 날짜가 현재 날짜에서 해당 기간만큼 연기됩니다.
다시 시작	지정된 암호화 사양에 대한 다른 활성 키가 없는 경우 일시 중단된 키에서 UI 작업을 사용하여 키를 다시 활성 상태로 이동할 수 있습니다.
해지함	활성 또는 일시 중단된 키는 해지된 상태로 이동할 수 있습니다. 해지된 키는 암호화 또는 서명과 같은 새 콘텐츠를 생성하는 데 사용할 수 없지만 암호 해독 또는 확인과 같은 기존 콘텐츠의 목적을 식별하는 데 계속 사용할 수 있습니다. 해지된 상태의 여러 키가 암호화 모듈의 지정된 암호화 사양에 대해 존재할 수 있습니다.
회전함	키를 회전하면 현재 활성 키가 비활성화되고 다른 키가 활성화됩니다. 다음 중에서 새 활성 키를 선택합니다. • 새 키 생성. • 가져온 기존 키를 가리킵니다. 모든 활성 키는 회전할 수 있습니다.
일시 중단됨	암호화 모듈에서 지정된 암호화 사양에 대해 일시 중단된 상태의 키가 여러 개 있을 수 있습니다. 키가 일시 중단되면 해당 암호화 사양에 대한 다른 활성 키가 없는 경우 키를 다시 시작하고 활성 상태로 다시 할당할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 관리 프레임워크와 함께 설치되는 역할

(KMF)는 핵심 관리 프레임워크 암호화 모듈 및 키 관리 관련 구성에 대한 특정 역할을 소개합니다.

중요사항: KMF 역할을 사용하려면 핵심 관리 프레임워크. 역할이 없는 KMF 사용자는 키 관리를 구성하는 데 사용되는 목록, 테이블 및 모듈에 액세스할 수 없습니다.



KMF 관리자 [sn_kmf.admin]

ServiceNow 핵심 관리 프레임워크를 둘러싼 작업을 수행할 다른 사용자에게 역할을 할당합니다.

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

중요사항: 보다 전문적인 역할을 사용할 수 있는 경우 관리자 역할을 부여하지 마십시오.

- 이 역할은 에 나와 있는 프로세스를 통해 할당됩니다.
- KMF 역할을 할당하고 KMF 암호화 관리자의 모든 기능을 수행하려면 이 역할이 있어야 합니다.

KMF 암호화 관리자 [sn_kmf.cryptographic_manager]

암호화 모듈(암호화 사용 및 알고리즘 구성에 키 연결) 및 모듈 접근 정책에 대한 작업을 생성, 읽기 및 업데이트합니다. 또한 KMF 암호화 관리자는 키 관리(생성, 회전, 해지) 및 수명 주기 작업을 수행할 수 있습니다.

역할 포함

역할에 포함된 역할 목록입니다.

없음.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

없음.

KMF 암호화 감사자 **[sn_kmf.cryptographic_auditor]**

암호화 모듈 정보, 키 메타데이터, 수명주기 관련 상세 정보뿐만 아니라 모듈 액세스 정책(MAP) 정보를 봅니다.

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

없음.

KMF 암호화 통합자 **[sn_kmf.cryptographic_integrator]**

외부 키 스토어 또는 시스템과 통합합니다 핵심 관리 프레임워크 .

역할 포함

역할에 포함된 역할 목록입니다.

없음.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

없음.

특별 고려 사항

없음.

KMF 암호화 연산자 **[sn_kmf.cryptographic_operator]**

키 수명주기의 일부에 ServiceNow 핵심 관리 프레임워크 액세스합니다(갱신, 교체, 해지).

역할 포함

역할에 포함된 역할 목록입니다.

없음.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그룹

기본적으로 이 역할이 할당된 그룹 목록입니다.

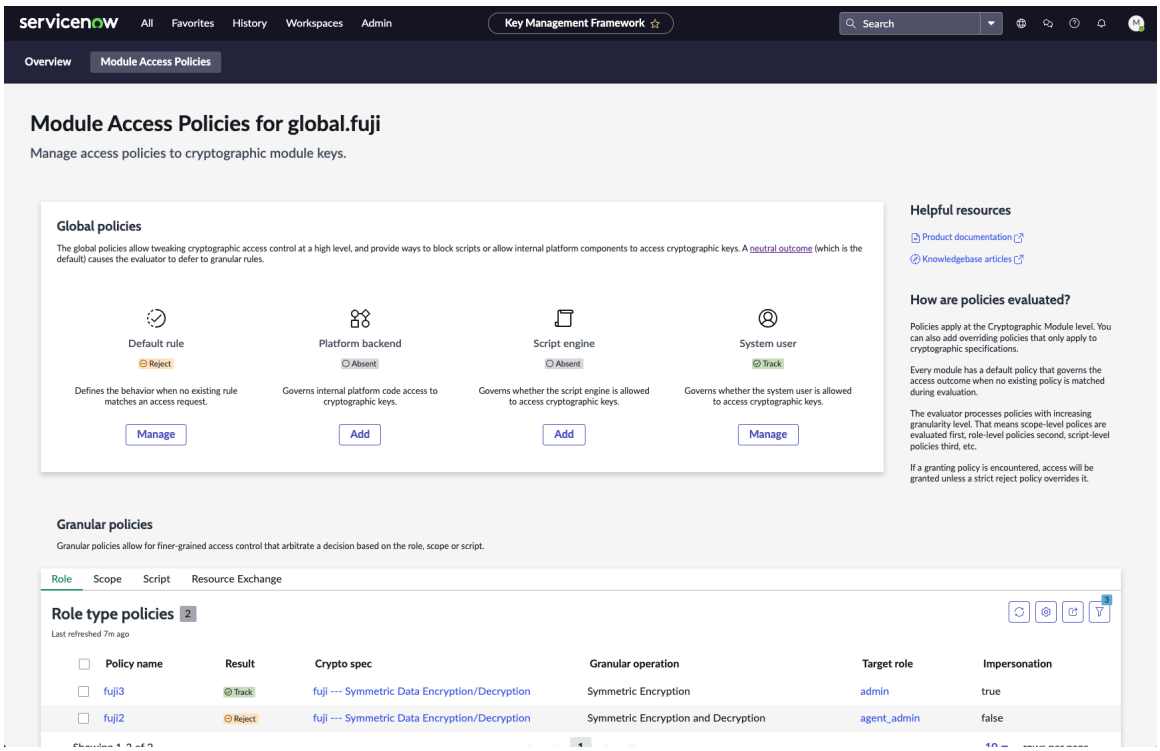
없음.

특별 고려 사항

없음.

모듈 액세스 정책 시각화

모듈 액세스 정책 시각화를 사용하여 단일 UI 페이지에서 모든 관련 암호화 모듈 정보를 봅니다.



Key Management Framework 관리자 및 암호화 관리자는 모듈 액세스 정책 UI 페이지를 사용하여 단일 암호화 모듈과 관련된 모든 액세스 제어 메커니즘을 볼 수 있습니다. 이 UI 페이지에서 수집한 정보를 사용하여 인스턴스의 암호화된 정보에 액세스할 수 있는 사용자를 확인합니다.

OR *sn_kmf.cryptographic_manager* 역할이 있는 *sn_kmf.admin* 사용자는 다음으로 이동하여 모듈 접근 정책 시각화 UI 페이지에 액세스할 수 있습니다. 모두 > 주요 운영 > 암호화 모듈 > 모두.

결과 레이블

모듈 액세스 정책에는 선택한 암호화 모듈에 대한 액세스 권한을 부여할지 여부를 결정하는 결과 필드가 포함되어 있습니다. UI 페이지는 해당 필드의 값을 기준으로 UI 페이지의 요소에 레이블을 표시합니다.

UI 레이블	결과 필드 값	정의
Track	*Track* 또는 *Allow*	스크립트를 포함하여 모든 사용자에게 액세스 권한이 부여됩니다.

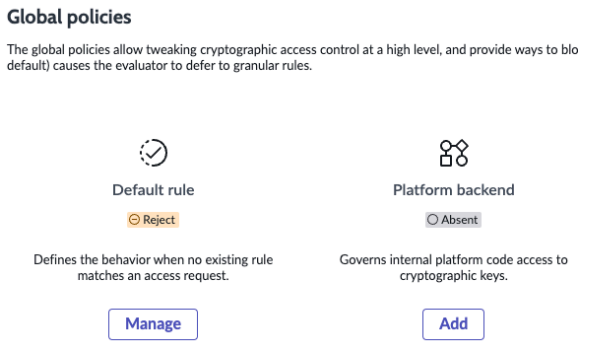
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

UI 레이블	결과 필드 값	정의
⊖ Reject	*Reject*	트랙 모듈 액세스 정책을 찾지 못한 경우 액세스가 거부됩니다.
⊗ StrictReject	*StrictReject*	접근이 거부되었습니다.
○ Absent	*N/A*	모듈 액세스 정책이 인스턴스에 없습니다. 모두에게 접근이 거부됩니다.

전역 정책

전역 정책 섹션을 사용하여 플랫폼 수준 액세스를 제어하는 모듈 액세스 정책을 검토합니다.

정책 아래에 있는 관리 버튼을 선택하여 해당 정책 기록으로 이동합니다. 정책이 없으면 해당 항목 아래에 추가 버튼이 나타납니다. 추가 버튼을 선택하여 정책을 정의할 수 있는 새 정책 기록으로 이동합니다.

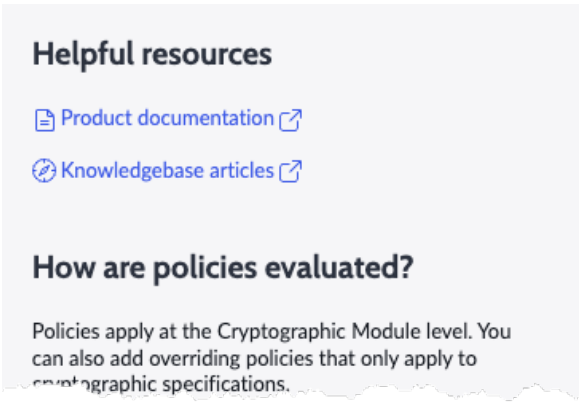


정책	정의
기본 규칙	기본 규칙 정책은 액세스 요청과 일치하는 기존 규칙이 없을 때 동작을 정의합니다.
플랫폼 백엔드	플랫폼 백엔드 정책은 암호화 키에 대한 내부 플랫폼 코드 액세스를 관리합니다.
스크립트 엔진	스크립트 엔진 정책은 스크립트 엔진이 암호화 키에 액세스할 수 있는지 여부를 제어합니다.
시스템 사용자	시스템 사용자 정책은 시스템 사용자가 암호화 키에 액세스할 수 있는지 여부를 제어합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

유용한 리소스

제품 설명서, 관련 지식 문서 및 플랫폼에서 모듈 액세스 정책이 평가되는 방식에 대한 간략한 설명에 대한 링크를 찾으려면 유용한 자원 섹션을 사용하십시오. 모듈 액세스 정책이 평가되는 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 모듈 접근 정책 디버거.

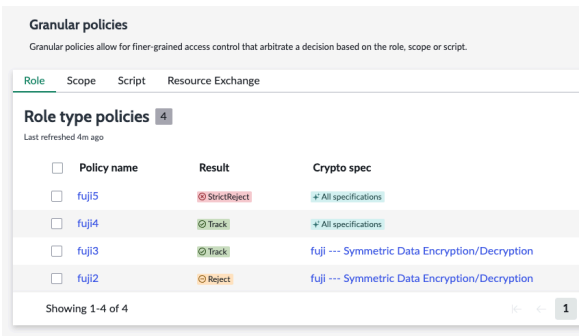


세분화된 정책

세분화된 정책 섹션을 사용하여 정책 유형별로 구분된 모듈 액세스 정책 목록을 봅니다. 목록 위의 탭을 사용하여 표시할 정책 범주를 선택합니다.

- 역할
- 범위
- 범위 및 도메인(도메인 분리가 활성 상태인 경우)
- 스크립트
- 자원 교환(암호화 모듈이 Password2 또는 필드 암호화 서브모듈인 경우)
- ID(비밀 관리 엔터프라이즈가 활성 상태인 경우)

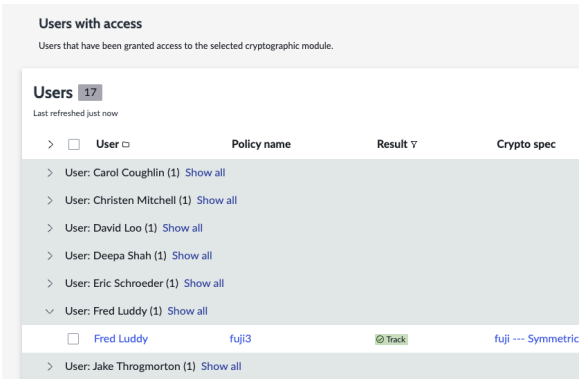
기본적으로 각 목록에는 활성 정책만 표시됩니다. 필터 아이콘을 사용하여 목록의 기본 필터를 변경합니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 권한이 있는 사용자

액세스 권한이 있는 사용자 섹션을 사용하여 선택한 암호화 모듈에 액세스할 수 있는 모든 사용자 목록을 봅니다. 단일 사용자가 암호화 모듈에 대한 액세스 권한을 부여하는 여러 역할을 가질 수 있으므로 목록은 사용자별로 그룹화됩니다.

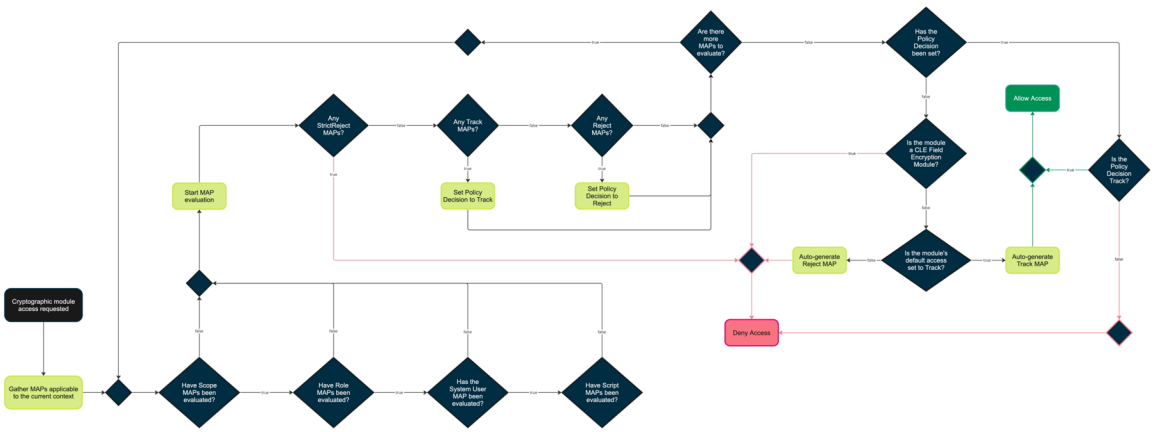


모듈 접근 정책 디버거

모듈 액세스 정책 디버거를 사용하여 로깅 정보를 검토하고 사용자에게 암호화 컨텍스트에 대한 액세스 권한이 부여되거나 부여되지 않는 이유를 이해합니다.

모듈 액세스 정책(MAP)은 암호화 모듈에 액세스하기 위한 인스턴스 수준 제어를 정의합니다. 호출자(예: 사용자 또는 스크립트)는 암호화 및 암호 해독에 암호화 모듈을 사용하기 위해 명시적 액세스 권한이 필요합니다. 디버거를 사용하여 호출자가 암호화 모듈에 액세스하려고 할 때 평가되는 정책을 확인합니다. 디버거를 사용하여 액세스 권한이 부여되거나 부여되지 않는 이유를 알아볼 수도 있습니다.

이 흐름도는 인스턴스가 암호화 모듈에 대한 액세스 요청을 평가하는 방법을 보여줍니다.



디버그 로그에 대한 접근 제어

모듈 액세스 디버그 로그에 대한 액세스는 역할에 따라 결정됩니다. 및 *sn_kmf.cryptographic_manager* 역할이 있는 *sn_kmf.admin* 사용자는 디버거에 액세스할 수 있습니다. 시스템 속성을 사용하여 다른 역할에 대한 액세스 권한을 *glide.kmf.module_access_policies.debugger.authorized.roles* 부여합니다. 이 속성의 값은 디버그 로그에 액세스하는 역할의 목록으로, 쉼표로 구분됩니다.

디버거 사용 또는 사용 안 함

모듈 액세스 정책에 대한 디버그 로깅 메시지를 사용하려면 다음으로 이동하십시오. 모두 > 진단 > 세션 디버그 > 디버그 모듈 액세스 정책 > .

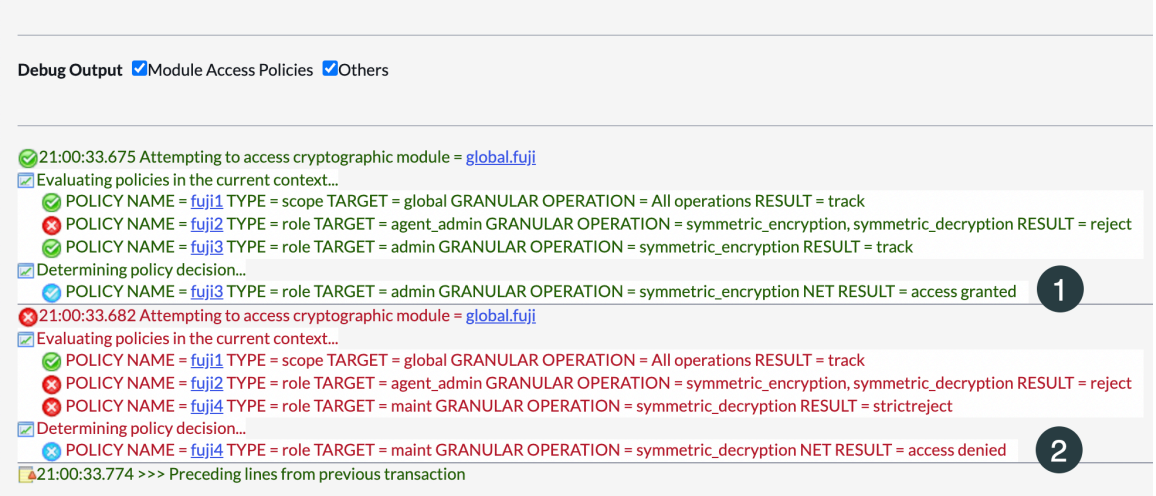
디버깅이 완료되면 다음으로 이동하여 로깅 메시지를 비활성화할 수 있습니다. 모두 > 진단 > 세션 디버그 > 모두 사용 안 함 > .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그에 액세스

디버깅을 활성화한 후 MAP 평가를 트리거하는 페이지로 이동하여 MAP 디버그 로그를 봅니다. 디버그 메시지는 페이지 하단에 나타납니다.

팁: 가장을 사용하여 다른 사용자의 액세스 문제를 해결할 수 있습니다. 가장에 대한 자세한 내용은 문서를 참조하십시오 사용자 가장 중 . 다른 사용자의 관점에서 디버그 로그를 보려면 해당 유형의 모듈 액세스 정책에 *role*가장 필드가 **true**로 설정되어 있는지 확인합니다.



이 예제에서 호출자는 `global.fuji` 암호화 모듈에 대한 두 개의 액세스 요청을 호출합니다. 부여된 대칭 암호화와 거부된 대칭 암호 해독.

로그 항목 이해

디버깅 정보는 이 형식을 사용하여 구조화됩니다.

1. 이 첫 번째 줄에는 액세스 요청을 받는 암호화 모듈이 표시됩니다.
2. 첫 번째 줄과 마지막 줄 사이의 줄에는 평가된 MAP이 평가 순서대로 표시되고 해당 이름, 유형, 대상, 세분화된 작업 및 결과가 포함됩니다.
3. 마지막 줄에는 정책 결정(해당하는 경우) 및 호출자에 대한 순 액세스 결과(호출자에게 액세스 권한이 부여되었는지 여부)가 표시됩니다.

각 줄은 메시지 유형을 나타내는 아이콘으로 시작합니다.

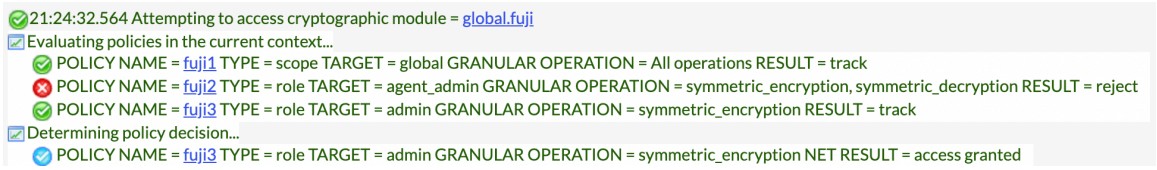
메시지 아이콘

아이콘	메시지 유형
	정보 메시지
	모듈 액세스 정책은 액세스 권한을 부여합니다.
	모듈 액세스 정책이 접근을 거부합니다.
	호출자에게 액세스 권한이 부여됨
	호출자의 액세스가 거부되었습니다.
	평가할 모듈 접근 정책 없음

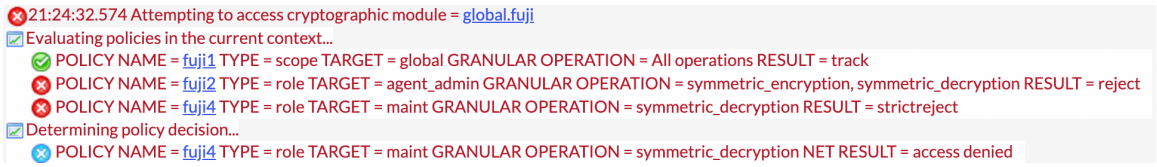
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

디버그 로그 예시

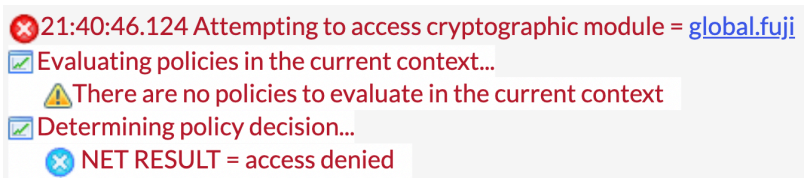
액세스 권한 메시지



접근 거부 메시지



액세스 거부됨(평가할 모듈 액세스 정책 없음)



접근 거부됨(권한 부족)



암호화 및 키 관리 구독 번들

키 관리를 필드 암호화 통해 고도로 구성 가능한 암호화 모듈을 포함하도록 추가 비용 없이 업그레이드됩니다. 필요에 따라 무제한 사용 라이센스로 업그레이드할 수도 있습니다. 및 를 포함하는 필드 암호화 엔터프라이즈 새 암호화 권리 번들인 Platform Encryption을 구독합니다 클라우드 암호화.

필드 암호화 기능

필드 암호화 with Encryption 모듈은 인스턴스에 무료로 포함되어 있으며 NIST 800-57 키 관리를 포함하며 다음을 지원합니다.

- ServiceNow 관리형 키가 지원됩니다(고객 제공 키는 지원되지 않음).
- 암호화 모듈에 대한 액세스는 역할 기반으로만 이루어집니다.
- 무제한 수동 키 회전.
- 최대 5개의 암호화 모듈.
- 최대 5개의 모듈 접근 정책.
- 기존 필드 유형이 지원됩니다. (이후 버전에서 생성된 필드 유형은 엔터프라이즈가 아닌 버전에서는 지원되지 않습니다.)
- API 지원은 역할 액세스에 따라 사용할 수 있습니다.
- 암호화 작업의 감사.
- 필드 암호화 가이드가 있는 둘러보기.

ServiceNow 플랫폼 암호화 그룹 기능

Platform Encryption 그룹은 다음과 같은 기능 및 오퍼링을 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 필드 암호화 엔터프라이즈:
  - 고객이 제공한 키입니다.
  - 자동 키 회전.
  - 고급 필드 유형 지원 및 향후 업데이트.

    주: 확장된 필드 유형 지원에는 저널, 저널 목록, 저널 입력, **HTML** 및 번역된(필드/텍스트/**HTML)** 필드 유형이 포함됩니다.

  - 고급 첨부 파일 지원.
  - 암호화 모듈 액세스는 다음에 따라 모듈 액세스 정책을 사용하여 부여할 수 있습니다.
    - 시스템 사용자
    - 스크립트
    - 특정 애플리케이션 범위
  - 무제한 암호화 모듈 및 모듈 접근 정책.
  - 웹 서비스에서 키를 임포트합니다.
  - 암호화 키의 향후 회전 날짜를 설정합니다.
- 클라우드 암호화 키 관리 포함.

추가 정보

키 관리에 대한 자세한 내용은 다음 문서를 참조하십시오 키 관리 프레임워크 탐색.

키 관리 작업

KMF의 핵심 기능 중 하나는 키 해지 또는 회전과 같은 키 관리 기능을 제공하는 것입니다. KMF는 최신 암호화 자료 및 수명 주기 작업으로 중요한 데이터를 적절하게 보호합니다.

다음 표에서는 주요 수명주기 운영 및 관리 작업에 대한 요약을 제공합니다. 암호화 모듈 목적은 암호화 모듈 구성으로 데이터에 적용되며 데이터에 영향을 주지 않습니다.

키 관리 작업	설명
키 작성	지정된 암호화 모듈에 대한 새 키를 작성합니다. 첫 번째로 생성된 키는 *##*으로 설정됩니다.
키 회전	현재 키를 비활성화하고 새 키를 작성합니다. 새 모듈 키는 현재(활성)로 설정됩니다.
키 해지	현재 키와 수명주기 상태를 해지됨으로 표시합니다. 암호화 모듈은 새 데이터에 새 키를 자동으로 생성하고 키 상태를 활성으로 설정합니다. 해지됨은 키가 더 이상 암호화에 사용되지 않음을 의미합니다. 그러나 여전히 암호 해독에 사용할 수 있습니다. 열쇠는 파괴할 수 없습니다.
키 일시 중단	현재 키를 일시 중단된 것으로 표시합니다. 암호화 모듈을 다시 사용하기 전에 일시 중단된 키를 수동으로 다시 시작하거나 일시 중단된 키를 취소하여 새 모듈 키를 생성하십시오.
다시 시작 키	일시 중단된 키를 활성 키로 표시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 관리 작업	설명
키 리뉴얼	현재 키의 수명을 연장합니다. 갱신 버튼은 다음과 같은 경우에 사용할 수 있게 됩니다. • 암호화 관리자 역할이 할당됩니다. • 수명주기 상태는 활성 또는 갱신됨으로 표시됩니다. • 만료 날짜는 모듈 수명주기 정의에 설정됩니다.

키 보기 및 관리

키의 상태를 검토하여 현재 키의 갱신, 교체, 일시 중단, 비활성화 또는 삭제 시기와 같은 추가 키 작업을 결정합니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager

프로시저

1. 다음으로 이동 모두 > 주요 운영 > 암호화 모듈 > 모두.
2. 암호화 모듈을 선택합니다.

   암호화 모듈〈모듈 이름> 양식이 나타납니다.

3. 모듈 키 탭에서 키 별칭을 선택하여 수명주기〈키 이름> 양식의 키 상태를 검토합니다.
4. 모든 필드가 읽기 전용이므로 양식을 검토합니다.

암호화 수명주기 키 필드

필드	설명
작성 날짜	키가 생성된 날짜를 표시합니다.
활성화 날짜	키가 활성화된 날짜를 표시합니다.
마지막 갱신 날짜	키가 마지막으로 갱신된 날짜를 표시합니다.
마지막 교대 날짜	키를 마지막으로 회전한 날짜를 표시합니다.
비활성화 날짜	키가 비활성화된 날짜를 표시합니다.
소멸 날짜	키가 삭제된 날짜를 표시합니다.
주요 수명주기 상태	키 수명주기 상태를 표시합니다.
추후 활성화 날짜	미래의 키 활성화 날짜를 표시합니다.
추후 갱신 날짜	향후 키 갱신 날짜를 표시합니다.
추후 순환 날짜	키 회전의 미래 날짜를 표시합니다.
추후 소멸 날짜	키가 삭제되는 미래 날짜를 표시합니다.
만료 날짜	키가 만료되는 날짜를 표시합니다.

5. 키에 대한 작업을 수행하려면 다음 중 하나를 선택하여 즉시 적용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 키 해지: 키를 비활성화하고 새 키를 생성하려면 선택합니다. 키를 해지하는 이유를 입력합니다.
- 키 회전: 현재 키를 비활성화하고 그 자리에 새 키를 생성하려면 선택합니다. 새 키가 모듈 키 테이블에 나열되고 키 버전 번호가 1씩 증가합니다. 자세한 내용은 다음을 참조하십시오.
- 키 중단: 현재 키를 비활성화하려면 선택합니다.
- 키 다시 시작: 일시 중단된 키를 활성 키로 표시하려면 선택합니다. 이 옵션은 활성 키가 일시 중단된 후에만 사용할 수 있습니다.

키 회전

보안을 강화하기 위해 미리 결정된 일정에 따라 암호화 키를 순환할 수 있습니다. 키 순환은 암호화 키를 폐기하고 새 암호화 키를 생성하여 이전 키를 교체하는 경우입니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager

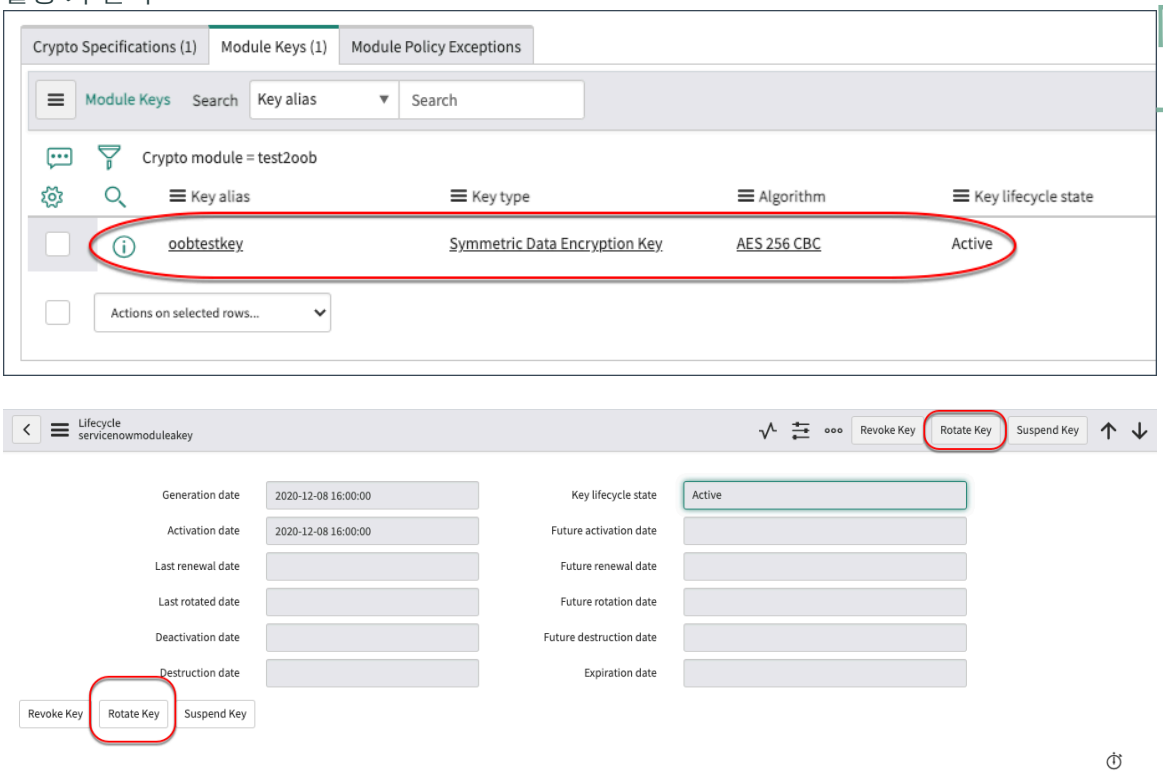
이 태스크 정보

암호화 컨텍스트와 달리 암호화 모듈은 새 키로 다시 암호화하기 위한 레코드 키 재입력을 지원합니다. 다음은 암호화 모듈에서 키 회전 작업을 수동으로 수행하는 방법을 보여 줍니다.

프로시저

1. 다음으로 이동 주요 운영 > 암호화 모듈 > 모두.
2. 키 회전을 위한 암호화 모듈을 선택합니다.
3. 모듈 키 탭에서 활성 키를 선택합니다.

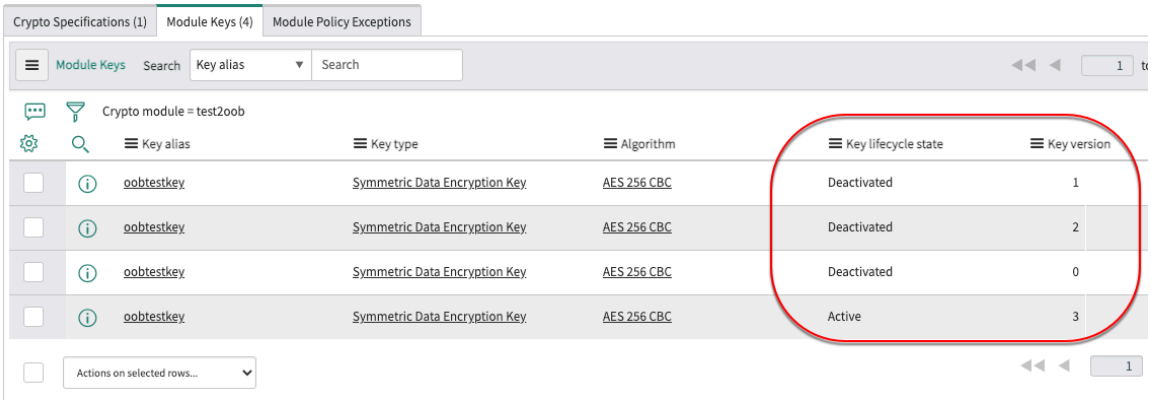
활성 키 선택



4. 키 회전을 선택합니다.
   주요 수명주기 상태가 "비활성화됨"으로 변경됩니다. 마지막 교대 날짜, 비활성화 날짜 및 키 버전 필드가 업데이트됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 반환 대상 암호화 모듈 > 모듈 키입니다.



테이블에 나열된 추가 모듈 키가 있습니다. 새로 회전한 키는 "활성"이 되고 마지막 키는 "비활성화됨"이 됩니다.

웹 서비스에서 키 임포트

웹 서비스에서 키 임포트(예: 키 REST API)를 사용하여 외부 고객 키를 인스턴스에 안전하게 업로드합니다. 대칭 및 비대칭 공개 키는 모두 대상 KMF 암호화 모듈로 가져올 수 있습니다.

임포트할 키(대상 키)는 인스턴스의 대상 암호화 모듈에 업로드되기 전에 래핑 키로 암호화되어야 합니다. 이 래핑 키는 인스턴스에 있어야 하는 공개/개인 키 쌍의 공개 구성 요소입니다. 키는 웹 서비스에서 임포트를 통해 래핑된 대상 키를 업로드하기 위한 필수 조건입니다.

이 두 가지 개별 절차(래핑 키 페어 가져오기 및 웹 서비스에서 래핑된 대상 키 가져오기)는 다음 설명서에 자세히 설명되어 있습니다. 이 키 페어를 작성하고 업로드해야 인스턴스의 내부 키 임포트 암호화 모듈에서 사용할 수 있습니다.

주: 이 예제에서는 키 및 인증서 생성에 OpenSSL을 사용하고 Postman API 테스트 도구를 사용하여 REST API 사용을 보여줍니다. 회사 요구 사항에 따라 다른 유사한 도구를 대체하십시오.

키 쌍의 래핑/래핑 해제 임포트

키를 임포트하기 전에 임포트 설정을 구성합니다 핵심 관리 프레임워크 .

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager

이 태스크 정보

이 예에서는 키 및 인증서 생성에 OpenSSL을 사용합니다. 회사 요구 사항에 따라 다른 유사한 도구를 대체하십시오.

프로시저

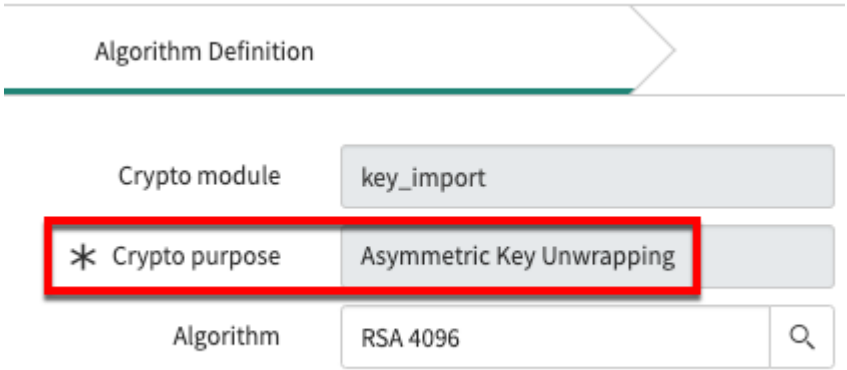
1. 로컬 환경에서 터미널을 사용하여 인증서를 생성합니다.
   예: `openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:4096 -keyout wrapping_private.key -out wrapping_public.crt`

   이 인증서는 키를 포함하는 공용 구성 요소입니다. 인증서는 AES 대칭 키를 래핑하는 데 사용됩니다.

2. 로컬 환경에서 터미널을 사용하여 공용 인증서(래핑 키 포함) 및 개인 래핑 해제 키가 포함된 키 저장소를 생성합니다.
   예:`openssl pkcs12 -export -in wrapping_public.crt -inkey wrapping_private.key -name "wrapping_key_alias" -out wrapping_keystore.p12`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 인스턴스에서 다음으로 이동합니다. 모두 > 주요 운영 > 설정 임포트 > 주요 임포트 설정.
4. Algorithm Definition(알고리즘 정의) 섹션에서 **Crypto Purpose** (암호화 목적)가 *Asymmetric Key Unwrapping(### # ##* 해제)으로 설정되어 있는지



확인합니다.

5. 임포트한 키 스토어의 비대칭 키 자료에 맞는 적절한 알고리즘을 선택합니다.
자세한 내용은 암호화 사양 문서를 참조하십시오.
6. 다음을 선택합니다.
7. 수명 주기 정의 섹션에서 다음을 선택하여 계속합니다.
8. **Key** Origin(키 원본) 섹션의 Origin(원본) 필드에서 **Import from** PKCS12(PKCS12에서 가져오기) 또는 **Import from** BCFKS(BCFKS에서 가져오기)를 선택합니다.

   주: 1단계의 예제 키 저장소를 사용하는 경우 PKCS12에서 가져오기를 선택합니다.

9. 키를 식별하기 위한 키 별칭 을 입력합니다.
이 별칭은 업로드할 인증서 또는 키 저장소를 생성할 때 지정된 키 별칭(또는 "식별 이름")과 일치해야 합니다. 위의 예를 계속하면 `wrapping_key_alias` 됩니다.
10. 다음을 선택합니다.
Key Creation 섹션에는 키 스토어를 업로드하는 대화 상자를 표시하는 **Import Key** 링크가 포함되어 있습니다. 예제를 계속하면 `wrapping_keystore.p12`가 됩니다.

웹 서비스에서 래핑된 키 임포트

웹 서비스 기능에서 키 임포트를 사용하여 래핑된 키를 암호화 모듈에 업로드합니다. 이 예제에서는 대칭 키를 사용합니다. 유사한 단계를 사용하여 비대칭 키를 가져올 수 있습니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager(모듈 구성), sn_kmf.cryptographic_operator(REST 운영 기본 인증)

이 태스크 정보

KMF 키 임포트 프로세스를 완료하려면 키 엔드포인트 임포트 액세스가 필요합니다.

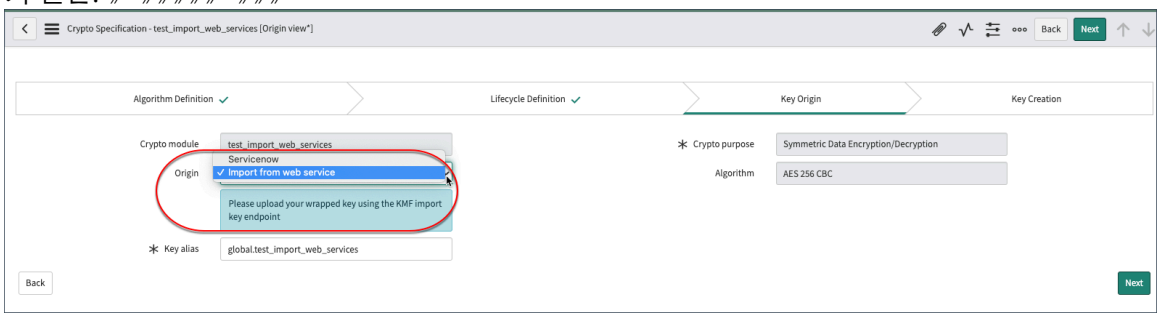
이 예제에서는 OpenSSL을 사용하여 키와 인증서를 생성합니다. 요구 사항에 따라 다른 유사한 도구를 대체할 수 있습니다.

프로시저

1. 로컬 장치의 터미널을 사용하여 키 임포트 모듈 공개 키 래핑 키를 사용하여 대칭 키를 래핑합니다.
예: `openssl pkeyutl -encrypt -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`
이 예제에서는 `wrapped_symmetric_key.txt`라는 래핑된 키 파일을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. API에 연결할 암호화 모듈을 생성합니다.
   자세한 내용은 또는 문서를 참조하십시오.
3. 다음 선택 항목으로 암호화 사양을 추가합니다.
   - 암호화 목적: *## ### ###/## ##*.
   - 키 원본: *# ##### ###*



   자세한 내용은 또는 문서를 참조하십시오.

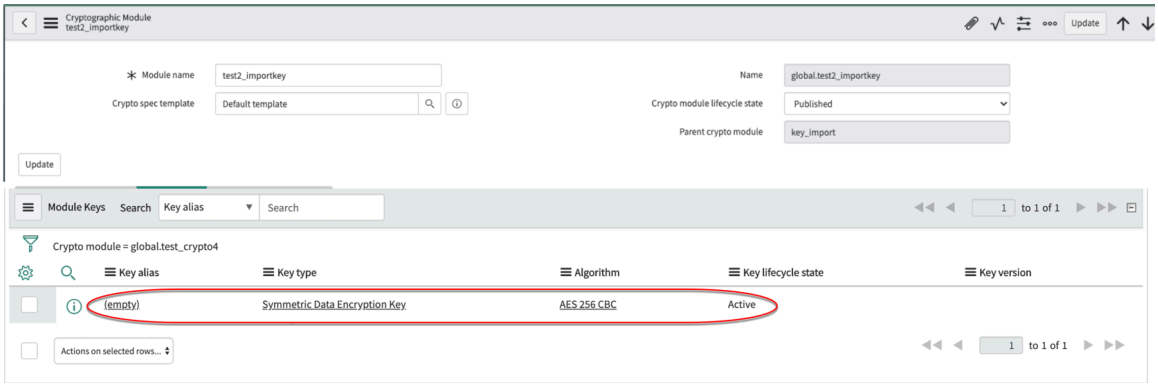
4. 웹 서비스 REST 엔드포인트에서 임포트하기 위해 *HTTP POST ###*실행합니다.

옵션	값/형식
엔드포인트의 URL	*https://<instance>/api/sn_kmf/key/import?cryptoSpecSysID=<sys_id_of_crypto_spec>*.
CryptoSpecSysID 매개변수	새로 만든 암호화 사양의 *sys_id*입니다. **팁:** 암호화 사양의 헤더를 마우스 오른쪽 버튼으로 클릭하여 *sys_id*복사합니다.
header-content-type	Application/octet-stream입니다.
본문	첨부 파일 이진 파일 및 가져올 공개 키 (wrapped_symmetric_key.txt)를 포함해야 합니다.
웹 서비스 REST 엔드포인트에서 임포트	*<### ##/##>*의 기본 인증을 사용합니다. **주:** 지정된 사용자에게 sn_kmf_cryptographic_operator 역할이 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

공개 키를 성공적으로 가져오면 *### 200*인 HTTP 응답 메시지가 표시됩니다.

5. 키를 대상 암호화 모듈로 성공적으로 임포트했는지 확인합니다.



핵심 관리 프레임워크 상태

에 핵심 관리 프레임워크대한 요청 시 상태 정보에 액세스합니다. 경고 및 오작동 오류에는 자세한 메시지가 포함되어 있습니다.

시작하기 전에

필요한 역할: sn_kmf_cryptographic 감사자 또는 sn_kmf_admin 또는 sn_kmf_cryptographic_manager

이 태스크 정보

의 핵심 관리 프레임워크 각 구성요소에 대한 설명이 표시되고 다음과 같은 상태와 색상이 보고됩니다.

- 녹색/운영: 구성요소가 정상 작동 중이며 보고할 오류가 없습니다.
- 회색/사용 안 함: 구성요소가 비활성 상태이므로 상태 검사가 수행되지 않습니다.
- 노란색/성능 저하: 경고, 구성 요소가 작동 중이지만 지연/일시적인 문제가 발생할 수 있습니다.
- 빨간색/오작동: 치명적인 오류로 인해 구성 요소가 작동하지 않아 부분 정전이 발생할 수 있습니다.

구성요소에는 개별 보고서가 있는 하위 구성요소가 포함될 수 있으며, 자체 상태는 다음과 같이 상위 항목에 영향을 미칩니다.

- 모든 하위 구성요소가 비활성 상태인 경우 상위는 비활성으로 표시됩니다. 비활성 하위 구성 요소는 부모의 상태에 영향을 미치지 않습니다.
- 하나 이상의 하위 구성요소가 성능 저하되거나 오작동하는 경우 상위 상태가 성능 저하됨으로 표시됩니다.
- 모든 하위 구성요소가 오작동으로 보고되면 상위 구성요소도 오작동으로 보고됩니다.

하위 구성요소에 대한 자세한 내용은 다음 문서를 참조하십시오 Key Management Framework의 인스턴스 수준 키.

주: 상태 검사는 15초마다 실행됩니다. 상태 페이지를 새로 고쳐 보고서를 다시 실행합니다.

프로시저

1. 다음으로 이동 모두 > 주요 운영 > > 진단.
2. 다음 상태 정보를 검토합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

진단 정보

범주	세부사항
키 보안	암호화를 시도하고 있는지 확인합니다.
파일 키 스토어	인스턴스 루트 키(IRK) 가져오기 시도가 발생하는지 확인합니다. 주: 파일 키 스토어는 온프레미스 인스턴스 및 개발자 인스턴스에 사용되는 Key Secure의 오프라인 대안입니다.
GlideEncrypter	GlideEncrypter 인스턴스 수준 암호화 모듈, 사양 및 키가 있는지 확인합니다. 주: GlideEncrypter는 를 핵심 관리 프레임워크통해 필드 및 기타 레거시 암호화 사용을 투명하게 암호화 Password2 할 수 있는 스크립트 가능 구성요소입니다.
인스턴스 키 암호화 키(IKEK)	파일 키 스토어 또는 KeySecure에서 키를 가져올 수 있는지 확인합니다.
인스턴스 HMAC 키	파일 키 스토어 또는 KeySecure에서 키를 가져올 수 있는지 확인합니다.
Vault PKI	Vault 연결을 검사하여 인스턴스 비대칭 암호화 키(IAEK) 및 인스턴스 서명 키(ISK)를 사용할 수 있고 Vault에서 가져올 수 있는지 확인합니다.
EJBCA PKI	LDAP 연결을 검사하여 IAEK 및 ISK를 사용할 수 있고 캐시 및 LDAP에서 가져올 수 있는지 확인합니다.
인스턴스 PKI	파일 키 저장소 및 KeySecure에서 키를 검사하고 인증서가 있으며 대칭 키와 일치하는지 여부를 확인합니다. 주: 인스턴스 PKI는 데이터센터 내의 인스턴스에서만 사용할 수 있습니다 ServiceNow .

문제 해결에 대한 지원이 필요한 경우 로 문의하십시오 고객 서비스 및 지원.

GlideEncrypter 사용 중단을 위한 인스턴스 준비

인스턴스 스캔 스크립트를 사용하여 인스턴스에서 GlideEncrypter API 호출을 찾아 제거합니다. 이러한 호출을 제거하는 것은 인스턴스에서 3DES 암호화를 사용 중단하는 데 필요한 단계입니다.

시작하기 전에
필요한 역할: 관리자

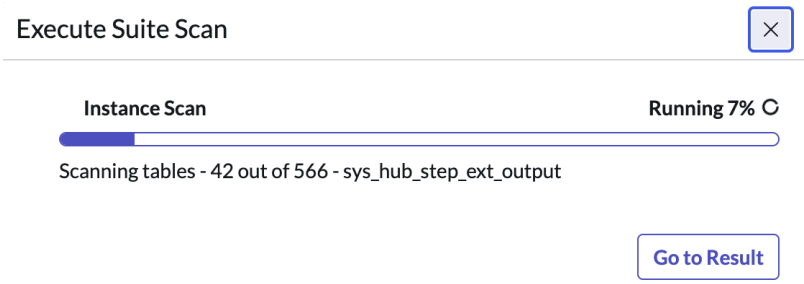
GlideEncrypter API는 의 취리히 릴리스 ServiceNow부터 더 이상 사용되지 않을 예정입니다. 스크립트에서 GlideEncrypter 호출을 제거하는 것도 인스턴스에서 3DES 암호화를 사용 중단하기 전에 필요한 단계입니다.

프로시저

1. 다음으로 이동 모두 > **Instance Scan** > 도구 모음.
2. 도구 모음 목록에서 **GlideEncrypter**를 선택하여 GlideEncrypter 사용량이 있는 기록을 식별합니다.
3. 도구 모음 기록에서 도구 모음 스캔 실행을 선택합니다.
4. 지금 스캔 도구 모음 창에서 전체 인스턴스를 선택한 다음 스캔 실행을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

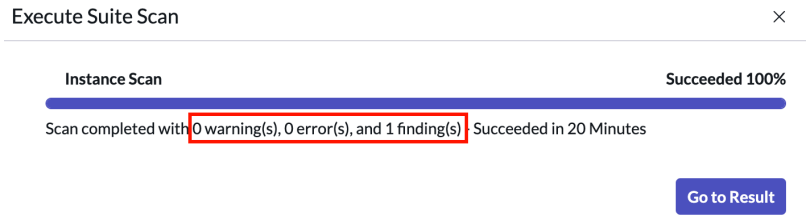
도구 모음 스캔이 실행됩니다. 검사 실행 중에 검사 실행 창에 검사 진행률이



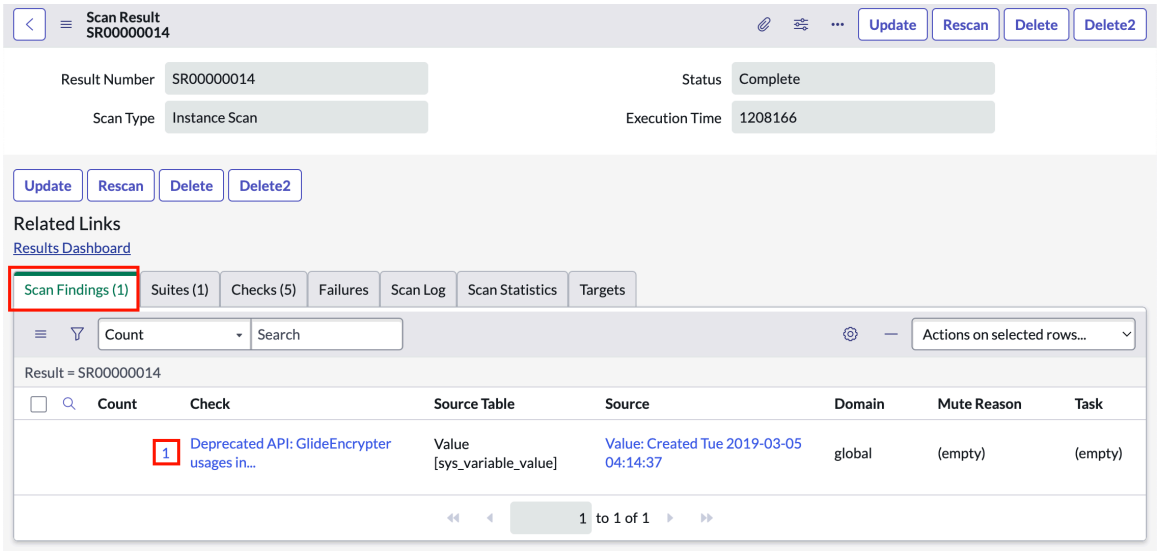
표시됩니다.

주: 이 스캔은 고객이 생성하거나 수정한 기록만 검사합니다.

5. 스캔이 완료되면 결과로 이동을 선택하여 스캔 결과 기록을 봅니다.



6. 스캔 결과 기록에서 스캔 결과 목록의 카운트 필드를 선택하여 기록으로 이동합니다.



7. **GlideEncrypter** API를 사용하는 기록의 스크립트를 수정합니다.
GlideEncrypter를 대체하는 방법에 대한 자세한 내용은 지원 중단된 GlideEncrypter API의 대체 항목을 참조하십시오.
8. 스크립트에서 **GlideEncrypter** 호출을 제거한 후 스캔을 다시 실행하여 API에 대한 호출이 남아 있지 않은지 확인합니다.

다음에 수행할 작업
password2 필드에 대한 3DES의 GlideEncrypter 사용 중단

password2 필드에 대한 3DES의 GlideEncrypter 사용 중단

인스턴스에서 3DES 암호화 표준의 GlideEncrypter 사용 중단 인스턴스에서 Password2 데이터의 암호화 및 복호화를 위해 더 안전한 AES(Advanced Encryption Standard)만 사용하는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

부터 Romepassword2 데이터는 최신 AES(Advanced Encryption Standard) 알고리즘을 사용하는 를 핵심 관리 프레임워크사용하여 보호됩니다. 그러나 password2 논리의 일부 구성 및 폴백에서는 암호화 및 암호 해독에 3DES 알고리즘을 계속 사용할 수 있습니다.

Vancouver 이 릴리스에서 관리자는 3DES 알고리즘을 완전히 사용 중단하도록 선택할 수 있습니다. 이 변경을 완료하면 인스턴스는 password2 데이터와 관련된 모든 암호화 및 암호 해독 작업에 AES 암호화만 사용합니다. 이러한 변경은 3DES 암호화에 비해 더 나은 인스턴스 보안을 제공하며 NIST 규정을 준수하는 데 필요합니다.

사용 중단 전 고려 사항

인스턴스 간 password2 데이터 전송

password2 암호화 텍스트를 다른 인스턴스로 전송할 때는 소스 인스턴스와 대상 인스턴스 간에 이 KMF 키 교환 기능이 활성화되어 있는지 확인해야 합니다. 이 구성을 통해 password2 텍스트를 암호화하는 데 사용되는 키를 두 인스턴스 모두에서 사용하여 password2 암호화된 텍스트를 해독할 수 있습니다. 3DES를 사용 중단하기 전에 인스턴스 간 password2 데이터에 영향을 줄 수 있는 다음 사용 사례를 고려하십시오.

- password2 데이터를 사용하는 인스턴스가 있는 경우 해당 인스턴스에 애플리케이션이 설치되어 있는지 KMF 자원 교환 확인합니다. KMF 자원 교환 소스 인스턴스에서 password2 데이터를 암호화하는 데 사용되는 인스턴스 수준 키를 대상 인스턴스에서 암호 해독에 사용할 수 있도록 합니다. 자세한 내용은 키 관리 프레임워크 자원 교환 문서를 참조하십시오.
- XML 또는 데이터 소스를 통해 password2 데이터를 익스포트하려는 경우 대상 인스턴스가 KMF 키 교환 활성화되어 있는지 확인합니다. 이렇게 구성하면 소스 인스턴스에서 password2 데이터를 암호화하는 데 사용되는 인스턴스 수준 키를 대상 인스턴스에서 암호 해독에 사용할 수 있습니다. 이 구성에 대한 자세한 내용은 을 참조하십시오 키 관리 프레임워크 키 교환.

> **중요사항:** 위의 예는 더 일반적인 시나리오이지만 인스턴스 간에 password2로 암호화된 텍스트를 전송하는 다른 방법을 사용하는 경우 대상 인스턴스가 password2 데이터를 해독할 수 있도록 구성해야 KMF 자원 교환 합니다.

3DES 사용 중단 후 인스턴스 다운그레이드

다음은 password2 필드가 있고 입력 길이가 125자를 초과하며 이미 3DES 암호화를 사용하지 않는 인스턴스에만 적용됩니다.

인스턴스 복제를 통하지 않고 Vancouver 일찍 릴리스하도록 인스턴스를 다운그레이드하려면 복제를 시작하기 전에 다음 단계를 수행합니다.

1. password2 필드 데이터를 보존하도록 데이터 보존이 구성되어 있는지 확인합니다.
2. 그렇다면 클론을 요청하기 전에 지원 부서에 연락하여 ServiceNow 3DES 사용 중단을 비활성화하십시오. 이유 필드에 "password2 지원을 위한 클론 다운그레이드 필수 구성요소"를 사용합니다.

레거시 password2 필드

인스턴스는 3DES 암호화를 사용하여 password2 데이터를 레거시(이전Rome) password2 데이터로 변환합니다. 3DES 암호화를 사용하지 않으면 이 옵션을 더 이상 사용할 수 없습니다. 이 기능이 여전히 필요한 경우 부분 사용 중단을 요청합니다 (다음 섹션의 세부 정보 참조).

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3DES 사용 중단 방법

앞의 사용 사례를 검토한 후 단계별 프로세스에 KB1704481 지식베이스 문서를 사용하여 인스턴스에서 DES 또는 Triple DES 알고리즘 사용을 안전하게 중단합니다. 자세한 내용은 KB1704481 참조하십시오.

중요사항: 보안 준수 모듈을 확인하고 다음 단계를 수행하려면 보안 관리자로 승격해야 합니다. 해당 프로세스에 대한 자세한 내용은 권한 있는 역할로 상승 문서를 참조하십시오.

GlideEncrypter 사용 중지 이후

사용 중단 프로세스가 완료되면 다음 정보가 인스턴스에 적용됩니다.

- password2 필드는 3DES 암호화 데이터의 암호 해독(암호화는 아님)을 계속 지원합니다.
- password2 필드의 기존 3DES 암호화 데이터는 사용자나 워크플로우가 필드 값을 업데이트할 때까지 그대로 유지됩니다.
- password2 필드 값을 업데이트하면 3DES 암호화 텍스트가 제거되고 AES를 사용하여 암호화된 KMF 텍스트로 바뀝니다.
- 암호 데이터를 저장할 때 인스턴스에 오류가 표시되는 경우도 있습니다.

  ```
  ## ###: #### ### ## ## ## ### # ####. ### #### KB1296997 ######.
  ```

  이 오류가 표시되면 지식베이스 문서 KB1296997 의 지원 정보를 참조하십시오.

키 관리 프레임워크 자원 교환

ServiceNow® 자원 교환KMF 는 안전한 방식으로 인스턴스 간에 자원을 교환할 수 있는 기능을 제공하는 기능입니다.

용어

를 자원 교환사용하는 경우 다음 용어를 참조하십시오.

자원 교환 용어

이름	설명
자원 교환	인스턴스 간에 자원을 교환하는 프로세스입니다.
키 교환 (KE)	인스턴스 간에 키를 교환하는 프로세스입니다.
키 소스 인스턴스(키 소스)	키를 소유한 인스턴스입니다.
키 대상 인스턴스(키 대상)	키를 요청하는 인스턴스입니다.

개요

자원 교환 는 KMF 암호화 API를 활용하여 기밀성, 무결성, 인증 및 부인 방지를 제공합니다. 자원 교환 현재 기능을 지원합니다키 교환. 자세한 내용은 키 관리 프레임워크 키 교환 문서를 참조하십시오.

키 관리 프레임워크 키 교환

KMF 키 교환 의 하위 집합 함수 KMF 자원 교환입니다. 키 교환 암호화된 데이터를 여러 인스턴스에 안전하게 전송합니다.

키 교환 개요

키 교환 인스턴스 간에 키를 안전하게 전송합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

KMF 키 교환 는 고객이 인스턴스 간에 키를 안전하게 교환할 KMF 수 있는 방법을 제공합니다. 한 가지 애플리케이션 사용 사례는 데이터 복제 프로세스입니다. 를 사용하면 키 교환구성요소의 KMF 데이터 복제 중에 암호화 모듈 키가 복사됩니다. 암호화 모듈, 모듈 키 사양 및 모듈 액세스 정책은 복제 프로세스에 포함됩니다. 키 전송은 포함되지 않습니다.

이 기능은 ServiceNow Platform Encryption 구독 번들에 포함된 에 핵심 관리 프레임워크포함되어 있습니다. 이 제품에 대한 자세한 내용은 를 참조하십시오 Key Management Framework.

키 교환 사용

를 사용하는 KMF 관리자는 데이터 필드 암호화 복제를 수행할 때 프로덕션 인스턴스 간에 키를 클론하는 데 사용할 키 교환 수 있습니다. 데이터 복제에서 관리자/ KMF 암호화 관리자는 다음을 수행할 수 있습니다.

- 모든 키를 다른 인스턴스로 교환합니다.
- 특정 키를 한 번 또는 주기적으로 다른 인스턴스로 교환합니다.
- 대상 인스턴스에서 키 소스 인스턴스로 요청 시 요청을 보냅니다.
- 암호 텍스트를 다시 입력하기 위해 소스에서 대상으로 키를 교환합니다.
  - 키가 만료된 경우 키를 삭제하거나 키 교환 요청을 거부할 수 있는 기능을 사용하여 요청의 만료 시간을 관리합니다.
  - 요청이 완료되고 키를 가져오면 사용된 키가 만료되고 타임스탬프가 지정된 것으로 설정됩니다.
  - 소스의 키로 암호화된 대상 인스턴스에서 암호 텍스트를 다시 입력합니다.

지원 모드

키 교환 는 암호화 모듈 암호화 사양 수준에서 여러 모드를 지원합니다.

모드	설명
자동(구성 없음, 기본 동작)	모든 키는 추가 구성 없이 데이터 복제 프로세스 중에 자동으로 전송됩니다.
구성 가능 (일회성 구성 설정)	관리자는 데이터 복제 프로세스 중에 보낼 키를 구성합니다.
수동(루프 내 사람)	관리자는 대상 인스턴스에 대한 요청 시 요청을 소스로 보냅니다. 요청은 키 소스 인스턴스에서 관리자가 승인해야 합니다.
키 다시 입력 (자동 요청)	관리자는 복제 설정 프로세스 중에 키 재설정 옵션을 선택합니다.

키 교환 구성

핵심 관리 프레임워크 (KMF)는 인스턴스를 새로 설치하거나 업그레이드하는 동안 지원되는 암호화 모듈에 대한 자동 키 교환 요청을 생성합니다. 인스턴스의 데이터 암호화 키를 로컬로 관리합니다.

시작하기 전에
키를 사용하는 암호화 모듈은 를 사용하기 키 교환전에 대상 인스턴스와 소스 인스턴스 모두에서 작성해야 합니다.

필요한 역할: sn_kmf.cryptographic_manager

이 태스크 정보
키 교환 요청은 대상 인스턴스에서 시작됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자동 키 교환은 인스턴스를 복제할 때 기본적으로 활성화되며, 이 경우 속성이 대상 인스턴스에 복제됩니다. 와 함께 KMF시스템 속성을 구성하여 인스턴스 클론 중 키가 처리되는 방식을 관리합니다.

- 자동 키 교환 끄기: 반복되는 *glide_encryption.auto_key_exchange.enabled* 클론 요청에 대해 속성을 아니오 로 설정합니다.
- 자동 키 교환 요청 보내기: 이 속성을 **true**로 설정합니다.

중요사항: 기본 시스템 속성은 기본적으로 **true** 로 설정되어 있으며, 이는 인스턴스를 복제할 때 자동 키 교환이 활성화됨을 의미합니다. 반복 키 교환 기능을 사용하는 키 교환을 사용하여 암호 텍스트 키 재입력 경우 이 값을 **false**로 설정해야 합니다. 자세한 내용은 Recurring Key Exchange 검토 과정 문서를 참조하십시오.

프로시저

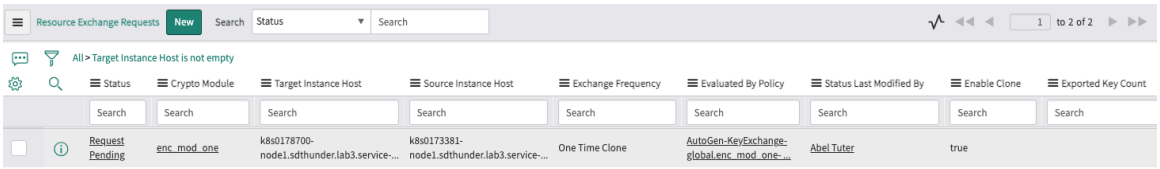
1. 다음으로 이동 모두 > 주요 운영 > 자원 교환 요청 > 신규.
2. 양식의 필드에 내용을 입력합니다.

자원 교환 요청 양식 필드

이름	설명
Exchange 빈도	◦ 임시: 키 대상 인스턴스에서 소스 인스턴스로 요청을 보냅니다. 소스에 대한 인스턴스 sys_id 및 호스트 정보를 입력합니다. 키 교환 키 다시 입력은 지원되지 않습니다. ◦ 일회성 클론: 소스 암호화 사양에서 대상 인스턴스로 키를 일회성 교환합니다. ◦ 반복 클론: 선택한 소스 암호화 사양의 키를 정의된 반복 클론의 대상 인스턴스로 교환합니다.
<Source or Target> 인스턴스 sys_id	◦ 임시: 키를 요청할 소스 인스턴스의 sys_id 입력합니다. ◦ 일회성 클론, 반복 클론: 요청을 보내는 대상 인스턴스의 sys_id 입력합니다. 팁: 애플리케이션 네비게이터에 `stats.do` 입력하여 인스턴스 ID를 찾습니다.
<Source or Target> 인스턴스 호스트	소스 또는 대상 인스턴스의 호스트 위치 또는 이름을 입력합니다. 팁: 예를 들면 `### #### instanceA.service-now.com`
암호화 사양	암호화 모듈에 있는 암호화 스펙의 키는 복제할 키를 정의합니다. 일회성 및 반복 클론 요청 모두에 대해 인스턴스가 자동으로 자원 교환 모듈 액세스 정책을 생성합니다. 정책을 수동으로 구성할 필요가 없습니다. 주: 목록을 사용하여 조회 아이콘(목록을)을 선택하여 사용 가능한 암호화 사양을 찾아봅니다.
키를 임포트한 후 키 입력 다시 입력 활성화	자동 키 재입력을 활성화하는 옵션입니다.

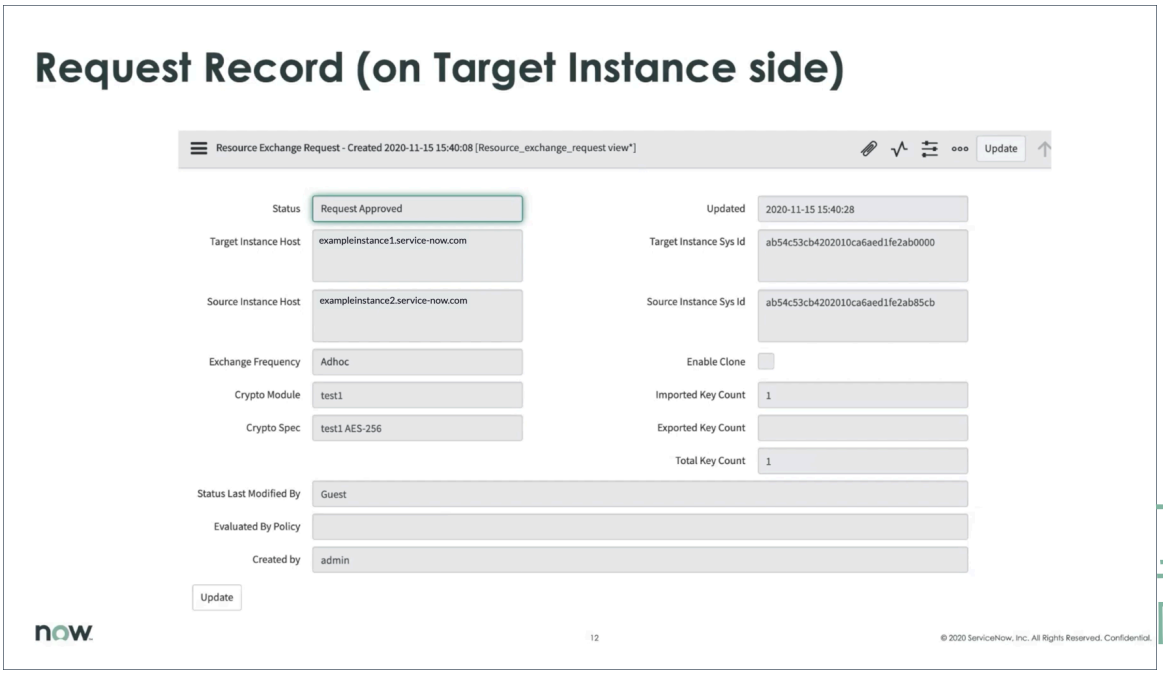
3. 제출을 선택합니다.
성공하면 양식 상단에 확인 메시지가 표시됩니다. 요청 테이블이 소스 인스턴스와 대상 인스턴스 모두에서 요청 보류 중 항목으로 업데이트됩니다. 요청 기록을 열어 대상 또는 소스 호스트에서 요청 상태, 임포트한 키 수 및 총 키 수를 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 보류 중인 요청이 소스 인스턴스에서 수락되어 교환을 완료합니다.

   클론 시 소스 인스턴스의 모듈 액세스 정책이 호출되어 요청을 자동 승인하고 새로 클론된 대상에 키를 보냅니다.



결과
키 교환을 시도한 후에는 비프로덕션 인스턴스가 시스템 속성을 업데이트합니다 *protected.script.values.kmf.rekeyed*. 이 속성은 키 교환이 시도된 후 시스템 속성 [sys_properties] 테이블에 표시됩니다. 교환된 키를 사용한 암호화에 성공하면 이 속성 값은 **true**입니다. 그렇지 않은 경우 속성 값은 **false**입니다. 값이 false이면 인스턴스는 다음 날 다시 암호화를 시도합니다.

키 교환을 사용하여 암호 텍스트 키 재입력

자원 교환 는 소스의 키로 암호화된 대상 인스턴스에서 암호 텍스트의 키 재입력을 지원합니다. 키 다시 입력 작업은 키 수명주기에서 추적됩니다.

개요

를 사용하는 KMF 관리자는 데이터 필드 암호화 복제를 수행할 때 프로덕션 인스턴스 간에 암호화 키의 키를 다시 입력하는 데 사용할 키 교환 수 있습니다. 키를 다시 입력하려면 활성 키가 필요하므로 먼저 대상 인스턴스에서 활성 키를 사용할 수 있어야 합니다. 암호화 작업은 시스템에서 자동으로 생성되고 실행되어 소스 키를 회전하고 키를 다시 입력하고 암호 텍스트를 다시 암호화합니다.

다음을 수행하는 데 사용합니다 키 교환 .

- 키를 다시 입력할 만료 시간 프레임을 설정합니다.

  요청이 만료된 경우 요청이 거부되고 키가 삭제됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 소스 인스턴스의 키로 암호화된 암호 텍스트 키 입력을 자동화합니다.

  새 복제된 암호화 키는 대상 인스턴스에서 암호 텍스트를 다시 암호화하는 데 사용됩니다.

- 키 다시 입력 목적은 복제 프로세스 중에 설정되며 클론의 일부로 자동화됩니다.
- 키 재입력 활동은 암호화 모듈의 **Modules** Key(모듈 키) 탭에서 추적됩니다. 키 활동의 키 수명주기 상태와 키 버전에 액세스합니다. 자세한 내용은 키 회전 문서를 참조하십시오.

를 키 교환 구성하고 활성화를 위해 키를 임포트한 후 키 다시 입력 사용 확인란을 선택합니다. 자세한 내용은 키 교환 구성 문서를 참조하십시오.



Recurring Key Exchange 검토 과정

이 연습에서는 및 를 사용하여 인스턴스에서 반복되는 키 교환을 자원 교환설정합니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager

이 태스크 정보

이 예시에서는 대상 인스턴스가 호스트 인스턴스에서 키를 요청하는 방법을 보여줍니다.

- 이 절차를 수행하려면 먼저 인스턴스를 복제해야 합니다. 자세한 내용은 시스템 클론 을 참조하십시오.
- 자동 키 교환: 기본 시스템 속성은 *glide_encryption.auto_key_exchange.enabled* 기본적으로 **true** 이며, 이는 인스턴스를 복제할 때 자동이 활성화됨을 의미합니다. 속성이 대상 인스턴스로 복제됩니다.
- 속성을 **false**로 설정하여 자동을 해제합니다.

프로시저

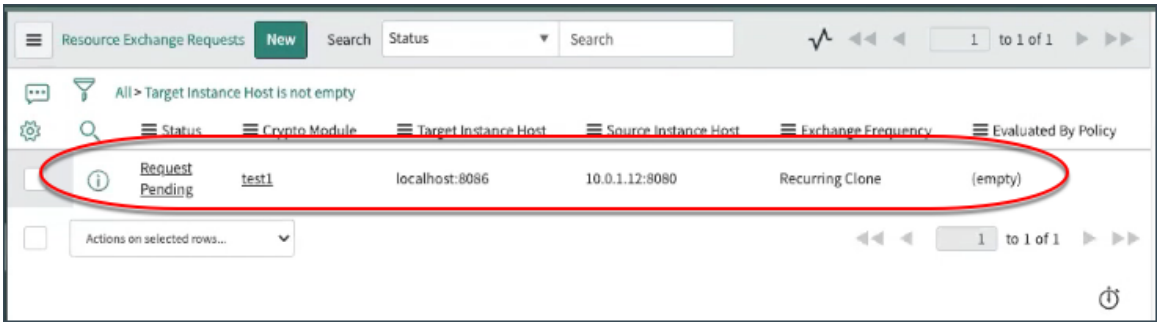
1. 소스 인스턴스에서 암호화 모듈을 생성하거나 column_level_encryption 사용하여 기존 암호화 모듈에 액세스하고 에 대한 키 교환암호 텍스트 암호화에 대한 암호화된 필드 구성을 설정합니다. 자세한 내용은 을 참조하십시오.

   a. 암호화 모듈에서 키가 생성되었는지 확인하십시오.

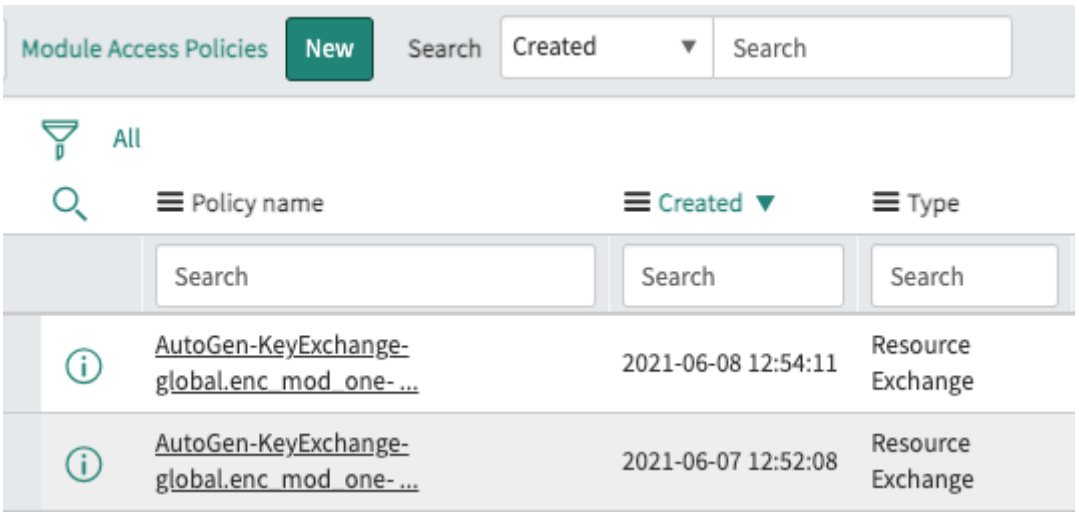
   주: 인스턴스는 클론 요청 실행 시 모듈 액세스 정책을 자동으로 생성합니다.

2. 복제된 인스턴스에서 다음으로 이동합니다. 주요 운영 > 자원 교환 요청 > 신규.
3. 양식을 완성하고 Exchange 빈도로 반복 클론 을 선택합니다.
4. 클론의 대상 인스턴스에서 다음으로 이동합니다. 주요 운영 > 자원 교환 요청.
   호스트 인스턴스의 요청이 테이블에 표시됩니다.

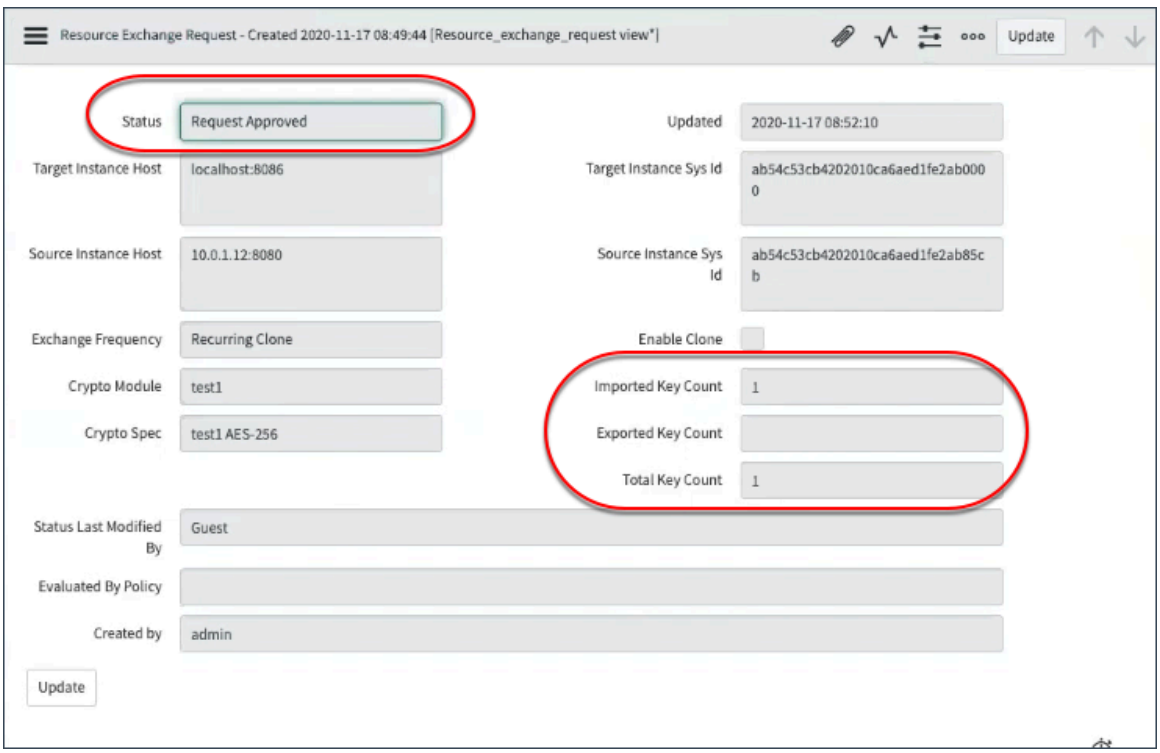
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



중요사항: 일회성 클론 요청과 반복 클론 요청 모두에 대해 인스턴스는 모듈 액세스 정책을 자동으로 생성합니다. 정책을 수동으로 구성할 필요가 없습니다. 클론 시 소스 인스턴스의 이 정책이 호출되어 요청을 자동 승인하고 새로 클론된 대상에 키를 보냅니다.



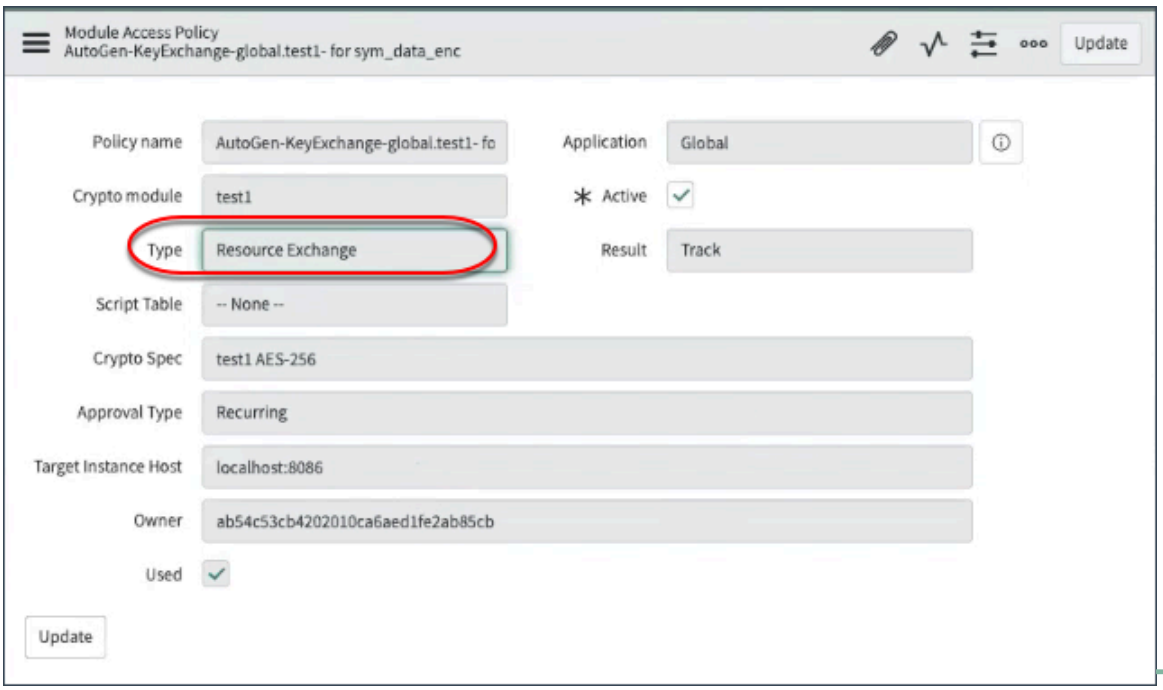
요청 양식에서 상태가 요청 승인됨 으로 업데이트되고 임포트한 키 카운트 필드가 기록에 나타납니다.



기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 호스트 인스턴스로 돌아갑니다.
6. 요청 기록을 보고 익스포트된 키 수를 확인합니다.
7. 모듈 액세스 정책 기록을 보고 유형이자원 교환.



주: 자원 교환 는 대상 인스턴스에서 암호문 키 재입력도 지원합니다. 자세한 내용은 다음을 참조하십시오.

결과
키 교환을 시도한 후에는 비프로덕션 인스턴스가 시스템 속성을 업데이트합니다 *protected.script.values.kmf.rekeyed*. 이 속성은 시스템 속성 [sys_properties] 테이블에 표시됩니다. 교환된 키를 사용한 암호화에 성공하면 이 속성 값은 **true**입니다. 그렇지 않은 경우 속성 값은 **false**입니다. 값이 false이면 인스턴스가 다음 날 다시 암호화를 시도합니다.

인프라 보안

인프라 보안 도구를 사용하여 인스턴스에서 클라이언트-서버로의 트래픽을 암호화하는 데 사용하는 인증서를 생성, 업로드 및 관리합니다.

인프라 보안 플러그인은 TLS(전송 계층 보안) 암호 및 인증서를 관리하는 데 사용할 수 있는 도구를 제공합니다. 인스턴스는 TLS를 사용하여 클라이언트에서 서버로의 트래픽을 암호화합니다.

인스턴스에 사용되는 암호 선택

TLS 페이지를 사용하여 관리자는 인스턴스에 사용할 데이터센터 암호를 구성하고 암호를 시도할 순서를 선택할 수 있습니다.

나만의 인증서 작성 및 업로드

인프라 보안 도구를 사용하여 선택한 인증 기관에서 서명할 수 있는 고유한 인증서 서명 요청을 생성합니다. 그런 다음 도구를 사용하여 서명된 인증서를 인스턴스의 로드 밸런서에 업로드할 수 있습니다.

암호 및 인증서의 상태 모니터링

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

TLS 설정 및 **SYOC** 설정 페이지를 사용하여 암호 및 인증서에 대한 변경 상태를 확인합니다.

인프라 보안 플러그인 설치

ServiceNow 이러한 기능 사용을 시작하려면 인프라 보안 설정(com.glide.infrastructure_security) 플러그인을 설치합니다. 플러그인 활성화에 대한 자세한 내용은 플러그인 활성화를 참조하십시오.

플러그인을 설치한 후 시스템 속성을 `true`로 설정하여 *`sn_infra_sec.syoc.enabled`* SYOC(보안 서명) 기능을 활성화합니다.

주: *`sn_infra_sec.syoc.enabled`*인스턴스에서 속성을 사용할 수 없는 경우 직접 생성해야 합니다. 이 프로세스에 대한 자세한 내용은 시스템 속성 추가 문서를 참조하십시오.

인증서 서명 요청 생성

Generate Certificate Signing (CSR)(인증서 서명(CSR) 생성) 페이지를 사용하여 인스턴스 부하 분산 장치에 대한 고객 서명 인증서를 지원하는 인증서 서명 요청을 생성합니다.

시작하기 전에

필요한 역할: 관리자

이러한 단계를 수행하려면 인프라 보안(com.glide.infrastructure_security) 플러그인을 설치해야 합니다. 이 플러그인에 대한 자세한 내용은 다음을 참조하십시오인프라 보안 .

와 함께 사용자 지정 URL을 ServiceNow사용하는 방법에 대한 자세한 내용은 문서를 참조하십시오 사용자 지정 URL을 인스턴스 URL로 설정.

프로시저

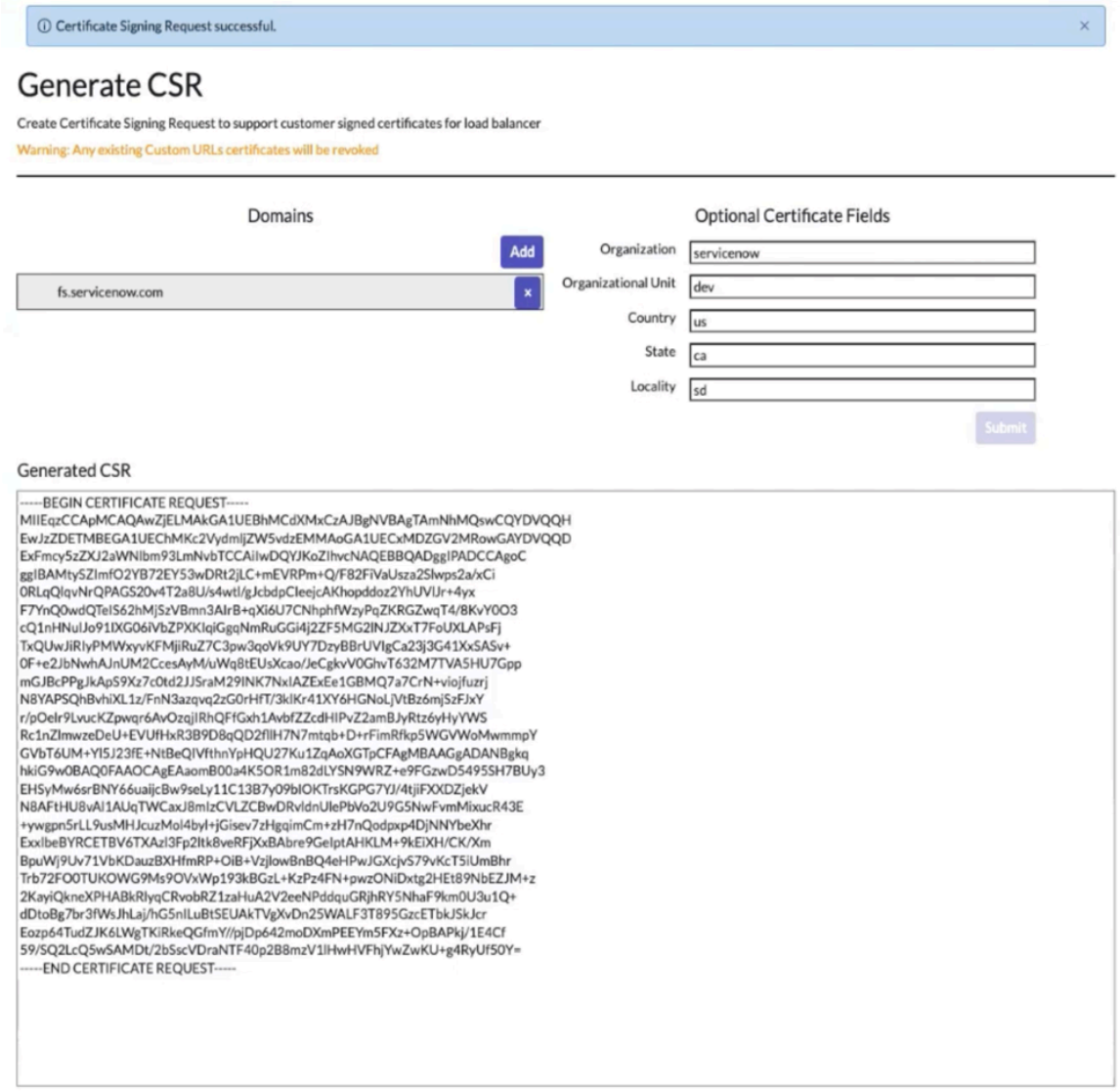
1. 다음으로 이동 모두 > 인프라 보안 설정 > **CSR** 작성.
2. 요청에 하나 이상의 도메인을 추가합니다.
   a. 도메인 제목 아래에서 추가 단추를 선택합니다.
   b. 팝업 창에서 도메인을 입력하고 확인을 선택합니다.
   c. 도메인에 더 추가하려면 필요한 만큼 이 단계를 반복합니다.

      주: 각 도메인 항목의 왼쪽에 있는 X 버튼을 선택하여 도메인을 제거할 수 있습니다.
3. 옵션 인증서 필드에 요청에 포함할 정보를 입력합니다.
4. 제출을 선택합니다.

   경고: 다른 요청이 생성되는 동안에는 요청을 제출할 수 없습니다. 이 문제가 발생하면 "충돌하는 리소스" 오류가 표시됩니다. 처리하려면 현재 요청을 취소하거나 현재 요청이 처리될 때까지 기다렸다가 다른 요청을 제출하십시오.

   제출을 선택하면 인스턴스가 인증서 서명 요청을 생성합니다. 생성된 **CSR** 필드에 요청이 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 생성된 **CSR** 필드의 내용을 복사합니다.

Key Management Framework (KMF)를 사용한 **Password2** 암호화

에서 핵심 관리 프레임워크지원하는 (양방향 암호화) 필드 유형을 사용하여 Password2 업무, 키 보호 및 수명 주기 관리의 분리로 사용자 지정 필드를 암호화하고 해독합니다. NIST 800-57 지침에 따라 작동하며 FIPS 140-2-L3 보호를 제공합니다.

Password2 는 양방향 암호화를 사용하여 암호를 저장하는 텍스트 필드입니다. 양방향 암호화는 비밀번호를 인스턴스 내에서 해독할 수 있는 안전한 암호화 값으로 저장합니다.

팁: 릴리스부터 Vancouver 관리자는 password2 필드에서 3DES 암호화를 폐지하고 새로운 AES(Advanced Encryption Standard)를 사용할 수 있습니다. 자세한 내용은 password2 필드에 대한 3DES의 GlideEncrypter 사용 중단 문서를 참조하십시오.

활성화

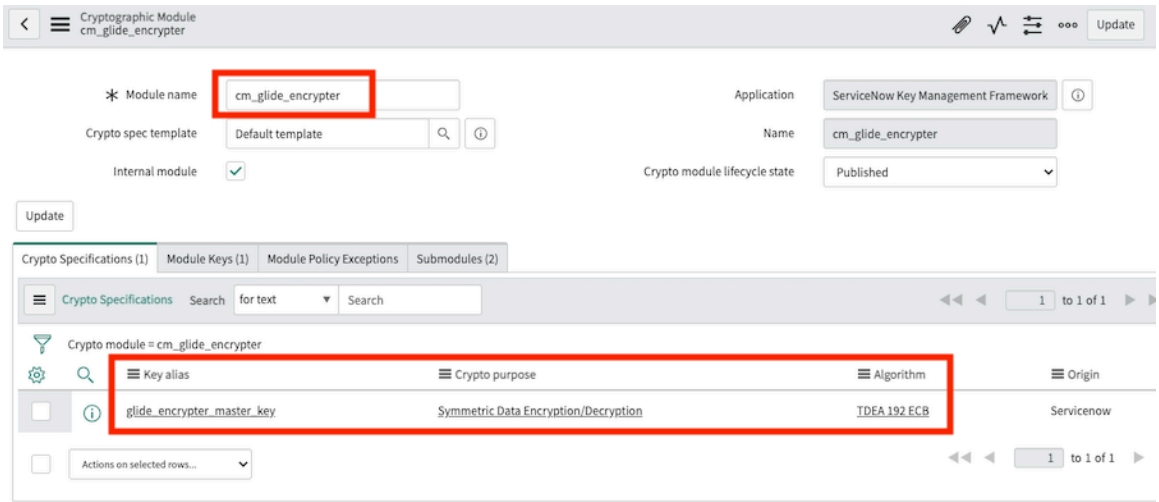
Password2 기능은 기본적으로 활성화됩니다. 이는 모든 새 인스턴스와 업그레이드에 *glide.kmf.encrypter.enabled* 대해 **true** 로 설정된 속성에 의해 제어됩니다. 를 사용하도록 Password2설정할 필드 암호화 엔터프라이즈 필요가 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Password2 작동 방식

핵심 관리 프레임워크 기본 시스템 상위 암호화 모듈 **cm_glide_encrypter** 제공합니다. 이 모듈은 암호화 사양과 레거시 Password2 필드를 해독할 수 있는 키를 제공합니다.

용 암호화 모듈 **Password2**



이 cm_glide_encrypter 모듈에는 각각 고유한 모듈 키와 사양이 있는 하위 모듈이 있을 수 있습니다. 필드가 있는 Password2 애플리케이션과 동일한 애플리케이션 범위와 함께 서브모듈이 존재하는 경우, 시스템은 서브모듈을 사용합니다. 예를 들어, 애플리케이션의 테이블에 ServiceNow® 고객 서비스 서브모듈이 있고 애플리케이션 범위에 있는 고객 서비스 테이블의 필드에 정보를 Password2 쓰는 경우, 암호화 프로세스는 서브모듈을 호출합니다고객 서비스. 또한 이 프로세스는 고유한 AES 256 GCM 암호화 키를 사용하여 암호화 및 암호 해독을 위해 해당 하위 모듈의 키를 사용합니다. 애플리케이션 범위당 하나의 서브모듈이 허용됩니다. 부모 모듈이 항상 전역 범위에 사용되는 것은 아닙니다. 일반적으로 새 필드는 instance_level_glide_encrypter 사용합니다.

주: 에서 Yokohama자체 하위 모듈을 생성할 수 없습니다. 하위 모듈은 의 Now Platform다양한 애플리케이션 플러그인에 제공됩니다. 하위 모듈에서는 키를 회전할 수 있지만 상위 cm_glide_encrypter 모듈에서는 회전할 수 없습니다.

도메인 분리 및 온 프레미스 고객

KMF Password2 은 도메인 분리를 지원하지 않습니다. 온프레미스 인스턴스와 함께 사용할 Password2 수 있습니다.

레거시 Password2 및 현재 Password2

에서 Yokohama기존 Password2 필드가 업그레이드되었습니다.

의 Password2현재 구현:

- 핵심 관리 프레임워크NIST 800-57 키 래핑 지침에 따라 사용하고 전체 키 계층 구조에 대해 FIPS 140-2-L3 보호를 제공합니다.
- 특정 애플리케이션을 위한 고유한 전용 KMF Password2 하위 모듈을 생성하는 기능이 포함되어 있어 애플리케이션 범위를 통해 통제를 제공합니다. 각 서브모듈에는 고유한 AES 256 GCM 암호화 키가 있습니다.

스크립트의 Password2 필드

스크립트를 사용하여 필드에 액세스할 Password2 때는 테이블 범위와 동일한 범위에서 스크립트를 실행합니다. `setDisplayValue()`를 사용하여 값을 암호화 Password2 하고 `getDecryptedValue()`를 사용하여 값을 해독하고 읽습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 필드에 `GlideEncrypter()` API Password2 를 사용하지 마십시오.

이 예시 스크립트는 테이블 'table_xyz'의 password2 열에서 `my@Password` 암호화하는 방법을 보여줍니다.

```
var  gr =  new GlideRecord('table_xyz');
gr.setDisplayValue('pwd2column_name', 'my@Password');
gr.insert();
```

중요사항: 필드에 `setValue()` API를 Password2 사용할 수 없습니다.

이 예시 스크립트는 값을 검색하기 위해 동일한 필드의 암호를 해독하는 방법을 보여줍니다.

```
var  gr =  new GlideRecord('table_xyz');
gr.query();
gr.next();
var ge=gr.getElement('pwd2column_name');
var ged1 = ge.getDecryptedValue();
```

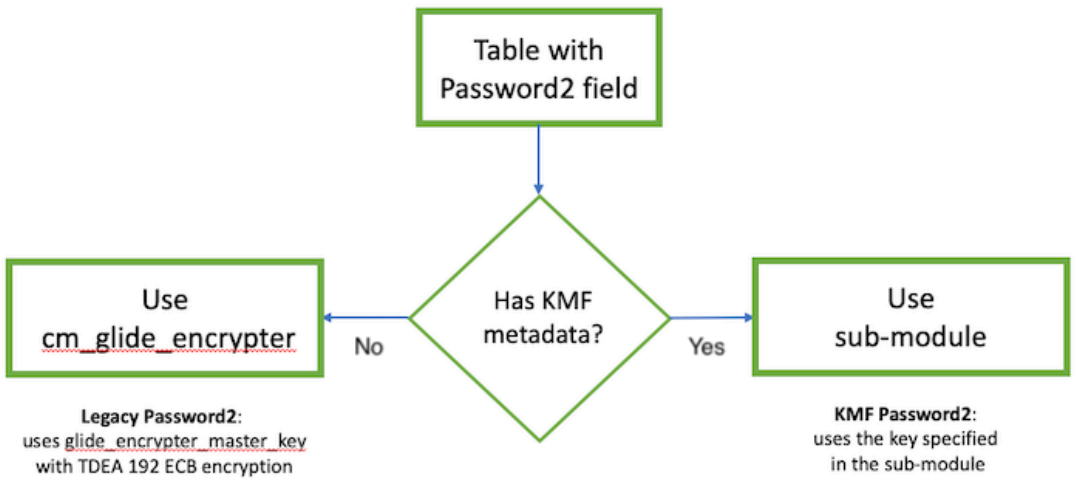
중요사항: `getDecryptedValue()` API는 범위가 지정되지 않습니다. 전 세계에서 사용할 수 있습니다.

1. 필드의 데이터를 Password2 암호화하면 시스템이 필드가 있는 애플리케이션의 Password2 범위를 결정합니다.
2. 그런 다음 시스템은 속성이 로 설정된 *true*경우 애플리케이션과 동일한 범위를 가진 **cm_glide_encrypter** 상위 모듈의 하위 모듈을 찾습니다.

   주: 같은 스코프를 가진 서브 모듈이 있으면, 서브 모듈 스펙과 키를 사용하여 암호화를 수행합니다.

이 그림은 인스턴스가 필드의 데이터를 Password2 해독하는 방법을 설명합니다.

Password2 암호 해독 플로우



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

KMF Password2 마이그레이션 작업

이전 릴리스에서 업그레이드하는 고객을 위해 마이그레이션 작업이 제공됩니다. 레거시 Password2 암호화로 암호화된 데이터를 서브모듈 키의 키 KMF Password2 로 다시 암호화합니다. 다시 암호화는 애플리케이션 범위에 필드가 있고 Password2 해당 범위에 대해 생성된 하위 모듈이 있는 테이블에만 적용됩니다. 예를 들어, **XYZ_example** 애플리케이션의 레거시 Password2 필드(**XYZ_example** 애플리케이션 범위 포함)는 **XYZ_example** 애플리케이션 범위에 대한 하위 모듈이 cm_glide_encrypter 상위 모듈 아래에 있는 경우에만 다시 암호화됩니다.

KMF Password2 서브모듈의 암호화 키는 키 계층 구조에서 KMF 보호됩니다(봉투 암호화).

인증서

인스턴스에는 보안 연결을 설정하고 서명의 유효성을 검사하는 인증서가 필요합니다.

탐색	구성
	
인증서의 주요 기능 및 비즈니스 가치에 대해 알아봅니다.	코어 구성을 계획합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

업로드 	
애플리케이션을 계획하고 설정합니다.	

인증서 탐색

인스턴스에는 보안 연결을 설정하고 서명의 유효성을 검사하는 인증서가 필요합니다.

인증서는 다음과 같은 기능에 사용됩니다.

- LDAPS
- 아웃바운드 웹 서비스 상호 인증
- 웹 서비스 보안
- MID 서버

인증서를 사용하려면 보안 서버 또는 클라이언트에 대한 인증서를 생성하거나 구매하여 인스턴스에 업로드해야 합니다.

LDAP 인증서

인스턴스가 LDAP 서버와의 LDAPS 프로토콜(LDAP over SSL) 연결을 설정하려면 SSL 인증서가 필요합니다.

인스턴스는 다음 두 가지 유형의 LDAP 인증서를 허용합니다.

인증서	유형	필수 대상
LDAP 서버 인증서	지원되는 모든 유형	모든 LDAP 구성
LDAP 클라이언트 인증서	Java 키 저장소 유형	상호 인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

서버 인증서가 여러 개 있는 경우 LDAP 서버가 연결을 허용할 때까지 인스턴스가 각 서버 인증서를 차례로 시도합니다. 여러 LDAP 서버를 사용하는 경우 각 LDAP 서버에 대한 SSL 인증서를 포함해야 합니다.

상호 인증을 사용하려면 클라이언트가 서버 외에 인증서를 제공해야 합니다. LDAP 서버에 상호 인증이 필요한 경우 Java 키 저장소 유형 인증서에 LDAP 서버의 클라이언트 인증서도 제공해야 합니다.

인증서 기준

유효한 인증서는 다음 기준을 충족해야 합니다.

- 인증서의 키 크기는 최대 2048비트일 수 있습니다.
- 인증서의 파일 확장명은 다음 중 하나여야 합니다.

확장명	설명
DER	고유 인코딩 규칙 형식은 이진 메시지 전송 구문입니다. 이 형식은 . CER 및 . CRT 파일 확장명입니다.
CER	고유 인코딩 규칙 형식을 사용하는 인증서에 대한 인증서 파일 확장명입니다.
CRT (영어)	고유 인코딩 규칙 형식을 사용하는 인증서에 대한 인증서 파일 확장명입니다.
PEM	Privacy Enhanced Mail 형식은 "-----BEGIN CERTIFICATE-----" 및 "-----END DIRECTORY-----" 텍스트 문자열 사이에 포함된 base-64 인코딩 DER 인증서입니다.

인증서 신뢰

기본적으로 인스턴스는 JVM(Java Virtual Machine)에서 인식하는 CA(인증 기관)의 인증서만 신뢰합니다. 자체 서명 및 엔터프라이즈 서명 인증서는 신뢰할 수 없습니다.

주: 인증서 사용에 영향을 미치는 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 커뮤니케이션 .

LDAP 클라이언트 인증서 생성

OpenSSL을 사용하여 상호 인증을 위한 LDAP 클라이언트 인증서를 생성합니다. 최종 출력은 Java 키 저장소 내에 저장된 PKCS#12 인증서입니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
인증서 생성에 대한 자세한 내용은 OpenSSL 설명서를 참조하십시오. 이 단계에서는 OpenSSL에 액세스할 수 있다고 가정합니다.

명령줄 인터페이스에 다음 명령을 입력합니다.

프로시저

1. 자체 서명된 클라이언트 인증서를 생성합니다.

Example
예를 들어, 이 명령은 test1-key.key 개인 키를 기반으로 클라이언트 인증서 test1-cert.crt를 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
 test1-key.key -out test1-cert.crt
```

2. 인증서 파일과 개인 키를 모두 PKCS#12(확장명이 .pfx 또는 .p12인 파일)로 변환합니다.

   Example
   예를 들어 이 명령은 클라이언트 인증서와 개인 키를 test1-certificate.pfx라는 PKCS#12 인증서로 변환합니다.

```
openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key
 -in test1-cert.crt
```

3. Java 키 스토어를 생성하고 pkcs12 파일을 가져옵니다.

   Example
   예를 들어, 이 명령은 인증서를 test1.jks Java 키 저장소로 가져옵니다.

```
keytool -importkeystore -srckeystore test1-certificate.pfx
 -srcstoretype PKCS12 -destkeystore test1.jks
```

4. 키 스토어 파일(`test1.jks`)의 인증서를 인스턴스에 업로드합니다.

   주:

   확장명이 .jks인 인증서를 사용하여 온프레미스 인스턴스에 업로드할 때 "애플리케이션 업로드를 처리할 유효한 인증서를 찾을 수 없습니다"라는 오류 메시지가 표시되는 경우 확장명이 .pfx인 인증서를 대신 사용합니다.

다음에 수행할 작업
인스턴스에 인증서 업로드

서버 인증서 생성

keytool을 사용하여 새 Java 키 저장소 파일을 생성하고, CSR(인증서 서명 요청)을 만들고, 개인 키, 공개 인증서 쌍 및 서명된 인증서를 키 저장소로 가져올 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
키 및 CSR 생성에 대한 자세한 내용은 Java keytool 설명서를 참조하십시오.

명령줄 인터페이스에 다음 명령을 입력합니다.

프로시저

1. Java 키 스토어와 키 페어를 생성합니다.

   Example
   예를 들어, 이 명령은 my.keystore라는 키 저장소를 만들고 키 저장소 내에 mydomain이라는 개인 키를 생성합니다.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. 기존 Java 키 스토어에 대한 CSR을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example
예를 들어, 이 명령은 mydomain.csr 또는 mydomain 키라는 CSR을 생성합니다.

```
keytool -certreq -alias mydomain -keystore my.keystore -file
 mydomain.csr
```

3. 루트 또는 중간 인증 기관(CA) 인증서를 Java 키 스토어로 임포트합니다.

Example
예를 들어 이 명령은 Thawte에 대한 CA 인증서를 가져옵니다. 이 명령은 Thwate가 CSR에 서명한 CA라고 가정합니다.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
 my.keystore
```

4. 서명된 기본 인증서를 Java 키 스토어로 임포트합니다.

Example
예를 들어, 이 명령은 서명된 인증서 mydomain.crt를 키 저장소로 임포트합니다.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt
 -keystore my.keystore
```

5. 키 스토어 파일(my.keystore)의 인증서를 인스턴스에 업로드합니다.

다음에 수행할 작업
인스턴스에 인증서 업로드

인스턴스에 인증서 업로드

인증서 모듈에서 인스턴스에 인증서를 추가합니다.

인스턴스에 인증서 업로드

인스턴스에 인증서를 업로드합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
ADFS 서버에서 인증서가 업데이트되면 업데이트된 인증서도 인스턴스에 업로드해야 합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 인증서.
2. 새로 만들기를 선택합니다.
3. 양식의 필드에 내용을 입력합니다.

필드	설명
이름	인증서의 고유 이름을 지정합니다.
만료 알림	(선택사항) 인증서가 만료되기 직전에 알림을 보낼지 여부를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	인스턴스가 보안 통신 및 서명 요청에 이 인증서를 사용할지 여부를 선택합니다.
간단한 설명	〔선택사항〕 요청자 또는 서버 이름과 같은 인증서에 대한 텍스트 설명을 입력합니다.
형식	인증서 형식을 선택합니다. 인스턴스는 PEM 및 DER 형식을 지원합니다.
유형	인증서 컨테이너를 선택합니다. 인스턴스는 신뢰 스토어, Java 키 스토어 및 PKCS#12 키 스토어의 인증서를 인식합니다.
PEM 인증서	DER 인증서가 포함된 base-64 인코딩 PEM 형식 텍스트를 입력합니다. 인스턴스는 인증서를 디코딩하여 유효 기간(시작), 만료됨, 며칠 후 만료됨, 발급자 및 제목 필드를 채웁니다.

4. 제출을 선택합니다.

   업로드하는 동안 모듈은 다음 필드에 인증서의 읽기 전용 속성을 추출하여 표시합니다.

   - 유효 기간 시작일
   - 만료 날짜
   - 발급자
   - 인증서 주체

5. **Validate Stores**/Certificates(저장소/인증서 확인)를 선택하여 인증서가 올바른지 확인합니다. 인스턴스에 인증서 또는 키 스토어에 오류가 발생하면 오류 메시지가 표시됩니다.

신뢰할 수 있는 서버 인증서 업로드

서비스 제공자의 신뢰할 수 있는 서버 인증서를 업로드하여 인스턴스가 유효하고 안전한 서비스에 연결되도록 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
인스턴스는 서비스 제공자가 제공한 인증서를 사용하여 아웃바운드 웹 서비스 호출의 유효성을 검사합니다.

프로시저

1. 믿을 수 있는 스토어 인증서 유형으로 새 인증서 기록을 생성합니다.
2. 다음 작업 중 하나를 수행합니다.
   - 서비스 제공자의 DER 형식 인증서를 첨부합니다.
   - 서비스 제공자의 PEM 형식 인증서를 복사하여 **PEM** 인증서 필드에 붙여넣습니다.

필드 암호화

를 사용하여 필드 암호화권한이 없는 사용자, 스크립트 또는 시스템 프로세스로부터 인스턴스의 암호화된 데이터를 보호합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 암호화 는 에 기반한 ServiceNow 핵심 관리 프레임워크암호화 제품입니다. 필드 암호화 인스턴스 내의 특정 필드 또는 첨부 파일의 암호화를 허용합니다. 클라우드 암호화 및 ACL(접근 제어 목록)과 함께 사용하면 필드 암호화 볼 수 있는 권한이 없는 로그인한 사용자로부터 중요한 정보를 보호할 수 있습니다.

필드 암호화 에는 두 가지 버전이 있습니다.

필드 암호화 스타터

필드 암호화 Starter는 플랫폼에 무료로 포함되며 ServiceNow 제한된 수의 필드에 대한 암호화를 지원합니다.

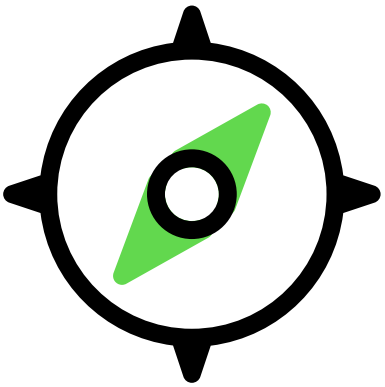
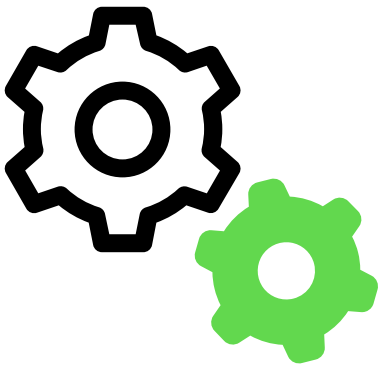
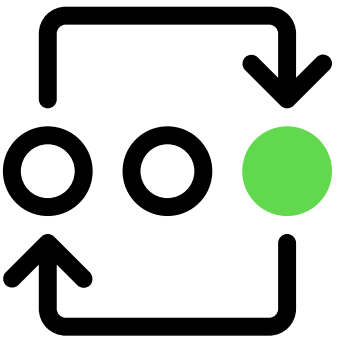
필드 암호화 기업

필드 암호화 Enterprise는 ServiceNow Vault, Platform Encryption 또는 필드 암호화 엔터프라이즈.

이러한 버전 간의 차이점에 대한 자세한 내용은 다음 문서를 참조하십시오 필드 암호화 탐색.

필드 암호화 이전 열 수준 암호화 릴리스에서 Xanadu 사용 가능한 제품을 대체합니다.

시작

탐색	구성	사용 .
		
의 Starter 및 Enterprise 버전의 필드 암호화이점에 대해 알아봅니다.	암호화 지원 열 수준 암호화또는 에서 마이그레이션을 활성화 및 구성하고 필드 암호화 엔터프라이즈관리하는 방법을 알아보십시오.	인스턴스에서 암호화된 데이터에 대한 접근을 관리하는 데 사용합니다 필드 암호화 .

유용한 리소스

유용한 정보를 제공할 수 있는 몇 가지 ServiceNow 리소스는 다음과 같습니다.

ServiceNow 커뮤니티

ServiceNow 커뮤니티

고객 성공 센터

Customer Success Center

개발자

developer.servicenow.com

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Impact

http://impact.servicenow.com

Now Learning

Now Learning

나우크리에이트

Now Create

파트너

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

ServiceNow

https://www.servicenow.com/

ServiceNow Store

https://store.servicenow.com/

지원

https://support.servicenow.com/now

알려진 오류 포털

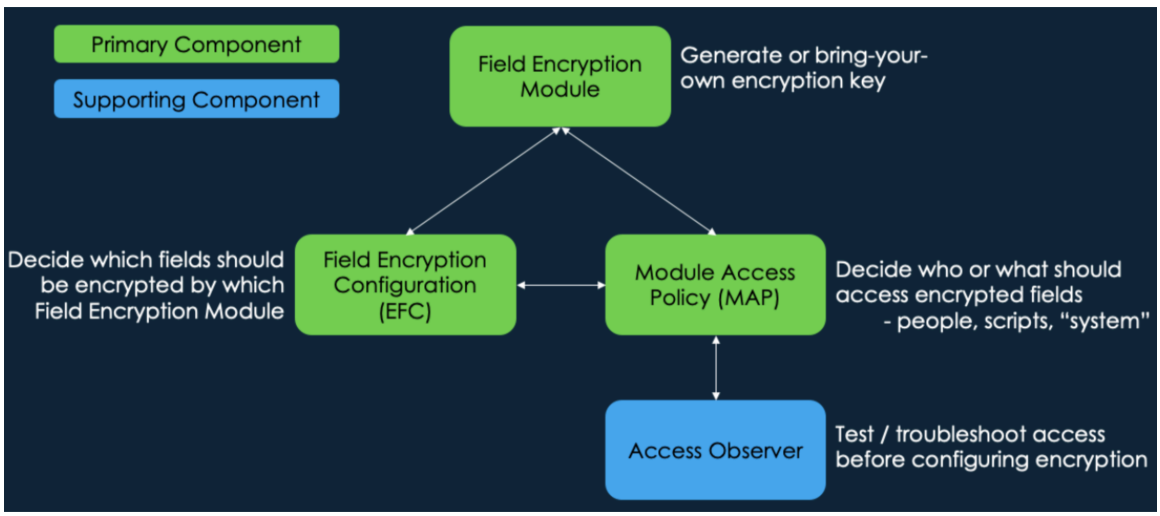
필드 암호화 탐색

Starter에 대한 필드 암호화 자세한 내용 알아보기 및 필드 암호화 엔터프라이즈

암호화 지원 액세스 제어

기본적으로 필드 암호화 모든 사용자, 스크립트 및 시스템 프로세스가 암호화된 데이터에 액세스하지 못하도록 차단합니다. 그러나 필드 암호화에는 접근 제어 목록(ACL)과 별도로 사용되지만 함께 사용되어 올바른 사용자, 스크립트 또는 시스템 프로세스만 암호화된 데이터에 액세스할 수 있도록 하는 접근 제어 기능이 있습니다.

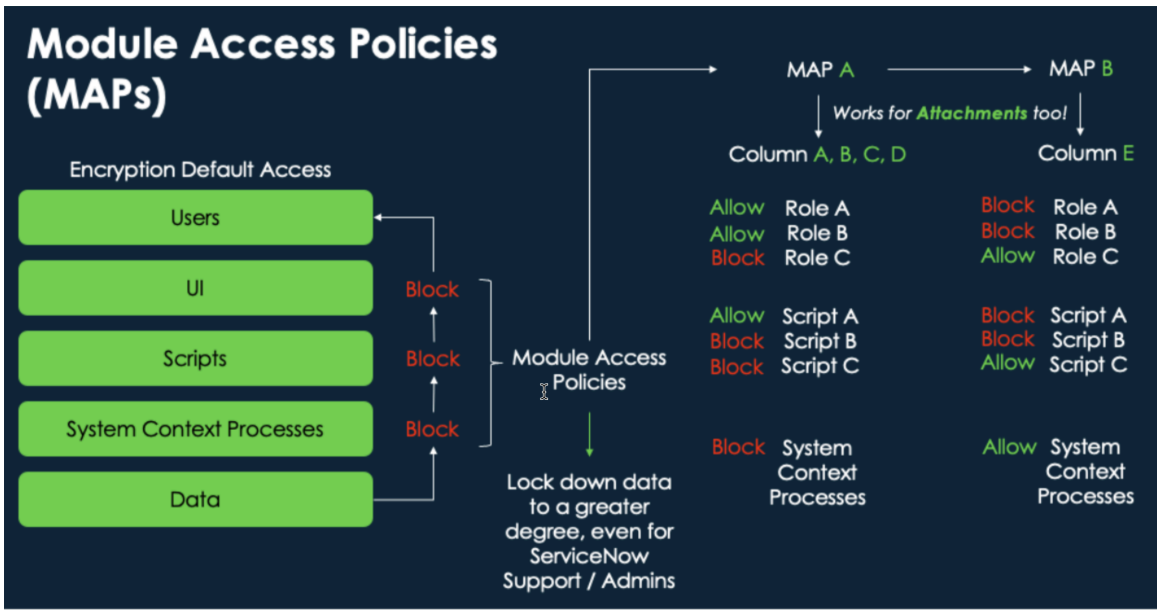
필드 암호화 모듈, 암호화된 필드 구성 및 모듈 액세스 정책의 조합을 통해 액세스 제어 기능을 구성할 필드 암호화수 있습니다. 다음 이미지는 이러한 세 가지 요소가 함께 작동하는 방식을 보여줍니다.



기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 액세스 정책(다음 이미지 참조)은 사용자, 스크립트 또는 시스템 프로세스가 암호화된 데이터에 액세스할 수 있는 권한을 부여하는 방법입니다(그러나 기본적으로 암호화된 데이터는 인스턴스의 모든 액세스에서 잠깁니다).



Starter와 Starter의 필드 암호화 차이점 필드 암호화 엔터프라이즈

기능 세트는 필드 암호화 Starter와 필드 암호화 엔터프라이즈.

기능	필드 암호화 스타터	필드 암호화 엔터프라이즈
암호화된 필드 수	최대 5개의 암호화된 필드	암호화된 필드 수에 대한 제한 없음
첨부 파일 암호화	아니요	예
키 관리	없음(키 회전에 대해서는 지원 서비스에 문의 ServiceNow)	Support의 ServiceNow 개입 없이 인스턴스에서 키 관리
지원되는 데이터 유형	지원되는 모든 데이터 유형	지원되는 모든 데이터 유형
필드 암호화 모듈 수	제한 없음	제한 없음
모듈 접근 정책 수	제한 없음	제한 없음

필드 암호화 사용자

사용자

사용자	설명
Key Management Framework (KMF)Admin 또는 KMF Cryptographic Manager	이러한 역할은 의 요소를 필드 암호화구성하는 데 사용됩니다. • 필드 암호화 모듈 및 모듈 키 • 암호화 사양 • 모듈 수명주기 정책 • 필드 및 첨부 파일에 대해 암호화된 필드 구성 • 모듈 접근 정책(MAP)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자

사용자	설명
	• 고객 공급 키 구성, 래핑 및 업로드 (의 경우 필드 암호화 엔터프라이즈) • 접근 관찰자를 구성하고 접근 관찰자 로그를 검토합니다. • 대량 암호화, 암호 해독 또는 키 다시 입력 예약
KMF 암호화 연산자	고객 공급 키의 속성 구성

다음으로 살펴볼 내용

필드 암호화 구성 및 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 필드 암호화 구성
- 필드 암호화 사용

필드 암호화 구성

암호화 지원을 활성화 및 구성하고 필드 암호화마이그레이션을 관리하는 방법을 알아봅니다.

필드 암호화 활성화
: 또는 필드 암호화 엔터프라이즈를 활성화하는 방법을 알아봅니다.

필드 암호화 구성에 필요한 역할
: 구성에 필드 암호화필요한 역할에 대해 알아봅니다.

암호화 지원에서 마이그레이션

예약된 작업을 사용하여 키와 암호화된 데이터를 레거시 암호화 지원 필드 암호화 엔터프라이즈에서 . 이 프로세스에 대한 자세한 내용은 다음을 참조하십시오. 다음으로 마이그레이션 중 필드 암호화 엔터프라이즈

첨부 파일 암호화 설정 변경

사용자가 암호화되지 않은 파일을 첨부하지 못하도록 하여 보안을 강화합니다. 자세한 내용은 단원을 참조하십시오사용자가 암호화되지 않은 파일을 첨부하지 못하도록 방지.

필드 암호화 활성화

필드 암호화 Starter 또는필드 암호화 엔터프라이즈

시작하기 전에
필요한 역할: 관리자

ServiceNow이(가Yokohama) 릴리스에서 beginning으로 필드 암호화 대체 열 수준 암호화 되었습니다.

Yokohama 릴리스에서 이전에 사용하지 열 수준 암호화 않은 고객은 스타터 또는 필드 암호화 엔터프라이즈 새 권리 구조를 사용할 필드 암호화 수 있습니다.

이전 릴리스에서 사용 열 수준 암호화 하던 고객이 를 사용하기 필드 암호화시작하려는 경우 다음과 같은 옵션이 제공됩니다.

필드 암호화 스타터

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

열 수준 암호화 Starter 고객은 다시 구현할 필요 없이 Starter를 설치할 필드 암호화 수 있습니다. 필드 암호화 Starter는 기존 구성을 인계받고 새로운 기능을 원활하게 추가합니다.

> ⚠ **경고:** Starter와 필드 암호화 Starter 간에 열 수준 암호화 권리에 차이가 있습니다. Starter를 설치하기 필드 암호화 전에 구성이 권리를 준수하는지 확인하십시오. Starter의 권리에 대한 필드 암호화 자세한 내용은 문서를 참조하십시오 필드 암호화 탐색.

필드 암호화 엔터프라이즈

열 수준 암호화 기업 고객은 계정 팀과 협력하여 에 대한 필드 암호화 엔터프라이즈올바른 권리가 있는지 확인해야 합니다. 이 경우 필드 암호화 엔터프라이즈 인스턴스에 플러그인을 설치할 수 있습니다.

> ℹ **중요사항:** 열 수준 암호화 Enterprise는 다른 대체 제품이므로 에 대한 필드 암호화 엔터프라이즈권리를 자동으로 부여하지 않습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 플러그인
2. 라이센스가 부여된 애플리케이션 및 플러그인 검색에서 `## ####` 검색합니다.
   검색에 플러그인이 표시되어야 합니다. 에 대한 필드 암호화 엔터프라이즈구독을 구매한 경우 이 플러그인을 사용할 수도 있습니다.

> ℹ **중요사항:** 활성화하려면 필드 암호화 엔터프라이즈먼저 구독을 구매해야 합니다. 고객 관리자는 일반적으로 며칠 이내에 조직의 프로덕션 및 비프로덕션 인스턴스에서 플러그인을 활성화하도록 준비할 수 있습니다.

3. 또는 필드 암호화 엔터프라이즈을 선택한 다음 설치를 선택합니다.

> ℹ **주:** 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

에 대한 역할 요구 사항 필드 암호화

구성에 필드 암호화필요한 역할에 대해 알아봅니다.

관리에는 다음 역할이 필요합니다. 는 를 핵심 관리 프레임워크기반으로 하므로 둘 다에 공통된 역할이 있습니다.

- 관리자
- 보안 관리자
- KMF 관리자
- KMF 암호화 관리자

역할에 대한 자세한 내용은 다음 문서를 참조하십시오 키 관리 프레임워크와 함께 설치되는 역할.

관리자 및 보안 관리자

보안 관리자 역할로 승격하려면 사용자에게 관리자 역할이 있어야 합니다. 암호화된 필드 구성 및 접근 관찰자 구성과 같은 높은 보안 작업을 수행하려면 보안 관리자 역할이 필요합니다.

관리자는 이 절차를 사용하여 보안 관리자로 승격할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 화면 오른쪽 상단의 프로필 사진에서 선택합니다.
2. 드롭다운 메뉴에서 역할 상승을 선택합니다.
3. 3. 보안 관리자를 선택합니다.
4. 저장을 선택합니다.

KMF 관리자

관리자 역할을 가진 사용자는 다음 프로세스를 사용하여 사용자를 KMF 관리자 역할에 할당할 수 있습니다.

1. 다음으로 이동 모두 > 시스템 보안 > 주요 운영 관리.
2. 사용 가능한 사용자 목록에서 KMF 관리자 역할이 필요한 사용자를 선택한 사용자 목록으로 이동합니다.
3. 저장을 선택합니다.

중요사항: 보안 문제를 방지하려면 둘 이상의 사용자에게 KMF 관리자 역할을 부여하지 마십시오. 보다 특수한 역할을 사용할 수 있는 경우 사용자에게 이 역할을 할당하지 마십시오.

KMF 암호화 관리자

KMF 암호화 관리자 역할의 사용자는 암호화 모듈 및 모듈 액세스 정책에 대한 작업을 만들고 업데이트할 수 있습니다. KMF 암호화 관리자는 키 관리 및 수명 주기 작업도 수행할 수 있습니다.

다음 프로세스를 사용하여 이 역할을 사용자에게 할당합니다.

1. 다음으로 이동 모두 > 시스템 보안 > 사용자.
2. 구성해야 필드 암호화하는 사용자를 선택합니다.
3. 역할 관련 목록에서 편집을 선택합니다.
4. `sn_kmf.cryptographic ####` 검색하고 선택한 사용자에게 역할을 추가합니다.
5. 저장을 선택합니다.

모듈 구성 필드 암호화

모듈 구성 필드 암호화 방법 알아보기

시작하기 전에

필요한 역할: KMF 관리자 또는 KMF 암호화 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 필드 암호화 모듈.
2. 새로 만들기를 선택합니다.
3. 모듈 양식에서 여기에 표시된 대로 필드를 작성합니다.

필드	값
모듈 이름	모듈의 이름을 선택합니다. 이 이름은 스크립트를 실행할 때 참조됩니다.
암호화 사양 템플릿	기본 템플릿으로 자동으로 채워집니다. 이 템플릿은 암호화 사양 및 권장 알고리즘에 대한 많은 암호화 목적의 매핑을 포함하는 암호화 모듈을 만드는 데 사용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	값
애플리케이션	이 모듈에 대한 애플리케이션 범위입니다. 이 필드는 자동으로 현재 애플리케이션으로 채워집니다.
이름	이 이름은 자동으로 생성됩니다. 다른 범위가 지정된 애플리케이션과의 충돌을 피하기 위해 애플리케이션 범위 이름이 앞에 추가된 모듈 이름입니다. 예를 들어 전역 애플리케이션 범위에서 `my_crypto_module` 라는 이름의 모듈을 만들면 이름은 `global.my_crypto_module`로 저장됩니다.
암호화 모듈 수명 주기 상태	"수명주기"라는 용어는 암호화 모듈의 생성, 사용 및 비활성화를 의미합니다. 구성 중에 처음에는 이 값을 초안 으로 설정합니다. 활성 사용을 위해 게시 됨으로 설정합니다. 주: 기본 템플릿은 게시됨으로 자동 설정됩니다.
상위 암호화 모듈	의 경우 필드 암호화이 값이 **column_level_encryption**로 설정되어 있는지 확인합니다.

4. 제출을 선택합니다.

다음에 수행할 작업

에서 에 대한 암호화 사양 필드 암호화암호화 키의 용도, 알고리즘, 키 길이, 모드 및 원본을 구성합니다.

에 대한 암호화 사양 필드 암호화

암호화 사양을 사용하여 암호화 키의 목적, 알고리즘, 키 길이, 모드 및 출처를 정의합니다.

시작하기 전에

필요한 역할: KMF 관리자 또는 KMF 암호화 관리자

이 태스크 정보

이 절차는 생성된 키를 구성하는 방법을 보여줍니다. 암호화 사양을 구성하면 데이터 암호화 키(모듈 키라고 함)가 자동으로 채워집니다.

고객 제공 키 구성은 다음 문서를 참조하십시오 에 대한 고객 공급 키 구성 필드 암호화 엔터프라이즈.

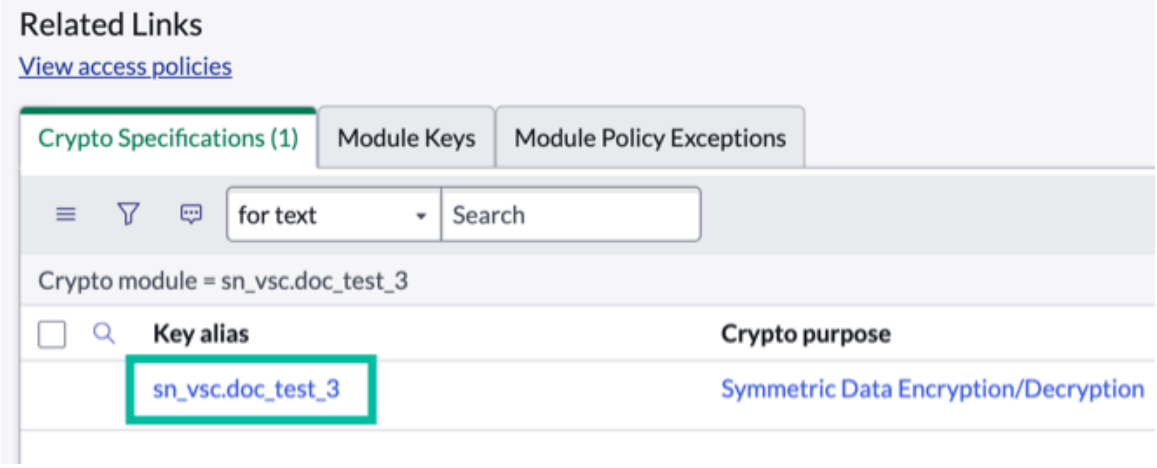
프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 필드 암호화 모듈.
2. 암호화 모듈 목록에서 구성하려는 모듈 기록을 엽니다.

   주: 목록에 표시되는 이름에는 범위가 추가됩니다(예: `global.[ ## ### ## ##]# ######`.

3. 암호화 사양 관련 목록에서 키 별칭 아래의 이름을 선택하여 암호화 특정 기록을 엽니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 암호화 사양 양식에서 필요에 따라 필드를 입력합니다.

주: 필드는 섹션으로 나뉩니다. 다음 또는 뒤로 버튼을 선택하여 섹션 사이를 이동합니다.

섹션	필드	설명
알고리즘 정의	암호화 모듈	선택한 암호화 모듈의 이름을 표시합니다.
	암호화 목적	선택한 알고리즘의 용도, 키, 길이 및 모드입니다. 의 경우 필드 암호화이 필드는 읽기 전용이며 대칭 데이터 암호화/암호 해독 값을 가집니다.
	알고리즘	암호화 목적을 달성하는 데 사용되는 알고리즘 유형을 선택합니다. 사용 가능한 옵션은 선택한 암호화 목적에 맞게 필터링됩니다.
수명주기 정의	적용 대상	수명 주기가 적용되는 선택한 키를 표시합니다.
	필드용	수명주기에 적용하려는 키의 제어 유형을 선택합니다. ◦ 만료 날짜 ◦ 추후 활성화 날짜 ◦ 추후 소멸 날짜 ◦ 추후 갱신 날짜 ◦ 추후 순환 날짜
	키 유형	
	수명주기 기본값	
	순서	암호화 사양의 키 수명 주기 상태를 처리하는 순서입니다. 낮은 값이 높은 값보다 먼저 실행됩니다.
	상대 기간	키가 유효한 년, 월 또는 일 수입니다.
	상대 기간 유형	수명주기의 기간 유형입니다. 년, 월 또는 일 중에서 선택합니다.
	상대 작업	이전 또는 이후를 선택합니다.
	관련 대상	기간이 기준이 되는 필드를 선택합니다. ◦ 활성화 날짜 ◦ 절충 날짜 ◦ 비활성화 날짜

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

섹션	필드	설명
		◦ 소멸 날짜 ◦ 만료 날짜 ◦ 작성 날짜 ◦ 마지막 갱신 날짜 ◦ 마지막 교대 날짜 ◦ 해지 날짜 주: 이 필드는 상대 작업 필드에서 선택한 값과 함께 작동합니다.
	유형	키 수명 주기의 값이 상대적인지 또는 절대적인지 선택합니다. 상대 키 생성, 활성화 및 비활성화와 같은 시스템의 다른 데이터 항목에 따라 달라지는 값을 입력합니다. 절대 날짜와 같은 정확한 값을 입력합니다.
주요 원본	암호화 모듈	선택한 암호화 모듈의 이름을 표시합니다.
	원본	키가 고객으로부터 시작되었거나 고객이 제공한 것인지 여부입니다. ◦ 우선 **ServiceNow**를 선택하십시오. ◦ 엔터프라이즈의 경우 **ServiceNow** 또는 **Customer Supplied** 선택
	키 별칭	이름 앞에 범위가 추가된 암호화 모듈의 이름입니다.
	암호화 목적	선택한 알고리즘의 목적, 키, 길이 및 모드를 표시합니다. 의 경우 필드 암호화이 필드는 읽기 전용이며 대칭 데이터 암호화/암호 해독 값을 가집니다.
	알고리즘	암호화 목적을 달성하는 데 사용되는 알고리즘을 표시합니다.
주요 작성	암호화 모듈	선택한 암호화 모듈의 이름을 표시합니다.
	키 별칭	이름 앞에 범위가 추가된 암호화 모듈의 이름을 표시합니다.
	키 작성	고객 제공 키가 아닌 생성된 키를 사용하는 경우 이 링크를 선택하여 데이터 암호화 키를 생성합니다.
	키 자동 작성	키 생성 링크를 선택하지 않으면 암호화 모듈을 사용하여 데이터를 처음 암호화해야 하는 동안 데이터 암호화 키가 자동으로 생성됩니다.
	암호화 목적	선택한 알고리즘의 목적, 키, 길이 및 모드를 표시합니다. 의 경우 필드 암호화이 필드는 읽기 전용이며 대칭 데이터 암호화/암호 해독 값을 가집니다.
	원본	키 원본 섹션에서 선택한 값을 표시합니다.
	알고리즘	암호화 목적을 달성하는 데 사용되는 알고리즘을 표시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 암호화 모듈로 이동을 선택하여 모듈 기록으로 돌아갑니다.
   이제 모듈 기록의 모듈 키 관련 목록에 항목이 있습니다. 키 별칭이 새 모듈 키로 이동했으므로 암호화 사양 관련 목록의 키 별칭 필드가 현재 비어 있습니다.

다음에 수행할 작업
고객 제공 키 사용에 대한 자세한 내용은 문서를 참조하십시오 에 대한 고객 공급 키 구성 필드 암호화 엔터프라이즈.

용 모듈 키 필드 암호화

모듈 키 탭에는 필드 암호화 데이터 암호화 키에 대한 요약 수준 정보가 표시됩니다. 키 별칭, 키 유형, 알고리즘, 키 수명 주기 상태 및 키 버전을 볼 수 있습니다.

모듈 키 정보 접근

암호화 모듈 [sys_kmf_crypto_module] 테이블의 기록에서 모듈 키에 액세스합니다. 암호화 모듈 기록에서 모듈 키 관련 목록의 기록에서 키 별칭 필드를 선택할 수 있습니다.

사용할 수 있는 정보는 인스턴스에서 활성화되어 있는 사용자의 필드 암호화 버전에 따라 다릅니다.

필드 암호화 스타터

Starter를 사용하여 필드 암호화 키 사용량 감사 데이터를 볼 수 있습니다.

필드 암호화 엔터프라이즈

키 사용 감사 데이터를 보는 것 외에도 갱신, 취소, 회전 또는 일시 중단과 같은 수동 키 작업을 수행할 수 있습니다.

모듈 키 정보

모듈 키에 대한 정보는 여기에 나열된 필드의 모듈 키 기록에 표시됩니다. 이러한 필드는 읽기 전용이며 정보 제공용으로만 사용됩니다.

필드	설명
작성 날짜	모듈 키가 생성된 시기
활성화 날짜	모듈 키가 활성화된 시기입니다.
마지막 갱신 날짜	모듈 키가 마지막으로 갱신된 시기입니다.
마지막 교대 날짜	모듈 키를 마지막으로 회전한 시간입니다.
비활성화 날짜	모듈 키가 비활성화된 경우입니다.
소멸 날짜	모듈 키가 파기되었을 때.
추후 활성화 날짜	모듈 키가 활성화되는 시기입니다.
추후 갱신 날짜	모듈 키가 갱신되는 시기.
추후 순환 날짜	모듈 키가 회전할 때.
추후 소멸 날짜	모듈 키가 파기되는 시기.
키 수명 주기 상태	현재 모듈 키의 상태입니다.

에 대한 모듈 수명주기 정책 예외 필드 암호화

모듈 수명주기 정책 예외를 사용하여 모듈 키의 수명주기를 사용자 지정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: KMF 관리자 또는 KMF 암호화 관리자

이 태스크 정보
모듈 수명주기 정책 예외는 표준 인스턴스 수준 수명주기 정책에서 모듈의 수명주기 정책을 필드 암호화 변경합니다. 예를 들어 인스턴스 수준에서 대칭 키를 1년으로 제한하도록 구성한 경우 특정 필드 암호화 모듈에 대한 모듈 수명 주기 정책 예외를 생성하여 키를 2년 동안 활성 상태로 유지할 수 있습니다.

프로시저
1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 필드 암호화 모듈.
2. 모듈 수명주기 정책 예외가 필요한 필드 암호화 모듈 기록을 선택합니다.
3. 필드 암호화 모듈 기록의 모듈 정책 예외 관련 목록에서 새로 만들기를 선택합니다.
4. 키 수명주기 정책 양식에서 필요에 따라 필드에 내용을 입력합니다.

필드	설명
암호화 모듈	이 정책 예외를 사용할 필드 암호화 모듈의 이름을 표시합니다.
적용 대상	지정된 키가 자동으로 채워집니다.
키 유형	키 유형을 선택합니다. 예외 정책은 특정 키와 관련이 있습니다. 모듈당 필드 암호화 여러 예외 정책을 생성할 수 있습니다.
정책 조건	드롭다운 메뉴에서 자격 조건을 생성하고 추가 제약 조건 기준을 완료합니다.
결과	키 사용을 거부하려면 거부 를 선택하고, 기준이 충족될 때 키 사용을 허용하려면 트랙을 선택합니다.

5. 제출을 선택합니다.

에 대한 고객 공급 키 구성 필드 암호화 엔터프라이즈
생성되는 암호화 키를 사용하는 ServiceNow 대신 고유한 데이터 암호화 키를 플랫폼으로 가져오십시오.

시작하기 전에
필요한 역할: KMF 관리자 또는 KMF 암호화 관리자

이 태스크 정보
를 사용하는 필드 암호화 엔터프라이즈경우 에 의해 ServiceNow생성된 암호화 키 대신 플랫폼에 대한 자체 데이터 암호화 키를 사용할 수 있습니다.

외부에서 ServiceNow생성된 대칭 키가 있어야 합니다. 이 문서의 예제에서는 OpenSSL을 사용합니다. OpenSSL에 대한 자세한 내용은 다음 문서를 참조하십시오 https://www.openssl.org . LibreSSL 또는 GnuTLS와 같은 다른 암호화 도구를 사용하는 경우 해당 제품의 설명서에서 유사한 단계를 참조하십시오.

프로시저
1. 컴퓨터의 명령줄(예: Terminal)에서 `openssl rand -hex 32 -out mykey.bin` 명령을 실행합니다.
   다음 단계에서 사용할 `mykey.bin` 파일을 저장합니다.
2. 인스턴스에서 다음으로 이동합니다. 모두 > 시스템 보안 > 필드 암호화 > 필드 암호화 설정.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 키 소스 필드를 **ServiceNow** 작성 키에서 고객 제공 키로 변경합니다.
4. 제출을 선택합니다.

다음에 수행할 작업
다음 단계에 따라 인스턴스에 생성한 대칭 키를 사용합니다.

1. 고객 제공 키에 대한 속성 구성
2. 고객 제공 키 래핑
3. 고객 공급 키 업로드

고객 제공 키에 대한 속성 구성

인스턴스가 고객 제공 키의 래핑을 해제하는 데 사용하는 임시 공개 래핑 키의 시스템 속성을 검토합니다.

시작하기 전에
필요한 역할: KMF 관리자 또는 KMF 암호화 연산자

이 태스크 정보
대칭 데이터 암호화 키를 ServiceNow 인스턴스에 업로드하려면 먼저 임시 공개 래핑 키를 사용하여 래핑해야 합니다.

키가 인스턴스에 업로드되면 인스턴스가 공개 키의 비공개 측을 사용하여 키를 언래핑합니다.

인스턴스의 시스템 속성을 사용하여 이 임시 공개 키의 키 패딩, 임시 키 페어 크기 및 키 유효 기간을 정의할 수 있습니다.

시스템 속성	설명	기본값
glide.kmf.ephemeral.key.padding	임시 래핑 키 패딩 체계입니다.	`OAEPWithSHA256AndMGF1Padding` OAEP SHA256이지만 SHA1이 지원됩니다.
glide.kmf.ephemeral.key.size	임시 래핑 키 크기입니다.	`4096` 4096비트이지만 2048비트도 지원됩니다.
Glide.kmf.ephemeral.key.validity	임시 래핑 키 유효 기간입니다.	`02:00:00` 2시간

프로시저

이러한 속성을 변경해야 하는 경우 지원 서비스에 문의하십시오 ServiceNow .

주: 이러한 시스템 속성은 관리자에게 표시되지 않으며 시스템 속성 [sys_properties] 목록에 나타나지 않습니다. 위의 테이블을 사용하여 기본값을 확인합니다.

다음에 수행할 작업
필요에 맞게 속성이 구성되면 로 고객 제공 키 래핑진행합니다.

고객 제공 키 래핑

대칭 데이터 암호화 키를 인스턴스에 업로드하기 전에 임시 공개 래핑 키로 래핑합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: KMF 관리자 또는 KMF 암호화 연산자

이러한 단계를 사용하려면 `.bin` 에 대칭 데이터 암호화 키가 있어야 합니다. 이 프로세스에 대한 지침은 다음 문서를 참조하십시오 에 대한 고객 공급 키 구성 필드 암호화 엔터프라이즈.

중요사항: 대칭 데이터 암호화 키는 이진 형식(. BIN). 다른 형식을 사용하는 경우 다음 오류 메시지가 표시됩니다.

```
## ### ######. #### ## ### ## ######.
```

이 태스크 정보
키의 크기, 패딩 알고리즘 및 유효 기간을 제어하는 선택적 속성을 수정하려면 문서를 참조하십시오 고객 제공 키에 대한 속성 구성.

키를 래핑할 암호화 도구가 있어야 합니다. 이 문서의 예에서는 OpenSSL 1.1을 사용합니다. OpenSSL에 대한 자세한 내용은 다음 문서를 참조하십시오 https://www.openssl.org . LibreSSL 또는 GnuTLS와 같은 다른 암호화 도구를 사용하는 경우 해당 제품의 설명서에서 유사한 단계를 참조하세요.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 필드 암호화 모듈.
2. 이전에 생성한 필드 암호화 모듈을 엽니다.

   주: 아직 필드 암호화 모듈을 생성하지 않은 경우 다음의 모듈 구성 필드 암호화단계를 사용하여 생성할 수 있습니다.

3. 모듈 관련 목록에서 키 별칭 아래의 이름을 선택하여 암호화 특정 기록을 엽니다.
4. 키 원본 섹션에 도달할 때까지 다음 단추를 선택합니다.
5. 원본 필드에 고객 공급 키 업로드 값이 있는지 확인합니다.
   그렇지 않고 해당 값을 선택할 수 없는 경우 의 3-5 에 대한 고객 공급 키 구성 필드 암호화 엔터프라이즈단계를 참조하십시오.
6. 키 별칭 필드에서 별칭을 생성합니다.
   키가 업로드되면 이 별칭을 사용합니다.
7. 다음을 선택합니다.
8. 래핑 키 다운로드 필드에서 링크를 선택합니다.

   `token_publickey` 파일이 컴퓨터에 다운로드됩니다. 이 파일의 이름을 바꾸지 마십시오.

9. 로컬 컴퓨터에서 `### ## token_publickey` 폴더를 엽니다.
   가져오기 토큰 파일(.txt)과 공개 키 파일(. PEM)을 사용합니다.
10. 생성한 대칭 데이터 암호화 키를 이 폴더로 이동합니다.
11. `token_publickey` 파일의 이름을 클립보드에 복사합니다.
12. 터미널 세션을 열고 `token_publickey` 폴더로 이동합니다.
13. 다음 명령을 입력합니다.

    중요사항: 괄호로 묶인 텍스트(〈〉)를 특정 파일 이름 및 정보로 바꿉니다. 다음 키 래핑 명령 예제 테이블을 가이드로 사용합니다.

```
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 ## 256>
```

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 래핑 명령 예시

지시	명령	예제
publickey_〈keyname〉을 입력합니다. 펨	`openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>. #`	`openssl pkeyutl -encrypt -pubin -inkey publickey_567898643ffff. #`
대칭 데이터 암호화 키의 이름 입력	`-in <keyname.bin>`	`-in mykey.bin`
<-out> 명령을 입력하여 래핑된 키 구성 요소가 128비트인지 256비트인지 지정합니다.	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	해당 사항 없음

다음에 수행할 작업
이제 키가 래핑되었으므로 의 절차를 고객 공급 키 업로드사용하여 인스턴스에 업로드할 수 있습니다.

고객 공급 키 업로드

래핑된 대칭 데이터 암호화 키를 인스턴스에 업로드하여 암호화 작업을 시작합니다.

시작하기 전에
필요한 역할: KMF 관리자 또는 KMF 암호화 관리자

이 태스크 정보

주: 고유한 키를 제공하지 않으려면 의 모듈 구성 필드 암호화ServiceNow단계를 사용하여 . 고객이 제공한 키는 취소할 수 없습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 필드 암호화 모듈.
2. 키를 사용할 필드 암호화 모듈을 엽니다.
3. 모듈 관련 목록에서 키 별칭 아래의 이름을 선택하여 암호화 특정 기록을 엽니다.
4. 키 원본 섹션에 도달할 때까지 다음 단추를 선택합니다.
5. 원본 필드에 고객 공급 키 업로드 값이 있는지 확인합니다.
   그렇지 않고 해당 값을 선택할 수 없는 경우 의 3-5 에 대한 고객 공급 키 구성 필드 암호화 엔터프라이즈단계를 참조하십시오.
6. 키 별칭 필드에 값이 있는지 확인합니다.
7. 다음을 선택합니다.
8. 고객 공급 키 업로드 링크를 선택합니다.
   이 링크는 키 래핑의 일부로 선택한 래핑 키 다운로드 링크 아래에 나타나야 합니다.
9. 찾아보기를 선택하고 다음 두 개의 파일을 선택합니다.
   a. wrapped_key_material 파일
   b. "토큰 임포트" 파일
10. 확인을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
고객이 제공한 키를 성공적으로 업로드했다는 확인 메시지가 표시됩니다. 키는 ## ## ##출처와 함께 모듈 키 관련 목록에도 나열됩니다.

이제 암호화 키가 구성되었으므로 암호화할 필드와 첨부 파일을 지정할 수 있습니다. 자세한 내용은 필드 또는 첨부 파일에 대해 암호화된 필드 구성 구성 문서를 참조하십시오.

필드 또는 첨부 파일에 대해 암호화된 필드 구성 구성

암호화된 필드 구성을 생성하여 테이블에서 암호화되는 필드와 테이블 첨부 파일의 암호화 여부를 지정합니다.

시작하기 전에
필요한 역할: KMF 관리자 또는 KMF 암호화 관리자, 보안 관리자

또는 고객 제공 키를 사용하여 ServiceNow 구성된 필드 암호화 모듈이 있어야 합니다. 아직 모듈을 구성하지 않은 경우 문서를 참조하십시오 모듈 구성 필드 암호화.

프로시저
1. 암호화하려는 테이블과 동일한 애플리케이션 범위에 있을 수 있는지 확인합니다.
2. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 암호화된 필드 구성.
3. 새로 만들기를 선택합니다.
4. 암호화된 필드 구성 양식에서 필요에 따라 필드의 필드입니다.

필드	값
유형	열 또는 첨부 파일 선택 주: 첨부 파일 암호화는 에서만 사용할 수 있습니다 필드 암호화 엔터프라이즈.
테이블	필드 또는 첨부 파일을 암호화할 테이블을 선택합니다.
열	유형 필드에서 열을 선택한 경우 암호화할 필드를 선택합니다. 주: 암호화하려는 필드를 사용할 수 없는 경우 지원되는 형식이 아닐 수 있습니다. 지원되는 필드 유형은 다음과 같습니다. ◦ 문자열(전체 UTF-8 포함) ◦ 날짜 ◦ 날짜/시간 ◦ URL ◦ HTML ◦ 필기장 ◦ 번역됨 ◦ 이메일 ◦ 전화
활성	구성이 활성 상태인지 여부입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	값
	중요사항: 활성화되면 인스턴스가 선택한 필드 또는 첨부 파일에서 새 데이터를 능동적으로 암호화합니다. 사용자는 연결된 모듈 액세스 정책을 통한 권한이 없는 경우 이 데이터에 액세스할 수 없습니다. 필드가 아직 모듈 접근 정책을 암호화하고 적용할 준비가 되지 않았는지 확인하지 마십시오. 암호화된 필드 구성이 활성화된 후 이력 데이터가 암호화되도록 하려면 열에서 대량 암호화 작업을 실행해야 합니다. 자세한 내용은 "대량 암호화, 암호 해독 또는 키 다시 입력 예약"을 참조하십시오.
암호화 모듈	이 암호화된 필드 구성에서 사용하는 필드 암호화 모듈입니다.
메서드	단일 모듈을 선택하여 모든 필드 또는 첨부 파일이 단일 필드 암호화 모듈로 암호화되도록 합니다. 다중 모듈을 선택하여 열 내의 다른 행이나 다른 첨부 파일에 대해 서로 다른 필드 암호화 모듈을 사용할 수 있도록 합니다. 다중 모듈 구성에 대한 자세한 내용은 문서를 참조하십시오 .
알고리즘 동등성 유지	암호화 모듈 필드에서 선택한 필드 암호화 모듈에서 동등성 유지가 활성화되었는지 여부를 표시합니다.

5. 제출을 선택합니다.

다중 모듈 암호화 필드 구성 구성

둘 이상의 암호화 모듈을 사용하는 암호화된 필드 구성을 생성합니다.

시작하기 전에

필요한 역할: KMF 관리자 또는 KMF 암호화 관리자, 보안 관리자

또는 고객 제공 키를 사용하여 ServiceNow 구성된 필드 암호화 모듈이 있어야 합니다. 아직 모듈을 구성하지 않은 경우 문서를 참조하십시오 모듈 구성 필드 암호화.

이 태스크 정보

암호화된 단일 필드 구성에 여러 암호화 모듈을 사용하여 다른 모듈 키를 사용하여 열 내의 다른 행(또는 동일한 테이블의 다른 첨부 파일)을 암호화합니다. 예를 들어 역할이 다른 사용자는 동일한 테이블의 데이터를 암호화할 수 있지만 서로의 암호화된 데이터를 해독할 수는 없습니다.

경고:

계속하기 전에 다중 모듈 암호화 필드 구성에 대한 다음 제한 사항을 확인하십시오.

- 다중 모듈 암호화 필드 구성에는 대량 암호화가 지원되지 않습니다.
- 필드 구성을 다중 모듈에서 단일 모듈로 변경할 수 없습니다. 대신 다중 모듈 필드 구성을 비활성화하고 새 단일 모듈 구성을 만들어야 합니다.
- 다중 모듈 필드 구성에서 사용하는 모듈 키는 필드에 데이터를 입력한 첫 번째 사용자에 의해 결정됩니다. 필드 암호화 모듈은 기록별로 설정되기 때문에 목록의 필드는 다른 필드 암호화 모듈로 암호화될 수 있습니다. 그러나 단일 기록 내에서는 하나의 필드 암호화 모듈로만 필드를 암호화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 암호화하려는 테이블과 동일한 애플리케이션 범위에 있는지 확인합니다.
2. 사용하려는 필드 암호화 모듈을 생성했는지 확인합니다.
   아직 수행하지 않은 경우 문서를 참조하십시오 모듈 구성 필드 암호화.
3. 각 모듈에 모듈 액세스 정책이 있는지 확인합니다.
   아직 수행하지 않은 경우 문서를 참조하십시오 필드 암호화에 대한 모듈 접근 정책 구성.
4. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 암호화된 필드 구성.
5. 열기 암호화된 필드 구성 기록 작성.
6. 방법 필드에서 여러 모듈을 선택합니다.
7. 필요에 따라 유형 필드에서 열 또는 첨부 파일을 선택합니다.
8. 테이블 필드에서 테이블을 선택하고 열 필드에서 열을 선택합니다(해당하는 경우).
9. 제출을 선택합니다.

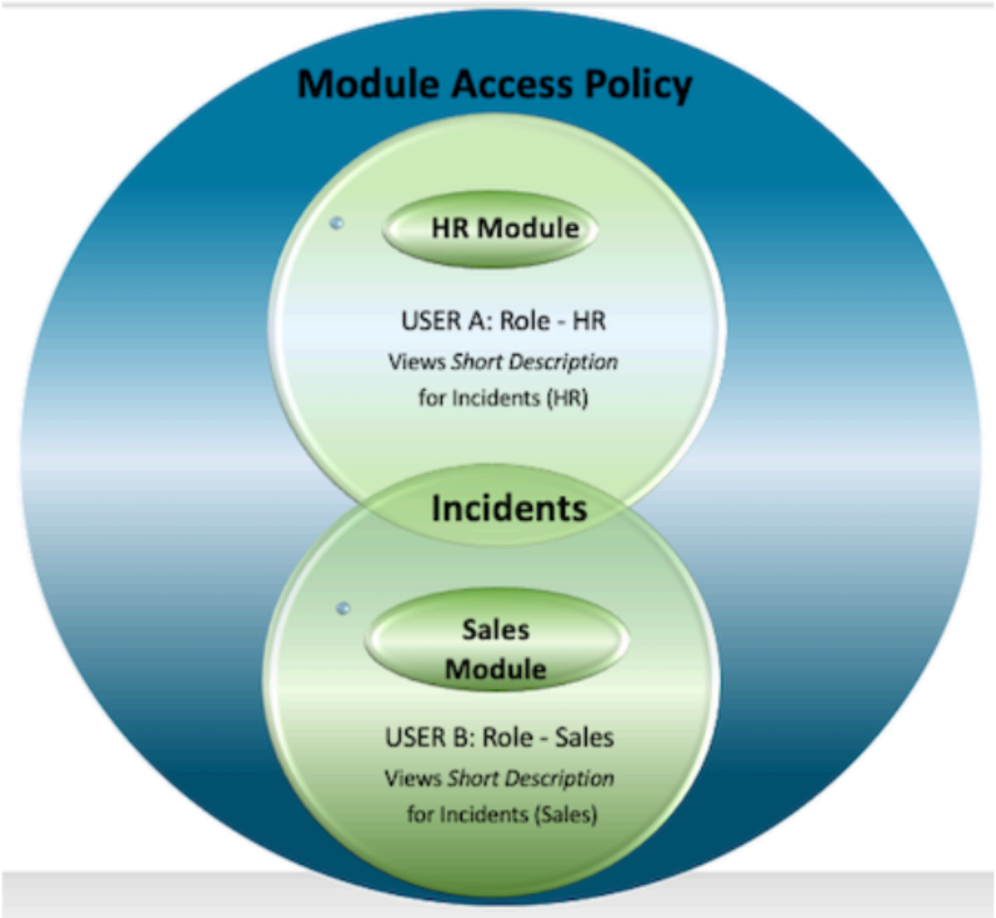
결과
기록이 저장되고 활성 필드가 활성화되면 지정된 필드에 대해 생성된 새 데이터가 관련 필드 암호화 모듈의 모듈 키로 암호화됩니다. 모듈 액세스 정책 "A"의 역할을 가진 사용자가 지정된 테이블에 쓰면 필드 암호화 모듈 "A"의 모듈 키로 데이터가 암호화됩니다. 이 경우 동일한 역할을 가진 사용자만 해당 데이터의 암호를 해독할 수 있습니다.

Example: 다중 모듈 암호화 필드 구성을 사용하여 인시던트 테이블의 간단한 설명 열 암호화

1. 두 개의 필드 암호화 모듈을 생성합니다. 이 예에서는 A와 B라고 합니다.
2. 각 필드 암호화 모듈에 대해 모듈 액세스 정책(MAP A 및 B)을 생성합니다.
   a. 필드 암호화 모듈 A의 경우 HR 역할이 있는 사용자에게 모듈 액세스 정책 A에 대한 액세스 권한을 부여합니다.
   b. 필드 암호화 모듈 B의 경우 판매 역할 액세스 권한을 가진 사용자에게 모듈 액세스 정책 B에 대한 권한을 부여합니다.
3. 인시던트 테이블의 간단한 설명 열을 지정하는 암호화된 필드 구성 기록을 생성하고 방법 필드에서 여러 모듈을 선택했는지 확인합니다.
4. 두 명의 사용자가 있어야 합니다.
   - MAP A 및 필드 암호화 모듈 A와 관련된 HR 역할을 가진 사람(사용자 A)
   - MAP B 및 필드 암호화 모듈 B와 관련된 판매 역할을 가진 사람(사용자 B)

   짧은 설명 값으로 인시던트 기록을 생성합니다. 두 사용자가 인시던트 목록을 보도록 합니다.
   a. 사용자 A가 만든 인시던트 기록에 대한 짧은 설명은 필드 암호화 모듈 A의 키로 암호화됩니다.
   b. 사용자 B가 만든 인시던트 기록에 대한 짧은 설명은 필드 암호화 모듈 B의 키로 암호화됩니다.
5. HR 및 Sales 역할이 있는 사용자는 인시던트에 액세스할 수 있습니다. HR 역할이 있는 사용자만 HR 역할을 가진사용자 A가 만든 인시던트에 대한 짧은 설명을 해독하고 볼 수 있습니다. Sales 역할을 가진 사용자만 사용자 B(Sales 역할이 있음)가 만든 인시던트에 대한 짧은 설명을 해독하고 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



필드 암호화에 대한 모듈 접근 정책 구성

필드 암호화 모듈로 암호화된 데이터를 암호화하거나 해독할 수 있는 사용자, 스크립트 또는 시스템 프로세스를 제어하는 모듈 액세스 정책을 생성합니다.

시작하기 전에

필요한 역할: KMF 관리자 또는 KMF 암호화 관리자, 보안 관리자

이 프로세스를 사용하려면 게시된 필드 암호화 모듈이 있어야 합니다. 아직 수행하지 않은 경우 문서를 참조하십시오 모듈 구성 필드 암호화.

이 태스크 정보

모듈 액세스 정책(MAP)은 데이터를 암호화하거나 암호 해독할 수 있는 사용자, 스크립트 또는 시스템 프로세스를 정의하기 위해 필드 암호화 모듈에 적용하는 접근 제어입니다. "시스템" 컨텍스트에서 실행되는 역할, 스크립트 또는 프로세스를 통해 사용자에 대한 MAP을 구성합니다. MAP이 없으면 사용자, 스크립트 또는 시스템 프로세스가 데이터를 암호화하거나 해독할 수 없으므로 엔드 투 엔드 워크플로우 프로세스가 제대로 작동하지 않을 수 있습니다.

MAP은 ACL(액세스 제어 목록)과 별개이지만 ACL과 함께 사용할 수 있습니다. MAP의 목적에 대한 자세한 내용은 을 참조하십시오 필드 암호화 탐색 .

의 경우 필드 암호화 엔터프라이즈검토하여 MAP이 필요한 사용자, 스크립트 또는 시스템 프로세스를 계획합니다.

프로시저

1. 다음으로 이동 모두 > 주요 운영 > 모듈 접근 정책 > 모두.
2. 새로 만들기를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 모듈 액세스 정책 양식에서 필요에 따라 필드를 채웁니다.

필드	설명
보험 이름	MAP의 이름
암호화 모듈	이 MAP에서 관리할 필드 암호화 모듈을 선택하십시오.
암호화 사양	옵션입니다. 이 MAP에 대한 새 암호화 사양을 선택하거나 작성합니다. 이 필드는 목적 지정 필드가 활성화된 경우에만 나타납니다.
유형	데이터를 암호화하거나 암호 해독하기 위해 이 MAP에 접근할 수 있는 사람 또는 대상을 결정합니다. 범위 지정된 애플리케이션 범위 내의 모든 항목이 이 MAP에 액세스할 수 있습니다. 역할 특정 역할을 가진 사용자만 이 MAP에 액세스할 수 있습니다. 스크립트 지정된 스크립트가 이 MAP에 액세스할 수 있는지 확인합니다. 시스템 접근 "시스템 컨텍스트"에서 실행 중인 프로세스가 이 MAP에 액세스할 수 있도록 허용합니다. 자원 교환 이 MAP에 대한 자원 교환 기능 액세스를 허용합니다. 이러한 다양한 유형의 MAP의 작동 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 필드 암호화 탐색.
대상 범위	이 MAP이 적용되는 범위를 선택합니다. 이 필드는 유형 필드가 범위로 설정된 경우에만 나타납니다.
목적 지정	옵션입니다. 양식에 암호화 사양 필드를 표시하려면 활성화합니다. 일부 사용자는 암호화할 수 있지만 해독할 수 없는 경우와 같은 세분화된 작업을 구성하려면 이 옵션을 활성화합니다.
세분화된 운영	옵션입니다. 암호화 사양에 대한 암호화 목적을 선택합니다. 사용 가능한 값은 선택한 암호화 사양 유형에 따라 다릅니다. 예를 들어 이 MAP에서 암호화만 허용하고 암호 해독은 허용하지 않거나, 그 반대의 경우, 또는 둘 다 허용하도록 지정할 수 있습니다. 이 필드는 암호화 사양 필드에 값이 있는 경우에만 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	◦ 사용자에게 암호화 접근 권한이 있지만 암호 해독 접근 권한이 없는 경우, 필드가 편집 모드로 표시되고 입력한 데이터는 별표로 표시됩니다. ◦ 사용자에게 암호 해독 액세스 권한이 있지만 암호화 액세스 권한은 없는 경우 필드에 해독된 데이터가 읽기 전용 모드로 표시됩니다. ◦ 사용자에게 암호화 및 암호 해독 접근 권한이 있는 경우, 암호화된 필드에 대해 읽기 및 쓰기 기능을 모두 사용할 수 있습니다.
대상 역할	이 MAP에 대한 액세스 권한을 가질 역할을 선택합니다. 이 필드는 유형 필드가 역할로 설정된 경우에만 나타납니다
스크립트 테이블	이 MAP에 적용할 스크립트 유형 선택: ◦ 접근 통제 ◦ 활동 디자이너 ◦ 비즈니스 규칙 ◦ 인바운드 이메일 동작 ◦ 기록 생성자 ◦ 예약된 스크립트 실행 ◦ 스크립트 포함 ◦ UI 작업 ◦ 위젯 ◦ 워크플로우 활동 이 필드는 유형 필드가 스크립트로 설정된 경우에만 나타납니다.
대상 스크립트	이 MAP에 대한 액세스 권한이 있어야 하는 스크립트 테이블 필드에서 선택한 유형 테이블의 특정 스크립트를 선택합니다. 이 필드는 유형 필드가 스크립트로 설정된 경우에만 나타납니다.
스크립트 버전 검사	선택하면 시스템이 대상 스크립트 필드에 지정된 버전으로 실행되는 스크립트의 버전을 확인합니다. 버전이 다른 경우 관리자에게 알림이 전송됩니다. 이 필드는 유형 필드가 스크립트로 설정된 경우에만 나타납니다.
승인 유형	1회 또는 반복을 선택합니다. 1회 관련된 필드 암호화 모듈의 대칭 데이터 암호화 키를 대상 인스턴스에 안전하게 한 번 공유할 수 있습니다. 반복 관련된 필드 암호화 모듈의 대칭 데이터 암호화 키를 대상 인스턴스에 반복적으로 안전하게 공유할 수 있습니다. 이 필드는 유형 필드가 자원 교환으로 설정된 경우에만 나타납니다.
대상 인스턴스 호스트	연결된 필드 암호화 모듈의 대칭 데이터 암호화 키가 전송되는 대상 인스턴스의 URL을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	이 필드는 유형 필드가 자원 교환으로 설정된 경우에만 나타납니다.
가장	이 옵션을 사용하면 다른 사용자를 가장하는 사용자가 두 사용자 모두로부터 MAP 권한을 얻습니다. 사용하지 않도록 설정하면 다른 사용자를 가장하는 사용자는 가장 이전에 부여된 MAP 권한만 갖습니다.
활성	이 MAP를 활성화하려면 활성화합니다.
결과	다음 중 하나를 선택합니다. 트랙 MAP의 액세스를 허용하고 사용을 모니터링합니다. 거부 다른 MAP에서 액세스 권한을 부여하지 않는 한 액세스를 거부합니다. StrictReject 다른 MAP에서 액세스 권한을 부여하더라도 모든 상황에서 액세스를 거부합니다.

4. 제출을 선택합니다.

다음으로 마이그레이션 중 필드 암호화 엔터프라이즈

예약된 작업은 키와 암호화된 데이터를 암호화 지원에서 로 마이그레이션합니다 필드 암호화 엔터프라이즈.

다음으로 이동하여 예약된 작업을 검토할 수 있습니다. 시스템 보안 > 높은 보안 설정 > 보안 작업:

- **autoKeyMigration**: 암호화 컨텍스트 키를 (KMF) 암호화 모듈 키로 마이그레이션합니다 핵심 관리 프레임워크 .
- **autoDataMigration**: 암호화 모듈 키를 사용하기 위해 이미 암호화한 데이터를 마이그레이션합니다 KMF .

이러한 예약된 작업은 실행 시기를 수정하고 언제든지 일시 중지하거나 다시 시작할 수 있습니다.

다음으로 이동하여 암호화된 필드 구성이 새로 마이그레이션된 모듈 키를 사용하고 있는지 확인합니다. 시스템 보안 > 필드 암호화 > 암호화된 필드 구성. 다음 항목을 찾습니다.

- 방법 필드는 단일 모듈입니다.
- 암호화 모듈 필드는 시스템이 자동으로 생성하는 암호화 모듈의 이름으로 채워집니다. 활성 상태이고 게시된 해당 모듈과 모듈 액세스 정책을 검토할 수 있습니다.

필드 암호화 엔터프라이즈 및 시스템 클론

가 인스턴스에 설치되어 있는 경우 필드 암호화 엔터프라이즈 새 필드 암호화 모듈 암호화 키가 클론 프로세스의 일부로 대상 클론 인스턴스에 자동으로 생성됩니다. 이러한 키는 사용자가 액세스할 수 있는 모든 모듈에 대해 생성되며 아직 키가 없습니다.

이로 인해 대상 클론 인스턴스의 필드 암호화 모듈에는 두 개의 모듈 암호화 키가 있을 수 있습니다.

- 활성 모듈 암호화 키입니다. 이 키는 사용자가 모듈에 액세스할 수 있고 이전 키가 없는 한 클론 후 생성된 새 키입니다.
- 비활성화된 암호화 모듈 키(자동화된 키 교환 전송에서

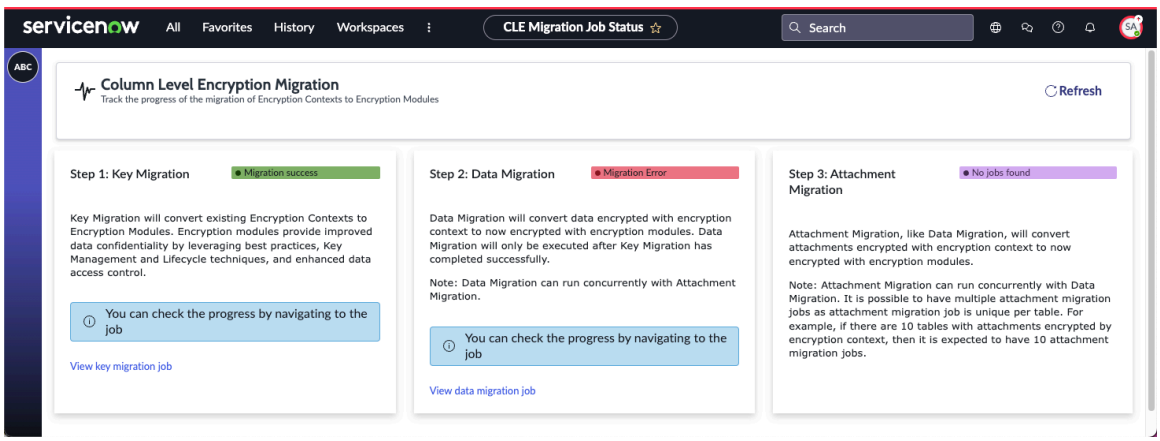
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

활성 모듈 암호화 키는 대상 클론 인스턴스에 필요한 대로 삽입된 데이터를 암호화하는 데 사용됩니다. 비활성화된 모듈은 시스템 클론의 일부로 클론된 기존 데이터를 해독하는 데 사용됩니다.

단일 키를 사용하여 모든 데이터를 해독하고 암호화하려면 모듈 키 재입력 작업을 실행할 수 있습니다. 모듈 키 변경 작업에 대한 자세한 내용은 대량 암호화, 암호 해독 및 키 변경 작업 예약을 참조하세요.

필드 암호화 마이그레이션 상태 페이지

마이그레이션 상태 페이지를 사용하여 암호화 컨텍스트가 암호화 모듈로 마이그레이션되는 과정을 추적합니다.

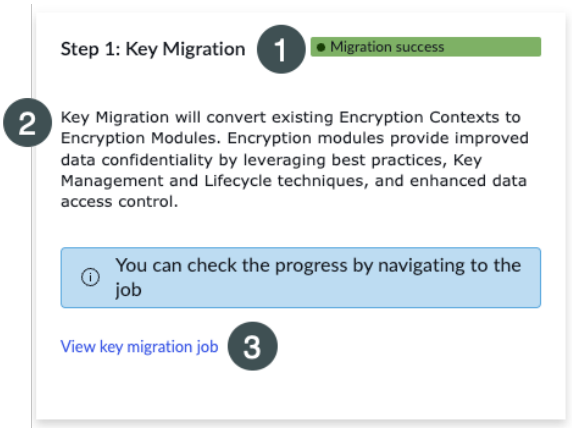


필드 암호화 마이그레이션 페이지에는 암호화 컨텍스트를 암호화 모듈로 마이그레이션하는 데 필요한 단계의 상태가 표시됩니다. 세 섹션 각각에는 프로세스의 특정 단계에 대한 상태가 표시됩니다.

페이지 섹션 카드

페이지에는 마이그레이션 진행 단계를 나타내는 세 개의 카드가 포함되어 있습니다. 이러한 카드는 다음을 표시합니다.

- (1) 현재 단계의 상태입니다. 이 상태는 단계가 성공적으로 완료되었는지 또는 처리할 작업이 없는지 여부를 표시합니다.
- (2) 나열된 단계에 대한 설명입니다.
- (3) 관련 암호화 작업 [sys_mass_encryption_job] 기록에 대한 링크.



에지 암호화 규칙에서 필드 암호화로 마이그레이션

에지 암호화 규칙에서 최신 보안 기능을 활용하기 위해 마이그레이션합니다 필드 암호화 .

마이그레이션 프로세스

이 주제에서는 다음 단계로 구성된 주제를 다룹니다.

1. Edge Encryption에서 로 열과 첨부 파일을 마이그레이션합니다 필드 암호화.
2. 에지 암호화 규칙 프록시 서버를 중지하고 사용하지 않도록 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 데이터 토큰화 해제
4. Service Catalog 항목 변수를 해독합니다.

제한

- 필드 암호화 는 현재 Edge Encryption과 같은 방식으로 데이터 토큰화를 지원하지 않습니다. 에지 암호화 규칙을 통해 토큰화된 데이터는 에 대한 필드 암호화암호화된 필드 구성에 포함되어야 합니다.
- 필드 암호화 는 현재 서비스 카탈로그 항목 변수 암호화를 지원하지 않습니다.

에지 암호화된 필드에 대해 구성 필드 암호화

Edge Encryptioned된 기존 필드를 로 필드 암호화마이그레이션하기 전에 이러한 필드에 대한 필드 암호화를 구성해야 합니다.

시작하기 전에
필요한 역할: 관리자

이 프로세스에서는 마이그레이션 필드 암호화하려는 에지 암호화 필드가 있다고 가정합니다.

프로시저

1. 다음으로 이동 모두 > 주요 운영 > 암호화 모듈 > 모두 > .
2. 암호화 모듈 목록에서 새로 만들기를 선택합니다.
3. 양식에서 다음 필드를 채웁니다.

필드	값
이름	설명이 포함된 이름 선택
암호화 사양 템플릿	기본 템플릿
암호화 모듈 수명 주기 상태	게시됨
상위 암호화 모듈	column_level_encryption

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
5. 암호화 사양 관련 목록에서 목록의 기록을 엽니다.
6. 암호화 사양 기록에서 다음을 세 번 선택하여 알고리즘 정의, 수명 주기 정의 및 키 원본 섹션을 완료합니다.
   이 섹션에서는 필드를 수정할 필요가 없습니다.
7. 키 생성 필드에서 키 생성 링크를 선택하여 키를 생성합니다.
8. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 암호화된 필드 구성.
9. 암호화된 필드 구성 목록에서 새로 만들기를 선택합니다.
10. 양식에서 다음 필드를 채웁니다.

필드	값
유형	암호화하려는 항목에 따라 열 또는 첨부 파일을 선택합니다.
암호화 모듈	이전 단계에서 작성한 암호화 모듈을 선택하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	값
테이블	암호화할 데이터가 포함된 테이블을 선택합니다.
메서드	## ## 선택
열	암호화할 테이블의 열(필드)을 선택합니다.

주: 암호화할 데이터는 테이블 및 열 필드에 의해 결정됩니다. 이러한 필드는 현재 에지 암호화 규칙을 사용하고 있는 테이블과 열(필드)이어야 합니다.

11. 제출을 선택합니다.
12. 다음으로 이동 모두 > 주요 운영 > 모듈 접근 정책 > 모두.
13. 새로 만들기를 선택합니다.
14. 양식에서 다음 필드를 채웁니다.

필드	값
정책 이름	설명이 포함된 이름 선택
암호화 모듈	이전 단계에서 작성한 암호화 모듈을 선택하십시오.
유형	## 선택
대상 역할	사용할 역할을 선택합니다. 이 역할은 열의 데이터를 암호화하고 해독할 수 있어야 합니다.
결과	원하는 작업을 선택합니다.

15. 제출을 선택합니다.
16. 구성을 확인하려면 로 필드 암호화암호화할 테이블로 이동하여 기록을 엽니다.

    예를 들어 사용자 [sys_user] 테이블에 액세스하려면 탐색 필터에 `sys_user.list` 를 입력합니다.

    이제 이전 단계에서 암호화를 위해 선택한 필드 옆에 필드 레이블 옆에 자물쇠 아이콘이 표시됩니다.

결과

에지 암호화된 필드를 필드 암호화로 마이그레이션할 준비가 되었습니다. 추가 필드를 구성하려면 각 필드에 대해 이전 단계를 반복합니다.

사용자가 암호화되지 않은 파일을 첨부하지 못하도록 방지

암호화 모듈 키에 액세스할 수 있는 사용자가 암호화되지 않은 첨부 파일을 첨부하지 못하도록 com.glide.encryption.enable_attachment_key_ui 속성을 수정합니다.

시작하기 전에

필요한 역할: security_admin

이 단계를 수행하는 security_admin 역할로 승격해야 합니다. 자세한 내용은 권한 있는 역할로 상승을 참조하십시오

기본적으로 암호화 모듈 키에 액세스할 수 있는 사용자는 암호화되지 않은 첨부 파일을 업로드할 수 있습니다. *com.glide.encryption.enable_attachment_key_ui* 시스템 속성을 사용하여 이 동작을 변경합니다.

첨부할 때 사용자는 다중 모듈 암호화 필드 구성이 있는 기록에서 UI 선택기를 볼 수 있습니다. 이 속성을 false로 설정하면 첨부 파일을 암호화하지 않는 옵션이 더 이상 표시되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 속성 > 모든 속성.
2. 시스템 속성 목록에서 시스템 속성을 찾아서 엽니다.
3. 속성 값을`false`로 설정합니다.

필드 암호화 사용

인스턴스에서 암호화된 데이터에 대한 접근을 관리하는 데 사용합니다 필드 암호화 .

관련 링크를 사용하여 공통 필드 암호화 작업에 대한 정보를 찾습니다.

관련 정보

- 용 암호화 모듈 생성 필드 암호화
- 여러 암호화 모듈 사용
- 에 대한 암호화 사양 만들기 필드 암호화
- 용 고급 알고리즘 구성 필드 암호화 엔터프라이즈
- 고객 공급 키의 속성 구성
- 필드 및 첨부 파일 암호화
- 필드 암호화 엔터프라이즈 예시

용 암호화 모듈 생성 필드 암호화

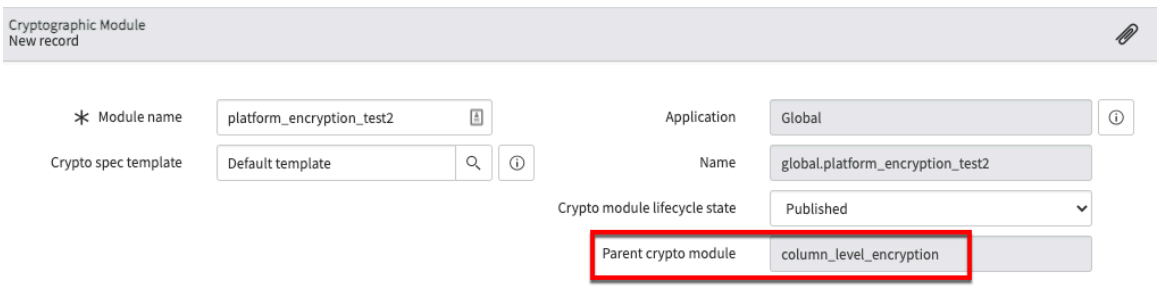
필드 암호화 암호화 모듈을 생성하여 암호화 작업에 사용되는 메커니즘을 정의합니다.

시작하기 전에
필요한 역할: sn_kmf.cryptographic_manager 또는 sn_kmf_admin, security_admin, admin

이 태스크 정보
이 절차에서는 기본 시스템에서 사용할 수 필드 암호화 있는 옵션과 기능과 함께 필드 암호화 엔터프라이즈 사용할 수 있는 추가 구성 옵션에 대해 설명합니다. 필드 암호화 엔터프라이즈 는 유료 구독으로 사용할 수 있습니다. 암호화 및 키 관리 구독 번들 각 오퍼링에서 사용할 수 있는 지원되는 기능 및 옵션을 참조하십시오. 를 얻는 필드 암호화 엔터프라이즈방법에 대한 자세한 내용은 를 참조하십시오필드 암호화 활성화.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 모듈 > 신규.



2. 양식의 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 모듈 양식

필드	설명
모듈 이름	스크립트를 실행할 때 참조할 영숫자 문자열입니다.
암호화 사양 템플릿	암호화 사양 및 권장 알고리즘에 대한 다양한 암호화 목적의 매핑을 포함하는 암호화 모듈을 생성하는 데 사용되는 기본 템플릿입니다.
애플리케이션	선택한 애플리케이션 범위입니다.
이름	모듈 생성 시 다른 범위가 지정된 애플리케이션과의 충돌을 피하기 위해 암호화 모듈 이름 앞에 애플리케이션 범위 이름이 추가됩니다. 예를 들어 전역 애플리케이션 범위에서 `my_crypto_module` 라는 이름의 모듈을 만든 경우 이름은 `global.my_crypto_module`로 저장됩니다.
암호화 모듈 수명 주기 상태	수명 주기라는 용어는 암호화 모듈의 생성, 사용 및 비활성화를 나타냅니다. 구성 중에 처음에는 초안 으로 설정합니다. 모듈을 사용할 때는 게시됨으로 설정합니다. 기본 템플릿은 게시됨으로 자동 설정됩니다.
상위 암호화 모듈	상위는 자동으로 **column_level_encryption**로 채워집니다.

3. 제출을 클릭합니다.

   성공적으로 제출하면 암호화 모듈이 암호화 모듈 테이블에 나열됩니다.

   ⚠ 경고:

   레거시 암호화 지원 사용자의 경우:

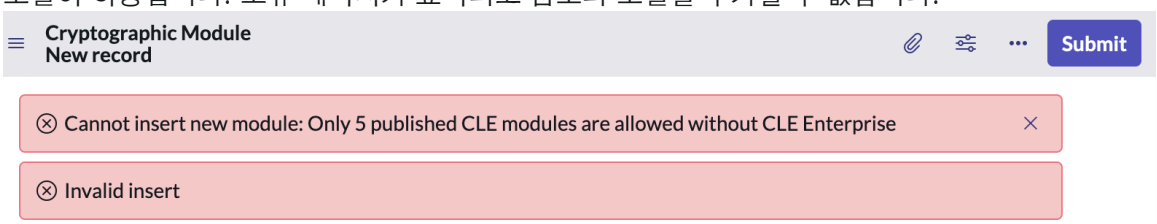
   의 엔터프라이즈가 아닌 버전을 필드 암호화사용하는 경우 모듈은 5개로 제한됩니다. 이 한도를 초과하면 다음과 같은 경고가 표시됩니다.

   이 삽입은 구독 제품에 부여된 게시된 모듈 수 제한을 필드 암호화 초과합니다. 추가 모듈에는 Enterprise 구독 필드 암호화 이 필요합니다. 계정 팀에 문의하십시오.

   기본 암호화 사양은 암호화 목적이 대칭 데이터 암호화/암호 해독으로 설정되고 알고리즘을 AES 256 CBC로 설정하여 생성됩니다. 업데이트 알고리즘을 선택합니다.

4. 구성 옵션을 열려면 새로 만든 암호화 모듈을 클릭합니다.

   ⓘ 주: 로 필드 암호화 엔터프라이즈업그레이드하기 전에 최대 5개의 필드 암호화 모듈이 허용됩니다. 오류 메시지가 표시되고 암호화 모듈을 추가할 수 없습니다.



다음에 수행할 작업
에 대한 암호화 사양 만들기 필드 암호화.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

여러 암호화 모듈 사용

여러 암호화 모듈을 사용하면 둘 이상의 암호화 모듈로 데이터를 암호화할 수 있습니다. 예를 들어, 각 모듈에 역할을 기반으로 하는 자체 액세스 정책이 있는 경우 서로 다른 역할을 가진 사용자는 동일한 테이블의 데이터를 암호화할 수 있지만 여전히 서로 암호화된 데이터를 볼 수 없도록 할 수 있습니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager 또는 sn_kmf.admin

이 태스크 정보

주: 열에 대한 암호화만 여러 모듈을 지원합니다. 첨부 파일 암호화는 그렇지 않습니다. 다중 암호화 모듈 방법을 사용하는 경우 대량 암호화를 사용할 수 없습니다.

단일 암호화 모듈을 사용하기 위해 여러 암호화 모듈을 사용하는 필드를 변경할 수 없습니다.

이 필드는 데이터를 입력한 첫 번째 사용자의 암호화 모듈에 의해 암호화됩니다. 암호화 모듈은 기록별로 설정되기 때문에 목록의 필드에는 다른 암호화 모듈이 있을 수 있습니다. 단일 기록 내에서 필드는 하나의 모듈로만 암호화할 수 있습니다.

프로시저

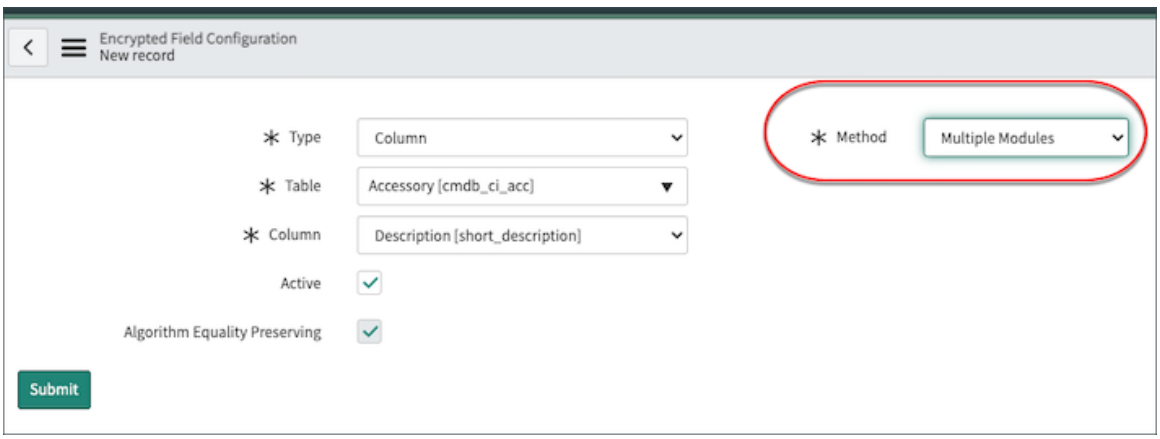
1. 여러 암호화 모듈을 생성하고 각 모듈에 대한 액세스 정책을 생성합니다.

   액세스 정책을 통해 서로 다른 암호화 모듈에 서로 다른 역할을 부여해야 합니다.

2. 다음으로 이동 시스템 보안 > 필드 암호화 > 암호화된 필드 구성.

   암호화된 필드 구성에 대한 자세한 내용은 문서를 암호화된 필드 구성 설정참조하십시오.

3. 유형 필드에서 열을 선택해야 합니다.
   첨부 파일 암호화는 여러 모듈을 지원하지 않습니다.
4. 방법 필드에서 여러 모듈을 선택합니다.



5. 암호화할 테이블의 테이블과 열을 선택합니다.
6. 제출을 클릭합니다.

결과

지정된 필드에 대해 새로 작성된 데이터는 관련 모듈의 키로 암호화됩니다. 모듈 A의 액세스 정책에 지정된 역할을 가진 사용자가 지정된 테이블에 쓰면 데이터는 모듈 A의 키로 암호화됩니다. 동일한 역할을 가진 사용자만 데이터를 읽을 수 있습니다.

Example:
인시던트 테이블의 간단한 설명 열을 암호화합니다. 다음을 수행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

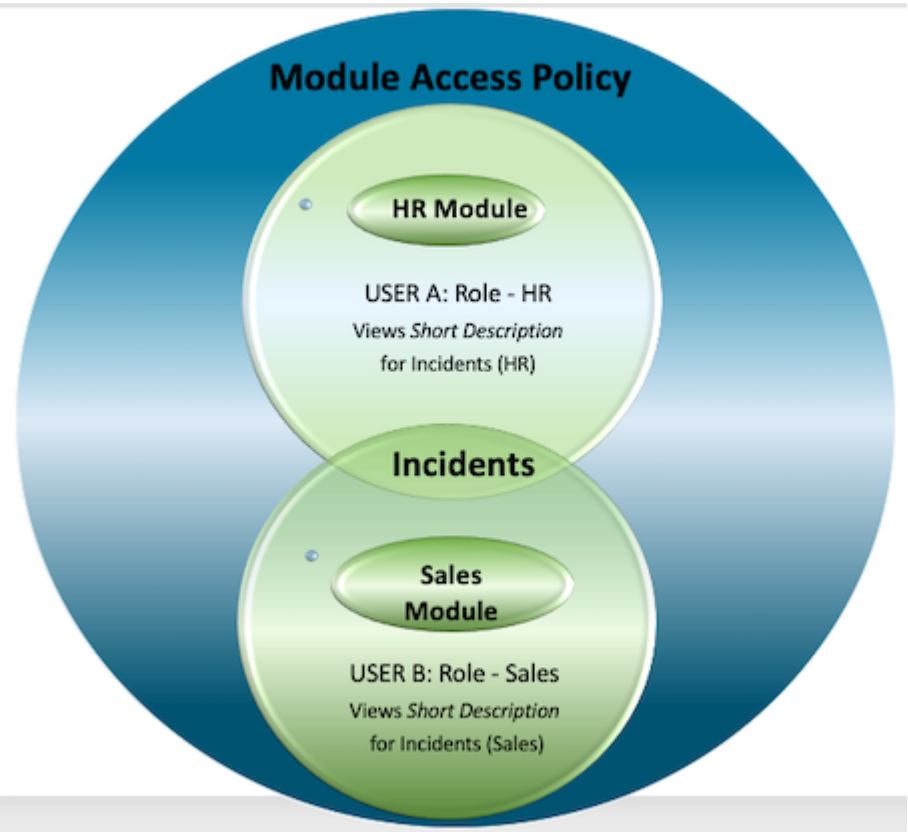
1. 두 개의 암호화 모듈 A와 B를 생성합니다.
2. 각 모듈에 대해 모듈 액세스 정책을 생성합니다.

   모듈 A의 경우 사용자에게 HR 역할 액세스 권한을 부여합니다. 모듈 B의 경우 사용자에게 Sales 역할 액세스 권한을 부여합니다.

3. 인시던트 테이블의 간단한 설명 열을 지정하여 암호화된 필드 구성 기록을 생성하고 메서드 필드에서 다중 모듈을 선택했는지 확인합니다.
4. HR 역할(사용자 A)과 판매 역할(사용자 B)을 가진 두 명의 사용자가 짧은 설명이 있는 인시던트를 만든 다음 두 사용자가 모두 인시던트 목록을 보도록 합니다.

   HR 역할의 사용자가 만든 인시던트의 짧은 설명은 모듈 A의 키로 암호화됩니다. 마찬가지로 판매 역할의 사용자가 만든 인시던트의 짧은 설명은 모듈 B의 키로 암호화됩니다.

   HR 및 판매 역할이 있는 모든 사용자가 인시던트에 액세스할 수 있지만, HR 역할이 있는 사용자만 HR 역할이 있는 사용자 A가 만든 인시던트에 대한 짧은 설명을 해독하고 볼 수 있습니다. 마찬가지로 Sales 역할을 가진 사용자만 Sales 역할을 가진 사용자 B가 만든 인시던트에 대한 짧은 설명을 해독하고 볼 수 있습니다.



에 대한 암호화 사양 만들기 필드 암호화

암호화 모듈을 만든 후 해당 암호화 사양에 액세스하여 알고리즘을 정의합니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager 또는 sn_kmf_admin and security_admin 또는 admin

이 태스크 정보

이 절차에서는 기본 시스템에서 사용할 수 필드 암호화 있는 옵션과 기능과 함께 필드 암호화 엔터프라이즈 사용할 수 있는 추가 구성 옵션에 대해 설명합니다. 필드 암호화 엔터프라이즈 기능은

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

유료 구독에서 사용할 수 있습니다. 암호화 및 키 관리 구독 번들 각 오퍼링에서 사용할 수 있는 지원되는 기능 및 옵션을 참조하십시오. 를 얻는 필드 암호화 엔터프라이즈방법에 대한 자세한 내용은 를 참조하십시오필드 암호화 활성화.

암호화 사양은 에 대한 필드 암호화 엔터프라이즈암호화 모듈을 작성할 때 시스템에 의해 작성됩니다.

.

프로시저

1. 다음으로 이동 시스템 보안 > 필드 암호화 모듈 > 모두.
2. 암호화 모듈을 선택하여 구성 옵션을 엽니다.
   암호화 모듈 정보가 화면 상단에 표시됩니다. 대칭 데이터 암호화/암호 해독 암호화 사양은 AES 256 CBC 알고리즘을 사용하여 자동으로 생성됩니다.
3. 테이블에서 암호화 사양을 선택하여 알고리즘 정의를 엽니다.
   용 고급 알고리즘 구성 필드 암호화 엔터프라이즈참조 필드 암호화 엔터프라이즈 .
4. 다음을 클릭하여 키 수명주기에 액세스합니다.

다음에 수행할 작업

다음 작업 중 하나를 수행합니다.

- 키 수명주기 테이블에서 항목을 선택하여 키 수명주기 동작을 정의합니다. 키에 대한 수명주기 정의를 완료하려면 자세한 내용을 참조하십시오 키 수명주기 상태 구성 .
- 다음을 클릭하여 암호화 키를 만듭니다. 이 프로세스에 대한 자세한 내용은 ServiceNow 암호화 키 작성 문서를 참조하십시오.

용 고급 알고리즘 구성 필드 암호화 엔터프라이즈

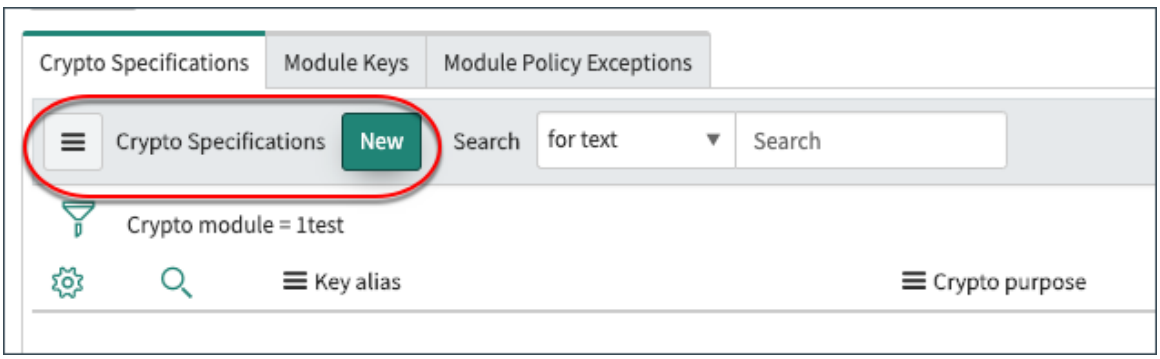
암호화 사양을 작성하여 암호화 모듈에 대한 알고리즘을 정의합니다. 에 사용할 필드 암호화 엔터프라이즈수 있는 고급 옵션으로 암호화 사양을 사용자 지정합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 암호화 사양**(#)** 탭에서 새로 만들기를 클릭합니다.



2. 양식의 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

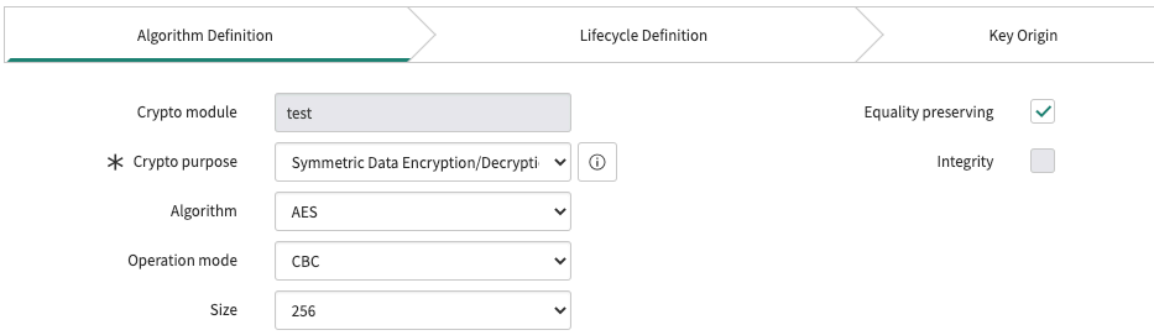
알고리즘 정의 양식

필드	설명
암호화 모듈	선택한 암호화 모듈의 이름이 채워집니다.
암호화 목적	값은 에 대한 필드 암호화 엔터프라이즈대칭 데이터 암호화/암호 해독입니다.
알고리즘	의 값은 **AES**필드 암호화 엔터프라이즈입니다.
작동 모드	의 경우 필드 암호화 엔터프라이즈값은 **CBC**입니다.
크기	가능한 값은 **256** 과 **128**입니다. 주: 256비트 크기는 암호화에 가장 안전하며 에 대한 필드 암호화 엔터프라이즈대칭 데이터 암호화/암호 해독에 사용됩니다.
동등 유지	결정적 암호화를 활성화하는 옵션입니다. 주: 이 옵션을 선택하면 필드 값이 동일하게 유지될 때 암호화된 필드 값이 동일해야 합니다. **CBC(Cipher Block Chaining)** 모드에서 **AES**를 사용하여 대칭 데이터 암호화/암호 해독을 활성화하는 옵션입니다.
무결성	GCM 작업에서 무결성을 제공하는 옵션이며 기능에는 필드 암호화 엔터프라이즈 적용되지 않습니다.

3. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 예제에서는 AES CBC-256 암호화를 보여 줍니다. 가 활성 상태이고 상위 모듈이 column_level_encryption 경우 필드 암호화 엔터프라이즈 대칭 데이터 암호화/암호 해독 AES CBC-256만 암호화 목적으로 적용됩니다. 자세한 내용은 암호화 사양 문서를 참조하십시오.



다음에 수행할 작업
다음 작업 중 하나를 수행합니다.

- 키 수명주기 테이블에서 항목을 선택하여 키 수명주기 동작을 정의합니다. 키에 대한 수명주기 정의를 완료하려면 자세한 내용을 참조하십시오 키 수명주기 상태 구성 .
- 다음을 선택하여 암호화 키를 만듭니다. 키 생성을 위해 다음 작업 중 하나를 참조하십시오.
  - ServiceNow 암호화 키 작성.
  - 고객 공급 키의 속성 구성.
  - 키 쌍의 래핑/래핑 해제 임포트.

와 함께 고객 제공 키 사용 필드 암호화 엔터프라이즈

시스템에서 생성된 키를 사용하는 ServiceNow® 대신 고객이 직접 제공한 키를 사용할 수 있습니다.

중요사항: 이러한 주제는 `com.glide.now.platform.encryption` 플러그인에서만 사용할 수 있는 를 사용하는 필드 암호화 엔터프라이즈인스턴스에만 적용됩니다. 이 플러그인을 구하는 방법에 대한 자세한 내용은 을 참조하십시오 필드 암호화 활성화 .

필드 암호화 엔터프라이즈 암호화를 위해 고유한 키를 사용할 수 있습니다. 관리자는 암호화를 위해 제공된 키 또는 자체 CSK(고객 제공 키)를 사용할 ServiceNow® 수 있습니다 Now Platform.

중요사항: 고객 제공 키 옵션을 사용하려면 고유한 암호화 키가 있어야 합니다.

키가 있으면 다음 단계에 따라 인스턴스에서 키를 사용할 수 있습니다.

1. 고객 공급 키의 속성 구성

   래핑 RSA 키 페어의 크기, 패딩 알고리즘 및 유효 기간을 정의하는 세 가지 시스템 속성이 있습니다. 이러한 속성을 검토하고 기본값이 필요에 맞지 않는 경우 해당 값을 조정합니다.

2. 고객 제공 키 래핑

   암호화 도구를 사용하여 OpenSSL과 같은 키를 래핑하여 다운로드한 공개 키로 암호화에 사용할 대칭 키를 래핑합니다.

고객 공급 키 구성 및 업로드

고객이 제공한 래핑된 키를 업로드하고 암호화 모듈을 구성하여 인스턴스에서 암호화에 키 사용을 시작합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

고객 공급 키의 속성 구성

플러그인이 필드 암호화 엔터프라이즈 활성화된 경우 시스템 속성을 사용하여 키 패딩, 임시 키 페어 크기 및 고객 제공 키의 키 유효 기간을 정의할 수 있습니다.

필드 암호화 엔터프라이즈 와 Key Management를 사용하면 데이터 암호화 키의 전체 키 수명주기를 관리할 수 있습니다. 필요에 따라 환경 내에서 생성된 데이터 암호화 키를 안전하게 교환할 수 있습니다.

키 관리를 포함한 플랫폼 암호화를 사용하면 데이터 암호화 키의 전체 키 수명주기를 관리할 수 있습니다. 필요에 따라 환경 내에서 생성된 데이터 암호화 키를 안전하게 교환할 수 있습니다.

키-페어 속성을 정의하기 위한 시스템 속성

고유한 키를 제공하는 경우 RSA 공개 키로 래핑해야 합니다. 래핑 RSA 키 페어의 크기, 패딩 알고리즘 및 유효 기간을 정의하는 세 가지 속성이 있습니다.

- *glide.kmf.ephemeral_key.key_padding* 임시 키에 대한 키 패딩 체계를 제어합니다. 기본 체계는 OAEP SHA256이지만 SHA1도 지원됩니다.
- *glide.kmf.ephemeral_key.key_size* 임시 키 쌍의 키 크기를 제어합니다. 기본값은 4096비트이지만 2048비트도 지원됩니다.
- *glide.kmf.ephemeral_key.key_validity_period* 임시 키 페어가 유효한 기간을 정의합니다. 기본값은 2시간입니다.

데이터 암호화 키를 인스턴스로 임포트한 후에는 보안 래핑 키가 인스턴스의 새 모듈 키를 보호합니다. 래핑 키는 SafeNet KeySecure의 하드웨어 보안 모듈(HSM)에서 생성된 인스턴스 키 암호화 키(IKEK)입니다. 키 유형에 대한 자세한 내용은 을 참조하십시오 Key Management Framework의 인스턴스 수준 키 .

계속 진행합니다 고객 제공 키 래핑.

고객 제공 키 래핑

다운로드한 공개 키로 암호화에 사용할 대칭 키를 래핑합니다.

시작하기 전에

주: 이 절차에서는 기본 시스템에서 사용할 수 KMF 있는 옵션 및 기능과 함께 필드 암호화 엔터프라이즈 사용할 옵션에 대해 설명합니다. 필드 암호화 엔터프라이즈 기능은 *com.glide.now.platform.encryption* 플러그인이 활성화된 경우에만 사용할 수 있습니다. 를 얻는 필드 암호화 엔터프라이즈방법에 대한 자세한 내용은 를 참조하십시오필드 암호화 활성화.

이 문서의 일부 단계에서는 로컬 디바이스에 설치된 암호화 툴을 사용해야 합니다. 이 작업의 예시에서는 OpenSSL 도구를 사용합니다. 이 도구에 대한 자세한 내용은 문서를 참조하십시오 https://www.openssl.org . LibreSSL 또는 GnuTLS와 같은 다른 암호화 도구를 사용하는 경우 해당 제품의 설명서에서 유사한 단계를 참조하십시오.

- 키의 크기, 패딩 알고리즘 및 유효 기간을 제어하는 선택적 속성을 수정합니다. 고객 공급 키의 속성 구성 문서를 참조하십시오.
- 대칭 키(. BIN)을 사용하여 암호화를 수행할 수 있습니다.

  중요사항: 키는 이진 형식이어야 합니다. 다른 형식을 사용하면 토큰 유효성 검사에 `### ####. #### ## ### ## ######.`오류 메시지가 표시됩니다.

- 키를 래핑할 암호화 도구가 있어야 합니다. 이 예에서는 OpenSSL 1.1을 사용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: sn_kmf.cryptographic_manager 또는 sn_kmf.admin

프로시저

1. 다음으로 이동 모두 > **Key Management Framework** > 암호화 모듈 > 모두.
2. 암호화 사양 관련 목록에서 고객 제공 키에 대해 생성한 암호화 모듈을 선택합니다.
3. 키 생성 단계로 이동합니다.
4. 이전에 래핑 키를 다운로드하지 않은 경우 링크를 클릭하여 *token_publickey<id>.zip* 파일을 다운로드하고 키와 동일한 위치에 저장합니다.

   주: 다운로드한 *token_publickey<id>* 파일의 이름을 바꾸지 마십시오.

5. 로컬 네트워크에 파일의 압축을 풉니다.
   zip 파일에는 가져오기 토큰과 공개 키의 두 개의 파일이 포함되어 있습니다 . PEM 인증서. 대칭 키를 공개 키로 래핑하여 암호화합니다.
6. *token_publickey* 파일의 이름을 클립보드에 복사합니다.
7. 명령줄에서 복사된 *token_publickey* 파일 이름을 사용하여 압축을 푼 파일의 폴더를 래핑된 키의 자리 표시자로 엽니다.
8. 예시를 암호화 파일의 이름으로 바꿔 이 스크립트를 편집합니다.

```
"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> "
```

   자세한 내용은 다음 표의 키 래핑 명령을 검토하십시오.

   키 래핑 명령

지시	명령	예제
래핑 토큰을 다운로드한 파일 디렉터리를 엽니다.	`cd`	`CD token_publickey123456789`
`## ## ### ######.PEM` 인증서.	`openssl pkeyutl -encrypt -pubin -inkey`	`publickey_586798643ffff.#`
여기에 키 이름을 붙여넣습니다.	`-in`	`mykey.bin`
<-out> 명령을 입력하고 키가 128비트인지 256비트인지 지정합니다.	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	해당 사항 없음

9. 명령을 실행합니다.
   시스템 메시지에 `token_publickey_<keynumber>`가 표시됩니다. 키가 생성되고 *#####wrapped_key_material* 파일이 추가됩니다.
10. 래핑된 키를 업로드합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
래핑된 키를 업로드하려면 돌아가기 고객 공급 키 구성 및 업로드

고객 공급 키 구성 및 업로드

시스템에서 생성된 키를 사용하는 ServiceNow® 대신 고객이 직접 제공한 키를 사용할 수 있습니다.

시작하기 전에
필요한 역할: security_admin, sn_kmf.cryptographic_manager

자체 키를 제공하지 않는 경우에는 이 절차를 수행할 필요가 없습니다. 키가 있는 ServiceNow® 암호화 모듈을 생성하려면 또는 암호화 모듈 생성용 암호화 모듈 생성 필드 암호화로 이동합니다.

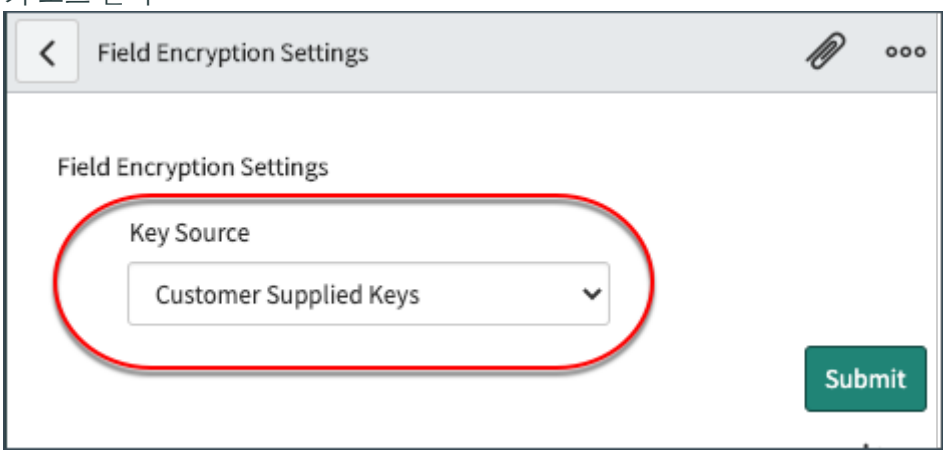
주: 이 절차는 기능에만 필드 암호화 엔터프라이즈 적용됩니다. 자세한 내용은 필드 암호화 활성화 문서를 참조하십시오.

중요사항: 고객이 제공한 키는 취소할 수 없습니다.

프로시저

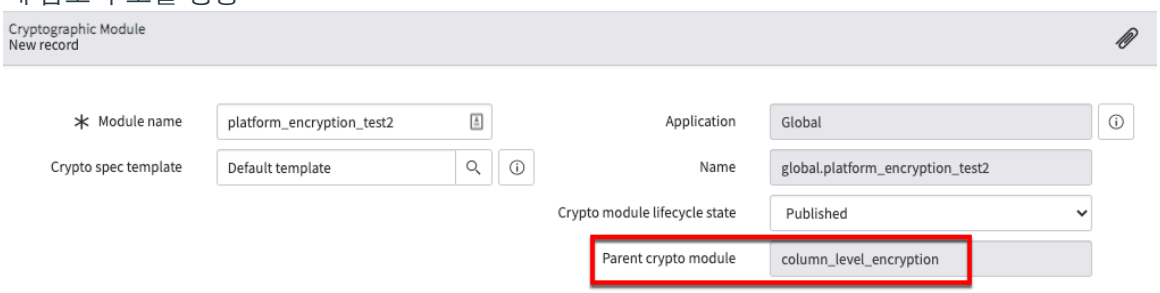
1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 설정 를 클릭하고 고객 제공 키가 선택되었는지 확인합니다.

키 소스 선택



2. 제출을 선택합니다.
3. 반환 대상 시스템 보안 > 필드 암호화 모듈 > > 새로 작성.

새 암호화 모듈 생성



4. 암호화 모듈 폼을 다음과 같이 작성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

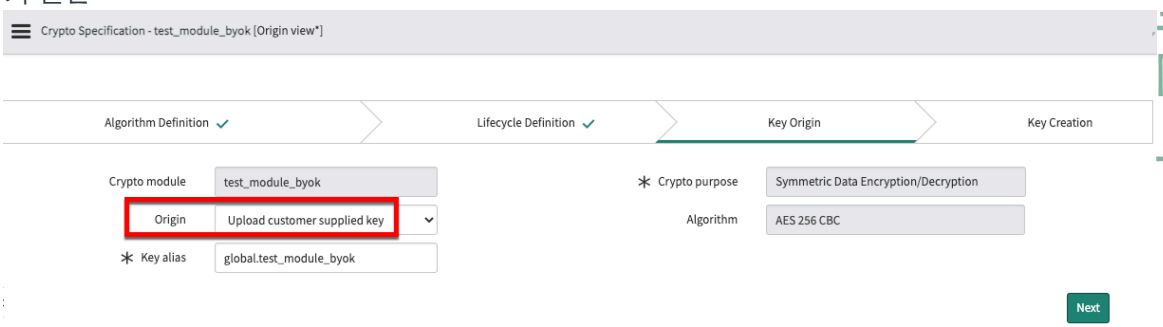
암호화 모듈 필드

필드	설명
모듈 이름	모듈의 이름을 입력합니다.
암호화 사양 템플릿	기본 암호화 템플릿이 선택됩니다.
이름	모듈 이름을 기준으로 자동으로 채워지며 애플리케이션이 적용되는지 확인하기 위해 이름 앞에 범위를 추가합니다. 이 경우 전역 범위가 적용됩니다.
암호화 모듈 수명 주기 상태	선택 게시됨 암호화 모듈을 활성화합니다.
상위 암호화 모듈	상위 모듈 **column_level_encryption** 은 고객이 제공한 키와 암호화 모듈을 사용할 때 자동으로 선택됩니다.

5. 제출을 선택합니다.
6. 테이블에서 새로 작성된 암호화 모듈을 선택합니다.
   암호화 사양 관련 목록에서 AES 256 CFB 알고리즘을 사용하여 자동 생성된 키 별칭을 선택합니다.

   시스템이 암호화 목적 및 알고리즘을 필드 암호화 자동으로 채우고 키 원본 단계로 이동합니다.
7. 고객이 제공한 업로드 키가원본이고 키 별칭이 이미 채워져 있습니다.

   키 원본



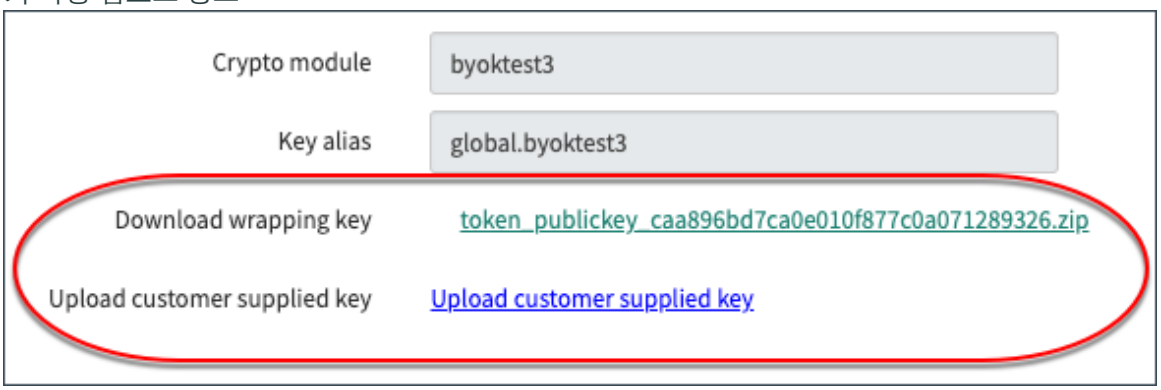
8. 다음을 선택하여 키 만들기 단계로 이동합니다.

   두 개의 링크가 있습니다.

   - 래핑 키 다운로드 가져오기 토큰 및 공개 키 인증서가 포함된 zip 파일에 키를 다운로드합니다 `.PEM` 파일. 임포트 토큰을 사용하여 인스턴스의 보안 사양에 따라 키 래핑이 성공했는지 확인합니다. 공개 키 인증서를 사용합니다 `.PEM` 파일을 사용하여 고객이 제공한 키를 토큰과 함께 업로드하기 전에 안전하게 래핑합니다.
   - 고객 제공 키 업로드 는 래핑한 토큰과 암호화된 키를 선택할 수 있는 파일 브라우저를 엽니다.

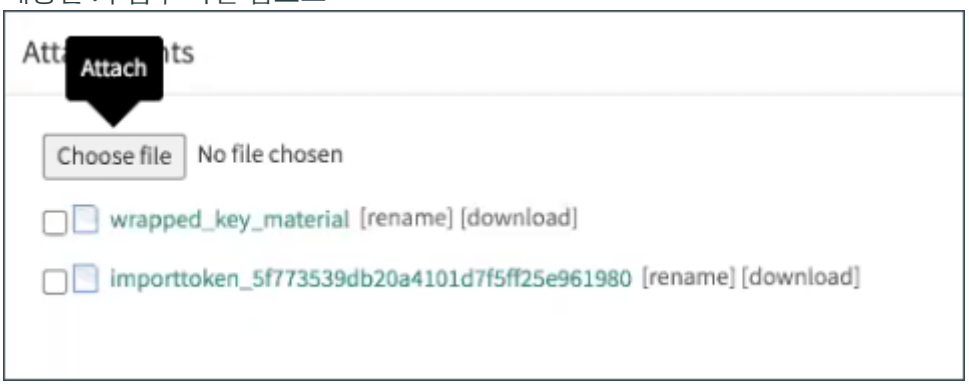
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 작성 업로드 링크



9. 래핑 키 다운로드를 선택하여 토큰을 저장합니다.
   키가 시스템에 저장된 것과 동일한 대상 위치에 토큰을 저장합니다. 다운로드한 토큰의 이름을 바꾸지 마십시오.
10. 터미널에서 BYOK 명령을 실행하여 키를 래핑합니다.
    자세한 내용은 고객 제공 키 래핑 문서를 참조하십시오.
11. 고객 공급 키 업로드를 선택합니다.
12. 찾아보기를 선택하여 래핑된 키와 토큰 파일이라는 두 개의 파일을 선택합니다.
    첨부 파일 창에 두 파일이 표시됩니다.

래핑된 키 첨부 파일 업로드



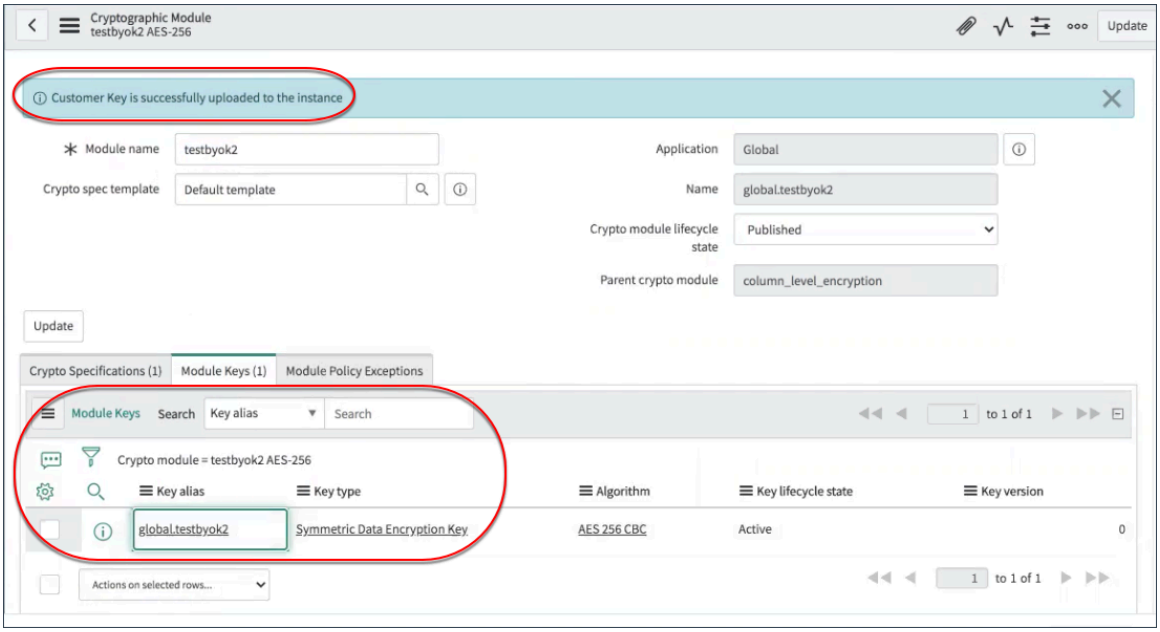
필요한 경우 제거하고 다시 업로드할 파일을 선택합니다.

13. 확인을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 모듈 화면으로 돌아갑니다. 고객 키를 성공적으로 업로드했다는 확인 메시지가 표시됩니다. 키는 모듈 키 관련 목록에도 나열됩니다.

키 업로드 확인



다음에 수행할 작업

이제 고객이 제공한 키로 암호화 모듈 구성을 마쳤으므로 다음으로 이동하십시오. 모듈 액세스 정책 생성

필드 및 첨부 파일 암호화

암호화 모듈을 만든 후 암호화된 필드 구성을 만들고 테이블의 필드를 암호화할지 아니면 첨부 파일을 암호화할지를 지정합니다.

필드를 암호화하는 방법

주: 암호화된 필드는 설계상 감사되지 않습니다. 이 동작은 구성할 수 없습니다.

1. 키 소스 지정: 시스템 생성 키 또는 고객이 제공한 키(자신의 키 가져오기) 시스템 보안 > 필드 암호화 설정.
2. 키 소스를 지정한 후 새 암호화 모듈을 생성하거나 기존 암호화 모듈을 사용합니다. 지침은 다음으로 암호화 모듈 생성 시작하십시오.

   주: 고객 제공 키를 사용하는 경우 및 고객 공급 키의 속성 구성의 지침을 용 암호화 모듈 생성 필드 암호화 따릅니다.

3. 암호화가 수행되는 테이블과 암호화할 테이블의 열 또는 첨부 파일을 지정하는 암호화된 필드 구성을 생성합니다. 실행을 시작하려면 암호화된 필드 구성 설정에서 확인할 수 있습니다.

주: 고객이 제공한 키를 사용하여 필드와 첨부 파일을 암호화하는 방법을 보여줍니다 필드 암호화 엔터프라이즈 예시 .

암호화된 필드 구성 설정

시스템에서 미리 구성된 암호화 모듈을 사용하여 암호화할 테이블, 열 또는 첨부 파일을 구성합니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager 및 security_admin 또는 보안 관리자로 역할 상승

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
해당 범위의 테이블을 볼 수 있도록 애플리케이션 범위가 올바른지 확인하십시오.

이 구성에 사용된 암호화 모듈에 대한 액세스 권한이 있는 사용자만 암호화된 테이블 열의 데이터를 읽거나 첨부 파일에 액세스할 수 있습니다.

- 사용자에게 쓰기 액세스 권한은 있지만 읽기 액세스 권한은 없는 경우, 필드가 편집 모드로 표시되고 입력한 데이터는 별표로 표시됩니다.
- 사용자에게 읽기 액세스 권한은 있지만 쓰기 액세스 권한은 없는 경우, 이 필드에는 해독된 데이터가 읽기 전용 모드로 표시됩니다.
- 사용자에게 전체 액세스 권한이 있는 경우 암호화된 필드에서 읽기/쓰기 기능을 모두 사용할 수 있습니다.

용 암호화 모듈 생성 필드 암호화 보거나 암호화 모듈 생성 시작하려면.

중요사항:

열을 암호화한 후에는 열에 삽입되는 모든 새 데이터가 자동으로 암호화됩니다. 그러나 암호화가 활성화되기 전에 열에 있었던 데이터는 자동으로 암호화되지 않습니다.

열이 암호화되기 전에 존재했던 데이터를 암호화하려면 별도의 대량 암호화 작업을 실행해야 합니다. 대량 암호화에 대한 자세한 내용은 를 참조하십시오 대량 암호화 또는 암호 해독 실행.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 암호화된 필드 구성 > 신규.
2. 새로 만들기를 선택합니다.
3. 양식을 작성합니다.

필드	설명
유형	테이블 열을 암호화하는 열 또는 첨부 파일을 암호화하여 테이블의 모든 첨부 파일을 암호화합니다. 암호화된 데이터 유형은 다음과 같습니다. ◦ 문자열 텍스트(전체 UTF-8) ◦ 첨부 파일 ◦ 날짜, 날짜/시간: 주: 암호화된 필드 구성을 생성하여 기존 날짜 및 날짜/시간 필드를 암호화할 수 있습니다. 상위 테이블에만 새 암호화 구성을 추가할 수 있습니다. 하위 테이블에는 새 암호화 구성을 추가할 수 없습니다. ◦ URL ◦ 필드 암호화 엔터프라이즈 는 다음 필드 유형도 지원합니다. ▪ HTML ▪ 필기장 ▪ 번역됨

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
테이블	필드 또는 첨부 파일을 암호화할 테이블입니다.
열	열을 유형으로 선택한 경우 암호화할 열(필드)입니다.
활성	구성을 활성으로 표시하려면 선택합니다. 구성이 아직 사용 중이 아닌 경우 선택을 취소합니다.
암호화 모듈	암호화된 필드 구성이 적용되는 암호화 모듈입니다.
메서드	단일 모듈을 선택하여 한 모듈에 걸쳐 필드 구성을 설정합니다. 둘 이상의 암호화 모듈에 걸쳐 있는 역할 기반 액세스를 위해 여러 모듈을 선택하십시오. 단일 모듈 단일 모듈을 사용하여 모든 첨부 파일을 암호화하려면 이 옵션을 사용합니다. 사용자는 이 모듈에 접근할 수 있어야 하며, 접근 권한이 없으면 첨부 파일을 업로드할 수 없습니다. 다중 모듈 이 옵션을 사용하면 사용자가 첨부 파일을 업로드할 때 모듈을 선택할 수 있습니다. 하나 이상의 모듈에 접근할 수 있는 사용자는 암호화에 사용할 모듈을 선택할 수 있습니다. 모듈 접근 권한이 없는 사용자는 암호화되지 않은 첨부 파일을 업로드할 수 있습니다.
알고리즘 암호화 보존 〔읽기 전용〕	선택한 암호화 모듈이 비결정적 암호화를 지원하도록 이미 구성되어 있는지 여부를 표시합니다. 즉, 동일한 데이터가 두 번 이상 암호화되면 매번 암호화가 다릅니다.

4. 제출을 선택합니다.

암호화 모듈에 대한 스크립트 액세스

스크립트를 실행하여 암호화 목적으로 암호화 모듈 정책에 액세스할 수 있습니다.

의 경우 핵심 관리 프레임워크정책은 스크립트 기반일 수 있습니다. 스크립트 액세스에 대한 액세스 정책이 트리거되면 백엔드 스크립트가 스크립트에서 모듈 정책 작업을 실행할 수 있습니다.

암호화 모듈은 비대칭 데이터 암호 해독 및 대칭 데이터 암호 해독과 같은 하나 이상의 암호화 목적을 지원할 수 있습니다. 각 암호화 목적에는 암호화 키 및 정의된 암호화 목적의 생성이 필요합니다.

암호화 스크립트 요청을 실행할 때는 다음 사항을 고려하십시오.

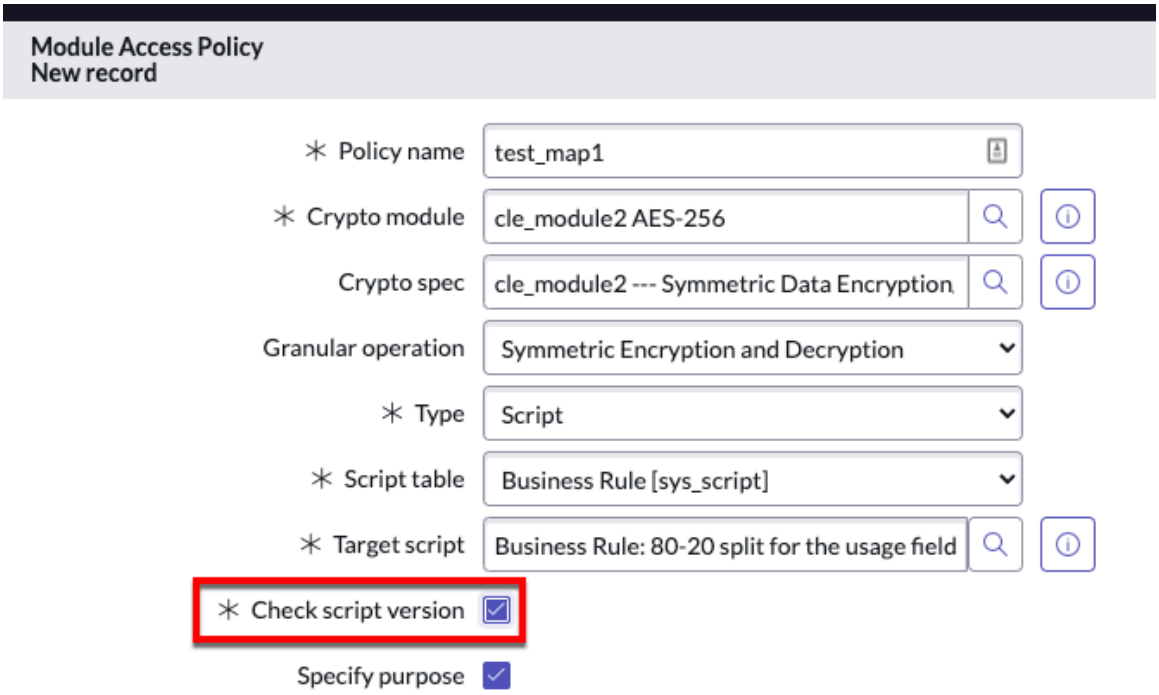
- 참조된 암호화 목적은 암호화 모듈에 정의되어야 합니다.
- 암호화 모듈에 대해 활성 작성 키가 있어야 합니다.
- 모듈 액세스 정책 유형을 스크립트로 설정해야 합니다.

스크립트 버전 검사

스크립트 유형으로 설정된 모듈 액세스 정책을 만들 때 액세스할 스크립트 버전의 무결성을 확인하는 데 사용할 수 있는 옵션이 있습니다. 할당된 스크립트 버전만 암호화 모듈에 액세스할 수 있습니다. 모듈 액세스 정책에서 스크립트 버전 확인 확인란을 선택하면 스크립트가 실행될 때마다 시스템에서 버전 비교를 수행합니다. 스크립트가 변경된 경우 사용자에게 알립니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트 버전 확인란 확인



암호화된 데이터에 대한 스크립트 접근 구성

암호화 목적으로 암호화 모듈 정책을 실행하는 스크립트를 실행합니다. 모듈 액세스 정책 작업 세분성에 따라 특정 읽기(암호 해독/래핑 해제) 또는 쓰기(암호화, 래핑) 액세스를 정의할 수 있습니다.

시작하기 전에

필요한 역할: sn_kmf.cryptographic_manager

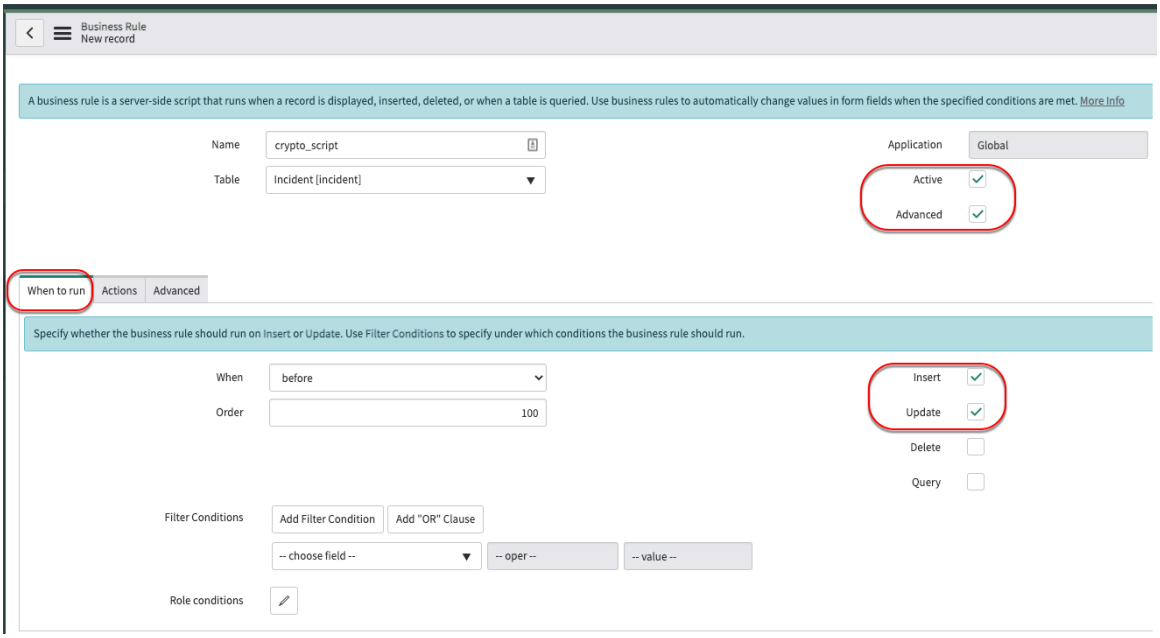
이 태스크 정보

사용 예로는 비즈니스 규칙 및 스크립트 포함이 있습니다. 이 절차에서는 비즈니스 규칙에 대한 스크립트를 사용합니다.

프로시저

1. 대칭 데이터 암호화/암호 해독 알고리즘을 사용하여 암호화 모듈을 생성합니다.
   자세한 내용은 암호화 모듈 생성 문서를 참조하십시오 데이터 또는 첨부 파일에 대한 특정 액세스는 다음과 같은 특징이 있는 모듈 액세스 정책으로 제어됩니다.
   - 대칭 암호화: 스크립트가 데이터를 암호화할 수 있지만 데이터를 해독할 수는 없습니다.
   - 대칭 암호 해독: 스크립트가 업로드된 암호화된 데이터 또는 첨부 파일의 암호를 해독할 수 있지만 데이터 또는 첨부 파일은 암호화할 수 없습니다.
   - 대칭 암호화 및 암호 해독: 스크립트는 데이터 또는 첨부 파일을 암호화하고 해독할 수 있습니다.
2. 다음으로 이동 시스템 정의 > 비즈니스 규칙.
3. 새로 만들기를 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



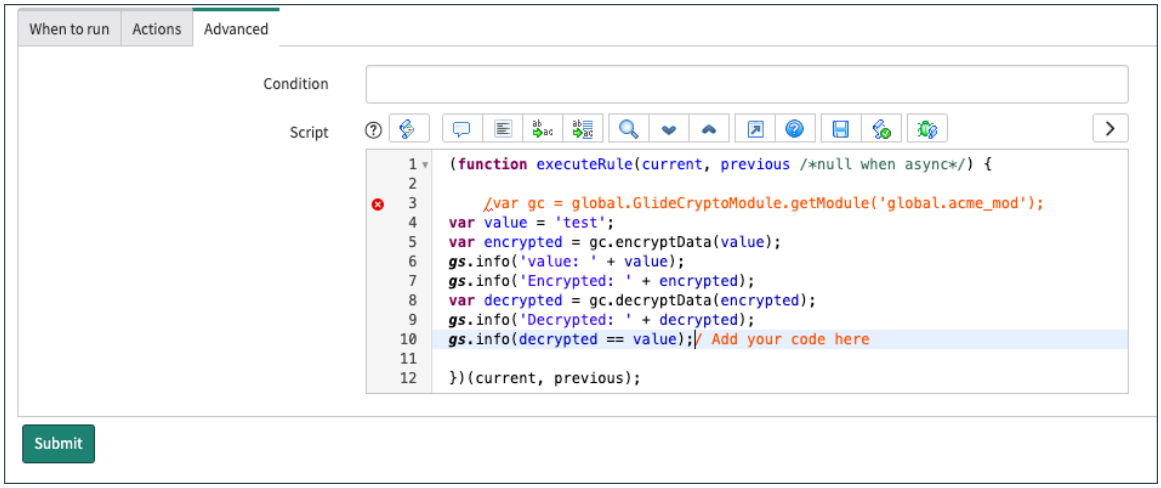
4. 실행 시기 탭에서 양식을 작성하고 고급 탭에서 스크립트를 입력합니다.

비즈니스 규칙 필드

필드	설명
이름	비즈니스 규칙의 이름을 입력합니다.
테이블	드롭다운 목록에서 인시던트 **[incident]**를 선택합니다.
애플리케이션	기본적으로 전역 이 선택됩니다.
활성	규칙을 활성으로 표시합니다.
고급	고급 옵션을 표시하려면 확인란을 선택합니다.
실행 시기 탭	실행 시기 탭에서 삽입 및 업데이트 필드를 활성화합니다.

고급 탭	고급 탭에서 다음 스크립트 텍스트를 3행에 붙여 넣습니다.
	`//`
	`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);`
	주: 자세한 내용은 "비즈니스 규칙 고급 탭" 이미지를 참조하십시오.

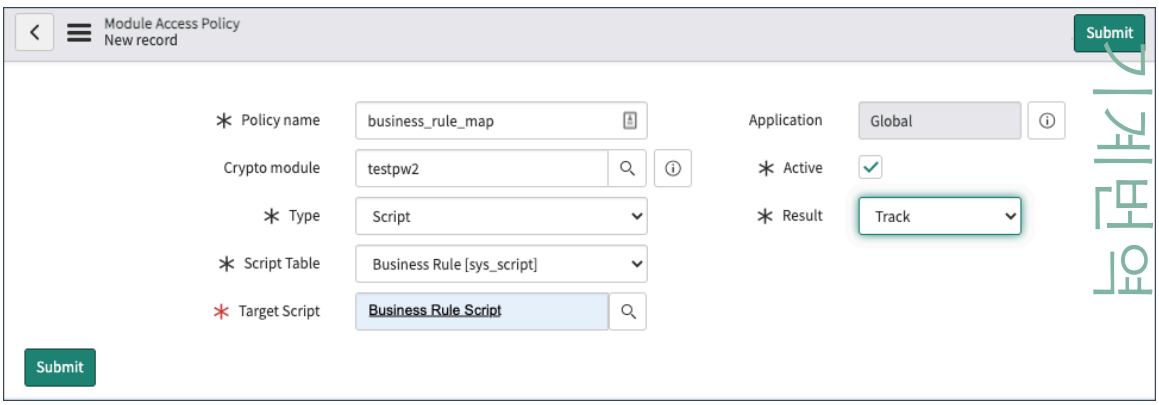
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 제출을 클릭합니다.
6. 다음으로 이동 주요 운영 > 모듈 접근 정책 > 모두.

   주: 자세한 내용은 다음 문서를 참조하십시오 모듈 액세스 정책 생성.

7. 새로 만들기를 클릭합니다.
8. 양식을



작성합니다.

모듈 접근 정책 필드

필드	설명
정책 이름	정책 이름을 입력합니다.
암호화 모듈	검색 아이콘을 클릭하여 대칭 데이터 암호화/암호 해독 알고리즘이 있는 모듈을 선택합니다.
유형	스크립트로 액세스를 제어하려면 스크립트를 선택합니다.
스크립트 테이블	스크립트 테이블 드롭다운 목록에서 값을 선택합니다. 이 예에서는 비즈니스 규칙 〔sys_script〕을 선택합니다.
대상 스크립트	정책의 스크립트 문서를 선택합니다. 테이블 이름을 선택한 다음 정책의 관련 문서를

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	선택합니다. 이 예에서는 이전 단계에서 생성한 비즈니스 규칙을 선택합니다.
활성	정책을 활성화하려면 선택합니다.
결과	스크립트에 모듈에 대한 액세스 권한을 부여하려면 결과 필드에서 추적을 선택합니다.

9. 제출을 클릭합니다.
   이제 스크립트에 대한 모듈 액세스 정책을 시스템에서 사용할 수 있습니다.

거부된 암호화 모듈 사용 요청 보기

지원되지 않는 암호화 메커니즘 때문에 스크립트의 암호화 요청을 거부한 암호화 모듈을 봅니다.

시작하기 전에
필요한 역할: sn_kmf.cryptographic_manager

이 태스크 정보
암호화 모듈은 비대칭 데이터 암호 해독 및 대칭 데이터 암호 해독과 같은 하나 이상의 암호화 목적을 지원할 수 있습니다. 암호화된 데이터는 모듈 액세스 정책에 따라서만 액세스할 수 있습니다. 스크립트가 모듈에 정의되지 않은 목적으로 암호화 모듈을 사용하려고 하면 스크립트가 암호화된 데이터에 액세스할 수 없습니다.

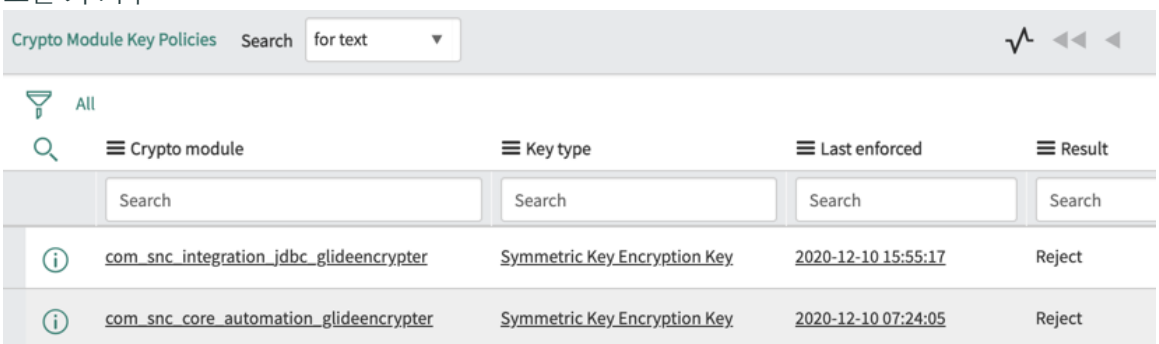
다음 예제에서는 암호화 목적이 암호화 모듈에 할당되었지만 키가 생성되지 않았습니다.

프로시저

다음으로 이동 모두 > 주요 운영 > 모듈 키 정책 > 모듈 키 거부.

요청을 거부한 암호화 모듈의 목록이 해당 스크립트에 사용된 암호화 키와 함께 표시됩니다.

모듈 키 거부



주: 다른 스크립트가 동일한 키 유형을 사용하여 동일한 암호화 모듈을 사용하려고 시도하는 경우 마지막으로 적용된 업데이트의 값입니다. 다른 행은 생성되지 않습니다.

이 예에서는 2020-02-10_15:55:17에서 module1의 키가 손상되었기 때문에 첫 번째 모듈에서 요청을 거부했습니다. 2020-02-10_07:24:05에서 두 번째 모듈의 키가 일시 중단되었기 때문에 두 번째 모듈에서 요청을 거부했습니다.

스크립트의 다음 실행 시 암호화 모듈을 사용할 수 있는 권한을 부여하려면 스크립트 암호화를 위한 모듈 액세스 정책을 작성하십시오. 자세한 내용은 암호화된 데이터에 대한 스크립트 접근 구성 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

대량 암호화, 암호 해독 및 키 변경 작업 예약

암호화, 암호 해독, 키 변경 작업이 인스턴스에 가장 적합한 시간에 실행되도록 예약합니다.

시작하기 전에

암호화, 암호 해독 및 키 변경 작업은 시간과 자원이 많이 소모될 수 있으므로 사용량이 많지 않은 시간에 예약하는 것이 좋습니다. 또한 작업을 예약하는 사용자에게 각 작업에 대한 적절한 액세스 권한이 있는지도 확인합니다.

필요한 역할: sn_kmf.cryptographic_manager

이 태스크 정보

대량 암호화 및 암호 해독은 암호화된 필드 구성 양식에서도 사용할 수 있습니다. 지침은 대량 암호화 또는 암호 해독 실행 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 보안 작업.
2. 새로 만들기를 클릭합니다.
3. 예약 양식을 작성합니다.

필드	설명
이름	암호화, 암호 해독 또는 키 변경 작업의 이름입니다.
유형	작업 유형: ◦ 모듈로의 키 마이그레이션 컨텍스트: 암호화 모듈의 접근 통제를 위한 모듈 접근 정책 기록 작성을 포함하여 암호화 컨텍스트 키를 암호화 모듈로 대량 마이그레이션 ◦ 모듈로 데이터 마이그레이션 컨텍스트: 암호화 컨텍스트로 암호화된 데이터를 암호화 모듈로 마이그레이션합니다. ◦ 대량 암호 해독 첨부 파일:D 테이블 필드에서 정의한 단일 테이블의 기록에서 암호화된 모든 첨부 파일을 암호화합니다. ◦ 대량 암호화 첨부 파일: 테이블 필드에서 정의한 단일 테이블에 대한 기록의 모든 첨부 파일을 암호화합니다. ◦ 대량 암호화 모듈: 필드 암호화 구성에 사용된 정의된 열/필드의 기존 값을 암호화합니다. ◦ 대량 암호 해독 모듈: 단일 모듈로 필드 암호화 구성에 사용된 정의된 열/필드의 기존 값을 해독합니다. ◦ 대량 암호 해독 다중 모듈: 다중 모듈을 사용하여 필드 암호화 구성에 사용된 정의된 열/필드의 기존 값을 해독합니다. ◦ 모듈 키 재입력: 모듈의 현재 활성 키를 사용하여 필드 암호화 구성에 사용된 정의된 열/필드의 기존 값을 다시 암호화합니다. ◦ 첨부 파일 컨텍스트를 모듈로 마이그레이션: 필드 암호화 구성에 정의된 테이블의 기존 첨부 파일을 암호화합니다. 이전에 컨텍스트로 암호화된 첨부 파일은 모듈을 사용하여 다시 암호화됩니다.
상태	초기 작업 상태는 신규입니다. 작업이 예정대로 실행되면 상태가 그에 따라 업데이트됩니다.
기간 시작	24시간 형식의 작업 시작 시간입니다.
기간 종료	24시간 형식의 작업 종료 시간입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
테이블	암호화하거나 해독할 테이블입니다.
필드	암호화하거나 해독할 필드입니다.
요약	작업이 실행 중이거나 완료되었거나 오류가 있을 때의 작업 상태 정보입니다.

주: 시스템 오버헤드로 인해 대량 암호화, 암호 해독 및 키 변경 작업이 사용량이 많지 않은 시간에 실행되도록 예약해야 합니다. Now Platform기간 시작과 기간 종료 사이에 작업을 실행합니다. 작업이 한 처리 기간 내에 완료되지 않은 경우 모든 처리가 완료될 때까지 지정된 다음 처리 기간 동안 작업이 계속됩니다.

4. 제출을 클릭합니다.
5. 작업을 예약한 후 다음을 수행할 수 있습니다.
   - 작업 취소를 클릭하여 실행 중인 작업을 취소합니다.
   - 작업을 즉시 시작하려면 시작을 클릭합니다.
   - 업데이트를 클릭하여 작업 일정에 대한 변경 내용을 저장합니다.
   - 삭제를 클릭하여 예약된 작업을 삭제합니다.

대량 암호화 또는 암호 해독 실행

암호화 구성에 대해 대량 암호화를 실행할 수 있을 뿐만 아니라, 대량 암호 해독을 실행하여 이전에 암호화된 값을 해독할 수도 있습니다.

시작하기 전에
필요한 역할: security_admin

이 태스크 정보
대량 암호화 및 암호 해독을 위해 예약된 작업을 생성할 수도 있습니다. 지침은 대량 암호화, 암호 해독 및 키 변경 작업 예약 문서를 참조하십시오.

대량 암호화 및 암호 해독은 암호화된 필드 구성에서 단일 암호화 모듈을 사용하는 경우에만 사용할 수 있습니다. 대량 암호 해독은 단일 및 다중 암호화 방법 모두에 사용할 수 있습니다.

주: 대량 암호화 및 암호 해독은 자원과 시간이 많이 필요하므로 사용량이 많지 않은 시간에만 실행해야 합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 필드 암호화 > 암호화된 필드 구성.
2. 대량 암호화 또는 암호 해독하려는 필드에 대해 암호화된 필드 구성을 엽니다.
3. 관련 링크에서 사용 가능한 옵션을 선택합니다.
   - 대량 암호 해독 작업 예약
   - 대량 암호화 작업 예약
4. 대화 상자에서 선택 항목을 확인합니다.

결과
대량 암호화를 실행 중인 경우, 모든 값은 암호화된 필드 구성 기록에 정의된 암호화 모듈로 암호화됩니다. 대량 암호 해독을 실행하면 액세스 권한이 있는 암호화 모듈로 암호화된 필드만 암호 해독됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 암호화 엔터프라이즈 예시

다음 예시에서는 고객이 제공한 키를 사용하여 필드와 첨부 파일을 암호화하는 과정을 안내합니다.

필드 암호화 엔터프라이즈 연습

이 연습에서는 ()KMF를 핵심 관리 프레임워크 사용하여 필드 암호화 엔터프라이즈 인스턴스의 필드를 암호화하는 방법을 보여줍니다. 또한 고유한 키를 사용하는 방법도 보여 줍니다.

시작하기 전에

주: 이 절차는 기능에만 필드 암호화 엔터프라이즈 적용됩니다. 를 얻는 필드 암호화 엔터프라이즈방법에 대한 자세한 내용은 를 참조하십시오필드 암호화 활성화.

필요한 역할: admin 또는 security_admin

주: security_admin 권한 있는 역할입니다. 권한 있는 역할 사용에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하십시오.

이 태스크 정보

이 검토 과정은 개인 암호화 키를 이미 만들어 업로드한 인스턴스부터 시작됩니다. 이 ServiceNow 키를 사용할 수 있지만 이 예시에서는 고객이 제공한 키를 사용합니다.

키가 암호화 모듈에 저장되면 특정 사용자의 액세스가 제한된 급여 또는 주민등록번호와 같이 인스턴스의 필드 구성을 시작할 수 있습니다. 암호화된 필드 구성에서 중요한 데이터에 액세스할 수 있는 권한 있는 직원을 지정합니다.

이 작업은 두 가지 시나리오를 보여 줍니다. 중요한 데이터를 볼 수 있는 권한이 없는 사용자를 위해 인시던트의 간단한 설명 필드를 암호화하는 예가 있습니다.

첨부 파일을 암호화하여 액세스 권한이 부여된 사용자에게만 표시하거나 데이터 보기가 제한되지 않은 모든 사용자에게 표시할 수도 있습니다. 첨부 파일을 암호화하려면을 참조하십시오 첨부 파일 암호화 검토 과정 .

프로시저

1. 활성화되어 있는지 확인하십시오 필드 암호화 엔터프라이즈 .
2. column_level_encryption용 암호화 모듈을 만듭니다.
   자세한 내용은 을 참조하십시오 용 암호화 모듈 생성 필드 암호화 암호화 모듈 생성 .
3. 다음으로 이동 시스템 보안 > 암호화된 필드 구성.
4. 새로 만들기를 클릭합니다.
5. 양식의 필드에 내용을 입력합니다.

암호화된 필드 구성 양식

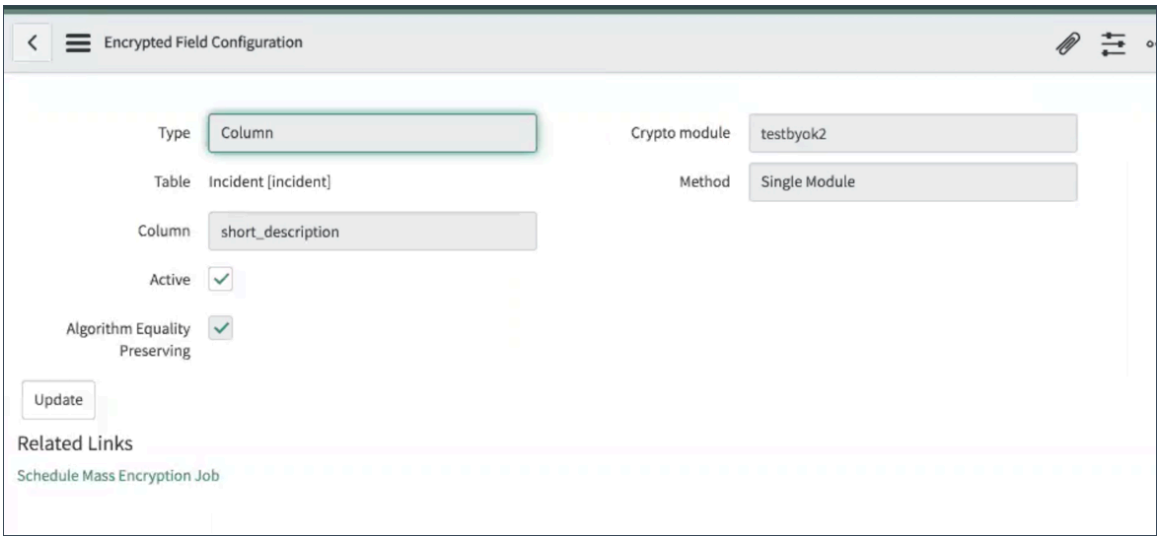
필드	설명
유형	개인 키를 사용하려면 열이 필요합니다.
테이블	중요한 정보를 저장하는 테이블입니다. 이 예에서는 인시던트 **[incident]**를 선택합니다.
열	암호화할 민감한 날짜를 나타내는 열 또는 특정 정보입니다. 이 예에서는 **short_description**를 선택합니다.
활성	필드 구성을 사용하기 위해 활성 으로 표시하는 옵션입니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
알고리즘 동등성 유지	이 옵션은 자동으로 선택됩니다.
암호화 모듈	개인 키와 함께 사용하기 위해 만든 모듈입니다.
메서드	단일 모듈 옵션은 한 모듈에 정책을 적용하는 데 사용됩니다. 다중 모듈은 여러 모듈에 정책을 적용하는 데 사용됩니다.

암호화 필드 구성 예



6. 제출을 클릭합니다.

   암호화 모듈에 대한 액세스를 할당하기 위한 모듈 액세스 정책을 수립합니다. 자세한 내용은 모듈 액세스 정책 생성 문서를 참조하십시오.

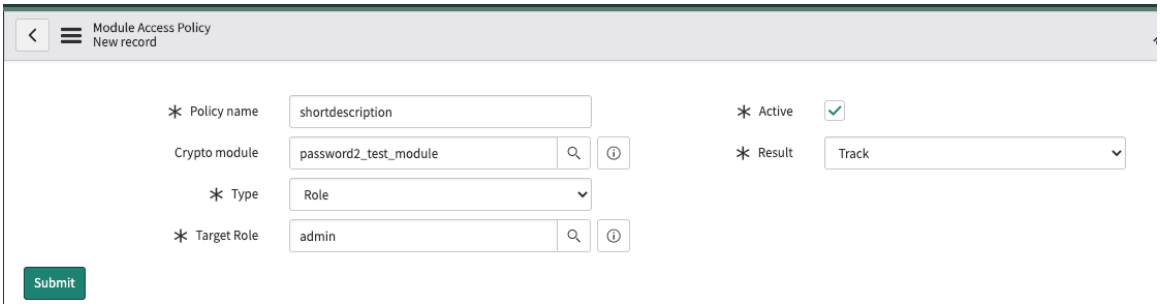
7. 다음으로 이동 주요 운영 > 모듈 접근 정책 > > 새로 작성 > .
8. 양식의 필드에 내용을 입력합니다.

모듈 접근 정책 양식

필드	설명
정책 이름	## ##과 같은 정책의 이름입니다.
암호화 모듈	키를 암호화하기 위해 생성한 암호화 모듈입니다.
유형	암호화 정책에 대한 접근 지정 유형입니다. 역할을 사용하여 할당된 역할이 있는 사용자에게만 암호화된 필드에 대한 액세스 권한을 부여합니다.
대상 역할	암호화된 필드에 액세스할 수 있는 역할입니다. 이 예에서는 관리자를 선택합니다.
활성	모듈 액세스 정책을 활성화하는 옵션입니다.
결과	추적옵션을 사용하면 선택한 역할의 필드에 액세스할 수 있습니다. (선택한 역할에 대해 해당 필드에 대한 액세스를 제한하려면 거부 또는엄격한 거부를 선택합니다.)

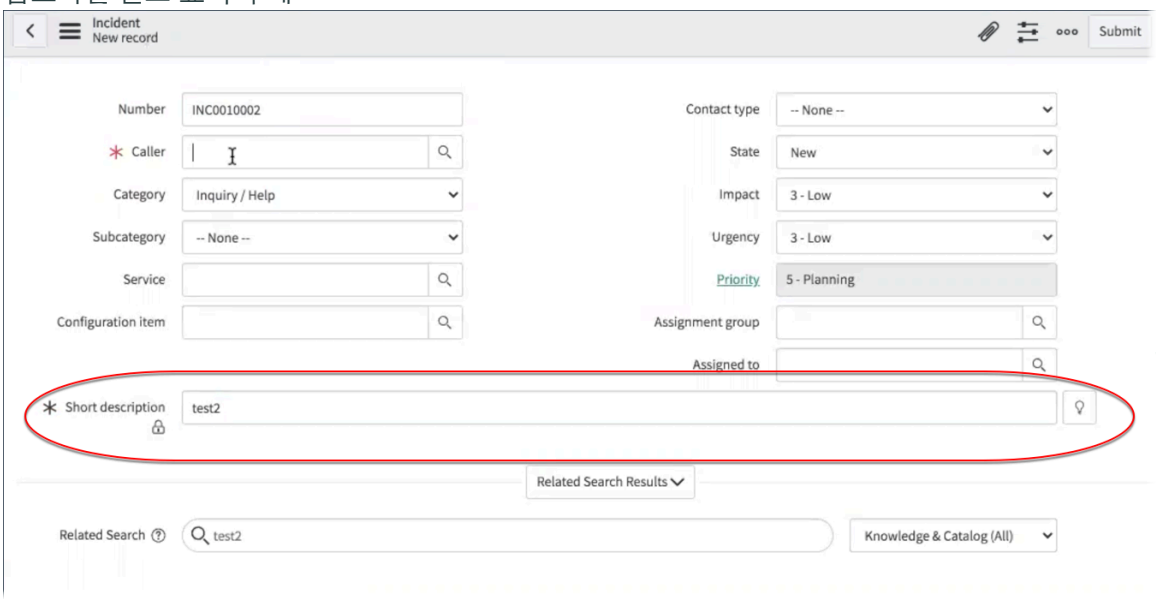
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈 접근 정책 예



9. 제출을 클릭합니다.
10. sn_kmf.admin 역할을 가진 사용자로 인시던트 > 신규.

암호화된 필드 표시의 예



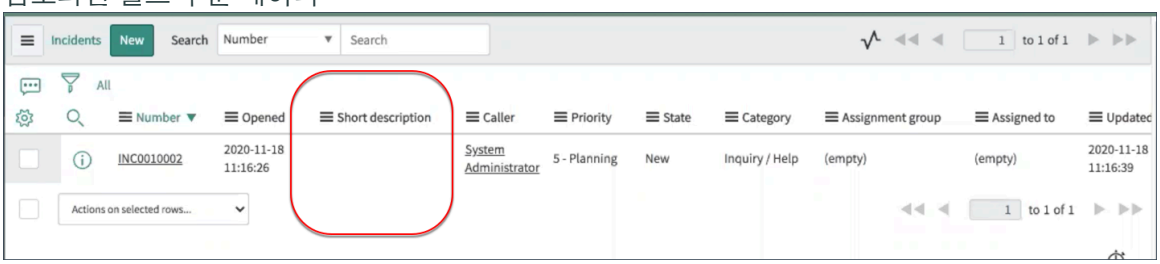
이제 모듈 액세스 정책 구성에 따라 간단한 설명 필드를 볼 수 있습니다.

주: 모듈 접근 정책을 추적으로 설정하여 sn_kmf.admin 역할에 암호화된 필드, 짧은 설명에 대한 사용자 접근 권한이 부여되었습니다. 필드 이름 아래에 있는 잠금 아이콘( )은 필드가 암호화된 필드임을 나타냅니다.

이제 최종 사용자로서 인시던트 모듈에 액세스하여 암호화된 필드 구성을 테스트할 수 있습니다.

11. 구성된 필드에서 암호화된 데이터를 볼 수 없도록 제한할 사용자로 로그인합니다.

암호화된 필드 수준 데이터



인시던트 번호에 액세스하면 짧은 설명의 데이터가 표시되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
대칭 키를 사용하여 를 사용하여 필드 암호화 엔터프라이즈특정 필드에 대한 접근을 제어했습니다.

첨부 파일 암호화 검토 과정

이 연습에서는 ()KMF를 핵심 관리 프레임워크 사용하여 필드 암호화 엔터프라이즈 인스턴스의 첨부 파일을 암호화하는 방법을 보여줍니다. 또한 고유한 키를 사용하는 방법도 보여 줍니다.

시작하기 전에

주: 이 절차는 기능에만 필드 암호화 엔터프라이즈 적용됩니다. 를 얻는 필드 암호화 엔터프라이즈방법에 대한 자세한 내용은 를 참조하십시오필드 암호화 활성화.

필요한 역할: kmf cryptographic manager

이 태스크 정보

이 검토 과정은 고객이 제공한 암호화 키를 이미 생성하고 업로드한 인스턴스부터 시작됩니다. 이 키를 사용할 수 있지만 이 예시에서는 고객이 제공한 키를 사용합니다.

인스턴스에 기밀 첨부 파일을 업로드하고 특정 사용자의 액세스를 제한합니다. 암호화된 필드 구성을 사용하여 중요한 데이터에 액세스할 수 있는 권한 있는 직원을 지정합니다.

액세스 권한이 부여된 사용자에게만 표시되거나 데이터 보기가 제한되지 않은 모든 사용자에게 표시되도록 첨부 파일을 암호화하는 방법을 보여 줍니다. 이 예에서는 특정 역할이 인시던트 모듈의 첨부 파일에 액세스할 수 없도록 제한합니다.

주: 와 함께 여러 모듈을 사용할 수 있지만 첨부 파일 암호화는 필드 암호화 엔터프라이즈단일 모듈을 사용해야 합니다.

프로시저

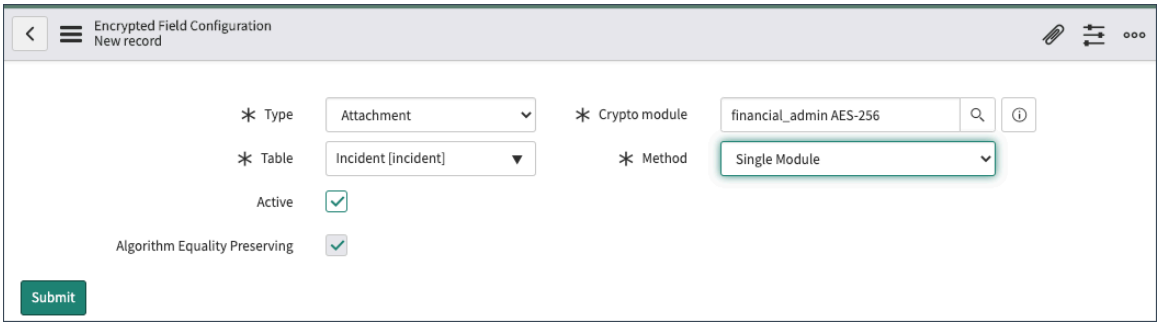
1. 활성화되어 있는지 확인하십시오 필드 암호화 엔터프라이즈 .
2. 암호화 모듈을 생성합니다.
   자세한 내용은 용 암호화 모듈 생성 필드 암호화 문서를 참조하십시오.
3. 다음으로 이동 시스템 보안 > 암호화된 필드 구성.
4. 새로 만들기를 클릭합니다.
5. 다음 폼을 작성합니다.

암호화된 필드 구성 필드

필드	설명
유형	선택한 테이블에서 첨부 파일을 암호화하는 데 개인 키를 사용하려면 첨부 파일을 선택합니다. 이 예에서는 인시던트를 선택합니다.
테이블	중요한 정보에 액세스하려면 테이블을 선택합니다. 이 예에서는 인시던트 **[incident]**를 선택합니다.
활성	필드 구성을 사용할 수 있도록 활성화 로 표시합니다.
알고리즘 동등성 유지	를 선택하면 필드 암호화 엔터프라이즈선택한 테이블에 따라 이 필드가 표시됩니다.
암호화 모듈	개인 키와 함께 사용하기 위해 생성한 모듈을 선택합니다.
메서드	단일 모듈 옵션은 한 모듈에 정책을 적용하는 데 사용됩니다. 다중 모듈은 여러 모듈에 정책을 적용하는 데 사용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화된 필드 구성 테이블



6. 제출을 클릭합니다.

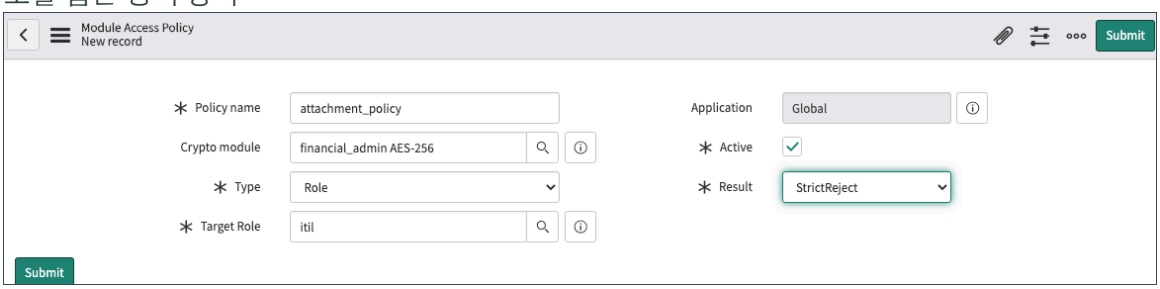
   암호화 모듈에 대한 액세스를 할당하기 위한 모듈 액세스 정책을 수립합니다. 자세한 내용은 을 모듈 액세스 정책 생성 참조하십시오.

7. 다음으로 이동 주요 운영 > 모듈 접근 정책 > 모두.
8. 새로 만들기를 클릭합니다.
9. 다음 폼을 작성합니다.

모듈 접근 정책 필드

필드	설명
정책 이름	정책의 이름(예: "첨부 파일 정책")을 입력합니다.
암호화 모듈	키를 암호화하기 위해 작성한 암호화 모듈을 선택하십시오.
유형	할당된 역할이 있는 사용자의 암호화된 필드에 대한 액세스를 제한하려면 역할을 선택하십시오.
대상 역할	암호화된 필드에 접근할 수 없는 역할을 선택하십시오. 이 예에서는 **itil**을 선택합니다.
활성	모듈 액세스 정책을 사용하려면 이 확인란을 선택합니다.
결과	선택한 역할에서 첨부 파일에 대한 액세스를 통제하려면 엄격한 거부 를 선택합니다. (선택한 역할에 대한 액세스 권한을 부여하려면 추적을 선택합니다.)

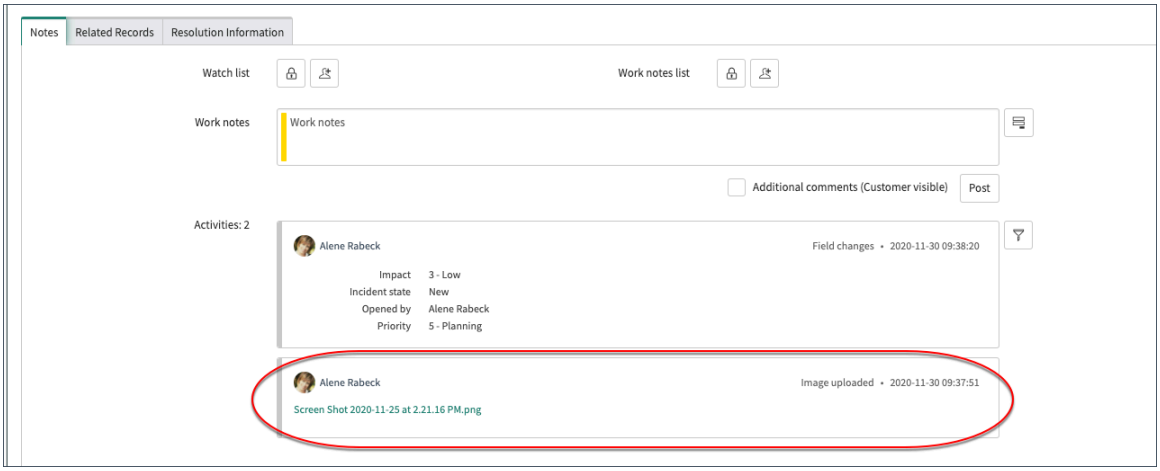
모듈 접근 정책 양식



10. 제출을 클릭합니다.
11. 관리자 또는 인시던트 작성자는 인시던트로 이동하여 메모 관련 목록의 활동에 첨부 파일을 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할당 사용 가능한 첨부 파일



12. 암호화된 첨부 파일에 대한 접근을 제한한 사용자로 로그인합니다.
13. 인시던트를 열고 활동: 섹션으로 스크롤합니다.
    제한된 역할을 가진 사용자는 첨부 파일을 여는 링크에 접근할 수 없습니다.
14. 이제 고객이 제공한 키를 사용하여 를 사용하여 필드 암호화 엔터프라이즈특정 첨부 파일에 대한 액세스를 제어할 수 있습니다.

필드 암호화 엔터프라이즈

필드 암호화 엔터프라이즈 는 핵심 관리 프레임워크 (KMF)를 활용하여 인스턴스에서 필드와 첨부 파일의 암호화 및 암호 해독 방법을 사용자 지정하고 관리할 수 있습니다. 를 사용하려면 필드 암호화 엔터프라이즈구독이 필요합니다.

중요사항: 이 항목에서는 의 엔터프라이즈 버전에 필드 암호화대해 설명합니다. 의 표준 버전에 필드 암호화대한 자세한 내용을 보거나 두 버전 간의 차이점에 대해 알아보려면 다음 문서를 참조하십시오 필드 암호화 탐색.

필드 암호화 엔터프라이즈 는 키 관리 기능을 전제로 필드 암호화 하며 이를 사용합니다 핵심 관리 프레임워크 . 필드 암호화 엔터프라이즈 는 애플리케이션 수준 필드 암호화를 위한 키 보호 및 키 수명주기 관리를 제공합니다. 모든 키는 궁극적으로 FIPS 140-2-L3 HSM(하드웨어 보안 모듈)에 뿌리를 둔 키 래핑 계층 구조로 보호됩니다.

필드 암호화 엔터프라이즈 를 사용하면 NIST 800-57 프랙티스에 따라 지원되는 필드를 암호화하고 해독하는 방법을 관리할 수 있습니다. 또한 적절한 키 보호 및 관리를 위한 통합을 포함하여 최신 버전의 필드 수준 암호화를 사용합니다.

특히 필드 암호화 엔터프라이즈 암호화 모듈을 활용하여 KMF 서버 측 암호화를 더 잘 제어할 수 있습니다. KMF 키 계층 구조 및 봉투 암호화를 사용하여 적절한 데이터 암호화 키 보호를 보장합니다. 인스턴스는 사용자가 구성하는 암호화 모듈을 통해 데이터를 암호화합니다. 각 모듈에 대한 액세스 정책을 만든 다음, 암호화 사양 및 액세스 정책을 구성하고 키 수명 주기 관리 제어를 제어할 수 있습니다.

필드 암호화 엔터프라이즈 다음을 기반으로 모듈 접근 정책을 지원합니다.

- 범위
- 역할
- 스크립트

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 자원 교환
- 시스템 사용자

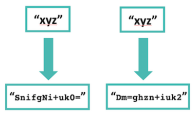
자세한 내용은 모듈 액세스 정책 생성 문서를 참조하십시오.

주: 의 필드 암호화 지원되는 기능과 권리를 업그레이드 및 구독 필드 암호화 엔터프라이즈 하는 방법에 대한 자세한 내용은 을 참조하십시오 암호화 및 키 관리 구독 번들.

암호화 용어

용어	설명
키 관리 	키 관리 지원 키 관리 프레임워크(KMF)의 기본입니다 필드 암호화 엔터프라이즈 . 다음과 같은 기능을 확보합니다. • 키 수명주기 관리. • 키 회전. 자세한 내용은 키 회전 문서를 참조하십시오. • FIPS 140-2-L3 HSM(하드웨어 보안 모듈)을 사용한 키 보호 및 키 생성. • 역할과 의무의 분리. • 프로덕션 및 비프로덕션 인스턴스와 같은 인스턴스 간에 데이터 암호화 키를 안전하게 전송합니다. • 키 래핑이 있는 CSK(고객 공급 키)입니다. • 비결정적 암호화. • 대량 암호화/암호 해독. • 키 액세스/사용에 대한 감사. 자세한 내용은 핵심 관리 프레임워크 참조 문서를 참조하십시오.
고객 제공 키 	고객 공급 키 지원 가장 필드 암호화 엔터프라이즈 큰 이점 중 하나는 암호화에 고유한 키를 사용할 수 있다는 것입니다. 관리자는 암호화를 위해 제공된 키 또는 자체 CSK(고객 제공 키)를 사용할 ServiceNow 수 있습니다 Now Platform®. 또한 키 수명주기를 관리하고 키의 해지, 교체 및 비활성화 시기를 결정할 수 있습니다. 고객이 제공한 키를 사용하도록 설정하고 암호화 모듈을 만든 후에는 토큰 및 공개 임시 키를 다운로드합니다. 토큰과 공개 키를 사용하여 키를 래핑한 다음 인스턴스에 업로드합니다. 고객 제공 키를 사용하려면 및 와 함께 고객 제공 키 사용 필드 암호화 엔터프라이즈 를 참조하십시오키 유형을 선택하도록 필드 암호화 설정 구성.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

용어	설명
필드 암호화 	필드 암호화와 첨부 파일 암호화 모두 지원 필드 암호화와 첨부 파일 암호화 모두 암호화 모듈을 활용하고 암호화된 필드 구성을 통해 정책을 액세스합니다. 암호화된 필드 구성 양식은 열 또는 첨부 파일 암호화의 암호화 유형을 선택하는 데 사용됩니다. 자세한 정보 및 지원되는 필드 유형은 을 참조하십시오 암호화된 필드 구성 설정 .
비결정적 암호화 	비결정적 암호화 지원 필드 암호화 엔터프라이즈 는 보안 강화를 위해 비결정적 암호화를 지원합니다. 시스템에서 동일한 데이터를 두 번 이상 암호화하는 경우 암호문은 매번 다릅니다. 비결정적 암호화는 CBC(Cipher Block Chaining)를 사용한 AES 암호화와 함께 사용할 수 있습니다. 암호화 사양의 알고리즘 정의 단계에서 동일성 유지 옵션을 통해 이 기능을 사용하도록 설정할 수 있습니다. 암호화 모듈에 대한 암호화 스펙을 작성하고 암호화 알고리즘을 정의하고 키를 생성하십시오. 암호화 작업에 사용되는 메커니즘을 정의하고 비결정적 암호화 사용에 대한 자세한 내용은 을 참조하십시오 암호화 모듈 생성 .
자원 교환 	자원 교환 필드 암호화 엔터프라이즈 기밀성, 무결성, 인증 및 부인 방지를 제공하기 위해 암호화 API를 사용하여 KMF 안전한 방식으로 인스턴스 간 키를 제공합니다. 자원 교환 는 KMF 안전한 방식으로 인스턴스 간에 자원을 교환할 수 있는 기능을 제공하는 기능입니다. 자세한 내용은 키 관리 프레임워크 자원 교환 문서를 참조하십시오.

주: 활성화 필드 암호화 엔터프라이즈하지 않기로 선택한 경우에도 를 사용할 필드 암호화수 있습니다. 자세한 내용은 다음을 참조하십시오 필드 암호화 탐색 .

필드 암호화 엔터프라이즈 는 온 프레미스 고객을 지원합니다. 도메인 분리를 지원하지 않습니다.

추가 모듈 및 모듈 접근 정책 지원

의 필드 암호화 표준 버전은 5개의 모듈과 MAP(모듈 액세스 정책)로 제한됩니다. 필드 암호화 엔터프라이즈 는 더 많은 수의 모듈과 MAP을 지원합니다.

지원되는 필드 정보

다음 필드 유형을 암호화할 수 있습니다.

- 첨부 파일
- 날짜
- 날짜/시간
- 이메일
- HTML

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 필기장
- 저널 입력
- 저널 목록
- 전화
- 문자열 텍스트
- 번역된 필드
- 번역된 HTML
- 번역된 텍스트
- URL

첨부 파일 암호화

기본적으로 첨부 파일 암호화

사용하는 필드 암호화 고객은 활성 EFC(암호화된 필드 구성) 유형이 *Attachment*인 테이블에서 기본적으로 암호화된 첨부 파일을 가지고 있습니다.

EFC 구성에 의해 정의된 이 기본 암호화는 관리자가 이러한 테이블에 대해 업로드 시 첨부 파일을 암호화해야 한다고 수동으로 선언할 필요가 없음을 의미합니다.

관리자는 사용자가 암호화되지 않은 파일을 첨부하지 못하도록 할 수 있습니다.

자세한 내용은 사용자가 암호화되지 않은 파일을 첨부하지 못하도록 방지 문서를 참조하십시오.

기본 암호화 옵트아웃

EFC 구성에 따라 기본적으로 암호화된 첨부 파일을 원하지 않는 경우 지원에 문의하여 ServiceNow 이 옵션을 옵트아웃할 수 있습니다.

이 기능을 옵트아웃하려면 지원을 사용하여 ServiceNow 지원 케이스를 생성하고 케이스 기록에 대한 설명에 다음 문장을 포함합니다.

`"#[## ##]#(#) ## ### ## #### ## ### ##### ### ## ##` ServiceNow `##, [## ##]# ######## ##### ## ## ###` ServiceNow `## # ### ### ## ### ##### ## #####."`

API 지원

필드 암호화 엔터프라이즈 는 `setDisplayValue()` 및 `setValue()` API를 업데이트하여 암호화된 필드에 암호화된 데이터를 삽입할 수 있도록 합니다. 또한 `getDisplayValue()` 및 `getValue()` 가 일반 텍스트 값을 반환할 수 있도록 합니다.

다음 스크립트는 인시던트 짧은 설명이 암호화된 경우 이러한 API 변경 내용을 보여줍니다.

```
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
```

`getValue()`를 사용하여 암호화된 텍스트를 가져올 때 스크립트는 더 이상 암호문을 반환하지 않습니다. 스크립트는 사용자가 암호화 모듈에 액세스할 수 있다고 가정하고 일반 텍스트를 반환합니다. `getValue()` 는 암호화 모듈에 액세스할 수 없는 사용자에 대한 암호문을 반환합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라우드 암호화 키 관리 포함

ServiceNow® 클라우드 암호화 향상된 키 관리와 함께 블록 암호화를 사용하여 데이터베이스에 암호화된 스토리지를 제공합니다. 클라우드 암호화 와 함께 사용할 수 있습니다. ServiceNow® Platform Encryption 구독 번들입니다.

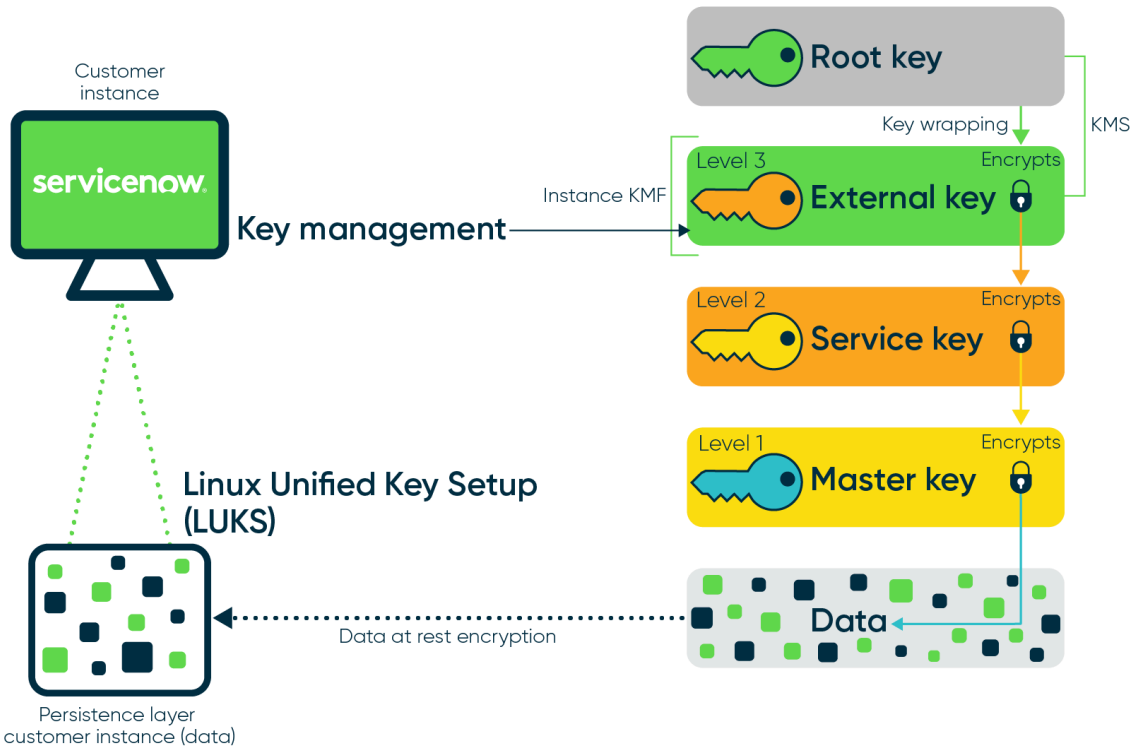
클라우드 암호화 제공:

- 직무 분리.
- 관리되는 키의 순환 ServiceNow .
- 고객 관리형 키 옵션.

> **주:** 조직에서 자체 암호화 도구 또는 라이브러리, 엔터프라이즈 키 관리 시스템 또는 HSM(하드웨어 보안 모듈)에서 생성된 키 자료를 사용하도록 요구하는 경우 이 옵션을 고려합니다. 자세한 내용은 키 관리 운영 문서를 참조하십시오.

다음 다이어그램에서는 작동 방식을 클라우드 암호화 보여 줍니다.

클라우드 암호화 개요



클라우드 암호화 키 관리 모듈은 다음 하위 모듈로 구성됩니다.

- 키 관리 운영:
  - 키 목록에 액세스합니다.
  - 키 전환 작업을 수행합니다.
  - 고객 관리형 키를 철회합니다.
- 키 관리 트랜잭션:

  사용된 키에 대해 발생한 모든 트랜잭션을 참조합니다.

  암호화에 고유한 고객 관리형 키를 사용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특정 상황에서는 고객 관리형 키를 사용할 때 키 철회 요청을 선택할 수 있습니다. 이렇게 하려면 Cloud Encryption 철회 및 재공급 선택적 추가 기능 SKU에 라이센스를 부여한 다음 팀 구성원이 키 철회 기능을 활성화하도록 요청해야 합니다 고객 서비스 및 지원 .

Quorum 제어 정책 설정 옵션은 철회 기능이 활성화되면 사용할 수 있게 되며, 그렇지 않으면 모듈이 메뉴에 표시되지 않습니다. 이 기능은 고객 관리형 키를 사용하는 경우에만 활성화할 수 있습니다. 이 정책을 사용하면 철회 기능이 활성화될 때 Quorum에 대한 설정을 구성할 수 있습니다. 이 기능에 대한 자세한 내용은 다음 문서를 참조하십시오 Quorum 통제 정책.

클라우드 암호화 는 MariaDB 및 RaptorDB 데이터베이스에 대한 프로덕션 및 비프로덕션 인스턴스를 지원합니다. 클라우드 암호화는 상용 클라우드, GCC(정부 고객 클라우드) 포드 101 및 ServiceNow SPP-AU(Protected Platform – Australia)ServiceNow에서 지원됩니다.

라이선싱 및 사용 클라우드 암호화

라이선싱 클라우드 암호화에 대한 자세한 내용은 문서를 참조하십시오 암호화 및 키 관리 구독 번들.

새 인스턴스가 있는 라이센스 고객의 경우, 새 인스턴스 프로비저닝에 포함됩니다 클라우드 암호화.

기존 인스턴스가 있는 라이센스 고객이 인스턴스 이동을 클라우드 암호화요청하려면 KB1117369 의 지침을 따르십시오. 인스턴스에서 클라우드 암호화를 사용하도록 서비스 카탈로그 항목을 요청하려면 고객 관리자 또는 파트너 관리자 역할이 있어야 합니다. 이 기능을 사용하려면 1시간의 유지 관리 기간이 필요합니다.

클라우드 암호화 **UI**

클라우드 암호화가 활성화되면 이 사용자에게 sn_kmf.admin 역할이 있으면 security_admin 사용자에게 클라우드 암호화 사용자 인터페이스(UI)가 표시됩니다.

탐색 모음에서 클라우드 암호화 키 관리를 검색하여 클라우드 암호화 UI에 액세스하려면 다음을 수행합니다. 활성 키의 상세 정보, 인스턴스에 클라우드 암호화가 활성화되어 있는지 여부와 같은 암호화 키에 대한 정보를 보려면 키 관리 운영 섹션으로 이동합니다.

키 관리 운영

키 관리 운영 서브모듈은 와 함께 ServiceNow 클라우드 암호화사용되는 모든 암호화 키를 보고 관리할 수 있는 액세스 권한을 제공합니다.

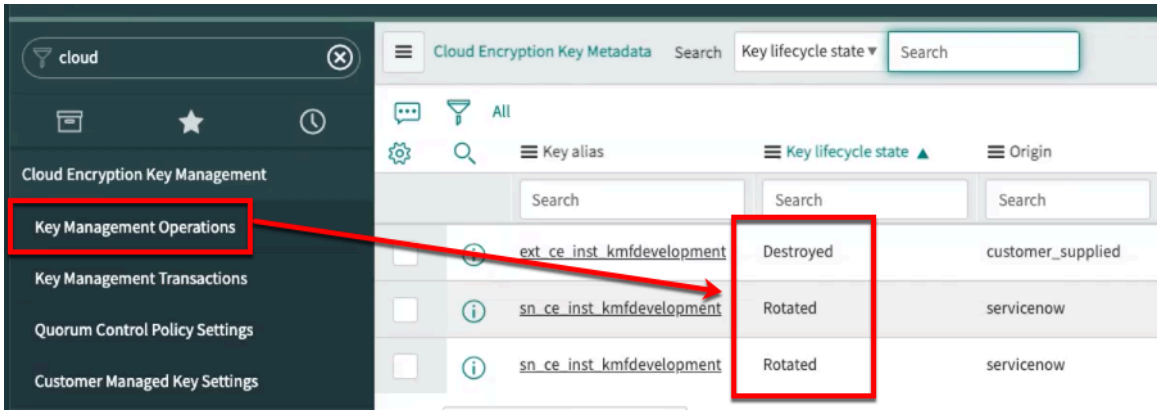
클라우드 암호화 시작하기

주요 수명주기 상태

시스템에는 지정된 시간에 하나의 활성 키만 있습니다. 키를 선택할 때 선택한 키에 대한 활동(예: 회전 또는 철회된 키 및 해당 타임스탬프)에 액세스합니다.

수행된 키 관리 작업에 따라 키 수명주기 상태가 업데이트됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



자세한 내용은 또는 고객 관리 키 교대 문서를 참조하십시오ServiceNow 관리 키 교체.

주: 키 회전 프로세스를 완료하는 데 최대 20분이 걸릴 수 있습니다.

ServiceNow 관리 키 교체

활성 클라우드 암호화 ServiceNow 관리 키를 회전합니다.

시작하기 전에
필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

중요사항: 고객 관리형 키를 사용하는 경우 다음을 참조하세요 고객 관리 키 교대.

프로시저

1. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 키 관리 운영.
   클라우드 암호화 키 메타데이터 목록이 로드됩니다. 인스턴스에 사용된 모든 키가 나열됩니다. 지정된 시간에 하나의 키만 활성화할 수 있습니다.

   모듈에 처음 액세스하는 클라우드 암호화 경우 초기 키 회전이 수행된 후 키 항목을 사용할 수 있습니다. ServiceNow 관리되는 키는 시스템의 기본값입니다.

2. 테이블에서 활성 키를 선택합니다.
   생성된 키에 대한 ServiceNow 일반 정보가 키 정의 테이블에 표시됩니다.
3. 키 회전 버튼을 선택합니다.
   키 회전을 계속하거나 작업을 취소하는 옵션이 포함된 알림이 표시됩니다.
4. 확인을 선택하여 키를 회전합니다.
   키 정의 페이지 상단에 확인 메시지가 표시됩니다.
5. 키 관리 작업 화면으로 돌아가 키 메타데이터 테이블을 새로 고치십시오 클라우드 암호화 .
   현재 활성 키와 현재 활성 키 대신 회전하기 위해 생성되는 키에 대한 항목이 나열됩니다. 사용 가능한 다른 상태를 확인합니다 핵심 관리 프레임워크 주요 수명주기 상태 .

   활성 키는 키 버전이 `0`으로 나열되고 생성된 키의 버전은 `1`입니다.

6. 키 관리 트랜잭션을 보려면 원래 키에 대한 항목을 엽니다.
   자세한 내용은 문서를 참조하십시오 키 관리 트랜잭션 .
   이전에 활성 키인 버전 `0`은 키 수명 주기 상태인 `Rotated`로 업데이트되었으며 새 키인 버전 `1`은 `Active`입니다.

고객 관리 키 준비

다음 단계에 따라 고객 관리 키를 인스턴스에 업로드할 준비를 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

이 태스크 정보
고객 관리형 키의 경우 암호화 라이브러리 또는 HSM을 사용하여 키를 생성할 수 있습니다. 이 키는 AES 256비트 키여야 하며 RSAES_OAEP_SHA_256 암호화 스키마가 있는 클라우드 암호화 래핑 인증서로 래핑되어야 합니다.

주:

OpenSSL 암호화 도구를 사용하여 키를 생성하도록 선택하는 경우 OpenSSL 버전은 버전 1.1.1x 이상이어야 합니다.

를 사용하여 Windows고객 관리형 키를 만들고 래핑하는 경우 Git Bash와 같은 Bash 셸 지원 애플리케이션을 통해 래핑된 키를 생성해야 합니다.

프로시저

1. OpenSSL을 사용하여 AES-256비트 대칭 키로 사용할 임의의 값을 생성합니다.

   예를 들어 openSSL을 사용하여 `openssl rand 32` 명령을 사용하여 이 키를 생성할 수 있습니다.

   호환성을 위해 대칭 키에는 다음과 같은 특성이 있어야 합니다.

속성	값
키 유형	AES(Advanced Encryption Standard) 알고리즘 기반 대칭 키.
키 크기	256비트(32바이트)
키 래핑 요구 사항	◦ RSA 암호화 알고리즘 ◦ OAEP(최적 비대칭 암호화 패딩) ◦ SHA-256 해시 함수(RSAES_OAEP_SHA_256) ◦ Base64 알고리즘을 사용하여 인코딩

2. 키를 파일에 저장합니다.
   예를 들어, `openSSL ## openssl rand 32 > plaintext_key.bin` 는 32바이트 키를 생성하여 `plaintext_key.bin`라는 파일에 저장합니다.

   중요사항: 나중에 참조할 수 있도록 이 파일을 안전하게 저장합니다. 이 키는 업로드할 공개 키로 래핑됩니다.

3. 인스턴스에서 다운로드한 래핑 인증서 파일에서 공개 키를 추출합니다.

```
openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
```

   주: 래핑 인증서를 다운로드하는 방법은 을 참조하십시오.

4. RSAES_OAEP_SHA_256 알고리즘을 사용하여 래핑 인증서와 함께 다운로드한 공개 키로 생성된 키를 래핑합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
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
```

이 명령에 지정된 파일에는 CMK 프로세스에 대해 SN에 제공할 수 있는 래핑된 고객 관리형 키가 포함되어 있습니다.

ServiceNow 키와 고객 관리형 키 간 전환

에서 사용할 ServiceNow 클라우드 암호화고객 관리형 키 또는 ServiceNow 관리형 키 간에 전환합니다.

기본적으로 인스턴스는 관리형 키를 ServiceNow 사용하도록 ServiceNow 구성되며 암호화 키 생성이 활성화됩니다. 그러나 관리자는 고객 관리형 키를 사용하도록 선택할 수 있습니다. 관리되는 키로 ServiceNow 돌아가도록 선택할 수도 있습니다.

고객 관리 키 교대

에 대한 클라우드 암호화고객 관리 키를 래핑한 후 고객 관리 키를 인스턴스로 회전합니다.

시작하기 전에
필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

프로시저

1. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 키 관리 운영.
   클라우드 암호화 키 메타데이터 목록이 로드됩니다. 인스턴스에서 사용된 모든 키가 나열됩니다.
2. 클라우드 암호화 키 메타데이터 목록에서 활성 키에 대한 기록을 엽니다.
   키가 여러 개인 경우 키 수명 주기 상태가##인 키를 선택합니다. 인스턴스에 활성 키가 하나만 있습니다.
3. 키 정의 기록에서 키 회전 버튼을 선택합니다.
4. 고객 관리 키 업로드 창에서 나열된 단계를 수행합니다.

   a. 래핑 인증서 다운로드를 선택합니다.
   *public_certificate.... zip*은 로컬 머신에 다운로드되고 고객 관리 키를 래핑하는 데 사용됩니다.

   ⚠ 경고: 고객 관리 키로 전환하거나 전환할 때마다 래핑 인증서를 다운로드하여 잠재적인 인증서 관련 문제를 방지합니다.

   b. 찾아보기를 선택하여 고객 관리 키를 업로드한 다음, 래핑된 암호화 키를 찾아 선택합니다.
   다른 파일을 선택하려면 파일을 선택하고 제거를 선택합니다.

   c. 첨부 파일 창을 닫습니다.

   d. 확인을 선택하여 키를 업로드합니다.
   키가 올바른 형식이면 확인 메시지가 나타나고, 그렇지 않으면 오류 메시지가 표시됩니다. 키 파일은 키 정의 기록에 첨부됩니다.

   키 관리 트랜잭션 테이블에 인증서 다운로드 및 키 업로드 단계가 나열됩니다. 요청 단계에 대한 자세한 내용은 을 참조하십시오 키 관리 트랜잭션 .

5. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 키 관리 운영 키 목록을 보려면
   키 목록에서 고객 관리형 키에 대한 새 레코드를 볼 수 있습니다. 이 새 키의 **Origin** 값은 **customer_supplied** 이며 활성 상태입니다. 이전 키가 회전됨 상태입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

고객 관리 키로 전환

에 대해 ServiceNow 클라우드 암호화고객 관리 키를 사용합니다.

시작하기 전에
필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

고객 관리 키로 전환하려면 이러한 단계의 일부로 업로드할 래핑된 고객 관리 키가 준비되어야 합니다. 업로드를 위해 이 키를 준비하는 방법에 대한 자세한 내용은 을 참조하십시오 고객 관리 키 준비. 키를 업로드한 후 이 프로세스는 새 키에 대한 키 회전을 시작합니다.

프로시저

1. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 키 관리 운영.
2. 클라우드 암호화 키 메타데이터 목록에서 활성 키에 대한 기록을 엽니다.
   키가 여러 개인 경우 키 수명 주기 상태가##인 키를 선택합니다. 인스턴스에 활성 키가 하나만 있습니다.
3. 양식의 관련 링크 섹션에서 고객 관리 키로 전환 링크를 선택합니다.
4. 고객 관리형 키로 전환 대화 상자에서 관리형 키 업로드 버튼을 선택합니다.
5. 고객 관리 키 업로드 대화 상자에서 나열된 단계를 수행합니다.

   a. 래핑 인증서 다운로드를 선택합니다.

   ⚠ 경고: 고객 관리 키로 전환하거나 전환할 때마다 래핑 인증서를 다운로드하여 잠재적인 인증서 관련 문제를 방지합니다.

   b. 찾아보기를 선택하고 프롬프트에 따라 디바이스에서 키를 선택하고 업로드합니다.

   c. 고객 관리 키로 전환을 선택합니다.

   고객 관리 키로 전환하기 위한 요청이 인스턴스에서 생성됩니다. 현재 양식에서는 원래 활성 키의 키 수명 주기 상태가회전됨으로 변경된 것을 볼 수 있습니다.
6. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 키 관리 운영 키 목록을 보려면
   키 목록에서 고객 관리형 키에 대한 새 레코드를 볼 수 있습니다. 이 새 키의 **Origin** 값은 **customer_supplied** 이며 활성 상태입니다.

결과
이제 인스턴스가 에 대해 ServiceNow 클라우드 암호화고객 관리형 키를 사용합니다.

ⓘ 중요사항: 키 관리 작업을 위해 암호화 키의 복사본을 항상 안전한 위치에 사용할 수 있는지 확인합니다. 이 키가 없으면 인스턴스에 액세스할 수 없게 될 수 있습니다.

ServiceNow 관리 키로 전환

고객 관리 키를 에 대한 ServiceNow 클라우드 암호화관리 키로 다시 전환합니다.

시작하기 전에
필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

프로시저

1. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 키 관리 운영.
2. 클라우드 암호화 키 메타데이터 목록에서 활성 키에 대한 기록을 엽니다.
   키가 여러 개인 경우 키 수명 주기 상태가##인 키를 선택합니다. 인스턴스에 활성 키가 하나만 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 양식의 관련 링크 섹션에서 **ServiceNow** 관리 키로 전환 링크를 선택합니다.
4. **ServiceNow** 관리 키로 전환 대화 상자에서 **ServiceNow** 관리 키로 전환 버튼을 선택합니다.
   인스턴스에서 관리 키로 전환 ServiceNow 하라는 요청을 생성합니다. 현재 양식에서는 원래 활성 키의 키 수명 주기 상태가회전됨으로 변경된 것을 볼 수 있습니다.
5. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 키 관리 운영 키 목록을 보려면
   키 목록에서 관리되는 키에 대한 ServiceNow 새 레코드가 있는 것을 볼 수 있습니다. 이 새 키는 **ServiceNow**의 **Origin** 값을 가지며 활성 상태입니다.

키 회전 예약

관리형 키의 자동 회전 ServiceNow 일정을 설정합니다. 이 프로세스는 암호화 키를 자동으로 폐기하고 이전 키를 새로 생성된 암호화 키로 대체합니다. 고객 관리형 키를 사용하는 경우 이 일정은 사용자 지정 키를 수동으로 교체하라는 미리 알림을 제공할 수 있습니다.

시작하기 전에

필요한 역할: sn_kmf.admin

프로시저

1. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 일정이 예약된 키 전환 설정.
2. 일정이 예약된 키 전환 활성화 확인란을 선택합니다.
3. 비즈니스 요구에 따라 나머지 필드를 채웁니다.

일정이 예약된 키 전환 설정

필드	설명
키 전환 사이의 개월 수(최대 60개월)	키 전환 사이의 개월 수입니다. 이 값은 기본적으로 `12` 이며 최대 `60` 개월까지 지정할 수 있습니다.
키 전환을 수행할 요일	키 회전이 수행되는 요일입니다.
키 전환을 수행할 일의 시간	키 회전이 수행되는 시간입니다.
다음 키 전환의 날짜 및 시간	다음으로 예약된 키 전환의 날짜 및 시간입니다. 이 값은 직접 편집할 수 없으며 선택 사항에 따라 자동으로 계산됩니다.
미리 알림을 보낼 키 전환 전 일 수(최대 15일)	인스턴스에서 알림을 보내는 키 교체 날짜 이전의 일 수입니다.
승인된 보안 관리자 목록으로 이메일 알림이 전송됩니다	키 회전에 대한 알림을 수신하는 사용자의 목록입니다. 기본적으로 시스템 관리자는 이 목록에 있습니다.

4. 제출을 선택합니다.
   제출을 선택하면 양식 상단에서 알림을 볼 수 있습니다. 알림은 키 회전 및 알림 일정을 확인합니다.

⚠ 경고:

예약된 각 키 회전에는 고유한 서명이 있어 작업의 무결성을 보장하고 무단 수정을 감지합니다. 예약된 작업의 서명은 각 인스턴스에서 고유합니다. 소스 인스턴스 A에서 대상 인스턴스 B로 예약된 키 회전 작업을 복제하는 경우 인스턴스 B의 예약된 작업은 서명 확인에 실패합니다. 이 경우 예약된 키 회전 사용 확인란을 선택 취소한 다음 다시 선택하여 서명을 다시 만들 수 있습니다. 이 문제에 대한 자세한 내용은 KB1247113 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

고객 관리 키 철회

고객 관리 키 철회 기능이 활성화되면 키 관리 작업 페이지에서 철회 작업을 사용할 수 있게 됩니다. 키 철회 및 쿼럼 승인 작업도 관리할 수 있습니다.

시작하기 전에

필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

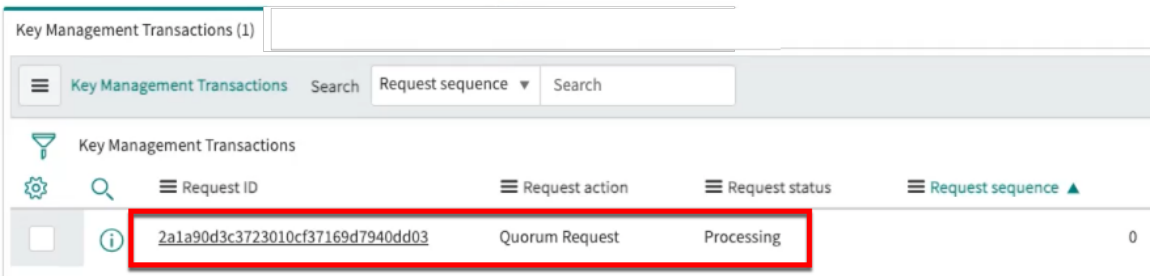
이 섹션은 에 대한 클라우드 암호화선택적 추가 기능인 Cloud Encryption 철회 및 재공급에 라이센스를 부여한 경우에만 적용됩니다.

프로시저

1. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > > 키 관리 운영.
2. 테이블에서 활성 고객 관리 키를 선택합니다.
   키 정의 테이블에 고객 키에 대한 일반 정보가 표시됩니다. 이제 철회 키 기능을 사용할 수 있습니다.
3. 철회 키를 선택하여 철회 프로세스를 트리거합니다.

> ⚠ 경고:
>
> 키 철회 경고 메시지가 표시됩니다. 키를 철회하면 철회된 키로 재개 작업이 수행될 때까지 인스턴스 종료가 트리거됩니다.
>
> 위험: 철회된 것과 동일한 키로만 복원 작업을 수행할 수 있습니다. 다른 키로 회전하려면 철회된 키를 복원한 후에 회전해야 합니다.
>
> 철회된 고객 관리 키가 백업을 보존하는 ServiceNow 기간 내에 복원되지 않으면 (자세한 내용은 백업 및 복원 SOP〔표준 운영 절차〕 참조) 인스턴스 데이터베이스 백업에 더 이상 액세스할 수 없습니다. 이러한 방식으로 손실된 백업 데이터는 복구할 수 없습니다.

4. 확인을 선택하여 키를 철회합니다.
   키 철회 기능에 대해 의심이 가는 경우 취소 를 선택합니다.
   키 정의 화면으로 돌아가고 확인 메시지가 표시됩니다.
5. 키 정의 페이지를 새로 고쳐 보류 중인 출금 요청을 확인합니다.



Quorum 통제 정책이 활성화된 경우 승인 워크플로우를 성공적으로 완료하여 키 철회를 완료해야 합니다. 자세한 내용은 Quorum 통제 관리 문서를 참조하십시오.

고객 관리 키 재공급

키 철회 작업이 완료된 후에는 고객 관리 키를 인스턴스에 다시 공급해야 합니다.

시작하기 전에

필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

> ⓘ 주: 이 섹션은 Cloud Encryption 철회 및 재공급에 라이선스를 부여한 경우에만 적용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 Now Support 이동하여 다음으로 이동합니다. 서비스 카탈로그 > 카탈로그 > 인스턴스 관리 > 인스턴스 복원 - 관리형 키 재공급.
2. 요청을 클릭합니다.
3. 인스턴스 복원 - 관리 키 재공급 창의 인스턴스 선택 드롭다운에서 인스턴스를 선택합니다.
4. 래핑 인증서 텍스트를 클릭하여 래핑 인증서를 다운로드합니다.

   ⚠ 경고: 고객 관리 키를 회전하거나 업로드할 때마다 새 래핑 인증서를 다운로드해야 합니다.

5. 업로드할 키를 준비합니다.
   이 프로세스에 대한 자세한 내용은 고객 관리 키 준비 문서를 참조하십시오.
6. 4단계 섹션에서 찾아보기 및 업로드를 클릭하여 로컬 디바이스에서 래핑된 키를 업로드합니다.
   키가 업로드되면 아래 파일이 성공적으로 업로드됨에서 키를 볼 수 있습니다. 키를 다시 업로드해야 하는 경우 파일 제거 를 클릭하고 이전 단계에서 설명한 대로 키를 다시 업로드합니다.
7. 키 회전을 클릭하여 재보급을 완료합니다.

Quorum 통제 정책

Quorum 통제 정책은 고객 관리형 키 철회를 위한 Quorum에 도달하기 위해 선택한 총 승인자 수 중에서 필요한 최소 승인 수를 지정합니다.

⚠ 경고: 키 철회 기능을 활성화하려면 법적 부록에 서명해야 합니다. Quorum Control Policy Settings(쿼럼 제어 정책 설정) 옵션은 철회 기능이 활성화되면 사용할 수 있게 되며, 그렇지 않으면 모듈이 앱 메뉴에 표시되지 않습니다. 키가 철회된 후에는 암호화 키가 다시 공급되고 다시 활성화될 때까지 인스턴스를 더 이상 사용할 수 없습니다.

특정 상황에서는 키 철회를 생성할 수 있습니다. 먼저 에서 키 철회 기능을 고객 서비스 및 지원요청해야 합니다.

Quorum 통제 정책은 고객 관리형 키 철회를 위한 Quorum에 도달하기 위해 선택한 총 승인자 수 중에서 필요한 최소 승인 수를 지정합니다. 예를 들어 총 5명의 승인자가 있지만 쿼럼에 도달하려면 4명의 승인만 필요합니다. 4개의 승인을 받으면 출금 요청이 처리되고 키가 철회됩니다.

Quorum 승인이 활성화된 그룹에서 철회 작업이 수행될 때마다 Quorum 승인을 위한 워크플로가 트리거됩니다. 승인을 허용할 수 있는 모든 사용자에게 이메일 알림이 전송됩니다. 승인자의 계정에서도 작업이 생성되어 승인자가 계정에 ServiceNow 로그인할 때 대시보드에 작업이 표시됩니다.

사용자는 인스턴스, 이메일 또는 키 관리 운영 페이지에서 승인을 부여할 수 있습니다. 키 철회 작업은 쿼럼이 충족될 때까지 차단됩니다.

최소 승인자 수에 도달하면 Quorum에 도달하고 키 철회가 트리거됩니다. 철회가 수행되고 요청을 승인한 사용자의 이름을 포함하여 기록됩니다.

설정 세부 정보는 을 참조하십시오 Quorum 통제 정책 설정 구성 .

Quorum 통제 정책 설정 구성

다음 단계에 따라 Quorum 제어 정책 설정을 구성합니다.

시작하기 전에
필요한 역할: sn_kmf.admin

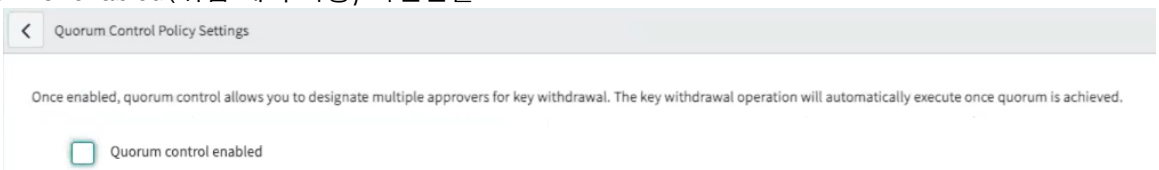
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

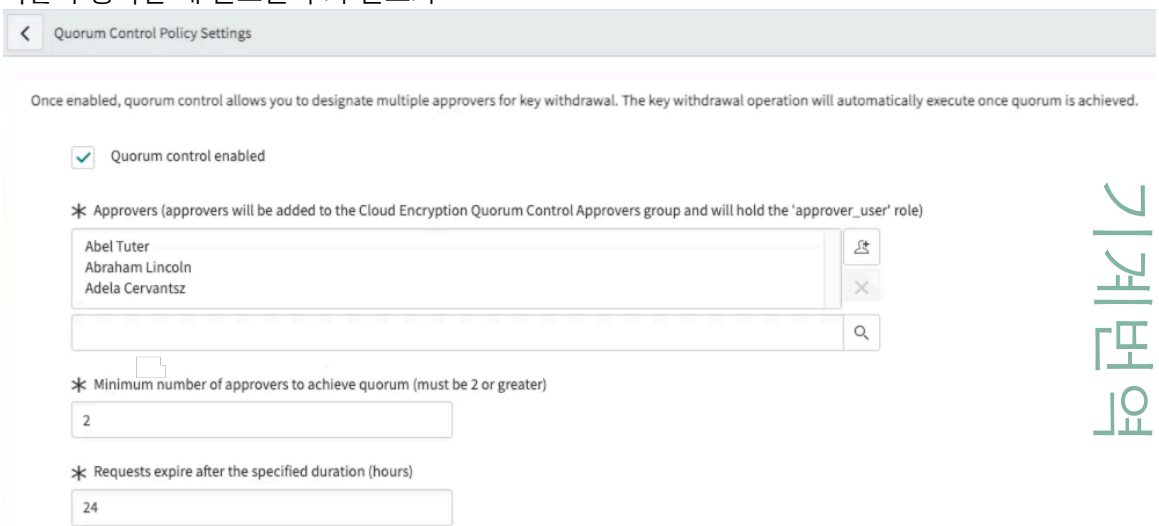
⚠ 경고: 키 철회 기능을 활성화하려면 법적 부록에 서명해야 합니다. Quorum Control Policy Settings(쿼럼 제어 정책 설정) 옵션은 철회 기능이 활성화되면 사용할 수 있게 되며, 그렇지 않으면 모듈이 앱 메뉴에 표시되지 않습니다. 키가 철회되면 암호화 키가 다시 활성화될 때까지 인스턴스를 더 이상 사용할 수 없습니다.

프로시저

1. 에서 고객 서비스 및 지원키 철회 기능을 요청합니다.
2. 다음으로 이동 클라우드 암호화 키 관리 > **Quorum** 통제 정책 설정.
3. **Quorum control** enabled(쿼럼 제어 사용) 확인란을



선택합니다.
Quorum 제어를 구성하는 데 필요한 추가 필드가



나타납니다.

4. 필드를 채워 양식을 작성합니다.

필드	설명
승인자	사용자 목록에서 쿼럼의 구성원을 지정합니다. 잠금 아이콘 사용자 디렉터리를 엽니다. 선택할 수 있는 승인자 수에는 제한이 없습니다.
Quorum을 달성하기 위한 최소 승인자 수	Quorum을 달성하는 데 필요한 최소 승인자 수를 지정합니다. 예를 들어 9명의 승인자가 선택된 경우 Quorum에 최소 5명을 구성할 수 있습니다. 시스템에서 5개의 승인을 받으면 Quorum에 도달하고 철회 작업이 시작됩니다. ⓘ 주: 필요한 승인자의 최소 수는 2명입니다.
요청은 지정된 기간(시간) 후에 만료됩니다.	획득할 최소 승인 수에 대해 할당된 최대 시간 값인 숫자 값을 시간 단위로 설정합니다. 기간이 만료되면 Quorum 요청도 만료됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	철회 요청을 계속하려면 새 Quorum 요청이 필요합니다.

5. 제출을 클릭합니다.
   확인 메시지가 표시됩니다.

다음에 수행할 작업
철회 작업은 에서 사용할 수 있습니다 키 관리 운영.

Quorum 통제 관리

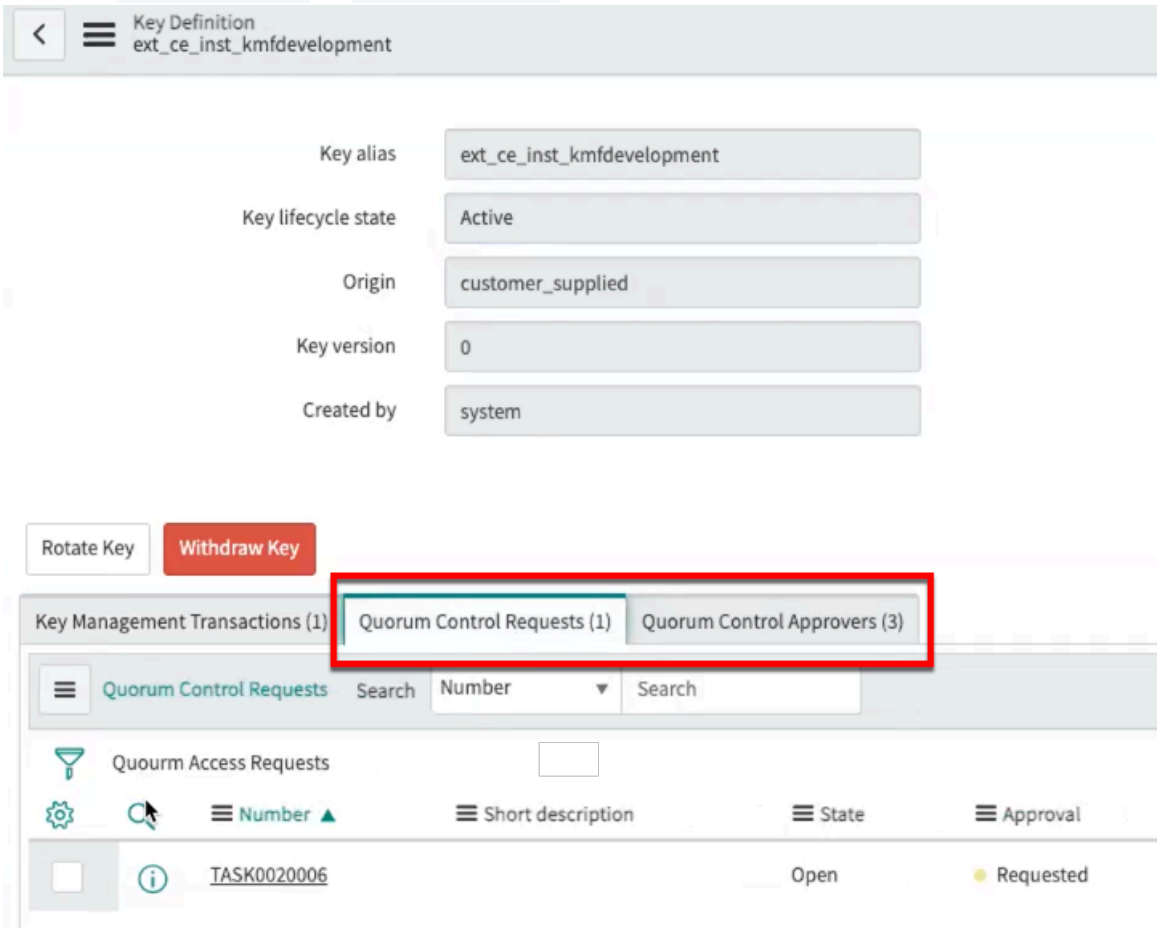
철회 작업 워크플로우가 트리거된 후 키 관리 작업 페이지에서 쿼럼 작업을 관리할 수 있습니다. 키 철회 작업은 쿼럼이 충족될 때까지 차단됩니다.

시작하기 전에
필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

Quorum이 승인 또는 거부되면 키 철회 요청자는 Quorum이 달성되었는지 또는 거부되었는지 여부를 알리는 이메일을 받게 됩니다.

프로시저

1. 에 키 관리 운영있는 고객 관리 키를 철회하는 단계를 수행합니다.
2. 활성화된 *Quorum ## ##*및 *Quorum ## ###*탭을 봅니다.

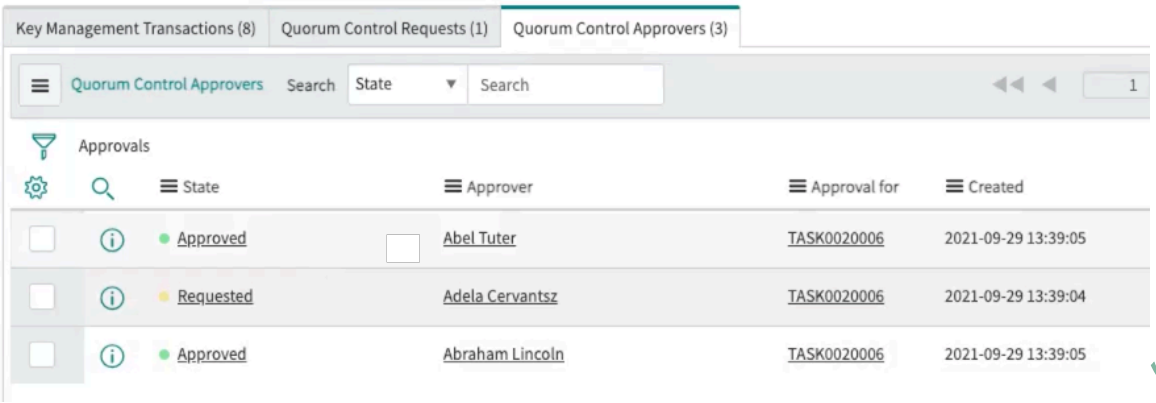


3. 열기 **Quorum** 통제 요청 생성된 실제 요청을 볼 수 있는 탭입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 상태:
  - 열림: 키 철회 작업이 충족되는 쿼럼을 보류 중입니다.
  - 완료 종결: Quorum이 충족되었으며 이 특정 Quorum 요청에 대해 추가 작업을 수행할 수 없습니다.
- 승인:
  - 요청됨: 승인 이메일이 전송되었으며 워크플로우가 Quorum에 도달하도록 트리거되었습니다.
  - 승인됨: 키가 철회되고 인스턴스가 종료됩니다.
  - 거부됨: Quorum 요청이 취소되고 이 요청에 대해 추가 작업이 수행되지 않습니다. 키를 인출하려면 새 인출 요청이 필요합니다.

4. Quorum 제어 승인자 탭을 열어 승인자 목록과 승인 요청 상태를 봅니다.



상태:

- 요청됨: 승인자가 승인 요청에 대한 작업을 아직 수행하지 않았습니다.
- 승인됨: 이메일 또는 승인 페이지에서 요청이 승인되었습니다.

5. 키 철회 요청 단계의 진행률을 보려면 키 관리 트랜잭션 탭을 선택합니다.
   - 0단계 - 쿼럼 요청: 실제 쿼럼 요청입니다. 키 철회 단계를 트리거하려면 Quorum 요청을 완료해야 합니다.
   - 1단계 - 키 철회: 키 철회 단계입니다. 이것은 2단계부터 7단계까지 구성됩니다.
   - 2단계 - Request_preparation: 래핑 및 회전을 트리거하는 요청을 생성합니다.
   - 3단계 - request_integrity_check: 요청이 합법적이고 안전한지 확인합니다.
   - 4단계 - request_validation: 진행 중인 요청이 있는지 확인합니다. 한 번에 하나의 교대 요청만 처리할 수 있습니다.
   - 5단계 - hsm_key_delete: KeySecure를 호출하여 활성 키를 삭제합니다.
   - 6단계 - key_metadata_withdraw: 활성 키 메타데이터 수명 주기 상태를 "제거됨"으로 변환합니다.
   - 7단계 - post_withdraw: 인스턴스를 종료하기 위해 호출합니다.

Quorum 통제 요청 승인 또는 거부

키 관리 트랜잭션의 Quorum 통제 요청을 승인하거나 거부합니다.

이 태스크 정보

Quorum 요청이 작성되면 구성원의 최소 승인 수가 필요합니다. 철회 작업 워크플로우가 트리거된 후 여러 가지 방법을 사용하여 쿼럼 작업을 관리할 수 있습니다. 사용자는 키 관리 운영 페이지, 인스턴스의 내 승인 또는 요청 이메일에서 직접 승인을 부여할 수 있습니다. 키 철회 작업은 쿼럼이 충족될 때까지 차단됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 절차에서는 키 관리 작업 페이지에서 쿼럼 요청을 승인하거나 거부하는 방법을 설명합니다.

시작하기 전에
필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

프로시저

1. 다음으로 이동 모두 > 클라우드 암호화 키 관리 > 키 관리 트랜잭션 > **Quorum** 통제 승인자.
2. 테이블에서 사용자 이름을 선택합니다.
3. 요청을 승인하거나 거부합니다.

Quorum 요청 승인 또는 거부

Quorum 요청이 작성되면 구성원의 최소 승인 수가 필요합니다. 철회 작업 워크플로우가 트리거된 후 여러 가지 방법을 사용하여 쿼럼 작업을 관리할 수 있습니다. 사용자는 키 관리 운영 페이지, 인스턴스의 내 승인 또는 요청 이메일에서 직접 승인을 부여할 수 있습니다. 키 철회 작업은 쿼럼이 충족될 때까지 차단됩니다.

시작하기 전에
필요한 역할: sn_kmf.admin 또는 sn_kmf.cryptographic_manager

키 관리 트랜잭션

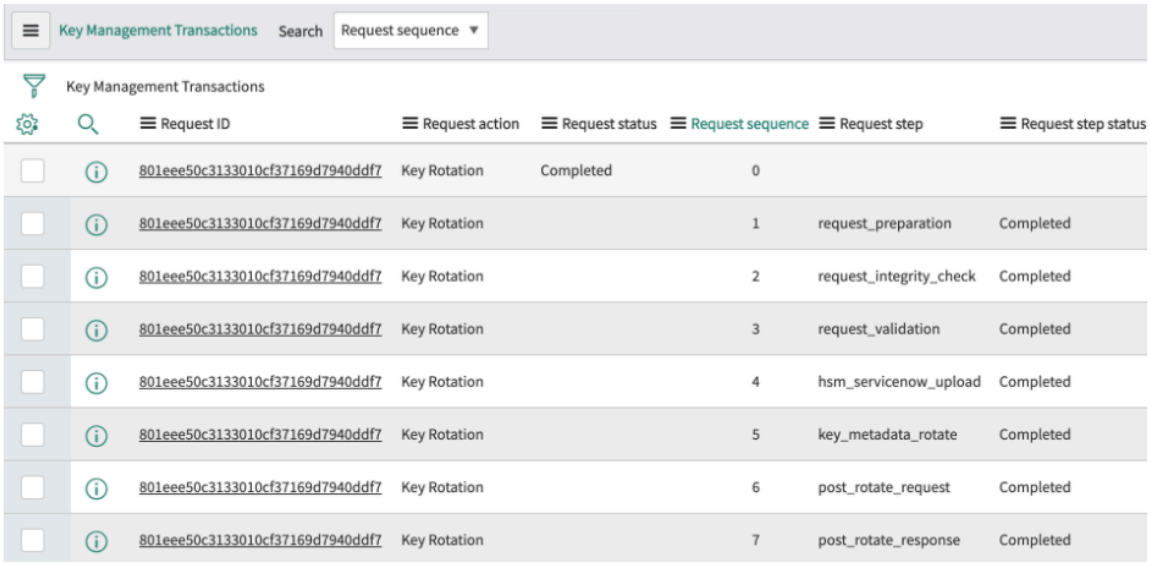
키 관리 트랜잭션 하위 모듈에는 인스턴스의 키에 ServiceNow 대해 발생한 모든 트랜잭션이 표시됩니다.

- 키 트랜잭션은 다음과 같이 정의됩니다.
  - 여러 요청 단계로 구성됩니다.
  - 단일 `## ID`가 모든 요청 단계에서 공유됩니다.
  - 트랜잭션의 초기 단계인 요청 시퀀스 0은 전체 트랜잭션의 현재 상태를 제공합니다.

    아래 이미지에서 볼 수 있듯이 초기 단계 0의 전체 `## ###`완료됨입니다.
- 개별 요청 단계에서 트랜잭션에 대해 다음 항목을 식별할 수 있습니다.
  - 트랜잭션의 각 단계 순서는 단계의 시퀀스 번호로 식별할 수 있습니다.
  - 각 트랜잭션의 상태는 요청 단계의 상태를 통해 볼 수 있습니다.
  - 초기 단계 이후의 단계가 하나라도 실패하면 전체 트랜잭션의 상태가 실패가 됩니다. 모든 단계가 완료되면 트랜잭션 상태도 완료됩니다.

다음 화면은 키 회전과 함께 표시되는 정보 유형의 샘플입니다 ServiceNow .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다음 테이블에는 주요 관리 트랜잭션 페이지에서 사용할 수 있는 필드 정보가 나와 있습니다.

키 관리 트랜잭션

필드	설명
요청 ID	수행 중인 작업에 대해 시스템에서 생성한 고유 ID 하나의 요청 ID가 모든 요청 단계에서 공유됩니다.
요청 작업	수행 중인 키 조작에 대한 작업을 표시합니다.
요청 상태	• 처리 중: 요청을 입력했지만 아직 완료되지 않았습니다. • 완료됨: 요청이 성공적으로 완료되었습니다. • 실패: 문제가 발생하여 프로세스가 완료되지 않았습니다. 주: 실패가 발생한 요청 번호를 연락하여 고객 서비스 및 지원 제공합니다.
키 별칭	영숫자 항목입니다.
주요 수명주기 상태	자세한 내용은 정의를 참조하십시오 핵심 관리 프레임워크 주요 수명주기 상태 .
원본	• ServiceNow 열쇠 • 고객 관리형 키
키 버전	키가 회전하면 버전 번호가 증가합니다.
요청 시퀀스	시스템에서 요청이 처리되는 순서를 표시합니다.
요청 단계	키 전환 중에 시스템에서 단계가 처리되고 있는지 여부를 표시합니다. 단계의 수와 내용은 수행된 키 작업의 유형에 따라 달라집니다. **1.** request_preparation: 래핑 및 회전을 트리거할 요청을 작성합니다. **2.** request_integrity_check: 요청이 합법적이고 안전한지 확인합니다. **3.** request_validation: 진행 중인 요청이 있는지 확인합니다. 한 번에 하나의 교대 요청만 처리할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 관리 트랜잭션

필드	설명
	4. attachment_process: 첨부 파일에서 래핑된 키 구성 요소를 추출합니다. (고객 관리 키를 회전하는 경우의 추가 단계) **5.** hsm_<key type>_upload: 래핑된 키 구성 요소를 HSM, KeySecure에 업로드합니다. **6.** key_metadata_rotate: 새 키 메타데이터를 작성합니다. **7.** post_rotate_request: 키 회전을 수행하는 요청을 보냅니다. **8.** post_rotate_response: 고객 인스턴스에서 요청에 따라 키 회전을 수행하는 응답입니다. 주: 요청 단계가 완료되지 않은 경우 상태 진행률을 분석하기 위해 고객 서비스 및 지원 요청 단계를 제공합니다.
요청 단계 상태	• 완료됨: 교대가 성공했습니다. • 실패: 교대가 성공하지 못했습니다. 주: 요청 단계가 완료되지 않은 경우 상태 진행률을 분석하기 위해 고객 서비스 및 지원 요청 단계를 제공합니다.

클라우드 암호화 로깅

에 대한 클라우드 암호화로깅 옵션에 대해 알아봅니다.

클라우드 암호화 로깅 테이블

이러한 테이블을 사용하여 인스턴스에서 클라우드 암호화 트랜잭션과 관련된 로깅 정보를 찾습니다.

테이블	설명
클라우드 암호화 메타데이터 [dare_key_metadata]	클라우드 암호화 메타데이터는 주요 수명주기 관리 메타데이터를 캡처합니다. 이 테이블에서 주요 수명주기, 상태 및 버전 정보를 찾을 수 있습니다. 이 테이블은 각 키 작업 후에 업데이트됩니다.
키 관리 트랜잭션 [dare_key_request]	키 관리 트랜잭션은 키 관리 트랜잭션 정보를 캡처합니다. 이 테이블에서 트랜잭션의 각 단계에 대한 로깅을 찾을 수 있습니다. 테이블은 오류 메시지 필드에 트랜잭션에 대한 오류 정보를 기록합니다.
시스템 감사[sys_audit]	시스템 감사 테이블은 인스턴스에서 감사된 모든 기록에 대한 삽입 및 업데이트를 캡처합니다. 이 테이블에서 인스턴스의 기록에 대한 변경 사항, 변경 시기, 변경을 시작한 사용자 계정을 찾을 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

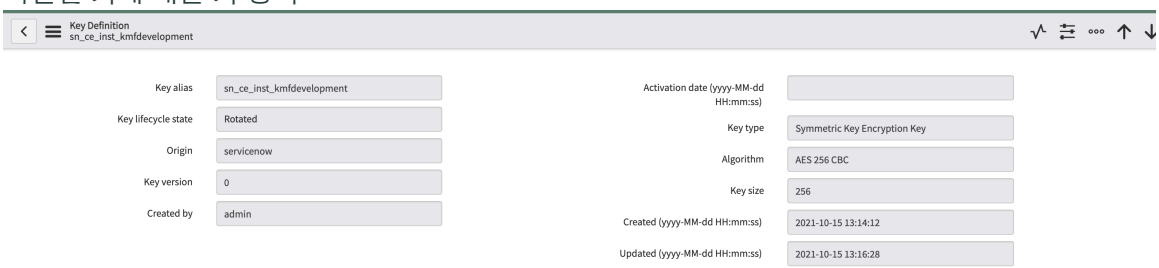
키 회전 작업 모니터링

클라우드 암호화 키 메타데이터 [dare_key_metadata] 테이블을 사용하여 키의 수명주기에 대한 정보를 찾습니다. 이 표에서 키의 원본, 활성화 날짜, 상태 및 버전과 같은 정보를 찾을 수 있습니다.

키 관리 트랜잭션 [dare_key_request] 테이블을 사용하여 키 작업의 트랜잭션을 모니터링할 수 있습니다. 이 테이블에서는 상태, 상태 및 요청이 진행 중인 프로세스 단계를 포함하여 키와 관련된 모든 요청을 찾을 수 있습니다. 완료된 요청은 이 테이블에 완료 됨 상태로 유지됩니다.

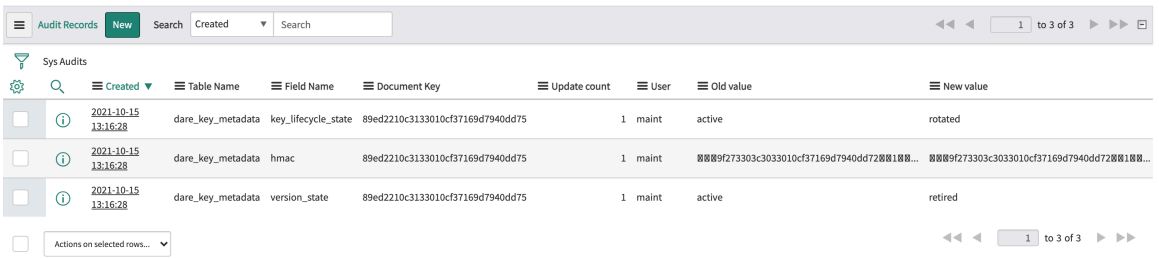
이 예제에서는 키 회전 작업을 보여 줍니다. 이 작업을 수행하는 동안 이전 키 수명주기 상태는 활성에서 회전됨으로 업데이트되고 버전 상태는 활성에서 폐기됨으로 업데이트됩니다.

회전된 키에 대한 키 정의



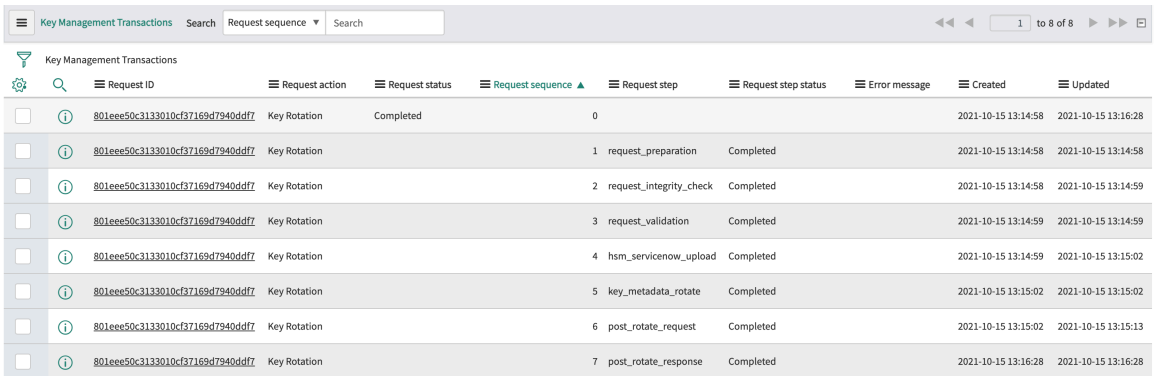
관리자는 시스템 감사[sys_audit] 테이블에서 클라우드 암호화 키 메타데이터 [dare_key_metadata] 테이블의 기록에 대한 변경 내용을 볼 수 있습니다. 관리자는 어떤 기록이 언제 업데이트되었는지 확인할 수 있습니다. 또한 로그 항목은 변경된 필드와 이전 값 및 새 값을 기록합니다.

철회된 키에 대한 감사 로그



관리자는 클라우드 암호화 키 메타데이터 [dare_key_metadata] 테이블의 기록을 볼 수 있습니다. 아래 감사 기록에서 요청 상태가 처리 중에서 완료됨으로 변경되었습니다.

철회된 키에 대한 감사 로그



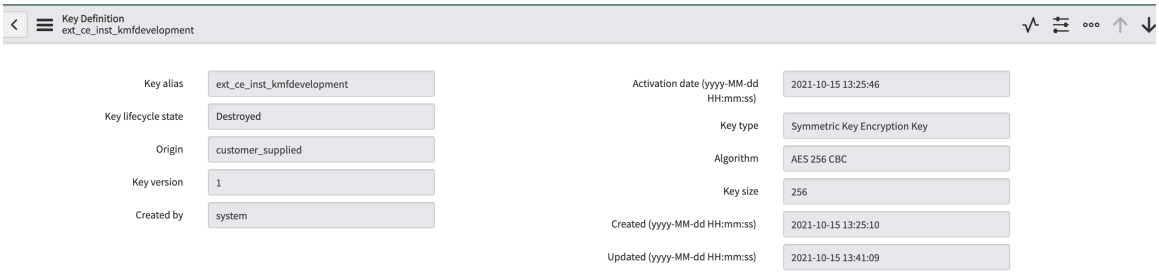
키 철회 작업에 대한 로깅

키 철회에 대한 로깅 정보는 감사 [sys_audit] 테이블에 저장됩니다. 이 로깅 정보에는 키 철회를 시작한 사람과 철회가 발생한 시기에 대한 정보가 포함되어 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

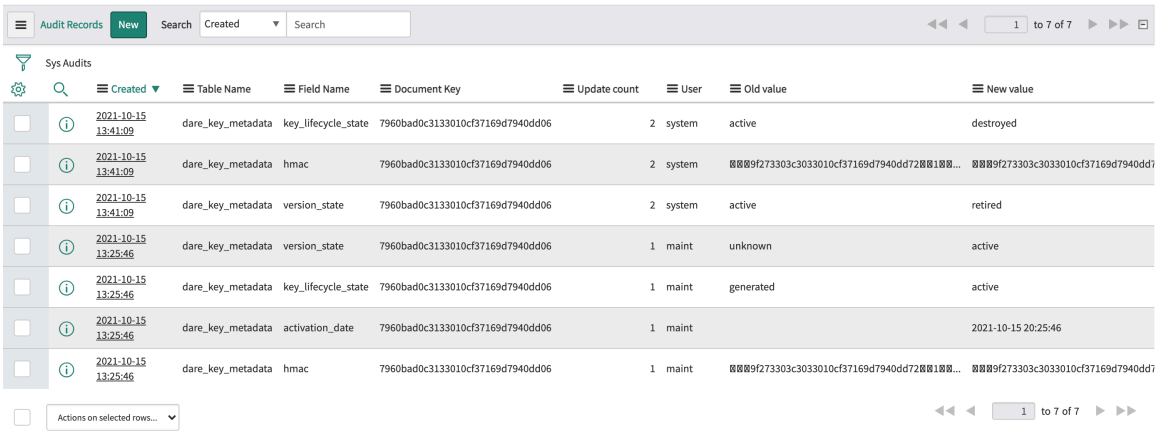
이 예제에서는 키 철회 작업을 보여 줍니다. 이 작업 중에 키 수명 주기 상태가 생성됨에서 활성, 제거됨으로 업데이트됩니다. 키 버전이 알 수 없음에서 활성, 폐기됨으로 업데이트됩니다.

철회된 키에 대한 키 정의



Sys Audits[sys_audit] 테이블에서 관리자는 클라우드 암호화 키 메타데이터 [dare_key_metadata] 테이블을 변경할 수 있습니다.

철회된 키에 대한 감사 로그



변조 탐지

변조 탐지를 사용하여 쿼럼 제어 설정에 대한 무단 변경을 탐지하여 보안을 강화합니다.

변조 감지 프로세스

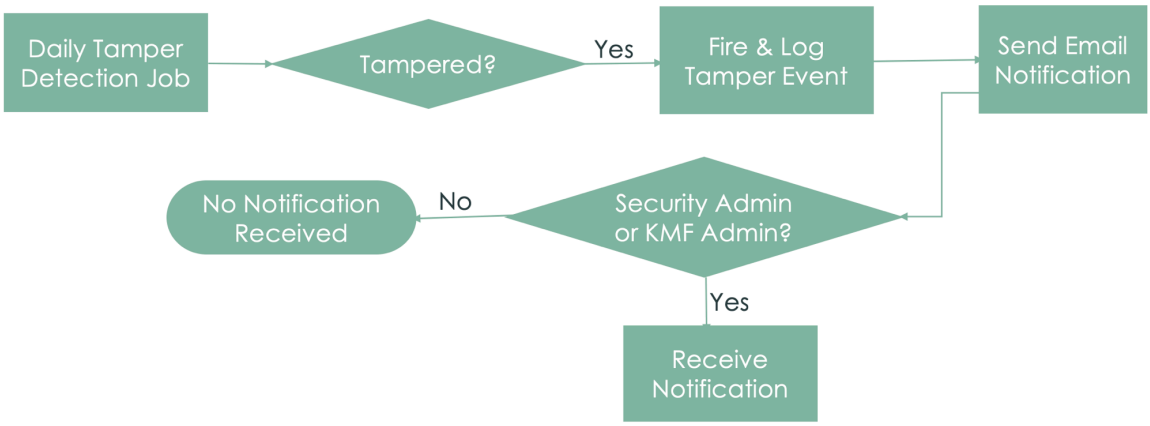
사용하도록 설정하면 변조 탐지는 무단 수정(변조)을 확인하여 쿼럼 제어 설정의 유효성을 검사합니다. 변조 탐지는 해시 기반 메시지 인증 코드(HMAC)를 사용합니다.

1. 설정이 변경되거나 생성되면 인스턴스가 HMAC를 생성합니다. HMAC는 설정(dare_property) 레코드의 값을 기반으로 합니다.
2. 인스턴스가 이러한 설정을 사용할 때마다 변조 탐지는 HMAC를 사용하여 유효성을 검사합니다.
3. 설정이 성공적으로 확인되면 플랫폼에서 사용할 수 있고, 그렇지 않으면 사용할 수 없습니다.

변조 탐지는 인스턴스에서 매일 실행됩니다.

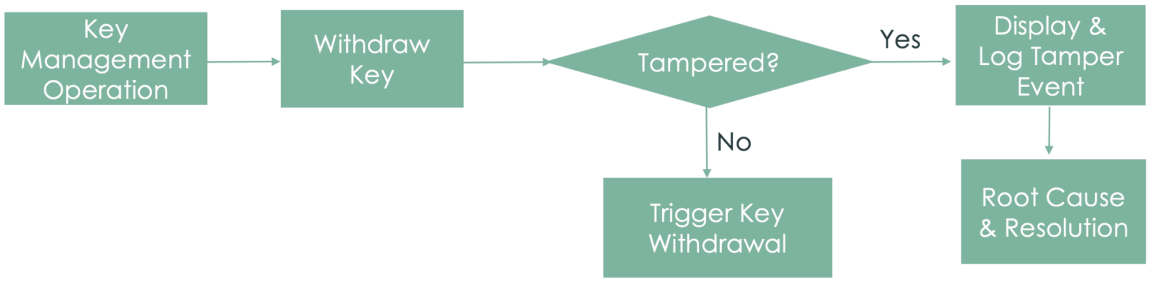
변조 탐지는 일일 예약 작업을 사용하여 변조에 대한 설정을 확인하고 노드 및 보안 로그에 유효성 검사 실패를 보고합니다. 변조 탐지 유효성 검사 실패에 대해 보안 및 KMF 관리자에게 알림을 보냅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



키 철회를 실행하기 전에 변조 탐지가 실행됩니다.

변조 감지는 키 철회를 요청할 때도 속성의 유효성을 검사합니다. 설정이 유효성 검사를 통과하지 못하면 키 철회가 실행되지 않습니다. 이 경우 키 철회가 경쟁하기 전에 유효성 검사 문제를 해결해야 합니다.



변조 식별

변조 탐지는 유효성 검사에 실패할 때 로그를 업데이트합니다.

변조 감지가 쿼럼 제어 설정의 유효성을 검사하지 못하면 이러한 오류가 노드 및 보안 로그에 표시됩니다. 로그 항목에는 확인에 실패한 설정(dare_property) 기록의 sys_id 포함됩니다.

```
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

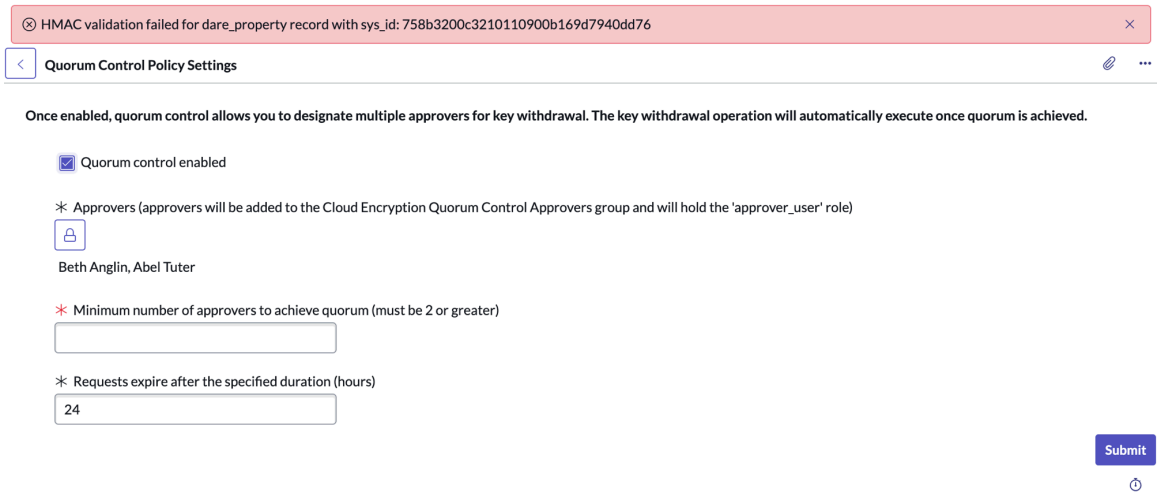
2022-06-28 13:47:35 (264) Default-thread-8
 B6FAC1F6C3D01110CF37169D7940DD6E txid=8e8cc972c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 758b3200c3210110900b169d7940dd76 failed HMAC validation
```

로깅은 유효성 검사에 실패할 때 이러한 예시와 유사한 정보를 표시합니다. 성공한 유효성 검사는 로그에 표시되지 않습니다.

변조 탐지는 Quorum 제어 설정 페이지에 경고 메시지를 표시합니다.

Quorum 제어 설정의 유효성 검사에 실패한 경우 인스턴스에서 Quorum 제어 정책 설정 페이지를 볼 때 경고가 표시될 수 있습니다. 경고에는 확인에 실패한 설정(dare_property) 레코드의 sys_id 포함됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



변조 탐지는 및 *KMF Admin* 역할을 가진 사용자에게 알림을 보냅니다. *Security Admin*

변조 검색이 쿼럼 제어 설정의 유효성을 검사하지 못하면 보안 관리자와 KMF 관리자는 다음 예제와 유사한 알림을 받습니다.

Subject: IMPORTANT: Cloud Encryption Properties Tampering Detected

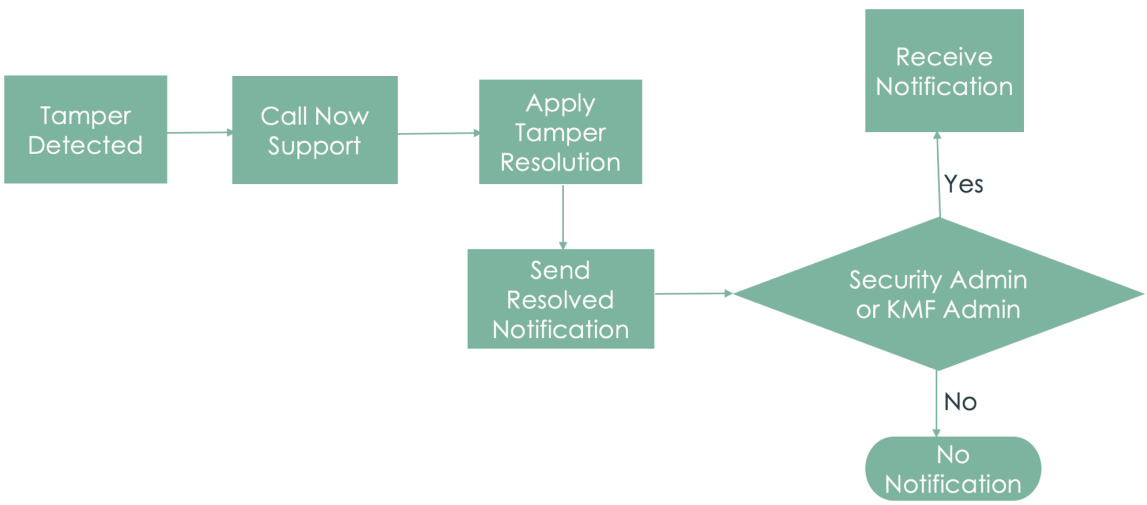
The following list of Cloud Encryption properties appear to have been tampered.
Contact ServiceNow support for additional information and how to correct this issue.

Tampered properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000109_q5pzYMS7hcgHXAoUhipc

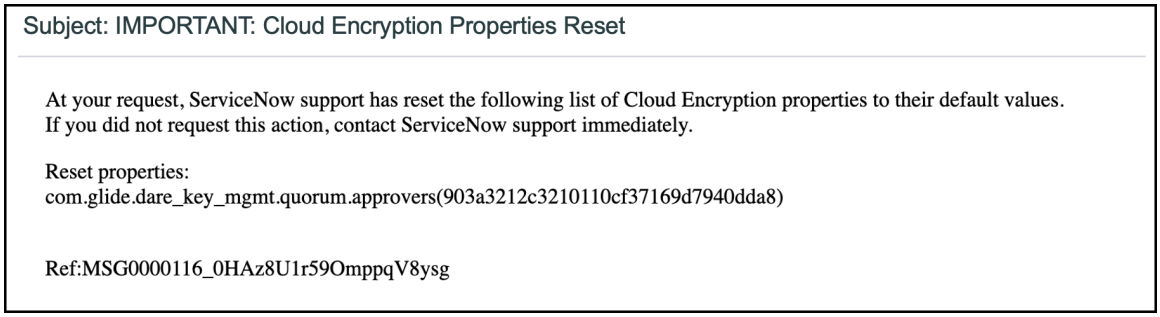
지원을 통한 **ServiceNow** 변조 문제 해결

중요사항: 변조 감지 유효성 검사 실패는 지원의 ServiceNow 도움을 받아야만 해결할 수 있습니다.



변조 감지가 쿼럼 컨트롤 설정의 유효성을 검사하지 못하는 경우 지원 서비스에 문의하여 문제 해결에 도움을 요청하십시오 ServiceNow . 지원 에이전트가 유효성 검사 실패를 해결한 후 보안 및 KMF 관리자는 문제가 해결되었음을 나타내는 알림을 받습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.


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

전체 디스크 암호화

FDE(전체 디스크 암호화)는 유일한 고객 데이터 저장 구성 요소이므로 데이터베이스 서버 내의 전체 스토리지 시스템에만 암호화를 적용합니다. FDE는 저장 장치의 물리적 손실 또는 도난에 대해서만 보호합니다. 암호화된 디스크 서버의 전원이 켜져 있고 데이터를 제공하는 경우 암호화는 추가 보호를 제공하지 않습니다.

전체 디스크 암호화

전체 디스크 암호화는 규제가 심한 조직과 관련이 있을 수 있지만 고객의 ServiceNow 배포에 상당한 비용이 추가될 수 있습니다. 저장 장치의 분실 또는 도난을 완화하기 위해 마련 ServiceNow 된 조치도 선택의 요인이 될 수 있습니다.

Now Platform 관점에서 모든 데이터 흐름은 해독됩니다.

상용 환경에서는 FIPS 140 검증 하드웨어 또는 검증 ServiceNow 과정에 있는 스토리지 장치와 함께 전체 디스크 암호화(FDE)를 사용하며 추가 비용으로 전용 하드웨어 옵션을 제공합니다. FDE는 하드웨어 자체에 적용되므로 사용자에게 할당된 모든 인스턴스에 저장된 모든 데이터에 대해 저장 시 암호화를 제공합니다.

FDE 및 전용 하드웨어 옵션 선택에 대한 자세한 내용은 담당자에게 ServiceNow 문의하십시오.

에지 암호화 규칙

ServiceNow® 에지 암호화 규칙 ™ 는 인터넷을 통해 인스턴스로 ServiceNow 전송하기 전에 회사 구내에서 중요한 데이터를 암호화하며(전송 중 암호화됨) 미사용 시 암호화된 상태로 유지됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색



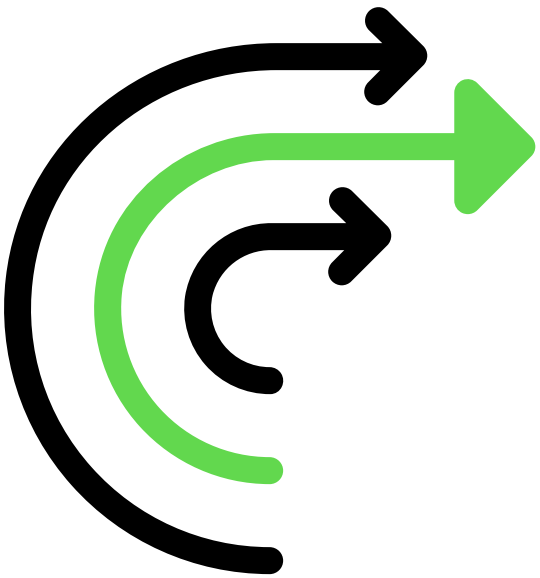
에지 암호화 규칙의 기능과 비즈니스 가치에 대해 알아보십시오.

계획



에지 암호화 규칙을 계획하는 방법을 이해합니다.

설치



에지 암호화 규칙을 설치합니다.

에지 암호화 규칙 업그레이드

업그레이드



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에지 암호화 규칙을 업그레이드하는 방법에 대해 알아봅니다.

구성



에지 암호화 규칙을 구성하는 방법을 이해합니다.

에지 암호화 규칙 탐색

에지 암호화 규칙 는 네트워크에 상주하며 데이터 센터와 ServiceNow 클라우드 간에 이동하는 중요한 데이터를 암호화하고 해독하는 네트워크 암호화 시스템입니다.

에지 암호화 규칙의 정의

'클라이언트 측' 암호화라고도 하는 Edge에서는 모든 양방향 사용자 트래픽이 인프라에서 유지 관리되는 프록시를 통과해야 합니다. 키가 인프라의 프록시 내에 저장되므로 키 관리를 완전히 제어할 수 있습니다. Now Platform 암호문을 해독하여 키에 액세스할 수 없습니다.

이 에지 암호화 규칙 기능은 데이터 및 키 관리의 엔드 투 엔드 암호화를 제어할 수 있는 기능을 제공하는 추가 비용 옵션입니다. 에지 암호화 규칙 는 사용자가 제공하고 ServiceNow 사용자 네트워크 내에 설치한 프록시 애플리케이션을 사용합니다. 이 프록시 애플리케이션은 지정된 데이터 패턴을 토큰화하거나 문자열 필드, 날짜 필드, 날짜/시간 필드 및 첨부 파일 데이터를 암호화한 후 사용자 환경에서 인스턴스로 전송합니다. 또한 프록시 애플리케이션은 사용자 네트워크 내에서만 저장된 키를 사용하여 동일한 데이터를 다시 사용자 네트워크 내에서만 해독합니다.

관련 암호화 키 및 구성은 네트워크 내의 Edge 프록시에만 존재하며 에는 ServiceNow표시되지 않습니다. 데이터는 환경을 떠나는 순간부터 암호화되며 검색 시에만 암호화됩니다. 어떤 경우에도 시스템이나 직원이 일반 텍스트 ServiceNow 로 데이터에 액세스할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에지 암호화 규칙 사용자

네트워크의 프록시 서버를 통해 인스턴스에 로그인한 사용자만 암호화된 데이터를 일반 텍스트로 볼 수 있습니다. 마찬가지로 네트워크의 프록시 서버를 통해 인스턴스에 로그인한 security_admin 사용자만 구성하고 관리할 에지 암호화 규칙수 있습니다.

프록시 서버는 네트워크에 상주하기 때문에 암호화 키를 소유하고 관리하며 해당 암호화 키는 인스턴스로 전송되지 않습니다. 따라서 ServiceNow 중요한 데이터를 일반 텍스트로 표시하지 않습니다.

Edge 프록시 구성 및 규칙 관리 외에도 Edge 프록시를 사용하도록 설정하고 지원하기 위해 환경 내에서 서버를 운영하기 위한 일반적인 요구 사항(호스팅, 라우팅, 백업, DNS 구성 등)을 수행해야 합니다.

암호화 및 토큰화

에지 암호화 규칙 는 중요한 정보를 보호하는 수단으로 암호화(암호화 구성을 통해)와 토큰화(암호화 패턴을 통해)를 모두 지원합니다.

암호화 구성

암호화 구성을 사용하여 개별 필드를 암호화할 수 있습니다. 에지 암호화 규칙 는 AES 128비트 및 AES 256비트 암호화 키를 지원합니다. 에지 암호화 규칙 는 표준, 동일성 유지 및 순서 유지 암호화 유형을 지원합니다.

첨부 파일 외에도 다음 필드 유형을 암호화할 수 있습니다.

- 날짜
- 이메일
- 날짜/시간
- HTML
- IP 주소
- 필기장
- 저널 입력
- 여러 줄 텍스트
- 한 줄 텍스트
- 문자열
- URL

주:

암호화되도록 표시된 저널 필드가 활동 스트림에 추가되면 필드에 대한 모든 사용자 입력이 활동 스트림에서 암호화됩니다.

지원되는 필드 유형 내의 멀티바이트 문자를 암호화할 수 있습니다.

다음 서비스 카탈로그 변수 유형을 암호화할 수도 있습니다.

- 문자열 유형
  - 한 줄 텍스트
  - 여러 줄 텍스트
  - 넓은 한 줄 텍스트
- 날짜

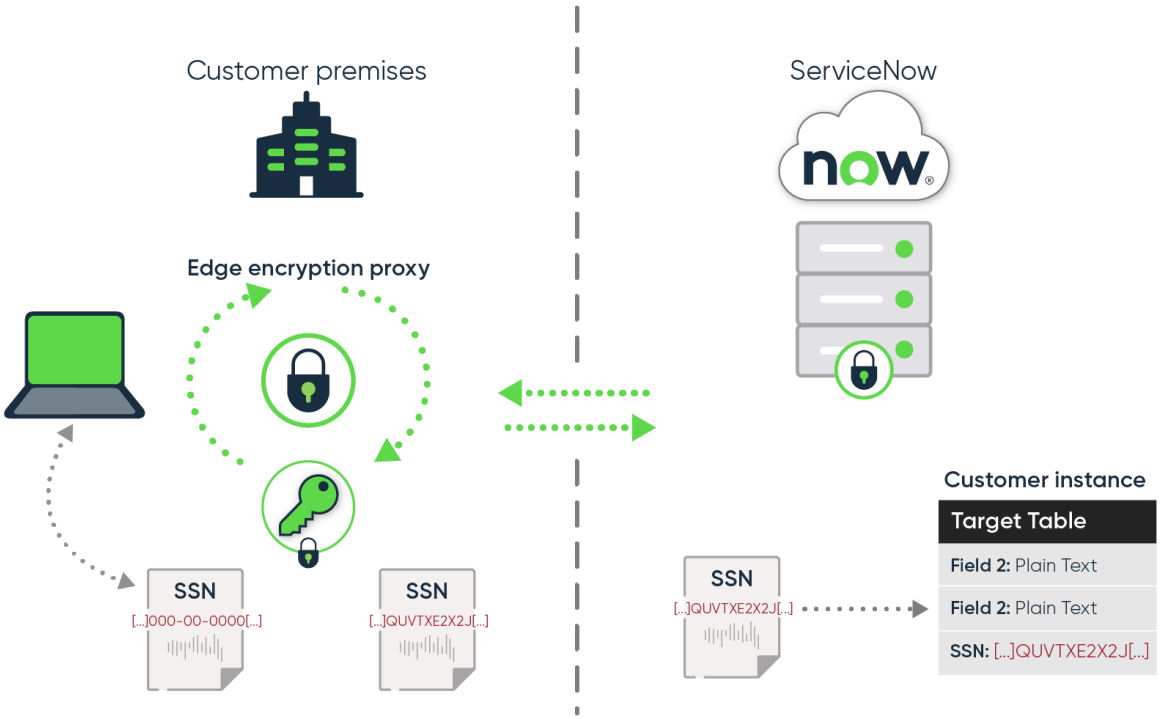
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 날짜/시간
- URL
- 이메일
- HTML
- IP 주소

암호화 패턴

암호화 패턴을 사용하여 주민등록번호나 신용카드 번호 등의 일반 패턴과 일치하는 문자열을 토큰화할 수 있습니다. 암호화 구성이 기본 암호화 방법이어야 하지만, 암호화 패턴을 보완 수단으로 사용하여 암호화된 필드 외부에 있는 중요한 정보를 보호합니다.

주: 프록시 서버에는 에지 암호화 규칙 순서 유지 암호화 또는 암호화 패턴을 사용하는 경우에만 네트워크에 MySQL 데이터베이스가 필요합니다. 일반 텍스트 값은 네트워크의 프록시 데이터베이스에 저장됩니다. 따라서 프록시 데이터베이스를 보호하고 정기적으로 백업하는 것이 중요합니다. 권장 사항은 다음 문서를 참조하십시오 에지 암호화 규칙 구성요소.



에지 암호화 규칙 - **Now Platform**

에지 암호화 규칙 브라우저와 인스턴스 사이의 게이트웨이 역할을 합니다 ServiceNow . 브라우저의 트래픽이 인스턴스로 ServiceNow 가는 도중에 게이트웨이를 통과합니다. 그러면 게이트웨이는 암호화로 표시된 아웃바운드 데이터를 암호화하도록 구성됩니다. 인바운드 트래픽은 게이트웨이를 통해 해독되며 최종 사용자는 브라우저에 일반 텍스트가 표시됩니다. 보안 통제 관점에서 이 구현의 장점은 암호화 및 키 관리가 외부에서 처리 ServiceNow된다는 것입니다.

장점과 단점

필드 암호화 엔터프라이즈 및 필드 암호화와 마찬가지로 는 에지 암호화 규칙 추가 보안의 결과로 인스턴스 내에 일부 기능적 제한을 적용합니다. 그러나 로컬 Edge 프록시는 열 수준 암호화와 비교할 때 정렬과 관련된 몇 가지 추가 기능도 제공합니다.

프로:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 에지 암호화 규칙 누가 귀하의 정보를 볼 수 있는지에 대한 절대적인 제어를 제공하고 데이터 침해를 방지합니다.
- 정보는 프록시 서버에 남아 있으며 네트워크를 암호화하지 않은 상태로 두지 않습니다.
- 정보는 인스턴스에 도달 ServiceNow 하기 전에 전송 중에 암호화됩니다.
- 모든 암호화 키를 보유하고 관리합니다. 다른 사람, 심지어 직원도 ServiceNow 열쇠에 접근할 수 없습니다.
- 암호화 알고리즘의 강도를 AES-128 또는 AES-256으로 선택할 수 있습니다.
- 에지 암호화 규칙 문자열 텍스트, 날짜 및 날짜/시간 필드, 첨부 파일, URL 및 저널을 암호화하는 기능이 포함됩니다.
- 에지 암호화 규칙 는 데이터베이스와 인스턴스 내에서 저장 중인 데이터의 표준, 동일성 유지 및 순서 유지 암호화를 제공합니다.
- 암호화 규칙을 사용하면 프록시 서버에 암호화할 항목과 암호화된 정보를 인스턴스에 저장할 위치를 구체적으로 알려주는 사용자 지정 스크립트를 작성할 수 있습니다. 이러한 스크립트는 데이터 구조가 인스턴스와 ServiceNow 정확히 일치하지 않을 때 유용합니다.
- 암호화 패턴을 사용하면 암호와 같은 정보를 토큰화할 수 있습니다.

죄수:

- 에지 암호화 규칙 Edge 프록시 클러스터를 통한 추가 네트워크 홉과 추가 처리가 필요하며, 이로 인해 트래픽 지연이 추가될 수 있습니다. 애플리케이션의 추가된 처리 지연 에지 암호화 규칙 은 네트워크 홉에 비해 무시할 수 있습니다.
- 자체 암호화 키를 유지 관리하는 것은 복잡하고 시간이 많이 걸릴 수 있습니다.
- 최대 두 개의 키를 유지할 수 있으며 열/데이터의 여러 하위 집합 또는 다른 역할에 대해 서로 다른 키를 정의할 수 있는 유연성 없이
- 에지 암호화 규칙 서버 또는 플랫폼이 암호 해독된 데이터를 조작하기 위해 데이터의 암호를 해독할 수 없다는 부작용이 있습니다. 따라서 에지 암호화 규칙을 사용하여 열을 암호화할 때 기능 Now Platform 및 데이터 처리가 제한될 수 있습니다.

시작하기 전에 알아야 할 사항

암호화 및 토큰화는 데이터의 에지 암호화 규칙 특성을 변화시키고 다른 인스턴스 프로세스에 영향을 줄 수 있기 때문입니다. 를 사용하기 에지 암호화 규칙전에 인스턴스에 미치는 영향을 신중하게 고려하십시오.

프록시 서버는 네트워크에 에지 암호화 규칙 설치되고 유지 관리되기 때문에 네트워크 관리 및 관리가 필요합니다. 원활한 구현을 위해 네트워크 요구 사항을 검토합니다.

다음 주제를 검토하여 Edge Encryption이 인스턴스에 미치는 영향을 이해하십시오.

- 에지 암호화 규칙 계획
- 에지 암호화 규칙 시스템 요구 사항
- 에지 암호화 규칙 환경 크기 조정
- 주문 보존 및 토큰화 데이터베이스 크기 계산
- 에지 암호화 규칙 제한
- 에지 암호화 규칙을 위한 키 관리

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에지 암호화 규칙 구성요소

에지 암호화 규칙는 네트워크의 에지 암호화 규칙 서버에서 실행되는 프록시 서버와 인스턴스에 설치해야 ServiceNow 하는 플러그인으로 에지 암호화 규칙 구성됩니다. 순서 유지 암호화 유형 또는 암호화 패턴을 사용하는 경우 프록시 데이터베이스도 네트워크에 설치해야 합니다.

프록시 애플리케이션

프록시 서버를 에지 암호화 규칙 통과 에지 암호화 규칙 할 때 플러그인을 사용하여 암호화해야 하는 필드, 패턴 및 첨부 파일을 지정할 수 있습니다. 또한 암호화 규칙을 관리하여 특정 요청을 암호화하고 대량 암호화 작업을 예약할 수 있습니다.

프록시 서버

에지 암호화 규칙 프록시 서버는 암호화 규칙을 사용하여 HTTP 요청에서 암호화해야 하는 항목(있는 경우)을 식별하고 이를 암호화한 후 요청을 인스턴스로 전달합니다. 암호 해독 에지 암호화 규칙 의 경우 프록시 서버는 암호화된 데이터에 대한 HTTP 응답을 확인하고 응답을 클라이언트로 다시 보내기 전에 암호를 해독합니다. 이 암호 해독이 발생하려면 모든 HTTP 요청 및 응답이 에지 암호화 규칙 프록시 서버를 통과해야 합니다. 이러한 HTTP 요청에는 브라우저에서 시작된 모든 요청과 SOAP 또는 REST 요청이 포함됩니다.

프록시 데이터베이스

순서 유지 암호화 또는 암호화 패턴을 사용하는 경우 프록시 서버는 네트워크에 있는 MySQL 데이터베이스를 사용합니다. 네트워크의 모든 프록시 서버는 동일한 데이터베이스를 사용해야 합니다.

프록시 데이터베이스에는 이러한 테이블이 포함되어 있습니다.

프록시 데이터베이스 테이블

이름	설명
db_id	고유 데이터베이스 ID
edge_token_map	암호화 패턴 데이터
token_map	순서 보존 암호화 데이터

프록시 데이터베이스 백업

암호화 패턴은 토큰화에 의존하기 때문에 일반 텍스트 값이 프록시 데이터베이스에 저장됩니다. 데이터베이스가 손실되면 명확한 텍스트 값을 복원할 수 없습니다. 정기적인 백업을 유지하는 것이 중요합니다. 데이터 손실을 방지하려면 권장 사항에 따라 ServiceNow 프록시 데이터베이스를 백업합니다.

- 24시간마다 데이터베이스를 백업하십시오.
- MySQL 데이터베이스 이진 로그 파일을 최소 2일 동안 유지합니다. 백업이 복원된 후 이진 로그를 사용하여 가장 최근 백업 이후 손실된 데이터를 다시 생성합니다.

에지 암호화 규칙 클라이언트

에지 암호화 규칙 는 세 개의 클라이언트를 사용하여 프록시가 실행 중임을 인스턴스에 알리고, 프록시와 인스턴스 간 요청을 동기화하며, 모든 최종 사용자 요청을 잠재적 암호화 후 인스턴스로 전달합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라이언트	설명
하트비트/연결 유지 클라이언트	5초마다 ServiceNow 인스턴스에 요청을 보내 이 프록시가 실행 중임을 인스턴스에 알리는 일을 담당합니다. 요청은 Edge 프록시 테이블의 last_response_on 필드를 구동하고 결과적으로 프록시 상태를 구동합니다. 시스템에서 요청을 보내는 데 문제가 있거나 요청 또는 요청 처리가 지연되는 경우 다른 클라이언트(사용자 트래픽용 클라이언트 포함)가 실행 중이더라도 인스턴스가 프록시를 응답 없음으로 표시할 수 있습니다. 또한 이 클라이언트는 인스턴스에서 프록시의 온라인 상태를 제어합니다. 이 *edgeencryption.proxy.keepalive.interval* 속성은 이 클라이언트의 폴링 속도를 제어합니다. 기본값은 5(초)입니다.
폴링/동기화 클라이언트	에지 암호화 규칙 구성에서 동기화하기 위해 프록시가 인스턴스에 보내는 다양한 요청(예: 암호화할 테이블, 열 또는 첨부 파일, 키, 작업, 규칙 및 토큰화 패턴)을 처리합니다. 이 *edgeencryption.config.poll.interval* 속성은 이 클라이언트의 폴링 속도를 제어합니다. ⚠ 경고: 이 설정은 변경하지 마십시오. 프록시 폴링 간격의 기본 설정을 변경하면 인스턴스에서 에지 암호화 규칙 설정을 업데이트할 때 동기화가 지연될 수 있습니다.
기본/사용자 트래픽 클라이언트	그 밖의 모든 경우, 이 클라이언트는 모든 최종 사용자 요청을 처리하고 잠재적인 암호화 후 ServiceNow 인스턴스로 전달합니다. 또한 이 클라이언트는 인스턴스의 응답을 처리하여 잠재적인 암호 해독 후 최종 사용자에게 전달합니다.

에지 암호화 규칙을 위한 키 관리

에서 사용하는 에지 암호화 규칙암호화 키를 제공하고 관리하는 것은 사용자의 책임입니다.

이 항목에서는 제품의 키를 참조합니다 에지 암호화 규칙 . 와 함께 필드 암호화사용할 수 있는 Key Management Framework에 대한 자세한 내용은 Key Management Framework를 참조하십시오.

에서 사용하는 에지 암호화 규칙암호화 유형을 지원하는 암호화 키를 구하고 만들 때는 다음 사항을 고려하십시오.

- AES 128비트를 사용할지 AES 256비트를 사용할지 여부입니다. 사용되지 않는 경우에도 기본 AES 128비트 암호화 키를 정의해야 합니다.
- 파일 시스템, Java KeyStore 또는 EKM(엔터프라이즈 키 관리) 중 무엇을 사용할지 여부입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 암호화 키 교체 시기
- 새 키를 사용하여 데이터를 다시 암호화하기 위해 대량 암호화 작업을 사용하는 경우 및 사용하는 경우입니다.

프록시 구성 파일 및 키 저장소에서 키를 제거하기 전에 키를 사용하는 인스턴스의 모든 데이터를 해독하는 것이 중요합니다. 새 암호화 키를 추가하고 대량 키 회전 작업을 예약하여 이 작업을 수행할 수 있습니다.

키 저장소

에지 암호화 규칙 는 다음과 같은 유형의 키 스토리지를 지원합니다.

파일 저장소

키는 프록시에서 액세스할 수 에지 암호화 규칙 있는 파일 시스템의 파일에 저장됩니다. 파일에 저장된 암호화 키는 암호화되지 않으므로 이러한 파일을 보호하는 것은 사용자의 책임입니다.

Java 키 스토어

키는 Java의 JCEKS KeyStore에 저장됩니다. Java KeyStore는 비밀번호로 보호되므로 파일 저장소의 파일에 키를 저장하는 것보다 더 안전합니다. 단일 Java KeyStore는 여러 키를 저장할 수 있으며 키는 키 별칭으로 식별되므로 여러 키를 더 쉽게 관리할 수 있습니다.

엔터프라이즈 키 관리(EKM)

키는 SafeNet KeySecure 또는 Unbound Technology 키 관리 시스템을 사용하여 저장 및 검색됩니다.

프록시는 에지 암호화 규칙# ### 디렉토리에 `keystore.jceks`라는 Java JCEKS 키 저장소 파일과 함께 제공됩니다. 이 키 스토어 파일에는 에서 서명한 ServiceNow암호화 규칙의 유효성을 검증하는 데 사용되는 공개 키가 들어 ServiceNow 있습니다.

주: 기본 시스템 Java JCEKS KeyStore가 아닌 다른 키 저장소를 사용하는 경우 공개 키를 키 저장소로 가져와야 ServiceNow 합니다. 공개 키 별칭은 *servicenow*입니다.

암호화 키 외에도 Java JCEKS KeyStore는 인스턴스에 저장된 암호화 구성 및 암호화 규칙에 디지털 서명하기 위한 RSA 키 쌍과 프록시가 에지 암호화 규칙 브라우저 및 기타 클라이언트와의 보안 연결을 설정하는 데 사용하는 디지털 인증서를 저장하는 데 사용됩니다.

에지 암호화를 위한 **SafeNet** 키 버전 관리

SafeNet 키 버전 관리를 사용하여 키 변경을 간소화하세요. SafeNet 키 버전 관리는 모든 새 키에 대해 별칭을 생성하는 대신 동일한 별칭을 유지하고 버전을 증가시킵니다.

Edge 프록시 서버에서 SafeNet 키 버전 관리를 구성하려면 먼저 SafeNet에서 키 버전 관리를 설정해야 합니다.

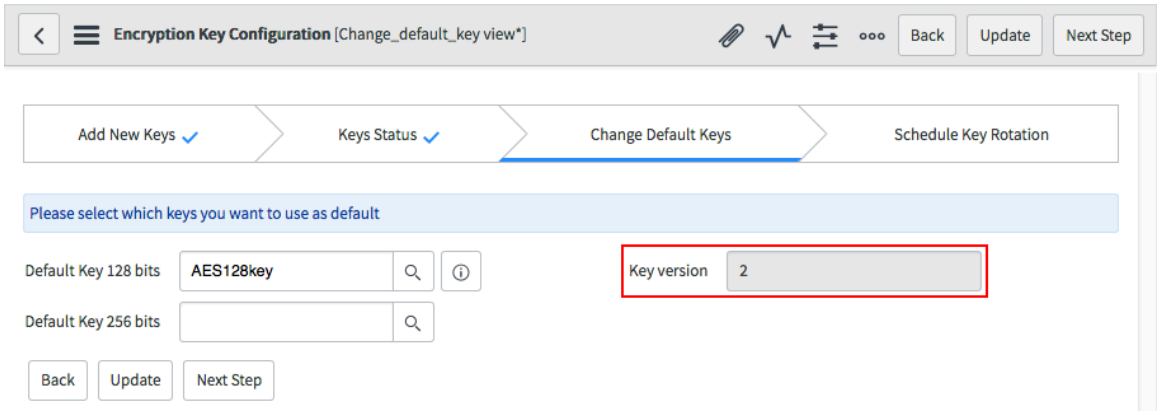
주: 출시 전에 설치된 Edge 프록시는 London SafeNet 키를 지원하지만 SafeNet 키 버전 관리는 지원하지 않습니다. 또는 이전 프록시에서 Kingston 실수로 버전이 지정된 키를 사용하는 경우 이후 릴리스로 London 업그레이드할 때 이후 프록시가 이 문제점을 London 발견하고 잠재적인 데이터 손실을 방지하기 위해 프록시가 시작되지 않습니다.

먼저 대량 키 회전 작업 또는 단일 키 회전 작업을 예약하여 이전 SafeNet 버전 지정 키를 버전이 지정되지 않은 키로 바꾼 다음, 필요한 경우 새 SafeNet 버전 지정 키를 생성해야 합니다. 이 새 버전이 지정된 키는 이후 버전의 프록시에서 London 안전하게 사용할 수 있으며 프록시를 다시 시작할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 키 구성

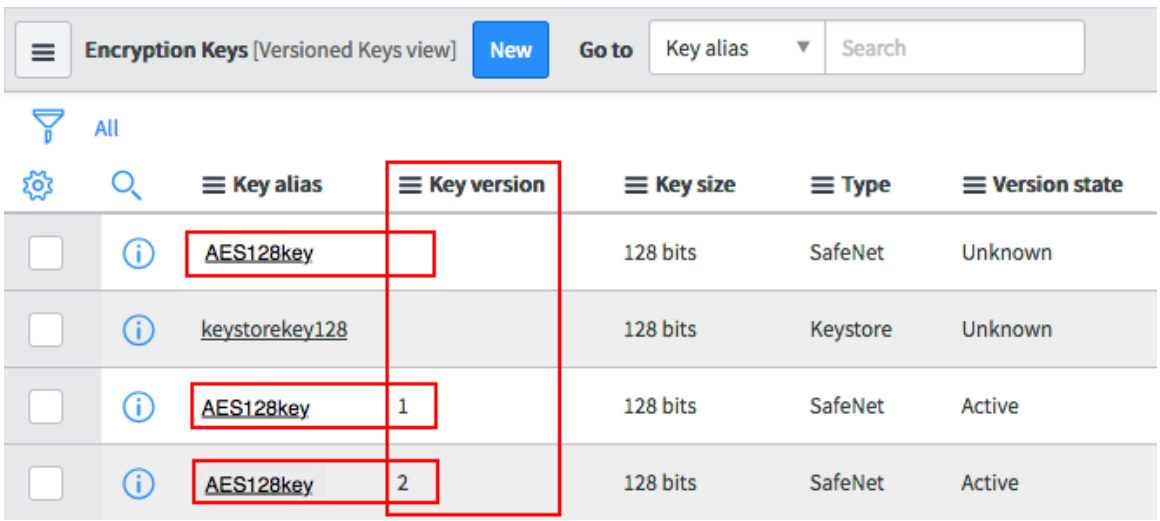
SafeNet 버전 키를 사용하는 경우 암호화 키 구성 양식의 기본 키 변경 섹션에 기본 128비트 및 256비트 키의 키 버전에 대한 새 필드가 포함되어 있습니다. 키 버전 필드는 회색으로 표시되며 편집할 수 없습니다.



절차는 다음 문서를 참조하십시오 인스턴스에서 암호화 키 구성.

버전이 지정된 키

SafeNet 버전 관리 키를 사용하는 경우 에지 암호화 규칙 구성 > 암호화 키 구성 > 모든 키, 버전이 지정된 키에는 키 버전이 포함됩니다.



암호화 키 구성 양식의 기본 키 변경 섹션에서 처음 입력한 항목에는 버전 번호가 표시되지 않습니다. 프록시 서버가 SafeNet에서 키를 요청하면 시스템은 별칭에 대한 새 줄을 추가하고 키 버전을 추가합니다.

위의 예에서 **AES128key** 는 세 번 나열됩니다.

- 키 버전이 표시되지 않은 첫 번째 목록이 초기 항목입니다.
- 키 버전 열에 **1**이 있는 두 번째 목록은 SafeNet에서 반환된 키의 첫 번째 버전입니다.
- 키 버전 열에 **2**가 있는 세 번째 목록은 SafeNet에서 반환된 키의 두 번째 버전입니다.
- SafeNet에서 다른 버전의 키가 반환되면 현재 사용 중인 키 버전을 기록하기 위해 새 줄이 추가됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 구성 및 패턴

를 사용하면 에지 암호화 규칙필드를 암호화하고 문자열을 토큰화할 수 있습니다.

암호화 구성

암호화 구성을 사용하여 개별 필드를 암호화할 수 있습니다. 에지 암호화 규칙 는 AES 128비트 암호화 키를 지원합니다. JCE(Java Cryptography Extension) 무제한 강도 관할 정책 파일이 설치된 경우 는 에지 암호화 규칙 각 암호화 유형에 대해 AES 256비트 암호화 키를 지원합니다. 에지 암호화 규칙 는 다음 유형의 암호화 구성을 지원합니다.

표준 암호화

암호화된 필드의 값은 필드 값이 동일하게 유지되더라도 필드가 암호화될 때마다 달라집니다. 표준 암호화는 가장 강력한 암호화 형식입니다. 표준 암호화를 사용하는 필드는 정렬, 그룹화 또는 필터링이 불가능합니다.

동일성 유지 암호화

암호화된 필드 값은 필드 값이 동일할 때 동일합니다. 필드에 대한 동등 비교 및 그룹화 기준 작업을 지원합니다.

> **주:** 이미 데이터가 포함된 필드에 대해 동일 유지 암호화를 선택한 경우, 한 필드는 암호화되고 다른 하나는 암호화되지 않은 경우 필드에 대해 그룹화 기준 작업을 수행하면 동일한 값을 가진 필드가 그룹화되지 않을 수 있습니다.

순서 유지 암호화

토큰과 암호화를 사용하여 프록시 데이터베이스의 데이터를 보호합니다. 같음 비교, 작업별 그룹화 및 데이터 정렬 기능을 지원합니다. 순서 유지 암호화 유형은 프록시 서버에 대해 에지 암호화 규칙 구성된 MySQL 데이터베이스가 있는 경우에만 지원됩니다.

> **주:** 순서 유지 암호화를 사용하고 프록시 데이터베이스가 다운된 경우 순서 유지 암호화를 사용하여 필드를 업데이트할 수 있습니다. 그러나 해당 필드를 기준으로 데이터를 정렬하려고 하면 정렬 순서가 올바르지 않습니다. 그룹도 예상대로 작동하지 않습니다. 프록시 데이터베이스가 다시 작동되면 주문 토큰 복구 작업을 예약하여 누락된 토큰을 복구합니다.

암호화 유형

다음 암호화 유형은 보안 품질 감소에 나열됩니다.

암호화 유형	설명
표준 AES 256	필드는 필터링, 정렬 또는 비교할 수 없습니다.
표준 AES 128	필드는 필터링, 정렬 또는 비교할 수 없습니다.
동일성 유지 AES 256	필드는 같음 비교를 사용하여 필터링할 수 있습니다.
동일성 유지 AES 128	필드는 같음 비교를 사용하여 필터링할 수 있습니다.
순서 유지 AES 256	필드를 정렬하고 동등 비교 필터링을 사용할 수 있습니다. 네트워크에서 MySQL 데이터베이스를 사용해야 합니다.
순서 유지 AES 128	필드를 정렬하고 동등 비교 필터링을 사용할 수 있습니다. 네트워크에서 MySQL 데이터베이스를 사용해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 패턴

암호화 패턴을 사용하여 문자열에 있는 민감한 데이터를 보호할 수 있습니다. 암호화 패턴이 저장되고 활성화되면 에지 암호화 규칙 프록시 서버는 요청의 패턴과 일치하는 문자열을 식별합니다. 일반 텍스트 문자열을 찾으면 프록시 데이터베이스에 저장되고 인스턴스에서 토큰으로 바뀝니다. 암호화 패턴을 사용하여 주민등록번호나 신용카드 번호 등의 일반 패턴과 일치하는 문자열을 토큰화합니다. 암호화 구성을 기본 암호화 방법으로 사용하는 것이 좋지만, 보완 수단으로 암호화 패턴을 사용하여 암호화된 필드 외부에 있는 중요한 정보를 찾아 보호합니다.

주: 프록시 서버에는 에지 암호화 규칙 순서 유지 암호화 또는 암호화 패턴을 사용하는 경우에만 네트워크에 MySQL 데이터베이스가 필요합니다. 일반 텍스트 값은 네트워크의 프록시 데이터베이스에 저장됩니다. 따라서 프록시 데이터베이스를 보호하고 정기적으로 백업하는 것이 중요합니다. 권장 사항은 다음 문서를 참조하십시오 에지 암호화 규칙 구성요소.

관련 정보

암호화 구성을 사용하여 필드 암호화

암호화 패턴을 사용하여 문자열 토큰화

에지 암호화 규칙과 함께 설치됨

에지 암호화 규칙 는 암호화 관련 데이터를 저장할 테이블, 기본 동작을 구성하는 시스템 속성, 관리할 에지 암호화 규칙edge_encryption 역할을 설치합니다.

에지 암호화 규칙 앱과 함께 설치되는 테이블

에지 암호화 규칙은 다음 테이블을 추가합니다.

에지 암호화 규칙 구성 [sys_encryption_configuration]

첨부 파일이 암호화되는 암호화된 필드와 테이블을 포함합니다.

에지 암호화 규칙 규칙 [sys_encryption_rule]

각 규칙에 대한 기록을 포함합니다. 규칙에는 이름, 사용 시기의 조건, 스크립트 및 순서 필드가 있습니다.

에지 암호화 규칙 잘못된 삽입 로그 [sys_edge_encryption_invalid_insert_log]

암호화되지 않은 데이터를 암호화된 필드에 저장하기 위해 생성된 로그 메시지를 포함합니다.

에지 암호화 규칙 프록시 [sys_encryption_proxy]

암호화 프록시 애플리케이션에 대한 정보를 포함합니다.

에지 프록시 암호화 유형 [sys_proxy_encryption_type]

암호화 양식에서 암호화 유형을 사용하거나 사용하지 않도록 설정하는 데 사용됩니다.

암호화 작업 실행 [sys_encryption_job_execution]

대량 암호화 작업을 지원합니다.

암호화 작업 실행 청크 [sys_encryption_job_execution_chunk]

대량 암호화 작업을 지원합니다.

예약된 암호화 작업 [sysauto_encryption_job]

암호화, 암호 해독, 키 회전, 토큰 복구 주문 및 데이터베이스 복구를 위해 예약된 작업을 나열합니다.

암호화 키 구성 [sys_encryption_key_configuration]

기본 암호화 키를 나열합니다.

암호화 키 [sys_encryption_key]

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용 가능한 키와 키 속성을 나열합니다.

프록시 암호화 키 [sys_encryption_proxy_key]

프록시 암호화 키를 나열합니다.

에지 암호화 규칙 앱과 함께 설치되는 속성

에지 암호화 규칙은 다음 속성을 추가합니다.

주: 시스템 속성 [sys_properties] 테이블을 열려면 탐색 필터에 `sys_properties.list`를 입력합니다.

glide.edge.pattern.disallowed.chars

패턴에 허용되지 않는 문자 목록입니다.

- 유형: 쉼표로 구분된 값 목록의 문자열
- 위치: 시스템 속성 [sys_properties] 테이블

glide.edge.pattern.min.size

허용되는 최소 패턴 크기입니다. 더 작은 패턴을 허용한다는 것은 더 많은 일치 항목을 찾는 것을 의미하며, 이로 인해 오버헤드가 증가합니다.

- 유형: 번호
- 기본값: 5
- 위치: 시스템 속성 [sys_properties] 테이블

sn_edge_encryption.logging.destination

메시지가 기록되는 위치입니다.

- 유형: 문자열
- 기본값: 파일
- 위치: 시스템 속성 [sys_properties] 테이블

sn_edge_encryption.logging.verbosity

사용할 로깅 수준입니다.

- 유형: 문자열
- 기본값: 정보
- 위치: 시스템 속성 [sys_properties] 테이블

sn_edge_encryption.encryption.proxy.buildtag

인스턴스에 등록된 프록시 버전입니다.

- 유형: 문자열
- 위치: 시스템 속성 [sys_properties] 테이블

sn_edge_encryption.cleartext.allowed

예일 경우 암호화된 필드에 일반 텍스트를 저장할 수 있습니다. 이 작업은 사용자가 프록시를 거치 에지 암호화 규칙 지 않고 인스턴스에 액세스할 때 발생합니다. false인 경우 일반 텍스트가 암호화된 필드에 저장되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 유형: 부울
- 기본값: false
- 위치: 시스템 속성 [sys_properties] 테이블

에지 암호화 규칙 계획

를 에지 암호화 규칙 성공적으로 구현하려면 계획과 준비가 필요합니다.

계획 단계에서 다음 질문에 답합니다.

- 어떤 필드를 암호화해야 합니까?
- 어떤 암호화 유형을 사용해야 합니까?
- 얼마나 많은 에지 암호화 규칙 프록시가 필요합니까? 권장 사항 및 고려 사항은 을 참조하십시오 에지 암호화 규칙 환경 크기 조정 .
- 암호화 유형 또는 암호화 패턴을 보존하는 순서를 사용할 경우 MySQL 데이터베이스는 어디에 있습니까?
- 어떤 키 관리 시스템을 사용해야 합니까?

시스템 관리자, 네트워크 관리자 및 보안 팀 구성원은 구현을 에지 암호화 규칙위해 서로 다른 작업을 수행해야 합니다.

- 시스템 관리자에게는 security-admin 역할이 필요합니다. 시스템 관리자는 다음을 수행해야 합니다.
  - 에지 암호화 규칙 프록시 애플리케이션을 다운로드합니다.
  - 에지 암호화 규칙 인스턴스에 연결하는 데 사용할 프록시의 사용자 계정을 설정합니다. 사용자에게 edge_encryption 역할이 할당되어야 합니다.
  - 암호화 키를 구성하고 기본 키를 설정합니다.
  - 인스턴스에서 구성합니다 에지 암호화 규칙 .
  - 암호화 작업을 예약합니다.
  - 모니터 에지 암호화 규칙.
  - 암호화 규칙을 만들고 편집합니다.
- 네트워크 관리자는 다음을 수행해야 합니다.
  - 에지 암호화 규칙 프록시 애플리케이션을 설치합니다.
  - 순서 유지 암호화 및 암호화 패턴에 사용되는 프록시 데이터베이스 및 프록시 서버의 네트워크 주소를 확인합니다.
  - 순서 유지 암호화 및 암호화 패턴에 사용할 프록시 데이터베이스를 설치합니다.
  - 프록시 애플리케이션을 시작하고 중지합니다.
  - 암호화 키 관리를 수행합니다.
  - 사용자를 암호화 프록시 애플리케이션에 매핑하는 방법을 결정합니다. 이 작업은 DNS 설정 또는 라우팅 규칙을 사용하여 수행할 수 있으며 각 네트워크에 따라 다릅니다.
  - 여러 프록시 서버를 관리합니다.
  - 부하 분산 장치 풀 및 설정을 구성합니다.
- 보안 관리자는 각 필드에 할당할 암호화 유형을 결정해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에지 암호화 규칙 시스템 요구 사항

Microsoft Windows 또는 Linux 운영 체제에서 에지 암호화 규칙 실행되는 서버 또는 가상 머신에서 프록시 애플리케이션을 실행할 수 있습니다. 최적의 성능을 위해 구성이 이러한 요구사항을 충족하는지 확인합니다.

Java 요구 사항

프록시 서버를 설치하거나 실행하는 에지 암호화 규칙 호스트 컴퓨터는 지원되는 Java 버전을 유지 관리해야 합니다. 현재 지원되는 버전은 11.x 버전 시리즈의 Java 11.0.6 이상입니다.

주: Java 8은 릴리스부터 Utah 더 이상 지원되지 않습니다. 프록시 버전을 에지 암호화 규칙 설치하기 Utah 전에 프록시를 에지 암호화 규칙 사용하여 환경을 Java 11로 업그레이드하십시오.

주: Java는 무제한 강도 키를 자동으로 허용하지 않습니다. 특히 AES 256비트 암호화 사용을 활성화해야 합니다.

OpenJDK 지원

OpenJDK 버전 11을 Now Platform 지원합니다.

프록시 서버 최소 구성

프록시 서버에는 다음과 같은 최소 구성이 필요합니다.

- 프록시 서버당 4GB의 RAM(대부분의 배포에 6GB 권장됨).

  주: 프록시 서버 호스트에는 프록시 서버보다 최소 1GB의 RAM이 더 필요합니다. 프록시 서버 호스트에는 운영 체제 서비스를 위해 1GB가 추가로 필요합니다. 예를 들어 프록시 서버가 4GB의 RAM을 사용하도록 구성하는 경우 프록시 서버 호스트에 최소 5GB의 RAM을 설치해야 합니다.

  프록시 서버에는 최소 4GB의 메모리가 필요하므로 32비트 JRE 및 32비트 운영 체제는 London 릴리스부터 더 이상 지원되지 않습니다.

- 3GHz CPU 이상(최적의 성능을 위해 4코어 CPU 선호).
- 부하 분산 장치 뒤에 있는 여러 프록시 서버. 필요한 프록시 서버의 수는 애플리케이션 노드 수, 동시 사용자 수 및 페일오버에 필요한 서버 수에 따라 다릅니다. 자세한 내용은 에지 암호화 규칙 환경 크기 조정을 참조하십시오.
- 서버 사용률 및 자원 가용성에 따라 다른 서비스와 동시에 실행할 수 있습니다.

프록시 서버 지원 시스템

다음 시스템이 지원됩니다.

지원 시스템	설명
Windows Server 2012, 2012-R2, 2016 및 2019 버전	• 가상 머신 또는 물리적 하드웨어 • 64비트 시스템
Linux	• 가상 머신 또는 물리적 하드웨어 • 64비트 시스템

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원 시스템	설명
	64비트 Linux 시스템에는 32비트 GNU C 라이브러리 (glibc)를 설치해야 합니다. CentOS의 설치 명령은 `yum install glibc.i686`입니다.

프록시 서버 버전 요구 사항

에지 암호화 규칙 프록시 버전을 인스턴스 버전과 동기화 ServiceNow 상태로 유지합니다(예: Tokyo동일한 주요 릴리스). 업그레이드 프로세스 중 다운타임을 제거하기 위해 프록시는 에지 암호화 규칙 이전 버전과 호환됩니다. 그러나 사용자가 새로운 기능과 중요한 버그 수정에 액세스할 수 없도록 가능한 한 빨리 업그레이드하는 것이 중요합니다.

프록시 서버 연결 요구 사항

응용 프로그램을 실행하는 에지 암호화 규칙 프록시 서버는 네트워크의 컴퓨터와 통신할 수 있어야 합니다. 프록시 서버에 다음 네트워크 권한이 있는지 확인합니다.

네트워크 권한	설명
방화벽 접근	연결을 허용하도록 프록시 서버와 클라이언트 장치 간의 방화벽을 구성합니다. 네트워크에서 DMZ(Demilitarized Zone)를 사용하여 LAN(Local Area Network)에 추가 보안 계층을 추가하는 경우 네트워크 보안 프로토콜이 네트워크 내에서 DMZ로의 포트 액세스를 제한하는 경우 DMZ 내의 컴퓨터에 프록시 서버를 배포해야 할 수 있습니다.
네트워크 접근	프록시 서버가 연결할 수 있도록 각 클라이언트를 구성합니다. 네트워크 보안으로 인해 클라이언트에 연결할 수 있는 새 컴퓨터를 구성할 수 없는 경우 연결 권한이 있는 기존 컴퓨터에 프록시 서버를 설치합니다.
인스턴스 접근	프록시 서버에 인스턴스에 대한 네트워크 액세스 권한이 있는지 확인합니다. TCP 포트 443을 통한 트래픽을 허용하도록 프록시 서버 네트워크를 구성해야 합니다.
네트워크 계정	로컬 또는 도메인 관리자를 통해 프록시 서버를 설치합니다.

주문 보존 및 토큰화 데이터베이스 시스템 요구 사항

순서 유지 암호화 및 암호화 패턴을 사용하려면 프록시 서버에 대해 에지 암호화 규칙 Oracle MySQL 데이터베이스를 구성해야 합니다. 순서 유지 암호화를 사용하면 데이터를 먼저 해독하지 않고도 모든 비교 작업을 암호화된 데이터에 직접 적용할 수 있습니다. 암호화 패턴을 사용하면 문자열 패턴을 데이터베이스로 전송하여 저장하기 전에 토큰(토큰화라고 함)으로 바꿀 수 있습니다. MySQL 데이터베이스의 크기 때문에 전용 프록시 서버를 사용하여 주문 보존 및 토큰화 데이터베이스를 실행합니다.

최소 데이터베이스 시스템 요구 사항은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MySQL 데이터베이스	요구사항
버전	MySQL 데이터베이스 버전 5.7 및 8.0 주: MySQL 버전 5.5 및 5.6은 더 이상 테스트되지 않으며 지원이 종료되었습니다.
OS	64비트 시스템
CPU	2GHz CPU 이상(최적의 성능을 위해 4코어 CPU 권장)
RAM	16GB
디스크	SAN(Storage Area Network) 또는 로컬 스토리지(RAID 10 권장)
크기	잠재적 기록 수에 기록 크기를 곱하여 결정됩니다. 주문 보존 및 토큰화 데이터베이스 크기 계산를 참조하십시오.
구성	고가용성 클러스터. MySQL 서버를 구성하는 방법을 잘 모르는 경우 MySQL 에 구성 정보를 문의하십시오.

에지 암호화 규칙 환경 크기 조정

사용자 환경에 대한 프록시 서버 수를 선택하는 것은 중요한 작업입니다. 사용자 수, 중복성 요구 사항, 허용 가능한 대기 시간을 고려하십시오.

중복

하드웨어 장애 시 중복 프록시 서버를 유지 관리합니다. 프록시 서버에 연결할 수 없는 경우 모든 사용자에게 기능 경로를 제공하기 위해 프록시 서버는 부하 분산 장치 뒤에 있어야 합니다. 최소한 두 개의 프록시 서버를 항상 사용할 수 있는지 확인하십시오.

크기

크기는 데이터 암호화로 인해 발생하는 추가 대기 시간을 방지하는 데 필요한 프록시 서버의 수를 나타냅니다. 용도에 따라 프록시 서버를 추가하여 대기 시간을 줄일 수 있습니다. 예를 들어 일반 대량 암호화가 실행되는 경우 추가 프록시 서버를 추가하여 부하를 처리하거나 사용자 부하가 적을 때 대량 암호화를 실행합니다. 또한 프록시 서버가 실행되는 하드웨어는 성능과 대기 시간에 영향을 줍니다. 더 빠른 CPU, 더 많은 CPU 및 더 많은 RAM이 있는 하드웨어에서 실행되는 프록시 서버는 느리고 제한된 시스템보다 처리량이 높습니다.

다음 지침에서는 프록시 서버가 최소 하드웨어 요구 사항 이상으로 실행되고 있다고 가정합니다. 프록시 서버 수를 확인하려면 다음을 수행합니다.

- 인스턴스의 애플리케이션 노드 2개마다 하나의 프록시 서버를 설정하는 것이 좋습니다.
- 중복성을 위해 부하 분산 장치 뒤에 최소 2개의 프록시 서버를 설정합니다.
- 동시 사용자 500명마다 추가 프록시 서버를 추가합니다.
- 원하는 중복성에 따라 페일오버를 위해 프록시 서버를 추가합니다.

예를 들어 사용자가 2,000명인 인스턴스의 경우 부하 분산 장치 뒤에 최소 5개의 프록시 서버가 있어야 합니다. 이 계산에는 사용자 500명당 하나의 프록시 서버와 페일오버를 위한 추가 프록시 서버가 포함됩니다. 사용자 500명의 임계치에 근접할 시기를 미리 결정하고 부하 분산 장치 풀에 다른 프록시 서버를 배치합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

부하 분산 장치

요청의 균형을 맞추고 서버 응답시간을 개선하려면 부하 분산 장치 풀에 프록시 서버를 분산합니다. "최소 연결" 방법을 사용하도록 부하 분산 장치를 구성합니다. 이 방법은 활성 연결이 가장 적은 프록시 서버에 요청을 연결하여 단일 프록시의 과부하를 방지합니다.

CPU 사용률

데이터 암호화 및 토큰화는 CPU를 많이 사용하는 작업이므로 데이터를 암호화하는 동안 CPU 스파이크는 정상이며 예상됩니다. CPU 사용률이 한 번에 몇 분 동안 80%를 초과하면 프록시 서버에서 수행할 작업이 너무 많음을 의미할 수 있습니다. 이 경우 CPU 사용률이 높은 기간 동안 대기 시간이 증가합니다. 대기 시간이 지속되는 경우 다른 프록시 서버를 추가하여 대기 시간을 줄이는 데 도움이 될 수 있습니다.

메모리

프록시 서버에는 최소 4GB의 RAM을 사용할 수 있어야 합니다(6GB 권장). 프록시 서버 초기 및 상한 메모리 제한을 권장 설정으로 설정합니다.

주문 보존 및 토큰화 데이터베이스 크기 계산

순서 유지 암호화 또는 암호화 패턴을 사용하는 경우 잠재적 레코드 수에 레코드 크기를 곱하여 MySQL 데이터베이스의 크기를 결정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
전용 머신을 사용하여 주문 보존 및 토큰화 데이터베이스를 실행합니다. 프록시 서버와 동일한 하드웨어에서 데이터베이스를 실행하지 마십시오.

프로시저

1. 주문 유지 암호화로 암호화된 필드를 포함할 수 있는 잠재적인 기록 수를 결정합니다.
   a. 순서 유지 암호화를 사용하는 암호화 구성 수에 각 구성이 적용되는 기록 수를 곱합니다.
   b. 성장을 허용하려면 결과에 3을 곱합니다.
2. 1단계의 결과에 1,536을 곱합니다.
   1,536은 기록의 평균 크기(바이트)입니다.
3. 암호화 패턴을 사용하는 경우 토큰화된 레코드에 대해 1-2단계를 수행하고 결과를 합계에 추가합니다.

결과
계산된 값은 주문 보존 및 토큰화 데이터베이스에 권장되는 크기(바이트)입니다.

에지 암호화 규칙 제한

에지 암호화 규칙 시스템 기능에 영향을 미칩니다. 필드 암호화의 영향을 신중하게 평가하십시오.

필드 유형 제한

다음 필드 유형만 암호화할 수 있습니다.

- 날짜
- 이메일
- 날짜/시간

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- HTML
- IP 주소
- 필기장
- 저널 입력
- 여러 줄 텍스트
- 한 줄 텍스트
- 문자열
- URL

다음 필드 유형은 암호화할 수 없습니다.

- 선택 필드
- 가상 필드
- sys_user의 특정 필드를 제외한 시스템 테이블의 필드
- 테이블의 시스템 필드
- 번호 필드 또는 자동 번호 매기기 구성표와 관련된 필드
- 위에 나열되지 않은 기타 필드 유형

추가 제한 사항:

- 저널 필드가 암호화되면 저널 필드가 여러 개 있고 그 필드 중 하나만 암호화되어도 게시 버튼은 비활성화됩니다.
- 암호화된 필드는 이동 및 헤더 필터 상자에서 사용할 수 없습니다.
- 인덱스로 사용되는 필드를 암호화할 때는 순서 유지 및 동일 유지 암호화 유형만 사용할 수 있습니다. 인덱싱된 필드는 표준 암호화 유형을 사용하여 암호화할 수 없습니다.

자세한 내용은 필드 유형을 참조하십시오.

필터링 및 검색 제한 사항

표준 암호화

표준 암호화된 필드 구성을 필터의 왼쪽 피연산자로 사용하여 문자열, 날짜, 날짜/시간 또는 URL 필드를 선택하면 필터링 옵션을 사용할 수 없습니다.

동일성 유지 암호화

필터의 왼쪽 피연산자로 같음을 유지하는 암호화된 필드 구성을 사용하여 문자열, 날짜, 날짜/시간 또는 URL 필드를 선택하면 다음 연산자를 사용할 수 있습니다.

- **=**
- 일치하지 않음
- 비어 있음
- 비어 있지 않음

순서 유지 암호화

필터의 왼쪽 피연산자로 순서 유지 암호화된 필드 구성이 있는 문자열 필드를 선택하면 **is**, **is not**, **is empty** 및 **is not empty** 연산자를 사용할 수 있습니다.

- 보다 큼
- 보다 작음

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

순서 유지 암호화된 필드 구성을 필터의 왼쪽 피연산자로 사용하여 날짜 또는 날짜/시간 필드를 선택하면 **is**, **is not**, **is empty** 및 **is not empty** 연산자를 사용할 수 있습니다.

- 이후
- 이전
- 이후 또는 이후
- 이전 또는 에서

날짜 및 날짜/시간 선택

날짜 필드의 경우 날짜 선택기를 사용하여 날짜를 지정합니다.



날짜/시간 필드의 경우 날짜 및 시간 선택기를 사용하여 날짜 및 시간을 지정합니다.



목록 조건 필터

일치 표시 및 필터링 옵션은 목록에서 지원됩니다. 정확히 일치하는 항목만 반환되거나 필터링됩니다.

> **주:** 조건 필터에서 암호화된 필드를 추가하는 것은 UI 정책 및 비즈니스 규칙과 같은 스크립트에서 지원됩니다.

구성 제한

암호화 구성의 제한 및 동작:

- 구성 테이블에 필드를 에지 암호화 규칙 추가한 후에는 구성 기록을 삭제할 수 없습니다. 필드를 더 이상 암호화하지 않으려면 구성 테이블에서 기록을 에지 암호화 규칙 비활성화하고 암호화 작업을 예약하여 데이터를 해독합니다.
- 상위 테이블의 필드가 암호화되도록 표시된 경우 상속된 모든 테이블에서도 필드가 암호화됩니다. 예를 들어, 작업 테이블의 간단한 설명 필드가 암호화되면 인시던트 테이블의 간단한 설명 필드 내용도 암호화됩니다.
- 상위 테이블에서 상속된 필드가 암호화되도록 표시된 경우 상위 테이블의 필드를 암호화할 수 없습니다. 예를 들어 인시던트 테이블의 간단한 설명 이 암호화되도록 표시된 경우 작업 테이블의

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

간단한 설명을 암호화할 수 없습니다. 이 예에서는 문제 테이블의 짧은 설명을 암호화할 수 있습니다.

- 암호화 구성이 정의된 필드를 임의의 형식으로 익스포트하면 프록시 서버를 통해 익스포트하는 경우에도 출력에 암호화된 값이 포함됩니다.
- 암호화 구성이 정의된 필드에는 데이터를 임포트할 수 없습니다.
- 상속된 날짜 및 날짜/시간 필드는 암호화할 수 없습니다. 상위 테이블에서 상속된 날짜 또는 날짜/시간 필드는 열 필드 드롭다운 목록에 나열되지 않으며 해당 필드에 대한 날짜 또는 날짜/시간 암호화 구성을 만들 수 없습니다.
- 상위 테이블이나 하위 테이블에서만 문자열 또는 URL 필드를 암호화할 수 있지만 둘 다에서 암호화할 수는 없습니다.

인스턴스 제한

사용이 에지 암호화 규칙 인스턴스에 미치는 영향:

- 백엔드 논리는 암호화된 데이터를 처리할 수 없습니다. 인스턴스에 암호화된 데이터가 포함되어 있으면 암호화된 필드의 데이터 평가에 의존하는 비즈니스 규칙, 백엔드 스크립트 또는 백엔드 기능이 제대로 실행되지 않습니다.

  주: 동일성 유지 또는 순서 유지 암호화로 암호화된 데이터는 동일한 암호화된 값과 비교할 때 여전히 동등성 검사를 통과합니다.

- 이메일 처리는 메일 시스템에서 인스턴스로 바로 이동하고 Edge 프록시를 통과할 수 없으므로 이메일을 통해 들어오거나 나가는 데이터는 Edge 프록시에서 암호화하거나 해독할 수 없습니다.
  - 인바운드 이메일의 데이터 및 첨부 파일은 암호화되지 않습니다.
  - 아웃바운드 이메일의 데이터 및 첨부 파일은 암호화된 상태로 유지되며 암호를 해독할 수 없습니다.
- 서버에서 실행되는 스크립트는 암호화된 데이터를 변경할 수 없습니다.
- 글로벌 검색은 지원되지 않습니다. 글로벌 검색은 암호화된 데이터와 일반 텍스트 데이터를 모두 검색하려고 시도하기 때문에 결과가 예상과 다를 수 있습니다.
- 암호화된 데이터는 필드가 암호화되지 않은 기록에 복사하여 붙여넣을 수 없습니다.
- 선택한 암호화 유형에 따라 암호화된 필드에 대한 사용자 인터페이스 기능이 줄어듭니다. 예를 들어 비교, 그룹화 기준, 정렬 및 검색할 수 있는 기능이 영향을 받을 수 있습니다. 일반적으로 선택한 암호화가 강력할수록 더 많은 기능이 줄어듭니다.
- Java KeyStore, SafeNet, Unbound Technology를 제외하고 타사 소프트웨어 또는 하드웨어 암호화 키 관리는 지원되지 않습니다.
- 단일 인스턴스에 연결된 여러 프록시 서버가 지원되지만 암호화 프록시 클러스터 관리 및 모니터링을 사용할 수 없습니다. 각 프록시는 별도로 관리해야 합니다.
- 작업 부하 및 암호화된 필드 수와 같은 시스템 구성은 암호화된 필드의 성능에 영향을 줄 수 있습니다.
- 에지 암호화 규칙 프록시 서버는 단일 인스턴스에만 연결할 수 있습니다.
- 인스턴스에서 Oracle 데이터베이스를 사용하고 암호화하도록 표시하려는 문자열 필드가 2925자를 초과하는 경우 암호화 순서를 유지해도 해당 필드를 정렬할 수 없습니다.
- 인스턴스에서 Oracle 데이터베이스를 사용하는 경우 유니코드 AL32UTF8 유일하게 지원되는 문자 집합입니다.
- 암호화된 데이터는 보고서에 사용할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 에지 암호화 규칙 은(는) 데이터 보관과 함께 사용할 수 없습니다.
- 에지 암호화 규칙 프록시는 배치 REST 요청 API를 사용하는 요청을 암호화할 수 없습니다. 에지 암호화 규칙 프록시를 사용하는 경우 `glide.uxf.disable_rest_batching` 시스템 속성을 true로 설정하여 REST 일괄 처리를 비활성화합니다.

에지 암호화 규칙 설치

프록시는 에지 암호화 규칙 수동으로 설치하거나 대화형 설치 관리자를 사용하여 설치할 수 있습니다 에지 암호화 규칙 .

Java 요구 사항

프록시 서버를 설치하거나 실행하는 에지 암호화 규칙 호스트 컴퓨터는 지원되는 Java 버전을 유지 관리해야 합니다. 현재 지원되는 버전은 17.x 버전 시리즈의 Java 17.0.3 이상입니다.

주: Java 11은 Yokohama 릴리스부터 더 이상 지원되지 않습니다. Yokohama 또는 이후 버전의 프록시를 설치하기 전에 프록시를 에지 암호화 규칙 사용하여 환경을 Java 17로 업그레이드합니다 에지 암호화 규칙 .

프록시 서버 설치

설치 에지 암호화 규칙 에는 다음 단계가 포함됩니다.

- 에지 암호화 규칙 대화형 설치 관리자 또는 수동 설치 관리자를 사용하여 네트워크의 서버에 프록시 애플리케이션을 설치합니다.
- 암호화 구성 및 암호화 규칙에 디지털 서명을 위한 RSA 키 쌍을 생성합니다.
- AES 256 암호화를 사용하려는 경우 JCE(Java Cryptography Extension)를 설치합니다.
- 보안 SSL 연결을 사용하는 경우 서버 인증서를 가져와서 Java KeyStore로 가져옵니다.
- 키 스토어와 암호화 키를 설정합니다.
- 순서 유지 암호화 유형 또는 암호화 패턴을 사용해야 하는 경우 네트워크의 컴퓨터에 MySQL 데이터베이스를 설정합니다.
- 원하는 속성을 설정합니다. 속성은 `edgeencryption.properties` 구성 파일에 있습니다.
- 프록시 서버가 해당 프록시 서버에서 들어오는 요청을 처리할 수 있도록 에지 암호화 규칙 신뢰할 수 있는 소스임을 지정합니다.

프록시 서버 액세스

설치가 완료되면 URL 형식(`<host>:<port>`)을 사용하여 각 사용자의 브라우저를 프록시로 에지 암호화 규칙 가리킵니다. 값은 `edgeencryption.properties` 파일의 host 및 port 특성에 의해 결정됩니다.

다음 값을 사용하는 예:

속성	예제 값
edgeencryption.proxy.host	hostname.mycompany.com
edgeencryption.proxy.http.port	8081

클라이언트는 `http://hostname.mycompany.com:8081/` 주소를 사용하여 프록시 서버에 액세스합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: DNS 설정 및 라우팅 규칙을 사용할 수 있습니다. 호스트 및 포트 값은 네트워크 관리자가 결정합니다.

에지 암호화 규칙 요청

플러그인(com.glide.edgeencryption)은 에지 암호화 규칙 별도의 구독으로 사용할 수 있습니다.

시작하기 전에

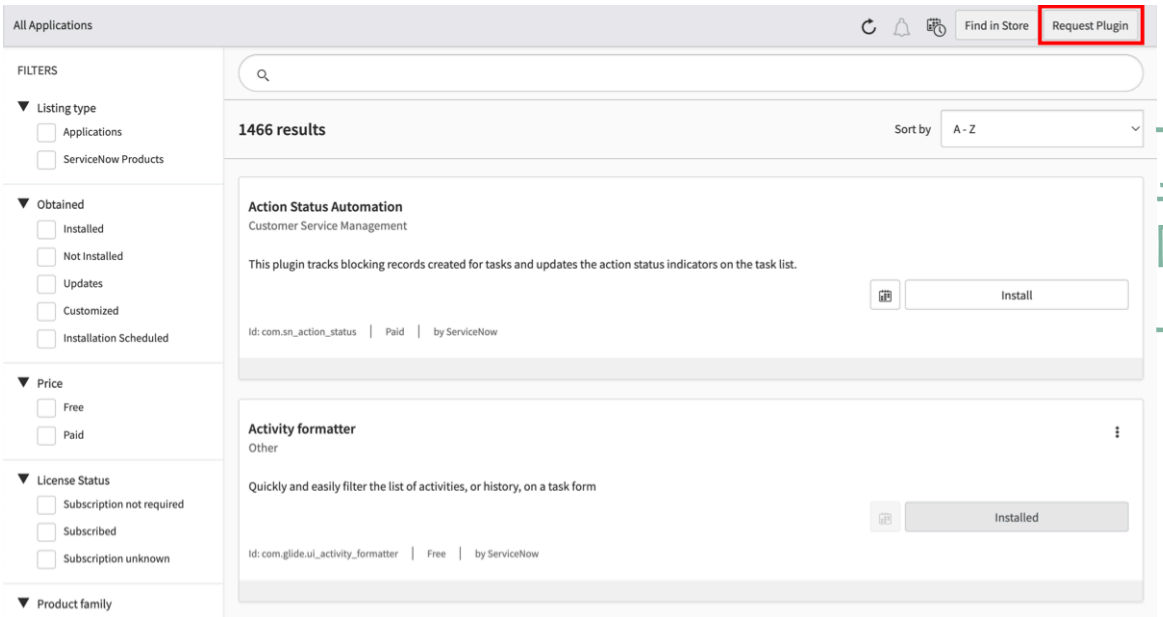
구독을 구매하려면 ServiceNow 계정 관리자에게 문의하십시오. 고객 관리자는 일반적으로 며칠 이내에 조직의 프로덕션 및 하위 프로덕션 인스턴스에서 플러그인을 활성화하도록 준비할 수 있습니다.

고객 관리자가 없거나 구매 후 정품 인증 지연을 결정하거나, 하위 프로덕션 인스턴스에서 무료로 제품을 평가하려면, 다음 단계를 수행하십시오.

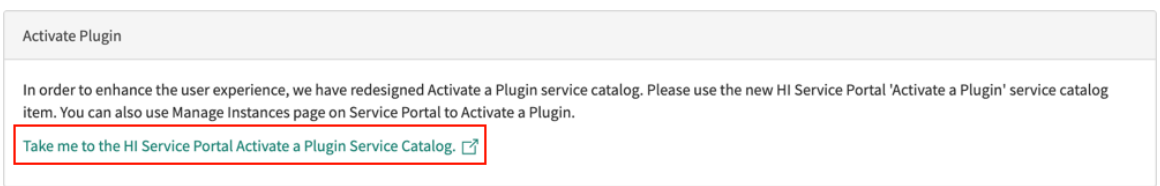
필요한 역할: 없음

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 모든 애플리케이션 페이지에서 플러그인 요청을 선택하여 Now Support의 플러그인 활성화 양식을 엽니다.



3. Now Support에서 Now Support 서비스 포털 서비스 카탈로그에 액세스하는 링크를 선택합니다.



4. 인스턴스를 선택합니다.
5. 작업 > 플러그인 활성화를 선택합니다.
6. 플러그인 활성화 양식에서 다음 정보를 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

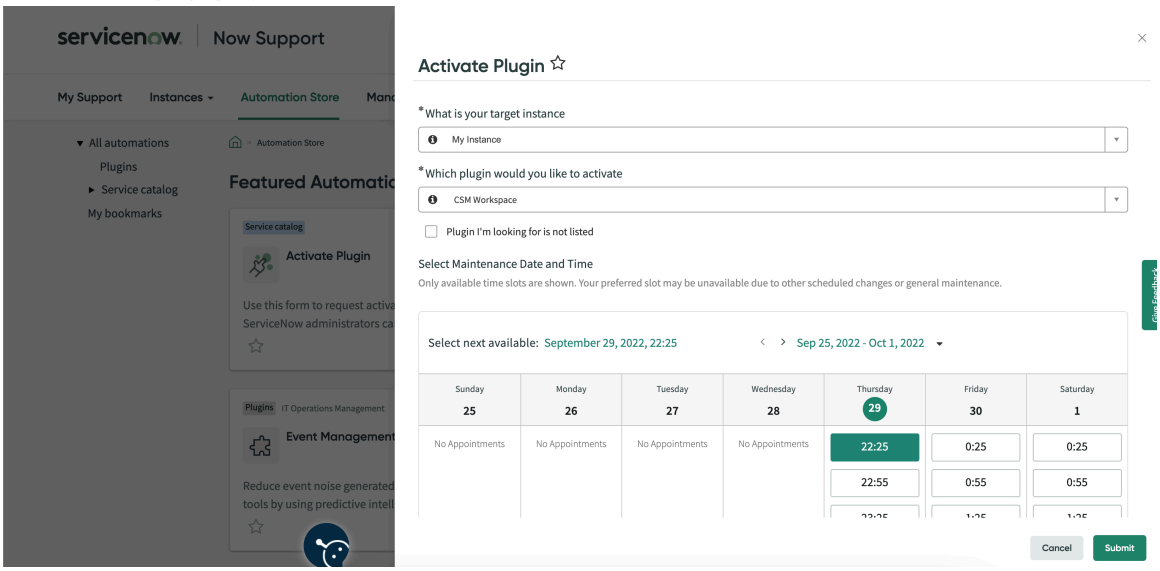
플러그인 활성화 양식

필드	설명
대상 인스턴스는 무엇입니까?	플러그인을 활성화할 인스턴스입니다.
어떤 플러그인을 활성화하시겠습니까?	활성화할 플러그인의 이름입니다. 주: 시스템에서 원하는 플러그인을 나열하지 않거나 OEM 또는 온프레미스 인스턴스에서 플러그인을 활성화하는 경우 찾고 있는 플러그인이 목록에 없음 확인란을 선택한 다음 플러그인 이름을 입력합니다.
유지관리 날짜 및 시간 선택	플러그인을 활성화하는 날짜 및 시간입니다. 주: 플러그인은 미국 태평양 시간대의 모든 영업일에 두 번(오전과 저녁에 각각 한 번씩) 활성화됩니다. 특정 시간에 플러그인을 활성화해야 하는 경우 이유/설명 필드에 요청을 입력합니다.

Example

예를 들어, 내 인스턴스라는 인스턴스에서 CSM Workspace 플러그인을 활성화하는 다음 양식을 참조하십시오.

플러그인 활성화 양식



7. 제출을 선택합니다.
   플러그인 요청에 대한 자세한 내용은 다음을 참조하십시오. 의 서비스 카탈로그 [KB0751715] 문서에서 플러그인 요청 Now Support 지식베이스.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에지 암호화 규칙 사용자 계정 설정

프록시는 에지 암호화 규칙 사용자로 인스턴스에 연결하여 암호화 구성 정보를 얻고 업데이트합니다. 이를 위해 사용자 계정을 만들고 사용자에게 edge_encryption 역할을 부여합니다.

시작하기 전에

에지 암호화 규칙 역할을 할당하려면 플러그인을 설치해야 합니다.

필요한 역할: admin

프로시저

1. ServiceNow 인스턴스에서 프록시 애플리케이션에 사용할 에지 암호화 규칙 사용자 계정을 생성합니다.
2. 사용자에게 edge_encryption 역할을 할당합니다.

에지 암호화 규칙 프록시 서버 다운로드

에지 암호화 규칙 인스턴스에서 프록시 서버 응용 프로그램을 다운로드한 다음 프록시 서버를 실행할 에지 암호화 규칙 각 컴퓨터에 파일을 복사합니다.

시작하기 전에

이 절차를 에지 암호화 규칙 시작하기 전에 인스턴스에 플러그인을 설치하고 활성화해야 합니다.

주: 프록시는 에지 암호화 규칙 Oracle JRE에서만 공식적으로 지원됩니다.

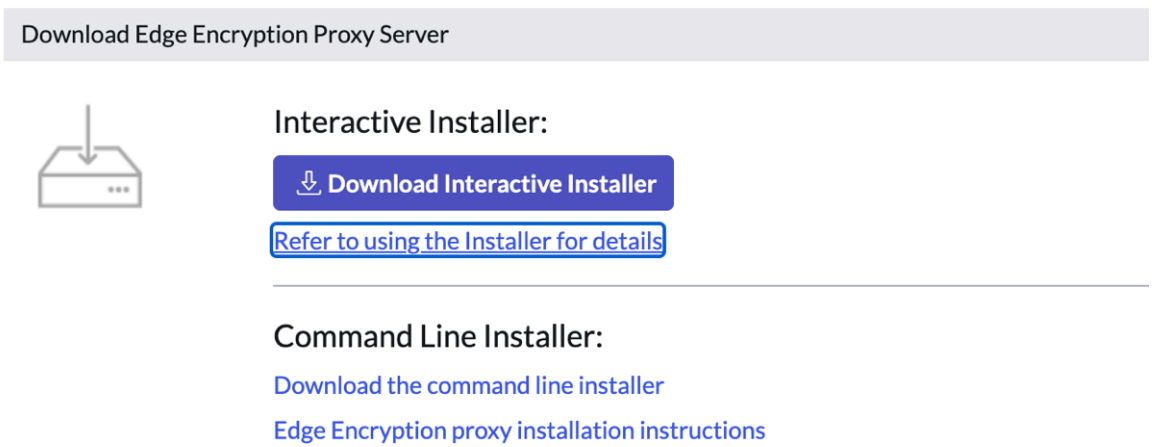
필요한 역할: security_admin

이 태스크 정보

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 설치 및 다운로드 > 다운로드.
2. 대화형 설치 관리자를 사용하려면 대화형 설치 관리자 다운로드를 클릭합니다.

   프록시 서버를 수동으로 설치하는 경우 프록시 서버의 OS 버전을 선택합니다.



주: 프록시 서버를 실행하려면 최소 4GB의 메모리가 필요하므로 릴리스부터 Washington DC 32비트 JRE 및 32비트 운영 체제가 더 이상 지원되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 프록시 서버를 실행할 에지 암호화 규칙 각 컴퓨터에 설치 관리자를 복사합니다.

> 주: 프록시 서버를 수동으로 설치하는 에지 암호화 규칙 경우 프록시 서버를 실행할 에지 암호화 규칙 각 컴퓨터에 ZIP 파일을 복사합니다.

다음에 수행할 작업

설치 관리자를 다운로드한 에지 암호화 규칙 후 대화형 설치 관리자를 사용하여 에지 암호화 규칙 프록시 서버 설치. 수동으로 설치하는 경우 명령줄 설치 관리자를 사용하여 에지 암호화 규칙 프록시 서버 설치.

대화형 설치 관리자를 사용하여 에지 암호화 규칙 프록시 서버 설치

에지 암호화 규칙 대화형 설치 관리자를 사용하여 Windows 또는 Linux 컴퓨터에 프록시 서버를 설치합니다.

시작하기 전에

> 주: SafeNet KeySecure 키 저장소 파일은 설치 프로그램에서 지원되지 에지 암호화 규칙 않습니다. SafeNet KeySecure 키 저장소를 명령줄 설치 관리자를 사용하여 에지 암호화 규칙 프록시 서버 설치사용하려면 .

에지 암호화 규칙 이 절차를 시작하기 전에 인스턴스에 플러그인을 설치하고 활성화해야 합니다. 설치 프로그램을 실행하는 에지 암호화 규칙 시스템에 Java 버전 11.0.6 이상이 설치되어 있는지 확인합니다.

필요한 역할:

- ServiceNow 인스턴스에서 security_admin
- Windows 호스트의 로컬 또는 도메인 관리자
- Linux 호스트에서 전체 파일 시스템 액세스 권한이 있는 서비스 사용자

이 태스크 정보

새 프록시 서버를 설치한 후 설치 관리자를 다시 실행하여 설치 문제를 감지하거나 현재 설정을 수정하는 테스트를 수행할 수 있습니다. 옵션은 다음과 같습니다.

- 새로 설치: 새 프록시 서버를 설치합니다.
- 설치 확인: 테스트를 수행하여 이전 설치의 문제를 감지하고 수정합니다.
- 기존 재설치: 테스트를 수행하여 이전 설치의 문제를 탐지 및 수정하고 기존 설정을 보거나 수정합니다.

> 주: 권한이 있는 포트(포트 80 또는 443)의 Linux 머신에 프록시 서버를 설치하는 경우 전체 파일 시스템 액세스 권한이 있는 루트 사용자로 설치 프로그램을 실행해야 합니다. 프록시 서버가 설치된 후 파일 시스템 액세스를 제한하려면 프록시 설치 관리자에서 SetUID 기능을 사용할 수 있습니다. 이 기능을 사용하려면 루트 또는 sudo 루트로 설치 관리자를 시작합니다. 설치 관리자가 메시지를 표시하면 권한이 없는 사용자의 사용자 이름과 사용자 그룹을 제공합니다. 프록시 서버는 지정된 사용자의 파일 시스템 권한으로 설치됩니다. 이 단계를 건너뛰면 루트 권한으로 기본 설치를 계속할 수 있습니다.

프로시저

설치 프로그램을 사용하여 인스턴스에 대한 여러 프록시를 여러 컴퓨터에 설치하여 다음 조건이 적용되는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 모든 프록시에는 암호화 구성 및 규칙에 디지털 서명하는 데 사용되는 동일한 암호화 키와 동일한 RSA 키 쌍이 있어야 합니다.
- 암호화 키는 인스턴스에 구성된 기본 키여야 합니다.
- 프록시 데이터베이스가 설치의 일부로 설정되면 모든 프록시가 동일한 프록시 데이터베이스를 사용해야 합니다.

  동등성 유지 암호화, 순서 유지 암호화 또는 토큰화를 위해 프록시 데이터베이스가 필요할 수 있습니다. 이러한 기능을 사용하지 않는 경우에는 프록시 데이터베이스가 필요하지 않습니다.

다음에 수행할 작업

키보드 사용자를 위해 제작된 접근성 지원 자바 애플리케이션을 읽도록 설계된 보조 기술 스크린 리더인 NVDA 를 사용하려면 자바 애플리케이션과 함께 32비트 NVDA를 사용하도록 Windows 64비트 호스트 구성 하기를 참고하세요.

프록시 서버를 설치한 에지 암호화 규칙 후 프록시 서버 초기 메모리 한도 및 상한 메모리 한도를 설정합니다.

에지 암호화 규칙 프록시 서버 설치(대화식 설치 관리자)

Windows 또는 Linux 컴퓨터에 프록시를 에지 암호화 규칙 설치합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 에지 암호화 규칙 프록시 서버 설치 관리자를 다운로드합니다.
2. 에지 암호화 규칙 프록시 설치 관리자를 엽니다.

   주: Windows 컴퓨터에 설치하는 경우 관리자 권한으로 설치 관리자를 실행해야 합니다.

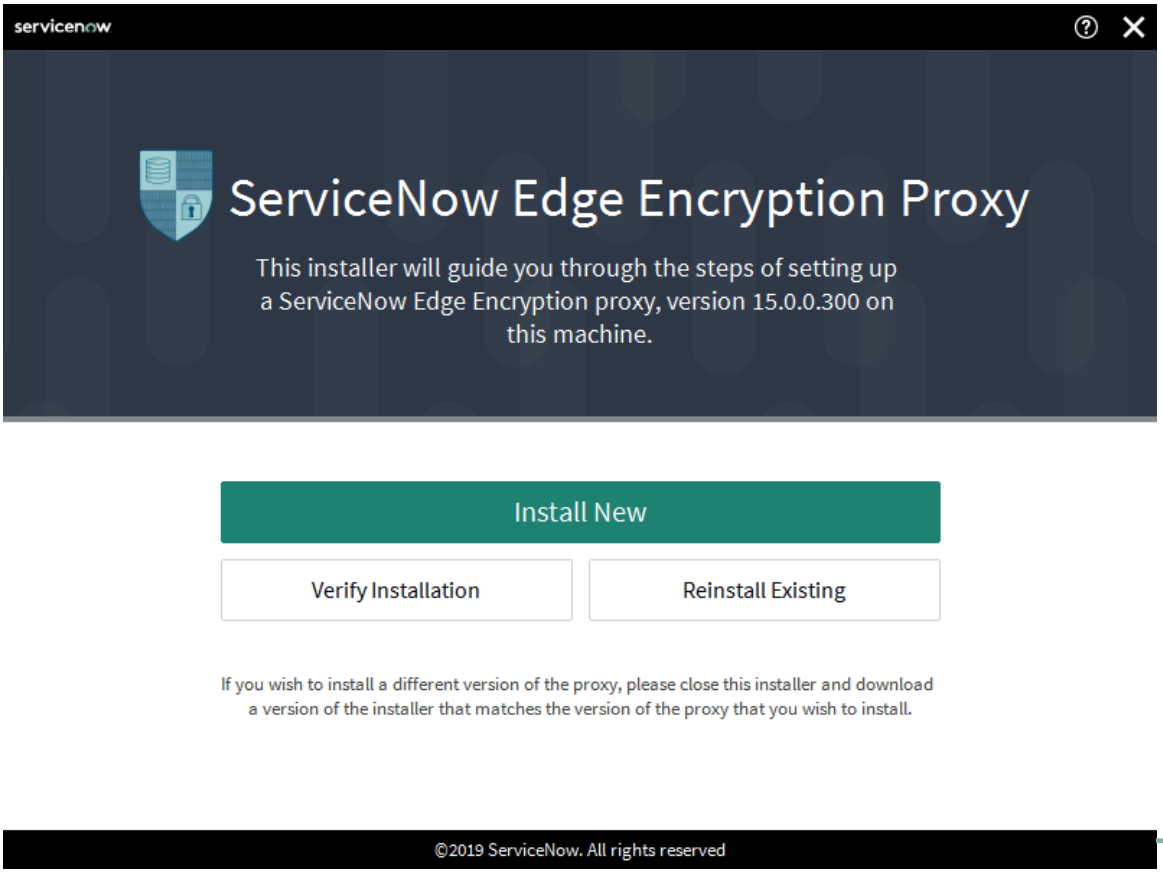
   a. Windows 컴퓨터에서 관리자 권한으로 설치 프로그램을 실행하려면 명령 프롬프트를 마우스 오른쪽 버튼으로 클릭하고 관리자 권한으로 실행을 선택합니다.

   b. 명령줄에서 다운로드한 .jar 파일이 들어 있는 디렉터리로 이동합니다.

   c. `java -jar <## ##>.jar` 명령을 실행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow 에지 암호화 규칙 프록시 설치 관리자



3. 새 프록시 서버를 설치하려면 새로 설치를 선택합니다.
   프록시가 이미 설치되어 있는 경우 설치 관리자를 실행하여 다음을 수행할 수 있습니다.
   - 설치 확인: 테스트를 수행하여 이전 설치의 문제를 감지하고 수정합니다.
   - 기존 재설치: 테스트를 수행하여 이전 설치의 문제를 탐지 및 수정하고 기존 설정을 보거나 수정합니다.
4. 설치 위치와대상 **ServiceNow** 인스턴스를 구성합니다.

   a. 찾아보기를 클릭하여 설치 위치를 선택하거나 설치 경로를 수동으로 입력합니다.

   b. 대상 ServiceNow 인스턴스의 URL을 입력합니다.
   프로토콜 및 포트 번호를 포함합니다.

   Example
   `https://example.servicenow.com:443`

   c. 대상 ServiceNow 인스턴스에서 edge_encryption 역할을 가진 사용자의 사용자 이름과 암호를 입력합니다.

5. 다음을 클릭합니다.
6. 연결 설정 및 프록시 설정을 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정	설명
프록시 호스트	프록시 서버를 설치할 컴퓨터의 전체 주소 도메인 이름입니다. 주: **FQDN** 검색을 클릭하여 컴퓨터의 정규화된 도메인 이름을 조회하고 프록시 호스트 필드를 자동으로 채웁니다. 포트와 함께 이 속성은 클라이언트가 프록시 서버에 액세스하는 데 사용하는 URL을 정의합니다.
HTTP 포트	HTTP 통신을 위한 프록시의 포트입니다.
HTTPS 포트	HTTPS 통신을 위한 프록시의 포트입니다.
프록시 이름	프록시 및 서비스의 이름입니다. 프록시 이름은 고유해야 합니다.
프록시 폴링 간격	폴링 간격(초)입니다. 기본 설정을 사용하면 프록시가 암호화 구성 변경 내용을 학습하는 데 5초가 걸립니다. 값이 클수록 인스턴스가 온라인 상태가 된 프록시를 탐지하는 데 시간이 더 오래 걸립니다. 주: 프록시 폴링 간격의 기본 설정을 변경하면 프록시가 온라인 상태가 될 때 탐지 지연이 발생할 수 있습니다.
프록시 연결 유지 Ping 간격	프록시에서 인스턴스에 대해 발급한 ping 사이의 시간(초)입니다. 프록시와 인스턴스 간의 연결을 확인하기 위해 Ping이 주기적으로 발행됩니다. 기본값은 10입니다. 최솟값은 5입니다.

7. 설치를 클릭합니다.
에지 암호화 규칙 프록시 서버가 설치됩니다. 설치하는 데 몇 분 정도 걸릴 수 있습니다.

CyberArk 속성 보호 구성

필요한 경우 CyberArk 속성 보호를 구성하여 중앙 집중식 보안 디지털 볼트에 암호를 안전하게 저장합니다 에지 암호화 규칙 .

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
프록시 서버에 대한 CyberArk 연결 매개변수 및 보호된 자격 증명을 구성하려면 먼저 CyberArk AIM(Application Identity Management)을 구입하고 구성해야 합니다. AIM 클라이언트 설치의 일부로 `JavaPasswordSDK.jar` 파일이 AIM 클라이언트 설치 디렉토리에 설치됩니다. CyberArk 볼트는 강화된 독립 서버에 설치되며 AIM 클라이언트는 해당 서버에 대한 보안 액세스를 허용합니다.

주: Edge 프록시가 설치된 모든 호스트 컴퓨터에 CyberArk AIM 클라이언트를 설치해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Edge 설치 관리자에서 Edge 프록시에 대한 CyberArk 연결을 설정하려면 `JavaPasswordSDK.jar` 파일의 위치를 지정해야 합니다. AIM Client를 설치하는 동안 정의한 다른 값도 입력해야 합니다.

CyberArk 암호 저장소 설정은 선택 사항입니다. CyberArk 암호 스토리지를 설정하지 않으려면 **CyberArk** 화면 건너뛰 기를 클릭합니다.

프로시저

1. 설치 프로그램의 CyberArk 연결 페이지에서 에지 암호화 규칙 CyberArk 연결 매개변수를 입력합니다.

CyberArk 연결 매개변수

설정	설명
PasswordSDK.jar 경로	CyberArk 구성 중 호스트 Windows 머신에 설치된 `JavaPasswordSDK.jar` 파일의 경로입니다.
앱 ID	CyberArk 구성 중에 입력한 앱 **ID** 입니다.
안전 이름	CyberArk 구성 중에 입력한 안전 이름입니다 .

2. 다음을 클릭합니다.
3. 설치 프로그램의 CyberArk 보호된 자격 증명 페이지에서 CyberArk로 보호할 자격 증명을 입력하십시오.
   - 보호된 모든 암호에 대해 단일 자격 증명 이름을 사용하려면 모든 자격 증명에 하나의 자격 증명 이름 적용 확인란을 선택하고 자격 증명 이름을 입력한 다음 적용을 클릭합니다.
   - 다음 필드 중 하나 이상에 대한 자격 증명 이름을 입력합니다. 자격 증명 이름은 CyberArk 구성 중 SSH 키에 대해 입력한 사용자 이름입니다.

CyberArk 보호 자격 증명

설정	설명
에지 암호화 규칙 사용자	에지 암호화 규칙 사용자의 CyberArk 자격 증명 이름입니다.
서명 키 키 스토어	서명 키 저장소의 CyberArk 자격 증명 이름입니다.
HTTPS 인증서 키 스토어	HTTPS 인증 키 스토어의 CyberArk 자격 증명 이름입니다.
암호화 키 저장소	암호화 키 저장소의 CyberArk 자격 증명 이름입니다.
데이터베이스	데이터베이스 키 저장소의 CyberArk 자격 증명 이름입니다.
SafeNet HTTPS 인증서 키 저장소	SafeNet HTTPS 인증 키 저장소의 CyberArk 자격 증명 이름입니다.
SafeNet 서버	SafeNet 서버의 CyberArk 자격 증명 이름입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정	설명
정방향 프록시	정방향 프록시의 CyberArk 자격 증명 이름입니다.

4. 다음을 클릭합니다.

서명 키 구성

프록시 설치 관리자를 통해 에지 암호화 규칙 프록시 서버를 설치한 후 서명 키를 구성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
서명 키는 프록시 서버에서 만든 구성 및 속성의 변경 사항에 서명합니다. 서명 키는 JCEKS 키 저장소의 비대칭 RSA 키 쌍이어야 합니다.

주: 여러 프록시를 설치하는 경우 각 프록시는 동일한 서명 키를 사용해야 합니다.

프로시저
1. 설치 관리자의 서명 키 페이지에서 에지 암호화 규칙 호스트 시스템의 키 저장소를 선택하여 서명 키를 저장합니다.
   - 새 **Java** 키 저장소 생성: 새 키 저장소의 디렉터리 위치, 이름 및 암호를 입력합니다.
   - 기존 키 저장소 사용: 키 저장소 파일 위치와 암호를 입력합니다.
2. 다음을 클릭합니다.
3. 서명 키를 선택하거나 만듭니다.
   - 새 키: 이 프록시에 대한 서명 키를 만듭니다.
   - 기존 키 사용: 선택한 키 저장소의 RSA 키 쌍을 사용합니다.
   - 기존 키 임포트: 다른 키 저장소에서 RSA 키 쌍을 임포트합니다. 키 저장소 파일을 찾아 키 저장소의 암호를 입력하고 키 별칭을 선택합니다. 키에 대한 새 별칭을 제공합니다.
4. 다음을 클릭합니다.

HTTPS 인증서 구성

클라이언트가 보안 SSL 연결을 사용하여 프록시 서버에 연결할 에지 암호화 규칙 수 있도록 하려면 HTTPS 인증서를 프록시 서버로 가져옵니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
프록시는 에지 암호화 규칙 연결을 시도하는 클라이언트에 HTTPS 인증서를 제공합니다.

프로시저
1. 설치 관리자의 HTTPS 인증서 페이지에서 에지 암호화 규칙 인증서를 저장할 키 저장소를 선택합니다.
   - 새 **Java** 키 저장소 생성: 새 키 저장소의 디렉터리 위치, 이름 및 암호를 입력합니다.
   - 기존 키 저장소 사용: 키 저장소 파일 위치와 암호를 입력합니다.
2. 다음을 클릭합니다.
3. 인증서를 선택하거나 임포트합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

키 별칭은 인증서에 대해 지정된 별칭입니다.

- 기존 인증서 사용: 선택한 키 저장소에서 기존 인증서를 사용합니다.
- 파일 또는 키 스토어에서 임포트: 다른 키 스토어 또는 .cer 파일에서 인증서를 임포트합니다. 키 저장소 또는 .cer 파일을 찾아 암호를 입력하고 별칭을 선택합니다. 인증서의 새 별칭을 제공해야 합니다.

4. 다음을 클릭합니다.

AES 128비트 암호화 키 구성

프록시 설치 관리자를 통해 에지 암호화 규칙 HTTPS 인증서를 구성한 후 AES 128비트 암호화 키를 구성하여 데이터를 암호화합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
암호화 키는 `/keys` 디렉토리 내의 일반 텍스트 파일 또는 키 저장소 내의 비밀 키입니다. AES 128비트 및 AES 256비트 암호화 키에 키 저장소를 사용하는 경우 둘 다 동일한 키 저장소를 사용해야 합니다.

Edge 프록시 서버에서 SSL 인증서를 업데이트하는 경우 SSL 인증서 업데이트를 참조하세요.

프로시저

1. 암호화 키 위치를 선택합니다.

옵션	설명
파일 저장소	파일을 사용하여 단일 암호화 키를 저장합니다. `/keys` 디렉토리에 있는 기존 파일을 사용하거나 새 파일을 생성할 수 있습니다. 새 파일을 생성하려면 별칭을 입력하고 생성을 클릭합니다. 암호화 키가 포함된 파일이 생성됩니다. **주:** 이 선택 항목은 스토리지 위치와 암호화 키를 모두 지정합니다. 파일 저장소를 선택하는 경우 다음을 클릭하고 5단계로 이동합니다.
새로운 Java KeyStore 생성	암호화 키를 저장할 키 저장소를 만듭니다.
Java KeyStore 파일	기존 Java KeyStore 파일에 암호화 키를 저장합니다.

2. 다음을 클릭합니다.

3. 암호화 키를 선택하거나 생성합니다.

옵션	설명
새 키	암호화 키 및 별칭을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	주: Java KeyStore 요구사항에 따라 별칭 이름(키 이름, 키 별칭)에 소문자와 숫자를 사용해야 합니다. keytool 유틸리티에 대한 자세한 내용은 Java SE 설명서를 참조하십시오.
기존 키 사용	선택한 키 저장소에서 기존 암호화 키를 사용하십시오.
기존 키 임포트	다른 키 저장소에서 암호화 키를 임포트합니다.

4. 다음을 클릭합니다.
5. 설치 관리자에 정의된 요구 사항에 따라 인스턴스에서 키를 구성합니다.
인스턴스에서 키를 구성하려면 인스턴스로 이동하여 기본 키를 정의합니다. 인스턴스에서 암호화 키 구성를 참조하십시오. 키 별칭, 크기 및 유형이 설치 관리자에 정의된 요구 사항과 일치하는지 확인합니다.

기본 키 요구 사항



6. 인스턴스에 키가 구성되면 설치 관리자로 돌아가서 다음을 클릭합니다.

AES 256비트 암호화 키 구성

Edge 프록시 설치 관리자를 통해 AES 128비트 키를 구성한 후 필요에 따라 AES 256비트 암호화 키를 구성하여 데이터를 암호화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
암호화 키는 `/keys` 디렉토리 내의 일반 텍스트 파일 또는 키 저장소 내의 비밀 키입니다. AES 128비트 및 AES 256비트 암호화 키에 키 저장소를 사용하는 경우 두 키 모두 동일한 키 저장소를 사용해야 합니다. AES 256비트 암호화 키를 구성하지 않으려면 건너뛰 기를 선택하여 프록시 서버 설치를 계속합니다.

Edge 프록시 서버에서 SSL 인증서를 업데이트하는 경우 SSL 인증서 업데이트를 참조하세요.

프로시저

1. 암호화 키 위치를 선택합니다.

옵션	설명
파일 저장소	파일을 사용하여 단일 암호화 키를 저장합니다. `/keys` 디렉토리에 있는 기존 파일을 사용하거나 새 파일을 생성할 수 있습니다. 새 파일을 생성하려면 별칭을 입력하고 생성을 선택합니다. 암호화 키가 포함된 파일이 생성됩니다. 주: 이 선택 항목은 스토리지 위치와 암호화 키를 모두 지정합니다. 파일 저장소를 선택하는 경우 다음을 선택하고 5단계로 이동합니다.
새로운 Java KeyStore 생성	암호화 키를 저장할 키 저장소를 만듭니다.
Java KeyStore 파일	기존 Java KeyStore 파일에 암호화 키를 저장합니다.

2. 다음을 선택합니다.

3. 암호화 키를 선택하거나 생성합니다.

옵션	설명
새 키	암호화 키 및 별칭을 생성합니다. 주: Java KeyStore 요구사항에 따라 별칭 이름(키 이름, 키 별칭)에 소문자와 숫자를 사용해야 합니다. keytool 유틸리티에 대한 자세한 내용은 Java SE 설명서를 참조하십시오.
기존 키 사용	선택한 키 저장소에서 기존 암호화 키를 사용하십시오.
기존 키 임포트	다른 키 저장소에서 암호화 키를 임포트합니다.

4. 다음을 선택합니다.

5. 옵션: AES 256비트 암호화를 사용하려면 문서를 참조하십시오 AES 256비트 암호화 키 구성.

6. AES 256비트 암호화를 사용하려면 인스턴스에서 AES 256비트 기본 암호화 키도 구성해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스를 탐색하고 기본 키를 정의하여 이 작업을 수행합니다. 인스턴스에서 암호화 키 구성 문서를 참조하십시오. 키 별칭, 크기 및 유형이 설치 관리자에 정의된 요구 사항과 일치하는지 확인합니다.

7. 인스턴스에 키가 구성되면 설치 관리자로 돌아가서 다음을 선택합니다.

SSL 인증서 업데이트

Edge 프록시 서버에서 SSL 인증서를 업데이트할 때 이전 인증서를 삭제해야 합니다.

시작하기 전에
필요한 역할: admin

이 태스크 정보
Edge 프록시 서버에서 SSL 인증서를 업데이트할 때 이전 인증서도 삭제해야 합니다. 그렇지 않으면 Edge 프록시 서버가 새 인증서를 사용하도록 구성된 경우에도 이전 인증서(KeyStore 파일의 별칭 형식)가 계속 사용됩니다.

프로시저

1. Edge 프록시 서버에서 Java KeyStore의 항목을 나열합니다.

```
keytool -list -keystore keystore.jceks -storetype jceks -storepass
 MY_SUPER_PASSWORD
```

2. 이전 SSL 인증서를 제거합니다.

```
keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype
 jceks -storepass MY_SUPER_PASSWORD
```

3. 새 SSL 인증서를 Java KeyStore에 추가합니다.

에지 암호화 규칙 프록시 데이터베이스 구성

순서 유지 암호화 유형 또는 암호화 패턴을 사용하는 경우 선택적으로 프록시 데이터베이스 속성을 구성할 에지 암호화 규칙 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
순서를 유지하는 암호화 유형 또는 암호화 패턴을 사용하려면 네트워크에서 실행 중인 MySQL 데이터베이스가 필수입니다. 이 태스크는 프록시를 데이터베이스에 연결하지만 데이터베이스를 설치하거나 구성하지는 않습니다.

주: 여러 프록시 서버를 사용하는 경우 모든 프록시 서버는 동일한 프록시 데이터베이스를 사용해야 합니다. 설치 관리자에 입력된 값은 모든 프록시 서버에 대해 동일해야 합니다.

프로시저

1. 프록시 데이터베이스의 위치인 데이터베이스 URL을 확인하거나 변경합니다.
2. 이름 필드에 프록시 데이터베이스의 이름을 입력합니다.
   기본값은 *edgeencryption*입니다.
3. 프록시 데이터베이스에 액세스하기 위한 사용자 이름 및 암호를 입력합니다.
4. 다음을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에지 암호화 규칙 프록시 서버 시작

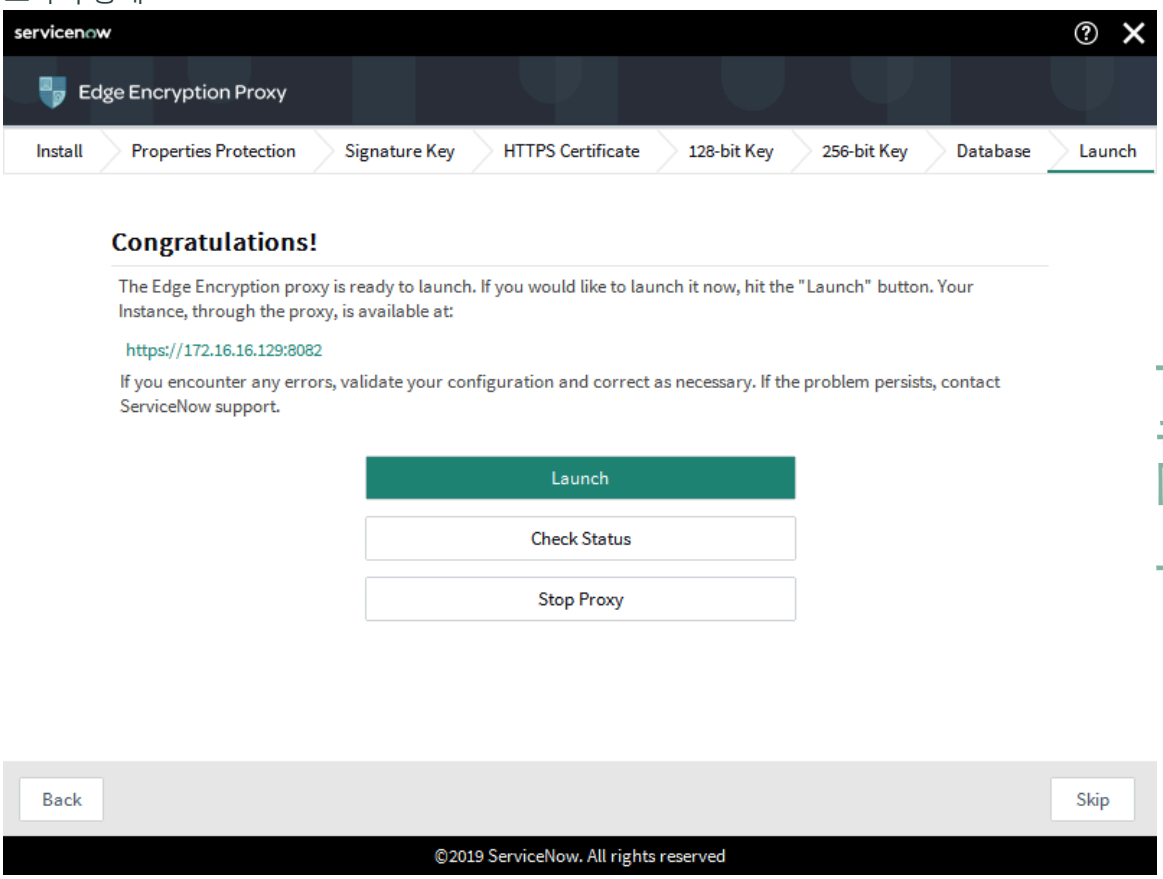
프록시를 에지 암호화 규칙 설치 및 구성한 후 설치 관리자에서 프록시를 시작할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 인스턴스에서 키를 구성하고 프록시 데이터베이스를 구성한 후 프록시 설치 프로그램으로 돌아가 에지 암호화 규칙시작을 클릭합니다.
2. 문제가 감지되거나 프록시 서버의 상태를 확인하려면 상태 확인을 클릭하여 프록시가 실행 중인지 확인할 수 있습니다.
   프록시 상태를 표시하는 메시지가 표시됩니다.

프록시 상태



다음에 수행할 작업
프록시 서버를 성공적으로 설치한 에지 암호화 규칙 후 프록시 서버 초기 메모리 제한 및 상한 메모리 제한 설정.

에지 암호화 규칙 프록시 서버 설치 확인 및 문제 해결

에지 암호화 규칙 프록시를 설치한 후 설치를 확인하여 문제를 찾거나 프록시를 시작 및 중지할 수 있습니다.

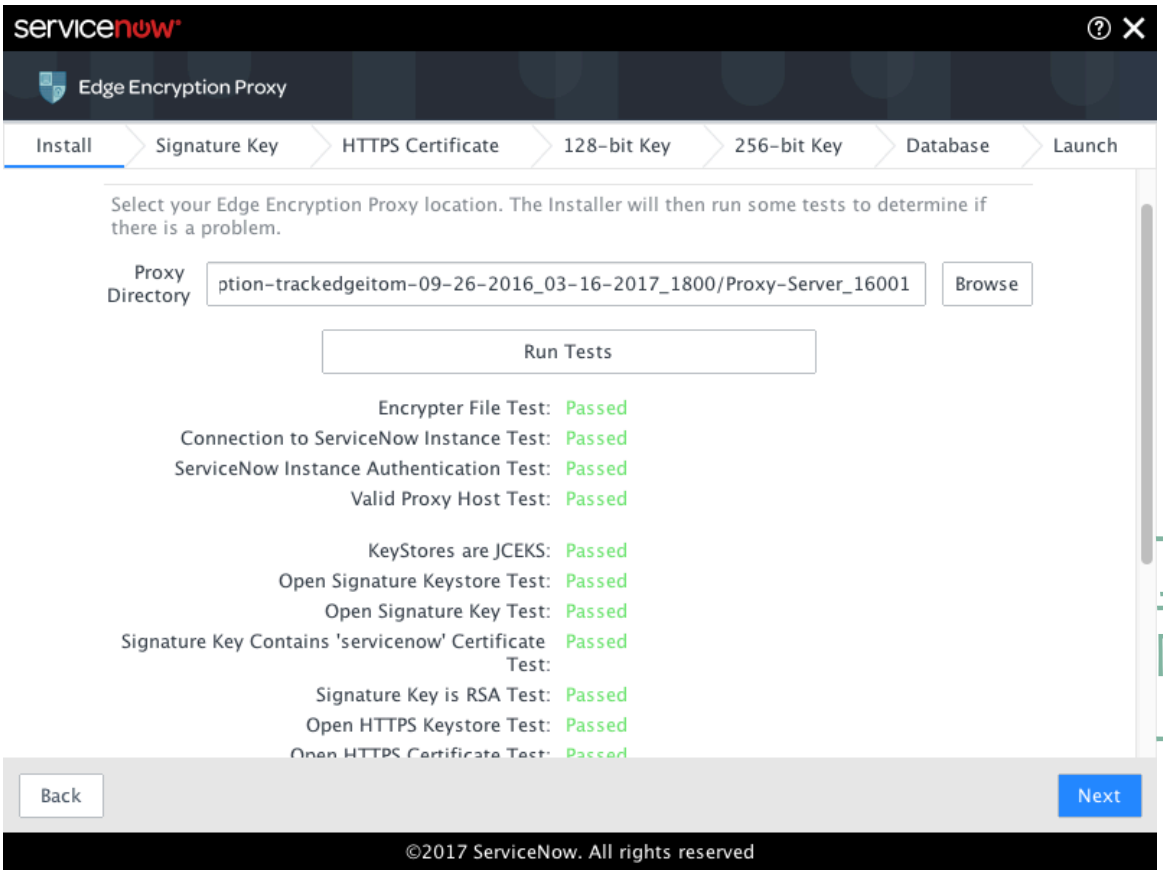
시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 에지 암호화 규칙 프록시 설치 관리자를 엽니다.
2. 설치 확인을 선택합니다.
3. 프록시 디렉터리를 클릭하고 프록시 디렉터리를 선택합니다.
4. 테스트 실행을 클릭합니다.
   테스트 결과가 표시됩니다.

에지 암호화 규칙 프록시 설치 테스트



5. 다음을 클릭합니다.
   문제가 발생하면 설치 관리자를 통해 이동하여 구성을 수정할 수 있습니다. 문제가 발생하지 않으면 설치 관리자가 실행 페이지로 이동합니다. 시작 페이지에서 프록시 상태를 확인하거나, 프록시를 중지하거나, 프록시를 시작할 수 있습니다.

명령줄 설치 관리자를 사용하여 에지 암호화 규칙 프록시 서버 설치

네트워크에 여러 에지 암호화 규칙 프록시 서버를 수동으로 설치합니다.

시작하기 전에

필요한 역할: 인스턴스의 security_admin ServiceNow 와 호스트 머신의 로컬 관리자.

순서 유지 암호화 유형 또는 암호화 패턴을 사용해야 하는 경우 네트워크의 컴퓨터에 MySQL 데이터베이스를 설정합니다(아직 없는 경우).

주: 와 함께 에지 암호화 규칙언바운딩 기술 암호화 키를 사용하는 경우 언바운딩 클라이언트 시스템에서 명령줄 설치 프로그램을 사용하여 프록시 서버를 설치합니다. 에지 암호화 규칙 프록시 서버는 언바운딩 기술 클라이언트와 동일한 컴퓨터에서 실행되어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

먼저 단일 에지 암호화 규칙 프록시 서버를 설정합니다. 첫 번째 프록시 서버가 성공적으로 실행된 후 한 인스턴스에 대한 프록시 서버를 추가하여 최적의 환경을 확보합니다. 필요한 추가 프록시 서버 수를 결정하려면 다음을 참조하십시오 에지 암호화 규칙 환경 크기 조정 .

에지 암호화 규칙 프록시 서버 설치(명령줄 설치 관리자)

64비트 Windows 또는 Linux 컴퓨터에 프록시를 에지 암호화 규칙 설치합니다.

시작하기 전에

필요한 역할: 관리자

설치 프로그램을 실행하려면 11.x 버전 시리즈의 Java 버전 11.0.6 이상이 필요합니다.

이 태스크 정보

에지 암호화 규칙 대상 컴퓨터에 적절한 명령을 사용하여 네트워크의 컴퓨터에 프록시 서버를 설치합니다. Windows 컴퓨터에 프록시 서버를 설치하는 에지 암호화 규칙 경우 프록시 서버를 Windows 서비스로 추가로 설치해야 합니다.

Edge 암호화 규칙 프록시 서버를 업그레이드하면 시스템은 현재 설치 디렉터리 아래의 `backup.dist-upgrade-<timestamp>` 디렉터리에 있는 이전 프록시를 백업합니다. 백업 디렉토리는 업그레이드 프로세스 중에 생성되고 이전 프록시 정보를 저장합니다.

명령줄을 통해 업그레이드를 실행하면 명령이 실행되는 디렉터리에 dist-upgrade.log 생성될 수 있습니다. dist-upgrade.log에는 업그레이드 프로세스에 대한 로그가 포함되어 있습니다.

업그레이드에 실패한 경우 시스템은 `failed-backup.dist-upgrade-<timestamp>` 디렉터리를 생성합니다. 또한 원래 프록시 디렉터리의 `##/wrapper.log` 에도 오류 정보가 포함될 수 있습니다.

프로시저

1. 설치 디렉터리를 만듭니다.
2. 에지 암호화 규칙 프록시 보관 파일을 설치 디렉터리에 다운로드합니다.
3. 터미널을 열고 설치 디렉터리로 변경합니다.

   주: Windows 컴퓨터에 설치하는 경우 관리자 권한으로 Windows 명령 프롬프트를 시작해야 합니다.

4. 대상 머신에 대해 이 명령을 실행하고 구성에 따라 변수를 변경합니다. `java -jar edgeencryption-<version>-all.jar -m install -n <proxy_name> --instancehost <host> -p <port> --protocol https -s <install_path>`

옵션	변수	설명
없음	버전	현재 작업을 수행하는 데 사용되는 프록시의 에지 암호화 규칙 버전 번호입니다.
-m	모드	런타임 모드. 옵션은 새 Edge 프록시 서버에 대한 "install" 또는 기존 Edge 프록시 서버를 업그레이드하는 "dist-upgrade"입니다.
-n	proxy_name	설치된 에지 암호화 규칙 프록시 서버의 이름입니다. 특정 프록시 인스턴스를 식별할

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	변수	설명
		수 있는 고유한 proxy_name 사용합니다.
--인스턴스 호스트	호스트	ServiceNow 인스턴스의 호스트 이름(예: `mycompany.service-now.com`)입니다.
-p	포트	ServiceNow 인스턴스가 수신하는 포트를 지정합니다. 일반적으로 보안 HTTPS 연결은 포트 **443** 에서 수신 대기하고 HTTP 연결은 포트 **80**에서 수신 대기합니다.
--프로토콜	프로토콜	설치된 에지 프록시가 백엔드 ServiceNow 호스트에 연결할 때 사용하는 프로토콜입니다. 이는 일반적으로 호스트 인스턴스가 지원하는 프로토콜에 따라 **HTTPS** (보안 TLS 연결에 선호됨) 또는 **HTTP** (TLS가 없는 연결)입니다.

주: 브라우저에서 명령을 복사하여 붙여넣지 마십시오. 경우에 따라 복사/붙여넣기 작업으로 인해 예기치 않은 문자가 대상 컴퓨터에 붙여넣어지고 명령이 잘못 실행되는 경우가 있습니다. 문서를 참조로 사용하여 직접 명령을 입력하는 것이 가장 좋습니다.

도움말 화면을 보려면 `-help` 옵션을 사용하여 `java -jar edgeencryption-<version>-all.jar --help` 명령을 실행합니다.

5. Windows 컴퓨터에 설치하는 경우 프록시를 에지 암호화 규칙 Windows 서비스로 설치합니다.

   a. 옵션: 새 프록시에서 `conf/wrapper.conf` 파일을 열고 다음 표의 속성을 설정하여 서비스 이름을 변경합니다.

속성	설명
wrapper.ntservice.name	프록시 서비스의 고유한 이름입니다 에지 암호화 규칙 .
wrapper.ntservice.displayname	에지 암호화 규칙 프록시 서비스 표시 이름입니다.
wrapper.ntservice.description (선택 사항)	프록시 서버 설명입니다.

   이 단계를 수행하지 에지 암호화 규칙 않으면 프록시 서비스가 에지 암호화 규칙이라는 이름으로 설치됩니다.

   b. 파일을 저장하고 닫습니다.

   c. Windows 명령 프롬프트를 열고 `cd# ServerName_port/bin`으로 `#####`.

   d. `edgeencryption.bat ###` 실행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
`ProxyName_port` 디렉토리는 현재 디렉토리에 작성됩니다. `edgeencryption.properties` 파일은 명령행의 host, port 및 protocol 값으로 업데이트됩니다.

디지털 서명을 위한 **RSA** 키 쌍 생성 및 구성

프록시 서버가 암호화 속성 및 구성에 대한 서명 변경을 위한 디지털 서명을 만드는 데 사용할 수 있는 RSA 키 쌍을 만듭니다.

시작하기 전에
필요한 역할: 관리자

디지털 서명을 생성하고 유효성을 검증하려면 RSA 키 쌍을 생성하여 JCEKS Java KeyStore에 저장해야 하며 각 프록시가 이 키 쌍을 사용하도록 구성되어야 합니다. keytool 명령을 사용하여 암호화 키 쌍을 생성합니다.

SElinux(CentOS)에 설치된 프록시와 함께 keytool 유틸리티를 사용하려면 프록시 java-installation 디렉토리에서 공유 라이브러리 로드를 활성화해야 합니다. 이렇게 하려면 다음 명령을 루트로 실행합니다.

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

Java 1.8 버전의 keytool 유틸리티를 사용해야 합니다. 유틸리티의 사본은 `<proxy install dir>java/jre/bin/keytool`에서 찾을 수 있습니다.

프로시저

1. 프록시 다운로드 디렉터리의 KeyStore 디렉터리로 변경합니다.
2. 기본 암호를 변경합니다.

   기본 암호는 *changeme*입니다.

   ```
   keytool -keystore keystore.jceks -storetype jceks -storepasswd -new
    <newpassword>
   ```

3. 암호화 키 쌍을 생성합니다.

   주: keytool 유틸리티에서 암호를 입력하라는 메시지가 표시될 때 키의 암호를 입력하지 마십시오.

   이 명령을 한 줄에 입력합니다.

   ```
   keytool -genkeypair -alias <key alias> -keyalg rsa -keystore
    keystore.jceks
   -storetype jceks -storepass <keystore password> -keysize 2048
   ```

4. 암호화 프록시 속성 파일(`edgeencryption.properties`)을 업데이트합니다.

   a. `<## ####>/conf/` 디렉터리로 변경합니다.

   b. `edgeencryption.properties` 파일을 엽니다.

   c. 디지털 서명의 속성을 입력합니다.

      이러한 속성은 모든 프록시에 대해 동일해야 합니다.

5. `edgeencryption.properties` 파일을 저장하고 닫습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 SSL 연결을 위한 인증서 임포트 및 구성

보안 SSL 연결을 사용하려면 서버 인증서를 가져와서 Java KeyStore에 추가하십시오.

시작하기 전에
필요한 역할: 관리자

Java KeyStore에 추가하기 전에 서버 인증서와 일치하는 개인 키를 가져와야 합니다.

프로시저

1. `openssl` 명령을 사용하여 CSR(인증서 서명 요청)을 생성합니다.

```
openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
```

2. CSR(위 예제의 MYCSR.csr)을 인증 기관으로 보내 서명을 받습니다.
3. `openssl` 명령을 사용하여 임포트할 P12 키 저장소를 생성합니다.

```
openssl pkcs12 -export -in MYSIGNEDCERT.pem -inkey PRIVATEKEY.key -name
 shared > MY_SERVER.p12
```

4. 인증서와 개인 키를 jceks 파일에 저장합니다.

```
keytool -importkeystore -destkeystore keystore.jceks -deststoretype
 jceks -srckeystore MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
```

   예시에 `MYALIAS` 로 표시된 별칭은 모든 값이 될 수 있습니다. 이 별칭은 `<installation directory>/conf/` 폴더에 있는 `edgeencryption.properties` 파일의 `edgeencryption.proxy.https.cert.alias` 속성에서 사용합니다.

5. Edge 프록시를 중지했다가 다시 시작합니다.

   주: 다시 시작하는 동안 프록시 서버는 잠시 동안 오프라인 상태입니다. 시간은 사용자 환경 및 프록시 서비스를 중지하고 다시 시작하는 데 걸리는 시간에 따라 결정됩니다.

키 저장소 및 암호화 키 설정

프록시 서버에서 사용하는 에지 암호화 규칙 키 저장소 및 암호화 키를 설정합니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 조직의 필요에 따라 사용할 적절한 유형의 키 저장소를 신중하게 결정하십시오.

지원되는 키 저장소	설명
파일 저장소	키는 프록시 서버에서 액세스하는 에지 암호화 규칙 파일 시스템의 파일에 저장됩니다. 파일에 저장된 암호화 키는 암호화되지 않으므로 이러한 파일을 보호하는 것은 사용자의 책임입니다.
Java 키 스토어	A Java KeyStore: ◦ Java JCEKS 키 저장소에 키를 저장합니다. ◦ 은 암호로 보호되며 파일 시스템의 파일에 키를 저장하는 것보다 더 안전합니다. ◦ 여러 키를 저장할 수 있습니다. 키 별칭은 각 키를 나타내므로 여러 키를 더 쉽게 관리할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 키 저장소	설명
	프록시는 에지 암호화 규칙# ### 디렉토리에 `keystore.jceks`라는 Java JCEKS 키 저장소 파일과 함께 제공됩니다. 이 키 스토어 파일에는 에서 서명한 ServiceNow암호화 규칙의 유효성을 검증하는 데 사용되는 공개 키가 들어 ServiceNow 있습니다.
엔터프라이즈 키 관리 **(EKM)**	**SafeNet KeySecure** 키는 SafeNet KeySecure 키 관리를 통해 저장 및 검색됩니다. 프록시 서버에서 키 저장소를 에지 암호화 규칙 구성하기 전에 Gemalto 로 라이선스를 보호하고, 라이브러리를 다운로드하고, 네트워크의 호스트 머신에 SafeNet KeySecure 키 저장소를 설치해야 합니다. 언바운드 기술 base64로 인코딩된 래핑된 암호화 키는 프록시 서버에 텍스트 파일로 에지 암호화 규칙 저장됩니다. 언바운딩 기술 구현(이전의 Dyadic Security)은 래핑 키에 대한 제어를 유지 관리합니다. 에지 암호화 규칙 프록시 서버는 언바운딩 기술 클라이언트와 동일한 컴퓨터에서 실행되어야 합니다.

주: 기본 시스템 Java JCEKS KeyStore가 아닌 다른 키 저장소를 사용하는 경우 공개 키를 키 저장소로 가져와야 ServiceNow 합니다. 공개 키 별칭은 *servicenow*입니다.

2. 로컬 네트워크에서 키 저장소 및 암호화 키를 설정합니다.

Java KeyStore 키 저장소 설정

Java KeyStore 키 저장소를 사용하여 암호화 키를 저장할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

Java 1.8 버전의 keytool 유틸리티를 사용해야 합니다. 유틸리티의 사본은 `<proxy install dir>/java/jre/bin/keytool`에서 찾을 수 있습니다.

이 태스크 정보
프록시는 에지 암호화 규칙# ### 디렉토리에 `keystore.jceks`라는 Java JCEKS 키 저장소 파일과 함께 제공됩니다. 이 키 스토어 파일에는 에서 서명한 ServiceNow암호화 규칙의 유효성을 검증하는 데 사용되는 공개 키가 들어 ServiceNow 있습니다.

프로시저

1. 키 스토어 속성을 설정합니다.

a. `<## ####>/conf/` 디렉터리로 변경합니다.

b. `edgeencryption.properties` 파일을 엽니다.

c. Java 키 스토어의 속성을 입력합니다.

2. `edgeencryption.properties` 파일을 저장하고 닫습니다.

다음에 수행할 작업
Java KeyStore를 설정한 후 Java KeyStore keytool을 사용하여 암호화 키 생성.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Java KeyStore keytool을 사용하여 암호화 키 생성

암호화 프록시 배포와 함께 제공되는 keytool을 사용하여 AES 128비트 및 AES 256비트 암호화 키를 생성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

Java 1.8 버전의 keytool 유틸리티를 사용해야 합니다. 유틸리티의 사본은 `<proxy install dir>/java/jre/bin/keytool`에서 찾을 수 있습니다.

keytool 유틸리티에 대한 자세한 내용은 Java SE 설명서를 참조하십시오.

이 태스크 정보

주: Java KeyStore를 사용하려면 별칭 이름(키 이름, 키 별칭)에 소문자와 숫자를 사용해야 합니다.

프로시저

1. 키 저장소 디렉터리 `<installation directory>/keystore/`로 변경합니다.
2. 암호화 키를 만들려면 다음 명령 중 하나를 실행합니다.

주: 키 저장소 디렉토리가 아닌 다른 디렉토리에서 이러한 명령을 실행하도록 선택하는 경우(즉, 이전 단계를 건너뛴 경우) 현재 디렉토리에서 키 저장소 디렉토리로의 경로를 포함하도록 *-keystore* 옵션을 변경해야 합니다. 예를 들어 `<## ####>\bin` 디렉터리에 있는 경우 옵션은 `-keystore .###. /keystore/keystore.jceks`입니다.

옵션	설명
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`

기본 키를 할당할 때 인스턴스에 별칭을 추가합니다.

주: 키 암호는 키 저장소 암호와 같아야 합니다.

SafeNet KeySecure 키 저장소 설정

SafeNet 키 저장소를 사용하는 경우 라이브러리 집합을 프록시 배포 디렉터리에 복사합니다.

시작하기 전에
필요한 역할: 관리자

이 단계를 수행하기 전에 SafeNet 키 저장소를 설치하고 설정해야 합니다. 라이브러리를 다운로드하려면 Thales 에서 라이선스를 확보하세요.

주: IngrianNAE 버전 8.12의 경우 `commons-collections.jar` 파일도 다운로드해야 합니다.

이 태스크 정보

주: Linux에서 파일 경로는 슬래시(/)를 사용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. <## ####>/conf/ 디렉터리로 변경하고 edgeencryption.properties 파일을 엽니다.
2. SafeNet 키 저장소의 속성을 입력합니다.

   주: 사용자 이름/비밀번호 인증 또는 클라이언트 인증서 인증을 사용하여 SafeNet 키 저장소를 구성할 수 있지만 두 가지를 조합하여 구성할 수는 없습니다.

Example

사용자 이름 및 비밀번호 인증을 사용하는 SafeNet 키 저장소의 예입니다.

```
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

클라이언트 인증서 인증을 사용하는 SafeNet 키 저장소의 예입니다. 이 인증 방법을 사용하면 SafeNet 서버 사용자 이름과 비밀번호를 속성 파일에 저장할 필요가 없습니다.

```
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
```

3. SafeNet 키 저장소에서 키를 추가하거나 생성합니다.
   기본 키를 할당할 때 인스턴스에 키 이름(별칭)을 추가합니다.
4. edgeencryption.properties 파일을 저장하고 닫습니다.

Kingston 이하에서 **London** 이상으로 업그레이드

Edge가 있는 키 스토리지에 SafeNet NAE 서버를 사용하는 경우 프록시를 이하에서 KingstonLondon 이상으로 업그레이드하기 전에 Gemalto SafeNet 클라이언트 ProtectApp JAR 파일을 복사하고 새 속성을 추가해야 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보

주: Linux에서 파일 경로는 슬래시(/)를 사용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. <## ####>/lib에서 <## ####>/nae ####로 다음 파일을 복사합니다.
   - commons-collections<version>.jar
   - ingrianlog4j-api-<version>.jar
   - ingrianlog4j-core-<version>.jar
   - ingrianNAE-<##>.jar
2. 프록시의 현재 버전(업그레이드되지 않음)에서 다음 두 속성을 추가하여 <installation directory>/conf/edgeencryption.properties 파일을 업데이트합니다.
   - *edgeencryption.ekm.provider.classname* = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   - *edgeencryption.thirdparty.vendor.library.path* = <1#### jar ### ### ##### #####>

     주: *edgeencryption.thirdparty.vendor.library.path* Java 11의 경우.
3. 변경 내용을 저장합니다.
4. 이상으로 London 업그레이드를 진행합니다.

언바운딩 기술 키 설정

base64로 인코딩된 래핑된 에지 암호화 규칙 암호화 키를 프록시 서버에 텍스트 파일로 저장하고 래핑 키 별칭을 제공하여 언바운딩 기술(이전의 Dyadic Security) 키를 에지 암호화 규칙 사용합니다. 언바운딩 기술 구현은 래핑 키에 대한 제어를 유지합니다.

시작하기 전에
필요한 역할: security_admin

언바운딩 기술 구현에서 래핑 키와 래핑 키를 모두 식별합니다. 래핑 및 패딩에 RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING 알고리즘을 사용합니다. 래핑된 키를 base64로 인코딩된 텍스트 형식으로 익스포트합니다. 키 별칭을 사용하여 파일 확장자가 없는 이름으로 파일을 저장합니다.

주: 와 함께 에지 암호화 규칙언바운딩 기술 암호화 키를 사용하는 경우 언바운딩 클라이언트 시스템에서 명령줄 설치 프로그램을 사용하여 프록시 서버를 설치합니다. 에지 암호화 규칙 프록시 서버는 언바운딩 기술 클라이언트와 동일한 컴퓨터에서 실행되어야 합니다.

프로시저

1. base64 인코딩 텍스트 형식으로 래핑된 암호화 키를 <proxy-installation-directory>/keys 디렉터리에 추가합니다.
   파일 이름은 파일 확장자가 없는 키 별칭이어야 합니다.
2. edgeencryption.properties 파일을 업데이트합니다.
   a. <proxy-installation-directory>/conf 디렉터리로 변경합니다.
   b. edgeencryption.properties 파일을 엽니다.
   c. 파일 저장소 속성을 입력하고 값을 *edgeencryption.keyfile.directory#*로 설정합니다.

      이 특성은 프록시 서버에 <Java-home-directory>/keys 디렉토리에서 암호화 키를 찾도록 지시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성에 대한 에지 암호화 규칙 자세한 내용은 Edge Encryption 프록시 서버 속성을 참조하십시오.

d. Dyadic 제공자 구성에 대한 속성의 주석 처리를 제거하고 언바운딩 구현에서 의 *edgeencryption.ekm.provider.rsa.wrapping.key.alias* 값을 래핑 키 별칭으로 설정합니다.

e. 파일을 저장하고 닫습니다.

다음에 수행할 작업

인스턴스에 암호화 키 별칭을 추가합니다. 암호화 키 별칭은 `<proxy-installation-directory>/keys` 디렉터리에 추가된 래핑된 암호화 키의 파일 이름입니다. 예를 들어 디렉터리에 있는 파일의 이름이 `myunboundkey`인 경우 이 이름을 키 별칭 필드에 추가합니다. 인스턴스에서 암호화 키 구성 문서를 참조하십시오.

파일에 저장된 암호화 키 만들기

간단한 텍스트 파일을 키 저장소로 사용할 수 있습니다. 각 파일에는 단일 암호화 키가 있습니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

이 단계에서는 키 스토리지와 암호화 키를 모두 생성합니다.

주: 키 파일의 이름은 인스턴스의 암호화 키 테이블에 지정된 키 별칭과 일치해야 합니다. 인스턴스에서 암호화 키 구성를 참조하십시오.

프로시저

1. 프록시 서버 설치 디렉터리의 `/keys` 폴더에 파일을 만듭니다.
2. 파일에 암호화 키를 추가합니다.

옵션	설명
AES 128	정확히 16바이트의 암호화 키를 파일에 넣습니다.
AES 256	정확히 32바이트의 암호화 키를 파일에 넣습니다.

3. `edgeencryption.properties` 파일을 업데이트합니다.
   a. `<## ####>/conf/` 디렉터리로 변경합니다.
   b. `edgeencryption.properties` 파일을 엽니다.
   c. 파일 저장소의 속성을 입력합니다.
   d. 파일을 저장하고 닫습니다.

인스턴스에서 암호화 키 구성

에지 암호화 규칙 는 프록시를 오프라인으로 전환하지 않고 암호화 키를 관리하는 도구를 제공합니다.

시작하기 전에

필요한 역할: security_admin

인스턴스에 새 암호화 키를 설정하기 전에 다음을 수행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 암호화 키를 생성합니다.
2. 모든 암호화 프록시에서 새 키를 사용할 수 있도록 합니다. 파일 또는 Java KeyStore 파일을 각 프록시에 복사하거나 각 프록시가 Java KeyStore 또는 EKM(Enterprise Key Management) 장치에 액세스할 수 있는지 확인하십시오.

이 태스크 정보

키 별칭은 고유해야 합니다. 각 키 별칭은 각 프록시에서 동일한 키 크기와 유형을 가져야 하며, 그렇지 않으면 키를 기본값으로 할당할 수 없습니다.

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 암호화 키 구성 > 키 설정.
2. 양식의 새 키 추가 섹션에서 다음 단계를 완료하여 새 키를 추가합니다.

> **중요사항:** SafeNet 버전 지정 키를 사용하는 경우 키 버전에 대한 추가 열이 표시됩니다. 키 버전을 편집할 수 없습니다. 관련 링크에서 최신 키 버전 검색 링크를 클릭하여 Edge 프록시에서 각 키의 최신 버전을 검색합니다.

목록에서 왼쪽 열에 **X** 가 있는 행은 삭제할 수 있습니다. 기본값으로 사용되었거나 사용 가능상태인 키는 삭제할 수 없습니다.

a. 새 행 삽입이라고 표시된 행을 두 번 클릭합니다.

b. 편집 상자에서 키 이름을 입력하고 확인 표시를 클릭합니다.

키 별칭은 소문자와 숫자입니다. 업데이트를 클릭하면 대문자가 소문자로 변경됩니다. 키 별칭은 고유해야 합니다.

> **주:** 언바운딩 기술 키를 사용하는 경우 암호화 키 별칭을 추가합니다. 암호화 키 별칭은 `<proxy-installation-directory>/keys` 디렉터리에 추가된 래핑된 암호화 키의 파일 이름입니다. 예를 들어 디렉터리에 있는 파일의 이름이 `myunboundkey`인 경우 이 이름을 키 별칭 필드에 추가합니다.

c. 같은 행에서 키 크기 열을 두 번 클릭합니다.

d. 선택 상자에서 키 크기(128비트 또는 256비트)를 선택한 다음 확인 표시를 클릭합니다.

e. 같은 행의 유형 열을 두 번 클릭합니다.

f. 선택 상자에서 키 유형(파일, 키 저장소, **SafeNet** 또는 언바운드)을 선택한 다음 확인 표시를 클릭합니다.

g. 키 추가가 완료되면 다음 단계를 클릭합니다.
진행하기 전에 각 키에 대한 별칭, 키 크기 및 키 유형을 지정해야 합니다.

3. 양식의 키 상태 섹션에서 키의 상태를 확인하고 사용 가능한지 확인합니다.
4. 키를 사용할 수 있음이면 다음 단계를 클릭합니다.
이 작업은 몇 분 정도 걸릴 수 있습니다.

> **주:** SafeNet 버전 지정 키를 사용하는 경우 키 버전에 대한 추가 열이 표시됩니다. 키 버전을 편집할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스는 모든 프록시에 사용할 수 있는 모든 암호화 키의 상태를 추적합니다. 모든 프록시에서 키를 사용할 수 있는 경우 해당 상태는 사용 가능이 됩니다. 몇 분 후에도 상태가 변경되지 않으면 모든 프록시에서 키를 사용할 수 있는지 확인합니다. 상태가 사용할 수 없음으로 유지되면 하나 이상의 프록시에 키가 없는 것입니다.

암호화 키 상태

상태	설명
사용 가능	모든 온라인 프록시에는 키가 있습니다.
사용할 수 없음	이는 새 키이며 프록시가 아직 키를 로드하지 않았거나 하나 이상의 프록시가 키를 로드하지 못했습니다.

5. 폼의 기본 키 변경 섹션에서 다음 중 하나를 수행합니다.
   - 키 별칭을 입력합니다.
   - 돋보기 아이콘을 클릭하고 별칭을 선택합니다.

   주: SafeNet 버전 관리 키를 사용하는 경우 키 버전에 대한 추가 필드가 표시됩니다. 키 버전은 회색으로 표시되며 편집할 수 없습니다. 가장 최근의 키 버전만 선택하십시오. 이전 버전을 선택한 경우 업데이트 또는 다음 단계를 클릭하면 다음 메시지가 나타납니다.

   ```
   One of the default keys chosen is not the latest version available
    for the key. Please use the latest version.
   ```

   기본 키가 SafeNet 키의 최신 버전이 아닌 경우 관련 링크에 기본 키를 최신 버전으로 업데이트 링크가 나타납니다. 링크를 클릭하여 기본 키를 업데이트하면 최신 버전을 사용할 수 있습니다.

6. 양식의 키 회전 예약 섹션에서 대량 키 회전 작업 또는 단일 키 회전 작업을 예약하여 새 암호화 키를 사용하여 기존 데이터를 암호화합니다.

   대량 키 회전 작업 또는 단일 키 회전 작업을 실행하지 않으면 데이터에 다시 액세스할 때까지 기존 데이터가 이전 키로 암호화된 상태로 유지됩니다.

에지 암호화 규칙 속성 파일에서 추가 속성 구성

네트워크에 프록시 서버를 설치하고 에지 암호화 규칙 키 저장소 및 키를 설정한 후 추가 에지 암호화 규칙 속성을 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. `<installation directory>/conf/edgeencryption.properties` 파일을 열고 다음 에지 암호화 규칙 프록시 서버 속성을 구성합니다.
   - 대상(인스턴스) 속성
   - 사용자 계정 속성
   - 프록시 속성

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 순서 유지 암호화 유형 또는 암호화 패턴을 사용하는 경우 프록시 데이터베이스 속성을 구성합니다
- 일반 텍스트 및 정적 IV 속성

2. 파일을 저장하고 닫습니다.

웹 프록시 구성

네트워크에서 웹 프록시를 사용하는 경우 웹 프록시를 사용하도록 프록시를 설정할 에지 암호화 규칙 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
네트워크에서 웹 프록시를 사용하지 않는 경우 구성 파일의 웹 프록시 속성을 주석 처리된 상태로 둡니다.

에지 암호화 규칙 프록시 서버는 웹 프록시에 대한 HTTP 연결 및 기본 인증을 지원합니다.

프로시저

1. `<## ####>/conf/` 디렉터리로 변경합니다.
2. `edgeencryption.properties` 파일을 엽니다.
3. 웹 프록시 속성을 구성합니다.
4. `edgeencryption.properties` 파일을 저장하고 닫습니다.
5. 웹 프록시가 고객 특정 서버 인증서를 사용하는 경우 프록시 서버에서 사용하는 에지 암호화 규칙 JVM에 이 인증서를 추가하여 웹 프록시와 에지 암호화 규칙 프록시 서버 간에 신뢰를 설정합니다.
   a. `cd` 명령을 사용하여 `<Java # ####>/jre/lib/security/cacerts`로 이동하십시오.
   b. `keytool -keystore cacerts -importcert -alias <chooseAlias> -file <certificateFile>` 명령을 실행합니다.

프록시 서버 초기 메모리 제한 및 상한 메모리 제한 설정

초기 메모리 한도 및 상한 메모리 한도를 설정하여 프록시 서버가 사용할 수 있는 메모리 양을 지정합니다. 구현에서 에지 암호화 규칙 성능 문제를 방지하려면 이러한 제한을 설정하십시오.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
지침에 따라 초기 메모리 제한과 상한 메모리 제한을 모두 같은 값으로 설정합니다. 모든 컴퓨터에서 2GB의 실제 메모리를 OS(운영 체제)에 할당합니다. 그런 다음, 초기 메모리 제한 및 상한 메모리 제한 속성을 사용하여 나머지 실제 메모리를 힙에 할당합니다. 예를 들어 메모리가 8GB인 컴퓨터에서 OS에 2GB를 할당하고 나머지 6GB(6144m)를 초기 및 상한 메모리에 할당합니다.

중요사항: 에지 암호화 규칙 프록시 서버가 실행 중인 경우 이러한 속성을 업데이트한 후 프록시 서버를 중지한 후 다시 시작해야 합니다.

프로시저

1. 프록시 서버 디렉터리에서 `<install dir>/conf/wrapper.conf#` 엽니다.
2. 초기 메모리 제한을 설정하려면 파일 끝에 다음 줄을 추가합니다.

```
wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

`wrapper.conf` 파일에 정의된 `wrapper.java.additional.<number>` 등록 정보 순서에 따라 `<number>`를 사용 가능한 다음 `<number>`로 설정합니다.

Example
예를 들어 `### ## wrapper.java.additional.<number>` 속성 목록이 있습니다.

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

위 목록의 최대 `<#>` 는 **2**입니다. `wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m` 줄을 추가할 때 `<number>`를 사용 가능한 다음 숫자인 **3**으로 설정합니다.

중요사항: 번호 매기기 순서에 공백을 두지 마십시오.

OS에 2GB의 메모리를 할당한 후 `<min_memory_in_MB>` 남은 메모리 메가바이트 수로 설정합니다.

3. 메모리 상한을 설정합니다.
기본 시스템에는 상한 메모리 상한이 설정되어 있지 않으므로 프록시 서버는 사용 가능한 모든 메모리를 사용할 수 있습니다. 서버에서 다른 서비스가 실행 중인 경우 상한 메모리 상한을 설정할 수 있습니다.

파일 끝에 다음 줄을 추가합니다.

`wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m`

`wrapper.conf` 파일에 정의된 `wrapper.java.additional.<number>` 등록 정보 순서에 따라 `<number>`를 사용 가능한 다음 `<number>`로 설정합니다.

Example
예를 들어 `### ## wrapper.java.additional.<number>` 속성 목록이 있습니다.

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

위 목록의 최대 `<#>` 는 **2**입니다. `wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m` 줄을 추가할 때 `<number>`를 사용 가능한 다음 숫자인 **3**으로 설정합니다.

주: 번호 매기기 순서에 공백을 두지 마십시오.

OS에 2GB의 메모리를 할당한 후 `<max_memory_in_MB>` 남은 메모리 메가바이트 수로 설정합니다.

4. 파일을 저장하고 닫습니다.

Example: 예: 프록시 서버 초기 및 상한 메모리 한계 설정

```
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
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
에지 암호화 규칙 프록시 시작.

에지 암호화 규칙 프록시 시작

프록시를 에지 암호화 규칙 설치 및 구성한 후 명령줄에서 프록시를 시작할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

암호화 프록시를 시작하기 전에 다음을 확인합니다.

- 플러그인이 에지 암호화 규칙 인스턴스에서 활성화됩니다.
- 이 컴퓨터의 `edgeencryption.properties` 파일이 구성되었습니다.
- 암호화 유형 또는 암호화 패턴을 유지하는 순서를 사용하는 경우 프록시 데이터베이스가 실행되고 있습니다.

주: `edgeencryption.properties` 파일을 처음 설정하거나 특성을 변경할 때 암호 암호화 특성을 설정하지 않을 수 있습니다. 모든 것이 작동하는지 확인한 후에는 암호 암호화 속성을 설정하고 프록시를 종료한 다음 프록시를 다시 시작할 수 있습니다.

프로시저

1. 프록시 서버를 실행합니다.

옵션	설명
Linux 컴퓨터에서	**a.** `CD`에서 `ServerName_port`로 **b.** `./startup.sh` 실행
Windows 컴퓨터에서	명령줄에서 관리자 권한으로 다음 단계를 수행합니다. **a.** `CD` 에서 `ServerName_port/bin##` **b.** `## edgeencryption.bat` 실행

2. 프록시 서버의 로그를 확인하여 프록시가 실행 중인지 확인합니다.

속성 파일에서 비밀번호 난독화

일반 텍스트 암호를 표시하지 않고 속성 파일을 공유할 수 있도록 `edgeencryption.properties` 파일에서 암호를 난독 처리합니다.

시작하기 전에
필요한 역할: 관리자

이 속성을 설정하기 전에 프록시 서버가 설정되어 있고 성공적으로 실행 중인지 에지 암호화 규칙 확인하십시오. 이 속성을 설정하기 전에 . 에지 암호화 규칙 프록시 중지

이 태스크 정보
이 속성을 설정하면 초기 시작 중에 연결 및 액세스 문제를 디버그하기 어려울 수 있습니다. 프로덕션 환경에서는 프록시가 성공적으로 설정되고 테스트된 후에만 이 속성을 설정하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. `<## ####>/conf/` 디렉터리로 변경합니다.
2. `conf` 디렉터리에서 프록시가 `edgeencryption.properties` 파일에서 암호를 난독화하는 데 사용하는 암호로 사용할 수 있는 복잡한 문자열 또는 구문이 포함된 텍스트 파일을 생성합니다. 이 암호는 암호 자체와 관련이 없는 임의의 복잡한 구문이어야 합니다.
3. `edgeencryption.properties` 파일을 엽니다.
4. 암호 암호화 속성을 설정합니다.
5. `edgeencryption.properties` 파일을 저장하고 닫습니다.

다음에 수행할 작업

이 속성을 설정한 후에는 다음을 수행할 수 있습니다 에지 암호화 규칙 프록시 시작.

추가 프록시를 수동으로 추가

첫 번째 에지 암호화 규칙 프록시가 올바르게 구성되고 테스트된 후 Linux 또는 Windows 컴퓨터에서 추가 프록시를 설정할 수 있습니다. 동일한 컴퓨터에 여러 프록시를 설치하는 것은 권장되지 않습니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

최적의 환경을 보장하기 위해 추가 머신에 프록시 서버를 추가합니다. 필요한 추가 프록시 수를 결정하려면 을 참조하십시오 에지 암호화 규칙 환경 크기 조정 .

> **주:** 모든 프록시에 암호화 구성 및 암호화 규칙에 디지털 서명하는 데 사용되는 동일한 암호화 키와 동일한 RSA 키 쌍이 있는지 확인합니다. 프록시 데이터베이스가 설치의 일부로 설정된 경우 모든 프록시는 동일한 프록시 데이터베이스를 사용해야 합니다.

프로시저

1. 적절한 명령을 사용하여 프록시를 설치합니다.
   자세한 내용은 에지 암호화 규칙 프록시 서버 설치(대화식 설치 관리자) 문서를 참조하십시오.
2. 첫 번째 프록시에서 새 프록시로 모든 암호화 키와 `edgeencryption.properties` 파일을 복사합니다.
   암호화 키는 프록시 키 저장소, `/keys` 디렉터리 또는 SafeNet KeySecure 키 저장소에 있을 수 있습니다.
3. 새 프록시에서 `edgeencryption.properties` 파일을 엽니다.
4. 다음 속성을 변경합니다.

속성	설명
edgeencryption.proxy.name	프록시 서버의 고유 이름
edgeencryption.proxy.host	프록시를 실행하는 컴퓨터의 서버 이름, IP 주소 또는 정규화된 도메인 이름입니다.
edgeencryption.proxy.http.port	HTTP 통신을 위한 프록시의 포트입니다. 컴퓨터의 모든 프로세스에서 고유해야 합니다.
edgeencryption.proxy.https.port	HTTPS 통신을 위한 프록시의 포트입니다. 컴퓨터의 프로세스 전체에서 고유해야 합니다.

5. Windows 컴퓨터에 프록시 서버를 설치하는 경우 서비스 이름을 변경해야 합니다. 새 프록시에서 `conf/wrapper.conf` 파일을 열고 다음 표에 나열된 속성을 추가합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 프록시 서버를 시작하기 전에 이 단계를 수행해야 합니다.

속성	설명
wrapper.ntservice.name	프록시 서비스의 고유한 이름입니다 에지 암호화 규칙 .
wrapper.ntservice.displayname	에지 암호화 규칙 프록시 서비스 표시 이름입니다.
wrapper.ntservice.description (옵션)	프록시 서버 설명입니다.

6. 파일을 저장하고 닫습니다.
7. 적절한 명령을 사용하여 프록시를 시작합니다.
   자세한 내용은 에지 암호화 규칙 프록시 시작 문서를 참조하십시오.

프록시 서버 인증 에지 암호화 규칙

프록시 서버가 해당 프록시 서버에서 들어오는 요청을 처리할 수 있도록 에지 암호화 규칙 신뢰할 수 있는 소스임을 지정합니다.

시작하기 전에

프록시 서버가 인증되지 않은 경우 콘솔 로그에는 다음 메시지가 포함됩니다.

```
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.
```

프록시에 액세스하려고 하면 다음 메시지가 표시됩니다. 이 `#### ### # ####`.

업그레이드 프로세스 중에 프록시를 작동 상태로 유지하려면 프록시 업데이트가 성공할 때까지 인증이 필요하지 않습니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 프록시.
2. 프록시를 선택하고 Authenticate(인증)를 클릭합니다.

결과

프록시가 인증되지 않음 에서 보류 중 , 인증됨으로 이동합니다. 인증을 시작하면 상태가 인증되지 않음 에서 보류 중 으로 변경됩니다. 인증이 완료되면 상태가 보류 중에서인증됨으로 변경되고 프록시 에지 암호화 규칙 에 액세스하고 프록시의 요청을 수락할 수 있습니다.

주: 프록시를 중지한 후 다시 시작하면 프록시가 인증된 상태로 유지되고 성공적으로 다시 시작됩니다.

에지 암호화 규칙 프록시 중지

명령줄에서 프록시를 에지 암호화 규칙 중지할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 프록시 서버를 중지합니다.

옵션	설명
Linux 컴퓨터에서	`./shutdown.sh` 실행
Windows 컴퓨터에서	`## edgeencryption.bat` 실행 Windows 서비스를 제거하려면 `edgeencryption.bat ##`를 실행합니다.

2. 프록시 서버의 로그를 확인하여 프록시가 중지되었는지 확인합니다.

Linux에서 에지 암호화 규칙 프록시 제거

프록시를 에지 암호화 규칙 제거할 수 있습니다. 프록시를 업그레이드하는 경우 현재 버전을 종료하고 제거할 필요가 없습니다.

시작하기 전에
필요한 역할: 관리자

프록시를 에지 암호화 규칙 실행하는 컴퓨터에 대한 액세스 권한이 있어야 합니다.

이 태스크 정보
프록시를 에지 암호화 규칙 종료하기 전에 프록시를 사용하여 인스턴스에 연결된 사용자가 없는지 확인합니다.

Linux에서 실행되는 암호화 프록시는 단일 프로세스로 작동합니다. 이 프로세스를 종료하여 암호화 프록시를 다른 호스트 시스템에 재배포하거나, 프록시 버전을 업데이트하거나, Java 버전을 업데이트하거나, 여러 프록시 서버에 암호화 프록시를 배포할 때 암호화 프록시의 고유 이름을 변경하는 등의 작업을 수행할 수 있습니다.

프로시저

1. 배포 디렉터리를 삭제하기 전에 `edgeencryption.properties` 파일을 저장할 수 있습니다.
2. `shutdown.sh` 셸 스크립트를 실행합니다.
3. 프록시 서버의 로그를 확인하여 프록시 서버가 종료되었는지 확인합니다.
4. 배포 폴더에 있는 파일을 삭제합니다.

Windows에서 에지 암호화 규칙 프록시 제거

프록시를 에지 암호화 규칙 제거할 수 있습니다. 프록시를 업그레이드하는 경우 현재 버전을 종료하고 제거할 필요가 없습니다.

시작하기 전에
필요한 역할: 관리자

프록시를 에지 암호화 규칙 실행하는 컴퓨터에 대한 액세스 권한이 있어야 합니다.

프록시를 에지 암호화 규칙 종료하기 전에 프록시를 사용하여 인스턴스에 연결된 사용자가 없는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 배포 디렉터리를 삭제하기 전에 `edgeencryption.properties` 파일을 저장할 수 있습니다.
2. `## edgeencryption.bat` 실행
3. `## edgeencryption.bat ##`
4. 프록시 서버의 로그를 확인하여 프록시 서버가 종료되었는지 확인합니다.
5. 배포 폴더에 있는 파일을 삭제합니다.

를 사용하여 복수 제공자 **SSO** 설정 에지 암호화 규칙

프록시 서버 URL 또는 인스턴스 URL을 통해 에지 암호화 규칙 로그인할 수 있도록 복수 제공자 SSO를 설정합니다. 활성화된 상태에서 에지 암호화 규칙 여러 제공자 1회 사용자 인증(SSO)을 구현하는 경우 일부 사용자는 프록시 서버를 통해 에지 암호화 규칙 인스턴스에 로그인해야 할 수 있지만 다른 사용자는 로그인하지 않을 수 있습니다.

시작하기 전에

- 통합 - 다중 제공자 1회 사용자 인증(SSO) 설치 관리자 플러그인 (com.snc.integration.sso.multi.installer)을 활성화합니다.
- 플러그인(com.glide.edgeencryption)을 에지 암호화 규칙 활성화하고 하나 이상의 프록시 서버가 네트워크에 설정되어 있는지 확인합니다.
- 사용자가 복수 제공자 SSO를 사용하여 로그인할 프록시 서버의 URL을 에지 암호화 규칙 결정합니다. 프록시 서버의 URL 에지 암호화 규칙 을 확인하려면 을 참조하십시오 에지 암호화 규칙 설치.

필요한 역할: 관리자

이 태스크 정보
로그인하는 사용자는 Edge 프록시를 사용하거나 Edge 프록시를 사용하지 않고 적절한 URL을 사용하여 로그인해야 합니다.

- 모든 사용자를 프록시 서버를 통해 라우팅하는 에지 암호화 규칙 경우 ID 제공자 기록을 설정하고 **ServiceNow** 홈페이지, 엔터티 ID/발급자 및 대상 **URI** 필드에 프록시 서버 URL을 정의합니다.
- 일부 사용자는 프록시 서버를 통해 라우팅하고 일부 사용자는 인스턴스로 라우팅하려면 두 개의 ID 제공자 기록을 생성합니다. 두 기록 모두 **ID** 제공자 **URL** 필드에서 동일한 값을 사용합니다. 그러나 기록 중 하나는 프록시 서버를 통해 라우팅되고 다른 하나는 인스턴스로 라우팅됩니다.
  - 인스턴스 이름을 통해 로그인: `https://<instance name>.service-now.com/login_with_sso.do?glide_sso_id=` 비 에지 프록시에 대한 IdP 기록의 <sys_id
  - 에지 프록시를 통해 로그인: 에지 프록시에 대한 `IdP ### https://<edge hostname>:<port>/login_with_sso.do?glide_sso_id=<sys_id`

프로시저

1. ID 제공자 기록에서 ID 제공자 URL의 중복을 활성화합니다.
   고유한 제약 조건은 두 개의 서로 다른 ID 제공자 기록에서 ID 제공자 URL이 중복되는 것을 방지합니다. 필드를 false로 설정하여 여러 IdP 기록에서 ID 제공자 URL의 중복을 활성화할 수 있습니다.
   a. 다음으로 이동 시스템 정의 > 딕셔너리.
   b. ID 제공자 테이블 〔saml2_update1_properties〕에서 **idp** 필드에 대한 정의 기록을 엽니다.
   c. 고유 필드를 추가하도록 양식을 구성합니다.
   d. 고유 필드의 값이 **false**로 설정되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 다음으로 이동 복수 제공자 **SSO** > **ID** 제공자.
3. 동일한 ID 제공자에 대해 두 개의 ID 제공자 기록을 만듭니다. 하나는 인스턴스 URL을 사용하고 다른 하나는 프록시 서버 URL을 에지 암호화 규칙 사용합니다.
   신원 확인 제공자 기록을 생성하려면 외부 신원 확인 제공자 생성을 참조하십시오.

   a. 프록시 서버 URL의 에지 암호화 규칙 경우 다음 값을 사용하여 양식을 작성합니다.

필드	값
계정 제공자 URL	IdP 메타데이터에서 임포트됩니다.
ServiceNow 홈페이지	프록시 서버 홈페이지의 URL입니다. 예: `https://<proxy hostname>:<port>/navpage.do`
엔터티 ID/발급자	`https://<### ### ##>:<port>`
대상 그룹 URI	`https://<### ### ##>:<port>`

   b. 제출을 클릭합니다.

   c. 인스턴스 URL의 경우 다음 값을 사용하여 양식을 작성합니다.

필드	값
계정 제공자 URL	IdP 메타데이터에서 임포트됩니다.
ServiceNow 홈페이지	`https://<instance>.service-now.com/navpage.do`
엔터티 ID/발급자	`https://<instance>.service-now.com/navpage.do`
대상 그룹 URI	`https://<instance>.service-now.com/navpage.do`

   d. 제출을 클릭합니다.

4. 옵션: 둘 이상의 ID 제공자를 사용하는 경우 MultiSSO 설치 종료를 수정합니다.

   a. 다음으로 이동 시스템 정의 > 설치 종료.
   시스템에 현재 설치 종료 목록이 표시됩니다.

   b. **MultiSSO** 설치 종료를 엽니다.

   c. 스크립트 필드에서 다음 문을 찾습니다.

```
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);
    }
}
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

d. 문을 다음 코드로 바꿉니다.

```
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) {
      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);
   }
```

주: IdP 시작 로그인은 이 구성에서 작동하지 않습니다.

e. 업데이트를 클릭합니다.

5. 옵션: 둘 이상의 회사를 사용하는 경우 복수 제공자 SSO에 맞게 사용자를 구성하고 사용자에 따라 ID 제공자 기록의 sys_id 업데이트합니다.

(Optional) 자세한 내용은 다중 제공자 SSO에 대한 사용자 구성을 참조하십시오.

- 프록시 서버를 통해 에지 암호화 규칙 로그인하도록 사용자를 구성하려면 프록시 서버 URL을 에지 암호화 규칙 사용하는 ID 제공자 기록의 sys_id 사용합니다.
- 인스턴스에 로그인하도록 사용자를 구성하려면 인스턴스 URL을 사용하는 ID 제공자 기록의 sys_id 사용합니다.

로그인 **URL**

URL	로그인 대상
`https://<proxy hostname>:<port>/login_with_sso.do?glide_sso_id=#### URL# ## IdP ### <sys_id>`	프록시 서버를 통해 로그인합니다.
`https://<#### ##>.service-now.com/login_with_sso.do?glide_sso_id=#### URL# ## IdP ### <sys_id>`	인스턴스를 통해 로그인합니다.

에지 암호화 규칙 프록시 서버 속성

`<## ####>/conf/` 폴더에 있는 `edgeencryption.properties` 구성 파일에는 환경을 구성하는 데 사용되는 속성이 포함되어 있습니다.

프록시 서버 속성을 변경한 후 프록시 서버를 다시 시작해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일반 텍스트 및 정적 IV 속성

EdgeEncryption.Customer.Assigned.Known.Cleartext	두 프록시가 동일한 키를 사용하고 있는지 인스턴스가 확인할 수 있도록 하는 명확한 텍스트입니다. 시작 시 프록시는 일반 텍스트를 암호화하고 암호화된 텍스트를 인스턴스로 보냅니다. 인스턴스는 명확한 텍스트를 알지 못하며 키가 인스턴스로 전송되지 않습니다. 이 속성은 모든 프록시에 대해 동일해야 합니다.
edgeencryption.encrypter.static.iv	동일성 유지 및 순서 유지 암호화에 사용되는 정적 IV(초기화 벡터)입니다. 이 속성은 모든 프록시에 대해 동일해야 하며 정확히 16바이트(16개의 ASCII 문자)여야 합니다.

디지털 서명 속성

edgeencryption.proxy.signature.keystore.path	경로 및 Java KeyStore 파일 이름입니다.
edgeencryption.proxy.signature.keystore.password	암호 기본 암호는 〈changeme〉입니다. Java KeyStore를 설치한 후 암호를 변경합니다.
EdgeEncryption.proxy.signature.keystore.keyalias	RSA 키 페어가 생성될 때 -alias 인수로 지정된 키 별칭입니다.

파일 저장소 속성

edgeencryption.keyfile.directory	디렉터리는 키 파일이 저장되는 위치를 지정합니다. 자바 KeyStore 또는 SafeNet KeySecure 키 저장소를 사용하는 경우 이 속성을 주석 처리된 상태로 둡니다. 예제: `edgeencryption.keyfile.directory=keys` 언바운딩 기술 키를 사용하는 경우 이 속성의 주석 처리를 제거하고 값을 keys 디렉터리로 설정합니다.

일반 구성 속성

edgeencryption.config.poll.interval	폴링 간격(초)입니다. 기본 설정은 프록시가 암호화 구성 변경 내용을 학습하는 데 5초가 걸린다는 것을 의미합니다. 값이 클수록 인스턴스가 오프라인 프록시를 탐지하는 데 시간이 더 오래 걸립니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

	⚠ 경고: 이 속성은 변경하지 마십시오. 프록시 폴링 간격의 기본 설정을 변경하면 프록시가 온라인 상태가 될 때 탐지 지연이 발생할 수 있습니다.
edgeencryption.rules.dir	암호화 규칙이 프록시에 저장되는 폴더입니다.
edgeencryption.encryption.order_preserving.cache.enable	설정을 캐싱하여 순서 유지 암호화 유형을 지원하는 데 사용되는지 여부를 결정합니다.
edgeencryption.encryption.order_preserving.cache.size	최대 캐시 크기(바이트)입니다.
EdgeEncryption.jobs.concurrency	이 프록시에서 동시에 실행할 수 있는 대량 암호화 작업의 최대 수입니다.
edgeencryption.jobs.requests_per_second	이 프록시에서 인스턴스로 보낼 수 있는 초당 http 작업 요청 수입니다.
EdgeEncryption.attachments.request.timeout.seconds	첨부 파일 업로드 요청 시간 제한(초)입니다.
EdgeEncryption.request.buffer.size	암호화 요청의 크기입니다. 암호화 요청이 이 크기보다 크면 초과분은 디스크에 저장됩니다. ⚠ 경고: 이 속성은 변경하지 마십시오.
EdgeEncryption.httpclient.request.buffer.size	클라이언트 요청의 크기입니다. 클라이언트 요청이 이 크기보다 크면 초과분이 디스크에 저장됩니다. ⚠ 경고: 이 속성은 변경하지 마십시오.
edgeEncryption.httpclient.header.size	요청/응답 헤더의 크기입니다. • 최소값: 8K • 최대값: 32K ⚠ 경고: 이 속성은 변경하지 마십시오.
edgeencryption.proxy.idle.timeout	트랜잭션 시간이 초과되기까지의 시간(초)입니다. 기본값: 300(초)
edgeencryption.proxy.keepalive.interval	프록시에서 인스턴스에 대해 발급한 ping 사이의 시간(초)입니다. 프록시와 인스턴스 간의 연결을 확인하기 위해 Ping이 주기적으로 발행됩니다. • 기본값: 10(초) • 최소값: 5(초)
EdgeEncryption.register.retry.count	프록시가 등록을 시도하도록 인스턴스를 ping하는 최대 횟수입니다. 기본값: 0(제한 없음)
edgeencryption.tokenization.exclusion.list	암호화 패턴은 이러한 필드에 있는 문자열을 토큰화할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Java KeyStore 속성

edgeencryption.keystore.path	Java 키 스토어의 경로입니다. 파일 저장소 또는 SafeNet KeySecure 키 저장소를 사용하는 경우 이 속성을 주석 처리된 상태로 둡니다. 예제: `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	프록시가 Java KeyStore에 연결하는 데 사용하는 암호입니다. 파일 저장소 또는 SafeNet KeySecure 키 저장소를 사용하는 경우 이 속성을 주석 처리된 상태로 둡니다.

로깅 속성

로깅 속성은 `<installation ####>/conf/` 디렉토리에 있는 lo4gj2.properties 파일에 있습니다. 이러한 속성은 문제 해결 또는 지원 부서의 지시가 ServiceNow 있는 경우에만 변경됩니다. 자세한 내용은 에지 암호화 규칙 프록시에 대한 디버그 로깅을 늘리는 방법을 참조하세요.

NAE 장치 키 저장소 속성

edgeencryption.nae.retries	재시도 횟수입니다.
edgeencryption.nae.enabled	설정은 NAE 장치를 사용할 수 있는지 여부를 나타냅니다.
edgeencryption.nae.server	NAE 서버의 이름입니다.
edgeencryption.nae.port	NAE 서버에서 사용하는 포트입니다.
edgeencryption.nae.protocol	NAE 서버에서 사용하는 프로토콜입니다.
edgeencryption.nae.keystore.path	NAE 서버의 키 저장소 경로입니다.
edgeencryption.nae.keystore.password	NAE 키 저장소 암호입니다.
edgeencryption.nae.username	NAE 장치로 인증하는 데 사용할 사용자 이름입니다.
edgeencryption.nae.password	NAE 장치로 인증하는 데 사용할 암호입니다.
edgeencryption.nae.client.certificate	NAE 서버의 키 저장소에 있는 인증서입니다. 사용자 이름과 암호 대신 인증서를 사용하여 인증하려면 이 속성을 설정합니다.

암호 속성

edgeencryption.encrypter.properties.password	`edgeencryption.properties` 파일에서 암호를 난독 처리하기 위해 보안 프로세스 내에서 사용되는 문자열이 포함된 `conf` 폴더의 파일 이름입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

	주: `edgeencryption.properties` 파일에서 암호를 난독 처리하기 위해 보안 프로세스 내에서 사용되는 문자열이 포함된 `conf` 폴더의 파일 이름입니다.

프록시 속성

edgeencryption.proxy.host	프록시를 실행하는 컴퓨터의 서버 이름, IP 주소 또는 정규화된 도메인 이름입니다. 포트와 함께 이 속성은 클라이언트가 프록시 서버에 액세스하는 데 사용하는 URL을 정의합니다.
edgeencryption.proxy.name	프록시 이름입니다. 각 프록시에 대해 고유해야 합니다.
edgeencryption.proxy.http.port	HTTP 통신을 위한 프록시의 포트입니다.
edgeencryption.proxy.https.port	HTTPS 통신을 위한 프록시의 포트입니다.

프록시 구성 잠금 속성

edgeencryption.proxy.locked	true인 경우 프록시는 인스턴스의 암호화 구성 변경 또는 암호화 규칙 변경을 수락하지 않습니다. 모든 암호화 구성 및 규칙이 최종화된 후 프로덕션 인스턴스에서 이 속성을 설정합니다.

프록시 데이터베이스 속성

edgeencryption.db.url	프록시 데이터베이스 위치입니다. 동일한 인스턴스에 연결하는 모든 암호화 프록시에 대해 동일해야 합니다.
edgeencryption.db.user	프록시 데이터베이스에 액세스하기 위한 사용자 이름입니다. 동일한 인스턴스에 연결하는 모든 암호화 프록시에 대해 동일해야 합니다.
edgeencryption.db.password	프록시 데이터베이스에 액세스하기 위한 암호입니다. 동일한 인스턴스에 연결하는 모든 암호화 프록시에 대해 동일해야 합니다.
edgeencryption.db.name	프록시 데이터베이스 이름입니다. 동일한 인스턴스에 연결하는 모든 암호화 프록시에 대해 동일해야 합니다. 이 속성의 기본값은 `edgeencryption`입니다.
edgeencryption.db.bootstrap.file	프록시 데이터베이스의 부트스트랩 파일입니다. 파일은 `sql/` 디렉토리에 상대적입니다. 동일한 인스턴스에 연결하는 모든 암호화 프록시에 대해 동일해야 합니다. 경고: 정상적인 상황에서는 이 매개변수를 변경하지 마십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프록시 서버 성능 속성

프록시 서버 성능 속성은 기본적으로 구성 파일에 없습니다. 기본값을 변경하려면 속성을 추가하고 프록시 서버를 다시 시작해야 합니다. 자세한 내용은 Edge Encryption 진단 및 성능을(를) 참조하십시오.

edgeencryption.stat.collection.enabled	프록시 서버 성능 대시보드에서 사용하는 통계 수집을 에지 암호화 규칙 활성화합니다. 기본값: true 프록시 서버 성능 대시보드에서 사용하는 통계 수집을 사용하지 않도록 설정하려면 이 속성을 추가하고 값을 false로 에지 암호화 규칙 설정합니다.
edgeencryption.stat.collection.interval	프록시 서버가 통계를 수집하는 간격 길이(초)입니다 에지 암호화 규칙 . 값은 30초보다 작을 수 없습니다. 기본값: 30(초)

SSL 인증서 속성

SSL 인증서 속성의 값을 변경하는 경우 프록시를 다시 시작합니다. 시스템은 시작 시 HTTPS 키 쌍을 사용하여 프록시 서버 연결을 설정하고 프록시가 클라이언트 요청에 응답하는 방법을 결정합니다.

edgeencryption.proxy.https.cert.alias	프록시 서버에서 연결 클라이언트에 제공하는 인증서의 별칭입니다.
edgeencryption.proxy.https.keystore.path	HTTPS 인증서가 들어 있는 키 저장소의 경로입니다.
edgeencryption.proxy.https.keystore.password	HTTPS 인증서가 들어 있는 키 저장소의 암호입니다.

대상(인스턴스) 속성

edgeencryption.target.host	인스턴스의 호스트 이름입니다. 동일한 인스턴스에 연결하는 모든 암호화 프록시에 대해 동일해야 합니다. 이 속성은 프록시가 설치될 때 설정됩니다. 예: `instancename.servicenow.com`
edgeencryption.target.port	인스턴스 포트입니다. 동일한 인스턴스에 연결하는 모든 암호화 프록시에 대해 동일해야 합니다. 이 속성은 프록시가 설치될 때 설정됩니다.
edgeencryption.target.protocol	인스턴스 프로토콜입니다. 동일한 인스턴스에 연결하는 모든 암호화 프록시에 대해 동일해야 합니다. 이 속성은 프록시가 설치될 때 설정됩니다. 옵션은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

	• http • https

언바운딩 기술 제공자 속성

edgeencryption.ekm.provider.classname	구현에 대한 내부 클래스 이름입니다. ⚠ 경고: 이 속성은 변경하지 마십시오.
edgeEncryption.thirdparty.vendor.library.path	언바운딩된 클라이언트 머신의 언바운딩된 API JAR 파일 경로입니다.
edgeencryption.ekm.provider.rsa.wrapping.key.alias	언바운딩 기술 구현의 래핑 키 별칭입니다. 모든 프록시에 대해 동일해야 합니다.

사용자 계정 속성

edgeencryption.target.username	프록시가 인스턴스에 로그인하는 데 사용하는 사용자 이름입니다. 사용자에게 edge_encryption 역할이 있어야 합니다. 에지 암호화 규칙 사용자 계정 설정를 참조하십시오.
edgeEncryption.target.password	프록시가 인스턴스에 로그인하는 데 사용하는 암호입니다.

웹 프록시 속성

edgeencryption.webproxy.host	웹 프록시 이름 또는 IP 주소입니다.
edgeencryption.webproxy.port	웹 프록시의 포트입니다.
edgeencryption.webproxy.user	웹 프록시에 연결하는 데 사용되는 사용자 이름입니다. 웹 프록시가 인증을 사용하지 않는 경우 이 속성을 주석 처리된 상태로 둡니다.
edgeencryption.webproxy.password	웹 프록시에 연결하는 데 사용할 암호입니다. 웹 프록시가 인증을 사용하지 않는 경우 이 속성을 주석 처리된 상태로 둡니다.

사용되지 않는 프록시 암호화 속성

edgeencryption.encrypter.default.key128

현재 AES 128 키의 이름을 지정합니다. AES 128 키를 사용하지 않는 경우에도 사용할 수 있어야 합니다. 모든 프록시에 대해 동일해야 합니다.

인스턴스에서 이러한 키의 유지관리를 수행합니다.

edgeencryption.encrypter.default.key256

현재 AES 256 키의 이름을 지정합니다. 모든 프록시에 대해 동일해야 합니다.

인스턴스에서 이러한 키의 유지관리를 수행합니다.

edgeencryption.encrypter.key

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

각 키의 키 이름을 지정하며 기본 키를 지정하는 데 사용됩니다. 이 별칭은 각 암호화된 항목에 포함되므로 인스턴스에 저장되는 메타데이터와 통합된 키 별칭입니다. 키 이름은 소문자를 사용해야 합니다.

edgeencryption.encrypter.type

암호화 키 저장소 시스템의 유형을 지정합니다.

edgeencryption.encrypter.파일

키와 연결된 텍스트 파일의 경로와 파일 이름을 지정합니다.

edgeencryption.encrypter.password

키 스토어에 액세스하기 위한 암호를 지정합니다.

CyberArk와 **Edge** 프록시 서버의 통합

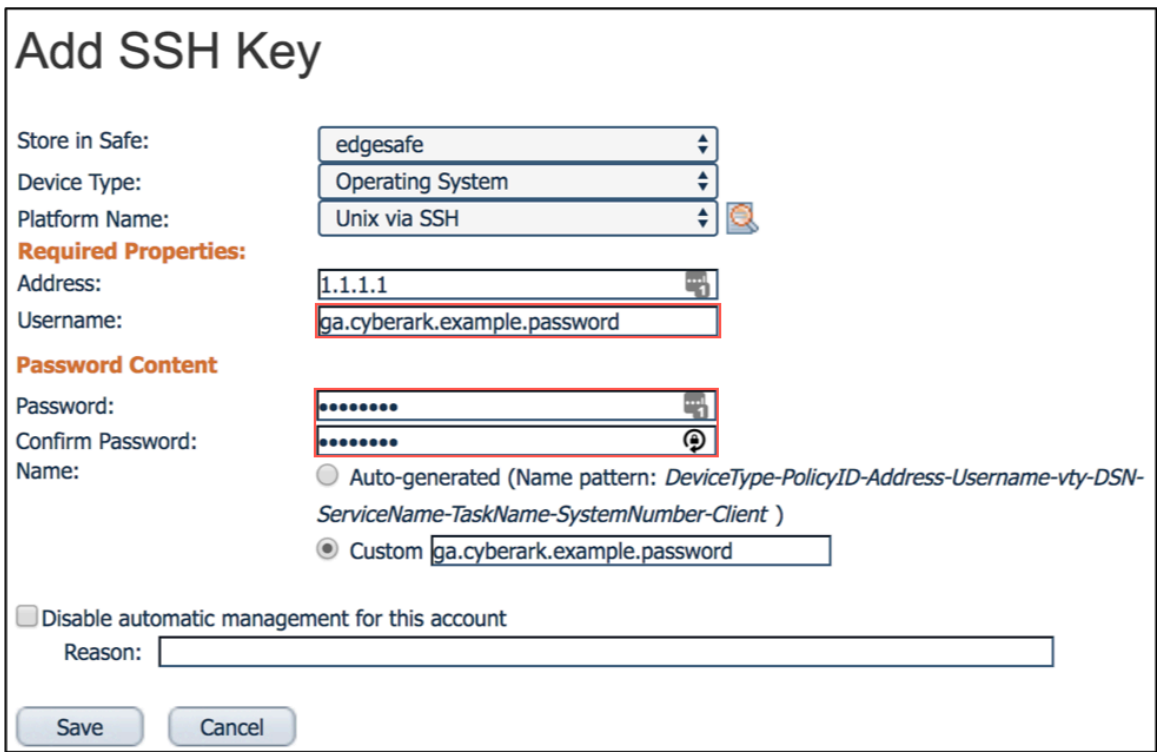
CyberArk를 사용하여 중앙 집중식 보안 디지털 볼트에 암호를 저장하여 이전에 일반 텍스트로 저장되고 파일 액세스로 보호되었거나 이전에 두 번째 파일을 통해 암호화된 암호를 보호합니다.

CyberArk AIM(Application Identity Management)은 하드 코딩되고 표시되는 암호를 제거하여 무단 액세스를 방지합니다. AIM은 비밀번호가 디지털 자격 증명으로 표시되는 독립적인 강화 서버의 디지털 볼트에 비밀번호를 저장합니다. AIM 클라이언트(Edge 프록시 서버)는 CyberArk 디지털 자격 증명을 사용하고 독립 서버에 액세스하여 보안 암호를 검색합니다. 암호는 에지 프록시 서버 또는 인스턴스에 저장되지 않습니다.

CyberArk Digital Vault 자격 증명

Edge 프록시 서버와 CyberArk 통합을 설정하려면 먼저 CyberArk를 구입하고 구성해야 합니다.

CyberArk에 자격 증명을 추가하려면(Edge 프록시에서 읽음) 자격 증명의 플랫폼 이름을SSH를 통해 **Unix** 로 설정하고 사용자 지정 자격 증명 이름을 생성하거나 자동 생성된 자격 증명 이름을 적어 둡니다. 이 자격 증명을 사용하도록 에지 프록시를 구성하면 프록시 서버는 이 자격 증명 이름을 프록시의 설정과 일치시킵니다.



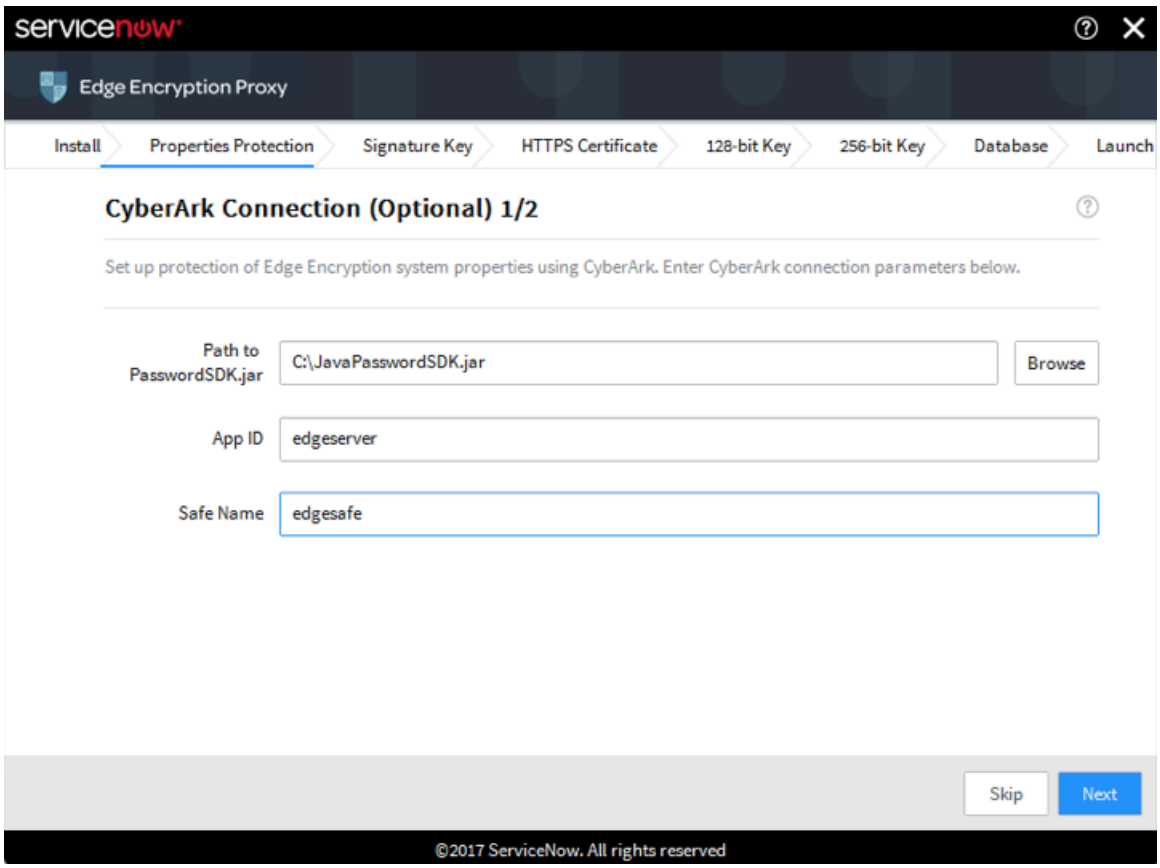
각 자격 증명 항목에는 보호되는 암호 와 애플리케이션에서 해당 암호에 액세스하는 데 사용하는 자격 증명 이름이 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: CyberArk 자격 증명은 암호화 키가 아닙니다.

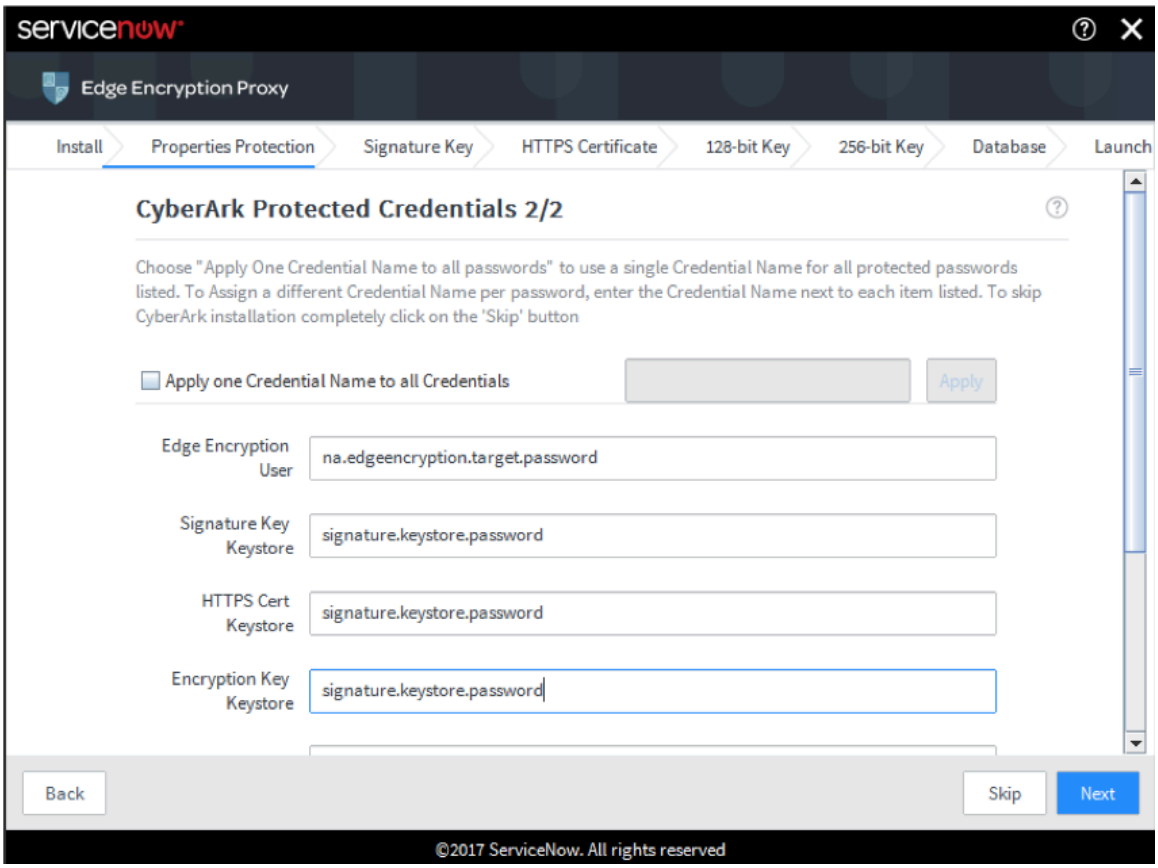
Edge 프록시 설치 중 CyberArk 추가

프록시 설치 관리자에는 CyberArk 통합을 위한 새 구성 페이지가 포함되어 있습니다. 프록시 설치 프로그램을 사용하여 프록시를 설치할 때 CyberArk를 포함하지 않으려는 경우 이 페이지는 선택 사항입니다. 구성 파일에서 CyberArk 통합을 수동으로 설정하고 구성할 수도 있습니다.



프록시 설치 프로그램에는 CyberArk로 보호되는 자격 증명을 위한 새 페이지도 포함되어 있습니다. 이 페이지에서는 단일 자격 증명 이름 또는 여러 자격 증명 이름을 사용하여 다양한 속성을 구성할 수 있습니다. 프록시 설치 프로그램을 사용하여 프록시를 설치할 때 CyberArk를 포함하지 않으려는 경우 이 페이지는 선택 사항입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



CyberArk 암호 보호

CyberArk 볼트에 CyberArk 자격 증명이 구성되어 있고 설치 관리자의 CyberArk 보호된 자격 증명 페이지에 지정된 Edge 프록시 설치 관리자의 암호 필드는 회색으로 표시되고 `CyberArk# ###` 메시지가 포함되어 있습니다.

에지 프록시 서버에서 부하 분산 장치 사용

부하 분산 장치를 사용하여 에지 암호화 규칙 프록시 설정의 프록시 서버 간에 부하를 분산할 수 있습니다. 부하 분산 장치 및 프록시 서버가 서로 다른 포트를 사용하는 경우 부하 분산 장치의 호스트 이름과 HTTPS 포트를 지정하여 사용자가 브라우저에서 응답을 볼 수 있도록 합니다.

중요사항: 모든 프로덕션 환경에는 중복성을 위해 두 개 이상의 에지 암호화 규칙 프록시 서버가 포함되어야 합니다.

부하 분산 장치 없이 에지 요청 처리

부하 분산 장치를 사용하지 않는 경우 아래 설명과 같이 요청이 처리됩니다.

1. 사용자가 브라우저에서 요청을 발행합니다.
2. 브라우저는 에지 프록시 서버로 요청을 보냅니다.
3. 프록시 서버는 ServiceNow 인스턴스에 요청을 보냅니다.
4. ServiceNow 인스턴스는 프록시 서버에 대한 응답을 반환합니다.
5. 프록시 서버는 사용자의 브라우저에 응답을 반환하기 전에 응답 헤더에 자체 포트 번호를 추가합니다.

사용자가 응답 헤더에 지정된 포트 번호에서 프록시 서버의 응답을 볼 수 있으므로 요청이 성공적으로 완료됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

부하 분산 장치를 사용한 에지 요청 처리

그러나 부하 분산 장치를 사용하는 경우 사용자의 브라우저는 프록시 서버가 아닌 부하 분산 장치와 직접 통신합니다. 요청은 아래에 설명된 대로 처리됩니다.

주: 다음 예에서는 프록시 서버 포트 번호로 `1025` 를 사용합니다.

1. 사용자가 브라우저에서 요청을 발행합니다.
2. 브라우저는 가상 서버라고도 하는 부하 분산 장치 가상 IP(VIP)에 요청을 보냅니다.
3. VIP는 프록시 서버(예: `10.2.200.148:1025`)를 가리키도록 구성되었으므로 부하 분산 장치는 요청을 프록시 서버로 전달합니다.
4. 프록시 서버는 ServiceNow 인스턴스에 요청을 보냅니다.
5. ServiceNow 인스턴스는 프록시 서버에 대한 응답을 반환합니다.
6. 프록시 서버는 `risk-servicenow.dev.echonet:1025`에 대한 속성에 구성된 값으로 응답의 위치 헤더를 다시 씁니다.
   - 호스트: `edgencryption.proxy.host`
   - **HTTP** 포트: `edgeencryption.proxy.http.port`
   - **HTTPS** 포트: `edgeencryption.proxy.https.port`
7. 프록시 서버는 위치 헤더가 프록시 서버 포트를 가리키는 부하 분산 장치에 응답을 전달합니다.

결과는 부하 분산 장치 및 프록시 서버가 동일한 포트를 사용하고 있는지 여부에 따라 달라집니다.

- 부하 분산 장치 및 프록시 서버가 동일한 포트를 사용하는 경우 사용자가 응답 헤더에 식별된 것과 동일한 포트에서 응답을 수신하므로 요청이 성공합니다.
- 부하 분산 장치 및 프록시 서버가 서로 다른 포트를 사용하는 경우 사용자의 브라우저는 부하 분산 장치와만 통신하지만 응답은 프록시 서버에 있기 때문에 요청이 실패합니다.

솔루션

동일한 포트에서 부하 분산 장치 및 모든 Edge 프록시 서버를 사용하여 문제를 해결할 수 있지만 이상적인 솔루션은 아닙니다. 더 나은 솔루션은 시스템에서 부하 분산 장치가 사용하는 포트를 알 수 있도록 하는 것입니다.

다음 속성을 사용하면 프록시 서버와 부하 분산 장치에서 서로 다른 포트를 사용하는 경우 에지 프록시 서버가 부하 분산 장치에 대한 응답 메시지를 다시 라우팅할 수 있습니다.

- *`edgeencryption.proxy.rewrite.location.host`* 부하 분산 장치를 통해 ServiceNow에 액세스하는 데 사용되는 호스트 이름을 지정합니다.
- *`edgeencryption.proxy.rewrite.location.https.port`* 는 부하 분산 장치를 통해 ServiceNow에 액세스하는 데 사용되는 HTTPS 포트를 지정합니다.

부하 분산 장치 구성

부하 분산 장치 및 프록시 서버가 서로 다른 포트를 사용하는 경우 부하 분산 장치의 호스트 이름과 HTTPS 포트를 지정하여 사용자가 브라우저에서 응답을 볼 수 있도록 합니다.

시작하기 전에
필요한 역할:

- Windows 호스트의 로컬 또는 도메인 관리자
- Linux 호스트에서 전체 파일 시스템 액세스 권한이 있는 서비스 사용자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 프록시 서버 호스트에 관리자, 도메인 관리자 또는 서비스 사용자로 로그인합니다.
2. Edge 프록시의 설치 디렉터리로 이동하고 `conf/edgeencryption.properties`를 선택합니다.
3. 다음 속성을 설정합니다.

속성	설명
edgeencryption.proxy.rewrite.location.host	Edge 구성에 프록시 서버 간에 부하를 분산하기 위한 부하 분산 장치가 포함되어 있는 경우 요청을 완료할 수 있도록 부하 분산 장치에 응답을 다시 작성합니다. ◦ 프록시 설정에 부하 분산 장치가 있는 경우 부하 분산 장치를 통해 ServiceNow에 액세스할 때 사용되는 호스트 이름을 지정합니다. ◦ 옵션: 프록시 설정에 로드 밸런서가 없는 경우, 이 값을 프록시 서버에서 사용하는 호스트 이름으로 설정할 수 있습니다.
edgeencryption.proxy.rewrite.location.https.port	에지 구성에 프록시 서버 간에 부하를 분산하기 위한 부하 분산 장치가 포함되어 있는 경우 부하 분산 장치를 통해 ServiceNow에 액세스하는 데 사용되는 HTTPS 포트를 지정합니다. ◦ 구성에 부하 분산 장치가 있는 경우 부하 분산 장치를 통해 ServiceNow에 액세스하는 데 사용되는 HTTPS 포트를 지정합니다. ◦ 옵션: 구성에 부하 분산 장치가 없는 경우 이 값을 프록시 서버에서 사용하는 HTTPS 포트로 설정할 수 있습니다.

4. 파일을 저장합니다.

결과
이제 사용자가 브라우저에서 응답을 볼 수 있으므로 요청을 완료할 수 있습니다.

에지 암호화 규칙 업그레이드

인스턴스 업그레이드와 프록시 서버 업그레이드는 에지 암호화 규칙 모두 환경에서 특별한 고려 사항이 필요합니다.

인스턴스 업그레이드

Edge 암호화 규칙 환경에서 인스턴스를 업그레이드하려면 인스턴스 업그레이드 후 Edge 컨트롤이 제대로 작동하는지 확인하는 데 주의해야 합니다.

인스턴스를 업그레이드하는 동안에는 다음을 추가, 편집 또는 삭제하면 안 됩니다.

- 에지 암호화 규칙 구성
- 에지 암호화 규칙 규칙
- 에지 암호화 규칙 토큰화 패턴
- 에지 암호화 규칙 예약된 작업

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 에지 암호화 규칙 키 구성
- 에지 암호화 규칙 예약된 업그레이드
- 에지 암호화 규칙 거부 목록 IP 구성

인스턴스 업그레이드 중에 실행되는 모든 예약된 작업은 완료되지 않습니다. 중단된 작업을 완료하려면 인스턴스가 업그레이드된 후에 작업을 다시 실행하십시오. 작업 일정을 조정해도 인스턴스 업그레이드 전에 발생한 처리는 손실되지 않으며 작업은 아직 처리되지 않은 데이터만 계속 처리합니다.

프록시 서버 업그레이드

인스턴스에서 프록시 서버를 업그레이드 에지 암호화 규칙 하거나 언제든지 프록시 서버를 수동으로 업그레이드할 수 있도록 프록시 업그레이드를 예약합니다.

⚠ **경고:** Windows에서 업그레이드하는 경우 파일 잠금 문제가 발생하여 업그레이드가 실패할 수 있습니다. 업그레이드가 성공하려면 설치 디렉터리 아래에 파일이 열려 있지 않아야 합니다. 또한 설치 디렉터리에 기존 셸이 없어야 합니다. 특히, 설치 디렉토리에 있는 동안 명령줄에서 (`bin\edgeencryption.bat install/start`를 통해) 프록시를 시작하는 경우 해당 쉘을 닫거나 나중에 설치 디렉토리 밖으로 이동해야 합니다. 설치 디렉터리 아래의 파일은 편집기나 다른 애플리케이션에서 열 수 없습니다.

외부 공급업체 라이브러리

Gemalto와 같은 외부 공급업체 라이브러리는 동일한 디렉터리에 보관되는 경우 인스턴스 및 프록시 서버 업그레이드 중에 손실됩니다. 다음을 수행하여 업그레이드 중에 외부 공급업체 라이브러리가 손실되지 않도록 할 수 있습니다.

1. edgeencryption.properties에 다음 속성을 수동으로 추가합니다.

   ```
   edgeencryption.ekm.provider.classname =
   com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   ```

2. *`edgeencryption.thirdparty.vendor.library.path`* 벤더 라이브러리 위치 속성을 추가하고 `/path/to/jars`로 설정합니다.

   예:

   ```
   edgeencryption.thirdparty.vendor.library.path = /app/servicenow/libs
   ```

3. SafeNet JAR을 해당 경로에 복사합니다.

설치 외부에 에지 암호화 규칙 타사 라이브러리를 설치한 후에는 업그레이드 중에 더 이상 손실되지 않습니다.

예약된 업그레이드

ⓘ **중요사항:** 인스턴스를 업그레이드하는 동안 ServiceNow 프록시 서버 버전도 인스턴스 버전에 맞게 업그레이드하여 호환성 문제의 가능성을 줄입니다.

인스턴스가 예약된 시간에 프록시 서버를 업그레이드할 수 있도록 업그레이드를 예약합니다. 이 기능은 업그레이드 후 기본적으로 사용할 수 있습니다. 예약된 업그레이드에는 다음 이벤트가 포함됩니다.

1. 프록시 서버는 인스턴스를 검사하여 업그레이드에 사용할 수 있는 새 버전이 있는지 확인합니다. 일반적으로 인스턴스가 업그레이드되면 새 버전을 사용할 수 있게 됩니다.
2. Proxy Server의 새 버전을 사용할 수 있을 때 관리자는 로그인할 때 알림을 받습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 관리자는 각 프록시 서버에 대해 에지 암호화 규칙 프록시 서버 업그레이드를 예약할 수 있습니다.

   주: security_admin 역할이 있는 사용자만 프록시 서버를 통해 업그레이드 일정을 만들 수 있습니다.

4. 업그레이드가 예약되면 프록시 서버는 예약된 시간에 자동으로 업그레이드합니다. 업그레이드하는 동안 프록시 서버는 잠시 동안만 오프라인 상태가 됩니다.

   주: 프록시 서버는 업그레이드 중에 다시 시작되기 때문에 잠시 동안 오프라인 상태입니다. 시간은 사용자 환경 및 프록시 서비스를 중지하고 다시 시작하는 데 걸리는 시간에 따라 결정됩니다.

5. 예약된 업그레이드 중에 새 프록시 디렉터리가 만들어지고 구성 파일이 새 디렉터리에 복사됩니다. 새 속성은 기존 속성 파일에 기록됩니다. 이전 프록시 디렉터리의 다음 파일 또는 디렉터리가 새 프록시 디렉터리로 복사됩니다.

   - `/conf` 디렉토리
   - `/keys` 디렉터리
   - `/keystore` 디렉터리
   - `java/jre/lib/security/cacerts` 파일

   결과적으로 키, 키 저장소, 설정 및 인증서가 보존됩니다.

   주: 위의 파일만 새 프록시 디렉터리에 복사됩니다. 프록시 서버 디렉터리의 다른 사용자 지정 파일은 예약된 업그레이드 중에 보존되지 않습니다. 업그레이드 로그 파일은 `<original-proxy-directory>/tmp/upgrade-wrapper/bin` 폴더의 원래 프록시 디렉터리에서 찾을 수 있습니다.

예약된 업그레이드의 필수 조건

에지 암호화 규칙 프록시에 대한 업그레이드를 예약하기 전에 다음 사항을 확인하십시오.

1. *JAVA_HOME* 환경 변수는 에지 암호화 규칙 프록시의 디렉터리 구조 외부에 있는 컴퓨터의 Java 설치를 가리킵니다.
2. *JAVA_HOME* 환경 변수는 버전 1.8_u144 이상의 Java 설치를 가리킵니다.
3. *-Djava.io.tmpdir* Edge Encryption 프록시의 wrapper.conf 파일에 있는 매개 변수는 Edge Encryption 프록시의 디렉터리 구조 외부에 있는 디렉터리를 가리키고 프록시에는 디렉터리에 대한 읽기/쓰기/실행 권한이 있습니다. 선택적으로 Java가 기본 tmp 위치를 사용하도록 매개변수를 완전히 주석으로 처리할 수 있습니다.

수동 업그레이드

업그레이드 일정을 생성하는 대신 명령줄을 통해 각 프록시 서버를 수동으로 업그레이드할 수 있습니다. Linux에서 실행되는 에지 암호화 규칙 프록시 서버 수동 업그레이드 또는 Windows에서 실행되는 에지 암호화 규칙 프록시 서버 수동 업그레이드 문서를 참조하십시오.

프록시 빌드 상태

프록시 서버가 오래되었는지 여부는 다음으로 이동하여 쉽게 식별할 수 있습니다. 에지 암호화 규칙 구성 > 프록시 > 모두. 프록시 빌드의 상태는 프록시 빌드 열에 다음 색상으로 표시됩니다.

녹색

프록시 서버가 최신 상태입니다.

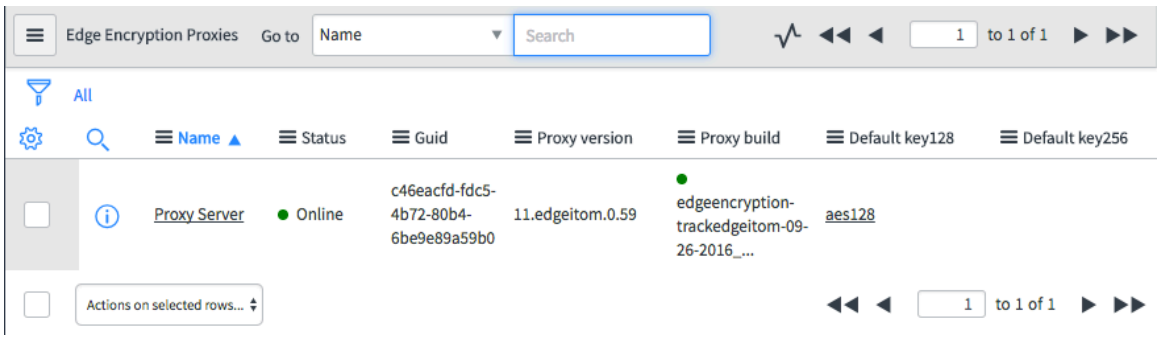
노란색

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프록시 서버가 오래되어 업그레이드가 필요합니다.

주황

업그레이드 실패. 다운타임이 없도록 프록시 서버가 이전 버전으로 되돌아갑니다.



실패한 예약된 프록시 업그레이드 문제 해결

예약된 프록시 업그레이드가 실패하면 프록시 서버가 업그레이드 이전 버전으로 되돌아갑니다. 모든 원본 데이터, 키 및 구성 파일이 보존됩니다. 이 프로세스는 몇 분 정도 걸릴 수 있습니다. 성공적인 업그레이드를 위해 문의하십시오 고객 서비스 및 지원 .

실패 이유를 확인하려면 업그레이드 일정에서 실패 이유를 확인할 수 있습니다. 또한 실패한 업그레이드에 대한 설치 디렉터리가 유지관리되므로 문제 해결에 로그 파일을 사용할 수 있습니다.

주: 추가 프록시 디렉터리를 삭제하기 전에 항상 로그 파일을 검토하여 현재 디렉터리를 확인합니다. 로그 파일에 최근 활동이 있는 경우 프록시가 인스턴스에 연결되어 있을 수 있습니다.

예약된 프록시 업그레이드가 반복적으로 실패하면 프록시 서버를 수동으로 업그레이드할 수 있습니다. Linux에서 실행되는 에지 암호화 규칙 프록시 서버 수동 업그레이드 및 Windows에서 실행되는 에지 암호화 규칙 프록시 서버 수동 업그레이드 문서를 참조하십시오.

Java 최소 요구 사항

프록시 서버를 설치하거나 실행하는 에지 암호화 규칙 호스트 컴퓨터는 지원되는 Java 버전을 유지 관리해야 합니다. 현재 지원되는 버전은 17.x 버전 시리즈의 Java 17.0.3 이상입니다.

주: Java 11은 Yokohama 릴리스부터 더 이상 지원되지 않습니다. Yokohama 또는 이후 버전의 프록시를 설치하기 전에 프록시를 에지 암호화 규칙 사용하여 환경을 Java 17로 업그레이드합니다 에지 암호화 규칙 .

Java 8 Update 141(8u141) 이하에서 AES 256비트 암호화를 사용하는 경우, JCE(Java Cryptography Extension) 관할 정책 파일을 각 에지 암호화 규칙 프록시 서버 호스트의 시스템 Java 홈 디렉토리에 복사하여 설치해야 합니다. 예약된 업그레이드 또는 수동 업그레이드를 수행하기 전에 `### ### <Java-home-directory>/jre/lib/security` 폴더에 추가하십시오. AES 256비트 암호화 정책 파일을 설치하려면 문서를 참조하십시오 AES 256비트 암호화 키 구성.

혼합 프록시 버전 환경

최신 버전의 프록시 서버로 이전 버전의 프록시 서버를 실행하는 환경에서는 권장되지 않지만 모든 프록시 서버가 인스턴스와 동일한 버전 제품군 내에 있는 경우 지원됩니다. 예를 들어 릴리스에 Yokohama 인스턴스가 있는 경우 환경은 모든 Yokohama 패치 또는 핫픽스의 프록시 서버를 지원합니다. 그러나 다음과 같은 제한 사항이 적용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 한 프록시 서버가 다른 프록시에서 지원하지 않는 기능을 지원하는 경우 사용되는 프록시 서버에 따라 일관성 없는 동작이 표시됩니다.
- 프록시 서버가 최신 버전이 아닌 경우 최근의 보안 강화 기능이 포함되지 않을 수 있습니다.

이전 릴리스의 프록시 서버가 인스턴스의 최신 릴리스에 등록된 경우 프록시 서버가 오래되었다는 알림을 정기적으로 받게 됩니다. 최적의 보안 환경을 ServiceNow 보장하려면 항상 프록시 서버를 인스턴스에서 지원하는 최신 버전의 소프트웨어로 업그레이드하는 것이 좋습니다.

에지 암호화 규칙 프록시 서버 업그레이드 예약

인스턴스가 오래된 프록시 서버를 업그레이드할 수 있도록 업그레이드 일정을 생성합니다.

시작하기 전에

업그레이드를 예약하려면 프록시 서버를 통해 인스턴스에 로그인해야 합니다.
Java 8 Update 141(8u141) 이하에서 AES 256비트 암호화를 사용하는 경우, JCE(Java Cryptography Extension) 관할 정책 파일을 각 에지 암호화 규칙 프록시 서버 호스트의 시스템 Java 홈 디렉토리에 복사하여 설치해야 합니다. 예약된 업그레이드 또는 수동 업그레이드를 수행하기 전에 `### ### <Java-home-directory>/jre/lib/security` 폴더에 추가하십시오. AES 256비트 암호화 정책 파일을 설치하려면 문서를 참조하십시오 AES 256비트 암호화 키 구성.

필요한 역할: security_admin

이 태스크 정보

업그레이드가 예약되면 프록시 서버는 예약된 시간에 자동으로 업그레이드합니다. 업그레이드하는 동안 프록시 서버는 잠시 동안만 오프라인 상태가 됩니다.

> **주:** 프록시 서버는 업그레이드 중에 다시 시작되기 때문에 잠시 동안 오프라인 상태입니다. 시간은 사용자 환경 및 프록시 서비스를 중지하고 다시 시작하는 데 걸리는 시간에 따라 결정됩니다.

예약된 업그레이드 중에 새 프록시 디렉터리가 만들어지고 구성 파일이 새 디렉터리에 복사됩니다. 새 속성은 기존 속성 파일에 기록됩니다. 이전 프록시 디렉터리의 다음 파일 또는 디렉터리가 새 프록시 디렉터리로 복사됩니다.

- `/conf` 디렉토리
- `/keys` 디렉터리
- `/keystore` 디렉터리
- `java/jre/lib/security/cacerts` 파일

결과적으로 키, 키 저장소, 설정 및 인증서가 보존됩니다.

> **주:** 위의 파일만 새 프록시 디렉터리에 복사됩니다. 프록시 서버 디렉터리의 다른 사용자 지정 파일은 예약된 업그레이드 중에 보존되지 않습니다. 업그레이드 로그 파일은 `<original-proxy-directory>/tmp/upgrade-wrapper/bin` 폴더의 원래 프록시 디렉터리에서 찾을 수 있습니다.

여러 프록시 서버가 만료된 경우 각 프록시 서버에 대해 개별적으로 업그레이드를 예약해야 합니다.

> **주:** 동일한 컴퓨터에서 여러 프록시 서버를 호스팅하지 마십시오. 그러나 환경에 이 구성이 포함된 경우 동일한 컴퓨터의 여러 프록시로 동시에 업그레이드를 예약하지 마십시오.

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 프록시 > 업그레이드 일정.
2. 새로 만들기를 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 양식을 작성하십시오.

에지 암호화 규칙 프록시 업그레이드 일정 양식

필드	설명
프록시 서버	업그레이드 중인 프록시 서버입니다.
대상 버전	프록시 서버를 업그레이드할 버전입니다. 이 값은 읽기 전용이며 인스턴스에 사용할 수 있는 최신 프록시 버전으로 설정됩니다.
예약된 시작 시간	업그레이드를 시작할 날짜 및 시간입니다.
활성	예약된 업그레이드가 활성 상태인지 여부입니다. 이 필드를 선택하지 않으면 업그레이드가 예약된 날짜 및 시간에 수행되지 않습니다.
상태	업그레이드 상태입니다. 이 값은 읽기 전용입니다. 가능한 상태는 다음과 같습니다. ◦ 보류 중 ◦ 실행 중 ◦ 완료 ◦ 실패

4. 제출을 클릭합니다.

다음에 수행할 작업

일반적인 업그레이드 시간은 15분 미만입니다. 업그레이드가 실행된 후 업그레이드 상세 정보를 검토하여 자세한 내용을 확인할 수 있습니다. 업그레이드에 실패한 경우 실패 이유를 검토하여 다음 단계를 결정합니다.

업그레이드 상세 정보

필드	설명
시작 버전	서버가 업그레이드된 버전입니다.
종료 버전	서버가 업그레이드된 버전입니다.
실제 시작 시간	업그레이드가 시작된 시간입니다.
종료 시간	업그레이드가 종료된 시간입니다.
장애 이유	업그레이드에 실패한 이유입니다.

Linux에서 실행되는 에지 암호화 규칙 프록시 서버 수동 업그레이드

Linux에서 실행되는 프록시를 업데이트합니다.

시작하기 전에

Java 8 Update 141(8u141) 이하에서 AES 256비트 암호화를 사용하는 경우, JCE(Java Cryptography Extension) 관할 정책 파일을 각 에지 암호화 규칙 프록시 서버 호스트의 시스템 Java 홈 디렉토리에 복사하여 설치해야 합니다. 예약된 업그레이드 또는 수동 업그레이드를 수행하기 전에 `### ### <Java-home-directory>/jre/lib/security` 폴더에 추가하십시오. AES 256비트 암호화 정책 파일을 설치하려면 문서를 참조하십시오 AES 256비트 암호화 키 구성.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 역할: 호스트 머신의 security_admin 또는 로컬 관리자

프로시저

1. 에지 암호화 규칙 proxy-update 아카이브 파일을 설치 디렉토리에 다운로드합니다.
   a. 다음으로 이동 에지 암호화 규칙 구성 > 설치 및 다운로드 > 다운로드
   b. 명령줄 설치 프로그램 다운로드 링크를 선택합니다.
   c. 다운로드가 시작되면 설치 디렉터리를 다운로드 위치로 선택합니다.
2. 설치 디렉터리로 변경합니다.
3. 다음 명령을 실행합니다.

```
java -jar edgeencryption-dist-<version>-linux-x86-64.jar -m dist-upgrade
-c <proxy directory>
```

옵션	설명
프록시 디렉터리	프록시가 처음 설치된 설치 디렉터리의 디렉터리입니다. 이 디렉터리는 설치에 의해 만들어집니다.

도움말 화면을 보려면 `## ## java -jar edgeencryption-dist-<version` 명령을 실행합니다>-linux-x86-64.jar

현재 타임스탬프를 사용하여 새 프록시 디렉터리가 만들어집니다. 이전 프록시 디렉터리의 백업은 새 프록시 설치 디렉터리에서 backup.dist-upgrade_timestamp로 유지됩니다. 이전 프록시가 종료되고 새 프록시가 시작됩니다. 이전 프록시 서버에서 열려 있는 모든 연결/트랜잭션이 종료됩니다.

4. 새 디렉터리와 인스턴스의 프록시 로그를 확인하여 새 프록시가 실행 중인지 확인합니다.

Windows에서 실행되는 에지 암호화 규칙 프록시 서버 수동 업그레이드

Windows에서 실행되는 프록시를 업데이트합니다.

시작하기 전에
Java 8 Update 141(8u141) 이하에서 AES 256비트 암호화를 사용하는 경우, JCE(Java Cryptography Extension) 관할 정책 파일을 각 에지 암호화 규칙 프록시 서버 호스트의 시스템 Java 홈 디렉토리에 복사하여 설치해야 합니다. 예약된 업그레이드 또는 수동 업그레이드를 수행하기 전에 `### ### <Java-home-directory>/jre/lib/security` 폴더에 추가하십시오. AES 256비트 암호화 정책 파일을 설치하려면 문서를 참조하십시오 AES 256비트 암호화 키 구성.

필요한 역할: 호스트 머신의 security_admin 또는 로컬 관리자

프로시저

1. 에지 암호화 규칙 proxy-update 아카이브 파일을 설치 디렉토리에 다운로드합니다.
   a. 다음으로 이동 에지 암호화 규칙 구성 > 설치 및 다운로드 > 다운로드
   b. 명령줄 설치 프로그램 다운로드 링크를 선택합니다.
   c. 다운로드가 시작되면 설치 디렉터리를 다운로드 위치로 선택합니다.
2. 관리자 권한으로 Windows cmd 터미널 프로그램을 시작합니다.
3. 설치 디렉터리로 변경합니다.
4. 다음 명령을 실행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
java -jar edgeencryption-dist-<version>-all.jar -m dist-upgrade -c <proxy directory>
```

옵션	설명
프록시 디렉터리	프록시가 처음 설치된 설치 디렉터리의 디렉터리입니다. 이 디렉터리는 설치에 의해 만들어집니다.

도움말 화면을 보려면 `## ## java -jar edgeencryption-dist-<version` 명령을 실행합니다>-all.jar

현재 타임스탬프를 사용하여 새 프록시 디렉터리가 만들어집니다. 이전 프록시 디렉터리의 백업은 새 프록시 설치 디렉터리에서 backup.dist-upgrade_timestamp로 유지됩니다. 이전 프록시가 종료되고 새 프록시가 시작됩니다. 이전 프록시 서버에서 열려 있는 모든 연결/트랜잭션이 종료됩니다.

5. 새 디렉터리와 인스턴스의 프록시 로그를 확인하여 프록시가 업데이트되었고 실행 중인지 확인합니다.

에지 암호화 규칙 프록시 서버 업그레이드 롤백

프록시 업그레이드에 실패한 경우 이전 버전으로 돌아갈 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
릴리스에서 Yokohama 예약된 업그레이드 기능을 사용할 때 업그레이드에 실패하면 프록시 서버가 자동으로 이전 버전으로 롤백합니다. 이전 프록시 서버는 백업 디렉토리에 수정되지 않은 상태로 저장됩니다.

수동 업그레이드를 롤백하려면 다음 단계를 수행할 수 있습니다.

프로시저

1. 프록시를 종료합니다.
2. 새 프록시 디렉터리를 삭제합니다.
3. 백업 디렉터리의 이름을 프록시 이름으로 바꿉니다.
   백업 디렉토리는 `<proxy name`이라는 이름의 프록시 설치 디렉토리에 있습니다>_backup
4. 프록시를 시작합니다.
5. 프록시 로그와 인스턴스를 확인하여 프록시가 온라인 상태인지 확인합니다.

에지 암호화 규칙 구성

에지 암호화 규칙 프록시 서버가 설치되어 실행되면 프록시 서버를 통해 관리합니다에지 암호화 규칙.

인스턴스에서 암호화 구성 및 암호화 패턴을 생성하기 전에 다음의 에지 암호화 규칙 설치 모든 단계를 완료해야 합니다.

주: 구성에 액세스하려면 에지 암호화 규칙 프록시 서버를 통해 로그인하고 security_admin 역할로 격상해야 합니다.

암호화 키 교대

인스턴스에서 암호화 키 순환을 수행합니다. 새 키를 추가하고 기본 키 할당을 변경한 다음 대량 키 회전 또는 단일 키 회전을 예약합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 키를 기본 키로 설정하기 전에 각 프록시에서 키를 사용할 수 있도록 합니다. 이렇게 하면 키가 기본 키로 할당될 때 프록시에서 데이터를 암호화할 수 있는 키를 갖게 됩니다. 모든 프록시는 키에 액세스할 수 있어야 해당 키를 기본 키로 할당할 수 있습니다.

⚠ 경고: 프록시에서 키를 삭제하기 전에 대량 키 회전 작업을 설정하고 실행하여 인스턴스의 데이터가 키를 사용하지 않도록 합니다. 해당 키로 암호화된 정보가 있는 경우 키를 삭제한 후에는 정보를 해독할 수 없습니다.

에지 필터링 및 정렬 동작

기본 키를 변경할 때마다 키 회전(대량 또는 단일 키 회전)을 수행해야 합니다. 그렇지 않으면 기록을 정렬하고 필터링할 때 예기치 않은 결과가 나타날 수 있습니다. 예를 들어, 다음과 같은 시나리오를 생각해 보겠습니다.

1. 하나의 암호화 키를 사용하여 암호화된 레코드를 만듭니다.
2. 새 키를 만들고 기본값으로 설정합니다.
3. 새 암호화 키를 사용하여 암호화된 기록의 새 집합을 만듭니다.

Edge 프록시를 통해 연결할 때 암호화된 필드를 기준으로 필터링하는 경우 모든 레코드가 올바르게 필터링되지 않거나 레코드가 예기치 않게 나타날 수 있습니다. 필터는 현재 기본 키를 사용하여 암호화된 레코드에 대해서만 작동합니다. 이전 기본 키를 사용하여 암호화된 기록은 목록 뷰에 계속 표시됩니다.

Edge 프록시를 통해 연결될 때 암호화된 필드를 기준으로 정렬하면 암호화된 필드에 동일한 사람이 읽을 수 있는 텍스트가 있는 두 개의 레코드 그룹이 표시됩니다.

단일 키 회전 작업 예약

지정된 키 별칭을 사용하여 암호화된 데이터를 찾은 다음 현재 기본 암호화 키를 사용하여 데이터를 다시 암호화하도록 작업을 예약합니다. 데이터는 기본 키로 다시 암호화되기 전에 해독됩니다.

시작하기 전에

필요한 역할: security_admin
이 작업을 예약하기 전에 다음에서 기본 키를 업데이트하십시오. 에지 암호화 규칙 구성 > 암호화 키 구성 > 기본 키 설정.

프로시저

1. 다음으로 이동 에지 암호화 규칙 구성 > 유지관리 > 단일 키 회전 예약.
2. 양식의 필드에 적절한 정보를 입력합니다.

필드	값
이름	설명적인 이름을 입력합니다.
작업 유형	단일 키 회전을 선택합니다.
키	폐기할 키를 입력합니다. 이 키가 더 이상 다음의 기본 키가 아닌지 확인합니다. 에지 암호화 규칙 구성 > 암호화 키 구성 > 기본 키 설정.
기록 수 추정	처리할 총 예상 기록 수입니다. 단일 키 회전을 실행할 때는 사용할 수 없습니다.
처리 이력 기록	필드가 감사되는 경우 감사 테이블에서 기록 기록을 처리하려면 선택합니다. 감사 테이블의 필드에 대한 이력 기록을 암호화하면 새 값과 이전 값이 모두 암호화됩니다. 이 필드는 읽기 전용이며 활성 상태입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	값
	감사된 필드에 대한 자세한 내용은 감사를 참조하십시오.
최대 감사 기록 카운트 추정	처리할 감사된 기록의 예상 최대 수입니다. 단일 키 회전을 실행할 때는 사용할 수 없습니다.
활성	이 작업을 비활성화하려면 이 확인란의 선택을 취소합니다.
실행	작업 실행 간격을 선택합니다.
시작	작업을 처음 실행할 날짜 및 시간을 입력합니다.

3. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
   감사된 필드를 처리할 때는 예상 기록 수가 지원되지 않습니다.

대량 키 회전 작업 예약

이전 키로 암호화된 데이터를 찾은 다음 현재 기본 암호화 키를 사용하여 데이터를 다시 암호화하도록 작업을 예약합니다. 데이터는 현재 기본 키로 다시 암호화되기 전에 해독됩니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 유지관리 > 대량 키 회전 예약.
2. 양식의 필드에 적절한 정보를 입력합니다.

필드	값
이름	설명적인 이름을 입력합니다.
작업 유형	질량 키 회전을 선택합니다.
기록 수 추정	처리할 총 예상 기록 수입니다. 대량 키 회전을 실행할 때는 사용할 수 없습니다.
처리 이력 기록	필드가 감사되는 경우 감사 테이블에서 기록 기록을 처리하려면 선택합니다. 감사 테이블의 필드에 대한 이력 기록을 암호화하면 새 값과 이전 값이 모두 암호화됩니다. 이 필드는 읽기 전용이며 활성 상태입니다. 감사된 필드에 대한 자세한 내용은 감사를 참조하십시오.
최대 감사 기록 카운트 추정	처리할 감사된 기록의 예상 최대 수입니다. 대량 키 회전을 실행할 때는 사용할 수 없습니다.
활성	이 작업을 비활성화하려면 이 확인란의 선택을 취소합니다.
실행	작업 실행 간격을 선택합니다.
시작	작업을 처음 실행할 날짜 및 시간을 입력합니다.

3. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
   감사된 필드를 처리할 때는 예상 기록 수가 지원되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

첨부 파일 키 회전 작업 예약

지정된 키 별칭을 사용하여 암호화된 첨부 파일을 찾은 다음 현재 기본 암호화 키를 사용하여 첨부 파일을 다시 암호화하도록 작업을 예약합니다. 첨부 파일은 기본 키로 다시 암호화되기 전에 암호 해독됩니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 유지관리 > 첨부 파일 키 회전 예약.
2. 양식의 필드에 적절한 정보를 입력합니다.

필드	값
이름	설명적인 이름을 입력합니다.
작업 유형	첨부 파일 키 회전을 선택합니다.
활성	이 작업을 비활성화하려면 확인 표시를 선택 취소하십시오.
테이블	테이블을 선택합니다.
실행	작업 실행 간격을 선택합니다.
시작	작업을 처음 실행할 날짜 및 시간을 입력합니다.

3. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
4. 업데이트할 기록의 예상 수를 보려면 예상 기록 수를 클릭합니다.
5. 작업을 즉시 실행하려면 지금 실행을 클릭합니다.

암호화 구성을 사용하여 필드 암호화

암호화 구성을 생성하여 필드를 암호화합니다.

구성하려면 에지 암호화 규칙프록시를 통해 인스턴스에 연결되어 있어야 합니다. 프로덕션 인스턴스에 적용하기 전에 비프로덕션 인스턴스에서 모든 변경 사항을 테스트합니다.

암호화 키 정의

하나 이상의 프록시를 설정하고 기본 암호화 키를 구성한 후 인스턴스는 모든 프록시에서 키를 사용할 수 있는지 확인합니다. 모든 프록시에 키가 없으면 암호화 키를 기본 키로 만들 수 없습니다. 기본 키를 정의한 후 암호화 구성을 만들 수 있습니다.

암호화할 필드 및 첨부 파일 할당

암호화할 필드와 첨부 파일을 할당한다는 것은 필드 또는 첨부 파일에 암호화 유형을 할당하는 것을 의미합니다. 필드를 암호화됨으로 표시하기 전에 이러한 문제를 평가하십시오.

- 영향을 받을 수 있는 시스템 기능을 확인합니다.
- 필드를 사용하기 위한 모든 스크립트를 검사하십시오.
- 필드 크기를 원하는 대로 조정합니다. 암호화하도록 필드를 구성한 후에는 필드 크기를 변경할 수 없습니다.

필드를 암호화할 것으로 표시하면 암호화된 데이터를 저장할 필드 크기가 확장됩니다. 필드의 크기를 확장하는 프로세스는 테이블의 기록 수에 따라 시간이 오래 걸릴 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

API 지원

필드 암호화 는 `setDisplayValue()` 및 `setValue()` API를 업데이트하여 암호화된 필드에 암호화된 데이터를 삽입할 수 있도록 합니다. 또한 `getDisplayValue()` 및 `getValue()` 가 일반 텍스트 값을 반환할 수 있도록 합니다.

다음 스크립트는 인시던트 짧은 설명이 암호화된 경우 이러한 API 변경 내용을 보여줍니다.

```
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
```

`getValue()`를 사용하여 암호화된 텍스트를 가져올 때 스크립트는 더 이상 암호문을 반환하지 않습니다. 스크립트는 사용자가 암호화 모듈에 액세스할 수 있다고 가정하고 일반 텍스트를 반환합니다. `getValue()` 는 사용자가 암호화 모듈에 액세스할 수 없는 경우 암호문을 반환합니다.

필드 암호화 구성 작성

암호화할 필드를 선택하고 암호화 유형을 식별합니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 암호화 구성 > 새로 작성.
2. 양식을 작성합니다.

필드	설명
테이블	암호화할 필드가 들어 있는 테이블입니다.
유형	테이블, 열 또는 테이블의 첨부 파일을 암호화할지 여부입니다. 열을 선택합니다.
열	암호화할 필드입니다. 유형이열인 경우에만 나타납니다. 문자열, 날짜, 날짜/시간, 저널, 저널 입력 및 URL 필드만 지원됩니다. ◦ 문자열 및 **URL** 필드: 상위 테이블 또는 하위 테이블에 암호화 구성을 추가할 수 있습니다. ◦ 날짜 및 날짜/시간 필드: 상위 테이블에만 암호화 구성을 추가할 수 있습니다. 하위 테이블에는 새 암호화 구성을 추가할 수 없습니다. 주: 암호화 중인 날짜 및 날짜/시간 필드의 영향을 받는 기록 수에 따라 암호화 구성을 생성하는 데 최대 몇 분이 걸릴 수 있습니다. 인스턴스의 트랜잭션 볼륨이 작을 때 날짜 및 날짜/시간 필드에 대한 암호화 구성을 생성해야 합니다.
암호화 유형	사용할 암호화 유형입니다.

주: 특정 테이블 및 필드 조합에는 한 번에 하나의 활성 구성만 있을 수 있습니다.

3. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업

암호화 구성 기록을 추가한 후 암호화 작업을 생성하여 기존 데이터를 암호화할 수 있습니다. 암호화 작업을 실행하지 않으면 Edge는 다음에 데이터가 변경될 때 기존 데이터를 암호화합니다. 자세한 내용은 암호화 작업 예약 문서를 참조하십시오.

변수 암호화 구성 작성

암호화할 서비스 카탈로그 변수를 선택하고 암호화 유형을 식별합니다.

시작하기 전에

필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 변수 암호화 구성.
2. **Edge** 암호화 변수 구성 목록에서 새로 만들기를 클릭합니다.
3. 양식을 작성합니다.

필드	설명
변수	암호화할 변수입니다.
암호화 유형	사용할 암호화 유형입니다.

4. 제출을 클릭합니다.

다음에 수행할 작업

암호화 구성 기록을 추가한 후 암호화 작업을 생성하여 기존 데이터를 암호화할 수 있습니다. 암호화 작업을 실행하지 않으면 Edge는 다음에 데이터가 변경될 때 기존 데이터를 암호화합니다. 자세한 내용은 암호화 작업 예약 문서를 참조하십시오.

암호화 구성 비활성화

암호화할 필드 또는 테이블의 첨부 파일을 구성한 후 암호화 구성을 비활성화하여 암호화를 중지할 수 있습니다. 암호화를 비활성화한 후에는 필드에 대한 암호 해독 작업 또는 첨부 파일에 대한 첨부 파일 암호 해독 작업을 실행하여 인스턴스에서 암호화된 데이터를 제거할 수 있습니다.

시작하기 전에

필요한 역할: security_admin

이 태스크 정보

⚠ 경고: 암호화 구성을 비활성화해도 암호화 기록은 삭제되지 않으며 암호화 유형을 변경할 수 없습니다.

프로시저

1. 다음으로 이동 에지 암호화 규칙 구성 > 에지 암호화 규칙 구성 > 모두.
   Edge Encryption 구성 목록이 표시됩니다.
2. 비활성화할 암호화 구성을 클릭합니다.
   에지 암호화 규칙 구성 양식이 표시됩니다.
3. 활성 상자를 클릭합니다.
   활성 상자의 선택이 취소됩니다.
4. 업데이트를 클릭합니다.
   Edge Encryption 구성 목록이 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
암호 해독 또는 첨부 파일 암호 해독 작업을 실행하여 인스턴스의 데이터를 해독할 수 있습니다. 작업을 실행하지 않으면 암호화된 데이터는 다음에 변경될 때 해독됩니다.

암호화 작업 예약

필드에 구성된 기본 암호화 키를 사용하여 지정된 필드에서 암호화되지 않은 데이터를 찾고 암호화하도록 작업을 예약할 수 있습니다. 암호화할 필드를 구성한 후 암호화 작업을 생성하지 않으면 새 값만 암호화됩니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 다음으로 이동 에지 암호화 규칙 구성 > 암호화 구성 > 모두 필드에 대한 작업을 작성하거나 에지 암호화 규칙 구성 > 변수 암호화 구성 변수에 대한 작업을 작성하기 위함입니다.
2. 암호화 작업을 예약할 필드를 클릭합니다.
3. 관련 링크에서 대량 암호화 작업 예약을 클릭합니다.

   모든 필드가 채워진 암호화 작업 양식이 표시됩니다. 양식 하단에는 이전 작업 실행에 대한 기록이 표시됩니다.

4. 양식의 필드에 적절히 입력합니다.

필드	값
이름	설명적인 이름을 입력합니다.
활성	이 작업을 비활성화하려면 이 확인란의 선택을 취소합니다.
작업 유형	암호화를 선택합니다.
테이블	테이블을 선택합니다.
열	열을 선택합니다.
추정된 기록 카운트	처리할 총 예상 기록 수입니다. 기록 수 추정을 선택한 후에 채워집니다.
처리 이력 기록	필드가 감사되는 경우 감사 테이블에서 기록 기록을 처리하려면 선택합니다. 감사 테이블의 필드에 대한 이력 기록을 암호화하면 새 값과 이전 값이 모두 암호화됩니다. 감사되는 필드에 대한 자세한 내용은 을 참조하십시오 감사.
최대 감사 기록 카운트 추정	처리할 감사된 기록의 예상 최대 수입니다. 기록 수 추정을 선택한 후에 채워집니다. 이 필드는 이력 기록 처리를 선택한 경우에만 표시됩니다. 주: 예상치는 처리된 실제 기록 수보다 클 수 있습니다.
실행	작업 실행 간격을 선택합니다.
시작	작업을 처음 실행할 날짜 및 시간을 입력합니다.

5. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
6. 업데이트할 예상 기록 수를 보려면 기록 수 추정을 클릭합니다.
7. 작업을 즉시 실행하려면 지금 실행을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호 해독 작업 예약

암호화된 필드의 데이터를 해독하여 인스턴스에 지우기 데이터를 저장하는 작업을 예약할 수 있습니다.

시작하기 전에

주: 암호 해독 작업을 실행하려면 필드의 암호화 기록을 비활성으로 표시해야 합니다(활성 상자 선택 취소).

필요한 역할: security_admin

프로시저

1. 다음으로 이동 에지 암호화 규칙 구성 > 암호화 구성 > 모두 필드에 대한 작업을 작성하거나 에지 암호화 규칙 구성 > 변수 암호화 구성 변수에 대한 작업을 작성하기 위함입니다.
2. 암호를 해독하려는 필드를 클릭합니다.
3. 관련 링크에서 대량 암호 해독 작업 예약을 클릭합니다.

   모든 필드가 채워진 암호화 작업 양식이 표시됩니다. 양식 하단에는 이전 작업 실행에 대한 기록이 표시됩니다.

4. 양식의 필드에 적절히 입력합니다.

필드	값
이름	설명적인 이름을 입력합니다.
작업 유형	암호 해독을 선택합니다.
활성	이 작업을 비활성화하려면 이 확인란의 선택을 취소합니다.
테이블	테이블을 선택합니다.
열	열을 선택합니다.
추정된 기록 카운트	처리할 총 예상 기록 수입니다. 기록 수 추정을 선택한 후에 채워집니다.
처리 이력 기록	필드가 감사되는 경우 감사 테이블에서 기록 기록을 처리하려면 선택합니다. 감사 테이블의 필드에 대한 이력 기록을 암호화하면 새 값과 이전 값이 모두 암호화됩니다. 감사되는 필드에 대한 자세한 내용은 을 참조하십시오 감사.
최대 감사 기록 카운트 추정	처리할 감사된 기록의 예상 최대 수입니다. 기록 수 추정을 선택한 후에 채워집니다. 이 필드는 이력 기록 처리를 선택한 경우에만 표시됩니다. 주: 예상치는 처리된 실제 기록 수보다 클 수 있습니다.
실행	작업 실행 간격을 선택합니다.
시작	작업을 처음 실행할 날짜 및 시간을 입력합니다.

5. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
6. 업데이트할 예상 기록 수를 보려면 기록 수 추정을 클릭합니다.
7. 작업을 즉시 실행하려면 지금 실행을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표준 암호화를 사용하여 첨부 파일 암호화

특정 테이블의 첨부 파일을 암호화할 수 있습니다.

테이블에 대한 모든 첨부 파일이 동일한 암호화 유형을 사용합니다. 텍스트 검색을 수행할 때 암호화된 첨부 파일은 검색되지 않습니다. 표준 암호화 유형만 첨부 파일에 허용됩니다. 순서 유지 또는 같음 유지 암호화 유형은 허용되지 않습니다.

프록시를 우회하는 세션의 에지 암호화 규칙 경우:

- 첨부 파일 암호화가 활성화된 기록에서:
  - 사용자는 첨부 파일과 첨부 파일 이름이 있는 것을 볼 수 있습니다.
  - 사용자는 새 첨부 파일을 추가할 수 없습니다.
- 첨부 파일 암호화가 활성화되지 않은 기록에서:
  - 사용자는 기존 첨부 파일을 열고 다운로드할 수 있습니다.
  - 사용자는 새 첨부 파일을 추가할 수 있습니다.

암호화 프록시를 사용하는 세션의 경우 사용자는 기존 첨부 파일을 열어 다운로드하고 새 첨부 파일을 추가할 수 있습니다.

첨부 파일 암호화 구성

첨부 파일을 암호화할 테이블을 선택하고 암호화 유형을 식별합니다.

시작하기 전에

필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 에지 암호화 규칙 구성 > 새로 작성.
2. 양식의 필드에 적절히 입력합니다.

에지 암호화 규칙 구성

필드	설명
테이블	첨부 파일을 암호화할 테이블을 선택합니다.
유형	테이블, 열 또는 테이블의 첨부 파일을 암호화할지 여부입니다. 첨부 파일을 선택합니다.
열	암호화할 테이블 필드입니다. 이 필드는 유형이첨부 파일인 경우에는 나타나지 않고 유형이 열인 경우에는 나타납니다.
암호화 유형	사용할 암호화 유형입니다. 첨부 파일의 경우 표준 AES128 및 표준 AES256만 허용됩니다.

3. 제출을 클릭합니다.

다음에 수행할 작업

암호화 기록이 추가된 후 첨부 파일 암호화 작업을 생성하여 기존 첨부 파일을 암호화할 수 있습니다. 첨부 파일 암호화 작업을 실행하지 않는 경우, 새 첨부 파일을 첨부할 때 시스템에서 새 첨부 파일을 암호화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 테이블의 컬렉션 딕셔너리 항목에서 *edge_encryption_clear_attachment_allowed* ###**true** 로 표시하면 첨부 파일을 암호화하기 위해 에지 암호화 규칙을 사용하여 암호화되지 않은 첨부 파일이 테이블에 추가됩니다. 이 속성을 사용하는 경우 추가된 암호화되지 않은 첨부 파일이 암호화되도록 "첨부 파일 암호화 작업"을 설정해야 합니다.

첨부 파일 암호화 작업 예약

테이블에 대해 구성된 기본 암호화 키를 사용하여 지정된 테이블에 대해 암호화되지 않은 첨부 파일을 찾고 암호화하도록 작업을 예약할 수 있습니다.

시작하기 전에

필요한 역할: security_admin

프로시저

1. 다음으로 이동 에지 암호화 규칙 구성 > 암호화 구성 > 모두.
2. 암호화 작업을 예약할 테이블을 클릭합니다.
3. 관련 링크에서 대량 암호화 작업 예약을 클릭합니다.

   모든 필드가 채워진 암호화 작업 양식이 표시됩니다. 양식 하단에는 이전 작업 실행에 대한 기록이 표시됩니다.
4. 양식의 필드에 적절히 입력합니다.

필드	값
이름	설명적인 이름을 입력합니다.
활성	이 작업을 비활성화하려면 이 확인란의 선택을 취소합니다.
작업 유형	첨부 파일 암호화를 선택합니다.
테이블	테이블을 선택합니다.
실행	작업 실행 간격을 선택합니다.
시작	작업을 처음 실행할 날짜 및 시간을 입력합니다.

5. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
6. 업데이트할 예상 기록 수를 보려면 기록 수 추정을 클릭합니다.
7. 작업을 즉시 실행하려면 지금 실행을 클릭합니다.

첨부 파일 암호 해독 작업 예약

지정된 테이블에 대해 암호화된 첨부 파일을 해독하고 인스턴스에 지우기 첨부 파일을 저장하는 작업을 예약할 수 있습니다.

시작하기 전에

주: 암호 해독 작업이 실행되기 전에 테이블의 암호화 기록을 비활성으로 표시해야 합니다(활성 상자 선택 취소). 그렇지 않으면 아무 일도 일어나지 않습니다.

필요한 역할: security_admin

프로시저

1. 다음으로 이동 에지 암호화 규칙 구성 > 암호화 구성 > 모두.
2. 암호를 해독하려는 첨부 파일이 있는 테이블을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 관련 링크에서 대량 첨부 파일 암호 해독 작업 예약을 클릭합니다.

   모든 필드가 채워진 암호화 작업 양식이 표시됩니다. 양식 하단에는 이전 작업 실행에 대한 기록이 표시됩니다.

4. 양식의 필드에 적절히 입력합니다.

필드	값
이름	설명적인 이름을 입력합니다.
작업 유형	첨부 파일 암호 해독을 선택합니다.
활성	이 작업을 비활성화하려면 확인 표시를 선택 취소하십시오.
테이블	테이블을 선택합니다.
실행	작업 실행 간격을 선택합니다.
시작	작업을 처음 실행할 날짜 및 시간을 입력합니다.

5. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
6. 업데이트할 예상 기록 수를 보려면 기록 수 추정을 클릭합니다.
7. 작업을 즉시 실행하려면 지금 실행을 클릭합니다.

필드 또는 첨부 파일의 암호화 유형 변경

기존 암호화 구성 기록에서 새 암호화 유형을 선택하여 필드 또는 첨부 파일의 암호화 유형을 변경할 수 있습니다. 특정 테이블 및 필드 조합은 한 번에 하나의 활성 구성만 가질 수 있습니다.

시작하기 전에

필요한 역할: security_admin

프로시저

1. 다음으로 이동 에지 암호화 규칙 구성 > 암호화 구성 > 모두.
   Edge Encryption 구성 목록이 표시됩니다.
2. 변경할 암호화 구성에 대한 기록을 엽니다.
3. 암호화 유형 드롭다운을 클릭하고 새 암호화 유형을 선택합니다.

   주: 첨부 파일의 경우 표준 AES128 및 표준 AES256만 허용됩니다.

4. 필요한 경우 암호화 또는 첨부 파일 암호화 작업을 실행합니다.
   암호화 작업을 실행할 필요는 없습니다. 암호화 작업을 실행하지 않으면 다음에 필드 또는 첨부 파일이 변경될 때 새 암호화 유형을 사용하여 필드 또는 첨부 파일이 암호화됩니다.

암호화 패턴을 사용하여 문자열 토큰화

문자열 패턴을 인스턴스로 전송하여 저장하기 전에 토큰으로 바꿀 수 있습니다.

시작하기 전에

암호화 패턴을 사용하려면 네트워크에 MySQL 데이터베이스를 설치하고 설정해야 합니다. 이 데이터베이스는 순서 유지 암호화에 사용되는 것과 동일한 데이터베이스입니다. 암호화 패턴을 생성하거나 편집하려면 프록시를 통해 인스턴스에 연결되어 있어야 합니다.

필요한 역할: security_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

기본 시스템 패턴을 사용하거나 패턴을 직접 생성할 수 있습니다. 기본 시스템 패턴은 고급 패턴입니다. 암호화 패턴에는 다음과 같은 제한 사항이 포함됩니다.

- 모든 알파벳 문자의 패턴은 허용되지 않습니다.
- 최소 패턴 크기는 5자입니다. 시스템 속성을 사용하여 이 설정을 변경할 수 있습니다.
- * 및 + 수량자는 암호화 패턴에서 금지됩니다.
- 암호화 패턴은 더 큰 문자열에 포함된 문자열의 일부가 아닌 전체 단어와 일치합니다. 단어는 패턴에 포함할 수 없는 공백과 문자로 정의됩니다.
- 동일한 문자열이 인스턴스에 여러 번 전송되면 동일한 토큰으로 대체됩니다.
- 정확히 일치하는 항목에 대한 텍스트 검색이 지원됩니다. 쿼리 문자열은 인스턴스로 전송될 때 토큰과 교환되고, 토큰에 대해 검색이 수행되며, 검색 결과가 프록시 서버로 반환될 때 토큰은 일반 텍스트로 대체됩니다. 형태소 분석과 같은 기능은 지원되지 않습니다.

패턴을 사용할 때 일반 텍스트가 네트워크를 벗어나지 않습니다. 프록시 서버가 인스턴스로 이동하는 요청의 패턴과 일치하면 프록시는 문자열을 동일한 크기의 토큰으로 바꿉니다. 토큰은 일반 텍스트 문자열 대신 인스턴스로 전송됩니다. 인스턴스에서 프록시 서버로 응답을 보내면 프록시는 토큰을 문자열로 대체합니다. 프록시 서버를 통해 볼 때 문자열은 명확한 텍스트로 표시됩니다.

주: 암호화된 필드는 암호화 패턴을 검사하지 않습니다.

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 암호화 패턴 > 새로 작성.
   또는 고급 패턴 으로 이동하여 미리 구성된 패턴을 활성화하거나 편집할 수 있습니다.
2. 패턴 이름을 입력합니다.
3. 에지 패턴 입력 유형을 정의합니다.

옵션	설명
기본	일련의 문자 유형입니다. 기본 패턴 입력 탭에서 추가를 클릭하고 문자 유형을 선택합니다. 샘플 패턴은 문자가 추가될 때 패턴을 표시합니다. 새 블록을 클릭하여 다음 문자를 다음 줄로 이동합니다. 이렇게 하면 긴 패턴으로 문자를 그룹화할 수 있습니다. **X**를 클릭하여 패턴의 마지막 문자를 삭제합니다.
고급	Java RegEx 표현식입니다. 고급을 선택하면 입력 유형을 다시 기본으로 변경할 수 없습니다. 샘플 일치 필드에 정규 표현식을 테스트할 샘플 패턴을 입력합니다. 패턴 필드에 Java RegEx 표현식을 입력합니다. 유효성 검사를 클릭하여 식이 샘플 패턴과 일치하는지 확인합니다.

   입력 유형은 패턴을 입력하는 방법을 정의합니다. 패턴 사용 방식에는 영향을 주지 않습니다.

4. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주문 보존 암호화된 데이터 복구 또는 복구

security-admin 역할이 있는 경우 순서 유지 암호화를 사용하는 필드를 복구하도록 프록시에서 에지 암호화 규칙 수행하는 작업을 예약할 수 있습니다.

작업을 예약하여 다음을 수행합니다.

- 수리 주문 토큰입니다.
- 프록시 데이터베이스를 다시 만듭니다.

이러한 작업을 실행하는 것은 프록시 성능에 에지 암호화 규칙 영향을 줄 수 있는 시간 소모적인 작업일 수 있습니다. 사용자 또는 최소 사용자 집합이 시스템을 사용하지 않는 시간(예: 주말 자정)에 이러한 작업을 예약합니다.

토큰 주문 복구 작업 예약

주문 토큰이 누락된 필드를 찾아 복구하도록 작업을 예약할 수 있습니다.

시작하기 전에
필요한 역할: security_admin

이 태스크 정보
이러한 작업을 사용하여 테이블의 개별 필드를 복구하거나 순서 유지 암호화를 사용하여 모든 필드를 복구합니다. 인스턴스가 실행되는 동안 프록시 데이터베이스가 오프라인 상태일 때 이 작업을 실행하여 순서 토큰이 누락된 필드를 순서대로 보존하게 됩니다.

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 유지관리 > 토큰 복구 주문 예약.
2. 양식의 필드에 적절히 입력합니다.

필드	값
이름	설명적인 이름을 입력합니다.
작업 유형	토큰 복구 주문을 선택합니다.
모든 필드	모든 테이블을 복구하려면 이 확인란을 선택합니다.
테이블	테이블을 선택합니다.
열	열을 선택합니다.
활성	이 작업을 비활성화하려면 이 확인란의 선택을 취소합니다.
실행	작업 실행 간격을 선택합니다.
시작	작업을 처음 실행할 날짜 및 시간을 입력합니다.

3. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
4. 업데이트할 기록의 예상 수를 보려면 예상 기록 수를 클릭합니다.

프록시 데이터베이스 복구 작업 예약

프록시 데이터베이스에서 데이터가 손실되면 이 작업을 실행합니다. 이 작업은 토큰(순서 유지 암호화 유형)으로 암호화된 모든 기록을 찾아 프록시 데이터베이스를 다시 빌드할 수 있도록 프록시로 보냅니다.

시작하기 전에
필요한 역할: security_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 유지관리 > 데이터베이스 복구 예약.
2. 양식의 필드에 적절히 입력합니다.

필드	값
이름	이 작업을 설명하는 이름을 입력합니다.
작업 유형	데이터베이스 복구를 선택합니다.
활성	이 작업을 비활성화하려면 이 확인란의 선택을 취소합니다.
실행	작업 실행 간격을 선택합니다.
시작	이 작업을 처음 실행할 날짜 및 시간을 입력합니다.

3. 양식 헤더에서 메뉴 아이콘을 클릭하고 저장을 선택합니다.
4. 업데이트할 예상 기록 수를 보려면 기록 수 추정을 클릭합니다.

IP 주소 거부 목록 구성

네트워크의 IP 주소가 인스턴스로 요청을 보내지 못하도록 방지

시작하기 전에
필요한 역할: security_admin
에지 암호화 규칙 프록시 서버는 네트워크에 상주하기 때문에 네트워크 소프트웨어에 의한 취약성 검사의 대상이 될 수 있습니다. IP 스캐너 또는 기타 요청이 인스턴스로 ServiceNow 전달되지 않도록 하려면 IP 주소, IP 범위 또는 네트워크 마스크를 거부 목록에 추가할 수 있습니다. 거부 목록에 나열된 주소에서 프록시 서버로의 모든 연결은 종료되고 인스턴스로 전달되지 않습니다.

거부 목록에 IP 주소를 배치하려면 프록시 서버를 통해 인스턴스에 로그인해야 합니다.

중요사항: 거부 목록에 네트워크의 IP 주소를 추가하기 전에 네트워크 토폴로지를 이해해야 합니다. 거부 목록에 IP 주소가 추가되면 해당 IP 주소를 가진 모든 사용자가 프록시 서버에 액세스할 수 에지 암호화 규칙 없도록 차단됩니다.

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 유지관리 > 거부 목록 **IP** 주소.
   암호화 프록시 IP 거부 목록 [edge_encryption_ip_blacklist] 목록 뷰가 열립니다.
2. 새로 만들기를 클릭합니다.
3. 양식을 작성합니다.

필드	설명
프록시 서버	에지 암호화 규칙 거부 목록에 있는 주소의 요청을 전달할 수 없는 프록시 서버입니다.
IP, IP 범위 또는 넷마스크	이 IP 주소, 범위 또는 네트워크 마스크의 요청은 인스턴스 ServiceNow 로 전달되지 않습니다. 값의 예는 다음과 같습니다. ◦ IP 주소: 10.10.10.5 ◦ IP 범위: 10.10.10.1-15 ◦ 네트워크 마스크: 10.10.10.0/24

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: IPv4 또는 IPv6 주소를 사용할 수 있습니다.
활성	기록의 활성화 여부입니다. 활성 기록의 IP 주소만 인스턴스로 요청을 보낼 수 없습니다.
설명	거부 목록 기록에 대한 설명입니다.

4. 제출을 클릭합니다.
5. IP 주소를 거부해야 하는 다른 모든 프록시에 대해 이 단계를 반복합니다.

결과
에지 암호화 규칙 프록시 서버는 거부 목록의 IP 주소, 범위 또는 네트워크 마스크에서 연결을 종료하고 요청을 인스턴스에 전달할 수 없습니다.

기록 생성자의 데이터 암호화

에지 암호화 규칙 기록 생성자 기록에서 암호화 규칙을 만들어 기록 생성자에서 삽입을 허용하도록 프록시 서버를 구성합니다.

시작하기 전에

필요한 역할: security_admin
기록 생성자를 사용하면 최종 사용자가 및 에서 인시던트 기록 서비스 카탈로그 과 같은 작업 기반 기록을 만들 수 있습니다 서비스 포털. 기록 생성자가 암호화로 표시된 필드에 데이터를 삽입하려고 하면 잘못된 삽입 메시지가 표시되고 데이터가 필드에 저장되지 않습니다.

기록 생성자의 데이터를 암호화하려면 대상 필드에 대해 정의된 암호화 구성이 필요합니다. 기록 생성자에서 암호화 규칙을 생성하기 전에 대상 필드 및 테이블에 대한 암호화 구성을 생성했는지 확인하십시오. 필드 암호화 구성 작성를 참조하십시오. 기록 생성자 첨부 파일 암호화 구성의 첨부 파일을 암호화하려면 .

프로시저

1. 프록시 서버를 통해 에지 암호화 규칙 인스턴스에 로그인합니다.
2. 다음으로 이동 서비스 카탈로그 > 카탈로그 정의 > 기록 생성자.
3. 기록 생성자 기록을 만들거나 기존 기록 생성자 기록을 엽니다.
4. 관련 링크에서 에지 암호화 규칙 생성을 선택합니다.
   기록 생성자에서 암호화 대상으로 표시된 필드로 전송되는 데이터를 암호화하기 위해 두 개의 비활성 암호화 규칙이 자동으로 생성됩니다.

암호화 규칙	설명
<RecordProducerName>	에서 POST 매개변수를 서비스 카탈로그 처리하고 변수를 인스턴스의 필드에 매핑하기 위해 생성된 규칙입니다.
<RecordProducerName>Json	에서 JSON 페이로드 서비스 포털 를 처리하고 변수를 인스턴스의 필드에 매핑하기 위해 생성된 규칙입니다.

5. 기록 생성자가 만든 필수 암호화 규칙을 활성화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 에지 암호화 규칙 구성 > 규칙 > 모두.

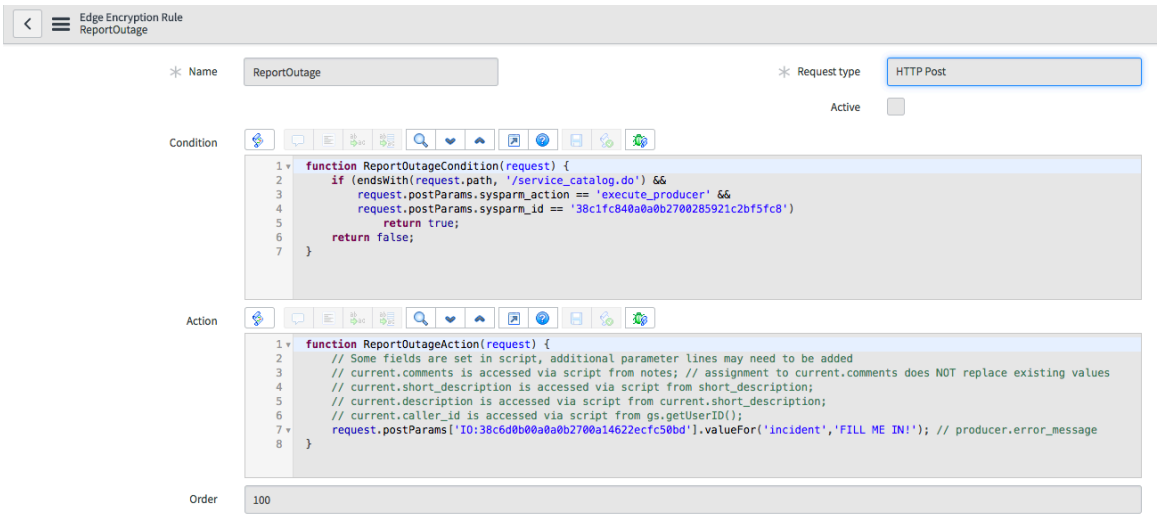
b. 기록 생성자가 사용될 위치에 따라, 기록 생성자가 만든 관련 암호화 규칙을 열고 활성 플래그를 선택합니다.
에서 서비스 카탈로그기록 생성자를 사용하는 경우 <RecordProducerName> 암호화 규칙을 활성화합니다. 에서 서비스 포털기록 생성자를 사용하는 경우 <RecordProducerName>Json 암호화 규칙을 활성화합니다.

6. 옵션: 암호화 규칙 작업 필드를 검사하고 필요한 필드 이름 또는 문을 추가합니다.

(Optional) 기록 생성자가 변수를 테이블의 필드에 직접 매핑하는 경우, 암호화 규칙은 변수를 올바른 필드에 자동으로 매핑합니다. 그러나 변수가 플랫폼의 다양한 스크립트를 통해 간접적으로 매핑되는 경우 각 변수를 올바른 필드에 매핑하기 위해 규칙을 업데이트해야 할 수 있습니다.

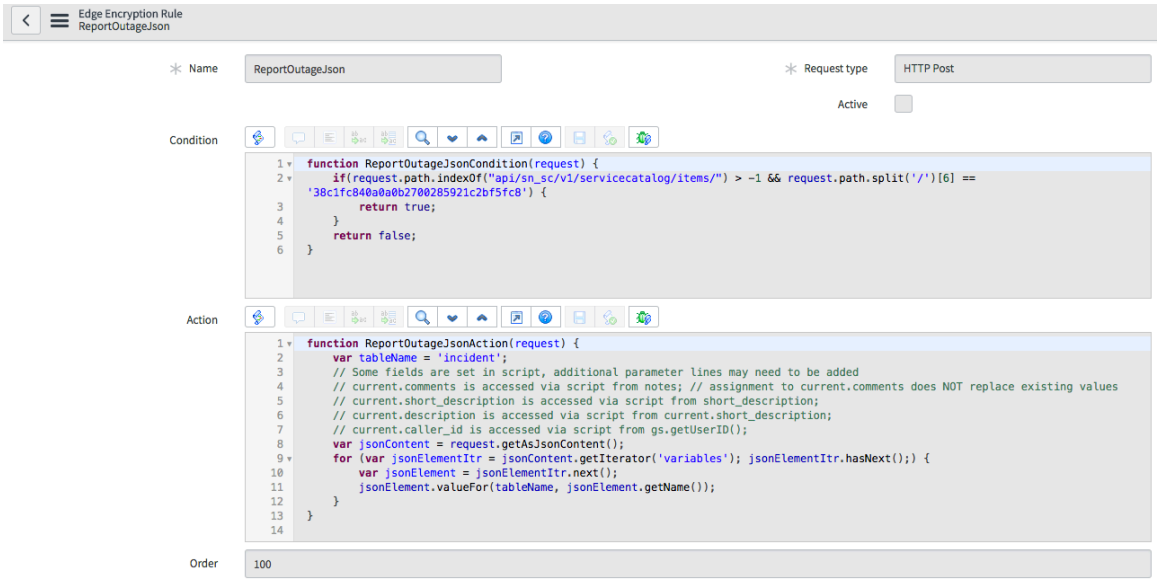
Example

(Optional) 아래 암호화 규칙은 보고서 중단 기록 생성자에서 생성되었으며 변수를 인스턴스의 필드에 매핑하기 위해 서비스 카탈로그 POST 매개변수를 처리합니다. `'FILL ME IN'`을 대상 필드로 바꿉니다.



아래 암호화 규칙은 중단 보고서 기록 생성자에서 생성되었으며 변수를 인스턴스의 필드에 매핑하기 위해 JSON 페이로드 서비스 포털 를 처리합니다. 추가 명령문을 추가하여 스크립트된 변수를 대상 필드에 매핑합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



기록 생성자의 페이로드를 검사할 때 error_message 요소에 short_description 필드의 값이 포함됩니다. 다음 문을 추가하여 스크립팅된 변수 error_message short_description 필드에 매핑할 수 있습니다.

```
if (jsonElement.getName() == 'error_message')
        jsonElement.valueFor(tableName, 'short_description');
```

작업 필드의 값은 다음과 같습니다.

```
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());
 }
}
```

결과
두 가지 암호화 규칙을 사용하면 기록 생성자가 또는 서비스 포털에서 암호화하도록 표시된 필드에 값을 삽입할 수 있습니다서비스 카탈로그.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 지정 암호화 규칙 정의

인스턴스로 가는 도중에 HTTP 요청에서 중요한 정보를 식별하고 암호화해야 할 수 있습니다. 이러한 요청의 데이터를 식별, 해석 및 암호화하는 암호화 규칙을 작성하여 요청의 필드를 인스턴스의 테이블 필드 이름에 매핑할 수 있습니다.

암호화 규칙이란?

암호화 규칙은 요청의 필드를 인스턴스의 테이블에 ServiceNow 있는 필드에 매핑하기 위해 프록시 서버에서 실행되는 에지 암호화 규칙 스크립트입니다. 암호화 규칙은 프록시 서버에 사용자 지정 페이로드의 데이터를 암호화하는 방법을 알려줍니다 에지 암호화 규칙 .

주: 암호화 규칙은 ECMAScript 3 이하만 지원합니다.

사용자 지정 규칙을 사용해야 하는 경우

일련의 암호화 규칙이 플러그인의 에지 암호화 규칙 일부로 포함됩니다. 이러한 규칙은 다음과 같은 여러 핵심 플랫폼 사용 사례를 처리합니다.

- 목록 편집 양식에서 필드 편집
- 기록 양식에서 기록 업데이트
- 직접 웹 서비스 관리
- REST API(애플리케이션 프로그램 인터페이스)에서 데이터 처리

표준 양식과 목록을 사용하여 만든 애플리케이션은 사용자 지정 암호화 규칙 없이 작동해야 합니다.

암호화해야 하는 데이터가 포함된 스크립트를 개발하는 경우 암호화 규칙을 생성하여 해당 데이터를 찾아 Glide 테이블 필드 이름에 매핑합니다. 예:

- 스크립팅된 프로세서
- 스크립트 기반 웹 서비스
- 스크립트된 REST API, UI 또는 Ajax 스크립트

암호화 규칙의 형식

규칙은 다음 세 부분으로 구성됩니다.

- 조건: 요청의 유형을 식별합니다.
- 작업: 요청의 필드를 테이블의 필드에 매핑하여 암호화 구성이 정의된 필드에 매핑되는 값을 암호화합니다.
- 순서: 규칙의 우선순위입니다. 충족 조건이 있는 가장 낮은 우선순위 규칙은 실행되는 유일한 규칙입니다. 비즈니스 규칙과 마찬가지로 규칙은 가장 낮은 규칙에서 가장 높은 순위로 실행됩니다.

첨부 파일 요청을 제외하고 HTTP 요청은 프록시 서버에서 평가됩니다 에지 암호화 규칙 . 에지 암호화 규칙 프록시 서버는 모든 조건이 false를 반환하거나 한 조건이 true를 반환할 때까지 우선 순위에 따라 모든 암호화 규칙 조건을 평가합니다. 조건이 true를 반환하면 요청에 따라 작업이 실행되고 결과가 인스턴스로 전달됩니다. 다른 조건은 평가되지 않습니다. 따라서 암호화 규칙 조건은 가능한 한 구체적이어야 합니다. 일반 규칙은 다른 규칙에 의해 처리되어야 하는 요청에 대해 true로 평가될 수 있으며, 이로 인해 잘못된 동작으로 요청이 처리될 수 있습니다. 일반 조건이 불가피한 경우 더 구체적인 규칙이 먼저 평가되도록 규칙을 높은 순서 값으로 표시해야 합니다.

암호화 규칙 생성 지침

효율적이고 최적화된 암호화 규칙을 작성하면 스크립트 확인 처리 시간을 줄일 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

전반적인 지침: 규칙이 길어지면 블록 수를 최소화하고 가능한 한 규칙을 분리하기 위해 최선을 다하십시오. 이상적으로 사용자 지정 규칙은 작업 스크립트에 `ifs` 또는 switch 문을 사용하여 여러 케이스를 포함하기보다는 특정 사용 사례에 적용되는 것이 좋습니다.

1. 가능할 때마다 규칙을 분할합니다. 예:
   - 테이블마다 서로 다른 규칙을 만들고 각 규칙이 해당 테이블에서만 실행되도록 합니다.
   - 대상으로 하는 각 기록 생성자에 대해 또는 최소한 기록 생성자의 각 하위 집합에 대해 서로 다른 규칙을 만듭니다. 수십 개의 `sys_ids` 대상으로 하는 하나의 규칙 대신 더 작은 하위 집합 레코드 생성자를 대상으로 하는 여러 개의 규칙을 만들거나 `sys_id`당 하나의 규칙을 만들 수도 있습니다.

     주: 여러 규칙을 생성하려면 더 많은 유지 관리가 필요합니다. 단점은 더 길고 복잡한 규칙보다 더 간단한 여러 규칙의 유효성을 더 효율적으로 검증할 수 있다는 것입니다.

2. 블록 수를 최소화합니다. 처리 엔진은 스크립트를 평가하는 동안 각 블록을 스캔하기 때문에 블록 수가 많으면 유효성 확인이 지연됩니다. 예:
   - 모든 `if` 블록을 배열 검색으로 바꾸고 배열 검색의 모든 블록을 하나의 `if` 블록으로 바꿉니다.
   - `if` 블록을 그룹화할 수 있을 때마다 결합합니다.

암호화 규칙 API

암호화 규칙은 JavaScript로 작성되며 API를 사용하여 에지 암호화 규칙 요청 본문에서 중요한 정보를 찾아 암호화합니다. API는 xPath와 유사한 표현식을 사용하여 JSON 및 XML 콘텐츠를 모두 탐색합니다.

에지 암호화 규칙 API는 출력 스트림에 기록되는 스트림에서 요청을 처리합니다. 스트림 구문 분석을 사용하면 암호화 규칙이 네트워크 성능을 발휘할 수 있습니다. 그러나 본문에서 콘텐츠를 여러 번 가져오고 구문 분석하면 예기치 않은 결과가 발생할 수 있습니다. 이 잠재적 문제를 무효화하려면 작업에서 요청을 한 번에 처리해야 합니다.

암호화 규칙을 만들 때 Glide API, 스크립트 포함, 비즈니스 규칙 또는 *`current`* 등의 전역 매개변수를 사용할 수 없습니다. HTTP 객체에 대해 규칙이 생성되기 때문에 전역 `##`객체를 사용할 수 있습니다.

암호화 규칙을 만들 때 허용 목록 관리자 또는 범위가 지정된 애플리케이션의 API를 사용할 수 없습니다.

오류 처리

암호화 규칙 조건 또는 작업에서 예외가 발생하는 경우 프록시 로그에서 문제 해결 정보를 확인합니다.

클라이언트 요청 검사

사용자 지정 암호화 규칙을 만들기 전에 프록시 서버에 들어가는 에지 암호화 규칙 클라이언트 요청의 형식을 결정해야 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
암호화 규칙은 클라이언트 요청을 반복하고 암호화해야 할 사항이 무엇인지 결정하기 때문에 규칙을 생성하는 요청 유형을 이해해야 합니다. 클라이언트 요청의 형식은 암호화 규칙의 구조와 규칙에서 사용할 수 있는 API를 결정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

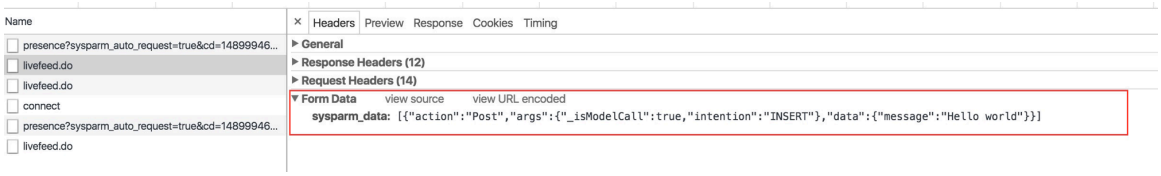
1. 클라이언트 요청을 검사합니다.

   요청 소스에 따라 다음 도구를 사용하여 요청을 검사하고 형식을 결정할 수 있습니다.

요청의 소스	사용 가능한 도구
클라이언트 브라우저	브라우저에서 개발자 콘솔을 사용하여 클라이언트 요청을 검사합니다. 유용한 도구는 다음과 같습니다. ◦ Firefox 네트워크 모니터 ◦ Chrome 네트워크 패널
외부 공급업체/외부 소스	HTTP 프로토콜 분석기를 사용하여 요청을 검사합니다. 유용한 도구는 다음과 같습니다. ◦ 와이어샤크 ◦ HTTP 특종 또는 외부 소스에 대한 설명서를 사용하여 요청 형식을 결정할 수 있습니다.

2. 클라이언트 요청에서 패킷을 검사하고 다음을 확인합니다.
   - 클라이언트 요청 메서드
   - 요청의 URL 경로
   - URL 매개변수
   - POST 매개변수(있는 경우)
   - 요청 본문의 형식(포함된 경우)

Example



결과
요청을 검사하면 암호화 규칙에서 필터링하고 반복해야 하는 필드를 이해할 수 있습니다. ##객체의 필드를 이해하려면 다음 문서를 참조하십시오요청.

암호화 규칙 생성

암호화 규칙은 프록시에서 암호화해야 하는 HTTP 요청에서 콘텐츠를 찾는 데 사용됩니다.

시작하기 전에
필요한 역할: security_admin
암호화 규칙을 만들기 전에 형식을 결정해야 합니다 클라이언트 요청 검사 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
암호화 규칙을 만들거나 편집하려면 암호화 프록시를 통해 인스턴스에 연결되어 있어야 합니다.

프로시저

1. 다음으로 이동 모두 > 에지 암호화 규칙 구성 > 규칙 > 새로 작성.
2. 이름 상자에 이름을 입력합니다.
3. 요청 유형에서 HTTP 메서드를 선택합니다.
   - **HTTP** 게시
   - **HTTP** 임포트
   - **HTTP** 넣기
   - **HTTP** 패치
   - **HTTP** 삭제

   주: Jakarta 사전 인스턴스는 **HTTP Get** 및 **HTTP Post** 메서드만 허용합니다.
4. 조건 상자에 규칙을 실행할 시기를 정의하는 JavaScript 문을 입력합니다.
5. 작업 상자에 조건이 true일 때 실행할 JavaScript 함수를 입력합니다.
6. 순서 상자에 규칙의 상대적 우선순위를 입력합니다.
7. 제출을 클릭하거나 양식을 저장합니다.

암호화 규칙 조건

암호화 규칙 조건에 따라 규칙을 실행해야 하는지 여부가 결정됩니다.

규칙이 HTTP 요청을 처리하는 경우 암호화 규칙 조건이 true를 반환해야 합니다. 그렇지 않으면 false를 반환해야 합니다.

조건을 빌드할 때 요청당 하나의 규칙만 실행된다는 점에 유의하십시오. 따라서 조건은 의도한 상황에서 실행하는 데 필요한 만큼 일반적이거나 구체적이어야 합니다.

주: 조건의 내용을 확인할 때 주의하십시오. 과도한 검사는 프록시 서버에 비용이 많이 들 수 있으며 복잡한 요청을 처리할 때 대기 시간이 증가할 수 있습니다.

조건은 메서드 유형, 콘텐츠 유형, URL 경로 또는 URL 쿼리 문자열 매개변수를 사용하여 규칙이 요청을 처리해야 하는지 여부를 결정할 수 있습니다. 조건은 객체를 통해 이러한 필드에 액세스할 수 있습니다 요청 . 암호화 규칙 조건을 생성하기 전에 클라이언트 요청을 검사하고 규칙을 트리거하는 데 필요한 조건을 이해해야 합니다.

주: 효율적인 규칙을 작성하려면 규칙으로 평가되지 않으려는 요청을 쉽게 배제할 수 있는 방법을 고려하십시오. 먼저 해당 요청에 대해 false를 반환하도록 조건을 빌드합니다. 이 방법은 성능을 향상시키고 요청을 올바른 규칙으로 신속하게 라우팅합니다.

암호화 규칙 객체 및 API 암호화 규칙 조건에 사용할 수 있습니다.

경로 및 **postParams** 사용 예

```
/*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) {
```

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
   if (endsWith(request.path, "/sample_processor.do") &&
 request.postParams.myPostParam) {
       return true;
   }
   return false;
}
```

urlParams 및 contentType 사용 예

```
/* 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;
}
```

암호화 규칙 작업

암호화 규칙은 클라이언트 요청의 필드를 인스턴스의 테이블에 있는 필드에 매핑하고 암호화로 표시된 필드를 식별합니다.

암호화 규칙 조건은 true를 반환하는 경우에만 암호화 규칙 작업이 실행됩니다. 암호화 규칙은 요청 페이로드에서 암호화할 데이터를 식별합니다. 규칙은 요청 개체의 콘텐츠를 반복하기 때문에 요청 본문의 형식과 구조를 이해하고 요청에서 암호화해야 하는 항목을 결정해야 합니다. 암호화할 데이터는 다음 위치에 있을 수 있습니다.

- POST 또는 URL 매개변수.
- POST 또는 URL 매개변수 내의 JSON 또는 XML 콘텐츠.
- JSON 페이로드입니다.
- XML 페이로드입니다.

암호화 규칙 작업을 작성하기 전에 다음을 확인하십시오.

- 클라이언트 요청 검사.
- 요청 객체에서 중요한 데이터가 있는 위치를 식별합니다.
- 데이터를 삽입할 필드 및 테이블 이름을 결정하거나 요청에서 동적으로 가져오는 방법을 이해합니다.

암호화 규칙 객체 및 API 암호화 규칙 작업 및 조건에 사용할 수 있습니다.

암호화 규칙 객체 및 API

암호화 규칙 API를 사용하여 프록시 서버를 통해 에지 암호화 규칙 인스턴스로 이동하는 요청의 값을 구문 분석하고 암호화합니다.

암호화 규칙에 사용할 수 있는 API는 요청 객체의 형식에 따라 달라집니다. 예를 들어 요청 객체의 contentType 매개 변수가 XML인 경우 페이로드 XML API 의 값을 구문 분석하고 암호화하는 데 사용할 수 있습니다. 요청에서 객체 유형을 결정한 후 사용 가능한 API를 사용하여 암호화 규칙을 빌드할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 규칙 API는 암호화 규칙 조건 및 작업 스크립트 모두에서 사용할 수 있습니다.

요청

*##*객체는 규칙, 작업 및 조건 스크립트에서 에지 암호화 규칙 사용할 수 있는 전역 객체입니다.

*##*개체는 프록시 서버로 들어오는 클라이언트 요청을 나타내는 JavaScript 개체입니다에지 암호화 규칙. *##*객체를 구문 분석하고, *##*객체 값을 인스턴스의 테이블에 있는 필드에 매핑하고, *##*객체의 민감한 데이터를 암호화하려면 암호화 규칙을 작성해야 합니다.

*##*객체에는 클라이언트 요청의 다음 속성과 데이터가 포함됩니다.

요청 객체 필드

필드	설명
경로	URL의 경로 부분입니다.
요청 방법	GET, POST, PUT, PATCH, DELETE.
contentType	Content-Type 헤더 필드입니다.
url매개변수	쿼리 문자열의 매개변수입니다. 이것은 String으로 평가될 수도 있습니다.
postParams	이것이 양식 게시물인 경우 여기에는 게시 매개변수가 포함됩니다.

요청 - getAsJsonContent()

요청을 *JsonNode* 형식의 반복 가능한 개체로 반환합니다.

이 메서드는 요청 본문이 유효한 JSON 페이로드인 경우 규칙에서만 에지 암호화 규칙 사용할 수 있습니다. 요청 본문에 포함된 형식이 확실하지 않은 경우 *##*객체의 contentType 필드를 확인합니다.

요청이 *JsonNode* 개체로 반환되면 개체를 JSON API 반복하고 필드를 암호화하는 데 사용할 수 있습니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
JsonNode	반복 가능한 *JsonNode*로서의 요청입니다.

요청 - getAsXmlContent()

요청 내용을 *XMLContent* 형식의 반복 가능한 개체로 반환합니다.

이 메서드는 요청 본문이 유효한 XML 페이로드인 경우에만 규칙에서 에지 암호화 규칙 사용할 수 있습니다. 요청 본문에 포함된 형식이 확실하지 않은 경우 *##*객체의 contentType 필드를 확인합니다.

요청이 *XMLContent* 객체로 반환되면 를 XML API 사용하여 객체를 반복하고 필드를 암호화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
XMLContent	*XMLContent* 형식의 반복 가능한 개체인 요청입니다.

요청 - XMLContains(문자열 경로)

지정된 경로가 XML DOM에 존재하는 경우 예를 반환합니다.

이 메서드는 요청 본문이 유효한 XML 페이로드인 경우에만 사용할 수 있습니다. 요청 본문에 포함된 형식이 확실하지 않은 경우 *##* 객체의 contentType 필드를 확인합니다.

매개변수

이름	유형	설명
경로	문자열	찾고 있는 XPath 문입니다.

반환

유형	설명
부울	지정된 경로가 XML DOM에 있는지 여부입니다.

POST 및 URL 매개변수 API

POST 및 URL 매개변수는 `request.postParams` 및 `request.urlParams`를 사용하여 *##* 객체의 속성으로 액세스할 수 있습니다.

`request.postParams.myParam`을 호출하여 *postParams* 및 *urlParams* 상위 객체의 속성으로 단일 매개변수에 액세스할 수 있습니다. 이러한 방식으로 액세스되는 모든 매개 변수는 기본 클래스 *ParameterValue*의 개체입니다. 이 클래스의 모든 API는 모든 매개변수에서 호출할 수 있습니다.

클라이언트 요청을 검사한 후 *##* 개체의 매개 변수 값에 액세스하고 암호화해야 할 수 있습니다. 클라이언트 요청의 데이터에 따라 값을 암호화하고 여러 가지 방법으로 인스턴스의 필드에 매핑할 수 있습니다.

알려진 테이블 및 필드의 값 암호화

암호화된 데이터를 저장할 인스턴스 테이블 및 필드의 이름을 알고 있는 경우 암호화 규칙에서 이를 명시적으로 정의할 수 있습니다. 예를 들어 인시던트를 생성하기 위한 요청이 인스턴스에서 처리되고 설명 필드의 텍스트 매개변수를 암호화하려 한다는 것을 알고 있을 수 있습니다. 이 경우 다음 작업을 만들 수 있습니다.

```
function SampleAction1() {
    request.postParams.text.valueFor('incident', 'description');
}
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

동적으로 정의된 테이블 및 필드의 값 암호화

반대로 암호화된 데이터가 채울 필드의 이름을 모르는 경우에는 **tableName** 및 **fieldName**을 사용하여 동적으로 정의할 수 있습니다.

아래 예시에서는 인스턴스의 여러 작업 테이블(예: 인시던트, 문제, change_request)에 데이터를 저장할 수 있는 일반 요청을 처리합니다.

```
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);
        }
    }
}
```

이 작업:

- URL 매개변수에서 대상 테이블을 가져옵니다.
- URL 매개변수를 반복합니다.
- 암호화 표시된 필드와 이름이 일치하는 URL 매개변수를 암호화하도록 프록시 서버에 요청합니다 에지 암호화 규칙 .
- *###*라는 특정 매개변수를 찾아 인시던트 테이블의 설명 필드에 대한 암호화 구성을 기반으로 값을 암호화하도록 프록시에 에지 암호화 규칙 요청합니다.

이 예제에서 valueFor() 메서드는 실제로 암호화를 수행하지 않습니다. 대신 메서드는 요청 개체의 테이블/필드 쌍이 암호화 구성을 사용하여 암호화하도록 표시되는지 여부를 확인하고 해당하는 경우 암호화하도록 프록시 서버에 요청합니다 에지 암호화 규칙 .

매개변수 내에서 **JSON** 또는 **XML** 암호화

POST 또는 URL 매개변수에는 JSON 또는 XML 컨텐츠가 포함될 수 있습니다. 이 경우 매개변수 내의 컨텐츠를 처리하고, 값을 반복하고, 필수 필드를 암호화할 수 있습니다. 이 예에서 **tableName** 은 POST 매개변수에서 계속 액세스되지만 필드 값은 JSON 객체 데이터입니다.

```
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);
        }
    }
}
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

POST 매개변수 내에서 XML을 처리하는 암호화 규칙 작업의 예입니다.

```
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);
        }
    }
}
```

쿼리 암호화

중요한 데이터를 포함하는 클라이언트 요청의 매개변수 내에서 인코딩된 쿼리가 발생할 수 있습니다. 쿼리의 필드를 인스턴스 데이터베이스의 암호화된 값과 일치시키려면 쿼리의 필드가 암호화되도록 표시되는지 여부를 확인하도록 프록시에 요청하는 암호화 규칙을 생성해야 합니다. encodedQueryFor() 메서드는 지정된 테이블에서 인코딩된 쿼리를 구문 분석하고 쿼리의 필드에 암호화 구성이 있는지 확인합니다.

이 예에서 규칙은 필터 매개변수를 찾는 매개변수를 반복하며, 이는 Glide로 인코딩된 쿼리가 될 것으로 예상됩니다.

```
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);
        }
    }
}
```

예를 들어 필터 값이 `short_description=# ### ##^##=INC000056^##=##`인 경우 쿼리는 인스턴스에서 `short_description=<####(# ### ##)>^##=INC000056^##=##` 이 됩니다.

ParameterValue - toString()

POST 또는 URL 매개변수 값을 문자열로 변환합니다.

매개변수

이름	유형	설명
없음		

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

반환

유형	설명
문자열	문자열로서의 매개변수 값입니다.

ParameterValue - getAsJsonContent()

요청을 *JsonNode* 형식의 반복 가능한 개체로 반환합니다.

이 메서드는 요청 본문이 유효한 JSON 페이로드인 경우 규칙에서만 에지 암호화 규칙 사용할 수 있습니다. 요청 본문에 포함된 형식이 확실하지 않은 경우 *##*객체의 contentType 필드를 확인합니다.

요청이 *JsonNode* 개체로 반환되면 개체를 JSON API 반복하고 필드를 암호화하는 데 사용할 수 있습니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
JsonNode	반복 가능한 *JsonNode*로서의 요청입니다.

ParameterValue - getAsXmlContent()

요청 내용을 *XMLContent* 형식의 반복 가능한 개체로 반환합니다.

이 방법은 규칙에서만 사용할 수 있습니다 에지 암호화 규칙 . 이 메서드는 요청 본문이 유효한 XML 페이로드라고 가정합니다. contentType을 확인하여 확인할 수 있습니다.

요청이 *XMLContent* 객체로 반환되면 를 XML API 사용하여 객체를 반복하고 필드를 암호화할 수 있습니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
XMLContent	*XMLContent* 형식의 반복 가능한 개체인 요청입니다.

ParameterValue - encodedQueryFor(String tableName)

요소의 값이 지정된 테이블에서 인코딩된 쿼리임을 지정합니다.

매개 변수에서 이 함수를 호출하면 매개 변수의 값이 지정된 테이블에 대한 인코딩된 쿼리 문자열 임을 프록시에 알릴 수 있습니다. 프록시는 인코딩된 쿼리를 구문 분석하고 암호화해야 하는 인코딩된 쿼리의 필드를 암호화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수

이름	유형	설명
tableName	문자열	쿼리가 실행될 테이블입니다.

반환

유형	설명
void	

ParameterValue - valueFor(문자열 테이블 이름, 문자열 필드 이름)

요소 값이 지정된 테이블의 지정된 필드에 매핑되도록 지정합니다.

요소 값에 대해 이 메서드를 호출하면 이 요소의 값이 지정된 테이블의 지정된 필드에 매핑됨을 프록시에 알립니다. 그런 다음 프록시는 필드를 암호화해야 하는지 확인합니다.

매개변수

이름	유형	설명
tableName	문자열	테이블 이름입니다.
fieldName	문자열	필드 이름입니다.

반환

유형	설명
void	

XML API

XML API는 요청 개체 또는 *ParameterValue* 속성에서 *getAsXmlContent()*를 호출한 후에 사용할 수 있습니다.

XML API를 사용하여 암호화 규칙을 작성하는 경우 다음과 같은 일반적인 형식을 따를 수 있습니다.

1. *##* 객체 또는 *ParameterValue* 속성에서 *getAsXmlContent()*를 호출합니다. *### XMLContent* 기본 클래스의 이터러블 객체를 반환합니다.
2. *XMLContent* 객체에서 *getIterator()* 또는 *getIterator(String xPath)*를 호출합니다. 그러면 XML 요소를 반복하는 데 사용할 수 있는 *XMLElementIterator* 객체가 반환됩니다.
3. *XMLElementIterator* 객체에서 *hasNext()* 메서드를 호출하여 다른 요소를 사용할 수 있는지 확인합니다.
4. *XMLElementIterator* 객체에서 *next()*를 호출하여 다음 XML 요소를 반환합니다. *hasNext()#* 먼저 호출하지 않고는 *next()*를 호출할 수 없습니다.
5. XML 요소에서 *valueFor(String tableName, String fieldName)* 를 호출합니다. 이 메서드는 이 요소의 값이 지정된 테이블의 지정된 필드에 매핑되도록 프록시에 지시합니다. 그런 다음 프록시는 필드를 암호화해야 하는지 확인합니다.

   주: XML 요소에서 *valueFor(String tableName, String fieldName)* 를 호출할지 여부를 결정하려면 *getName()* 메서드를 사용하여 요소의 이름을 반환할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스의 알려진 테이블 필드에 매핑

이 예시에서는 XML 페이로드가 인스턴스에서 처리되어 인시던트 테이블에 기록을 삽입합니다. 설명 필드는 인시던트의 short_description 채웁니다.

```
<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>
```

다음 암호화 규칙 작업을 적용할 수 있습니다.

```
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');
    }
}
```

이 작업은 설명 태그를 반복하고 프록시 서버에 값을 암호화하여 인스턴스의 incident.short_description에 삽입하도록 요청합니다.

주: 이 규칙은 XML 페이로드의 모든 기록 태그 내에서 모든 설명 태그를 찾습니다. 암호화할 태그가 하나만 있는 경우 규칙에서 xPath 및 반복기 구조를 계속 사용합니다. 그러나 루프에서 한 번만 반복됩니다.

인스턴스의 알 수 없는 테이블 필드에 매핑

이 예에서 규칙은 레코드 태그를 반복하지만 레코드 태그 내에서 예상되는 태그는 알 수 없습니다. 유일하게 알려진 것은 레코드 태그 내의 태그가 테이블 URL 매개변수에 지정된 열의 이름과 일치한다는 것입니다.

또한 이 규칙은 테이블이 인시던트인 경우 설명 태그의 데이터를 암호화하여 인스턴스의 short_description 필드에 저장하도록 지정합니다.

```
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());
    }
}
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
function encryptFieldsInRecord(xmlElement) {
    //Then, iterate over all tags representing fields in the table
    var fieldIterator = xmlElement.getIteratorOverAllChildren();
    while (fieldIterator.hasNext()) {
        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);
        }
    }
}
```

encryptFieldsInRecord() 함수에서 *valueFor()* 메서드는 요청에 따라 동적으로 할당된 테이블 및 필드에서 호출됩니다. 테이블과 필드 이름은 변경될 수 있지만 규칙은 정의된 암호화 구성에 따라 테이블의 필드를 암호화해야 하는지 여부를 확인하도록 프록시에 요청합니다.

필드가 암호화되도록 구성되지 않았거나 태그가 테이블의 필드와 일치하지 않는 경우 프록시는 해당 태그를 건너뜁니다. 태그가 암호화 에지 암호화 규칙 로 표시된 필드와 일치하면 프록시 서버가 값을 암호화합니다.

인코딩된 쿼리 사용

이 예에서 모든 태그에는 태그에 인코딩된 쿼리가 포함되어 있는지 여부를 나타내는 **filter** 속성이 있습니다.

```
<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>
```

다음 암호화 규칙 작업을 적용할 수 있습니다.

```
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());
   }
}
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
function encryptFieldsInRecord(xmlElement) {
   //this time we want to iterate over all tags representing fields in
 the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
   while (fieldIterator.hasNext()) {
       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);
       }
   }
}
```

필터 속성 값이 true이면 규칙은 프록시 서버에 인코딩된 쿼리의 값을 암호화하도록 요청합니다. false인 경우 규칙은 프록시에 필드 암호화 여부를 확인하도록 요청합니다.

XMLContent

XML 콘텐츠를 반복하는 메서드를 제공하는 전역 객체입니다.

객체에서 getAsXmlContent()를 호출하여 *XMLContent* 객체에 액세스할 수 있습니다.

`request.postParams.<parameter name>.getAsXmlContent()` 또는 `request.urlParams.<parameter name>.getAsXmlContent()`를 호출하여 POST 또는 URL 매개변수의 XML 데이터에 액세스합니다.

XMLContent - getIterator()

XML 내용에 대한 *XMLElementIterator* 객체를 반환합니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
XMLElementIterator	*XMLContent* 개체의 요소를 반복하는 데 사용할 수 있는 개체입니다.

XMLContent - getIterator(문자열 xPath)

지정된 매개 변수를 기반으로 XML 내용에 대한 *XMLElementIterator* 객체를 반환합니다.

매개변수

이름	유형	설명
xPath	문자열	*XMLContent* 객체에서 시작할 위치를 지정하는 xPath와 유사한 표현식입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

반환

유형	설명
XMLElementIterator	*XMLContent* 개체의 요소를 반복하는 데 사용할 수 있는 개체입니다.

XMLElementIterator

XML 요소를 반복하기 위한 메서드를 제공합니다.

XMLContent 클래스의 *getIterator()* 메서드를 호출하여 *XMLElementIterator* 객체를 가져옵니다.

XMLElementIterator - hasNext()

사용할 수 있는 다른 요소가 있는지 확인합니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
부울	다른 요소를 사용할 수 있으면 True입니다.

XMLElementIterator - 다음**()**

반복기의 다음 요소를 반환합니다.

hasNext()# 먼저 호출하지 않고는 *next()*를 호출할 수 없습니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
XMLElement	다음 XML 요소입니다.

XMLElement

XML 요소를 반복하고 값을 테이블의 필드에 매핑하는 메서드를 제공합니다.

XMLElementIterator 객체의 *next()* 메서드를 호출하여 *XMLElement* 객체를 얻습니다.

XMLElement - getIterator(문자열 **xPath)**

지정된 매개 변수를 기반으로 XML 요소에 대한 *XMLElementIterator* 개체를 반환합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수

이름	유형	설명
xPath	문자열	*XMLElement* 객체에서 시작할 위치를 지정하는 xPath와 유사한 표현식입니다.

반환

유형	설명
XMLElementIterator	*XMLElement* 개체의 요소를 반복하는 데 사용할 수 있는 개체입니다.

XMLElement - getIteratorOverAllChildren()

지정된 매개 변수를 기반으로 XML 요소의 모든 하위 요소를 포함하는 *XMLElementIterator* 개체를 반환합니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
XMLElementIterator	*XMLElement* 개체의 요소를 반복하는 데 사용할 수 있는 개체입니다.

XMLElement - valueFor(문자열 테이블 이름, 문자열 필드 이름)

요소 값이 지정된 테이블의 지정된 필드에 매핑되도록 지정합니다.

요소 값에 대해 이 메서드를 호출하면 이 요소의 값이 지정된 테이블의 지정된 필드에 매핑됨을 프록시에 알립니다. 그런 다음 프록시는 필드를 암호화해야 하는지 확인합니다. 테이블 및 필드 이름을 알 수 없는 경우 요청에 따라 동적으로 할당된 테이블 및 필드에서 *valueFor()* 메서드를 호출할 수 있습니다.

매개변수

이름	유형	설명
tableName	문자열	테이블 이름입니다.
fieldName	문자열	필드 이름입니다.

반환

유형	설명
void	

XMLElement - encodedQueryFor(String tableName)

요소의 값이 지정된 테이블에 대한 인코딩된 쿼리임을 지정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요소에서 이 함수를 호출하면 요소의 값이 지정된 테이블에 대한 인코딩된 쿼리 문자열 임을 프록시에 알릴 수 있습니다. 프록시는 인코딩된 쿼리를 구문 분석하고 암호화해야 하는 인코딩된 쿼리의 필드를 암호화합니다.

매개변수

이름	유형	설명
tableName	문자열	쿼리가 실행될 테이블입니다.

반환

유형	설명
void	

XMLElement - getName()

요소 이름을 반환합니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
문자열	요소 이름입니다.

XMLElement - getAttributeValue(문자열 속성)

지정된 속성의 값을 반환합니다.

매개변수

이름	유형	설명
속성	문자열	속성 이름입니다.

반환

유형	설명
문자열	속성 값입니다.

JSON API

JSON API는 요청 개체 또는 *ParameterValue* 속성에서 *getAsJsonContent()*를 호출한 후에 사용할 수 있습니다.

JSON API를 사용하여 암호화 규칙을 작성하는 경우 다음과 같은 일반적인 형식을 따를 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. *##* 객체에서 *getAsJsonContent()*를 호출합니다. *### JsonNode* 기본 클래스의 반복 가능한 객체를 반환합니다.
2. *JsonNode* 객체에서 *iterator()* 또는 *getIterator(String xPath)#* 호출합니다. JSON 객체의 노드를 반복하는 데 사용할 수 있는 *JsonNodeIterator* 객체를 반환합니다.
3. *JsonNodeIterator* 객체에서 *hasNext()* 메서드를 호출하여 다른 요소를 사용할 수 있는지 여부를 확인합니다.
4. *JsonNodeIterator* 객체에서 *next()*를 호출하여 다음 JSON 요소를 반환합니다. *hasNext()#* 먼저 호출하지 않고는 *next()*를 호출할 수 없습니다.
5. JSON 요소에서 *valueFor(String tableName, String fieldName)* 를 호출합니다. 이 메서드는 이 요소의 값이 지정된 테이블의 지정된 필드에 매핑되도록 프록시에 지시합니다. 그런 다음 프록시는 필드를 암호화해야 하는지 여부를 확인합니다.

   주: JSON 요소에서 *valueFor(String tableName, String fieldName)* 를 호출할지 여부를 결정하려면 *getName()* 메서드를 사용하여 요소의 이름을 반환할 수 있습니다.

인스턴스의 알려진 테이블 필드에 매핑

이 예시에서는 JSON 페이로드가 인스턴스에서 처리되어 인시던트 테이블에 기록을 삽입합니다. 설명 필드는 인시던트의 short_description 채웁니다.

```
{
    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"
}
```

다음 규칙이 적용될 수 있습니다.

```
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');
    }
}
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 작업은 설명 노드를 반복하고 프록시 서버에 값을 암호화하여 인스턴스의 incident.short_description에 삽입하도록 요청합니다.

주: 이 규칙은 JSON 페이로드 내에서 모든 설명 노드를 찾습니다. 암호화할 노드가 하나만 있는 경우 규칙은 여전히 xPath 및 반복기 구조를 사용합니다. 그러나 루프에서 한 번만 반복됩니다.

인스턴스의 알 수 없는 테이블 필드에 매핑

이 예시에서 규칙은 기록을 반복하지만 어떤 노드가 예상될지는 확실하지 않습니다. 유일하게 알려진 것은 레코드 내의 각 개체에 대해 노드가 테이블 URL 매개 변수에 지정된 열의 이름과 일치한다는 것입니다.

또한 이 규칙은 테이블이 인시던트인 경우 설명 노드의 데이터를 암호화하여 인스턴스의 short_description 필드에 저장하도록 지정합니다.

```
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);
            }
    }
}
```

encryptFieldsInRecord() 함수에서 *valueFor()* 메서드는 요청에 따라 동적으로 할당된 테이블 및 필드에서 호출됩니다. 테이블과 필드 이름은 변경될 수 있지만 규칙은 정의된 암호화 구성에 따라 테이블의 필드를 암호화해야 하는지 여부를 확인하도록 프록시에 요청합니다.

필드가 암호화되도록 구성되지 않았거나 노드 이름이 테이블의 필드와 일치하지 않는 경우 프록시는 해당 노드를 건너뜁니다. 노드 이름이 암호화로 표시된 필드와 일치하면 프록시가 값을 암호화합니다.

인코딩된 쿼리 사용

```
function sampleJsonAction3() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // 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());
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
        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);
    }
}
```

이 예에서 규칙은 데이터를 반복합니다. 기록을 찾으면 두 번째 예시와 동일한 논리를 수행하여 각 노드의 필드를 반복합니다. 쿼리 노드를 찾으면 *encodedQueryFor()*를 호출하여 쿼리에서 암호화해야 하는 값을 암호화합니다.

JsonNode

JSON 컨텐츠를 반복하는 메서드를 제공하는 전역 객체입니다.

객체에서 getAsJsonContent()를 호출하여 *JsonNode* 객체에 액세스할 수 있습니다.

`request.postParms.<parameter name>.getAsJsonContent()` 또는 `request.urlParms.<parameter name>.getAsJsonContent()`를 호출하여 POST 또는 URL 매개변수에서 JSON 콘텐츠에 액세스합니다.

JsonNode - getIterator(문자열 xPath)

JSON 콘텐츠에 대한 *JsonNodeIterator* 객체를 반환합니다.

이 메서드는 루트 노드에서만 사용할 수 있지만 JSON 개체 깊숙이 트래버스하는 데 사용할 수 있습니다. 후속 순회는 *iterator()* 메서드를 사용해야 합니다.

매개변수

이름	유형	설명
xPath	문자열	xPath 식입니다.

반환

유형	설명
JsonNodeIterator	JSON 객체의 노드를 반복할 수 있는 객체입니다.

JsonNode - 반복기 ()

현재 노드의 모든 자식 노드를 반복하는 *JsonNodeIterator* 개체를 반환합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
JsonNodeIterator	JSON 객체의 노드를 반복할 수 있는 객체입니다.

JsonNode - getAsString()

현재 노드 값을 문자열로 반환합니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
문자열	현재 노드 값입니다.

JsonNode - getAsString(문자열 속성 이름)

지정된 속성의 문자열 값을 반환합니다.

매개변수

이름	유형	설명
propertyName	문자열	속성의 이름입니다.

반환

유형	설명
문자열	속성 값입니다.

JsonNode - getName()

현재 JSON 노드의 이름을 반환합니다.

매개변수

이름	유형	설명
없음		

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

반환

유형	설명
문자열	현재 JSON 노드의 이름입니다.

JsonNode - valueFor(String tableName, String fieldName)

JSON 속성이 지정된 테이블의 지정된 필드에 매핑되도록 지정합니다.

JSON 속성에서 이 메서드를 호출하면 이 속성 값이 지정된 테이블의 지정된 필드에 매핑됨을 프록시에 알립니다. 그런 다음 프록시는 필드를 암호화해야 하는지 여부를 결정합니다. 테이블 및 필드 이름을 알 수 없는 경우 요청에 따라 동적으로 할당된 테이블 및 필드에서 `valueFor()` 메서드를 호출할 수 있습니다.

매개변수

이름	유형	설명
tableName	문자열	테이블 이름입니다.
fieldName	문자열	필드 이름입니다.

반환

유형	설명
void	

JsonNode - encodedQueryFor(문자열 tableName)

JSON 속성 값이 지정된 테이블에 대해 인코딩된 쿼리임을 지정합니다.

JSON 노드에서 이 함수를 호출하면 해당 값이 지정된 테이블에 대해 인코딩된 쿼리 문자열 임을 프록시에 알릴 수 있습니다. 프록시는 인코딩된 쿼리를 구문 분석하고 암호화해야 하는 인코딩된 쿼리의 필드 값을 암호화합니다.

매개변수

이름	유형	설명
tableName	문자열	쿼리가 실행될 테이블입니다.

반환

유형	설명
void	

JsonNodeIterator

`JsonNode` 클래스의 `getIterator()` 또는 `iterator()` 메서드를 호출하여 `JsonNodeIterator` 객체를 가져옵니다.

JsonNodeIterator - hasNext()

사용할 수 있는 다른 속성이 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
부울	다른 속성을 사용할 수 있는 경우 True입니다.

JsonNodeIterator - 다음()

반복기에서 다음 속성을 반환합니다.

hasNext()# 먼저 호출하지 않고는 *next()*를 호출할 수 없습니다.

매개변수

이름	유형	설명
없음		

반환

유형	설명
JsonNode	다음 *JsonNode*입니다.

print(문자열 메시지)

래퍼 로그 파일에 메시지를 인쇄합니다. `<proxy server directory>/logs/wrapper_<date>.log`.

이 메서드는 규칙 작업 스크립트에서만 사용할 수 있습니다 에지 암호화 규칙 .

매개변수

이름	유형	설명
메시지	문자열	래퍼 로그 파일에 기록할 메시지입니다.

반환

유형	설명
void	

금지된 키워드

프록시는 에지 암호화 규칙 규칙을 저장하기 전에 암호화 규칙 스크립트의 유효성을 검사합니다. 암호화 규칙 스크립트에는 많은 JavaScript 키워드가 허용되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

금지된 키워드

키워드
__DIR__
__파일__
__줄__
__부모__
__프로토__
오류
평가
클래스 다운로드
getPrototypeOf
Java
자바스
자바FX
자바임포터
로드
loadWithNewGlobal
새로 만들기
패키지
객체
프로토타입
정규 표현식
setPrototypeOf
이
던지다

에지 암호화 규칙 딕셔너리 속성

테이블 및 필드에 딕셔너리 속성을 추가하여 에지 암호화 규칙 작동 방식을 제어합니다.

딕셔너리 속성을 true로 설정하려면 속성 필드에 `attribute=true`를 입력해야 합니다. 레코드에 딕셔너리 속성을 추가하려면 다음 문서를 참조하십시오 딕셔너리 속성을 사용하여 테이블 및 필드 변경 .

에지 암호화 규칙 제외됨 [edge_encryption_excluded]

필드를 암호화에서 제외할지 여부를 결정합니다.

#로 설정하면 필드나 테이블을 암호화할 수 없습니다. `false`로 설정하면 필드를 암호화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 값: 예/아니오
- 대상 요소: 필드 또는 테이블
- 기본값: false

에지 암호화 규칙 사용 [edge_encryption_enabled]

필드가 암호화 구성을 통해 암호화할 수 있는지 여부를 결정합니다.

`true`로 설정하면 필드를 암호화할 수 있습니다. `false`로 설정하면 필드가 암호화될 수 없습니다. 이 특성은 시스템에서 사용되며 수정할 수 없으므로 사용자에게 표시되지 않습니다.

주: 이 속성은 필드가 암호화되었음을 나타내지 않으며 필드에서 암호화 논리를 트리거하지도 않습니다. 대신 속성은 사용자가 필드를 암호화할 가능성을 결정합니다.

- 값: 예/아니오
- 대상 요소: field
- 기본값: 문자열 필드에 대해 예

에지 암호화 일반 텍스트 허용됨 [edge_encryption_clear_text_allowed]

서버 측 스크립트가 프록시 서버를 통해 수행되는 사용자 작업 또는 예약된 작업과 같은 서버 측 자동화 스크립트에 대한 필드 내의 암호화된 문자열에 암호화되지 않은 데이터를 추가할 수 있는지 여부를 결정합니다.

`true`로 설정하면 데이터를 추가할 수 있습니다. `false`로 설정하면 데이터를 추가할 수 없습니다.

- 값: 예/아니오
- 대상 요소: field
- 기본값: false

도메인 분리 및 에지 암호화 규칙

도메인 분리는 와 함께 에지 암호화 규칙제한된 상황에서 지원됩니다. 는 프록시 에지 암호화 규칙 에 정의된 특정 구성, 규칙 및 키를 사용하여 고객의 환경 내에서 데이터를 암호화하는 에지 암호화 규칙 기능을 제공합니다. 프록시는 에지 암호화 규칙 도메인을 인식하지 않으며 도메인별 설정을 지원할 수 없습니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 지원 없음

- 도메인 필드가 데이터 테이블에 존재할 수 있지만 데이터를 관리할 비즈니스 논리가 없습니다.
- 이 수준은 도메인으로 구분된 것으로 간주되지 않습니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원을 참조하십시오.

에지 암호화 규칙에서 도메인 분리가 작동하는 방식

에지 암호화 규칙은 도메인별 키, 구성 및 규칙이 필요하지 않은 경우에 사용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

서비스 제공자용 도메인 분리

와의 데이터 통합 에지 암호화 규칙

를 사용하여 에지 암호화 규칙타사 데이터를 인스턴스와 통합하려면 지원되는 통합을 사용하여 프록시 서버를 통해 에지 암호화 규칙 데이터를 라우팅해야 합니다. 지원되는 통합은 각 페이로드의 데이터를 테이블의 필드에 매핑하는 기본 시스템 암호화 규칙을 사용합니다.

암호화 대상으로 표시된 필드에 데이터 업로드

에지 암호화 규칙 은 암호화 구성이 정의된 필드에서 Excel, CSV, XML 또는 기타 파일 형식으로 데이터를 가져오거나 내보내는 것을 지원하지 않습니다.

ODBC 드라이버

ODBC 드라이버를 사용하여 프록시 서버를 통해 에지 암호화 규칙 요청 및 쿼리 데이터를 암호화합니다.

자세히 알아보기: 에지 암호화 규칙 ODBC 드라이버 통합

MID 서버

프록시 서버를 통해 데이터를 라우팅하도록 구성할 MID 서버 수 있습니다 에지 암호화 규칙 . 그러나 몇 가지 제한 사항이 적용됩니다.

자세히 알아보기: 에지 암호화 규칙 MID 서버 통합

REST/SOAP 웹 서비스

프록시 서버를 통해 에지 암호화 규칙 레코드 데이터를 업데이트하거나 검색하려면 REST/SOAP 웹 서비스를 사용합니다.

자세히 알아보기: 웹 서비스

JSONv2 웹 서비스

JSONv2 웹 서비스 API를 사용하여 프록시 서버를 통해 에지 암호화 규칙 기록 데이터를 업데이트하거나 검색합니다. 기본 시스템 암호화 규칙은 데이터 검색 및 데이터 수정 API를 지원합니다.

- 데이터 수정 API를 사용하여 단일 레코드를 삽입하려면 `insert()` 또는 `insertMutiple()` 메서드를 사용합니다.
- 데이터 수정 API를 사용하여 여러 레코드를 삽입하려면 `insertMultiple()` 메서드를 사용합니다.

자세히 보기: JSONv2 웹 서비스

위에 나열되지 않은 사용자 지정 타사 통합의 데이터를 암호화하려면 사용자 지정 암호화 규칙을 생성합니다. 사용자 지정 암호화 규칙 정의를 참조하십시오.

암호화로 표시된 기록에 첨부 파일 업로드

REST 및 SOAP 웹 서비스를 사용하여 구성된 첨부 파일 암호화를 사용하여 첨부 파일을 테이블에 업로드할 수 있습니다.

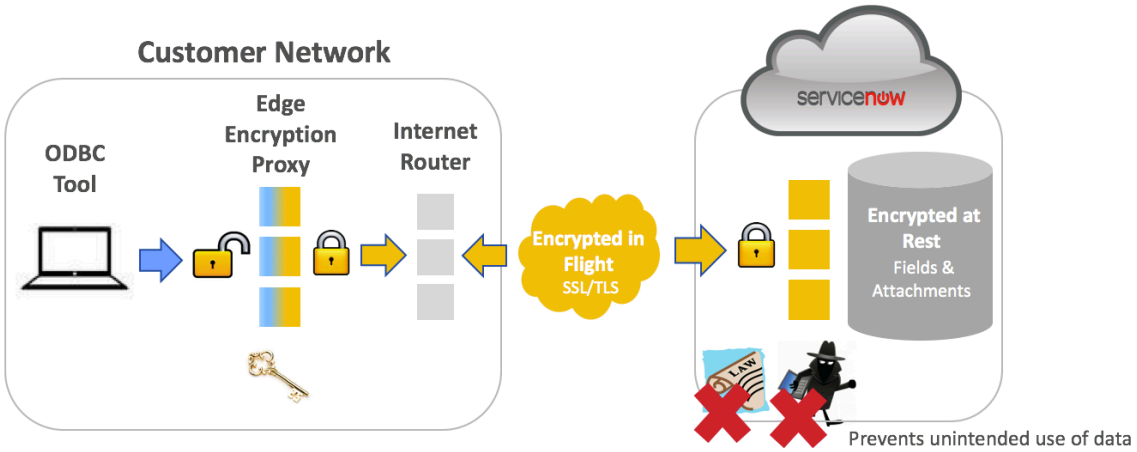
기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

에지 암호화 규칙 **ODBC** 드라이버 통합

로 암호화된 에지 암호화 규칙데이터를 쿼리하도록 ODBC 드라이버를 구성합니다. 에지 암호화 규칙 프록시 서버는 ODBC 드라이버와 통합될 때 에지 암호화 규칙 인스턴스에 대한 ServiceNow ODBC 드라이버 요청을 암호화합니다.

인스턴스의 암호화된 응답은 네트워크의 ODBC 드라이버로 전달되기 전에 프록시 서버를 통해 에지 암호화 규칙 해독됩니다.



통합에 성공하려면 ODBC 드라이버가 프록시 서버 인증서를 신뢰 에지 암호화 규칙 해야 합니다. 에지 암호화 규칙 ODBC 드라이버 에지 암호화 규칙 에서 신뢰하는 인증 기관에서 프록시 서버 인증서에 서명하면 프록시 서버가 자동으로 신뢰됩니다. 그러나 ODBC 드라이버에서 신뢰하는 인증 기관이 프록시 서버 인증서에 에지 암호화 규칙 서명하지 않은 경우 자체 서명된 인증서를 ODBC 신뢰 저장소로 가져와야 합니다.

자체 서명된 인증서를 **ODBC** 신뢰 저장소로 임포트

ODBC 드라이버에서 신뢰하는 인증 기관이 프록시 서버 인증서에 에지 암호화 규칙 서명하지 않은 경우 자체 서명된 인증서를 ODBC 신뢰 저장소로 가져와야 합니다. 프록시 서버에서 인증서를 에지 암호화 규칙 내보내고 ODBC 신뢰 저장소로 가져올 수 있습니다.

시작하기 전에
필요한 역할: 관리자

ODBC 드라이버에서 신뢰하는 인증 기관이 프록시 서버 인증서에 에지 암호화 규칙 서명했는지 여부를 확인하려면 프록시 홈 디렉토리의 키 저장소 디렉토리에서 다음 명령을 실행하여 ODBC 드라이버에서 신뢰하는 인증 기관 목록을 봅니다.

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts"
 -list
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

대부분의 경우 클라이언트는 부하 분산 장치를 통해 프록시에 연결 에지 암호화 규칙 되므로 인증서는 부하 분산 장치에 구성된 인증서가 됩니다.

클라이언트와 Edge 프록시 서버 사이에 부하 분산 장치가 없는 경우 인증서는 Edge 프록시에서 제공하는 인증서이며 파일에 구성됩니다 *edgeencryption.properties*.

```
edgeencryption.proxy.https.port = 9090
edgeencryption.proxy.https.keystore.path = keystore/keystore
edgeencryption.proxy.https.keystore.password = password
edgeencryption.proxy.https.cert.alias = jetty
```

속성 편집에 대한 자세한 내용은 Edge Encryption 속성 파일에서 추가 속성 구성을 참조하십시오.

프로시저

1. 프록시 홈 디렉토리의 키 저장소 디렉토리로 변경합니다.
2. 자체 서명된 인증서에 대한 키 저장소를 확인합니다.

   a. 인증서의 키 저장소를 확인하려면 다음 명령을 실행하여 키 저장소의 모든 항목을 나열할 수 있습니다.

   ```
   keytool -list -keystore keystore.jceks -storetype jceks -v
   ```

   b. 항목 목록에서 키 별칭을 찾습니다.

3. 키 별칭을 사용하여 인증서를 .cer 파일로 익스포트합니다.

   ```
   keytool -export -alias <key alias> -keystore keystore.jceks -storetype
    jceks -rfc -file <file name>.cer
   ```

4. ODBC 신뢰 저장소 디렉토리(`ODBC\ip\Java\jre\lib\security\cacerts`)로 변경합니다.
5. 인증서를 ODBC 신뢰 저장소로 가져옵니다.

   ```
   keytool -keystore cacerts -importcert -alias $<key alias> -file <file
    name>.cer
   ```

ODBC 드라이버 속성 설정

프록시 서버를 통해 에지 암호화 규칙 요청을 라우팅하도록 ODBC 드라이버 속성을 설정합니다.

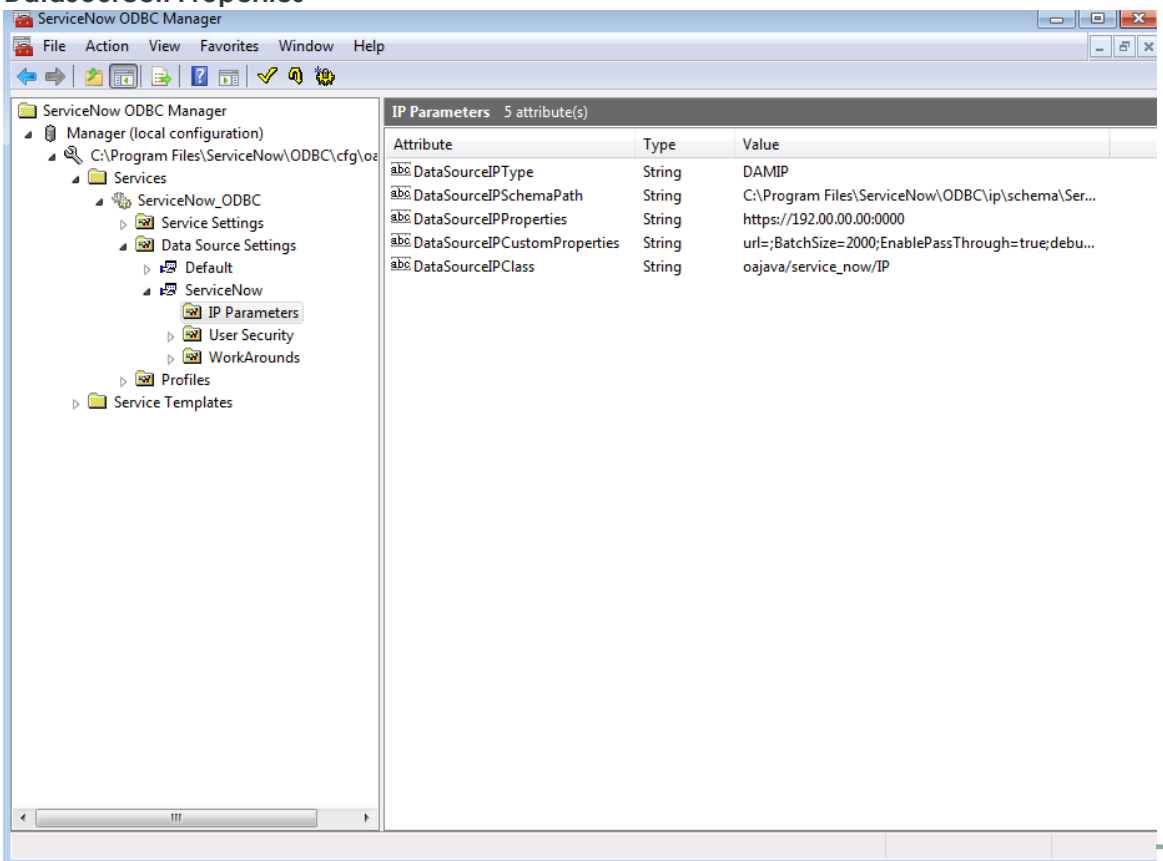
시작하기 전에
필요한 역할: 관리자

프로시저

1. Windows에서 시작 > 프로그램 > **ServiceNow ODBC** 관리 콘솔.
2. 콘솔 트리의 루트를 `ServiceNow ODBC Manager\Manager\<installation location>\Services\ServiceNow_ODBC\Data Source Settings\ServiceNow\IP Parameters`로 확장합니다.
3. **DataSourceIPProperties** 특성을 두 번 클릭합니다.
4. 값을 에지 암호화 규칙 프록시 서버의 URL(예: `https://<IP ##>:<port>`)로 변경합니다>

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

DataSourceIPProperties



5. 확인을 클릭합니다.

다음에 수행할 작업

이제 ODBC 드라이버가 프록시 서버를 통해 에지 암호화 규칙 인스턴스로 요청을 라우팅하도록 구성되었습니다.

에지 암호화 규칙 **MID** 서버 통합

MID 서버 프록시 서버를 통해 데이터를 라우팅하도록 에지 암호화 규칙 구성합니다.

와 에지 암호화 규칙 통합MID 서버되면 프록시 서버는 의 엔드포인트 역할을 MID 서버합니다. 에지 암호화 규칙 그런 다음 ServiceNow 프록시 서버는 인스턴스와 .MID 서버

MID Server와 통합 시 제한 사항

데이터가 프록시 서버를 통과 에지 암호화 규칙 하도록 구성된 경우 MID 서버 다음 제한 사항이 적용됩니다.

- ECC 큐 필드의 암호화는 지원되지 않습니다.
- 암호화된 데이터는 또는 서비스 매핑와 함께 디스커버리 사용할 수 없습니다.

MID 서버가 에지 암호화 규칙 프록시 서버를 가리키도록 합니다.

프록시 서버를 통해 데이터를 전달하려면 프록시 에지 암호화 규칙MID 서버 서버를 가리키도록 구성 파일을 업데이트합니다MID 서버.MID 서버에지 암호화 규칙

시작하기 전에

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

프록시 MID 서버 서버를 통과 에지 암호화 규칙 하도록 구성할 때 구성 파일의 웹 프록시 속성을 MID 서버 사용하여 프록시 서버를 통해 에지 암호화 규칙 인스턴스로 트래픽을 라우팅할 수 없습니다. 대신 프록시 서버를 의 엔드포인트로 MID 서버설정해야 에지 암호화 규칙 합니다.

프로시저

1. 로컬 MID 서버 디렉터리로 이동하여 `config.xml` 파일을 엽니다.
2. `<parameter name="url" value="https://YOUR_INSTANCE.service-now.com" />` 요소를 찾아 value 속성을 프록시 서버의 URL 에지 암호화 규칙 로 변경합니다.
   예: `http://hostname.mycompany.com:8081`
   이 단계에서는 트래픽을 에지 암호화 규칙 인스턴스 대신 프록시 서버로 전달하도록 지시 MID 서버 합니다. 에지 암호화 규칙 그런 다음 프록시 서버는 필요한 필드를 암호화하고 페이로드를 인스턴스에 전달합니다.
3. 파일을 저장하고 닫습니다.
4. 실행 중인 MID 서버경우 .

Edge Encryption 진단 및 성능

프록시 서버 성능 추세를 모니터링하고 에지 암호화 규칙 프록시 서버에서 생성된 오류를 드릴다운합니다 에지 암호화 규칙 .

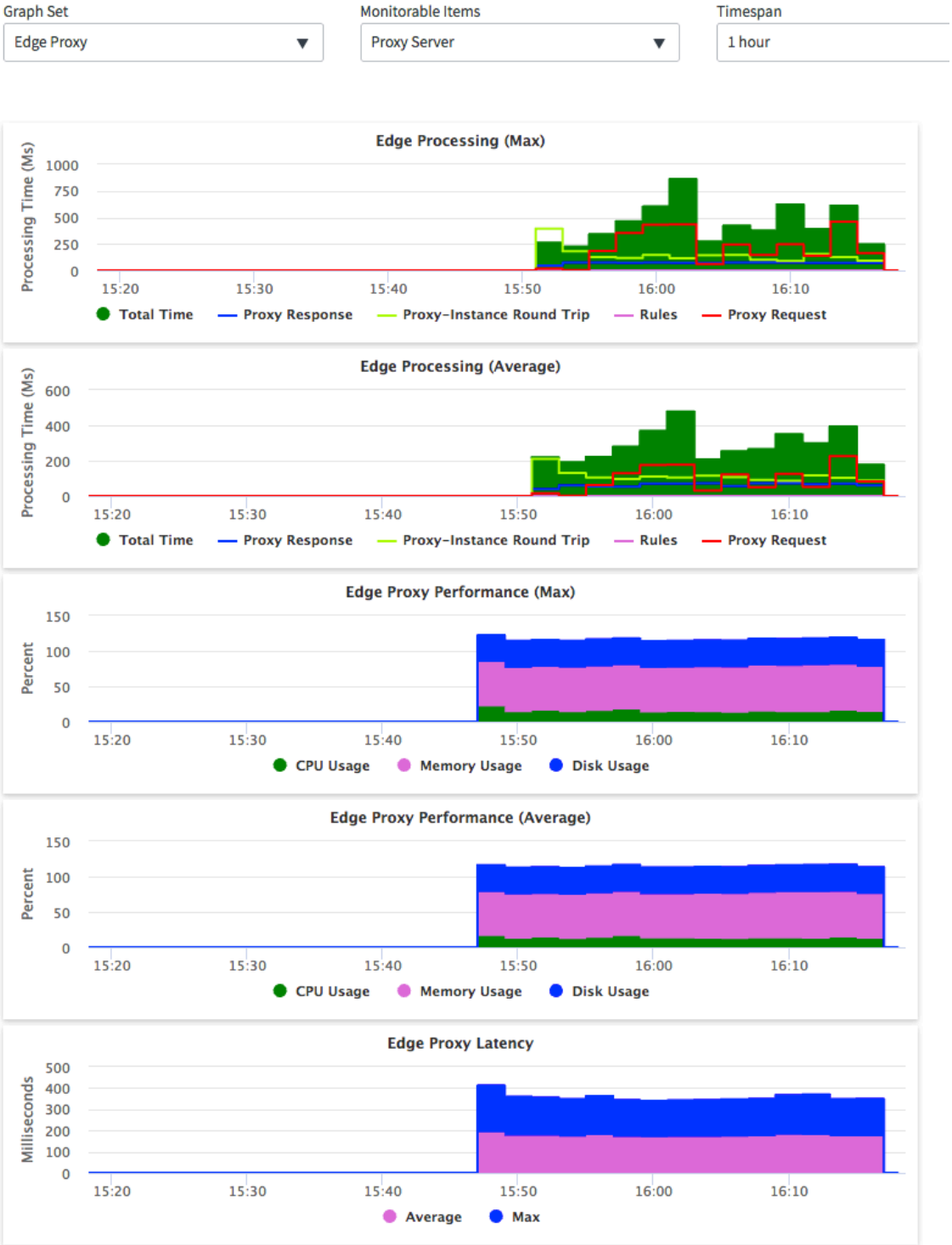
에지 프록시 성능

성능 홈페이지에 설정된 에지 프록시 그래프를 사용하여 주요 에지 암호화 규칙 프록시 서버 성능 추세를 ServiceNow 봅니다. 모니터링되는 추세는 다음과 같습니다.

- 클라이언트, 프록시 서버, 인스턴스 간의 최대 및 평균 응답시간입니다.
- 호스트 컴퓨터의 CPU, 디스크 공간 및 메모리 사용량입니다.
- 프록시 서버와 ServiceNow 인스턴스 간의 최대 및 평균 네트워크 대기 시간입니다.

주: 에지 암호화 규칙 이름이 중복된 프록시 서버는 성능 추세를 보고하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



에지 처리(최대값 및 평균)

요청을 처리하는 데 걸리는 최대 및 평균 시간(밀리초)입니다. 이러한 데이터 요소는 시간 경과에 따른 일반적인 추세입니다.

- 총 시간: 프록시 서버가 클라이언트로부터 요청을 수신하고 응답을 보내는 시간입니다. 이 데이터 요소는 후속 데이터 요소의 합계입니다.
- 프록시 응답: 프록시 서버가 인스턴스의 응답을 처리하는 데 소요되는 시간입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 프록시-인스턴스 왕복: 프록시 서버가 인스턴스에 요청을 보내고 응답을 받는 시간입니다. 프록시 서버와 인스턴스 간의 네트워크 대기 시간 및 인스턴스가 요청을 처리하는 데 소요된 시간을 포함합니다.
- 규칙: 프록시 서버가 정의된 암호화 규칙을 사용하여 요청을 평가하는 시간입니다.
- 프록시 요청: 프록시 서버가 클라이언트 요청을 처리하고 인스턴스로 전달하는 데 소요되는 시간입니다.

에지 프록시 성능(최대 및 평균)

호스트 머신에서 사용된 자원의 최대 및 평균 백분율입니다.

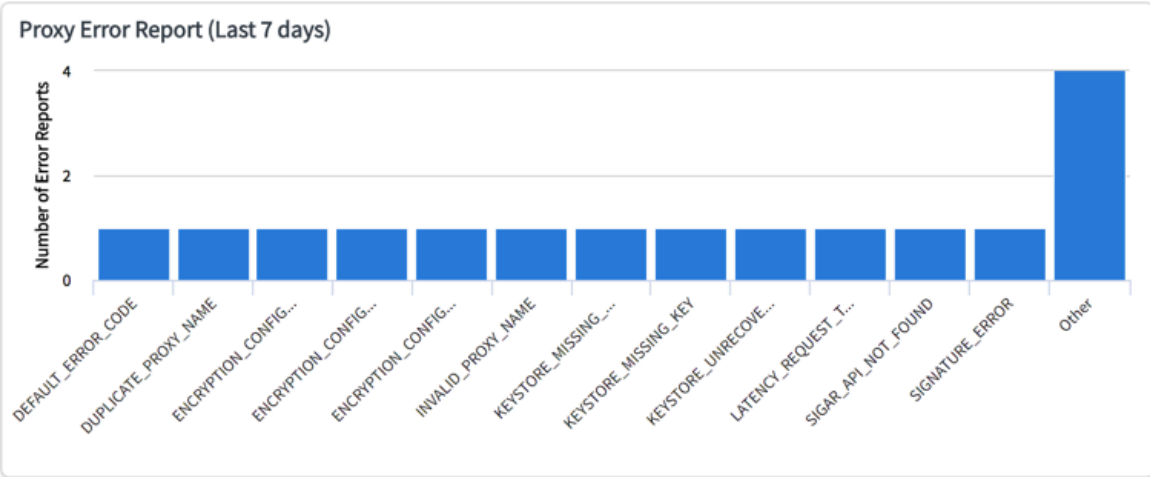
- CPU 사용량
- 메모리 사용량
- 디스크 사용량

에지 프록시 대기 시간

지정된 시점의 최대 및 평균 네트워크 대기 시간(밀리초)입니다. 대기 시간은 프록시 서버가 인스턴스에 간단한 ping을 보내고 응답을 받는 왕복 시간에 의해 결정됩니다.

프록시 오류 보고서

다음으로 이동 에지 암호화 규칙 구성 > 진단 및 문제 해결 > 프록시 오류 보고서 지난 7일 동안 수집된 모든 프록시 서버 오류를 봅니다.



오류는 1분 동안 수집됩니다. 1분마다 오류 보고서가 생성됩니다. 세로 축에는 각 오류를 포함하여 지난 7일 동안의 오류 보고서 수가 표시됩니다. 예를 들어 DEFAULT_ERROR_CODE 오류가 1분 보고서 기간 동안 여러 번 throw되더라도 DEFAULT_ERROR_CODE 막대는 오류 보고서 수 축의 1에만 도달합니다.

이 뷰에서 다음을 수행할 수 있습니다.

- 각 프록시 오류 코드 표시줄을 클릭하여 각 프록시 서버의 단일 오류에 대한 보고서를 봅니다. 이 뷰에서 막대를 다시 클릭하면 프록시 통계 테이블 〔edge_encryption_stat〕의 에지 암호화 규칙 오류 텍스트를 볼 수 있습니다. 오류 텍스트의 링크를 따라 이동하여 자세한 정보 및 가능한 정정 단계를 확인합니다.
- 기타를 클릭하여 오류 보고서의 2페이지를 봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 이름이 같은 프록시 서버가 두 개 이상 있는 경우 프록시 오류 보고서에 단일 DUPLICATE_PROXY_NAME 오류가 나타납니다. 이름이 중복된 프록시 서버에 대해서는 다른 오류가 보고되지 않습니다. 이 오류가 발생하면 모든 프록시 서버의 이름이 고유한지 확인합니다.

추가 모니터링 자원

인스턴스는 모든 암호화 프록시를 추적합니다. 각 에지 암호화 규칙 프록시 서버는 시작될 때 등록됩니다. 다음과 같은 경우 인스턴스에 알림이 전송됩니다.

- 새 에지 암호화 규칙 프록시 서버가 시작됩니다.
- 에지 암호화 규칙 프록시 서버가 의도적으로 종료되었습니다.

에지 암호화 규칙 프록시 서버가 설치되지 않은 에지 암호화 규칙 인스턴스에 등록하려고 하면 프록시가 시작되지 않습니다.

모든 암호화 구성 파일이 감사됩니다. 삭제된 기록은 모든 암호화 구성 파일에서 감사됩니다. 감사 기록은 sys_audit 테이블에 저장됩니다. 특정 구성 기록의 이력을 보려면 기록을 보고 이력 > 목록 메뉴에서. 대량 암호화 작업은 감사되지 않습니다.

다음 추가 자원을 사용하여 프록시 서버를 모니터링합니다.

테이블	설명
잘못된 삽입 시도 [sys_edge_encryption_invalid_insert_log]	암호화된 필드에 다음 데이터를 저장하려는 시도 목록입니다. • 암호화되지 않은 데이터입니다. • 프록시에서 에지 암호화 규칙 제공되지 않은 데이터입니다. 인스턴스는 이 데이터를 저장하려는 모든 시도를 거부하고 기록합니다. security-admin 역할이 있는 경우 잘못된 삽입 시도 목록에서 로그를 볼 수 있습니다.
작업 오류 [sys_encryption_job_execution]	성공적으로 실행되지 않은 작업의 목록입니다.
시스템 로그	인스턴스는 등록된 각 프록시 서버의 메시지를 주기적으로 확인합니다. 프록시 서버가 필요한 시간 내에 메시지를 보내지 않으면 오류가 기록됩니다. 로그 메시지에는 암호화 프록시에 대한 정보와 프록시가 인스턴스를 마지막으로 ping한 시간이 포함됩니다. 인스턴스가 온라인 상태인 암호화 프록시가 없음을 확인하면 메시지를 로깅합니다. 이러한 메시지는 시스템 로그에 추가됩니다.

에지 프록시 통계 수집 사용 안 함 또는 줄이기

프록시 서버가 에지 프록시 그래프 세트 통계를 성능 홈페이지로 ServiceNow 보내지 못하도록 하거나 에지 암호화 규칙 통계 수집 빈도를 줄입니다.

시작하기 전에

필요한 역할: admin 또는 security_admin

이 태스크 정보

`edgeencryption.properties` 구성 파일에 속성을 추가하여 다음을 수행할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Edge Proxy 그래프 세트를 비활성화합니다.
- 프록시 서버에서 통계를 수집하는 에지 암호화 규칙 간격을 변경합니다. 기본적으로 통계는 30초마다 수집됩니다.

프로시저

1. 프록시 서버 설치 디렉터리에서 `<installation ####>/conf/` 폴더에 있는 `edgeencryption.properties` 구성 파일을 엽니다.
2. 다음 에지 암호화 규칙 프록시 서버 속성중 하나를 추가합니다.
3. 프록시 서버를 다시 시작합니다.

프록시에 에지 암호화 규칙 대한 디버그 로깅 증가

로그를 해석하고 프록시로 문제를 디버깅하기 위한 로깅 수준을 높입니다.

현재 프록시에서 디버그 로깅을 에지 암호화 규칙 늘리기 위한 세 가지 옵션이 있습니다. 문제를 디버깅하기 위한 로깅 수준을 높이고, 보다 자세한 로그 문의 이점을 활용하여 문제를 조사하기 위한 정보를 기술 지원에 제공합니다.

디버깅 중인 문제에 따라 다음 세 가지 방법 중 하나로 디버그 로깅을 설정합니다.

- SSL 연결 이외의 문제 디버깅
- 프록시를 통한 요청에 대한 타이밍 메트릭 로깅
- 에지 암호화 프록시와 인스턴스 간의 SSL 연결 문제 디버깅

모든 디버그 케이스의 경우 직접 로그를 보고 해석하거나 인시던트를 열어 기술 지원에서 ServiceNow 문제에 대한 설명과 재현 방법을 제공하는 해석을 얻을 수 있습니다.

SSL 연결 이외의 애플리케이션 문제 에지 암호화 규칙 디버깅

이 메서드를 사용하여 프록시를 에지 암호화 규칙 중지한 후 다시 시작하지 않고 애플리케이션의 문제를 디버깅할 수 있습니다. 이러한 단계는 로깅 수준을 높이고 보다 자세한 로그 문을 통해 근본 원인 문제를 해결하는 데 도움이 됩니다.

시작하기 전에
필요한 역할: 관리자

> **주:** `$proxy_installation_location/conf/log4j2.properties` 파일에 대한 변경사항은 변경 후 약 60초 내에 프록시에 의해 채택됩니다. 프록시를 다시 시작할 필요가 없습니다.

프로시저

1. `$proxy_installation_location/conf/log4j2.properties` 파일에서 다음 행을 찾으십시오.

```
logger.edge.level=info
```

2. 위의 줄을 다음과 같이 변경합니다.

```
logger.edge.level=debug
```

3. 변경 내용을 저장합니다.
변경 내용을 적용하는 데 최대 60초가 걸릴 수 있지만 프록시를 다시 시작할 필요는 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 문제를 재현합니다.
5. `$proxy_installation_location/logs/edgeencryption.log` 파일에서 애플리케이션과 관련된 디버그 로그 문을 확인합니다.

결과
속성을 변경한 후 `$proxy_installation_location/logs/edgeencryption.log` 파일에서 추가 상세 정보를 볼 수 있습니다. 디버깅을 완료하면 `$proxy_installation_location/conf/log4j2.properties` 파일에 대한 변경사항을 되돌립니다.

프록시를 통한 요청에 대한 타이밍 메트릭 로깅

타이밍 메트릭 로깅을 활성화하여 프록시에서 처리 에지 암호화 규칙 한 각 요청에 대한 메트릭 설명을 추가합니다. 이러한 각 타이밍 메트릭 로그 문에는 처리 시간 및 사용된 암호화 규칙과 같은 요청에 대한 유용한 정보가 포함되어 있습니다.

시작하기 전에
필요한 역할: 관리자

주:

추가 로깅 설정이 `$proxy_installation_location/conf/log4j2.properties` 파일에 추가됩니다. 변경 사항은 파일이 변경된 후 약 1분 이내에 프록시에 의해 동적으로 적용되므로 프록시를 다시 시작할 필요가 없습니다.

프로시저

1. 파일 끝에 다음 행을 추가하여 `$proxy_installation_location/conf/log4j2.properties` 파일을 수정합니다

```
appender.timinglog.type=RollingFile
appender.timinglog.name=TimingLog
appender.timinglog.fileName=../logs/edgenetwork.log
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.EdgeEncryptionTimingM
etricCache
logger.timing.level=debug
logger.timing.additivity=false
logger.timing.appenderRef.rolling.ref=TimingLog
```

2. 파일을 저장합니다.

결과
`log4j.properties` 파일이 저장된 후 네트워크 시간에 대해 다음 유형의 메시지가 `$proxy_installation_location/logs/edgenetwork.log` 로그 파일에 나타납니다.

```
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=1658433375
754 request_method=POST client_request_received="2022-07-21 12:56:15,015"
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
 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=:y5HGsTTqo
3Pjq6G0xk4LoazCwCiWRJk4/6SpbXuBzqg=:6816f79cc0a8016401c5a33be04be441
 jsessionid_suffix=037A66
```

로그 메시지의 값은 다음과 같습니다.

```
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

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
```

프록시와 인스턴스 간의 에지 암호화 규칙 SSL 연결 문제 디버깅

이 방법을 사용하여 프록시를 통한 인스턴스 액세스 실패 등의 프록시와 인스턴스 간의 에지 암호화 규칙 SSL 연결 문제를 디버깅할 수 있습니다. 이러한 단계는 로깅을 늘리고 자세한 로그 문을 찾는 데 도움이 됩니다.

시작하기 전에
필요한 역할: 관리자

주: SSL 연결 디버깅은 TLS 연결 유형 문제를 해결할 때만 관련이 있습니다. 실제로 이것은 일반적이지 않으며 거의 필요하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 프록시 서버를 중지합니다.
2. Java 시작 속성인 `$proxy_installation_location/conf/wrapper.conf` 파일에 다음 행을 추가하십시오.

```
wrapper.java.additional.<next available number in sequence> =
 -Djavax.net.debug=all
```

예:

```
For example: wrapper.java.additional.4 = -Djavax.net.debug=all
```

3. 변경 내용을 저장하고 프록시 서버를 다시 시작합니다.
4. 연결 문제를 재현합니다.

결과
문제를 재현한 후 SSL 교환과 관련된 디버그 로그 문은 `$proxy_installation_location/logs/wrapper_<current date>.log` 파일에서 찾을 수 있습니다. 디버깅이 완료되면 이전 단계에서 만든 줄을 제거하거나 주석 처리하여 추가 로깅을 원격으로 수행할 수 있습니다.

데이터베이스 암호화

ServiceNow® 는 모든 데이터에 대해 미사용 데이터 보호가 필요할 수 있는 데이터 보호에 대한 법적 의무가 있는 고객을 위해 데이터베이스 암호화(DBE) 및 전체 디스크 암호화 방법을 제공합니다.

중요사항: 릴리스부터 Washington DC 데이터베이스 암호화는 향후 사용 중단을 준비 중입니다. 클라우드 암호화는 저장 데이터 암호화를 대체하는 솔루션입니다. 자세한 내용은 다음을 참조하십시오. 클라우드 암호화 키 관리 포함

탐색	요청	참조
		
데이터베이스 암호화의 주요 기능 및 비즈니스 가치에 대해 알아봅니다.	데이터베이스 키 회전을 요청하는 방법에 대해 자세히 알아보세요.	DBE-CCS(고객 제어 스위치를 사용한 데이터베이스 암호화)는 데이터베이스에서 사용하지 않을 때 모든 저장 데이터를 암호화하는 암호화 솔루션입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

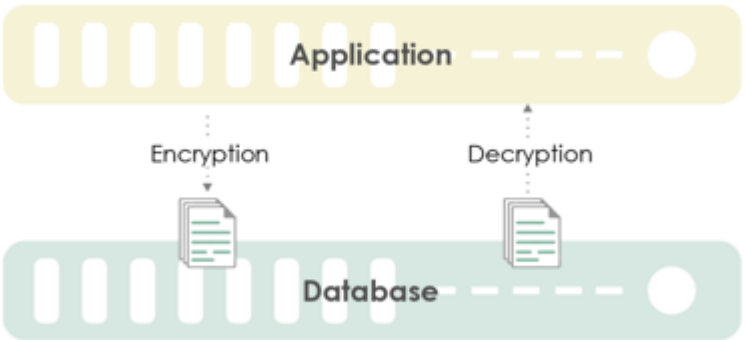
데이터베이스 암호화 탐색

ServiceNow® 는 모든 데이터에 대해 미사용 데이터 보호가 필요할 수 있는 데이터 보호에 대한 법적 의무가 있는 고객을 위해 데이터베이스 암호화(DBE) 및 전체 디스크 암호화 방법을 제공합니다.

중요사항: 릴리스부터 Washington DC 데이터베이스 암호화는 향후 사용 중단을 준비 중입니다. 클라우드 암호화는 저장 데이터 암호화를 대체하는 솔루션입니다. 자세한 내용은 다음을 참조하십시오. 클라우드 암호화 키 관리 포함

데이터베이스 암호화를 사용하면 데이터베이스가 온라인이든 오프라인이든 관계없이 대칭 AES-256 암호화로 모든 데이터를 보호할 수 있습니다. Now Platform 관점에서 모든 데이터 흐름은 해독됩니다.

- 데이터베이스 암호화는 저장된 모든 데이터를 실시간으로 암호화하여 기능 손실 없이 온라인 및 오프라인 데이터를 보호할 수 있도록 지원합니다.
- 전체 디스크 암호화는 디스크 손실 또는 도난이 있는 경우 오프라인 데이터를 보호합니다.

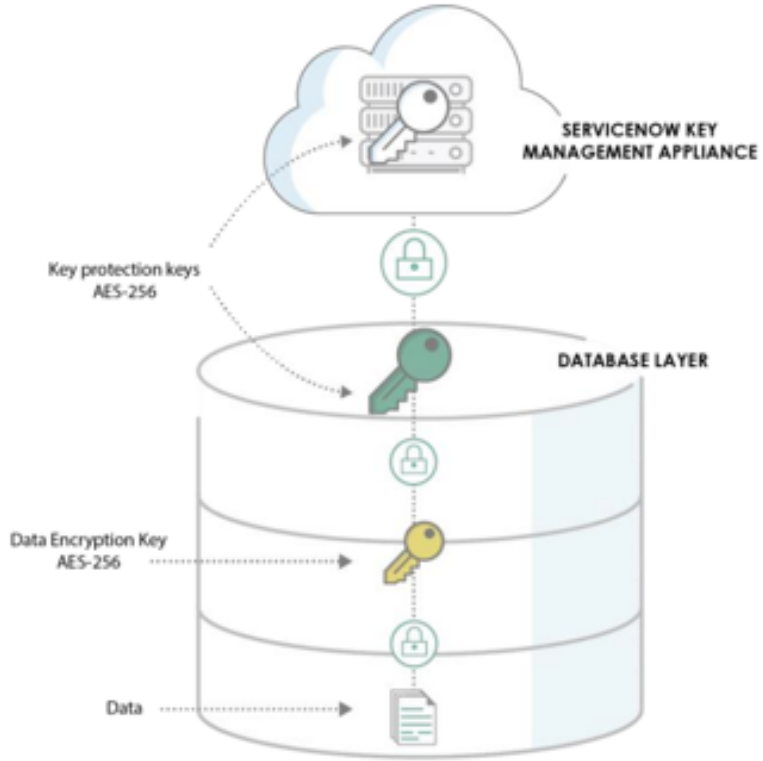


데이터베이스 암호화를 사용하면 저장된 모든 데이터가 암호화되고 개별 기록 또는 테이블이 액세스하는 동안 메모리에서 해독됩니다. 새 데이터 또는 변경된 데이터는 테이블에 입력될 때 암호화되며 관련 활동 로그 파일(bin, 다시 실행, 실행 취소 및 오류)도 암호화됩니다.

데이터베이스 암호화는 기능 손실 없이 사용자에게 투명합니다. 이 기능을 사용하면 복제 트래픽 및 백업과 함께 모든 인스턴스가 암호화됩니다. 인스턴스 클론은 최대 5%의 데이터베이스 암호화 사용 시 성능에 약간의 영향을 주지만 계속 사용할 수 있습니다. 지원되는 릴리스 Now Platform 의 새 인스턴스와 기존 인스턴스 모두 데이터베이스 암호화를 이용할 수 있습니다.

그림과 ServiceNow 같이 3단계 키 계층 구조를 사용하여 키를 저장하고 관리합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



1. 고객별 AES-256 키는 데이터베이스 엔진에 의해 생성되며 데이터를 암호화하는 데 사용됩니다.
2. 두 번째 고객별 AES-256 키는 데이터베이스 엔진에 의해 생성되며 첫 번째 수준 키를 보호하는 데 사용됩니다.
3. 세 번째 AES-256 키는 데이터 센터의 FIPS 140 유효성이 검사된 키 관리 어플라이언스 ServiceNow에 의해 생성되고 저장됩니다. 이 키는 두 번째 수준 키를 보호하며 고객 인스턴스마다 고유합니다.

또한 Now Platform 고객 제공 스위치인 DBE와 CCS를 사용한 데이터베이스 암호화도 지원합니다. 데이터베이스에서 사용하지 않을 때 모든 저장 데이터를 암호화하는 암호화 솔루션입니다. 기능에는 영향을 주지 않고 산업 표준 AES 암호화를 사용합니다. 데이터베이스는 디스크에 기록될 때 데이터를 암호화하고 디스크에서 읽을 때 데이터를 해독합니다. 즉, 애플리케이션에는 영향을 주지 않고 필요한 논리와 기능을 수행할 수 있도록 항상 암호화되지 않은 상태의 데이터가 있습니다.

주: 데이터베이스 암호화는 온프레미스 인스턴스에 대해 지원되지 않습니다.

데이터베이스 암호화에 고유한 키를 사용하는 경우 을 참조하십시오 고객 통제 스위치를 사용한 데이터베이스 암호화.

데이터베이스 키 회전 요청

데이터베이스 키를 매년 또는 필요에 따라 지원 요청을 제출하여 회전합니다.

시작하기 전에
필요한 역할: 관리자

중요사항: 릴리스부터 Washington DC 데이터베이스 암호화는 향후 사용 중단을 준비 중입니다. 클라우드 암호화는 저장 데이터 암호화를 대체하는 솔루션입니다. 자세한 내용은 다음을 참조하십시오. 클라우드 암호화 키 관리 포함

이 태스크 정보
키 회전은 만료 날짜 이전 24시간 이내에 야간에 발생하며 인스턴스에 대한 서비스를 중단하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 현재 키 순환은 상업용, GCC(정부 커뮤니티 클라우드), 프랑스 및 싱가포르 환경에서만 사용할 수 ServiceNow 있습니다.

프로시저

다음 키 교대 작업을 요청하려면 연락처 고객 서비스 및 지원 로 문의하십시오.

- 지정된 모든 인스턴스에서 연간 키 교대를 수행하려면 등록하십시오.
- 다음 정보가 포함된 마지막 세 가지 키 교대에 대한 이력 보고서를 얻습니다.
  - 인스턴스 이름입니다.
  - 키 이름 및 버전
  - 교대 날짜 및 시간입니다.
- 연간 예정된 교대 이외의 조기 키 교대를 예약합니다.

고객 통제 스위치를 사용한 데이터베이스 암호화

DBE-CCS(고객 제어 스위치를 사용한 데이터베이스 암호화)는 데이터베이스에서 사용하지 않을 때 모든 저장 데이터를 암호화하는 암호화 솔루션입니다.

개요

고객 통제 스위치를 사용하는 데이터베이스 암호화는 기능에 영향을 주지 않고 업계 표준 AES 암호화를 사용합니다. 데이터베이스는 디스크에 기록되고 디스크에서 읽을 때 데이터베이스에서 암호를 해독할 때 데이터를 암호화합니다. 애플리케이션에는 필요한 논리와 기능을 수행하기 위해 항상 암호화되지 않은 상태의 데이터가 있습니다.

DBE-CCS는 테이블스페이스 암호화 또는 투명한 데이터 암호화라고도 하는 데이터베이스 고유의 기술을 활용합니다. 이 기술에 대한 자세한 내용은 MariaDB 웹 사이트의 "테이블스페이스 암호화"를 참조하십시오.

DBE-CCS를 사용하려면 인스턴스에 주기적으로 비밀 키를 제공하는 HTTPS REST 서비스 엔드포인트를 설정해야 합니다 ServiceNow . 그런 다음 CCS 엔드포인트는 데이터베이스 인스턴스의 공개 키로 암호화된 고객 비밀 키를 반환합니다.

고객 엔드포인트

중요사항: CCS 엔드포인트를 설정하고 유지 관리할 책임은 전적으로 조직에 있습니다. 고객 엔드포인트 사양은 KB0789788 로 제공됩니다.

ServiceNow 기술 파트너인 Fortanix를 통해 고객 엔드포인트를 자동으로 구현할 수 있습니다. 통합에 대한 자세한 내용은 기술 파트너에게 직접 문의하십시오. 자세한 내용은 ServiceNow에서 Fortanix Data Security Manager 사용을 참조하십시오.

여러 **ServiceNow** 버전 지원

중요사항: 데이터베이스 암호화는 릴리스에 구애받지 않는 유료 인프라 오퍼링입니다. 지원되는 모든 릴리스와 새 인스턴스 또는 기존 인스턴스에 적용할 수 있습니다.

기타 참조

DBE와 CCS에 대한 자세한 내용은 다음 참조를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

참조	설명
KB0993681	데이터베이스 암호화 아키텍처 고객 제어 스위치
KB0789788	DBE와 CCS의 구현 가이드

주: KB 문서에 액세스하려면 먼저 에 인증 Now Support해야 합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 관리

접근 관리를 사용하면 인스턴스에 안전하게 접근할 ServiceNow® 수 있습니다.

제로 트러스트 액세스



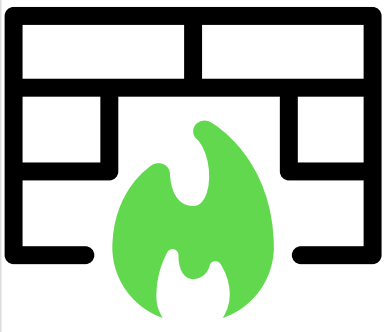
제로 트러스트 액세스는 애플리케이션 및 데이터에 대한 모든 액세스 권한이 사용자의 ID 확인 및 위험 평가 후에만 최소 권한을 기반으로 부여되도록 합니다.

도메인 분리



ServiceNow 플랫폼을 통해 서비스 제공자(SP)는 고객에게 보다 빠른 온보딩을 제공하고, 규정 준수를 충족하며, 도메인 분리를 사용하여 데이터를 보호할 수 있습니다.

인증



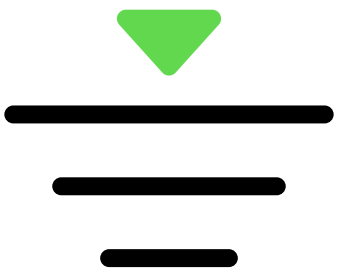
ServiceNow의 인증은 인스턴스에 액세스하는 사용자의 ID를 확인한 다음, 사용자에게 사용자의 역할 또는 직무 기능과 일치하는 기능을 사용할 수 있는 권한을 부여합니다.

ACL



접근 제어 목록(ACL)에 대한 규칙은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 액세스를 제한합니다.

데이터 필터링



데이터 필터링을 사용하여 읽기 쿼리를 수행할 때 제목 속성을 기반으로 테이블 및 기록에 대한 액세스를 제어합니다.

보안 역할



보안 역할은 추가 보안을 제공하며, 인스턴스가 내부 및 외부 사용자를 구분할 수 있도록 모든 사용자에게 하나 이상의 역할이 있어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연결 및 자격 증명



디스커버리, 서비스 매핑 및 클라우드 관리를 위해 컴퓨터나 네트워크 장치에 접근 권한을 획득하거나 오케스트레이션을 사용하여 작업을 수행하려면 자격 증명과 연결 정보가 필요합니다.

ServiceNow 접근 제어



SNC 접근 제어 플러그인을 사용하면 인스턴스에 액세스할 수 있는 고객 서비스 및 지원 직원과 시기를 제어할 수 있습니다.

제로 트러스트 액세스

ZTA(제로 트러스트 액세스)는 기본적으로 사용자 또는 디바이스를 신뢰할 수 없다고 가정하는 보안 모델입니다.

탐색



활성화



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제로 트러스트 액세스의 기능과 비즈니스 가치에 대해 알아봅니다.

제로 트러스트 액세스를 활성화하는 방법을 이해합니다.

구성



제로 트러스트 액세스를 구성합니다.

참조 - 속성



제로 트러스트 액세스의 속성에 대해 알아봅니다.

제로 트러스트 액세스 탐색

ZTA(제로 트러스트 액세스)는 기본적으로 사용자 또는 디바이스를 신뢰할 수 없다고 가정하는 보안 모델입니다.

ZTA는 사용자의 신원 확인 및 위험 평가 후에만 애플리케이션 및 데이터에 대한 모든 액세스 권한이 최소 권한 기준으로 부여되도록 합니다.

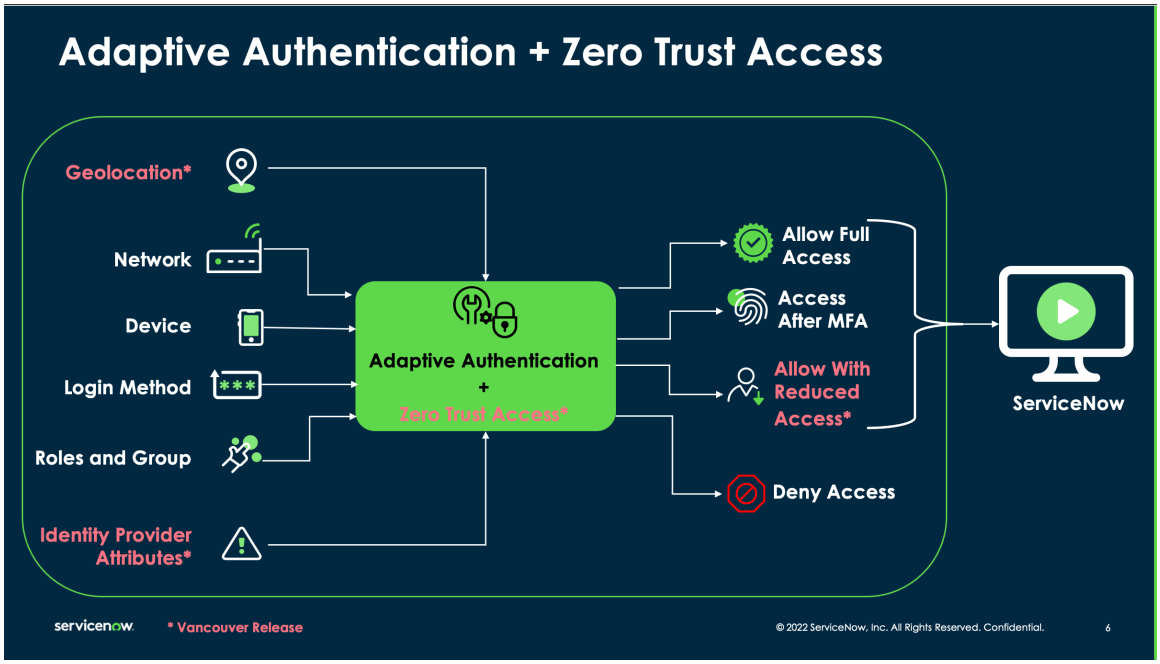
제로 트러스트 - 정책 기반 세션 액세스

ServiceNow 제로 트러스트 - 정책 기반 세션 액세스(세션 액세스)를 사용하면 조직이 IP 주소, 위치, 인증 방법, 사용자의 역할, 그룹, MFA를 가진 사용자 및 ID 제공자(IDP)가 공유하는 속성 등 다양한 요소를 기반으로 웹 세션에서 사용자 권한을 동적으로 줄일 수 있습니다. 이렇게 하면 권한이 높은 사용자가 신뢰할 수 없는 장치 또는 위치에서 애플리케이션에 액세스하는 경우에도 무단 액세스 및 데이터 침해로부터 조직을 보호할 수 있습니다.

제로 트러스트 - 정책 기반 세션 액세스

보안 관리자는 적응형 인증 정책을 사용하여 IP 주소, 위치, ID 제공자 속성 및 사용자 속성을 기반으로 세션에서 사용자 액세스를 줄이거나 제한할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:

- 세션 액세스 구성은 `security_admin` 역할로만 수행할 수 있습니다. 역할을 `security_admin`로 승격해야 합니다.
- 세션 액세스는 통합을 지원하지 않습니다.
- 축소되거나 제한된 역할이 사용자에게 할당되지 않은 경우 세션 액세스는 영향을 주지 않습니다. 이 경우 로그인한 세션은 변경되지 않습니다. 사용자는 할당된 권한으로 인스턴스에 계속 접근합니다.
- 사용자가 인스턴스에 이미 로그인되어 있고 동시에 관리자가 정책을 구성하는 동안에는 세션 액세스에 영향을 주지 않습니다. 정책이 적용되려면 사용자가 세션에서 로그아웃해야 합니다.
- 사용자가 신뢰할 수 있는 네트워크에 있고 나중에 세션 내에서 VPN(위치 또는 네트워크 변경)으로 전환할 때 세션 액세스는 영향을 주지 않습니다.
- 세션 액세스는 로그인 시 적용됩니다. 세션 중에 위험 매개변수가 변경되어도 액세스가 줄어들지 않습니다. 예를 들어 세션을 설정한 후 사용자가 회사 네트워크에서 신뢰할 수 없는 네트워크로 전환하면 로그아웃했다가 다시 로그인하지 않는 한 액세스가 줄어들지 않습니다.
- 세션 액세스(제로 트러스트 액세스 - ZTA) 기능, `snc_internal` 및 `snc_external` 와 같은 역할은 제거할 수 없습니다.
- 세션 액세스(제로 트러스트 액세스 - ZTA) 기능은 `sys_user_has_role` 또는 사용자 그룹 구성원 자격 테이블에서 역할을 제거하지 않습니다. ZTA 정책에 따라 축소되거나 제한된 역할로 사용자 세션을 설정합니다.
- 시스템 컨텍스트에서 실행되는 스크립트는 ZTA 세션 역할을 따르지 않습니다.

사용 케이스

다음은 제로 트러스트 액세스의 몇 가지 사용 사례입니다.

- 세션과 관련된 위험에 따라 권한을 줄입니다. 예를 들어 신뢰할 수 있는 네트워크 외부에서 로깅하는 이행자 역할 사용자는 세션에 대한 요청자 역할만 갖도록 구성할 수 있습니다.
- 사용자가 신뢰할 수 없는 장치를 사용하는 경우 사용자 세션에 대한 IDP 응답에 따라 액세스를 줄입니다. 자세한 내용은 세션 접근에 대한 IDP 속성 구성 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 역할 강등은 사용자가 세션에서 다른 기존 권한을 갖지 않도록 합니다. 사용자가 신뢰할 수 있는 네트워크에서 로그인하면 모든 기존 권한이 세션에 할당됩니다.

정책의 일부로 여러 IP 조건과 여러 역할 또는 그룹 할당을 정의할 수 있습니다.

제로 트러스트 액세스 - 모바일

적응형 인증 정책 내에서 제로 트러스트 액세스 - 세션 액세스 정책을 사용하여 모바일에서 특정 세션의 역할이나 권한을 줄일 수 있습니다.

제로 트러스트 액세스 - 세션 액세스 모바일은 시스템 속성 테이블에서 **glide.authenticate.session_access.mobile.enabled** 를 활성화하여 활성화할 수 있습니다.

IDP 속성으로 제로 트러스트 액세스 - 세션 액세스 모바일을 사용하려면 **glide.authenticate.session_access.mobile.refresh_token_interval** 필드를 구성할 수 있습니다. 이렇게 하면 관리자가 새로 고침 토큰을 기반으로 세션 액세스를 효과적으로 제어할 수 있습니다.

자세한 내용은 모바일용 제로 트러스트 액세스 구성 문서를 참조하십시오.

제로 트러스트 액세스 활성화

제로 트러스트 - 정책 기반 세션 액세스 `com.snc.zero_trust_session_access` 정책을 활성화하여 보안 관리자가 적응형 인증 정책을 사용하여 IP 주소, 위치, ID 제공자 속성 및 사용자 속성을 기반으로 세션에서 사용자 액세스를 줄이거나 제한할 수 있도록 합니다.

시작하기 전에
필요한 역할: 관리자

플러그인 유형: 유료이며 라이센스가 필요합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준과 검색 창을 사용하여 **Zero Trust - Policy Based Session Access** (`com.snc.zero_trust_session_access`) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

세션 액세스 역할 구성

적응형 인증 정책을 사용하여 IP, 위치, ID 제공자 속성 및 사용자 속성을 기반으로 세션에서 사용자 액세스를 줄이도록 세션 액세스를 구성합니다.

시작하기 전에
필요한 역할: security_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 세션 액세스 구성은 `security_admin` 역할로만 수행할 수 있습니다. 역할을 `security_admin`로 승격해야 합니다.
- 세션 액세스는 통합을 지원하지 않습니다.
- 축소되거나 제한된 역할이 사용자에게 할당되지 않은 경우 세션 액세스는 영향을 주지 않습니다. 이 경우 로그인한 세션은 변경되지 않습니다. 사용자는 할당된 권한으로 인스턴스에 계속 액세스할 수 있습니다.
- 사용자가 인스턴스에 이미 로그인되어 있고 동시에 관리자가 정책을 구성하는 동안에는 세션 액세스에 영향을 주지 않습니다. 정책이 적용되려면 사용자가 세션에서 로그아웃해야 합니다.
- 세션 액세스는 로그인 시 적용됩니다. 세션 중에 위험 매개변수가 변경되어도 액세스가 줄어들지 않습니다. 예를 들어 세션을 설정한 후 사용자가 회사 네트워크에서 신뢰할 수 없는 네트워크로 전환하는 경우 사용자가 로그아웃했다가 다시 로그인하지 않는 한 액세스가 줄어들지 않습니다.
- 세션 액세스(제로 트러스트 액세스 - ZTA) 기능, `snc_internal` 및 `snc_external` 와 같은 역할은 제거할 수 없습니다.
- 세션 액세스(제로 트러스트 액세스 - ZTA) 기능은 `sys_user_has_role` 또는 사용자 그룹 구성원 자격 테이블에서 역할을 제거하지 않습니다. ZTA 정책에 따라 축소되거나 제한된 역할로 사용자 세션을 설정합니다.
- 시스템 컨텍스트에서 실행되는 스크립트는 ZTA 세션 역할을 따르지 않습니다.

프로시저

1. 다음으로 이동 모두 > 제로 트러스트 액세스 > 세션 접근 역할 구성.
2. 세션 액세스 역할 구성을 만들려면 새로 만들기를 선택합니다.
3. 양식에서 필드에 다음을 입력합니다.

세션 접근 역할 구성

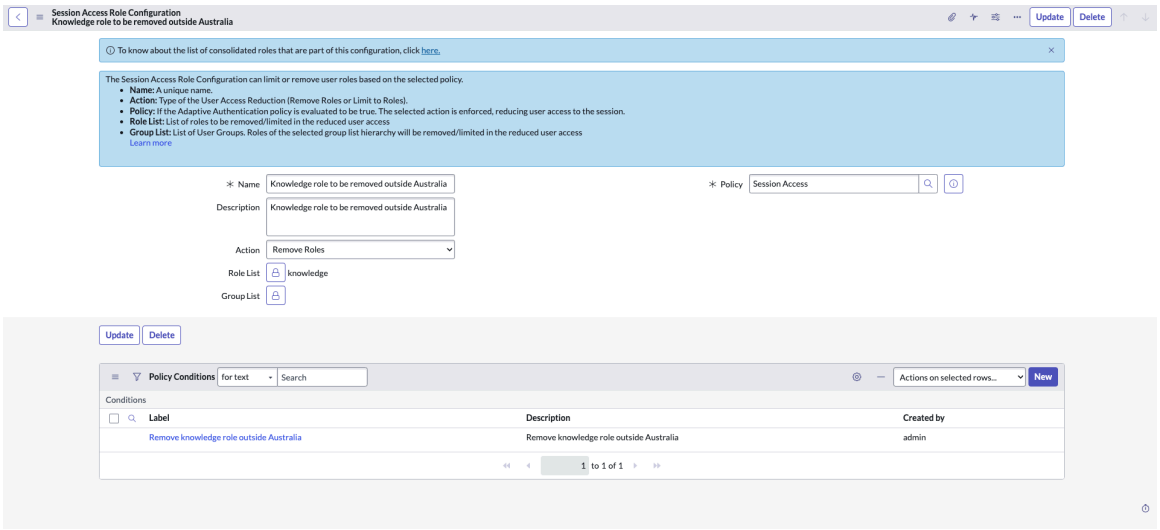
필드	설명
이름	구성의 이름
설명	구성에 대한 간단한 설명입니다.
정책	적응형 인증 정책을 선택합니다. 조회 아이콘을 사용하여 정책 목록을 봅니다.
동작	역할을 제거하거나역할로 제한합니다. ◦ 역할 제거: 구성된 사용자가 로그인하면 세션에 대해 역할 또는 그룹 목록에 제공된 역할 목록이 제거됩니다. ◦ 역할로 제한: 구성된 사용자가 로그인하면 선택한 역할만 사용자에게 제공되고 세션에 대한 다른 모든 역할은 제거됩니다.
역할 목록	역할 목록에서 역할을 선택합니다.
그룹 목록	그룹 목록에서 제거하거나 사용자로 제한할 역할을 선택합니다.

4. 선택, 제출.

구성된 국가를 기반으로 하는 사용자의 로그인은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 역할 제거에서 선택한 역할이 있는 구성된 국가의 사용자는 더 이상 세션에 대한 역할을 갖지 않습니다.
- 역할 제한에서 선택한 역할이 있는 구성된 국가의 사용자는 세션에 대한 역할만 갖습니다.

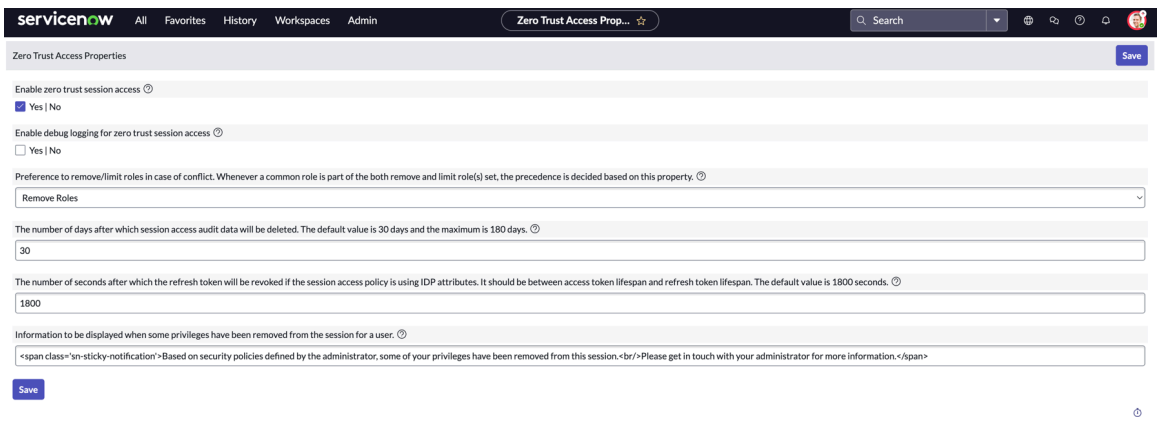


샘플 사용 사례와 함께 설명된 세션에 대한 역할을 제거하거나 제한하는 방법에 대한 자세한 내용은 문서를 참조하십시오 자습서: 제로 트러스트 액세스 사용.

제로 트러스트 액세스 시스템 속성

시스템 속성을 사용하여 보안 요구 사항에 맞게 제로 트러스트 액세스를 활성화하고 사용자 지정합니다.

속성



제로 트러스트 액세스 시스템 속성

속성	설명
제로 트러스트 세션 액세스 사용	관리자가 제로 트러스트 세션 액세스 기능을 사용할 수 있도록 하는 옵션입니다. 기본적으로 이 값은 `false`입니다.
제로 트러스트 세션 액세스에 대한 디버그 로깅 사용	제로 트러스트 세션 액세스에 대한 디버그 로깅을 활성화하는 옵션입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제로 트러스트 액세스 시스템 속성

속성	설명
상충이 발생한 경우 역할을 제거/제한하는 기본 설정입니다. 공통 역할이 제거 및 제한 역할 세트의 일부일 때마다 우선순위는 이 속성에 따라 결정됩니다.	역할 제거 또는 역할 제한
세션 액세스 감사 데이터가 삭제된 후의 일 수입니다. 기본값은 30일이고 최대값은 180일입니다.	기본적으로 30일입니다.
세션 액세스 정책이 침입 탐지 및 방지(IDP) 속성을 사용하는 경우 새로 고침 토큰이 해지되기까지의 시간(초)입니다. 액세스 토큰 수명과 새로 고침 토큰 수명 사이에 있어야 합니다. 기본값은 1800초입니다.	기본적으로 1800초입니다.
사용자에 대한 세션에서 일부 권한이 제거된 경우 표시되는 정보입니다.	권한 제한 또는 제거와 관련하여 사용자에게 표시할 설명입니다. 샘플 설명: `#### ### ## ### ## # #### ## ### #######. ### ### ##### ######.`

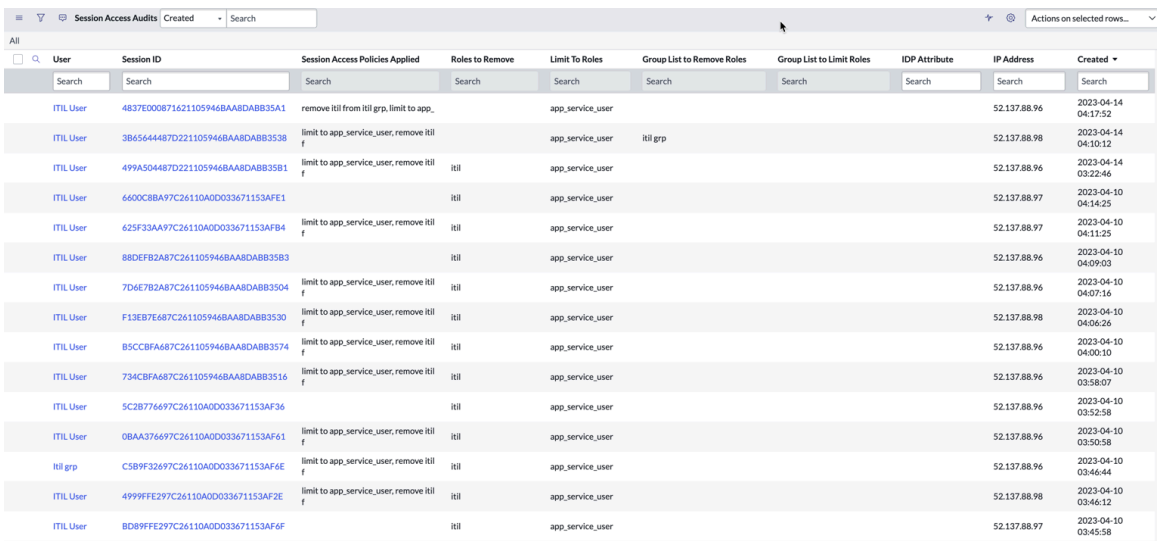
세션 접근 감사

세션 액세스 감사는 사용자의 세션과 관련된 세션 액세스 로그 및 정보를 표시합니다.

감사

세션 액세스 감사에는 다음과 같은 감사 정보가 표시됩니다.

주: `glide.authenticate.session_access.log_audit_event` 속성을 사용하여 감사 정보를 채웁니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세션 접근 감사

필드	설명
사용자	사용자의 상세 정보입니다.
세션 ID	고유 ID로 표시되는 세션에 대한 상세 정보입니다.
모바일 클라이언트	모바일 클라이언트 상세 정보입니다. **ServiceNow** 에이전트 (Now Agent) 및 **ServiceNow Request** (Now Mobile)
세션 접근 정책 적용됨	적용되는 세션 액세스 정책입니다.
제거할 역할	로깅하는 동안 사용자로부터 제거된 역할입니다.
역할에 대한 제한	로깅하는 동안 사용자로 제한된 역할입니다.
역할을 제거할 그룹 목록	사용자의 역할을 제거한 그룹에 대한 정보입니다.
역할을 제한할 그룹 목록	사용자에 대해 제한된 역할을 가진 그룹에 대한 정보입니다.
모바일 클라이언트	모바일을 통해 로그인했으며 접근 권한이 제한되거나 제거된 사용자의 상세 정보입니다.
IDP 속성	해당 세션에 사용된 IDP입니다.
IP 주소	사용자가 로그인하는 데 사용하는 IP 주소의 상세 정보입니다.
작성됨	생성된 사용자 기록의 날짜 및 시간에 대한 상세 정보입니다.

자습서: 제로 트러스트 액세스 사용

엔드 투 엔드 사용 사례에서 제로 트러스트 액세스 기능을 사용하는 절차입니다.

시작하기 전에
필요한 역할: security_admin

세션 접근 사용 속성을 활성화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 세션 액세스 구성은 `security_admin` 역할로만 수행할 수 있습니다. 역할을 `security_admin`로 승격해야 합니다.
- 세션 액세스는 통합을 지원하지 않습니다.
- 축소되거나 제한된 역할이 사용자에게 할당되지 않은 경우 세션 액세스는 영향을 주지 않습니다. 이 경우 로그인한 세션은 변경되지 않습니다. 사용자는 할당된 권한으로 인스턴스에 계속 액세스할 수 있습니다.
- 사용자가 인스턴스에 이미 로그인되어 있고 동시에 관리자가 정책을 구성하는 동안에는 세션 액세스에 영향을 주지 않습니다. 정책이 적용되려면 사용자가 세션에서 로그아웃해야 합니다.
- 세션 액세스는 로그인 시 적용됩니다. 세션 중에 위험 매개변수가 변경되어도 액세스가 줄어들지 않습니다. 예를 들어 세션을 설정한 후 사용자가 회사 네트워크에서 신뢰할 수 없는 네트워크로 전환하는 경우 사용자가 로그아웃했다가 다시 로그인하지 않는 한 액세스가 줄어들지 않습니다.
- 세션 액세스(제로 트러스트 액세스 - ZTA) 기능, `snc_internal` 및 `snc_external` 와 같은 역할은 제거할 수 없습니다.
- 세션 액세스(제로 트러스트 액세스 - ZTA) 기능은 `sys_user_has_role` 또는 사용자 그룹 구성원 자격 테이블에서 역할을 제거하지 않습니다. ZTA 정책에 따라 축소되거나 제한된 역할로 사용자 세션을 설정합니다.
- 시스템 컨텍스트에서 실행되는 스크립트는 ZTA 세션 역할을 따르지 않습니다.

세션 액세스는 사용자가 신뢰할 수 없는 네트워크에서 로그인, 다른 장치에서 로그인 등 다양한 환경에서 인스턴스에 로그인하려고 할 때 관리자가 사용자에 대한 역할 집합을 동적으로 줄이거나 제한할 수 있도록 하는 기능입니다.

세션 액세스는 구성을 수행할 때 생성된 정책과 선택한 작업으로 제어할 수 있습니다. 일부 시나리오는 다음과 같습니다.

- 정책이 true이고 역할 작업이 역할 제거로 설정된 경우 인스턴스에 로그인하려고 할 때 선택한 역할 및 연결된 하위 역할이 사용자에 대해 제거됩니다.
- 정책이 true이고 역할 작업이 역할로 제한으로 설정되어 있으면 인스턴스에 로그인하려고 할 때 선택한 역할 및 연결된 하위 역할만 사용자에게 할당됩니다.

다음 절차에서는 인스턴스에 로그인하는 사용자로 역할이 제한되는 세션 액세스 구성의 엔드 투 엔드 구성을 설명합니다. 마찬가지로 구성 중에 역할 제거 옵션을 선택하여 역할을 제거할 수도 있습니다.

프로시저

1. 다음으로 이동 모두 > 세션 접근 > 세션 접근 역할 구성.
2. 세션 액세스 역할 구성 페이지에서 새로 만들기를 선택합니다.
3. 사용자의 역할을 제한하려면 양식에서 다음 필드를 채웁니다.
   - 이름
   - 설명
   - 정책
   - 동작
   - 역할 목록
   - 그룹 목록

   a. [**Limit To Roles]** 를 선택하여 사용자의 역할을 제한합니다.
   예: **itil**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

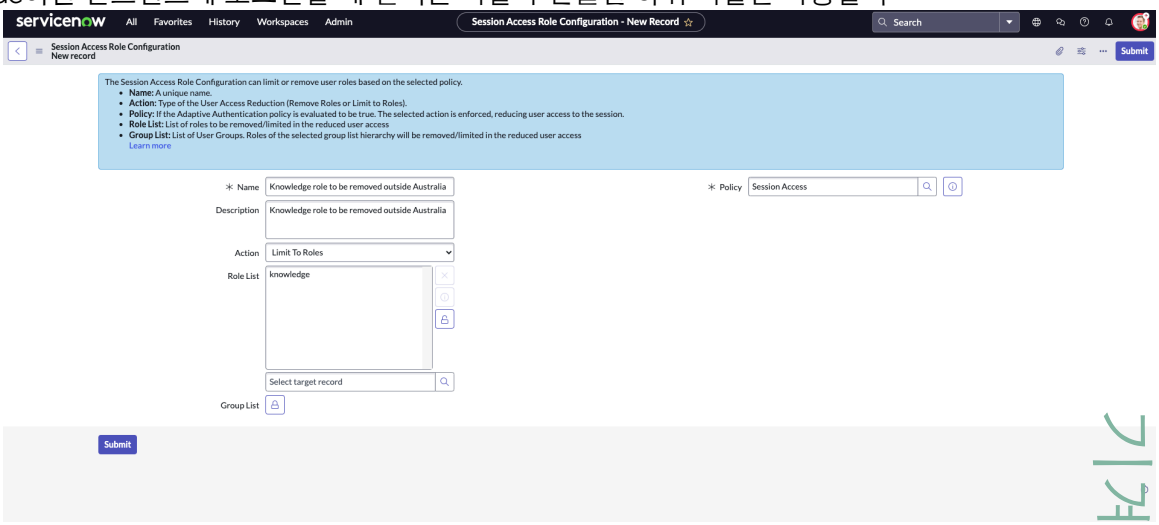
b. 역할 목록에서 **Knowledge** 역할을 선택합니다.

c. 정책을 선택합니다.

정책 입력 및 조건과 함께 인증 정책 및 필터 기준(역할, 그룹, IP, 위치)을 사용하여 세션 액세스 정책을 만들 수 있습니다.

세션 액세스 구성에서 정책을 사용합니다. 예를 들어, 역할(지식)을 위치(호주) 외부에서 로그인하는 사용자로 제한하려고 합니다.

d. 작업을 역할에 대한 제한으로 선택합니다.
정책이 true이면 인스턴스에 로그인할 때 선택한 역할과 연결된 하위 역할만 사용할 수 있습니다.

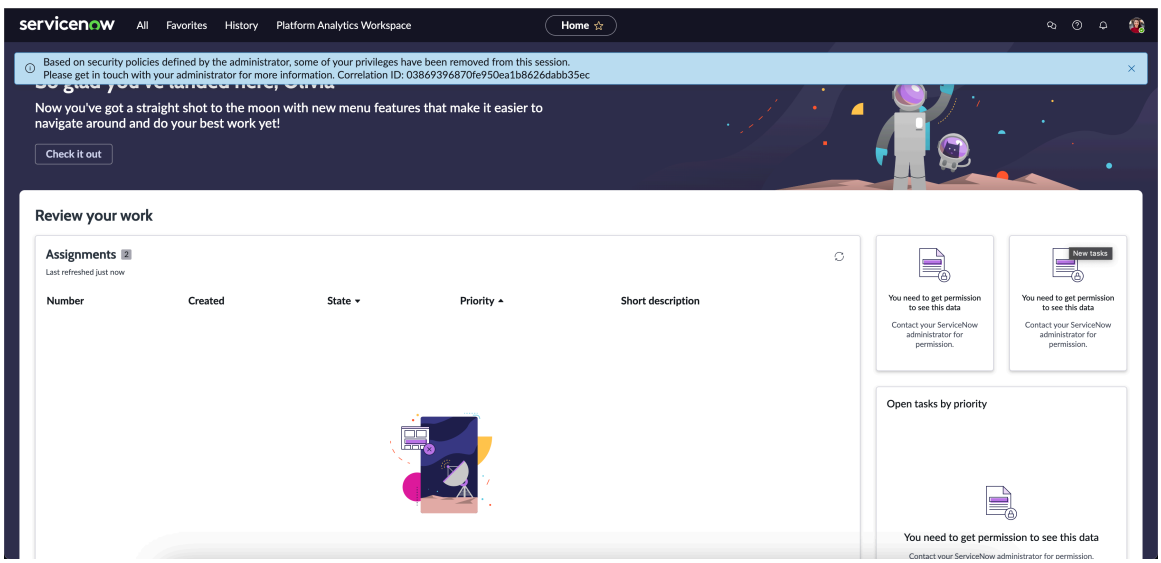


e. 제출을 선택합니다.

마찬가지로 그룹 목록에서 그룹을 선택하여 그룹 내의 사용자에 대한 역할을 제한하거나 제거할 수 있습니다.

사용자가 호주 외부의 인스턴스에 로그인하면 기록된 세션에 **Knowledge** 역할 및 관련 하위 역할만 할당되고 사용자에 대한 다른 역할은 제한됩니다.

로그인하면 플랫폼의 프로필 섹션에 다음 오류 메시지와 함께 사용자가 표시됩니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자는 관리자에게 문의하고 조사를 위해 상관 관계 ID를 제공할 수 있습니다.

주: 상관 관계 ID는 세션 액세스 감사 테이블에 있는 해당 감사 기록의 sys_id입니다.

세션 접근에 대한 IDP 속성 구성

인스턴스에 대한 사용자 세션 액세스를 제거하거나 제한하기 위해 SAML(보안 어설션 마크업 언어) 응답에서 생성된 신원 확인 제공자(IDP) 속성을 사용합니다.

시작하기 전에

필요한 역할: security_admin

세션 접근 사용 속성을 활성화합니다.

주: 세션 액세스 역할 구성을 사용하려면 역할을 `security_admin`로 승격해야 합니다.

세션 액세스는 구성을 수행할 때 생성된 정책과 선택한 작업으로 제어할 수 있습니다. 일부 시나리오는 다음과 같습니다.

- 정책이 true이고 역할 작업이 IDP 속성 입력 및 조건과 함께 역할 제거 로 설정된 경우 인스턴스에 로그인하려고 할 때 선택한 역할 및 연결된 하위 역할이 사용자에 대해 제거됩니다.
- 정책이 true이고 역할 작업이 IDP 속성 입력 및 조건과 함께 역할로 제한 으로 설정된 경우, 인스턴스에 로그인을 시도할 때 선택한 역할 및 연결된 하위 역할만 사용자에게 할당됩니다.

다음 절차는 세션 액세스를 제어하기 위한 정책 입력인 SAML 응답에서 침입 탐지 및 방지(IDP) 속성을 구성하는 단계를 보여줍니다.

프로시저

1. 다음으로 이동 모두 > 세션 접근 > 세션 접근 역할 구성.
2. 세션 액세스 역할 구성 페이지에서 새로 만들기를 선택합니다.
3. 사용자의 역할을 제거하려면 양식에서 다음 필드를 채웁니다.
   - 이름
   - 설명
   - 정책
   - 동작
   - 역할 목록
   - 그룹 목록

   a. [**Remove Roles**]를 선택하여 사용자의 역할을 제거합니다.
   예: **itil**.

   b. 역할 목록에서 **itil** 역할을 선택합니다.

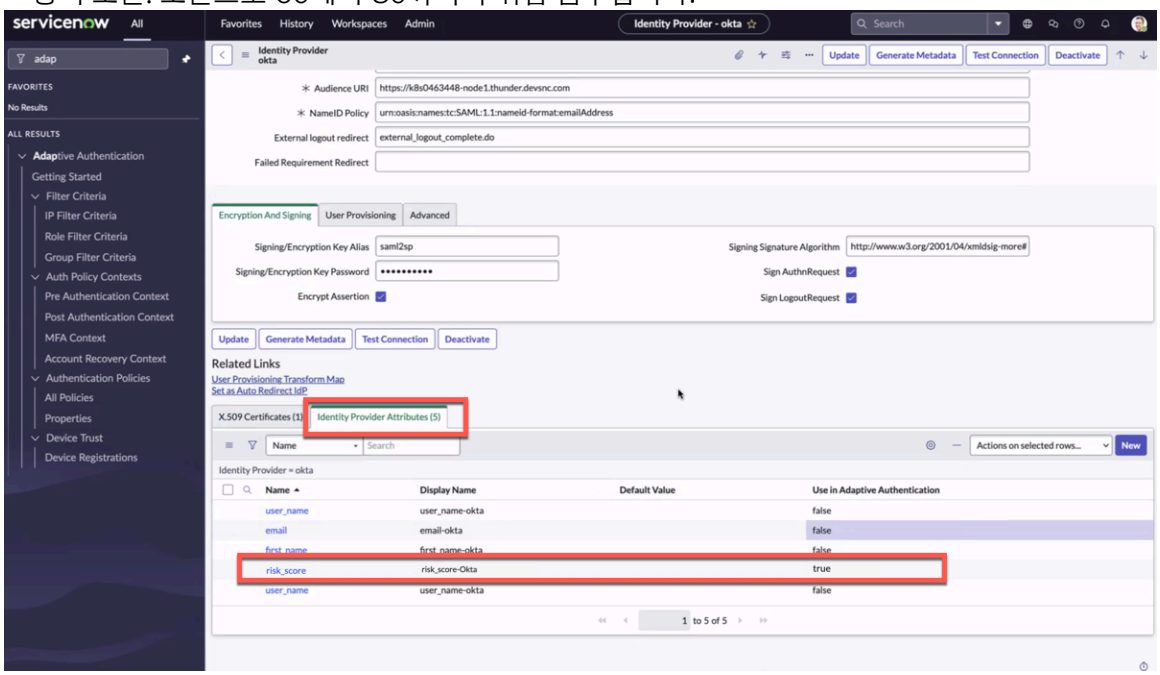
   c. 정책을 선택합니다.
   적응형 인증 정책 생성을 사용하여 다른 필터 기준을 사용하여 정책을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 필터 기준.

   d. 작업을 역할 제거로 선택합니다.
   정책이 true이고 역할 작업이 역할 제거로 설정된 경우 인스턴스에 로그인하려고 할 때 사용자에 대해 선택한 역할이 제거됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 정책 입력에서 정책 입력 및 정책 조건을 생성합니다.
예:

- 정책 입력: Okta의 위험 점수 속성(IDP).
- 정책 조건: 조건으로 60에서 80까지의 위험 점수입니다.



이 구성에 따라 Okta(IDP)의 위험 점수 속성 값이 80을 초과하면 사용자는 인스턴스에 제거된 역할(직원) 및 해당 하위 역할로 인증되지 않으며, 사용자는 할당된 다른 역할로만 인증됩니다. 위험 점수가 60에서 80 사이인 경우 사용자는 모든 역할과 함께 인스턴스에 인증됩니다.

정책 입력 및 조건을 사용하여 사후 인증 컨텍스트의 정책을 만드는 방법에 대한 자세한 내용은 문서를 참조하십시오 사후 인증 컨텍스트.

주: 세션 액세스 사용 속성이 비활성 상태인 경우 세션 액세스에 대한 구성은 사용자의 역할을 제한하거나 제거하지 않습니다.

f. 제출을 선택합니다.

모바일용 제로 트러스트 액세스

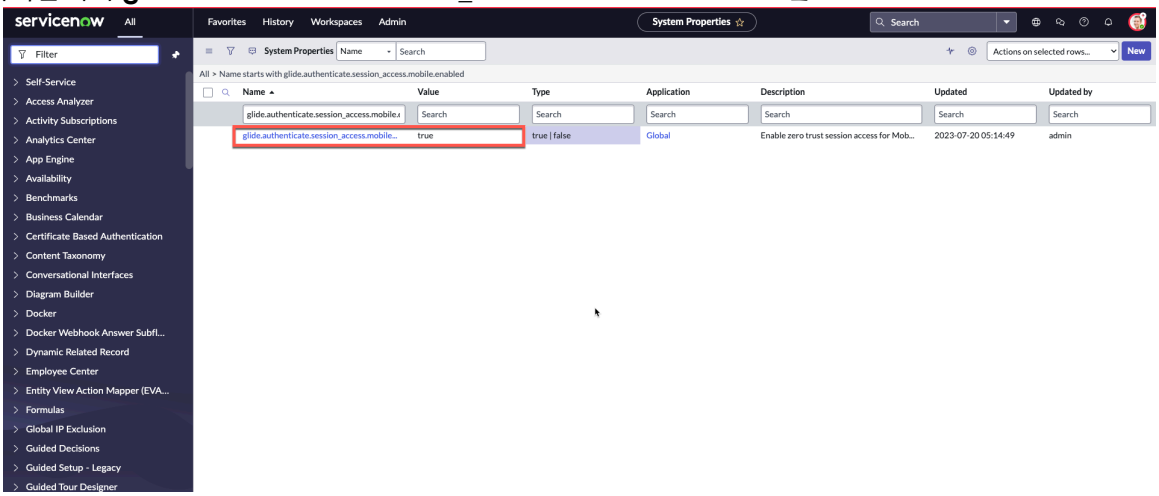
ZTA(제로 트러스트 액세스)는 기본적으로 사용자 또는 디바이스를 신뢰할 수 없다고 가정하는 보안 모델입니다.

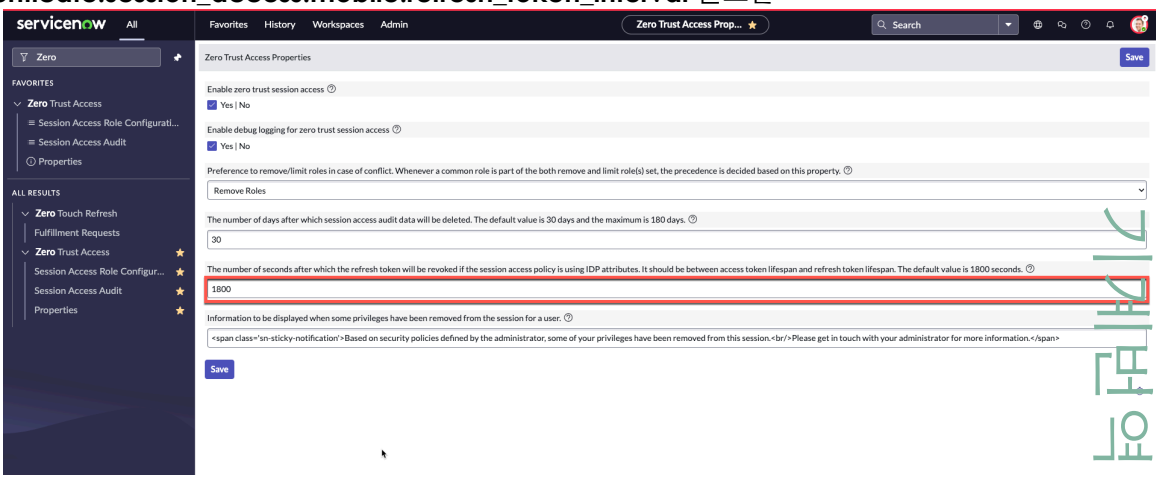
적응형 인증 정책 내에서 제로 트러스트 액세스 - 세션 액세스 정책을 사용하여 사용자를 위한 모바일에서 특정 세션의 역할이나 권한을 줄일 수 있습니다.

모바일에서 제로 트러스트 액세스를 활성화하려면 다음 작업을 수행해야 합니다.

- 세션 액세스 구성은 `security_admin` 역할로만 수행할 수 있습니다. 역할을 `security_admin`로 승격해야 합니다.
- 제로 트러스트 - 정책 기반 세션 액세스 `com.snc.zero_trust_session_access` 정책을 활성화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 시스템 속성 테이블에서 **glide.authenticate.session_access.mobile.enabled** 를 

활성화합니다.
- 새로 고침 토큰을 기반으로 모바일에서 세션 액세스를 제어하도록 **glide.authenticate.session_access.mobile.refresh_token_interval** 필드를 

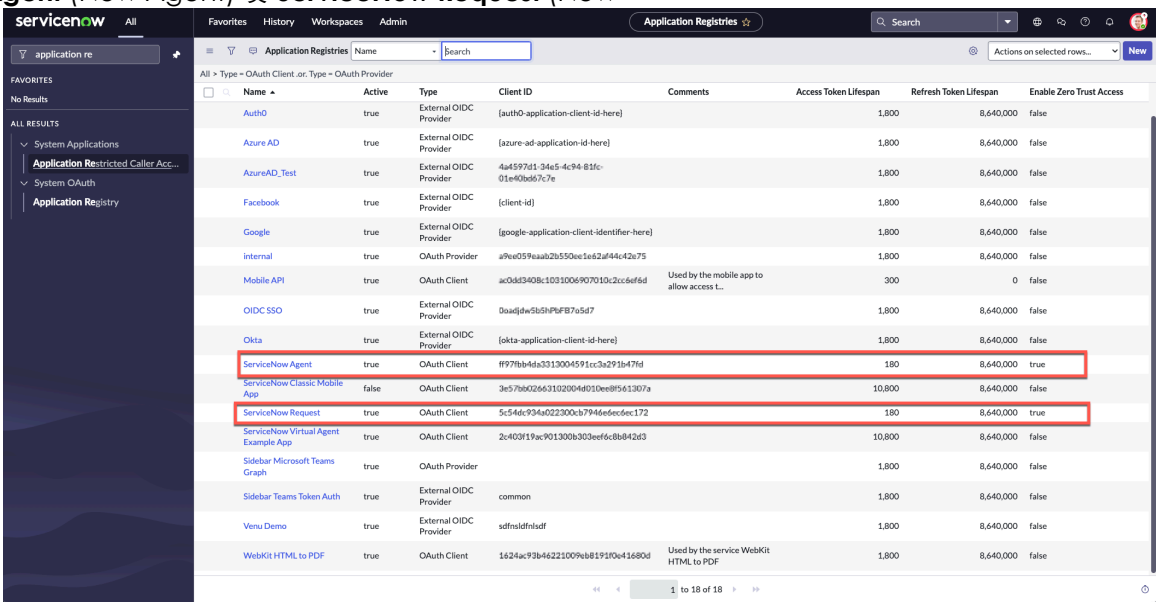
구성합니다.

> 주: 모바일 앱 로그인에 IDP를 사용할 때 새로 고침 토큰(초)을 구성해야 합니다. 기본적으로 사용자는 1,800초(30분) 후에 모바일 앱에서 로그아웃됩니다.

- 제로 트러스트 액세스 사용은 모바일 클라이언트 애플리케이션(OAuth 클라이언트)의 애플리케이션 레지스트리 에서 활성화됩니다. 이 경우에는

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow Agent (Now Agent) 및 **ServiceNow Request** (Now Mobile) 입니다.



- 정책 입력 및 조건에 따라 사용자 로깅에 대한 역할을 줄이거나 제거하도록 세션 접근 역할을 구성합니다. 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 세션 액세스 역할 구성.

구성은 로그인을 평가하여 정책 필터 및 조건에 따라 인스턴스에 액세스하는 ServiceNow® 사용자의 역할을 줄이거나 제거합니다. 자세한 내용은 모바일용 제로 트러스트 액세스 구성 문서를 참조하십시오.

연속 인증

ServiceNow의 연속 인증을 사용하면 사용자가 보호되는 자원에 액세스하는 경우 사용자를 다시 확인하고 인증할 수 있습니다.

기계번역

탐색



활성화

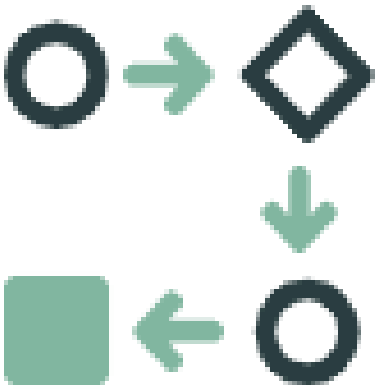


연속 인증의 기능 및 비즈니스 가치에 대해 알아봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연속 인증을 활성화하는 방법을 이해합니다.

구성



연속 인증을 구성합니다.

참조 - 속성



연속 인증의 속성에 대해 알아봅니다.

연속 인증 살펴보기

ServiceNow의 연속 인증(CA)을 사용하면 사용자가 보호되는 자원에 액세스하는 경우 사용자를 다시 확인하고 인증할 수 있습니다.

ServiceNow의 연속 인증은 초기 로그인뿐만 아니라 사용자의 전체 세션에서 사용자의 ID를 확인하도록 설계된 보안 메커니즘입니다. CA는 의 제로 트러스트 액세스 보안 아키텍처를 기반으로 ServiceNow구축되었으며, 이는 초기 인증 프로세스 후에도 사용자가 주장하는 정체성을 유지하도록 하여 보안을 강화하는 것을 목표로 합니다.

CA는 다음과 같은 제로 트러스트 액세스 원칙에 따라 작동합니다.

- 명시적으로 확인: 위치에 관계없이 네트워크 내의 사용자, 장치 또는 시스템에 대한 암시적 신뢰가 없습니다. 모든 사용자와 장치는 위치나 과거 액세스에 관계없이 명시적으로 인증되고 권한을 부여받아야 합니다.
- 최소 권한 액세스 사용: 특정 작업을 수행하는 데 필요한 최소 액세스 권한 또는 권한만 부여하고 손상된 계정 또는 시스템으로 인한 잠재적 손상을 제한합니다."
- 위반 가정: 예방에만 의존하는 대신 위반을 가정하고 사전 예방적 탐지, 억제 및 대응에 집중합니다.

CA는 사용자가 액세스하는 데이터와 수행 중인 활동에 따라 단계별 인증 또는 재인증을 적용하는 기능을 제공합니다. 테이블 또는 데이터 클래스 수준에서 보안 정책을 만들기 위해 관리자가 선택할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자가 PII(개인 식별 정보) 및 중요한 데이터에 액세스하려고 할 때마다 로그인한 세션 내에서 MFA(스텝업 인증) 또는 재인증(SSO - SAML 또는 OIDC)을 적용할 수 있습니다.

주: 라이선스가 필요한 CA 옵트(opting CA)를 위해 제로 트러스트 `-com.snc.zero_trust_continuous_authentication`(연속 인증)을 설치해야 합니다.

복지

다음은 CA를 사용할 때의 몇 가지 이점입니다.

- 향상된 보안: 시스템은 사용자의 ID를 지속적으로 확인함으로써 잠재적인 보안 위협을 보다 신속하게 감지하고 대응할 수 있습니다.
- 계정 탈취 위험 감소: 공격자가 사용자의 세션에 대한 액세스 권한을 얻더라도 지속적인 인증을 통해 기밀 데이터에 액세스하지 못하도록 방지할 수 있습니다.

사용 케이스

다음은 CA 사용에 대한 몇 가지 사용 사례입니다.

- 다른 정책을 사용하여 민감한 데이터에 대한 액세스를 허용하기 전에 재인증을 적용합니다.
- 다른 정책을 사용하여 주기적인 재인증 또는 단계별 인증을 적용합니다.
  - IdP의 MFA, IdP의 SSO를 포함할 수 있는 재인증을 사용합니다.
  - 의 MFA와 함께 ServiceNow스텝업 인증을 사용합니다.

CA의 역할

CA에는 다음과 같은 역할이 있습니다.

- CA 관리자(ca_admin): CA 정책을 만들고, 편집하고, 볼 수 있습니다. CA 속성을 구성하고 CA의 대시보드(메트릭)를 봅니다.
- 정책 관리자(ca_policy_admin): CA 정책을 생성, 편집 및 볼 수 있습니다.
- 감사자(ca_auditor): CA의 대시보드(메트릭)를 볼 수 있습니다. 그리고 CA의 정책과 로그.

CA를 구성하려면 역할을 **ca_admin** 로 상승시키고 정책 구성을 수행해야 합니다.

주: 이 3가지 역할은 모두 상승된 역할입니다.

CA의 모듈

다음은 CA 내의 다양한 모듈입니다.

- 정책: 생성된 다양한 연속 인증 정책을 봅니다.
- 메트릭: KPI 목적을 위한 연속 인증에 대한 다양한 메트릭을 보고 조직 내 CA 사용량을 이해합니다.
- 시스템 속성: 시스템 속성을 사용하여 제로 트러스트 액세스 보안 요구 사항을 충족하도록 연속 인증(CA)을 활성화하고 사용자 지정합니다.

관련 정보

정책

메트릭

시스템 속성

연속 인증을 위한 사전 작업

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 연속 인증 활성화
- 연속 인증 구성
- 높은 보증 연속 인증

정책

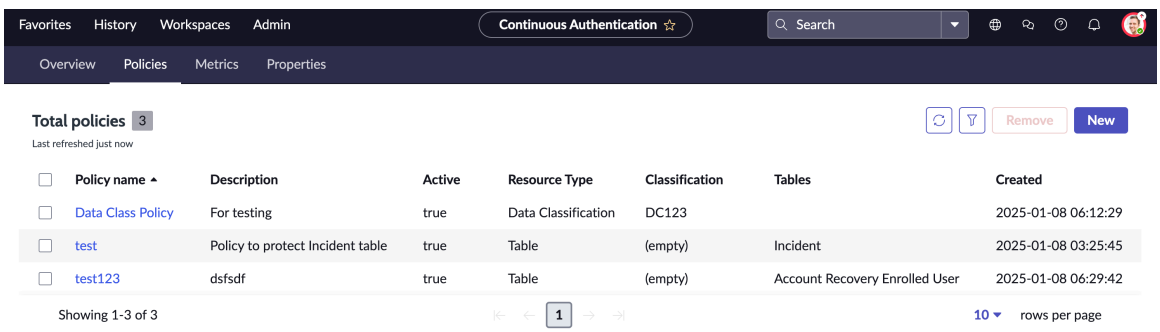
생성된 다양한 연속 인증 정책을 봅니다.

CA 정책 양식에는 테이블 또는 데이터 클래스에 대해 생성된 CA 정책의 상세 정보가 포함되어 있습니다. 사용자 지정 정책에서 정책 기록을 관리할 수 있습니다.

정책 페이지에 액세스하려면 다음으로 이동합니다. 모두 > 연속 인증에서 정책 탭을 선택합니다. 페이지에 표시되는 정책 세부 정보는 다음과 같습니다.

정책 페이지

필드	설명
보험 이름	정책 이름
설명	정책 설명
활성	정책 상태
자원 유형	정책에 사용되는 선택된 자원 유형
분류	정책에 대해 선택된 데이터 분류
테이블	정책에 대해 선택된 테이블
작성됨	정책 생성 상세 정보



관련 정보

- 메트릭
- 시스템 속성
- 연속 인증 살펴보기

메트릭

연속 인증에 대한 다양한 메트릭을 봅니다.

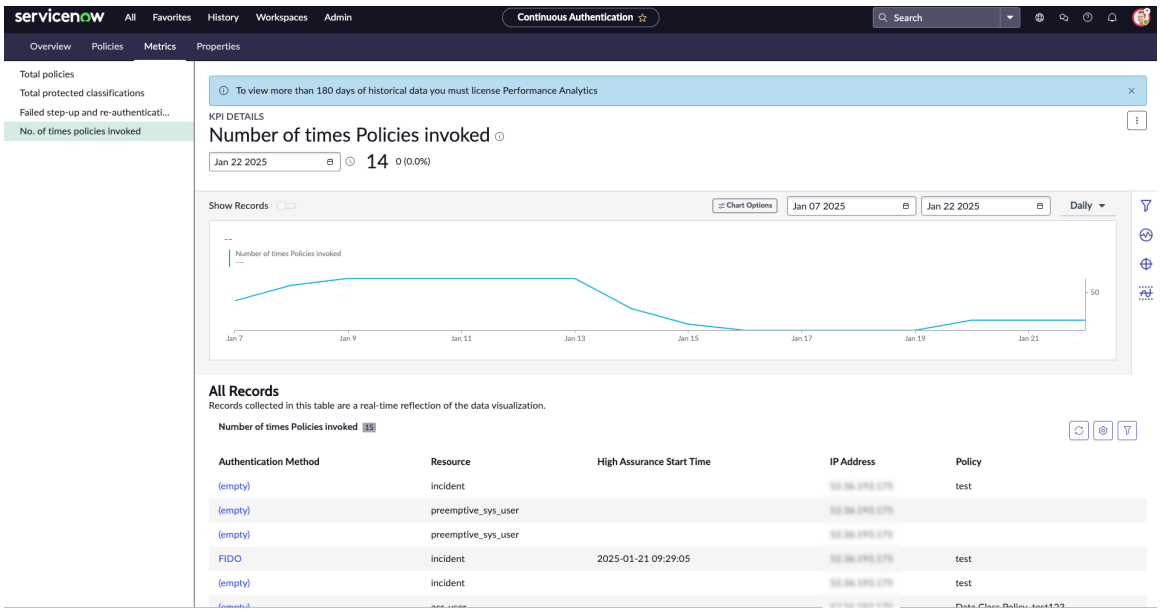
메트릭 페이지에 액세스하려면 다음으로 이동합니다. 모두 > 연속 인증에서 메트릭 탭을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 연속 인증에 대해 볼 수 있는 다양한 KPI 세부 정보입니다.

메트릭

메트릭	설명
총 정책	사용자에 대해 생성된 연속 인증 정책 수에 대한 KPI입니다.
총 보호된 분류	CA 정책 생성으로 인해 보호되는 분류 수에 대한 KPI입니다.
스텝업 또는 재인증 실패	실패한 스텝업(MFA) 또는 재인증(SSO) 수에 대한 KPI입니다.
정책이 적용된 횟수	CA 정책이 적용된 총 횟수에 대한 KPI입니다.



주: KPI 세부 정보는 180일 동안 표시됩니다. 180일 이상의 기록 데이터를 보려면 퍼포먼스 분석 라이센스가 있어야 합니다.

관련 정보

- 정책
- 메트릭
- 시스템 속성
- 연속 인증 살펴보기

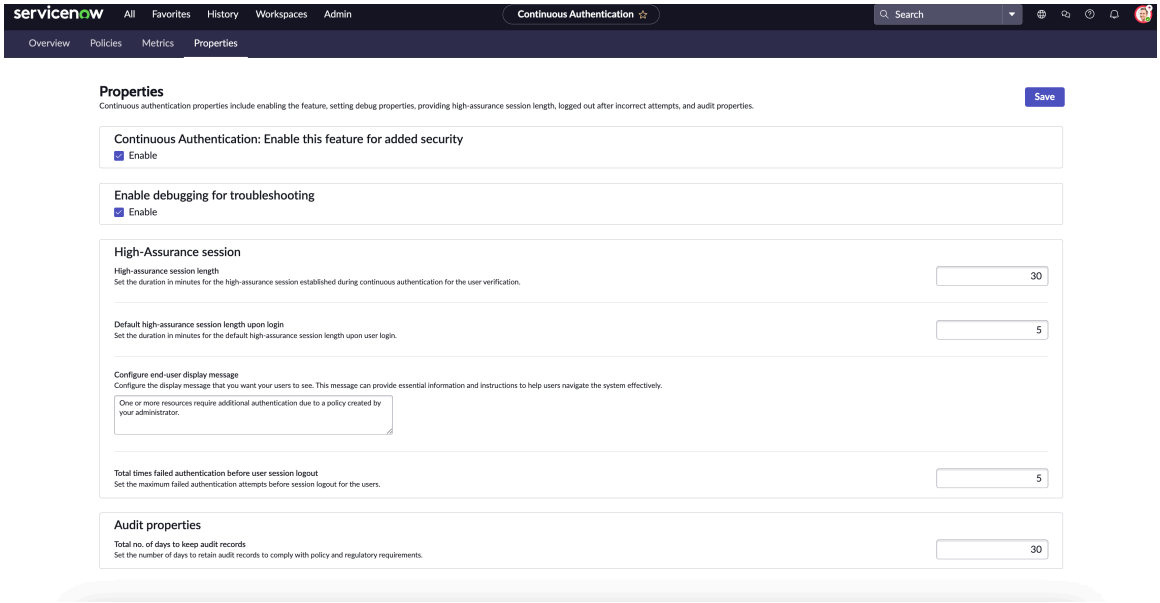
시스템 속성

시스템 속성을 사용하여 제로 트러스트 액세스 보안 요구 사항을 충족하도록 연속 인증(CA)을 활성화하고 사용자 지정합니다.

속성

속성 페이지에 액세스하려면 다음으로 이동하십시오. 모두 > 연속 인증에서 속성 탭을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다음은 CA에 대한 다양한 시스템 속성입니다.

연속 인증 시스템 속성

속성	설명
일반 속성	
연속 인증 (*glide.zta.continuous_authentication.enabled*)	연속 인증 기능 사용
디버깅 사용 (*glide.zta.continuous_authentication.debug.enabled*)	연속 인증과 관련된 디버깅 정보를 보려면 활성화합니다.
높은 보증	
높은 보증 세션 길이 (*glide.zta.high_assurance.session.timeout*)	최종 사용자가 재인증해야 하는 높은 보증 세션 길이를 지정합니다. 기본값: 10분. 주: 값은 1에서 480 사이여야 합니다.
로그인 시 기본 높은 보증 세션 길이	사용자 로그인 시 높은 보증 세션 길이의 기본 기간(분)을 지정합니다. 기본값: **5** 분. 주: 이 속성은 로컬 로그인에만 적용할 수 있습니다.
최종 사용자 표시 메시지 ()*glide.zta.high_assurance.session.message* 구성	재인증을 위해 최종 사용자에게 표시되는 메시지를 지정합니다. 기본 메시지: `#### ## #### ## ## ### ### ## ### #####`.
사용자 계정 잠금 전 인증에 실패한 총 시간 (*glide.zta.high_assurance.session.max.login.failed.attempts*)입니다	사용자가 로그아웃되기 전에 실패한 인증 시도 최대 횟수를 설정합니다. 주: 값은 3에서 10 사이여야 합니다.
감사 속성	

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연속 인증 시스템 속성

속성	설명
감사 기록을 보관할 총 일 수 (*glide.zta.continuous_authentication.audit.lifespan*)	CA에 대한 감사 기록을 저장할 일 수를 지정합니다. 주: 값은 1에서 180 사이여야 합니다.
총 번호 비활성화된 후 정책이 삭제되기까지의 일수 () *glide.zta.continuous_authentication.policy.lifespan*	CA 정책이 삭제되는 일 수를 지정합니다.

관련 정보

연속 인증 살펴보기

정책

메트릭

연속 인증을 위한 사전 작업

연속 인증을 위한 사전 작업

연속 인증(CA)을 사용하기 전에 다음 사전 작업을 수행해야 합니다.

CA는 의 제로 트러스트 액세스 보안 아키텍처를 기반으로 ServiceNow구축되었으며, 이는 초기 인증 프로세스 후에도 사용자가 주장하는 정체성을 유지하도록 하여 보안을 강화하는 것을 목표로 합니다.

주: 라이선스가 필요한 CA 옵트(opting CA)를 위해 제로 트러스트 `-com.snc.zero_trust_continuous_authentication`(연속 인증)을 설치해야 합니다.

CA 구성은 다음을 기반으로 수행할 수 있습니다.

- LDAP 또는 로컬 로그인(사용자 이름 및 암호)
- SSO 로그인(SAML 또는 OIDC)입니다.

로컬 로그인용 CA

사용자가 로컬 로그인을 수행하고 사용자의 ID를 확인하기 위해 MFA가 인증 메커니즘으로 사용됩니다. 사용자가 MFA를 설정하지 않은 경우 설정을 완료해야 합니다.

주:

- Yokohama에서는 로컬 로그인을 수행하는 모든 로그인에 ServiceNow 대해 사용자에게 MFA가 적용됩니다.
- MFA 속성이 활성 상태이고 요구 사항에 따라 구성되어 있는지 확인합니다. MFA 속성에 대한 자세한 내용은 다음 문서를 참조하십시오 다단계 인증 시스템 속성.

자세한 내용은 를 참조하십시오 비 SSO 로그인에 대한 높은 보증 세션.

SSO 로그인을 위한 CA

사용자가 SSO 기반 로그인(SAML 또는 OIDC)을 수행하는 경우. 사용자의 ID를 확인하기 위해 초기 로그인 중에 사용된 것과 동일한 SSO가 재인증 또는 IdP의 MFA를 통한 재검증으로 표시됩니다.

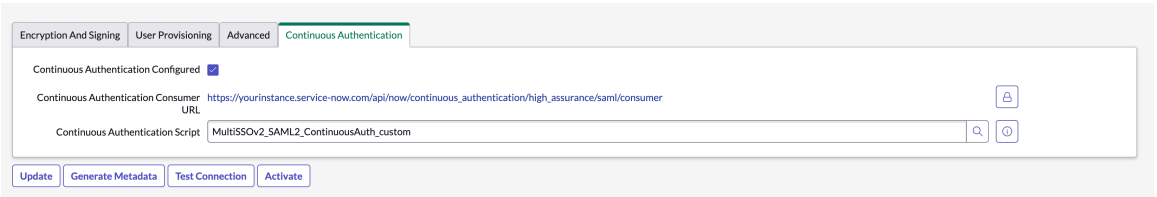
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 라이선스가 필요한 CA 옵트(opting CA)를 위해 제로 트러스트 -com.snc.zero_trust_continuous_authentication(연속 인증)을 설치해야 합니다.
- 통합 - 다중 제공자 1회 사용자 인증(SSO) 플러그인을*com.snc.integration.sso.multi.installer*활성화합니다.

다음과 같이 CA에 대한 IDP를 구성해야 합니다.

- 지정된 복수 SSO 기록에서 설정해야 하는 확인란을 활성화하여 CA를 사용할 준비가 된 세트를 확인합니다.



- OIDC의 경우 CA는 IDP에서 구성해야 하는 api/now/continuous_authentication/high_assurance/oidc/consumer 엔드포인트로 다시 리디렉션합니다. 재인증과 IdP의 MFA 옵션을 모두 사용할 수 있습니다.
- SAML의 경우 SSO 기록은 모든 신원 확인 제공자(IdP)에 대한 기본 재인증 스크립트를 사용하여 재인증을 지원합니다.

주:

- **Okta**에 대한 스텝업을 구성하기 위해 IdP 기록의 **ContinuousAuth_Okta_StepUp_Script** 사용할 수 있습니다. 자세한 내용은 이 설명서를 참조하십시오.
- 인트라 **ID** 또는 **Azure**에 대한 단계를 구성하려면 **ContinuousAuth_Azure_StepUp_Script** 사용하고 필요한 클레임을 추가할 수 있습니다. 자세한 내용은 이 설명서를 참조하십시오.

자세한 내용은 를 참조하십시오 SSO 로그인에 대한 높은 보증.

관련 정보

연속 인증 살펴보기

연속 인증 활성화

연속 인증 구성

연속 인증 활성화

인스턴스에서 연속 인증 기능을 활성화하려면 제로 트러스트 - 연속 인증 (com.snc.zero_trust_continuous_authentication) 플러그인을 설치합니다.

시작하기 전에
필요한 역할: 관리자

이 플러그인을 사용하면 보안 관리자가 사용자가 액세스하는 데이터와 수행 중인 활동에 따라 로그인한 세션 내에서 MFA(스텝업 인증) 또는 재인증(SSO)이 필요한 보안 정책을 정의할 수 있습니다.

라이선스가 필요한 CA 옵트(opting CA)를 위해 제로 트러스트 -com.snc.zero_trust_continuous_authentication(연속 인증)을 설치해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 **Zero Trust -**`com.snc.zero_trust_continuous_authentication`(연속 인증) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

관련 정보

연속 인증을 위한 사전 작업

연속 인증 구성

높은 보증 연속 인증

연속 인증 구성

사용자가 보호하는 자원에 액세스하려는 시도가 있는 경우 사용자를 다시 인증하도록 CA(연속 인증) 정책을 구성합니다.

시작하기 전에

- 필요한 역할: 관리자(ca_admin)

  주: 역할을 **ca_admin**로 승격해야 합니다.

- 라이선스가 필요한 CA 옵트(opting CA)를 위해 제로 트러스트 -`com.snc.zero_trust_continuous_authentication`(연속 인증)을 설치해야 합니다.
- 연속 인증()*glide.zta.continuous_authentication.enabled*시스템 속성을 활성화합니다. 자세한 내용은 시스템 속성 문서를 참조하십시오.
- 통합 - 다중 제공자 1회 사용자 인증(SSO) 플러그인을*com.snc.integration.sso.multi.installer*활성화합니다.
- 인스턴스에 대한 CA를 구성하기 전에 필요한 사전 작업을 이해합니다. 자세한 내용은 연속 인증을 위한 사전 작업 문서를 참조하십시오.
- 데이터 클래스 또는 테이블에 대해 CA 정책을 구성할 수 있습니다.

프로시저

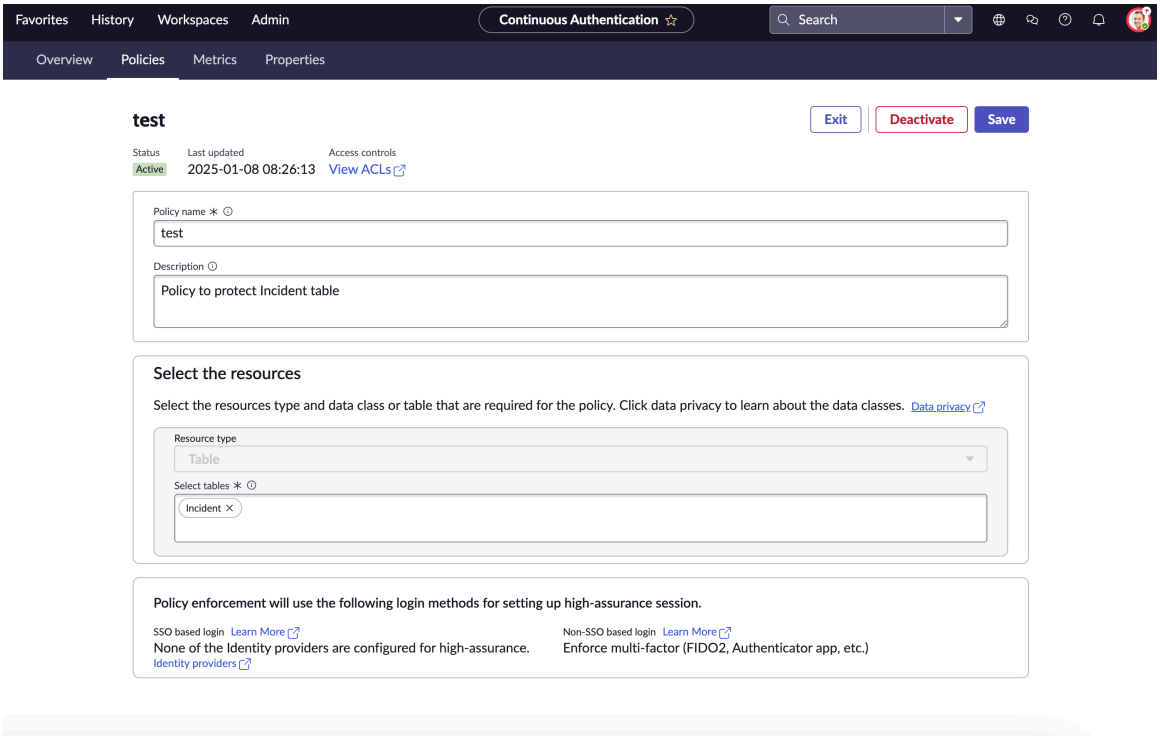
1. 다음으로 이동 모두 > 연속 인증.
2. 정책 탭을 선택합니다.
3. 새로 만들기를 선택합니다.
4. 양식에서 필드에 다음을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연속 인증

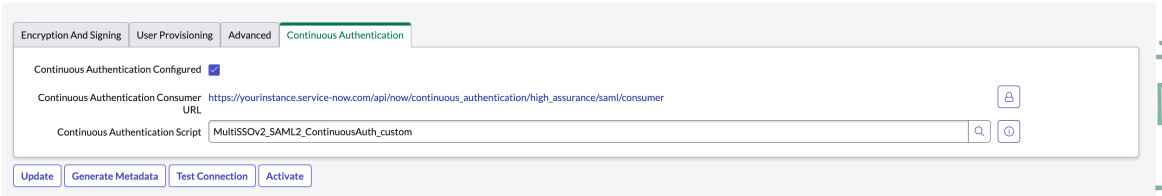
필드	설명
보험 이름	정책 이름
설명	정책에 대한 일반적인 설명
자원 선택	옵션: ◦ 데이터 클래스. 데이터 클래스를 생성하여 CA 정책 구성에 사용할 수 있습니다. 다음은 선택할 수 있는 샘플 데이터 클래스입니다. ▪ 내부 ▪ 개인 식별 정보 ▪ 제한함 ▪ 기밀 ▪ 공개 주: 데이터 클래스를 만드는 방법에 대한 자세한 내용은 을 참조하십시오 데이터 분류. ◦ 테이블 주: ◦ 메타데이터와 함께 선택된 테이블에 오류가 표시됩니다. ◦ 사용자에 대한 구성 액세스에 영향을 줄 수 있으므로 실제로 메타데이터 테이블에 대한 액세스를 제한할지 확인해야 합니다. ◦ **sys_properties**, **sys_continuous_auth_policysys_user** 테이블은 CA에 대해 제외되며 CA 정책 구성에 추가할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주: CA 정책에 대한 로그인 방법 중 하나를 사용할 수 있습니다.

- **SSO** 기반 로그인: ID 제공자 기록 내의 **Continuous** Authentication(연속 인증) 탭에 필드를 지정하고 ID 제공자 기록을 활성으로 설정합니다.



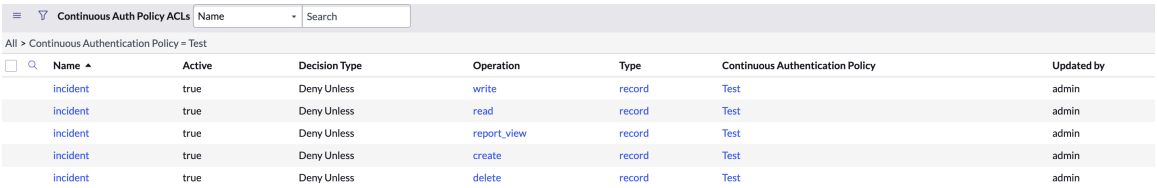
ID 제공자 구성에 대한 자세한 내용은 OIDC 및 SAML을 참조하십시오.

- **SSO** 기반이 아닌 로그인: 기본적으로 연속 인증 구성을 사용하는 ID 제공자가 없는 경우 로그인 방법으로 MFA(다단계 인증)가 사용됩니다. MFA 속성이 활성 상태이고 요구 사항에 따라 구성되어 있는지 확인합니다. MFA 속성에 대한 자세한 내용은 다음 문서를 참조하십시오 다단계 인증 시스템 속성.

5. 저장 및 활성화를 선택합니다.

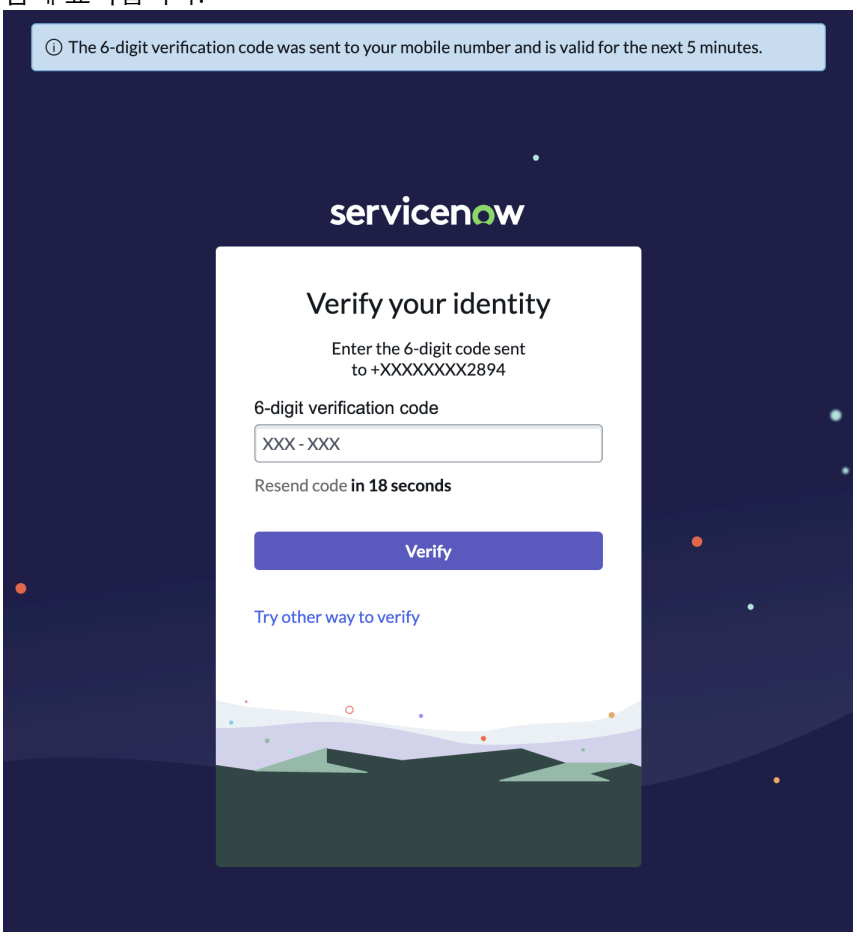
결과
구성에 제공된 상세 정보를 기반으로 선택한 테이블 또는 데이터 클래스에 대한 ACL(접근 제어 목록)을 사용하여 CA 정책이 생성됩니다. 정책 페이지에서 **ACL** 보기**(View ACLs**)를 선택하여 생성한 ACL의 상세 정보를 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



생성된 CA 정책은 다음 시나리오에 따라 정책을 사용하여 보호한 테이블 또는 데이터 클래스에 액세스하기 위한 인증을 사용자에게 요청합니다.

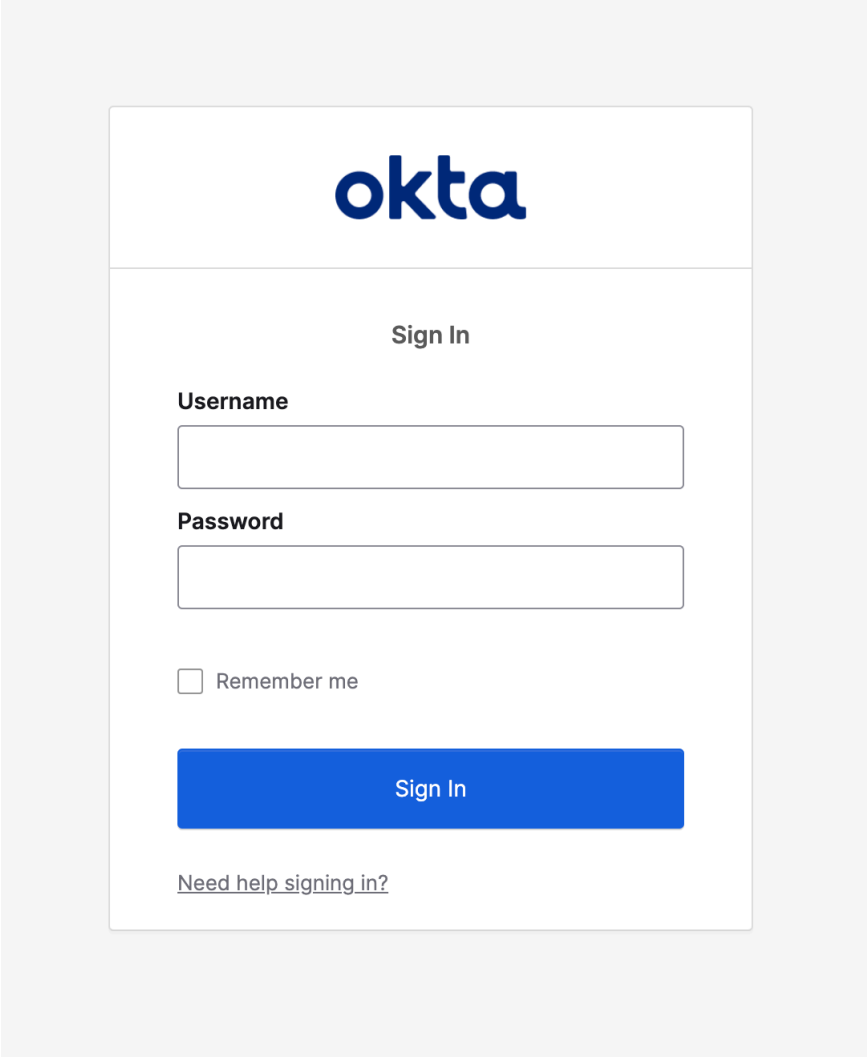
- 인스턴스에 로그인하기 위해 로컬 로그인을 수행한 사용자는 단계별 인증을 위해 플랫폼 MFA와 함께 표시됩니다.



주: 사용자가 최근에 사용한 MFA 요소가 인증을 위해 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인스턴스에 로그인하기 위해 SSO 로그인(OIDC 또는 SAML)을 수행한 사용자가 재인증을 위해 SSO와 함께 표시됩니다.



이제 사용자에 대한 높은 보증 세션이 설정됩니다. 높은 보증 세션은 높은 보증 세션 길이(*glide.zta.high_assurance.session.timeout*) 시스템 속성으로 제한됩니다. 높은 보증 세션 시간이 속성 길이를 초과하면 사용자에게 재인증 또는 스텝업 인증을 요청하는 메시지가 표시됩니다.

테이블 또는 데이터에 대한 연속 인증의 엔드 투 엔드 구성에 대한 자세한 내용은 다음을 참조하십시오.

- 자습서: 테이블에 대한 연속 인증 구성.
- 자습서: 데이터 클래스에 대한 연속 인증 구성.

관련 정보

연속 인증 살펴보기

연속 인증을 위한 사전 작업

연속 인증 활성화

자습서: 테이블에 대한 연속 인증 구성

테이블에 대한 연속 인증 정책의 엔드 투 엔드 구성과 구성 변경이 사용자에게 미치는 영향을 설명하는 절차입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

- 필요한 역할: 관리자(ca_admin)

  주: 역할을 **ca_admin**로 승격해야 합니다.

- 라이선스가 필요한 CA 옵트(opting CA)를 위해 제로 트러스트 `-com.snc.zero_trust_continuous_authentication`(연속 인증)을 설치해야 합니다.
- 연속 인증()*glide.zta.continuous_authentication.enabled*시스템 속성을 활성화합니다. 자세한 내용은 시스템 속성 문서를 참조하십시오.
- 통합 - 다중 제공자 1회 사용자 인증(SSO) 플러그인을*com.snc.integration.sso.multi.installer*활성화합니다.
- 인스턴스에 대한 CA를 구성하기 전에 필요한 사전 작업을 이해합니다. 자세한 내용은 연속 인증을 위한 사전 작업 문서를 참조하십시오.

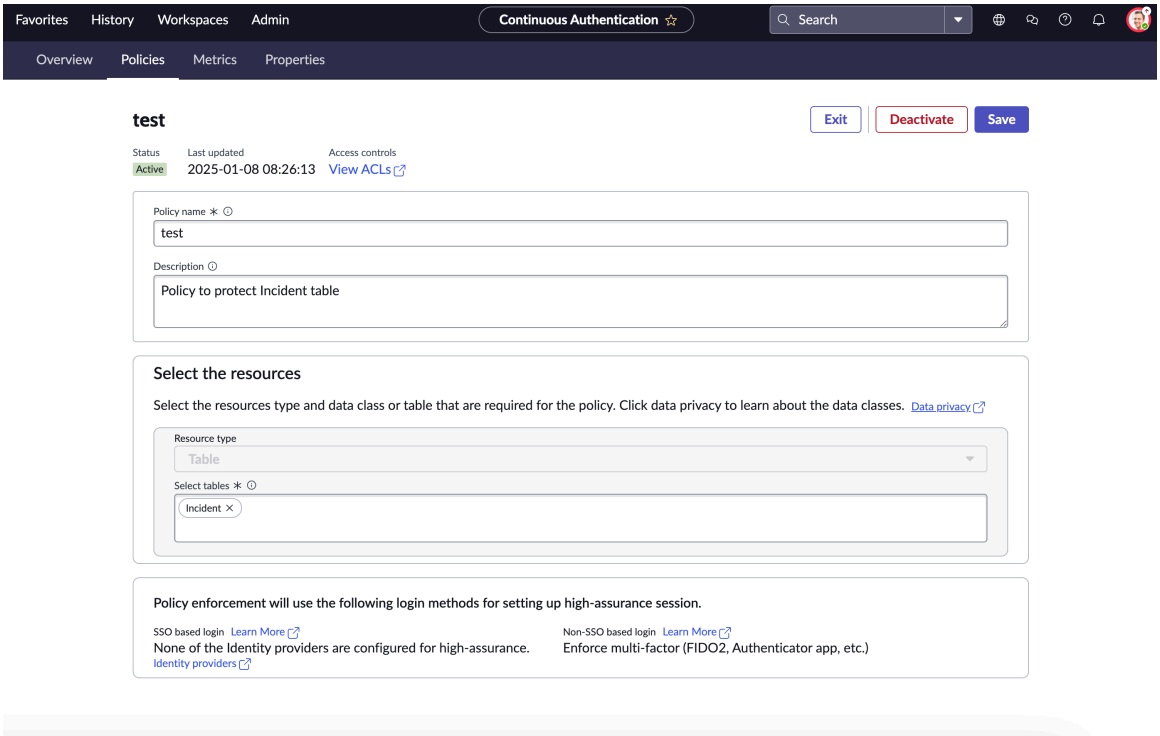
프로시저

1. 다음으로 이동 모두 > 연속 인증.
2. 정책 탭을 선택합니다.
3. 새로 만들기를 선택합니다.
4. 양식에서 필드에 다음을 입력합니다.

연속 인증

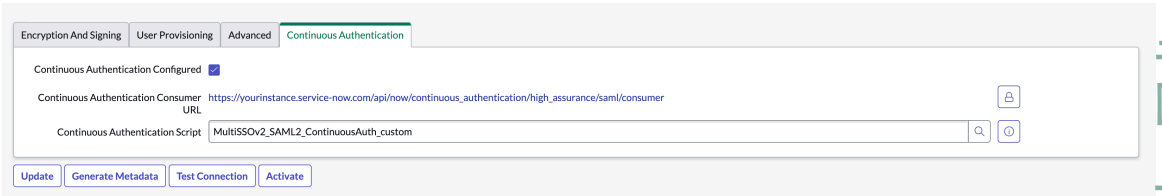
필드	설명
보험 이름	정책 이름
설명	정책에 대한 일반적인 설명
자원 선택	테이블을 선택합니다. 주: ◦ 이 예에서는 인시던트 테이블이 선택되어 있습니다. 요구 사항에 따라 테이블을 원하는 만큼 선택할 수 있습니다. ◦ 메타데이터와 함께 선택된 테이블에 오류가 표시됩니다. 사용자에 대한 구성 액세스에 영향을 줄 수 있으므로 실제로 메타데이터 테이블에 대한 액세스를 제한할지 확인해야 합니다. ◦ **sys_properties**, **sys_continuous_auth_policysys_user** 테이블은 CA에 대해 제외되며 CA 정책 구성에 추가할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주: CA 정책에 대한 로그인 방법 중 하나를 사용할 수 있습니다.

- **SSO** 기반 로그인: ID 제공자 기록 내의 **Continuous** Authentication(연속 인증) 탭에 필드를 지정하고 ID 제공자 기록을 활성으로 설정합니다.



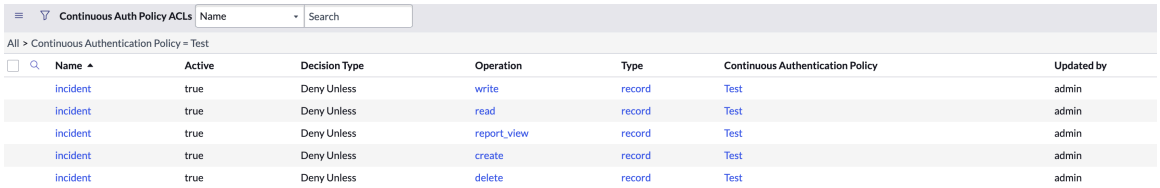
ID 제공자 구성에 대한 자세한 내용은 OIDC 및 SAML을 참조하십시오.

- **SSO** 기반이 아닌 로그인: 기본적으로 연속 인증 구성을 사용하는 ID 제공자가 없는 경우 로그인 방법으로 MFA(다단계 인증)가 사용됩니다. MFA 속성이 활성 상태이고 요구 사항에 따라 구성되어 있는지 확인합니다. MFA 속성에 대한 자세한 내용은 다음 문서를 참조하십시오 다단계 인증 시스템 속성.

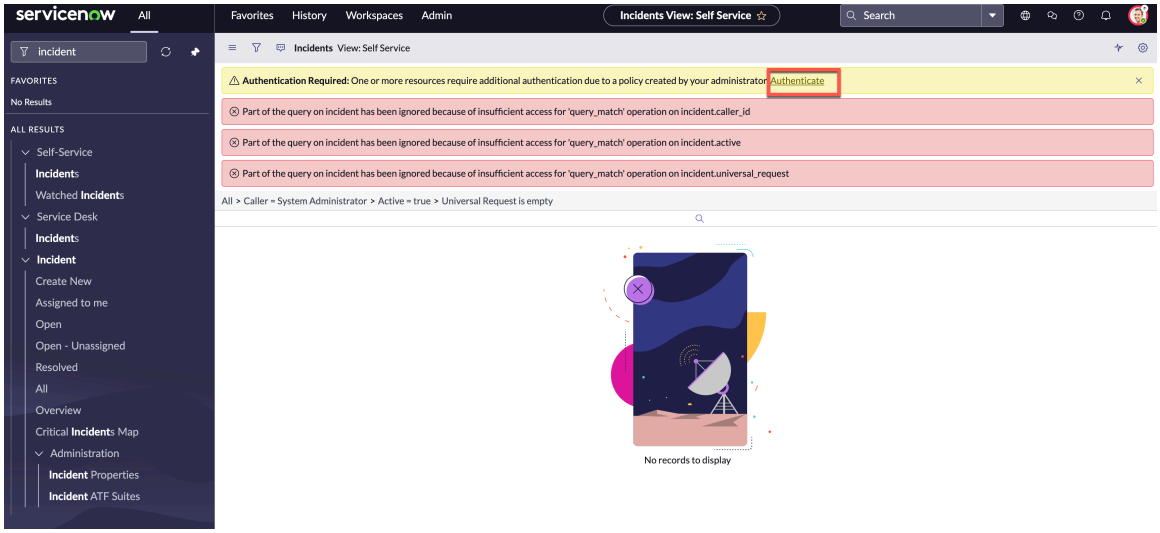
5. 저장 및 활성화를 선택합니다.

결과
구성에 제공된 상세 정보를 기반으로 선택한 테이블 또는 데이터 클래스에 대한 ACL(접근 제어 목록)을 사용하여 CA 정책이 생성됩니다. 정책 페이지에서 **ACL** 보기**(View ACLs**)를 선택하여 생성한 ACL의 상세 정보를 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



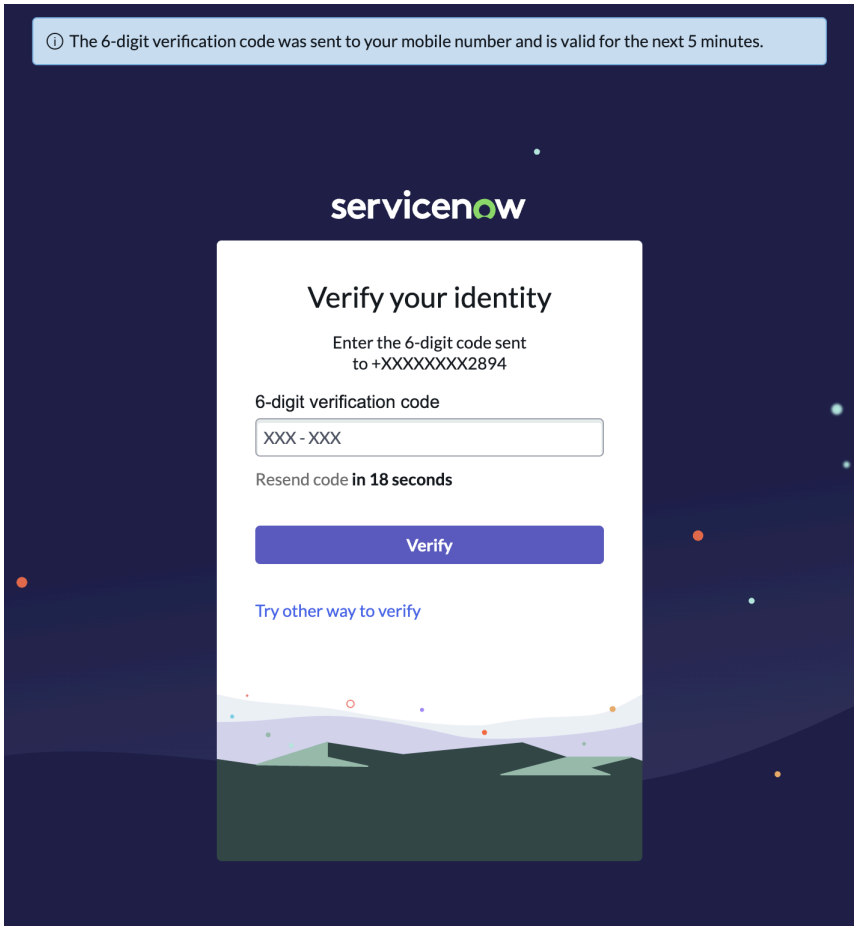
생성된 CA 정책은 정책을 사용하여 보호한 테이블(이 경우 인시던트 테이블)에 액세스하기 위한 인증을 사용자에게 요청합니다. 사용자는 인증 옵션을 선택할 수 있습니다.



다음에 따라 인증을 수행합니다.

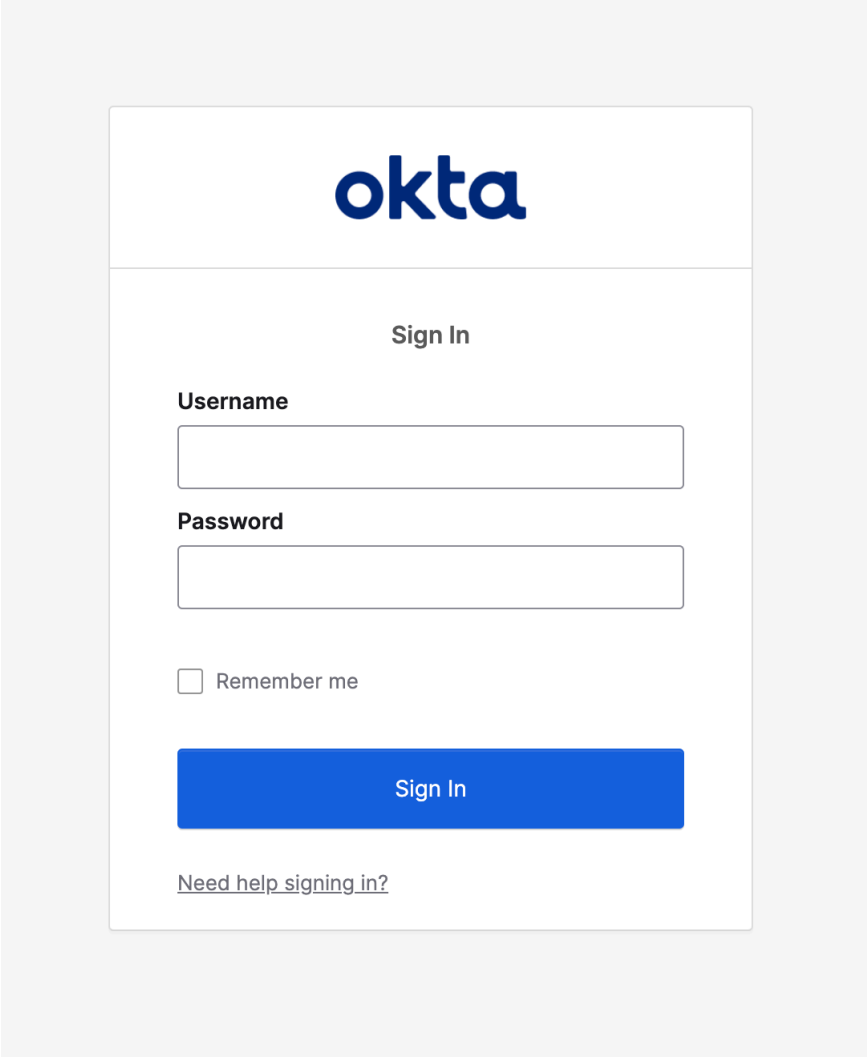
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인스턴스에 로그인하기 위해 로컬 로그인을 수행한 사용자는 단계별 인증을 위해 플랫폼 MFA와 함께 표시됩니다.

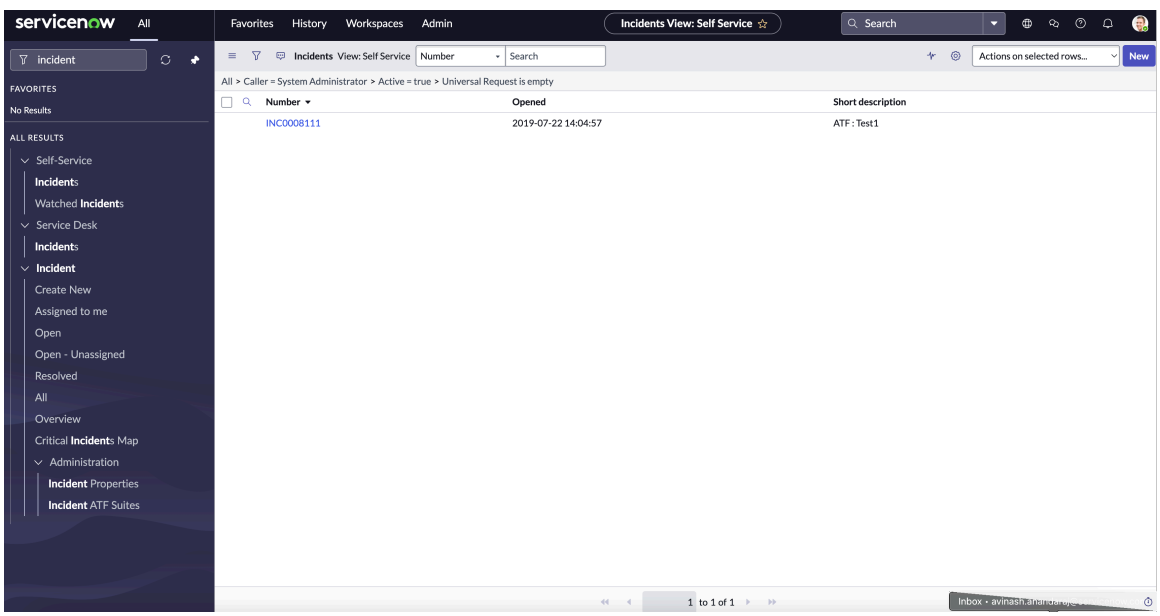


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인스턴스에 로그인하기 위해 SSO 로그인(OIDC 또는 SAML)을 수행한 사용자가 재인증을 위해 SSO와 함께 표시됩니다.



인증에 성공하면 테이블이 표시됩니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이제 사용자에 대한 높은 보증 세션이 설정됩니다. 높은 보증 세션은 높은 보증 세션 길이(*glide.zta.high_assurance.session.timeout*) 시스템 속성으로 제한됩니다. 높은 보증 세션 시간이 속성 길이를 초과하면 사용자에게 재인증 또는 스텝업 인증을 요청하는 메시지가 표시됩니다.

관련 정보

연속 인증 구성

높은 보증 연속 인증

연속 인증 살펴보기

자습서: 데이터 클래스에 대한 연속 인증 구성

데이터 클래스에 대한 연속 인증 정책의 엔드 투 엔드 구성과 구성 변경이 사용자에게 미치는 영향을 설명하는 절차입니다.

시작하기 전에

- 필요한 역할: 관리자(ca_admin)

  주: 역할을 **ca_admin**로 승격해야 합니다.

- 라이선스가 필요한 CA 옵트(opting CA)를 위해 제로 트러스트 `-com.snc.zero_trust_continuous_authentication`(연속 인증)을 설치해야 합니다.
- 연속 인증()*glide.zta.continuous_authentication.enabled*시스템 속성을 활성화합니다. 자세한 내용은 시스템 속성 문서를 참조하십시오.
- 통합 - 다중 제공자 1회 사용자 인증(SSO) 플러그인을*com.snc.integration.sso.multi.installer*활성화합니다.
- 인스턴스에 대한 CA를 구성하기 전에 필요한 사전 작업을 이해합니다. 자세한 내용은 연속 인증을 위한 사전 작업 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 연속 인증.
2. 정책 탭을 선택합니다.
3. 새로 만들기를 선택합니다.
4. 양식에서 필드에 다음을 입력합니다.

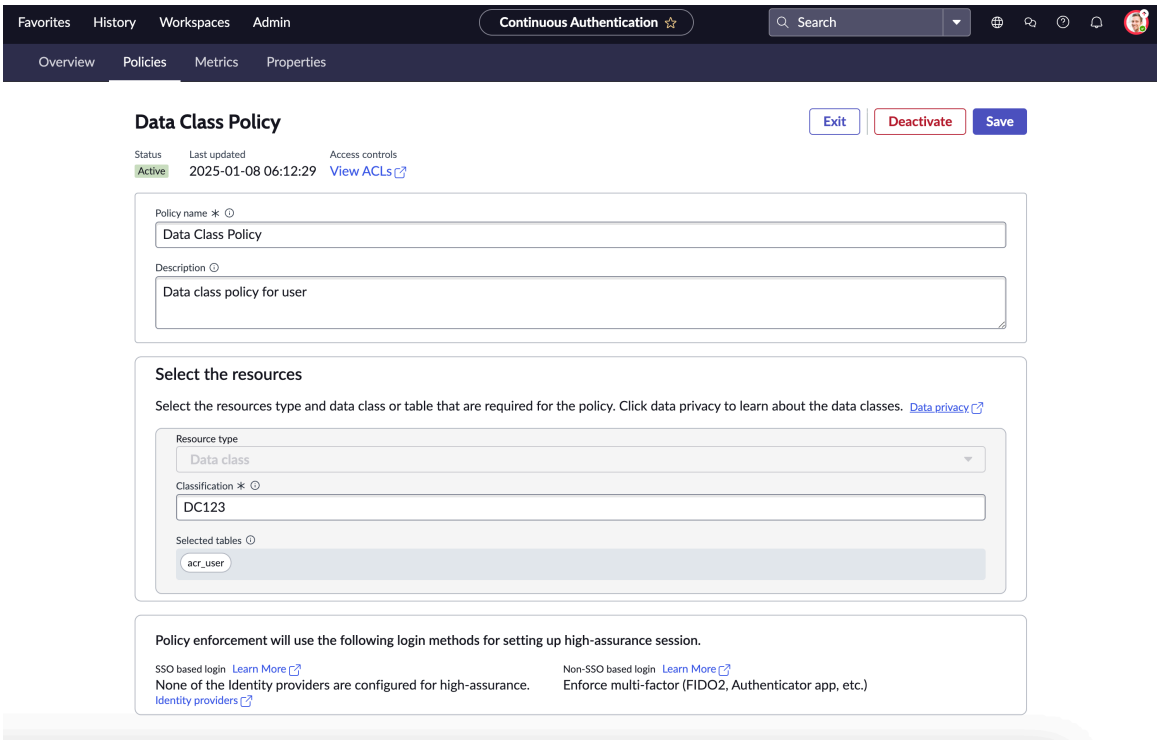
연속 인증

필드	설명
보험 이름	정책 이름
설명	정책에 대한 일반적인 설명
자원 선택	데이터 클래스를 선택합니다. 데이터 클래스를 생성하여 CA 정책 구성에 사용할 수 있습니다. 다음은 선택할 수 있는 샘플 데이터 클래스입니다. ◦ 내부 ◦ 개인 식별 정보 ◦ 제한함 ◦ 기밀 ◦ 공개

기계번역

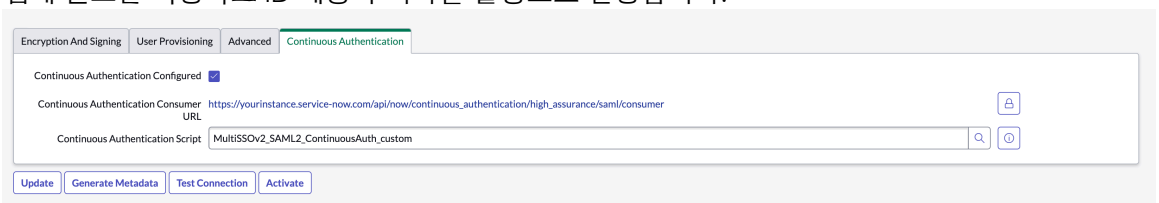
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 데이터 클래스를 만드는 방법에 대한 자세한 내용은 을 참조하십시오 데이터 분류.



주: CA 정책에 대한 로그인 방법 중 하나를 사용할 수 있습니다.

- **SSO** 기반 로그인: ID 제공자 기록 내의 **Continuous** Authentication(연속 인증) 탭에 필드를 지정하고 ID 제공자 기록을 활성으로 설정합니다.



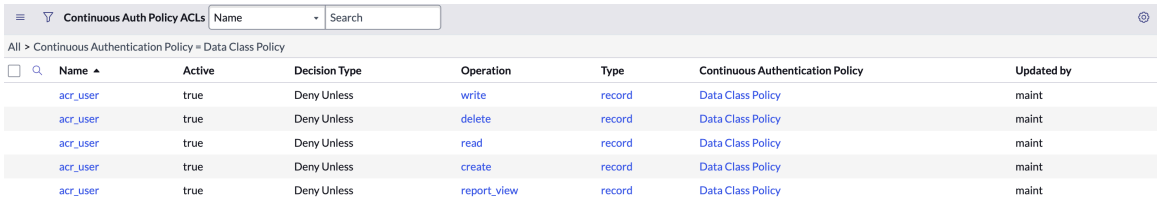
ID 제공자 구성에 대한 자세한 내용은 OIDC 및 SAML을 참조하십시오.

- **SSO** 기반이 아닌 로그인: 기본적으로 연속 인증 구성을 사용하는 ID 제공자가 없는 경우 로그인 방법으로 MFA(다단계 인증)가 사용됩니다. MFA 속성이 활성 상태이고 요구 사항에 따라 구성되어 있는지 확인합니다. MFA 속성에 대한 자세한 내용은 다음 문서를 참조하십시오 다단계 인증 시스템 속성.

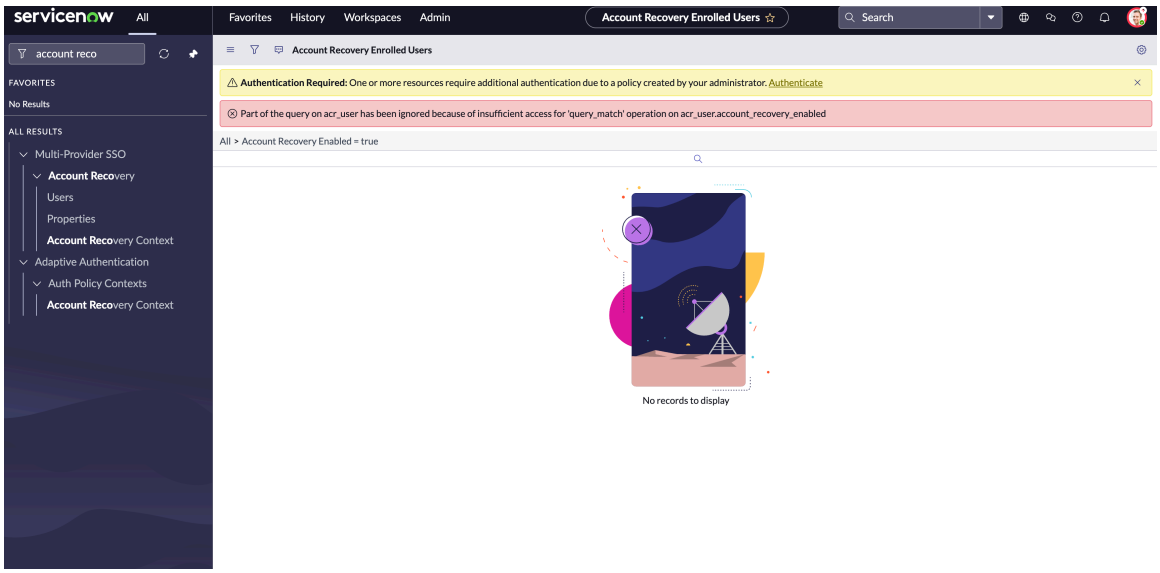
5. 저장 및 활성화를 선택합니다.

결과
구성에 제공된 상세 정보를 기반으로 선택한 테이블 또는 데이터 클래스에 대한 ACL(접근 제어 목록)을 사용하여 CA 정책이 생성됩니다. 정책 페이지에서 **ACL** 보기**(View ACLs**)를 선택하여 생성한 ACL의 상세 정보를 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



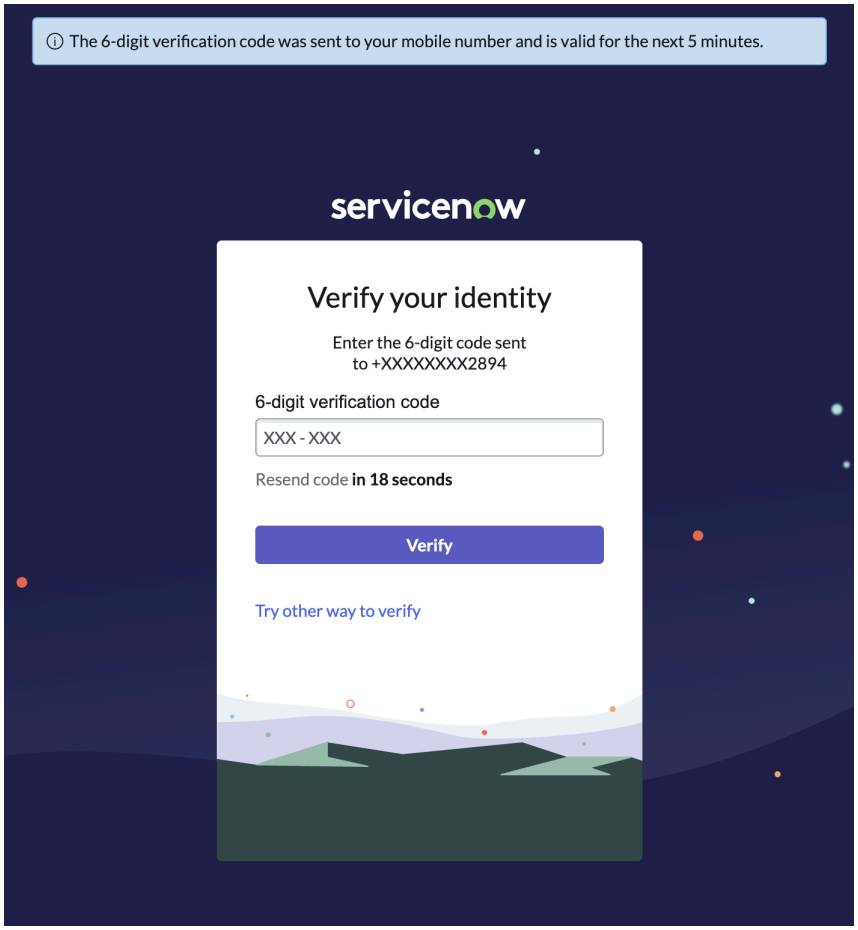
생성된 CA 정책은 정책을 사용하여 보호한 데이터 클래스(이 경우 **Account Recovery** 테이블에 대해 설정된 데이터 클래스)에 대한 인증을 사용자에게 묻는 메시지를 표시합니다. 사용자는 인증 옵션을 선택할 수 있습니다.



다음에 따라 인증을 수행합니다.

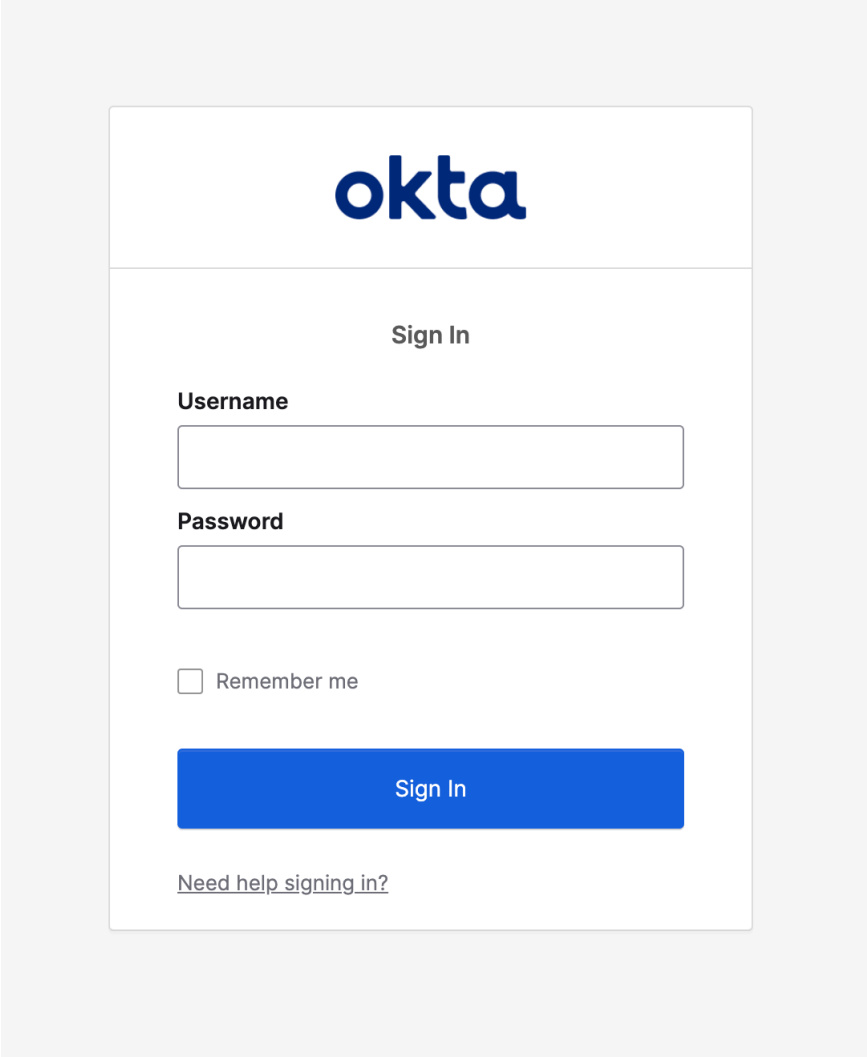
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인스턴스에 로그인하기 위해 로컬 로그인을 수행한 사용자는 단계별 인증을 위해 플랫폼 MFA와 함께 표시됩니다.

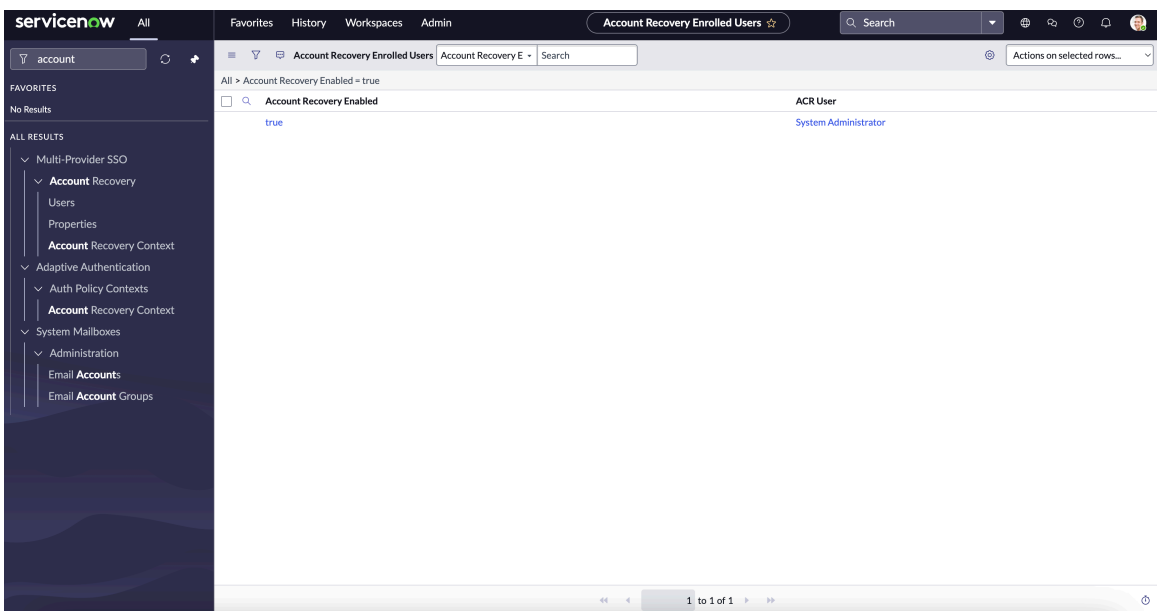


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인스턴스에 로그인하기 위해 SSO 로그인(OIDC 또는 SAML)을 수행한 사용자가 재인증을 위해 SSO와 함께 표시됩니다.



인증에 성공하면 데이터 클래스가 있는 테이블이 표시됩니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이제 사용자에 대한 높은 보증 세션이 설정됩니다. 높은 보증 세션은 높은 보증 세션 길이(*glide.zta.high_assurance.session.timeout*) 시스템 속성으로 제한됩니다. 높은 보증 세션 시간이 속성 길이를 초과하면 사용자에게 재인증 또는 스텝업 인증을 요청하는 메시지가 표시됩니다.

관련 정보

- 연속 인증 구성
- 높은 보증 연속 인증
- 연속 인증 살펴보기

높은 보증 연속 인증

연속 인증에 ServiceNow대해 높은 보증 세션을 설정합니다.

높은 보증 세션은 데이터에 액세스하고 높은 수준의 신뢰도로 확인된 ID(사용자)와 안전하고 신뢰할 수 있는 연결을 설정하기 위한 보안 조치입니다.

ServiceNow사용자의 높은 보증은 사용자가 중요한 데이터에 액세스하려고 할 때 MFA(Multi-factor Authentication) 및 SSO(Single Sign On)와 같은 방법을 사용하여 재인증을 적용하는 강력한 인증 방법을 통해 달성됩니다.

사용자가 다시 인증하거나 MFA(스텝업 인증)를 수행할 때 사용자가 CA 정책 구성에 따라 CA 관리자가 보호하는 데이터에 액세스할 수 있는 기능을 제공하는 높은 보증 세션이 설정됩니다.

다음은 로그인 유형에 따라 높은 보증을 설정하는 데 사용되는 재인증 방법입니다.

- SSO 로그인에 대한 높은 보증
- 비 SSO 로그인에 대한 높은 보증

사용자가 만든 높은 보증 세션은 CA 관리자가 결정한 높은 보증 세션 길이 ()*glide.zta.high_assurance.session.timeout*를 기준으로 유효합니다.

높은 보증 세션은 높은 보증 시스템 속성을 설정하여 요구 사항에 따라 사용자 지정할 수 있습니다.

높은 보증 시스템 속성

필드	설명
높은 보증 세션 길이 (*glide.zta.high_assurance.session.timeout*)	최종 사용자가 재인증해야 하는 높은 보증 세션 길이를 지정합니다. 기본값: 10분. 주: 값은 1에서 480 사이여야 합니다.
로그인 시 기본 높은 보증 세션 길이	사용자 로그인 시 높은 보증 세션 길이의 기본 기간(분)을 지정합니다. 기본값: **5** 분.
최종 사용자 표시 메시지 ()*glide.zta.high_assurance.session.message* 구성	재인증을 위해 최종 사용자에게 표시되는 메시지를 지정합니다. 기본 메시지: `#### ## #### ## ## ### ### ## ### #####.`
사용자 계정 잠금 전 인증에 실패한 총 시간 (*glide.zta.high_assurance.session.max.login.failed.attempts*)	사용자가 로그아웃되기 전에 실패한 인증 시도 최대 횟수를 설정합니다. 주: 값은 3에서 10 사이여야 합니다.

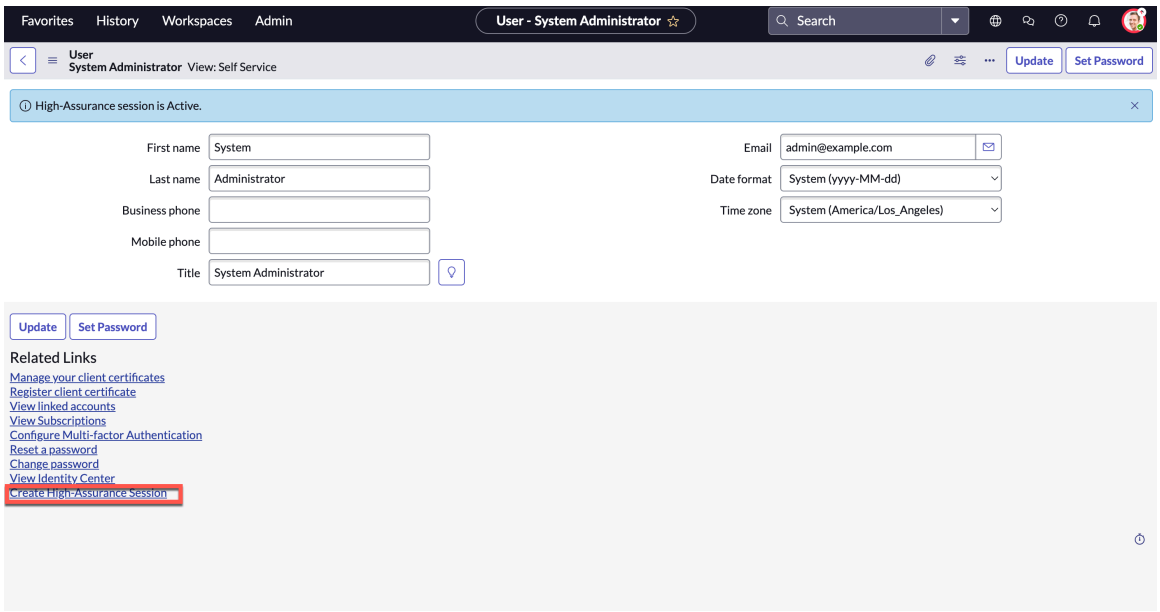
기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

선제적 조치로서의 높은 보증 세션

금융 거래, 정부 정보, PII와 같은 높은 권한 데이터를 사용하는 사용자는 로그인한 세션 동안 빈번한 인증 알림을 피하기 위한 선제적 조치로 높은 보증 세션을 설정할 수 있습니다.

높은 보증 세션은 직접 만들 수 있습니다. 높은 보증 세션을 생성하려면 다음을 선택합니다. 사용자 프로파일 > 프로파일. 관련 링크 섹션에서 높은 보증 세션 생성을 선택합니다. ID를 검증하여 높은 보증 세션을 생성합니다.



관련 정보

- 연속 인증 살펴보기
- 연속 인증을 위한 사전 작업
- 연속 인증 구성

SSO 로그인에 대한 높은 보증

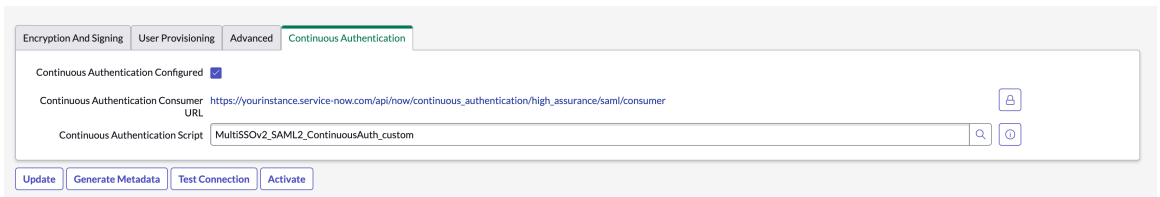
연속 인증을 사용하여 ServiceNowSSO 로그인에 대한 높은 보증 세션을 설정합니다.

높은 보증 세션은 사용자가 자신의 ID를 확인하고 특정 시간 프레임 동안 특정 ID 또는 ID 제공자로 인증해야 하는 세션입니다.

ServiceNow의 CA(연속 인증) 기능을 사용하면 PII(개인 식별 정보), 중요한 데이터에 액세스하는 사용자에게 높은 보증 세션을 생성하거나 보호하려는 명시적 데이터에 대한 액세스를 제한하는 정책을 만들 수 있습니다.

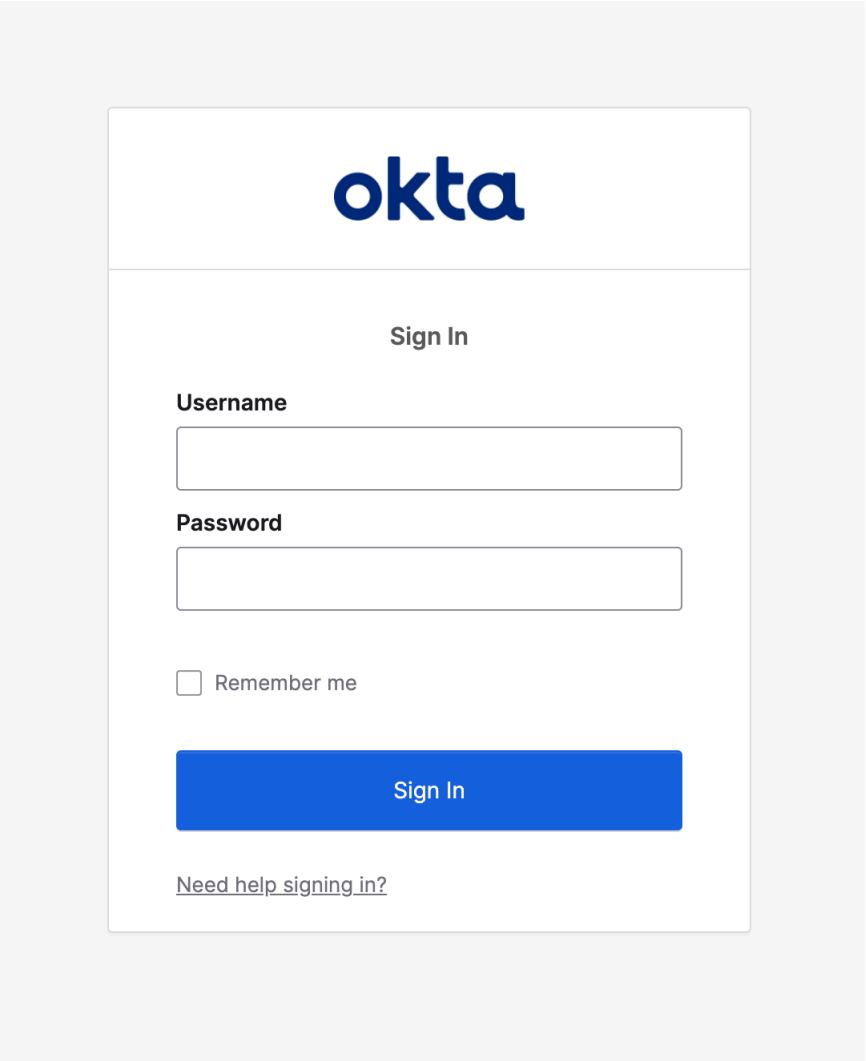
사용자가 다시 인증하면 높은 보증 세션이 설정되어 사용자가 CA 정책 구성에 따라 CA 관리자가 보호하는 데이터에 액세스할 수 있는 기능을 제공합니다.

CA 정책을 생성하여 사용자가 보호한 데이터에 액세스할 수 있도록 사용자 ID 및 인증을 확인할 수 있습니다. CA 정책을 구성하고 ID 제공자 기록에 ID 제공자 세부 정보를 제공하여 높은 보증 세션을 설정할 수 있습니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SSO 기반 로그인(SAML 또는 OIDC)을 수행하는 사용자와 보호된 데이터에 액세스하려고 시도할 때마다 초기 로그인 중에 사용자가 사용한 것과 동일한 SSO를 사용하여 재인증 화면에 메시지가 표시됩니다.



SSO 인증에 성공하면 보호된 데이터가 특정 기간 동안 사용자에게 표시됩니다. 요구 사항에 따라 시간 제한을 변경하도록 속성을 구성할 수 있습니다. 자세한 내용은 를 참조하십시오 높은 보증 연속 인증.

SSO 로그인(SAML 또는 OIDC)으로 재인증을 수행하면 보호된 데이터에 액세스하는 ID(사용자)와 안전하고 신뢰할 수 있는 연결을 설정하는 높은 보증 세션이 생성됩니다.

사용자에 대해 설정된 높은 보증 세션은 높은 보증 세션 길이 ()*glide.zta.high_assurance.session.timeout* 시스템 속성으로 제한됩니다. 높은 보증 세션 시간이 속성 길이를 초과하면 사용자에게 재인증 또는 스텝업 인증을 요청하는 메시지가 표시됩니다.

관련 정보

- 높은 보증 연속 인증
- 연속 인증을 위한 사전 작업
- 연속 인증 구성

비 **SSO** 로그인에 대한 높은 보증 세션

의 연속 인증을 사용하여 ServiceNow비 SSO 로그인(로컬 또는 LDAP)에 대해 높은 보증 세션을 설정합니다.

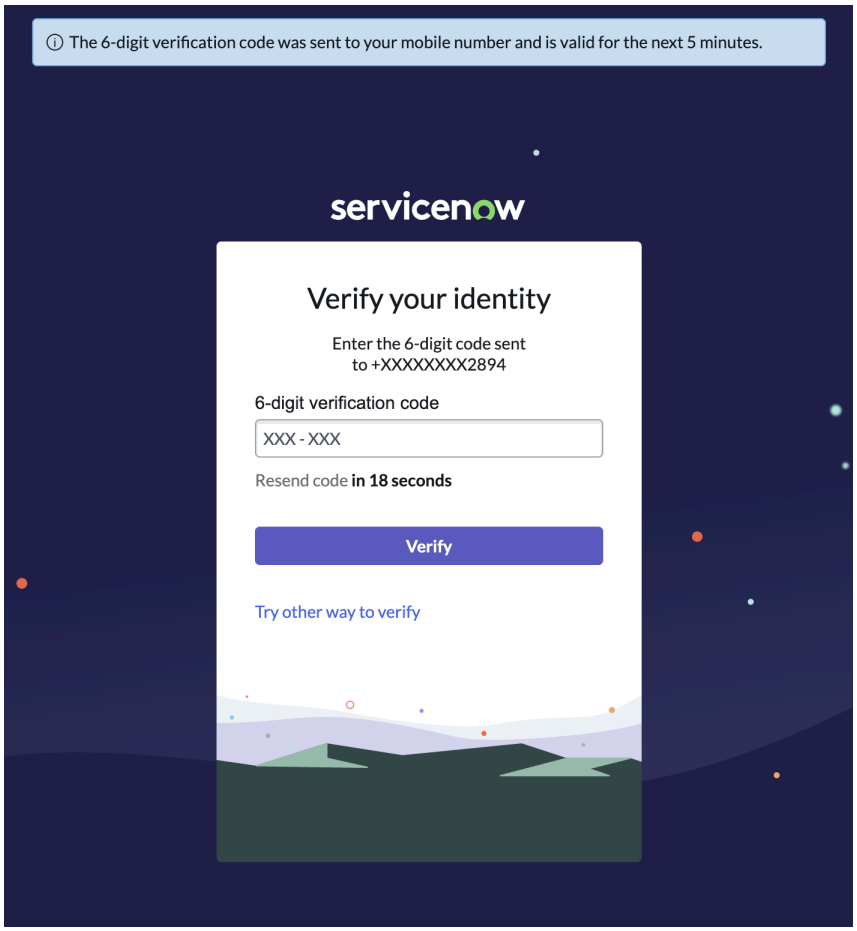
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

높은 보증 세션은 사용자가 자신의 ID를 확인하고 특정 시간 프레임 동안 특정 ID 또는 ID 제공자로 인증해야 하는 세션입니다.

ServiceNow의 CA(연속 인증) 기능을 사용하면 PII(개인 식별 정보), 중요한 데이터에 액세스하는 사용자에게 높은 보증 세션을 생성하거나 보호하려는 명시적 데이터에 대한 액세스를 제한하는 정책을 만들 수 있습니다.

사용자가 MFA(스텝업 인증)를 수행할 때 사용자가 CA 정책 구성에 따라 CA 관리자가 보호하는 데이터에 액세스할 수 있는 기능을 제공하는 높은 보증 세션이 설정됩니다.

CA 정책을 생성하여 사용자가 보호한 데이터에 액세스할 수 있도록 사용자 ID 및 인증을 확인할 수 있습니다. 비 SSO 기반 로그인(로컬 또는 LDAP)을 수행하는 사용자와 보호된 데이터에 액세스하려고 할 때마다 스텝업 인증(MFA) 화면이 사용자에게 표시됩니다.



인증에 성공하면 보호된 데이터가 특정 기간 동안 사용자에게 표시됩니다. 요구 사항에 따라 시간 제한을 변경하도록 속성을 구성할 수 있습니다. 자세한 내용은 를 참조하십시오 높은 보증 연속 인증.

주: 사용자가 MFA를 설정하지 않은 경우 설정을 완료해야 합니다.

MFA(스텝업 인증)를 수행하면 보호된 데이터에 액세스하는 ID(사용자)와 안전하고 신뢰할 수 있는 연결을 설정하는 높은 보증 세션이 생성됩니다.

사용자에 대해 설정된 높은 보증 세션은 높은 보증 세션 길이 ()*glide.zta.high_assurance.session.timeout* 시스템 속성으로 제한됩니다. 높은 보증 세션 시간이 속성 길이를 초과하면 사용자에게 재인증 또는 스텝업 인증을 요청하는 메시지가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

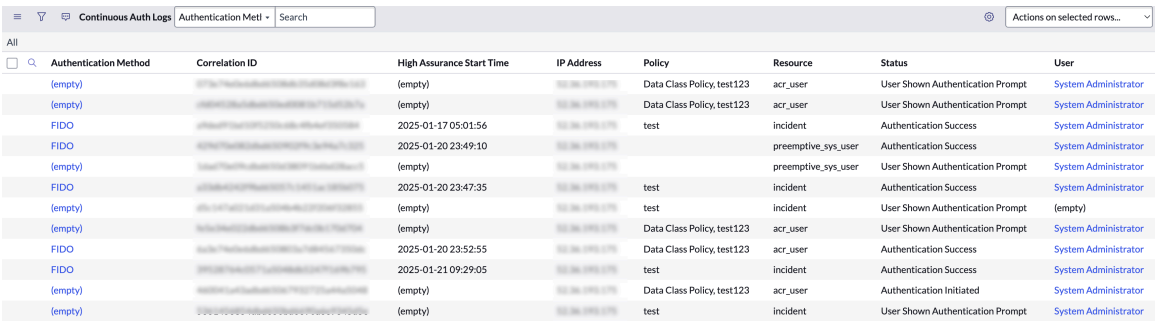
관련 정보

- 높은 보증 연속 인증
- 연속 인증을 위한 사전 작업
- 연속 인증 구성

연속 인증 감사 로그

CA(연속 인증) 로그에 대한 상세 정보를 설명합니다. CA 로그에는 사용자가 수행한 모든 인증 시도가 표시됩니다.

CA 관련 로그 감사 정보는 continuous_auth_log에서 확인할 수 있습니다 . 목록 페이지. continuous_auth_log 입력할 수 있습니다 . **LIST** 를 클릭하여 CA 로그를 봅니다.


Continuous Auth Logs | Authentication Meth | Search | Actions on selected rows...

All

Authentication Method	Correlation ID	High Assurance Start Time	IP Address	Policy	Resource	Status	User
(empty)		(empty)		Data Class Policy, test123	acr_user	User Shown Authentication Prompt	System Administrator
(empty)		(empty)		Data Class Policy, test123	acr_user	User Shown Authentication Prompt	System Administrator
FIDO		2025-01-17 05:01:56		test	incident	Authentication Success	System Administrator
FIDO		2025-01-20 23:49:10			preemptive_sys_user	Authentication Success	System Administrator
(empty)		(empty)			preemptive_sys_user	User Shown Authentication Prompt	System Administrator
FIDO		2025-01-20 23:47:35		test	incident	Authentication Success	System Administrator
(empty)		(empty)		test	incident	User Shown Authentication Prompt	(empty)
(empty)		(empty)		Data Class Policy, test123	acr_user	User Shown Authentication Prompt	System Administrator
FIDO		2025-01-20 23:52:55		Data Class Policy, test123	acr_user	Authentication Success	System Administrator
FIDO		2025-01-21 09:29:05		test	incident	Authentication Success	System Administrator
(empty)		(empty)		Data Class Policy, test123	acr_user	Authentication Initiated	System Administrator
(empty)		(empty)		test	incident	User Shown Authentication Prompt	System Administrator

로그 페이지에는 인증 방법, 상관관계 ID에 대한 정보와 사용자 세션과 관련된 기타 세부 정보가 표시됩니다.

서비스 제공자용 도메인 분리

ServiceNow 플랫폼에서는 서비스 제공자(SP)가 도메인 분리를 사용하여 고객에게 더 빠른 온보딩을 제공하고, 규정 준수를 충족시키고, 데이터를 보호할 수 있습니다. 클라이언트 데이터, 프로세스 및 보고서를 도메인이라는 논리적 그룹으로 분리할 수 있습니다. SP는 누가 어떤 컨텐츠를 보고 액세스하는지 제어합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색



도메인 분리에 대해 알아보기

구성



도메인 분리를 구성합니다.

참조



도메인 분리에 대한 상세 정보를 얻으십시오.

분석



Domain Separation을
분석하는 방법 자세히 알아보기

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 분리 탐색

도메인 분리를 사용하면 데이터, 프로세스 및 관리 작업을 논리적으로 정의된 도메인으로 분리할 수 있습니다.

도메인 분리는 다음과 같은 고객에게 가장 적합합니다.

- 비즈니스 엔터티 간에 절대 데이터 분리(데이터 분리)를 적용해야 합니다.
- 각 도메인에 대한 비즈니스 프로세스 정의 및 사용자 인터페이스를 사용자 지정하는 경우(위임된 관리).
- 단일 인스턴스에서 일부 전역 프로세스와 전역 보고를 유지하는 경우.
- 서비스 제공자, 고객, 파트너 또는 하위 조직 간에 데이터를 분리합니다.
- 고객 간에 프로세스 차이가 작거나 보통입니다.

개별 인스턴스와 비교한 도메인 분리

도메인 분리는 다중 테넌시 지원을 제공하지만 다중 테넌시는 여전히 단일 인스턴스 내에 포함되어 있습니다. 일부 전역 속성, 데이터, 프로세스는 모든 도메인에서 공유됩니다. 예를 들어 시스템의 로그인 페이지에 시스템 로그인 정보 저장 이 있는 것은 전역이며 도메인별로 지정할 수 없습니다.

모든 시스템 속성의 완전하고 완전한 분리가 필요하고 전역 보고 또는 전역 프로세스가 필요하지 않은 경우 별도의 인스턴스가 가장 좋은 옵션입니다.

데이터 분리

도메인의 구성원은 도메인 또는 도메인 계층의 하위 도메인에 포함된 데이터만 볼 수 있습니다. 기본적으로 관리자가 특정 도메인에 할당하지 않는 한 모든 사용자와 레코드는 전역 도메인의 구성원입니다. 사용자나 레코드를 도메인에 할당하면 인스턴스는 사용자의 도메인을 레코드의 도메인과 비교하여 사용자가 레코드를 볼 수 있는지 여부를 결정합니다.

ServiceNow 애플리케이션은 다음과 같은 증분 지원 수준으로 정의됩니다. 이러한 수준은 실제 사용 사례 및 가상 사용자의 관점을 기반으로 합니다.

데이터 분리: 테넌트는 볼 수 있는 권한이 있는 데이터만 볼 수 있습니다. 테넌트는 다른 테넌트 데이터에 대한 액세스 권한을 부여받을 수 있지만 액세스 권한이 없는 경우 테넌트 데이터를 쿼리할 수 없습니다.

UI 분리: 뷰, 목록, 레이블 등과 같은 UI 요소에 대한 테넌트별 환경을 지원합니다.

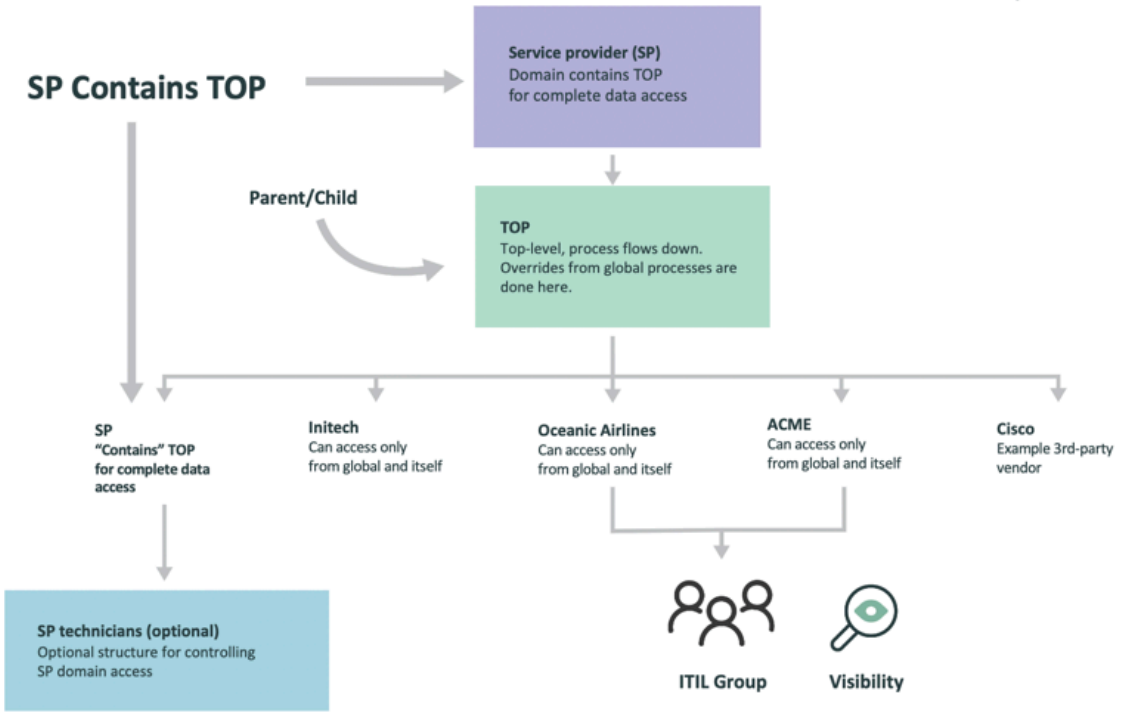
비즈니스 논리 분리: 이메일 알림, 비즈니스 규칙, 클라이언트 스크립트, UI 정책 및 UI 작업과 같은 테넌트별 시스템 정책을 만들 수 있습니다.

계층 구조 모델링: 상위 테넌트가 하위 테넌트 리소스에 액세스할 수 있도록 중첩된 다중 테넌트입니다. 상위 테넌트에 대한 비즈니스 논리는 하위 테넌트에 대해 자동으로 실행되며 모든 수준에서 재정의할 수 있습니다.

테넌트 간 인텔리전스(도메인 범위): 추가 테넌트 데이터에 액세스할 수 있는 테넌트의 데이터, 메타데이터, 비즈니스 논리 및 처리 컨텍스트를 자동으로 처리합니다.

일반적으로 도메인 계층 구조의 상위 수준에서 정의된 데이터는 계층 구조의 하위 수준에 표시되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

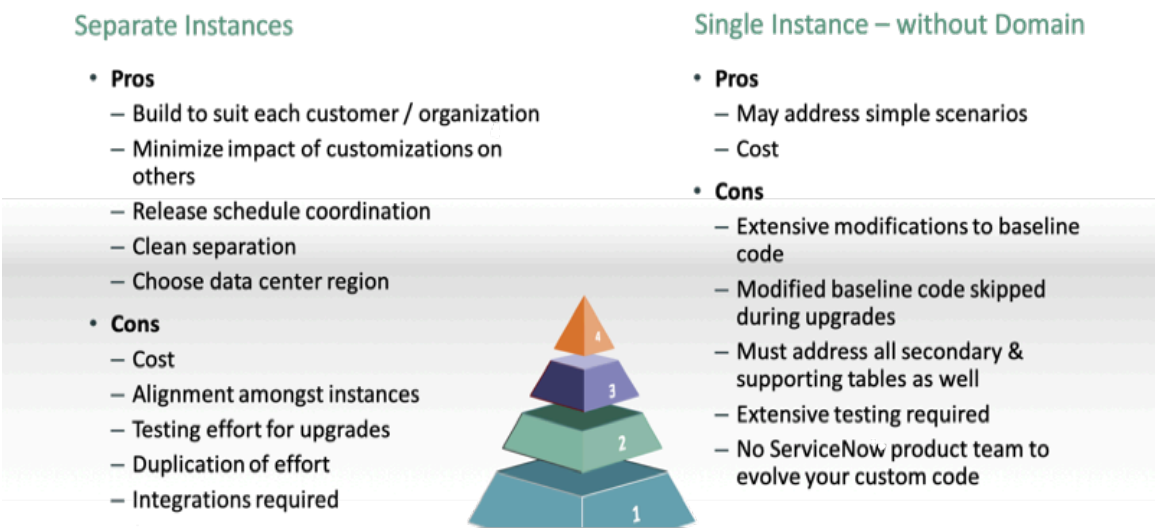


도메인 경로 마이그레이션

도메인 경로는 모든 고객에 대해 사용됩니다. 도메인 번호 매기기는 사용되지 않습니다. 고객 서비스 및 지원 가 업그레이드를 지원할 수 있습니다.

Domain Separation의 대체 앱

개별 인스턴스는 도메인 분리의 일반적인 대안입니다. 이를 통해 고객과 이해 관계자의 요구 사항을 충족하는 데 있어 상당한 유연성을 제공하며 다른 사람에게는 거의 또는 전혀 영향을 미치지 않습니다.



⚠ 경고: 도메인 분리를 활성화하기 전에 담당자에게 문의하여 사용자 환경에 적합한지 확인하십시오. 도메인 분리는 관리 오버헤드 수준을 추가합니다. 비활성화할 수는 있지만 인스턴스에서 제거할 수는 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

서비스 제공자를 위한 도메인 분리 권장 방법

도메인 분리 플러그인

내부 또는 외부 고객에게 위임할 수 있는 구성

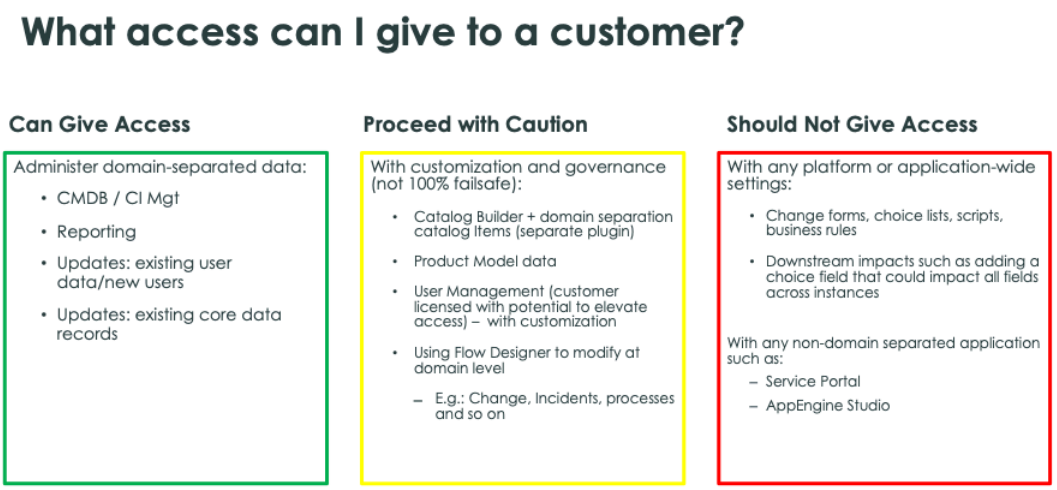
도메인 분리 는 SP(서비스 제공자)가 고객에게 제공하는 서비스를 구성할 수 있도록 설계되었습니다 ServiceNow® . 이 항목에서 자세히 설명하는 몇 가지 영역을 제외하고 고객이 이러한 서비스를 직접 관리할 수 있도록 설계되지 않았습니다.

개요

SP 고객은 라이센스나 다른 고객에게 영향을 주지 않는 도메인 내의 데이터를 안전하게 관리할 수 있습니다. 예를 들어 고객이 새 보고서를 만들거나 구성 항목을 관리하는 것은 안전하지만 동일한 인스턴스에서 다른 고객에게 영향을 줄 수 있는 필드, 선택 사항, 비즈니스 규칙 및 기타 프로세스를 사용자 지정하는 것은 안전하지 않습니다.

ServiceNow 플랫폼의 기본 시스템 관리 역할과 해당 액세스 제어 ServiceNow 는 인스턴스당 단일 관리 팀을 위해 설계되었습니다. 예를 들어 SP의 자원 중 하나에 domain_admin 역할이 부여되어 인스턴스에 대한 모든 도메인 설정을 관리하고 새 도메인을 만듭니다. 도메인별 관리 작업의 경우 SP는 새로운 "고객 관리자" 역할과 액세스 제어를 생성하여 고객에게 특정 액세스 권한을 부여해야 합니다.

다음 이미지는 고객이 안전하게 수행할 수 있는 다양한 범주의 일반적인 관리자 기능에 대한 개요입니다.



🟢 접근 권한을 부여할 수 있음

예제:

- CMDB의 CI 데이터 관리
- 보고서 작성
- 기존 사용자 데이터에 대한 업데이트 또는 역할이 없는 신규 사용자에 대한 업데이트
- 부서, 그룹, 위치, 비용 센터 또는 역할이 없는 새 그룹, 새 부서/비용 센터/위치와 같은 기존 핵심 데이터 기록에 대한 업데이트입니다.

🟡 주의해서 진행

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예제:

- 카탈로그 항목: 고객이 업데이트할 수 있는 고객별 카탈로그 항목을 작성하기 위해 두 가지 기능을 함께 사용할 수 있습니다. 카탈로그 항목에 대한 도메인 분리(도메인 분리 및 Service Catalog)를 사용하면 인스턴스 소유자가 고객의 도메인에 항목을 작성할 수 있습니다. 인스턴스 소유자는 고객이 가격, 설명 및 이미지와 같은 안전한 필드를 업데이트할 수 있는 역할을 만들 수 있습니다. 카탈로그 작성기 (Quebec 릴리스의 새로운 기능)를 통해 SP 관리 팀은 고객에게 안전하게 배포할 수 있는 항목 템플릿을 생성하여 후속 대응적 UI 환경 내에서 도메인 내 새 항목을 생성할 수 있습니다.
- 사용자/그룹 관리: 사용자 기록을 만들고 수정할 수 있는 "고객 관리자" 역할을 만드는 것은 안전하지만 역할을 추가하고 제거하면 보안 및 라이선싱에 영향을 줄 수 있습니다. 기본 시스템에서는 고객이 안전하게 부여할 수 있는 역할을 세분화할 수 있는 방법이 없습니다. 그룹을 만들고 수정할 때도 마찬가지입니다. 그룹 자체를 수정할 수 있지만 역할의 추가 또는 제거를 제어해야 합니다.
- 플로우 디자이너 : ServiceNow 플로우 디자이너 테이블에 대한 프로세스(워크플로우)를 만드는 데 사용되는 빌드 도구입니다. flow_designer 역할은 고객에게 플로우 빌드에 대한 스크립트 없는 액세스를 제공합니다. 계층 구조에서 상위 도메인의 모든 플로우를 읽고 복제할 수 있습니다. 자신의 도메인에서 플로우를 만들고 수정할 수 있습니다. 그러나 이것은 사일로에서 일어날 수 없습니다. 프로세스에 영향을 줄 수 있는 사람은 누구나 거버넌스를 위해 전역 관리 팀에 추가되어야 프로세스가 서로 상쇄되거나 다른 상충이 발생하지 않습니다.

접근 권한을 부여하지 않음

선택 필드의 작동 방식을 이해하면 SP 관리자 팀만 선택 필드를 관리해야 하는 이유를 이해하는 데 도움이 됩니다.

- 선택 필드의 구조: 선택 필드 값은 sys_choice 테이블에 저장되고 테이블, 도메인 및 언어를 기준으로 그룹화됩니다.

  예를 들어, 작업의 상태 필드는 작업을 확장하는 모든 테이블에서 사용할 수 있습니다. 즉, 각 테이블은 고유한 값을 가질 수 있고, 이러한 값을 도메인으로 곱할 수 있으며, 도메인 값은 언어로 곱할 수 있습니다.

  모든 테이블, 도메인 및 언어에서 상태에 대한 모든 값은 상태 필드의 값으로 간주됩니다.

- 선택 필드 변경 작동 방식: 선택 필드가 업데이트되면 해당 필드(테이블, 도메인, 언어)의 모든 값을 사용하여 페이로드가 생성됩니다. 인스턴스에 이 페이로드를 설치하면 필드에 대한 기존 값이 모두 삭제되고 새 값이 로드됩니다. 이렇게 하면 중복 항목이나 더 이상 유효하지 않은 남은 값이 없습니다.

  이러한 이유로 전체 인스턴스에 영향을 미치기 때문에 도메인 분리된 인스턴스의 고객에게 선택 필드를 직접 업데이트할 수 있는 기능을 제공하는 것은 불가능합니다. 또한 프로덕션 인스턴스에서 직접 선택 사항을 업데이트할 수 없는데, 임포트하여 해당 필드에 영향을 주는 업데이트 세트가 기존 선택 사항을 덮어쓰기 때문입니다. 경우에 따라 선택 필드는 프로세스 자체를 구동할 수 있으며, 고객이 해당 필드를 변경하면 중단될 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- 사용자 관리 탐색
- ACL 규칙 생성
- NowLearning의 서비스 제공자 학습 경로
- 서비스 제공자용 도메인 분리
- 서비스 제공자 개념
- 도메인 분리를 위한 애플리케이션 지원
- 도메인 분리 릴리스 정보

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 할당

기본적으로 도메인 분리는 테이블과 해당 확장에 도메인 필드를 추가합니다.

테이블의 딕셔너리 정의에 **sys_domain** 필드를 추가하여 새로 만든 테이블로 도메인 분리를 확장할 수도 있습니다. 기본적으로 시스템 전용 도메인은 플랫폼 및 베이스라인 애플리케이션 테이블을 적절하게 분리합니다.

⚠ 경고: ServiceNow 에서는 예기치 않은 결과가 발생할 수 있으므로 플랫폼 테이블(딕셔너리 항목 [sys_dictionary] 및 딕셔너리 항목 무효화 [sys_dictionary_override] 테이블과 같이 sys_ 프리픽스가 있는 테이블)을 도메인 분리 하지 않는 것이 좋습니다.

각 기록에는 단일 도메인이 할당됩니다. 해당 도메인은 **sys_domain**필드에 저장됩니다. 기본적으로 여러 테이블에 **sys_domain** 열이 있으며 이미 도메인으로 분리되어 있습니다.

sys_domain 필드의 값에는 다음 중 하나에 의해 기록에 할당된 도메인이 포함됩니다.

- 사용자가 속한 회사
- 기록을 작성할 때의 비즈니스 규칙
- 기록을 작성할 때 사용되는 모듈
- 기록을 작성할 때 사용된 양식 템플릿
- 상위 기록의 도메인
- 도메인 담당자 사용자 기록
- 작성한 사용자의 도메인

시스템은 다음 테이블이 도메인으로 분리되는 것을 방지합니다.

- 접근 제어 `[sys_security_acl]`
- 스크립트 포함 `[sys_script_include]`
- 시스템 속성 `[sys_properties]`
- 보안 제외/포함 목록 엔터티 `[sys_security_restricted_list]`
- 딕셔너리 항목 `[sys_dictionary]`
- 딕셔너리 항목 재정의 `[sys_dictionary_override]`

회사에 사용자 할당

관리자는 사용자를 회사에 할당하여 도메인에 빠르게 할당할 수 있습니다. 사용자가 도메인에 할당되면 기록은 자동으로 사용자의 도메인을 상속합니다.

예를 들어, Bow Ruggeri를 ACME 회사에 할당하면 ACME 도메인에 자동으로 할당됩니다. Don Goodliffe를 Initech 회사에 할당하면 Initech 도메인에 자동으로 할당됩니다. 생성한 모든 기록은 해당 도메인에 자동으로 추가됩니다.

비즈니스 규칙을 사용하여 도메인 할당

관리자는 비즈니스 규칙을 사용하여 기록을 만들 때 도메인 값을 자동으로 설정할 수 있습니다. 비즈니스 규칙은 **sys_domain** 필드에 값을 설정해야 합니다. 관리자는 기록의 테이블에 사용할 수 있는 **sys_domain** 열이 있는지 확인해야 합니다. 자세한 내용은 문서를 참조하십시오 서비스 제공자를 위한 도메인 분리 권장 방법.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모듈을 사용하여 도메인 할당

관리자는 **sysparm_domain** URL 매개변수를 사용하여 모듈에서 특정 도메인에 새 기록을 자동으로 할당할 수 있습니다. 관리자는 인수 값이 `#### sysparm_domain=sys_ID`인 모듈을 만들어야 합니다.

양식 템플릿을 사용하여 도메인 할당

관리자는 양식 서식 파일을 사용하여 특정 도메인에 새 기록을 자동으로 할당할 수 있습니다. 관리자는 양식에 **sys_domain** 필드를 추가하고 도메인 값을 선택해야 합니다. 예를 들어 **sys_domain** 필드를 **TOP/ACME** 도메인 으로 설정하면 이 템플릿의 모든 기록이 TOP/ACME 도메인에 자동으로 할당됩니다.

테이블의 도메인 상속

기본적으로 관련 기록은 상위 기록의 도메인을 상속합니다. 예:

- 변경 작업 기록은 상위 변경 요청 기록의 도메인을 상속합니다.
- 문제 기록은 상위 인시던트 기록의 도메인을 상속합니다.

사용자 도메인을 기준으로 자동 도메인 할당

다른 도메인 조건이 적용되지 않으면 기록은 기록을 만드는 사용자의 도메인을 자동으로 상속합니다.

가시성 도메인 및 포함 도메인

가시성 도메인은 특정 사용자 또는 사용자 그룹이 볼 수 있는 내용을 제어합니다. "포함" 도메인은 전체 사용자 도메인이 볼 수 있는 내용을 제어합니다.

가시성 도메인

"가시성 도메인" 요소는 한 도메인의 사용자가 다른 도메인의 기록에 액세스할 수 있는지 여부를 결정합니다. 이 요소를 해당 기록의 관련 목록에 있는 사용자 [sys_user] 및 그룹 [sys_user_group] 기록과 연결합니다. 그룹은 구성원에게 그룹의 가시성 도메인을 부여합니다. 사용자가 그룹을 탈퇴하면 그룹의 가시성 도메인을 잃게 됩니다. 사용자에게 가시성 도메인을 부여하면 ACL(접근 제어 목록) 규칙에 따라 해당 도메인의 기록에 대한 모든 권한이 부여됩니다.

가시성 도메인:

- 사용자와 도메인 간의 관계이며 명시적으로 부여됩니다.
- 하위 도메인이 아닙니다.
- 도메인 선택기의 선택에 의해 제어되지 않습니다. 가시성 도메인에 액세스할 수 있는 사용자는 항상 해당 도메인과 해당 하위 도메인의 데이터를 볼 수 있습니다.

주: 가시성 도메인을 과도하게 사용하는 것은 권장되지 않습니다. 가시성은 사용자가 기록에 액세스할 수 있도록 하는 한 가지 방법이지만 보다 강력한 제어를 위해 포함 도메인을 사용하는 것이 가장 좋습니다.

도메인 포함

일반적으로 상위-하위 관계는 도메인 계층 구조를 정의합니다. 포함 도메인을 사용하면 상위-하위 관계와 관계없이 필요에 따라 도메인을 연결할 수 있습니다. 그러나 도메인 포함은 도메인 데이터에만 대한 가시성을 부여합니다. 프로세스는 포함 관계의 영향을 받지 않습니다.

A 도메인 포함:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 는 다대다, 도메인 간 관계입니다.
- 하위 도메인이 있을 수 있습니다. 도메인을 선택하면 해당 도메인과 해당 하위 도메인의 데이터를 볼 수 있습니다.
- 도메인 선택기의 선택에 의해 제어됩니다.

주: 도메인 기록을 열면 범위가 해당 기록의 도메인으로 설정되므로 하위 도메인만 볼 수 있습니다. 메뉴에서 도메인 범위 전환**(Toggle Domain Scope**)을 선택하여 관련 목록을 채웁니다.

도메인 예시 포함

사용자의 홈 도메인이 A이고 A 도메인에 도메인 B와 C가 포함되어 있으면 모두 피어 도메인이 됩니다. 즉, 사용자는 홈 도메인 A에 있는 동안 도메인 A, B 및 C의 데이터를 볼 수 있습니다. 사용자가 도메인 선택기를 사용하여 도메인을 도메인 B로 변경하면 도메인 B의 데이터만 표시됩니다. 사용자가 도메인 B 또는 도메인 C의 기록과 직접 상호작용하는 경우에는 해당 도메인의 데이터만 표시됩니다.

가시성 도메인 예

도메인 가시성을 사용하여 Don Goodliffe가 Database 도메인에 있고 Bow Ruggeri가 Network 도메인에 있으며 전역 도메인에 인시던트가 없는 경우 Don은 데이터 분리로 인해 Bow의 인시던트에 액세스할 수 없습니다.

그룹 구성원 자격에 따라 가시성 도메인 상속

도메인 테이블을 그룹 [sys_user_group] 테이블로 설정하면 사용자는 그룹 구성원 자격에 따라 가시성 도메인을 상속할 수 있습니다.

관련 정보

쿼리 및 도메인 액세스 포함

서비스 제공자를 위한 도메인 분리 권장 방법

도메인 범위

도메인 범위는 사용자가 접근할 수 있는 것과 접근할 수 없는 것을 정의합니다.

도메인 분리 인스턴스에서 세션을 설정할 때 모든 사용자는 두 개의 도메인 범위를 갖습니다.

- 세션 범위는 사용자의 사용자 기록에 나열된 도메인으로 세션 설정 시 설정됩니다. 사용자는 도메인 선택기에서 세션 도메인 범위를 수동으로 변경할 수 있습니다.
- 기록 범위는 기록의 도메인을 사용하며 기록의 양식을 볼 때 활성화됩니다.

기본적으로 기록 범위는 세션 범위보다 우선하므로 상위 수준 도메인의 사용자는 각 기록의 데이터 및 프로세스 제약 조건을 준수합니다. 그러나 이러한 사용자는 도메인 범위를 확장하거나 축소하여 다른 도메인의 데이터를 표시하거나 숨기도록 선택할 수 있습니다. 예를 들어 SP(서비스 제공자) 도메인의 사용자는 ACME 도메인과 같은 하위 도메인도 볼 수 있습니다. ACME 도메인에서 인시던트 기록을 볼 때 사용자는 도메인 범위를 확장하여 SP 도메인의 값을 표시하거나 도메인 범위를 축소하여 기록의 ACME 도메인과 일치하는 기록 값만 표시하도록 선택할 수 있습니다.

주: 사용자는 도메인 가시성에 의해 명시적으로 부여된 도메인의 데이터에 항상 액세스할 수 있습니다.

domain_expand_scope 사용자 역할을 가진 사용자는 양식의 도메인 범위 **UI** 전환 작업에서 도메인 범위를 선택할 수 있습니다. 기록 범위가 적용되는 경우 UI 작업을 클릭하여 세션 범위로 확장하고 사용자의 도메인 및 하위 도메인에 따라 사용할 수 있는 모든 데이터를 표시합니다. 세션 범위가

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

적용되는 경우, UI 작업을 클릭하여 기록 범위를 축소하고 현재 기록의 도메인과 일치하는 데이터만 표시합니다.

주: 기록이 전역 도메인에 있거나 사용자의 도메인이 기록의 도메인과 일치하는 경우 도메인 범위를 전환하는 UI 작업은 기록에 표시되지 않습니다.

다른 도메인에서 기록 값 선택

여러 도메인을 볼 수 있는 사용자는 기록의 도메인과 다른 도메인에서 기록 값을 선택할 수 있습니다.

예를 들어 서비스 제공자를 위해 일하는 서비스 데스크 에이전트는 특정 인시던트를 자신에게 할당하여 고객을 대신하여 문제를 해결할 수 있습니다. 이렇게 하면 인시던트 기록 자체가 ACME와 같은 하위 도메인과 연결되어 있더라도 인시던트 할당 대상 필드에 SP 도메인의 사용자가 포함될 수 있습니다.

다른 도메인에서 기록 값을 선택해도 기록의 도메인은 변경되지 않습니다. 기록은 원래 도메인을 유지합니다. 사용자가 여러 도메인의 값이 포함된 기록을 볼 때 사용자의 도메인 가시성에 따라 표시되는 내용이 결정됩니다.

기록 값 선택

이러한 조건이 충족될 경우	사용자는 다음과 같은 **UI** 요소에 액세스할 수 있습니다.
사용자는 필드에서 참조되는 현재 기록의 도메인에 액세스할 수 있습니다.	사용자는 다음을 수행할 수 있습니다. • 참조 필드 표시 값을 참조하십시오. 예를 들어, 할당 대상 필드에서 사용자 이름을 확인합니다. • 참조 아이콘에서 관련 기록을 확인합니다. 예를 들어, 할당 대상 필드에서 해당 사용자의 사용자 기록을 볼 수 있습니다. • 표시되는 도메인에서 값을 선택합니다. 예를 들어 SP 및 ACME 도메인에서 사용자를 선택할 수 있습니다.
사용자는 필드에서 참조되는 현재 기록의 도메인에 액세스할 수 없습니다.	사용자는 다음을 수행할 수 있습니다. • 참조 필드 표시 값을 볼 수 없습니다. (Madrid 또는 이후 릴리스에서 도메인 분리가 활성화되었고 사용자가 해당 기록의 도메인에 액세스할 수 없는 경우입니다.) • 기록의 도메인에 있는 값만 선택하십시오. 예를 들어 ACME 도메인에서만 사용자를 선택할 수 있습니다.

도메인 및 관련 회사

도메인 분리를 사용하면 회사 기록에 대해 적용한 변경 사항을 도메인 및 회사에 연결된 기타 기록으로 단계적 전환할 수 있습니다.

기본적으로 시스템은 사용자를 회사와 동일한 도메인에 자동으로 할당합니다. 예를 들어 ACME 회사의 모든 사용자는 자동으로 TOP/ACME 도메인의 구성원이 됩니다.

주: 관리자 역할을 가진 사용자는 자신의 사용자 기록을 변경할 수 있으므로 도메인을 변경할 수 있습니다. 서비스 제공자는 위임된 관리를 사용하지 않도록 설정하거나 승인 프로세스를 설정하여 사용자에게 관리자 역할이 필요한지 확인할 수 있습니다.

회사의 도메인을 변경하면 인스턴스가 자동으로 다음 연결된 기록의 도메인을 회사의 새 도메인과 일치하도록 변경합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 위치
- 부서
- 그룹
- 사용자

주: 인스턴스는 관리되는 도메인 확인란을 선택한 기록의 도메인을 자동으로 변경하지 않습니다.

도메인 비활성화 및 관련 회사

도메인을 비활성화하면 인스턴스가 다음 작업도 자동으로 완료합니다.

- 도메인의 모든 회사를 비활성화합니다.
- 비활성 회사에 할당된 모든 사용자의 로그인을 방지합니다.

주: 비활성 회사의 사용자가 로그인을 시도하면 회사 비활성과 유사한 오류 메시지가 표시됩니다 . `# ##### ## ### ### ####.`

예를 들어, 샘플 데이터에서 ACME 도메인을 비활성화하면 인스턴스도 ACME 회사를 비활성화하고 세 명의 샘플 사용자가 잠깁니다.

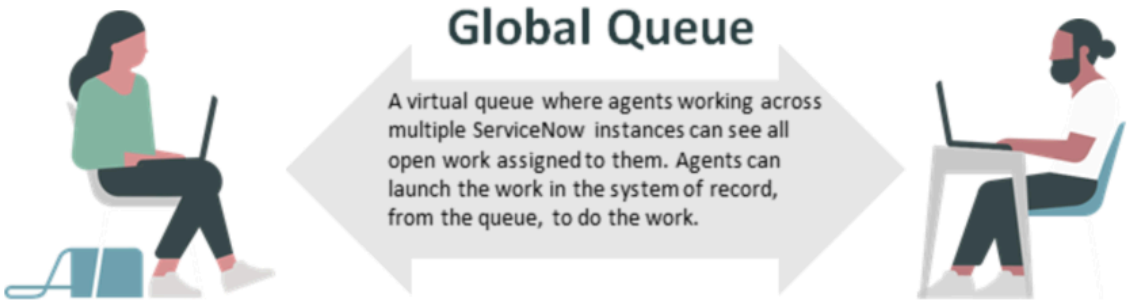
서비스 제공자를 위한 개념

이러한 개념은 기존 ServiceNow 플랫폼 기능과 함께 작동하여 일반적인 사용 사례를 해결하는 데 도움이 됩니다.

전역 큐 **v.2**

전역 큐 개념은 여러 인스턴스에 있는 작업에 대한 단일 가상 뷰를 제공합니다. 이 개념은 작업이나 데이터를 복제할 필요 없이 여러 인스턴스에 상주하는 작업의 이행자 뷰를 제공하는 사용자 지정 애플리케이션을 만듭니다.

개요



여러 시스템에서 작업을 수행하는 에이전트가 있는 서비스 제공자는 데이터를 중앙 인스턴스에 다시 통합하거나 인스턴스 간 "회전 의자"로 통합하는 경향이 있습니다. 이 방법이 적절한 경우도 있지만 빌드하고 유지 관리하는 데 많은 비용과 시간이 소요될 수 있습니다. 또한 이 방법을 통해 공급자는 현재 데이터가 있는 모든 인스턴스에서 GDPR(일반 데이터 보호 규정)과 같은 잠재적인 감사 및 데이터 요구 사항 고려 사항을 충족할 수 있습니다.

전역 큐 v.2를 대안으로 사용할 수 있습니다. 이 방법을 사용하면 에이전트가 로그인한 인스턴스에 유지되는 소버린 데이터 없이 단일 인스턴스에서 할당된 데이터를 볼 수 있습니다. 예를 들어, 클라이언트에 데이터 보존 요구 사항이 있지만 다른 국가의 에이전트가 액세스할 수 있도록 허용하는 경우 공급자는 Global Queue v.2를 사용하여 "24시간 지원체계" 헬프 데스크를 사용할 수 있습니다.

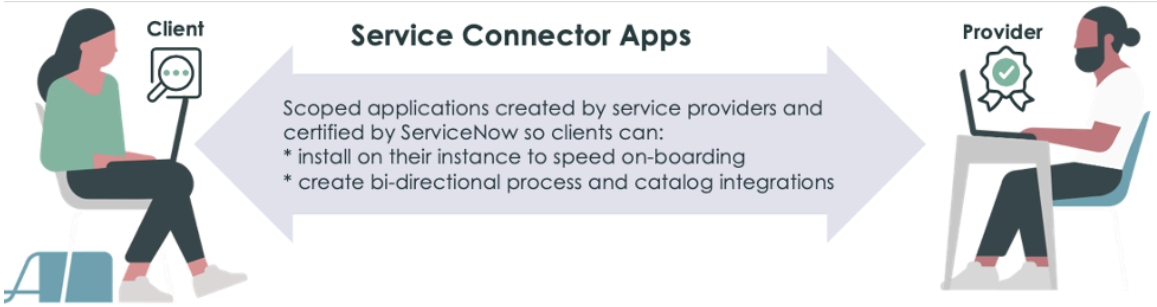
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Knowledge 사이트에서 전역 큐 v.2 개념 증명 에 대해 자세히 알아보십시오ServiceNow.

주: Quebec 릴리스 이후에서는 전역 큐 개념 증명이 전역 큐 v. 2로 업그레이드되었습니다.

서비스 제공자 커넥터

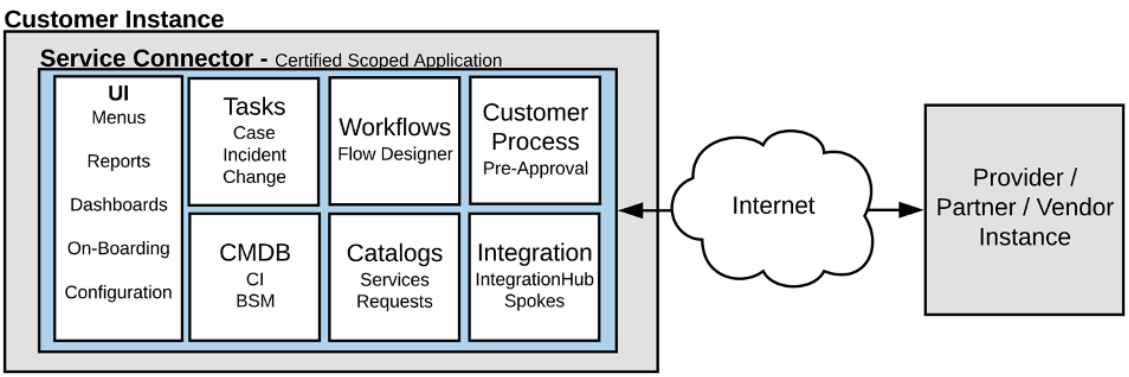
서비스 제공자 커넥터 애플리케이션은 고객이 시스템과 통합하는 데 사용할 스토어 애플리케이션을 만들기 ServiceNow 위한 참조 디자인입니다. 서비스 제공자 애플리케이션을 사용하면 온보딩 속도를 높이고 표준화된 통합을 생성할 수 있습니다.



서비스 커넥터의 이점

서비스 제공자(벤더, 공급업체, 파트너)가 커넥터를 게시하면 고객 온보딩이 더 빨라지므로 청구가 더 빨라집니다. 통합 인스턴스는 생산성을 높이고, 에코시스템의 ServiceNow 가시성을 높이며, 파트너 프로그램의 이점을 제공합니다. 구체적인 이점은 다음과 같습니다.

- 제공과 유지관리에 필요한 서비스 비용을 비롯하여 사용자 지정 통합을 제거합니다.
- 서비스는 해당 ServiceNow 인스턴스 내에서 제공자가 정의하므로 사용자 지정 통합의 복잡성과 비용이 필요하지 않습니다.
- 워크플로우 및 카탈로그 요청을 제공자의 프로세스보다 먼저 고객의 프로세스 및 승인과 동기화할 수 있으므로 고객은 자신의 프로세스를 따를 수 있습니다.
- 제공자의 인스턴스에서 고객에 대해 생성되거나 수정된 데이터(예: CI)는 프로세스에서 보고 사용하기 위해 고객의 인스턴스로 다시 동기화될 수 있습니다.



주요 기능

기능	설명
사용자 인터페이스	서비스 커넥터에는 최소한 다음 UI 구성요소가 포함되어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기능	설명
	• 보고서/대시보드 – 가상 사용자가 미리 정의한 보고서 및 대시보드는 가시성에 도움이 됩니다. • 메뉴 및 모듈 – 고객은 설명이 포함된 메뉴 제공자 **XYZ** 서비스를 통해 애플리케이션을 찾을 수 있어야 합니다. • 역할 – 모든 커넥터에는 고객이 액세스를 제어할 수 있도록 사용자 및 관리자 역할이 필요합니다. 예: "x_snc_xyz_user" 또는 "x_snc_xyz_admin" • 온보딩 – 신속한 온보딩은 우수한 고객 경험에 필수적이며 고객이 라이브로 전환하는 데 전문 서비스가 필요하지 않은 방식으로 플레이북, 안내 설정 또는 카탈로그 항목을 통해 포함되어야 합니다. (전문 서비스를 이용할 수 있지만, 전문 서비스 없이도 온보딩이 가능합니다.) • 구성 – 고객이 달성해야 하는 대부분의 일반 프로세스 구성을 고려하기 위해 데이터 포인트를 프로세스에 구축해야 합니다. 이것은 가능한 한 전문 서비스를 제거합니다. • 문서화 – 철저한 문서화는 고객 만족도와 사용 편의성을 높입니다. • 지원 통합 또는 연락처 정보 – 고객은 문제, 질문 또는 요청에 대해 서비스 제공자와 쉽게 연락할 수 있는 방법이 필요합니다.
작업	서비스 브리지 (레거시) 인시던트, 케이스, 변경, 문제 등과 같은 작업에 애플리케이션을 사용하려면 커넥터에서 미리 정의해야 합니다. 이러한 통합은 최고 수준의 복원력과 성능을 보장하기 플로우 디자이너 위해 빌드됩니다 통합 허브 .
CMDB	적절한 ITIL 프로세스에 필요한 CI와 같은 핵심 데이터 동기화는 제공자와 고객 인스턴스 간에 동기화 상태를 유지해야 합니다.
워크플로우	모든 워크플로는 복원력과 성능을 보장하도록 설계 플로우 디자이너 되어야 합니다.
카탈로그	고객이 요청하는 제공자의 카탈로그는 애플리케이션에 기록 생성 카탈로그로 포함되어야 합니다. 고객 인스턴스의 항목에 의해 생성된 요청은 제공자의 인스턴스와 eBonded되어야 합니다. 제공자의 워크플로우는 요청을 업데이트된 상태로 유지하고 고객의 인스턴스와 다시 동기화합니다.
고객 프로세스	요청을 제공자의 인스턴스와 동기화하는 모든 메커니즘은 요청이 제공자의 인스턴스로 전송되기 전에 고객 프로세스가 요청과 상호 작용할 수 있도록 허용해야 합니다. 제공자가

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기능	설명
	처리하는 동안 필요에 따라 고객의 인스턴스로 승인을 보낼 수 있습니다.
통합	통합은 최고 수준의 복원성과 성능을 보장하기 위해 및 통합 허브 를 사용하여 플로우 디자이너 구축되어야 합니다.

서비스 커넥터에 포함할 수 있는 가능한 구성요소

구성요소	설명
인스턴스 데이터 복제(IDR)	복제가 목표인 경우: • 프로세스 통합에 사용할 수 있지만 복잡성에 따라 너무 엄격할 수 있습니다. 상태 전환에 기반한 통합 논리입니다. • 자세한 내용은 인스턴스 데이터 복제 단원을 참조하십시오
통합 허브	프로세스 통합이 목표인 경우: • 흐름 중간에 복잡하거나 조건부 단계의 일부로 프로세스 중간에 쉽게 삽입 가능 • 자세한 내용은 IntegrationHub 를 참조하십시오.
전역 작업 큐(가상)	작업 페더레이션이 목표이고 데이터를 외부에 저장하는 것이 허용되지 않는 경우: • 에이전트가 여러 ServiceNow 인스턴스에서 작업 중이고 자신에게 할당된 모든 오픈 작업을 확인해야 하는 경우에 사용됩니다. • 반환되는 행은 1,000 미만으로 제한되어야 합니다. • 자세한 내용은 글로벌 작업 큐를 참조하십시오.
원격 테이블	스토리지 없이 외부 데이터를 사용하는 것이 목표인 경우: • 인스턴스를 타사 소스 또는 다른 인스턴스에 연결하여 외부 데이터를 검색하고 선택적으로 메모리에 캐시하는 데 사용됩니다. 데이터는 그룹, 정렬, 집계 및 필터와 같은 읽기 전용 목적으로 인스턴스에서 테이블로 처리됩니다. • 자세한 내용은 원격 테이블 및 스크립트를 사용하여 외부 데이터 검색을 참조하십시오.
플로우 디자이너	프로세스 설계가 목표인 경우

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성요소	설명
	• 단일 설계 환경에서 프로세스를 자동화하는 데 사용됩니다. 프로세스 소유자는 코딩 없이 자연어를 사용하여 승인, 작업, 알림 및 기록 작업을 자동화할 수 있습니다. • 자세한 내용은 플로우 디자이너 문서를 참조하십시오.

Knowledge 사이트에서 서비스 커넥터 개념 ServiceNow 증명에 대해 자세히 알아보십시오.

도메인 분리와 함께 설치되는 구성요소

도메인 분리를 통해 여러 플랫폼 구성요소가 추가되거나 수정됩니다.

역할

역할	설명
domain_admin	도메인을 만들고, 편집하고, 삭제할 수 있습니다.

[sys_domain] 필드에 추가

sys_domain 필드는 다음 테이블에 추가됩니다.

sys_domain 필드가 있는 테이블

테이블
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

작업 테이블 필드

MSP 확장은 작업 테이블에 task_for 필드를 추가합니다. 이 참조 필드는 사용자 테이블을 참조합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그룹 유형에 대한 옵션

MSP 확장은 그룹 테이블의 유형 필드에 몇 가지 새로운 기본 옵션을 추가합니다. 도메인을 지원하는 데 필요한 경우 이러한 유형을 추가하거나 업데이트합니다.

테이블
보안
지원
가시성

비즈니스 규칙

이름	테이블	설명
도메인 - 활성화/비활성화	core_company	회사 중 하나 이상이 활성 상태인 경우 관련 도메인을 활성화합니다. 모든 관련 회사가 비활성 상태인 경우 관련 도메인을 비활성화합니다.
도메인 - 계단식 회사	core_company	회사 도메인을 사용자, 그룹, 부서 및 위치와 동기화된 상태로 유지합니다.
도메인 - 계단식 도메인 - 이메일	sys_email	이메일의 도메인을 첨부 파일과 동기화된 상태로 유지합니다.
도메인 - 계단식 도메인 - 그룹	sys_user_group	그룹의 도메인을 상속된 역할(sys_group_has_role 기록)과 동기화 상태로 유지합니다.
도메인 - 계단식 도메인 - Knowledge	kb_knowledge	지식 문서의 도메인을 관련 피드백과 동기화된 상태로 유지합니다.
도메인 - 계단식 도메인 - 작업	작업	wf_context, wf_executing, wf_history, 첨부 파일, 이메일, task_sla 및 워크플로우, sysapproval_approver 및 워크플로우, sysapproval_group 및 워크플로우에 대한 관련 작업과 도메인을 동기화 상태로 유지합니다.
도메인 - 계단식 도메인 - 사용자	sys_user	사용자의 도메인을 sys_user_grmember(그룹 구성원 자격) 및 역할(sys_user_has_role) 기록과 동기화 상태로 유지합니다.
도메인 - 계단식 도메인 - 버전	wf_workflow_version	도메인을 wf_activity 및 wf_transition 관련 워크플로우 버전과 동기화된 상태로 유지합니다.
도메인 - 회사 비활성화	도메인	도메인이 비활성화되면 관련 회사를 비활성화합니다.
도메인 - 기본값 - 작업	작업	사용자의 도메인에 대한 작업을 기준으로 작업 도메인을 설정합니다. 이 도메인이 전역이면 대신 도메인을 기본값으로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	테이블	설명
도메인 - 기본값 - 사용자	sys_user	도메인이 전역일 경우 사용자의 도메인을 기본값으로 설정합니다.
도메인 - 전역 도메인 기록 허용 안 함	도메인	이름이 전역인 도메인을 만들 수 없도록 차단합니다.
도메인 - 재정의 복사본	sys_app_application	도메인에 대해 애플리케이션이 재정의되면 새 애플리케이션에 대한 해당 모듈의 복사본을 만듭니다.
도메인 - 재정의 복사본	sys_data_policy2	도메인의 데이터 정책이 재정의되면 는 새 데이터 정책에 대한 데이터 정책 규칙의 복사본을 만듭니다.
도메인 - 재정의 복사본	sys_gauge	도메인에 대한 게이지가 재정의되면 새 게이지에 대한 게이지 수의 복사본이 만들어집니다.
도메인 - 재정의 복사본	sys_ui_action	도메인에 대한 UI 작업이 재정의되면 는 새 UI 작업에 대한 UI 작업 뷰의 복사본을 만듭니다.
도메인 - 재정의 복사본	sys_ui_list_control_embedded	도메인에 대해 포함된 목록 컨트롤이 재정의되면 에서는 새로 포함된 목록 컨트롤에 대한 클라이언트 및 서버 스크립트의 복사본을 만듭니다.
도메인 - 재정의 복사본	sys_ui_policy	도메인에 대한 UI 정책이 재정의되면 는 새 UI 정책에 대한 UI 정책 작업의 복사본을 만듭니다.
도메인 - 설정 도메인 - 승인	sysapproval_approver	승인 중인 기록에 따라 도메인을 설정합니다.
도메인 - 도메인 설정 - 첨부 파일	sys_attachment	상위 기록의 도메인을 기준으로 도메인을 설정합니다.
도메인 - 도메인 설정 - CMDB_CI	cmdb_ci	CI의 도메인을 회사의 도메인으로 설정합니다.
도메인 - 설정 도메인 - 부서	cmn_department	부서의 도메인을 회사의 도메인으로 설정합니다.
도메인 - 도메인 설정 - 도메인	도메인	도메인의 도메인을 자체로 설정합니다.
도메인 - 도메인 설정 - 이메일	sys_email	상위 기록의 도메인을 기준으로 도메인을 설정합니다. 이메일의 상위 기록은 인스턴스 필드에 지정된 기록입니다.
도메인 - 도메인 설정 - 피드백	kb_feedback	지식 피드백의 도메인을 지식 문서의 도메인으로 설정합니다.
도메인 - 설정 도메인 - 그룹	sys_user_group	그룹의 도메인을 회사의 도메인으로 설정합니다.
도메인 - 설정 도메인 - 그룹 승인	sysapproval_group	승인 중인 기록에 따라 도메인을 설정합니다.
도메인 - 도메인 설정 - 그룹 역할	sys_group_has_role	그룹 역할의 도메인을 해당 그룹의 도메인으로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	테이블	설명
도메인 - 도메인 설정 - 위치	cmn_location	위치의 도메인을 회사의 도메인으로 설정합니다.
도메인 - 도메인 설정 - 작업 SLA	task_sla	작업 SLA의 도메인을 해당 작업의 도메인으로 설정합니다.
도메인 - 설정 도메인 - 사용자	sys_user	사용자의 도메인을 회사의 도메인으로 설정합니다.
도메인 - 도메인 설정 - 사용자 역할	sys_user_has_role	사용자 역할의 도메인을 해당 사용자의 도메인으로 설정합니다.
도메인 - 설정 도메인 - WF 활동 내역	wf_history	상위 워크플로우 컨텍스트의 도메인을 기준으로 워크플로우 활동 내역 도메인을 설정합니다.
도메인 - 도메인 설정 - WF 컨텍스트	wf_context	참조된 기록의 도메인(있는 경우)을 기준으로 워크플로우 컨텍스트 도메인을 설정합니다.
도메인 - 도메인 설정 - WF 실행 활동	wf_executing	상위 워크플로우 컨텍스트의 도메인을 기반으로 워크플로우 실행 활동 도메인을 설정합니다.
도메인 - 다음에 대한 작업 설정 - 변경	change-request	티켓을 변경 요청으로 변환할 때 요청자 필드를 티켓의 작업 대상 값으로 설정합니다.
도메인 - 작업 설정 - 인시던트	인시던트	티켓을 인시던트로 변환할 때 호출자 필드를 티켓의 작업 대상 값으로 설정합니다.
도메인 - 기본값 확인	도메인	하나의 도메인만 기본 확인란이 선택되어 있는지 확인합니다.
도메인 - 기본 확인	도메인	하나의 도메인에만 기본 확인란이 선택되어 있는지 확인합니다.
Domain Support 플러그인과 함께 설치되는 비즈니스 규칙		
도메인 세트 변경	sys_dictionary	도메인 세트를 현재 도메인으로 설정합니다.
도메인 지원 속성	sys_properties	도메인 쿼리 방법(도메인 경로 또는 도메인 번호 매기기)과 일치하도록 시스템 속성을 설정합니다.

클라이언트 스크립트

클라이언트 스크립트	설명
도메인 - 회사 및 위치 설정 (sys_script)	인시던트 호출자 필드에 변경 사항이 있는지 모니터링합니다. 회사 및 위치 필드에 아직 값이 없는 경우 스크립트는 호출자 기록에서 이 정보를 추가합니다. 회사 및 위치 필드에 이미 값이 있으면 스크립트는 기존 값을 유지합니다.
비활성화된 스크립트	

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라이언트 스크립트	설명
(BP) 위치를 사용자로 설정	인시던트 위치 필드를 모니터링하고 위치 필드를 호출자의 위치로 설정합니다.

관련 정보

서비스 제공자를 위한 도메인 분리 권장 방법

도메인 분리를 위한 애플리케이션 지원

대부분의 ServiceNow 애플리케이션이 기본 시스템에서 도메인 분리를 지원하지만 일부만 지원합니다. 지원되는 일부 애플리케이션에는 도메인으로 구분할 수 있는 데이터 및 관리 설정에 대한 제한 사항이 포함되어 있습니다. 이러한 정의는 실제 사용 사례와 이를 사용하는 사용자의 관점에서 도메인 분리 지원 수준을 설명합니다.

도메인 분리 지원 수준

ServiceNow 도메인 분리를 지원하는 애플리케이션은 데이터 분리 및 데이터 라우팅만 지원하거나, 고급 비즈니스 논리 분리를 지원하거나, 애플리케이션의 테넌트(고객) 수준 관리를 지원할 수 있습니다. ServiceNow 애플리케이션은 다음과 같은 증분 지원 수준으로 정의됩니다.

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

지원 없음

- 도메인 필드가 데이터 테이블에 존재할 수 있지만 데이터를 관리할 논리가 없습니다.
- 이 수준은 도메인으로 구분된 것으로 간주되지 않습니다.

기본

- 비즈니스 논리: 데이터가 애플리케이션의 서비스 제공자(SP) 사용 케이스에 적합한 도메인으로 들어가도록 보장합니다.
- 애플리케이션에서 사용자 인터페이스, 캐시 키, 보고, 롤업, 집계 등은 모두 운영 런타임 시 도메인을 사용합니다.
- 인스턴스 소유자는 여러 테넌트에서 작동하도록 애플리케이션을 설정할 수 있어야 합니다.

샘플 사용 사례: SP가 채팅을 사용하여 테넌트 고객의 메시지에 응답할 때 고객이 SP의 응답을 볼 수 있어야 합니다.

표준

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기본 수준 지원을 포함합니다.
- 비즈니스 논리: 프로세스는 서비스 제공자(SP)가 고객별로 만들거나 수정할 수 있습니다. 사용 사례는 여러 SP 고객이 단일 인스턴스에서 애플리케이션을 올바르게 사용하는 것을 반영합니다.
- 인스턴스 소유자는 특정 애플리케이션에 필요한 대로 테넌트별 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성할 수 있어야 합니다.

샘플 사용 사례: 관리자가 한 테넌트에 대해서는 기록이 닫히지만 다른 테넌트에 대해서는 기록이 닫히지 않는 경우 설명을 필수로 설정할 수 있어야 합니다.

강화

- 기본 및 표준 수준을 포함합니다.
- 서비스 제공자 고객은 데이터 기반 프로세스를 통해 정의된 사용 사례를 기반으로 하는 비즈니스 논리를 수정할 수 있습니다. 이러한 구성은 한 고객의 구성이 다른 고객에 영향을 주지 못하도록 UI 기반 및 페일 세이프로 되어 있습니다.
- 인스턴스 테넌트는 자신을 위한 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성할 수 있어야 합니다. 이 논리와 매개변수는 애플리케이션의 정상적인 기능에 필요합니다.

샘플 사용 사례: 공유 환경의 테넌트 고객이 자신의 도메인 내에서 우선순위를 설정하기 위해 영향, 긴급도, 우선순위 매트릭스를 변경할 수 있어야 합니다.

주: 유효 도메인**(*)**

경우에 따라 플랫폼 기능 또는 애플리케이션은 도메인 프레임워크가 없어도 SP 사용 사례를 효과적으로 지원할 수 있습니다. 이 경우 사용 사례에서 도메인 분리 지원을 자세히 설명해야 합니다. 지원 수준 뒤의 별표(*)는 이러한 종류의 구성을 나타냅니다.

지원되는 기능	기본	표준	Enhanced
기본 시스템 애플리케이션 테이블에 대한 도메인 열이 있습니다.	●	●	●
도메인별 구성은 인스턴스 소유자가 관리합니다.	●	●	●
테넌트 도메인이 자체 애플리케이션 데이터를 관리할 수 있습니다.		●	●
애플리케이션 속성은 필요한 경우 도메인을 인식합니다.		●	●
비즈니스 논리 및 프로세스의 도메인을 인스턴스 소유자별로 분리할 수 있습니다.		●	●
비즈니스 논리 및 프로세스는 테넌트 도메인에서 관리할 수 있습니다.			●

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션별 지원 수준

제품군	애플리케이션	지원 수준
하이퍼오토메이션 및 로우코드	App Engine Studio	지원 안 함
	자동화 센터	기본
	RPA(로보틱 프로세스 자동화) 허브	기본
	ServiceNow 스튜디오	지원 안 함
	Table Builder	기본
	앱 엔진 관리 센터	지원 안 함
	결정 테이블 탐색	표준
	전사적 자원 관리 통합	지원 안 함
	전사적 자원 관리 커스터마이제이션 마이닝	지원 안 함
	넥스트 경험 UI 빌더	기본
고객 서비스 관리	Communities	지원 안 함
	고객 서비스 관리	기본
	릴리스 관리	기초의*
	Order Management for Customer Service Management	기본
	사후 판매 지원	기본
	고객 서비스를 위한 워크포스 최적화의 도메인 분리	기본
DevOps	도메인 분리 및 DevOps 변경 속도	지원 안 함
	도메인 분리 및 DevOps 구성	
Employee Service Management	HR Service Delivery	기초의*
	안전보건	지원 안 함
	계약 관리 프로	기본
	Legal Service Delivery	기본
	PSM(Procurement Service Management)	지원 안 함
	Safe Workplace Suite	개별 애플리케이션 지원 수준에 대해서는 애플리케이션 사이트를 참조하십시오.
	SharePoint Online 검색 커넥터	기본
	Universal Request	기본
	범용 작업	기본
	HR용 워크포스 최적화	기본

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제품군	애플리케이션	지원 수준
Environmental, Social, and Governance Management	Environmental, Social, and Governance Management	기본
현장 서비스 관리	Field Service Management	기본
거버넌스, 리스크 및 컴플라이언스	Business Continuity Management	기본
	거버넌스, 리스크 및 컴플라이언스 (GRC)	기본
	Operational Resilience	기본
산업별 제품		
• 재무 서비스	Financial Services Card Operations	기본
	Financial Services Deposit Operations	
	Financial Services Payment Operations	
	사기를 위한 지능형 서비스	
	재산 및 상해 보험 서비스	
	생명 보험 서비스	
	보험 클레임	
	Financial Services Know Your Customer	
	금융 서비스 신용 운영	
	금융 서비스 문서 프로세서	
• Healthcare and Life Sciences	EMR Help	기본
	Healthcare and Life Sciences Service Management Core	기본
	Pre-Visit Management	기본
	환자 지원 서비스	기본
	Vaccine Administration Management	기본
제조 상업 운영	MCO는	기본
	소매 코어	기본
	소매 작업 관리	기본
• 제조	Manufacturing Process Manager산업 프로세스 관리자	표준
	운영 기술 관리자	표준
	운영 기술 취약성 대응	표준
	운영 기술 관리자	표준

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제품군	애플리케이션	지원 수준
IT Asset Management	Cloud Insights	지원 안 함
	Hardware Asset Management	Enhanced
	소프트웨어 자산 관리	Enhanced
	Enterprise Asset Management	표준
전략적 포트폴리오 관리	Agile 개발	기초의*
	Alignment Planner Workspace	기본
	Application Portfolio Management	기본
	비용 관리	지원 안 함
	요구 관리	기본
	재무 관리	지원 안 함
	Investment Funding	기본
	프로젝트 포트폴리오 관리	기초의*
	릴리스 관리	기초의*
	SAFe(스케일드 애자일 프레임워크)	기초의*
	Test Management	기초의*
	목표 프레임워크	기본
IT Operations Management	Cloud Provisioning and Governance	기본
	에이전트 클라이언트 수집기	기본
	검색	표준
	Event Management	기본
	ITOM용 서비스 운영 작업 공간	기본
	Health Log Analytics	기본
	메트릭 인텔리전스	기본
	Service Mapping	기본
	Cloud Migration Assessment	기본
	작업 라이브러리	지원 안 함
	클라우드 구성 거버넌스	지원 안 함
	태그 거버넌스	기본
	클라우드 인사이트 청구	지원 안 함
	Cloud Provisioning and Governance: Google Cloud	기본
	Cloud Provisioning and Governance Terraform	기본

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제품군	애플리케이션	지원 수준
	클라우드 운영 작업 공간	기본
	클라우드 디스커버리	표준
IT Service Management	벤치마크	지원 안 함
	변경 관리	기본
	코칭	기본
	지속적 개선 관리	기본
	계약 관리	지원 안 함
	경비 라인	지원 안 함
	Incident Communications Management	표준
	인시던트 관리	표준
	Facilities Service Management	표준
	인시던트 관리	표준
	당직 일정 관리	표준
	자산 관리	기본
	문제 관리	표준
	구매	표준*
	제품 카탈로그	표준
	요청 관리	표준
	서비스 카탈로그	표준
	Service Level Management	기본
	서비스 포트폴리오 관리	기초의*
	사이트 신뢰성 운영	기초의*
	작업 중단	기본
	도메인 분리 및 벤더 관리 작업 공간	지원 안 함
	워크업 경험	기본
Mobile 구성 및 탐색	모바일	기본
Now Intelligence	대시보드	기본
	Performance Analytics	Enhanced
	Process Optimization	기본
	보고	기본
	User Experience Analytics	기본
The Now Platform	관리	
	도메인 분리 및 에이전트 채팅	표준

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제품군	애플리케이션	지원 수준
	Now Platform 기능	
	사용자 인터페이스	
	Advanced Work Assignment	표준
	AI Search	검색은 인덱싱된 레코드의 도메인 제한을 존중합니다.
	App Engine Studio	지원 안 함
	Application Management	지원 안 함
	평가	표준
	Automated Test Framework	표준*
	ServiceNow 음성 기능	
	코드 서명	기본 지원
	Contextual Search	표준
	Configuration Management(CMDB)	표준
	콘텐츠 관리 시스템	지원 안 함
	자격 증명 및 연결	표준
	Data Certification	기초의*
	데이터 분류	Enhanced
	데이터 개인정보 보호	지원 안 함
	데이터 관리	기초의*
	위임된 개발	지원 안 함
	Dependency Views	기본
	문서 서비스	지원 안 함
	Dynamic Translation	기본
	Edge Encryption	기본 지원
	외부 콘텐츠 커넥터	지원 없음*
	필드 암호화	지원 안 함
	필드 암호화 엔터프라이즈	지원 안 함
	키 관리를 사용한 클라우드 암호화	기본 지원
	필드 표준화	지원 안 함
	플로우 디자이너	표준*
	안내 설정	지원 안 함
	도메인 분리 및 통합 허브	표준*
	외부 공급업체 애플리케이션 및 데이터 소스와의 통합	기본+표준
	Knowledge Management	표준

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제품군	애플리케이션	지원 수준
	메시징 서비스	지원 안 함
	Managed Documents	지원 안 함
	MetricBase	기본
	천연 세탁 이해	기본+표준
	알림	표준
	ODBC 드라이버	기초의*
	오케스트레이션	표준*
	Password Reset	표준
	Platform Security	도메인 분리 방문 페이지
	데이터 개인정보 보호	지원 안 함
	예측 인텔리전스	표준
	사전 예방적 트리거	기본
	Process Automation Designer	기본
	원격 테이블	지원 안 함
	일정	기본
	스크립트 디버거	기본
	검색 제안	지원 안 함
	Service Portal	지원 안 함
	서비스 그래프 커넥터	지원 안 함
	도메인 분리 및 사이드바	표준
	상태 플로우	지원 안 함
	Subscription Management	기초의*
	설문조사 관리	기초의*
	작업 인텔리전스	지원 안 함
	도메인 분리 및 시간 카드	기초의*
	UI Builder	표준
	가상 에이전트	기본
	Visual Task Boards	기본
	웹 서비스	표준*
	Workflow	표준*
	작업 공간	표준
보안 운영	Configuration Compliance	표준
	Configuration Data Management	기본
	IBM QRadar Offense Ingestion	기본

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제품군	애플리케이션	지원 수준
	Microsoft Graph 보안 API 경보 수집 통합	기본
	Security Incident Response	표준
	Threat Intelligence	표준
	Vulnerability Response	표준
Service Management	Facilities Service Management	표준
	계획된 유지보수	표준*
	사전 예방적 트리거	기본
	NOW 코드 편집기	지원 안 함
	ITSM용 워크포스 최적화	기본
	벤더 관리 작업 공간	기본

서비스 제공자를 위한 도메인 분리 권장 방법

애플리케이션 및 서비스에 대한 도메인 분리를 만들고, 구현하고, 유지관리할 수 있습니다.

도메인 기본 사항

도메인 분리(멀티테넌트 플랫폼 아키텍처라고도 ServiceNow 함)를 사용하면 테넌트 간 인텔리전스를 사용하여 계층 구조 모델링을 지원하는 단일 고객 인스턴스에서 애플리케이션 데이터, 사용자 인터페이스 및 비즈니스 논리를 분리할 수 있습니다. 비즈니스 논리는 도메인 분리가 구성되는 방식과 구성에 영향을 주는 규칙을 설명합니다.

도메인 분리 여정을 시작하기 전에 따라야 할 몇 가지 모범 사례는 다음과 같습니다. 원하는 주제를 선택하거나 이미지 아래의 링크를 클릭하여 순서대로 팔로우합니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 분리 설명

도메인 분리를 사용하면 애플리케이션 데이터, UI 및 비즈니스 로직(예: 규칙 또는 워크플로우)을 단일 고객 인스턴스에서 분리할 수 있습니다. 이러한 요소를 논리적으로 정의된 도메인으로 분리하면 애플리케이션을 사용하는 모든 고객에 대한 특정 계층 구조가 지원됩니다.

도메인 기본 사항

멀티테넌트 플랫폼 아키텍처라고도 ServiceNow 하는 도메인 분리는 인스턴스 관리에 상당한 오버헤드를 추가합니다. 하지만 도메인 분리를 올바르게 사용하면 효율성을 개선하고, 보안을 강화하며, 고객 인스턴스의 성능을 높일 수 있습니다.

시스템 속성 및 테이블 스키마와 같은 일부 글로벌 표준 및 속성은 테넌트별로 구분할 수 없습니다.

도메인 분리를 시작하기 전에 다음 지침을 읽어보세요.

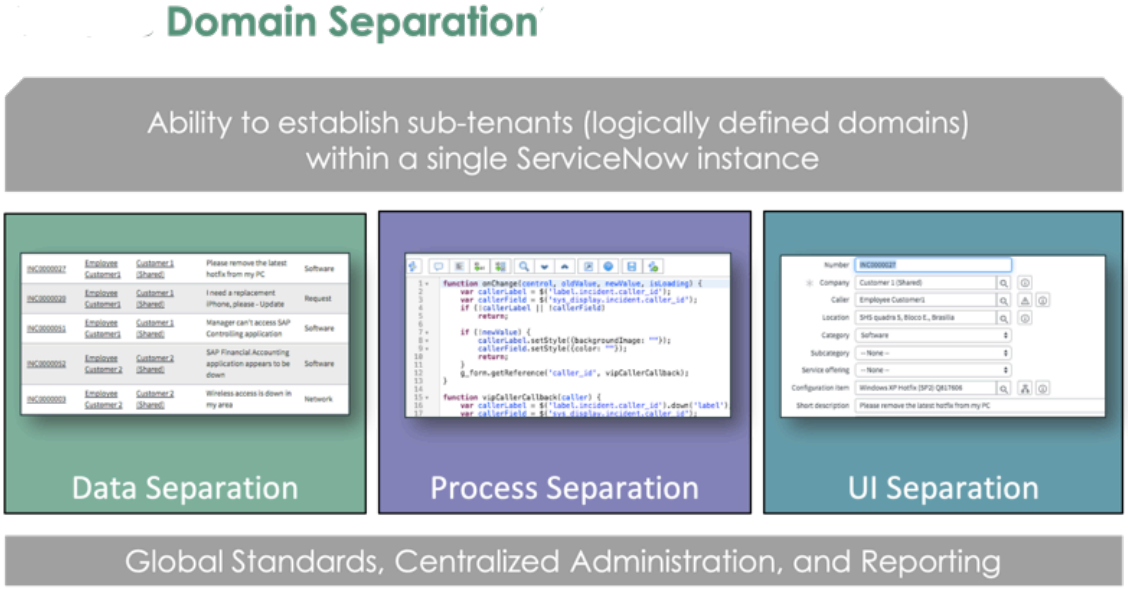
도메인 분리로 수행할 수 있는 작업

- 데이터 분리: 도메인의 테넌트가 볼 수 있는 권한이 있는 데이터만 볼 수 있도록 합니다. 테넌트는 다른 테넌트 데이터에 대한 액세스 권한을 부여받을 수 있지만 액세스 권한이 없는 테넌트 데이터는 쿼리할 수 없습니다.
  - 데이터 기록을 업데이트하면 업데이트 세트 기록이 생성되지 않습니다.
  - 통합에 사용되는 고객 계정을 포함한 사용자는 액세스 권한이 있는 도메인의 데이터만 볼 수 있습니다.
  - 고객, 에이전트 및 이행자는 지원하는 고객 및 조직과 관련된 데이터를 볼 수 있습니다.
- UI 분리: 뷰, 목록, 레이블 등과 같은 UI 요소에 대한 테넌트별 환경을 지원합니다.
  - 애플리케이션 메뉴, 목록, 양식 및 대시보드를 포함한 브라우저 기반 사용자 인터페이스를 재정의할 수 있습니다. 기본 프로세스 논리를 유지하면서 특정 도메인 또는 도메인 집합에 대해 사용자 지정할 수도 있습니다.
  - 서비스 제공자는 개별 고객의 요구에 맞게 표시된 브랜딩 및 UI 요소를 변경할 수 있습니다.
- 비즈니스 논리 분리: 이메일 알림, 비즈니스 규칙, 클라이언트 스크립트, UI 정책 및 UI 작업과 같은 테넌트별 시스템 정책을 만듭니다.
- 계층적 모델링: 상위 테넌트가 하위 테넌트 리소스에 액세스할 수 있도록 여러 테넌트를 중첩합니다. 상위 테넌트에 대한 비즈니스 논리는 하위 테넌트에 대해 자동으로 실행되며, 모든 수준에서 재정의할 수 있습니다.
- 테넌트 간 인텔리전스: 추가 테넌트 데이터에 액세스할 수 있는 테넌트의 데이터, 메타데이터, 비즈니스 논리 및 처리 컨텍스트를 자동으로 처리합니다.

도메인 분리 개요

다음 그래픽에서는 데이터 분할, 프로세스 및 UI 분리를 보여줍니다. 이러한 개념은 권장 사례 섹션에서 자세히 설명합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

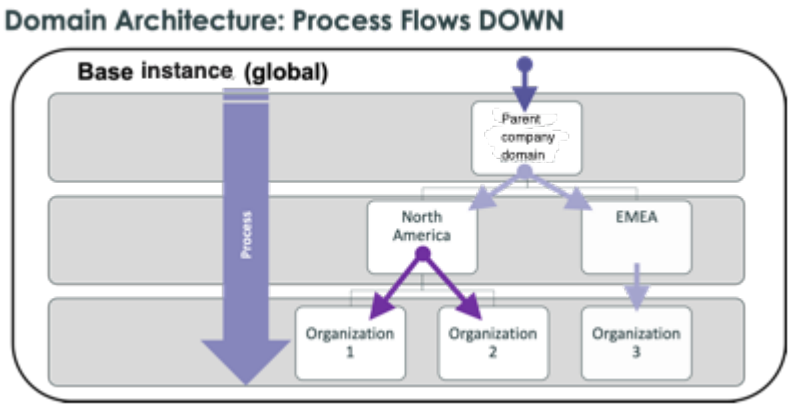


도메인 아키텍처

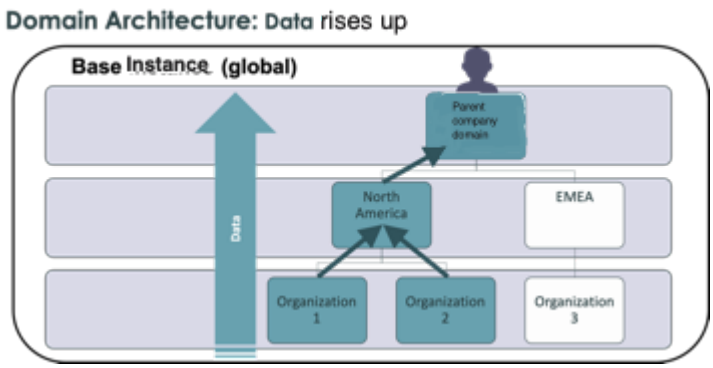
사용자 기록에는 사용자의 홈 도메인을 나타내는 도메인 값이 할당됩니다. 사용자는 상위 도메인, 피어 도메인 또는 계층 구조의 다른 분기에 있는 도메인의 데이터를 액세스할 수 없습니다.

추가 도메인 가시성을 부여하는 고급 옵션에 대해서는 를 참조하십시오 쿼리 및 도메인 액세스 포함 .

다음 다이어그램에서는 아키텍처 프로세스가 하위 도메인으로 어떻게 진행되는지



보여줍니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 분리 가치 제안

도메인 분리를 통해 서비스 제공자는 고객에게 효율적이고 안전하게 오퍼링을 제공하는 멀티테넌트 인스턴스 아키텍처를 구축할 수 있습니다. 강력한 범용 프로세스 표준, 데이터 기반 프로세스 설계, 엄격한 관리 및 중앙 집중식 관리는 이러한 이점을 극대화하는 데 도움이 됩니다.

도메인 분리의 이점

도메인의 테넌트는 빠른 투자 수익률, 낮은 관리 오버헤드, 인스턴스 소유자가 제공하는 비즈니스 서비스 활용의 이점을 누릴 수 있습니다.

다음은 이러한 이점에 대한 간략한 보기입니다.

인스턴스 소유자	도메인 테넌트
서비스 제공자 직원 생산성	보안 강화
프로세스 델타만 유지됨	사전 구축된 프로세스 및 기능
관리 효율성	필요한 직원 감소
클라이언트 통합 감소	빠른 온보딩
업그레이드 가능성 및 확장성	최신 릴리스의 활용
데이터 분리	인스턴스 소유자가 제공하는 서비스
전역 보고	

도메인 분리의 정의

도메인 분리(멀티테넌트 플랫폼 아키텍처라고도 ServiceNow® 함)를 사용하면 테넌트 간 (고객) 인텔리전스를 사용하여 계층적 모델링을 지원하는 단일 고객 인스턴스에서 애플리케이션 데이터, UI 및 비즈니스 논리를 분리할 수 있습니다.

도메인 분리의 속성

도메인으로 구분된 ServiceNow 애플리케이션은 다음 속성으로 정의됩니다.

데이터 분리

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

고객이 볼 수 있는 권한이 있는 데이터만 볼 수 있습니다. 고객은 다른 고객 데이터에 대한 액세스 권한을 부여받을 수 있지만 액세스 권한이 없는 경우 고객 데이터를 쿼리할 수는 없습니다.

UI 분리

뷰, 목록, 레이블 등과 같은 UI 요소에 대한 고객별 경험을 지원합니다.

비즈니스 논리 분리

이메일 알림, 비즈니스 규칙, 클라이언트 스크립트, UI 정책 및 UI 작업과 같은 고객별 시스템 정책을 지원합니다.

계층적 모델링

상위 테넌트(고객)가 하위 고객 자원에 액세스할 수 있도록 중첩 다중 테넌트를 지원합니다. 상위 고객에 대한 비즈니스 논리는 하위 고객에 대해 자동으로 실행되며 모든 수준에서 재정의할 수 있습니다.

고객 간 인텔리전스(도메인 범위)

추가 테넌트 데이터에 액세스할 수 있는 테넌트의 데이터, 메타데이터, 비즈니스 논리 및 처리 컨텍스트를 자동으로 처리합니다.

도메인 분리 계층 구조

프로세스와 워크플로우를 추적하기 위해 도메인 아키텍처를 정의할 때 계층 구조를 생성합니다.

샘플 도메인 분리 계층 구조

다음 다이어그램은 도메인 아키텍처를 정의하는 데 좋은 출발점입니다. TOP 도메인과 하위 도메인 간의 관계와 프로세스, 데이터, 비즈니스 규칙이 상위 도메인과 하위 도메인에 미치는 영향을 보여줍니다.

- 다음 예시에서는 TOP가 프로세스 도메인입니다. 사용자를 포함해서는 안됩니다. 인스턴스 소유자가 개발하는 새로운 프로세스와 전역 도메인에서 이러한 프로세스를 재정의하는 프로세스는 오히려 TOP에 포함되어야 합니다.
- SP(서비스 제공자)만이 기본 도메인에 액세스할 수 있습니다. 이 도메인에는 활성 사용자가 포함되지 않습니다. 올바른 도메인에 재할당해야 하는 "손실"된 데이터만 포함되어 있습니다.

  주: 데이터가 특정 도메인에 할당되지 않은 경우 기본 도메인으로 이동합니다. 일시적으로 "손실"되어 올바른 도메인에 할당되어야 합니다.

- 도메인이 없는 작업과 사용자는 도메인을 만들거나 업데이트할 때 자동으로 기본 도메인에 배치됩니다. 이 기록에 대한 기본 옵션을 해제하거나 다른 도메인 기록에서 기본 옵션을 선택하여 해당 작업을 재정의할 수 있습니다. 아직 기본 도메인을 설정하지 않은 경우 도메인이 없는 작업과 사용자는 전역 도메인으로 이동합니다.
  - 인스턴스를 사용하는 동안에는 도메인 간에 데이터를 옮기지 마십시오.
  - 데이터가 기본 도메인에 위치하게 된다면 처리할 구성 또는 절차적 문제가 있다는 뜻입니다.

전역 도메인이 없기 때문에 이 다이어그램에는 "전역"이라는 단어가 없습니다. "전역"은 기록에 도메인이 없음을 의미함을 기억하십시오.

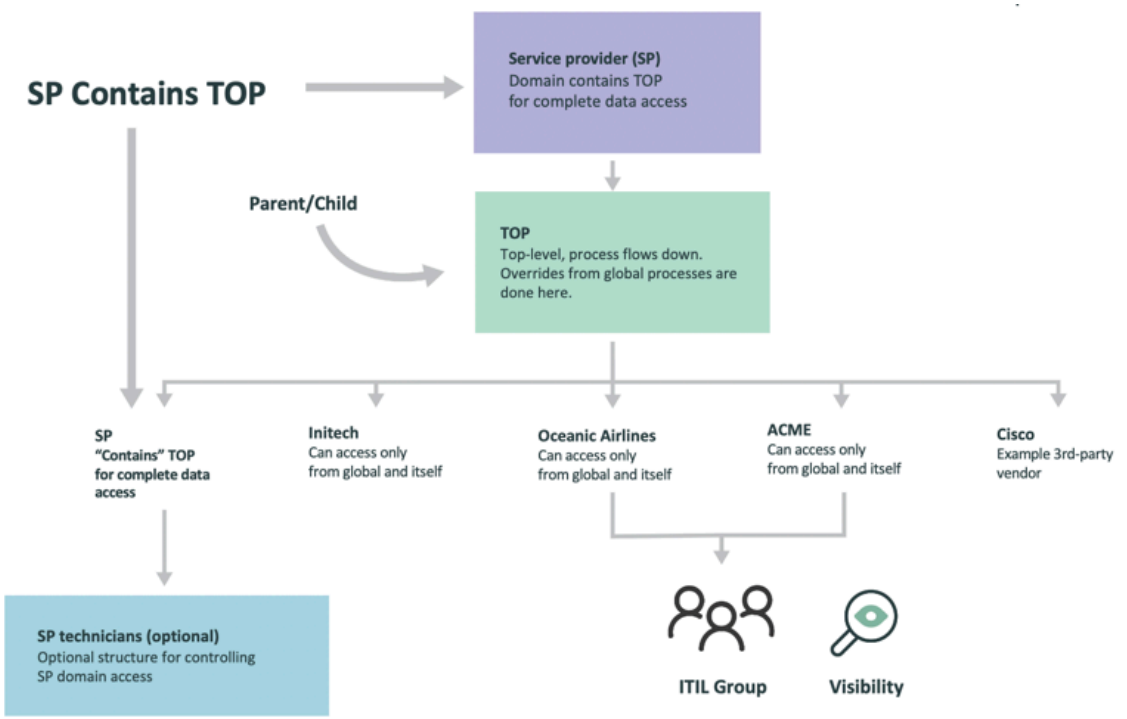
예를 들어 테이블에 도메인 필드가 없으면 테이블에 모든 전역 기록이 포함된다는 것을 의미합니다. 테이블에 도메인 필드가 있으면 도메인이 없는 모든 기록이 전역 도메인임을 의미합니다.

도메인 필드에 "전역"이라는 단어가 표시됩니다. 기록에 도메인이 없으면 자동으로 여기에 배치됩니다.

전역 기록은 보안 구성으로 제한되지 않은 한 인스턴스의 모든 사용자가 사용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 기본 도메인을 사용하여 기록이 전역 기록이 없어야 하는 테이블의 전역 도메인에 배치되지 않도록 합니다.
- 그런 다음 인스턴스 소유자는 기본 도메인에서 기록을 분류하여 올바른 도메인으로 이동해야 합니다.



도메인 계층 구조

- 상위/하위: 영향을 받는 프로세스 및 데이터
  - 프로세스 흐름을 기반으로 하는 설계입니다.
  - 상위 도메인은 하위 도메인의 모든 데이터에 접근할 수 있습니다.
- "Contains" 도메인: 데이터만 영향을 받습니다. 예를 들어 다이어그램의 SP에 TOP를 포함시켜도 SP의 프로세스가 TOP 도메인에서 하향식으로 실행되지 않습니다.
  - 특정 도메인에 대한 전용 액세스가 필요한 그룹의 개인에게 데이터 액세스 권한을 부여합니다.
  - 대규모 도메인 및 데이터 세트에서 성능 문제를 일으킬 수 있는 데이터베이스 쿼리에 추가할 원인 또는 조건을 포함합니다.
- 가시성: 접근 권한을 제공하면 사용자에게 항상 표시되는 계층 구조입니다. 데이터만 영향을 받으며, 프로세스는 영향을 받지 않습니다.
  - 상위 및 하위 계층 구조를 구축할 때 접근 권한이 없는 도메인에 도메인의 데이터 접근 권한을 부여합니다.
  - 가시성이 있는 도메인의 모든 데이터를 사용자가 작업 중인 레코드에 관계없이 항상 볼 수 있도록 합니다.

> **주:** 가시성은 원하지 않는 전체적인 접근 권한을 허용할 수 있으므로 자주 사용하지 마십시오.

도메인 계층 구조 정의의 기본 원칙

도메인 분리의 제한되지 않은 사용 사례와 및 제한된 사용 사례입니다.

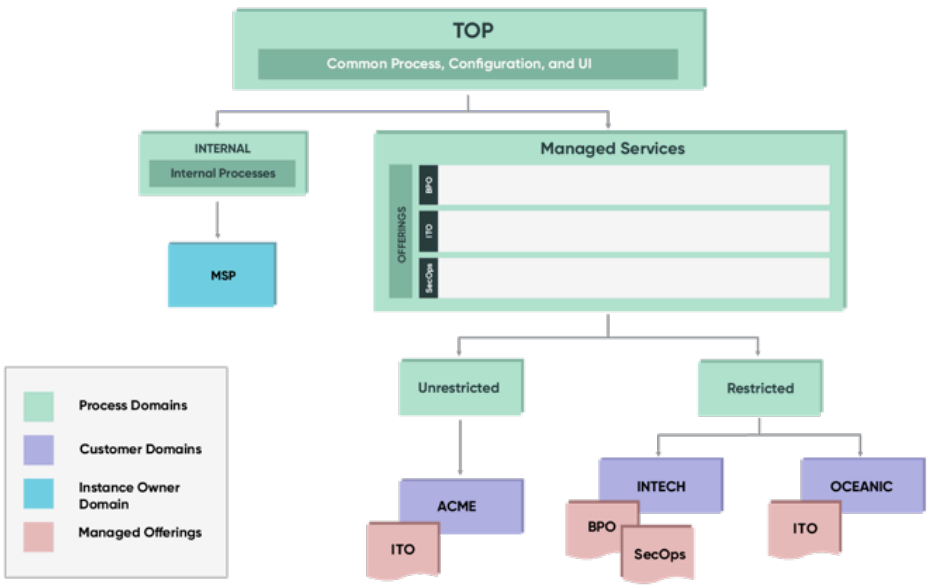
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다수의 SP에는 도메인에 대한 액세스가 엄격하게 규제되어야 한다고 암시적으로 언급하는 고객이 있으며, 이로 인해 TOP 도메인에서 "Contains" 기능의 사용이 제한됩니다. 다음 다이어그램에서는 도메인을 Restricted 도메인과 Unrestricted 도메인으로 나누어 이 규정을 완화하는 방법을 설명합니다.

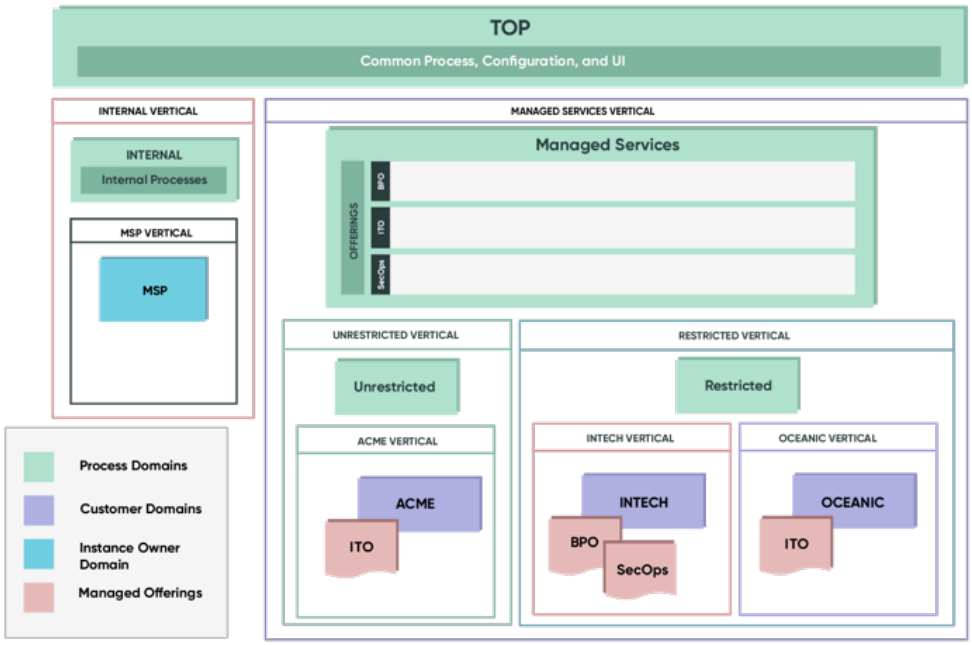
1. 고객은 도메인 분리 계층 구조의 특정한 "수직 계열"에 있습니다. 즉, 고객은 자신의 도메인 및 계층 구조상의 모든 상위 도메인에 정의된 프로세스만을 소비합니다. 도메인에서 정의된 프로세스 중 수식선상 상위-하위 구조에 없는 모든 프로세스는 적용되지 않습니다.

   주: 고객 또는 "테넌트"는 서로 완전히 분리된 독립체이며, 서로 자원을 공유하는 부서 또는 비즈니스 단위와는 다릅니다.

2. 슈퍼 수직 계열(Restricted, 관리자 서비스 등)은 고객이 그 중 하나에만 속하는 경우에만 허용됩니다.
3. 모든 고객들에게 수평적으로 제공되어야 하는 서비스, 제품, 또는 제안은 별도의 도메인 계층 구조 내에서 정의되지 않습니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



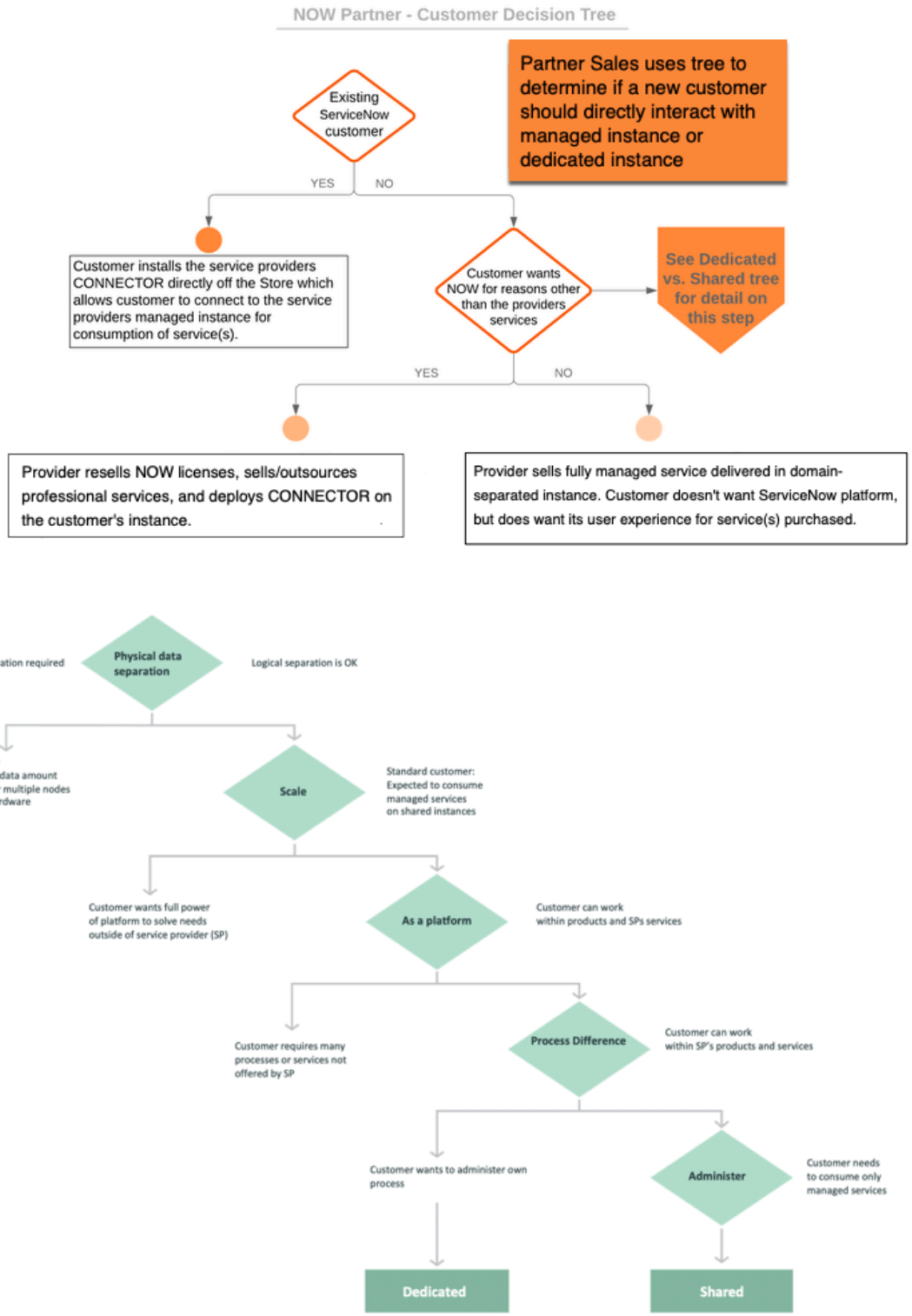
다음은 몇 가지 단순한 사용 케이스입니다.

- TOP 아래에 Unrestricted 및 Restricted라는 두 가지 도메인을 만듭니다.
  - SP 가시성 제한이 없는 고객의 경우, 고객 및 해당 도메인을 Unrestricted 아래에 배치합니다.
  - 이 요구 사항이 있는 고객의 경우 고객과 해당 도메인을 Restricted 아래에 배치합니다.
- 그러면 시스템 관리자가 효율적이고 대상화된 방식으로 "포함" 및 "가시성" 기능을 사용할 수 있습니다.
  - Unrestricted에 "contains"를 적용하여 하나의 "contains"가 대부분의 고객에게 가시성을 부여할 수 있도록 합니다.
  - "도메인 가시성 그룹"을 사용하는 도메인 가시성을 필요에 따라 특정 도메인에 적용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

고객 의사 결정 트리

다음 다이어그램은 사용자에게 적합한 계층 구조 모델을 선택하는 방법을 설명합니다. 도메인 구조에서 원하는 프로세스와 기능에 따라 별도의 계층 구조, 하이브리드 또는 공유 계층 구조를 선택할 수 있습니다.



계층 구조 아키텍처에 대한 자세한 내용은 서비스 제공자 참조 아키텍처 문서를 참조하십시오.

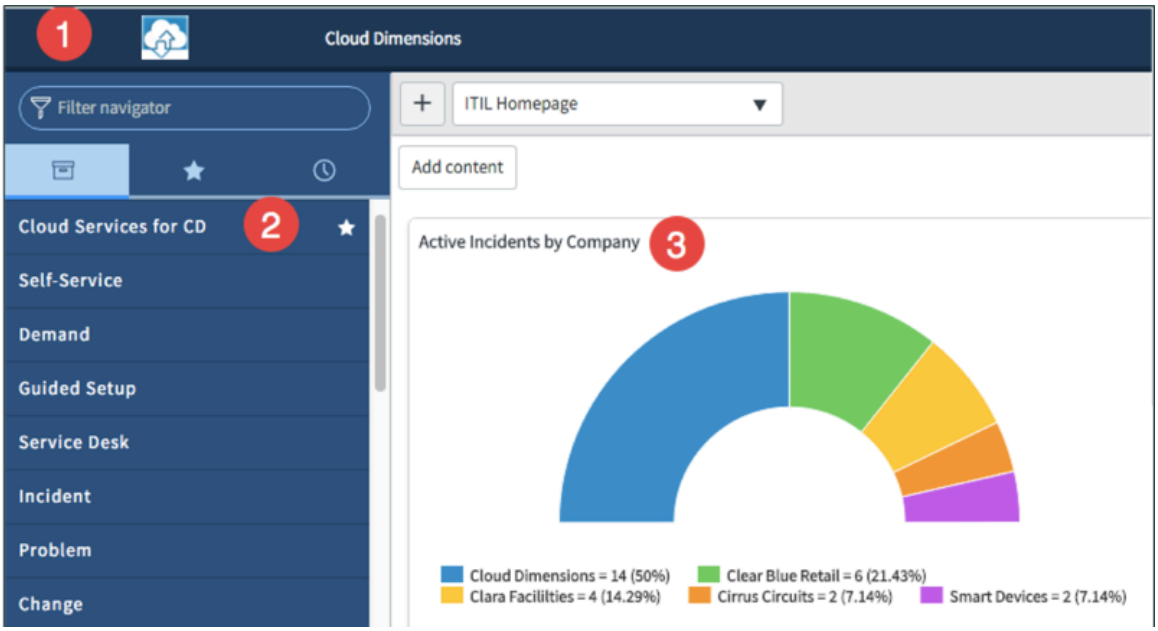
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

컨텍스트 및 도메인 분리

사용자가 목록 뷰, 홈페이지, 보고서, 지식 문서를 탐색할 때 사용자 세션의 컨텍스트에 따라 프로세스, 데이터 및 UI(사용자 인터페이스)가 결정됩니다. 컨텍스트는 생성하는 프로세스, 설정하는 비즈니스 규칙, 워크플로우 및 기타 요인에 의해 결정됩니다.

사용자 세션 컨텍스트

사용자 프로파일, 그룹, 회사 기준 등 여러 요인이 사용자 세션의 컨텍스트를 결정합니다. 다음 다이어그램에서는 회사가 만든 인시던트가 컨텍스트의 일부임을 알 수 있습니다.



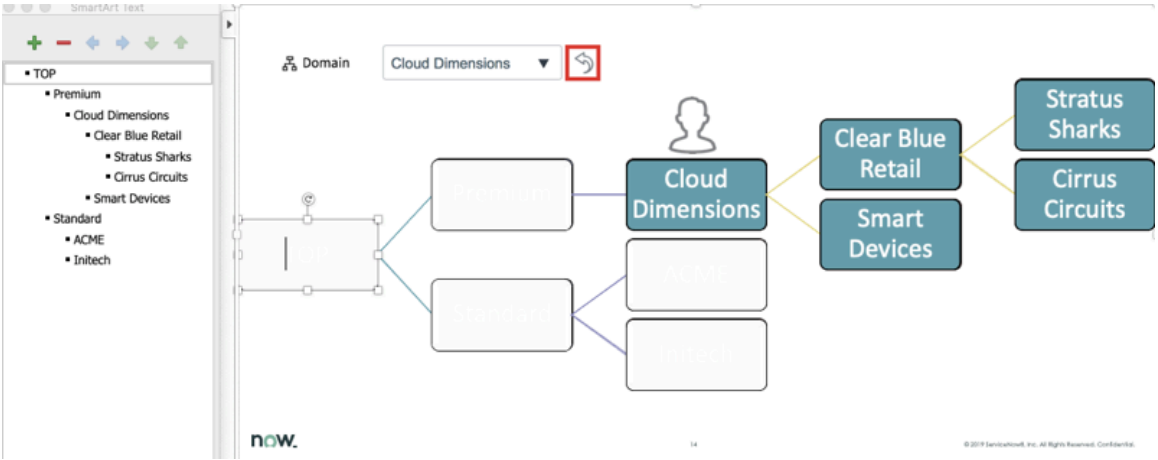
이 예시의 사용자는 Cloud Dimensions의 홈 도메인을 가지고 있습니다.

1. 브랜딩은 Cloud Dimensions 도메인 및 회사 기록의 설정을 반영합니다.
2. 애플리케이션 내비게이터는 상위 수준 도메인에서 상속된 항목과 Cloud Dimensions 도메인에 정의된 모듈을 보여줍니다.
3. 홈페이지 및 목록 데이터는 사용자에게 표시되는 데이터를 반영합니다. 이 데이터는 사용자의 세션 컨텍스트를 기반으로 합니다. 이 경우 Cloud Dimensions 도메인의 사용자는 Cloud Dimensions, 하위 도메인 및 전역 도메인의 데이터를 볼 수 있습니다.

사용자 세션 컨텍스트는 홈 도메인에서 시작됩니다.

다음 다이어그램에서는 컨텍스트의 요소를 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



시스템 관리자는 사용자 기록에 사용자의 홈 도메인을 설정합니다. 일반적으로 사용자의 홈 도메인은 회사의 도메인과 동일한 도메인으로 설정됩니다. 사용자가 로그인하면 도메인 선택기가 자동으로 사용자의 홈 도메인으로 설정됩니다. 사용자는 도메인 선택기에서 화살표 아이콘을 클릭하여 언제든지 홈 도메인으로 돌아갈 수 있습니다.

도메인 선택기 목록에는 사용자의 세션 컨텍스트 내에 있는 도메인이 포함됩니다. 사용자는 선택기로 하위 도메인을 선택하여 세션 컨텍스트를 더 제한할 수 있습니다.

사용자 세션의 컨텍스트에는 사용자의 홈 도메인과 모든 하위 도메인이 포함됩니다. 사용자의 세션 컨텍스트에 있는 이 도메인 집합은 데이터베이스로 전송되는 모든 쿼리에 자동으로 추가됩니다. 이렇게 하면 결과가 이러한 도메인과 전체 데이터의 데이터로만 제한됩니다. 이 프로세스는 액세스할 수 없는 컴파일된 코드에 포함됩니다.

통합에 사용되는 서비스 계정에도 사용자 세션 컨텍스트가 있습니다. 사용자 컨텍스트 및 기록 컨텍스트가 있으며, 각각은 자체 도메인에 자체 데이터가 있습니다. 이러한 컨텍스트는 통합에 영향을 줍니다. 데이터베이스 쿼리(레코드)는 대화형 사용자(사용자)와 동일한 방식으로 제한되므로 정상적으로 작동하지만 개발자가 구성한 제약 조건에 의해 제한됩니다.

에서 서비스 제공자 참조 아키텍처사용자의 세션 컨텍스트에 도메인을 추가하는 다른 방법에 대해 알아볼 수 있습니다.

기록 컨텍스트

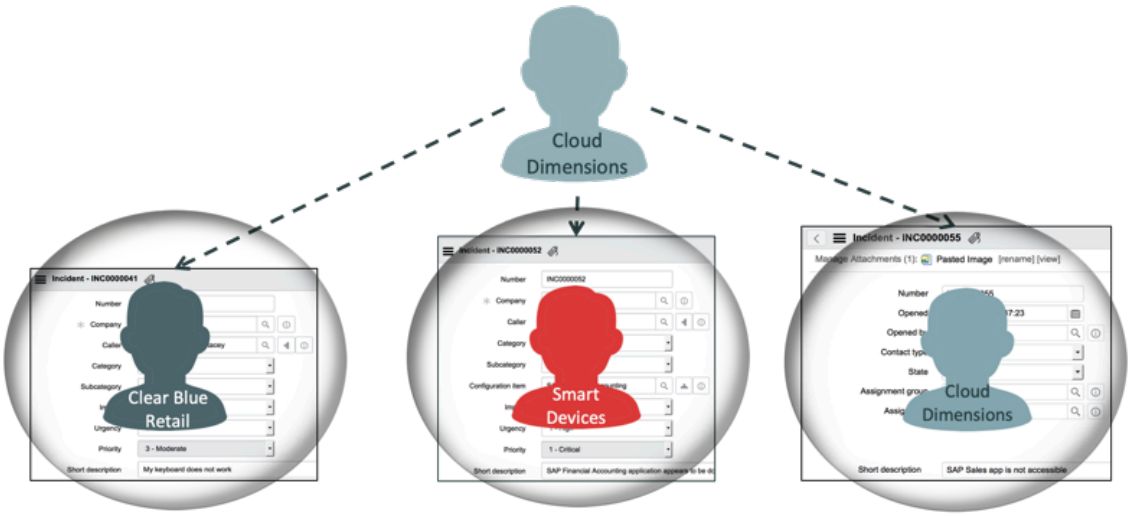
사용자가 개별 기록을 드릴다운하면 기록 컨텍스트가 활성화됩니다. 기록 컨텍스트에 따라 기록에 적용할 UI 요소와 프로세스가 결정됩니다.

기록의 도메인은 프로세스, 데이터, 기록 내 UI 요소의 가용성을 결정합니다.

주:

- 사용자의 도메인이 변경되어도 기록 컨텍스트는 유지됩니다.
- 사용자는 자신의 기록 컨텍스트를 유지하면서 여러 브라우저 탭에서 동시에 기록을 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

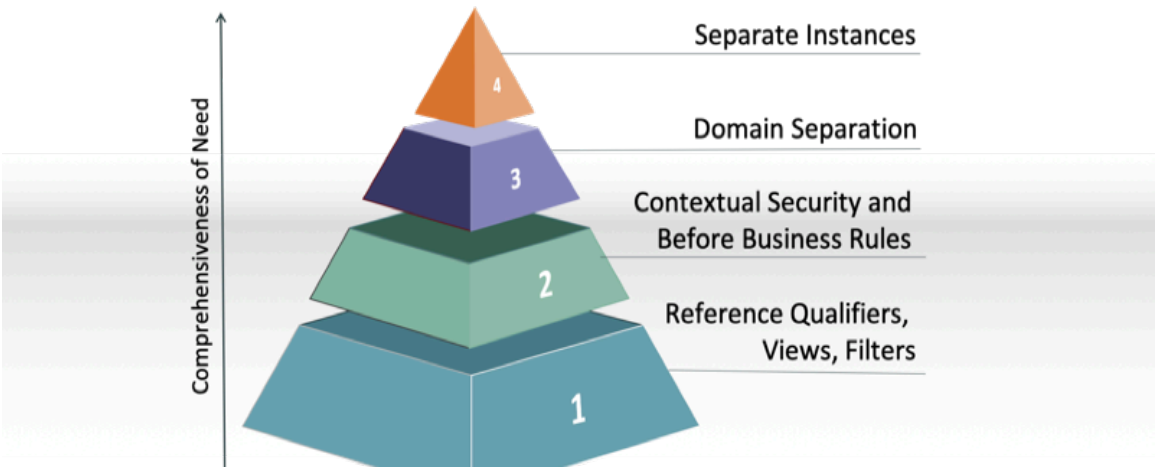


도메인 분리를 사용하여 데이터 분리 및 보안

고객의 필요에 따라 여러 가지 방법으로 플랫폼에서 데이터를 ServiceNow 분리하고 보호할 수 있습니다.

다양한 방법으로 데이터 분리

다음 다이어그램에서는 데이터를 분리할 수 있는 네 가지 방법을 보여 줍니다. 별도의 인스턴스, 도메인 분리, 상황별 보안 및 비즈니스 규칙, 참조 아키텍처 자체를 데이터 분리 방법으로 사용할 수 있습니다.



다음 네 가지 방법으로 데이터를 분리할 수 있습니다.

1. 한정자와 필터로 참조 아키텍처를 사용자 지정하여 회사 내의 부서와 그룹이 각자의 작업에 집중할 수 있도록 합니다. 이러한 부서 또는 그룹 간에 데이터를 분리하면 부서 또는 그룹이 다른 부서 또는 그룹의 기록을 볼 수 없습니다.
2. 데이터 유출을 방지하기 위해 상황별 보안 및 쿼리 전 비즈니스 규칙을 추가 보안 계층으로 추가합니다. 이전 비즈니스 규칙 쿼리 도메인 분리 및 비즈니스 규칙에 대한 자세한 내용을 참조하십시오컨텍스트 및 도메인 분리.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 도메인 분리를 사용하여 회사에 다른 수준의 보안을 추가합니다. 모든 데이터베이스 쿼리의 데이터는 상황별 보안 및 비즈니스 규칙이 실행되기 전에 도메인에 표시되는 데이터로 제한됩니다.
4. 별도의 인스턴스를 사용하여 데이터베이스 및 애플리케이션 계층에서 데이터 분리

개별 인스턴스, 도메인 분리, 상황별 보안 및 비즈니스 규칙, 참조 아키텍처는 데이터를 분리하는 방법입니다. 이 네 가지 방법은 다이어그램의 필요의 포괄성 화살표에서 알 수 있듯이 서로 관련이 있습니다. 각 계층이 다른 계층과 상호 작용하는 방법은 도메인 분리 구성을 설정하는 방법에 따라 달라집니다.

모든 조직에 도메인 분리가 필요한 것은 아닙니다. 별도의 인스턴스 또는 도메인이 없는 단일 인스턴스와 같은 다른 대안을 찾을 수 있습니다. 이러한 대안에 대한 자세한 내용은 다음 문서를 참조하십시오 도메인 분리의 필요성 평가.

테넌트 간 인텔리전스

다중 테넌트 아키텍처는 단일 인스턴스가 여러 테넌트에 서비스를 제공하는 경우입니다. 테넌트에 대한 데이터, 메타데이터, 비즈니스 논리 및 처리 컨텍스트는 추가 테넌트 데이터에 대한 액세스를 통해 자동으로 처리됩니다.

단일 테넌트와 다중 테넌트 비교

단일 테넌트 인스턴스

ServiceNow 고객은 라이센스를 구입했으며 원하는 서비스를 결정하는 것은 귀하에게 달려 있습니다. 원할 때 업그레이드하고, 모든 새 기능의 미리 보기를 확인하고, 인스턴스를 즉시 구성할 수 있습니다. 단일 테넌트가 되면 다음과 같은 이점과 제한 사항이 있습니다.

- 초기 비용과 관리 오버헤드가 더 높지만 리모델링 및 확장에 더 많은 자유가 있습니다.
- 인스턴스를 확보하고 유지하며 관리 직원을 공급하는 데 드는 비용이 더 많이 듭니다. 필요에 따라 환경을 자유롭게 빌드할 수 있지만 권장 사례 및 표준을 준수해야 ServiceNow 합니다.

다중 테넌트 인스턴스

다른 사람이 인스턴스를 소유하며, 여러 고객을 보유한 서비스 제공자일 수 있습니다. 원할 때 업그레이드하고 원할 때 인스턴스에 새 서비스를 추가합니다. 서비스 제공자의 고객이라면 서비스 제공자가 제공하는 것을 원했기 때문에 해당 인스턴스를 사용하고 있을 가능성이 큽니다. 여러 테넌트에는 다음과 같은 이점과 제한 사항이 있습니다.

- 중앙 집중식 직원이 구성, 통합 및 업그레이드를 관리합니다.
- 인스턴스 소유자는 추가 서비스를 제공합니다.
- 도메인 테넌트는 플랫폼을 사용하는 ServiceNow 데 드는 초기 비용이 낮고, 많은 테넌트와 공유하기 때문에 월별 비용이 저렴하며, 환경을 관리하기 위해 직원을 고용할 필요가 없습니다.
- 다른 테넌트에서 시작한 요청 또는 변경에서 공유되는 이익입니다.

Domain Separation의 대체 앱

고객을 위한 도메인 분리의 대안으로 별도의 인스턴스를 사용할 수 있습니다. 별도의 인스턴스를 사용하면 다른 사람에게 거의 또는 전혀 영향을 미치지 않으면서 조직의 그룹 및 부서 내에서 데이터 분리에 대한 요구 사항을 유연하게 충족할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개별 인스턴스

개별 인스턴스의 장단점

개별 인스턴스	단일 인스턴스 - 도메인 없음
장점	장점
각 고객/조직에 맞게 제작	간단한 시나리오를 다룰 수 있습니다.
사용자 지정이 다른 사용자에게 미치는 영향을 최소화합니다.	비용
릴리스 일정 조정	단점
깨끗한 분리	베이스라인 코드에 대한 광범위한 수정
데이터 센터 지역 선택	업그레이드 중 건너뛴 수정된 기본 시스템 코드
단점	모든 보조 테이블과 지원 테이블도 다루어야 합니다.
비용	광범위한 테스트 필요
인스턴스 정렬	사용자 지정 코드를 발전시킬 제품 팀이 없음 ServiceNow
업그레이드에 대한 테스트 작업량	
중복 작업량	
통합 필요	

각 인스턴스에 대해 개별적으로 업그레이드 및 릴리스 시기를 정할 수 있습니다. 그러나 별도의 인스턴스를 사용하기로 선택하는 경우 인스턴스를 관리하는 다른 사람들과 많은 조정을 수행해야 합니다. 상황별 보안, 양식 뷰, 참조 한정자, 필터 및 강력한 조건을 갖춘 인스턴스를 구성하면 회사에서 도메인 분리를 사용할 필요가 없습니다.

별도의 인스턴스를 사용하면 데이터 및 프로세스 분리를 처리할 수 있지만 인스턴스 소유자는 별도의 인스턴스에 필요한 광범위한 사용자 지정을 유지 관리하고 유지해야 합니다.

관련 정보

컨텍스트 및 도메인 분리

서비스 제공자 참조 아키텍처

도메인 분리의 필요성 평가

도메인 분리가 고객의 조직에 항상 적합한 것은 아닙니다. 고객의 요구 사항을 고려하여 도메인 분리를 사용하기로 결정하는 것이 가장 좋습니다.

도메인 분리의 필요성 평가

도메인 분리 이유

다음 요인은 고객의 조직에 대한 도메인 분리를 선택하는 결정을 내리는 데 도움이 될 수 있습니다.

- 고객은 프로세스와 일반적인 플랫폼 요구 사항이 적당히 일치합니다.
- 고객은 요청자가 아닌 이행자로서 작업을 수행하려고 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 고객이 데이터 레코드를 격리해야 하는 계약에 동의했지만 인스턴스 소유자가 해당 요구 사항을 구성의 다른 곳에서 해결할 수 있다고 결정했습니다.
- 회사의 인스턴스 소유자에게는 물리적으로 분리된 조직으로 운영되고 데이터를 공유하지 않는 전체 엔터티가 있지만 전체 보고는 여전히 필요합니다. 별도의 도메인은 올바르게 구성되면 데이터를 볼 수 있습니다.

도메인 분리가 없는 이유

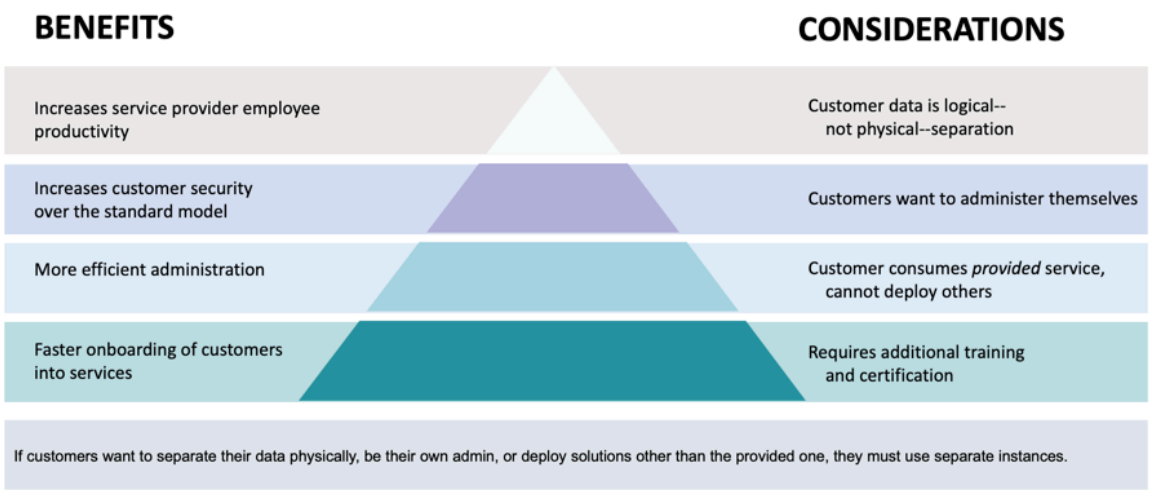
이러한 요인들은 고객의 조직이 도메인 분리 설정을 꺼리는 이유를 가리킬 수 있습니다.

- 고객은 환경을 관리하고, 환경에 대한 완전한 소유권을 갖고, 확장을 위한 로드맵을 설정하기를 원합니다.
- 고객은 실제 또는 데이터베이스 수준에서 데이터와 프로세스를 완전히 격리할 것을 요구합니다.

주:

도메인 분리 인스턴스에는 공유 데이터베이스가 포함되어 있으므로 격리 요구 사항이 약화됩니다.

- 고객 조직의 부서에서 기록을 분리하려고 합니다. (접근 제어로 충분할 수 있습니다.)
- 고객은 모두 고유한 프로세스, 비즈니스 규칙 및 워크플로우를 원합니다.
- 기업 문화는 고객 조직 간의 비협업 중 하나입니다.
- 고객은 최종 사용자로서만 플랫폼과 상호작용합니다.



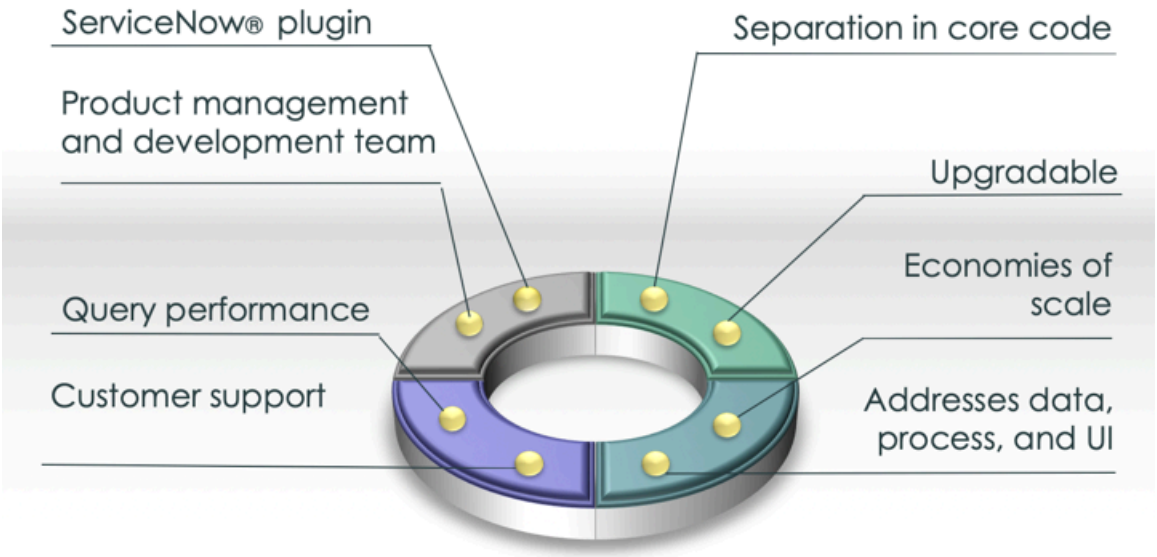
도메인 분리의 이점

도메인 분리는 그룹과 부서 간에 데이터를 분리하는 다른 방법보다 고객의 조직에 더 적합할 수 있습니다.

도메인 분리의 이점 한눈에 보기

핵심 플랫폼에 기능이 내장된 플러그인을 사용하여 ServiceNow 도메인 분리를 활성화할 수 있습니다. 별도의 도메인 구성은 개발 팀의 지원을 받는 제품 관리자가 관리합니다. 도메인 분리 기능에 대한 개선 사항 및 수정 사항이 릴리스에 ServiceNow 포함되어 있으며 고객이 바로 사용할 수 있습니다. 도메인 분리에 대한 지원이 필요한 경우 인스턴스 소유자는 Service Portal 과 같은 자원을 사용할 고객 서비스 및 지원 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



데이터베이스 쿼리가 도메인 분리와 함께 작동하는 방식

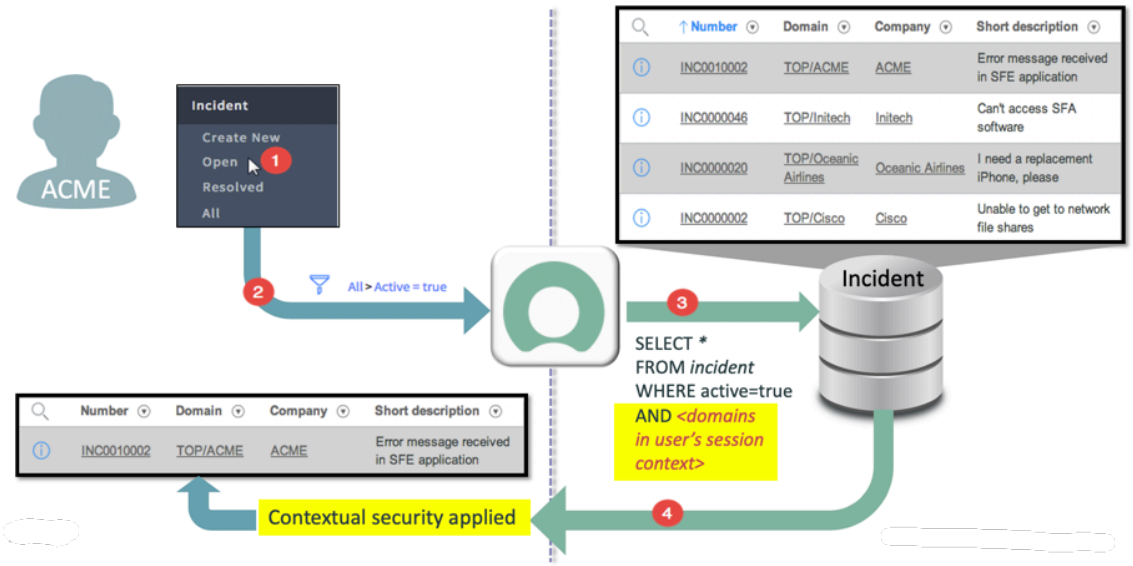
고객의 애플리케이션에서 도메인 분리와 함께 데이터베이스 쿼리를 사용하면 고객의 데이터를 보호하는 데 도움이 됩니다. 그런 다음 이러한 쿼리는 구성 속도를 높이고 프로세스를 빌드합니다.

도메인 분리가 데이터를 보호하는 방법

다음 그림에서 인시던트 테이블 (incident)에는 인시던트의 작업에서 상속된 도메인 필드가 있습니다. 이 도메인 필드를 보면 테이블의 기록에 도메인 할당이 있을 수 있음을 알 수 있습니다.

사용자가 로그인하면 홈 도메인이 액세스할 수 있는 도메인 세트와 함께 나타납니다. 이를 사용자의 세션 컨텍스트라고 합니다. 세션 컨텍스트에 대한 자세한 내용은 다음 문서를 참조하십시오 컨텍스트 및 도메인 분리.

도메인 분리가 있는 데이터베이스 쿼리



1. 브라우저에서 Acme 회사 중 하나의 사용자가 Open Incidents 모듈을 선택하여 active=true인 모든 인시던트를 봅니다.
2. active=true 필터가 애플리케이션에 제출됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 그런 다음 응용 프로그램은 WHERE 절을 active=true에 추가하여 데이터베이스에 쿼리를 보냅니다. WHERE 절은 사용자의 도메인 또는 사용자가 액세스할 수 있는 도메인에 있는 기록으로 반환되는 인시던트 기록을 제한합니다. 이러한 도메인의 기록만 처리를 위해 애플리케이션에 반환됩니다.
4. 상황별 보안이 적용되어 사용자에게 반환되는 데이터가 더욱 제한됩니다. 인시던트 기록이 미해결 인시던트 목록에 나타납니다.

주:

상황별 보안을 적용할 때 사용자에게 반환되는 데이터에 대한 제한을 만듭니다. 이러한 제한은 사용자에게 표시하지 않을 수 있는 다른 콘텐츠를 보호합니다.

상황별 보안에 대한 자세한 내용은 다음 문서를 참조하십시오 컨텍스트 및 도메인 분리.

주: 이 처리 논리는 통합을 사용하여 트리거되는 쿼리를 포함하여 데이터베이스에 대한 모든 쿼리에 적용됩니다.

도메인 분리 지원 수준

고객 조직의 애플리케이션 도메인 분리에 대한 세 가지 범주 중에서 선택합니다.

도메인 분리를 지원하는 애플리케이션은 데이터 분리 및 데이터 라우팅만 지원하거나, 고급 비즈니스 논리 분리를 제공하거나, 애플리케이션의 테넌트(고객) 수준 관리를 지원할 수 있습니다. 이러한 정의는 실제 사용 사례와 이를 구현하는 사용자의 관점에서 지원 수준을 설명합니다.

증분 **ServiceNow** 지원 수준

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

수준	유형	요약
지원 안 함		• 도메인 필드가 데이터 테이블에 존재할 수 있지만 데이터를 관리할 비즈니스 논리가 없습니다. • 이 수준은 도메인으로 구분된 것으로 간주되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수준	유형	요약
기본	고객 데이터 관리	• 비즈니스 논리: 데이터가 애플리케이션의 서비스 제공자 사용 사례에 적합한 도메인으로 들어가도록 보장합니다. • 애플리케이션, 사용자 인터페이스, 캐시 키, 보고, 롤업, 집계 등에서 모두 런타임 시 도메인의 속성을 고려합니다. • 인스턴스 소유자는 여러 테넌트에서 정상적으로 작동하도록 애플리케이션을 설정할 수 있어야 합니다. 사용 사례: 서비스 제공자가 채팅을 사용하여 고객의 메시지에 응답할 때 고객이 응답을 볼 수 있어야 합니다.
표준	고객 프로세스 관리	• 기본 수준 포함 • 비즈니스 논리: 프로세스는 서비스 제공자가 고객별로 만들거나 수정할 수 있습니다. 사용 사례는 여러 서비스 제공자 고객이 단일 인스턴스에서 애플리케이션을 사용하는 방법을 반영합니다. • 인스턴스 소유자는 특정 애플리케이션에 대해 고객별로 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성할 수 있어야 합니다. 사용 사례: 관리자가 한 고객에 대해서는 기록이 닫히지만 다른 고객에 대해서는 기록이 닫히지 않는 경우 설명이 필요하도록 설정할 수 있어야 합니다.
Enhanced	고객 자체 관리형 구성	• 기본 및 표준 수준 포함 • 서비스 제공자 고객이 정의된 사용 사례를 기반으로 하는 비즈니스 논리를 수정할 수 있습니다. 이러한 구성은 한 고객의 구성이 다른 고객에게 영향을 주지 못하도록 UI 기반 및 페일 세이프로 되어 있습니다. • 인스턴스 고객은 MVP 비즈니스 논리 및 데이터 매개 변수 자체를 구성할 수 있어야 합니다. 사용 사례: 공유 환경의 고객은 도메인 내의 영향, 긴급도 또는 우선순위에 따라 변경할 수 있어야 합니다.
유효 도메인*		경우에 따라 플랫폼 기능 또는 애플리케이션은 도메인 프레임워크를 사용하지 않는 경우에도 서비스 제공자 사용 사례를 지원할 수 있습니다. 도메인 분리를 지원하려면 사용 사례를 자세히 설명해야 합니다. 지원 수준 뒤의 별표(*)는 이러한 종류의 구성을 나타냅니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수준	유형	요약
		사용 사례: New York 릴리스 서비스 카탈로그 이전에는 도메인 지원이 없었지만 인스턴스 소유자가 사용자 기준을 사용하여 도메인 분리 인스턴스에서 각 테넌트에 대해 별도의 카탈로그와 항목을 구성할 수 있었습니다. 그 결과 각 테넌트는 표준 수준에서 서비스 카탈로그를 사용할 수 있게 되었습니다.

지원 수준별로 나열된 모든 애플리케이션을 보려면 문서를 참조하십시오 도메인 분리를 위한 애플리케이션 지원.

요약

도메인 분리는 애플리케이션에서 고객을 인식하도록 하기 위해 사용해야 하는 프레임워크입니다.

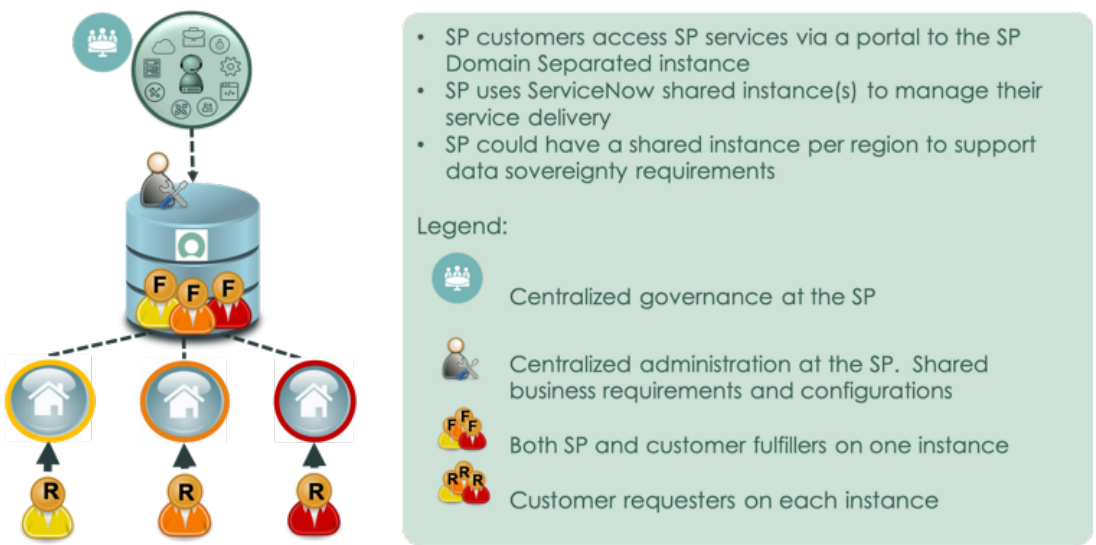
도메인 프레임워크 기능, 애플리케이션의 비즈니스 사용 사례, 가상 사용자의 정의, 애플리케이션을 사용하는 방법을 먼저 고려하여 프레임워크를 사용하여 애플리케이션을 지원할 수 있도록 합니다.

서비스 제공자 참조 아키텍처

고객은 도메인 분리 인스턴스에 도달할 수 있도록 설계된 포털을 사용하여 SP(서비스 제공자) 서비스에 액세스할 수 있습니다.

서비스 제공자 참조 아키텍처의 기본 속성

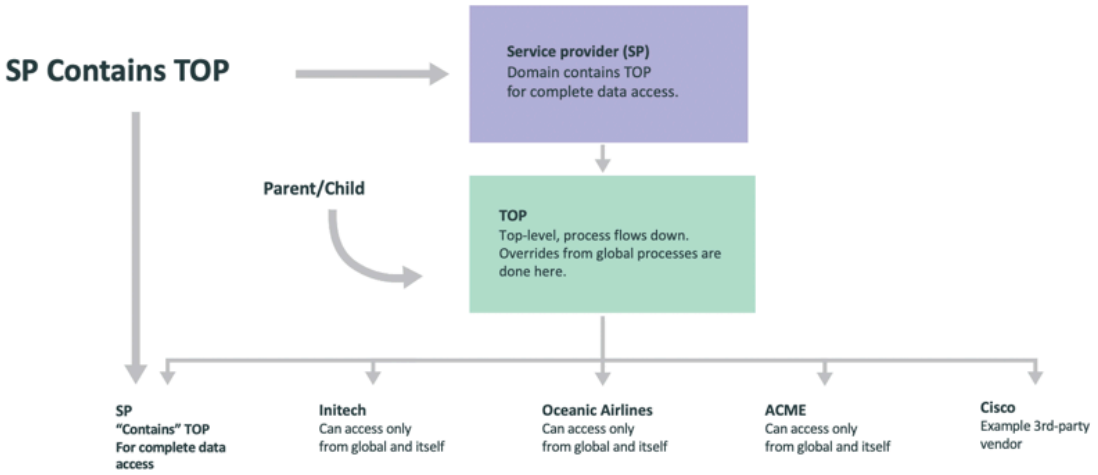
- 이행자를 도메인에 할당하지 마십시오. 그 대신 도메인 간에 공유합니다. 이로 인해 도메인당 얼마나 많은 이행자가 있는지 감사하기가 더 어려워집니다.
- 도메인 관리를 공유하고 활용할 수 있습니다. 즉, 오버헤드가 없으므로 라이센스를 최적화할 수 있습니다.
- 새 고객을 받으면 인스턴스의 사용자 수가 변경됩니다. 신규 고객 한 명으로 인해 시스템에서 수만 또는 수십만 명의 신규 사용자가 생길 수 있습니다. 공유 환경 한 곳의 총 사용자 수는 사실상 무제한입니다.



SP 서비스 포털은 SP 공유 인스턴스에 전용으로 제공되거나 공유됩니다. 서비스 제공자는 ServiceNow 공유 인스턴스를 사용하여 서비스 제공을 관리합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 분리 인스턴스에 대한 참조 계층 구조



SP 참조 아키텍처 비교

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.

서비스 제공자 참조 아키텍처 의사 결정 트리

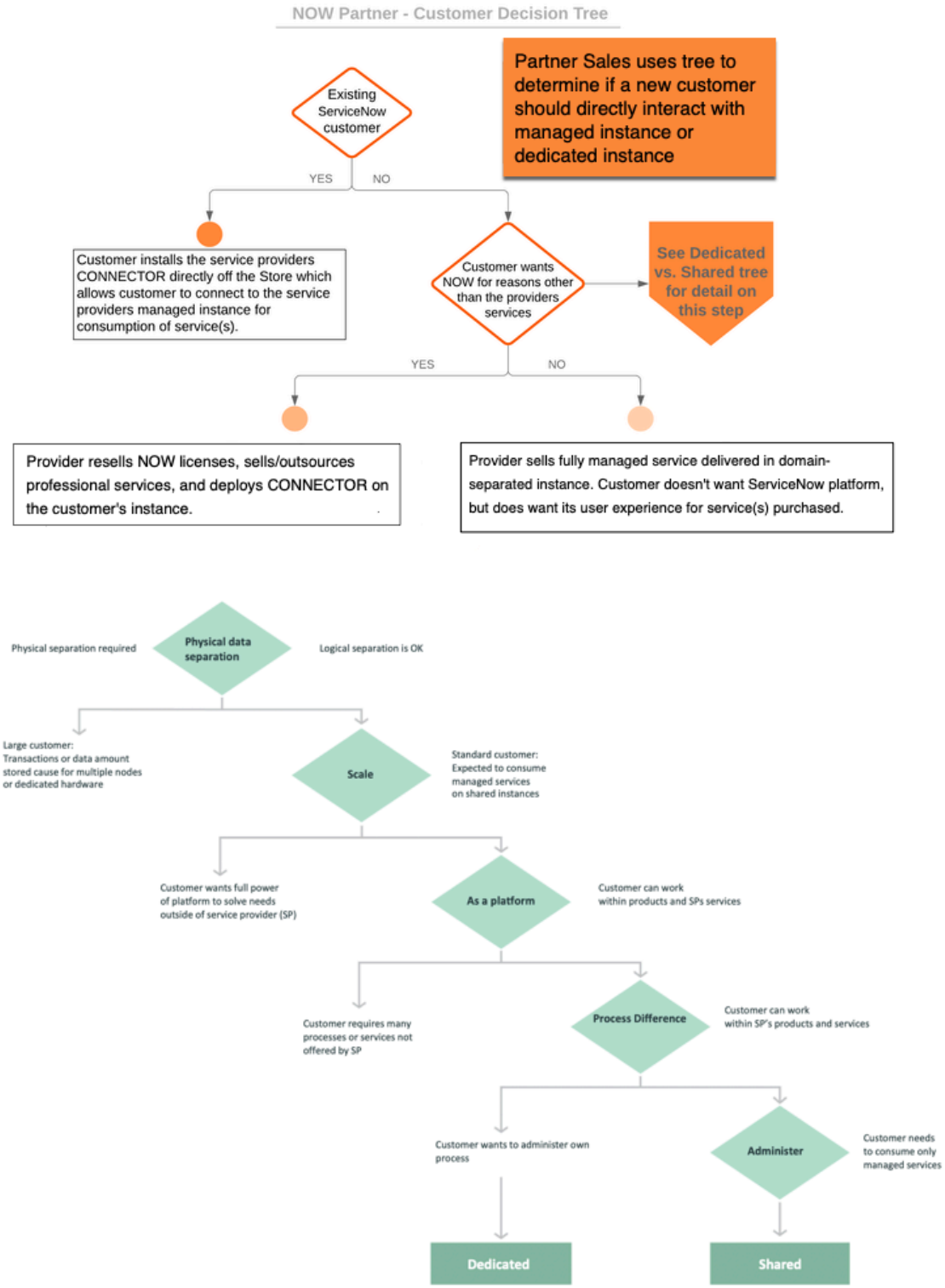
결정 트리와 비교 차트를 사용하여 신규 고객을 공유 인스턴스에 추가해야 하는지 아니면 전용 인스턴스에 추가해야 하는지 결정할 수 있습니다.

결정 트리

이러한 결정 트리를 사용하면 고객이 관리형 인스턴스를 사용할지 전용 인스턴스를 사용할지 결정하는 데 도움이 됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

고객 의사 결정 트리



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

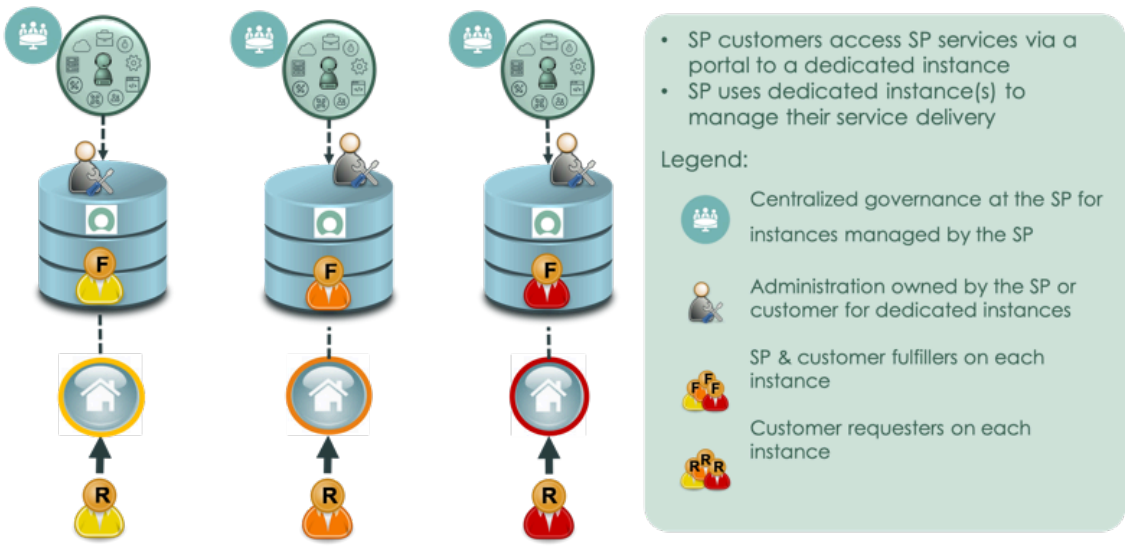
SP 참조 아키텍처 비교

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.

전용 인스턴스에 대한 서비스 제공자 참조 아키텍처

SP(서비스 제공자) 고객은 전용 인스턴스에 대한 포털을 사용하여 SP 서비스에 액세스할 수 있습니다. SP는 이러한 전용 인스턴스를 사용하여 서비스 제공을 관리합니다.

전용 인스턴스



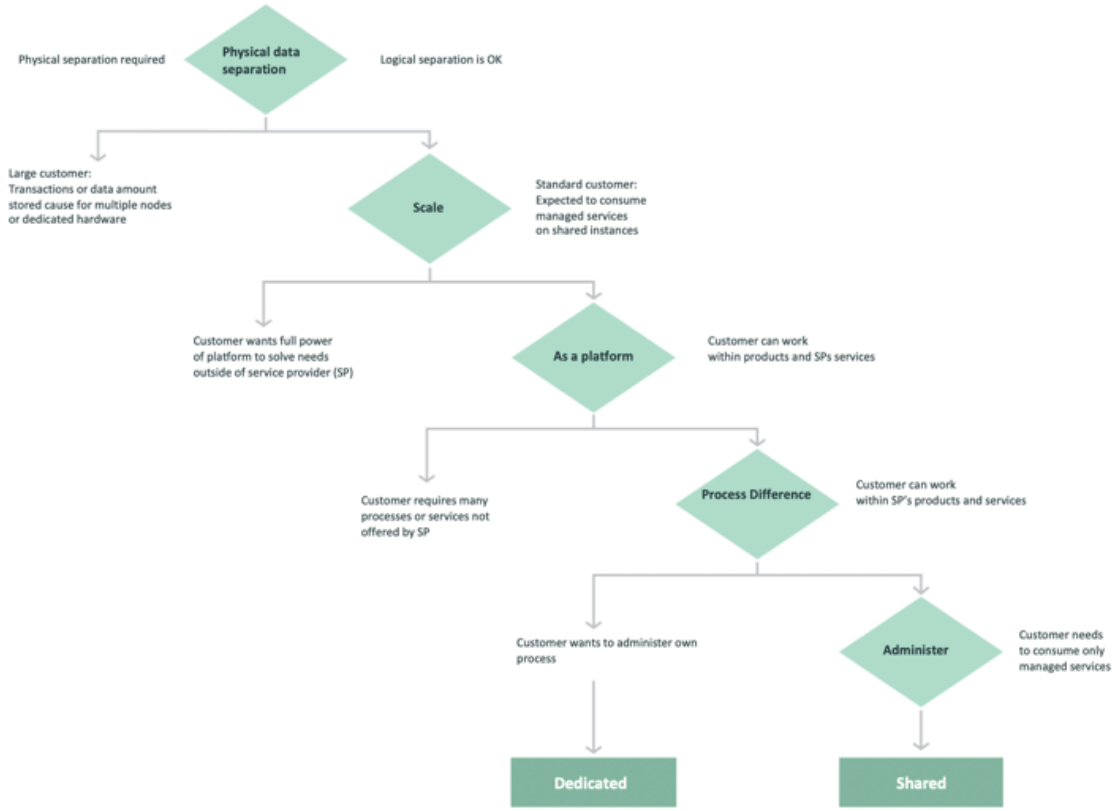
속성

- 전용 인스턴스를 사용하려면 별도의 관리 및 전담 팀이 있어야 합니다. 여러 인스턴스에 로그인하는 관리자와 개발자를 위해 여러 라이센스가 필요합니다.
- 각 인스턴스에는 한정된 수의 요청자와 이행자 수가 있습니다. 신규 고객을 확보할 때는 고객 회사의 규모와 규모에 맞는 인스턴스를 구매해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

공유 인스턴스

전용 및 공유 인스턴스 비교



SP 참조 아키텍처 비교

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.

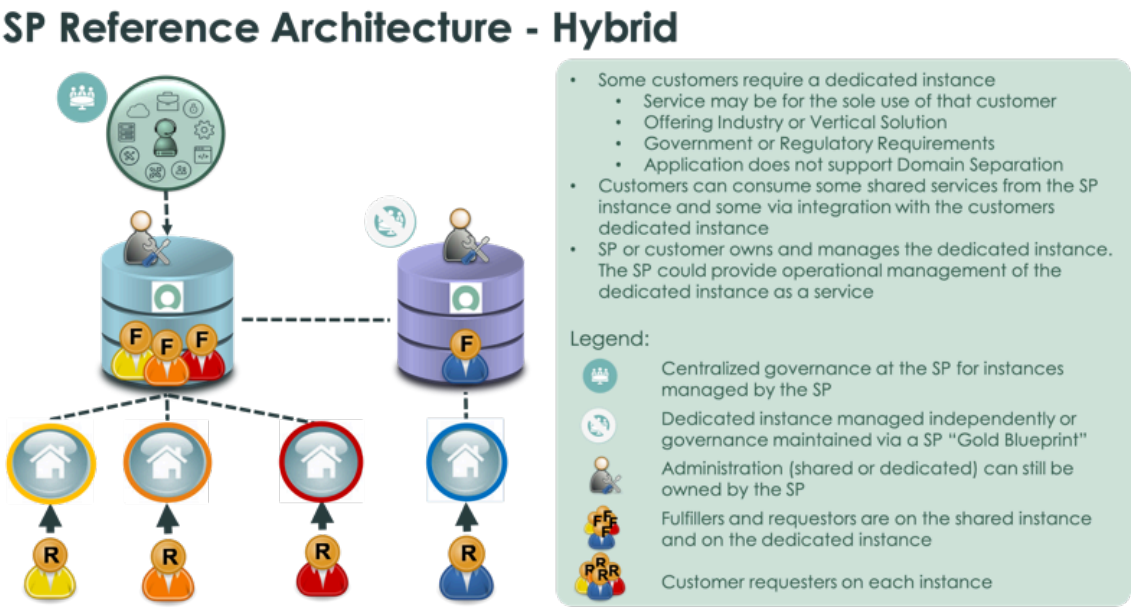
하이브리드용 서비스 제공자 참조 아키텍처

사용자 지정 솔루션에 하이브리드 서비스 제공자(SP) 참조 아키텍처를 사용합니다. 고객에게는 특정 서비스에 대한 전용 인스턴스가 필요합니다. 다른 서비스에 공유 SP 인스턴스를 계속 사용할 수 있지만 각 인스턴스를 통합해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

하이브리드 아키텍처

이 추가 서비스를 직접 제공할 책임은 고객에게 있습니다. 고객이 제공할 수 있는 여러 속성의 하이브리드 솔루션을 구축해야 합니다.



속성

- 인스턴스 관리를 공유하고 활용할 수 있습니다. 즉, 오버헤드가 없으며 라이센스를 최적화할 수 있습니다.
- 분산 환경에 대한 새 인스턴스가 있는 경우 프로그램 팀은 해당 인스턴스에 대한 전담 관리자 사용자로서 책임을 지고 그에 따라 자금을 지원합니다. 모든 인스턴스가 Blueprint에서 비롯되는 중앙 집중식 환경에서는 중복 관리 라이센스가 필요합니다.
- 이행자를 도메인에 할당하지 마십시오. 대신 도메인 간에 공유할 수 있습니다.
- 고객이 공유 환경과 전용 환경을 모두 공유하는 경우 두 환경 모두에서 이행자가 필요합니다. 공유 인스턴스와 전용 인스턴스에 대한 프로세스에는 인스턴스마다 다른 작업이 필요하기 때문에 이는 각 팀에 더 많은 작업을 의미합니다.
- 새 고객을 받으면 인스턴스의 사용자 수가 변경됩니다. 신규 고객 한 명으로 인해 시스템에서 수만 또는 수십만 명의 신규 사용자가 생길 수 있습니다. 공유 환경 한 곳의 총 사용자 수는 사실상 무제한입니다.
- 각 인스턴스에는 한정된 수의 요청자와 이행자 수가 있습니다. 신규 고객을 확보할 때는 고객 회사의 규모와 규모에 맞는 인스턴스를 구매해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SP 참조 아키텍처 비교

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.

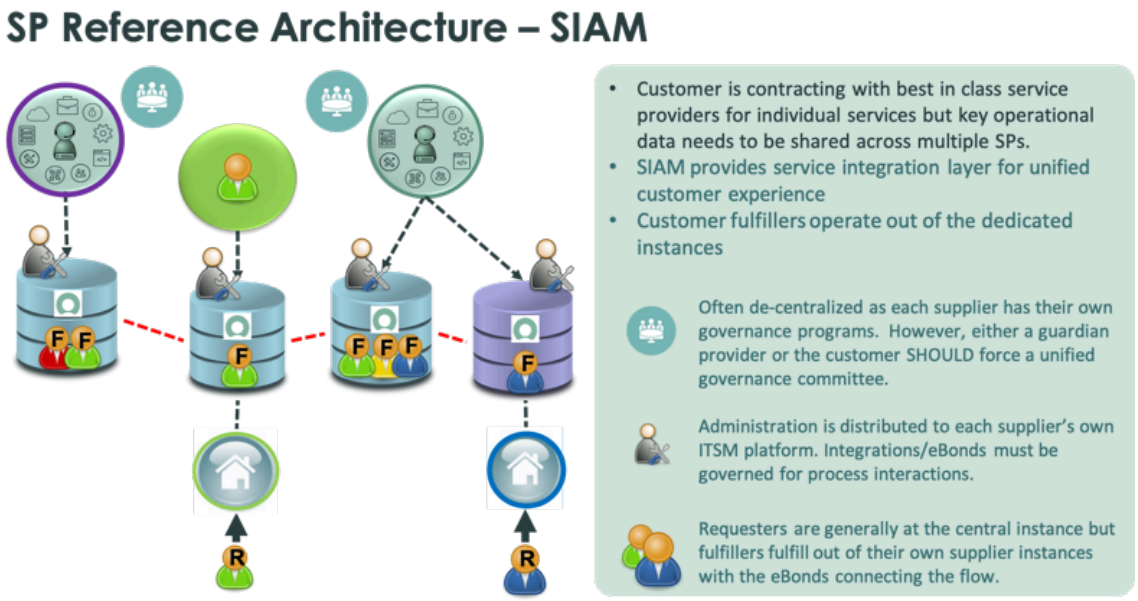
(SIAM)에 대한 서비스 통합 관리 서비스 제공자 참조 아키텍처

서비스 제공자(SP)용 SIAM(Service Integration and Management) 아키텍처는 서비스 통합 관리 통합 고객 경험을 위해 서비스를 통합합니다.

SIAM 아키텍처의 속성

- 고객은 SP 공유 인스턴스에 대한 전용 또는 공유 포털에서 SP 서비스에 액세스합니다.
- SP는 공유 인스턴스를 사용하여 ServiceNow 서비스 제공을 관리합니다.

SIAM 아키텍처 개요



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SP 참조 아키텍처 비교

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.

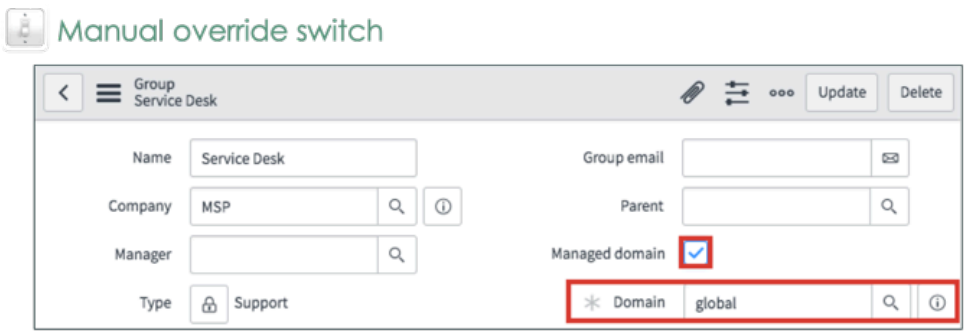
도메인 분리 용어

ServiceNow 인스턴스를 사용하면 고객 조직의 효율성을 높이고, 보안을 강화하고, 성과를 높일 수 있습니다. 구성을 만들 때 가장 일반적인 용어 몇 가지를 이해하면 도움이 됩니다.

관리되는 도메인

관리되는 도메인에서 관리되는 도메인 필드를 사용하면 도메인 관리자가 회사 기록에서 자동으로 할당된 도메인을 사용하는 대신 사용자, 그룹, 부서, 위치 또는 CI 기록에 대한 도메인을 수동으로 선택할 수 있습니다.

이러한 속성을 변경하려면 속성을 재정의하여 각 도메인에서 애플리케이션의 기능을 추가로 사용자 지정할 수



- Common Use Cases
  - Set admins to 'global'
  - Set support groups to 'global'
- UI Policy shows Domain when Managed domain = true

Tables with managed_domain	
User [sys_user]	Location [cmn_location]
Group [sys_user_group]	Department [cmn_department]
Configuration Item [cmdb_ci]	

있습니다.

프로세스 테이블

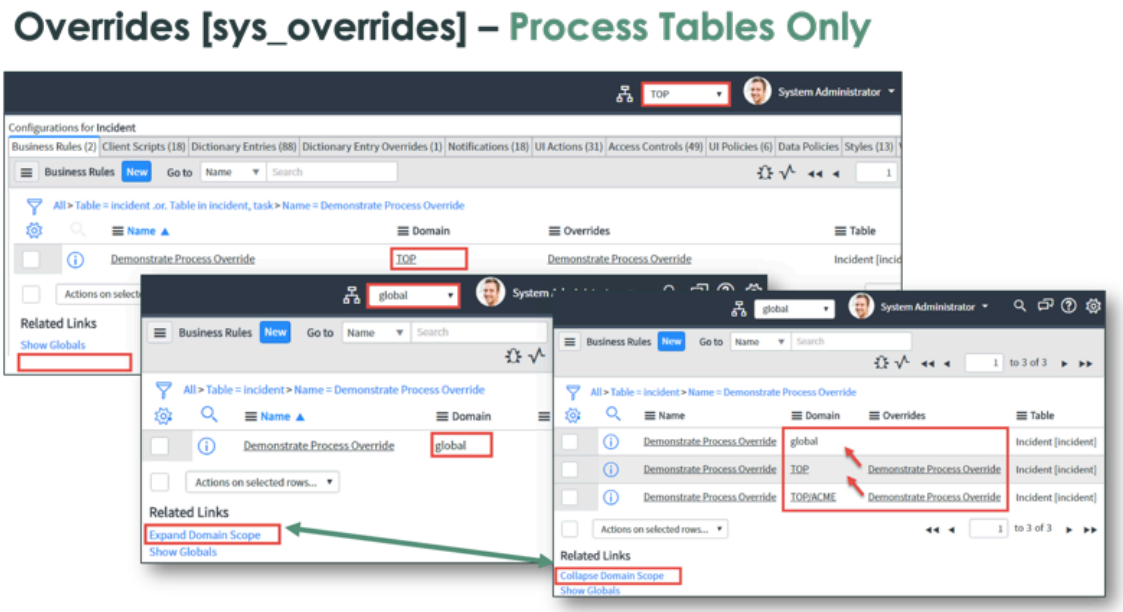
프로세스 테이블에서 무효화 **[sys_overrides]** 필드에 값이 표시되면 프로세스 무효화 기록이 존재하는 것입니다. 즉, 관리자가 도메인별 정책을 설정할 수 있는 방법인 위임된 관리가 적용됩니다. 전역 도메인의 관리자는 도메인 범위 확장/축소 관련 링크를 사용하여 기록 재정의를 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 보고서는 도메인으로 구분되며 무효화 필드를 포함합니다. 전역 도메인의 모든 보고서를 보려면 도메인 범위 확장 관련 링크를 사용합니다.

도메인에서 프로세스 테이블을 보면 선택한 도메인에 대한 관련 프로세스 기록만 표시됩니다. 전역 도메인에서 프로세스 테이블을 볼 때 도메인 범위 확장 관련 링크가 표시되어 재정의를 포함한 모든 프로세스 기록을 볼 수 있습니다. 전역에 대한 관련 프로세스 기록만 다시 보려면 도메인 범위 축소 관련 링크를 사용합니다.

도메인 범위 기능은 프로세스 테이블에만 사용되며 테이블의 데이터 가시성이 반대 방향으로 이동하게 합니다. 예를 들어 상위 도메인의 기록은 하위 기록에서 볼 수 있지만 상위 기록은 하위 기록을 볼 수 없습니다. 이렇게 하면 프로세스가 하위 도메인으로 플로우다운될 수 있습니다.



도메인 유형

다양한 유형의 도메인은 프로세스와 데이터를 구성하고 애플리케이션 또는 기능에서 작동하는 방식을 구성하는 데 도움이 될 수 있습니다.

고객 도메인

고객의 도메인에는 사용자 인터페이스와 데이터 사용 방법을 제어하는 프로세스가 있습니다.

다음 이미지에서 ACME 도메인은 고객 도메인입니다.

프로세스 도메인

데이터가 사용되는 방식과 도메인에서 수행하는 작업에 대한 프로세스를 생성합니다. 이러한 프로세스에는 다음 속성이 있어야 합니다.

- 도메인 세트의 특정 프로세스 및 UI 설정
- 어떤 종류의 핵심 데이터(예: 특정 사용자 데이터)도 없습니다.
- 다음 이미지의 TOP 도메인은 프로세스 도메인입니다.

데이터 도메인

데이터 도메인에는 여러 고객과 관련된 데이터가 있습니다. 실제 고객 도메인을 공유하지 않고도 해당 데이터를 공유할 수 있습니다. 각 고객은 고유한 데이터 도메인을 가지고 있으며 해당 도메인에 액세스할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

이러한 종류의 도메인은 일반적이지 않으며 과도하게 사용할 경우 성능 문제가 발생할 수 있습니다. 사용하기 전에 SP 아키텍트와 상의하십시오.

예: 도메인에는 ACME, Cisco 및 SP가 모두 상호작용해야 하는 작업이 있을 수 있습니다.

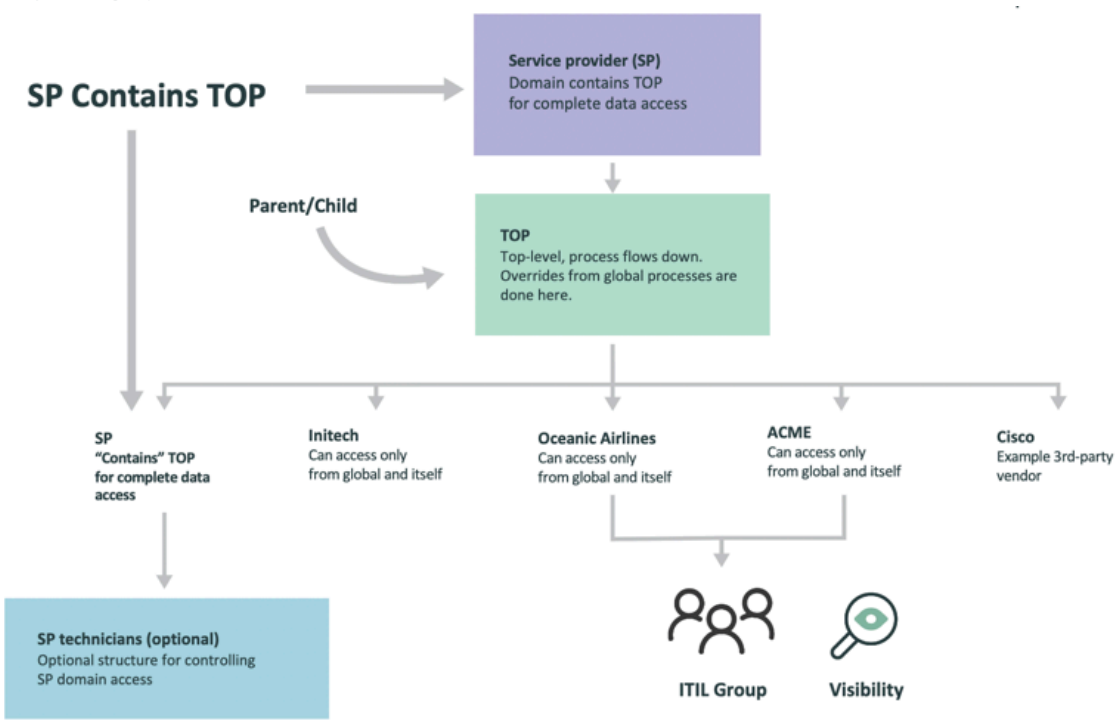
다음 이미지에서 기본 도메인은 데이터 도메인입니다.

사용자 데이터

사용자 기록 데이터는 전역 도메인이나 프로세스 도메인에 속할 수 없습니다. 사용자는 주로 고객 도메인에서 생성되며 경우에 따라 데이터 도메인에서 생성될 수 있습니다.

관리자 계정은 인스턴스의 일상적인 사용자로 사용해서는 안 되며 관리 기능을 용이하게 하기 위해 전역 도메인에 있어야 하므로 특별합니다.

도메인 계층 구조



목록, 관리자, 전역 프로세스

목록

전역 도메인에서 선택 필드의 레이블을 마우스 오른쪽 버튼으로 클릭하고 선택 사항 구성을 선택한 다음 새 선택 항목을 추가하면 선택 항목이 해당 필드의 모든 도메인별 목록으로 자동으로 푸시됩니다. 새 옵션이 선택됨으로 표시되면 활성으로 추가됩니다. 새 옵션이 사용 가능으로 표시되면 비활성으로 추가됩니다.

인스턴스 관리

인스턴스 소유자의 관리자는 도메인으로 분리된 인스턴스에서 모든 일반 프로세스 생성, 수정, 유지관리를 처리해야 합니다. 개별 도메인 관리자는 데이터 기반 프로세스의 일부를 유지 관리할 수 있습니다. 도메인 관리자 유형은 사용자 관리, 지원 그룹 구성원 자격 및 위치를 유지 관리하거나 테넌트 관리를 염두에 두고 설계된 응용 프로그램을 관리합니다.

전역 프로세스/매개변수

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

전역 도메인에 영향을 주는 프로세스를 생성 및 유지관리할 수 있을 뿐만 아니라 매개변수를 설정할 수도 있습니다. 이러한 속성은 도메인 분리 인스턴스의 모든 사용자에게 공통적으로 적용됩니다.

예: 시스템 속성, 딕셔너리 무효화, `sys_documentation` (필드 레이블), 데이터 모델(클래스, CI 유형 등), 테이블 및 필드 `[sys_dictionary]` (접근을 제한할 수 있음), 인덱싱(텍스트 인덱스 및 데이터베이스), ACL, 설치 종료, 인바운드 작업, 공용 페이지 및 인터셉터.

사용자 지정 테이블을 도메인 분리

별도의 도메인에 사용자 지정 테이블을 만들어야 할 수도 있습니다. 이 주제에서는 사용자 지정 테이블을 도메인 분리하는 절차와 개념을 모두 다룹니다.

1. sys_domain 필드 생성

주: 시스템 테이블 또는 테이블이 Domain Separation 플러그인에 의해 도메인 분리되지 않은 경우 도메인 분리하지 않는 것이 좋습니다.

이러한 점을 지침으로 사용하여 sys_domain 필드를 생성합니다.

- 새 필드를 *domain_id*유형으로 생성합니다.
  - 열 이름: sys_domain
  - 기타 속성: 자동으로 정의됨
- Sys_domain_path 자동으로 생성됩니다.

sys_domain 열 이름은 에서 Now Platform예약되어 있으며, 이는 시스템에서 이를 인식하고 적절한 필드 유형과 속성을 자동으로 적용한다는 것을 의미합니다. 이 자동 구성은 해당 **sys_domain_path** 필드도 생성합니다.

- 레이블을 사용하는 대신 열 이름을 `sys_domain` 로 설정합니다.
- 도메인 분리가 모든 테이블에 적합한 것은 아닙니다. 일반적으로 테이블이 기본 인스턴스의 일부이고 해당 테이블에 **sys_domain** 필드가 없는 경우 그대로 두어야 합니다.

sys_domain 필드는 이름이 "sys_domain"인 domain_id 유형 필드를 만들 때 자동으로 만들어집니다.

2. 비즈니스 규칙을 추가하여 도메인 설정

비즈니스 규칙 포함하지 않음

도메인은 레코드를 만드는 사용자의 현재 도메인으로 설정됩니다.

비즈니스 규칙 포함

도메인은 일반적으로 회사 필드를 기반으로 하는 스크립팅된 논리를 사용하여 할당됩니다.

사용자 지정 테이블에는 `sys_domain ##` 외에도 도메인 - 도메인 설정 - 작업과유사한 비즈니스 규칙이 있어야 도메인 필드의 값을 설정할 수 있습니다. 또한 첫 번째 규칙에서 도메인을 할당하지 못한 경우 도메인이 없는 기록을 기본 도메인으로 이동하는 도메인 – 기본 – 작업이 필요합니다.

작업 테이블에서 도메인에 대한 비즈니스 규칙을 검토합니다. 주문 필드에 특히 주의하십시오. 실행 우선순위는 순서 필드에 낮음에서 높음으로 지정됩니다.

실행되는 첫 번째 규칙인 도메인 – 도메인 설정 – 작업은 기록의 회사의 도메인을 기준으로 기록의 도메인을 설정하려고 시도합니다.

첫 번째 규칙이 적절한 도메인을 찾지 못하면 두 번째 규칙인 **Domain – Default – Task**가 실행됩니다. 이 규칙은 기록의 도메인을 기본 도메인으로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

마지막으로, 작업 기록의 도메인이 변경되면 도메인 - 단계적 도메인 - 작업 비즈니스 규칙이 워크플로우, 메트릭, SLA 및 첨부 파일과 같은 작업과 관련된 모든 기록의 도메인을 변경합니다.

3. 2단계가 실패한 경우 비즈니스 규칙 추가

초기 비즈니스 규칙에서 도메인을 설정하지 못하고 도메인이 여전히 비어 있거나 전역인 경우 두 번째 비즈니스 규칙이 실행됩니다. 이 규칙은 호출자 또는 `requested_for` 필드를 기반으로 하는 `task_for` 필드를 검사합니다. 이 규칙은 사용자의 도메인을 기반으로 기록의 도메인을 설정할 수 있는지 확인합니다. 그렇지 않은 경우 비즈니스 규칙은 도메인을 기본 도메인으로 설정합니다.

다음은 비즈니스 규칙에 대한 샘플 스크립트입니다.

```
/* essentially
If (task_for is set)
  set the domain to the user's domain
ELSE
  set the domain to the default domain
*/
```

4. 도메인 – 계단식 도메인 – 작업

작업에는 비즈니스 목적을 위해 함께 작동하는 여러 관련 테이블이 있을 수 있습니다. 이러한 관련 기록에는 워크플로우, SLA, 승인, 첨부 파일 및 이메일이 포함됩니다. 작업의 도메인이 변경되면 관련 기록 도메인도 변경되어야 새 도메인의 사용자에게 계속 표시됩니다.

이 계단식 규칙은 일반적으로 기본 도메인에서 기록을 지울 때 트리거됩니다.

스크립트에 포함된 계단식 도메인에 대한 관련 기록은 다음 예시와 유사하게 표시됩니다.

```
/*
* Keep domains in sync w/related records for:
* workflow context
* workflow history
* approver tables and related workflows
* attachments
* emails
*/
```

도메인 속성 및 테마 사용자 지정

구성한 도메인 내에서 고객의 회사 속성과 테마를 사용자 지정할 수 있습니다. 사용자 지정을 통해 인스턴스는 회사의 전체적인 모양과 느낌에 맞춰집니다.

회사 테마 및 로고 사용자 지정

회사 기록에서 각 회사의 특정 디자인 테마와 로고를 사용자 지정할 수 있습니다.

도메인 사용자 지정

기본적으로 서비스 제공자 플러그인이 설치되어 있으면 핵심 테이블에 포함된 표준 비즈니스 규칙으로 인해 기록의 도메인이 기록과 연결된 회사의 도메인으로 설정됩니다. 회사는 작업, 사용자, 그룹, 위치, 부서 등의 테이블을 제어할 수 있습니다.

작업 테이블을 제외한 이러한 모든 테이블을 사용하여 기록이 생성되는 도메인을 재정의할 수 있습니다. 이렇게 하면 더 많은 사용자 지정 옵션이 제공됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

특정 용도의 도메인 분리 관리

이메일 알림에 대한 별도의 도메인을 설정하고 카탈로그, 테이블, 사용자, 그룹 및 뷰의 속성을 사용자 지정할 수 있습니다. 이를 통해 각 도메인에서 보다 구체적인 동작을 제공하여 고객에게 더 많은 유연성을 제공할 수 있습니다.

이메일

이메일 알림 및 재정의에 별도의 도메인을 사용할 수 있습니다. 알림에 별도의 도메인을 사용하는 경우 사용자의 전체 도메인이 아닌 첨부된 기록의 도메인만을 기반으로 재정의할 수 있습니다.

서비스 카탈로그

이제 고객이 카탈로그를 보고 액세스할 수 있도록 Service Catalog가 도메인으로 분리됩니다. 여러 항목을 사용하는 경우 항목은 OR 조건으로 처리됩니다. 서비스 제공자는 범주와 항목 자체를 관리하여 특히 자체 기준에 맞도록 해야 합니다.

사용자 및 그룹

관리자는 모든 도메인에 액세스해야 하므로 전역 도메인의 관리자 계정만 사용하십시오. 전역 도메인이 아닌 실제 도메인에서 모든 애플리케이션 테스트를 수행합니다. 전역 도메인에서 재정의가 제대로 처리되지 않습니다. 또한 관리자가 애플리케이션을 사용하려면 프로덕션에서 사용자 계정을 제공해야 합니다.

필드 작업

필드를 사용할 때 고려해야 할 몇 가지 사항이 있습니다. 이러한 필드에는 구성에 영향을 주는 다양한 변형이 있을 수 있으므로 세심한 주의를 기울여야 합니다.

목록

개인, 전역 및 도메인 목록과 각각에 대한 여러 보기가 있습니다.

양식

전역 및 도메인 목록과 각각에 대한 여러 뷰가 있습니다.

하나의 데이터베이스

작성하는 모든 필드는 하나의 데이터베이스에 모든 사용자에 대해 존재합니다. 새로 만들기 전에 전체 영향을 고려합니다.

주: ACL 스크립트는 실행되지 않기 때문에 목록에서 필드를 볼 수 없게 할 수 없습니다. ACL이 역할 기반만 있는 경우 읽기 ACL을 추가하여 사용자에게 필드를 숨길 수 있습니다.

테이블 생성

테이블을 생성할 때 `sys_domain` 또는 `sys_overrides` 필드를 추가해야 합니다. 인스턴스 사용자가 액세스해야 하는 데이터를 포함하는 모든 테이블에는 `sys_domain` 필드가 필요합니다. 프로세스를 확장하거나 지원하며 하위 도메인으로 플로우다운해야 하는 테이블에도 `sys_domain` 필드가 필요합니다.

도메인 선택기를 사용하여 도메인 분리 구성

도메인 선택기를 현명하게 사용하고 80/15/5 접근 방식을 기억하여 너무 많이 사용자 지정하여 인스턴스 성능에 영향을 주지 않도록 하십시오.

변경하기 전에 도메인 확인

도메인 선택기가 선택할 수 있도록 모든 도메인을 목록으로 수집합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세션 시간이 초과되고 로그아웃되지 않더라도 세션이 사용자 기록의 도메인으로 폴백됩니다. 동시에 상승된 역할도 잃게 됩니다. 이 경우 목록의 상단 프레임이 다시 로드되지 않은 경우 도메인 선택기에 마지막으로 선택한 도메인이 계속 표시될 수 있습니다. 따라서 인스턴스에서 잠시 자리를 비운 경우 목록을 완전히 다시 로드해야 합니다.

TOP 도메인 또는 전역 도메인에서 구성

도메인 분리는 구성과 사용자 및 그룹 정의에서 대부분 표준인 서비스를 고객에게 제공할 때 가장 적합합니다. "일회성" 솔루션을 더 많이 사용자 지정하고 생성할수록 오류 여지가 더 많이 생성됩니다. 프로세스와 비즈니스 논리를 만들 때 모든 변형은 각 고객에 대해 자동으로 작동하는 속성에 있어야 합니다. 프로세스는 필요에 따라 조정할 수 있지만 단일 고객을 위한 고유한 구성을 생성하는 시기와 범위를 결정할 때는 세심한 주의를 기울여야 합니다.

도메인을 구성할 때 "80-15-5" 접근 방식을 사용하여 커스터마이제이션에 너무 큰 여백을 만들어 오류를 발생시키지 않도록 해야 합니다.

- 구성에 권장되는 접근 방식:
  - **80%** 이상 표준
  - **15%** 이상 파라메트릭
  - 구성 **5%** 미만
- 제안된 변경이 전역 속성인지 구성 가능한 속성인지 결정합니다.
- 관리해야 하는 커스터마이제이션을 점점 더 추가하여 과도하게 빌드하지 마십시오. 대신 다음을 수행합니다.
  - 기본 시스템 기능부터 시작하여 변경하기 전에 간격이 있는지 확인합니다.
  - 노코드 솔루션을 찾으십시오.
  - 서버 측 스크립트를 사용하고, 모듈식 API를 빌드하고, 도메인으로 구분된 속성을 빌드합니다.
  - 클라이언트 스크립팅을 사용해야 하는 경우 API만 ServiceNow 사용합니다. "동기" 호출(클라이언트에서 서버로 오가는 호출, AJAX라고도 함)을 제한합니다.
  - 모든 스크립트를 논리적으로 작성하여 간단하고 효과적으로 유지하십시오. 코드 변경에 대한 동료 검토를 실시하고 모든 사람이 이 섹션의 내용을 서비스 제공자를 위한 도메인 분리 권장 방법 따르고 있는지 확인합니다.

도메인 분리 성능 고려 사항

애플리케이션 및 서비스에서 도메인 분리를 구성할 때는 생성하는 도메인의 수와 속성을 고려해야 합니다. 속성이 많은 도메인이 너무 많으면 인스턴스 성능에 영향을 줄 수 있습니다.

속성이 많은 도메인 제한

필요한 만큼 도메인을 생성할 수 있지만 인스턴스에 불필요한 도메인을 생성하지 마십시오. 속성이 많은 인스턴스에서 너무 많은 도메인에 가중치를 부여하면 인스턴스 성능에 영향을 줄 수 있습니다.

도메인의 수는 성능에 영향을 미치는 것이 아니라 도메인 안에 있는 것입니다. 속성이 너무 많으면 도메인 선택 속도가 느려져 고객의 전반적인 사용자 경험이 느려질 수 있습니다. 도메인 선택기를 로드하고 속성이 많은 도메인이 이미 많은 경우 도메인 선택기가 세션에서 제어권을 부여하기 전에 모든 도메인을 로드해야 합니다. 이 프로세스로 인해 도메인 선택기가 완료될 때까지 인스턴스의 아무 항목에도 액세스할 수 없는 중단이 발생할 수 있습니다. 새 도메인을 생성하기 전에 아래의 도메인 계층 구조로 이동합니다 도메인 관리 > 도메인 맵 그리고 실제로 새 도메인을 만들어야 하는지 또는 기존 도메인 계층 구조 가 작동할 수 있는지 여부를 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 선택기 사용 코어 UI

도메인 참조 선택기는 다음에서 사용할 수 있습니다 코어 UI. 참조 선택기를 사용하면 모든 도메인을 한 번에 로드하는 것이 아니라 도메인 선택기에 도메인 이름을 입력하기 시작할 때 도메인이 검색됩니다.

다음 단계에 따라 도메인 참조 선택기 코어 UI 를 활성화합니다.

1. 애플리케이션 네비게이터에서 `sys_properties.list`를 입력합니다.
2. *glide.ui.domain_reference_picker.enabled*속성을 True로 설정합니다.
3. 브라우저를 새로 고칩니다.

> 주: 먼저 몇 가지 테스트를 수행하지 않고 통합 또는 임포트 세트를 통해 많은 수의 도메인(30개 이상)을 업로드하지 마십시오. 그렇지 않으면 인스턴스가 작동 중지될 수 있습니다.

도메인 계층 구조 설정

도메인 계층 구조의 작동 방식을 알고 적절하게 설정하면 인스턴스의 속도 저하 및 성능 영향을 방지할 수 있습니다.

도메인 계층 구조에 따라 사용자는 홈 도메인과 모든 하위 도메인의 데이터에 액세스할 수 있습니다. 프로세스가 하위 도메인으로 흐르고 데이터가 위로 올라갑니다.

필요한 경우에만 기존 도메인 계층 구조를 변경합니다. 도메인의 상위 도메인을 업데이트하면 시스템은 도메인 계층 구조를 변경하는 모든 하위 도메인과 함께 상위 도메인을 다시 설정합니다. 도메인 계층 구조가 업데이트되면 시스템은 해당 도메인에 생성된 기록의 도메인과 관련된 모든 테이블에서 단계적 업데이트를 트리거합니다. 따라서 많은 수의 지원 테이블도 업데이트해야 합니다.

같은 이유로 도메인 계층 구조를 변경해야 하는 경우에도 대량 업데이트를 수행하지 마십시오. 도메인 계층 구조를 변경하기 위해 시스템에서 실행해야 하는 쿼리 수를 상상해 보십시오. 항상 작은 배치로 업데이트를 수행하십시오. 다음 업데이트 배치를 시작하기 전에 DWR(도메인 작업 요청) 기록이 처리되었는지 확인합니다. DWR은 도메인 계층 구조를 변경한 후 오류가 있는지 여부를 표시하는 보고서입니다.

DWR 기록 추적

syslog_domain 테이블의 메시지 열에서 완료된 **DWR** 실행 에 대한 정보 항목을 찾습니다. DWR이 완료되었는지 확인합니다.

도메인 로그에서 오류 및 경고 확인

도메인 경로, 프로세스 및 계층 구조 구성에서 오류 또는 경고를 찾으려면 도메인 로그를 확인합니다.

도메인 로그[syslog_domain] 테이블에서 도메인 로그를 찾을 수 있습니다. 도메인 계층 구조가 업데이트되면 시스템은 도메인 경로를 다시 계산하는 예약된 작업을 트리거합니다. 도메인 로그 테이블은 결과를 캡처합니다.

이 테이블에서 오류와 경고를 찾습니다. 이 테이블을 검토한 후 이러한 오류를 해결하고 도메인 경로 유효성 검사기를 다시 실행해야 합니다.

이 로그 예에서 시스템은 sys_ui_list 테이블에서 10개의 고아 기록을 탐지했습니다. 이러한 기록의 오류를 수정해야 도메인 경로가 성공적으로 실행될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

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:11722b0147323100 7f47563dbb9a7154 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

도메인 분리 오류에 대한 자세한 내용은 다음 문서를 참조하십시오 도메인 분리 오류 문제 해결.

기본 도메인의 중요도

도메인 구성은 도메인 분리 프로세스에서 매우 중요한 부분입니다. 기본 도메인을 설정하지 않으면 새 작업과 사용자 기록이 전역 도메인으로 이동합니다. 누구나 전역 도메인의 기록을 볼 수 있으므로 데이터를 볼 필요가 없을 때도 데이터를 볼 수 있습니다.

기본 도메인을 설정하면 해당 기록은 관리자 이외의 사용자에게 표시되지 않습니다.

주: 사용자에게 기본 도메인 또는 상위 도메인에 대한 가시성을 부여하여 기본 액세스를 변경할 수 있습니다.

인스턴스의 도메인 레코드에 대해 항상 하나의 기본 도메인을 설정해야 합니다. 기본 도메인은 시스템에서 아직 도메인에 할당되지 않은 작업 및 사용자 기록을 자동으로 할당하는 위치입니다.

Domain Administration 화면에서 기본 도메인을 만들 때 이름 필드에 이름 Default를 추가하여 다른 도메인과 구별합니다. 기록에 대한 기본 확인란을 선택합니다.

기본 도메인에서 만든 레코드를 정기적으로 유지관리하고 올바른 도메인으로 이동합니다. 기록이 기본 도메인에 자주 표시되는 경우 이유를 조사해야 할 수 있습니다. 이상적으로는 모든 기록이 전역 도메인이나 기본 도메인이 아닌 적절한 도메인에서 생성되었는지 확인해야 합니다.

쿼리 및 도메인 액세스 포함

사용자 또는 그룹이 액세스할 수 없는 도메인의 데이터를 확인해야 하지만 해당 사용자를 도메인으로 이동하지 않으려는 경우와 같은 특수한 경우에만 "포함" 쿼리를 사용합니다. 도메인 "포함" 및 도메인에 대한 사용자 또는 그룹 액세스 권한을 만드는 것은 반드시 필요한 경우에만 예외여야 합니다.

"Contains"는 다대다인 도메인 간 관계이며 프로세스 플로우에 영향을 주지 않습니다. 많은 수의 도메인 "포함" 관계를 만들거나 광범위한 액세스 권한을 제공하면 OR 조건이 너무 많은 쿼리가 생성됩니다. OR 조건이 느려지고 인스턴스 성능에 영향을 미치는 경우 너무 많은 "포함" 관계를 사용하는 대신 다음과 같이 도메인 계층 구조를 설정합니다.

샘플 쿼리

```
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
```

사용자를 도메인으로 이동하기 전에 해당 도메인에 대한 액세스 권한이 있는지 확인합니다. 이점과 한계를 비교하십시오. 위의 쿼리는 하나의 포함 관계에 대한 것입니다. 도메인에 다른 도메인이 포함되어 있고 해당 도메인이 다른 여러 도메인의 상위 도메인인 경우 더 많은 OR 조건이 있습니다. 도메인 맵을 생성할 때는 인스턴스 성능에 영향을 주지 않도록 주의해야 합니다.

도메인 경로 쿼리 메서드

도메인 경로를 사용하여 효과적인 쿼리를 만들 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 스풀링(sys_domain) 또는 도메인 번호 매기기 대신 도메인 경로를 사용합니다. 도메인 경로를 사용하는 쿼리는 스풀링이나 번호 매기기 보다 훨씬 빠릅니다.

도메인 경로는 도메인 분리를 사용하는 인스턴스에 대한 기본 쿼리 방법입니다.

인스턴스에서 쿼리 방법을 확인하려면 관리자 대시보드에서 다음 시스템 속성을 찾습니다.

- *If domain path is enabled*: 시스템 속성 테이블에 glide.sys.domain.provider=domain_paths 및 glide.sys.domain.paths.installed=true가 표시됩니다.
- *If domain path is not enabled*: 시스템 속성 테이블에 glide.sys.domain.provider != domain_paths,glide.sys.domain.paths.installed=false가 표시됩니다.

느린 쿼리 및 SQL 디버깅

SQL 및 느린 쿼리를 디버깅하면 인스턴스의 속도 저하 문제를 해결하는 데 도움이 될 수 있습니다.

인스턴스를 디버그할 때 SQL 디버깅을 사용하도록 설정하여 느린 쿼리를 찾거나 시스템 진단 > 통계 > 느린 쿼리로 이동하여 느린 쿼리 [sys_query_pattern] 테이블을 확인하여 느린 쿼리를 찾을 수 있습니다. 이 테이블은 인스턴스에 느린 쿼리를 모두 저장합니다.

테이블을 검색할 때 domain_path 가 포함된 쿼리를 찾아 느린 쿼리가 인스턴스의 도메인 경로 때문인지 확인합니다.

느린 쿼리를 찾으면 느린 이유를 분석해 보세요.

쿼리 속도가 느린 일반적인 이유

- 쿼리에 OR 조건이 너무 많습니다(자세한 내용은 문서 쿼리 및 도메인 액세스 포함참조). 도메인 계층 구조에서 포함 또는 가시성이 필요하지 않은 계층 구조 수준에 사용자 또는 도메인을 배치합니다.
- 쿼리 메서드는 도메인 경로 쿼리 메서드가 아닙니다(자세한 내용은 문서를 참조 도메인 경로 쿼리 메서드). 도메인 경로 쿼리 메서드를 사용하지 않는 경우 에 문의하십시오 고객 서비스 및 지원.
- 데이터베이스에 있는 내용을 빠르게 볼 수 있도록 쿼리를 인덱싱해야 합니다. 느린 쿼리를 식별할 수 있는 경우 "계획 설명"을 실행하여 사용 가능한 인덱싱 옵션이 있는지 확인합니다. "계획 설명"은 쿼리와 쿼리에서 진행 중인 작업을 보여주는 SQL 함수입니다.

이전 비즈니스 규칙 쿼리

쿼리 전 비즈니스 규칙을 사용하여 인스턴스에서 데이터 분리를 지원할 수 있습니다. ServiceNow 도메인 분리를 지원하는 애플리케이션은 데이터 분리 및 데이터 라우팅만 지원하거나, 고급 비즈니스 논리 분리를 지원하거나, 애플리케이션의 테넌트(고객) 수준 관리를 지원할 수 있습니다.

쿼리 전 비즈니스 규칙은 도메인 분리 환경 내에서 데이터 분리를 지원하는 데 사용하는 보조 코드입니다.

⚠ 경고: Domain Separation 플러그인 대신 쿼리 전 비즈니스 규칙을 사용하지 마십시오. 이 비즈니스 규칙은 플러그인만큼 안전하게 데이터 유출을 방지하지는 않습니다.

데이터 분리에 Before Query 비즈니스 규칙 사용

다음 상황에서 데이터 분리와 함께 쿼리 전 비즈니스 규칙을 사용할 수 있습니다.

- 애플리케이션에서 도메인 분리를 지원하지 ServiceNow 않으며 서비스 제공자 조직 외부에 있는 하나 이상의 비내부 고객에게 테이블 또는 행 액세스 권한을 부여하거나 제한해야 하는 경우.

  ⓘ 주: 개발을 시작하기 전에 고객 지원에 해당 제품의 애플리케이션 로드맵에 대해 문의하십시오 ServiceNow . 도메인 지원 향상은 향후 릴리스에서 제공될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 테이블이 도메인으로 분리되어 있지만 시스템의 도메인 세트에만 적용되는 특정 조건에 따라 해당 행에 대한 액세스를 허용하거나 제한해야 하는 경우.

  주: 예를 들어 X 도메인의 고객에게 해당 도메인을 지원하는 벤더가 여러 개 있고 해당 벤더에게는 할당된 기록만 볼 수 있는 액세스 권한이 부여됩니다.

쿼리 전 비즈니스 규칙을 생성하기 전에 고려해야 할 사항

Before Query 비즈니스 규칙을 스크립팅하여 사용자 정보, 그룹 구성원 자격, 회사, 역할 또는 기록별 필드 조건의 조합을 기반으로 상위 및 하위 테이블 액세스를 방지할 수 있습니다. 이전 쿼리 비즈니스 규칙은 별도의 도메인에 배치되고 도메인 계층 구조의 특정 분기에 전역적으로 적용되도록 생성됩니다.

- 가능한 경우 도메인 계층 구조의 가능한 최하위 부분에 쿼리 전 비즈니스 규칙을 생성하여 적용되는 사용자에 대해서만 규칙이 실행되도록 합니다.
- 시스템에는 비즈니스 규칙이 실행되지 않을 수 있거나 사용자가 트리거한 상호작용이 비즈니스 규칙 실행을 트리거하지 않을 수 있는 시나리오가 있음을 알고 있습니다. 예를 들어, 비즈니스 규칙 실행이 꺼진 변환 맵이나 워크플로우가 비활성화된 스크립트가 있는 경우 비즈니스 규칙이 실행되지 않습니다.
- 항상 조건 필드를 채워 규칙이 실행되는 시기를 지정합니다. 예를 들어 비즈니스 규칙이 도메인의 특정 벤더에만 적용되는지 여부를 지정할 수 있습니다.

  경고: 비즈니스 규칙(특히 쿼리 비즈니스 규칙)을 디자인하고 코딩할 때 인덱스되지 않은 필드에서는 OR 절과 검색을 제한합니다. 인덱스되지 않은 필드에 OR 절과 검색이 너무 많으면 쿼리 속도가 느려지거나 인스턴스 성능에 영향을 줄 수 있습니다.

- 필요한 경우에만 비즈니스 규칙 쿼리 이전을 사용합니다. 쿼리 전 규칙이 너무 많으면 인스턴스의 성능에 영향을 줄 수 있습니다.

쿼리 이전 비즈니스 규칙은 ACL(접근 제어 목록)보다 먼저 실행되며 일반적으로 성능이 더 좋습니다. 이는 리턴된 결과를 시스템의 여러 도메인에 액세스할 수 있는 SP(서비스 제공자) 환경의 사용자로 제한하는 경우에 특히 그렇습니다.

주: 데이터를 필터링할 때 `### #### ####` 메시지가 표시되지 않는 사용자에게는 데이터 필터링이 투명합니다(ACL과 달리).

쿼리 전 비즈니스 규칙 및 ACL을 사용하지 않는 경우

쿼리 전 비즈니스 규칙 및 ACL을 사용하여 고객 데이터를 분리할 때는 주의하십시오. 비즈니스 규칙과 ACL을 모두 사용하여 사용자 지정을 만든 다음 유지 관리해야 합니다. 사용자 지정은 잠재적으로 성능 문제를 일으킬 수 있습니다. 개발 팀은 시스템을 손상시키지 않도록 프로세스를 만들어야 합니다.

도메인 분리는 널리 지원되는 프레임워크인 현재 도메인 경로 쿼리 메서드(v3)를 통해 확장성과 거버넌스를 모두 제공합니다. ServiceNow 플랫폼 및 앱 팀은 프레임워크를 유지관리하여 고객의 부담을 덜어줄 책임이 있습니다.

많은 인스턴스에 많은 고객이 있는 회사의 경우 이전 쿼리 및 ACL을 과도하게 사용하면 데이터베이스 쿼리가 제대로 수행되지 않을 수 있습니다.

도메인 분리를 사용하는 방법

플러그인을 사용하여 도메인 분리를 활성화할 수 있습니다 ServiceNow . 개발 팀의 지원을 받는 제품 관리자가 기능을 관리합니다. 도메인 분리 기능에 대한 개선 사항 및 수정 사항이 릴리스에 ServiceNow 포함되어 있습니다. 인스턴스 소유자는 에서 https://support.servicenow.com 와 같은 서비스 포털자원을 참조 고객 서비스 및 지원 하여 도메인 분리에 대한 지원을 받을 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트에서 도메인 경로 방지

도메인 경로로 인해 스크립트 값이 변경되거나 손상될 수 있으므로 스크립트에 도메인 경로를 사용하지 마십시오.

도메인 계층 구조를 변경하면 도메인 경로가 다시 계산되고 해당 값이 변경되므로 스크립트는 도메인 경로에 종속되지 않아야 합니다. 이 경우 스크립트가 쓸모 없거나 오류가 발생하거나 중단될 수 있습니다. 가장 좋은 전략은 도메인 경로를 기반으로 스크립트를 작성하지 않는 것입니다.

도메인 경로에 의존하는 대신 스크립트에서 **sys_domain** 필드를 사용합니다. 도메인 계층을 변경하면 도메인 경로가 다시 계산되고 해당 값이 변경되어 스크립트가 무용지물이 되거나, 오류가 발생하거나, 중단될 수 있습니다. 스크립트를 직접 작성하기 전에 몇 가지 아이디어를 얻으려면 **sys_domain** 필드를 사용하는 기본 시스템 비즈니스 규칙을 찾아보십시오.

ServiceNow 플랫폼은 각 인스턴스의 도메인 계층 구조 차이 문제를 방지하기 위해 업데이트 세트의 sys_domain_path 값을 캡처하지 않습니다. 따라서 업데이트 세트를 임포트한 후 도메인 계층 구조를 확인하여 기록의 도메인 경로 값이 올바른지 확인해야 합니다.

도메인 경로에 대한 자세한 내용은 해당 문서를 도메인 분리 센터참조하십시오도메인 분리 요청.

도메인 할당

도메인을 할당하는 방법은 sys_domain 필드의 값에 영향을 줍니다. 할당에는 각 도메인에서 애플리케이션이 작동하는 방식에 영향을 주는 디자인 및 비즈니스 속성이 포함됩니다.

sys_domain 필드의 값

sys_domain 필드의 값에는 다음 중 하나에 의해 기록에 할당된 도메인이 포함됩니다.

- 사용자가 속한 회사
- 기록을 만들 때 사용되는 비즈니스 규칙
- 기록을 만들 때 사용되는 모듈
- 기록을 만들 때 사용되는 양식 템플릿
- 상위 기록의 도메인
- 사용자 기록에 할당된 도메인
- 작성한 사용자의 도메인

도메인 할당 전략과 설계가 잘 문서화되고 테스트되어 이러한 전략과 설계가 올바른 도메인에 삽입될 때 기록을 생성하는지 확인하십시오. 이렇게 하면 각 도메인을 복제하거나 수정해야 하는 경우 각 도메인의 속성을 확인할 수 있습니다.

도메인 분리 및 고객 서비스 관리**(CSM)** 플러그인

최상의 결과를 얻으려면 플러그인의 속성이 어떻게 작동하는지 알고 있어야 합니다 CSM . 플러그인이 사용 설정되면 도메인의 기록 상태를 볼 수 있습니다.

인스턴스 소유자는 이 속성을 사용하도록 *csm_auto_account_domain_generation* 문의 고객 서비스 및 지원 해야 합니다.

주: 이 기본 시스템 속성은 시스템 속성 테이블에 있으며 CSM 플러그인이 활성화된 후에 사용할 수 있습니다.

속성의 기능

고객 서비스 애플리케이션에서 새 계정이 생성될 때마다 도메인이 생성되어 TOP 도메인 아래에 배치됩니다. 계정 양식의 상위 필드가 채워지고 새 기록이 삽입되면 해당 계정이 상위 계정의 하위 도메인으로 생성됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 속성이 예가 아니고 도메인을 사용하는 경우 발생하는 작업

도메인 분리 환경의 새 계정 기록은 자동으로 기본 도메인에 배치됩니다.

헤더 막대에서 플러그인이 활성화된 기록의 상태를 볼 수 있습니다.

도메인 분리 도움말

도메인 분리에 대한 추가 지원

도메인 분리의 비디오 개요

탐색, 학습, 개발



권장 프랙티스

도메인 구조를 현명하게 생성하고 개발하기 위한 팁 및 힌트

서비스 제공자를 위한 개념

플랫폼과 함께 ServiceNow 작동하여 일반적인 사용 사례를 해결하는 데 도움이 되는 개념



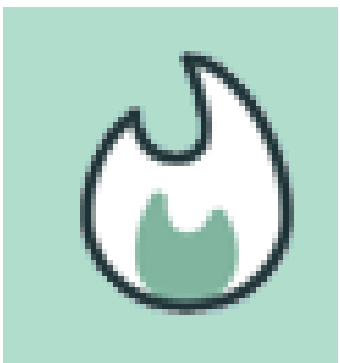
애플리케이션별 지원 수준

애플리케이션이 도메인 분리를 지원합니까? 지원 수준 및 사용 사례를 참조하십시오.



클래스

- 개발자의 경우: ServiceNow 개발자 사이트 도메인 분리
- 서비스 제공자의 경우: 서비스 제공자용 도메인 분리(Now Learning 로그인 필요)



Safe Workplace Suite 및 도메인 분리

ServiceNow Safe Workplace 애플리케이션은 COVID-19와 같은 긴급 상황 및 팬데믹 이후 직장을 다시 열고 직원의 건강과 안전을 지원하는 데 도움이 됩니다. 이 제품군에는 조직의 이동성, 복구 및 재구축에 도움이 되는 여러 애플리케이션이 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



설정 및 관리

- 업그레이드
- 도메인 분리 요청
- 도메인 생성
- 내부 또는 외부 고객에게 위임할 수 있는 구성



문제 해결

- 알려진 오류 포털에서 알려진 오류 문서 검색
- 연락처 고객 서비스 및 지원
- 커뮤니티에서 질문 또는 답변하기

도메인 분리 설정 및 관리

도메인 분리를 설정하려면 플러그인 활성화를 요청하고, 옵션을 설정하고, 도메인에 사용자와 기록을 할당해야 합니다.

도메인 분리를 설정하려면 다음을 수행합니다.

1. 도메인 분리 요청
2. 도메인 생성
3. 테이블에 도메인 필드 추가

도메인에서 다음과 같은 기본 관리 작업을 수행할 수도 있습니다.

- 도메인 활성화 또는 비활성화
- 도메인 관계 보기
- 도메인 범위 확장
- 도메인별 선택 목록 만들기

도메인 분리를 설정하고 기본 관리를 수행한 후에 수행할 작업 목록은 을 참조하십시오 고급 도메인 분리 관리 .

도메인 분리 요청

모든 도메인 지원 기능은 **Domain Support - Domain Extensions Installer**라는 플러그인으로 활성화됩니다. 관리자는 이 플러그인의 활성화를 요청할 수 있습니다.

시작하기 전에

구독을 구매하려면 ServiceNow 계정 관리자에게 문의하십시오. 고객 관리자는 일반적으로 며칠 이내에 조직의 프로덕션 및 하위 프로덕션 인스턴스에서 플러그인을 활성화하도록 *com.glide.domain.msp_extensions.installer* 준비할 수 있습니다.

고객 관리자가 없거나 구매 후 정품 인증 지연을 결정하거나, 하위 프로덕션 인스턴스에서 무료로 제품을 평가하려고 할 경우, 다음 단계를 수행하십시오.

필요한 역할: 관리자

이 태스크 정보

Domain Support - Domain Extensions Installer 플러그인이 이미 활성 상태인 경우 기존 구현과의 충돌을 방지하기 위해 Domain Support - Domain Extensions Installer 플러그인의 컨텐츠가 설치되지 않습니다.

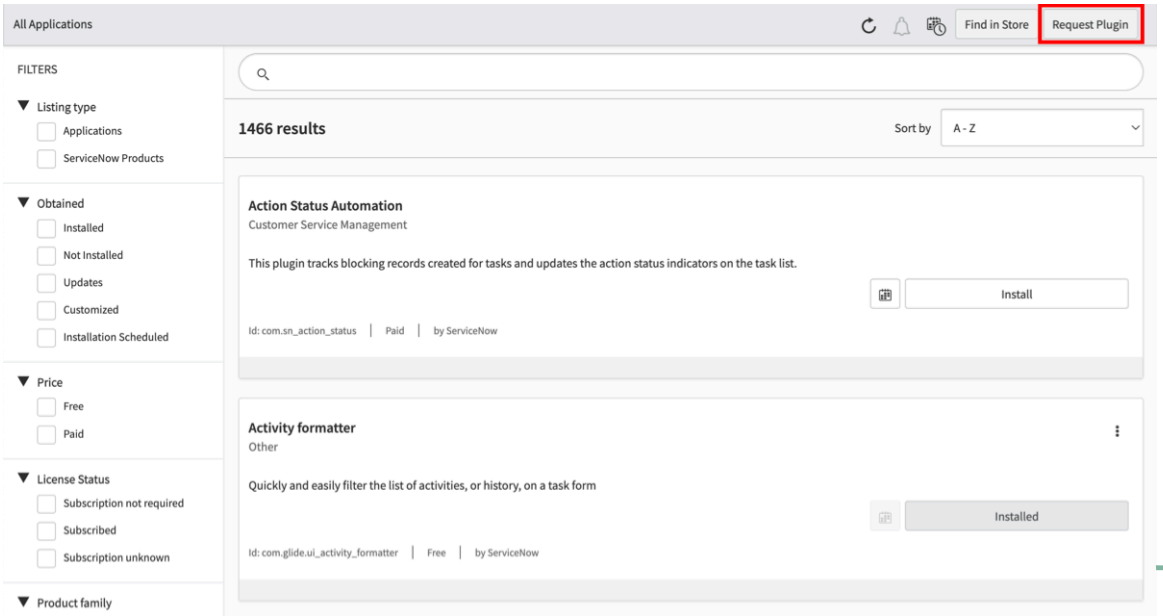
도메인 분리가 회사 분리를 대체합니다. Helsinki 릴리스부터 Company Separation 플러그인을 더 이상 활성화할 수 없습니다. 그러나 도메인 분리를 활성화할 때 회사 분리가 이미 활성화되어 있으면 두 플러그인이 동시에 활성화됩니다. 속성을 사용하여 회사 분리 활성화 상태를 제어할 수 있습니다 *glide.db.separation.field*.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

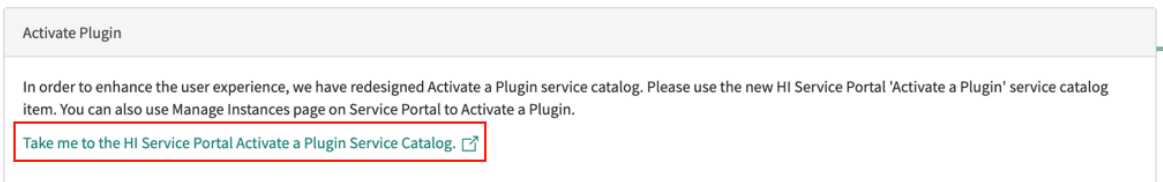
주: 도메인 경로는 헬싱키 이상의 모든 고객에 대해 사용됩니다. 도메인 번호 매기기는 더 이상 사용되지 않습니다. 고객 서비스 및 지원 가 업그레이드를 지원할 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 모든 애플리케이션 페이지에서 플러그인 요청을 선택하여 Now Support의 플러그인 활성화 양식을 엽니다.



3. Now Support에서 Now Support 서비스 포털 서비스 카탈로그에 액세스하는 링크를 선택합니다.



4. 인스턴스를 선택합니다.
5. 작업 **>** 플러그인 활성화를 선택합니다.
6. 플러그인 활성화 양식에서 다음 정보를 입력합니다.

플러그인 활성화 양식

필드	설명
대상 인스턴스는 무엇입니까?	플러그인을 활성화할 인스턴스입니다.
어떤 플러그인을 활성화하시겠습니까?	활성화할 플러그인의 이름입니다.

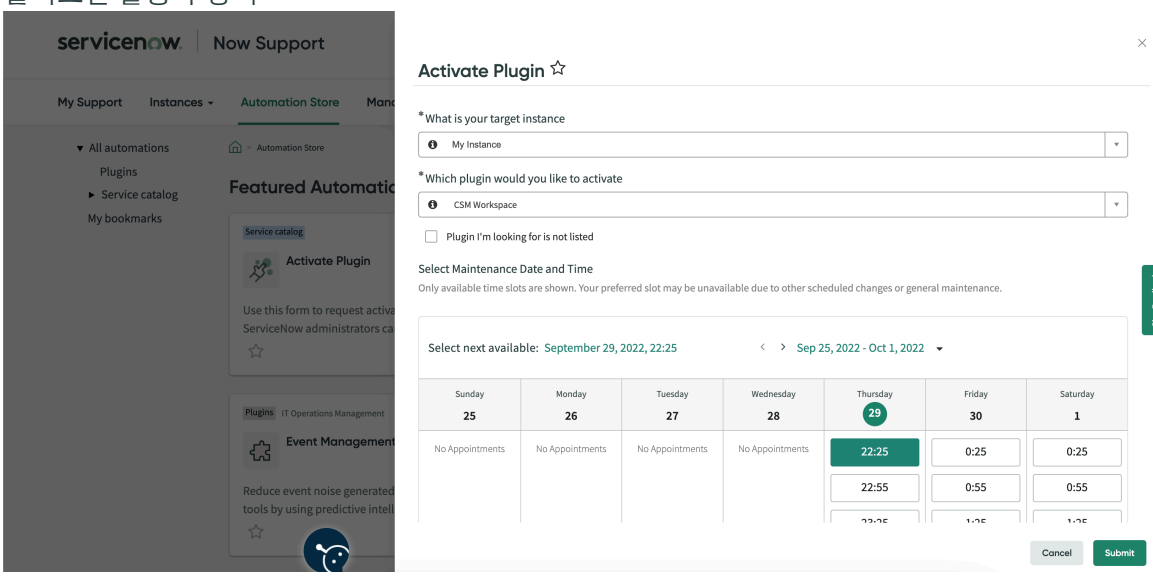
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 시스템에서 원하는 플러그인을 나열하지 않거나 OEM 또는 온프레미스 인스턴스에서 플러그인을 활성화하는 경우 찾고 있는 플러그인이 목록에 없음 확인란을 선택한 다음 플러그인 이름을 입력합니다.
유지관리 날짜 및 시간 선택	플러그인을 활성화하는 날짜 및 시간입니다. 주: 플러그인은 미국 태평양 시간대의 모든 영업일에 두 번(오전과 저녁에 각각 한 번씩) 활성화됩니다. 특정 시간에 플러그인을 활성화해야 하는 경우 이유/설명 필드에 요청을 입력합니다.

Example

예를 들어, 내 인스턴스라는 인스턴스에서 CSM Workspace 플러그인을 활성화하는 다음 양식을 참조하십시오.

플러그인 활성화 양식



7. 제출을 선택합니다.
   플러그인 요청에 대한 자세한 내용은 다음을 참조하십시오. 의 서비스 카탈로그 [KB0751715] 문서에서 플러그인 요청 Now Support 지식베이스.

결과
Domain Extension Installer 플러그인을 활성화하면 다음 기능을 사용할 수 있습니다.

- 도메인 분리는 도메인 `[sys_domain]` 테이블을 기반으로 합니다.
- 위임된 관리를 사용하면 각 도메인이 별도의 정책을 가질 수 있습니다.
- 모든 기록은 전역 도메인의 일부입니다.
- 현재 사용자의 도메인은 다른 도메인의 기록을 보거나 작업할 때 사용할 도메인을 결정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

도메인 분리 플러그인

도메인 분리 플러그인

Domain Support - Domain Extensions Installer 플러그인은 여러 도메인 분리 기능 및 속성을 한 번에 활성화합니다. 이 플러그인을 일반적으로 도메인 분리 플러그인이라고 합니다.

Domain Separation 플러그인 활성화를 위한 권장 방법

도메인 분리 개발의 일부로 관리자는 이 플러그인의 활성화를 요청 해야 합니다. 최상의 결과를 얻으려면 개발 프로세스를 시작할 때, 가급적이면 다른 플러그인을 사용하기 전에 Domain Separation 플러그인을 활성화하십시오.

중요사항: 도메인 분리(플러그인 com.snc.pa.domain_support)를 활성화하기 전에 Domain Extensions Installer 플러그인(com.glide.domain.msp_extensions.installer)을 활성화하도록 요청합니다.

구현이 ServiceNow 끝날 무렵에 도메인 분리를 사용하거나 인스턴스가 활성화되면 애플리케이션이 성능과 프로세스 모두에서 위험에 처하게 됩니다. 기존 인스턴스에서는 개발 구조에 따라 플랫폼과 그 유용성에 대한 위험이 높을 수 있습니다. 도메인 분리 프로세스에 대한 자세한 내용은 다음 문서를 참조하십시오 도메인 분리 탐색.

예를 들어 Domain Separation 플러그인이 활성화되면 도메인 (sys_domain) 열이 작업 테이블에 추가되고 모든 기존 기록이 자동으로 전역에 배치됩니다. 스크립트를 사용하여 모든 기록을 올바른 도메인에 할당하려면 상위/하위 계층 구조를 설정해야 합니다. 이러한 유형의 스크립트 작업은 데이터 손상 또는 손실의 위험이 있으며 많은 양의 데이터가 이동됨에 따라 프로덕션 중단 시간이 발생할 수 있습니다. 또한 플랫폼 코드의 대부분은 비즈니스 규칙, 클라이언트 스크립트, 양식 뷰 및 워크플로우와 같은 전역에 배치됩니다.

고객이 코드를 만들거나 수정 ServiceNow 하면 플랫폼 성능과 사용성에 위험이 있습니다. 인스턴스 소유자는 이러한 유형의 접근 방식으로 구현이 심각하게 지연되거나 가동 중지 시간이 길어질 수 있습니다.

Domain Separation 플러그인의 기능

이러한 기능은 플러그인을 활성화할 때 활성화됩니다.

- 도메인 분리는 도메인 `[sys_domain]` 테이블을 기반으로 합니다.
- 위임된 관리를 사용하면 각 도메인이 별도의 정책을 가질 수 있습니다.
- 모든 기록은 전역 도메인의 일부입니다.
- 현재 사용자의 도메인은 다른 도메인의 기록을 보거나 작업할 때 사용할 도메인을 결정합니다.

관련 정보

서비스 제공자를 위한 도메인 분리 권장 방법

도메인 시스템 속성 및 사용자 기본 설정

관리자는 도메인 범위를 제어하는 속성 및 사용자 기본 설정에 액세스할 수 있습니다.

속성

도메인 분리를 새로 활성화하면 모든 관련 데이터 또는 프로세스에 대한 도메인 범위가 기록의 도메인으로 자동으로 제한됩니다. 사용자가 양식에서 기록을 볼 때 기록의 관련 데이터(예: 참조 선택기 및 관련 목록 데이터) 및 적용된 프로세스(예: 비즈니스 규칙 및 클라이언트 스크립트)는 기록의 도메인 범위로 제한됩니다. 여러 탭에 기록이 있는 경우 각 탭에는 해당 탭 내에서 연 기록에

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

따라 고유한 도메인 범위가 있습니다. 다음 속성은 도메인 범위를 기록의 도메인과 사용자의 현재 세션 도메인으로 제한합니다.

도메인 시스템 속성

속성	세부사항
glide.sys.domain.use_record_domain_for_processes	모든 프로세스에 대해 도메인 범위를 기록의 도메인으로 제한합니다. 이 속성은 비즈니스 규칙에 적용되지 않습니다. 비즈니스 규칙은 항상 도메인 기록에서 처리됩니다. • 유형: true | false • 기본값: True • 위치: 시스템 속성 [sys_properties] 테이블
glide.sys.domain.use_record_domain_for_data	모든 데이터에 대해 도메인 범위를 기록의 도메인으로 제한합니다. • 유형: true | false • 기본값: Fuji에서 새 도메인을 활성화하면 True입니다(Fuji 이전 인스턴스에서의 업그레이드는 테이블에 이 속성이 없음). • 위치: 시스템 속성 [sys_properties] 테이블

or 속성이 true로 설정되면 설정에 관계없이 다음 속성이 사용되지 않습니다.*glide.sys.domain.use_record_domain_for_dataglide.sys.domain.use_record_domain_fo*

- *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*

전체 속성 목록은 사용 가능한 시스템 속성을 참조하십시오.

주:

Jakarta 릴리스부터 도메인 분리를 새로 활성화하면 세션 도메인이 도메인 테이블에서 실행되는 비즈니스 규칙을 결정합니다. 이전 버전에서는 도메인 테이블에서 실행된 비즈니스 규칙이 새로 생성된 도메인의 계층 구조에 따라 설정되었습니다. 이 동작은 속성에 의해 수정됩니다 *glide.sys.domain.skip_domain_insert_businessrules*. 이 속성을 true로 설정하면 도메인 삽입 성능이 크게 향상됩니다.

도메인 테이블에서 실행되는 비즈니스 규칙의 도메인 범위 속성

속성	세부사항
glide.sys.domain.skip_domain_insert_businessrules	도메인 테이블에서 실행되는 비즈니스 규칙의 도메인 범위를 지정합니다. 도메인 분리를

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 테이블에서 실행되는 비즈니스 규칙의 도메인 범위 속성

속성	세부사항
	새로 활성화하면 속성 기본값이 true이고 비즈니스 규칙은 세션 도메인에 의해 결정됩니다. 기존 구현에서 속성 기본값은 false이고 비즈니스 규칙은 새로 생성된 도메인의 계층 구조에 따라 결정됩니다. • 유형: true | false • 기본값: Jakarta로 시작하는 새 도메인 활성화에서 True입니다. 기존 구현에서는 False입니다.
glide.sys.domain.skip_non_global_businessrule_if_nodomain	queryNoDomain()을 사용하거나 테이블이 도메인으로 구분되지 않은 경우 전역 도메인의 bus.rules만 실행되므로 다른 비즈니스 규칙을 건너뛸 수 있습니다. • 유형: true | false • 속성을 false로 설정하면 이전 동작이 복원되고 권장 사례에 ServiceNow® 맞지 않습니다. • 권장: 테이블을 도메인 분리하십시오. 항상 세션 도메인보다는 레코드의 도메인을 사용하십시오.

사용자 기본 설정

또한 사용자 관리자는 전역 또는 사용자 단위로 다음 사용자 기본 설정을 설정할 수 있습니다.

도메인 범위 사용자 기본 설정

기본 설정	범주	업데이트한 사람	세부사항
glide.domain.session_scope	도메인	관리자만	예일 때는 기본 범위를 기록의 도메인이 아닌 사용자의 세션 도메인으로 설정합니다. false인 경우 기본 범위는 기록의 도메인입니다. domain_expand_scope 사용자 역할을 가진 사용자는 필요에 따라 도메인 범위를 변경할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 범위 사용자 기본 설정

기본 설정	범주	업데이트한 사람	세부사항
			• 유형: true | false • 기본값: false
glide.domain.session_scope_notification	도메인	관리자만	true인 경우, 기록 값에 확장된 도메인 범위가 포함되어 있다는 시각적 신호를 표시합니다. false인 경우 알림이 숨겨집니다. • 유형: true | false • 기본값: True

관련 정보

도메인 분리 애플리케이션 속성

도메인 생성

[domain] 테이블에 레코드를 생성하여 도메인을 생성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
새 도메인을 만들 때는 다음 사항에 유의하십시오.

- 하나의 도메인만 기본 도메인이 될 수 있습니다.
- 하나의 도메인만 주요 도메인이 될 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 도메인 관리 > 도메인.
2. 새로 만들기를 클릭합니다.
3. 필요한 필드를 입력합니다(표 참조).
4. 제출을 클릭합니다.

도메인 양식 필드

필드	설명
이름	도메인의 고유한 이름을 입력합니다.
유형	도메인을 설명하는 도메인 유형을 선택합니다. 기본적으로 도메인 유형은 벤더, 고객 및 *MSP*입니다. 원하는 항목을 추가할 수도 있습니다.
기본	이 도메인이 계층 구조의 최상위 도메인이 될 경우 확인란을 선택합니다. 최상위 도메인에는 하위 도메인만 있고 상위 도메인은 없습니다.
기본값	이 도메인이 계층 구조의 기본 도메인이 될 경우 선택합니다.
상위	이 도메인을 포함하는 계층 구조에서 더 높은 도메인의 이름을 선택합니다. 이 필드에는 도메인 맵에 표시할 도메인에 대한 값이 있어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	도메인을 사용할 수 있도록 하려면 확인란을 선택합니다. 이 도메인이 도메인 맵에 나타나도록 하려면 이 옵션을 선택해야 합니다.
설명	도메인에 대한 설명을 입력합니다.

또한 각 도메인 기록에는 다음과 같은 여러 관련 기록이 있을 수 있습니다.

- 회사
- 도메인 포함
- 포함 기준

다음에 수행할 작업
도메인 계층 구조를 변경하려면 도메인 포함 관련 목록으로 이동하여 포함 관계의 하위(포함된) 도메인인 도메인 기록을 선택합니다.

도메인을 기본값으로 설정

도메인을 아직 도메인에 할당되지 않은 작업 및 사용자 기록이 시스템에서 자동으로 할당되는 기본 도메인으로 설정했습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보

주: 기본 도메인을 설정하지 않으면 새 작업과 사용자 기록이 전역 도메인에 배치됩니다.

프로시저

1. 다음으로 이동 모두 > 도메인 관리 > 도메인.
2. 기본 도메인으로 지정할 도메인(예: Main)을 엽니다.
3. 기본 필드를 추가하도록 양식 레이아웃을 구성합니다.
4. 기본값 확인란을 선택합니다.
5. 업데이트를 클릭합니다.

특정 기록에 대한 도메인을 수동으로 관리

기본적으로 시스템은 사용자의 회사 기록을 기반으로 도메인을 자동으로 할당합니다. 그러나 도메인 관리자가 특정 기록이 속한 도메인을 수동으로 관리하려는 경우도 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
관리되는 도메인 필드를 사용하면 도메인 관리자가 회사 기록에서 자동으로 할당된 도메인을 사용하는 대신 사용자, 그룹, 부서, 위치 또는 CI 기록에 대한 도메인을 수동으로 선택할 수 있습니다. 관리되는 도메인 필드는 다음 기록 유형에서 사용할 수 있습니다.

- 사용자 기록
- 그룹 기록
- 부서 기록

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 위치 기록
- CI 기록

프로시저

1. 수동으로 관리할 기록으로 이동합니다.
2. 관리되는 도메인 확인란을 선택합니다.
3. 도메인 필드에서 기록에 대한 도메인을 선택합니다.
4. 업데이트를 클릭합니다.

관리되는 도메인 확인란의 선택을 취소하면 도메인 필드가 숨겨지고 기록은 기록 회사의 도메인 값을 사용합니다.

관련 정보

서비스 제공자를 위한 도메인 분리 권장 방법

도메인 분리 테이블

도메인 분리 테이블 기능을 사용하면 인스턴스에서 도메인 분리된 테이블을 한눈에 볼 수 있습니다.

개요

도메인 분리 테이블 기능을 사용하여 도메인으로 구분된 테이블을 확인합니다. 왼쪽 탐색 창의 도메인 분리 테이블에 액세스하려면 모두 필터에 "도메인"을 입력하기 시작합니다.

이 뷰를 필터링하여 열 이름을 표시하거나 제거하여 테이블에 포함된 특정 속성이나 속성을 찾을 수 있습니다. 목록에는 두 가지 테이블 유형이 표시됩니다.

- 명시적 *sys_domain* 열이 있는 테이블로, 열 이름이 목록에 값을 표시합니다 *sys_domain*.
- 속성을 사용하여 *domain_master* 참조된 기록에서 도메인 분리를 파생시키는 테이블로, 속성 열에 값이 포함됩니다 *domain_master=ref-field-value*.

열 이름 메뉴에서 일치 표시 또는 필터링 선택 항목을 사용하면 이 두 가지 유형의 테이블을 볼 수 있습니다.

도메인 재정의 뷰어

도메인 재정의 뷰어를 사용하면 전체 인스턴스에서 모든 프로세스 재정의를 한 번에 보고 관리할 수 있습니다.

개요

스크립트에서 재정의에 대한 정교한 검색을 생성하는 대신 도메인 재정의 뷰어를 사용하여 빠르게 찾을 수 있습니다. 왼쪽 탐색 창의 **Domain Override Viewer**에 액세스하려면 **All** 필터에 "domain"을 입력하기 시작합니다.

도메인 무효화 뷰어의 테이블 선택기에는 해당 테이블의 무효화 횟수와 함께 기록 무효화가 포함된 테이블 목록만 표시됩니다. 테이블을 선택하면 재정의가 포함된 모든 상위 기록 목록이 반환됩니다. 모든 상위 기록, 상위 기록의 도메인 및 각 기록에 대한 재정의 횟수 를 빠르게 볼 수 있습니다.

뷰 재정의를 선택하면 상위 기록을 포함한 모든 재정의가 표준 목록 뷰에 표시되는 새 탭이 로드됩니다. 드롭다운 목록에서 테이블을 선택하여 모든 기록과 재정의를 표시합니다. 기록별 재정의를 모두 보려면 기록에 대한 무효화 보기를 선택합니다.

주: 재정의가 있는 테이블만 나열됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자세한 내용은 도메인으로 구분된 속성 재정의 만들기를 참조하세요.

도메인 활성화 또는 비활성화

도메인을 활성화하거나 비활성화하면 활성화 상태가 도메인 내 회사로 계단식으로 설정됩니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
회사 기록을 활성화하면 도메인 분리를 통해 회사의 연결된 도메인이 자동으로 활성화됩니다. 예를 들어 ACME 회사를 활성화하면 TOP/ACME 도메인도 활성화됩니다.

프로시저

1. 도메인 기록으로 이동합니다.
2. 활성 확인란의 선택을 취소하거나 선택합니다.
3. 업데이트를 클릭합니다.

> **경고:** 도메인을 삭제하지 마십시오. 더 이상 필요하지 않은 도메인은 삭제하는 대신 비활성화합니다.

테이블에 도메인 필드 추가

관리자는 사용자 지정 테이블에 sys_domain 필드를 추가하여 도메인 분리할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보

주:

기본 시스템 테이블에 도메인을 추가하지 마십시오.

프로시저

1. 테이블의 목록 뷰로 이동합니다.
   예를 들어 <table name>`.list` 탐색 필터에서.
2. 목록 헤더를 마우스 오른쪽 버튼으로 클릭하고 구성 > 목록 레이아웃.
3. 새 필드 만들기 섹션에서 이름으로`sys_domain` 입력하고 `#### ### ID`를 입력합니다.
4. 추가를 클릭합니다.
5. 저장을 클릭합니다.

주:

필드를 생성하는 다른 방법은 열 이름에 **u_** 접두사를 추가합니다. 그러나 도메인 필드를 사용하면 **u_** 프리픽스가 없는 필드가 자동으로 생성됩니다. 다음 기능을 바로 가기로 사용할 수 있습니다. **sys_domain**필드를 만들 때마다 이름을 **sys_domain** 지정하고 필드 유형은 그대로 둡니다. 시스템에서 자동으로 필드 유형을 도메인 **ID** 로 설정하고 필드 레이블을 도메인으로 설정하여 몇 번의 클릭을 줄일 수 있습니다.

기본 시스템 테이블에 도메인을 추가하려면 엄청나게 철저한 테스트, 업데이트 및 새 로직 추가가 필요합니다. 또한 많은 경우 고객이 소스 코드에 액세스할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 관계 보기

도메인 맵은 도메인 관리자에게 인스턴스의 활성 도메인과 그 사이의 관계를 읽기 전용으로 표현합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
모든 도메인 맵에는 하나의 도메인이 기본 도메인으로 설정되어 있어야 합니다. 또한 도메인 맵의 각 도메인이 다음 기준을 충족해야 합니다.

- 상위 필드를 채워야 합니다(기본 도메인은 이에 대한 유일한 예외임).
- 활성 확인란을 선택해야 합니다.

도메인 맵은 매핑 조건을 충족하지 못하는 도메인에 대해서는 도메인 관계를 그리지 않습니다.

프로시저

1. 다음으로 이동 모두 > 도메인 관리 > 도메인 맵.
2. 도메인 헤더에서 더하기**(+)** 또는 빼기**(+-**) 아이콘을 클릭하여 하위 도메인을 표시하거나 숨깁니다.

기본 도메인 선택

primary 도메인은 도메인 맵의 최상위 도메인을 나타냅니다.

시작하기 전에
필요한 역할: 관리자

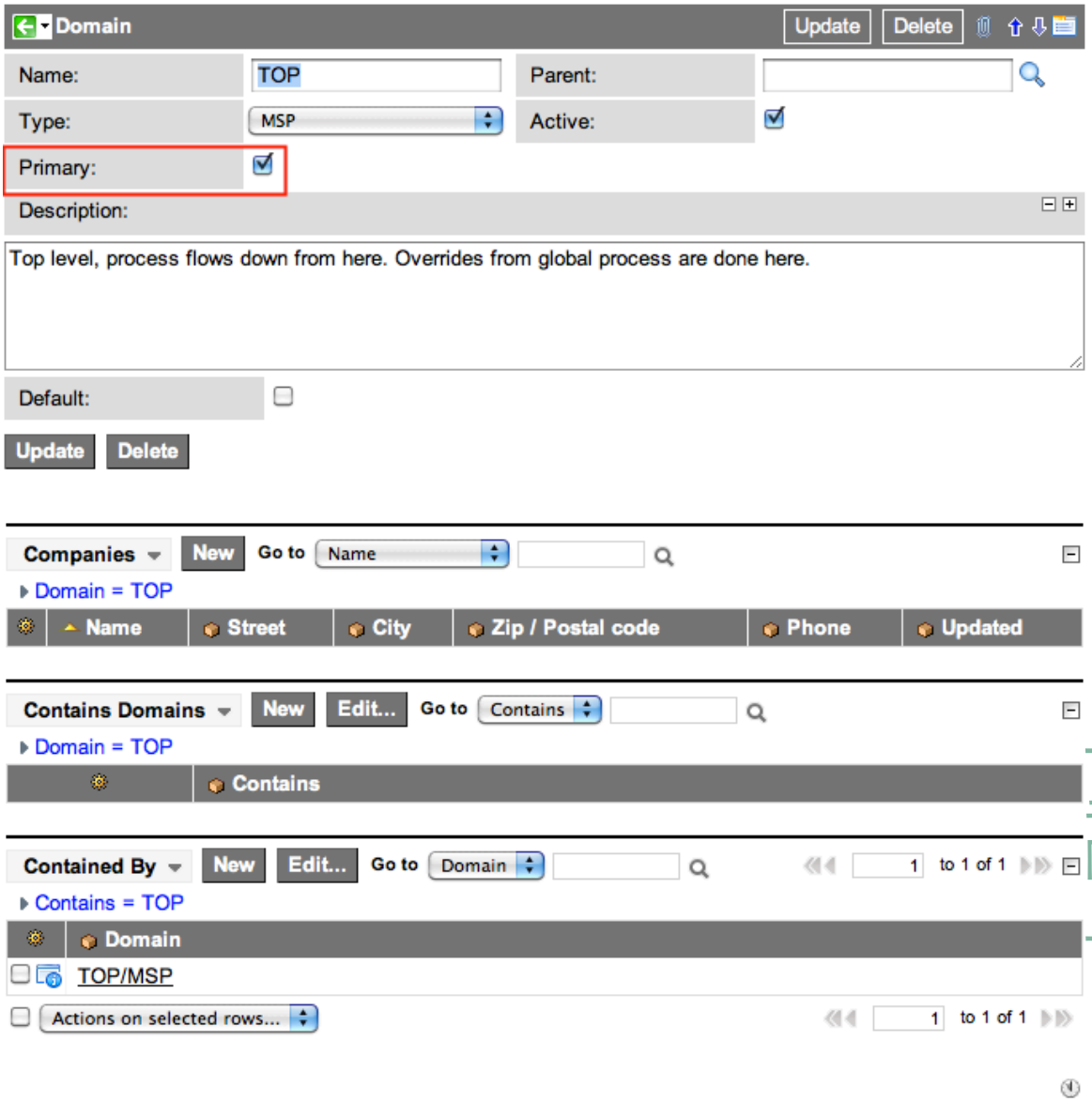
이 태스크 정보
기본 도메인에는 상위 도메인이 있을 수 없으며 하나 이상의 하위 도메인이 있어야 합니다. 한 번에 하나의 기본 도메인만 있을 수 있습니다. 다른 도메인을 기본 도메인으로 선택하면 이전 기본 도메인이 재정의됩니다.

프로시저

1. 다음으로 이동 모두 > 도메인 관리 > 도메인.
2. 기본 도메인으로 사용할 도메인(예: TOP)을 선택합니다.
3. 기본 확인란을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 업데이트를 클릭합니다.



도메인 간의 **Contains** 관계 생성

도메인 간의 "포함" 관계를 생성하여 도메인 계층 구조를 변경합니다.

시작하기 전에
필요한 역할: 관리자

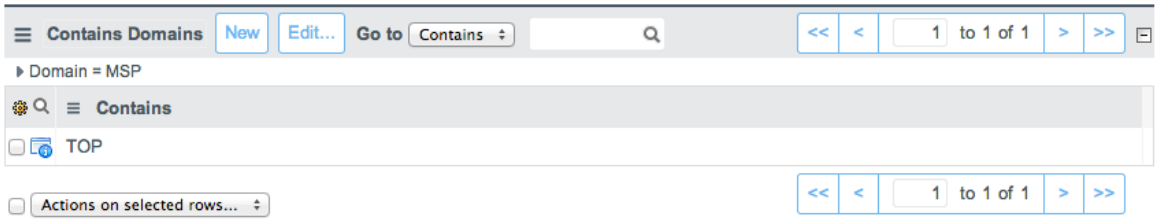
이 태스크 정보
포함 관계의 도메인은 포함하는 도메인의 설정을 상속합니다. 포함하는 도메인을 사용하면 사용자가 포함된 도메인뿐만 아니라 해당 하위 도메인의 데이터도 볼 수 있습니다. 프로세스는 포함 관계의 영향을 받지 않습니다.

프로시저

1. 도메인 테이블로 이동합니다.
2. 새 포함 관계의 상위(컨테이너) 도메인인 도메인 기록을 선택합니다.
3. 필요한 경우 도메인 범위를 전환하여 세션 범위와 기록 범위 간에 전환합니다.
4. 도메인 포함 관련 목록에서 편집을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 포함 관계의 하위(포함된) 도메인에 해당하는 도메인 기록을 선택합니다.
   도메인 선택기가 전역으로 설정된 경우 기본적으로 하위 도메인만 나타납니다. 모든 도메인을 보려면 도메인 범위를 전환합니다.
6. Save(저장)를 클릭한 다음 Update(업데이트)를 클릭합니다.



관련 정보

서비스 제공자를 위한 도메인 분리 권장 방법

도메인 범위 확장

기본적으로 전역 도메인의 사용자가 **sys_overrides** 열이 포함된 테이블을 볼 때 사용자는 전역 도메인의 기록만 볼 수 있습니다. 전역 도메인의 관리자가 프로세스 테이블을 볼 때 해당 관리자는 해당 프로세스 테이블에 있는 기록만 볼 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. *glide.sys.restrict_global_domain_processes* 속성을 **true**로 변경합니다.
2. 모든 도메인의 레코드를 보려면 관련 링크에서 도메인 범위 확장을 클릭합니다.
3. 전역 도메인에서만 기록 보기로 돌아가려면 도메인 범위 축소를 클릭합니다.

가시성 도메인 목록에 도메인 추가

가시성 도메인을 추가하면 사용자 또는 그룹의 일반 도메인 구성원 자격에 관계없이 사용자 또는 그룹이 다른 도메인의 기록을 보고 잠재적으로 편집할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
가시성 도메인을 개별 사용자에게 부여하는 것보다 그룹의 모든 구성원에게 가시성 도메인을 할당하는 것이 좋습니다.

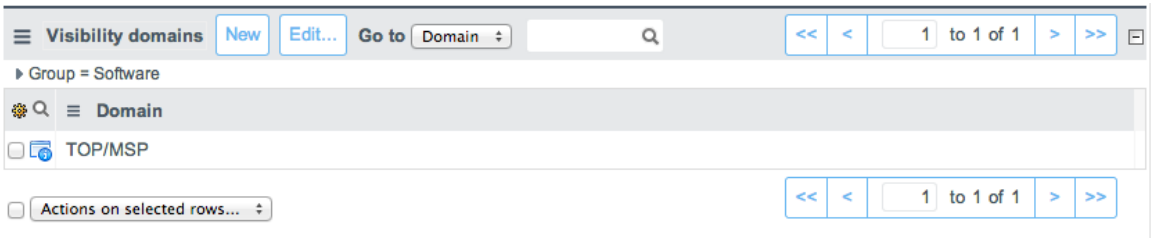
> 주: 가시성 도메인을 추가해도 테이블 또는 기록의 접근 제어 규칙 요구 사항은 변경되지 않습니다.

프로시저

1. 그룹 테이블로 이동합니다.
2. 가시성 도메인을 제공할 그룹을 선택합니다.
3. 가시성 도메인 관련 목록을 양식에 추가합니다.
4. 가시성 도메인 관련 목록에서 편집을 클릭합니다.
5. 그룹 또는 도메인에 표시할 도메인 기록을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. Save(저장)를 클릭한 다음 Update(업데이트)를 클릭합니다.



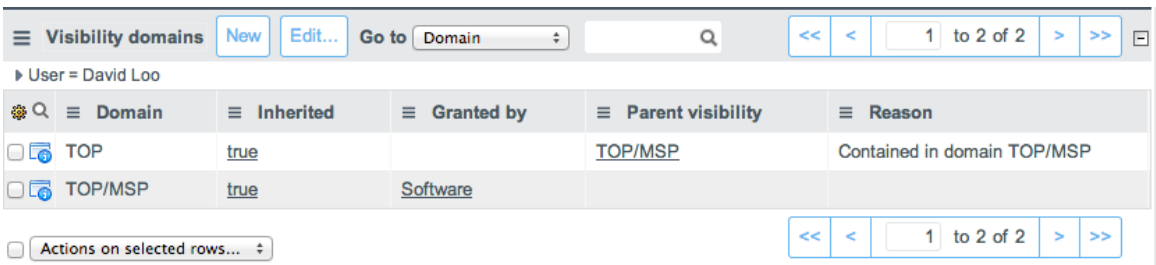
개별 사용자에게 가시성 도메인 부여

사용자 양식에서 특정 사용자에 대한 가시성 도메인을 추가할 수 있지만 그룹을 통해서만 추가하는 것이 가장 좋습니다. 이는 개인이 부서를 변경하거나 퇴사하는 경우 권한 및 액세스를 통제합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 사용자 관리 > 사용자.
2. 가시성 도메인을 제공할 사용자를 선택합니다.
3. 가시성 도메인 관련 목록을 양식에 추가합니다.
4. Visibility Domains(가시성 도메인) 관련 목록에서 Edit(편집)를 클릭합니다.
5. 사용자가 볼 기록이 있는 도메인을 선택합니다.
6. Save(저장)를 클릭한 다음 Update(업데이트)를 클릭합니다.



가시성 도메인 포함된 목록에는 다음 필드가 포함되어 있습니다.

필드	설명
도메인	그룹 또는 사용자에게 표시되는 도메인입니다.
상속됨	도메인은 도메인 가시성 또는 상위 도메인에서 상속됩니다.
부여한 사람	도메인 가시성을 부여한 그룹의 이름입니다.
상위 가시성	상위 도메인의 이름으로, 기록을 그룹화하는 데 사용됩니다. 상위 기록이 삭제되면 상위 항목이 동일한 모든 기록도 삭제됩니다.

도메인별 선택 목록 만들기

관리자는 특정 도메인과 관련된 항목을 포함하도록 선택 목록을 구성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 선택 항목을 추가할 도메인 선택기에서 도메인을 선택합니다.
2. 사용자 지정할 선택 필드를 마우스 오른쪽 버튼으로 클릭하고 선택 사항 구성을 선택합니다.
3. 선택 사항을 업데이트하거나 추가합니다.
4. 업데이트 세트와 같은 일반 변경 프로세스를 통해 변경 사항을 밀어넣습니다.

> **주:** 관리자는 전역 도메인에서 관리 혼동을 방지하기 위해 도메인 간에 선택 항목이 고유한지 확인해야 합니다.

관리자가 전역 도메인에서 새 선택 항목을 추가하면 계층 구조에서 하위 도메인의 사용자는 현재 선택 목록의 끝에 새 선택 항목이 표시됩니다. 새 선택이 전역 수준에서 활성화되어 있지 않으면 도메인 사용자는 선택 사항 구성을 통해 사용할 수 있지만 활성 선택으로 표시되지는 않습니다.

고급 도메인 분리 관리

관리자는 도메인 분리에 대한 정보를 보고, 잠재적인 문제를 식별하고, 구성 설정을 변경할 수 있습니다.

도메인에서 다음과 같은 고급 관리 작업을 수행할 수 있습니다.

- 도메인 선택 메뉴 사용
- 도메인 관계 보기

도메인 선택 메뉴 사용

인스턴스는 두 가지 메뉴 형식을 통해 도메인 선택을 제공합니다.

- 도메인 선택기: 사용 가능한 도메인의 간단한 드롭다운 목록을 제공합니다.
- 도메인 참조 선택기: 필터링 및 자동 완성 자동 완성 입력 기능을 제공하는 참조 필드를 활성화합니다. 긴 목록에 이 형식을 사용합니다.

이러한 선택기의 배치와 표시 또는 숨기기 절차는 사용자 인터페이스 버전에 따라 다릅니다.

에서 도메인 선택 메뉴 사용 코어 **UI**

에 코어 UI 도메인 선택기를 표시하면 기본적으로 도메인 선택기가 활성화됩니다. 도메인 선택기를 활성화한 후 시스템 속성을 추가하여 도메인 참조 선택기를 활성화할 수 있습니다.

시작하기 전에

> **주:** 도메인 참조 선택기를 사용하려면 도메인 분리(플러그인 com.snc.pa.domain_support)가 필요합니다.

필요한 역할: 관리자

이 태스크 정보

프로시저

1. 헤더에서 기어 아이콘을 클릭합니다.
2. 일반 탭에서 헤더에 도메인 선택기 표시 스위치를 클릭합니다.
   도메인 선택기가 헤더에 코어 UI 나타납니다.
3. 옵션: 도메인 참조 선택기를 활성화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 도메인 참조 선택기를 활성화하면 목록에서 전역 옵션이 제거됩니다. 홈 도메인으로 돌아가려면 참조 필드 옆에 있는 반환 화살표를 클릭합니다. 관리 사용자는 반환 화살표를 클릭하여 전역 도메인으로 돌아갈 수 있습니다.

a. 애플리케이션 네비게이터에 `sys_properties.list`를 입력합니다.

b. 아직 없는 경우 `glide.ui.domain_reference_picker.enabled` 속성을 추가하고 값을 **true**로 설정합니다.

c. 브라우저를 새로 고칩니다.
도메인 참조 선택기가 헤더에 코어 UI 나타납니다.

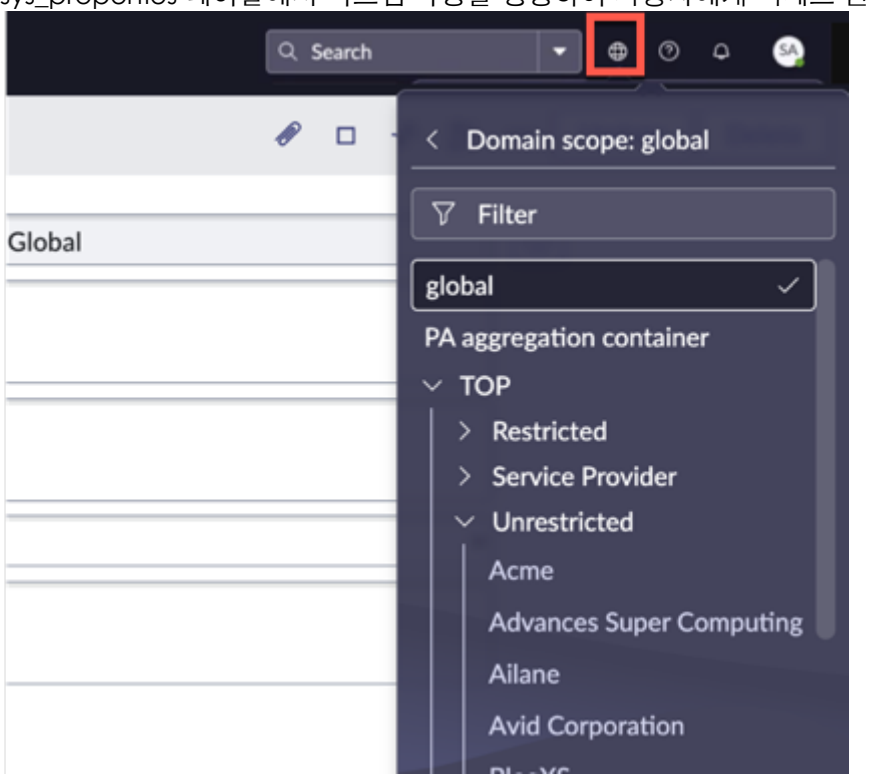
도메인 선택기에 대한 접근 제한

시스템 속성을 사용하여 및 넥스트 경험의 도메인 선택기 코어 UI 에 대한 액세스를 제한합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
기본적으로 ITIL 역할을 가진 사용자와 ITIL 역할을 포함하는 역할(예: 관리자)은 의 도메인 선택기 넥스트 경험에 액세스할 수 있습니다. 다른 역할을 속성에 추가하여 액세스 권한을 부여하거나 제거하여 역할을 제한할 수 있습니다. 역할은 관리자로만 제한하는 것이 좋습니다.

관리자는 sys_properties 테이블에서 시스템 속성을 생성하여 사용자에게 액세스 권한을 부여할 수 있습니다.



프로시저

1. 시스템 속성 [sys_properties] 테이블을 엽니다.
2. 이 속성 추가: `glide.ui.polaris.domain_picker.role`
3. 속성 값을 쉼표로 구분된 역할 목록으로 구성합니다. **admin, itil**.
자세한 내용은 넥스트 경험 선택기 구성을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 분리 애플리케이션 속성

Domain Separation 플러그인에는 서비스 제공자가 도메인 분리를 사용하는 애플리케이션을 보다 유연하게 사용자 지정할 수 있도록 2개의 새 테이블이 있습니다. 이러한 테이블은 시스템 애플리케이션 속성 테이블 [sys_application_property] 및 시스템 애플리케이션 속성 값 테이블 〔sys_application_property_value〕입니다.

새 테이블은 더 많은 옵션을 제공합니다.

SP(서비스 제공자) 애플리케이션의 경우 특정 작업은 도메인에 따라 다를 수 있습니다. ServiceNow® 그러나 기본 시스템 시스템 속성 [sys_properties] 테이블은 도메인으로 구분되지 않으므로 도메인 분리를 사용하는 애플리케이션의 요구 사항을 충족하지 않습니다.

각 SP 고객은 각기 다른 방식으로 애플리케이션을 사용자 지정하기를 원할 수 있습니다. 이전에는 사용자 지정할 수 있는 기능이 하나의 전역 값으로만 정의되었습니다. 애플리케이션 개발자에게는 보다 유연한 테이블이 필요합니다. 이제 기능을 추가하거나 변경할 때마다 코드를 만들 필요 없이 애플리케이션을 수정할 수 있습니다.

새 테이블에서 재정의가 작동하는 방식

개발자는 일반적으로 시스템 속성 [sys_properties] 테이블을 사용하여 ServiceNow 애플리케이션에서 다양한 함수를 만듭니다. 다른 도메인에서 다르게 동작하는 응용 프로그램을 개발하려면 직접 사용자 정의해야 합니다.

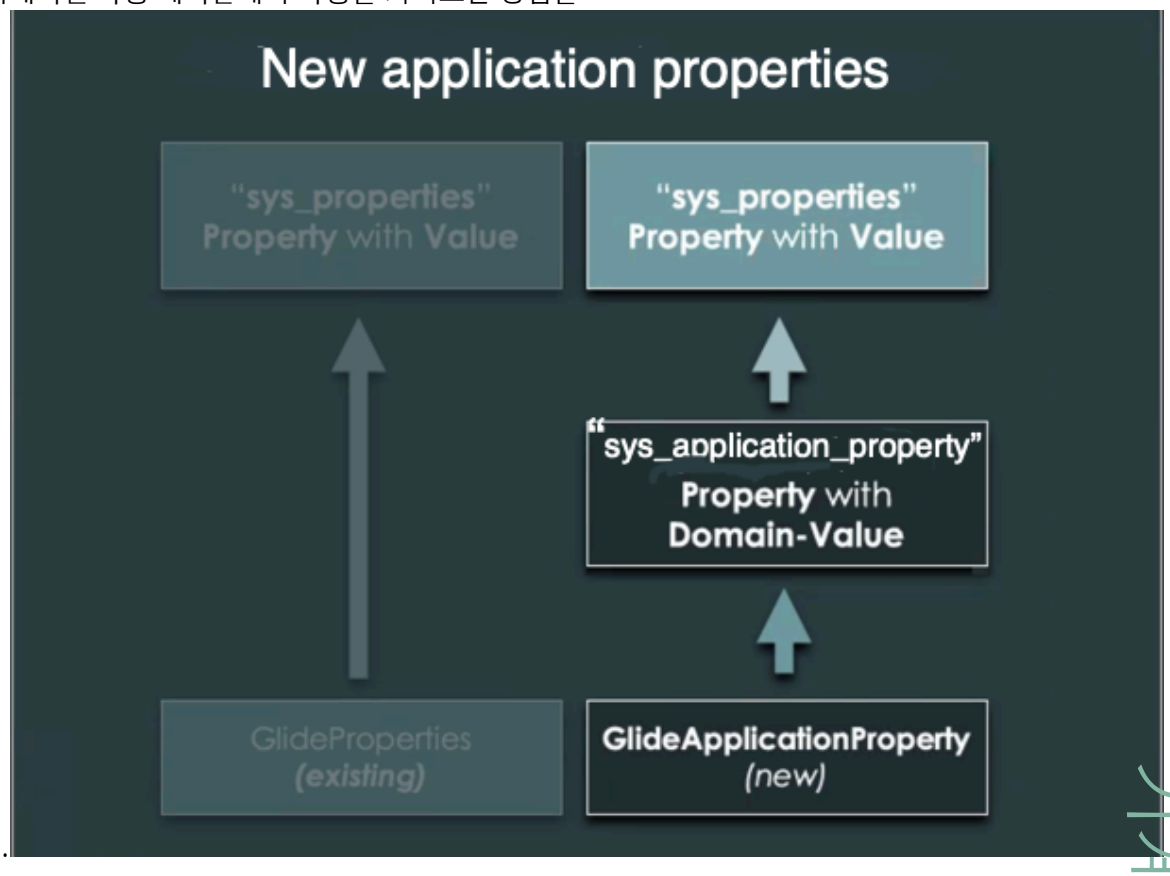
Paris 릴리스에서는 새로운 애플리케이션 속성 [sys_application_property] 테이블이 이러한 사용자 지정을 단순화합니다. 애플리케이션 속성 테이블은 값을 얻기 위해 시스템 속성 테이블로 직접 이동하지 않고 시스템 애플리케이션 테이블로 먼저 이동합니다. 이제 이 새 테이블에는 애플리케이션을 구성하는 데 필요한 논리가 저장됩니다. 새 테이블에서 속성을 찾으면 해당 콘텐츠를 사용합니다. 해당 테이블에 정보가 없으면 기본 시스템 속성 테이블로 이동합니다.

도메인 분리에 대한 지원을 구성할 때 이 새 애플리케이션 속성 테이블에 도메인 논리를 추가할 수 있습니다. 이 테이블에는 시스템 속성 테이블에 없는 속성이 포함될 수 있습니다. 또는 시스템 속성 테이블에서 선택한 모든 속성을 재정의할 수 있는 속성을 구성 테이블에 추가할 수 있습니다.

예를 들어, 주의 첫 번째 날 기능으로 애플리케이션을 구성하려 한다고 가정해 보겠습니다. 때로는 주의 첫 번째 날을 일요일로 지정하고 싶을 수도 있습니다. 다른 경우에는 주의 첫 번째 날을 월요일로 설정할 수 있습니다. 기본 시스템 테이블에는 1일 옵션(일요일) 하나만 있을 수 있습니다. 새 테이블을 사용하여 다른 속성을 저장하여 1일차는 일요일이고 하위 도메인은 월요일로 만들 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 그림은 시스템이 시스템 속성 [sys_properties] 테이블로 이동하기 전에 애플리케이션 속성 테이블에서 속성을 가져오는 방법을

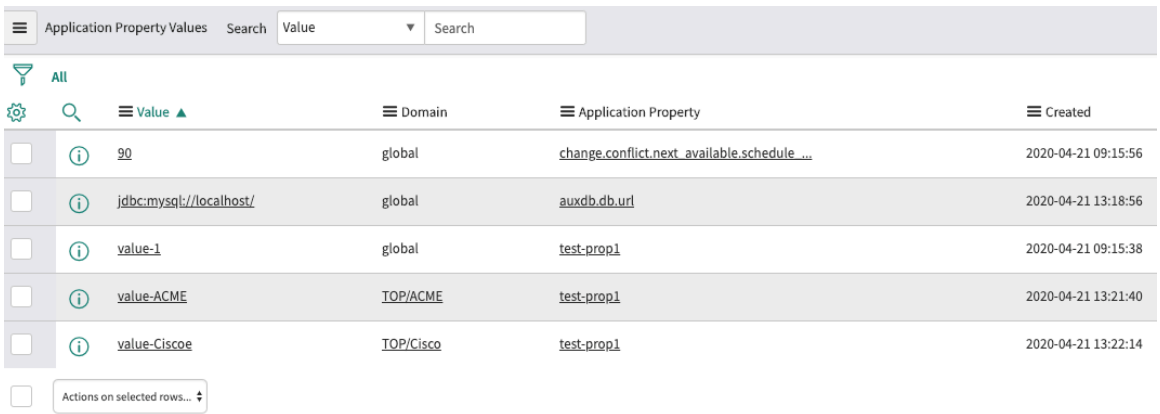


보여줍니다.

범위가 지정된 앱이 새 테이블에서 작동하는 방식

새 애플리케이션 속성 테이블은 범위가 지정된 애플리케이션에서 지원됩니다. 시스템 속성 이름과 비슷한 애플리케이션 속성 이름은 고유하며, 전역이 아닌 경우 범위 이름 앞에 접두사가 붙습니다. 애플리케이션의 범위는 구성에 영향을 미칩니다. 범위에 따라 일요일로 정의되는 Day 1과 월요일로 정의되는 날이 결정될 수 있습니다. 동일한 속성을 사용할 수 있지만 Day 1, Sunday가 상위 도메인이고 Day 1, Monday가 하위 도메인이 되도록 사용자 지정할 수 있습니다. 새 테이블에는 도메인 열과 범위 열이 모두 있으므로 각각에 대해 이러한 속성을 설정할 수 있습니다.

다음 이미지와 같이 sys_application_property_value 테이블의 도메인 범위 확장 보기를 사용하여 모든 재정의를 표시할 수 있습니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

이러한 테이블을 사용할 수 없는 경우 Domain Extension Installer(com.glide.domain.msp_extensions.installer) 플러그인을 활성화했는지 확인합니다.

새 애플리케이션 속성 테이블

새 시스템 애플리케이션 속성 [sys_application_property] 테이블에는 다음 필드가 포함되어 있습니다.

- 이름
- 설명
- 유형(문자열, 참|거짓, 정수, 시간대, 색상 등 선택)
- default_value
- 속성(sys_properties 참조)
- usage_notes
- read_roles
- write_roles
- 고유 키: (이름)

새 시스템 애플리케이션 속성 값 [sys_application_property_value] 테이블에는 다음 필드가 포함되어 있습니다.

- sys_application_property(sys_application_property 참조)
- sys_domain
- sys_overrides
- 값
- 고유 키: (sys_application_property, sys_domain)

새 **API**

새 API는 범위가 지정된 앱에서도 지원됩니다. 도메인으로 구분된 애플리케이션 속성에는 고유한 API가 있습니다. GlideApplicationProperty API에는 전역 및 범위가 지정된 애플리케이션 모두에서 사용할 수 있는 두 가지 새로운 스크립트 가능 메서드가 있습니다. 이러한 새 API에 대한 자세한 내용은 GlideApplicationProperty - 범위가 지정됨, 전역 을 참조하십시오.

관련 정보

서비스 제공자를 위한 도메인 분리 권장 방법

도메인 마이그레이션 도구

도메인 마이그레이션 도구를 사용하여 고객을 도메인 분리 환경에서 자체 전용 인스턴스로 이동합니다.

Domain Migration Tool 플러그인

Domain Migration Tool 플러그인(com.glide.domain.migration_tool)은 고객을 도메인 분리 환경에서 보다 유연한 전용 인스턴스로 이동하는 작업을 단순화합니다. 고객은 별도의 인스턴스로 마이그레이션하여 역량을 더욱 효과적으로 활용 Now Platform 하고자 할 수 있습니다. Domain Separation 플러그인이 설치되어 있더라도 데이터 및 프로세스 분리 속성은 꺼져 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 복제된 인스턴스를 요청하고 Domain Migration Tool 플러그인을 사용하려면 먼저 활성화를 요청해야 합니다.

Domain Migration Tool는 도메인 분리 인스턴스에서 데이터와 프로세스 분리가 모두 활성화된 경우에만 실행됩니다.

- *glide.sys.domain.partitioning* 데이터 속성을 **true**로 설정해야 합니다.
- 프로세스 *glide.sys.domain.delegated_administration* 속성을 **true**로 설정해야 합니다.

마이그레이션 도구의 기능

- 마이그레이션 프로세스 대부분, 특히 데이터 정리를 자동화합니다.
- 도메인 분리 인스턴스를 새 전용 인스턴스로 마이그레이션합니다.
- 전용 인스턴스에서 데이터를 삭제합니다.

  주: 이 도구는 전역, 대상 도메인 또는 추가 데이터 도메인(지정된 경우)에 있는 데이터를 삭제하지 않습니다.

- 프로세스 데이터를 축소하거나, 축소할 수 없는 경우 프로세스 데이터를 삭제합니다.
- 대상 도메인에 표시되는 프로세스 기록 유지
- sys_choice, sys_ui_list 및 sys_ui_related_list 특수 테이블을 업데이트합니다.
- 도메인 분리 플러그인에 의해 추가된 기록을 정리합니다.
  - 비즈니스 규칙
  - UI 작업
  - 예약된 작업
  - 설치 종료
  - 탐색 모듈
- 도메인 분리를 사용하지 않도록 설정하고 복제된 인스턴스에서 도메인을 제거합니다.
  - 복제된 인스턴스에서 다음 속성을 아니오 로 설정합니다.
    - *glide.sys.domain.partitioning*
    - *glide.sys.domain.delegated_administration*
    - *glide.sys.domain.enabled*
  - 대상 도메인과 지정된 추가 데이터 도메인을 제외한 모든 도메인을 삭제합니다.
- domain_migration_tool_status 테이블의 상태 필드를 업데이트합니다.

테이블의 개별 상태

상태	설명
보류 중	마이그레이션 중 도메인 분리 테이블의 기본 상태입니다. 테이블이 마이그레이션될 예정이지만 아직 마이그레이션을 시작하지 않았습니다.
실패	테이블 수준 오류입니다. 마이그레이션 프로세스가 오류와 함께 종료된 경우 이 상태는 오류가 있는 테이블을 나타냅니다.
실행 중	현재 마이그레이션 중인 테이블의 상태입니다. 하나의 테이블만 이 상태를 가질 수 있으며 현재 마이그레이션 중입니다.
성공	성공적으로 마이그레이션된 테이블의 상태입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태	설명
성공적으로 완료됨	마이그레이션 프로세스가 오류 없이 완료됩니다.
완료되었으나 오류 있음	마이그레이션 프로세스가 오류와 함께 완료되었습니다.

- 진행률과 상태를 syslog_domain에 기록

  원본은 마이그레이션과 연결된 모든 로그 항목에 대한 **MigrationTool** 입니다.

  - 각 데이터 테이블과 남아 있는 데이터 테이블 수를 기록합니다.
  - 각 프로세스 테이블과 현재 비활성화 또는 삭제 중인 도메인의 기록을 기록합니다.

마이그레이션 도구가 수행하지 않는 작업

- 인스턴스 클론
- 다른 도메인 분리 인스턴스 생성
- 도구를 실행하기 전에 데이터 또는 프로세스 분리 속성이 비활성화된 경우 기록(데이터 또는 프로세스) 마이그레이션
- 소스 인스턴스의 모든 데이터 변경
- 전역, 대상 도메인 또는 추가 데이터 도메인(지정된 경우)에 있는 데이터를 삭제합니다

도구를 실행한 후 수행해야 할 작업

Domain Migration Tool은 원하는 도메인(대상 도메인, 추가 데이터 도메인 및 전역 도메인) 외부의 데이터 제거를 자동화합니다. 나머지 구성을 모두 평가하여 전용 인스턴스에 적합하고 작동하는지 확인해야 합니다. 예를 들어 기록에 도메인 필드를 설정하는 비즈니스 규칙이 있는 경우 더 이상 목적을 달성하지 못하므로 이 비즈니스 규칙을 사용하지 않도록 설정할 수 있습니다.

도메인 분리 인스턴스를 전용 인스턴스로 마이그레이션

고객을 도메인 분리 환경에서 자체 전용 인스턴스 환경으로 이동합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

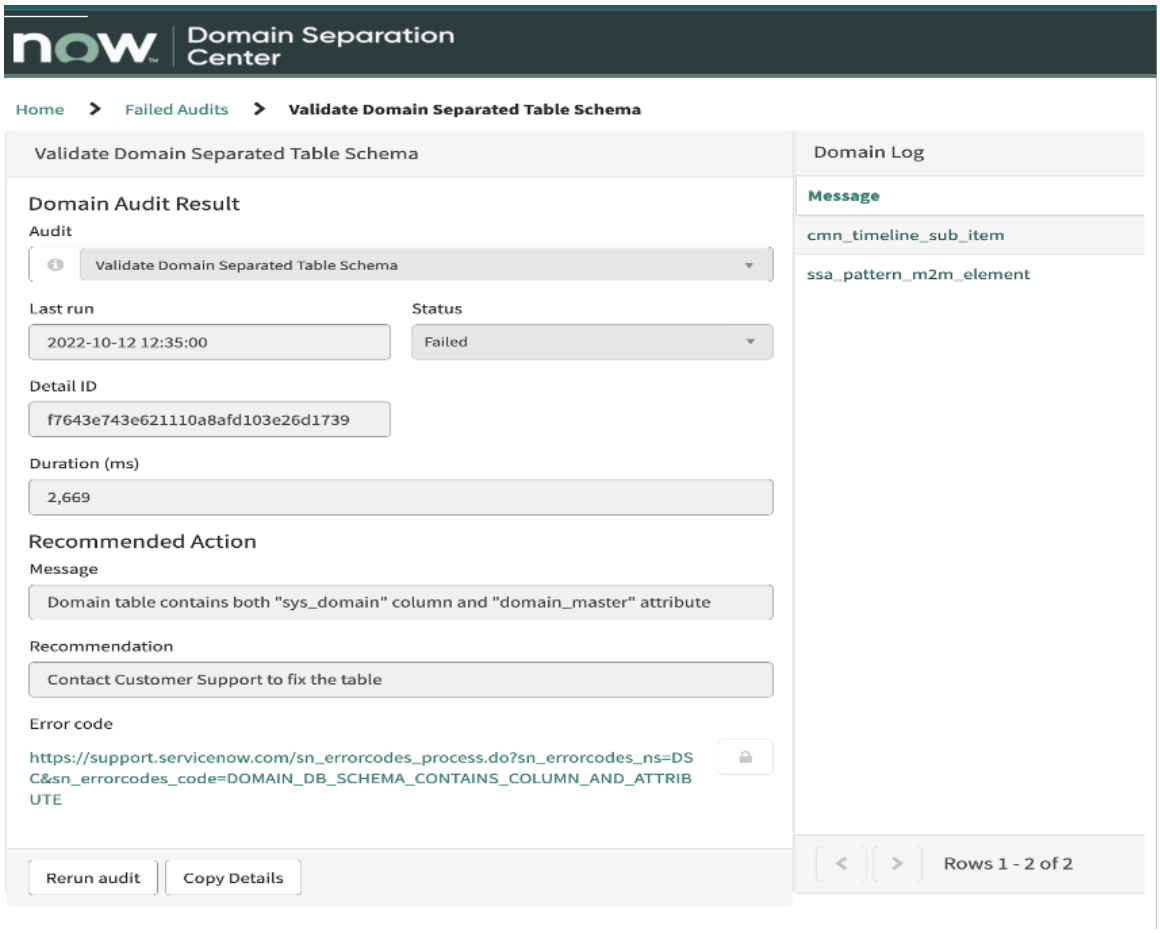
1. security_admin 역할로 승격합니다.
   자세한 내용은 권한 있는 역할로 상승 문서를 참조하십시오.
2. 다음으로 이동 모두 > 도메인 관리 > 도메인 마이그레이션 도구.
   또한 **domain_migration_tool_status.list**로 액세스하십시오.
3. 새로 만들기를 클릭합니다.
4. 양식을 작성합니다.

필드	설명
대상 도메인	마이그레이션하려는 프로세스와 데이터 모두에 사용되는 도메인을 지정합니다. 추가 데이터 도메인 필드에 지정되지 않은 경우 대상 도메인만 유지되며 하위 도메인은 유지되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
추가 데이터 도메인	필요에 따라 마이그레이션하려는 추가 데이터 도메인을 지정합니다. 대상 도메인과 모든 하위 항목을 마이그레이션하려면 모든 하위 항목을 지정해야 합니다.

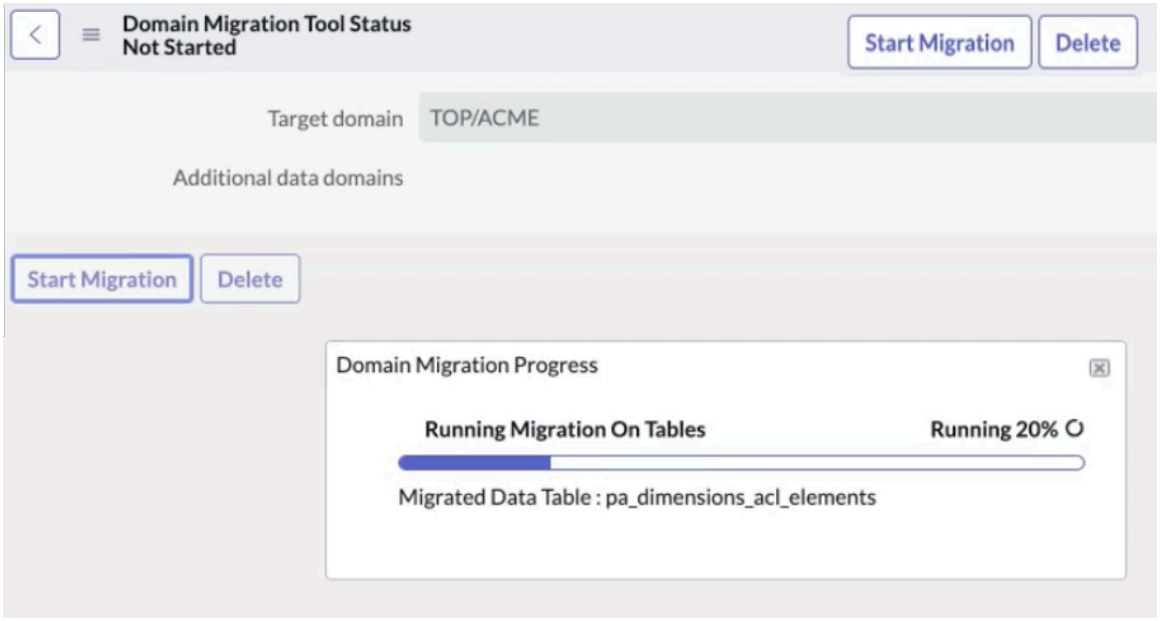
5. 제출을 선택합니다.
6. 방금 제출한 양식을 엽니다.
7. 다음으로 이동 모두 > 도메인 분리 센터 > 감사 구성 .
   자세한 내용은 도메인 분리 센터 문서를 참조하십시오.
8. 도메인으로 구분된 테이블 스키마 확인 감사를 활성으로 설정하고 일정을 할당합니다.
   이는 도메인 분리된 테이블의 상태에 대한 스키마를 미리 검사하기 위한 사전 예방적 도메인 감사입니다. 이렇게 하면 마이그레이션을 실행하기 전에 오류를 수정할 수 있습니다.
9. 스키마가 포함된 감사 일정을 실행합니다.
   자세한 내용은 즉시 감사 실행 문서를 참조하십시오.
10. 감사에서 반환된 문제를 해결합니다.



11. 마이그레이션 시작을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ 실행 추적기 진행률 표시줄과 도메인 마이그레이션 도구가



트리거됩니다.

◦ 현재 진행 중인 마이그레이션 테이블이 성공적으로 마이그레이션된 테이블의 총 백분율과 함께 표시됩니다.

◦ 도메인으로 구분된 모든 테이블이 마이그레이션 상태, 각 테이블의 총 기록 수 및 마이그레이션된 기록 수와 함께 기록되는 테이블입니다.

◦ 마이그레이션에 실패한 테이블 수도 기록됩니다.

◦ 도구가 기능을 수행함에 따라 상태가 업데이트됩니다.

◦ 진행률 표시줄을 닫아도 도메인 마이그레이션이 백그라운드에서 계속 실행 중입니다. *sys_execution_tracker* 테이블에 액세스하고 테이블에서 마이그레이션 실행을 찾아 백그라운드에서 실행 중인 마이그레이션 프로세스를 확인합니다.

Domain Migration Tool 상태에 다음 필드가 표시됩니다.

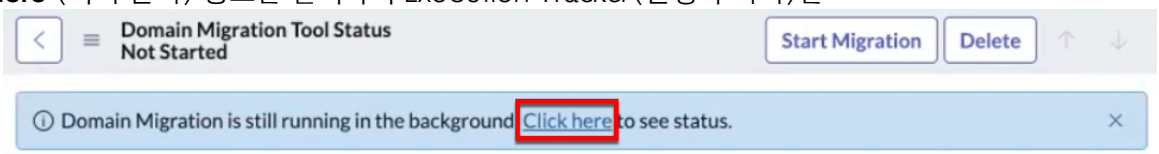
도메인 마이그레이션 도구 상태 필드

필드	설명
상태	마이그레이션 상태를 표시합니다. ◦ 데이터 테이블 마이그레이션 중...: 진행 중 상태입니다. ◦ 마이그레이션 성공: 마이그레이션 성공 후 업데이트된 상태입니다. ◦ 도메인으로 구분된 테이블 중 하나에서 잘못된 구성이 관찰되었습니다. 데이터 마이그레이션 실패를 나타냅니다. 스키마 오류가 발견되었습니다. 마이그레이션이 시작되지 않습니다. 감사 실행 도메인으로 구분된 테이블 스키마의 유효성을 확인합니다. 감사가 실패하고 스키마 표준을 따르지 않는 테이블이 표시됩니다. ◦ 재방문 테이블의 오류와 함께 마침: 스키마 마이그레이션을 처리할 테이블 수가 나열됩니다. 재방문 테이블 카운트에서 오류를 찾고 스키마 문제를 해결합니다. ◦ 테이블에 대한 도메인 마이그레이션 실패...: 비대상 기록은 실패한 테이블에서 수동으로 삭제해야 합니다. ◦ 성공적으로 완료됨: 모든 테이블이 마이그레이션된 경우입니다.
대상 도메인	마이그레이션을 위해 선택한 대상 도메인입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

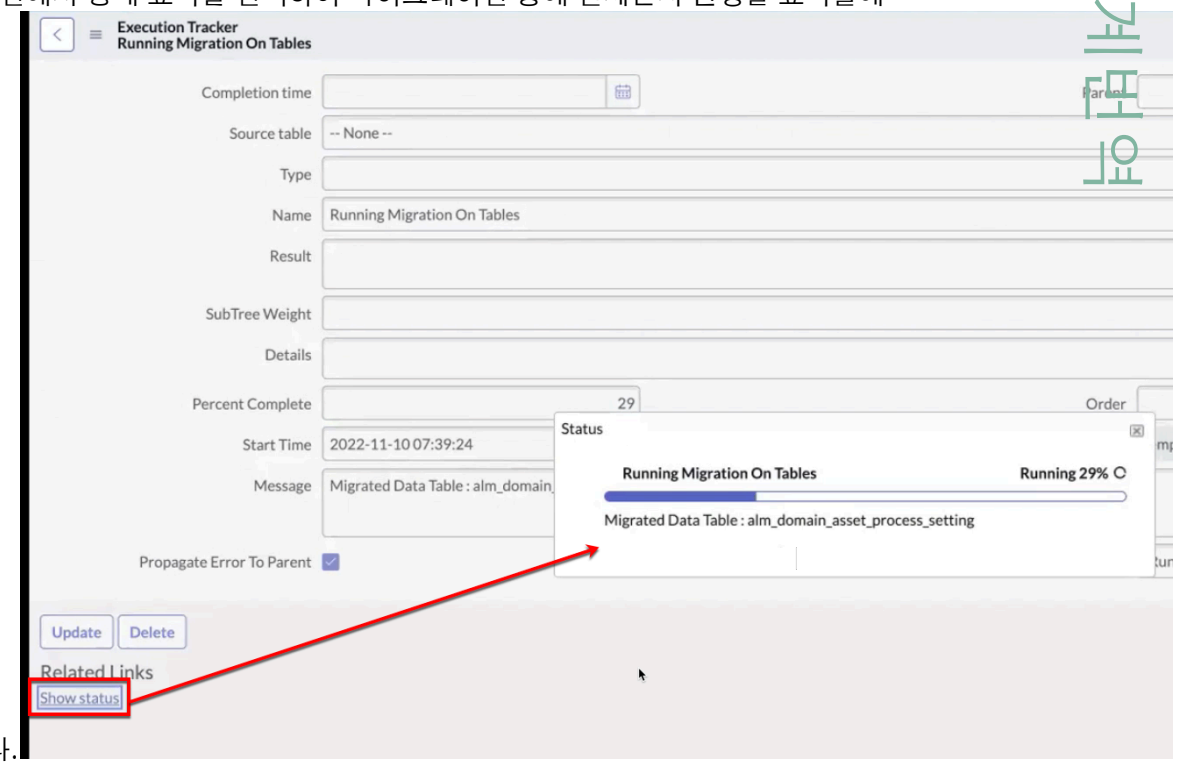
필드	설명
추가 데이터 도메인	여러 마이그레이션 도메인이 선택된 경우 입력합니다.
재방문 테이블 수	이 필드는 테이블 마이그레이션에 실패한 경우에만 채워집니다. 오류가 없는 경우 이 개수는 0입니다. 이 경우 마이그레이션을 다시 시도하기 위해 테이블을 다시 검토합니다. 오류가 발생하지 않으면 테이블을 다시 방문하거나 마이그레이션을 다시 시도할 필요가 없습니다.
현재 진행 중인 테이블	현재 마이그레이션 중인 테이블의 이름을 표시합니다. 마이그레이션에 성공하면 이 필드가 비어 있게 됩니다.

12. Domain Migration Tool Status(도메인 마이그레이션 도구 상태) 페이지에서 **Click here** (여기 클릭) 링크를 선택하여 Execution Tracker(실행 추적기)를 엽니다.



sys_execution_tracker 테이블에 액세스하고 테이블에서 마이그레이션 실행을 찾아 백그라운드에서 실행 중인 마이그레이션 프로세스를 확인할 수도 있습니다.

13. 관련 링크 섹션에서 상태 표시를 선택하여 마이그레이션 중에 언제든지 진행률 표시줄에 액세스합니다.

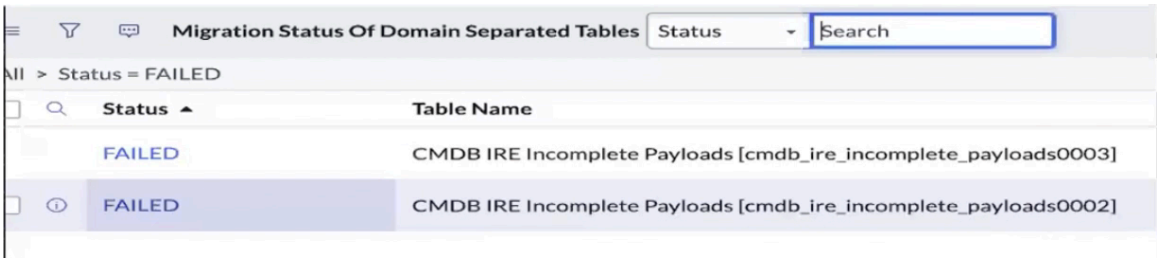


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

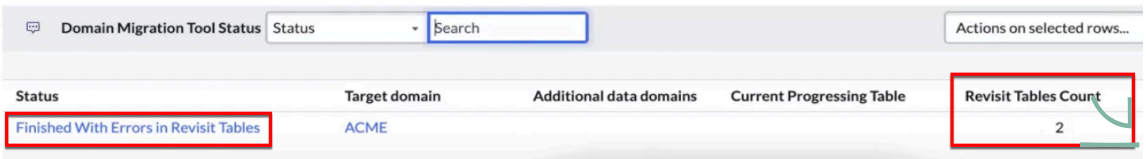
테이블이 스키마 검사에 실패한 경우 도메인 분리 테이블의 마이그레이션 상태 전체 상태는 실패가 됩니다.



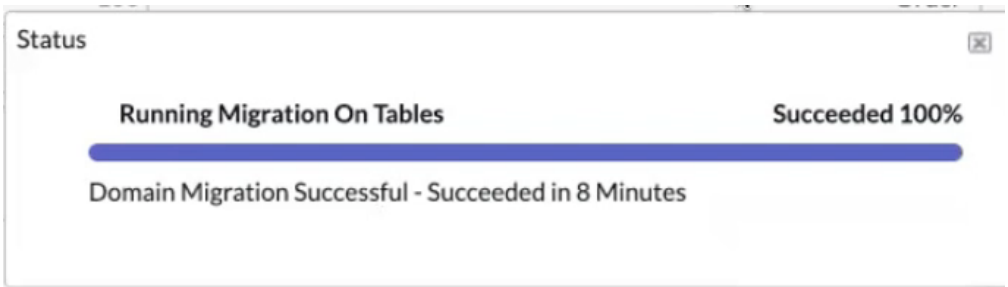
해당하는 테이블마다 **Failed** 항목이 있을 것입니다.



마이그레이션의 나머지 부분이 계속되고 실패한 모든 테이블에 대한 요약과 총 재방문 테이블 수가 도메인 마이그레이션 도구 상태에 채워집니다.



마이그레이션이 완료되면 상태가성공적으로 완료 됨입니다.



프로세스 관리

프로세스 관리를 통해 관리자는 도메인별 정책을 설정할 수 있습니다.

도메인 계층 구조에서 더 낮게 설정된 정책은 도메인 계층 구조에서 더 높게 설정된 정책을 재정의합니다. 도메인에 있는 동안 관리자는 다음 전역 정책 및 설정의 도메인별 버전을 설정할 수 있습니다.

- 클라이언트 스크립트
- 시스템 정책
- 애플리케이션 및 모듈 이름
- 애플리케이션 역할
- 모듈 필터

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

⚠ 경고: 관리자는 ACL 규칙을 재정의하고 모든 역할 검사를 통과할 수 있기 때문에 관리자 역할이 있는 모든 사용자는 모든 시스템 기능, 함수 및 데이터에 대한 특별한 접근 권한을 갖습니다. 이 권한은 신중하게 부여해야 합니다.

사용자에게 관리자 역할이 있으면 할당된 도메인에 관계없이 인스턴스의 모든 정책을 사용할 수 있습니다. 특정 도메인에 진입할 수 있으며, 해당 도메인 이상의 보험만 관련 트랜잭션 중에 표시되고 처리됩니다. 관리자가 상위 도메인 또는 전역 도메인에 있는 정책을 수정하면 시스템에서 해당 관리자의 현재 도메인에 대한 새 기록을 자동으로 생성합니다. 원래 정책, 애플리케이션 또는 모듈 기록은 수정되지 않습니다. 이 새 레코드는 원본을 재정의합니다.

하위 수준 도메인의 정책을 변경하려면 해당 도메인으로 이동하여 정책을 수정합니다. 이 접근 방식은 더 높은 수준의 원래 정책 기록을 재정의하는 도메인 내 정책 기록을 생성합니다.

상위 수준 정책을 변경한 다음 해당 정책의 도메인 필드를 변경하지 마십시오. 이 접근 방식은 하위 수준 도메인에 정책 레코드를 생성하지 않으며 상위 수준 도메인에 대한 정책 레코드를 유지하지도 않습니다.

sys_overrides 필드는 계층 구조의 하위 수준에 있는 정책, 애플리케이션 또는 모듈이 상위 수준에 있는 기록을 재정의한다는 것을 나타냅니다. 관리자가 상위 계층 구조에 있는 다른 도메인에 속한 정책, 애플리케이션 또는 모듈을 수정하려고 하면 시스템에서 자동으로 이 필드를 설정합니다.

상위 레벨 기록을 변경하는 대신, 시도된 업데이트는 삽입으로 변경되고, **sys_overrides** 필드는 재정의되는 상위 레벨 정책, 애플리케이션 또는 모듈을 나타내도록 설정됩니다. 나중에 관련 트랜잭션에 대한 기록이 로드되면 원래 대신 재정의되는 도메인별 정책, 애플리케이션 또는 모듈이 사용됩니다.

프로세스 관리를 위한 도메인

기본적으로 프로세스 관리는 항상 기록의 도메인을 사용하여 적용할 정책을 결정합니다.

레코드의 도메인이 사용자의 도메인보다 우선합니다. 레코드의 도메인에 정책이 없는 경우 위임된 관리는 도메인 계층 구조의 다음으로 높은 수준에 있는 정책을 확인합니다. 도메인 정책 검색은 전역 도메인에 도달할 때까지 도메인 계층 구조에서 계속됩니다. 도메인 계층 구조 하위에 도메인 정책이 없으면 프로세스 관리에서 전역 도메인에 대한 정책을 사용합니다.

예를 들어, Fred Luddy는 Acme: Atlanta, Acme: San Diego 및 Acme: NY 하위 도메인의 하위 도메인에 있는 기록을 볼 수 있는 Acme 도메인의 사용자입니다. 이 사용자가 Acme: San Diego 도메인에서 기록을 열면 프로세스 관리는 먼저 Acme: San Diego 도메인의 정책을 확인합니다. 도메인 계층 구조의 이 수준에 정책이 없는 경우 프로세스 관리는 Acme 도메인의 정책을 확인합니다. Acme 도메인에 정책이 없으면 도메인 계층 구조에 상위 도메인이 없으므로 프로세스 관리에서 전역 도메인 정책을 사용합니다.

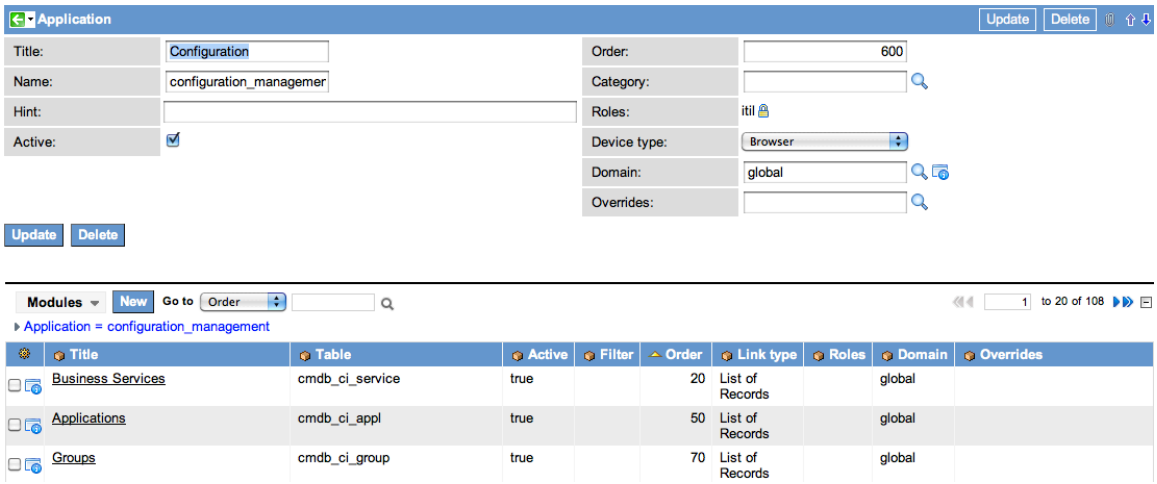
도메인별 애플리케이션을 사용한 샘플 프로세스 관리

다음 예는 도메인별 애플리케이션 및 모듈을 사용한 프로세스 관리를 보여줍니다.

Oceanic 도메인의 관리자인 David Loo는 구성 애플리케이션을 사용자 지정하기로 결정합니다. 우선 David는 구성 애플리케이션 모듈에서 사용할 수 있는 모듈을 검토합니다.

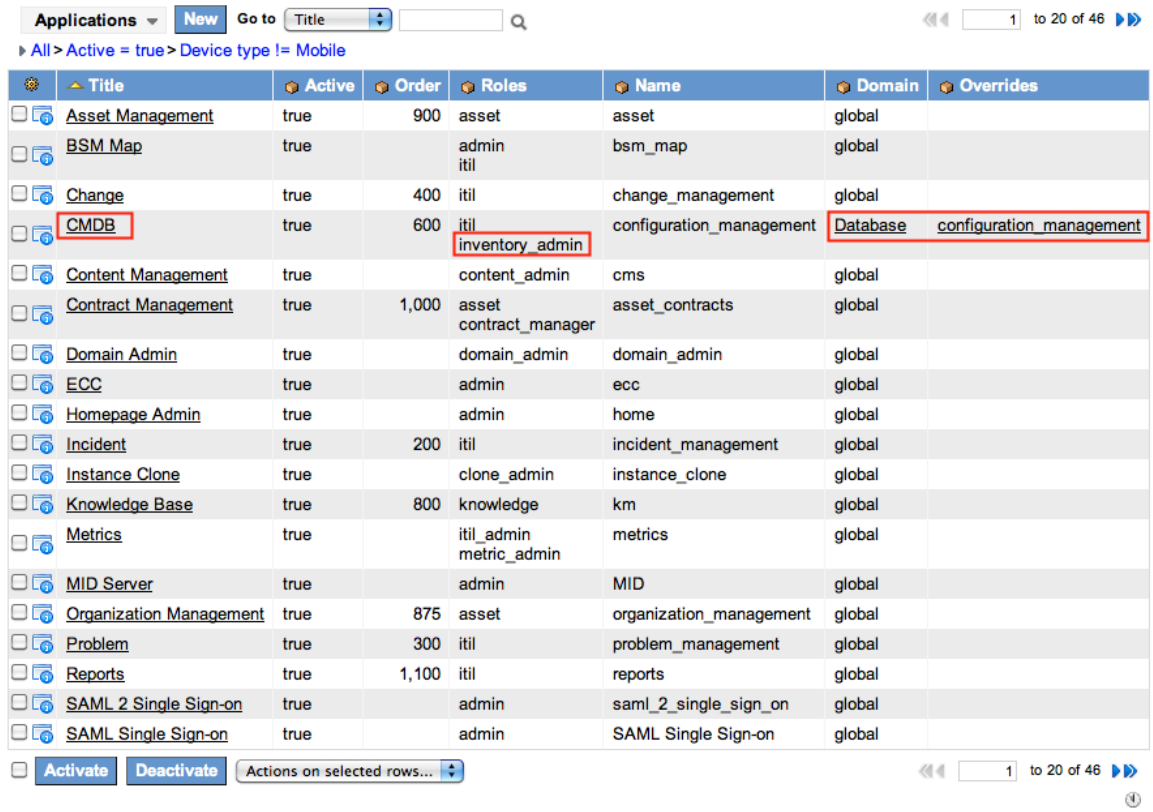
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 애플리케이션의 시작 뷰



David는 구성 애플리케이션의 이름을 CMDB로 바꾸고 inventory_admin 역할이 애플리케이션을 볼 수 있도록 하기로 결정했습니다.

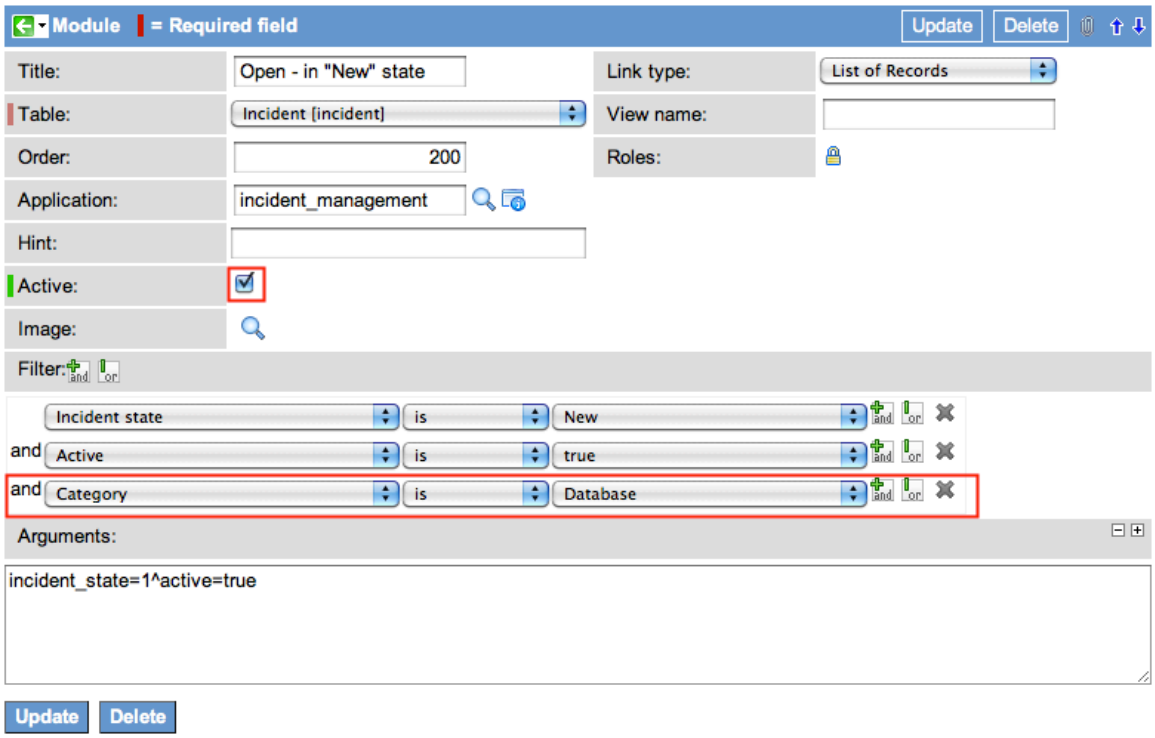
구성 애플리케이션에 대한 도메인별 변경 내용 샘플



다음으로 David는 "신규" 상태의 열기 모듈을 활성화하고 새 필터 항목을 추가해 Oceanic 범주에 미해결 인시던트를 표시해 인시던트 애플리케이션을 변경하기로 했습니다.

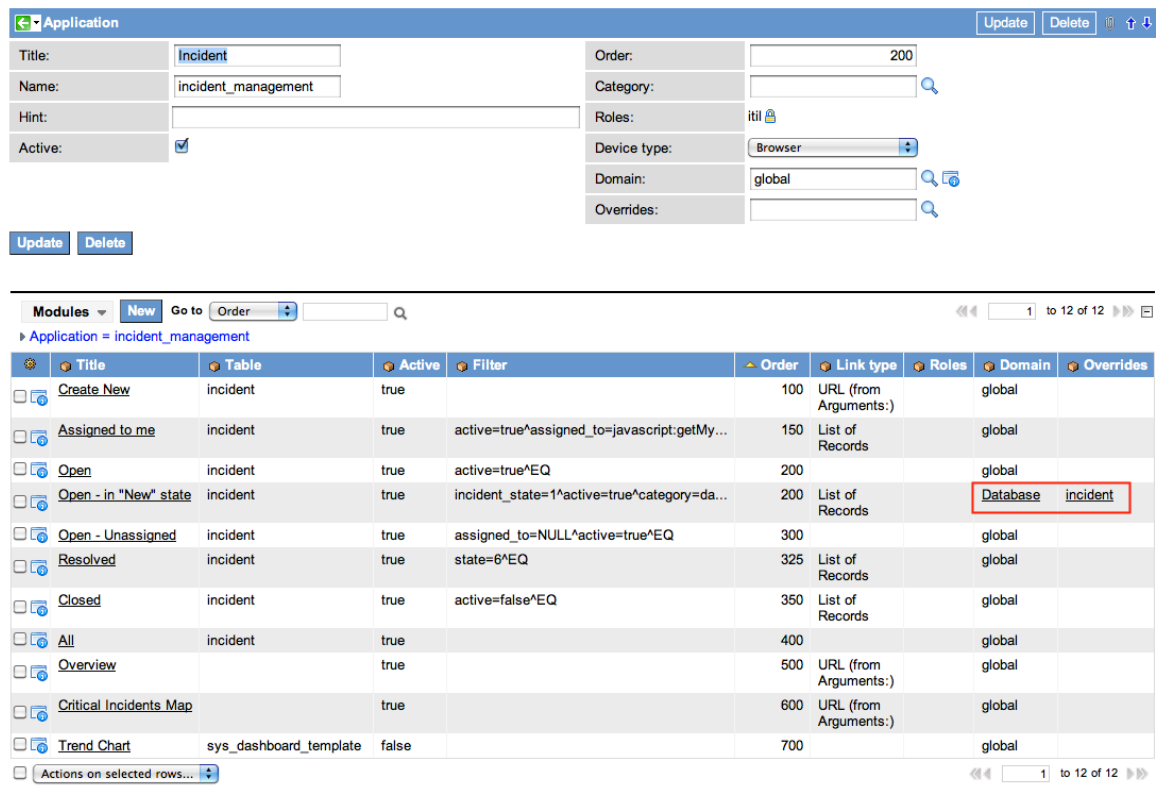
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

오픈 - "새" 상태 모듈에 대한 도메인별 변경 내용 샘플



이렇게 하면 전역 도메인의 기존 모듈을 덮어쓰지 않고 애플리케이션에 새 모듈 항목이 생성됩니다.

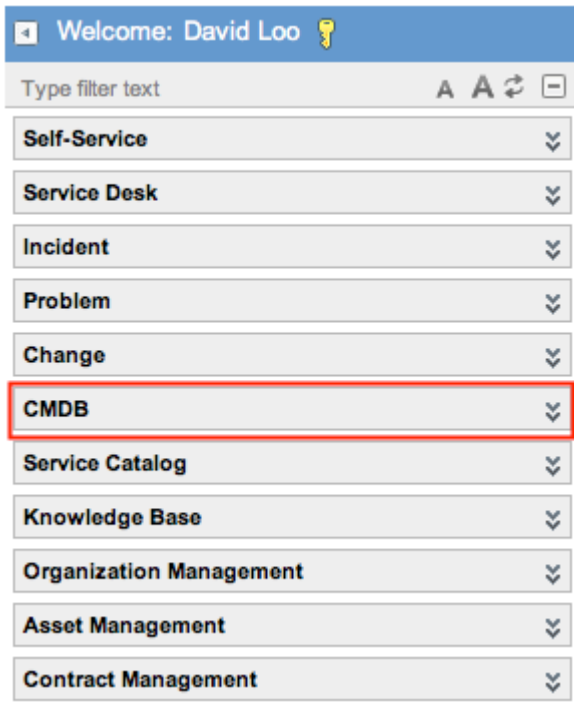
인시던트 애플리케이션의 도메인별 뷰



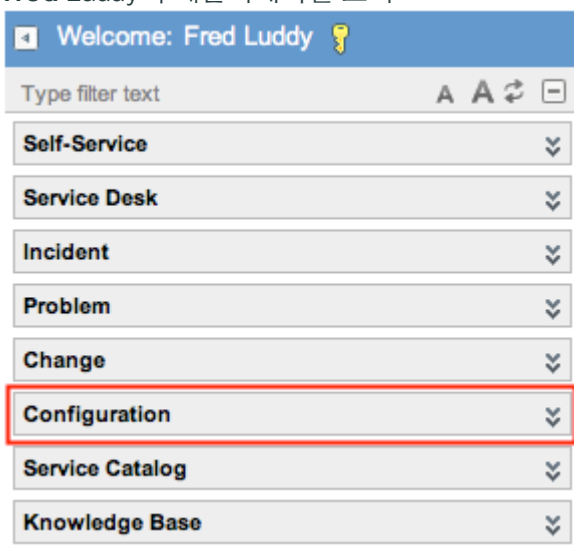
Fred Luddy와 같은 다른 도메인의 다른 관리자가 로그인하여 구성 애플리케이션을 확인하면 전역 도메인의 설정이 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

David Loo의 애플리케이션 보기



Fred Luddy의 애플리케이션 보기



자세한 정보 도메인 로깅 및 디버그 메시지 사용

도메인 로그 및 디버그 메시지를 사용하면 도메인 구성 오류 문제를 해결할 수 있습니다.

시작하기 전에
필요한 역할: 관리자
최상의 성능을 위해 최신 인스턴스인지 확인하십시오.

프로시저

1. Domain Separation Center에서 **Domain Admin**으로 이동합니다.
2. **Configure Domain** Center(도메인 센터 구성)를 클릭합니다.
3. 자세한 정보 도메인 로깅 사용**(Enable verbose domain logging)**에서 예**(Yes)** 확인란을 선택합니다.
4. 업데이트를 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

실시간 도메인 메시지 보기

시스템 로그에서 실시간 도메인 메시지를 볼 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 자세한 정보 도메인 로깅 사용: 다음으로 이동합니다. 모두 > 도메인 관리 > 도메인 분리 센터 > 도메인 센터 구성 > 상세 도메인 로깅 사용 > 예 또는 `glide.sys.domain.verbose` 속성을 **True**로 설정하십시오.
2. 다음으로 이동 시스템 진단 > 세션 디버그 > 모두 사용.
   이는 실시간 검토이므로 로그 파일을 확인하기 전에 디버그 세션을 실행할 필요가 없습니다.
3. 세션 디버그 콘솔로 이동하여 자세한 시스템 도메인 로그를 확인합니다.
4. 테이블에 대한 쿼리 텍스트를 검색합니다.

   이 쿼리는 다음 형식의 로그 메시지를 찾습니다.

```
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]]
```

   이 예에서 인시던트 테이블을 보는 사용자는 데이터베이스 Atlanta, 데이터베이스, 데이터베이스 San Diego, 전역 및 NY DB 도메인과 일치하는 기록만 볼 수 있습니다.

이력 도메인 메시지 보기

로그 파일에서 기록 도메인 메시지를 확인하여 도메인 분리 문제를 해결합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 자세한 정보 도메인 로깅 사용: 다음으로 이동합니다. 모두 > 도메인 관리 > 도메인 분리 센터 > 도메인 센터 구성 > 상세 도메인 로깅 사용 > 예 또는 `glide.sys.domain.verbose` 속성을 **True**로 설정하십시오.
2. 다음으로 이동 시스템 진단 > 세션 디버그 > 모두 사용.
3. 로그 파일을 확인하기 전에 디버그 세션을 일정 기간(예: 하루) 동안 실행하도록 합니다.
4. 다음으로 이동 시스템 로그 > 공공 서비스 > 노드 로그 파일 다운로드.
5. 보려는 날짜의 기록을 엽니다.
   로그 파일은 `localhost_log.<yyyy-mm-dd>.txt` 명명 형식을 사용합니다.
6. 로그 다운로드 관련 링크를 클릭합니다.
7. 텍스트 편집기에서 다운로드한 로그 파일을 열고 다음 형식의 로그 메시지를 검색합니다.

   도메인 값에 의해 제한된 테이블 인시던트에 대한 쿼리 `[##, #####[8a4dde73c6112278017a6a4baf547aa7]]`

   이 예에서 사용자는 전역 및 소프트웨어 도메인과 일치하는 인시던트 테이블의 기록만 보았습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

도메인 분리 오류 문제 해결

도메인 분리 문제가 발생하면 이 솔루션 목록을 검토하십시오.

오류 또는 증상	솔루션
도메인이 존재하지 않는 도메인을 가리키는 sys_id	이 오류는 사용자 또는 작업 기록과 같은 데이터 기록에 `sys_id` 현재 도메인 테이블에 없는 `sys_domain` 열 값이 있을 때 발생합니다. 도메인 `sys_id` 실수로 삭제되었거나 도메인 테이블을 변경한 경우 이전 도메인 테이블을 참조할 수 있습니다. 오류를 해결하려면 오류가 포함된 테이블의 목록을 열고 잘못된 `sys_domain` 값을 필터링합니다. 그런 다음 올바른 `sys_domain` 값을 수동으로 입력하거나 제거합니다. 주: 도메인 테이블을 참조하는 모든 테이블에 잘못된 도메인 `sys_ids` 있을 수 있습니다. 예를 들어 사용자 가시성 도메인 `[sys_user_visibility]`, 그룹 가시성 도메인 `[sys_user_group_visibility]` 및 포함된 도메인 `[domain_contains]` 테이블에서 잘못된 도메인 ID가 발생할 수 있습니다.
잘못된 도메인을 가리키는 도메인 경로 또는 도메인 번호가 sys_id	이 오류는 도메인 번호 또는 도메인 경로 쿼리가 실제 도메인 이름과 동기화되지 않은 경우에 발생합니다. 이 오류는 도메인 추가 시 다시 번호를 매겨야 하거나 도메인 번호에서 도메인 경로로 변환하는 동안 도메인 번호에서 발생할 수 있습니다. 오류를 해결하려면 에서 도메인 분리 센터결과를 확인하십시오. 오류가 지속되면 적절한 도메인을 가리키도록 `sys_domain_path` 또는 `sys_domain_number` 열의 값을 수동으로 편집할 수 있습니다.
도메인 트리 구조가 손상되었습니다.	이 오류는 도메인 간에 무한 루프를 생성하는 일련의 도메인 포함 관계가 있는 경우에 발생합니다. 오류를 해결하려면 도메인 테이블의 목록을 열고 도메인에 루프가 형성되지 않도록 값 포함을 수동으로 편집합니다.

사후 프로덕션 도메인 분리 활성화 유틸리티

사후 프로덕션 도메인 분리 활성화 유틸리티는 실제 환경에서 도메인 분리를 활성화하는 데 도움이 됩니다.

사후 프로덕션 도메인 분리 활성화 유틸리티 플러그인

사후 프로덕션 도메인 분리 활성화 유틸리티 플러그인(com.glide.domain.activation_utility)은 사후 프로덕션 라이브 환경에서 도메인 분리 환경을 생성하는 작업을 단순화합니다. 고객은 사후 프로덕션 환경에서 Domain Separation을 활성화하여 기능을 더욱 효과적으로 활용하고자 할 수 있습니다 Now Platform . 이 유틸리티는 도메인을 생성하기 위한 단계별 안내 설정을 제공합니다.

주: 도메인 분리 테이블의 도메인 기록을 채우는 프로세스에는 다운타임 또는 인스턴스에 대한 제한된 액세스가 필요합니다.

활성화 유틸리티의 기능

- 도메인을 생성하기 위한 단계별 안내 설정을 제공합니다.
- 백그라운드 작업을 실행하여 프로세스 및 데이터 분리 속성을 모두 사용하지 않도록 설정한 상태에서 도메인 분리 설치를 처리합니다.
- 대상(첫 번째) 도메인에 표시되는 프로세스 기록 유지

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 도메인 생성 프로세스 중 오류 탐지, 식별 및 기록
- 일반적인 오류에 대한 해결 방법 제시
- 감사 목적으로 설정 프로세스 중에 수행된 모든 작업을 기록합니다.
- 수행한 모든 작업, 생성된 도메인 및 시스템에 대한 변경 내용을 포함하여 자세한 요약을 생성합니다.

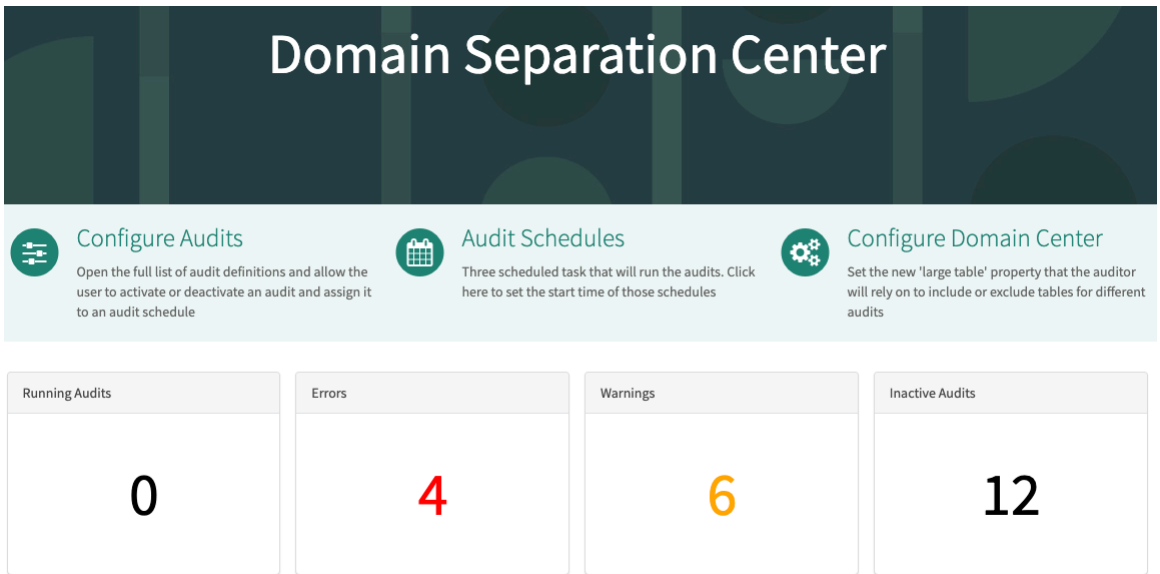
도메인 분리 센터

도메인을 정기적으로 감사하여 문제를 파악합니다.

개요

Domain Separation Center는 domain_audit_definition 테이블에 저장된 모든 도메인에 대한 감사를 예약하고 구성할 수 있는 대시보드입니다. 대시보드를 사용하면 감사 결과를 검토하고 도메인 오류 및 경고를 더 깊이 파고들 수 있습니다. Domain Separation Center 대시보드는 `<ServiceNow-instance-name>/domaincenter`에서 찾을 수 있습니다.

Domain Separation 센터에서는 다양한 감사를 제공합니다. 직접 만들 수는 없습니다. 그러나 실행 빈도는 구성할 수 있습니다. 감사는 domain_audit_definition 테이블에 저장된 모든 도메인에서 실행됩니다.



감사 구성

감사가 활성 상태인지 여부와 실행 빈도를 구성할 수 있습니다.

1. Domain Separation 센터에서 **Configure** Audits(감사 구성)를 선택합니다.

   Configure Audits 페이지가 표시됩니다.

2. 활성화할 각 감사를 구성합니다. 감사는 기본적으로 비활성 상태입니다.
   a. 감사를 선택합니다.
   b. 감사를 활성화하려면 활성 상자를 선택합니다.
   c. 빈도 필드에서 감사가 실행되는 빈도를 지정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Domain Separation 센터에서는 동일한 빈도로 표시된 모든 감사를 동시에 실행합니다. 큰 테이블에서 실행되는 감사에 대해 매일 을 선택하지 마십시오.

d. 활성화하려는 각 감사에 대해 이 단계를 반복합니다.

3. 저장을 선택합니다.

감사 일정

매일, 매주 또는 매월 실행되도록 하나 이상의 감사를 구성합니다. 스케줄러는 이러한 감사를 실행할 요일과 시간을 지정합니다. 일정 빈도가 동일한 모든 감사는 구성한 시점을 응시하여 순차적으로 실행됩니다.

1. Domain Separation 센터에서 감사 일정을 선택합니다.

감사 일정 페이지가 표시됩니다.

2. 감사 일정을 구성합니다.

a. 일정 이름을 선택합니다.

b. 감사를 실행할 시간을 지정합니다.

시간 단위는 24시간제로 측정되며, 14는 오후 2시와 같습니다.

c. 주별 일정의 경우 감사를 실행할 요일을 선택합니다. 여기서 1은 일요일입니다.

d. 월별 일정의 경우 감사를 실행할 월의 일을 선택합니다.

e. 다른 일정에 대해 이 절차를 반복합니다.

3. 저장을 선택하여 구성 변경 내용을 저장합니다.

4. 오른쪽 창 상단에 표시된 빈도로 실행되도록 예약된 모든 감사를 실행하려면 지금 실행을 선택합니다. 예를 들어 창 제목이 도메인 감사 일정 **-** 매일인 경우 매일 실행되는 모든 감사가 실행됩니다.

실행 중인 감사의 상태를 보려면 Domain Separation 센터의 **Running** Audits(감사 실행 중) 상자에서 숫자를 선택합니다.

즉시 감사 실행

감사는 일반적으로 일정대로 실행됩니다. 그러나 명령에 따라 모든 감사를 실행할 수 있습니다.

1. Domain Separation 센터에서 감사 일정을 선택합니다.

감사 일정 페이지가 표시됩니다.

2. 실행할 감사 일정의 이름(예: 매일, 매주 또는 매월)을 선택합니다.

3. 지금 실행을 선택합니다.

실행 중인 감사의 상태를 보려면 Domain Separation 센터의 **Running** Audits(감사 실행 중) 상자에서 숫자를 선택합니다.

Domain Separation Center 구성

1. Domain Separation Center에서 **Configure Domain** Center(도메인 센터 구성)를 선택합니다.

2. 도메인 센터 구성 페이지의 세부 정보 도메인 로깅 사용에 대해 예를 선택하여 도메인 관련 문제를 진단하는 데 도움이 되는 자세한 로그를 저장합니다. 자세한 로깅으로 인해 성능 문제가 발생할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이러한 로그는 syslog_domain 테이블의 서버 측 로그를 참조합니다. 로그 보기에 대한 자세한 내용은 경고 및 실패가 있는 감사 보기를 참조하세요.

3. 슬러시버킷에서 모든 대형 테이블을 선택하고 선택됨 열로 이동합니다.

   일일 감사는 큰 테이블에서 실행해서는 안 됩니다. 선택됨 열의 회색으로 표시된 테이블 이름이 커서 사용 가능 열로 이동할 수 없습니다.

4. 업데이트를 선택합니다.

경고 및 실패가 있는 감사 보기

대시보드에서 오류 및 경고 는 문제가 발생한 감사에 대한 자세한 정보를 제공합니다. 도메인 분리와 관련된 로그는 서버의 syslog_domain 테이블에 있습니다.

1. Domain Separation 센터의 오류 또는 경고 상자에서 숫자를 선택합니다.

   오류 또는 경고 페이지가 각각 표시됩니다.

2. 목록에서 감사 중 하나를 선택합니다.

   이 페이지에는 선택한 감사의 문제에 대한 자세한 정보가 표시됩니다. 감사 결과 상세 정보의 메시지는 오류 또는 경고를 표시하는 테이블 감사에 대한 syslog_domain 테이블의 값을 참조합니다.

3. 경고 또는 오류 감사에 대한 정보를 제공하는 서버의 로그를 보려면 다음을 수행합니다.
   a. 경고 또는 오류의 왼쪽 패널에서 상세 정보 **ID** 값을 복사합니다.
   b. HI의 필터 탐색기에서 *syslog_domain.do*를 입력합니다.

      Domain Log(도메인 로그) 페이지가 표시됩니다.

   c. 소스 검색 필드에 `=<Detail-ID>`(등호 뒤에 공백 없음)를 입력합니다(예: =f6a00fd29a85b300a9503a81b9169678).

      도메인 로그 페이지에는 지정한 상세 ID가 있는 감사와 관련된 로그만 표시됩니다. 테이블의 각 행은 감사에서 문제가 발견된 다른 기록을 지정합니다. 이 페이지의 메시지 필드는 도메인 서비스 센터의 메시지 열에 표시된 값과 일치합니다. 메시지 형식이 감사 유형과 일치합니다.

4. 선택:
   - **Rerun** Audit(감사 다시 실행) - 감사를 다시 실행하여 경고나 오류가 계속 발생하는지 확인합니다.
   - 감사 비활성화 - 감사를 비활성화합니다.
   - 세부정보 복사 - 감사 세부정보를 클립보드에 복사합니다.

실행 중인 감사 및 보류 중인 감사 보기

활성 감사는 정기적으로 실행되거나 예약된 대로 실행되도록 큐에 대기됩니다. 실행 시 상태를 볼 수 있습니다.

1. 현재 실행 중이거나 실행 보류 중인 감사를 보려면 감사 실행 중 상자에서 숫자를 선택합니다.

   Running Audits 페이지가 표시됩니다.

2. 감사에 대한 자세한 내용을 보려면 감사를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

비활성 감사 보기

1. 비활성 감사 상자에서 숫자를 선택합니다.

   비활성 감사 페이지에는 현재 비활성화된 모든 감사가 표시됩니다.

2. 감사 중 하나를 선택하여 자세한 정보를 표시합니다.
3. 감사를 활성화하려면 활성 상자를 선택하고 빈도 필드를 사용하여 감사 실행 빈도를 지정합니다.
4. 업데이트를 선택합니다.

Domain Separation Center 구성

도메인의 어떤 테이블이 큰지, 자세한 로깅을 사용할지 여부를 지정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
감사가 매일, 매주 또는 매월 실행되도록 예약할 수 있습니다. 큰 테이블에서 실행되는 감사에는 상당한 시간이 걸릴 수 있습니다. 따라서 큰 테이블에 대해 매일 감사를 실행하지 마십시오. 실행하는 데 하루 이상 걸리는 감사에 대해 새로운 감사를 시작하면 부정적인 결과를 초래할 수 있습니다.

자세한 로깅은 감사 중에 발견된 문제에 대한 보다 뛰어난 인사이트를 제공할 수 있지만 성능 문제를 일으킬 수 있습니다.

프로시저

1. Domain Separation Center에서 **Configure Domain** Center(도메인 센터 구성)를 선택합니다.
   Configure Domain Center(도메인 센터 구성) 페이지가 나타납니다.
2. 도메인 관련 문제를 진단하는 데 도움이 되는 자세한 로그를 저장하려면 상세 도메인 로깅 사용에 대해 예를 선택합니다.
   이러한 로그는 도메인 로그 [syslog_domain] 테이블의 서버 측 로그를 참조합니다. 로그 보기에 대한 자세한 내용은 경고 및 실패가 있는 감사 보기 섹션을 참조하세요.
3. 목록에서 큰 테이블을 모두 선택됨 열로 이동합니다.
   일일 감사는 큰 테이블에서 실행해서는 안 됩니다. 선택됨 열의 회색으로 표시된 테이블 이름이 커서 사용 가능 열로 이동할 수 없습니다.
4. 업데이트를 선택합니다.
5. 감사해서는 안 되는 큰 테이블이 있는 경우 시스템 속성을 쉼표로 구분된 해당 테이블 이름 목록으로 설정합니다 *com.glide.domain.audit.big_tables.additional*.

감사 구성

감사가 활성 상태인지 여부와 실행 빈도를 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. Domain Separation Center에서 **Configure** Audits(감사 구성)를 클릭합니다.
   T가 나타납니다.
2. 감사 구성 페이지에서 활성화할 각 감사를 구성합니다.
   감사는 기본적으로 비활성 상태입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 감사를 클릭합니다.

b. 활성 확인란을 클릭하여 감사를 활성화합니다.

c. 빈도 필드에서 감사가 실행되는 빈도를 지정합니다.
Domain Separation 센터에서는 동일한 빈도로 표시된 모든 감사를 동시에 실행합니다. 큰 테이블에서 실행되는 감사에 대해 매일 을 선택하지 마십시오.

d. 활성화하려는 각 감사에 대해 a-c 단계를 반복합니다.

3. 저장을 클릭합니다.

일정 감사

감사를 실행할 시간과 날짜를 지정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
하나 이상의 감사 를 매일, 매주 또는 매월 실행하도록 구성했습니다. 스케줄러는 이러한 감사를 실행할 요일과 시간을 지정합니다. 일정 빈도가 동일한 모든 감사는 구성 시점부터 순차적으로 실행됩니다.

프로시저

1. Domain Separation Center에서 **Audit** Schedules(감사 일정)를 클릭합니다.
감사 일정 페이지가 나타납니다.

2. 감사 일정을 구성합니다.

a. 일정 이름을 클릭합니다.

b. 감사를 실행할 시간을 지정합니다.
시간 단위는 24시간제를 사용합니다(즉, 14는 오후 2시와 같음).

c. 주별 일정의 경우 감사를 실행할 요일을 선택합니다. 여기서 1은 일요일입니다.

d. 월별 일정의 경우 감사를 실행할 월의 일을 선택합니다.

e. 다른 일정에 대해 이 절차를 반복합니다.

3. Save(저장)를 클릭하여 구성 변경 내용을 저장합니다.

4. 옵션: 지금 실행을 클릭하여 오른쪽 창 상단에 표시된 빈도로 실행하도록 예약된 모든 감사를 실행합니다.
예를 들어 창 제목이 도메인 감사 일정 **-** 매일인 경우 지금 실행 은 매일 실행하도록 예약된 모든 감사를 즉시 실행합니다.

다음에 수행할 작업
실행 중인 감사의 상태를 보려면 Domain Separation 센터에서 실행 중인 감사 상자의 숫자를 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

즉시 감사 실행

감사는 일반적으로 일정대로 실행됩니다. 그러나 명령에 따라 모든 감사를 실행할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
개별 감사는 수동으로 실행할 수 없습니다. 그러나 동일한 일정 빈도로 구성된 모든 감사를 실행할 수 있습니다. 예를 들어 매일 실행하도록 구성된 모든 감사를 실행할 수 있습니다.

프로시저

1. Domain Separation Center에서 **Audit** Schedules(감사 일정)를 클릭합니다.
2. 실행할 감사 일정의 이름(예: 매일, 매주 또는 매월)을 클릭합니다.
3. 지금 실행을 클릭합니다.

다음에 수행할 작업
실행 중인 감사의 상태를 보려면 Domain Separation 센터에서 실행 중인 감사 상자의 숫자를 클릭합니다.

경고 및 오류가 있는 감사 보기

Domain Separation 센터에서는 감사 오류 및 경고에 대한 상세 정보를 제공합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Domain Separation Center 대시보드에서 오류 및 경고는 문제가 발생한 감사에 대한 자세한 정보를 제공합니다. 도메인 분리와 관련된 로그는 서버의 syslog_domain 테이블에 있습니다. 오류는 즉각적인 주의가 필요한 문제입니다. 경고는 실패로 이어지지는 않지만 도메인 이름을 너무 길게 만들지 않는 것과 같은 모범 사례를 제시합니다.

프로시저

1. Domain Separation 센터에서 오류 또는 경고 상자의 숫자를 클릭합니다.
   오류 또는 경고 페이지가 나타납니다.
2. 목록에서 감사 중 하나를 클릭합니다.
   이 페이지에는 선택한 감사의 문제에 대한 자세한 정보가 표시됩니다. 감사 결과 상세 정보의 메시지는 오류 또는 경고를 표시하는 테이블 감사에 대한 서버의 syslog_domain 테이블에 있는 값을 참조합니다.
3. 경고 또는 오류 감사에 대한 정보를 제공하는 서버의 로그를 보려면 다음을 수행합니다.

   a. 경고 또는 오류의 왼쪽 패널에서 상세 정보 **ID** 값을 복사합니다.

   b. Domain Separation Center를 실행하는 인스턴스의 필터 탐색기에서 *syslog_domain.list*를 입력합니다.
   Domain Log(도메인 로그) 페이지가 나타납니다.

   c. 원본 열의 검색 필드에 `=<Detail-ID>`(등호 뒤에 공백 없음)를 입력합니다(예: `=f6a00fd29a85b300a9503a81b9169678`).
   도메인 로그 페이지에는 지정한 상세 ID가 있는 감사와 관련된 로그만 표시됩니다. 테이블의 각 행은 감사에서 문제가 발견된 다른 기록을 지정합니다. 이 페이지의 메시지 필드는 도메인 서비스 센터의 메시지 열에 표시된 값과 일치합니다. 메시지에 포함된 정보가 감사 유형과 일치합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 옵션: 다음 중 하나를 선택합니다.
   - **Rerun** Audit(감사 다시 실행) - 감사를 다시 실행하여 경고나 오류가 계속 발생하는지 확인합니다.
   - 감사 비활성화 — 감사를 비활성화합니다.
   - 세부 정보 복사 — 감사 세부 정보를 클립보드에 복사합니다.

실행 중인 결과 및 보류 중인 결과 보기

실행 중인 감사와 보류 중인 감사를 보고 상태를 확인할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
활성 감사는 정기적으로 실행되거나 예약된 대로 실행되도록 큐에 대기됩니다. 실행 시 상태를 볼 수 있습니다.

프로시저
1. 현재 실행 중이거나 실행 보류 중인 감사를 보려면 감사 실행 중 상자의 숫자를 클릭합니다.
   Running Audits(감사 실행) 페이지가 나타납니다.
2. 해당 감사에 대한 정보를 보려면 실행 중이거나 보류 중인 감사를 클릭하십시오.

비활성 감사 보기

한 곳에서 모든 비활성 감사를 보고 선택적으로 활성화할 수 있습니다.

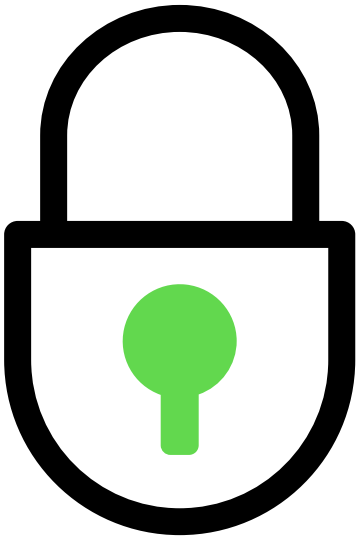
시작하기 전에
필요한 역할: 관리자

프로시저
1. 비활성 감사 상자에서 숫자를 클릭합니다.
   비활성 감사 페이지에는 현재 비활성화된 모든 감사가 표시됩니다.
2. 감사 중 하나를 클릭하여 자세한 정보를 표시합니다.
3. 옵션: 활성 상자를 클릭하고 빈도 필드에서 감사 실행 빈도를 지정하여 감사를 활성화합니다.
4. 업데이트를 클릭합니다.

인증

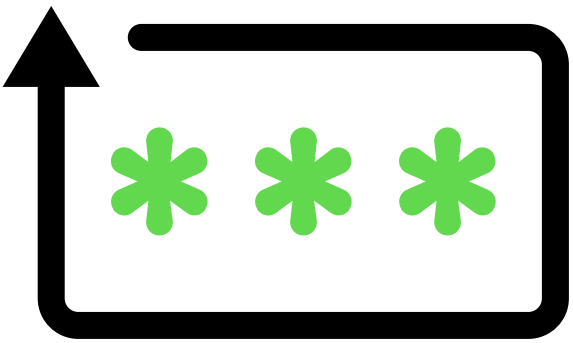
ServiceNow®의 인증은 인스턴스에 액세스하는 사용자의 ID를 확인한 다음, 사용자에게 사용자의 역할 또는 직무 기능과 일치하는 기능을 사용할 수 있는 권한을 부여합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



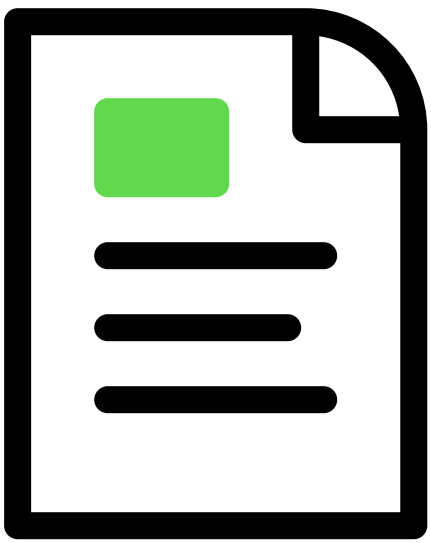
다중 제공자 1회 사용자 인증**(SSO)**

데이터베이스에 일치하는 사용자 계정이 있는 ID 공급자에서 구성한 사용자 이름 및 암호입니다.



OAuth 인바운드 및 아웃바운드

OAuth 기반 인증은 인증 프로토콜을 사용하여 시스템에서 신뢰를 설정하려고 시도하는 클라이언트의 ID를 확인합니다.



API 접근 정책

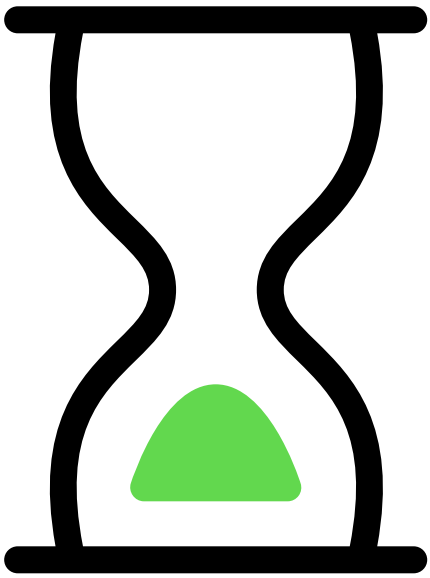
API 액세스 정책은 정책을 통해 제어할 수 있는 API에 대한 권한과 액세스를 정의합니다.



다이제스트 토큰 인증

사용자 이름과 테이블의 암호는 SHA1, SHA 256 또는 MD5와 같은 사용자별 해시 작업을 수행합니다. 이 값은 쿼리 매개변수에서 작동하는 URL 접미사의 일부로 추가되어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



시간 제한 인증

에서 링크 기반 인증 구성

ServiceNow

인스턴스. 구성된 링크는 이메일 또는 SMS를 통해 사용자와 공유할 수 있으며 사용자는 해당 링크를 사용하여 인스턴스에 로그인할 수 있습니다.



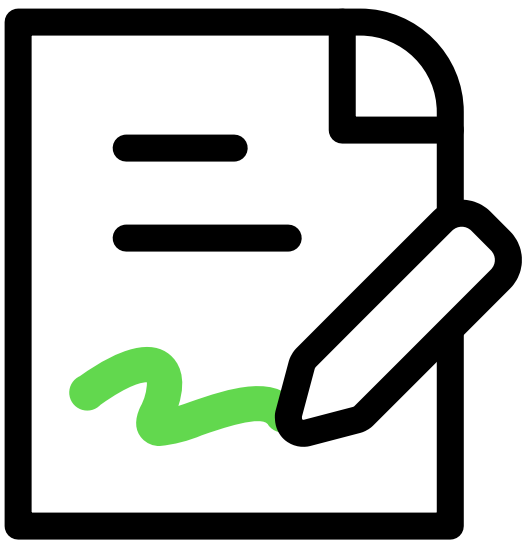
다단계 인증**(MFA)**

MFA를 사용하면 인증 앱, 하드웨어 키, 생체 인식 인증기, SMS 또는 이메일의 암호 사용을 포함하는 두 번째 수준의 인증을 제공할 수 있습니다.



인증서 기반 인증

인증서 기반 인증을 위한 사용자 이름과 암호 대신 사용자에게 매핑된 고유한 PEM 인코딩 인증서입니다.

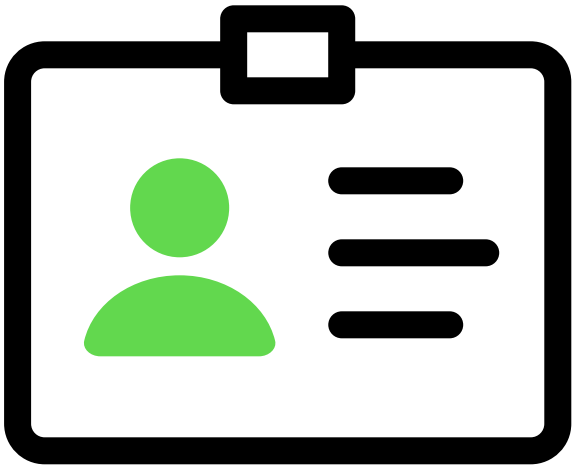


자체 등록

외부 사용자 자체 등록을 사용하여 대량의 외부 사용자를 인스턴스에 온보딩합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



LDAP

LDAP(Lightweight Directory Access Protocol) 디렉터리와 통합하여 사용자 로그인 프로세스를 간소화합니다.

여러 가지 방법을 사용하여 사용자를 인증할 수 있습니다. 사용자 자격 증명은 각 방법에 대해 저장된 다른 자격 증명과 일치합니다.

주:

- SSO 플러그인은 Okta 사용 중단되었습니다.
- 권한 부여 처리에 영향을 주는 보안 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 접근 통제 .
- 복수 제공자 SSO 애플리케이션을 통해 SAML 및 다이제스트 인증을 사용할 수 있습니다.

적응형 인증

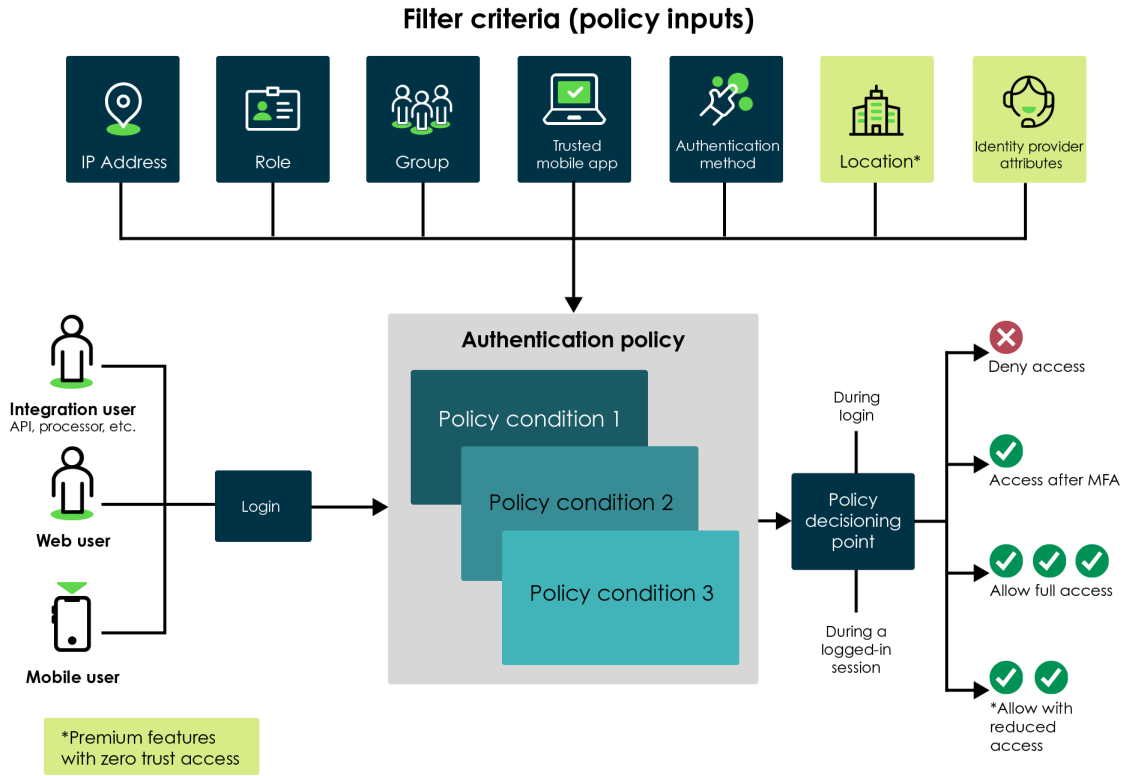
적응형 인증 정책 프레임워크를 사용하여 상황별 인증 제어를 적시에 적절한 사용자에게 적용합니다. 적응형 인증은 인증 정책을 사용하여 인증 요청을 평가한 다음 지정된 정책 조건에 따라 인스턴스에 대한 액세스를 거부하거나 허용합니다.

적응형 인증 정책 및 컨텍스트를 사용하여 IP 주소, 사용자 역할, 사용자 그룹과 같은 기준에 따라 사용자 및 API에 대한 인스턴스 액세스를 제한합니다. 보안 요구 사항에 따라 기본 제공 인증 정책을 구성할 수 있습니다.

예를 들어, 관리자는 신뢰할 수 있는 IP 주소 범위 내에 있고 특정 역할의 구성원인 사용자의 로그인을 허용하도록 을 *Allow Access Policy* 구성할 수 있습니다. 에 할당 *Post-authentication context*되면 액세스 정책은 신뢰할 수 없는 IP 주소의 액세스를 거부합니다.

인스턴스의 언어로 사용자 지정 메시지를 설정하려면 `sys_ui_message.list` 에 키, 값 쌍을 추가하고 `sys_ui_message` 기록을 업데이트해야 합니다. 잘못된 암호로 로그인하면 기본 설정 언어로 된 사용자 지정 메시지가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



적응형 인증 구성요소

인증 정책

인증 정책은 지정된 정책 조건에 따라 인증 요청을 평가하고 정책 조건 평가의 출력에 따라 액세스를 허용하거나 거부합니다. 예를 들어 액세스 허용 정책에 지정된 모든 정책 조건이 true로 평가되는 경우에만 액세스가 허용됩니다.

인증 정책은 필터 기준에서 제공하는 정보를 사용하여 정책 조건과 비교하여 인스턴스에 대한 액세스 권한을 부여할지 여부를 결정합니다. 예를 들어 필터 조건은 사용자의 IP 주소를 제공하고 정책 조건은 액세스 권한을 부여하기 전에 이 주소가 특정 범위 내에 있는지 여부를 확인합니다. 인증 정책에 대한 자세한 내용은 을 참조하십시오 인증 정책.

인증 정책 컨텍스트

인증 정책 컨텍스트는 로그인 프로세스 중에 정책을 적용하는 방법과 시기를 정의합니다. 사전 인증 컨텍스트는 사용자에게 로그인 화면이 표시되기 전에 실행됩니다. 사후 인증 컨텍스트는 사용자가 자격 증명을 입력한 후에 실행됩니다. 정책을 사용하려면 정책 컨텍스트에 할당해야 합니다. 이러한 컨텍스트에 대한 자세한 내용은 다음 문서를 참조하십시오 인증 정책 컨텍스트.

필터 기준

필터 기준(정책 입력이라고도 함)은 정책 조건의 입력으로 사용됩니다. 정책 조건은 이러한 입력을 사용하여 인증 요청의 요구 사항을 확인하고 충족합니다. 이러한 입력은 사용자 역할, IP 범위 및 ID 제공자와 같은 정보를 제공합니다. 필터 조건에 대한 자세한 내용은 다음 문서를 참조하십시오 필터 기준.

인증 속성

인증 속성을 사용하여 인스턴스에서 적응형 인증이 활성 상태인지 여부를 제어합니다. 또한 속성을 사용하여 디버깅을 활성화하고 액세스가 차단될 때 사용자에게 표시되는 메시징을 정의할 수 있습니다. 이러한 속성에 대한 자세한 내용은 문서를 참조하십시오 적응형 인증 속성 구성.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

REST API 접근 정책

적응형 인증 프레임워크의 필터 기준을 사용하여 인바운드 ServiceNow REST API에 대한 액세스를 제한할 수 있습니다. 자세한 내용은 REST API 접근 정책 문서를 참조하십시오.

도메인 분리 및 적응형 인증

적응형 인증은 인증 정책 조건 수준의 도메인 분리 인스턴스에서 지원됩니다. 정책 조건은 기록 도메인 [sys_domain] 필드의 도메인에 영향을 미칩니다. 전역 도메인의 정책 조건은 모든 도메인에 영향을 줍니다.

적응형 인증 이벤트

적응형 인증 이벤트 테이블을 사용하여 적응형 인증 기능과 관련하여 발생한 이벤트에 대해 알 수 있습니다. 자세한 내용은 적응형 인증 이벤트 문서를 참조하십시오.

적응형 인증 활성화

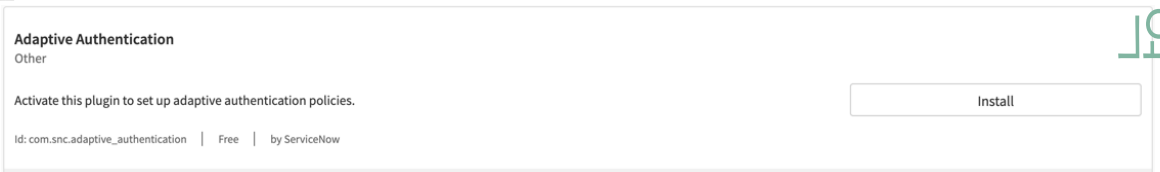
관리자 역할이 있는 경우 Adaptive Authentication용 Adaptive Authentication 플러그인 (com.snc.adaptive_authentication)을 활성화할 수 있습니다.

시작하기 전에
필요한 역할: admin.

이 태스크 정보

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 **Adaptive Authentication** (com.snc.adaptive_authentication) 플러그인을



찾습니다.

이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.

3. 설치를 선택하여 설치 프로세스를 시작합니다.

> 주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

다음에 수행할 작업
인스턴스에 상황별 인증 통제를 적용하도록 인증 정책을 구성합니다.

정책이 구성되면 인증 정책 사용 정책을 사용하여 적응형 인증을 활성화합니다. 적응형 인증 속성에 대한 자세한 내용은 문서를 참조하십시오 적응형 인증 속성 구성.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필터 기준

필터 기준(정책 입력이라고도 함)은 인증 요청의 요구 사항을 확인하고 충족하기 위한 정책 조건의 입력으로 사용됩니다.

필터 기준을 사용하여 사용자의 IP 주소, 역할 또는 그룹과 같은 정보 인증 정책을 제공합니다. 정책의 정책 조건 섹션에 이러한 기준을 추가합니다.

적응형 인증에 사용되는 필터 기준에는 7가지 유형이 있습니다. 인증 정책은 이러한 조건 중 하나 이상을 사용하여 인증 요청을 평가할 수 있습니다.

주: 제로 트러스트 액세스 기능에서 위치 필터와 ID 제공자 필터를 사용할 수 있습니다. 자세한 내용은 제로 트러스트 액세스 문서를 참조하십시오.

필터 기준 유형

유형	설명
IP 필터 기준	IP 필터 기준을 사용하여 사용자의 IP 주소를 기준으로 사용자를 필터링합니다. IPv4와 IPv6가 모두 지원됩니다.
역할 필터 기준	역할 필터 기준을 사용하여 역할에 따라 사용자를 필터링합니다.
그룹 필터 기준	그룹 필터 기준을 사용하여 사용자가 속한 사용자 그룹을 기반으로 사용자를 필터링합니다.
위치 필터 기준	위치 필터 기준을 사용하여 사용자 위치를 기준으로 사용자를 필터링합니다.
ID 제공자 속성 필터 기준	IdP로부터 SAML 응답으로부터 받은 ID 제공자 속성을 인증을 위한 필터 기준으로 사용합니다.

일반 기준

위에 나열된 유형 외에도 네 가지 일반 필터 기준이 있습니다. 이러한 기준은 필터 탐색기에 나타나지 않지만 인증 정책에 정책 입력을 추가하는 동안 선택할 수 있습니다.

일반 필터 기준 유형

유형	설명
인증 체계	사용자의 인증 체계를 기반으로 필터링하는 데 사용합니다. 이 기준은 다음 두 가지 옵션이 있는 선택 유형입니다. • 로컬 로그인을 나타내는 사용자 이름 및 암호 • SSO는 다중 SSO(SAML, OIDC 또는 다이제스트) 기반 로그인을 나타냅니다. 주: 이 필터 기준은 통합 - 다중 제공자 1회 사용자 인증(SSO) 설치 관리자[com.snc.integration.sso.multi.installer] 플러그인이 설치된 경우에만 사용할 수 있습니다.
ID 제공자	사용자의 ID 제공자를 기반으로 필터링하는 데 사용합니다. 인증 체계 기준과 함께 사용하여 로그인 프로세스를 세부적으로 제어할 수 있습니다. 이 기준은 **ID** 제공자 [sso_properties] 테이블에 대한 참조입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일반 필터 기준 유형

유형	설명
	주: 이 필터 기준은 통합 - 다중 제공자 1회 사용자 인증(SSO) 설치 관리자[com.snc.integration.sso.multi.installer] 플러그인이 설치된 경우에만 사용할 수 있습니다.
역할 기반 MFA	역할 기반 MFA 기능을 기반으로 필터링하는 데 사용합니다. 이 기준은 사용자에 대해 역할 기반 MFA를 사용할 수 있는지 여부를 나타내는 부울 유형 필터 기준입니다.
사용자 기반 MFA	사용자 기반 MFA 기능을 기반으로 필터링하는 데 사용합니다. 이 기준은 사용자에 대해 사용자 기반 MFA를 사용할 수 있는지 여부를 나타내는 부울 유형 필터 기준입니다.
신뢰할 수 있는 모바일 앱	모바일 앱에서 인스턴스 액세스를 활성화하기 위한 신뢰할 수 있는 모바일 앱 필터입니다.

IP 필터

IP 필터 기준을 사용하여 사용자의 IP 주소를 기준으로 사용자를 필터링합니다. IPv4와 IPv6가 모두 지원됩니다.

IP 필터 기준을 사용하면 사용자의 IP 주소를 기준으로 사용자를 필터링할 수 있습니다. 특정 주소 또는 주소 범위에 대한 액세스를 허용하거나 거부하도록 인증 정책을 구성할 수 있습니다.

IP 필터 기준 생성

IP 필터 기준을 사용하면 사용자의 IP 주소를 기준으로 사용자를 필터링할 수 있습니다. 특정 주소 또는 주소 범위에 대한 액세스를 허용하거나 거부하도록 인증 정책을 구성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

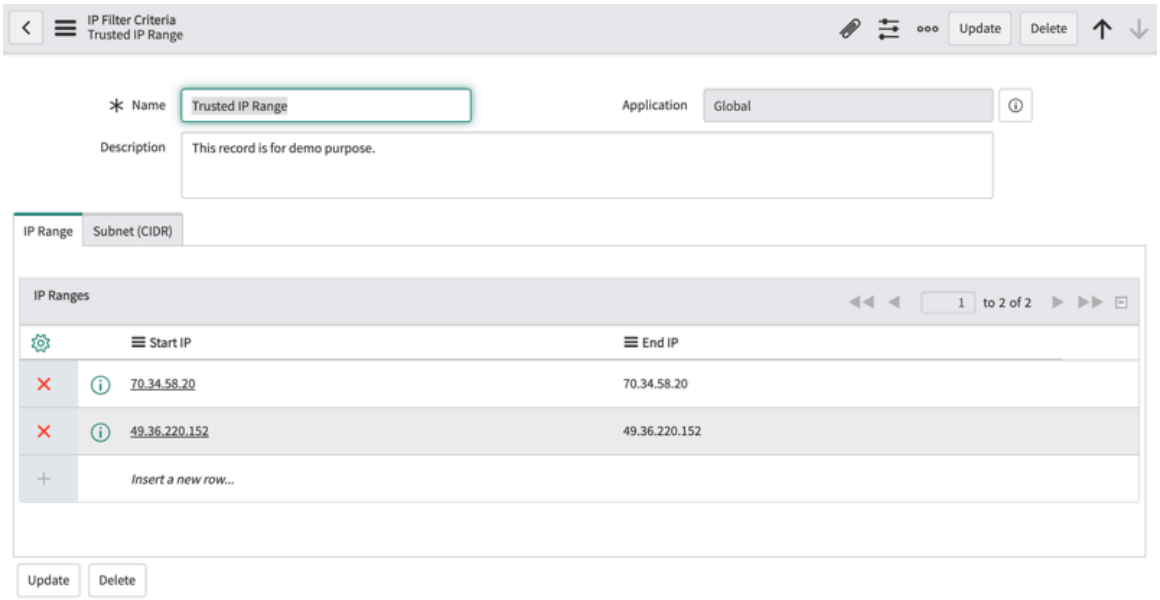
1. 다음으로 이동 모두 > 적응형 인증 > 필터 기준 > **IP** 필터 기준.
2. 새로 만들기를 클릭합니다.
3. 양식에서 다음과 같은 필드를 채웁니다.

IP 필터 기준 양식

필드	설명
이름	IP 네트워크를 식별하기 위한 이름입니다.
설명	IP 네트워크에 대한 간단한 설명입니다.
애플리케이션	애플리케이션의 범위입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

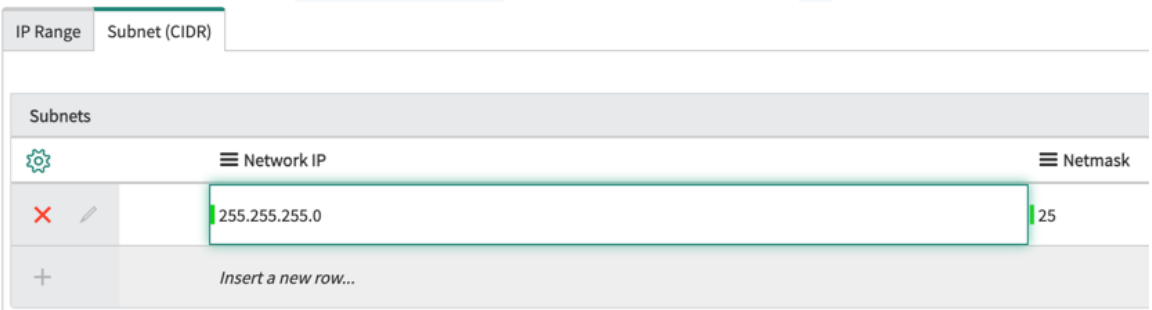
예시 **IP** 필터 기준 기록



4. 양식 헤더를 마우스 오른쪽 단추로 클릭하고 저장을 클릭합니다.
5. **IP** 범위 탭에서 새 행 삽입을 두 번 클릭합니다.
   단일 IP 주소 또는 여러 IP 주소 범위를 입력할 수 있습니다. 예를 들어 IP 주소 범위의 경우 시작 **IP** 열에 `192.0.2.0`을 입력하고 끝 **IP** 열에 `192.0.2.255`를 입력합니다.

   주: 단일 IP 주소의 경우 시작 **IP** 주소 열과 끝 **IP** 열에 동일한 IP 주소를 입력해야 합니다. 시작 **IP** 열에 IP 주소를 입력할 때 끝 **IP** 열을 비워 두고 레코드를 저장합니다. 끝 **IP** 열은 동일한 시작 **IP** 주소로 자동으로 채워집니다.

6. 서브넷**(CIDR)** 탭에서 새 행 삽입을 두 번 클릭합니다.
   네트워크 IP 주소 및 넷마스크를 CIDR(Classless Inter-Domain Routing) 형식으로 입력합니다. 예를 들어 네트워크 IP로 `255.255.255.0` 을 입력하고 넷마스크로 `25` 를 입력합니다.



역할 필터

역할 필터 기준을 사용하여 역할에 따라 사용자를 필터링합니다.

역할 필터 기준을 사용하면 역할을 기반으로 사용자를 필터링할 수 있습니다. 사용자 역할 목록에 대한 액세스를 허용하거나 거부하도록 인증 정책을 구성할 수 있습니다.

역할 필터 기준 생성

역할 필터 기준을 사용하면 역할을 기반으로 사용자를 필터링할 수 있습니다. 사용자 역할 목록에 대한 액세스를 허용하거나 거부하도록 인증 정책을 구성할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

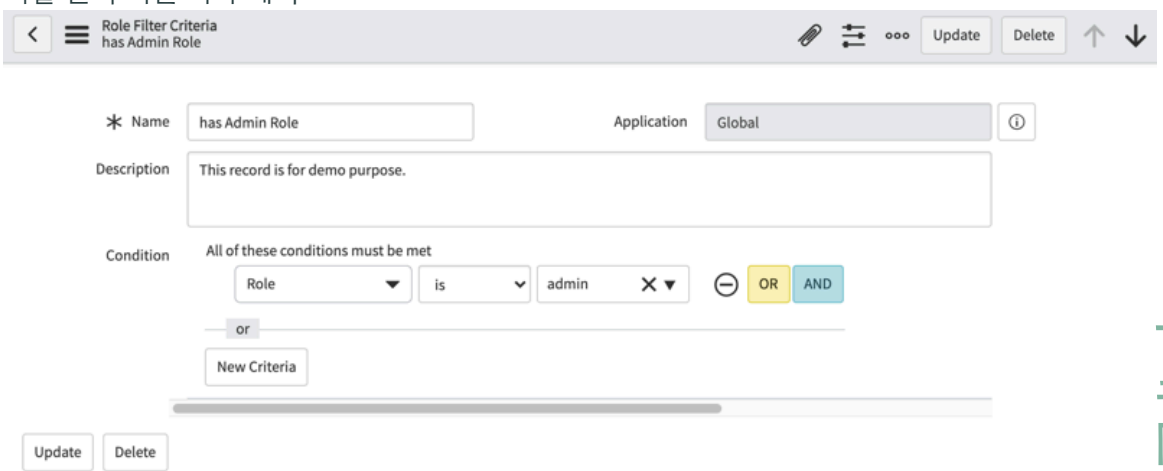
프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 필터 기준 > 역할 필터 기준.
2. 새로 만들기를 클릭합니다.
3. 양식에서 다음과 같은 필드를 채웁니다.

역할 필터 기준 양식

필드	설명
이름	역할을 식별하는 이름입니다.
애플리케이션	애플리케이션의 범위입니다.
설명	역할에 대한 간단한 설명입니다.

역할 필터 기준 기록 예시



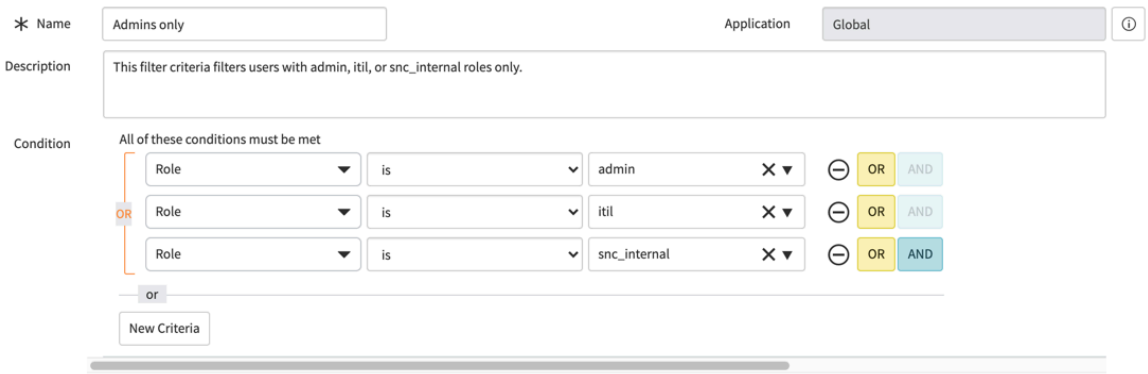
4. 역할에 대한 기준에서 새 행 삽입을 두 번 클릭합니다.
5. 조건 작성기를 사용하여 특정 역할에 대한 조건을 생성합니다.

   예를 들어 관리자, itil 또는 snc_internal 역할을 가진 사용자만 허용하는 조건을 만들 수 있습니다. 조건 작성기에 대한 자세한 내용은 조건 작성기를 사용하여 조건문 생성 단원을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 현재 닷워킹은 역할 필터 기준에서 지원되지 않습니다.
- 역할 필터 기준에 대해 다음 연산자가 지원되지 않습니다.
  - 일치하지 않음
  - 포함하지 않음
  - 다음과 다름
  - 비어 있음
  - 다음과 동일함
  - 비어 있지 않음
  - 빈 문자열임



그룹 필터

그룹 필터 기준을 사용하여 사용자가 속한 사용자 그룹을 기반으로 사용자를 필터링합니다.

그룹 필터 기준은 사용자가 속한 사용자 그룹에 따라 사용자 접근을 허용하거나 거부합니다.

그룹 필터 기준 생성

그룹 필터 기준은 사용자가 속한 사용자 그룹에 따라 사용자 접근을 허용하거나 거부합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

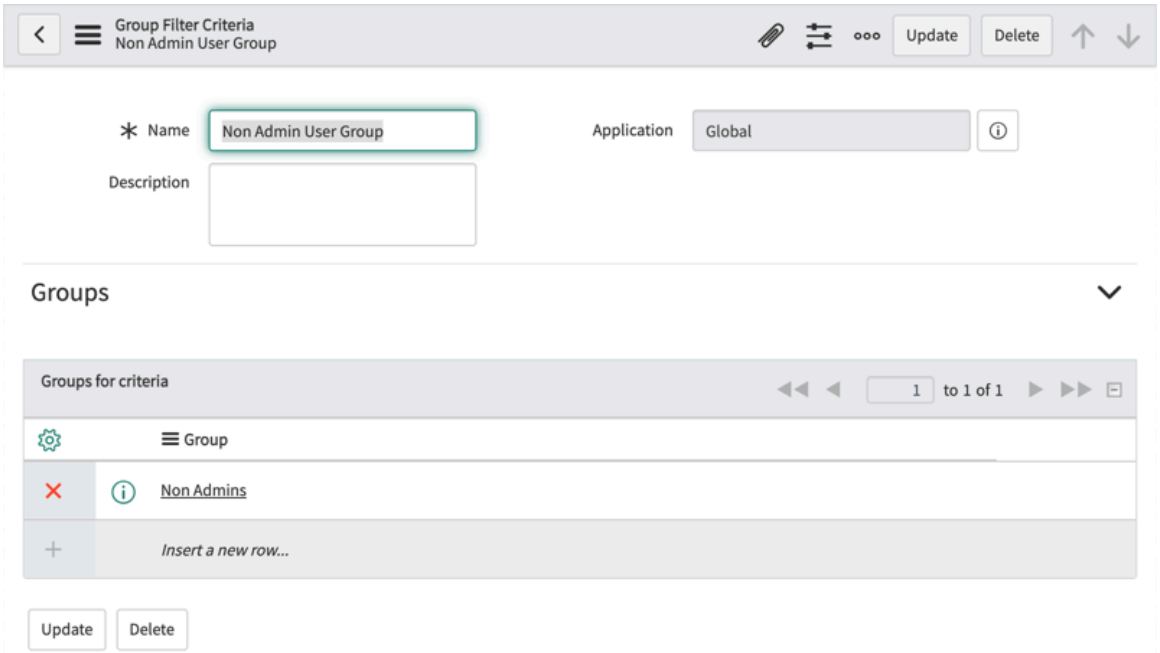
1. 다음으로 이동 모두 > 적응형 인증 > 필터 기준 > 그룹 필터 기준.
2. 새로 만들기를 클릭합니다.
3. 양식에서 다음과 같은 필드를 채웁니다.

그룹 필터 기준

필드	설명
이름	그룹을 식별하는 이름입니다.
설명	그룹에 대한 간단한 설명입니다.
애플리케이션	애플리케이션의 범위입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예시 그룹 필터 기준 기록



4. **Groups for** criteria(기준 그룹) 탭에서 **Insert a new** row(새 행 삽입)를 두 번 클릭합니다.
5. 검색 아이콘을 클릭하고 검색 클릭한 다음 사용자 그룹을 조회하고 선택합니다.
6. 저장 을 누릅니다.

위치 필터

위치 필터 기준은 사용자 위치를 기반으로 사용자에 대한 필터 입력으로 사용할 수 있습니다.

위치 필터는 관리자가 장치의 실제 위치를 기반으로 인증 정책을 작성하는 동안 사용할 수 있는 필터 기준입니다.

주:

- 위치 필터는 제로 트러스트 액세스 기능과 함께 사용할 수 있습니다. 자세한 내용은 제로 트러스트 액세스 문서를 참조하십시오.
- 인스턴스는 ADCv2에 있어야 합니다. 인스턴스가 ADCv2에 없는 경우 사용자 위치 정보를 사용할 수 없습니다.

위치 필터 기준을 사용하여 다음을 수행할 수 있습니다.

- 정책 입력으로 작동 정책 조건이 인증 요구 사항을 검증하고 충족하도록 합니다.
- 국가를 기반으로 적응형 인증 정책을 생성하는 기능을 제공합니다.
- 지정된 지리에 대한 인스턴스 액세스를 허용하거나 허용하지 않습니다.
- 지리적 위치 기반 사전 인증 또는 사후 인증 정책을 사용하여 다음을 수행합니다.
  - 엄격한 개인 정보 보호 통제 지역 외부의 제재 국가, 회사 재량에 대한 액세스를 차단합니다.
  - 해당 개인정보 보호 지역 및 회사 재량에 속하는 영역에만 액세스를 허용합니다.
  - 인증을 위한 국가 기반 허용 목록을 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용 케이스

다음은 적응형 인증에 위치 필터 기준을 사용하는 몇 가지 사용 사례입니다.

- 국가에서 인스턴스에 대한 액세스를 차단합니다.
- 특정 국가에서만 인스턴스에 액세스할 수 있도록 허용합니다.
- 국가를 기준으로 로그인하려면 스텝업 인증 또는 MFA를 적용합니다.
- 국가에 따라 사용자의 역할을 줄이거나 제한합니다.
- 위치 필터 기준은 MFA, 제로 트러스트 액세스(ZTA), 사전 인증 컨텍스트 및 사후 인증 컨텍스트에 사용할 수 있습니다.

위치 식별

사용자의 위치를 식별하기 위한 위치 서비스는 타사 서비스인 MaxMind에서 제공합니다.

사용자의 위치는 x-forwarded-for 헤더에서 VPN을 통해 식별됩니다. 서비스에 의해 채워진 헤더가 없는 경우 VPN IP(위치)만 사용자 위치로 표시됩니다.

주: 위치 필터 구성 후 잘못된 위치가 표시되는 경우 KB 문서를 참조하여 문제를 해결하십시오.

위치 기반 액세스 활성화

제로 트러스트 - 위치 기반 액세스(`com.snc.zero_trust_location_access`)를 활성화하여 관리자가 사용자의 위치에 따라 적응형 인증 정책을 구성할 수 있도록 합니다.

시작하기 전에

필요한 역할: 관리자

- 종속 플러그인: 적응형 인증
- 플러그인 유형: 유료이며 라이센스가 필요합니다.
- 인스턴스는 ADCv2에 있어야 합니다. 인스턴스가 ADCv2에 없으면 사용자 위치 정보를 사용할 수 없습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 Zero Trust - `com.snc.zero_trust_location_access`(위치 기반 액세스) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

위치 필터 기준 생성

위치 필터 기준을 사용하여 사용자 위치를 기반으로 사용자 인증에 대한 입력을 필터링합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

필요한 플러그인: 제로 트러스트 - 위치 기반 액세스 (`com.snc.zero_trust_location_access`).

속성: 적응형 인증 속성을 사용하도록 설정합니다.

주: 관리자는 현재 사용자 세션에 위치를 사용할 수 있는 경우에만 위치 필터를 기반으로 정책을 만들 수 있습니다.

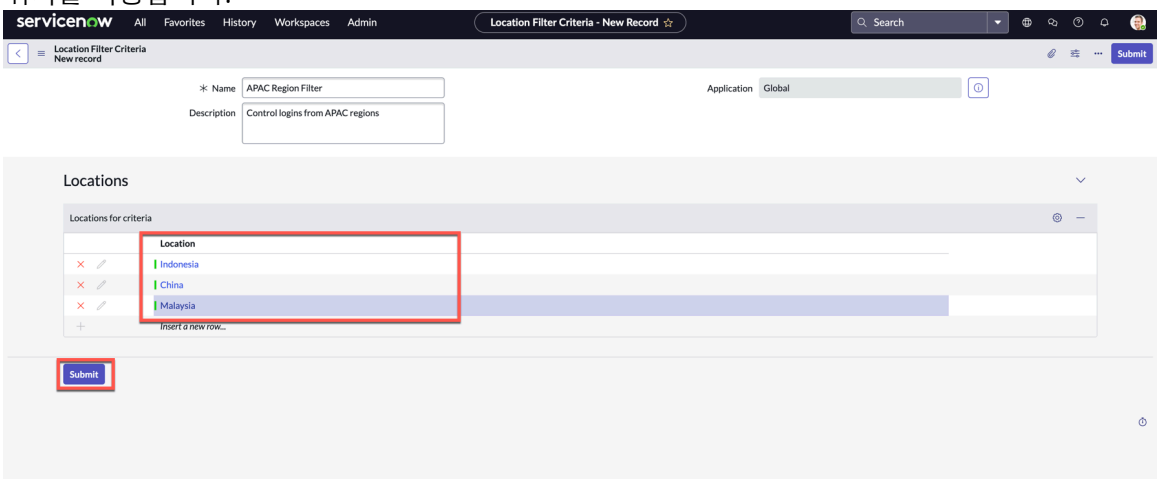
프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 필터 기준 > 위치 필터 기준.
2. 새로 만들기를 선택합니다.
3. 양식에서 다음과 같은 필드를 채웁니다.

위치 필터 기준 양식

필드	설명
이름	기준을 식별하는 이름입니다.
설명	기준에 대한 짧은 설명입니다.
애플리케이션	애플리케이션의 범위입니다.

4. 위치 섹션의 기준 위치 탭에서 새 행을 두 번 클릭하여 삽입합니다.
5. 위치를 지정합니다.



6. 제출을 선택합니다.

튜토리얼: 위치 필터 기준 사용

인증 정책에서 위치 필터 기준을 사용하고 위치에 따라 사용자에 대한 액세스를 제한하는 단계를 설명합니다.

시작하기 전에
필요한 역할: 관리자

필요한 플러그인: 제로 트러스트 - 위치 기반 액세스 (`com.snc.zero_trust_location_access`).

속성: 적응형 인증 속성을 사용하도록 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 관리자는 현재 사용자 세션에 위치를 사용할 수 있는 경우에만 위치 필터를 기반으로 정책을 만들 수 있습니다.

다음 절차에서는 인증 정책에서 위치 필터 조건을 만들고 사용하는 방법을 설명합니다.

프로시저

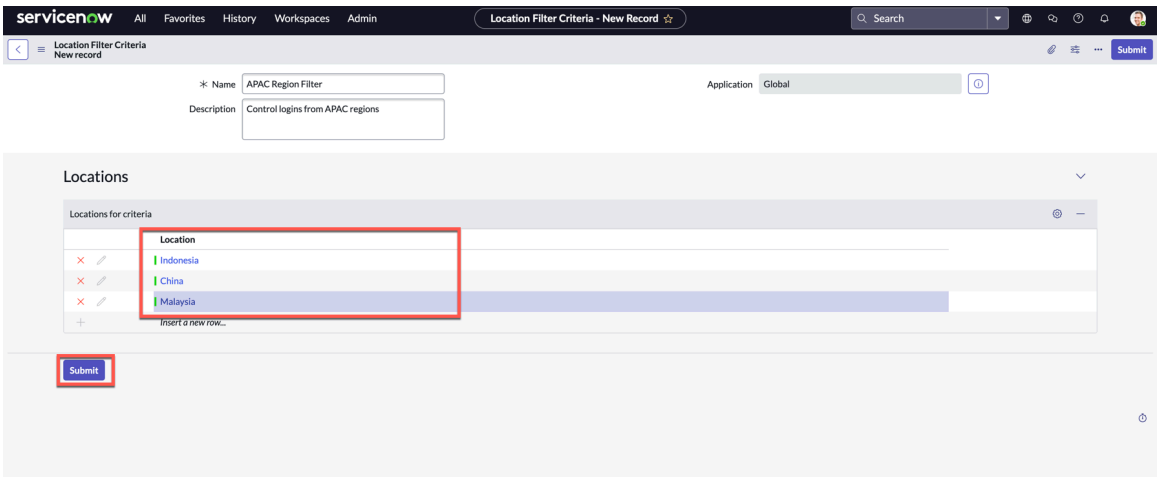
1. 다음으로 이동 모두 > 적응형 인증 > 필터 기준 > 위치 필터.
2. 새로 만들기를 선택합니다.
3. 양식에서 다음과 같은 필드를 채웁니다.

위치 필터 기준 양식

필드	설명
이름	기준을 식별하는 이름입니다.
설명	기준에 대한 짧은 설명입니다.
애플리케이션	애플리케이션의 범위입니다.

4. 위치 섹션의 기준 위치 탭에서 새 행을 두 번 클릭하여 삽입합니다.
5. 위치를 지정합니다.

예를 들어 일부 APAC 지역을 사용하여 APAC에서 오는 사용자의 로그인을 제어합니다.



예시에 설정된 기준에 따라 `##### ## #####`, `##` 및 `#####` 에서의 로그인을 제어할 수 있습니다.

6. 제출을 선택합니다.
7. 인증 컨텍스트(사전, 사후, MFA) 및 세션 액세스에서 생성된 필터 기준을 사용합니다.

인증 컨텍스트 및 세션 액세스를 기반으로 하는 구성에 대한 자세한 내용은 다음을 참조하십시오.

- 사전 인증 컨텍스트의 위치 필터
- 사후 인증 컨텍스트의 위치 필터
- MFA 컨텍스트의 위치 필터
- 세션 접근을 위한 위치 필터

인증 정책 실패(`glide.auth.policy.ui.error.message`)로 인해 로그인이 실패할 때 사용자에게 표시되는 속성 ID - 오류 메시지를 사용하여 오류 메시지를 사용자 지정할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사전 인증 컨텍스트에서 위치 필터 사용

사전 인증 컨텍스트에서 생성된 위치 필터 기준을 사용합니다.

시작하기 전에

필요한 역할: 관리자

필요한 플러그인: 제로 트러스트 - 위치 기반 액세스 (`com.snc.zero_trust_location_access`).

위치를 기반으로 사용자에 대한 액세스를 제한하려는 국가를 사용하여 위치 필터를 생성합니다. 자세한 내용은 위치 필터 기준 생성 문서를 참조하십시오.

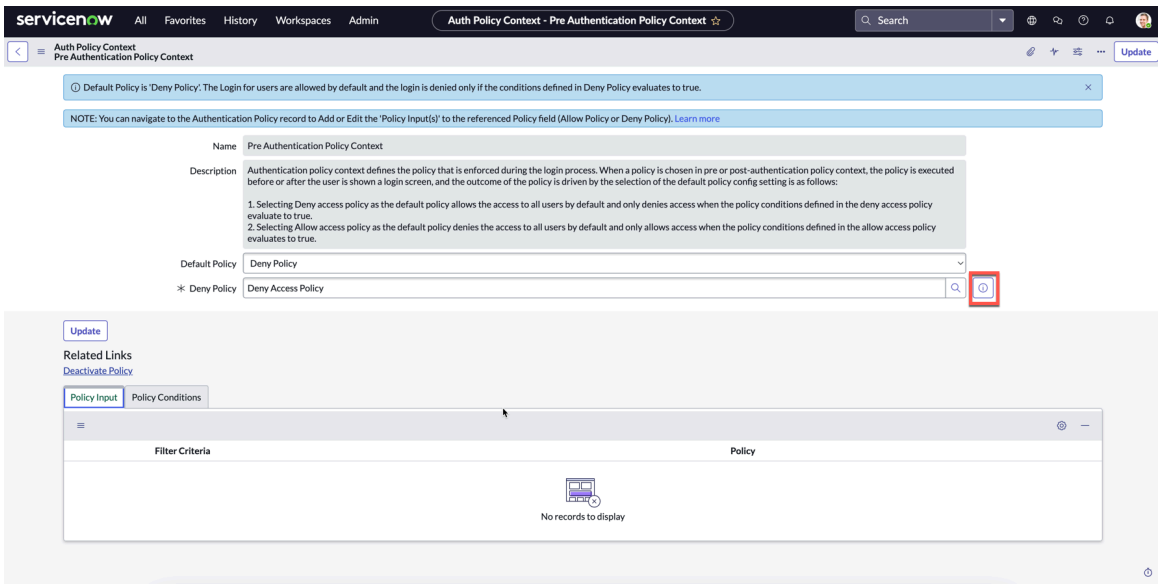
프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트 > 사전 인증 컨텍스트.

   사전 인증 정책 컨텍스트에서 정책을 선택한 경우:

   - 액세스 거부 정책을 기본 정책으로 선택하면 기본적으로 모든 사용자에 대한 액세스가 허용되고 액세스 거부 정책에 정의된 정책 조건이 예로 평가되는 경우에만 액세스가 거부됩니다.
   - 액세스 허용 정책을 기본 정책으로 선택하면 기본적으로 모든 사용자에 대한 액세스가 거부되고 액세스 허용 정책에 정의된 정책 조건이 예로 평가되는 경우에만 액세스가 허용됩니다.

   이 예시에서는 지정된 위치에서의 로그인을 제한할 수 있는 방법을 보여줍니다. 액세스 거부 및 관련 정책(액세스 거부)을 사전 인증 정책으로 선택하고 정책 입력 및 조건을 지정할 수 있습니다.

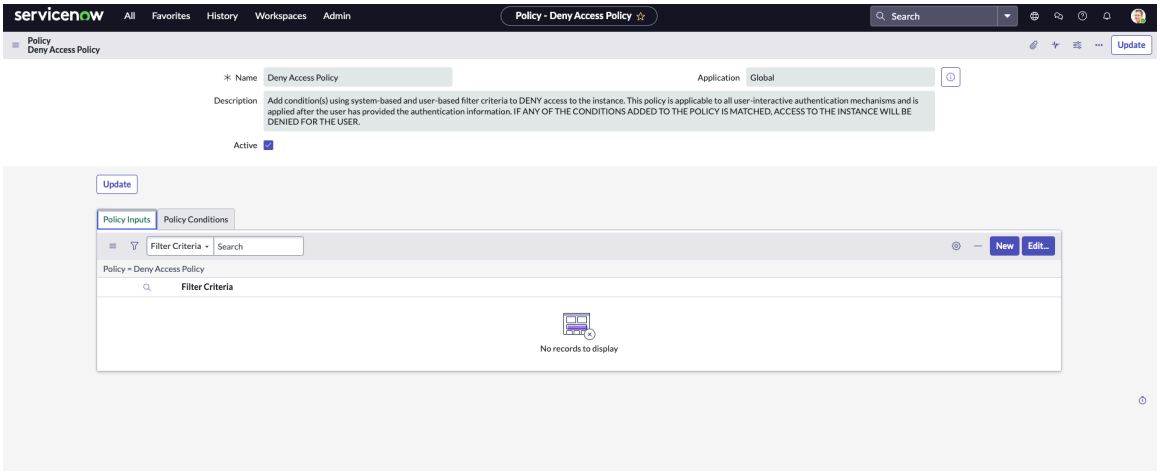


2. 정보 아이콘을 선택하여 거부 정책 기록을 엽니다.

   > **주:** 이 작업에 설명된 예는 거부 정책입니다. 또한 허용 정책을 사용하고 그에 따라 조건을 설정하여 로그인을 제어할 수 있습니다.

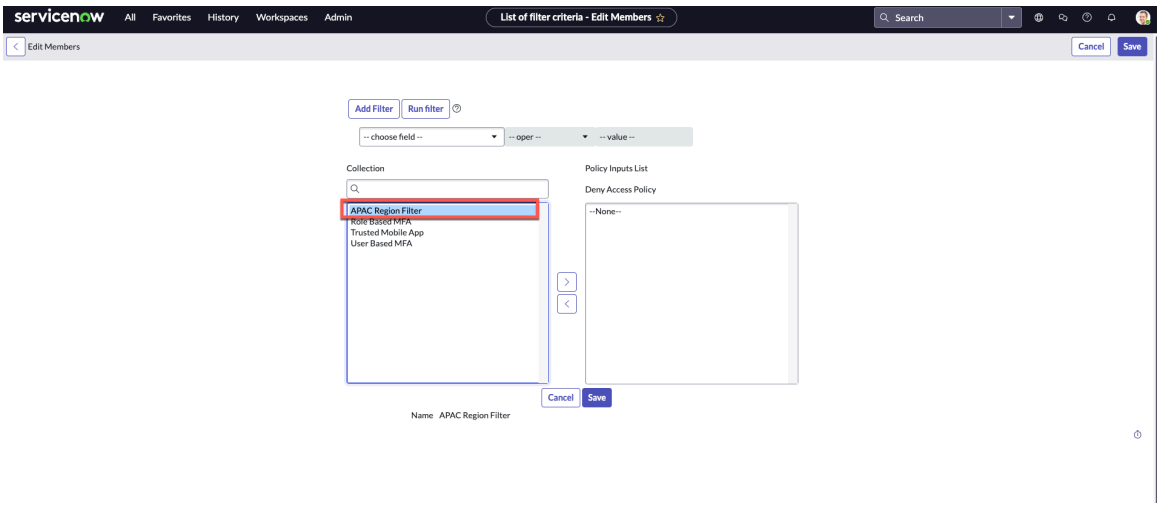
3. Deny Access Policy(액세스 거부 정책)의 Policy Inputs(정책 입력) 섹션에서 New(새로 만들기)를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



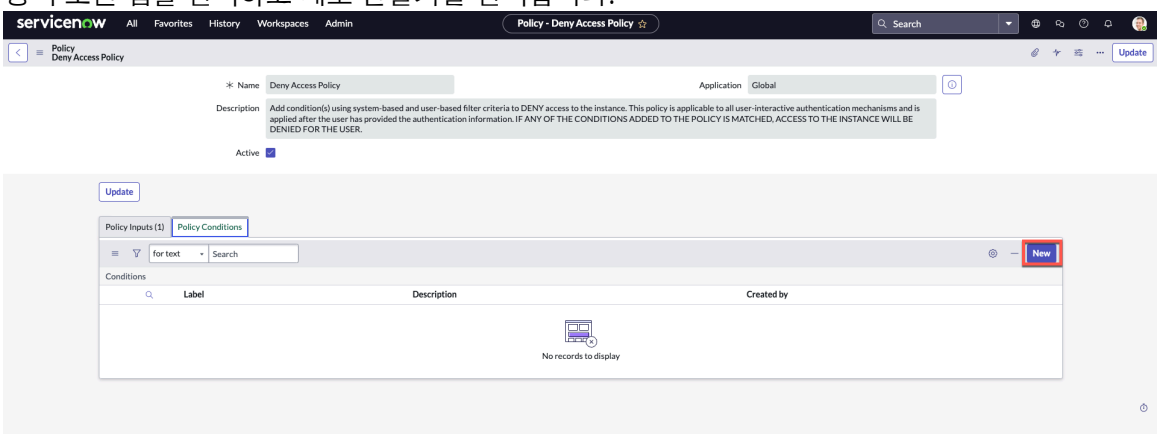
4. 위치 필터 입력을 추가하고 저장합니다.

   예: APAC 지역.



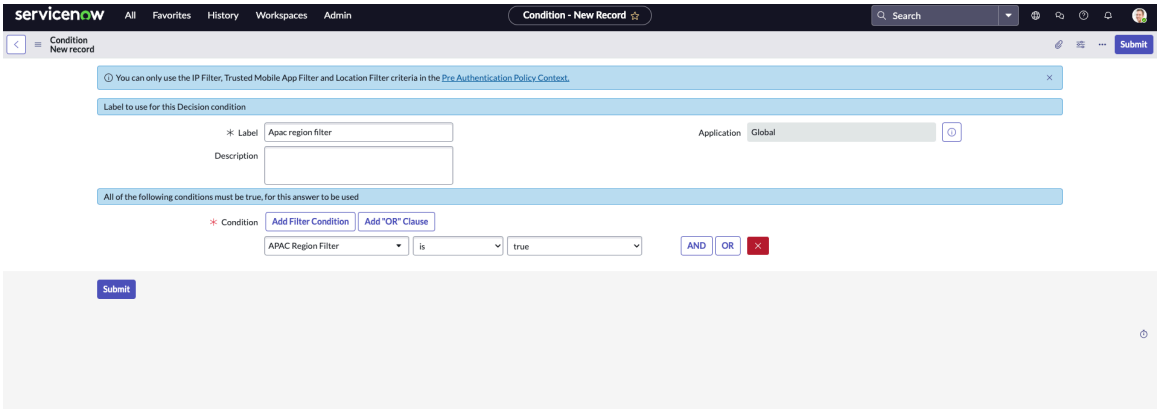
   필터가 정책 입력으로 추가됩니다.

5. 정책 조건 탭을 선택하고 새로 만들기를 선택합니다.



6. 조건 페이지에서 레이블, 조건을 입력하고 true로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:

- 이 예에서 true를 조건으로 선택하면 구성된 리전에서 로깅하는 사용자가 인스턴스에 로그인할 수 없습니다.
- 조건이 false로 설정된 경우 구성된 리전의 사용자만 인스턴스에 로그인할 수 있고 다른 사용자는 인스턴스에 로그인할 수 없습니다.

7. 제출을 선택합니다.
   인스턴스 링크를 선택하고 구성된 국가에서 로깅하는 사용자에게 액세스 거부에 대한 오류 메시지(정책 속성 페이지에서 관리자가 구성한 오류 메시지)가 표시됩니다.

위치 필터 사용 사후 인증 컨텍스트

사후 인증 컨텍스트에서 생성된 위치 필터 기준을 사용합니다.

시작하기 전에

필요한 역할: 관리자

필요한 플러그인: 제로 트러스트 - 위치 기반 액세스 (`com.snc.zero_trust_location_access`).

위치를 기반으로 사용자에 대한 액세스를 제한하려는 국가를 사용하여 위치 필터를 생성합니다. 자세한 내용은 위치 필터 기준 생성 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트 > 사후 인증 컨텍스트.

   사후 인증 정책 컨텍스트에서 정책을 선택한 경우:

   - 액세스 거부 정책을 기본 정책으로 선택하면 기본적으로 모든 사용자에 대한 액세스가 허용되고 액세스 거부 정책에 정의된 정책 조건이 예로 평가되는 경우에만 액세스가 거부됩니다.
   - 액세스 허용 정책을 기본 정책으로 선택하면 기본적으로 모든 사용자에 대한 액세스가 거부되고 액세스 허용 정책에 정의된 정책 조건이 예로 평가되는 경우에만 액세스가 허용됩니다.

   이 예시에서는 조건을 가진 `itil` 사용자가 지정된 위치(미국)에서만 인스턴스에 액세스하도록 구성하는 방법을 보여줍니다. 그리고 `itil` 사용자는 다른 국가에서 로그인할 수 없습니다.

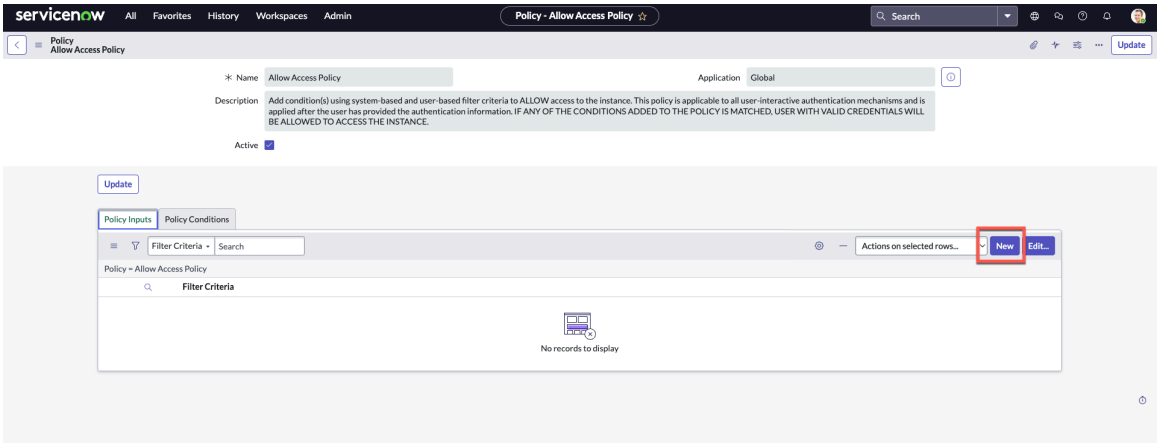
   사용자가 로그인 페이지에서 자격 증명을 제공한 후. 액세스 허용 및 관련 정책(액세스 허용)을 사후 인증 정책으로 선택하고 정책 입력 및 조건을 지정할 수 있습니다.

2. 정보 아이콘을 선택하여 정책 허용 기록을 엽니다.

   주: 이 작업에서 설명하는 예는 정책 허용입니다. 거부 정책을 사용하고 그에 따라 조건을 설정하여 로그인을 제어할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

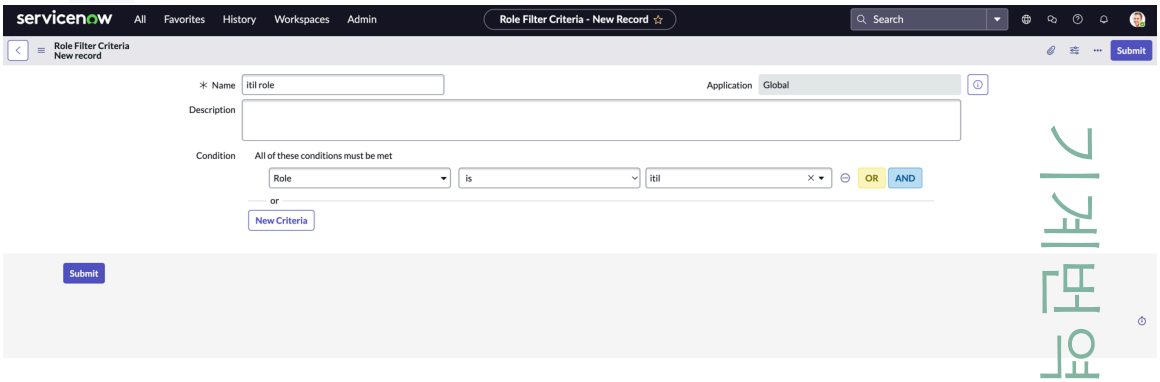
3. Allow Access Policy(액세스 허용 정책)의 Policy Inputs(정책 입력) 섹션에서 New(새로 만들기)를 선택합니다.



4. 역할 필터 기준 및 위치 필터 기준을 추가합니다.

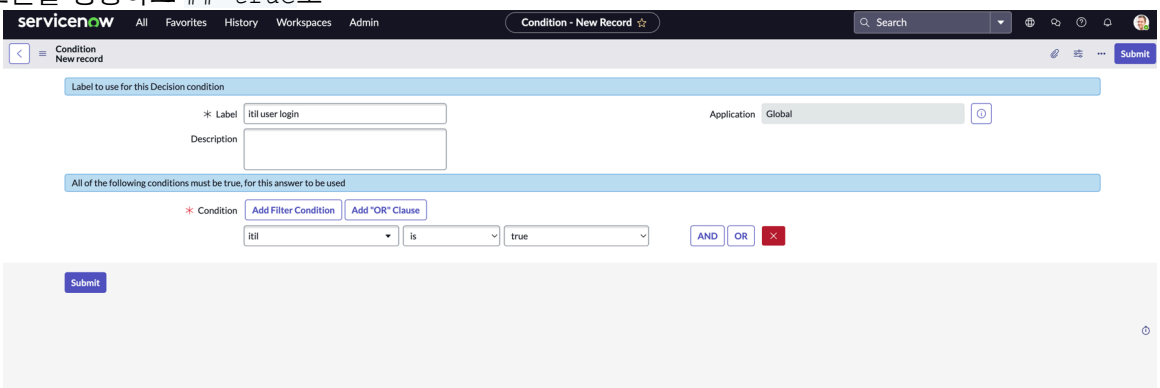
   a. 역할 필터 기준 추가:

   - 역할 필터 입력을 `itil`로



   생성합니다.

   - 역할 필터 조건을 생성하고 `## true`로



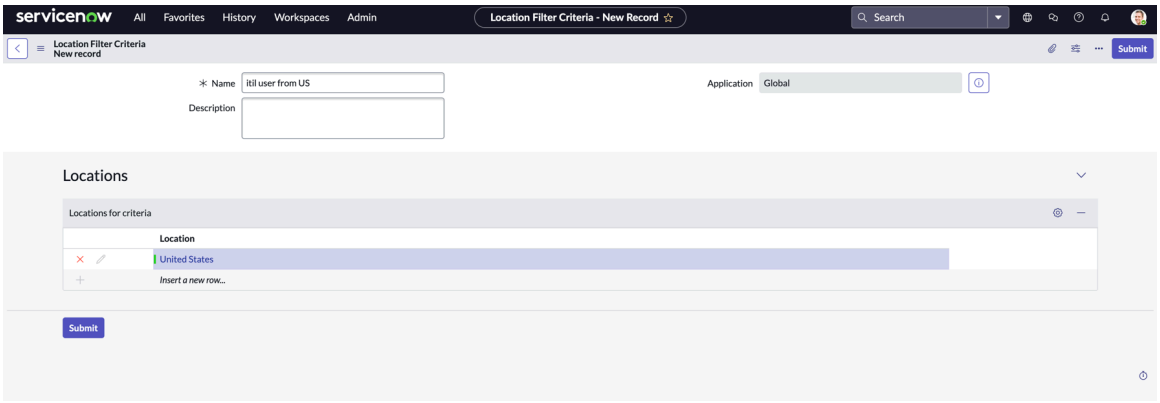
   설정합니다.

   역할 필터 조건을 만드는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 역할 필터 기준 생성.

   b. 위치 필터 기준 추가:

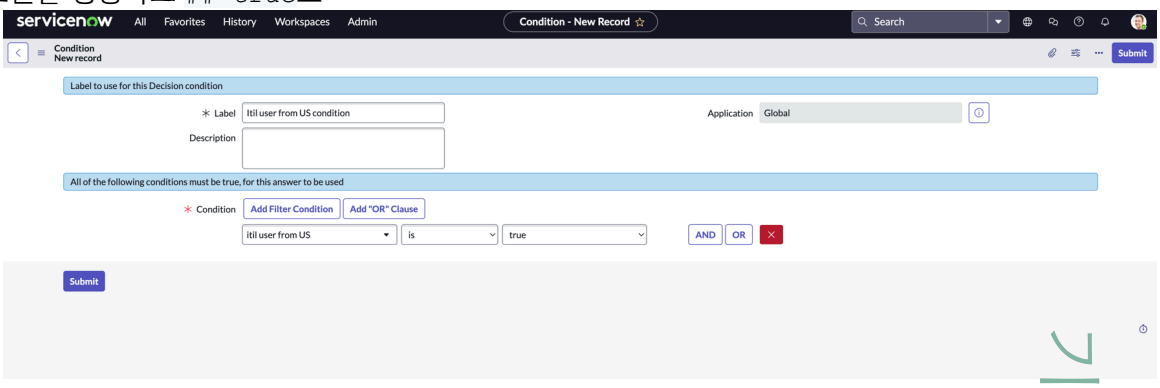
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 위치 필터 입력을 생성합니다. 위치에 미국을



추가합니다.

- 위치 필터 조건을 생성하고 `## true`로



설정합니다.

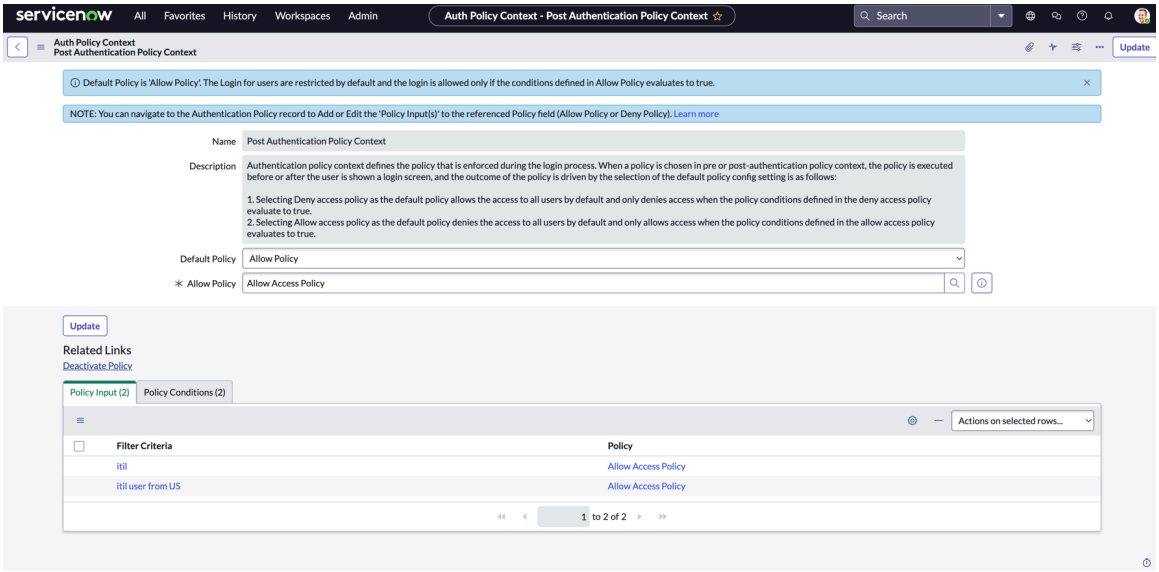
역할 필터 조건을 만드는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 위치 필터 기준 생성.

액세스 허용 정책에는 이전 단계에서 생성된 정책 입력 및 조건이 표시됩니다.

- 정책 입력: itil, 미국의 itil 사용자
- 정책 조건: itil 사용자 로그인, 미국의 itil 사용자 조건.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:

- 이 예에서 true를 조건으로 선택하면 구성된 국가(미국)에서 로깅하는 `itil` 사용자가 인스턴스에 로그인할 수 있습니다.
- 조건이 false로 설정되면 구성된 국가(미국)의 `itil` 사용자는 인스턴스에 로그인할 수 없으며 다른 사용자도 인스턴스에 로그인할 수 없습니다.

5. 제출 또는 업데이트를 선택하여 사후 인증 컨텍스트를 업데이트합니다.
인스턴스 링크를 선택하고 자격 증명을 지정한 다음 구성된 국가(미국) 외부에서 로깅하는 `itil` 사용자에게는 액세스 거부에 대한 오류 메시지가 표시됩니다(정책 속성 페이지에서 관리자가 구성한 오류 메시지).

MFA 컨텍스트에서 위치 필터 사용

MFA 컨텍스트에서 생성된 위치 필터 기준을 사용합니다.

시작하기 전에

필요한 역할: 관리자

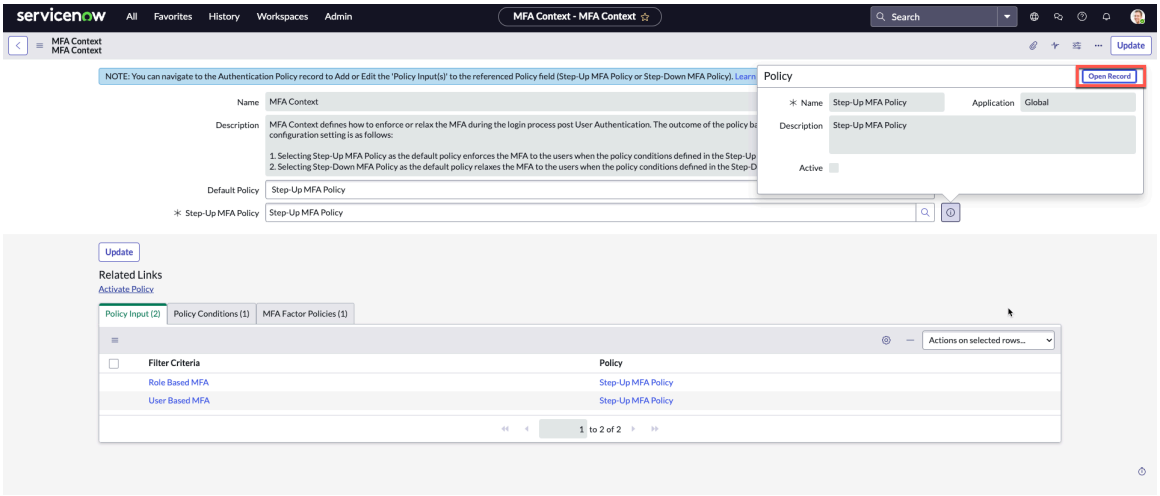
필요한 플러그인: 제로 트러스트 - 위치 기반 액세스 (`com.snc.zero_trust_location_access`).

다음 절차에서는 위치를 기반으로 사용자에 대한 인증을 위한 두 번째 단계로 MFA를 구성하려는 국가를 사용하여 위치 필터를 생성하는 방법에 대해 설명합니다.

프로시저

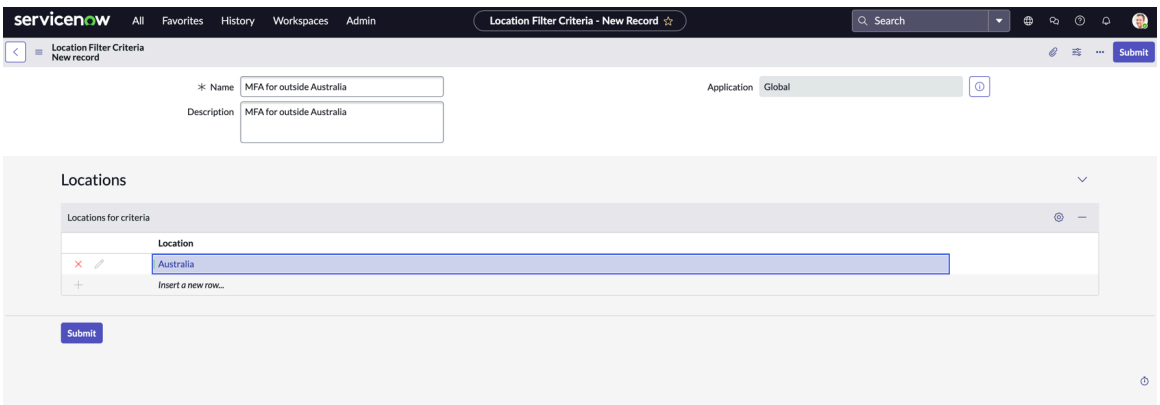
1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트 > **MFA** 컨텍스트.
2. **MFA** 컨텍스트 페이지에서 스텝업 **MFA** 정책 정보 아이콘을 선택하고 기록을 엽니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

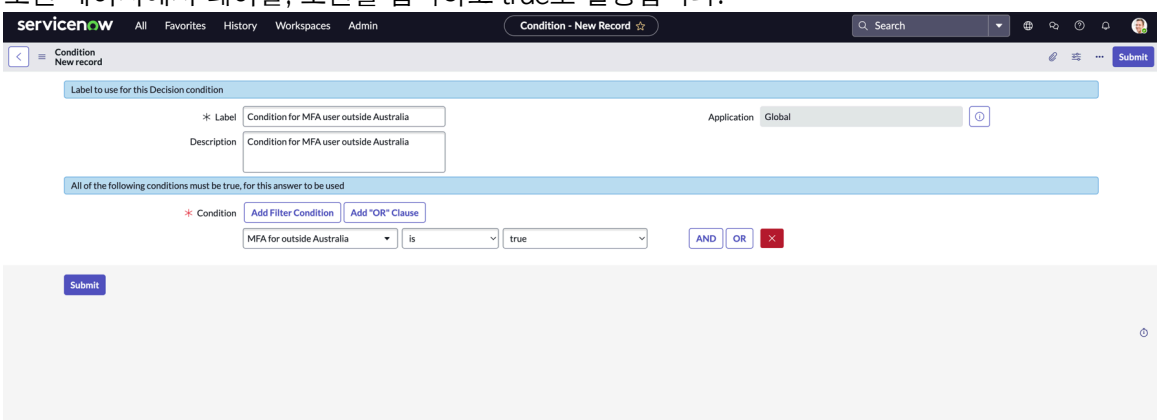


3. Step-Up MFA Policy(스텝업 MFA 정책) 페이지의 Policy Inputs(정책 입력) 탭에서 New(새로 만들기)를 선택합니다.
4. 위치 필터 입력을 추가하고 제출합니다.

   예를 들어, 호주 외부에서 인스턴스에 로그인하는 사용자에 대한 MFA를 표시하려고 합니다.



5. 스텝업 MFA 정책 페이지에서 정책 조건 탭을 선택하고 새로 만들기를 선택합니다.
6. 조건 페이지에서 레이블, 조건을 입력하고 true로 설정합니다.



7. 제출을 선택합니다.
8. 스텝업 MFA 정책 페이지에서 MFA 정책이 비활성화된 경우 활성화합니다.
9. 업데이트를 선택하여 구성을 업데이트합니다.

   구성된 국가(호주) 외부의 사용자가 인스턴스 링크를 선택하고 자격 증명을 지정합니다. 인스턴스에 로그인하기 위한 두 번째 단계 자격 증명을 제공하기 위해 MFA 화면과 함께 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세션 접근에 위치 필터 사용

세션 액세스에서 생성된 위치 필터 기준을 사용하여 사용자의 위치에 따라 역할을 줄입니다.

시작하기 전에

필요한 역할: 관리자

필요한 플러그인: 제로 트러스트 - 위치 기반 액세스 (`com.snc.zero_trust_location_access`).

다음 절차에서는 제거할 국가를 사용하여 위치 필터를 생성하거나 위치에 따라 역할을 사용자로 제한하는 방법에 대해 설명합니다.

프로시저

1. 다음으로 이동 모두 > 제로 트러스트 액세스 > 세션 접근 역할 구성.
2. 세션 액세스 역할 구성을 만들려면 새로 만들기를 선택합니다.
3. 양식에서 필드에 다음을 입력합니다.

세션 접근 역할 구성

필드	설명
이름	구성의 이름
설명	구성에 대한 간단한 설명입니다.
정책	액세스 정책을 선택합니다. 조회 아이콘을 사용하여 정책 목록을 봅니다. 주: 정책 기록을 열어 위치 필터 입력 및 조건을 추가해야 합니다.
동작	역할을 제거하거나역할로 제한합니다. ◦ 역할 제거: 구성된 사용자가 로그인하면 로그인한 세션에 대해 역할 또는 그룹 목록에 제공된 역할 목록이 제거됩니다. ◦ 역할로 제한: 구성된 사용자가 로그인하면 선택한 역할만 사용자에게 제공되고 로그인한 세션에 대한 다른 모든 역할은 제거됩니다.
역할 목록	역할 목록에서 역할을 선택합니다.
그룹 목록	그룹 목록에서 역할을 선택합니다.

4. 선택, 제출.

구성된 국가를 기반으로 하는 사용자의 로그인은 다음과 같습니다.

- 역할을 제거하면 위치 필터에서 구성된 국가의 사용자가 세션에 대해 구성된 역할과 함께 제거됩니다.
- 역할로 제한하는 경우 위치 필터에서 구성된 국가의 사용자는 세션에 대해 구성된 역할만 가집니다.

세션의 역할을 제거하거나 제한하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 자습서: 제로 트러스트 액세스 사용.

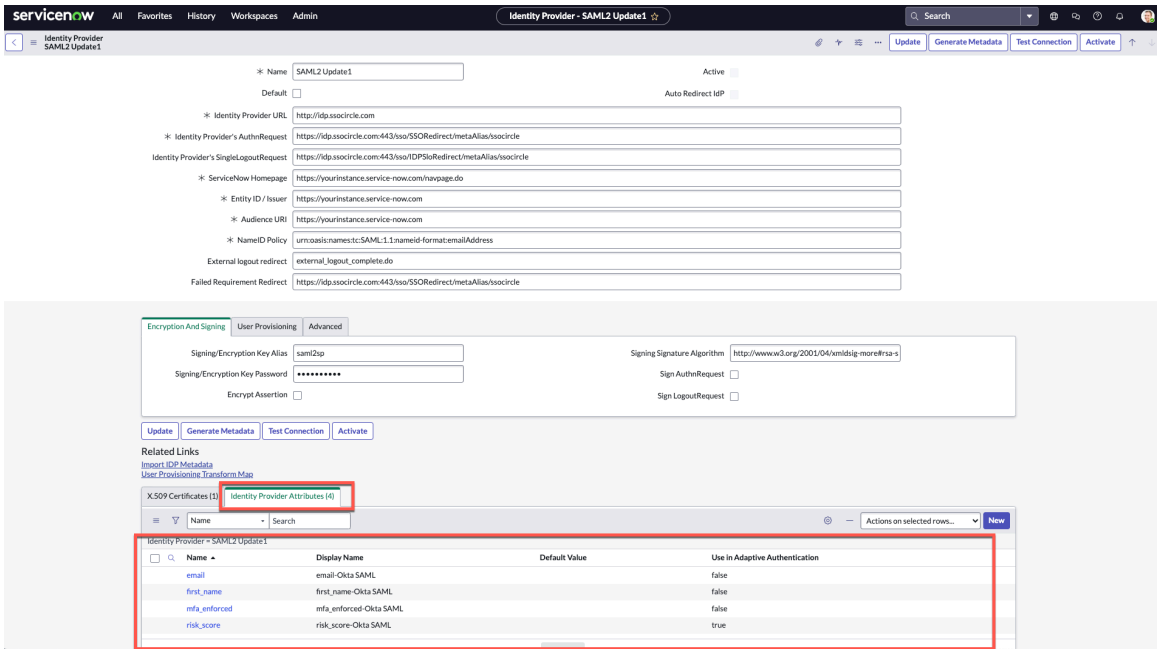
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ID 제공자 속성 필터

IdP(ID 제공자)의 SAML(보안 어설션 마크업 언어) 응답에서 받은 ID 제공자 속성을 인증을 위한 필터 기준으로 사용합니다.

SAML 응답을 통해 IdP에서 모든 속성을 가져오려면 IdP와의 연결 테스트를 수행해야 합니다. 연결 테스트가 성공적으로 완료되면 ID 제공자 구성 페이지의 새 탭에 속성이 추가됩니다.

주: 제로 트러스트 액세스 기능과 함께 ID 제공자 필터를 사용할 수 있습니다. 자세한 내용은 제로 트러스트 액세스 문서를 참조하십시오.



ID 제공자 특성 섹션에서 새로 만들기를 선택하여 특성을 추가하고 `true`로 설정하여 적응형 인증에 해당 특성을 사용할 수도 있습니다.

ID 제공자 속성이 다음과 같은 상세 정보와 함께 표시됩니다.

위치 필터 기준 양식

필드	설명
이름	ID 제공자가 제공하는 속성 이름입니다.
표시 이름	표시 이름은 필터 기준에 사용되는 상세 이름입니다. 주: 읽을 수 있는 이름을 표시 이름으로 제공할 수 있습니다. 경우에 따라 ID 제공자가 제공하는 표시 이름이 길어서 읽을 수 없습니다.
기본값	SAML 응답에 속성이 누락된 경우 필터 기준 평가에 기본값이 사용됩니다.
적응형 인증에서 사용	적응형 인증에서 속성을 사용하는 옵션입니다.

주: Azure IdP에서 채워진 특성은 특성의 이름 길이로 인해 이름 및 표시 이름이 문자로 제한됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ID 제공자 특성 섹션에서 새로 만들기를 선택하여 새 특성을 추가할 수도 있습니다.

적응형 인증에서 사용이 true로 설정된 경우 선택한 속성이 일반 필터 기준의 필터 조건으로 추가됩니다. 예를 들어 `risk_score true`로 설정됩니다. 일반 필터 기준 페이지에 새 필터가 생성됩니다.

ID 제공자 속성을 필터 기준으로 사용

SAML(보안 어설션 마크업 언어) 응답의 ID 제공자(IDP) 속성을 인증 정책의 필터 기준으로 사용합니다.

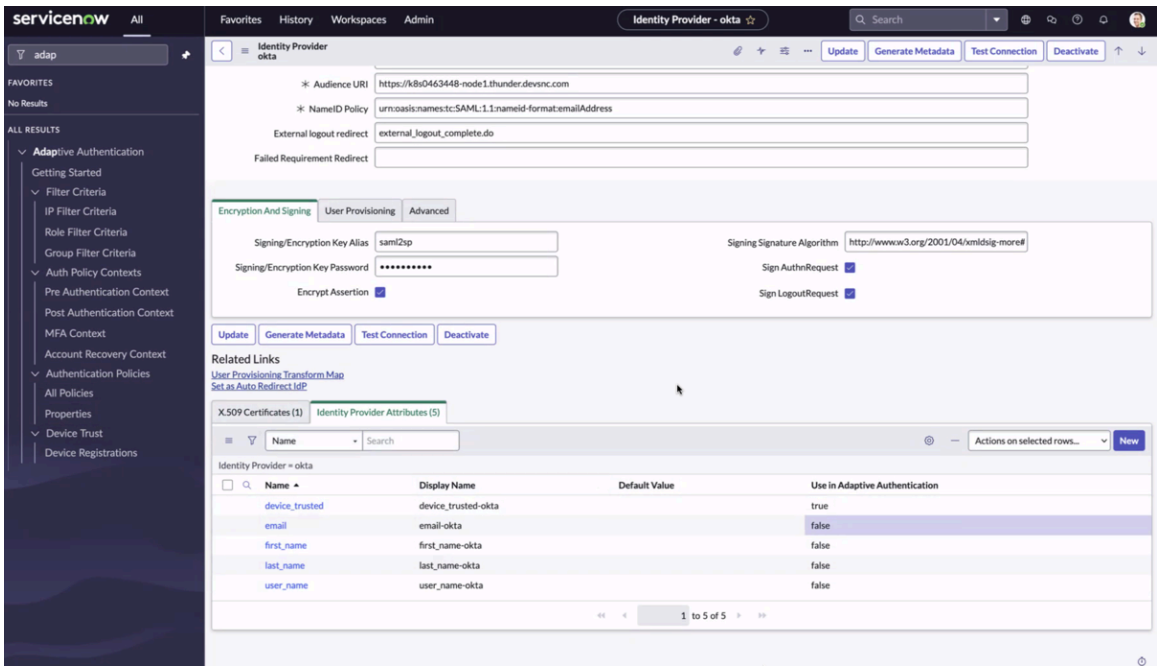
시작하기 전에

필요한 역할: 관리자

정책 입력 및 조건과 함께 정책 컨텍스트(사전 인증, 사후 인증, 다단계 인증) 및 필터 기준(역할, 그룹, IP, 위치)을 사용하여 세션 액세스 정책을 생성할 수 있습니다.

다음 절차에서는 SAML 응답에서 IdP 속성을 정책 입력으로 구성하여 사후 인증 컨텍스트, MFA(다단계 인증) 컨텍스트 및 제로 트러스트 - 정책 기반 세션 액세스에서 인증을 제어하는 단계를 보여줍니다.

Okta IDP 속성은 다음 스크린샷과 같습니다. 사후 인증 컨텍스트, MFA(다단계 인증) 컨텍스트 및 제로 트러스트 - 정책 기반 세션 액세스 정책에서 사용하려면 적응형 인증에서 사용을 예로 설정해야 합니다.



주: 사후 권한 부여, MFA, 제로 트러스트 - 정책 기반 세션 액세스의 정책은 사용자가 자격 증명 또는 SSO 응답을 입력한 후 실행됩니다.

프로시저

1. 사후 인증 정책 컨텍스트에서 IDP 속성을 사용합니다.
   예: 장치를 신뢰할 수 있는 경우 Okta 침입 탐지 및 방지(IDP) 속성에서 로그인을 활성화하도록 구성합니다.

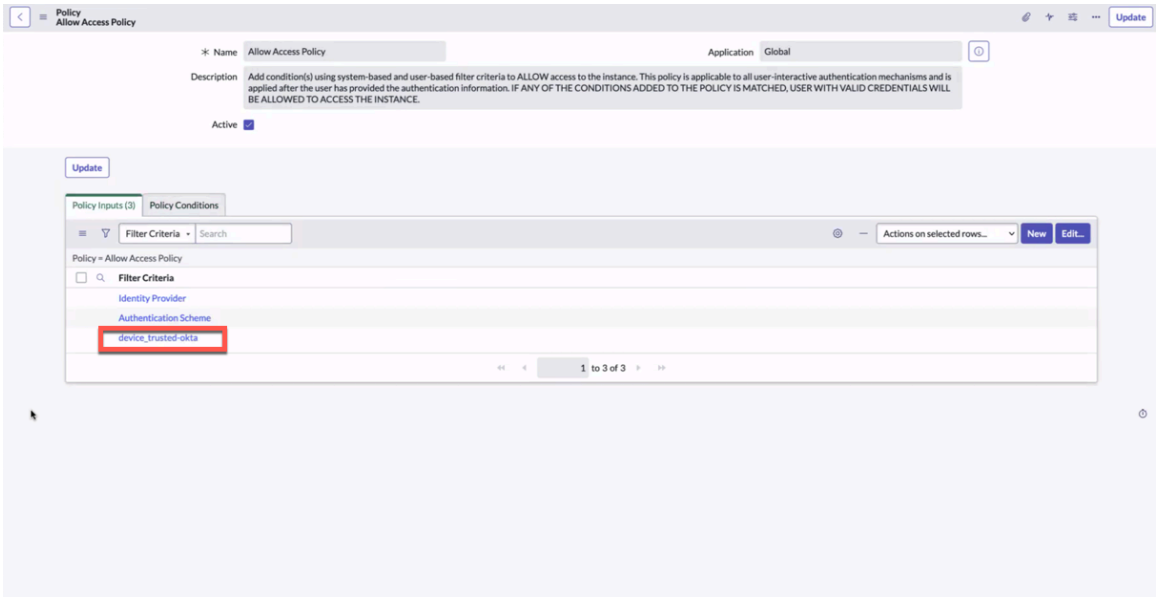
   a. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트 > 사후 인증 정책 컨텍스트입니다..

   b. 정책 허용을 선택하고 정책 기록을 엽니다.

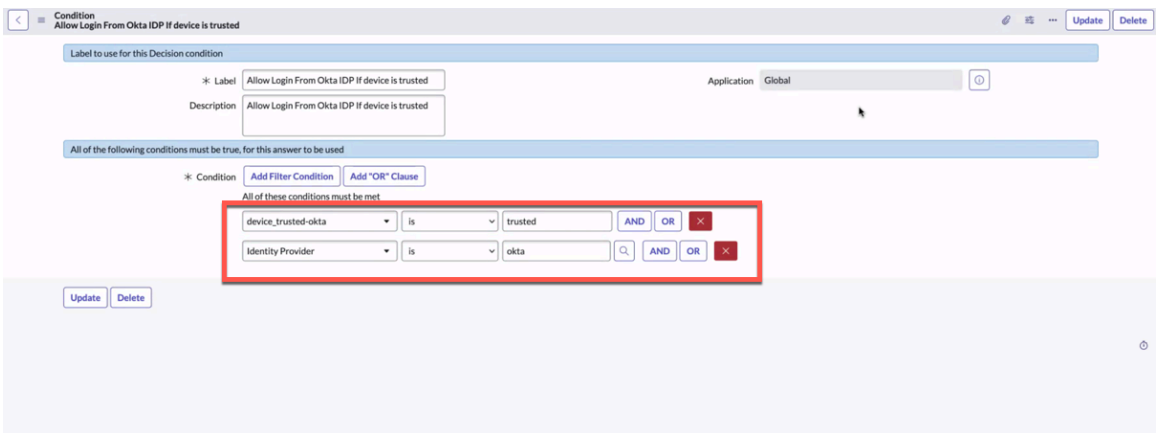
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 정책 입력에서 정책 입력 및 정책 조건을 생성합니다.

- 정책 입력: **device_trusted-okta**를 추가합니다.



- 정책 조건: **device_trusted-okta** 는 `### #` 있고 **ID** 제공자 는 `okta`입니다.



이 구성에 따라 Okta(IdP)에서 장치를 신뢰하면 사용자가 인스턴스에 인증됩니다.

정책 및 조건을 사용하여 사후 인증 컨텍스트를 생성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 사후 인증 컨텍스트.

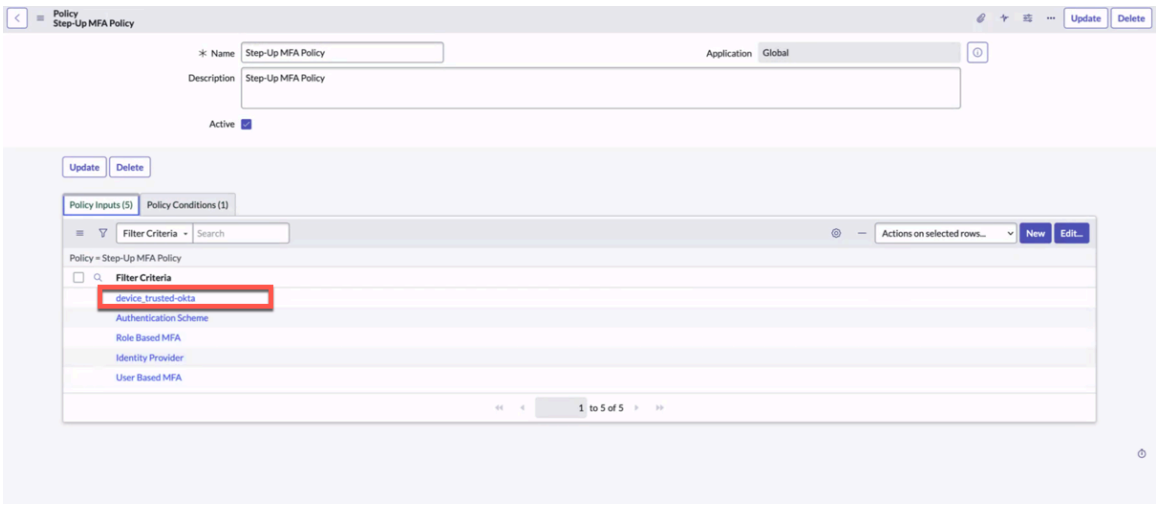
2. MFA 정책 컨텍스트에서 IDP 속성의 사용.
예: 디바이스를 신뢰할 수 없는 경우 Okta 침입 탐지 및 방지(IDP) 속성에서 MFA를 활성화하도록 구성.

a. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트 > **MFA** 인증 정책 컨텍스트..

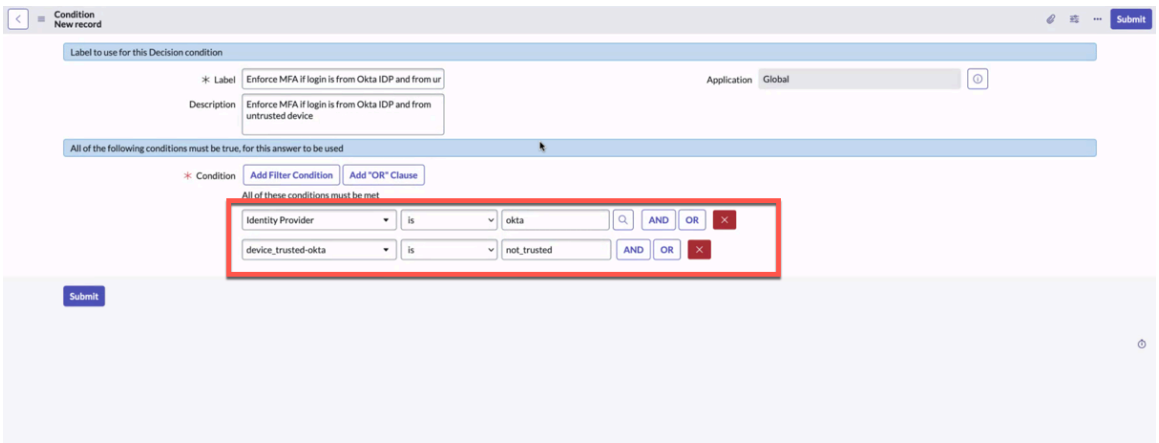
b. 정책 입력에서 정책 입력 및 정책 조건을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정책 입력: **device_trusted-okta**를 추가합니다.



- 정책 조건: **device_trusted-okta** 는 `not_trusted` 이고 **ID** 제공자 는 `okta`입니다.



이 구성에 따라 Okta(IdP)에서 장치를 신뢰하지 않으면 사용자에게 인스턴스에 로그인하기 위한 두 번째 단계 인증이 표시됩니다.

정책 및 조건을 사용하여 MFA 컨텍스트를 생성하는 방법에 대한 자세한 내용은 다음을 참조하십시오 MFA(다단계 인증) 컨텍스트.

3. 제로 트러스트 - 정책 기반 세션 액세스에서 IDP 속성 사용.
예: 디바이스를 신뢰할 수 없는 경우 Okta IDP 속성에서 `Itil` 역할의 권한을 줄이도록 구성합니다.

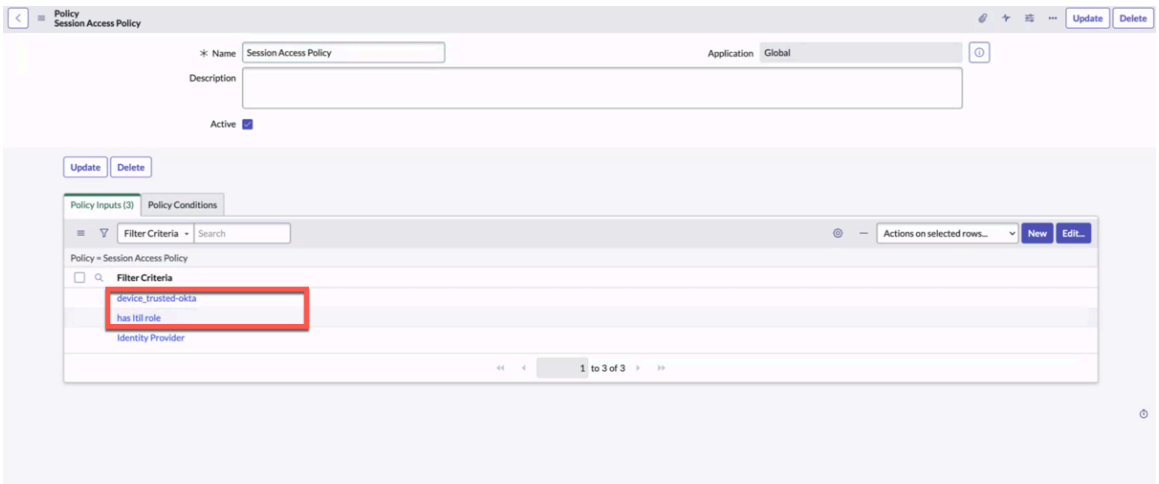
a. 다음으로 이동 모두 > 제로 트러스트 액세스 > 세션 접근 역할 구성.

b. 세션 액세스 역할 구성을 생성합니다.

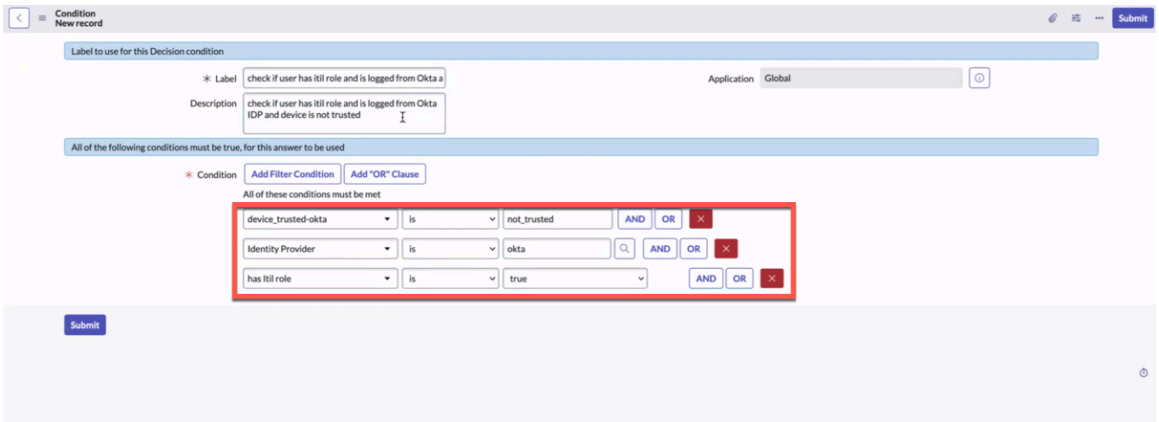
c. 정책 입력에서 정책 입력 및 정책 조건을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정책 입력: **device_trusted-**okta를 추가하고 **itil** 역할을 가집니다.



- 정책 조건: **device_trusted-okta** 는 `not_trusted`이고, **ID** 제공자 는 `okta`이고, **has itil role** 은 ####.



이 구성에 따라 `itil` 사용자가 Okta(IdP)에서 신뢰할 수 없는 디바이스를 사용하는 경우 로그인한 세션에 대한 사용자의 권한이 줄어듭니다.

정책 및 조건을 사용하여 제로 트러스트 - 정책 기반 세션 액세스를 만드는 방법에 대한 자세한 내용은 을 참조하십시오 제로 트러스트 액세스.

인증 정책 컨텍스트

인증 정책 컨텍스트를 사용하여 인스턴스가 인증 정책을 적용하는 방법과 시기를 결정합니다.

인증 컨텍스트는 로그인 프로세스 중에 정책을 적용하는 방법과 시기를 정의합니다. 정책 컨텍스트에 정책을 할당하여 인스턴스가 인증을 처리하는 방법에 대한 입력 및 조건을 정의합니다.

사전 인증 컨텍스트

사전 권한 부여 컨텍스트의 정책은 사용자가 인스턴스에 처음 액세스할 때 로그인 화면이 표시되기 전에 실행됩니다. 사전 권한 부여 컨텍스트를 사용하여 선택한 정책에 따라 사용자에게 로그인 자격 증명을 입력하라는 메시지가 표시되기 전에 액세스를 허용하거나 거부할 수 있습니다. 이러한 정책은 사용자가 정보를 입력하기 전에 평가되기 때문에 사용자의 역할이나 그룹과 같은 기준을 고려할 수 없습니다.

이 컨텍스트에 대한 자세한 내용은 다음 문서를 참조하십시오 사전 인증 컨텍스트.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사후 인증 컨텍스트

사후 권한 부여 컨텍스트의 정책은 사용자가 자격 증명 또는 SSO 응답을 입력한 후에 실행됩니다. 인스턴스는 선택한 정책에 따라 액세스를 허용하거나 거부합니다. 사용자가 로그인 자격 증명을 통해 자신을 식별했기 때문에 정책에서 사용자 정보를 사용하여 액세스 권한을 부여할지 여부를 결정할 수 있습니다.

이 컨텍스트에 대한 자세한 내용은 다음 문서를 참조하십시오 사후 인증 컨텍스트.

MFA(다단계 인증) 컨텍스트

MFA 컨텍스트에 할당된 정책은 로그인 프로세스 중에 MFA를 적용할지 여부를 정의합니다. 인스턴스가 MFA를 적용하는지 여부는 이 컨텍스트의 정책 구성에 따라 결정됩니다. 이 컨텍스트에 대한 자세한 내용은 다음 문서를 참조하십시오 MFA(다단계 인증) 컨텍스트.

계정 복구 컨텍스트

관리자는 SSO 구성 오류 또는 만료된 인증서 해결과 같은 복구 활동을 수행하도록 계정 복구(ACR)를 구성할 수 있습니다. 계정 복구를 사용하려면 하나 이상의 관리자 계정을 계정 복구 사용자로 등록해야 합니다. 하나 이상의 계정이 구성될 때까지 인스턴스에서 Single Sign-On을 활성화할 수 없습니다. 설정할 수 있는 컨텍스트에 대한 자세한 내용은 다음 문서를 참조하십시오 계정 복구 컨텍스트.

세션 확인 컨텍스트

세션 확인 컨텍스트는 적응형 인증 정책 프레임워크와 함께 사용할 수 있습니다. 프레임워크는 인증 정책을 사용하여 인증 요청(세션)을 평가한 다음 정책 조건에 따라 액세스를 거부하거나 허용합니다. 자세한 내용은 세션 확인 컨텍스트 문서를 참조하십시오.

기본 정책

정책 컨텍스트 내에서 기본 정책 필드에서 기본 정책을 정의할 수 있습니다. 이 기본값은 인스턴스가 정책 결과에 응답하는 방식을 정의합니다. 사용 가능한 기본 정책 옵션은 사용 중인 컨텍스트에 따라 결정됩니다. 이러한 옵션에 대한 자세한 내용은 이러한 개별 컨텍스트를 설명하는 문서에서 찾을 수 있습니다.

사전 인증 컨텍스트

사전 인증 정책 컨텍스트는 로그인 프로세스 중에 정책을 적용하는 방법과 시기를 정의합니다. 이 컨텍스트에서 사용되는 정책은 사용자에게 로그인 화면이 표시되기 전에 실행됩니다.

사전 인증 컨텍스트 기록

사전 인증 컨텍스트의 정책은 사용자가 인스턴스에 처음 액세스할 때 실행 후 로그인 화면이 표시됩니다.

선택한 정책에 따라 사용자에게 로그인 자격 증명을 입력하라는 메시지가 표시되기 전에 사전 인증 컨텍스트를 사용하여 액세스를 허용하거나 거부할 수 있습니다. 이러한 정책은 사용자가 정보를 입력하기 전에 평가되기 때문에 사용자의 역할이나 그룹과 같은 기준을 고려할 수 없습니다.

사전 인증 정책 컨텍스트 기록의 필드를 사용하여 인스턴스에서 정책을 사용하는 방식을 정의합니다.

사전 인증 컨텍스트 양식

필드	설명
이름	정책 컨텍스트의 이름입니다. 이 필드는 정적이며 변경할 수 없습니다.
설명	컨텍스트 설명

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사전 인증 컨텍스트 양식

필드	설명
기본 정책	정책을 평가할 때 이 컨텍스트의 기본 동작을 정의합니다. 다음 옵션 중에서 선택합니다. 정책 허용 는 기본적으로 모든 사용자에 대한 접근을 거부하며, 정책 허용 필드에서 선택한 정책의 조건이 예로 평가되는 경우에만 접근을 허용합니다. 거부 정책 기본적으로 모든 사용자에 대한 액세스를 허용하고 거부 정책 필드에서 선택한 정책의 조건이 예로 평가되는 경우에만 액세스를 거부합니다.
정책 허용	이 컨텍스트에 사용되는 정책은 다음을 사용합니다. 이 필드는 기본 정책 필드가 정책 허용으로 설정된 경우에만 나타납니다.
거부 정책	이 컨텍스트에 사용되는 정책은 다음을 사용합니다. 이 필드는 기본 정책 필드가 거부 정책으로 설정된 경우에만 나타납니다.

주:

사전 인증 정책 컨텍스트에서만 IP 필터, 신뢰할 수 있는 모바일 앱 필터 및 위치 필터 기준을 사용할 수 있습니다.

정책 입력 및 조건

정책 입력 및 정책 조건 탭에는 허용 정책 또는 거부 정책 필드에서 선택한 정책의 입력과 조건이 표시됩니다. 이러한 탭은 참조 역할을 하지만 정책 입력 또는 조건을 변경하는 데 사용할 수 없습니다.

정책을 수정하려면 허용 정책 또는 거부 정책 필드 옆에 있는 참조 아이콘( )을 사용하여 정책으로 이동합니다.

이 예에서는 기본적으로 액세스를 거부하도록 구성된 사전 인증 정책 컨텍스트 기록을 보여줍니다. 컨텍스트에서는 액세스 거부 정책이라는 정책을 사용합니다. 해당 정책에는 정책 입력 및 정책 조건 탭에 표시되는 입력 및 조건 세트가 있습니다.

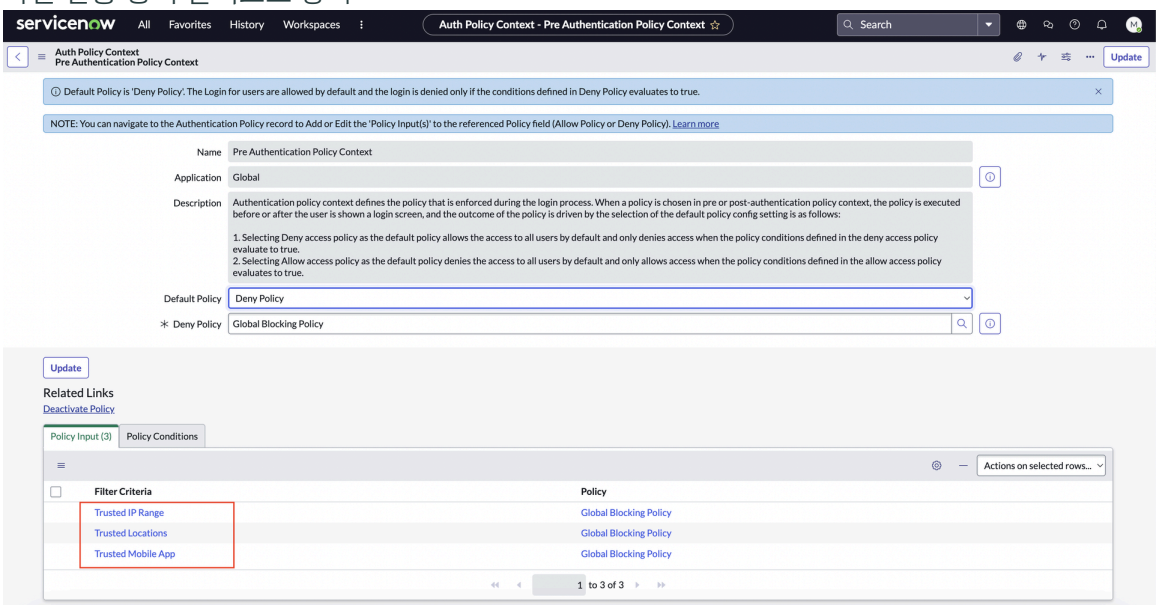
주:

- 사전 인증 정책 컨텍스트에서는 IP 기반 필터, 위치 기반 필터 또는 신뢰할 수 있는 모바일 앱 필터만 사용할 수 있습니다.
- 절대적이지 않은 조건 또는 필터 기준으로 사전 인증 세트가 있을 때마다 정책 또는 컨텍스트를 구성할 수 없다는 오류 메시지가 표시됩니다. 사전 인증 컨텍스트를 인스턴스에 실행하기 전에 사전 인증 컨텍스트에 대한 모든 입력의 유효성을 검사하는 것이 좋습니다.

  예를 들어 관리자가 신뢰할 수 있는 네트워크 외부에 있고 IP 범위로 사전 인증 컨텍스트를 구성하는 경우 IP 범위가 관리자의 현재 세션과 일치하지 않으면 관리자가 차단됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사전 인증 정책 컨텍스트 양식



사후 인증 컨텍스트

사후 인증 정책 컨텍스트는 로그인 프로세스 중에 정책이 적용되는 방법과 시기를 정의합니다. 이 컨텍스트에서 사용되는 정책은 사용자에게 로그인 화면이 표시된 후에 실행됩니다.

사후 인증 컨텍스트 기록

사후 권한 부여 컨텍스트의 정책은 사용자가 자격 증명 또는 SSO 응답을 입력한 후에 실행됩니다. 인스턴스는 선택한 정책에 따라 액세스를 허용하거나 거부합니다. 사용자가 로그인 자격 증명을 통해 자신을 식별했기 때문에 정책에서 역할 또는 그룹과 같은 사용자 정보를 사용하여 액세스 권한을 부여할지 여부를 결정할 수 있습니다.

사후 인증 정책 컨텍스트 기록의 필드를 사용하여 인스턴스에서 정책을 사용하는 방식을 정의합니다.

사후 인증 컨텍스트 양식

필드	설명
이름	정책 컨텍스트의 이름입니다. 이 필드는 정적이며 변경할 수 없습니다.
설명	컨텍스트 설명
기본 정책	정책을 평가할 때 이 컨텍스트의 기본 동작을 정의합니다. 다음 옵션 중에서 선택합니다. 정책 허용 는 기본적으로 모든 사용자에 대한 접근을 거부하며, 정책 허용 필드에서 선택한 정책의 조건이 예로 평가되는 경우에만 접근을 허용합니다. 거부 정책 기본적으로 모든 사용자에 대한 액세스를 허용하고 거부 정책 필드에서 선택한 정책의 조건이 예로 평가되는 경우에만 액세스를 거부합니다.
정책 허용	이 컨텍스트에 사용되는 정책은 다음을 사용합니다. 이 필드는 기본 정책 필드가 정책 허용으로 설정된 경우에만 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사후 인증 컨텍스트 양식

필드	설명
거부 정책	이 컨텍스트에 사용되는 정책은 다음을 사용합니다. 이 필드는 기본 정책 필드가 거부 정책으로 설정된 경우에만 나타납니다.

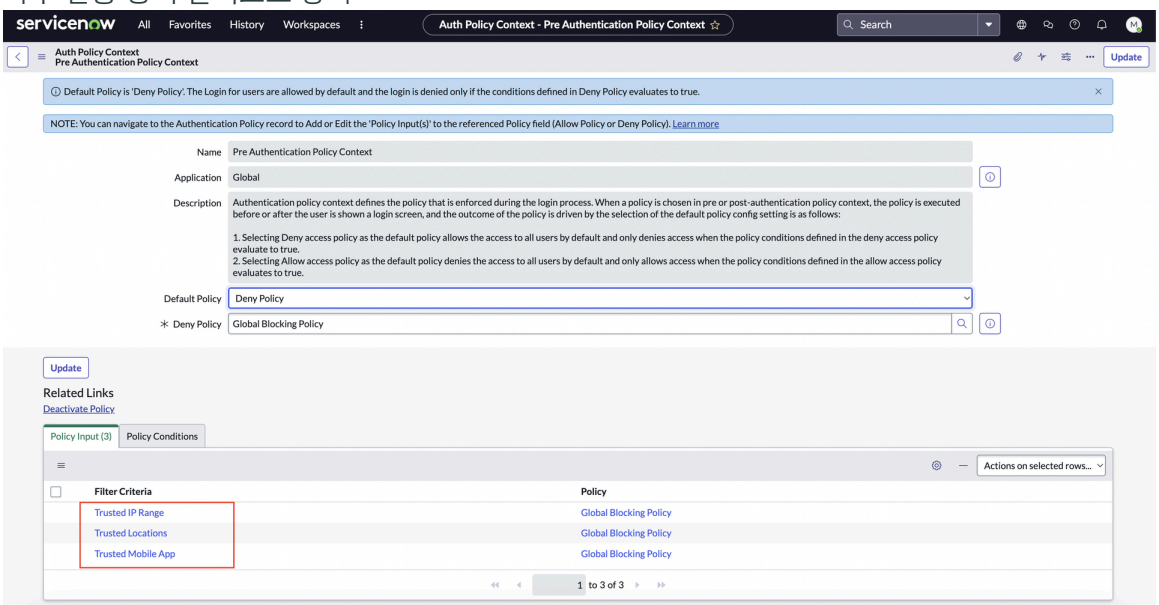
정책 입력 및 조건

정책 입력 및 정책 조건 탭에는 허용 정책 또는 거부 정책 필드에서 선택한 정책의 입력과 조건이 표시됩니다. 이러한 탭은 참조 역할을 하지만 정책 입력이나 조건을 변경하는 데 사용할 수 없습니다.

정책 설정을 수정하려면 허용 정책 또는 거부 정책 필드 옆에 있는 참조 아이콘(ⓘ)을 사용하여 정책으로 이동합니다.

이 예에서는 기본적으로 액세스를 거부하도록 구성된 사후 인증 정책 컨텍스트 레코드를 보여줍니다. 컨텍스트에서는 액세스 거부 정책이라는 정책을 사용합니다. 해당 정책에는 정책 입력 및 정책 조건 탭에 표시되는 입력 및 조건 세트가 있습니다.

사후 인증 정책 컨텍스트 양식



MFA(다단계 인증) 컨텍스트

MFA(다단계 인증) 정책 컨텍스트는 정책을 사용하여 로그인 프로세스 중에 MFA가 적용되는 방법과 시기를 정의합니다.

MFA 컨텍스트 기록

MFA(다단계 인증) 정책 컨텍스트는 사용자가 로그인할 때 두 번째 인증 형식을 제공해야 하는지 여부를 정의합니다. 이 컨텍스트는 사후 인증 및 사전 인증 정책으로 인스턴스에 대한 접근을 거부하지 않습니다. 이 컨텍스트에서 선택하는 정책은 다단계 인증에 대한 사용자 또는 역할 기반 구성보다 우선합니다.

MFA 컨텍스트에 액세스하려면 다음으로 이동합니다. 모두 > 다단계 인증 > **MFA** 컨텍스트.

사후 인증 정책 컨텍스트 기록의 필드를 사용하여 인스턴스에서 정책을 사용하는 방식을 정의합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 기본 정책이 스텝업 **MFA** 정책인 경우 스텝업 **MFA** 정책에 구성된 정책이 예로 평가되면 사용자가 다단계 인증으로 표시됩니다. 정책은 사용자 또는 역할 기반 구성보다 우선합니다.
- SSO 로그인을 통한 MFA는 `glide.authenticate.mfa.with.multisso.enabled` 속성이 예로 설정된 경우에만 사용할 수 있습니다.
- 인증 정책 기록으로 이동하여 참조된 정책 필드(스텝 업 **MFA** 정책 또는 스텝 다운 **MFA** 정책)에 "정책 입력"을 추가하거나 편집할 수 있습니다.
- MFA 컨텍스트 정책은 사용자 로그인에만 적용됩니다. API 인증, 기본 인증 및 OAuth 자원 소유자 암호 자격 증명 부여에는 적용되지 않습니다.

MFA 컨텍스트 양식

필드	설명
이름	정책 컨텍스트의 이름입니다. 이 필드는 정적이며 변경할 수 없습니다.
설명	컨텍스트 설명
기본 정책	정책을 평가할 때 이 컨텍스트의 기본 동작을 정의합니다. 다음 옵션 중에서 선택합니다. 스텝업 MFA 정책 스텝업 **MFA** 정책 필드에 정의된 정책 조건이 예로 평가되면 사용자에게 MFA를 적용합니다. 스텝다운 MFA 정책 기본적으로 MFA를 적용합니다. MFA는 스텝다운 **MFA** 정책 필드에 정의된 정책 조건이 true로 평가되는 경우에만 적용되지 않습니다.
스텝업 MFA 정책	이 컨텍스트에 사용되는 정책은 다음을 사용합니다. 이 필드는 기본 정책 필드가 스텝업 **MFA** 정책으로 설정된 경우에만 나타납니다.
스텝다운 MFA 정책	이 컨텍스트에 사용되는 정책은 다음을 사용합니다. 이 필드는 기본 정책 필드가 스텝다운 **MFA** 정책으로 설정된 경우에만 나타납니다.

정책 입력 및 조건

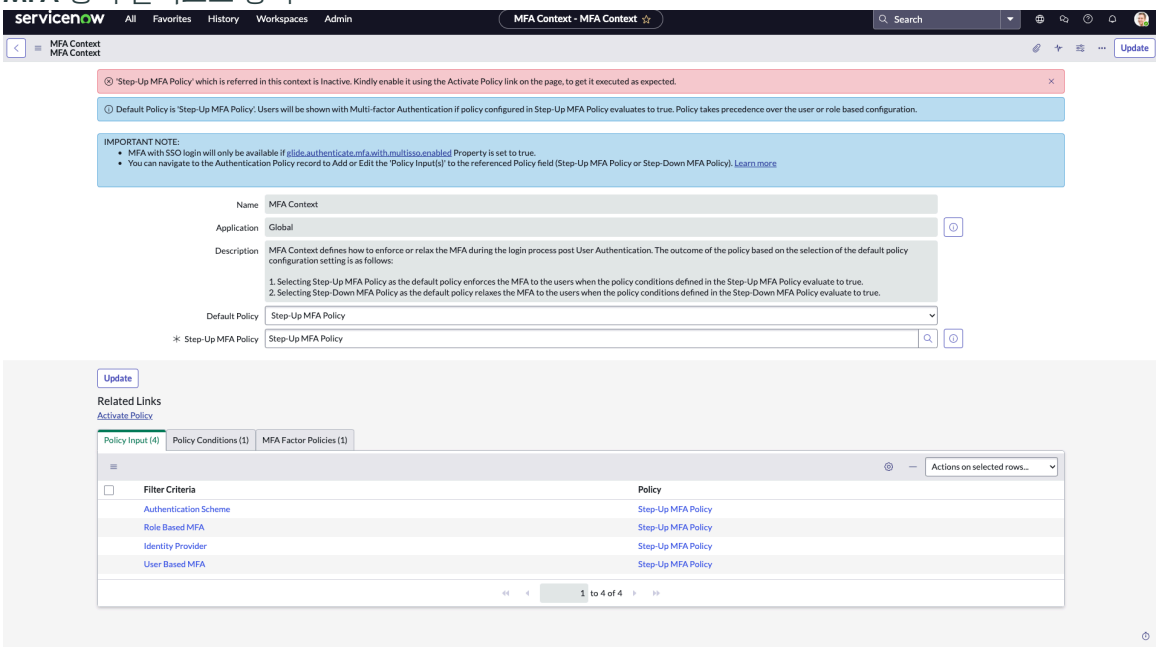
정책 입력 및 정책 조건 탭에는 스텝업 **MFA** 정책 또는 스텝다운 **MFA** 정책 필드에서 선택한 정책의 입력과 조건이 표시됩니다. 이러한 탭은 참조 역할을 하지만 정책 입력이나 조건을 변경하는 데 사용할 수 없습니다. 정책 설정을 수정하려면 스텝업 **MFA** 정책 또는 스텝다운 **MFA** 정책 필드 옆에 있는 참조 아이콘( )을 사용하여 정책으로 이동합니다.

주: 여기에서 정책 조건을 만들 수 있지만 정책 페이지에서 새 정책 조건을 추가하는 것이 좋습니다.

이 예는 스텝업 MFA 정책을 사용하여 구성된 MFA 컨텍스트 기록을 보여줍니다. 이 기본 정책은 정책에 정의된 조건이 true로 평가되는 경우에만 MFA가 적용됨을 의미합니다. 컨텍스트는 스텝업 **MFA** 정책이라는 정책을 사용합니다. 해당 정책에는 정책 입력 및 정책 조건 탭에 표시되는 입력 및 조건 세트가 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MFA 정책 컨텍스트 양식



계정 복구 컨텍스트

계정 복구 컨텍스트는 정책을 사용하여 계정 복구를 설정할 수 있는 방법과 시기를 정의합니다.

관리자는 다음으로 이동하여 이 컨텍스트와 관련 정책을 보고 수정할 수 있습니다. 복수 제공자 **SSO** > 계정 복구 > 계정 복구 컨텍스트.

주: 기본적으로 정책은 허용 정책입니다. 사용자에 대한 로그인은 기본적으로 제한되며 허용 정책에 정의된 조건이 true로 평가되는 경우에만 로그인이 허용됩니다.

계정 복구 컨텍스트 기록의 필드를 사용하여 인스턴스에서 정책을 사용하는 방법을 정의합니다.

계정 복구 컨텍스트 양식

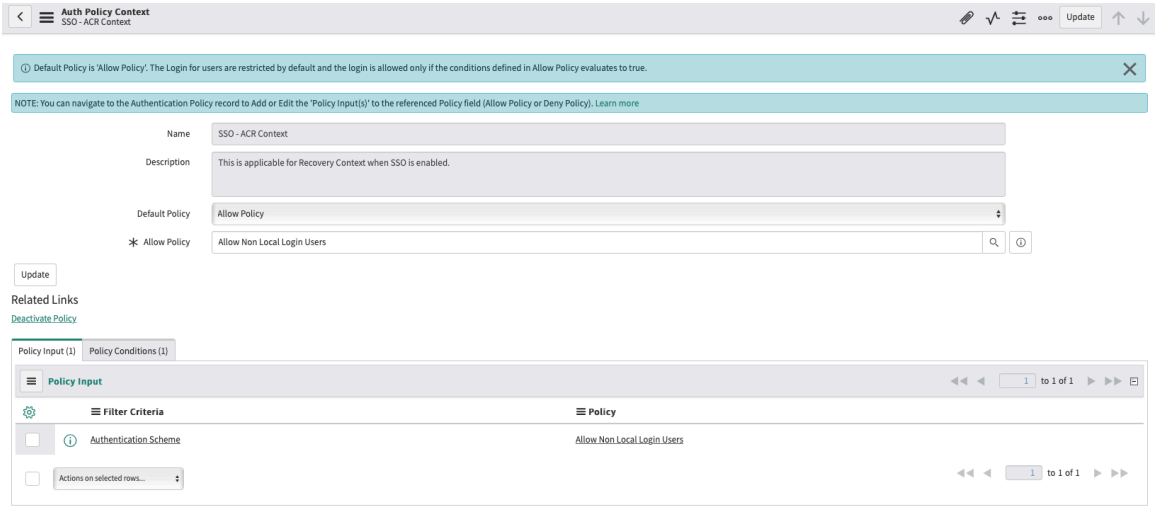
필드	설명
이름	정책 컨텍스트의 이름입니다. 이 필드는 정적이며 변경할 수 없습니다.
설명	컨텍스트 설명
기본 정책	정책을 평가할 때 이 컨텍스트의 기본 동작을 정의합니다. 다음 옵션 중에서 선택합니다. • 정책 허용 • 거부 정책
정책 허용	이 필드는 기본 정책 필드가 정책 허용으로 설정된 경우에만 나타납니다.
거부 정책	이 필드는 기본 정책 필드가 거부 정책으로 설정된 경우에만 나타납니다.

정책 입력 및 조건

정책 입력 및 정책 조건 탭에는 허용 정책 또는 거부 정책 필드에서 선택한 정책의 입력과 조건이 표시됩니다. 이러한 탭은 참조 역할을 하지만 정책 입력이나 조건을 변경하는 데 사용할 수 없습니다. 정책 설정을 수정하려면 허용 정책 또는 거부 정책 필드 옆에 있는 이 기록 미리 보기 아이콘을 사용하여 정책으로 이동합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 여기에서 정책 조건을 만들 수 있지만 정책 페이지에서 새 정책 조건을 추가하는 것이 좋습니다.



세션 확인 컨텍스트

세션 확인 컨텍스트를 세션 또는 쿠키 하이재킹에 대한 추가 보호 계층으로 사용합니다.

정책 프레임워크와 함께 세션 확인 컨텍스트를 사용할 수 있습니다 적응형 인증 . 프레임워크는 인증 정책을 사용하여 인증 요청을 평가한 다음 정책 입력 및 조건에 따라 액세스를 거부하거나 허용합니다.

세션 유효성 검사 컨텍스트 정책은 관리자가 로그인한 세션 동안 특정 또는 모든 사용자에게 IP 제한을 적용할 수 있는 사후 인증 정책과 함께 사용할 수 있습니다.

세션 확인 컨텍스트 기능은 사용자가 설정한 조건에 따라 IP 주소를 평가하고 세션 내에서 인스턴스에 대한 액세스를 허용합니다. 세션 확인 컨텍스트 결과는 다음과 같습니다.

- 거부 정책: 액세스 거부 정책을 기본 정책으로 선택하면 사용자가 기본적으로 세션을 계속할 수 있습니다. 액세스 거부 정책에 정의된 정책 조건 중 하나가 true로 평가되는 경우에만 세션이 종료됩니다.
- 정책 허용: 액세스 허용 정책을 기본 정책으로 선택하면 액세스 허용 정책에 정의된 정책 조건 중 하나가 true로 평가되지 않는 한 사용자 세션이 즉시 종료됩니다.

주:

- 인증 정책의 세션 유효성 확인 컨텍스트는 기본적으로 허용 정책 으로 설정됩니다.
- 세션 확인 컨텍스트는 허용 정책을 통해 구현됩니다. 컨텍스트를 거부 정책으로 설정하는 것은 권장되지 않습니다.

세션 확인 컨텍스트는 다음 메커니즘을 기반으로 작동합니다.

- 사용자 요청에서 세션 생성 시 사용자의 IP 주소를 캡처하여 세션 및 데이터베이스에 저장합니다.
- IP 주소가 세션 내 또는 고객이 정의한 올바른 IP 범위 외부에서 다를 경우 요청을 거부합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 세션 확인 컨텍스트는 다음과 같습니다.

- 인증된 사용자만 사용할 수 있습니다.
- 게스트 사용자 세션 또는 네이티브 모바일 앱에는 적용되지 않습니다.
- 선택 사항이며 구성할 수 있다는 요구 사항을 따릅니다.
- 사후 로그인 요청에 대해서만 실행됩니다.

세션 확인의 이점

세션 확인 컨텍스트에는 다음과 같은 이점이 있습니다.

- 하이재커가 세션을 가장하기 위해 사용자의 세션 쿠키를 한 장치에서 다른 장치로 복사하는 경우 액세스를 ServiceNow® 제한합니다.
- 안전하지 않은 네트워크를 사용하는 경우 사용자의 세션 액세스를 제한합니다.
- 사용자 로그인에 대한 사용자 그룹 또는 역할별로 다양한 규칙과 IP 범위를 구성합니다.

세션 확인 컨텍스트 기록

세션 확인 컨텍스트의 정책은 사후 로그인 요청을 실행합니다.

세션 확인 정책 컨텍스트 기록의 필드를 사용하여 인스턴스에서 정책을 사용하는 방식을 정의합니다.

세션 확인 컨텍스트 양식

필드	설명
이름	정책 컨텍스트의 이름입니다. 이 필드는 정적이며 변경할 수 없습니다.
설명	컨텍스트에 대한 설명입니다.
기본 정책	정책을 평가할 때 이 컨텍스트의 기본 동작을 정의합니다. 다음 옵션 중에서 선택합니다. 정책 허용 는 기본적으로 모든 사용자에 대한 접근을 거부하며 허용 정책 필드의 조건이 예로 평가될 때만 접근을 허용합니다. 거부 정책 기본적으로 모든 사용자에 대한 액세스를 허용하고 거부 정책 필드의 조건이 예로 평가되는 경우에만 액세스를 거부합니다.
정책 허용	이 컨텍스트에 사용되는 정책입니다. 이 필드는 기본 정책 필드가 정책 허용으로 설정된 경우에만 나타납니다.
거부 정책	이 컨텍스트에 사용되는 정책입니다. 이 필드는 기본 정책 필드가 거부 정책으로 설정된 경우에만 나타납니다.

정책 입력 및 정책 조건에 따라 세션 확인 정책을 허용 정책 또는 거부 정책으로 선택할 수 있습니다.

주:

세션 확인 정책에는 IP, 역할 및 그룹 필터 기준만 사용할 수 있습니다.

정책 입력 및 조건

정책 입력 및 정책 조건 탭에는 허용 정책 또는 거부 정책 필드에서 선택한 정책의 입력과 조건이 표시됩니다. 이 탭은 참조 역할을 합니다. 그러나 정책 입력이나 조건을 변경하는 데 사용할 수는

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

없습니다. 정책을 수정하려면 허용 정책 또는 거부 정책 필드 옆에 있는 참조 아이콘( )을 사용하여 정책으로 이동합니다.

세션 확인 컨텍스트 활성화

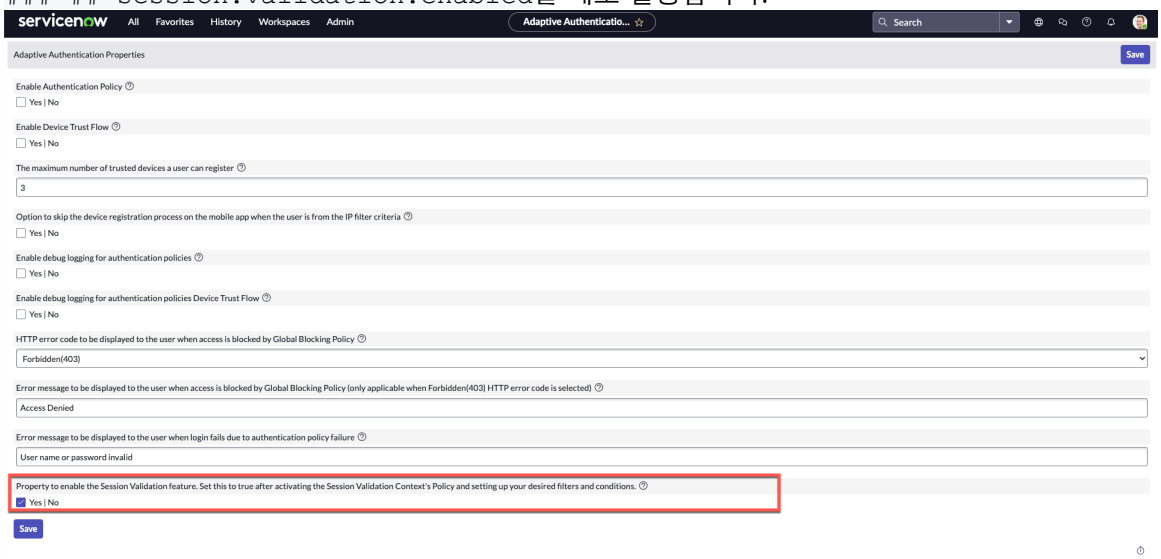
세션 유효성 검사 컨텍스트를 사용하여 하이재커가 사용자의 세션 쿠키를 한 장치에서 다른 장치로 복사하여 세션을 가장하거나 안전하지 않은 네트워크를 사용하는 경우 사용자의 세션 액세스를 제한하는 경우 액세스를 ServiceNow® 제한합니다.

시작하기 전에
필요한 역할: 관리자

세션 유효성 검사를 사용하려면 다음 단계를 수행해야 합니다.

프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 모든 정책.
2. 정책(`sys_authentication_policy_list.do`) 페이지에서 세션 확인 정책을 선택합니다.
3. 정책 입력 및 정책 조건을 지정합니다.
4. 추가한 필터에 대한 조건을 **true** 또는 **false** 로 설정합니다.
5. 정책 입력 및 조건으로 세션 확인 정책을 설정한 후 정책을 활성화하려면 활성 확인란을 선택합니다.
6. 인스턴스에 SSO가 구성되어 있는 경우 sso_properties 테이블에서 기본 신원 확인 제공자에 대해 **Force AuthnRequest** 확인란을 선택합니다.
7. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 속성.
8. `### ## session.validation.enabled`를 예로 설정합니다.



결과
세션 확인 기능이 활성화됩니다. 기능을 사용하도록 정책에 대한 정책 입력 및 조건을 구성할 수 있습니다. 자세한 내용은 자습서: 세션 검증 구성 문서를 참조하십시오.

자습서: 세션 검증 구성

적응형 인증 프레임워크 내에서 세션 확인을 구성하여 세션 또는 쿠키 하이재킹에 대한 추가 보호 계층을 제공합니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필요한 플러그인: 적응형 인증 (com.snc.adaptive_authentication)

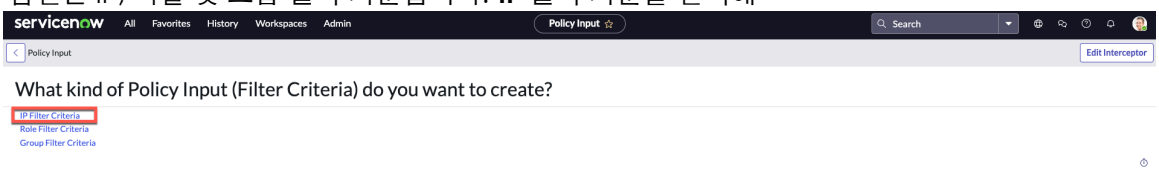
세션 확인을 구성하려면 다음 단계를 수행해야 합니다.

프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 모든 정책.
2. 정책(`sys_authentication_policy_list.do`) 페이지에서 세션 확인 정책을 선택합니다.
3. 정책 입력을 선택합니다.

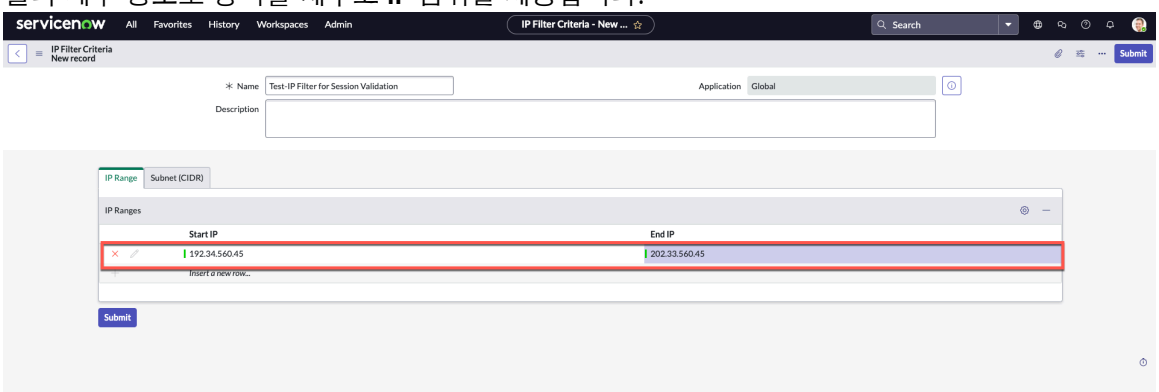
   a. 새로 만들기 또는 편집을 선택합니다.

   b. 생성하려는 정책 입력(필터 기준)의 종류를 선택합니다.
   사용 가능한 옵션은 IP, 역할 및 그룹 필터 기준입니다. **IP** 필터 기준을 선택해



   보겠습니다.

   c. 필터 세부 정보로 양식을 채우고 **IP** 범위를 제공합니다.



   IP 필터를 만드는 방법에 대한 자세한 내용은 문서를 참조하십시오 IP 필터 기준 생성.

   d. 제출을 선택합니다.

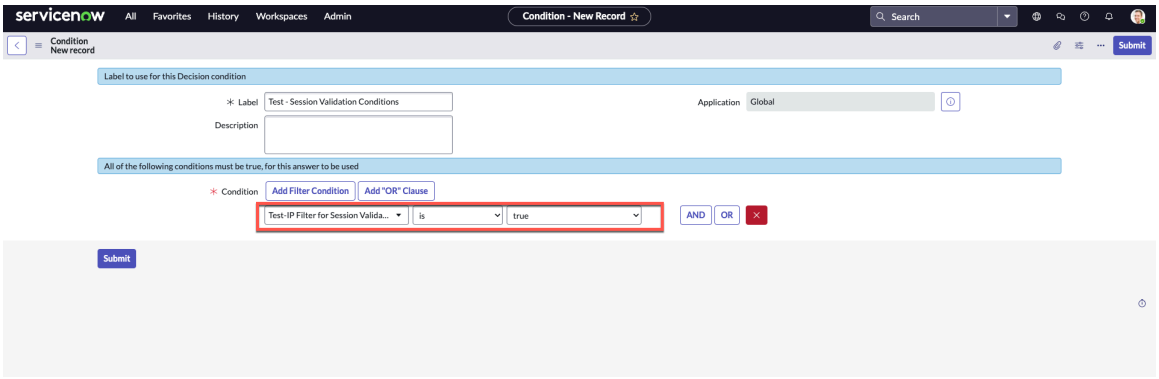
4. 세션 확인 정책 페이지에서 정책 조건을 선택합니다.

   a. 새로 만들기를 선택합니다.

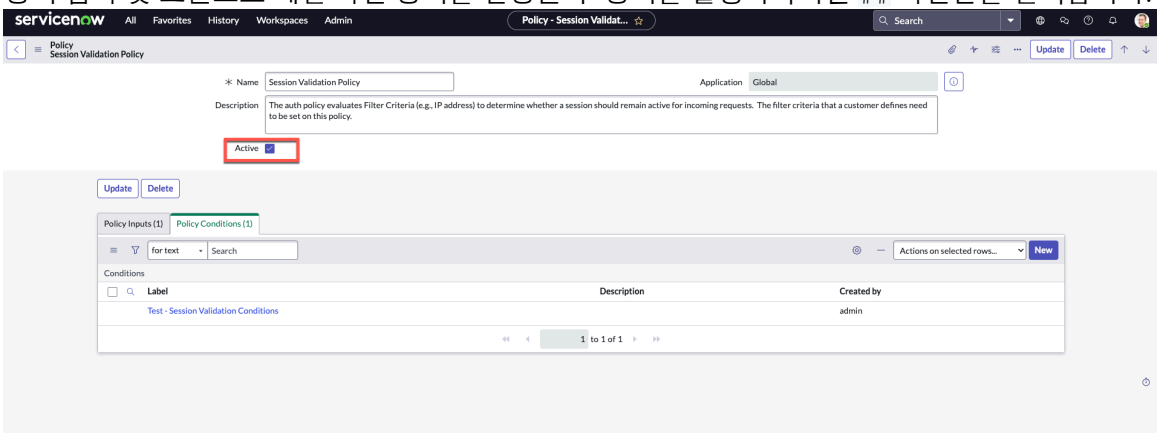
   b. 양식을 작성하고 정책 입력에 대한 조건을 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

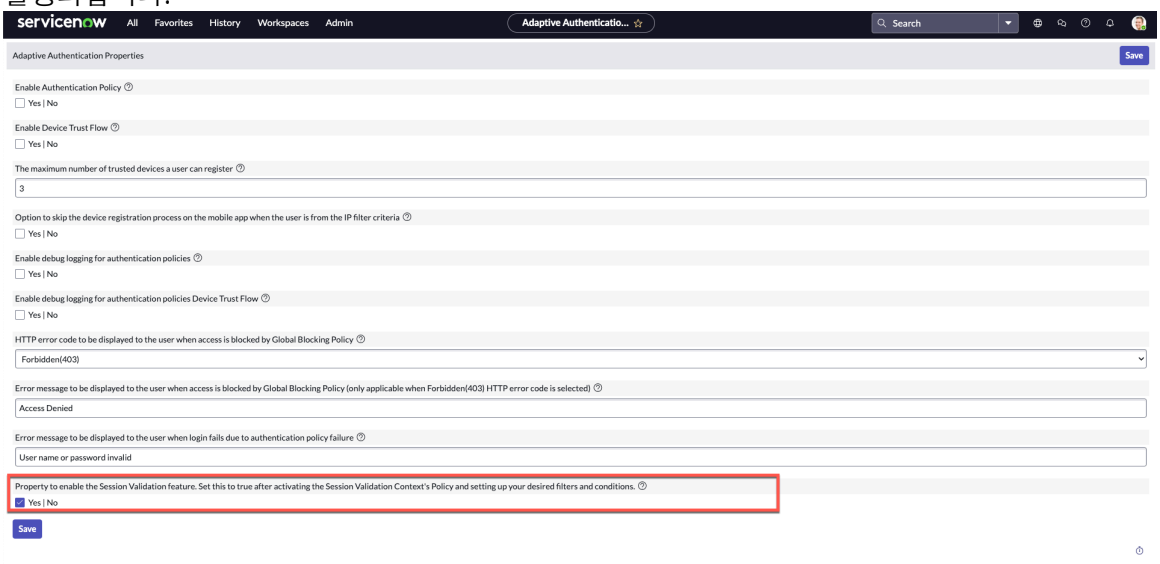
주: 정책 입력의 구성에 따라 조건을 `true` 또는 `false` 로 설정할 수 있습니다. 이 예시에서는 `true`로 설정되어 있습니다. 이 경우 조건을 true로 설정하면 구성된 IP 주소를 가진 사용자만 로그인할 수 있습니다.



5. 정책 입력 및 조건으로 세션 확인 정책을 설정한 후 정책을 활성화하려면 ## 확인란을 선택합니다.



6. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 속성 을 클릭하고 세션 유효성 검사 속성을 활성화합니다.

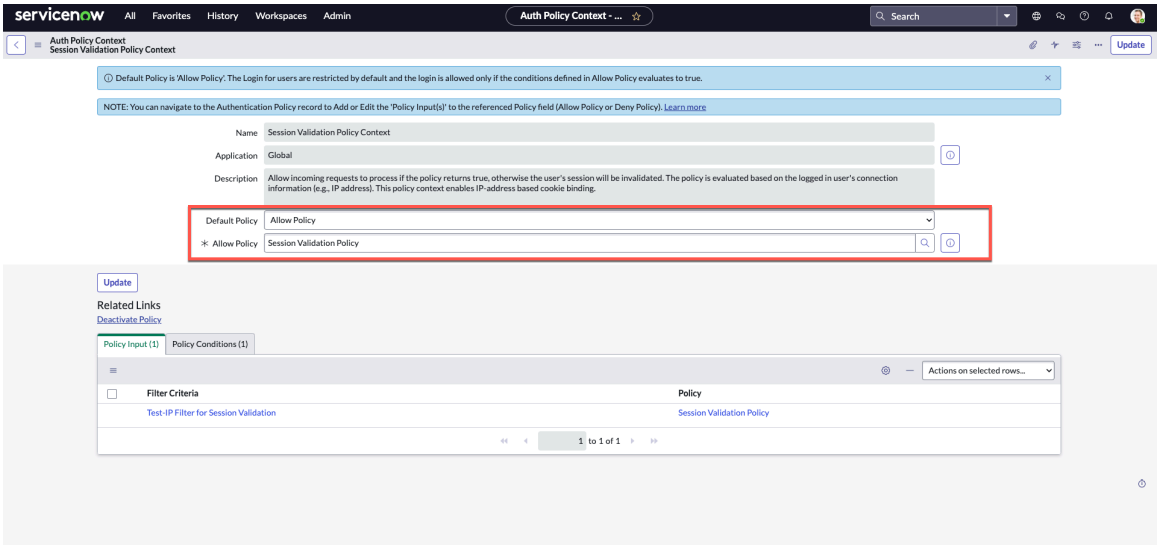


7. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트 > 세션 확인 컨텍스트.
8. 기본 정책을 허용 정책 또는 거부 정책 으로 설정하여 정책 입력 및 정책 조건에 따라 세션 확인 컨텍스트를 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 기본적으로 다음과 같이 수행됩니다.

- 세션 유효성 확인 컨텍스트가 정책 허용으로 설정됩니다.
- 정책 허용이 세션 확인 정책으로 선택됩니다.



결과
구성은 다음을 기반으로 로그인 세션을 평가합니다.

- 하이재커가 세션을 가장하기 위해 사용자의 세션 쿠키를 한 장치에서 다른 장치로 복사하는 경우 인스턴스에 대한 액세스를 ServiceNow® 제한합니다.
- 안전하지 않은 네트워크를 사용하는 경우 사용자의 세션 액세스를 제한합니다.

인증 정책

인증 정책은 지정된 정책 조건에 따라 인증 요청을 평가하고 정책 조건 평가의 출력에 따라 액세스를 허용하거나 거부합니다. 예를 들어 액세스 허용 정책에 지정된 모든 정책 조건이 true로 평가되는 경우에만 액세스가 허용됩니다.

기본 제공 인증 정책을 사용하거나 보안 요구 사항에 따라 인증 정책을 생성합니다. 다음으로 이동하여 인스턴스의 정책을 찾을 수 있습니다. 적응형 인증 > 인증 정책 > 모든 정책.

주: 언제든지 허용 액세스 정책 또는 거부 액세스 정책 중 하나를 실행할 수 있지만 둘 다 실행할 수는 없습니다.

정책	설명
접근 정책 허용	기본적으로 모든 인증 요청을 거부합니다. 지정된 정책 조건과 일치하는 인증 요청만 허용합니다.
사전 인증 접근 정책 허용	사전 인증 접근 정책을 허용합니다.
로컬 이외의 로그인 사용자 허용	로컬 이외의 로그인 사용자를 허용하려면 이 정책을 선택합니다. SSO 복구 플로우의 컨텍스트에서 사용됩니다.
접근 거부 정책	기본적으로 인증 요청을 허용합니다. 지정된 정책 조건과 일치하는 인증 요청만 거부합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정책	설명
전역 차단 정책	인증 전에 사용자 및 API의 접근 요청을 거부합니다. 이 정책은 IP 주소 액세스 제어의 대안으로 사용할 수 있습니다.
세션 확인 정책	인증 정책은 필터 조건(예: IP 주소)을 평가하여 들어오는 요청에 대해 세션을 활성 상태로 유지해야 하는지 여부를 결정합니다. 이 정책에서 필터 기준을 설정해야 합니다.
로컬 로그인 거부 정책	모든 로컬 로그인을 차단하려면 이 정책을 선택합니다. SSO 복구 플로우의 컨텍스트에서 사용됩니다.
스텝다운 MFA 정책	사용자에게 MFA 인증이 필요하지 않은 경우 **Step-Down MFA** Policy(스텝다운 **MFA** 정책)를 기본 정책으로 선택합니다. 스텝업 MFA 정책에 정의된 정책 조건이 true로 평가되면 사용자는 MFA를 사용하여 로그인할 필요가 없습니다.
스텝업 MFA 정책	Step-Up MFA Policy(스텝업 MFA 정책)에 정의된 정책 조건이 true로 평가될 때 MFA 인증을 요구하려면 **Step-Up MFA** Policy(스텝업 **MFA** 정책)를 기본 정책으로 선택합니다.

인증 정책 구성

인스턴스에 대한 액세스 권한을 부여하거나 다단계 인증을 적용하는 데 사용할 입력 및 조건을 정의하도록 인증 정책을 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 모든 정책.

> 주: 완료된 정책의 예를 보려면 인스턴스에서 다음 정책을 검토할 수 있습니다.
> - 데모 정책 - 신뢰할 수 있는 IP 범위의 관리자에게만 로컬 로그인 허용
> - 데모 정책 - 관리자만 로컬 로그인 허용
> - 데모 정책 - 특정 사용자에 대한 사용자 이름 및 암호 기반 인증 제한

2. 새로 만들기 버튼을 클릭하여 새 정책 기록을 생성합니다.

3. 정책 양식의 필드에 내용을 입력합니다.

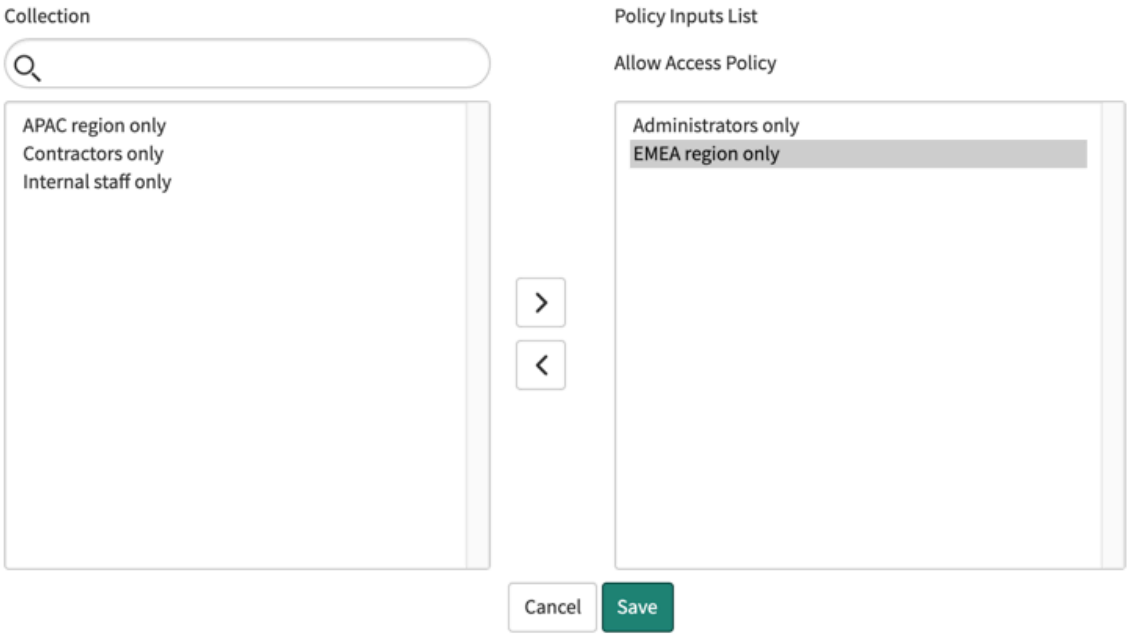
정책 양식

필드	설명
이름	정책 이름입니다.
애플리케이션	정책에 대해 범위가 지정된 애플리케이션입니다. 이 필드는 자동으로 현재 애플리케이션으로 채워집니다.
설명	정책 설명

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	정책이 활성 상태인지 여부입니다.

4. **Policy** Inputs(정책 입력) 탭에서 Edit(편집)를 클릭합니다.
5. 컬렉션 목록에서 하나 이상의 필터 기준을 선택하고 액세스 허용 정책 목록의 정책 입력 목록으로 이동합니다.



주: 이 섹션에서 사용할 고유한 필터 기준을 만드는 방법에 대한 자세한 내용은 을 참조하십시오 필터 기준.

6. 정책 조건 탭에서 새로 만들기를 클릭합니다.
7. 양식의 필드에 내용을 입력합니다.

조건 양식

필드	설명
레이블	조건을 식별하는 이름입니다.
설명	조건에 대한 설명입니다.
조건	인증 요청을 평가하는 데 사용되는 여러 정책 입력(필터 기준)의 논리적 조합입니다. 예를 들어, 신뢰할 수 있는 IP 주소 목록에서 협력업체만 허용하는 조건을 생성할 수 있습니다.

8. 옵션: 7단계를 반복하여 추가 정책 조건을 생성합니다.

주: 여러 정책 조건을 생성하는 경우 액세스 정책의 최종 출력은 모든 정책 조건의 논리적 OR 출력에 따라 달라집니다. 즉, 정책 조건 중 하나가 충족되면 정책이 true로 평가됩니다.

9. 저장을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인증 정책 컨텍스트에 인증 정책 추가

인증 정책 컨텍스트 중 하나에 인증 정책을 추가합니다. 인증 컨텍스트는 정책 입력 및 조건을 사용하여 인스턴스에 대한 액세스 권한이 사용자에게 부여되는지 또는 MFA가 사용자에게 적용되는지 여부를 결정합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트을 클릭하고 필요에 따라 항목 중 하나를 선택합니다.

   사전 인증 컨텍스트

   사전 권한 부여 컨텍스트를 사용하여 사용자가 로그인 화면을 보기 전에 정책을 평가합니다. 이 평가에 따라 사용자에게 액세스가 부여되거나 거부됩니다.

   사후 인증 컨텍스트

   사용자가 로그인 자격 증명을 입력한 후 정책을 평가하려면 사후 권한 부여 컨텍스트를 사용합니다. 이 평가에 따라 사용자에게 액세스가 부여되거나 거부됩니다. 이 평가는 인스턴스가 사용자를 식별한 후에 수행되므로 이 컨텍스트의 정책은 역할 또는 그룹과 같은 사용자 데이터를 기반으로 평가할 수 있습니다.

   MFA 컨텍스트

   MFA 컨텍스트를 사용하여 사용자가 로그인할 때 다단계 인증을 사용해야 하는지 여부를 결정합니다.

   세션 확인 컨텍스트

   세션 확인 컨텍스트를 사용하여 필터로 정의된 조건에 따라 설정된 IP 주소를 평가하고 세션 내에서 인스턴스에 대한 액세스를 허용합니다.

2. 기본 정책 필드에서 값을 선택합니다.
   이 필드의 값은 컨텍스트에서 정책 조건의 결과를 사용하는 방법을 결정합니다.

   이 필드에서 사용할 수 있는 옵션은 선택한 컨텍스트에 따라 다릅니다. 이러한 컨텍스트에 대한 자세한 내용은 다음 문서를 참조하십시오 인증 정책 컨텍스트.

3. 컨텍스트에 정책을 할당합니다.
   필드 이름은 선택한 컨텍스트에 따라 달라집니다.

   사전 인증 및 사후 인증 컨텍스트

   이러한 컨텍스트에는 기본 정책 필드의 선택 항목에 따라 거부 정책 또는 허용 정책 필드가 있습니다.

   MFA 컨텍스트

   이 컨텍스트에는 기본 정책 필드의 선택에 따라 스텝업 **MFA** 정책 또는 스텝다운 **MFA** 정책 필드가 있습니다.

   세션 확인 컨텍스트

   이 컨텍스트에는 기본 정책 필드의 선택에 따라 허용 정책 또는 거부 정책 필드가 있습니다.

4. 업데이트를 클릭합니다.
   기록을 업데이트한 후에는 정책 입력 및 정책 조건 탭에서 정책의 입력과 조건을 볼 수 있습니다.

적응형 인증 이벤트

적응형 인증 이벤트 테이블을 사용하여 이벤트에 대해 알 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 적응형 인증 이벤트 테이블에서 추적할 수 있는 몇 가지 로그입니다.

- `glide.adaptive.auth.log.success.event`: 사후 인증, API 로그인에 대한 `##` 이벤트를 알고 있습니다.
- `glide.adaptive.auth.log.mfa.relax.event`: MFA 컨텍스트에 대한 `mfa_relaxation` 이벤트를 확인합니다.

주:

- 사전 인증 컨텍스트의 경우 "`pre_auth`" 유형의 REST API 접근 정책: 기본적으로 `##` 이벤트가 기록됩니다. `##` 이벤트를 기록할 수 `####` .
- 인증 후 컨텍스트의 경우 "`pre_auth`" 이외의 유형의 REST API 접근 정책: 기본적으로 `##` 이벤트 또는 로깅됨. `##` 이벤트를 기록하려면 `glide.adaptive.auth.log.success.event` 속성을 사용하도록 설정해야 합니다.
- MFA의 경우: 기본적으로 `MFA ##` 이벤트가 기록됩니다.
- MFA 완화 이벤트를 로그하려면 `glide.adaptive.auth.log.mfa.relax.event` 속성을 활성화해야 합니다. `MFA ##` 는 `MFA ##`과 동일한 이벤트를 기록하지만, `##` 필드가 `False`로 채워집니다.

적응형 인증 속성 구성

적응형 인증을 활성화한 후 보안 요구 사항에 따라 적응형 인증 속성을 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 속성.
2. 다음 속성을 구성합니다.

적응형 인증 속성

속성	설명	값
인증 정책 사용 (glide.authenticate.auth.policy.enabled)	인증 정책을 활성화하는 옵션입니다.	예 | 아니요
인증 정책 (glide.authenticate.policy.debug)에 대한 디버그 로깅을 활성화합니다.	인증 정책에 대한 디버그 로깅을 활성화하는 옵션입니다.	예 | 아니요
전역 차단 정책 (glide.authenticate.global.blocking_policy.error_code)에 의해 접근이 차단될 때 사용자에게 표시되는 HTTP 오류 코드	전역 차단 정책이 사용자 로그인을 차단할 때 로그인 중에 표시되는 HTTP 오류 코드입니다.	다음 중에서 선택합니다. ◦ 금지됨(403) ◦ 찾을 수 없음(404)
전역 차단 정책에 의해 접근이 차단되는 경우 사용자에게 표시되는 오류 메시지 (금지 된(403) HTTP 오류 코드가 선택된 경우에만 적용됨) (glide.authenticate.global.blocking_policy.error_message)	전역 차단 정책이 액세스를 차단할 때 표시되는 오류 메시지입니다.	텍스트 필드
장치 신뢰 플로우 사용 (glide.authenticate.preauth.allow.trusted_device)	신뢰할 수 있는 장치 플로우를 활성화하는 옵션입니다.	예 | 아니요

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명	값
사용자가 등록할 수 있는 신뢰할 수 있는 장치의 최대 수 (glide.trusted.device.max.count)	사용자가 등록할 수 있는 신뢰할 수 있는 최대 장치 수입니다.	텍스트 필드
사용자가 신뢰할 수 있는 네트워크 출신인 경우 장치 신뢰 플로우에 대한 장치 등록을 건너뜁니다 (glide.authenticate.preauth.skip.user.registration).	사용자가 신뢰할 수 있는 네트워크에서 등록을 시도하는 경우 등록을 건너뛰는 옵션	예 | 아니요
세션 확인 기능을 활성화하는 속성입니다. 세션 확인 컨텍스트의 정책을 활성화하고 원하는 필터 및 조건(session.validation.enabled)을 설정한 후 이를 예로 설정합니다.	세션 확인 기능을 활성화하는 옵션입니다. 세션 확인 컨텍스트의 정책을 활성화하고 원하는 필터 및 조건을 설정한 후 이를 예로 설정합니다.	예 | 아니요

자습서: 적응형 인증 구성

다음 예시 단계를 사용하여 인스턴스에서 적응형 인증을 구성하십시오.

이 자습서를 사용하려면 적응형 인증 이 활성화된 인스턴스가 있어야 합니다. 이 프로세스에 대한 자세한 내용은 적응형 인증 활성화 문서를 참조하십시오.

이 예시에서는 새 정책을 생성하고 인스턴스에 적용하는 방법을 안내합니다. 이 튜토리얼에서는 다음 작업을 수행합니다.

필터 기준 기록 생성

정책에 대한 입력으로 사용할 그룹 필터 기준 기록을 생성합니다. 이 기록을 사용하면 정책이 사용자 그룹을 기반으로 액세스를 결정할 수 있습니다. 이 단계에서는 정책이 액세스를 결정하는 데 사용하는 그룹을 정의합니다.

정책 생성

사용자가 인스턴스에 액세스할 수 있는지 여부를 결정하는 정책을 만듭니다. 이 정책은 생성한 그룹 필터 기준 기록을 입력으로 사용합니다. 이 단계에서는 정책이 정책 입력을 사용하여 사용자 액세스를 결정하는 방법을 정의하는 정책 조건도 정의합니다.

정책 컨텍스트 구성

새 정책을 사용하도록 사후 인증 정책 컨텍스트 를 구성합니다. 구성된 경우 인스턴스는 필터 기준 기록에 정의된 그룹 내 사용자에 대한 접근을 거부합니다.

필터 기준 기록 생성

적응형 인증 정책에 대한 정책 입력으로 사용할 기준 기록을 생성하는 방법에 대해 알아봅니다.

시작하기 전에
필요한 역할: 관리자

사용자 그룹을 기반으로 인스턴스에 대한 액세스를 거부하려면 그룹 필터 기준 기록을 생성해야 합니다. 이 기록은 정책이 액세스를 허용하거나 거부할 수 있는 사용자 그룹 또는 사용자 그룹 집합을 정의합니다. 이 예시에서는 단일 사용자 그룹에 대한 그룹 필터 기준 기록을 만듭니다.

사용자 그룹 및 사용자 그룹이 인스턴스에서 사용되는 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 사용자 관리 탐색 .

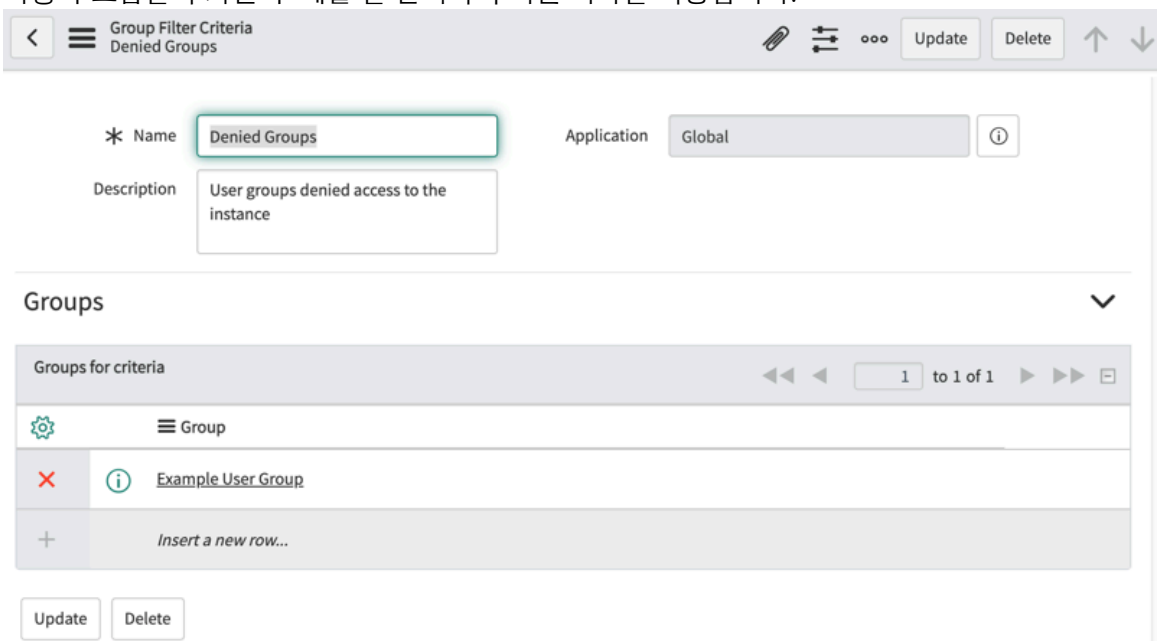
프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 필터 기준 > 그룹 기준.

2. 새로 만들기를 클릭하여 새 기록을 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 이름 필드에 기록 이름을 입력합니다.
   (예: ### ##)
4. 설명 필드에 간단한 설명을 입력합니다.
   예를 들어 ### ### #### #### #######.
5. 기준 그룹 목록에서 새 행 삽입...을 두 번 클릭합니다.
6. 사용자 그룹의 이름을 입력하거나 참조 아이콘( )을 눌러 목록에서 그룹을 선택합니다.
   필터 기준에 대한 새 사용자 그룹을 만들려면 참조 아이콘( )을 클릭한 다음 새로 만들기 단추를 클릭합니다. 사용자 그룹 생성에 대한 자세한 내용은 사용자 그룹 생성을 참조하십시오.
7. 사용자 그룹을 추가한 후 제출 을 클릭하여 기준 기록을 저장합니다.



정책 생성

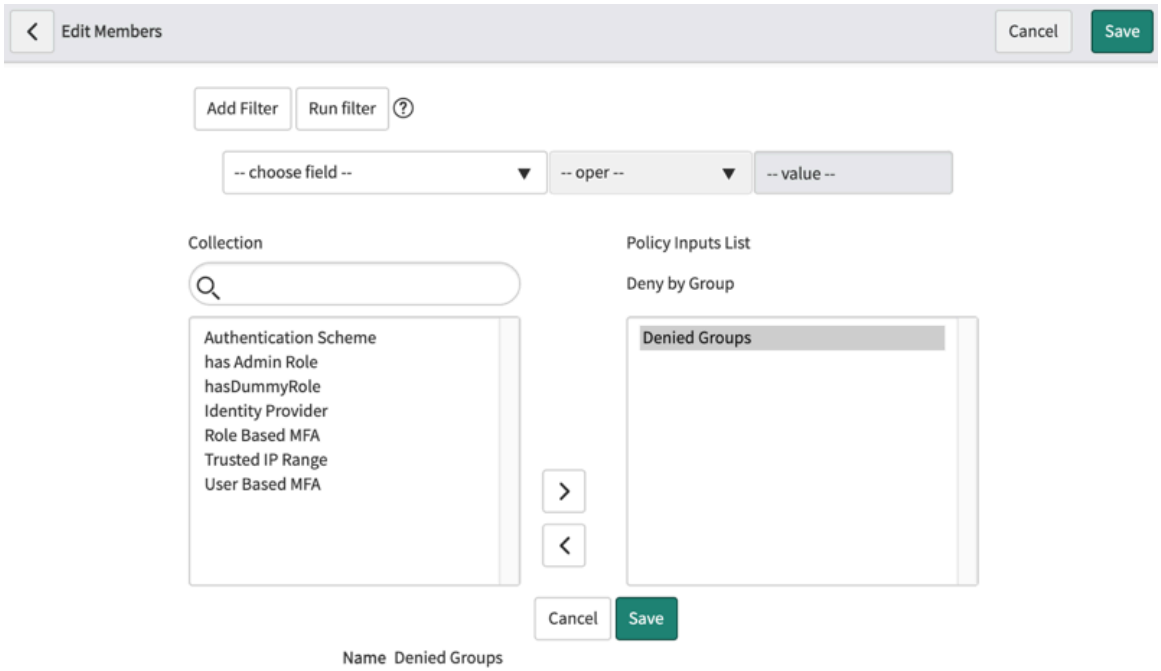
그룹 필터 기준에 정의된 사용자 그룹에 대한 접근을 거부하는 정책을 만드는 방법을 알아봅니다.

시작하기 전에
필요한 역할: 관리자

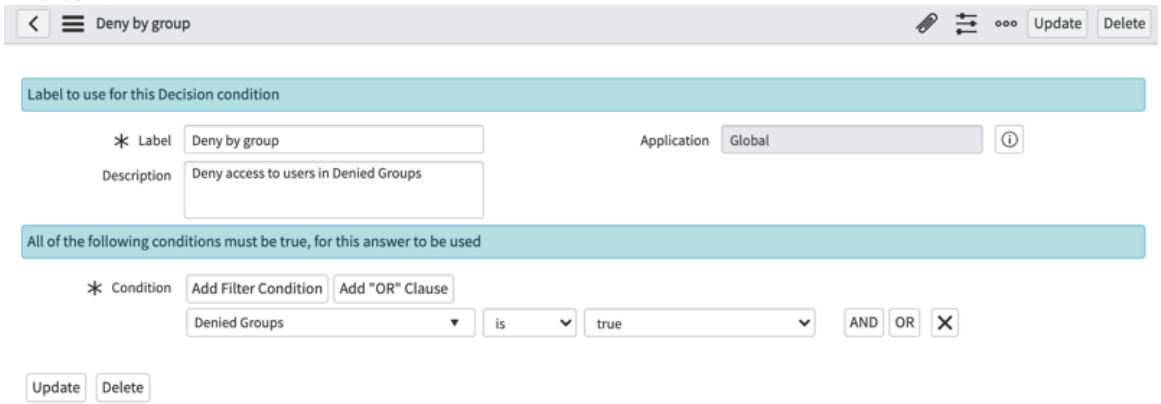
프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 모든 정책.
2. 정책 목록에서 새로 만들기를 클릭합니다.
3. 이름 필드에 기록 이름을 입력합니다.
   (예: ### ##)
4. 설명 필드에 간단한 설명을 입력합니다.
   예를 들어 ### ### #### #### #######.
5. 양식 헤더를 마우스 오른쪽 단추로 클릭하고 저장을 클릭합니다.
   저장하면 정책 입력 및 정책 조건 목록이 양식에 표시됩니다.
6. 정책 입력 목록에서 편집을 클릭합니다.
7. 목록 수집기에서 이전 단계에서 만든 필터 기준을 정책에 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



8. 저장을 클릭합니다.
   인스턴스가 정책 입력을 저장하고 정책 기록이 다시 표시됨을 표시합니다.
9. 정책 조건 목록에서 새로 만들기를 클릭합니다.
10. 레이블 필드에서 이 조건에 대한 레이블(예: `### ##`)을 생성합니다.
11. 설명 필드에 간단한 설명을 입력합니다.
    (예: `### ### #### ## ### ##`)
12. 조건 필드에서 이전 단계에서 생성한 필터 기준을 선택한 다음 **is**, **true**를 차례로 선택하여 조건을 완성합니다.



13. 저장을 클릭합니다.

정책 컨텍스트 구성

새 정책을 사용하도록 사후 인증 정책 컨텍스트를 구성합니다. 구성된 경우 인스턴스는 필터 기준 기록에 정의된 그룹 내 사용자에 대한 접근을 거부합니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 적응형 인증 > 인증 정책 컨텍스트 > 사후 인증 컨텍스트.
   이 자습서에 사용된 정책은 사용자가 속한 그룹을 평가해야 하므로 사후 인증 컨텍스트 를 사용해야 합니다. 이 정보는 자격 증명을 입력한 후에만 사용할 수 있습니다.
2. **Default** Policy(기본 정책) 필드에서 `Deny Policy(## ##)`를 선택합니다.
   이 선택은 기본적으로 사용자에게 액세스 권한을 부여하고 정책 조건이 예로 평가되는 경우에만 액세스를 거부합니다.
3. 거부 정책 필드에서 이전 단계에서 생성한 정책을 선택합니다.
4. 업데이트를 클릭하여 정책 컨텍스트 기록을 저장합니다.

신뢰할 수 있는 모바일 앱에 대한 적응형 인증

ServiceNow 를 사용하여 신뢰할 수 없는 네트워크에서 액세스하십시오Now Mobile 앱.

신뢰할 수 있는 모바일 앱에 대한 적응형 인증

Trusted Mobile Apps에 대한 적응형 인증을 사용하면 사용자가 ServiceNowNow Mobile 앱. 인스턴스는 신뢰할 수 있는 IP 네트워크 경계 뒤에 보호됩니다.

다음은 네트워크 외부에 있는 동안 인스턴스에 액세스해야 하는 몇 가지 시나리오입니다.

직원은 네트워크 외부에서 및 Employee Service Center(포털)에 Now Mobile 앱 액세스해야 합니다. 신뢰할 수 있는 모바일 앱 필터를 사용하면 사용자 계정에 연결된 신뢰할 수 Now Mobile 앱 있는 항목에서 시작되는 수신 요청을 식별할 수 있습니다.

관리자는 정책을 구성할 수 있습니다. 이 정책을 통해 사용자는 모바일 장치를 등록하고 신뢰할 수 있는 네트워크의 인스턴스에 액세스할 수 있습니다.

사용자는 인스턴스에 표시된 QR을 스캔하여 모바일 장치를 등록할 수 있습니다. 등록 후에는 자격 증명을 사용하여 에서 인스턴스에 Now Mobile 앱로그인할 수 있습니다.

> **주:** 모바일 장치를 등록하려면 신뢰할 수 있는 네트워크에 있어야 합니다. 등록 후에는 다른 네트워크에서도 인스턴스에 로그인할 수 있습니다.

기능

관리자는 다음 기능을 사용할 수 있습니다.

- 신뢰할 수 있는 앱 필터 기준을 사용하여 정책을 구성합니다.
- 신뢰할 수 있는 모바일 앱에 대한 새 필터 기준을 사용하여 정책 조건을 생성합니다.
- 신뢰할 수 있는 모바일 앱에서 사용자에 대해 모든 로그인 방법을 지원합니다(로컬 로그인, SAML, OIDC 및 MFA).
- 신뢰할 수 있는 장치를 해지합니다.
- 모든 장치 등록 또는 해지 작업에 대한 보안 이벤트를 추가합니다. 이벤트를 사용하여 사용자에게 알릴 수 있습니다.
- 서명 실패, 쿠키 유효성 검사 실패, 잘못된 토큰, 잘못된 헤더 또는 쿼리 매개변수에 대한 보안 이벤트를 지원합니다.
- 등록된 장치의 최대 수를 제어합니다.
- 사용자가 이미 페어링된 장치를 제거하지 않는 한 새 장치 등록을 방지합니다.
- 장치가 마지막으로 사용된 시간을 캡처합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

신뢰할 수 있는 모바일 앱 활성화

인증 정책 및 필터 조건을 사용하여 Trusted Mobile 앱으로 적응형 인증을 활성화합니다.

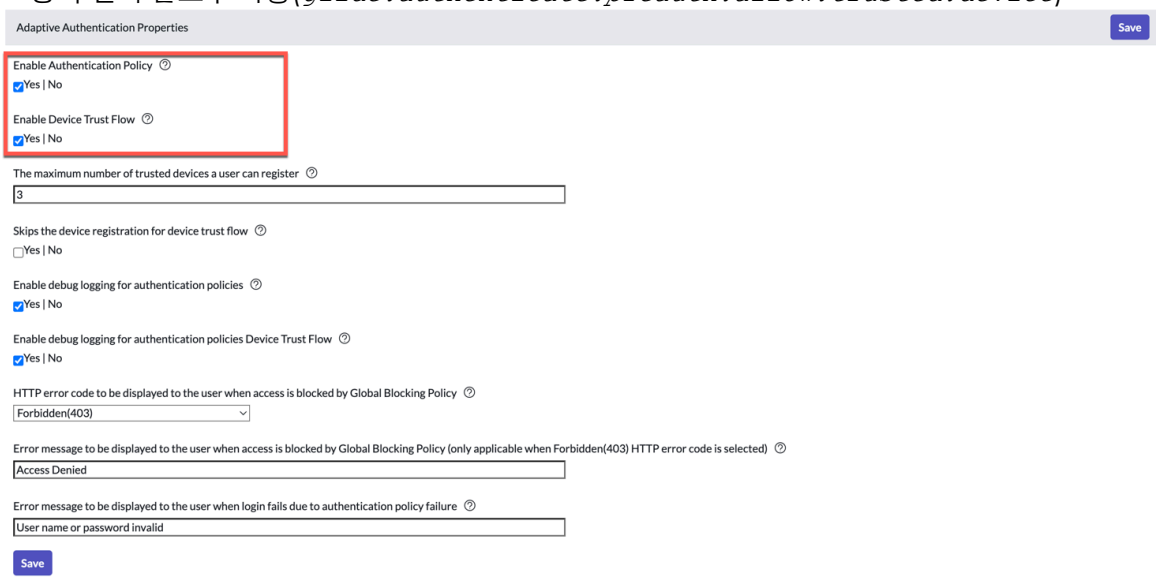
시작하기 전에

적응형 인증(*com.snc.adaptive_authentication*) 플러그인이 설치되어 있는지 확인합니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 속성.
2. 적응형 인증 속성 페이지에서 다음 속성을 활성화합니다.
   - 인증 정책()*glide.authenticate.auth.policy.enabled*을 활성화합니다.
   - 장치 신뢰 플로우 사용(*glide.authenticate.preauth.allow.trusted.device*)



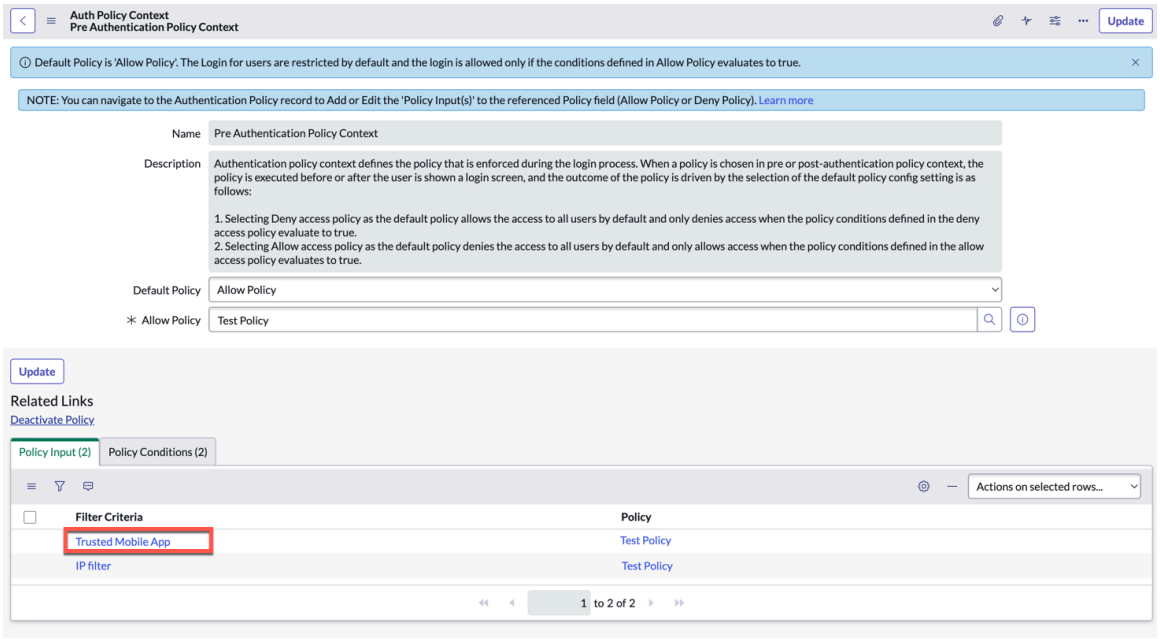
> 주: 장치 신뢰 플로우 속성을 비활성화하려면 신뢰할 수 있는 모바일 필터를 사용하여 조건을 제거해야 합니다. 그렇지 않으면 조건을 제거하라는 오류 메시지가 표시됩니다.

3. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트 > 사전 인증 컨텍스트.
4. 사전 인증 컨텍스트에서 조건을 정의합니다.
   자세한 내용은 사전 인증 컨텍스트 문서를 참조하십시오.

> 주: 기본적으로 정책 조건은 거부 정책입니다. 정책 허용으로 변경할 수 있습니다. 이 두 정책은 정반대입니다.
>
> - 허용 정책을 사용하면 기본적으로 모든 사용자의 액세스가 거부되며 액세스 허용 정책 조건이 true인 경우에만 액세스가 허용됩니다.
> - 거부 정책을 사용하면 기본적으로 모든 사용자의 액세스가 허용되며, 거부 액세스 정책 조건이 true인 경우에만 액세스가 거부됩니다.

정책 입력에서 정책 입력 **Trusted Mobile App** 은 신뢰할 수 있는 모바일 앱에 대한 정책 입력입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

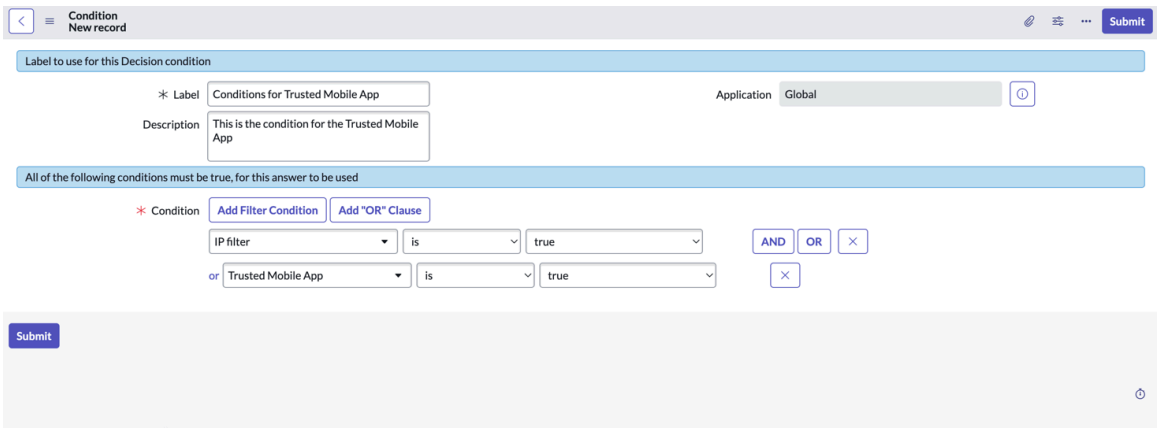


5. 정책 조건에서 새로 만들기를 클릭하여 조건을 생성합니다.

6. 양식에서 필드를 채웁니다.

필터 조건 양식

필드	설명
레이블	조건 이름
설명	조건 설명
애플리케이션	이 기록에 대한 애플리케이션 범위입니다.
조건	AND 및 OR를 기반으로 하는 조건입니다. 인증 정책이 **Allow** Policy(허용 정책)이므로 이미지에 표시된 예에서 Trusted Mobile App(신뢰할 수 있는 모바일 앱)의 조건이 true로 설정됩니다.



7. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
신뢰할 수 있는 장치 기능에 대한 정책 입력 및 필터 조건이 생성됩니다. 사용자는 신뢰할 수 있는 장치 기능을 사용하여 신뢰할 수 없는 네트워크에서 인스턴스에 액세스할 ServiceNow 수 있습니다 Now Mobile 앱. 자세한 내용은 신뢰할 수 있는 장치 등록 문서를 참조하십시오.

신뢰할 수 있는 장치 등록

신뢰할 수 있는 장치를 등록하여 네트워크 외부의 인스턴스에 액세스합니다 ServiceNow .

시작하기 전에
신뢰할 수 있는 장치 등록을 수행하려면 신뢰할 수 있는 네트워크에 있어야 합니다.

필요한 역할: 없음

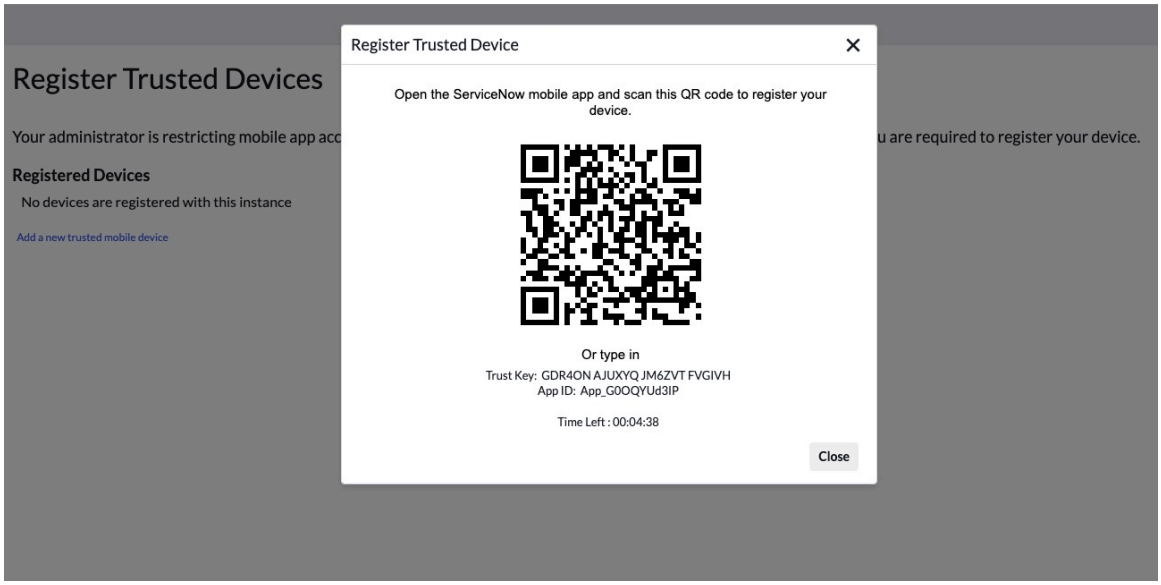
프로시저
1. 다음 메뉴 옵션 중 하나로 이동합니다.
   - 에서 Now Platform다음으로 이동합니다. 모두 > 셀프 서비스 > 내 프로필.

     주: 인스턴스 헤더에서 사용자 이름을 클릭하여 프로파일에 액세스할 수도 있습니다.



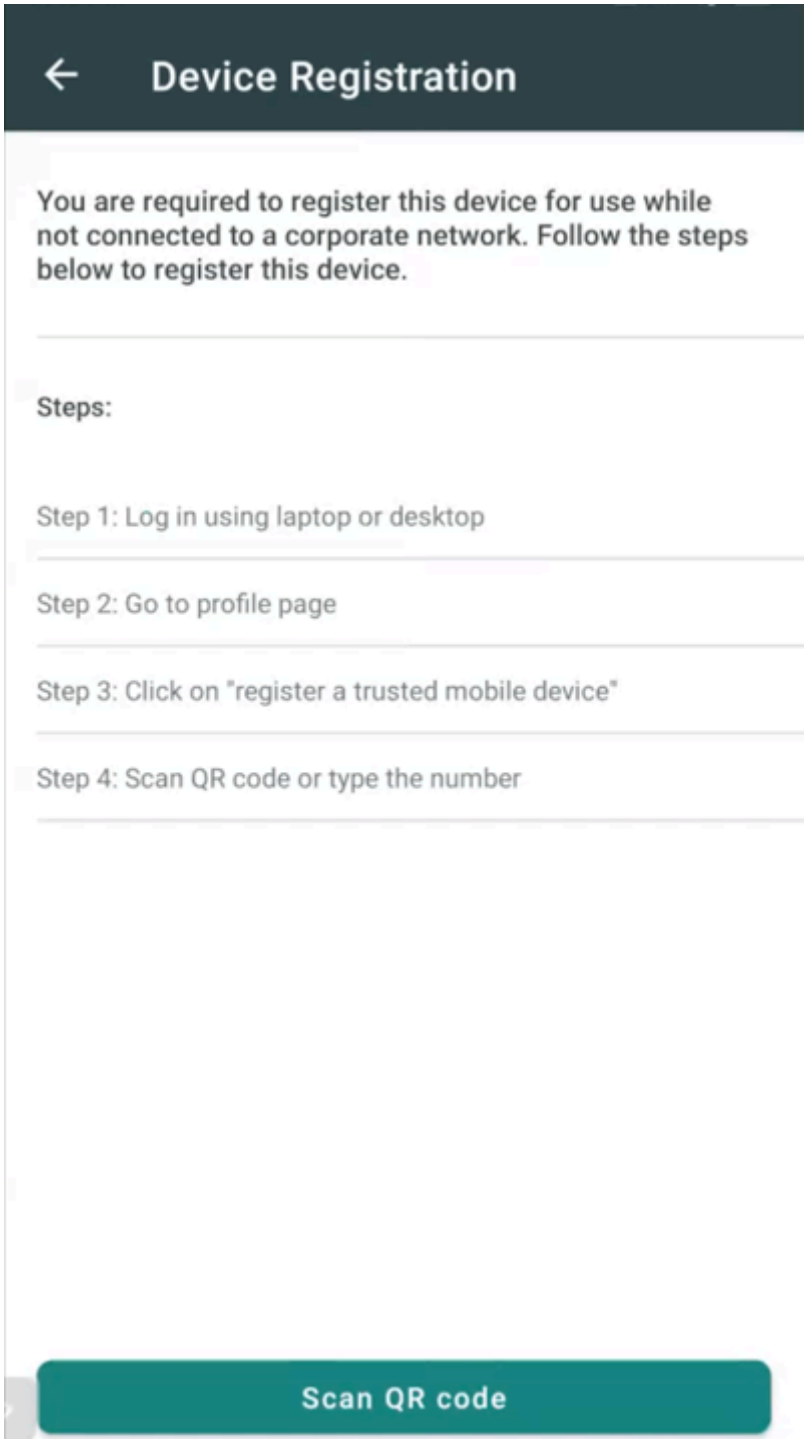
   - 에서 프로파일을 클릭하고 Trusted Device(Now Support신뢰할 수 있는 장치)를 선택합니다.
2. 사용자 프로필의 관련 링크 섹션에서 신뢰할 수 있는 모바일 장치 등록을 클릭합니다.
   Register Trusted Devices(신뢰할 수 있는 장치 등록) 페이지가 표시됩니다.
3. 새 신뢰할 수 있는 모바일 장치 추가를 클릭하여 새 장치를 등록합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 모바일 앱의 장치 등록 화면에서 ServiceNow**QR** 코드 스캔 버튼을 누르고 노트북 또는 데스크톱에 표시된 QR 코드를 스캔합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

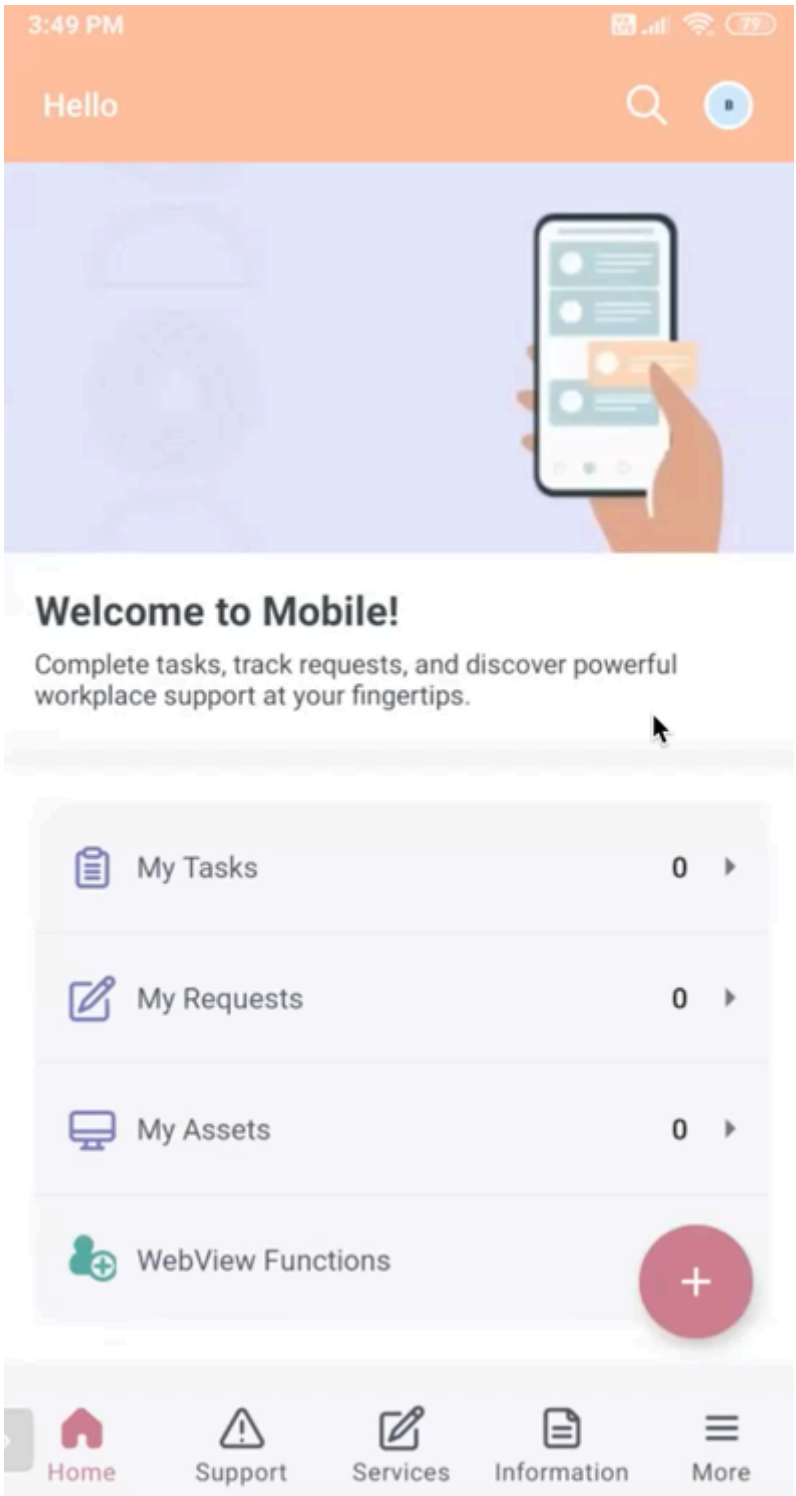


등록 프로세스가 완료되고 인증을 완료하라는 로그인 페이지가 표시됩니다.

5. 자격 증명을 지정하고 에 로그인합니다 Now Mobile 앱.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

모바일 홈 화면이 표시됩니다.



결과
랩톱 또는 데스크톱의 Register Trusted Devices(신뢰할 수 있는 장치 등록) 페이지에 등록된 장치가 표시됩니다. 페이지에서 등록된 장치를 제거하려는 경우 아이콘을 사용할 수 있습니다.

다음에 수행할 작업
다음으로 이동 모두 > 적응형 인증 > 장치 신뢰 > 장치 등록 등록된 장치의 모든 상세 정보를 볼 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

신뢰할 수 있는 장치 관리

신뢰할 수 있는 장치 등록 페이지에서 신뢰할 수 있는 장치를 관리합니다.

시작하기 전에
필요한 역할: 없음

프로시저

1. 다음 메뉴 옵션 중 하나로 이동합니다.
   - 에서 Now Platform다음으로 이동합니다. 모두 > 셀프 서비스 > 내 프로필.

     주: 인스턴스 헤더에서 사용자 이름을 클릭하여 프로파일에 액세스할 수도 있습니다.

   - 에서 프로파일을 클릭하고 Trusted Device(Now Support신뢰할 수 있는 장치)를 선택합니다.
2. 사용자 프로파일의 Related Links(관련 링크) 섹션에서 **Register Trusted** Device(신뢰할 수 있는 장치 등록)를 클릭합니다.
   Register Trusted Devices(신뢰할 수 있는 장치 등록) 페이지가 표시됩니다.
3. Register Trusted Devices(신뢰할 수 있는 장치 등록) 페이지에서 아이콘을 클릭하여 장치를 제거합니다.

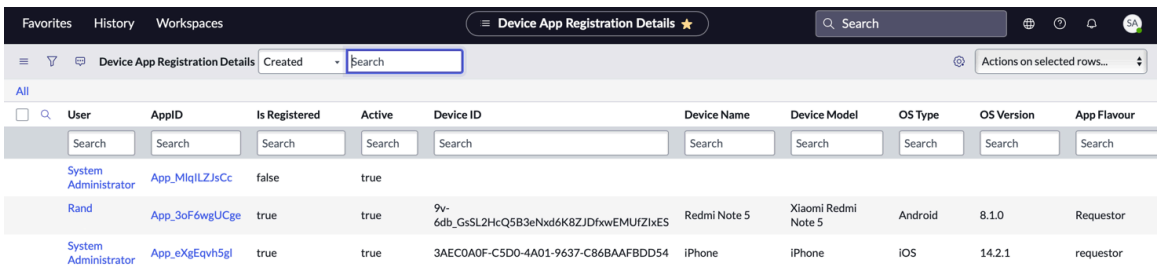
   주: 인스턴스에 액세스하려면 삭제된 모바일 장치를 다시 등록해야 합니다.

등록된 장치의 등록 상세 정보

인스턴스에 등록된 ServiceNow 장치의 상세 정보를 봅니다.

인스턴스에 등록된 장치의 모든 상세 정보를 보려면 다음으로 이동합니다. 모두 > 적응형 인증 > 장치 신뢰 > 장치 등록.

필터를 사용하여 장치를 식별합니다. **AppID** 필드를 클릭하여 등록된 장치에 대한 자세한 내용을 확인합니다.

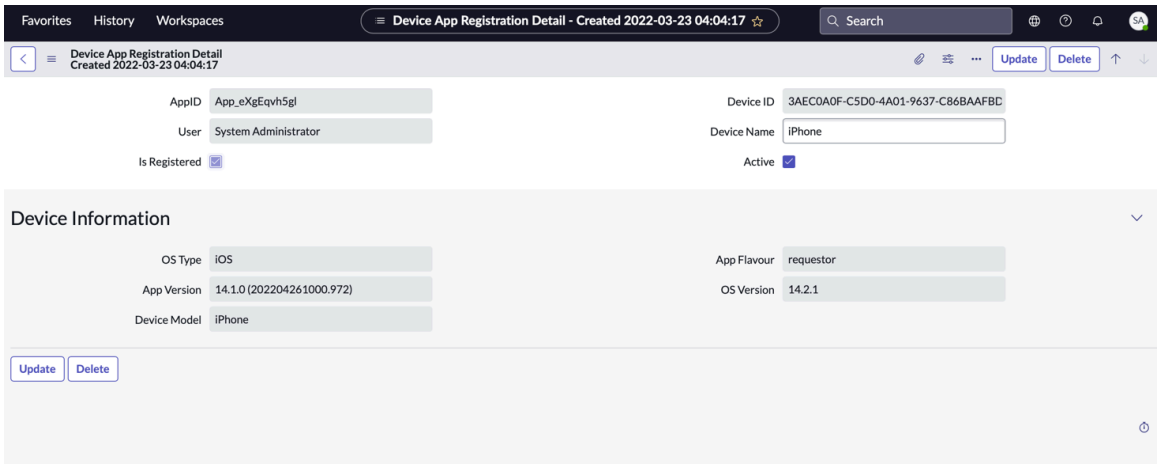


장치에 대해 다음과 같은 상세 정보가 표시됩니다.

- AppID
- 장치 ID
- 사용자
- 장치 이름
- 다음과 같은 장치 정보:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- OS 유형
- 앱 버전
- 앱 버전
- OS 버전
- 장치 모델



신뢰할 수 있는 모바일 앱 문제 해결

이러한 문제 해결 시나리오를 검토하여 Trusted Mobile 앱의 문제를 해결하십시오.

다음 섹션에서는 몇 가지 문제 해결 시나리오와 문제 해결 방법에 대해 설명합니다.

인스턴스와 모바일 간의 시간 차이(클럭 오차)

클럭 오차가 있는 경우 신뢰할 수 있는 장치 사용을 위해 모바일 장치의 시계를 조정하거나 재설정할 수 있습니다.

QR 코드 5분 이내 만료

신뢰할 수 있는 장치 기능에 대한 QR 코드는 5분 이내에 만료됩니다. 이 경우 클릭하면 새 QR 코드를 찾을 수 있습니다.

주: QR 코드 만료를 연장할 수 있습니다. 코드 만료를 연장하려면 관리자에게 문의하십시오.

시스템 속성이 변경됨

시스템 속성이 변경된 경우 로그인에 사용할 수 있는 유효한 자격 증명에 대한 시스템 속성을 기반으로 등록을 확인합니다.

등록된 최대 장치 수

최대 장치 등록 수에 도달하면 기존 장치를 제거하거나 관리자에게 문의하여 최대 장치 수를 변경합니다.

API 인증

API에 대한 인증 구성입니다.

의 ServiceNow®API 기반 인증은 인스턴스에 액세스하는 사용자의 ID를 확인한 다음, 인스턴스에 대한 API 호출을 ServiceNow® 수행하는 동안 사용자의 역할 또는 직무 기능과 일치하는 기능에 대해 사용자에게 권한을 부여합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

의 ServiceNow®API 인증 유형은 다음과 같습니다.

- 인증서 기반 인증
- OAuth
- 토큰 기반 인증

인증서 기반 인증

인증서 기반 인증을 사용하면 신뢰할 수 있는 CA(인증 기관)의 인증서를 사용하여 인바운드 API 요청을 상호 인증할 수 있습니다.

인바운드 웹 서비스에 대한 인증서 기반 인증

SOAP 및 REST API에 대한 ServiceNow 인바운드 요청을 인증합니다. 인바운드 웹 서비스에 대한 상호 인증을 설정하려면 문서를 참조하십시오 인증서 기반 인증 설정.

OAuth

OAuth 기반 인증은 인증 프로토콜을 사용하여 시스템에서 신뢰를 설정하려고 시도하는 클라이언트의 ID를 확인합니다.

OAuth 2.0 - Open Authorization은 웹 애플리케이션, 데스크톱 애플리케이션 및 모바일 장치에 대한 특정 권한 부여 흐름을 제공하면서 클라이언트 개발자의 단순성을 유지하는 업계 표준 권한 부여 프로토콜입니다.

인바운드

인스턴스에 액세스하려는 외부 클라이언트에 대한 엔드포인트를 생성합니다. 이렇게 하면 OAuth 클라이언트 애플리케이션 레코드가 생성되고 클라이언트가 인스턴스의 제한된 자원에 액세스하는 데 필요한 클라이언트 ID 및 클라이언트 비밀이 생성됩니다. 자세한 내용은 OAuth 인바운드 문서를 참조하십시오.

토큰 기반 인증

API 키 또는 HMAC를 사용하는 인바운드 REST API 구성에 대한 토큰 기반 인증입니다.

사용자 인증에 사용할 수 있도록 ServiceNow® REST API 엔드포인트에 대한 API 토큰을 지원합니다.

인바운드 REST API 구성에 대한 토큰 기반 인증은 API 키 또는 HMAC 토큰이 있는 인스턴스에서 수행할 ServiceNow® 수 있습니다.

인바운드 **REST** API에 대한 **API** 키 및 **HMAC** 인증

사용자 이름과 암호가 웹후크 URL에 표시되지 않도록 REST API 엔드포인트 ServiceNow® 에 대한 API 토큰을 지원합니다.

API 키 기반 인증을 활성화하여 인바운드 웹후크 URL을 안전하게 인증합니다.

API Key와 HMAC 인증을 사용하려면 인스턴스에 (플러그인: `com.glide.tokenbased_auth`) ServiceNow® 를 설치해야 합니다.

⚠ 경고: 중요한 정보를 서버에 제출할 때 **POST** 요청을 사용합니다.

API 키 및 HMAC 인증 설치는 다음 플러그인에 종속되어 있습니다.

- REST API 인증 범위 플러그인(`com.glide.rest.auth.scope`)
- REST API Access Policy 플러그인(`com.glide.rest.policy`)
- 인증 범위(`com.glide.auth.scope`)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

복지

인바운드 REST API에 대한 API 키 및 HMAC 인증을 통해 다음을 수행할 수 있습니다.

- REST API 인증을 위해 API 키 또는 HMAC 토큰을 지정하는 기능입니다.
- 사용자 계정을 API 키 또는 HMAC 토큰과 연결하는 기능입니다.
- REST API 호출 내에서 토큰을 쿼리 매개변수 또는 헤더로 지정하는 기능입니다.
- API 키를 특정 범위와 연결된 API를 호출하는 데만 사용할 수 있도록 인증 범위를 API 키 또는 HMAC 토큰 구성과 연결하는 기능입니다.
- API 키 또는 HMAC 토큰 구성을 API 액세스 정책에 사용할 수 있는 인증 프로파일과 연결하는 기능입니다.

API 키 및 HMAC 인증 활성화

인스턴스에서 플러그인 API 키 및 HMAC 인증(`com.glide.tokenbased_auth`)을 활성화할 수 있습니다 ServiceNow® .

시작하기 전에
필요한 역할: admin.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 API 키 및 HMAC 인증 플러그인 (`com.glide.tokenbased_auth`)을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

API 키 구성 - 토큰 기반 인증

REST API 엔드포인트에 대한 인증을 지원하도록 API 키를 구성합니다.

시작하기 전에
필요한 역할: 관리자

필요한 플러그인: API 키 및 HMAC 인증(`com.glide.tokenbased_auth`)

프로시저

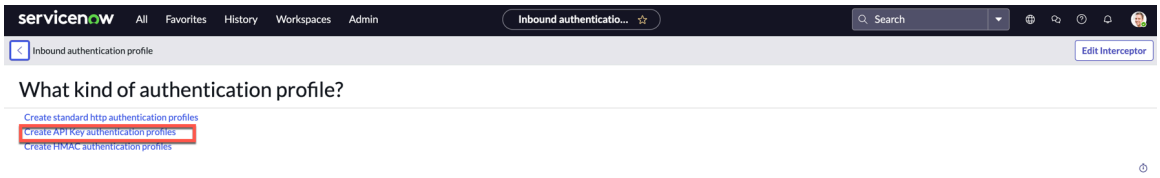
1. 인바운드 인증 프로파일을 생성합니다.

   a. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > 인바운드 인증 프로파일.

   b. 새로 만들기를 선택합니다.
   `#### What kind of authentication profile(## ##### ##)###` 메시지가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. **API** 키 인증 프로필 만들기를 선택합니다.

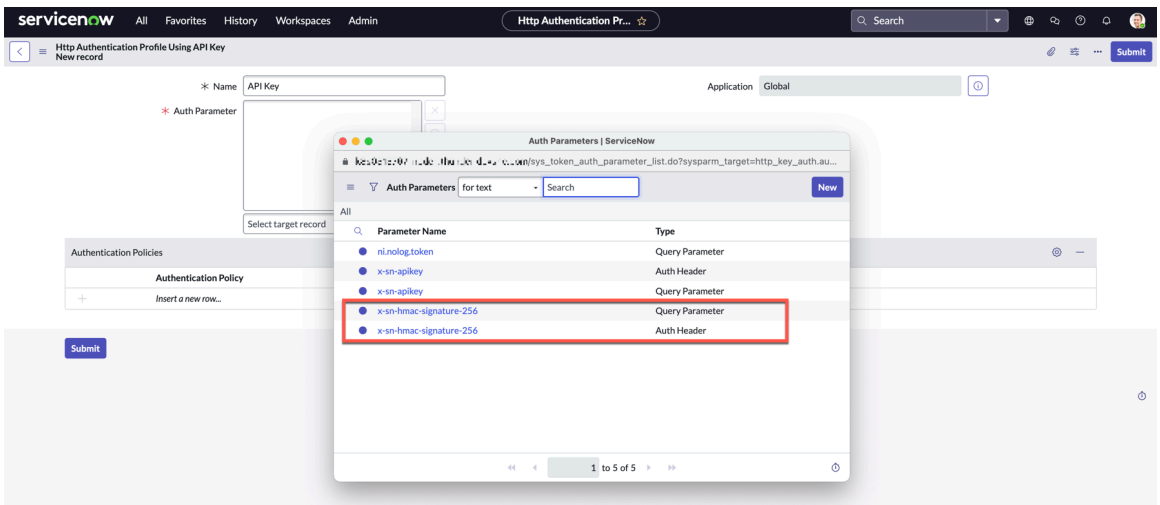


d. 양식의 필드에 내용을 입력합니다.

API 키 인증 프로파일

필드	설명
이름	인증 정책을 식별하는 이름입니다.
애플리케이션	인증 정책의 범위입니다.
인증 매개변수	인증 요청에 대한 인증 매개변수를 선택합니다. 기본 옵션을 선택하거나 새 인증 매개변수를 생성할 수 있습니다. ▪ x-sn-apikey: 인증 헤더 ▪ x-sn-apikey: 쿼리 매개변수 헤더

주: 선택한 옵션은 인증 헤더 또는 쿼리 매개변수의 REST 호출에서 정의되어야 합니다.



주: API 키에 대한 프리픽스를 추가하려면 선택한 인증 매개변수 파일을 열고 프리픽스 필드를 지정합니다.

e. 양식을 제출합니다.

2. REST API 키를 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > **REST API** 키.

b. 새로 만들기를 선택합니다.

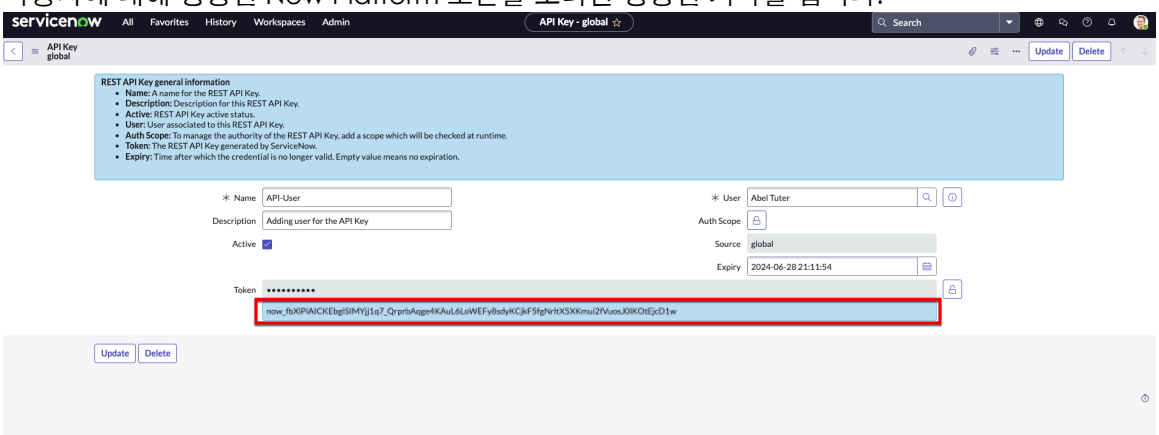
c. 양식에서 필드에 다음을 입력합니다.

API 키

필드	설명
이름	REST API 키를 식별하기 위한 이름
설명	REST API 키에 대한 설명입니다.
활성	REST API 키의 상태입니다.
사용자	REST API 키와 연결된 사용자입니다. 조회 아이콘을 사용하여 사용자를 선택합니다.
인증 범위	REST API 키의 권한을 관리하기 위해 인증 범위를 추가하는 옵션입니다.
토큰	에서 생성된 REST API 키입니다 Now Platform. 헤더 또는 쿼리 매개변수 내에서 REST API 호출의 일부로 사용할 키를 복사합니다.
만료	자격 증명이 더 이상 유효하지 않게 되는 시간입니다. 값이 비어 있으면 만료되지 않습니다. 주: 토큰 만료에 대한 자세한 내용은 다음 문서를 참조하십시오 토큰 만료 정리 중 .

d. 양식을 제출합니다.

e. 사용자에 대해 생성된 Now Platform 토큰을 보려면 생성된 기록을 엽니다.



3. REST API 접근 정책을 생성합니다.

a. 다음으로 이동 모두 > 시스템 웹 서비스 > **REST API** 접근 정책.

b. 새로 만들기를 선택합니다.

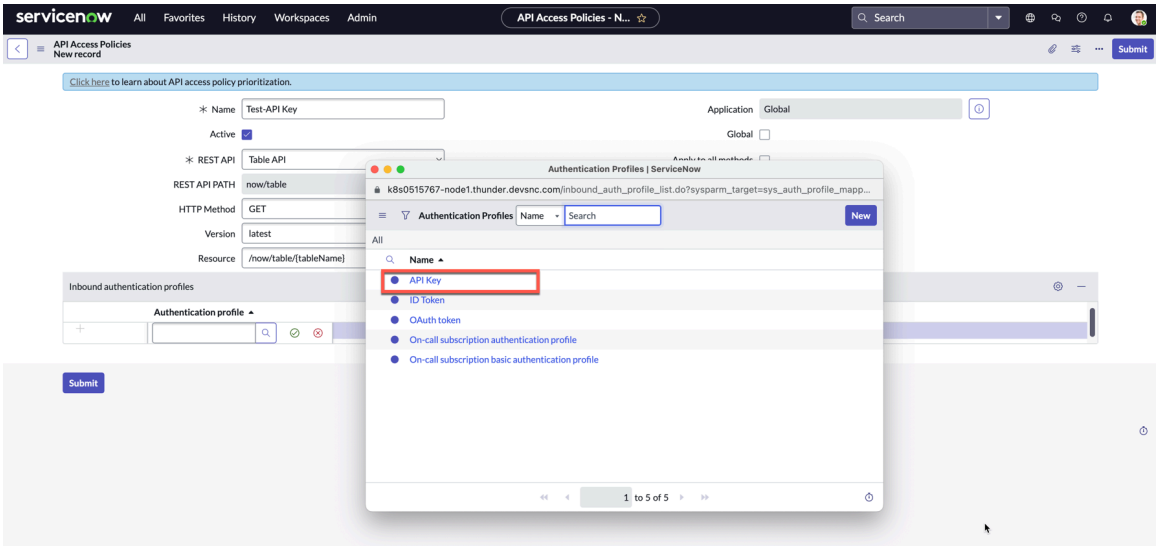
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 양식의 필드에 내용을 입력합니다.

API 접근 정책

필드	설명
이름	API 접근 정책의 고유한 이름입니다.
활성	API 접근 정책을 활성화하는 옵션입니다.
REST API	액세스 정책이 적용되는 REST API입니다. 예를 들어 첨부 파일 **API**입니다.
REST API 경로	REST API의 API 경로입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 예: **now/attachment**.
HTTP 메서드	API와 상호작용하는 데 사용되는 메서드입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다.
버전	API의 버전입니다. 예: **v1**. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 주: REST API의 모든 버전에 대한 인증 정책을 만들려면 각 버전에 대해 개별 정책을 만들어야 합니다.
자원	REST API의 하위 자원입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 예: **/now/attachment**
애플리케이션	애플리케이션의 범위입니다.
전역	API의 모든 메서드, 버전 및 자원에 인증 정책을 적용하려면 이 필드를 활성화합니다. 주: 전역 REST API 정책에서는 토큰 기반 인증을 사용할 수 없습니다.
모든 메서드에 적용	API에 대한 인증 정책을 API의 모든 메서드, 버전 및 자원에 적용하려면 이 필드를 활성화합니다.
모든 자원에 적용	API에 대한 인증 정책을 모든 버전에 적용하려면 이 필드를 활성화합니다.
모든 버전에 적용	API에 대한 인증 정책을 모든 자원에 적용하려면 이 필드를 활성화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



d. 생성된 API 인증 프로파일을 추가합니다.

e. 양식을 제출합니다.

인증 구성에 따라 Header 또는 Query 파라미터 내에서 API Key 생성 시 생성된 Now Platform x-sn-apikey(토큰)를 사용하여 REST API 호출을 전송할 수 있습니다.

⚠ 경고: 중요한 정보를 서버에 제출할 때 **POST** 요청을 사용합니다.

HMAC 구성 - 토큰 기반 인증

REST API 엔드포인트에 대한 인증을 지원하도록 HMAC를 구성합니다.

시작하기 전에
필요한 역할: 관리자

필요한 플러그인: API 키 및 HMAC 인증(`com.glide.tokenbased_auth`)

프로시저

1. HMAC 구성을 생성합니다.

a. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > **HMAC** 구성.

b. 새로 만들기를 선택합니다.

ⓘ 주: 플러그인 설치 시 생성되는 기본 **HMAC SHA256 Base64** 인코딩 을 사용할 수도 있습니다.

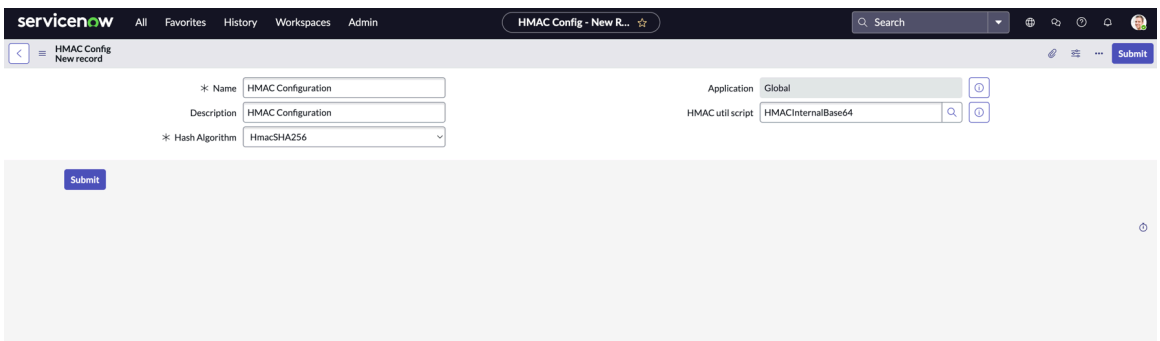
c. 양식에서 필드에 다음을 입력합니다.

HMAC 구성

필드	설명
이름	HMAC 구성의 이름입니다.
애플리케이션	구성의 범위입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	구성에 대한 자세한 설명입니다.
해시 알고리즘	해시 알고리즘을 선택합니다. 사용 가능한 옵션: ▪ HmacSHA256 ▪ HmacSHA384 ▪ HmacSHA512
HMAC 유틸리티 스크립트	HMAC에 대한 유틸리티 스크립트입니다. 주: 키 ID가 없는 요청 본문, 타임스탬프 및 비밀을 사용하여 HMAC 인증을 확인하는 경우 다음을 수행합니다. ▪ HMAC 유틸리티 스크립트로 사용자 지정된 스크립트 포함 작성 ▪ 해당 스크립트 포함 유틸리티를 사용하여 전달된 타임스탬프 및 요청 본문을 해석합니다. 인스턴스에서 생성된 모든 공유 암호에는 ServiceNow® 키 ID가 있습니다. 키 ID를 HMAC 인증 프로필의 기본 키 ID로 구성해야 합니다.



d. 기록을 제출합니다.

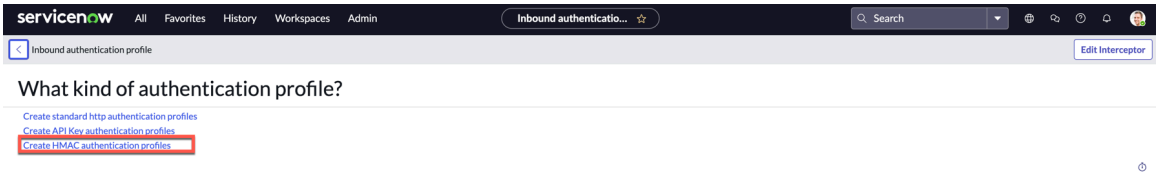
2. 인바운드 인증 프로파일을 생성합니다.

a. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > 인바운드 인증 프로파일.

b. 새로 만들기를 선택합니다.
`#### What kind of authentication profile(## ##### ##)###` 메시지가 표시됩니다.

c. HMAC 인증 프로필 만들기를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

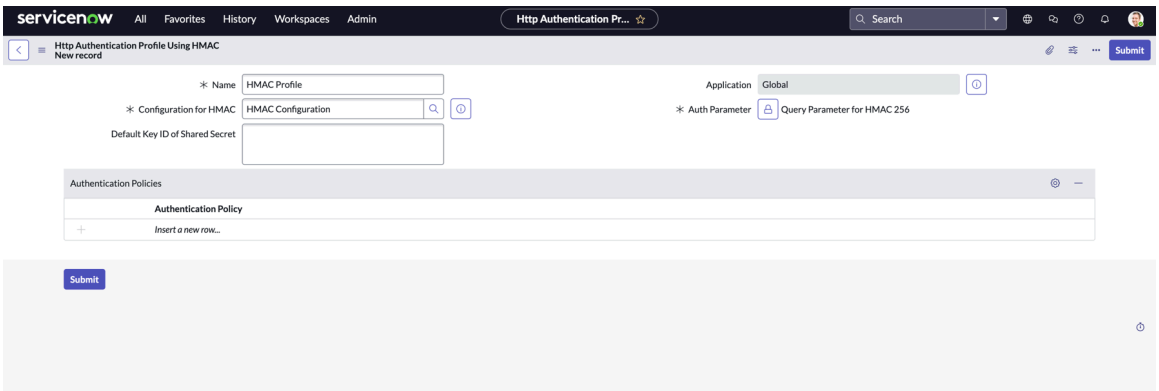


d. 양식의 필드에 내용을 입력합니다.

HMAC 인증 프로파일

필드	설명
이름	인증 정책을 식별하는 이름입니다.
애플리케이션	인증 정책의 범위입니다.
HMAC에 대한 구성	생성된 HMAC 구성을 선택합니다.
인증 매개변수	인증 요청에 대한 인증 매개변수를 선택합니다. 기본 옵션을 선택하거나 새 인증 매개변수를 생성할 수 있습니다. ▪ x-sn-hmac-signature-256: 인증 헤더 ▪ x-sn-hmac-signature-256: 쿼리 매개변수
공유 암호의 기본 키 ID	HMAC를 사용하기 위해 이 필드에서 업데이트할 수 있는 토큰 정보입니다.

주: 선택한 옵션은 REST 호출에서 인증 헤더 또는 쿼리 매개변수의 일부로 정의되어야 합니다.



e. 양식을 제출합니다.

3. HMAC 암호를 만듭니다.

a. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > **REST API HMAC** 암호.

b. 새로 만들기를 선택합니다.

c. 양식에서 필드에 다음을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

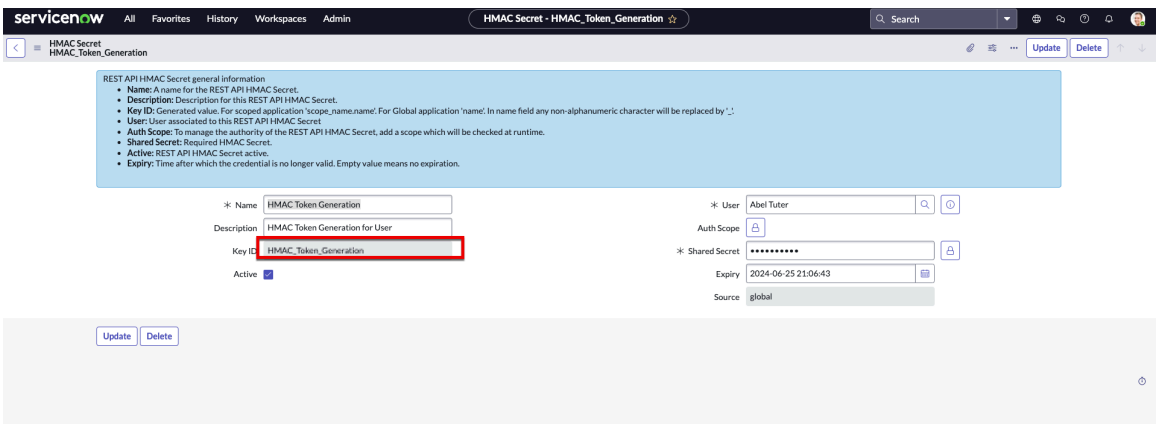
REST API HMAC 암호

필드	설명
이름	REST API HMAC 암호를 식별하는 이름입니다.
설명	REST API HMAC 암호에 대한 설명입니다.
활성	REST API HMAC 암호의 상태입니다.
사용자	REST API HMAC 암호와 연결된 사용자입니다. 조회 아이콘을 사용하여 사용자를 선택합니다.
키 ID	REST 호출의 일부로 보내야 하는 키 ID입니다. 양식을 제출한 후 키 ID가 생성됩니다.
공유 암호	사용자의 공유 암호입니다. 예를 들어 암호입니다.
소스	기록의 소스입니다.
만료	자격 증명이 더 이상 유효하지 않게 되는 시간입니다. 값이 비어 있으면 만료되지 않습니다. 주: 토큰 만료에 대한 자세한 내용은 다음 문서를 참조하십시오 토큰 만료 정리 중 .

d. 양식을 제출합니다.

e. 생성된 기록을 엽니다.

사용자에 Now Platform 대해 생성된 키 ID를 찾습니다.



주: API 호출에 대한 Auth 또는 Query 매개변수를 지정하지 않으려면 HMAC에 대해 작성된 인증 프로파일의 키 ID 중에 작성된 키 ID를 추가할 수 있습니다.

4. REST API 접근 정책을 생성합니다.

a. 다음으로 이동 모두 > 시스템 웹 서비스 > **REST API** 접근 정책.

b. 새로 만들기를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

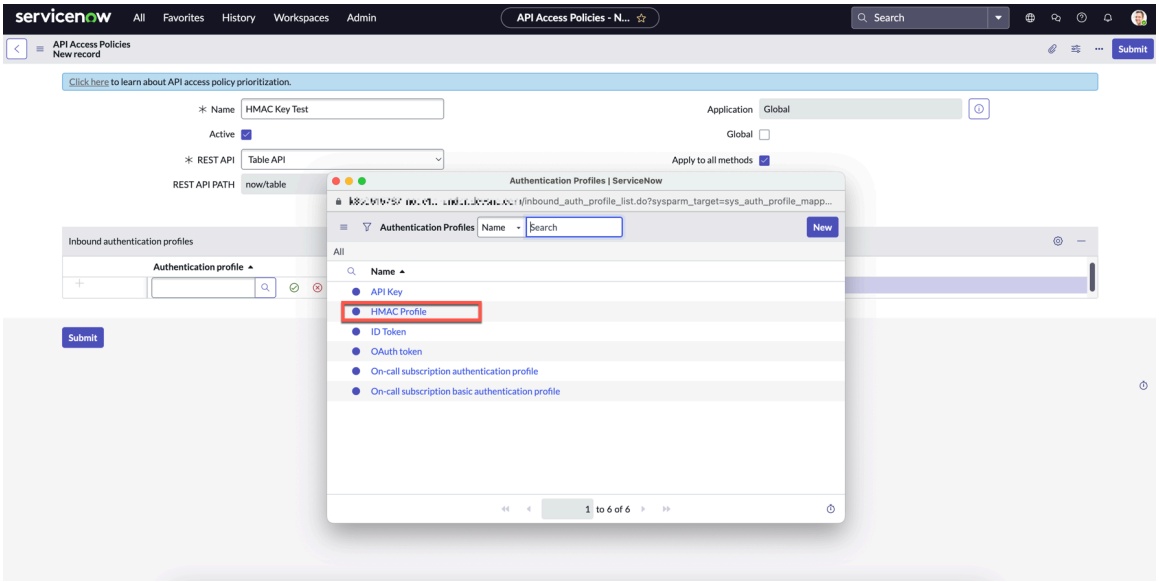
c. 양식의 필드에 내용을 입력합니다.

API 접근 정책

필드	설명
이름	API 접근 정책의 고유한 이름입니다.
활성	API 접근 정책을 활성화하는 옵션입니다.
REST API	액세스 정책이 적용되는 REST API입니다. 예를 들어 첨부 파일 **API**입니다.
REST API 경로	REST API의 API 경로입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 예: **now/attachment**.
HTTP 메서드	API와 상호작용하는 데 사용되는 메서드입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다.
버전	API의 버전입니다. 예: **v1**. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 주: REST API의 모든 버전에 대한 인증 정책을 만들려면 각 버전에 대해 개별 정책을 만들어야 합니다.
자원	REST API의 하위 자원입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 예: **/ now/attachment**
애플리케이션	애플리케이션의 범위입니다.
전역	API의 모든 메서드, 버전 및 자원에 인증 정책을 적용하려면 이 필드를 활성화합니다. 주: 전역 REST API 정책에서는 토큰 기반 인증을 사용할 수 없습니다.
모든 메서드에 적용	API에 대한 인증 정책을 API의 모든 메서드, 버전 및 자원에 적용하려면 이 필드를 활성화합니다.
모든 자원에 적용	API에 대한 인증 정책을 모든 버전에 적용하려면 이 필드를 활성화합니다.
모든 버전에 적용	API에 대한 인증 정책을 모든 자원에 적용하려면 이 필드를 활성화합니다.

d. 생성된 API 인증 프로파일을 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



e. 양식을 제출합니다.
REST API 호출을 보낼 수 있습니다.

- 인증 구성에 따라 헤더 또는 쿼리 매개변수 내에서 API 키를 생성하는 동안 생성된 ServiceNow® x-sn-hmac-signature-256을 사용합니다.
- 공유 비밀이 요청의 일부로 지정된 사전 요청 스크립트

⚠ 경고: 중요한 정보를 서버에 제출할 때 **POST** 요청을 사용합니다.

토큰 만료 정리 중

다양한 시스템 속성을 사용하여 토큰 만료를 정리하는 방법에 대한 상세 정보입니다.

API 키 또는 HMAC 암호가 만료되면 세부 정보는 7일 동안 보존됩니다. 예약된 작업: `### ## ## ## ## ##` 는 그 후 만료된 API 키 또는 HMAC 암호를 삭제합니다. 다음 속성을 사용하여 이 동작을 구성하고 삭제를 제어할 수 있습니다.

- **com.snc.platform.security.token.auth.cleanup**: 만료된 API 키 및 HMAC 토큰을 삭제하려면 이 속성을 사용합니다. 기본적으로 `true`입니다.
- **com.snc.platfrom.security.token.auth.days.expired.api_key.is.kept**: 요구 사항에 따라 값을 설정하여 만료된 `API` 토큰을 시스템에 보관할 일 수를 결정합니다. 기본적으로 7입니다.
- **com.snc.platfrom.security.token.auth.days.expired.hmac_key.is.kept**: 요구 사항에 따라 값을 설정하여 만료된 `HMAC` 토큰을 시스템에 보관할 일 수를 결정합니다. 기본적으로 7입니다.

토큰 만료 속성으로 이동하려면 탐색 모음에 `sys_properties.list` 를 입력한 후 다음 속성을 검색합니다. 요구 사항에 따라 만료를 변경합니다.

API 접근 정책

API 액세스 정책은 API에 대한 액세스 권한 및 기간을 정의합니다.

API 액세스 정책을 사용하면 액세스 정책의 인증 유형 및 지정된 필터 기준에 따라 인바운드 ServiceNow® API에 대한 액세스를 제한할 수 있습니다.

다음은 비대화형 세션에 대한 세 가지 수준의 인증 정책 지원입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- **REST API**: 관리자는 전역 API 인증 정책 또는 API 특정 인증 정책을 정의할 수 있습니다.
- **SOAP API**: 관리자는 전역 API 인증 정책 또는 API 특정 인증 정책을 정의할 수 있습니다.
- 시스템/내보내기 프로세서: 관리자는 프로세서 API 인증 정책 또는 프로세서별 인증 정책에 인증 프로필을 적용하는 데 사용할 수 있는 5개의 기본 시스템 인증 프로필을 정의할 수 있습니다.

주: 전역 인증 정책을 추가하는 경우 정책은 모든 REST API, SOAP API 또는 시스템/익스포트 프로세서에 적용됩니다.

다음은 API 정책 및 인증 범위에 대해 자동 설치된 플러그인입니다.

- com.glide.rest.policy
- com.glide.soap.policy
- com.glide.processor.policy
- com.glide.rest.auth.scope

기본 전역 차단 정책을 구성하거나 보안 요구 사항에 따라 사용자 지정 API 액세스 정책을 만들 수 있습니다. 그리고 인증 정책에 대한 정책 입력으로 사용되는 필터 조건 또는 쿼리가 포함된 필터 기준을 적용합니다.

에서 지원되는 API 접근 정책은 다음과 같습니다.ServiceNow®

- REST API 접근 정책
- SOAP API 접근 정책

내보내기 프로세서와 관련된 정책에 대한 자세한 내용은 다음 문서를 참조하십시오 시스템/익스포트 프로세서에 대한 접근 정책.

REST API 접근 정책

REST API 액세스 정책을 사용하면 액세스 정책의 인증 유형 및 지정된 필터 기준에 따라 인바운드 REST API에 대한 액세스를 제한할 수 있습니다.

RESTful API라고도 하는 REST API는 REST 아키텍처 스타일의 지침을 준수하는 애플리케이션 프로그래밍 인터페이스(API)의 유형입니다. REST API는 높은 수준의 유연성을 제공하여 웹 전반에 널리 사용됩니다.

필터 기준에는 인증 정책의 정책 입력으로 사용되는 필터 조건 또는 쿼리가 포함됩니다.

기본 전역 차단 정책을 구성하거나 보안 요구 사항에 따라 사용자 지정 API 액세스 정책을 만들 수 있습니다. 예를 들어 지정된 IP 주소 범위에서 OAuth 2.0 인증 유형만 허용하는 사용자 지정 API 액세스 정책을 만들 수 있습니다. 다른 인증 유형의 인증 요청 및 지정된 IP 주소 이외의 IP 주소에서의 액세스 요청은 거부됩니다.

REST API 접근 정책 활성화

관리자 역할이 있는 경우 REST API Access Policy 플러그인(com.glide.rest.policy)을 활성화할 수 있습니다. 애플리케이션은 데모 데이터를 포함하며 관련 ServiceNow® Store 애플리케이션 및 플러그인이 아직 설치되어 있지 않은 경우 이를 설치합니다.

시작하기 전에
필요한 역할: admin.

이 태스크 정보
REST API 접근 정책과 함께 다음 항목이 설치됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 플러그인: com.gilde.auth.profile, com.snc.adaptive_authentication, com.snc.platform.security.oauth
- 테이블: sys_api_access_policy, sys_auth_profile_mapping, auth_policy_mapping, inbound_auth_profile, std_http_auth.

자세한 내용은 적응형 인증 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 REST API Access Policy 플러그인(com.glide.rest.policy)을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

인증 프로파일 생성

인증 프로파일을 만들고 프로파일에 하나 이상의 인증 정책을 추가합니다. 기본적으로 사용할 수 있는 **ID** 토큰 및 **OAuth** 토큰 인증 프로파일을 구성할 수도 있습니다.

시작하기 전에

필요한 역할: 관리자

주: 상호 인증 및 사용자 지정 인증을 사용하여 인증 정책, IP 범위, 역할 기반, 사용자 기반 등을 적용할 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > 인바운드 인증 프로파일.
2. 새로 만들기를 선택합니다.
   시스템에 메시지가 표시됩니다. ## ### ## #######?
3. 표준 **http** 인증 프로필 만들기를 선택합니다.
4. 양식의 필드에 내용을 입력합니다.

   표준 인증 프로파일 양식

필드	설명
이름	인증 정책을 식별하는 이름입니다.
설명	인증 정책에 대한 설명입니다.
활성	인증 정책을 활성화하는 옵션입니다.
애플리케이션	인증 정책의 범위입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
유형	사용할 수 있는 인증의 유형입니다. 기본 인증, **ID** 토큰, 인증서 기반 인증 또는 **OAuth**를 선택할 수 있습니다.
OAuth 엔터티	OAuth 엔터티 프로파일. 이 필드는 유형에서 **ID** 토큰 또는 **OAuth**를 선택한 경우에만 나타납니다.

5. 새 행 삽입을 두 번 클릭합니다.
6. 목록에서 인증 정책을 선택하고 저장 아이콘을 선택합니다.

주: Allow Access Policy(액세스 정책 허용) 또는 Deny Access Policy(액세스 거부 정책)를 선택하지 마십시오. 이 정책은 사용자 로그인에만 적용됩니다.

인증 프로파일에 대해 하나 이상의 인증 정책을 추가할 수 있습니다.

주:

인증 헤더 [www-authenticate].

REST API 접근 정책이 활성 상태이면 인증 헤더에서 가장 최근에 매핑된 인증 프로파일을 반환합니다. 서버가 모든 인증 체계를 반환하도록 하려면 `glide.security.response.authenticate.header.auth_profile.first_scheme_only` 속성을 사용하고 **false**로 설정합니다. 응답은 여러 헤더와 함께 반환됩니다. 예:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

REST API 접근 정책 작성

API 액세스 정책을 생성하고 인증 프로파일을 매핑하여 REST API의 인증 유형을 제한합니다. 예를 들어 REST API에 대한 ID 토큰 인증만 허용하는 API 액세스 정책을 만들 수 있습니다.

시작하기 전에

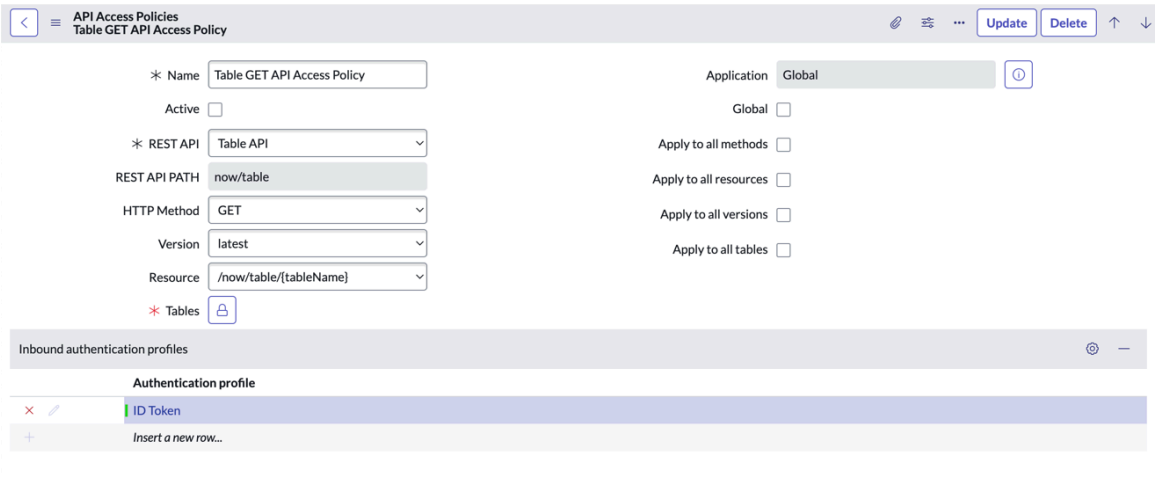
인증 프로파일이 생성되었는지 확인합니다. 자세한 내용은 인증 프로필 만들기를 참조하세요.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > **REST API** 접근 정책.
2. 새로 만들기를 선택합니다.
3. 양식의 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



API 접근 정책

필드	설명
이름	API 접근 정책의 고유한 이름입니다.
활성	API 접근 정책을 활성화하는 옵션입니다.
REST API	액세스 정책이 적용되는 REST API입니다. 예를 들어 첨부 파일 **API**입니다.
REST API 경로	REST API의 API 경로입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 예: **now/attachment**.
HTTP 메서드	API와 상호작용하는 데 사용되는 메서드입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다.
버전	API의 버전입니다. 예: **v1**. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 주: REST API의 모든 버전에 대한 인증 정책을 만들려면 각 버전에 대해 개별 정책을 만들어야 합니다.
자원	REST API의 하위 자원입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 예: **/ now/attachment**
테이블	API 접근 정책이 적용되는 테이블입니다. 이 옵션은 *Table* API에 대한 정책에만 적용됩니다.
애플리케이션	애플리케이션의 범위입니다.
전역	API의 모든 메서드, 버전 및 자원에 정책을 적용하는 옵션입니다.
모든 메서드에 적용	API의 모든 메서드, 버전 및 자원에 정책을 적용하는 옵션입니다.
모든 자원에 적용	모든 또는 API 자원에 정책을 적용하는 옵션입니다.
모든 버전에 적용	모든 버전 또는 API 버전에 정책을 적용하는 옵션입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

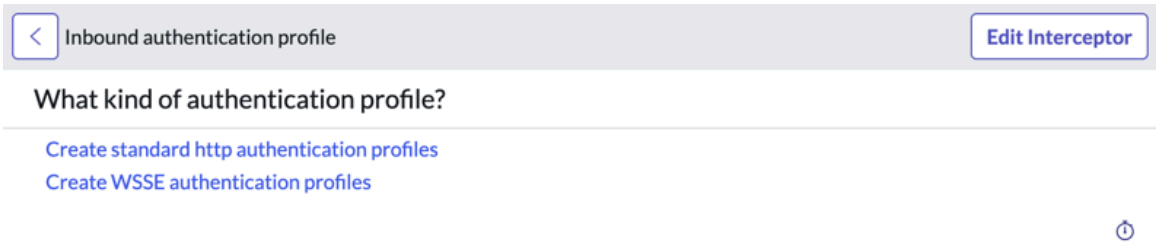
필드	설명
모든 테이블에 적용	모든 테이블에 정책을 적용하는 옵션입니다. 이 옵션은 *Table* API에 대한 정책에만 적용됩니다.

주: API 액세스 정책 우선순위 지정에 대한 자세한 내용은 다음 문서를 API 접근 정책 우선순위 지정참조하십시오.

4. 새 행 삽입을 두 번 클릭합니다.
5. 목록에서 인바운드 인증 프로파일을 선택하고 저장 아이콘 선택합니다.
   예를 들어 기본 인증, **ID** 토큰, 인증서 기반 인증, **OAuth** 또는 **WSSE** 인증을 추가할 수 있습니다.

   a. 하나 이상의 인바운드 인증 프로파일을 추가하려면 새로 만들기를 선택하여 새 프로파일을 만듭니다.

   b. **Choose What Kind of authentication** profiles(인증 프로파일의 종류를 선택하십시오)?.
      - 표준 **http** 인증 프로파일 작성
      - **WSSE** 인증 프로필 작성



   c. 인증 프로파일을 생성한 후 기록을 저장합니다.

6. 제출을 선택하여 REST API 액세스 정책을 제출합니다.

API 접근 정책 우선순위 지정

인스턴스에 여러 API 액세스 정책이 구성되어 ServiceNow® 있는 경우 정책 우선순위 지정 논리에 대해 알아봅니다.

API 접근 정책은 인스턴스에 설정된 REST API 정책의 유형에 따라 우선순위가 ServiceNow® 지정됩니다.

이 접근 방식은 메서드, 리소스 및 버전과 같은 API의 각 부분에 대해 서로 다른 가중치를 정의합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

API 정책은 비전역에 대해 우선 순위가 지정되고 그 다음으로 전역에 우선합니다. 즉, 비전역 액세스 정책은 항상 전역 API 액세스 정책을 재정의합니다.

우선순위 지정 논리는 다음과 같습니다.

우선순위 지정

필드	우선순위	우선순위 지정 논리
메서드, 자원 및 버전	1	3개의 필드가 정책과 일치하면 해당 정책이 첫 번째 우선순위를 갖습니다.
메서드+ 자원	2	2개의 필드가 정책과 일치하면 해당 정책이 첫 번째 우선순위를 갖습니다.
리소스 + 버전	3	모든 메서드에 적용 필드가 있는 2개의 필드가 정책과 일치하면 해당 정책이 3번째 우선순위를 갖습니다.
자원	4	필드가 모든 메서드에 적용 정책과 일치하면 해당 정책이 4번째 우선순위를 갖습니다.
메서드 + 버전	5	필드 2개와 모든 자원에 적용 필드가 정책과 일치하면 해당 정책이 5번째 우선순위를 갖습니다.
메서드	6	필드가 '모든 자원에 적용' 필드와 정책과 일치하면 해당 정책이 5번째 우선순위를 갖습니다.
버전	7	필드가 모든 메서드에 적용 및 모든 버전에 적용 필드가 정책과 일치하면 해당 정책이 7번째 우선순위를 갖습니다.
전역 및 모든 메서드에 적용	8	전역 필드가 `true`이고 모든 메서드에 적용이 `false`이면 해당 정책이 8번째 우선순위를 갖습니다.
전역 및 모든 메서드에 적용	9	전역 필드가 `True`이고 모든 메서드에 적용이 `True`이면 해당 정책의 우선순위는 9번째입니다.

REST API 인증 범위

REST API에 대한 인증 범위 지원.

이전에는 모든 액세스 토큰 또는 OIDC 토큰이 사용자의 REST API에 대한 모든 권한이 있는 `### ##` 범위와 연결되었습니다. 릴리스부터 Yokohama 특정 REST API에 대한 액세스만 제공하기 위해 **REST API** 인증 범위가 도입되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

REST API 인증 범위 기록을 생성한 후 이 REST API에 액세스하려면 이 REST API에 대한 액세스 권한이 있어야 하는 OAuth 엔터티에 동일한 인증 범위를 연결해야 합니다. 새 OAuth 엔터티의 경우 기본 인증 범위가 비어 있습니다.

주: REST API 인증 범위 기록이 없으면 유효한 모든 OAuth 엔터티에서 REST API에 액세스할 수 있습니다.

OAuth 엔터티 내에서 인증 범위를 수동으로 연결해야 합니다. `### ###` 특수 범위로, OAuth 엔터티와 연결된 경우 다른 인증 범위로 REST API 인증 범위 기록을 생성했더라도 모든 API에 액세스할 수 있습니다.

주:

- REST API 인증 범위가 활성화되고 REST API의 인증 범위에 추가된 후에는 관리자가 해당 OAuth 엔터티에 이 인증 범위를 추가하지 않는 한 기존의 모든 OAuth 토큰이 더 이상 이 API에 액세스할 수 없습니다
- 관리자는 인증 범위를 REST API와 연결한 후 oauth_entity에 올바른 인증 범위가 있는지 확인해야 합니다.
- 에서 ServiceNow 발급한 OAuth 액세스 토큰은 인증 범위를 지원합니다.
- 에서 ServiceNow 발급하지 않은 OIDC 토큰은 에서 ServiceNow유효성을 검사합니다.
- ID 토큰이 필요한 경우 OIDC 토큰의 범위는 IDP입니다. 여기서 인증 범위는 외부 공급업체(IdP)가 아닌 대상입니다 ServiceNow .

REST API 범위에 대한 구성

REST API 범위를 구성하려면 다음 작업을 수행합니다.

- 인증 범위 생성
- REST API와 인증 범위 연결
- OAuth 엔터티와 인증 범위 연결
- OAuth 플로우를 수행하여 OAuth 액세스 토큰 가져오기
- OAuth 액세스 토큰을 사용하여 API 호출

REST API 인증 범위 활성화

REST API Auth Scope 플러그인(com.glide.rest.auth.scope)을 활성화하여 OAuth 엔터티를 인증 범위와 연결할 수 있습니다.

시작하기 전에
다음 플러그인을 설치합니다.

- OAuth 2.0
- REST API 제공자
- 인증 범위
- REST API 범위

주: 플러그인은 *REST API Scope* 릴리스의 Tokyo 일부로 추가됩니다.

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 REST API 인증 범위(*com.glide.rest.auth.scope*) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.

3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

REST API 인증 범위 속성 및 테이블

REST API Auth Scope 플러그인(com.glide.rest.auth.scope)에는 다음과 같은 시스템 속성, 테이블 및 스크립트가 포함됩니다.

REST API 인증 범위 속성

REST API 인증 범위는 다음 시스템 속성을 추가합니다.

속성

이름	설명
com.glide.rest.api.auth.scope.check.enabled	이 속성은 플랫폼 수준 인증 범위 검사를 해제하는 데 사용됩니다. false로 설정하면 런타임 중에 RETS API와 연결되어 있는지 여부에 관계없이 인증 범위 검사를 건너뜁니다. 기본적으로 이 속성은 true로 설정됩니다. 이 속성은 이전 릴리스 동작으로 되돌리려는 경우에 사용됩니다.
com.glide.oauth.token.scope.useraccount	이 속성은 인증 범위가 삭제되고 최종 사용자가 수동으로 다시 추가할 때만 *useraccount* 사용됩니다. 이 경우 의 *useraccount* 시스템 ID가 변경됩니다. 이 속성을 새 sys_id로 업데이트해야 합니다. 런타임 중에는 인증 범위 이름 대신 인증 범위 시스템 ID가 사용됩니다.

REST API 인증 범위 테이블

REST API 인증 범위는 다음 테이블입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

테이블

이름	설명
인증 범위(sys_auth_scope)	이 테이블은 REST API 및 OAuth 엔터티와 연결할 수 있는 인증 범위를 정의합니다. 인증 범위 이름은 고유해야 하며 전역입니다.
REST API 인증 범위(sys_api_access_scope)	이 테이블은 REST API를 인증 범위와 연결합니다.

REST API 인증 범위 구성

OAuth 엔터티를 인증 범위와 연결하여 인증 범위와 연결된 REST API에 액세스하기 위한 토큰을 관리합니다.

시작하기 전에
다음 플러그인을 설치합니다.

- OAuth 2.0
- REST API 제공자
- 인증 범위
- REST API 인증 범위

주: 플러그인은 *REST API Auth Scope* 릴리스의 Tokyo 일부로 추가됩니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > **API** 인증 범위 > **REST API** 인증 범위.
   REST API 인증 범위 페이지가 표시됩니다.
2. 새 REST API 인증 범위를 구성하려면 신규를 클릭하십시오.
3. 양식의 필드에 내용을 입력합니다.

REST API 인증 범위

이름	REST API 인증 범위를 식별하는 고유 이름입니다.
활성	구성을 활성화하려면 확인란을 선택합니다.
애플리케이션	읽기 전용 애플리케이션 범위입니다.
REST API	인증 범위가 적용되는 REST API입니다. 예를 들어 테이블 API입니다.
인증 범위	조회 아이콘에서 인증 범위를 선택합니다.
REST API 경로	REST API의 API 경로입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 예: now/table
HTTP 메서드	API와 상호작용하는 데 사용되는 메서드입니다. 드롭다운 목록에서 방법을 선택합니다.

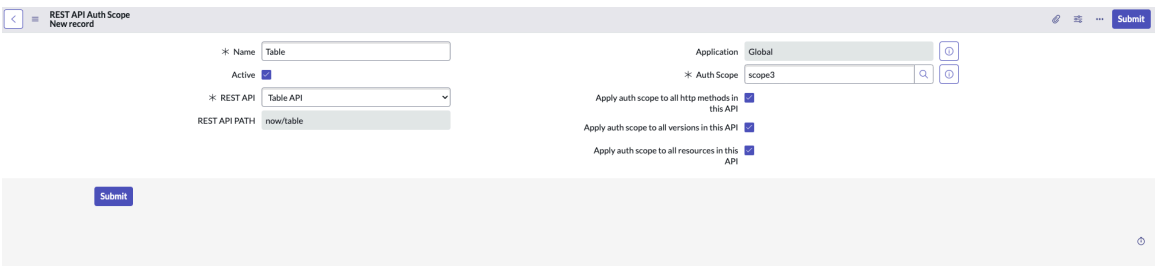
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

	양식에서 이 **API** 필드의 모든 **http** 메서드에 인증 범위 적용을 수동으로 비활성화하여 메서드를 선택할 수 있습니다.
REST API 버전	API의 버전입니다. 예: v1. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 양식에서 이 API의 모든 버전에 인증 범위 적용 필드를 수동으로 비활성화하여 버전을 선택할 수 있습니다.
자원	REST API의 하위 자원입니다. 이 필드는 선택한 REST API에 따라 자동으로 채워집니다. 예: /now/table. 양식에서 이 API의 모든 자원에 인증 범위 적용 필드를 수동으로 비활성화하여 자원을 선택할 수 있습니다.
이 API의 모든 http 메서드에 인증 범위 적용	활성화되면 API의 모든 http 메서드에 인증 범위를 적용합니다.
이 API의 모든 버전에 인증 범위 적용	hen이 활성화되면 API의 모든 버전에 인증 범위가 적용됩니다.
이 API의 모든 자원에 인증 범위 적용	사용하도록 설정하면 API의 모든 자원에 인증 범위가 적용됩니다.

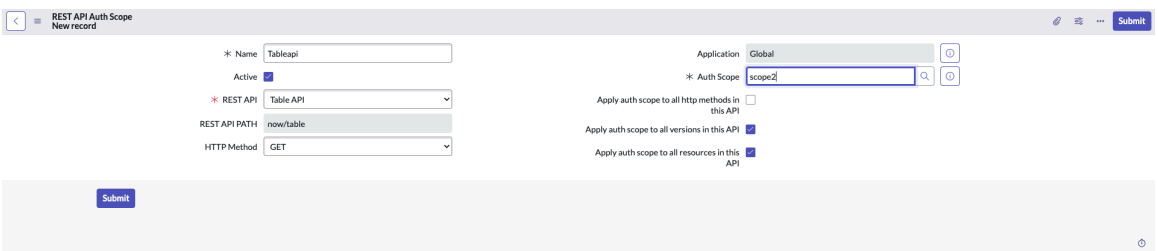
4. 제출을 클릭합니다.
   API는 선택한 REST API 및 인증 범위에 따라 범위에 해당하는 정보를 검색합니다.

Example: 테이블 API에 대해 3개의 **REST API** 인증 범위를 생성하는 것이 좋습니다.

첫 번째 인증 범위는 모든 http 메서드, 버전 및 리소스가 활성화된 테이블 **API** 에 매핑됩니다.

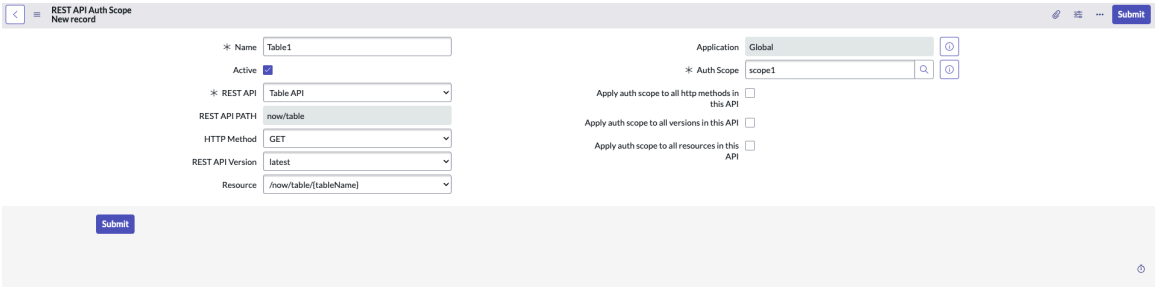


두 번째 인증 범위는 모든 버전과 자원이 활성화된 테이블 **API** 에 매핑됩니다. 그러나 HTTP 메서드(이 예제에서는 **GET** 메서드)를 선택합니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

세 번째 인증 범위는 http 메서드, 버전 및 리소스가 활성화되지 않은 테이블 **API** 에 매핑됩니다. 그러나 HTTP 메서드, 버전 및 리소스를 수동으로 선택합니다. 이 예에서 HTTP 메서드는 **GET**이고, REST API 버전은 최신이고, 리소스는 `/now/table/{tableName}`입니다.



이러한 인증 범위가 모두 생성되면 세 가지 범위 모두에서 **GET** 메서드를 사용할 수 있지만 **POST**,**PUT**, **DELETE** 또는 **PATCH** 메서드의 경우 **scope3** 만 사용할 수 있습니다.

REST API 범위 문제 해결

문제 해결 작업은 REST API 범위를 설정하거나 실행할 때 발생하는 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

문제 해결

문제	동작
REST API는 인증 범위와 연결되어 있지만 런타임에는 전달자 토큰 인증을 사용해도 인증 범위 검사가 없습니다.	• sys_api_access_policy 기록이 활성 상태인지 확인합니다. 런타임은 비활성 기록을 무시합니다. • 속성이 *com.glide.rest.api.auth.scope.check.enable* 아니오로 설정되어 있는지 확인하십시오. • OAuth 토큰에 `### ##` 인증 범위가 있는지 확인합니다.
REST API는 와 연결되어 *auth_scope1*있지만 액세스 *auth_scope2* 토큰도 액세스할 수 있습니다.	• 이 기록이 활성 상태인지 확인합니다. • 이 REST를 검사하고 API는 동일하지만 적용 방법, 버전 또는 자원이 다른 다른 기록이 있는지 확인합니다.
REST API는 인증 범위와 연결되지만 런타임에는 및 *mutualAuth*에 대한 *basicAuth* 인증 범위 검사가 없습니다.	REST API 인증 범위는 OAuth 액세스 토큰 또는 OIDC 토큰에만 적용되므로 예상됩니다. BasicAuth, 세션 쿠키 및 인증서 기반 인증은 적용되지 않습니다.
OAuth 액세스 토큰을 사용하는 경우 REST API 호출이 403을 반환합니다.	"필요한 API 액세스 범위 누락"이라는 오류 메시지를 확인합니다. 발견되면 이 REST API에 대한 인증 범위 검사가 실패합니다.
미리 정의된 `### ###` 삭제되었으며 복원이 확실하지 않습니다.	`## ###### ### ###xml`로 익스포트하여 임포트하거나 `### ###` 생성하고 시스템 속성을 *glide.oauth.token.scope.useraccount* 새로 만든 sys_id 기록으로 수정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자주 묻는 질문

다음은 REST API 인증 범위를 사용할 때 자주 묻는 질문입니다.

하나의 OAuth 토큰을 여러 인증 범위와 연결할 수 있습니까?

예, 하나의 `oauth_entity` 여러 인증 범위와 연결할 수 있으며 이 `oauth_entity` 에서 발급한 모든 OAuth 토큰에는 동일한 인증 범위가 있습니다.

인증 범위가 다른 다른 OAuth 토큰이 동일한 REST API에 액세스할 수 있나요?

예, 동일한 REST API의 경우 다른 인증 범위에서 액세스할 수 있습니다. 하나의 인증 범위가 일치하는 한 인증 범위는 결과를 반환합니다.

`### ##` 인증 범위가 있는 OAuth 액세스 토큰이 REST API에 액세스할 수 있습니까?

예, `### ##` 에는 인증 범위에 대한 전체 액세스 권한이 있습니다.

OAuth 액세스 토큰 OAuth 범위를 동적으로 변경할 수 있습니까?

예. 인증 범위가 `oauth_credential` 테이블에서 액세스 토큰으로 하드 코딩되지 않습니다. 대신 런타임 중에 연결된 `oauth_entity` 에서 인증 범위를 가져옵니다.

OAuth 토큰은 새로 고침 후 동일한 인증 범위를 유지할 수 있나요?

예, oauth_entity와 연결된 인증 범위를 수정 `##` 않는 한 토큰 새로 고침 후 인증 범위가 변경되지 `oauth_admin`.

미리 정의된 `### ##` 인증 범위 기록이 삭제됩니다. `### ##` 이름의 새 인증 범위를 만들 수 있습니까?

동일한 `### ####` 새 인증 범위를 만들 수 없습니다. 런타임에서 이름 대신 `sys_id` 를 사용하여 인증 범위 검사를 수행하고 시스템 속성을 *`glide.oauth.token.scope.useraccount`* 새로 만든 `sys_id` 기록으로 수정합니다.

관리자가 `oauth_entity`와 연결된 인증 범위를 수정하면 이 OAuth 엔터티에서 발급한 기존 OAuth 액세스 토큰도 모두 변경됩니까?

예, 인증 범위는 OAuth 액세스 토큰과 직접 연결되지 않으며 런타임 중에 `oauth_entity` 에서 가져옵니다.

동일한 `oauth_entity` 에서 발급한 다른 OAuth 액세스 토큰의 인증 범위가 다를 수 있습니까?

아니요, 토큰에 대한 모든 액세스는 동일한 `oauth_entity` 에서 발급되며 항상 동일한 인증 범위를 갖습니다.

사용자가 특정 엔드포인트에 대해 다른 인증 범위를 정의할 수 있습니까?

아니요, 특정 REST API 엔드포인트에 대한 고유한 제한 검사가 있습니다. 그러나 동일한 REST API 엔드포인트의 경우 일치하는 인증 범위가 두 개 이상 있을 수 있습니다.

인증 범위 검사는 BasicAuth에도 사용됩니까?

아니요, 인증 범위 검사는 OAuth 접근 토큰 및 OIDC 토큰일 뿐이며 *`basicAuthmutualAuth`*

SOAP API 접근 정책

SOAP API 액세스 정책을 사용하면 액세스 정책의 인증 유형 및 지정된 필터 기준에 따라 인바운드 SOAP API에 대한 액세스를 제한할 수 있습니다.

SOAP API 액세스 정책을 사용하면 인바운드 SOAP 및 스크립트된 SOAP API에 인바운드 인증 프로파일 및 API 액세스 정책을 적용할 수 있습니다.

IP 범위 및 역할 기반 제한과 같은 API 액세스 정책을 활용하여 ServiceNow 인증을 기반으로 인바운드 SOAP API 호출을 허용하거나 허용하지 않을 수 있습니다.

관리자는 다음 작업을 수행하여 정책을 적용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- SOAP API 접근 정책 및 인증 프로파일 플러그인을 활성화합니다. 자세한 내용은 SOAP API 접근 정책 활성화 문서를 참조하십시오.
- SOAP API 접근 정책을 생성하고 해당 정책을 인증 프로파일과 연결합니다. 자세한 내용은 SOAP API 접근 정책 작성 및 인증 프로파일 생성 문서를 참조하십시오.

  주: 정책은 SOAP 테이블 API 또는 스크립트된 SOAP API에 적용할 수 있습니다. 표준 `http` 및 `WSSE` 인증 프로필 외에.

- IP 범위, 역할 기반 제한과 같은 인증 정책을 생성하고 이 정책을 인증 프로파일에 연결합니다. 자세한 내용은 API 인증 정책 만들기 문서를 참조하십시오.

SOAP API 접근 정책 활성화

SOAP API 액세스 정책의 경우 SOAP API 액세스 정책(`com.glide.soap.policy`) 플러그인을 설치합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
다음 항목이 SOAP API Access Policy 플러그인과 함께 설치됩니다. 프로세서 액세스 정책 (`com.glide.processor.policy`)

종속 플러그인: 인증 프로필(`com.glide.auth.profile`)

프로시저
1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 SOAP API Access Policy 플러그인 (`com.glide.soap.policy`)을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

인증 프로파일 생성

인증 프로파일을 만들고 프로파일에 하나 이상의 인증 정책을 추가합니다. 기본적으로 사용할 수 있는 **ID** 토큰 및 **OAuth** 토큰 인증 프로파일을 구성할 수도 있습니다.

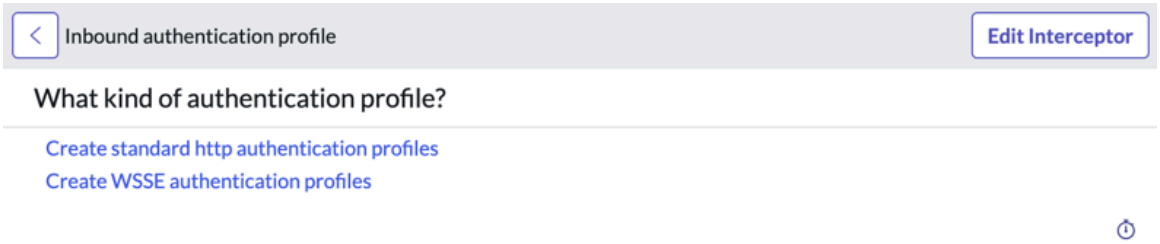
시작하기 전에
필요한 역할: 관리자

주: 상호 인증 및 사용자 지정 인증을 사용하여 인증 정책, IP 범위, 역할 기반, 사용자 기반 등을 적용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > 인바운드 인증 프로파일.
2. 새로 만들기를 선택합니다.
   시스템에 메시지가 표시됩니다. ## ### ## #######?
3. **Choose What Kind of authentication** profiles(인증 프로파일의 종류를 선택하십시오)?.
   - 표준 **http** 인증 프로파일 작성
   - **WSSE** 인증 프로필 작성



4. 양식의 필드에 내용을 입력합니다.

표준 인증 프로파일 양식

필드	설명
이름	인증 정책을 식별하는 이름입니다.
설명	인증 정책에 대한 설명입니다.
활성	인증 정책을 활성화하는 옵션입니다.
애플리케이션	인증 정책의 범위입니다.
유형	사용할 수 있는 인증의 유형입니다. 기본 인증, **ID** 토큰, 인증서 기반 인증, **OAuth** 또는 **WSSE**(WSSE 인증 프로파일의 경우)를 선택할 수 있습니다.
OAuth 엔터티	OAuth 엔터티 프로파일. 이 필드는 유형에서 **ID** 토큰 또는 **OAuth**를 선택한 경우에만 나타납니다.

5. 새 행 삽입을 두 번 클릭합니다.
6. 목록에서 인증 정책을 선택하고 저장 아이콘 을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: **Allow Access** Policy(액세스 정책 허용) 또는 **Deny Access** Policy(액세스 거부 정책)를 선택하지 마십시오. 이 정책은 사용자 로그인에만 적용됩니다.

인증 프로파일에 대해 하나 이상의 인증 정책을 추가할 수 있습니다.

인증 프로필이 변경되면 권한 부여 헤더는 해당 시점의 변경 내용과 관련된 값을 반환합니다. "WWW-Authenticate" 헤더에 반환된 모든 인증 체계를 가져오려면 `glide.security.response.authenticate.header.auth_profile.first_scheme_only`를 **false**로 활성화해야 합니다. 응답은 여러 헤더와 함께 반환됩니다. 예:

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

SOAP API 접근 정책 작성

API 액세스 정책을 생성하고 인증 프로파일을 매핑하여 SOAP API의 인증 유형을 제한합니다. 예를 들어 SOAP API에 대한 ID 토큰 인증만 허용하는 API 액세스 정책을 만들 수 있습니다.

시작하기 전에

- 인증 프로파일이 생성되었는지 확인합니다. 자세한 내용은 인증 프로필 만들기를 참조하세요.
- 필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > **SOAP API** 접근 정책.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

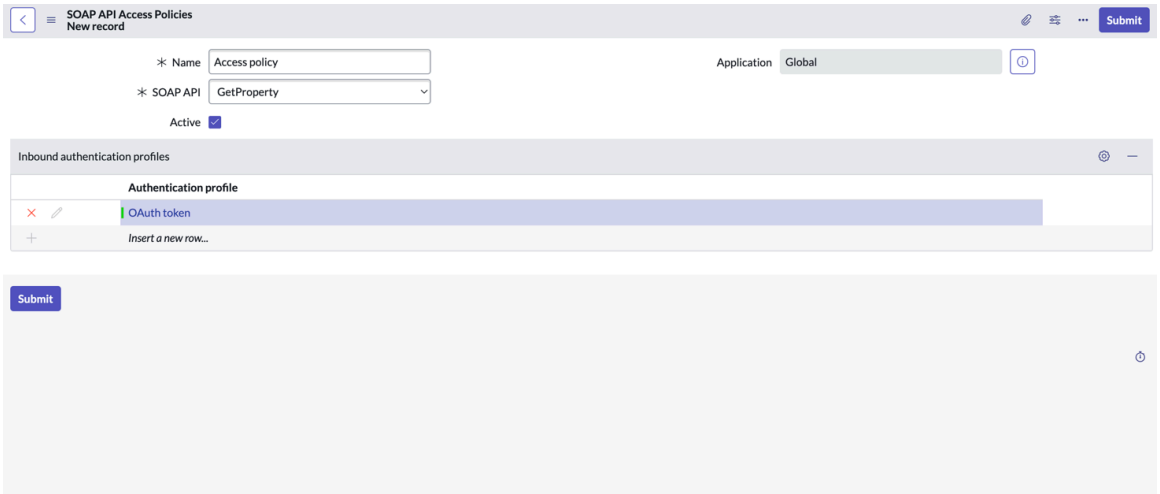
API 접근 정책 양식

필드	설명
이름	API 접근 정책의 고유한 이름입니다.
SOAP API	액세스 정책이 적용되는 SOAP API입니다. 예를 들어 **GetProperty API**입니다.
애플리케이션	애플리케이션의 범위입니다.
활성	API 접근 정책을 활성화하는 옵션입니다.

4. 인바운드 인증 섹션에서 새 행 삽입을 두 번 클릭합니다.
5. 목록에서 인바운드 인증 프로파일을 선택하고 저장 아이콘 저장 을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

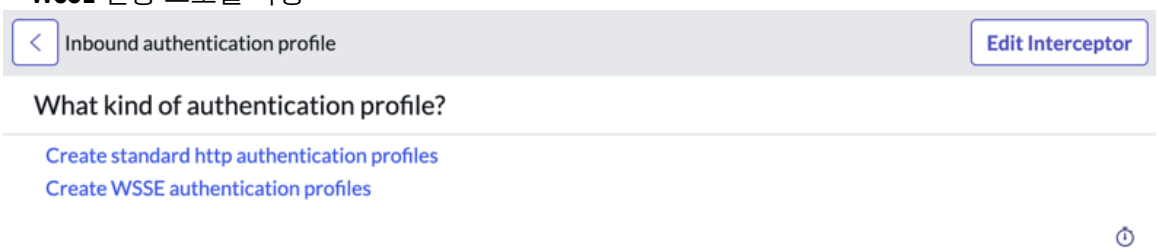
예를 들어 기본 인증, **ID** 토큰, 인증서 기반 인증, **OAuth** 또는 **WSSE** 인증을 추가할 수 있습니다.



a. 하나 이상의 인바운드 인증 프로파일을 추가하려면 새로 만들기를 클릭하여 새 프로파일을 만듭니다.

b. Choose What Kind of authentication profiles(인증 프로파일의 종류를 선택하십시오)?.

- 표준 **http** 인증 프로파일 작성
- **WSSE** 인증 프로필 작성



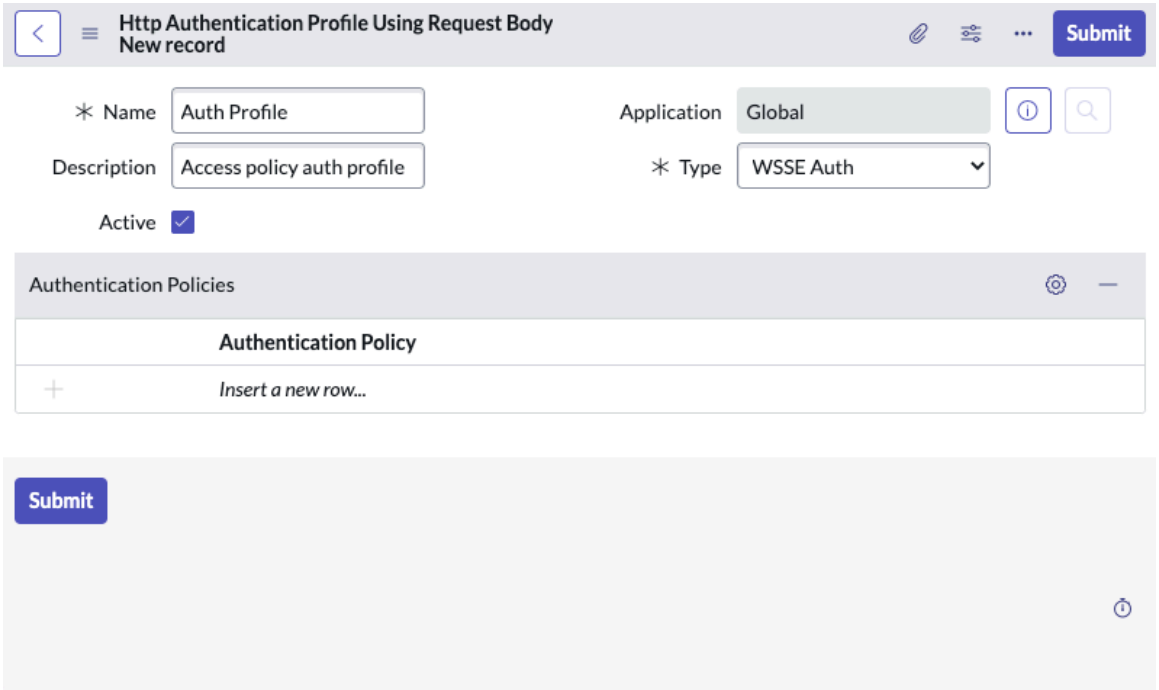
c. WSSE 인증 프로파일을 만들려면 양식의 필드에 내용을 입력합니다.

WSSE 인증 프로파일

필드	설명
이름	API 접근 정책의 고유한 이름입니다.
설명	인증 프로파일에 대한 설명입니다.
애플리케이션	애플리케이션의 범위입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	API 접근 정책을 활성화하는 옵션입니다.
유형	인증 프로파일로서의 WSSE Auth WSSE(웹 보안).



d. 인증 프로파일을 생성한 후 기록을 저장합니다.

6. 제출을 클릭하여 SOAP API 접근 정책을 제출합니다.

SOAP API를 보호하기 위한 전역 **API** 액세스 정책 생성

단일 전역 API 액세스 정책을 생성하여 모든 SOAP API를 보호합니다.

시작하기 전에

- 필요한 역할: 관리자
- 프로세서 액세스 정책(`com.glide.processor.policy`) 플러그인 설치
- 인증 프로파일이 생성되었는지 확인합니다. 자세한 내용은 인증 프로필 만들기를 참조하세요.

다음 단계에서는 모든 SOAP API를 보호하기 위해 단일 전역 액세스 정책을 만드는 방법을 설명합니다.

주: 개별 SOAP API 레벨에서 정의된 정책은 **SOAPProcessor** 레벨 전역 액세스 정책을 오버라이드합니다.

프로시저

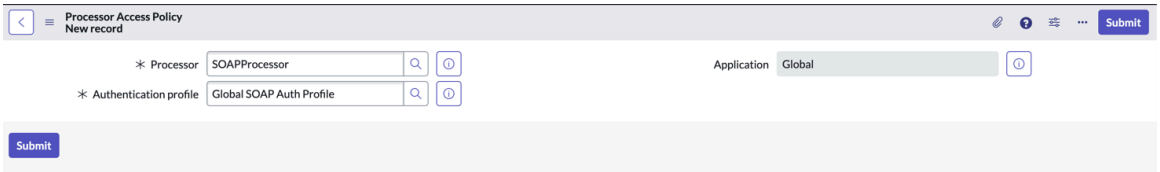
1. 다음으로 이동 모두 > 시스템 보안 > 프로세스 접근 정책.

2. 양식의 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로세스 접근 정책 양식

필드	설명
프로세서	인증 정책을 식별하는 이름입니다. 예를 들어, **SOAPProcessor** (인증 프로파일)를 선택합니다.
애플리케이션	인증 정책의 범위입니다. 기본값: 전역
인증 프로파일	인증 프로파일의 유형입니다. 전역 **SOAP** 인증 프로파일을 선택합니다.



3. 제출을 선택합니다.

API에 대한 필터 기준

필터 기준에는 인증 정책의 정책 입력으로 사용되는 필터 조건 또는 쿼리가 포함됩니다. 정책 입력은 하나 이상의 필터 기준을 그룹화하고 인증 정책의 정책 조건을 정의하는 데 사용됩니다. 예를 들어, IP 필터 기준은 CIDR(Classless Inter-Domain Routing) 형식 또는 IP 주소 범위의 IP 주소를 정의합니다.

사용자의 IP 주소, 역할 및 사용자가 속한 사용자 그룹을 기반으로 필터 기준을 만들 수 있습니다.

주: 적응형 인증 모듈에서 만든 필터 기준도 사용합니다. 자세한 내용은 적응형 인증 문서를 참조하십시오.

적응형 인증에 대한 필터 기준과 동일한 프로세스를 사용하여 API에 대한 필터 기준을 만들 수 있습니다. 자세한 내용은 필터 기준 문서를 참조하십시오.

관련 정보

- IP 필터 기준 생성
- 역할 필터 기준 생성
- 그룹 필터 기준 생성

API 인증 정책

인증 정책은 지정된 정책 조건에 따라 인증 요청을 평가하고 일치 기준에 따라 액세스를 허용하거나 거부합니다.

기본 제공 전역 차단 정책을 사용하거나 보안 요구 사항에 따라 인증 정책을 만들 수 있습니다. 전역 차단 정책은 지정된 필터 기준에 따라 사용자 및 API의 인증 요청을 거부합니다.

주: 액세스 허용 정책 및 액세스 거부 정책을 사용하거나 수정하지 마십시오. 이 정책은 사용자 로그인에만 적용됩니다.

API 인증 정책 만들기

인증 정책을 사용하면 지정된 필터 기준에 따라 API에 액세스 제한을 적용할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

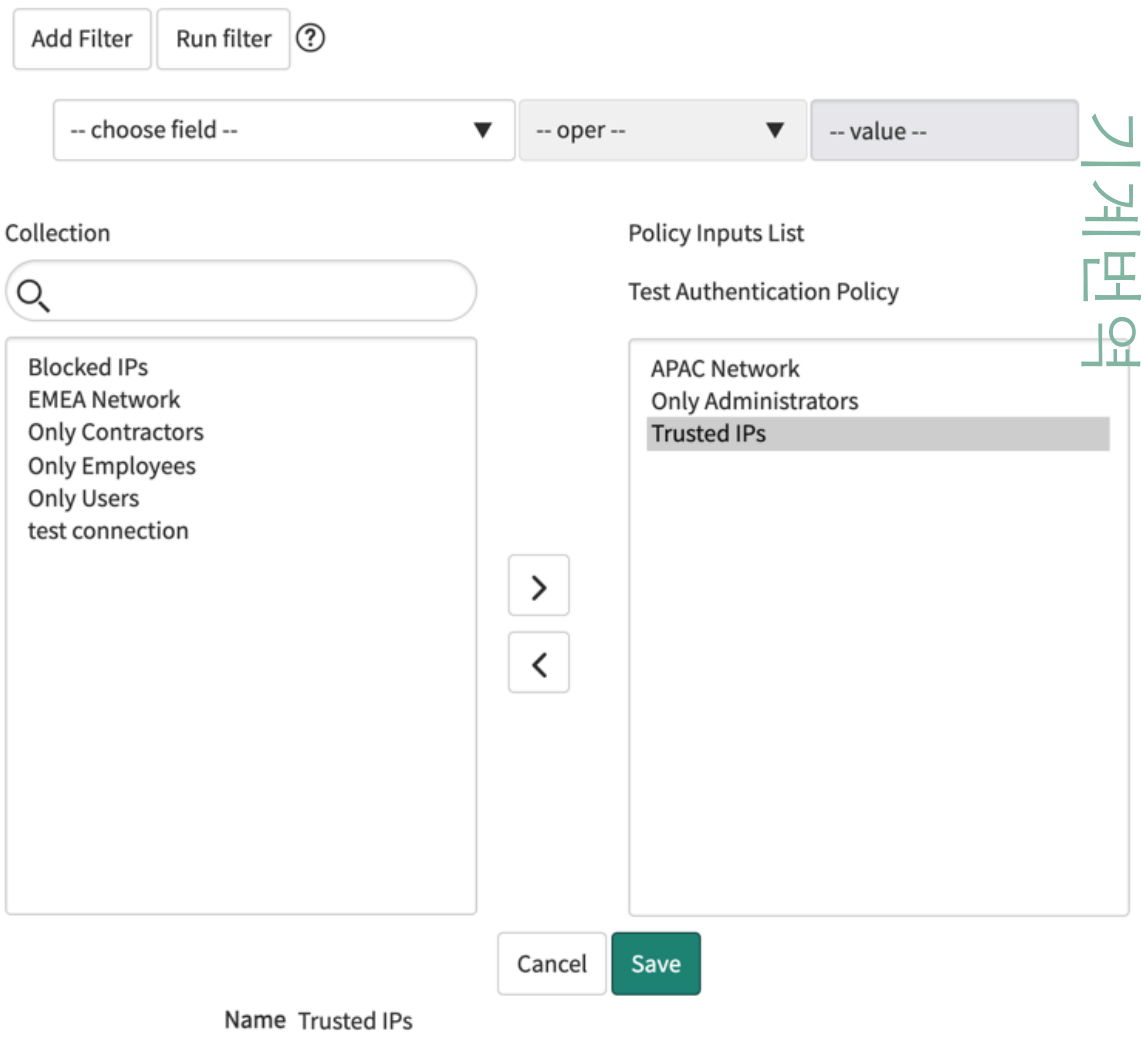
프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 인증 정책.
2. 새로 만들기를 클릭합니다.
3. 양식에서 다음과 같은 필드를 채웁니다.

정책 양식

필드	설명
이름	정책을 식별하기 위한 이름입니다.
설명	정책에 대한 간단한 설명입니다.
애플리케이션	애플리케이션의 범위입니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.
5. 정책 입력 탭에서 편집을 선택하여 기존 필터 기준을 추가합니다.
   새 정책 입력을 만들 수도 있습니다. 자세한 내용은 정책 입력 만들기를 참조하세요.
6. 하나 이상의 필터 기준을 컬렉션 목록에서 정책 입력 목록으로



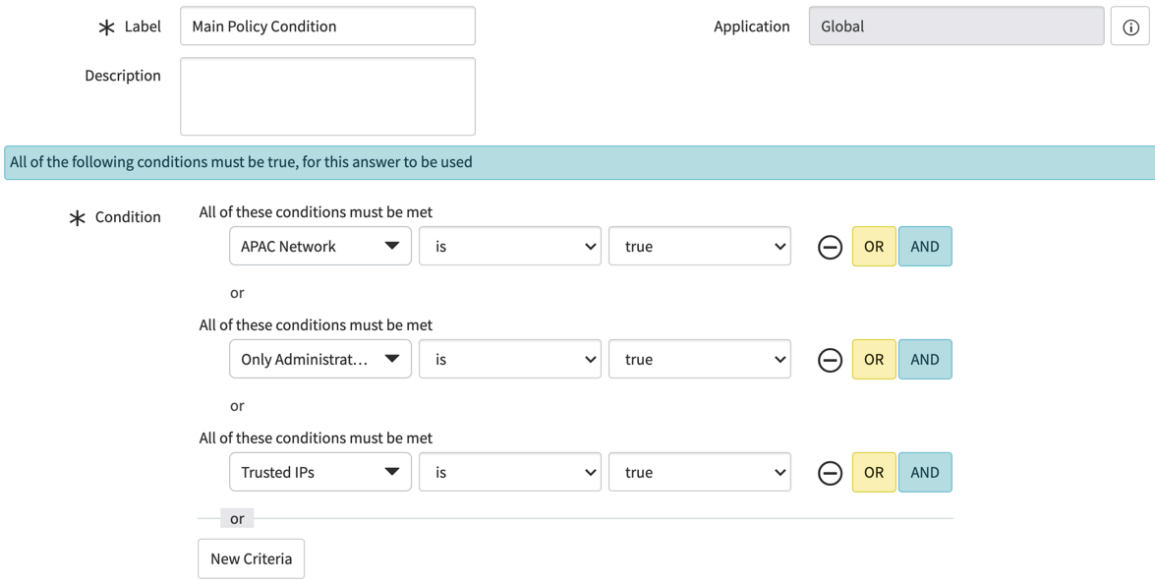
   이동합니다.
7. 저장을 선택합니다.
8. 정책 조건 탭에서 새로 만들기를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

9. 양식에서 다음과 같은 필드를 채웁니다.

조건 양식

필드	설명
레이블	정책 조건의 이름입니다.
설명	정책 조건에 대한 짧은 설명입니다.
애플리케이션	애플리케이션의 범위입니다.
조건	**OR** 필터와 결합된 하나 이상의 조건입니다.



10. 제출을 선택합니다.

API에 대한 전역 차단 정책 구성

전역 차단 정책은 지정된 정책 조건에 따라 사용자 및 API의 인증 요청을 거부합니다. 이 정책은 IP 주소 액세스 제어의 대안으로 사용할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > **API** 접근 정책 > 전역 차단 정책.
2. **Policy** Inputs(정책 입력) 탭에서 Edit(편집)를 클릭합니다.
3. 컬렉션 목록에서 하나 이상의 필터 기준을 선택하고 전역 차단 정책 목록으로 이동합니다.
   필터를 추가할 수도 있습니다.
4. 정책 조건 탭에서 새로 만들기를 클릭합니다.
5. 양식에서 다음 필드를 채웁니다.

조건 양식

필드	설명
레이블	조건을 식별하는 이름입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
설명	조건에 대한 설명입니다.
조건	인증 요청을 평가하는 데 사용되는 여러 정책 입력(필터 기준)의 논리적 조합입니다. 예를 들어, 신뢰할 수 있는 IP 주소 목록에서 협력업체만 허용하는 조건을 생성할 수 있습니다.

시스템/익스포트 프로세서에 대한 접근 정책

시스템/익스포트 프로세서가 프로세서 액세스 정책을 활용하여 모든 익스포트 엔드포인트를 보호할 수 있는 기능입니다.

모든 익스포트 엔드포인트를 보호하고 전역 또는 인스턴스 수준에서 인바운드 인증 프로파일 및 프로세서 액세스 정책을 적용하는 기능입니다.

주:

- CSV, PDF 등과 같은 익스포트 프로세서를 포함한 비공개 프로세서는 액세스 정책에 대해 지원됩니다.
- 액세스 정책에도 스크립트 프로세서가 지원됩니다.

샘플 사용 사례

- 관리자는 RSS 프로세서를 사용하지 않으려는 경우 API 접근 정책을 활용하여 RSS 프로세서를 차단할 수 있습니다.
- 관리자는 기본 인증을 사용하여 인증 프로파일을 생성하고 항상 false로 평가되는 인증 정책을 연결할 수 있습니다.

  예를 들어 `0.0.0.0` 에서 `255.255.255.255` 사이의 IP 기준을 생성한 다음(Ipv6 주소 공간도 추가) false 연산자를 사용하여 정책 조건을 추가합니다. 이렇게 하면 정책 조건이 항상 false로 평가되고 API 액세스 정책은 요청이 시작된 위치에 관계없이 액세스를 차단합니다.

- 신뢰할 수 있는 네트워크에서만 프로세서에 액세스할 수 있습니다.

프로세서 액세스 정책 활성화

프로세서의 경우 프로세서 액세스 정책(`com.glide.processor.policy`) 플러그인을 설치합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

다음 항목이 프로세서 액세스 정책과 함께 설치됩니다.

- 시스템 속성: com.glide.auth.profile.supported.processor.list
- 탐색의 모듈: 프로세서 액세스 정책

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 프로세서 액세스 정책(`com.glide.processor.policy`) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

다음에 수행할 작업

.
프로세서에 대한 인증 프로파일을 구성합니다. 자세한 내용은 을 참조하십시오 프로세서에 대한 인증 프로파일 구성.

프로세서에 대한 인증 프로파일 구성

익스포트 프로세서에 대한 인증 프로파일을 적용합니다.

시작하기 전에
필요한 역할: 관리자

필요한 플러그인: 프로세서 액세스 정책(`com.glide.processor.policy`)

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 프로세스 접근 정책.
2. 프로세서에 인증 프로파일을 추가하려면 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

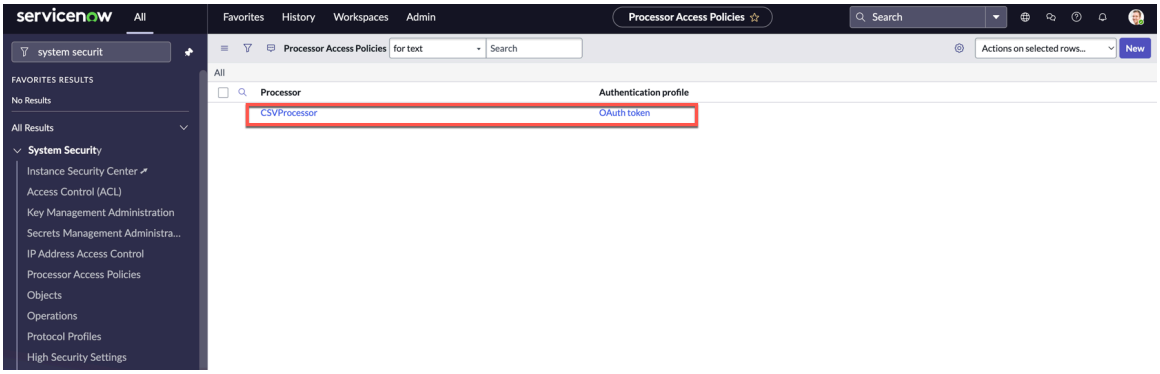
   프로세스 접근 정책 양식

필드	설명
프로세서	인증 정책을 식별하는 이름입니다. 주: 공용 프로세서는 지원되지 않습니다. 지원되지 않는 프로세서를 선택하면 프로세서를 제출하는 동안 오류가 표시됩니다.
애플리케이션	인증 정책의 범위입니다. 기본값: 전역
인증 프로파일	인증 프로파일의 유형입니다. **ID** 토큰 또는 **OAuth** 토큰을 선택할 수 있습니다.

4. 제출을 클릭합니다.
   인증 프로파일이 프로세서에 적용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 OAuth 인증 프로파일은 CSV 프로세서용으로 구성됩니다. 이 경우 CSV를 익스포트 옵션으로 사용하여 익스포트하려면 OAuth 액세스 토큰을 사용해야 합니다.



인증서 기반 인증

인증서 기반 인증을 사용하면 신뢰할 수 있는 CA(인증 기관)의 인증서를 사용하여 사용자 로그인 또는 인바운드 API 요청을 상호 인증할 수 있습니다.

주: 온 프레미스 및 에지 암호화 사용 인스턴스에서는 인증서 기반 인증이 지원되지 않습니다.

사용자 인터페이스 로그인을 위한 인증서 기반 인증

최종 사용자가 사용자 이름과 암호를 사용하는 대신 PIV(개인 신원 검증) 또는 CAC(공통 액세스 카드) 카드를 사용하여 OR 서비스 포털 에 Now Platform 로그인할 수 있도록 합니다. 사용자 인터페이스 로그인에 대한 상호 인증을 설정하려면 을 참조하십시오 인증서 기반 인증 설정.

인증서 기반 인증이 설정되면 최종 사용자가 설정을 완료하고 로그인할 수 있습니다. 인증서 기반 인증을 사용하여 로그인 문서를 참조하십시오.

인바운드 웹 서비스에 대한 인증서 기반 인증

SOAP 및 REST API에 대한 ServiceNow 인바운드 요청을 인증합니다. 인바운드 웹 서비스에 대한 상호 인증을 설정하려면 문서를 참조하십시오 인증서 기반 인증 설정.

인증서 기반 인증 설정

사용자 인터페이스 기반 로그인 또는 인바운드 웹 서비스에 대한 상호 인증을 설정합니다.

시작하기 전에
필요한 역할: 관리자

인스턴스가 ADCv2 부하 분산 장치를 사용하고 있는지 확인합니다. 자세한 내용은ADCv2 마이그레이션 지식 문서를 참조하세요. 인스턴스가 ADCv2 부하 분산 장치를 사용하지 않는 경우에 문의하십시오 Now Support.

프로시저

다음을 위해 인증서 기반 인증을 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 최종 사용자가 PIV 또는 CAC 카드를 사용하거나 안전하게 로그인할 Now Platform서비스 포털 수 있도록 합니다. 인증서 기반 인증을 사용하도록 설정한 후에는 PEM 인증서를 자체 등록하거나 관리자가 인증서를 매핑할 수 있습니다. 인증서 기반 인증을 사용하여 로그인 문서를 참조하십시오.
- 인바운드 웹 서비스에 대한 상호 인증을 활성화합니다. 인증서 기반 인증이 설정되면 시스템은 제공된 인증서를 사용하여 REST 및 SOAP API에 액세스하기 ServiceNow 위한 요청을 상호 인증합니다.

인증서 기반 인증 활성화

관리자 역할이 있는 경우 인증서 기반 인증 플러그인(com.glide.auth.mutual) Now Platform 을 활성화할 수 있습니다.

시작하기 전에
필요한 역할: admin.

이 태스크 정보
다음 테이블이 인증서 기반 인증과 함께 설치됩니다.

- sys_user_certificate
- sys_ca_certificate
- sys_ca_certificate_api_track

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 인증서 기반 인증 플러그인(com.glide.auth.mutual)을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.

3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

CA 인증서 등록

루트 인증서 또는 중간 인증서를 등록하여 인증에 사용할 수 있도록 합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 인증서 기반 인증 > **CA** 인증서 체인.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상호 인증 **CA** 인증서 양식

필드	설명
이름	인증서를 식별하는 이름입니다.
만료 알림	인증서가 만료되려고 할 때 사용자에게 경고하는 옵션입니다.
만료 시 알림	인증서가 만료될 때 알림을 받을 사용자 목록입니다.
만료되기 전 경고	인증서가 만료되기 전에 사용자에게 알림이 전송되는 일수입니다.
활성	클라이언트 인증서를 활성화하는 옵션입니다.
형식	PEM
유형	인증서의 유형입니다. 옵션은 다음과 같습니다. ◦ **CA** 인증서: 루트 CA 인증서입니다. 체인에 중간 인증서를 포함할 수도 있습니다. CA 인증서는 부하 분산 장치와 자동으로 동기화됩니다. 가능한 경우 이 옵션을 사용하여 체인에서 필요한 인증서가 누락되지 않도록 합니다. ◦ 중간 인증서: 인증서 체인의 중간 인증서입니다. 이 인증서는 인스턴스에만 유지되며 부하 분산 장치와 동기화되지 않습니다. 기존 체인에 중간 인증서를 추가해야 하는 경우에만 이 옵션을 사용합니다.
간단한 설명	사용자 클라이언트 인증서에 대한 간단한 설명입니다.

주: 인증서를 업로드하는 동안 읽기 전용 필드인 유효 기간(시작), 만료됨, 만료일(일),발급자 및 제목, 인증서 체인 및 **PEM** 인증서가 추출되고 자동으로 채워집니다.

4. 제출을 클릭합니다.
5. 옵션: **Validate Stores**/Certificates(저장소/인증서 확인)를 클릭하여 인증서를 확인합니다.

PEM 인증서를 사용자에게 매핑

PEM 인증서를 사용자에게 매핑하여 PIV 또는 CAC 카드를 사용하여 로그인하거나 인바운드 요청을 인증할 수 있도록 합니다. 여러 PEM 인증서를 사용자에게 매핑할 수 있습니다.

시작하기 전에

- 필요한 역할: 관리자
- 사용자의 PEM(Privacy Enhanced Mail) 인증서가 있는지 확인합니다.

주: PEM 인증서를 사용자에 매핑 구성 후 "인증서 확인"이 실패합니다. PEM 인증서가 저장되지 않았기 때문입니다.

프로시저

1. 다음으로 이동 모두 > 인증서 기반 인증 > 사용자 **-** 인증서 매핑 을 클릭하고 신규를 클릭합니다.
2. 양식의 필드에 내용을 입력합니다.

사용자 클라이언트 인증서 양식

필드	설명
이름	사용자 클라이언트 인증서의 이름입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
만료 알림	인증서가 만료되려고 할 때 사용자에게 경고하는 옵션입니다.
만료되기 전 경고	인증서가 만료되기 전에 사용자에게 알림이 전송되는 일수입니다.
만료 시 알림	인증서가 만료될 때 알림을 받을 사용자 목록입니다.
활성	클라이언트 인증서를 활성화하는 옵션입니다.
사용자	클라이언트 인증서에 매핑되는 사용자입니다. 시스템은 인바운드 요청 또는 인증서 등록에서 클라이언트 인증서를 받은 다음 이 필드에 지정된 사용자를 사용하여 요청을 실행하기 위한 세션을 시작합니다.
간단한 설명	사용자 클라이언트 인증서에 대한 간단한 설명입니다.
형식	PEM(Privacy Enhanced Mail) 형식은 base-64로 인코딩된 DER(고유 인코딩 규칙) 인증서입니다.
유형	클라이언트 인증서. 이 필드는 읽기 전용입니다.

주: 인증서를 업로드하는 동안 읽기 전용 필드인 유효 기간(시작), 만료됨, 며칠 후 만료됨, 발급자 및 제목 이 추출되고 자동으로 채워집니다.

3. 첨부 파일 아이콘을 클릭하고 인증서를 업로드합니다.
4. 제출을 클릭합니다.
   신뢰할 수 있는 CA(인증 기관)에서 발급한 인증서인 경우 인증서의 유효성이 검사되고 지정된 사용자에게 매핑됩니다.

인증서 기반 인증 속성 구성

시스템 속성을 사용하여 인증서 기반 인증 기능을 사용하거나 사용하지 않도록 설정합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 인증서 기반 인증 > 속성.
2. 양식의 필드에 내용을 입력합니다.

인증서 기반 인증 속성 양식

속성	설명
인증서 기반 인증을 사용	사용자 인터페이스 로그인과 인바운드 웹 서비스 모두에 대해 인증서 기반 인증을 활성화하는 옵션입니다. 기본값: true
로그인 화면에 "PIV/CAC로 로그인" 옵션 표시	로그인 화면에 **PIV/CAC** 카드로 로그인 옵션을 표시합니다. 사용자가 사용자 인터페이스를 통해 인증서 기반 인증을 통해 로그인할 수 있습니다. 기본값: false

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
인증서 기반 로그인에 대해 자동 리디렉션 사용	등록된 인증서를 선택하고 PIN을 입력한 후 사용자가 **PIV/CAC** 카드로 로그인을 클릭하도록 요구할지 여부를 결정합니다. 사용자가 등록된 클라이언트 인증서를 선택하고 PIN을 입력한 후 자동으로 로그인하려면 활성화합니다. 비활성화하여 사용자가 등록된 클라이언트 인증서를 선택하고 PIN을 입력한 후 **PIV/CAC** 카드로 로그인을 클릭하도록 요구합니다. 기본값: false

인증서 기반 인증을 사용하여 로그인

관리자가 인증서 기반 인증을 설정한 후 클라이언트 인증서를 등록하고 PIV(개인 신원 확인) 또는 CAC(공통 액세스 카드) 카드를 사용하여 로그인할 수 있습니다.

PIV 또는 **CAC** 카드에 대한 클라이언트 인증서 등록

PIV 또는 CAC 카드를 사용하여 Now Platform에 로그인하기 전에 PIV 또는 CAC 카드의 클라이언트 인증서를 등록해야 합니다. 클라이언트 인증서를 등록할 수 없는 경우 관리자에게 문의하십시오. 관리자는 PIV 또는 CAC 카드의 클라이언트 인증서를 등록할 수도 있습니다.

시작하기 전에

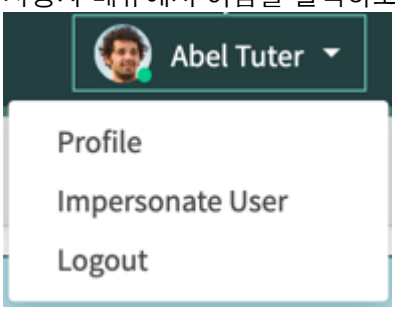
- 인증서 기반 인증을 사용할 수 있는지 확인합니다.
- 카드 리더가 컴퓨터에 연결되어 있고 PIV 또는 CAC 카드가 삽입되어 있는지 확인합니다.
- 필요한 역할: 없음

이 태스크 정보

클라이언트 인증서를 등록하기 위해 관리자가 필요한 경우 문서를 참조하십시오 PEM 인증서를 사용자에게 매핑.

프로시저

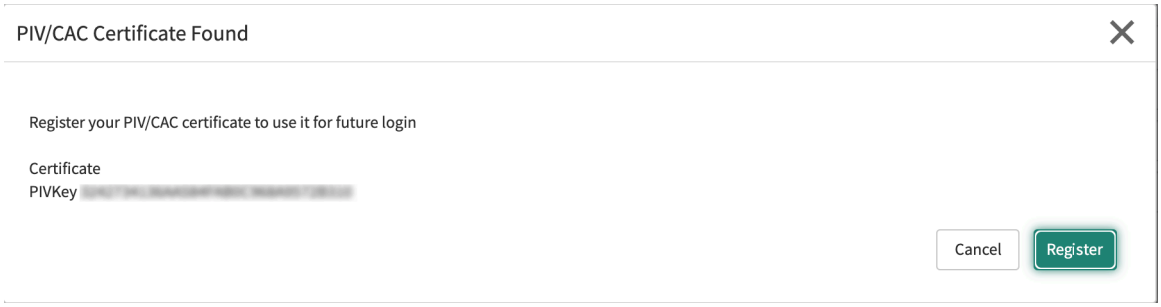
1. 사용자 이름과 암호를 사용하여 Now Platform에 로그인합니다.
2. 사용자 메뉴에서 이름을 클릭하고 프로파일을 선택합니다.



3. **Related** Links(관련 링크)에서 **Register client** certificate(클라이언트 인증서 등록)를 클릭합니다.

   유효한 인증서를 사용할 수 있는 경우 다음 메시지가 표시됩니다.

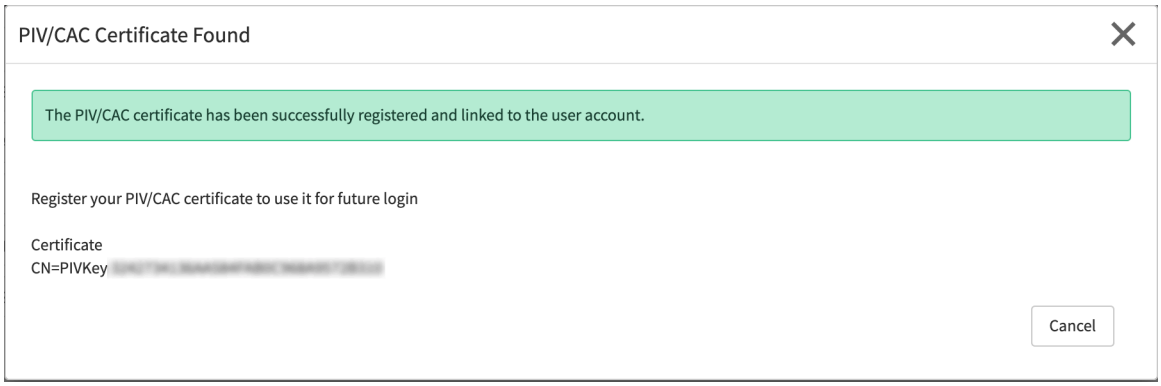
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 등록을 클릭합니다.

   등록에 성공하면 다음 메시지가 표시됩니다.

   `PIV/CAC #### ##### #### ### ### #######.`



다음에 Now Platform에 로그인할 때 PIV 또는 CAC 카드를 사용하여 로그인할 수 있습니다. 자세한 내용은 PIV 또는 CAC 카드를 사용하여 로그인 Now Platform 문서를 참조하십시오.

PIV 또는 CAC 카드를 사용하여 로그인 Now Platform

에서 Now Platform인증서 기반 인증을 사용하는 경우 사용자 이름과 암호 대신 PIV 또는 CAC 카드로 로그인할 수 있습니다.

시작하기 전에

- 필요한 역할: 없음
- 인증서 기반 인증을 사용할 수 있는지 확인합니다.
- PIV 또는 CAC 카드 리더가 컴퓨터에 연결되어 있는지 확인하십시오.
- PIV 또는 CAC 카드의 클라이언트 인증서가 사용자에게 매핑되어 있는지 확인하십시오. 자세한 내용은 CA 인증서 등록 문서를 참조하십시오.

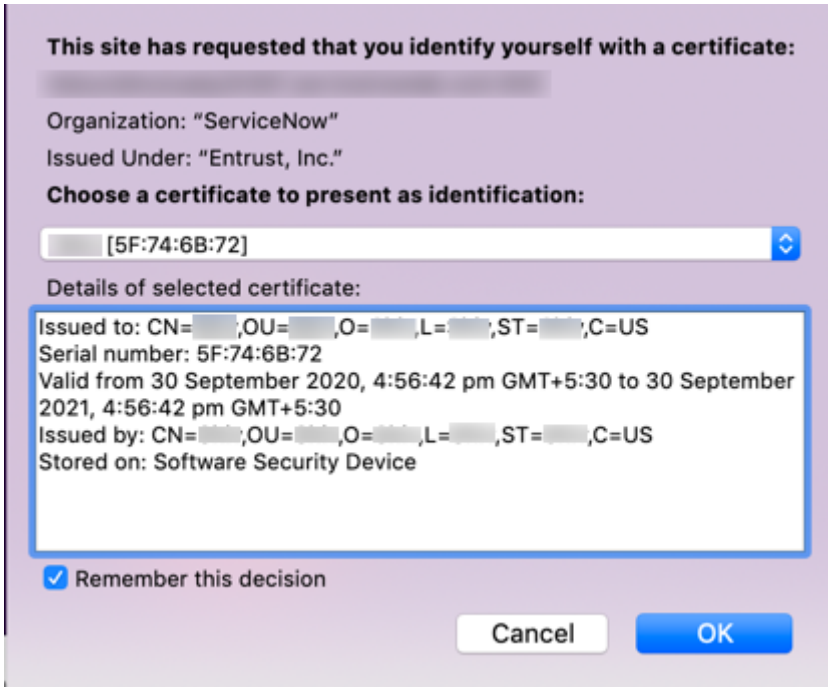
프로시저

1. PIV 또는 CAC 카드를 카드 리더기에 삽입합니다.
2. 브라우저에서 인스턴스로 이동합니다.
   PIV 또는 CAC 카드의 PIN을 입력하라는 메시지가 브라우저에 표시됩니다.
3. 브라우저 프롬프트에 PIV 또는 CAC 카드의 PIN을 입력합니다.

   주: PIN을 잊어버린 경우 관리자에게 문의하십시오.

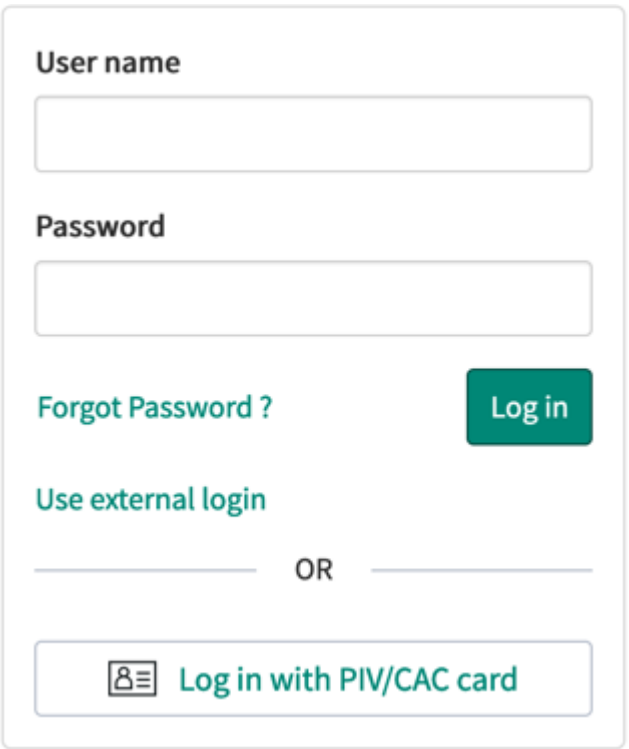
4. 올바른 PIN을 입력하면 브라우저에 인증서를 선택하라는 프롬프트가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 브라우저 프롬프트에서 인증서를 선택합니다.

   인증서가 유효하고 사용자에게 매핑된 경우 로그인 페이지로



   리디렉션됩니다.

6. **PIV/CAC** 카드로 로그인 버튼을 클릭합니다.

   Now Platform에서 로그아웃하려면 카드 리더에서 PIV 또는 CAC를 제거한 다음 브라우저를 닫아야 합니다.

클라이언트 인증서 관리

계정과 연결된 클라이언트 인증서를 보고 삭제합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

- 인증서 기반 인증을 사용할 수 있는지 확인합니다.
- 필요한 역할: 없음

프로시저

1. 사용자 이름과 암호를 사용하여 로그인합니다 Now Platform .
2. 사용자 메뉴에서 이름을 클릭하고 프로파일을 선택합니다.



3. **Related** Links(관련 링크)에서 **Manage your client** certificates(클라이언트 인증서 관리)를 클릭합니다.
   사용자 클라이언트 인증서 [sys_user_certificate] 테이블이 열리고 계정과 연결된 인증서가 표시됩니다.
4. 계정과 연결된 인증서를 보거나 삭제합니다.

인스턴스에 **Custom URL** 연결

회사 브랜드 또는 사용자 지정 URL에서 인스턴스에 액세스할 수 있도록 설정할 ServiceNow 수 있습니다.

사용자 지정 **URL** 개요

사용자 지정 URL을 사용하면 ServiceNow 하나 이상의 회사 브랜드 또는 사용자 지정 URL에서 인스턴스에 액세스할 수 있습니다.

사용자 지정 URL은 특정 포털과 연결할 수 있습니다. 예를 들어 관리자는 CSM 포털에 대한 `http://support.acme.com` 와 HR 포털에 대한 `http://hr.acme.com` 정의할 수 있습니다. 이러한 상황에서는 사용자가 액세스하는 사용자 지정 URL을 기반으로 인증을 위해 사용자를 다른 IdP로 리디렉션해야 합니다.

중요사항:

- 인스턴스당 도메인이 100개를 초과하는 사용자 지정 URL을 생성하지 마십시오.
- 먼저 인스턴스에서 사용자 지정 URL 기록을 ServiceNow 삭제한 다음 DNS 서버에서 DNS(Domain Name Server) 항목을 삭제해야 합니다.
- 인스턴스에서 사용자 지정 URL 기록을 ServiceNow 삭제하기 전에 DNS 서버에서 DNS 항목을 삭제하면 에서 해당하는 다른 사용자 지정 URL 기록 ServiceNow의 삭제가 차단됩니다.

에서 Tokyo사용자가 사용자 지정 URL 기록에 정의된 지정된 IdP로 자동 리디렉션하도록 허용할 수 있습니다.

주: 온프레미스 고객 또는 개발자 인스턴스에는 사용자 지정 URL을 사용할 수 없습니다. 또한 URL은 공개되어야 합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

최상위 도메인(TLD) 또는 하위 도메인의 소유자만 DNS 하위 도메인에 대한 사용자 지정 URL을 구성할 수 있습니다. 예를 들어 인스턴스에 다음과 같이 지정된 URL과 추가 사용자 지정 URL이 있을 수 있습니다.

사용자 지정 **URL** 예

예제 **URL**	사용량
`https://acme.service-now.com`	인스턴스와 함께 제공된 Acme의 ServiceNow 초기 도메인 이름입니다.
`https://support.acme.com`	인스턴스에 연결된 사용자 지정 URL입니다 ServiceNow . 이 URL을 초기 도메인 이름의 별칭(CNAME)이라고 합니다.
`https://US-support.acme.com`	인스턴스의 서비스 포털에 연결되는 보조 사용자 지정 URL입니다. 인스턴스는 동일한 서비스 포털에 대한 여러 사용자 지정 URL을 지원할 수 있습니다.

인스턴스 외부의 사용자 지정 **URL** 고려 사항

사용자 지정 URL을 연결하려면 먼저 도메인 공급업체를 통해 URL을 소유하거나 구매해야 합니다. 인스턴스에서 사용자 지정 URL을 만들고 연결하려면 특정 구성이 필요합니다.

사용자 지정 **URL** 구성

구성 항목	설명
공급자로 CNAME 설정	CNAME 기록을 인스턴스 URL로 ServiceNow 설정해야 합니다.
VIP 전담 상태 결정	VIP의 상태입니다.

주: 인스턴스를 가리키는 CNAME 레코드를 삭제하거나 업데이트할 때 인스턴스에 레코드가 매달리지 않도록 하려면 다음 순서를 따라야 합니다. 먼저 인스턴스에서 CNAME 레코드를 삭제한 다음 DNS 공급자에서 CNAME 설정을 제거하거나 업데이트합니다.

사용자 지정 **URL** 활성화

인스턴스에 사용자 지정 URL을 설정할 수 있습니다 ServiceNow . 관리자 역할이 있는 경우 사용자 지정 URL 플러그인(com.snc.customurl)을 활성화할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 플러그인.
2. **Custom URL** 플러그인을 찾아서 클릭합니다.

   주: 스크립팅된 사용자 지정 URL API의 내부 구성요소인 **Custom URL - Internal** 플러그인을 선택하지 마십시오.

3. 사용자 지정 URL 기록에서 활성화/복구 관련 링크를 클릭합니다.
4. 플러그인 활성화 창에서 활성화를 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플러그인이 활성화되었다는 메시지와 함께 플러그인 활성화 창이 다시 열리면 **Close & Reload Form** 을 클릭하여 이 폼에 머물러 있습니다.

5. 플러그인 파일 관련 목록에서 다음 속성을 찾아 설정 값을 변경합니다.

옵션	설명
glide.customurl.enabled	Custom URL을 사용하려면 값을 **True**로 설정합니다. 기본적으로 이 속성은 **False**로 설정되어 있으므로 사용자 지정 URL을 연결할 수 없습니다. 주: 이 기능을 사용하지 않으려면 이 속성을 다시 **False**로 설정합니다.

6. 업데이트를 클릭합니다.

사용자 지정 URL을 인스턴스 URL로 설정

URL 대신 ServiceNow 사용할 사용자 지정 URL을 인스턴스 구성에 추가합니다.

시작하기 전에

필요한 역할: 관리자

인스턴스에 사용자 지정 URL을 추가하기 전에 사용자 지정 URL 플러그인을 활성화하고 URL을 구입하거나 등록해야 합니다.

프로시저

1. 다음으로 이동 모두 > 사용자 지정 **URL** > 사용자 지정 **URL**.
2. 다음 중 하나를 수행해야 합니다.
   - 신규를 클릭하여 인스턴스에 새로운 새 도메인 이름을 연결합니다.
   - 인스턴스 URL로 설정하도록 이미 설정된 사용자 지정 URL을 선택하십시오.
3. 적절한 필드를 입력합니다.

사용자 지정 **URL** 필드

필드	설명
도메인 이름	사용자 지정 URL의 FQDN(전체 주소 도메인 이름)입니다. FQDN은 사용자 지정 도메인에 대한 이름 서버 레코드에서 생성된 CNAME 리디렉션입니다. 주: 예를 들어, acme.com 의 이름 서버에서 다음과 같은 항목을 만들 수 있습니다. `support.acme.com 300 IN CNAME acme.servicenow.com`
인스턴스 URL	모든 아웃바운드 URL에 대해 이 사용자 지정 URL을 사용하도록 설정하는 확인란입니다. 활성 사용자 지정 URL은 하나만 인스턴스 URL이 될 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	사용자 지정 URL에 대해 이 설정을 사용하려면 URL 기록에서 인스턴스 URL로 설정을 클릭합니다. 그러면 이전의 모든 맞춤 URL이 삭제됩니다.
상태	사용자 지정 URL 기록의 상태입니다. 상태가 활성이면 사용자 지정 URL이 프로비저닝되어 사용할 준비가 된 것입니다.
서비스 포털	사용자 지정 URL을 사용하여 사용자를 인스턴스로 리디렉션할 때 사용하려는 서비스 포털입니다.
ID 제공자	사용자 지정 URL의 신원 확인 제공자를 사용하면 사용자가 사용자 지정 URL 기록에 정의된 지정된 IdP로 자동 리디렉션할 수 있습니다.

사용자 지정 URL은 인스턴스에서 6시간 이내에 활성화되어야 합니다.

주:

- 먼저 인스턴스에서 사용자 지정 URL 기록을 ServiceNow 삭제한 다음 DNS 서버에서 DNS(Domain Name Server) 항목을 삭제해야 합니다.
- 인스턴스에서 사용자 지정 URL 기록을 ServiceNow 삭제하기 전에 DNS 서버에서 DNS 항목을 삭제하면 에서 해당하는 다른 사용자 지정 URL 기록 ServiceNow의 삭제가 차단됩니다.

신원 확인 제공자를 사용하는 사용자 지정 URL

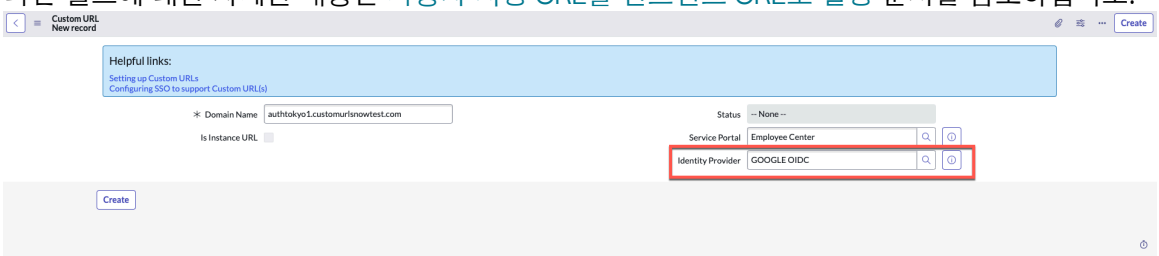
사용자가 IdP로 로그인할 수 있도록 신원 확인 제공자를 사용하는 사용자 지정 URL을 설정합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

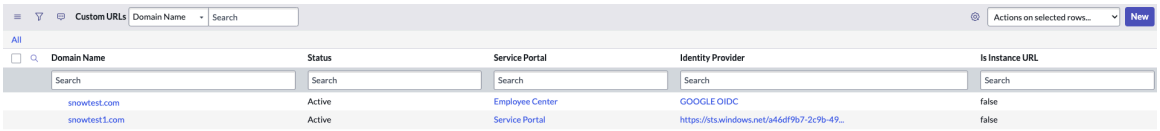
1. 다음으로 이동 모두 > 사용자 지정 **URL** > 사용자 지정 **URL**.
2. 새로 만들기를 클릭합니다.
3. IdP의 상세 정보를 신원 확인 제공자 필드에 제공합니다.
   다른 필드에 대한 자세한 내용은 사용자 지정 URL을 인스턴스 URL로 설정 문서를 참조하십시오.



4. 생성을 클릭합니다.

   기록이 생성되고 사용자 지정 URL 페이지에 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



사용자 지정 URL에 액세스하면 사용자가 구성된 신원 확인 제공자에게 리디렉션됩니다. 이 경우 `snowtest.com`에 액세스하면 사용자가 직원 센터로 이동한 다음 Google 신원 확인 제공자에게 리디렉션됩니다.

주:

- 서비스 포털 필드가 비어 있고 신원 확인 제공자 필드가 정의되면 사용자가 사용자 지정 URL에 액세스할 때 구성된 신원 확인 제공자로 직접 이동됩니다.
- 서비스 포털 및 신원 확인 제공자 필드가 모두 정의되고 사용자가 정의된 서비스 포털로 사용자 지정 URL에 액세스하면 사용자가 구성된 신원 확인 제공자로 직접 이동됩니다.
- 서비스 포털 및 신원 확인 제공자 필드가 모두 정의되고 사용자가 정의되지 않은 다른 포털로 사용자 지정 URL에 액세스하면 인스턴스에 구성된 경우 사용자가 자동 리디렉트 신원 확인 제공자로 이동됩니다.

5. 자격 증명을 사용하여 애플리케이션에 로그인합니다.

사용자 지정 **URL** 데이터센터 작업 정보

인스턴스에 연결된 모든 사용자 지정 URL에는 해당 ServiceNow 데이터센터 작업이 있으며, 이 작업은 테이블에 설명된 대로 인스턴스와 관련된 URL 정보를 실행하고 표시합니다.

작업 필드	설명
작업 ID	사용자 지정 URL의 도메인을 확인하는 작업의 고유 ID입니다.
마지막 실행 시간	작업을 마지막으로 실행한 날짜 및 시간입니다.
페이로드	CERT 프로비저닝을 위해 데이터 센터로 전송된 도메인 또는 사용자 지정 URL의 목록입니다.
폴링 횟수	이 작업에 대해 결과가 폴링된 횟수입니다.
결과	페이로드로 전송된 각 도메인 또는 사용자 지정 URL을 검증하고 유효성을 검증합니다.
상태	데이터센터 작업의 상태입니다.

SAML/SSO 사용자 지정 **URL** 설치를 위한 **SP** 메타데이터 생성

SAML 또는 SSO 설치는 사용자 지정 URL 인스턴스가 생성되기 전에 IdP에 대해 생성된 SP 메타데이터를 필요로 합니다.

시작하기 전에
필요한 역할: admin
IdP는 요청을 인증하고 전달하기 위해 인스턴스에 대한 SP 메타데이터가 필요합니다.

주: SP 로그인 URL(Assertion Consumer Service URL)을 추가하는 작업은 IdP(Azure, ADFS 또는 Okta)마다 다를 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 설치된 SSO 플러그인을 선택합니다.

옵션	설명
복수 제공자 SSO	다음으로 이동 복수 제공자 **SSO** > **ID** 제공자. IdP를 선택하고 메타데이터 생성 버튼을 클릭합니다. 통합은 시스템 속성 설정에서 인스턴스의 SP 메타데이터를 자동으로 생성합니다.
SAML 2 SSO	다음으로 이동 **SAML 2** 1회 사용자 인증 **(SSO)** > 메타데이터. 통합은 시스템 속성 설정에서 인스턴스의 SP 메타데이터를 자동으로 생성합니다.

2. 텍스트 상자에서 SP 메타데이터를 복사합니다.

예:

```
<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:emailAddres
s</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. 인스턴스 SP 메타데이터를 IdP에 제공합니다.
예를 들어 SSOCircle을 사용하면 사용자가 SP 메타데이터를 온라인으로 제공할 수 있습니다.

4. 옵션: Azure에서 사용자 지정 URL을 설정하려면 다음을 수행합니다.

a. 앱 등록으로 이동합니다.

b. 메뉴에서 모든 앱을 선택합니다.

c. **ServiceNow** 앱을 선택합니다.

d. 설정을 클릭하여 URL을 구성합니다.

5. 옵션: Okta에서 사용자 지정 URL을 설정하려면 다음을 수행합니다.

a. 두 개의 ServiceNow UD Okta 애플리케이션을 생성합니다.

b. "service-now.com" 인스턴스 URL에 대한 Okta 애플리케이션 1개.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 사용자 지정 URL에 대한 Okta 애플리케이션 1개.

주:

- 연결 테스트가 성공적으로 실행되도록 Okta 구성 내에서 **Force Authentication** 사용 안 함**(Disable Force Authentication)**을 비활성화합니다.
- 기본 URL과 연결된 ID 제공자 기록을 테스트하는 경우 기본 URL을 사용하여 인스턴스에 로그인해야 합니다.
- 사용자 지정 URL과 연결된 자격 증명 제공자를 테스트하는 경우 사용자 지정 URL을 사용하여 인스턴스에 로그인해야 합니다.

6. 옵션: OAuth 인증을 사용하려면 외부 클라이언트 애플리케이션에 대한 OAuth 애플리케이션 엔드포인트 구성에서 리디렉션 URL을 등록된 모든 사용자 지정 URL로 설정합니다. 리디렉션 URL은 권한 부여 서버가 리디렉션하는 콜백 URL과 동의어입니다.
7. 옵션: Google reCAPTCHA 서비스를 사용하려면 API 키 쌍을 설정합니다.

사용자 지정 URL 오류 및 수정

사용자 지정 URL 설정 및 구성에 대한 일반적인 오류 및 관련 수정 사항 목록입니다.

설정 중 오류 발생

오류 메시지	고정
사용자 지정 URL을 작성할 수 없습니다. 나중에 다시 시도하십시오.	사용자 지정 URL 생성을 방해하는 제어 범위를 벗어난 문제가 있을 수 있습니다. 지원 센터에 문의하기 전에 다른 시간에 실행하십시오. 주: 일반적으로 사용자 지정 URL을 만드는 데 30분이 걸립니다. 시간이 더 오래 걸리는 경우 에 문의하십시오 https://support.servicenow.com/now?draw=case.
인스턴스에 대한 다른 사용자 지정 URL 요청이 아직 진행 중이므로 새 사용자 지정 URL 요청을 제출할 수 없습니다.	새 요청을 제출하기 전에 사용자 지정 URL 작업의 상태를 확인하십시오.
인스턴스 URL을 설정하려면 먼저 Glide 프록시, Glide 서블릿 속성을 지워야 합니다.	
<custom_domain> 프로비저닝이 아직 진행 중입니다. 이 프로세스는 최대 X시간이 걸릴 수 있습니다. 이 프로세스가 완료되면 인스턴스 관리자가 알림을 받게 됩니다.	사용자 지정 URL에 대한 인스턴스 프로비저닝이 시작되면 상태가 변경되기 전에 프로세스가 완료될 때까지 기다려야 합니다.
이제 <custom_domain> 새 인스턴스 URL로 설정되었습니다. <base.service-now.com>는 여전히 서비스 중이지만 알림과 같은 모든 새 URL은 <custom_domain> 사용합니다.	하나의 URL만 인스턴스 URL로 지정할 수 있습니다. 인스턴스와 연결된 다른 URL을 활성화할 수 있지만 인스턴스 URL만 알림을 사용할 수 있습니다.
사용자 지정 URL <custom_domain>는 인스턴스 구성에서 즉시 제거된 후 다시 <base.service-now.com>로 되돌리도록 설정됩니다. <custom_domain> DNS의 CNAME 레코드가	이 메시지는 사용자 지정 URL을 변경하려다는 것을 확인합니다. 이 확인을 수락하면 인스턴스에 대한 URL 변경을 시작합니다. 사용자 지정 URL로 도메인 이름 목록에 있는 모든 URL은 공급자의

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

오류 메시지	고정
설정되어 있는 한 이 인스턴스와의 연결을 계속합니다.	CNAME 레코드에서 제거하지 않는 한 활성 상태일 수 있습니다.
glide.servlet.uri는 수정할 수 없습니다. 이 속성은 사용자 지정 URL에 의해 설정됩니다.	
glide.proxy.host는 수정할 수 없습니다. 이 속성은 사용자 지정 URL에 의해 설정됩니다.	
〈custom_domain〉에 대한 CNAME 기록이 <base.service-now.com> 가리키지 않습니다.	URL 제공자 측의 구성이 올바르지 않습니다. CNAME 레코드에서 구성을 확인합니다.
〈custom_domain〉에 대한 CNAME 기록이 없습니다.	인스턴스에 대한 사용자 지정 URL을 설정하려면 먼저 URL 제공자로부터 CNAME 기록을 구성해야 합니다.

설치 종료

설치 엑시트는 Java로 다시 돌아가기 전에 스크립트를 호출하기 위해 Java에서 종료하는 사용자 정의입니다.

주: 여기에 설명된 기능을 사용하려면 관리자 역할이 필요합니다.

사용 가능한 설치 종료

다음으로 이동 시스템 정의 > 설치 종료. 일부 설치 종료 이름(로그인, 로그아웃, ValidatePassword, ExternalAuthentication)은 예약되어 있으며 변경할 수 없습니다. 다른 설치 종료는 기본 설치 종료의 스크립트를 대체하는 사용자 지정 스크립트로 이를 대체할 수 있습니다.

기본 시스템에서 다음 설치 종료를 사용할 수 있습니다.

설치 종료	설명
로그인	사용자 이름과 암호 쌍을 사용하고 사용자 객체로 인증합니다.
로그아웃	로그아웃 시 사용자를 시작 페이지로 이동시킵니다. LogoutRedirect에 의해 재정의될 수 있습니다.
로그아웃 리디렉션	로그아웃 시 사용자를 지정된 URL로 이동시킵니다.
외부 인증	헤더, 매개변수 또는 쿠키를 사용하여 인증합니다. DigestSingleSignOn 및 PGPSingleSignOn에 의해 재정의될 수 있습니다.
다이제스트싱글사인온	헤더, 매개변수 또는 쿠키를 사용하여 인증하고 다이제스트 암호화를 해독합니다.
PGPSingleSignOn	헤더, 매개변수 또는 쿠키를 사용하여 인증하고 PGP 암호화를 해독합니다.
암호 확인	릴리스부터 기본적으로 활성화됩니다. 고객이 자신의 암호 확인을 정의할 수 있습니다. ValidatePasswordStrongerger로 재정의할 수 있습니다.Helsinki
ValidatePasswordStronger	비밀번호는 8자 이상이어야 하며 숫자, 대문자 및 소문자를 포함해야 합니다.
GetIntegrationSessionTimeout	기본 통합 세션 시간 제한 동작을 구현합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그인 수정

로그인 설치 종료를 다음과 같이 수정하면 사용자가 로그인할 때 각 사용자의 세션 제한시간 값이 설정됩니다. 이 특정 예에서 사용자 이름이 *admin*인 경우 세션은 30초 후 시간 제한으로 설정됩니다.

```
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");

          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, "");
       }

}
```

IP 주소에 따라 세션 시간 제한을 설정할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
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");

          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, "");
       }

}
```

관련 정보

인증

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

IP 범위 기반 인증

웹 기반 응용 프로그램을 보호하는 한 가지 방법은 IP 주소를 기반으로 액세스를 제한하는 것입니다.

악의적인 개인의 것으로 의심되는 특정 주소 또는 주소 범위에 대한 액세스를 차단할 수 있습니다. 이 인스턴스를 사용하면 IP 주소로 액세스를 제어할 수 있습니다.

주: 적응형 인증(AA) 사전 인증 컨텍스트 정책을 사용하여 추가 기능에 대한 IP 기반 인증 및 제한을 적용합니다. 자세한 내용은 적응형 인증 문서를 참조하십시오.

참고 및 제한 사항:

- 시스템은 자신을 잠그는 것을 허용하지 않으므로 현재 주소가 잠기도록 규칙을 추가하려고하면 시스템에서 경고하고 삽입을 거부합니다.
- 회사 인트라넷 내부에 있는 경우 IP 규칙 설정에 매우 주의해야 합니다. 자신의 컴퓨터에 표시되는 IP 주소(예: 10.10.10.25)는 일반적으로 인터넷에 실제로 표시되는 IP 주소와 관련이 없습니다. 귀하의 회사는 귀하의 주소를 프록시 및/또는 NAT하여 네트워크 팀에 문의해야 할 수 있는 예측 가능한 아웃바운드 주소 집합으로 만들 수 있습니다.
- 액세스 규칙에 따라 액세스가 제한된 사용자의 브라우저에는 403 오류가 표시됩니다.
- 제한된 사용자는 트랜잭션, 세마포를 사용하지 않으며 서버 자원 개수에 포함되지 않습니다.
- 이 기능은 예를 들어 데이터 센터에서 VPN을 실행하는 경우 기존 액세스 제어 규칙을 대체하거나 재정의하지 않습니다. PIX에 설정했을 수 있는 액세스 제어 외에 충족해야 하는 추가 검사입니다.
- 허용 규칙은 항상 거부 규칙을 대체합니다. 따라서 주소가 (한 가지 규칙에 의해) 허용되고 (두 번째 규칙에 의해) 거부된다면, 그것은 실제로 허용된다.
- 별표 및 CIDR 블록은 현재 지원되지 않습니다.
- 전달된 프록시 주소의 경우 허용 규칙이 체인의 각 주소에 적용된 다음 허용 규칙이 일치하지 않으면 체인의 각 주소에 거부 규칙이 적용됩니다.
- IP 범위 기반 인증은 업데이트 세트의 전송에 영향을 줄 수 있습니다. 소스 인스턴스에서 IP 주소 액세스 제어가 활성화된 경우 인스턴스를 지원하는 모든 애플리케이션 노드의 IP 주소를 예외로 추가합니다.

  주: 인스턴스 IP 정보를 찾으려면 ServiceNow - NOW 지원 을 클릭하고 내 **IP** 정보 서비스 카탈로그 항목을 검색합니다.

주: 특정 IP 범위에 대한 인스턴스 액세스를 제한하는 and *glide.ip.authenticate.strict* 속성에 대한 *com.snc.ipauthenticator* 자세한 내용은 인스턴스 보안 강화 설정의 다음 주제를 참조하십시오.

- 특정 IP 범위 플러그인에 대한 액세스 제한 [보안 센터 1.3에서 업데이트됨]
- 허용된 ServiceNow 내부 IP 주소 정의 [Security Center 1.3 및 1.5에서 업데이트됨]

IP 주소 접근 통제

아웃바운드 트래픽, 인바운드 트래픽 또는 양방향 트래픽에 IP 액세스 제어를 적용합니다. 일치하는 거부 규칙이 있고 일치하는 허용 규칙이 없는 경우 시스템은 IP 주소만 차단합니다. 기본적으로 인스턴스에 대한 액세스에는 제한이 없습니다.

시작하기 전에

주: 적응형 인증(AA) 사전 인증 컨텍스트 정책을 사용하여 추가 기능에 대한 IP 기반 인증 및 제한을 적용합니다. 자세한 내용은 적응형 인증 문서를 참조하십시오.

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

⚠ 경고: IP 주소 제어는 외부 IP에 대해서만 구성되며 ServiceNow의 내부 IP 주소는 차단하지 않습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > **IP** 주소 접근 통제 IP 액세스 제어 목록을 보려면 IP 범위 기반 인증 [com.snc.ipauthenticator] 플러그인을 활성화해야 할 수 있습니다.
2. 양식을 작성합니다.

   ⓘ 주: 인스턴스 IP 정보를 찾으려면 ServiceNow - NOW 지원 을 클릭하고 내 **IP** 정보 서비스 카탈로그 항목을 검색합니다.

필드	설명
유형	포함할 접근 통제 규칙의 유형입니다. ◦ 허용: 이 범위의 모든 IP 주소가 이 인스턴스와 상호작용할 수 있습니다. ◦ 거부: 이 범위의 모든 IP 주소는 허용 규칙에 나열되지 않는 한 이 인스턴스와 상호 작용할 수 없습니다. 또한 거부 규칙을 추가할 때 자체 퍼블릭 IP 주소를 거부할 수 없거나 인스턴스가 거부 규칙을 업데이트하지 않습니다. ⓘ 주: 유지관리, 업그레이드 등을 고객 서비스 및 지원지원하기 위해 일부 ServiceNow 내부 IP는 거부 규칙에 의해 차단될 수 없습니다.
방향	IP 접근 제어 규칙의 방향입니다. ◦ 인바운드: 인바운드 트랜잭션을 허용하거나 거부합니다. 이는 인스턴스 외부에서 시작된 트랜잭션입니다. ◦ 아웃바운드: 아웃바운드 트랜잭션을 허용하거나 거부합니다. 이는 인스턴스 내에서 시작된 트랜잭션입니다. ◦ 양방향: 인바운드 및 아웃바운드 트랜잭션을 모두 허용하거나 거부합니다.
활성	선택하면 양식이 활성화됩니다.
설명	접근 제어에 대한 설명입니다.
범위 시작	허용 또는 거부할 IP 주소의 시작 범위입니다. ⓘ 주: 이러한 규칙은 업데이트 세트 전송에도 영향을 줍니다. IP 주소 액세스 제어로 인해 업데이트 세트가 실패하지 않게 하려면 대상 인스턴스를 예외로 추가하십시오.
범위 끝	허용 또는 거부할 IP 주소의 끝 범위입니다. ⓘ 주: 특정 VPN 주소로만 액세스를 제한하려면 거부 필드에 0.0.0.0에서255.255.255.255까지의 거부 범위를 입력하고 허용된 특정 VPN 범위만 입력합니다.

3. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

거부된 IP 주소 찾기

인스턴스의 노드 로그 파일에서 거부된 IP 주소를 찾습니다.

시작하기 전에
필요한 역할: admin.

이 태스크 정보
차단된 IP 주소에 대한 로그 항목은 다음과 같이 나타납니다. `2015-10-21 18:37:43 (175) http-30 ## *** ## *** ## ###: #### ###(xx.xx.xxx.xxx ### ##).`

> **주:** 거부된 IP 주소는 볼 수 있는 인스턴스의 노드 로그 파일이며 시스템 로그에서 볼 수 없습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 로그 > 공공 서비스 > 노드 로그 파일 브라우저입니다..
2. 기간 및 메시지와 같은 기준에 따라 로그를 찾아봅니다.
3. 또한 찾고 있는 로그가 있는 경우 다음으로 이동하여 로그 파일을 다운로드할 수 있습니다. 시스템 로그 > 공공 서비스 > 노드 로그 파일 다운로드.

LDAP 통합

LDAP 통합을 통해 인스턴스에서 기존 LDAP 서버를 사용자 데이터의 기본 소스로 사용할 수 있습니다.

관리자는 LDAP(Lightweight Directory Access Protocol) 디렉터리와 통합하여 사용자 로그인 프로세스를 간소화하고 사용자 생성 및 역할 할당과 같은 관리 작업을 자동화합니다. LDAP 통합을 통해 시스템은 기존 LDAP 서버를 사용자 데이터의 기본 소스로 사용할 수 있습니다. 일반적으로 LDAP 통합은 SSO(Single Sign-On) 구현의 일부이기도 합니다.

통합은 LDAP 서비스 계정 자격 증명을 사용하여 LDAP 서버에서 사용자 DN(고유 이름)을 검색합니다. 사용자의 DN 값이 지정되면 통합은 사용자의 DN 및 암호를 사용하여 LDAP와 다시 재결합합니다. 사용자가 입력하는 암호는 전적으로 HTTPS 세션에 포함되어 있습니다. 통합은 LDAP 암호를 저장하지 않습니다.

통합은 LDAP 디렉터리에 쓰지 않는 읽기 전용 연결을 사용합니다. 통합은 정보를 쿼리하기만 하고 그에 따라 내부 데이터베이스를 업데이트합니다.

> **주:** 통합 설정에 대한 자세한 내용은 다음 문서를 LDAP 통합 설정참조하십시오.

> **주:** 인스턴스가 LDAP 통합을 사용 중이고 Active Directory 설정에서 사용자가 로그인 시 암호를 재설정하도록 요구하는 경우 사용자는 인스턴스에 로그인할 수 없습니다. 인스턴스는 사용자의 Active Directory 암호를 변경할 수 없습니다.

LDAP 통합의 기능

LDAP 통합 기능에는 다음이 포함됩니다.

예약된 LDAP 새로 고침

LDAP 서버의 예약된 검사는 일반적으로 밤에 한 번 실행됩니다. 적용 가능한 모든 사용자 기록의 속성을 쿼리하고 서버의 계정과 비교합니다. 차이가 있는 경우 변경된 속성으로 사용자 기록을 수정합니다. 새로 고치는 동안 LDAP 서버에 가해지는 부하는 쿼리되는 레코드 수와 비교되는 속성 수에 따라 달라집니다. 사용량이 적은 시간에 새로 고침을 예약하는 것이 좋습니다. 대규모 새로 고침 작업은 보고서 실행과 같은 다른 예약된 작업에 영향을 줄 수 있으므로 충돌을 최소화하도록 계획해야 합니다.

LDAP 수신기

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

LDAP 수신기는 지속적인 쿼리(또는 지속적인 검색)의 버전입니다. LDAP 서버에 대한 변경 사항에 대해 대기 쿼리를 발행하고 지속적으로 응답을 수신합니다. 서버가 지속적인 검색을 지원한다고 가정할 경우, 해당 LDAP 계정에 대한 모든 변경 사항은 LDAP 수신기로 반환되고 약 10초 이내에 인스턴스로 전송됩니다. 이것은 매우 유용한 도구로, 다음 예약된 새로 고침을 기다릴 필요 없이 사용자 계정 세부 정보를 거의 실시간으로 복사할 수 있습니다.

요청 시 LDAP 로그인

LDAP 통합이 설정되면 인스턴스에서는 아직 인스턴스에 계정이 없는 경우에도 새 사용자가 시스템에 로그인할 수 있도록 허용할 수 있습니다. 새 사용자가 인스턴스에 로그인을 시도하면 통합은 이 사용자가 인스턴스에 계정을 가지고 있는지 확인합니다. 통합에서 기존 사용자 계정을 찾지 못하면 입력된 사용자 이름을 LDAP 서버에 자동으로 쿼리합니다. 일치하는 LDAP 계정이 발견되면 통합은 사용자가 입력한 암호로 인증을 시도합니다. 암호가 유효하면, 인스턴스가 사용자에 대한 계정을 생성하고, 모든 해당 LDAP 정보로 계정을 채우고, 사용자를 인스턴스에 로그인합니다.

요청 시 로그인은 LDAP 사용자 임포트 변환 맵을 사용합니다. 변환 맵 요구 사항에 대한 자세한 내용은 다음 문서를 참조하십시오 LDAP 변환 맵.

LDAP 데이터 채우기

주: 이 통합에 설명된 기능은 기본적으로 사용할 수 없습니다. 이 통합에는 숙련된 관리자 또는 ServiceNow 전문 서비스 컨설턴트가 수행하는 배포 후 사용자 지정이 포함됩니다.

LDAP 서버에 통합하면 기존 LDAP 데이터베이스의 사용자 기록으로 인스턴스의 데이터베이스를 빠르고 쉽게 채울 수 있습니다. 데이터 불일치를 방지하기 위해 수신 LDAP 기록을 생성, 무시 또는 건너뛸 수 있습니다.

LDAP 속성을 지정하여 통합이 임포트하는 데이터를 제한함으로써 인스턴스에 노출할 데이터만 임포트할 수도 있습니다. 일반적으로 사용자가 지정하는 LDAP 속성은 통합 변환 맵의 일부가 됩니다. LDAP 속성을 지정하지 않으면 통합은 LDAP 서버에서 사용 가능한 모든 객체 속성을 임포트합니다. 인스턴스는 임포트한 LDAP 데이터를 임시 임포트 세트 테이블에 저장하므로, 임포트한 속성이 많을수록 임포트 시간이 길어집니다. 자세한 내용은 LDAP 속성 지정 문서를 참조하십시오.

LDAP 인증

LDAP Authentication을 사용하여 LDAP 자격 증명 사용에 액세스합니다.

사용자가 로그인 페이지에 네트워크 자격 증명을 입력하는 경우:

1. 인스턴스는 인스턴스를 찾을 수 있도록 자격 증명을 LDAP 서버에 전달합니다.
2. RDN을 사용하면 사용자의 DN 문자열을 검증합니다. `table=sys_user`인 LDAP OU 구성 중 하나 이상에 RDN이 구성되어 있는 경우에만 유효성을 검증합니다.
3. LDAP 서버는 시스템이 액세스 권한을 부여해야 하는지 여부를 판별하는 데 사용하는 인증되거나 인증되지 않은 메시지로 응답합니다.

LDAP 서버에 대해 인증하면 사용자는 네트워크 도메인의 다른 내부 자원에 사용하는 것과 동일한 자격 증명으로 플랫폼에 액세스합니다. 또한 이미 시행 중인 기존 암호 및 보안 정책을 다시 사용할 수 있습니다. 예를 들어 LDAP 서버에 계정 잠금 및 암호 만료 정책이 이미 있을 수 있습니다.

LDAP를 활성화하면 시스템이 이러한 필드로 사용자 기록을 업데이트합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

LDAP 사용자 기록 업데이트

필드	설명
소스	사용자를 검증하는 데 LDAP를 사용할지 여부를 식별합니다. 소스가 ldap로 시작하면 사용자는 LDAP를 통해 검증됩니다. 소스가 ldap로 시작하지 않으면, 로그인 시 사용자 기록의 비밀번호를 사용하여 사용자를 확인합니다.
LDAP 서버	여러 LDAP 서버가 있을 때 사용자를 인증하는 LDAP 서버를 식별합니다.

주: 시스템은 MID 서버를 통한 LDAP 암호 인증을 지원하지 않습니다. 암호 인증을 지원하려면 인스턴스가 LDAP 서버와 직접 연결할 수 있어야 합니다.

LDAP 통합 이해

LDAP 통합을 통해 인스턴스에서 기존 LDAP 서버를 사용자 데이터의 기본 소스로 사용할 수 있습니다.

LDAP 통합 필수 조건

- 디렉터리 서비스 서버는 LDAP v3을 준수해야 합니다.
- 방화벽을 통한 인바운드 네트워크 액세스가 허용되어야 합니다(LDAP 서버에 대한).
- LDAP 서버의 외부 IP 또는 이름입니다
- 읽기 전용 접근 권한이 있는 사용자 자격 증명
- LDAPS의 경우 PKI 인증서

LDAP 통합 타이밍

LDAP 통합은 일반적으로 인스턴스가 가동되기 전에 수행되지만, 언제든지 통합될 수 있습니다.

LDAP 서버 데이터 무결성

일부 사용자는 제3자(이 경우 인스턴스)가 LDAP 서버를 변경(쓰기)하는 것을 우려합니다. LDAP 통합에서 인스턴스는 내부 LDAP 디렉터리에 쓰지 않습니다. 인스턴스가 정보를 쿼리하고 그에 따라 데이터베이스를 업데이트합니다.

인스턴스가 내부 LDAP 서버를 변경하지 않습니다. 서비스 계정은 읽기 전용입니다.

전체 LDAP 통합의 구성요소 수에 따라 LDAP 서버에 대한 대부분의 변경 사항(추가 항목 포함)은 몇 초 이내에 인스턴스에서 사용할 수 있습니다.

LDAP 기록을 동기화된 상태로 유지하려면 LDAP 서버의 주기적인 검사를 예약하여 변경 사항을 선택합니다.

인스턴스는 부서 기록을 동기화하지 않습니다. 사용자 및 그룹 구성원 자격은 LDAP 수신기 메커니즘과 일일 전체 LDAP 찾아보기를 통해 최신 상태로 유지되지만, LDAP에서 사라지면 인스턴스는 이러한 항목을 삭제하지 않습니다.

항목이 삭제되면 전체 기록도 삭제되고 그에 대한 모든 참조가 지워지거나 삭제됩니다. 구성 항목(CI), SLA 계약, 소프트웨어 라이센스, 구매 주문서 및 서비스 카탈로그 항목에는 모두 부서에 대한 참조가 있으며 부서가 삭제되면 해당 참조가 지워집니다. 사용자에 대한 참조가 많으므로 사용자를 삭제하면 해당 사용자가 수행한 작업에 대한 모든 기록이 손실됩니다. 현재 삭제 여부는 고객이 결정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안

연결은 방화벽의 특정 포트를 통해 고정 IP 주소를 사용하는 단일 시스템에서 이루어집니다. 인증은 선택한 읽기 전용 LDAP 계정으로 수행됩니다. 표준 LDAP를 사용하거나 디렉토리에 설치된 SSL 인증서의 공개 측을로드 할 수 있습니다.이 경우 LDAPS를 사용할 수 있습니다. 또 다른 보안 계층을 추가하기 위해 지점 간 IPSEC VPN 터널 옵션도 제공합니다. 자세한 내용 및 가격은 계정 관리자에게 문의하십시오.

보안 **LDAP** 연결

연결	설명
MID 서버	외부 네트워크 트래픽으로부터 LDAP 서버를 보호하려면 로컬 네트워크에 MID 서버를 설치하고 보안 채널을 통해 MID 서버와 통신하도록 시스템을 구성합니다.
LDAPS	암호화된 LDAPS 연결을 설정하려면 LDAP 서버 SSL 인증서의 공개 쪽을 로드합니다. 통합은 인증서를 사용하여 LDAP 서버와 인스턴스 간의 모든 통신을 암호화합니다.
VPN	암호화된 지점 간 IPSEC VPN 터널로 LDAP 서버를 보호하려면 계정 관리자에게 자세한 내용 및 가격을 문의하십시오.

고려해야 할 또 다른 보안 측면은 LDAP 통합에서 공유되는 데이터입니다. 인스턴스에 노출되는 데이터를 제한하려면 변환 맵에 속성을 지정하십시오. 자세한 내용은 LDAP 변환 맵 문서를 참조하십시오.

LDAP 데이터를 인스턴스로 임포트

필수 데이터만 임포트하도록 속성을 정의하는 것이 좋습니다. 정의된 속성은 인스턴스 사용자 데이터베이스에 매핑됩니다.

어떤 특정 속성이 필요한지에 대한 질문에 답할 수 없는데, 이는 프로젝트의 범위와 비즈니스 요구 사항에 따라 결정되기 때문입니다.

지원되는 **LDAP** 서버 유형

인스턴스가 Microsoft Active Directory, Novell, Domino(Lotus Notes) 및 Open LDAP와 성공적으로 통합되었습니다. JNDI를 사용하여 LDAP 서버와 인터페이스합니다. LDAP 서버가 LDAP v3을 준수하면 통합이 성공합니다.

LDAP SSO(Single Sign-On)

LDAP 가져오기와 함께 제공되는 데이터 채우기 기능과 함께 애플리케이션에서 지원하는 외부 인증 기능을 사용하여 사용자가 매번 로그온할 필요가 없도록 할 수 있습니다.

여러 **LDAP** 도메인

여러 도메인을 처리할 때 권장되는 방법은 각 도메인에 대해 별도의 LDAP 서버 기록을 만드는 것입니다. 각 LDAP 서버 기록은 해당 도메인의 도메인 컨트롤러를 가리켜야 합니다. 즉, 로컬 네트워크는 각 도메인 컨트롤러에 대한 연결을 허용해야 합니다.

둘 이상의 네트워크 도메인으로 확장한 후에는 애플리케이션 사용자 이름에 대한 고유한 LDAP 속성을 식별하고 병합 값을 임포트하는 것이 중요합니다. Active Directory의 일반적인 고유 병합 특성은 objectSid 입니다. 고유한 사용자 이름은 LDAP 데이터 설계에 따라 다를 수 있습니다. 일반적인 특성은 `email` 또는 `userPrincipalName`입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

쿼리 제한 처리

기본적으로 Active Directory 2000/2003에는 과도한 로드 및 서비스 거부 공격을 방지하기 위해 1000개의 개체로 제한되는 LDAP 쿼리 제한(maxPageSize)이 있습니다. 이 제한을 처리하는 두 가지 방법이 있습니다.

기본 방법은 한 번에 1,000개 미만의 개체를 반환하도록 쿼리를 분할하는 것입니다. 예를 들어, 문자 'a'로 시작하는 객체만 쿼리한 다음 'b' 객체를 쿼리합니다. 대규모 환경에서 보다 효율적인 방법은 페이징을 사용하도록 설정하는 것입니다. 페이징은 모든 Microsoft Active Directory 서버에서 기본적으로 지원됩니다. 결과를 여러 결과 집합으로 자동으로 분할하므로 쿼리를 여러 요청으로 분할할 필요가 없습니다.

LDAP 쿼리 유형

LDAP 비밀번호가 제공되면 "단순 바인드"가 수행됩니다. LDAP 암호를 제공하지 않으면 "없음"이 사용되며, 이 경우 LDAP 서버는 익명의 로그인을 허용해야 합니다.

LDAP 인증

LDAP에 제공된 서비스 계정 자격 증명을 사용하여 LDAP 서버에서 사용자 DN을 검색합니다. 사용자의 DN 값이 지정되면 사용자 DN과 제공된 암호가 제공된 LDAP와 다시 바인딩합니다.

암호 스토리지

사용자가 입력하는 암호는 전적으로 HTTPS 세션에 포함되어 있습니다. 우리는 그 암호를 어디에도 저장하지 않습니다.

LDAP 인증 설정

LDAP와 관련된 사용자 기록의 다음 필드:

- 소스: 소스 필드는 LDAP를 사용하여 사용자의 유효성을 검사할지 여부를 식별합니다. 소스 필드가 "ldap"로 시작하면 사용자는 LDAP를 통해 검증됩니다. 소스 필드가 'ldap'로 시작하지 않으면, 로그인 시 사용자 기록의 비밀번호를 사용하여 사용자를 확인합니다.
- **LDAP** 서버: 인스턴스는 여러 LDAP 서버를 지원하므로 LDAP 서버 필드는 사용자를 인증하는 데 사용해야 하는 서버를 결정합니다.

LDAP 통합 요구 사항

PKI 인증서, LDAP 호환 디렉터리 서비스 서버를 포함하는 LDAP 통합에 대한 요구 사항을 검토합니다.

LDAP 통합에는 다음이 필요합니다.

- LDAP v3 호환 디렉터리 서비스 서버
  - 방화벽을 통해 (LDAP 서버에 대한) 인바운드 네트워크 액세스 허용
  - (선택 사항) 익명 로그인 허용
  - (선택 사항) 큰 LDAP 쿼리에 대한 페이징 지원
- LDAP 서버의 외부 IP 주소 또는 정규화된 도메인 이름입니다. MID 서버를 사용할 수도 있습니다.
- 선택한 읽기 전용 LDAP 계정
- 여러 도메인의 경우 각 도메인 컨트롤러에 대한 네트워크 액세스
- LDAPS의 경우 PKI 인증서
- LDAP 수신기의 경우 지속적 쿼리(ADNotify)를 지원하는 Microsoft Active Directory 서버

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되는 LDAP 서버

JNDI를 사용하여 LDAP 서버와 인터페이스하면 인스턴스가 다음 서버와 성공적으로 통합됩니다.

- Microsoft Active Directory
- 노벨
- Domino(Lotus Notes)
- LDAP 열기

LDAP 쿼리 제한

기본적으로 Active Directory 2000/2003에는 과도한 로드 및 서비스 거부 공격을 방지하기 위해 1000개의 개체로 제한되는 LDAP 쿼리 제한(maxPageSize)이 있습니다. 시스템에는 이 제한을 처리하는 두 가지 방법이 있습니다.

- 기본 방법은 한 번에 1,000개 미만의 개체를 반환하도록 쿼리를 분할하는 것입니다. 예를 들어, 문자 a로 시작하는 객체만 쿼리한 다음 b 객체를 쿼리합니다.
- 대규모 환경에서 보다 효율적인 방법은 모든 Microsoft Active Directory 서버에서 기본적으로 지원되는 페이징을 사용하도록 설정하는 것입니다. 페이징은 자동으로 결과를 여러 결과 세트로 분할하므로 통합에서 쿼리를 여러 요청으로 분할할 필요가 없습니다.

LDAP 통합 설정

관리자는 LDAP 통합을 사용하여 회사 LDAP 디렉터리에서 사용자의 로그온을 허용할 수 있습니다.

LDAP는 일반적으로 이러한 유형의 통신 채널 중 하나를 사용합니다.

LDAP 커뮤니케이션 채널

연결	설명	LDAP 임포트 지원?	LDAP 인증 지원?
MID 서버 연결	기본적으로 포트 80에서 HTTP를 통해 통신합니다. 이 커뮤니케이션 채널에는 인증서가 필요하지 않습니다. MID 서버와 인스턴스 간의 연결은 HTTPS(포트 443)를 통해 이루어집니다. MID 서버를 사용하여 LDAP를 통해 데이터를 임포트할 수 있지만 LDAP 인증에는 MID 서버를 사용할 수 없습니다. LDAP 서버 정의를 진행합니다.	예	아니요
표준 LDAP 통합	기본적으로 포트 389에서 TCP를 통해 통신합니다. 이 커뮤니케이션 채널에는 인증서가 필요하지 않습니다. LDAP 서버 정의를 진행합니다.	예	예
SSL 암호화 LDAP 통합 (LDAPS)	기본적으로 포트 636에서 TCP를 통해 통신합니다. 이 통신 채널에는 인증서가 필요합니다. 인증서를 가져와 업로드하려면 계속 진행하십시오 LDAP X.509 SSL 인증서 설치 .	예	예
VPN 연결	IPSEC 터널을 통해 통신합니다. 로컬 네트워크에서 IPSEC 터널을 구입하거나 생성합니다. LDAP 서버 정의를 진행합니다.	예	예

MID 서버를 사용하는 경우 MID 서버는 인스턴스에 연결되고 MID 서버도 LDAP 서버에 연결됩니다. 두 경우 모두 MID Server가 연결을 시작합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. 먼저 MID Server는 포트 389의 LDAP를 통해 LDAP 서버에 연결합니다.
2. 그런 다음 MID 서버는 포트 443에서 인스턴스에 대한 HTTPS 암호화 연결을 시작하여 데이터를 인스턴스로 푸시합니다.

VPN, MID Server 및 LDAP에 대한 자세한 내용은 커뮤니티에서 VPN이 필요하지 않음 파트 II 를 참조하세요.

LDAP X.509 SSL 인증서 설치

LDAP 통합을 위해 X.509 인증서를 설치할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. LDAP 서버에서 SSL 인증서를 구입하거나 생성합니다.
2. 다음으로 이동 **LDAP** > 인증서 을 클릭하고 신규를 클릭합니다.
3. 양식 필드를 입력합니다.

필드	설명
이름	인증서 이름입니다.
만료 알림	만료 시 알림 필드에서 선택한 사용자에게 알림을 보내려면 이 옵션을 선택합니다. 기본적으로 이 기능은 사용 설정되어 있습니다.
만료 시 알림	인증서 만료와 관련된 알림을 되살릴 사용자를 선택합니다. 선택한 사용자가 없으면 기본적으로 관리자 역할을 가진 마지막 로그인한 사용자 두 명과 함께 로그인한 사용자가 추가됩니다.
만료되기 전 경고	인스턴스가 알림을 보내는 만료 전 일수입니다. 20 이상의 값을 입력합니다. Istanbul 및 이후 릴리스로 업그레이드된 인스턴스에서는 더 큰 값을 지정하지 않는 한 이 값이 20으로 설정됩니다.
활성	이 인증서가 활성 상태임을 나타내는 확인란입니다.
형식	인증서의 형식입니다.
유형	인증서 컨테이너입니다. 인스턴스는 신뢰 스토어, Java 키 스토어 및 PKCS#12 키 스토어의 인증서를 인식합니다.
유효 기간 (시작)	인스턴스가 이 필드에 유효한 인증 시작일을 자동으로 추가합니다. 인증서를 X.509 인증서 기록에 첨부하여 이 필드를 채웁니다.
만료	인스턴스가 이 필드에 인증서 만료 날짜를 자동으로 추가합니다. 인증서를 X.509 인증서 기록에 첨부하여 이 필드를 채웁니다.
며칠 후 만료	만료까지 계산된 일수입니다.
간단한 설명	인증서에 대한 설명입니다.
발급자	인스턴스가 이 필드에 인증서 발급자를 자동으로 추가합니다. 인증서를 X.509 인증서 기록에 첨부하여 이 필드를 채웁니다.
제목	인스턴스는 이 필드에 제목의 인증서를 자동으로 추가합니다. 인증서를 X.509 인증서 기록에 첨부하여 이 필드를 채웁니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
PEM 인증서	X509 인증서의 값을 입력합니다.

주: 통합은 현재 인스턴스와 IdP 간의 통신에서 인증서에 서명하지 않습니다.

4. 저장을 클릭합니다.

다음에 수행할 작업
Validate Stores/Certificates(저장소/인증서 확인)를 클릭하여 신뢰 저장소와 인증서를 테스트합니다.

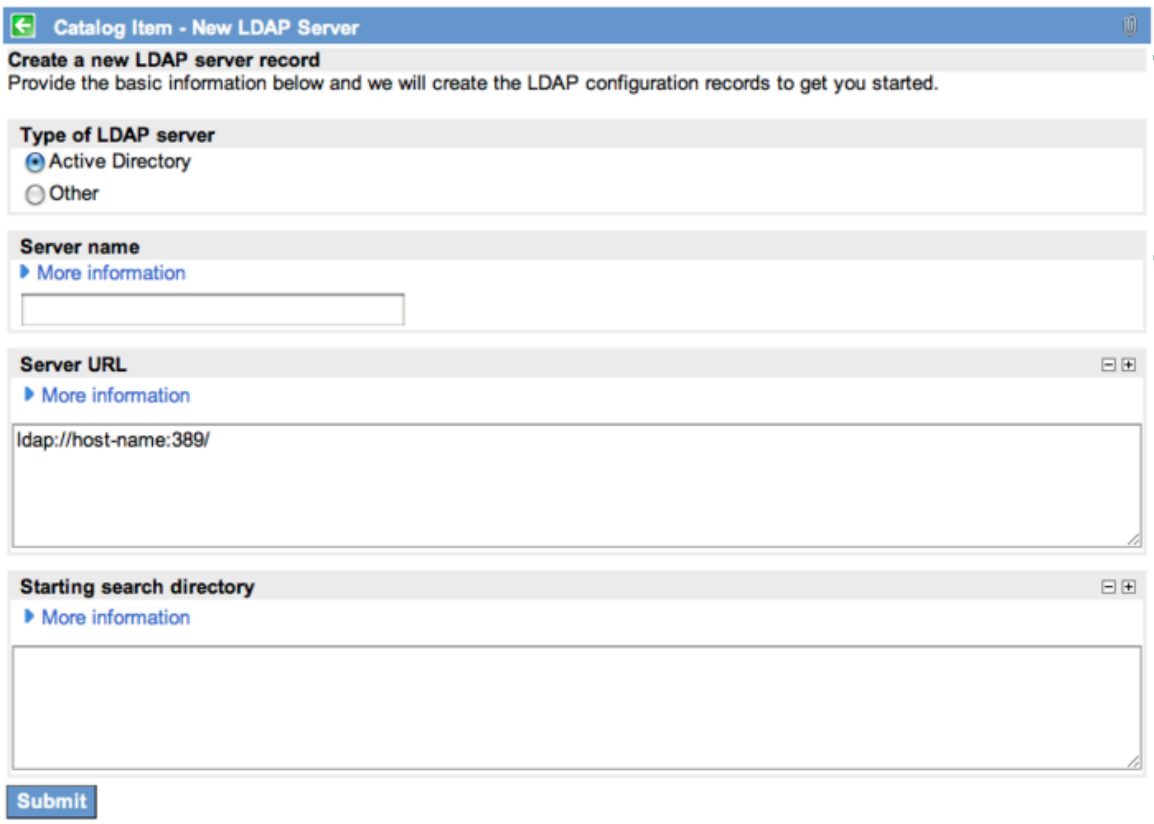
LDAP 서버 정의

인스턴스에 새 LDAP 서버 기록을 생성합니다.

시작하기 전에
필요한 역할: admin.

프로시저

1. 다음으로 이동 모두 > 시스템 **LDAP** > 새 서버 작성.
2. 양식 필드를 채웁니다.



서버 **URL** 필드에서 모든 서버의 유효한 URL은 공백으로 구분되어 나타납니다. 서버는 먼저 운영 상태별로 정렬되며, 작동 중인 서버가 먼저 나열된 다음 지정한 순서 값에 따라 정렬됩니다. 나열된 첫 번째 서버가 기본 LDAP 서버입니다. 나머지는 중복 서버입니다.

주: 실제 작동 상태의 변경과 디스플레이 사이에는 약간의 지연이 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

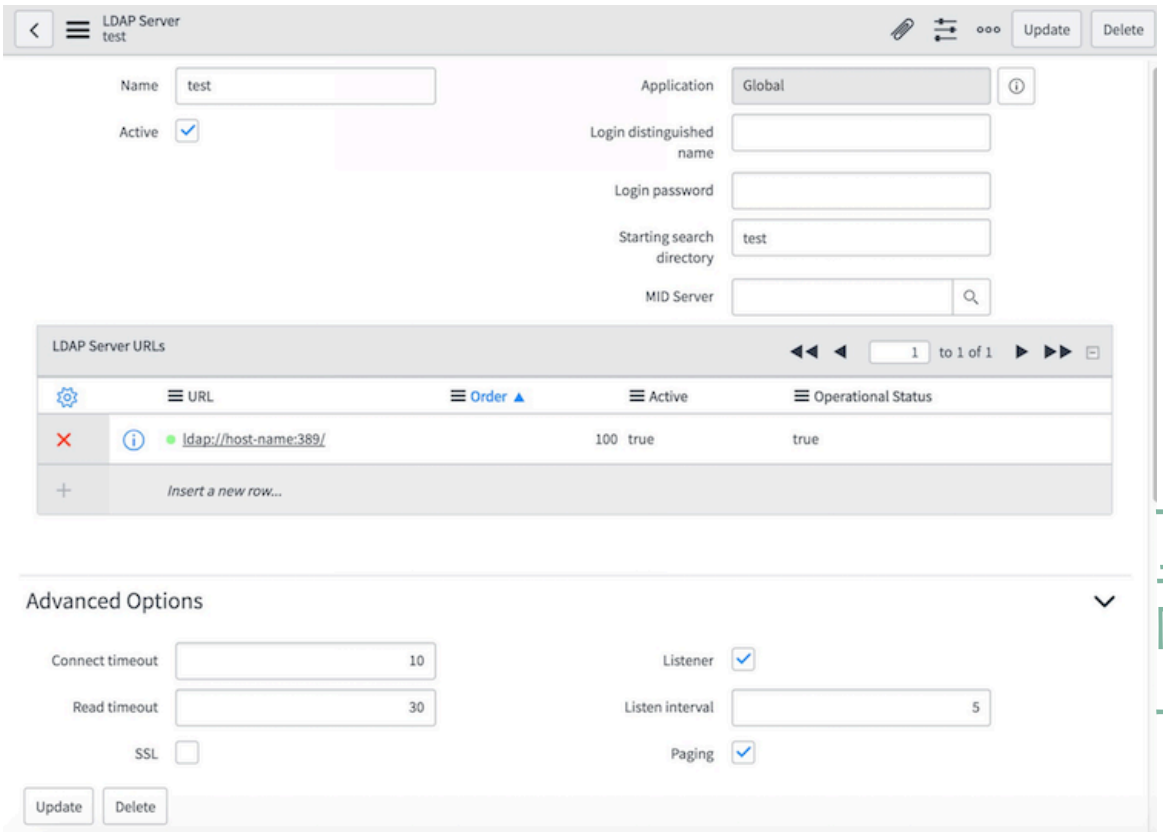
또는 기존 LDAP 서버 기록으로 이동한 다음 LDAP 서버 URL 포함된 목록에 행을 삽입하여 중복 LDAP 서버를 추가할 수 있습니다.

3. 제출을 클릭합니다.

   주: 다음으로 이동하여 기존 LDAP 서버 기록을 수정할 수도 있습니다. 시스템 **LDAP** > **LDAP** 서버 필요한 변경을합니다.

4. 필요에 따라 필드를 변경합니다.

LDAP 서버 양식



필드	설명
이름	서버 이름을 입력합니다.
활성	서버가 활성 상태인 경우 이 확인란을 선택합니다.
LDAP 서버 URL	기본 및 백업 LDAP 서버의 URL을 입력합니다. 서버는 먼저 운영 상태별로 정렬되며, 작동 중인 서버가 먼저 나열된 다음 지정한 순서 값에 따라 정렬됩니다. 나열된 첫 번째 서버가 기본 LDAP 서버입니다. 나머지는 중복 서버입니다.
서버 URL	서버의 URL을 입력합니다. 필요한 경우 이 필드를 추가하도록 양식을 구성합니다. 이 필드는 **LDAP** 서버 **URL** 필드에서도 볼 수 있는 LDAP 서버 목록을 공백으로 구분하고 운영 상태 및 URL 순서 값별로 정렬하여 표시하는 계산된 읽기 전용 필드입니다.
로그인 고유 이름	LDAP 연결을 인증하는 사용자의 고유 이름(DN)을 입력합니다. LDAP 디렉터리 서버에 액세스하려면 사용자 이름이 전체 고유 이름 형식이어야 합니다. `servicenow@service-now.com`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
로그인 암호	서버의 암호를 입력합니다.
검색 시작 디렉터리	기본 검색 디렉터리의 상대 고유 이름(RDN)을 입력합니다. 이 LDAP 서버에 대한 모든 쿼리는 이 RDN에서 시작됩니다.
MID 서버	LDAP 서버에 연결하는 데 사용할 MID 서버를 선택합니다. MID 서버를 사용하여 LDAP 연결을 설정하면 LDAP 서버를 외부 네트워크 트래픽에 노출할 필요가 없습니다. 또한 LDAP 서버와 ServiceNow 데이터 센터 간에 VPN 터널을 설정할 필요가 없습니다. 주: ◦ LDAP 서버 구성 기록을 읽을 수 있으려면 MID 서버 사용자에게 user_admin 역할이 있어야 합니다. ◦ MID Server에서 사용할 수 없는 것은 다음과 같습니다. ▪ LDAP 인증 ▪ SSL 연결
연결 제한 시간	MID 서버가 구성된 경우 이 설정에 관계없이 10초 후에 연결 시간이 초과됩니다. 이 설정은 하드 코딩되어 있으며 변경할 수 없습니다.
읽기 제한 시간	통합이 LDAP 데이터를 읽어야 하는 시간(초)을 지정합니다. 연결이 읽기 제한 시간을 초과하면 통합에서 LDAP 데이터 읽기를 중지합니다. SSL 연결을 사용하는 경우 시스템 속성을 사용하여 읽기 제한 시간 값을 설정할 수도 있습니다 *com.glide.ssl.read.timeout*. 이 필드와 시스템 속성 모두에 시간 제한 값을 입력하면 가장 낮은 시간 제한 값이 우선합니다.
SSL	LDAP 서버가 SSL로 암호화된 연결을 만들도록 하려면 이 확인란을 선택합니다. MID 서버를 선택한 경우 이 필드를 사용할 수 없습니다. LDAPS 통합을 사용하고 기본 SSL 포트가 636인 경우 추가 구성이 필요하지 않습니다. SSL이 자동으로 활성화됩니다. LDAPS 통합에서 다른 SSL 포트를 사용하는 경우 대체 SSL 연결 속성을 정의합니다. 주: 네트워크 관리자가 로컬 방화벽을 구성하여 응용 프로그램 서버가 LDAP 서버에 액세스할 수 있도록 해야 합니다. LDAP 서버가 내부 네트워크 내에 있는 경우 방화벽은 올바른 포트의 방화벽을 통해 응용 프로그램 서버의 IP 주소를 전달(또는 NAT)합니다.
수신기	통합에서 영구 검색 요청 제어를 지원하는 Active Directory 서버 또는 LDAP 서버를 주기적으로 폴링 Microsoft 하려면 이 확인란을 선택합니다. 또한 MID 서버를 선택한 경우 해당 MID 서버에서 수신기 기능을 사용할 수 있습니다. 자세한 내용은 LDAP 수신기 활성화 및 시스템 속성 설정 문서를 참조하십시오.
수신 대기 간격 (시간 제한 값)	통합이 모든 연결에서 LDAP 데이터를 수신하는 수신기 시간 제한 값(분)을 지정합니다. 연결이 수신 대기 간격을 초과한 후 통합에서 LDAP 데이터에 대한 수신 대기를 중지합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
페이징	LDAP 서버가 여러 쿼리를 제출하지 않고 LDAP 속성 데이터를 여러 결과 세트로 분할하도록 하려면 이 확인란을 선택합니다.

주: LDAP 암호를 제공하면 통합에서 단순 바인딩 작업을 수행합니다. LDAP 암호를 제공하지 않으면 LDAP 서버에서 익명 로그인을 허용해야 하며, 그렇지 않으면 통합이 LDAP 서버에 바인딩할 수 없습니다.

결과
LDAP 서버 기록이 활성으로 설정되면 시스템은 자동으로 모든 연결을 테스트하여 유효성을 확인합니다.
확인 포함 사항:

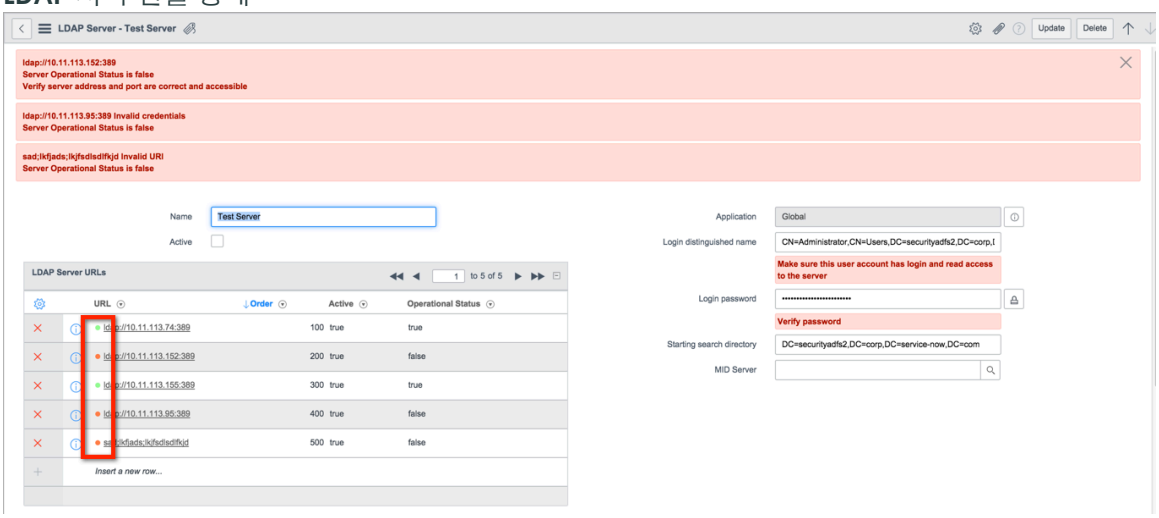
- 제공된 URL 및 포트에서 LDAP 서버에 액세스할 수 있습니다.
- LDAP 서버 URL의 형식이 올바로 지정되었습니다.
- 로그인 자격 증명이 유효합니다.

Fuji 릴리스부터 시스템은 각 서버 URL 옆에 색이 지정된 점을 표시합니다.

LDAP 서버 연결 아이콘

색상	설명
녹색	서버가 활성 상태이고 작동 중인 경우입니다.
회색	서버가 활성 상태도 아니고 작동 중도 아닙니다.
적색	서버가 활성 상태이지만 작동하지 않습니다.

LDAP 서버 연결 상태



LDAP 수신기 활성화 및 시스템 속성 설정

수신기 활성화는 선택 사항입니다. 활성화된 경우, 수신기는 LDAP 서버에 업데이트가 있는 직후 LDAP 레코드를 처리하도록 시스템에 알립니다.

시작하기 전에
필요한 역할: admin.

이 태스크 정보
수신기는 LDAP 서버의 변경 내용을 주기적으로 검색하는 전용 프로세스입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수신기는 지속적 쿼리(ADNotify)를 지원하는 Microsoft Active Directory 서버 또는 지속적 검색 요청 제어를 지원하는 LDAP 서버(OID 2.16.840.1.113730.3.4.3)에 배포할 수 있습니다.

LDAP 서버가 지속적인 검색을 지원하는 경우, LDAP 수신기는 해당 LDAP 계정에 대한 사용자 및 그룹 변경 사항을 인식하여 약 10초 내에 인스턴스로 전달합니다. 이렇게 하면 인스턴스가 예약된 다음 새로 고침을 기다릴 필요 없이 사용자 계정 상세 정보의 거의 실시간 복사본을 가질 수 있습니다. LDAP 수신기는 사용자 [sys_users] 테이블과 그룹 [sys_user_group] 테이블에 매핑되는 객체만 동기화할 수 있습니다.

주: 수신기를 통해 사용자가 추가되었지만 사용자가 OU 필터에 정의된 요구 사항을 충족하지 않는 경우 인스턴스는 LDAP 서버의 기록을 무시합니다. 기준을 충족하면 사용자가 인스턴스에 추가됩니다.

수신기를 활성화하려면:

프로시저

1. 다음으로 이동 모두 > 시스템 **LDAP** > **LDAP** 서버.
2. 구성할 LDAP 서버를 선택합니다.
3. 수신기 확인란을 선택합니다.
4. 업데이트를 클릭합니다.

주:

시스템은 LDAP OU 필터와 일치하는 사용자 기록만 임포트합니다. 필터 요구 사항을 충족하지 않는 수신 사용자 기록은 잘못된 것으로 플래그가 지정되고 임포트에서 무시됩니다. 관리자는 자세한 LDAP 로깅을 사용하여 수신 기록이 LDAP OU 필터와 일치하지 않는지 확인할 수 있습니다.

5. 옵션: 시스템 속성 [sys_properties] 테이블로 이동하여 LDAP 수신기 시스템 속성을 설정합니다.

LDAP 수신기 속성

속성	설명
glide.ldap.listener.use_background_transaction	true일 때는 LDAP 수신기가 백그라운드 트랜잭션으로 시 LDAP 수신기를 백그라운드 트랜잭션으로 실행하면 할당 수신기 시작/중지 트랜잭션은 최대 기간(기본적으로 5분 후 트랜잭션을 취소할 수 있습니다. 이 동작은 LDAP 수신 대기하는 것을 방지합니다. 주: 이 속성은 MID 서버를 사용하지 않는 LDAP 연결에만 적용됩니다. MID 서버를 통과하는 LDAP 연결의 동작을 제어하는 데 사용합니다 *glide.ldap.listener.mid.use_background* ◦ 유형: true | false ◦ 기본값: false ◦ 위치: 시스템 속성 [sys_properties] 테이블에 추가
glide.ldap.listener.mid.use_background_transaction	true일 때는 LDAP 수신기가 백그라운드 트랜잭션으로 시 LDAP 수신기를 백그라운드 트랜잭션으로 실행하면 할당 수신기 MID 트랜잭션 시작/중지가 최대 기간(기본적으로 후 트랜잭션을 취소할 수 있습니다. 이 동작은 LDAP 수신 대기하는 것을 방지합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	주: 이 속성은 MID 서버를 사용하는 LDAP 연결에만 적용됩니다. MID 서버를 통과하지 않는 LDAP 연결의 동작을 제어하는 데 사용합니다 *glide.ldap.listener.use_background_tra* ◦ 유형: true | false ◦ 기본값: false ◦ 위치: 시스템 속성 [sys_properties] 테이블에 추가
glide.ldap.listener.mid.one_listener	true일 때는 단일 ECC 큐 메시지만 작성되어 MID 서버를 수신기를 시작 또는 중지합니다. false인 경우, 여러 ECC 생성될 수 있으며, 이로 인해 LDAP 수신기를 시작하거나 스레드가 생성됩니다. ◦ 유형: true | false ◦ 기본값: true ◦ 위치: 시스템 속성 [sys_properties] 테이블에 추가

LDAP 속성 지정

LDAP 서버 속성 필드를 사용하여 LDAP 서버 쿼리 에 포함된 속성을 지정합니다. 이렇게 하면 성능뿐만 아니라 보안도 향상할 수 있습니다.

기계번역

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
기본적으로 시스템은 LDAP 서버에서 읽을 수 있는 권한이 있는 각 객체에 대한 모든 속성을 로드합니다. 속성 필드를 사용하여 LDAP 쿼리가 반환하는 속성을 지정하고 그에 따라 제한할 수 있습니다. 대규모 LDAP 임포트에 이 접근 방식을 사용하면 임포트 속도를 크게 향상시킬 수 있습니다.

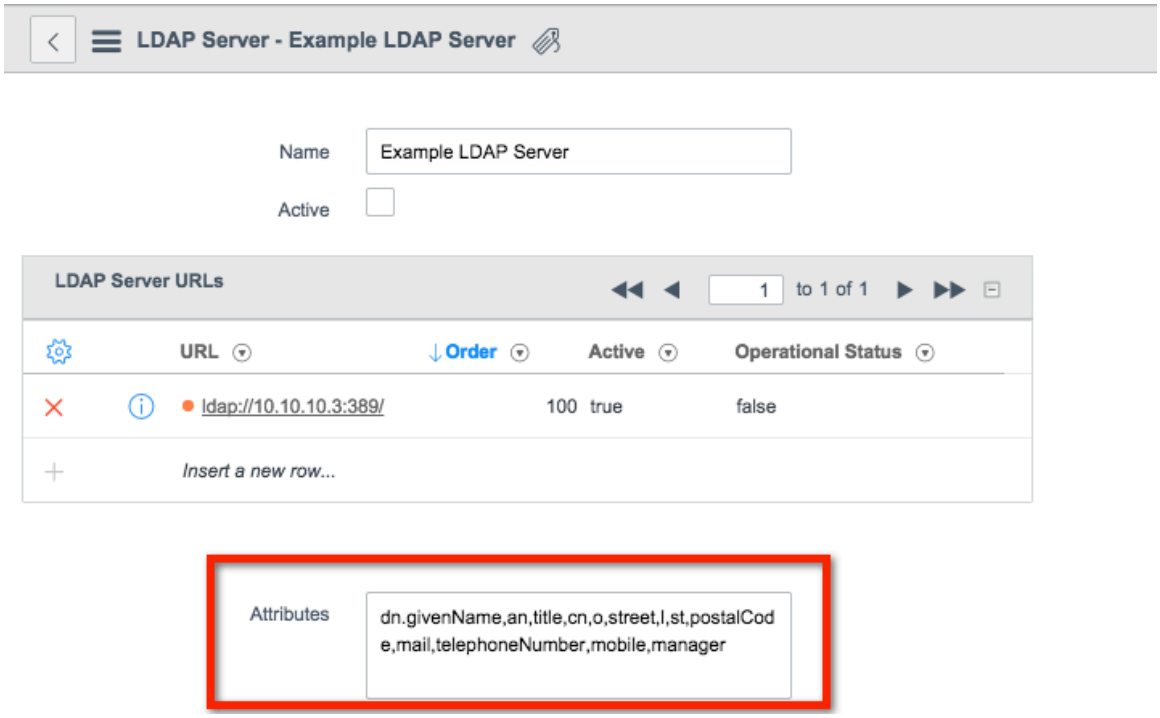
프로시저

가능한 경우 속성을 명시적으로 정의합니다.

인스턴스에 노출하고 싶지 않은 정보가 있는 경우 속성을 제외합니다. LDAP 서버 속성을 지정하지 않으면 시스템이 새 속성에서 데이터를 로드하느라 새 속성이 LDAP 서버 객체에 추가될 때 사용자 트랜잭션이 오랜 시간 동안 동결될 수 있습니다.

주: LDAP 데이터에 대한 변환 맵 선택 또는 작성에 설명된 관리자 조회 스크립트를 사용하려면 속성 필드에 관리자 및 **dn**(고유 이름)을 지정합니다. 두 속성 모두 변환 맵의 일부가 될 필요는 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



LDAP 연결 테스트

사용자가 LDAP 서버 양식을 열 때마다 인스턴스가 자동으로 연결을 테스트합니다. 또는 LDAP 서버 양식에서 LDAP 서버에 대한 연결을 수동으로 테스트할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
기본적으로 LDAP 서버에 연결하는 데 문제가 있는 경우 LDAP 서버 양식에 오류 메시지가 나타납니다.

주: 직원은 인스턴스와 LDAP 서버 간의 연결을 확인할 수도 있습니다. LDAP 연결을 확인하는 데 도움이 필요하면 기술 지원에 문의하십시오.

연결을 수동으로 테스트하려면:

프로시저

1. 다음으로 이동 모두 > 시스템 **LDAP** > **LDAP** 서버.
2. 테스트할 LDAP 서버를 선택합니다.
3. 관련 링크에서 연결 테스트를 클릭합니다.
4. 관련 링크에서 찾아보기를 클릭하여 적절한 LDAP 디렉토리 구조가 시스템에 표시되는지 확인합니다.
5. 옵션: 연결에 성공한 경우 찾아보기 를 클릭하여 인스턴스에 표시되는 소스 LDAP 디렉터리 구조를 봅니다.

   주: 찾아보기 창의 왼쪽에 있는 필터 및 **RDN** 필드는 오른쪽의 검색 필드를 사용할 때 무시됩니다.

결과
이 인스턴스는 연결 테스트 결과에 따라 LDAP 서버의 운영 상태를 변경합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인스턴스가 운영 상태 값이 다운인 서버에 대한 연결을 설정하면 운영 상태 값이 자동으로 가동으로 변경됩니다. 이 기능은 자동 및 수동 연결 테스트 모두에 대해 지원됩니다.
- 운영 상태 값이 **UP**인 서버에 연결할 수 없는 경우 운영 상태 값은 자동으로 **DOWN**으로 변경됩니다. 이 기능은 수동 테스트가 아닌 자동 연결 테스트에만 지원됩니다.

LDAP 조직 단위 정의

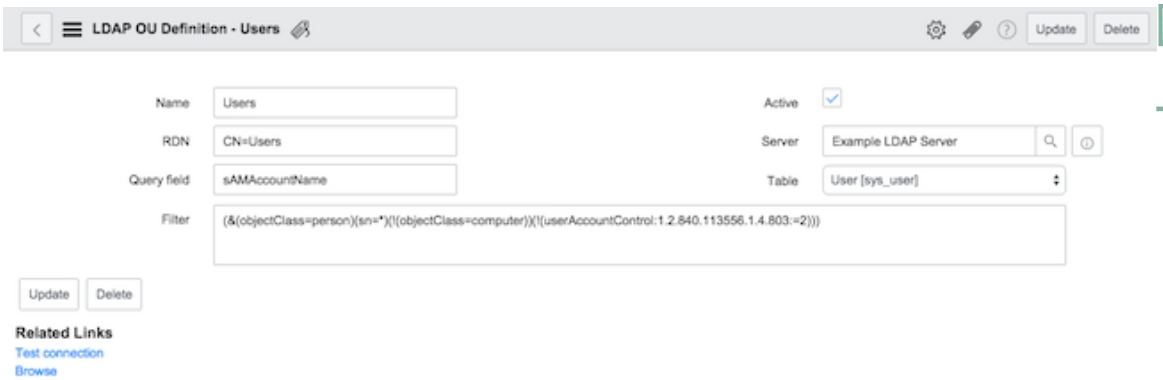
OU(조직 단위) 정의는 통합에 사용할 수 있는 LDAP 소스 디렉터리를 지정합니다.

시작하기 전에
필요한 역할: admin.

이 태스크 정보
OU 정의에는 위치, 사람 또는 사용자 그룹이 포함될 수 있습니다. 모든 LDAP 서버 정의에는 두 개의 샘플 OU 정의가 있는데 하나는 그룹을 시스템으로 가져오는 데 사용되는 정의이고 다른 하나는 사용자에 대한 정의입니다.

프로시저

1. 다음으로 이동 모두 > 시스템 **LDAP** > **LDAP** 서버.
2. 구성할 LDAP 서버를 선택합니다.
3. **LDAP OU** 정의 관련 목록에서 그룹 또는 사용자 샘플 OU 정의를 선택합니다.
4. LDAP OU 정의 양식을 작성합니다(표 참조).
5. 업데이트를 클릭합니다.
   시스템이 LDAP 서버에 대한 연결을 자동으로 테스트합니다.
6. 관련 링크에서 찾아보기를 클릭하여 OU 정의가 반환하는 LDAP 디렉터리 레코드를 봅니다.



OU 정의 양식

필드	설명
이름	이 OU를 참조할 때 통합이 사용하는 이름을 지정합니다. 여기에 입력한 이름은 데이터 소스 기록에서 LDAP 대상이 됩니다.
RDN	검색할 하위 디렉터리의 상대적 고유 이름을 지정합니다. 이 RDN은 LDAP 서버 정의의 검색 시작 디렉토리와 결합되어 이 조직 구성 단위에 대한 정보를 포함하는 하위 디렉토리를 식별합니다. 예를 들어 샘플 OU 정의는 `CN=Users` 의 RDN 값을 사용하여 LDAP 디렉터리 `CN=Users,DC=service-now,DC=com` 및 이 지점 아래의 모든 디렉터리를 검색합니다. 이 필드는 LDAP 시스템의 하위 디렉토리와 일치해야 합니다.
쿼리 필드	LDAP 서버 내에 기록을 쿼리할 속성의 이름을 지정합니다. 쿼리 필드는 단일 및 여러 도메인 인스턴스 모두에서 고유해야 합니다. 최상의 결과를 내려면 여러 도메인 인스턴스에서 사용자를 고유하게 식별할 수 있는 이메일 주소 또는 기타 자격 증명을

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	사용하십시오. Active Directory는 **sAMAccountName** 특성을 사용합니다. 다른 LDAP 서버는 **cn** 속성을 사용하는 경향이 있습니다. 주: 쿼리 필드는 사용자 [sys_user] 테이블의 사용자 **ID** 필드에 매핑되어야 합니다. 예를 들어 Active Directory 사용자가 `joe.example`로 로그인하는 경우 사용자 **ID** 값이 **joe.example** 인 사용자 레코드와 **sAMAccountName** 값이 **joe.example**인 LDAP 레코드가 있어야 합니다.
활성	OU 정의를 활성화하고 관리자가 데이터 임포트를 테스트할 수 있도록 하려면 이 확인란을 선택합니다. 그러나 통합은 활성 OU 정의에서만 시스템으로 데이터를 가져올 수 있습니다.
테이블	LDAP 서버에서 매핑된 데이터를 수신하는 테이블을 지정합니다. 사용자의 경우 사용자 **(sys_user)**를 선택하고 그룹의 경우 그룹**(sys_group)**을 선택합니다.
필터	LDAP 필터 문자열을 입력하여 OU에서 임포트할 특정 기록을 선택합니다. LDAP 필터 쿼리가 구체적일수록 쿼리의 효율성이 높아집니다. 예를 들어, 사용자 LDAP OU 정의는 다음 필터를 사용하여 사람으로 분류되고, **sn** 속성 값을 가지며, 컴퓨터가 아니고, 비활성으로 플래그가 지정되지 않은 기록을 선택합니다. `(&(objectClass=person)(sn=*)(!( objectClass=###)) (! ( userAccountControl:1.2.840.113556.1.4.803:=2)))` 인터넷에서 `LDAP ## RFC`를 검색하여 LDAP 필터 구문에 대한 설명을 찾을 수 있습니다.

Example: 조직 단위 정의 예시

다음과 같은 디렉터리 구조를 가진 LDAP 서버가 있다고 가정합니다.

dc=내 도메인, dc=com

- ou=그룹
  - cn=개발
  - cn=HR
  - cn=판매
- ou=사용자
  - ou=개발
  - ou=HR
  - ou=판매

또한 애플리케이션에서 HR 그룹 및 HR 사용자를 제외하려 한다고 가정해 보겠습니다. 다음을 따르십시오.

1. dc=my-domain,dc=com의 시작 검색 디렉터리를 사용하여 LDAP 서버 기록을 생성합니다.
2. cn=HR을 제외하는 필터로 ou=그룹에 대한 OU 정의 기록을 생성합니다.
3. ou=HR을 제외하기 위한 필터를 사용하여 ou=Users에 대한 OU 정의 기록을 생성합니다.

OU 정의를 사용하여 추가 속성이나 필터를 지정하지 않으면 LDAP 쿼리는 시작 디렉터리 및 RDN의 전체 하위 트리를 반환합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 예에서 RDN 값이 ou=Groups이고 필터가 없는 OU 정의는 모든 그룹을 반환했을 것입니다. 마찬가지로 RDN 값이 ou=Users이고 필터가 없는 OU 정의는 모든 사용자 및 자식 조직 구성 단위를 반환했을 것입니다.

LDAP에 대한 데이터 소스 작성

각 LDAP OU(조직 단위) 정의에는 고유한 관련 데이터 소스 목록이 있습니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

주: 로드 테스트 작업이 제대로 작동하려면 **LDAP** 서버와**LDAP OU** 정의 가 모두 활성 상태여야 합니다. 테스트 로드가 처음 활성화되면 시스템은 최대 20개의 기록을 샘플링하여 임포트 세트 필드의 길이를 결정합니다. 샘플링된 기록에 사용자 **ID** 필드에 대한 값이 포함되어 있지 않으면 시스템은 모든 후속 임포트의 필드 길이를 기본 길이인 40으로 설정합니다. 임포트는 임포트 세트 테이블 필드 길이를 초과하는 임포트된 데이터를 자릅니다. 또한 사용자 **ID** 필드는 최대 40자로 잘립니다. 로드된 20개의 기록은 변환할 수 없으며 테스트 목적으로만 사용된다는 점에 유의하십시오. 테스트 기록에 사용자 **ID** 필드에 대한 값이 포함되어 있으면 테스트 기록에서 가장 긴 사용자 ID의 필드 길이를 기준으로 필드 길이가 설정됩니다.

새 데이터 소스를 만들려면 다음을 수행합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 **LDAP** > **LDAP** 서버.
2. 구성할 LDAP 서버를 선택합니다.
3. **LDAP OU** 정의 관련 목록에서 그룹 또는 사용자 같은 항목을 선택합니다.
4. 데이터 소스 관련 목록에서 새로 만들기를 클릭합니다.
5. 데이터 소스 양식을 작성합니다(표 참조).
6. 제출을 클릭합니다.
7. 관련 링크에서 20개 기록 로드 테스트를 클릭하여 데이터 소스가 LDAP 데이터를 임포트 테이블로 가져올 수 있는지 테스트합니다.

데이터 소스 양식

필드	설명
이름	이 데이터 소스를 참조할 때 통합이 사용하는 이름을 지정합니다.
임포트 세트 테이블 이름	시스템이 임포트한 LDAP 기록 및 속성을 임시로 저장할 스테이징 테이블의 이름을 입력합니다. 임포트된 LDAP 기록을 보려면 이 테이블을 검토하십시오. 모든 LDAP 데이터 소스에 대해 동일한 임포트 세트 테이블 이름을 사용할 수 있습니다.
유형	임포트한 데이터가 LDAP 데이터임을 표시하려면 **LDAP** 를 선택합니다. **LDAP** 유형을 선택하면 양식에 **LDAP** 대상 필드가 표시됩니다.
LDAP 대상	이 데이터 소스와 연결된 LDAP OU 정의를 선택합니다.

LDAP 사용자 자동 프로비저닝

LDAP 서버에는 있지만 아직 인스턴스에는 없는 사용자를 자동으로 프로비저닝합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

시스템 속성 [sys_properties] 테이블에 다음 속성을 생성합니다.

LDAP 속성

LDAP 속성	설명
glide.ldap.authentication	사용자를 인증하기 위해 LDAP를 사용하여 LDAP 인증을 사용하도록 설정합니다. 이 속성을 **true** (기본값)로 설정합니다.
glide.ldap.user.autoprovision	사용자가 LDAP에는 있지만 아직 인스턴스에는 없는 경우 시스템이 사용자 [sys_user] 테이블에 사용자를 자동으로 생성할 수 있도록 합니다. 이 속성을 **true** (기본값)로 설정합니다.

자동 프로비저닝이 작동하려면 이 두 속성을 모두 **true** 로 설정해야 합니다.

MID 서버를 통한 **LDAP** 통합

관리자는 MID(Management, Instrumentation, Discovery) 서버에서 LDAP 데이터 소스를 사용하여 통합할 수 있습니다.

MID 서버를 사용하면 외부 애플리케이션, 데이터 소스 및 서비스 간에 Now Platform 데이터를 통신하고 이동할 수 있습니다. MID 서버 설치에 대한 자세한 내용은 MID 서버 설치를 참조하십시오.

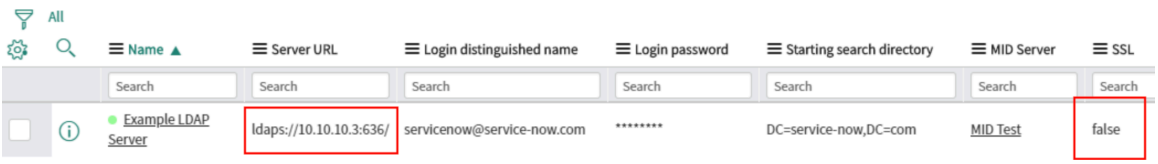
MID 서버를 사용하여 LDAP 연결을 설정하면 LDAP 서버를 외부 네트워크 트래픽에 노출할 필요가 없습니다. LDAP 서버와 데이터센터 간에 VPN 터널을 설정할 필요가 없습니다. MID 서버 사용자에게 LDAP 서버 구성 기록을 읽을 수 있는 user_admin 역할이 있어야 합니다.

주: MID 서버는 LDAP에서 사용자 및 그룹 기록을 새로 고치기 위해 `UI ## <instance>/sys_ui_action.do?sys_id=1b4f7ef30a0001060058e223c9a5744c` 를 사용하는 것을 허용하지 않습니다.

MID Server 연결은 기본적으로 포트 80에서 HTTP를 통해 통신합니다. 이 커뮤니케이션 채널에는 인증서가 필요하지 않습니다. MID 서버와 인스턴스 간의 연결은 HTTPS(포트 443)를 통해 이루어집니다. 인스턴스는 LDAP 또는 LDAPS를 사용하여 LDAP 서버에 직접 연결합니다. 이 연결은 인터넷 또는 VPN 터널을 통해 이루어질 수 있습니다.

주: LDAP는 암호 인증을 사용하여 MID 서버를 통해 통신할 수 없습니다.

SSL을 통한 보안 통신의 경우 MID 서버용 SSL 인증서를 추가해야 합니다. LDAP 서버 URL을 LDAP에서 LDAPS로 변경하고 포트 636으로 변경합니다.



주: 새 LDAP 서버를 만드는 경우 MID 서버 SSL 플래그는 기본적으로 false로 설정됩니다. 이 동작은 무시해도 됩니다.

특정 LDAP 서버에 대한 연결 속성을 설정하려면 문서를 참조하십시오 LDAP 서버 정의.

LDAP 연결 모니터링 구성

LDAP 연결 모니터링 및 알림을 변경하거나 사용하지 않도록 설정합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
LDAP 서버 연결이 실패하면 인스턴스가 LDAP 관리자 그룹에 구성된 사용자에게 이메일을 자동으로 보냅니다. 이는 **LDAP** 연결 테스트예약된 작업으로 시작되는 이메일 알림을 사용합니다. 이 이메일 알림은 기본적으로 사용 설정되어 있습니다.

주: LDAP 관리자 그룹에 구성원이 하나 이상 없으면 인스턴스가 이메일 알림을 보내지 않습니다. 이메일을 수신할 사용자로 이 그룹을 채워야 합니다.

기본적으로 예약된 작업은 15분마다 연결을 테스트합니다. 이 간격을 변경하거나 모니터링을 비활성화하려면 다음을 수행합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 예약된 작업.
2. **LDAP** 연결 테스트를 엽니다.
3. 다음 중 하나를 수행합니다.
   - 반복 간격 필드에서 간격을 변경합니다.
   - 활성 확인란의 선택을 취소하여 모니터링을 비활성화합니다.

MID 서버를 통해 이진 데이터 임포트

관리자는 MID 서버를 통해 LDAP 통합으로 BLOB(Binary Large Object) 데이터를 임포트할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보

프로시저

1. 이진 데이터를 임포트할 LDAP 열의 이름을 시스템 속성 `glide.ldap.binary_attributes`에 추가합니다.
2. 이름 `glide.ldap.binary_attributes` 와 시스템 속성에 대해 설정한 값과 동일한 값을 사용하여 MID 서버 속성을 추가합니다.

MID 서버를 통한 **LDAP** 통합 문제 해결

MID 서버를 통해 LDAP를 통합하는 동안 다음 영역에서 문제가 발생할 수 있습니다.

ECC(External Communication Channel) 큐(디스커버리 > 출력 및 아티팩트 > **ECC** 큐).

연결 테스트 문제

서버 내에서 OU를 정의할 때 LDAP 연결을 확인하는 데 사용되는 연결 테스트 관련 목록이 있습니다. 이 링크를 클릭하면 ECC 큐에 주제 이름이 **LDAPConnectionTesterProbe**인 단일 출력 메시지가 표시되어야 합니다. MID 서버에서 테스트가 완료되면 ECC 큐에 동일한 주제 이름을 가진 입력 메시지가 표시되어야 합니다. 입력 메시지의 이름 열에 **true**가 표시되면 테스트가 성공한 것입니다. 기록을 드릴다운하여 페이로드를 보고 오류 메시지가 포함되어 있지 않은지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연결 테스트

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

문제 찾아보기

서버 내에서 OU를 정의할 때 OU 정의가 반환하는 LDAP 디렉터리 기록을 보는 데 사용되는 찾아보기 관련 목록이 있습니다. 이 링크를 클릭하면 ECC 큐에 주제 이름이 **LDAPBrowseProbe**인 단일 출력 메시지가 표시되어야 합니다. MID 서버에서 데이터가 반환되면 ECC 큐에 동일한 주제 이름을 가진 입력 메시지가 표시되어야 합니다. 입력 메시지의 이름 열에 **true**가 표시되면 테스트가 성공한 것입니다. 기록을 드릴다운하여 페이로드를 보고 오류 메시지가 포함되어 있지 않은지 확인합니다.

임포트 문제 로드

데이터를 업로드할 때(예: 20개 기록 로드 테스트 기능 사용) ECC 큐는 주제 이름이 **LDAPProbe**인 단일 출력 메시지를 표시해야 합니다.

MID 서버에서 데이터가 반환된 후 ECC 큐는 **LDAPProbeCompleted**라는 또 다른 입력 메시지를 표시해야 합니다. 이 입력 메시지의 이름 열에는 반환된 총 기록 수가 표시됩니다.

추가 입력 메시지(**LDAPProbe**라고도 함)가 표시됩니다. 이 입력 메시지의 이름 열에는 배치에서 가장 높은 레코드 번호가 표시됩니다. 반환되는 총 레코드 수가 258이고 일괄 처리 크기가 200(기본값)인 경우 두 개의 LDAPProbe(200, 258) 수신 메시지가 수신되고 LDAPProbeCompleted(258) 수신 메시지 한 개가 수신됩니다.

기록을 드릴다운하여 페이로드를 보고 오류 메시지가 포함되어 있지 않은지 확인합니다.

임포트 로드

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

또한 **LDAPProbeError**라는 출력 메시지를 주시하십시오.

오류 메시지

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.

오류의 상세 정보를 보려면 이름 열의 링크를 클릭하십시오.

LDAP 페이징

LDAP 서버의 페이징 크기가 1000보다 작으면 LDAP 페이징이 작동하지 않습니다. MID 서버 속성을 *glide.ldap.max_results* LDAP 서버 페이징 크기보다 작거나 같은 값으로 설정합니다.

LDAP에서 이진 데이터를 임포트하지 못함

LDAP를 통해 이진 데이터(예: 사용자 사진)를 임포트하려면 MID 서버 속성에 *glide.ldap.binary_attributes*이진 속성을 포함해야 합니다. 사용자 사진 예의 경우 속성은 `jpegphoto`일 수 있습니다.

데이터 임포트 및 맵

LDAP 임포트 맵은 LDAP 데이터베이스의 필드를 인스턴스의 필드와 일치시킵니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: LDAP 매핑은 성능에 영향을 미치므로, 사용량이 적은 시간에 매핑하도록 예약하거나 한 번에 몇 개의 기록을 처리하여 시스템 가용성을 유지하는 방법이 권장됩니다.

필요한 속성 또는 필수 속성만 임포트하는 변환 맵을 정의합니다. 사용 중인 인스턴스의 버전에 따라 LDAP 매핑 관계를 지정하는 방법은 다양합니다.

LDAP 통합을 위해 시스템 LDAP 애플리케이션을 사용하는 버전을 실행 중인지 여부를 알 수 있는 가장 쉬운 방법은 애플리케이션 네비게이터에서 애플리케이션을 찾는 것입니다.

비즈니스 규칙 실행 옵션은 대상 테이블에만 적용됩니다. 대상 테이블에 연결된 변환 맵만 다른 테이블에 연결된 비즈니스 규칙을 실행합니다. 사용자 그룹을 업데이트하고 사용자 그룹 테이블에서 비즈니스 규칙이 실행되고 있는 경우, 그룹에 역할이 정의되어 있어야 합니다.

LDAP 임포트 매핑 옵션

시스템 **LDAP** 애플리케이션?	지도
예	변환 맵을 사용하여 매핑을 지정합니다.
아니요	LDAP 레거시 임포트 맵을 사용하여 매핑 또는 베이스라인 인스턴스에 포함된 기본 LDAP 변환을 지정합니다. 잊지 말고 올바른 필드와 일치하도록 병합 필드를 조정하십시오.

예약된 임포트

예약된 임포트를 사용하면 관리자가 정기적으로 LDAP 데이터를 임포트할 수 있습니다. 기본적으로 LDAP 통합에는 두 개의 샘플 예약된 임포트가 포함됩니다.

- 예제 LDAP 사용자 임포트
- 예제 LDAP 그룹 임포트

두 예 모두 기본적으로 활성화되지 않습니다. 이러한 예약된 임포트를 회사의 비즈니스 요구에 맞게 변경합니다.

LDAP 변환 맵

변환 맵은 임포트 세트 테이블에서 대상 테이블(사용자 또는 그룹)로 데이터를 이동합니다.

LDAP 통합은 표준 임포트 세트와 변환 맵을 사용합니다. 사용자 정의 LDAP 변환 맵을 생성할 수도 있습니다.

중요사항: 사용자 지정 LDAP 변환 맵을 선택하든 작성하든 소스 및 대상 테이블 세트에 대한 활성 변환 맵이 하나 있어야 합니다. 동일한 소스 및 대상 테이블에 대해 여러 변환 맵을 사용하면 일치하는 필드에 대해 병합하지 않으면 대상 테이블에 중복 항목이 생성될 수 있습니다.

기본 **LDAP** 변환 맵

기본적으로 시스템은 LDAP 데이터에 대해 두 개의 변환 맵을 제공합니다.

기본 **LDAP** 변환 맵

변환 맵	소스 테이블	대상 테이블	설명
LDAP 사용자 임포트	[ldap_import]	[sys_user]	LDAP 요청 시 로그인의 일부로 LDAP 자격 증명에서 사용자 기록을 작성하기 위한 기본 변환 맵입니다. Active Directory LDAP 서버에 대한 매핑을 포함합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 **LDAP** 변환 맵

변환 맵	소스 테이블	대상 테이블	설명
LDAP 그룹 임포트	[ldap_group_import]	[sys_user_group]	LDAP OU에서 그룹 기록을 작성하기 위한 기본 변환 맵. Active Directory LDAP 서버에 대한 매핑을 포함합니다.

주: 기본적으로 시스템에는 LDAP 부서 기록에 대한 변환 맵이 없습니다.

사용자 지정 **LDAP** 변환 맵에 대한 요구 사항

사용자 지정 변환 맵을 생성하도록 선택하는 경우 변환 맵은 다음 매핑 요구 사항을 충족해야 합니다.

사용자 지정 **LDAP** 변환 맵에 대한 요구 사항

소스 테이블	소스 필드	대상 테이블	대상 필드	병합	설명
`ldap_import`	`u_source`	`sys_user`	소스	거짓	**u_source** 필드는 임포트한 사용자 또는 그룹의 LDAP DN을 식별합니다. 시스템은 이 필드를 사용하여 사용자가 LDAP 인증을 필요로 하는지 확인하고, 사용자의 관리자를 찾고, 사용자를 그룹에 배치합니다.
`ldap_import`	다음 필드 중 하나를 선택합니다. • `u_samaccountname` • `u_dn` • `u_cn`	`sys_user`	`user_name`	예	LDAP가 Active Directory에 통합되면 **u_samaccountname** 필드를 소스 필드로 선택합니다. 다른 LDAP 디렉터리를 사용하는 경우 **u_dn** 또는 **u_cn** 소스 필드로 선택합니다.

LDAP 변환 맵과 레거시 임포트 맵의 차이점

변환 맵을 사용하여 LDAP 매핑 관계를 지정할 때 관리자와 부서에 대해 참조 필드를 설정하는 방법에 큰 차이가 있습니다.

변환 맵을 사용할 경우 변환 스크립트를 사용하여 참조를 생성해야 합니다. 이는 "manager"와 같은 LDAP 속성과 연결된 값이 관리자의 고유 이름(DN)이기 때문입니다.

몇 가지 추가 논리를 사용하지 않으면 LDAP에서 해당 사용자의 고유 이름인 관리자 이름을 가진 사용자 기록이 생성됩니다. 통합에는 이러한 참조를 쉽게 생성할 수 있는 변환 스크립트가 포함됩니다. 기본 변환 맵 "LDAP 사용자 임포트"에는 이러한 참조에 대한 변환 스크립트가 포함됩니다.

기존 매핑 관계

레거시 임포트 맵을 변환 맵으로 업데이트할 때 시스템 LDAP 애플리케이션을 추가하기 전에 존재했던 LDAP 매핑 관계를 유지할 수 있습니다. LDAP 서버에는 레거시 임포트 맵에 대한 참조인 맵 필드가 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 기본적으로 이 필드는 숨겨져 있으므로 이를 표시하도록 양식을 구성해야 합니다.

변환 맵 사용으로 전환하려면 레거시 임포트 맵에 대한 참조를 지웁니다.

LDAP 임포트 맵 설정

속성을 확인하고 사용하여 통합이 LDAP 소스에서 임포트하는 필드를 제한합니다. 또한 user_name 필드를 사용자의 로그인 ID가 포함된 LDAP 속성에 매핑하는 것이 중요합니다. Active Directory의 경우 일반적으로 sAMAccountName 특성입니다. 이진 속성(예: objectSID 또는 objectGUID)을 임포트하고 병합하려면 사용자 지정 변환 스크립트를 만들어야 합니다.

주: user_name 필드에 매핑된 모든 값은 고유해야 합니다.

변환 맵(예: LDAP 사용자 임포트)을 지정하지 않으면 통합은 다음과 같은 기본 매핑을 사용합니다.

LDAP 임포트 기본 매핑

사용자 필드 또는 변수	**LDAP** 속성
user_name	sAMAccountName
이메일	메일
전화	전화 번호
home_phone	집전화
mobile_phone	모바일
first_name	지정된 이름
last_name	sn
제목	제목
부서	부서
매니저	매니저
middle_name	이니셜
u_memberof	그룹
u_member	구성원
u_manager	매니저

LDAP 데이터 변환

LDAP 속성에 단순 데이터가 포함되어 있으면 변환 맵은 가져온 LDAP 속성을 대상 테이블(사용자 또는 그룹)의 해당 필드에 링크합니다. 예를 들어, sAMAccountName 속성의 샘플 데이터는 사용자 테이블의 사용자 **ID** 필드에 매핑됩니다.

임포트한 LDAP 데이터가 참조 필드에 매핑되는 경우, 인스턴스는 일치하는 기존 기록을 검색합니다. 일치하는 기록이 없으면 필드 매핑에서 별도로 지정하지 않는 한 인스턴스가 참조 필드에 대한 새 기록을 생성합니다.

예를 들어, LDAP 속성 l이 사용자 테이블의 위치 참조 필드에 매핑된다고 가정합니다. 임포트 시 기존 위치 기록 값과 일치하지 않는 속성 값을 가져올 때마다 변환 맵에서 새 위치 기록이 생성됩니다. 새 위치 기록은 임포트한 속성과 동일한 값을 가지며, 임포트한 사용자 기록에는 이제 새 위치 기록에 대한 링크가 포함됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

그러나 LDAP 속성이 기본적으로 LDAP 디렉토리 내의 다른 기록에 대한 참조인 고유 이름(DN)을 반환하는 경우가 있습니다. 예를 들어, 일반적으로 관리자 속성에는 현재 LDAP 디렉토리 항목의 관리자에 대한 고유 이름이 포함됩니다. 가져온 DN은 일반적으로 긴 텍스트 문자열을 사용합니다(예: cn=Beth Anglin,ou=Users,dc=my-domain,dc=com).

⚠ 경고: 대상 필드가 DN을 포함할 수 있을 만큼 충분히 긴지 확인합니다. 대부분의 텍스트 필드는 기본 길이인 40을 사용하는데, 이는 일부 DN 값에 대해 충분히 길지 않을 수 있습니다. ServiceNow 시스템은 필드 길이를 초과하는 모든 값을 자릅니다.

일반적으로 관리자는 새 사용자가 기존 사용자와 연결되어 있지 않기 때문에 시스템이 DN 값에서 새 사용자를 생성하는 것을 원하지 않습니다. 대신 관리자는 임포트를 통해 관리자의 기존 사용자 기록을 찾아 새로 임포트한 사용자와 연결하기를 원합니다. `LDAPUtils` 스크립트 포함에는 DN을 구문 분석하고 기존 사용자를 검색할 수 있는 `setManager` 및 `processManagers` 함수가 포함되어 있습니다. 최상의 결과를 얻으려면 다음 함수를 사용하여 사용자 지정 변환 맵을 생성하십시오.

예를 들어, `LDAP ### ###` 변환 맵 스크립트는 `setManager` 함수를 호출합니다.

```
//
// 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 ) ;
```

경우에 따라 통합은 연결된 관리자의 사용자 기록을 임포트하기 전에 사용자의 기록을 임포트합니다. 이러한 경우를 처리하려면 변환이 완료된 후 `processManagers` 함수를 호출할 수 있습니다. 예를 들어, **LDAP** 사용자 임포트 변환 맵은 `onComplete` 변환 스크립트를 사용하여 `processManagers` 함수를 호출합니다.

```
// 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 ( ) ;
```

LDAP 통합에서 관리자 속성을 사용하지 않는 경우 `setManager` 및 `processManagers` 함수 호출을 제거하거나 주석 처리합니다.

LDAP 스크립팅

사용자 지정 변환 맵, 스크립트 및 비즈니스 규칙을 생성하여 데이터 임포트 시 요구사항을 지정합니다.

사용자 지정 변환 맵에는 `onStart` 및 `onAfter` 변환 스크립트가 포함되어야 합니다.

`onStart` 스크립트는 `LDAPUtils` 스크립트 포함을 호출하고 로깅을 시작해야 합니다. 예를 들어, **LDAP** 사용자 임포트 변환 맵에는 다음 코드를 사용하는 `onStart` 스크립트가 있습니다.

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

`onAfter` 스크립트는 `addMembers` 함수를 호출해야 합니다. 예:

```
ldapUtils.addMembers (source , target ) ;
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

비활성화된 **Active Directory** 사용자를 비활성으로 설정

연결된 AD 사용자가 비활성화될 때 다음 스크립트를 사용하여 사용자를 자동으로 비활성화합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
`userAccountControl` 특성의 값을 확인하여 비활성화된 Active Directory 사용자를 식별할 수 있습니다. 이 규칙은 `userAccountControl` 값이 변경될 때마다 실행되며 사용자 계정 컨트롤이 비활성화된 AD 계정을 나타내는 경우 사용자 계정을 비활성화합니다.

연결된 AD 사용자가 비활성화될 때 다음 스크립트를 사용하여 사용자를 자동으로 비활성화합니다.

프로시저

1. 사용자 양식을 구성하고 사용자 계정 컨트롤이라는 새 정수 필드를 만듭니다.
2. userAccountControl(외부)에 대한 매핑을 새 필드에 추가합니다.
3. 다음 속성을 사용하여 새 비즈니스 규칙을 생성합니다.

AD 사용자 비즈니스 규칙 사용 안 함

비즈니스 규칙 필드	값
이름	AD 사용자 사용 안 함
테이블	사용자 [sys_user]
시기	이전
조건	current.u_user_account_control.changes()

스크립트 필드에는 다음이 포함되어야 합니다.

```
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';
}
```

LDAP 필드 값 할당

스크립트를 사용하여 필드 매핑이 있는 모든 필드에 값을 할당할 수 있습니다.

예를 들어, sys_user.company 필드에 값을 할당하려면 회사 필드에 대한 필드 맵을 만들고 다음과 같은 변환 스크립트를 추가합니다.

```
company = "Don's Sporting Goods";
```

특정 **LDAP** 사용자 제외

LDAP 필터 속성을 사용하여 LDAP 사용자 목록을 완전히 필터링할 수 없는 경우 맵 스크립트를 사용하여 사용자를 제외할 수 있습니다.

임포트하면 안 되는 사용자를 식별하는 논리를 실행한 후 user_name 필드를 빈 문자열로 설정하면 이 사용자는 임포트되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
user_name='';
```

필터링할 사용자를 식별하는 한 가지 방법은 `distinguishedName` 특성에서 문자열을 찾는 것입니다. 예를 들어 이 스크립트는 사용자 OU에 없는 계정을 제외합니다. 대상 OU LDAP 옵션에 포함할 사용자 OU가 너무 많은 경우 이 스크립트를 사용할 수 있습니다.

```
//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);
}
```

더 복잡한 필터링 방법은 정규식을 사용하는 것입니다.

```
//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 = "";
}
```

참조 필드 임포트에 대한 선택 작업 설정

LDAP 변환 맵은 임포트 세트 테이블의 필드가 인시던트나 사용자 등 기존 테이블의 필드에 매핑되는 방식을 결정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
LDAP 변환 맵이 임포트 세트 테이블의 필드를 업데이트하면 LDAP 데이터에 새 기록이 있을 때마다 통합에서 자동으로 새 기록을 생성합니다. LDAP 변환 맵이 다른 테이블의 데이터를 저장하는 참조 필드를 업데이트할 경우 관리자는 새 LDAP 기록을 작성, 무시 또는 거부할 수 있습니다.
예를 들어, 통합이 기존 부서와 일치하지 않는 새 부서 기록을 수신하는 경우, 인스턴스에서 새 부서 기록을 만들지 않고 다른 모든 LDAP 기록 필드를 업데이트할 수 있습니다. 변환 맵을 사용하면 각 참조 필드에 대한 기록 생성 옵션을 설정할 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 **LDAP** > 변환 맵.
2. 필드 맵 관련 목록의 선택 작업 필드에서 다음 작업 중 하나를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ 생성 – 일치하는 기록이 없는 경우 새 참조 필드 기록을 생성합니다.

◦ 무시 – 참조 필드의 새 기록을 무시하고 변환 맵의 다른 모든 필드 처리를 완료합니다.

◦ 거부 – 전체 기록에 대한 변환을 중지합니다.

주: 필드 맵에는 참조 필드에 대한 선택 작업 필드만 표시됩니다.

LDAP 매핑 확인

LDAP 변환 맵을 작성한 후 LDAP 데이터를 새로 고쳐 변환 맵이 예상대로 작동하는지 확인합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 **LDAP** > 예약된 로드.
2. LDAP 가져오기 작업을 클릭합니다.
3. 지금 실행을 클릭합니다.

LDAP 통합 문제 해결

LDAP 서버를 통합하는 중에 질문이 있는 경우 다음 항목이 문제 해결에 도움이 될 수 있습니다.

예비 점검

- LDAP를 사용할 수 없는 경우 사용자는 인스턴스에 로그인할 수 없습니다. LDAP가 다운된 경우 관리자가 인스턴스에 계속 액세스할 수 있도록 관리자용 로컬 계정을 사용하는 것이 좋습니다.
- 서비스 계정을 확인하여 만료되거나 잠겨 있지 않은지 확인합니다.
- 사용자 이름의 형식을 확인하십시오. 사용자 이름만 사용하는 대신 사용자 이름으로 도메인을 사용하거나 username@domain 사용해 보십시오.
- `ldap_server_config` 기록에서 `system_id` 항목을 변경했는지 확인합니다. 업데이트 세트를 사용하여 의도치 않게 `system_id` 수정하면 `system_id` 대상 인스턴스에 대해 잘못된 노드를 가리키고 작동하지 않습니다.

오류 코드

LDAP 로그 파일에는 LDAP와 Active Directory(AD) 모두에 대한 산업 표준 오류 코드가 나열됩니다. LDAP 로그 파일은 래퍼 파일에 포함되어 있습니다. LDAP 오류 코드는 2자리 숫자이고 Active Directory 오류 코드는 3자리 숫자입니다. 가장 일반적인 오류 코드 목록은 LDAP 오류 코드를 참조하십시오.

다중 도메인 통합

동일한 포리스트 내에서 또는 완전히 신뢰할 수 없는 도메인에서 여러 도메인을 통합할 수 있습니다. 각 도메인에 대해 별도의 LDAP 서버 기록을 생성하는 것이 좋습니다. 각 LDAP 서버 기록은 해당 도메인의 도메인 컨트롤러를 가리켜야 합니다. 즉, 각 도메인 컨트롤러에 대한 연결을 허용해야 합니다. 하나의 LDAP 계정으로 LDAP를 통한 여러 AD 포리스트는 지원되지 않습니다.

둘 이상의 도메인으로 확장할 때는 애플리케이션 사용자 이름에 대한 고유한 LDAP 속성을 식별하고 병합 값을 가져오는 것이 중요합니다. Active Directory의 일반적인 고유 병합 특성은 `objectSid`입니다. 고유한 사용자 이름은 LDAP 데이터 설계에 따라 다릅니다. 일반적인 고유 속성은 `email` 또는 `userPrincipalName`입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수신 기록

참조 필드에서 일치하는 값이 누락된 수신 LDAP 기록을 통합에서 처리하는 방법을 설정하려면 내용을 참조하십시오 LDAP 변환 맵 .

일반적인 인증 오류

- 사용자가 로그인할 수 없음(잘못된 DN)
- 잘못된 CN
- 잘못된 연결

자동 **LDAP** 연결 테스트

LDAP 서버에 대한 연결을 수동으로 테스트하거나 ServiceNow 연결을 자동으로 테스트할 수 있습니다.

시스템은 연결을 자동으로 테스트합니다.

- 사용자가 LDAP 서버 양식을 열 때마다.
- 기본적으로 15분마다 실행되는 LDAP 연결 테스트 예약된 작업을 통해

  이 예약된 작업이 실행되는 빈도를 변경할 수 있습니다. 이 예약된 작업이 연결을 설정할 수 없는 경우 새 일회성 예약 작업은 5분 후 또는 예약된 작업의 반복 간격 값의 절반 중 먼저 발생하는 값 후에 연결 테스트를 다시 시도합니다.

LDAP 서버에 연결하는 데 문제가 있는 경우 양식에 오류 메시지가 나타납니다. MID Server 뒤에 있는 서버에 대한 연결 테스트도 지원됩니다.

LDAP 모니터 보기

LDAP 모니터를 사용하여 LDAP 서버 및 수신기에 대한 현재 정보를 볼 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
사용 가능한 상태는 다음과 같습니다.

- 활성
- 비활성
- 오류
- 활성(종료 중...)
- 오류(종료 중...)

모니터에는 현재 상태 외에도 다음이 표시됩니다.

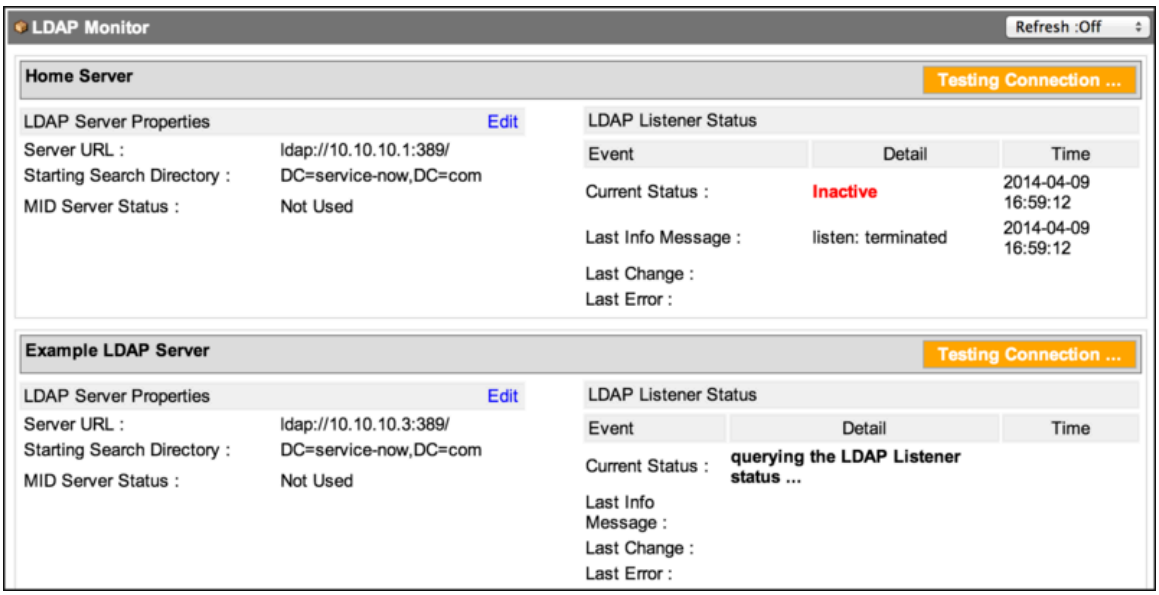
- LDAP 변경 대기 중, 연결 오류 등과 같이 수신기에서 검색한 마지막 메시지입니다.
- 새 사용자, 업데이트된 사용자 등의 마지막 LDAP 사용자 변경입니다.
- 마지막으로 발생한 오류입니다.

LDAP 모니터를 보려면 다음을 수행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

다음으로 이동 모두 > **LDAP** > 시스템 **LDAP** > **LDAP** 모니터.



화면의 속성 및 필드에 대한 설명은 테이블을 참조하십시오.

LDAP 모니터

필드	설명
새로 고침	LDAP 서버 모니터 헤더 표시줄에서 새로 고침 필드를 클릭하고 각 데이터 새로 고침 사이의 시간(초)을 선택하여 새로 고침 빈도를 구성할 수 있습니다. 없음을 선택하여 새로 고침을 억제할 수도 있습니다.
연결 상태	서버 연결 표시기는 LDAP 수신기 상태 필드 오른쪽 위에 있습니다. 서버가 연결되면 상자가 녹색으로 표시되고 연결됨이 표시됩니다. 서버가 연결되지 않은 경우 상자가 빨간색으로 표시되고 연결되지 않음이 표시됩니다. 서버 연결을 테스트 중일 때 상자는 노란색이며 연결 테스트 중이라고 표시됩니다.
LDAP 서버 속성	
편집	LDAP 서버를 모니터링할 때 LDAP 서버 모니터 화면에서 편집을 클릭하여 속성을 변경할 수 있습니다.
서버 URL	LDAP 서버가 수신 대기 중인 서버 이름과 서버 포트의 조합입니다. 포트는 다음 중 하나로 설정되는 경우가 많습니다. • 389: 일반 텍스트로 LDAP에 연결하기 위한 기본 포트 • 636: SSL 연결을 통해 LDAP에 연결하기 위한 표준 포트 예제 값: ldap://10.10.10.3:389/ LDAP 서버에는 둘 이상의 URL 주소가 있을 수 있습니다. 이렇게 하면 다른 LDAP 서버 항목을 작성하여 데이터를 가져올 수 있는 여러 디렉토리 구조가 설정되지는 않지만, 단일 실패 지점을 피하기 위해 여러 LDAP 서버가 있을 때 중복성을 제공합니다. LDAP URL 주소는 공백으로 구분되며, 시스템은 올바른 연결이 이루어질 때까지 각 서버 주소를 차례로 차례로 시도합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
검색 시작 디렉터리	시스템이 사용자 또는 그룹 검색을 시작하는 시작 디렉터리 또는 RDN(상대 고유 이름)입니다. 예제 값: DC=service-now,DC=com 이 포인트 위의 데이터는 임포트할 수 없습니다. 인스턴스는 LDAP 계층 구조에서 지정된 디렉터리와 그 아래의 디렉터리를 볼 수 있습니다.
MID 서버 상태	MID 서버의 현재 연결 상태입니다.
LDAP 수신기 상태	
현재 상태	이는 수신기가 활성 상태인지 여부를 나타냅니다.
마지막 정보 메시지	여기에는 사용자 및 그룹 변경과 관련하여 LDAP 서버가 받은 마지막 메시지와 메시지를 받은 시간이 표시됩니다.
마지막 변경	LDAP 서버에 대한 마지막 변경 내용과 변경 시간이 표시됩니다.
마지막 오류	LDAP 서버에서 발생한 마지막 오류와 발생 시간이 표시됩니다.

LDAP 오류 코드

LDAP 로그 파일에는 LDAP와 Active Directory(AD) 모두에 대한 산업 표준 오류 코드가 나열됩니다.

표준 오류 코드

표준 **LDAP** 오류

오류/데이터 코드	텍스트	설명
0	LDAP_SUCCESS	요청된 클라이언트 작업이 성공적으로 완료되었음을 나타냅니다.
2	LDAP_PROTOCOL_ERROR	서버가 클라이언트로부터 잘못되었거나 잘못된 형식의 요청을 받았음을 나타냅니다.
3	LDAP_TIMELIMIT_EXCEEDED	클라이언트 또는 서버에서 지정한 작업 시간 제한이 초과되었음을 나타냅니다. 검색 작업에서 불완전한 결과가 반환됩니다.
4	LDAP_SIZELIMIT_EXCEEDED	검색 작업에서 클라이언트 또는 서버에서 지정한 크기 제한을 초과했음을 나타냅니다. 불완전한 결과가 반환됩니다.
5	LDAP_COMPARE_FALSE	오류 조건을 나타내지 않습니다. 비교 작업의 결과가 false임을 나타냅니다.
6	LDAP_COMPARE_TRUE	오류 조건을 나타내지 않습니다. 비교 작업의 결과가 true임을 나타냅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표준 **LDAP** 오류

오류/데이터 코드	텍스트	설명
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	바인딩 작업 중에 클라이언트가 LDAP 서버에서 지원하지 않는 인증 방법을 요청했음을 나타냅니다.
8	LDAP_STRONG_AUTH_REQUIRED	다음 중 하나를 나타냅니다. 바인딩 요청에서 LDAP 서버는 강력한 인증만 허용합니다. 클라이언트 요청에서 클라이언트는 강력한 인증이 필요한 삭제와 같은 작업을 요청했습니다. 원치 않는 연결 끊김 알림에서 LDAP 서버는 클라이언트와 서버 간의 통신을 보호하는 보안이 예기치 않게 실패하거나 손상되었음을 발견합니다.
9		예약.
10	LDAP_REFERRAL	오류 조건을 나타내지 않습니다. LDAPv3에서 는 서버가 요청의 대상 항목을 보유하지 않지만 referral 필드의 서버가 보유할 수 있음을 나타냅니다.
11	LDAP_ADMINLIMIT_EXCEEDED	관리 권한에 의해 설정된 LDAP 서버 한계가 초과되었음을 표시합니다.
12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	하나 이상의 중요 확장을 사용할 수 없어 LDAP 서버가 요청을 충족할 수 없음을 나타냅니다. 서버에서 컨트롤을 지원하지 않거나 컨트롤이 작업 유형에 적합하지 않습니다.
13	LDAP_CONFIDENTIALITY_REQUIRED	세션이 세션 기밀성을 제공하는 TLS(전송 계층 보안)와 같은 프로토콜로 보호되지 않음을 나타냅니다.
14	LDAP_SASL_BIND_IN_PROGRESS	오류 조건을 나타내지는 않지만 서버가 프로세스의 다음 단계를 수행할 준비가 되었음을 나타냅니다. 클라이언트는 프로세스를 계속하기 위해 서버에 동일한 SASL 메커니즘을 보내야 합니다.
15		사용하지 않습니다.
16	LDAP_NO_SUCH_ATTRIBUTE	수정 또는 비교 작업에 지정된 속성이 항목에 없음을 나타냅니다.
17	LDAP_UNDEFINED_TYPE	수정 또는 추가 작업에 지정된 속성이 LDAP 서버의 스키마에 없음을 나타냅니다.
18	LDAP_INAPPROPRIATE_MATCHING	검색 필터에 지정된 일치 규칙이 속성의 구문에 대해 정의된 규칙과 일치하지 않음을 나타냅니다.
19	LDAP_CONSTRAINT_VIOLATION	DN 수정, 추가 또는 수정 작업에 지정된 속성 값이 속성에 지정된 제약 조건을 위반함을 나타냅니다. 제약 조건은 크기

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표준 **LDAP** 오류

오류/데이터 코드	텍스트	설명
		또는 내용(문자열만, 이진 아님) 중 하나일 수 있습니다.
20	LDAP_TYPE_OR_VALUE_EXISTS	수정 또는 추가 작업에 지정된 특성 값이 해당 특성의 값으로 이미 존재함을 나타냅니다.
21	LDAP_INVALID_SYNTAX	추가, 비교 또는 수정 작업에 지정된 특성 값이 특성에 대해 인식되지 않거나 잘못된 구문임을 나타냅니다.
22-31		사용하지 않습니다.
32	LDAP_NO_SUCH_OBJECT	대상 개체를 찾을 수 없음을 나타냅니다. 이 코드는 검색 베이스를 찾지만 검색 필터와 일치하는 항목을 찾을 수 없는 검색 작업에서는 반환되지 않습니다. 작업을 바인딩합니다.
33	LDAP_ALIAS_PROBLEM	별칭이 역참조될 때 오류가 발생했음을 나타냅니다.
34	LDAP_INVALID_DN_SYNTAX	DN의 구문이 올바르지 않음을 나타냅니다. (DN 구문이 올바르지만 LDAP 서버의 구조 규칙이 작업을 허용하지 않는 경우 서버는 코드 53: LDAP_UNWILLING_TO_PERFORM을 반환합니다.)
35	LDAP_IS_LEAF	리프 항목에서 지정된 작업을 수행할 수 없음을 나타냅니다. (이 코드는 현재 LDAP 사양에 없지만 이 상수용으로 예약되어 있습니다.)
36	LDAP_ALIAS_DEREF_PROBLEM	검색 작업 중에 클라이언트에 별칭이 지정된 개체의 이름을 읽을 수 있는 액세스 권한이 없거나 역참조가 허용되지 않음을 나타냅니다.
37-47		사용하지 않습니다.
48	LDAP_INAPPROPRIATE_AUTH	바인딩 작업 중에 클라이언트가 올바르게 사용할 수 없는 인증 방법을 사용하려고 시도하고 있음을 나타냅니다. 예를 들어 다음 중 하나로 인해 이 오류가 발생합니다. 강력한 자격 증명이 필요한 경우 클라이언트는 단순 자격 증명을 반환합니다... 또는... 클라이언트는 항목에 정의된 암호가 없는 경우 간단한 바인딩을 위해 DN과 암호를 반환합니다.
49	LDAP_INVALID_CREDENTIALS	바인딩 작업 중 클라이언트가 잘못된 DN 또는 암호를 전달했거나, 암호가 만료되어 암호가 잘못되었거나, 침입자 탐지로 인해 계정이 잠겼거나, 기타 유사한 이유로 다음 중 하나가

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표준 **LDAP** 오류

오류/데이터 코드	텍스트	설명
		발생했음을 나타냅니다. 자세한 내용은 데이터 코드를 참조하십시오.
49 / 52e	AD_INVALID 자격 증명	사용자 이름이 유효하지만 암호와 사용자 자격 증명의 조합이 유효하지 않을 때 반환되는 AD(Active Directory) AcceptSecurityContext 오류를 나타냅니다. 이는 LDAP 오류 코드 49에 해당하는 AD입니다.
49 / 525	사용자를 찾을 수 없음	사용자 이름이 올바르지 않을 때 반환되는 AD(Active Directory) AcceptSecurityContext 데이터 오류를 나타냅니다.
49 / 530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	사용자가 현재 로그온할 수 없기 때문에 로그온 실패인 Active Directory(AD) AcceptSecurityContext 데이터 오류를 나타냅니다. 유효한 사용자 이름 및 유효한 암호 자격 증명이 제공된 경우에만 반환합니다.
49 / 531	RESTRICTED_TO_SPECIFIC_MACHINES	사용자가 이 컴퓨터에서 로그온할 수 없기 때문에 발생하는 로그온 실패인 AD(Active Directory) AcceptSecurityContext 데이터 오류를 나타냅니다. 유효한 사용자 이름 및 유효한 암호 자격 증명이 제공된 경우에만 반환합니다.
49 / 532	PASSWORD_EXPIRED	로그온 실패인 AD(Active Directory) AcceptSecurityContext 데이터 오류를 나타냅니다. 지정된 계정 암호가 만료되었습니다. 유효한 사용자 이름 및 암호 자격 증명이 제공된 경우에만 반환합니다.
49 / 533	ACCOUNT_DISABLED	로그온 실패인 AD(Active Directory) AcceptSecurityContext 데이터 오류를 나타냅니다. 계정이 현재 비활성화되어 있습니다. 유효한 사용자 이름 및 암호 자격 증명이 제공된 경우에만 반환합니다.
49 / 568	ERROR_TOO_MANY_CONTEXT_IDS	로그온 시도 중에 사용자의 보안 컨텍스트에 너무 많은 보안 ID가 누적되었음을 나타냅니다. 이는 LDAP 관리자가 조사해야 하는 특정 LDAP 사용자 객체/계정의 문제입니다.
49 / 701	ACCOUNT_EXPIRED	로그온 실패인 AD(Active Directory) AcceptSecurityContext 데이터 오류를 나타냅니다. 사용자 계정이 만료되었습니다. 유효한 사용자 이름

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표준 **LDAP** 오류

오류/데이터 코드	텍스트	설명
		및 암호 자격 증명이 제공된 경우에만 반환합니다.
49 / 773	사용자는 암호를 재설정해야 합니다.	AD(Active Directory) AcceptSecurityContext 데이터 오류를 나타냅니다. 처음 로그온하기 전에 사용자의 암호를 변경해야 합니다. 유효한 사용자 이름 및 암호 자격 증명이 제공된 경우에만 반환합니다.
50	LDAP_INSUFFICIENT_ACCESS	호출자에게 요청된 작업을 수행할 수 있는 충분한 권한이 없음을 나타냅니다.
51	LDAP_BUSY	LDAP 서버 사용량이 너무 많아 현재 클라이언트 요청을 처리할 수 없지만 클라이언트가 기다렸다가 요청을 다시 제출하면 서버가 요청을 처리할 수 있음을 나타냅니다.
52	LDAP_UNAVAILABLE	일반적으로 클라이언트의 바인딩 요청이 종료되기 때문에 LDAP 서버가 클라이언트의 바인딩 요청을 처리할 수 없음을 나타냅니다.
52e	AD_INVALID 자격 증명	사용자 이름이 유효하지만 암호와 사용자 자격 증명의 조합이 유효하지 않을 때 반환되는 AD(Active Directory) AcceptSecurityContext 오류를 나타냅니다. LDAP 오류 코드 49: LDAP_INVALID_CREDENTIALS에 해당하는 AD입니다.
53	LDAP_UNWILLING_TO_PERFORM	서버 정의 제한사항으로 인해 LDAP 서버가 요청을 처리할 수 없음을 나타냅니다. 이 오류는 다음과 같은 이유로 반환됩니다. 항목 추가 요청이 서버의 구조 규칙을 위반합니다... 또는... 속성 수정 요청은 사용자가 수정할 수 없는 속성을 지정합니다... 또는... 암호 제한으로 인해 작업을 수행할 수 없습니다. 또는... 연결 제한으로 인해 작업을 수행할 수 없습니다.
54	LDAP_LOOP_DETECT	클라이언트가 별칭 또는 조회 루프를 검색하여 이 요청을 완료할 수 없음을 나타냅니다.
55-63		사용하지 않습니다.
64	LDAP_NAMING_VIOLATION	DN 추가 또는 수정 작업이 스키마의 구조 규칙을 위반함을 나타냅니다. 예를 들어, 요청은 항목을 별칭에 종속시킵니다. 이 요청은 포함 규칙에 의해 금지된 컨테이너에 하위 항목을

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

표준 **LDAP** 오류

오류/데이터 코드	텍스트	설명
		배치합니다. 항목의 RDN은 금지된 속성 유형을 사용합니다.
65	LDAP_OBJECT_CLASS_VIOLATION	DN 추가, 수정 또는 수정 작업이 항목에 대한 객체 클래스 규칙을 위반함을 나타냅니다. 예를 들어, 다음 유형의 요청은 이 오류를 반환합니다. 추가 또는 수정 작업은 필수 속성에 대한 값 없이 항목을 추가하려고 시도합니다. 추가 또는 수정 작업은 클래스 정의에 포함되지 않은 속성에 대한 값을 사용하여 항목을 추가하려고 시도합니다. 수정 작업은 필요에 따라 속성을 정의하는 보조 클래스를 제거하지 않고 필수 속성을 제거하려고 합니다.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	요청된 작업이 리프 항목에서만 허용됨을 나타냅니다. 예를 들어, 다음 유형의 요청은 이 오류를 반환합니다. 클라이언트는 상위 항목에 대한 삭제 작업을 요청합니다. 클라이언트는 상위 항목에 대한 DN 수정 작업을 요청합니다.
67	LDAP_NOT_ALLOWED_ON_RDN	수정 작업이 항목의 상대적 고유 이름을 형성하는 특성 값을 제거하려고 시도했음을 나타냅니다.
68	LDAP_ALREADY_EXISTS	추가 작업에서 이미 있는 항목을 추가하려고 시도했거나 수정 작업에서 이미 있는 항목의 이름으로 항목 이름을 바꾸려고 시도했음을 나타냅니다.
69	LDAP_NO_OBJECT_CLASS_MODS	수정 작업에서 객체 클래스의 구조 규칙을 수정하려고 시도했음을 나타냅니다.
70	LDAP_RESULTS_TOO_LARGE	CLDAP용으로 예약되어 있습니다.
71	LDAP_AFFECTS_MULTIPLE_DSAS	DN 수정 작업이 항목을 한 LDAP 서버에서 다른 LDAP 서버로 이동하며 둘 이상의 LDAP 서버가 필요함을 나타냅니다.
72-79		사용하지 않습니다.
80	LDAP_OTHER	알 수 없는 오류 조건을 나타냅니다. 이것은 다른 LDAP 오류 코드에 매핑되지 않는 NDS 오류 코드의 기본값입니다.
775	USER_ACCOUNT_LOCKED	사용자 계정이 잠겨 있기 때문에 사용자가 로그인할 수 없음을 나타냅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 지정 오류 코드

사용자 지정된 **LDAP** 오류 코드

오류/데이터 코드	텍스트
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_REFUSED
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

LDAP 서버가 다운되면 일회용 암호 보내기

LDAP 서버가 다운되어 사용자가 로그인할 수 없는 경우, LDAP 속성을 사용하여 사용자에게 일회용 암호를 보낼 수 있습니다. 비밀번호가 유효한 기간을 제어하도록 다른 속성을 구성할 수도 있습니다.

시작하기 전에

필요한 역할: 관리자

일회용 암호를 받으려면 사용자의 사용자 프로파일에 알림이 설정되어 있어야 합니다. 알림은 이메일 메시지일 뿐입니다. SMS 메시지는 지원되지 않습니다.

이 태스크 정보

두 속성 모두 기본적으로 사용하도록 설정됩니다. 암호 유효성을 제어하는 속성의 기본값은 10분입니다.

프로시저

1. 애플리케이션 네비게이터의 필터에 `sys_properties.list` 를 입력하여 시스템 속성 목록을 엽니다.
2. 부동산을 *glide.ldap.onetime.password.enabled*찾습니다.
3. 속성을 `true`로 설정합니다.
4. 사용자의 암호 유효 시간을 변경하려면 다음 속성을 분 *glide.authenticate.onetime.password.validity*의 정수로 설정합니다.

LDAP 기록 동기화

관리자는 비활성, 비활성화 또는 삭제된 LDAP 기록을 LDAP 기록과 동기화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

LDAP 기록 동기화는 LDAP 서버에서 비활성 기록을 검색하고 해당 LDAP 기록을 업데이트하는 프로세스입니다. 비활성 LDAP 레코드를 검색하려면 각 사용자 개체에 대해 일관성 있는 데이터 표시기를 정의하고, LDAP 데이터를 가져오고, 데이터 표시기를 평가해야 합니다.

데이터 표시기에는 다음이 해당될 수 있습니다.

- 날짜 필드
- 특정 OU의 멤버 자격(특성을 구문 분석하여 *dn* 식별), 특성 사용 *useraccountcontrol*
- 이러한 표시기의 조합

임포트한 데이터는 데이터를 평가하고 처리할 수 있는 임포트 세트 테이블을 통해 인스턴스로 들어옵니다.

임포트 프로세스는 여러 임포트 작업에 사용할 LDAP 새로 고침 필터수 있으며 여러 유형의 사용자 기록을 나누고 별도의 처리를 위해 기록을 분리할 수 있습니다.

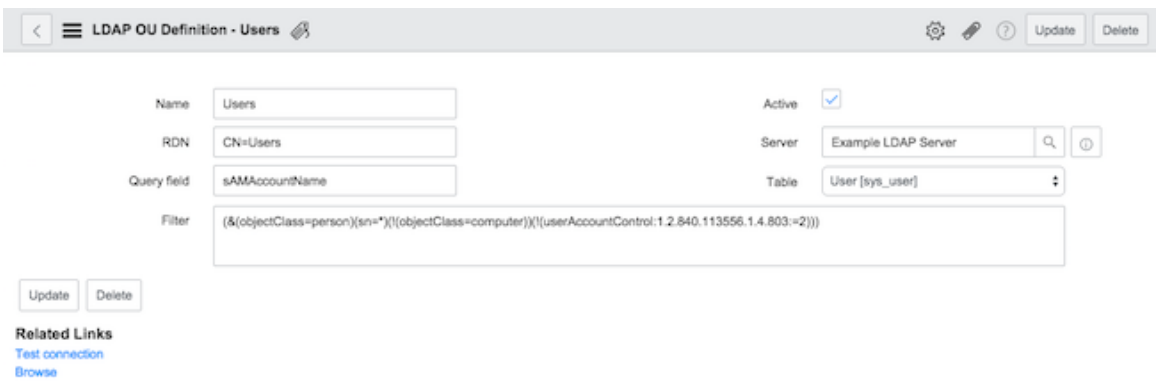
LDAP 새로 고침 필터

LDAP 새로 고침 프로세스의 필터를 사용하여 비활성화된 사용자의 삽입을 무시하는 처리를 지정할 수 있습니다.

LDAP OU 필터를 느슨하게 하여 모든 데이터(비활성 사용자 포함)를 임포트 세트 테이블로 가져온 다음 비활성화된 사용자의 삽입을 무시하는 처리를 지정할 수 있습니다. 인스턴스가 바로 사용 가능한 LDAP 샘플에서 제공하는 샘플 'Users' OU 정의에는 필터가 포함되어 있습니다.

이 필터는 평가할 임포트 세트 테이블로 가져온 사용자 기록을 정의하기 때문에 중요합니다. 이 필터는 데이터 로드를 더 적게 수행하지만 비활성 사용자를 필터링하므로 비활성 사용자 기록이 임포트 세트 임시 테이블로 임포트되지 않는다는 제한이 있습니다. 비활성 사용자 기록이 표시되지 않으므로 기록 표시기를 평가할 수 없습니다.

LDAP OU 필터



기본 LDAP 새로 고침 프로세스 내에서 필터링을 사용하려면 필터를 변경하여 모든 사용자 기록을 가져옵니다. 그 결과 모든 기록이 평가 및 변환될 수 있는 임포트 세트 임시 테이블로 로드됩니다.

주: 여기에는 예방 조치가 있습니다. 필터링이 모든 기록을 가져오기 때문에 인스턴스에 삽입해서는 안 되는 오래된 비활성 LDAP 계정이 대량으로 생성될 수 있습니다. 비활성화된 사용자에 대한 사용자 기록을 생성해서는 안 됩니다.

LDAP 추출

비활성화된 사용자를 탐지하기 위해 LDAP 추출 프로세스를 구현할 수 있습니다.

LDAP 소스에서 추출할 때는 임포트의 모든 기록에 대해 '아니오'로 설정할 수 있는 활성 플래그를 사용하여 비활성화된 사용자를 필터링할 수 있습니다. ("target.active=false")를 지정하고 테이블 변환 맵 기록의 스크립트 필드에 직접 복사합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

복지

이 방법의 이점은 다음과 같습니다.

- 간단한 스크립팅
- 기존 사용자 기록은 처리와 관련이 없습니다.
- 비활성 사용자는 임시 임포트 테이블에 로드되지 않습니다.
- 성능 영향 없음

단점

이 방법의 단점은 다음과 같습니다.

- 추가 프로세스가 생성됩니다.
- 추출 세트는 데이터 원본에서 액세스할 수 있는 위치에 배치해야 합니다.

대체 방법

LDAP 새로 고침 필터 여러 임포트 작업을 사용하여 서로 다른 유형의 사용자 기록을 나누고 별도의 처리를 위해 기록을 분리합니다.

비활성 **LDAP** 사용자 계정

기존의 현재 사용자 계정이 비활성 상태이거나 Active Directory(AD) LDAP에서 비활성화 또는 삭제되었는지 탐지합니다.

일반적인 LDAP 통합 문제는 Active Directory(AD)에서 비활성화되거나 삭제된 사용자를 탐지한 다음 인스턴스에서 비활성화하는 방법입니다. Active Directory LDAP에서는 일반적으로 새로 고침할 때 비활성 사용자를 제외하도록 필터가 설정되므로 인스턴스는 AD에서 비활성화되거나 삭제된 사용자를 인식하지 못합니다. 문제는 기존의 현재 사용자가 비활성 상태이거나 AD에서 삭제되었음을 감지하는 방법입니다.

비활성 계정을 찾는 방법에 대한 자세한 내용은 userAccountControl 필드를 사용하여 비활성 LDAP 계정 찾기를 참조하세요.

> **주:** 권장되는 방법은 사용자 기록 및 기타 모든 유형의 기록을 삭제하는 것이 아니라 비활성화하는 것입니다. 각 기록은 다른 기록에 연결되며 기록을 삭제하면 다른 기록에 대한 모든 관계가 삭제됩니다. 기록을 비활성화하면 해당 관계가 그대로 유지됩니다.

userAccountControl 필드를 사용하여 비활성 **LDAP** 계정 찾기

Active Directory(AD) 사용자가 삭제되거나 비활성화되는 시기를 식별합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

한 가지 방법은 AD 사용자의 활성 상태를 추적하고 AD 계정이 비활성 상태일 때 해당 계정을 업데이트하는 비즈니스 규칙을 만드는 것입니다.

프로시저

1. 사용자 [sys_user] 테이블에 새 문자열 필드를 만들어 AD **userAccountControl** 필드의 값을 추적합니다.
   예: `u_ad_user_account`.
2. LDAP 변환 스크립트를 생성하여 필드 값을 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example

```
target.u_ad_user_account = source.userAccountControl
```

3. 사용하지 않도록 설정된 AD 계정을 표시하도록 LDAP 필터를 업데이트합니다.

   Example
   다음은 필터의 예입니다.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer))(!
   (userAccountControl:1.2.840.113556.1.4.803:=2)))
   ```

   다음은 사용할 수 있는 교체 필터의 예입니다.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer)))
   ```

4. u_ad_user_account 필드의 값이 514일 때마다 활성 필드를 false로 설정하는 onChange 비즈니스 규칙을 생성합니다.
   '514'는 비활성 계정을 나타냅니다.

LDAP 스크립트 예

다음 스크립트 예시에서는 LDAP 서버에 Active Directory(AD)를 사용한다고 가정합니다.

userAccountControl 속성 값 스크립트

이 예제에서는 비활성화된 사용자(514 또는 546)와 연결된 userAccountControl 특성 값의 원본을 테스트합니다.

```
//Deactivate LDAP-disabled users during transform based on
 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol ==
 '546'){
   target.active=false;
   target.locked_out=true;
}
```

다음은 비트 검사를 사용하는 예제입니다.

```
if(source.u_useraccountcontrol & 2){
   active = false;
}
```

userAccountControl 속성 스크립트

이 예제에서는 userAccountControl 특성을 검사하지만 특정 값을 테스트하지는 않습니다. 또한 LDAP 사용자 계정을 다시 활성화하는 옵션도 포함되어 있습니다.

```
/*
* 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);

/*
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
* 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 변환 맵 스크립트

다음은 onBefore 변환 맵 스크립트의 예입니다. 스크립트가 비활성화된 기록과 삽입 중인 기록을 식별합니다. 비활성화된 사용자를 삽입하는 경우 작업 변환은 기록을 무시합니다.

```
//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;
}
```

DN 구성원 스크립트

이 스크립트 예제에서는 546 및 514 userAccountControl 값에 의존하지 않고 대신 사용자가 특정 DN(고유 이름)의 구성원인지 여부를 확인하여 유연성을 제공합니다. 이 스크립트는 '테이블 변환 맵' 기록의 스크립트 필드나 onBefore 변환 맵 스크립트에서 사용할 수 있습니다.

```
//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;
}
```

ADAM(Active Directory 응용 프로그램 모드)

ADAM(Active Directory Application Mode)은 LDAP(Lightweight Directory Access Protocol) 호환 디렉터리 서비스입니다.

주: 이 항목을 이해하려면 Server 및 Active Directory에 대한 Microsoft Windows 기본적인 이해가 필요합니다. ADAM에 대해 구성할 서버에 대한 관리자 권한도 있어야 합니다.

다음은 샘플 절차입니다. 설치 및 환경 차이로 인해 직접적인 지원을 제공할 수 없습니다. 컨설턴트와 협력하는 Microsoft 것이 좋습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ADAM은 설치가 간단하며 운영 체제에서 서비스로 Windows 실행됩니다. 이는 애플리케이션 구성요소로 완전히 사용자 정의 및 배포하거나 독립형 LDAP 디렉터리로 사용할 수 있습니다. ADAM은 Active Directory 도메인 컨트롤러에서 볼 수 있는 것과 동일한 기술(복제 및 위임 기능 포함)을 사용하며 고유한 관리 및 사용자 지정 기능을 가지고 있습니다. 서비스로 실행할 Windows 수 있습니다. ADAM은 XP, 2000, 2003 및 2008 운영 체제에 설치할 Windows 수 있습니다. ADAM은 Server 2003 R2 및 Windows Server 2008의 Windows 일부로 포함되어 있습니다. 이전 운영 체제에 대한 다운로드는 http://www.microsoft.com/downloads 에서 사용할 수 http://www.microsoft.com/downloads 있습니다.

보안

일부 회사 보안 정책은 외부 공급업체 및 파트너가 Active Directory(AD) 도메인 컨트롤러에 직접 연결하는 것을 금지합니다. 특정 AD 개체 또는 특성을 외부 공급업체 또는 파트너에게 노출하는 것이 금지된 경우 AD 보안 액세스 제어 항목(ACE 또는 ACL)을 사용하여 개체 및 특성에 대한 액세스를 차단할 수 있습니다. 보안 요구 사항에 따라 이 방법을 사용하면 통합이 복잡해질 수 있습니다. 여러 도메인과 포리스트를 통합하는 것이 좋습니다. 모든 LDAP 가져오기 및 인증을 단일 소스를 통해 채널링해야 하는 경우 ADAM을 통합 소스로 사용할 수 있습니다. 2008년 Windows 출시와 함께 이 기능은 Light-Weight-Directory Service, LDS로 이름이 변경되었습니다. 설치 및 구성은 Server 2003 R2와 Windows 유사합니다.

권장 지식

이 작업을 위해서는 AD, 객체 클래스 및 속성을 이해해야 합니다. 통합에 성공하려면 현재 AD 개체 구조에 대해 잘 알고 있어야 하고, Active Directory 위임에 익숙해야 하며, ADAM을 사용하는 방법과 용도에 대한 전략이 있어야 합니다. AD 또는 ADAM에 익숙하지 않은 경우 AD 관리자와 협력하여 새 ADAM 환경을 구성합니다.

신탁

userProxy 개체를 사용하는 경우 ADAM을 호스팅하는 컴퓨터는 AD 계정이 있는 도메인의 구성원이거나 트러스트된 도메인의 구성원이어야 합니다.

내부 연결

userProxy 개체를 사용하는 경우 ADAM 컴퓨터는 프록시 인증을 수행하기 위해 관련 도메인 컨트롤러에 연결할 수 있어야 합니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM을 사용하여 인스턴스 구성

처음 설치할 때 ADAM 파일을 컴퓨터에 복사하고, 등록하고, 구성 요소를 요구하고, 응용 프로그램 바로 가기를 만듭니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

기본적으로 모든 응용 프로그램 파일은 `%systemroot%\ADAM`에 설치됩니다.

- Windows Server 2003 R2 - ADAM은 제어판 **>** 프로그램 추가 및 제거 **>** 선택적 구성요소 관리자.
- Windows Server 2000 & Windows XP - Microsoft에서 다운로드 http://www.microsoft.com/downloads .

ADAM에서 호스팅되는 첫 번째 디렉터리 서비스로 작동하는 첫 번째 인스턴스 서비스를 만듭니다. 다음 중 하나를 수행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

- ADAM 폴더에서 *adaminstall.exe* 실행합니다.
- 다음에서 **ADAM** 인스턴스 만들기 바로 가기를 사용합니다. 시작 메뉴 > 프로그램 > **ADAM** 폴더.

1. 고유 인스턴스 설치 옵션을 선택합니다.

   주: 이 옵션을 사용하여 두 번째 서버에 인스턴스 복제본을 설치하여 내결함성 시스템을 제공할 수 있습니다.

2. 필드를 완성합니다.

ADAM 인스턴스

필드	설명
인스턴스 이름	서비스 이름 및 표시 이름을 식별하는 데 주로 사용됩니다.Windows
포트	은 LDAP 및 LDAPS 수신기에 사용할 포트 번호를 설정합니다. 기본 LDAP 포트는 389, LDAPS는 636입니다. 이러한 포트가 서버에서 사용 중인 경우 설정 마법사에서 새 포트를 선택합니다. 네트워크 관리자와 협력하여 사용하기에 가장 적합한 포트를 결정하십시오.
애플리케이션 디렉터리 파티션	응용 프로그램 디렉터리 파티션을 만듭니다. 이 단계에서는 필요하지 않으므로 지금 새 파티션을 만드는 것이 좋습니다. 포리스트 또는 도메인과 동일한 고유 이름을 사용하되 최상위 도메인을 com 또는 local 대신 adam으로 바꾸는 것이 좋습니다. 예를 들어 포리스트 파티션이 *dc=myCompany,dc=com*다음과 같은 경우 ADAM 파티션을 다음과 같이 만들 수 있습니다. *dc=myCompany,dc=adam*
파일 위치	ADAM 파티션 데이터의 위치를 선택합니다.
서비스 계정 선택	인스턴스가 실행되는 서비스 계정을 선택합니다. 독립 실행형 서비스의 경우 기본 네트워크 서비스 계정을 사용할 수 있습니다. 복제본을 사용하려는 경우 모든 ADAM 인스턴스에 액세스할 수 있는 계정을 사용해야 합니다.
ADAM 관리자	Windows 통합 인증을 활용하는 ADAM 디렉터리의 위임입니다. 이것이 관리를 위한 초기 접근 권한이 부여되는 방법입니다. 초기 계정에 권한이 부여되면 이 사용자나 그룹은 다른 Windows 사용자나 ADAM 사용자에게 권한을 위임합니다. 기본값을 선택하여 현재 사용자에게만 관리자 액세스 권한을 부여하거나 필요에 따라 다른 사용자 또는 그룹에 액세스 권한을 부여할 수 있습니다.
LDIF 파일 임포트	임포트할 파일입니다. MS-UserProxy는 가져올 가장 중요한 파일이지만 스키마에 대한 오버헤드가 거의 없고 요구 사항이 확장되면 나중에 확장할 필요가 없기 때문에 사용 가능한 모든 파일을 추가할 가치가 있습니다. 상세 정보를 확인하면 마법사가 구성을 완료합니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM 콘솔 설정

ADAM 콘솔을 설정합니다. ADAM과 Active Directory 사이에는 많은 유사점이 있지만 사용자 및 컴퓨터 관리 콘솔이 없기 때문에 관리 방식이 매우 다를 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
대부분의 일반 관리는 **ADAM** 시작 메뉴에서 사용할 수 있는 ADAM ADSI MMC 콘솔을 사용하여 수행됩니다. ADAM ADSI 콘솔을 처음 실행할 때는 만든 파티션에 연결해야 합니다.

프로시저

1. 왼쪽 프레임에서 **ADAM ADSI** 편집 항목을 마우스 오른쪽 단추로 클릭합니다.
2. 새 연결에 이름을 지정하고 인스턴스를 만들 때 사용한 정보로 서버 이름 및 포트 필드를 업데이트합니다.
3. 고유 이름 또는 이름 지정 컨텍스트를 선택하고 이전에 작성한 애플리케이션 파티션의 고유 이름을 지정합니다.
   고급 구성 옵션을 위해 `## # ###`파티션에 연결할 수 있습니다.
   이제 LostAndFound, NTDS 할당량 및 역할에 대한 파티션 및 기본 컨테이너를 볼 수 있습니다. 역할 컨테이너가 아직 구성되지 않았습니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM용 컨테이너 및 조직 구성 단위 만들기

ADAM에 저장된 개체를 Active Directory에서와 마찬가지로 컨테이너 및 OU(조직 구성 단위)로 논리적으로 그룹화합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 루트 파티션을 마우스 오른쪽 버튼으로 클릭하고 신규 > 객체 > 조직 단위.

   주: 사용 가능한 다른 객체의 목록을 볼 수도 있습니다. 이 목록은 LDF 파일을 가져올 때 설치된 스키마 확장에 따라 달라집니다.

2. 값을 입력하라는 메시지가 표시되면 `OU`의 이름(예: Users)을 입력합니다.
   화면에 추가 속성 버튼이 표시됩니다.
3. 이 버튼을 사용하여 추가 속성에 값을 할당합니다.
   OU 및 컨테이너의 경우 추가 값이 필요하지 않습니다.
   OU를 만든 후에는 새 OU가 루트 개체의 자식으로 나열됩니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM을 사용한 위임

OU 구조가 만들어지면 권한 위임을 정의하여 제한된 사용자에게 개체를 적절하게 보호합니다.

Active Directory와 마찬가지로 사용 권한을 부여하는 두 가지 일반적인 방법이 있습니다.

- 적절한 권한이 이미 할당된 그룹에 사용자를 추가합니다.
- ADAM 개체에 대한 새 사용 권한을 정의합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 작업에서는 객체 수준 권한에 대해 설명합니다. 그룹 구성원 자격에 대한 자세한 내용은 그룹 관리 섹션을 참조하십시오.

ADAM용 사용자 및 컴퓨터 콘솔이 없기 때문에 모든 개체 수준 권한은 Active Directory 유틸리티 *DSACLS.exe* 사용하여 정의됩니다. 이 파일은 ADAM 프로그램 디렉터리에 있습니다. ADAM 유틸리티를 실행할 때는 ADAM 도구 명령 프롬프트를 시작하는 것이 가장 좋습니다. 이렇게 하면 도구의 적절한 버전이 보장됩니다. DSALCS는 개체 액세스 권한을 보고 설정하는 데 사용됩니다.

예: "`dsacls \\localhost:50010\dc=myCompany,dc=adam`"은 localhost, 포트 50010에서 실행되는 파티션 *dc=myCompany,dc=adam* 의 루트에 할당된 권한을 표시합니다. DSACLS는 복잡한 위임을 만드는 데 사용되는 복잡한 도구입니다. 사용 참고 사항에 대해 *"DSACLS /?"#* 실행합니다.

관련 정보

ADAM용 컨테이너 및 조직 구성 단위 만들기

ADAMSync를 사용하여 ADAM 채우기

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM 개체 채우기

ADAM 개체에는 사용자 개체, UserProxy 개체 및 그룹 개체가 포함됩니다.

사용자 객체

OU를 만들 때와 마찬가지로 ADAM ADSI Edit 콘솔을 사용하여 사용자를 만들 수 있습니다. 이 문서의 범위를 벗어나는 AD 명령줄 도구를 사용하여 사용자를 관리할 수도 있습니다. 새 사용자 개체에 대한 유일한 필수 속성은 짧은 이름 또는 사용자의 전체 이름인 입니다 *cn*. Active Directory 사용자 특성과 유사한 다양한 선택적 특성도 있습니다. 사용자 객체에서 속성을 선택하여 전체 속성 목록에 액세스할 수 있습니다.

UserProxy 객체

LDAP 통합의 경우 ServiceNow ADAM에서 관련 AD 사용자 계정에 연결하는 프록시 계정을 만드는 *UserProxy* 개체를 사용하는 것이 좋습니다. 이렇게 하면 ADAM이 도메인 컨트롤러에 직접 연결하지 않고도 ServiceNow 도메인의 AD 사용자 이름 및 암호를 사용하여 로그온 자격 증명을 인증하도록 할 수 있습니다. *UserProxy* 개체는 암호를 저장하지 않고 연결된 AD User 개체의 SID를 포함하는 *objectSID* 특성이 있다는 점을 제외하고 AD 및 ADAM User 개체와 매우 유사합니다. 이것이 프록시가 작동하는 방식입니다. *UserProxy* 개체는 *ADSIEdit* 콘솔 또는 명령줄 도구를 사용하여 만들어지지만 지루할 수 있습니다. 아래에 정의된 대로 자동화된 프로세스를 사용하는 것이 좋습니다.

그룹 객체

그룹은 ADSIEdit 콘솔 및 AD 명령줄 도구를 사용하여 만들어집니다. 그룹 개념은 AD와 유사하며 그룹과 구성원을 에 통합하는 ServiceNow데 사용됩니다. 가장 큰 차이점은 ADAM 그룹에는 ADAM 또는 신뢰할 수 있는 AD 도메인의 구성원이 포함될 수 있다는 것입니다.

ADAM 개체 만들기 자동화

Active Directory 계정을 ADAM에 동기화하려면 다음을 사용하는 것이 좋습니다. Microsoft *ADAMSync* 도구. LDAP 통합에 ADAM을 ServiceNow 사용하는 가장 일반적인 방법입니다.

권한 위임 정보

ADAM에는 기본 권한이 있는 몇 가지 기본 제공 그룹이 포함되어 있습니다. 이러한 그룹은 *cn=roles,dc=myCompany,dc=adam* 컨테이너에 있습니다. 이는 도메인 수준 그룹과 유사하며 현재 파티션의 개체에 대한 권한을 갖습니다. AD 포리스트와 마찬가지로 *cn=roles,cn=configuration,dc=myCompany,dc=adam*의 기본 그룹을 사용하여 더 높은

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

수준의 권한을 설정할 수도 있습니다. *ADSIEdit*의 구성 파티션에 연결해야 합니다. Administrators 그룹에는 기본적으로 설치 중에 지정된 계정이 포함됩니다. 이 구성원은 구성 그룹을 통해 상속되므로 항상 표시되지는 않습니다. 관리자는 모든 파티션 개체를 완전히 제어할 수 있습니다. Readers 그룹에는 기본적으로 멤버가 포함되어 있지 않으며 파티션의 모든 개체에 대한 읽기 권한이 있습니다. 사용자 그룹은 Active Directory에서와 마찬가지로 동적 그룹입니다. 전이적으로 파티션에 만들어진 모든 ADAM 사용자가 포함됩니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM 설정 테스트 및 문제 해결

테스트에 사용되는 기본 도구는 LDP입니다. 이렇게 하면 사용자 인증을 완전히 테스트할 수 있습니다.

대부분의 개체 관리는 ADAM ADSI Edit 콘솔을 사용하여 완료할 수 있으며, 이 콘솔은 개체 및 특성의 전체 컬렉션에 대한 액세스를 제공합니다. 가장 높은 수준의 제어 및 문제 해결 ADAM 서비스는 인스턴스 설치 중에 만든 서비스를 사용하는 Windows 것입니다. 서비스 이름은 작성된 인스턴스 이름에 따라 달라집니다. ADAM 서비스를 실행하려면 이 서비스가 실행되고 있어야 합니다. 연결 문제가 발생하는 경우 네트워크 구성을 검토하여 서버 및 ADAM 포트에 연결할 수 있는 적절한 네트워크 액세스 권한이 있는지 확인해야 합니다. 설치된 각 ADAM 인스턴스에 대해 Windows 이벤트 로그가 만들어집니다. 또한 ADAM 서비스 문제를 해결하는 데 유용한 도구입니다.

보안 이벤트 로그는 Windows *userProxy* 인증 문제를 해결할 때도 유용합니다. 모든 *userProxy* 로그온 시도는 보안 로그에 기록되고 원격 클라이언트 디바이스 주소, 로그온하려는 사용자의 고유 이름 및 결과 또는 상태 코드를 참조합니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM을 사용한 백업 및 복구

모든 ADAM 데이터는 표준 파일 시스템 백업 방법을 사용하여 백업할 수 있습니다.

중복

ADAM에는 AD와 동일한 기술을 기반으로 하는 복제 유틸리티가 내장되어 있습니다. ADAM 파티션의 전체 읽기 및 쓰기 복제본은 동일한 컴퓨터나 다른 컴퓨터에 존재할 수 있습니다. 이 복제본을 다양한 방법으로 사용하여 인스턴스와 내결함성 LDAP 통합을 제공할 수 있습니다. 한 가지 옵션은 방화벽을 통해 두 파티션을 인스턴스에 모두 노출하고 LDAP 등록 정보 서버 필드에서 두 서버를 모두 정의하는 것입니다.

관련 정보

ADAM(Active Directory 응용 프로그램 모드)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM과 함께 **LDAPS** 사용

userProxy 오브젝트 인증의 기본 구성은 LDAPS(보안 LDAP) 통신을 적용하는 것입니다. LDAPS는 네트워크 트래픽을 보호하기 위해 SSL 인증서가 필요합니다.

이 요구 사항을 제거하려면 구성 파티션에 연결된 *ADSIEdit* 콘솔을 사용하여 다음과 같이 변경합니다.

```
Object: CN=Directory Service, CN=Windows NT, CN=Services,
 CN=Configuration
```

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
Attribute: msDS-Other-Setings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

새 설정을 사용하려면 ADAM 서비스를 다시 시작합니다.

보안 바인드를 지원하고 전송되는 사용자 및 비밀번호 정보를 암호화하려면 서버 및 LDAP 클라이언트에 SSL 인증서를 설치해야 합니다. ADAM 서비스에는 제한적이고 제어된 사용이 있기 때문에 인증서 비용을 발생시키거나 CA(인증 기관) 인프라를 구축하지 않고도 요구 사항을 충족하는 자체 서명된 인증서를 사용할 수 있습니다. CA가 이미 있는 경우 인증서를 발급할 수 있습니다. 그렇지 않으면 자체 서명된 인증서를 만듭니다.

자체 서명된 인증서 만들기

selfssl 유틸리티를 사용하려면 IIS(인터넷 정보 서비스)가 설치되어 있어야 합니다. 인증서를 생성한 후 이 서비스를 제거할 수 있습니다. IIS 리소스 키트에서 selfssl.exe 유틸리티를 가져올 수 있습니다. IIS가 이미 설치되어 있는 경우 인증서 생성 중에 현재 사이트가 영향을 받지 않도록 새 웹 사이트를 만듭니다. Selfssl은 자체 발급한 새 인증서를 유효한 웹 사이트에 임시로 첨부해야 합니다.

Selfssl은 명령줄 도구이며 다음과 같은 공통 매개변수가 있습니다.

selfssl 매개변수 설명

매개변수	설명
/T	로컬 컴퓨터의 "신뢰할 수 있는 인증서"에 인증서를 추가합니다.
/N:cn	인증서의 일반 이름을 설정합니다. 인증서를 사용하여 웹 서비스를 실행하는 서버의 정규화된 도메인 이름과 일치해야 합니다.
/K	키 크기의 강도를 비트 단위로 설정합니다.
/V	인증서가 유효한 일 수
/S	인증서를 첨부할 웹 사이트 ID
/P	웹 서비스의 IP 포트

일반 이름 특성은 인스턴스가 ADAM 컴퓨터에 연결하는 데 사용할 외부 이름 또는 주소와 일치해야 합니다. 기본 웹 사이트인 1을 사용하지 않는 한 IIS 웹 사이트 사이트 ID를 가져와야 하며 selfssl 명령에서 정의할 필요가 없습니다. myCompany에 대한 인증서를 생성하는 샘플 명령은 다음과 같습니다.

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /
P:50001 /T
```

이 문은 10년 동안 유효한 인증서를 만듭니다. 값을 원하는 기간으로 설정하되, 이전 인증서가 만료되기 전에 새 인증서를 생성하여 인스턴스에 제출해야 합니다. 인증서의 만료 날짜를 기록해 두는 것이 좋습니다.

인증서가 생성되면 웹 사이트에서 제거하거나 임시 사이트를 만든 경우 전체 웹 사이트를 삭제할 수 있습니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM에 인증서 할당

보안 바인딩을 지원하고 전송되는 사용자 및 비밀번호 정보를 암호화하기 위해 서버 및 LDAP 클라이언트에 SSL 인증서를 설치합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
ADAM 서비스에는 제한적이고 제어된 사용이 있기 때문에 인증서 비용을 발생시키거나 CA(인증 기관) 인프라를 구축하지 않고도 자체 서명된 인증서를 사용하여 요구 사항을 충족할 수 있습니다.

프로시저

1. 인증서 MMC 콘솔을 열고 새 ADAM 서비스에서 로컬 컴퓨터 인증서와 로컬 컴퓨터 서비스 인증서에 대한 두 개의 콘솔 연결을 만듭니다.
   새 인증서는 `###(## ###)\##\###`에서 찾을 수 있습니다.
2. 인증서를 ADAM 서비스 `### - ###(ADAM ### ##)\ADAM_ADAM ### ##\### # ## ## ### \####` 컨테이너에 복사하고 인증서를 `### - ###(ADAM ### ##)\ADAM_ADAM ### ##\## \###`에 복사합니다.
3. 복사한 인증서의 세부 정보 탭을 열고 유효 기간(시작) 날짜 스탬프를 기록한 다음 인증서 키 파일에 대한 읽기 권한을 할당합니다.
   `C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA \MachineKeys`로 이동하여 타임스탬프가 일치하는 인증서를 식별합니다. ADAM을 실행하는 서비스 계정에 읽기 및 실행 권한을 할당합니다. 기본적으로 네트워크 서비스입니다.
4. ADAM 서비스를 다시 시작하여 새 인증서를 활성화합니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

공개 키 인증서 익스포트

인스턴스를 포함한 LDAPS 클라이언트는 ADAM에 대한 보안 연결을 만들기 위해 공개 키 인증서가 필요합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
위에서 사용한 서버 인증서 콘솔에서 클라이언트가 사용할 공개 키를 내보냅니다.

프로시저

1. 인증서를 선택하고 마우스 오른쪽 단추를 클릭한 다음 모든 작업/내보내기를 선택합니다.
   개인 키를 내보내지 마십시오. 기본 DER로 인코딩된 이진 X.509 형식을 선택하고 익스포트 파일 이름을 지정합니다.
2. LDAPS를 사용하여 서버에 연결하는 LDAP 클라이언트에 공용 인증서를 설치합니다.
   메시지가 표시되면 `### # ## ## ## ##`저장소에 인증서를 추가합니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAM(Active Directory Application Mode) 액세스 계정

시스템에서 응용 프로그램 인스턴스로 가져온 ADAM(Active Directory Application Mode) 개체 정보를 읽으려면 사용자 계정이 필요합니다.

다음 방법 중 하나를 사용하여 계정을 만듭니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 로컬 ADAM 사용자 계정을 만들고 암호를 할당하고 사용 권한을 할당합니다.
- ADAM 파티션의 Windows 도메인 계정에 사용 권한을 할당합니다.
- *userProxy* 계정을 사용합니다.

ADAM을 LDAP 원본으로 사용하는 경우 인스턴스의 LDAP 서버에 있는 로그인 고유 이름 필드에 ADAM 계정의 정규화된 고유 이름(FQDN)을 지정해야 합니다.

관련 정보

ADAM(Active Directory 응용 프로그램 모드)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

LDAPS 연결 테스트

LDAPS 연결을 테스트합니다. 두 개의 콘솔 연결이 있는데, 하나는 로컬 컴퓨터 인증서용이고 다른 하나는 새 ADAM 서비스의 로컬 컴퓨터 서비스 인증서용입니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. ADAM 설치 폴더 `c:\windows\adam`에서 *LDP.exe* 실행합니다.
   표준 LDP 클라이언트가 아니 Windows 므로 ADAM 버전이 선택되어 있는지 확인합니다.
2. 연결/연결 메뉴를 사용하여 새 연결을 엽니다.
   서버 이름은 인증서에 할당된 CN과 일치해야 합니다.
3. **LDAPS** 포트를 입력하고 **SSL** 확인란을 선택합니다.
   성공적인 연결의 결과는 몇 가지 일반 서버 정보이며 오류가 없습니다.
4. 서비스에 바인딩(로그인)합니다.
   일반적인 LDAP 클라이언트 연결을 복제하려면 단순 바인드 옵션을 선택합니다. 사용자 필드와 연결된 암호에 유효한 ADAM 사용자 또는 *userProxy* 고유 이름을 입력합니다.
   '다음으로 인증됨:....' 그러면 LDAPS를 사용하여 성공적으로 연결되었습니다.

관련 정보

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

ADAMSync를 사용하여 **ADAM** 채우기

관리자는 MS ADAMSync를 사용하여 MS ADAM을 사용하는 LDAP 디렉터리를 채웁니다.

주:

이 문서에서는 사용자가 Microsoft Windows Server, Active Directory 및 ADAM에 대해 최소한 기본적인 수준의 이해를 가지고 있으며 파티션이 있는 기능 ADAM(Active Directory 응용 프로그램 모드) 인스턴스가 이미 있다고 가정합니다.

다음은 샘플 절차입니다. 사용자 환경에서 실행 중이라는 사실과 복잡성으로 인해 직접적인 지원을 제공할 수 없습니다. 문제가 발생할 경우 컨설턴트 Microsoft 와 협력 Microsoft 하는 것이 좋습니다.

ADAM이 설치되고 첫 번째 파티션이 만들어지면 개체로 채울 수 있습니다.

다음 옵션을 사용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- GUI 또는 스크립트를 사용한 수동 객체 생성. 이 옵션은 비효율적이고 느립니다.
- Integration Information Server를 사용하여 Microsoft Active Directory와 통합합니다. 이 옵션은 궁극적으로 가장 많은 유연성과 기능을 제공하지만 일부 고급 구성이 필요합니다. Active Directory, ADAM 및Microsoft Exchange의 전체 주소 목록과 호환되는 무료 MIIS 버전이 있습니다. MIIS에 대한 경험이 아직 없는 경우 LDAP 통합만을 위한 새 환경을 구현하려고 시도하지 않는 것이 좋습니다.
- ADAM을 제공하는 동기화 도구 Microsoft 인 ADAMSync를 사용합니다. 이 옵션은 여기에 설명되어 있습니다.

ADAM 사용자 계정 정의

ADAM에서 사용자 계정을 정의합니다. 한 사용자 계정은 인스턴스를 연결하는 데 사용되고 다른 사용자 계정은 ADAMSync용입니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
이러한 계정은 로컬 ADAM 사용자 개체, UserProxy 개체 또는 트러스트된 도메인의 Windows 계정일 수 있습니다.

이 계정에는 *ADAM User* 인스턴스로 임포트하는 디렉터리 구조에 대한 읽기 전용 액세스 권한이 필요합니다. 이를 수행하는 가장 좋은 방법은 cn=roles,dc=myCompany,dc=adam에 있는 Readers 그룹의 멤버 특성에 계정을 추가하는 것입니다.

새 ADAM 사용자 계정은 기본적으로 사용할 수 없습니다. 새 계정을 활성화하고 암호를 설정해야 합니다.

프로시저

1. msDS-UserAccountDisabled 특성을 FALSE로 변경하여 사용자를 활성화합니다.
2. 사용자 객체를 마우스 오른쪽 버튼으로 클릭하고 암호를 재설정합니다.
3. 에 ADAM(Active Directory 응용 프로그램 모드) 정의된 대로 LDP를 사용하여 새 계정을 테스트하여 연결할 수 있는지 확인합니다.
   다음 사용 **LDAP** > 뷰/트리 옵션을 선택하고 기본 DN을 비워 두어 새 계정을 사용하여 디렉터리의 개체를 볼 수 있도록 합니다. 구성, 스키마 및 도메인 파티션이 왼쪽 창에 표시되어야 합니다. 도메인 파티션을 트래버스합니다. 새 로컬 ADAM 계정을 사용하는 경우 개체에 대한 읽기 권한이 없음을 의미하는 '자녀 없음'이 표시됩니다. 그룹 구성원 자격을 설정하고 다시 테스트합니다.

   ADAMSync는 이 *ADAMSync User* 계정을 사용하여 ADAM 파티션의 개체를 관리합니다. 이 계정은 ADAM 개체를 생성, 업데이트 및 삭제하므로 관리자 수준의 권한이 필요합니다.

   ADAMSync는 이 *ADAMSync AD* 계정을 사용하여 ADAM에 동기화될 AD 개체를 읽습니다.

ADAMSync 설정

ADAMSync는 Server 2003 R2에 포함되어 있습니다 Windows . 다른 OS를 사용하는 경우 ADAMSync를 다운로드하여 설치합니다.

스키마 확장

ADAMSync를 지원하도록 ADAM 스키마를 확장해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. c:\windows\adam에서 다음 명령을 실행하여 ADAMSync 스키마 확장을 가져옵니다. 현재 사용자에게 액세스 권한이 없는 경우 server:port를 변경하고 자격 증명을 추가해야 할 수 있습니다. 자세한 내용은 AdamSyncMetadata.ldf 파일을 참조하십시오.

```
ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c
 "cn=Configuration,dc=X" #configurationNamingContext
```

2. MS-AdamSchemaW2k3.ldf와 동일한 작업을 수행하여 Windows 2003 특성을 지원합니다.

```
ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c
 "cn=Configuration,dc=X" #configurationNamingContext
```

권장 스키마 변경

다음은 권장되는 몇 가지 추가 스키마 변경 사항입니다.

1. 새 MMC 콘솔을 열고 ADAM 스키마 스냅인을 추가합니다.
2. ADAM 인스턴스에 연결합니다.
3. 클래스 폴더를 확장하고 userProxy 클래스를 찾은 다음 속성을 엽니다.
4. 속성 탭에서 다음 선택적 속성을 확인하고 아직 존재하지 않는 속성을 추가합니다.
   - 회사
   - 부서
   - given나네
   - 메일
   - physicalDeliveryOfficeName
   - sAMAccountName
   - sn
   - 전화 번호
   - 제목
   - userAccountControl
   - userPrincipalName
5. ADAM 서비스를 다시 시작하여 새 설정을 사용하도록 설정합니다.

ADAM 구성 파일 설치

Windows 명령줄을 통해 ADAM 구성 파일을 설치합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 구성 파일을 설치합니다.

```
C:\WINDOWS\adam>adamsync /install localhost:50000
MS-AdamSyncConf-SNC.XML
```

2. 동기화 파일을 실행하여 콘솔에 기록합니다.

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. ADSIEdit 콘솔을 사용하여 결과를 검토합니다.
   ADAMSync에서 만든 새 개체와 특성이 표시됩니다.
4. ldap를 실행하여 UserProxy 인증을 테스트합니다.
   동기화 프로세스 자동화

   동기화 프로세스를 Windows 예약된 작업으로 설정합니다. 구성 파일 또는 명령줄에서 자격 증명을 제공하거나 액세스 권한이 있는 계정으로 예약된 작업을 실행해야 합니다.

   특별 참고 사항

   - 여러 소스의 ADAM을 동기화하기 위해 여러 구성 파일 및 예약된 작업을 만들 수 있습니다.

     이 예에서는 응용 프로그램 로그온으로 사용할 수 있는 sAMAccountName 특성을 가져옵니다. 소스를 동기화하려는 경우 로그온 자격 증명에 사용할 수 있는 고유한 특성 값이 있는지 확인해야 합니다. sAMAccountName은 도메인 내에서 고유하도록 보장되지만 여러 도메인에서 고유하지는 않습니다.

   - Exchange를 사용하는 Microsoft 경우 개체 필터 구성의 일부로 cn=SystemMailbox* 개체를 제외하는 것이 좋습니다.

ADAM 구성 파일 예

ADAMSync에 대한 모든 구성은 xml 파일에 저장됩니다.

주석이 있는 기본 구성 파일

ADAMSync 설치에는 MS-AdamSyncConf.xml라는 기본 구성 파일이 포함되어 있습니다. 나중에 참조할 기본 예제를 만들 수 있도록 이 파일의 복사본을 만듭니다. 이 예제는 주석이 추가된 기본 구성 파일입니다.

```
<?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>;
  <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>;
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
<!-- 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>;
```

LDAP 필터 구성 파일

구성 파일의 object-filter 값에 모든 수준의 필터링을 제공할 수 있습니다. 표준 연산자 대신 다음 xml 이스케이프 문자와 함께 표준 LDAP 쿼리 구문을 사용합니다.

- AND = "&"는 &로 대체합니다.
- OR = "|"(수직선) 바꾸기 |
- NOT = "!" 로 바꿉니다!

참조 구성 파일

다음은 샘플로 참조할 수 있는 실제 구성 파일입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
<?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>;
  <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>;
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 **LDAPS** 통신을 위한 **Microsoft Active Directory** 구성

인증서 쌍을 사용하여 Microsoft Active Directory(AD) LDAPS 통신을 활성화합니다.

주: 이러한 절차는 Windows 2003 R2 Standard Edition을 사용하여 설계 및 테스트되었으며 모든 버전의 Windows 2003에서 작동합니다.

LDAPS(보안 LDAP) 통신은 서버와 클라이언트 간의 데이터를 암호화한다는 점에서 SSL(HTTPS) 통신과 유사합니다. 이를 위해 서버와 클라이언트는 인증서 쌍을 사용하여 공통 정보를 공유합니다. 서버는 개인 키 인증서를 보유하고 클라이언트는 공개 키 인증서를 보유합니다. 이러한 인증서는 Microsoft AD(Active Directory) LDAPS 통신을 활성화하는 데 필요합니다.

Active Directory에 대해 LDAPS를 구성하려면 다음을 수행해야 합니다.

- Active Directory 도메인이 설정되어 있고 인스턴스가 방화벽을 통해 Active Directory 서버에 연결할 수 있어야 합니다.
- DC(도메인 컨트롤러)에 대한 인증서를 발급할 수 있는 CA(인증 기관)가 있는지 확인합니다. CA 인프라가 아직 없는 경우 두 가지 옵션이 있습니다.
  - 인증서를 발급할 독립 실행형 CA 설정
  - 외부 공급업체 인증서 요청
- CA가 이미 있는 경우 내부 CA에서 인증서를 생성할 수 있습니다.

모든 인증서에는 인증서 속성에서 볼 수 있는 정의된 만료 날짜가 있습니다. 인증서가 만료되면 모든 LDAPS 트래픽이 실패하고 사용자가 더 이상 인스턴스에 로그인할 수 없습니다. 이를 해결하려면 새 인증서를 발급하고 인스턴스에 설치해야 합니다.

Microsoft CA 인증서의 기본 만료 기간은 1년입니다. 외부 CA 인증서는 일반적으로 1년 단위로 구입합니다. 인증서가 만료되거나 애플리케이션의 만료 알림 기능(시스템 **LDAP** > 인증서). 이전 인증서가 만료되기 전에 새 인증서를 준비해야 합니다. 이렇게 하면 이전 인증서가 만료되기 전에 새 인증서를 설치하고 테스트할 수 있습니다.

Active Directory에 대한 독립 실행형 인증 기관 설정

SSL 액세스를 위해 Microsoft Active Directory를 구성하는 첫 번째 단계는 독립 실행형 CA(인증 기관)를 설정하는 것입니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
인증서를 발급한 후에는 필요한 서비스(IIS 및 CA)를 모두 비활성화할 수 있으므로 추가 자원 사용률에 대해 걱정하지 마십시오.

프로시저

1. IIS(Internet Information Server)를 설치합니다.
2. 독립 실행형 모드에서 인증 기관 서비스를 설치합니다.
3. 인증서 서비스 웹 응용 프로그램이 설치되어 있고 활성 상태인지 확인합니다.

다음에 수행할 작업
IIS 관리자 콘솔을 사용하여 로컬 컴퓨터를 확장하고 웹 사이트를 선택합니다. 기본 웹 사이트의 상태는 실행 중이어야 합니다. 또한 기본 웹 사이트 아래에 나열된 *CertSrv* 응용 프로그램이 표시됩니다. 사이트가 실행되고 있지 않거나 응용 프로그램이 없는 경우 계속하기 전에 문제를 해결해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

내부 인증 기관에서 인증서 생성

SSL 액세스를 위해 Microsoft Active Directory를 구성할 때 내부 인증서를 생성하고 외부 인증서를 요청해야 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
이러한 단계는 Microsoft CA 서비스에 적용됩니다. 다른 내부 CA 플랫폼이 있는 경우 로컬 CA 관리자에게 도움을 요청하십시오.

프로시저

1. 인증서를 만들려는 DC(도메인 컨트롤러)에서 `http://localhost/certsrv` 찾거나 원격 서버에 있는 경우 CA 서버 이름을 지정합니다.
2. 시작 페이지에서 인증서 요청을 클릭하고 고급 인증서 요청을 선택합니다.
3. 고급 인증서 요청 페이지에서 이 CA에 요청 만들기 및 제출을 선택합니다.
4. 다음과 같이 고급 인증 요청을 완료합니다.

고급 인증서 요청 필드

필드	항목
이름	인증서를 요청하는 DC의 FQDN(정규화된 도메인 이름)입니다.
이메일	인증서 담당자의 이메일 주소입니다.
회사	회사 이름입니다.
키 옵션 설정	
새 키 세트 작성	그것을 선택하십시오.
인증서 서명 요청	Microsoft RSA SChannel 암호화 공급자입니다.
주요 사용량	교환.
키 크기	1024를 권장합니다. 인스턴스는 최대 2048을 지원합니다.
자동 키 컨테이너 이름	그것을 선택하십시오.
로컬 컴퓨터 인증서 저장소에 인증서 저장	그것을 선택하십시오.

5. 제출을 클릭합니다.
   요청 **ID**를 제공하는 페이지로 이동합니다. 이 ID를 기록해 둡니다.
6. 보류 중인 요청을 처리하려면 다음을 완료하십시오.
   a. 인증 기관 관리 콘솔을 엽니다.
   b. 서버 노드를 확장하고 보류 중인 요청을 선택합니다.
   c. 방금 제출한 요청의 요청 ID를 찾아 마우스 오른쪽 버튼을 클릭하고 모든 작업/문제를 선택하여 요청을 승인하고 인증서를 발급합니다.
7. 발급된 인증서를 검색하려면 다음을 완료하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 요청한 DC에서 `http://localhost/certsrv` 찾거나 원격 서버에 있는 경우 CA 서버 이름을 지정합니다.

b. `## ## ### ### ## ###` 선택합니다.

c. 새 인증서에 대한 링크를 선택합니다.

d. 이 인증서 설치 링크를 선택합니다.

다음에 수행할 작업

외부 공급업체 인증서를 요청해야 합니다. 외부 CA의 인증서는 연간 $30 정도에 구입할 수 있습니다. 외부 CA에서 인증서를 요청하는 방법에 대한 자세한 절차는 Microsoft 문서 321051 를 참조하십시오. 인증서를 수신, 설치 및 테스트한 후 내보내기 절차를 따릅니다.

로컬에서 **LDAPS** 연결 테스트

SSL 액세스를 위해 Microsoft Active Directory를 구성할 때 내부 및 외부 공급업체 인증서를 설치한 후 LDAPS 연결을 테스트합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. Windows 지원 도구가 DC(도메인 컨트롤러)에 설치되어 있는지 확인합니다.
   지원 도구 설정(suptools.msi)은 Windows Server CD의 `\Support\Tools` 디렉토리에 있습니다.
2. 다음으로 이동 시작 > 모든 프로그램 > **Windows** 지원 도구 > 명령 프롬프트.
   명령행에 `ldp` 를 입력하여 도구를 시작합니다.
3. *LDP* 창에서 연결 > 커넥트 로컬 FQDN 및 포트 번호(636)를 제공합니다.
   또한 *SSL*을 선택합니다.
   성공하면 Active Directory SSL 연결과 관련된 정보가 표시되고 나열됩니다. 연결에 실패하면 시스템을 다시 시작하고 이 절차를 반복합니다.

LDAP 인증서를 신뢰하도록 공개 키 인증서 익스포트

SSL 액세스를 위해 Microsoft Active Directory를 구성할 때 공개 키 인증서를 익스포트하고 애플리케이션으로 임포트합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

인증 기관이 신뢰할 수 있는 타사 벤더가 아닌 경우 발급 CA의 인증서를 내보내야 Microsoft가 신뢰할 수 있고 연결을 통해 LDAP 서버 인증서를 신뢰할 수 있습니다. MS 인증서 서비스 사용자의 경우, 익스포트하는 데 사용된 콘솔에서 인증서를 확인하여 인증서 경로를 볼 수 있습니다. 인증서 경로 탭을 선택합니다. 체인의 모든 인증서를 내보내야 합니다. Certificate Path(인증서 경로)에서 이름을 찾아 LDAP 인증서와 동일한 폴더에서 CA 인증서를 찾을 수 있습니다. 인스턴스로 임포트할 모든 인증서를 제출합니다.

프로시저

1. 현재 또는 새 MMC 콘솔에서 인증서(로컬 컴퓨터) 스냅인을 추가합니다.
2. `##/###` 폴더를 엽니다.
3. 새 인증서를 찾습니다.
   발급 대상 열에는 도메인 컨트롤러의 FQDN이 표시됩니다.
4. 인증서를 마우스 오른쪽 단추로 클릭하고 모든 작업/내보내기를 선택합니다.
5. DER 또는 Base-64 형식으로 익스포트합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

`MyCompany.cer` 형식을 사용하여 파일 이름을 지정합니다. 도메인 컨트롤러와 안전하게 통신하기 위해 인스턴스에서 사용해야 하는 공개 키 인증서입니다.

6. 인증서를 인스턴스에 제출하기 전에 LDAPS를 로컬로 테스트합니다.

다음에 수행할 작업

이 절차를 완료한 후 공개 키 인증서를 애플리케이션으로 가져옵니다.
애플리케이션에 인증서를 업로드하려면 을(를) LDAP X.509 SSL 인증서 설치 참조하십시오.

LDAP 글로벌 카탈로그 사용

DC에 GC(글로벌 카탈로그) 역할을 부여할 수 있습니다. GC(글로벌 카탈로그) 역할은 포리스트 내 모든 도메인의 모든 개체에 대한 부분 표현으로 구성된 LDAP 호환 디렉터리입니다.

관리자는 다음 호스팅 방법 중 하나를 사용하여 LDAP(Lightweight Directory Access Protocol) 디렉터리 정보를 호스트하도록 Active Directory를 구성합니다.

- LDAP 디렉토리 정보를 호스팅하는 일반적인 방법은 포트 389 또는 636에서 기본 LDAP 또는 LDAPS(보안 LDAP)를 사용하는 것입니다. 이러한 표준 LDAP 포트는 항상 DC(도메인 컨트롤러)에 존재하며 거의 변경되지 않습니다. 이 디렉터리 파티션에 액세스하면 DC에서 호스트되는 도메인 내의 모든 개체에 액세스할 수 있습니다. 이 방법을 사용하여 다른 도메인의 객체에 액세스할 수 있는 방법은 없습니다.
- DC에 GC(글로벌 카탈로그) 역할을 부여할 수도 있습니다. GC(글로벌 카탈로그) 역할은 포리스트 내 모든 도메인의 모든 개체에 대한 부분 표현으로 구성된 LDAP 호환 디렉터리입니다. 이 LDAP 디렉터리는 포트 3268에서 액세스할 수 있으며 LDAPS는 포트 3269에서 액세스할 수 있습니다. LDAPS 및 기본 LDAP 포트의 인증서 요구 사항은 동일합니다.

글로벌 카탈로그 LDAP 의존성

- 인스턴스가 연결되는 도메인 컨트롤러에서 글로벌 카탈로그 역할이 활성화되어 있어야 합니다.
- 방화벽 규칙은 포트 3268(LDAP) 또는 3269(LDAPS)의 도메인 컨트롤러에 대한 인바운드 트래픽을 허용해야 합니다.

특별 참고 사항

- 모든 특성이 GC 파티션에 복제되는 것은 아닙니다. 이름, 성, 이메일, 전화 번호, 설명 및 주소와 같은 일반적인 속성이 포함됩니다. 추가 특성을 GC에 추가할 수 있지만 포리스트 복제 트래픽에 미치는 영향을 최소화하도록 제한해야 합니다.
- 표준 LDAP 통합은 대개 sAMAccountName을 인스턴스의 UserID로, 그리고 도메인 내에서 고유함이 보장되기 때문에 LDAP 임포트 맵의 병합 키로 사용합니다. 이 특성은 전체 도메인 포리스트를 볼 때 더 이상 고유하지 않습니다. 새 고유 속성은 UserID 및 병합 키로 식별되어야 합니다. 이들은 동일한 속성일 필요는 없으며 포리스트 디자인에 따라 다를 수 있습니다. Active Directory 관리자에게 문의하십시오. 일반적으로 userPrinicpalName은 도메인 전체에서 고유한 속성이지만 로그인할 때 사용자에게 친숙한 이름이 아닐 수 있지만 임포트의 고유 식별자에 사용할 수 있습니다. UserID에 사용되는 공통 속성은 이메일 주소입니다. 이러한 결정은 LDAP 속성 및 LDAP 매핑에 영향을 미칩니다.
- LDAP 임포트 맵에서 병합 키에 사용되는 값은 고유해야 하며 임포트되는 모든 객체에 존재해야 합니다. 고유하지 않거나 존재하지 않는 경우 잘못된 기록이 변경 내용으로 업데이트됩니다.
- LDAP 통합이 이미 있고 이를 GC로 변경하려는 경우 임포트 병합 키를 변경합니다. 병합 키를 변경하려면 먼저 새 키 값을 임포트해야 합니다.
- 통합을 중단하는 LDAP 통합을 변경하는 경우 첫 번째 단계는 해당 변경 내용을 되돌리는 것입니다. 그런 다음 시도하고 있는 것에 대한 완전한 정보를 가지고 연락하십시오 고객 서비스 및 지원 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OpenLDAP 부 스키마 수정

back-bdb (Berkley 백엔드)를 사용하는 OpenLDAP 2.3 시스템에서 관리자는 통합을 용이하게 하기 위해 스키마를 약간 수정합니다.

⚠ 경고: 여기서 설명하는 사용자 지정은 특정 인스턴스에서 사용하도록 개발되었으며, Now Support에서 지원되지 않습니다. 이 메서드는 있는 그대로 제공되며 구현 전에 철저히 테스트되어야 합니다. 이 사용자 지정에 대한 모든 질문과 의견을 커뮤니티 포럼 에 게시합니다.

OpenLDAP 2.3에서 back-bdb는 불평등 인덱싱(순서)을 제한적으로 지원합니다. generalizedTime 및 ChangeSequenceNumber 구문에 대해서만 구현됩니다. 부분 문자열을 지원하는 구문에서는 지원되지 않습니다. 불평등을 포함하는 검색 필터는 현재 상태 인덱스를 사용하여 처리됩니다.

이를 위해 이미 인덱싱되어 있거나 스키마에 있는 항목(예 *servnowid*:)을 변경하는 대신 사용자 지정 속성을 만드는 것이 좋습니다.

OpenLDAP 스키마 수정

OpenLDAP 스키마를 수정합니다. 이 단계에서는 고객 중 한 명이 인스턴스와 통합하는 데 도움이 되도록 제공한 OpenLDAP 2.3의 스키마 수정을 자세히 설명합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

⚠ 경고: 여기서 설명하는 사용자 지정은 특정 인스턴스에서 사용하도록 개발되었으며, Now Support에서 지원되지 않습니다. 이 메서드는 있는 그대로 제공되며 구현 전에 철저히 테스트되어야 합니다. 이 사용자 지정에 대한 모든 질문과 의견을 커뮤니티 포럼 에 게시합니다.

인스턴스와의 통합을 위해 OpenLDAP 스키마를 수정하려면 다음을 수행합니다.

프로시저

1. 사용자 지정 속성을 생성합니다.

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. 선택한 objectclass OID에 속성을 포함합니다.

Example

```
objectclass ( 1.3.6.1.4.1.3403000.2.2.1
    NAME 'BcfUserIdentifiers' SUP top AUXILIARY
  MAY ( uniqid $ unixid $ servnowid ) )
```

OpenLDAP 2.3에서는 서버 설정을 동적으로 변경할 수 있지만 스키마만 확장할 수 있습니다. 기존 스키마는 수정하거나 삭제할 수 없습니다. 동적 구성에서 이 속성에 대해 다른 objectclass를 작성하는 대신, 정적 구성 파일 slapd.conf를 사용하십시오.

3. slapd.conf에서 기본 데이터베이스 백엔드의 bdb 섹션에 새 속성에 대한 인덱싱을 포함합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example

```
database bdb (configs here) ....

index servnowid pres

(other indexes here) .....
```

4. 루트로 slapindex를 실행하여 이 속성을 인덱싱하면 검색 필터에서 사용할 수 있습니다. slapindex를 시작하기 전에 OpenLDAP 데몬이 실행 중이 아니거나 읽기 전용 모드인지 확인하십시오.

LDAP 삭제 기록

기본적으로 인스턴스는 LDAP에서 항목이 사라진 후에는 항목을 삭제하지 않습니다.

기록이라고도 하는 항목을 삭제하면 전체 이력과 삭제된 항목에 대한 참조도 삭제됩니다.

예를 들어, 구성 항목(CI), SLA 계약, 소프트웨어 라이센스, 구매 주문서 및 서비스 카탈로그 항목에는 모두 부서에 대한 참조가 있으며 부서가 삭제되면 통합은 해당 부서에 대한 모든 참조를 지웁니다. 또한 사용자를 삭제하면 해당 사용자가 수행한 작업에 대한 모든 기록이 손실됩니다.

조직의 필요에 따라 유지 테이블에서 모든 기록 삭제 할지 여부를 결정합니다.

동시 세션 제한

모든 노드에서 인스턴스의 사용자 또는 역할에 대한 동시 대화형 세션 수를 제한할 수 있습니다.

탐색



동시 세션 제한의 기능과 비즈니스 가치를 알아봅니다.

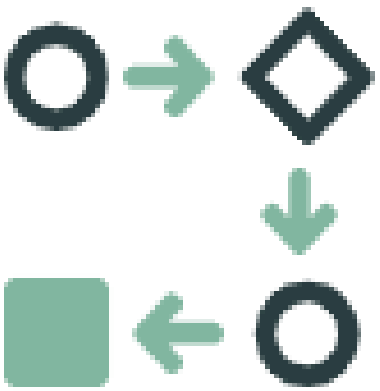
활성화



동시 세션 제한을 활성화하는 방법을 이해합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

설정



사용자 또는 역할에 대한 동시 세션 제한을 설정합니다.

사용 안 함



동시 세션 제한을 비활성화하는 방법에 대해 알아봅니다.

동시 세션 제한 탐색

모든 노드에서 인스턴스의 사용자 또는 역할에 대한 동시 대화형 세션 수를 제한할 수 있습니다.

동시 대화형 세션은 사용자가 인스턴스당 ServiceNow 활성화할 수 있는 세션 수를 나타냅니다. 활성 인스턴스 세션은 특정 ServiceNow 인스턴스에 새로 로그인할 때마다 발생합니다. 기본적으로 사용자가 가질 수 있는 활성 인스턴스 세션 수에는 제한이 없습니다.

Jakarta 릴리스에서는 사용자당 활성 동시 세션 수를 제한할 수 있습니다. 사용자가 최대 활성 세션 수에 도달한 후 로그인하면 가장 오래된 활성 세션이 종료되고 새 대화형 세션이 활성화됩니다. 사용자가 브라우저를 통해 닫힌 세션에 액세스하려고 하면 사용자는 로그인 페이지로 리디렉션됩니다.

주: 최대 세션 제한을 사용하려면 동시 세션 제한 플러그인이 활성 상태여야 합니다. 제한은 glide.authenticate.max.concurrent.interactive.sessions 속성을 통해 설정됩니다. 최대 제한 값은 제한 속성이 활성화된 모든 사용자 또는 역할에 적용됩니다. 시작할 세션 제한에 대해 사용자 또는 역할에 연결된 사용자 또는 역할이 limit_concurrent_sessions 값을 true로 설정해야 합니다. Jakarta 릴리스의 경우 이 기능은 네이티브 모바일 앱 또는 비대화형 메커니즘을 통해 생성된 세션을 지원하지 않습니다.

최대 동시 세션 1이 설정된 경우의 일반적인 사용 사례는 다음과 같습니다.

1. 사용자는 Chrome을 통해 초기 ServiceNow 인스턴스에 액세스합니다.
2. 사용자가 성공적으로 로그인하면 ServiceNow 사용자에 대한 세션 1(S1)이 생성됩니다.
3. 사용자가 Firefox를 통해 인스턴스에 대한 다른 액세스를 ServiceNow 시작하기로 결정합니다.
4. 사용자가 성공적으로 로그인하면 ServiceNow 사용자에 대한 세션 2(S2)가 생성됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 사용자의 최대 동시 세션 제한이 1이므로 S2가 생성되면 S1 세션이 무효화됩니다.
6. 사용자가 Chrome을 통해 다시 돌아가 S1 인스턴스에 액세스하면 S1 ServiceNow 이 유효하지 않으므로 사용자가 로그인 페이지로 리디렉션됩니다.

동시 세션 제한은 SAML, LDAP 및 로컬 데이터베이스 인증과 같은 모든 ServiceNow 인증 메커니즘에서 작동합니다. 또한 다단계 인증 및 모든 대화형 ServiceNow 인증 메커니즘과 함께 작동합니다. 세션의 소스는 유형 열 아래의 **sys_user_session** 테이블을 통해 볼 수 있습니다. 값은 다음과 같습니다.

- 웹 브라우저
- 모바일 브라우저
- ServiceNow 모바일 앱
- 비대화형(SOAP, WSDL, OAuth)

동시 세션 제한 플러그인 활성화 및 구성

관리자 역할이 있는 경우 동시 세션 제한 플러그인(com.glide.limit.concurrent.sessions)을 활성화할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보

프로시저
1. 다음으로 이동 모두 > 시스템 정의 > 플러그인.
2. 동시 세션 제한 플러그인을 찾아서 클릭합니다.
3. 시스템 플러그인 양식에서 플러그인 상세 정보를 검토한 다음 활성화/업그레이드 관련 링크를 클릭합니다.
4. 활성화를 클릭합니다.
5. 이 기능을 활성화하고 동시 세션의 최대 한도를 설정하려면 플러그인 파일 탭으로 이동하여 다음 속성을 찾아 설정 값을 변경합니다.

옵션	설명
glide.authenticate.limit.concurrent.interactive.sessions	값을 **True**로 설정하여 동시 세션을 제한하는 기능을 활성화할 수 있습니다. 기본적으로 이 속성은 **False**로 설정되어 있으며, 이는 사용자가 활성화할 수 있는 대화형 세션의 수에 제한이 없음을 의미합니다. 주: 이 기능을 사용하지 않으려면 이 속성을 다시 **False**로 설정합니다.
glide.authenticate.max.concurrent.interactive.sessions	모든 노드에서 사용자가 인스턴스에 대해 가질 수 있는 동시 활성 대화형 세션의 최대 수를 설정할 수 있습니다.

6. 옵션: 필요한 경우 다음 속성을 수정할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
glide.authenticate.session.types.to.limit.concurrency	이 속성은 세션 유형을 제한합니다. 기본적으로 웹 브라우저 세션에만 제한이 있습니다. 세션 유형은 다음과 같습니다. ◦ 웹 브라우저 (1) ◦ 모바일 브라우저 (2) ◦ ServiceNow 모바일 앱 (3) ◦ 비대화형 (10) 웹 브라우저의 경우 "1", 모바일 브라우저의 경우 "2" 또는 둘 다 "1,2"로 값을 구성하고 설정할 수 있습니다. 주: 웹 및 모바일 브라우저 세션에만 제한이 있을 수 있습니다. 모바일 앱 또는 비대화형 세션에서 ServiceNow 시작된 세션에는 제한이 없습니다.
glide.authenticate.limit.concurrent.sessions.across.cluster.nodes	이 속성은 인스턴스의 모든 노드에 ServiceNow 동시 세션 제한을 제한하는 대신 노드당 동시 세션 제한을 제한합니다. 기본적으로 이 값은 true로 설정되어 모든 노드에서 사용자 세션을 제한합니다. 속성이 false로 설정된 경우 다른 노드의 세션이 아닌 해당 노드의 세션에만 제한이 적용됩니다.

7. 업데이트를 클릭하여 설정을 적용합니다.

다음에 수행할 작업

사용자 또는 역할별로 동시 세션 제한 설정.

관련 정보

플러그인 목록(Yokohama)

사용자 또는 역할별로 동시 세션 제한 설정

특정 사용자 또는 특정 역할에 대해 동시 세션 제한을 설정할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 사용자 관리 > 사용자 또는 사용자 관리 > 역할.

2. 동시 세션 제한을 설정할 사용자 또는 역할을 선택하고 동시 세션 제한 확인란을 선택한 후 업데이트를 클릭합니다.
사용자 또는 역할에는 한 번에 열 수 있는 동시 세션 수에 제한이 있습니다.

사용자 또는 역할로 동시 세션 제한 비활성화

특정 사용자 또는 특정 역할에 대한 동시 세션 제한을 비활성화할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 사용자 관리 > 사용자 또는 사용자 관리 > 역할.
2. 동시 세션 제한을 비활성화할 사용자 또는 역할을 선택하고 동시 세션 제한 확인란의 선택을 취소한 다음 업데이트를 클릭합니다.
   사용자 또는 역할에는 한 번에 열 수 있는 동시 세션 수 제한이 적용되지 않습니다.

로컬 인증

로컬 인증을 사용하여 ServiceNow® 로컬 장치에서 사용자 로그인을 보호합니다.

로컬 인증은 로컬 장치에서 사용자의 ID를 확인하는 방법입니다. 사용자가 소유한 고유한 특성 또는 자격 증명을 사용하여 사용자의 로그인을 확인합니다.

의 로컬 인증 기능을 사용하여 ServiceNow®로컬 장치의 인스턴스에 안전하게 액세스합니다 ServiceNow® .

로그인 및 인증 보안

인스턴스에 대한 액세스를 제어하도록 로그인 보안 옵션을 구성합니다.

로그인 보안 구성	로그인 시나리오 정의
	
로그인 보안을 구성하는 방법을 이해합니다.	로그인 시나리오를 정의합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호 재설정



로그인 암호 재설정에 대해 알아보십시오.

로그인 및 인증 보안 살펴보기

인스턴스에 대한 액세스를 제어하도록 로그인 보안 옵션을 구성합니다.

보안 옵션

사용자 로그인 및 인증 보안의 여러 측면을 제어할 수 있습니다.

기능	설명	관련 주제
로그인/로그아웃 통제	로그인 시 표시되는 방문 페이지를 지정하고 사용자가 로그아웃하는 방법을 제어하는 등 사용자 로그인 및 로그아웃 프로세스의 여러 측면을 제어합니다.	• 로그인 시나리오 정의 • 로그아웃 확인 프롬프트 구성 • 설치 종료 • 실패한 로그인 시도에

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기능	설명	관련 주제
		대한 잠금 지정
인증 보안	암호 재설정 프로세스 및 메일 주소 저장 옵션과 같은 기능을 제어합니다. 또한 IP 주소 기반 제어를 사용하여 인스턴스에 액세스하고 SSO(Single Sign-On) 다이제스트 인증과 함께 사용할 nonce를 구현할 수 있습니다.	• 암호 정책 구성 • 암호 재설정 • 메일 주소 저장 • IP 범위 기반 인증 • nonce 구현

로그인 시나리오 정의

로그인 후 모든 사용자를 동일한 페이지로 안내할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
사용자가 인스턴스에 직접 로그온하면(예: http://{instance_name}.service-now.com/) 시스템은 다음을 수행합니다.

1. 속성의 *glide.entry.page.script*값에 액세스합니다. 속성의 기본값은 *CMSEntryPage*라는 스크립트 포함에서 파생됩니다.
2. 항목 페이지에 로그인이 필요한 경우 사용자를 인스턴스 로그인 페이지로 안내합니다.
3. 로그인 규칙이 있는 경우 사용자에게 적용합니다.

로그인 후 시스템에서 모든 사용자를 같은 페이지로 안내하도록 강제하려면:

프로시저

1. 다음으로 이동 모두 > 콘텐츠 관리 > 구성 > 구성 페이지.
2. 로그인 페이지 필드의 값을 선택하거나 원하는 대로 새 페이지를 생성합니다.

   이 페이지가 사이트 기본 페이지가 아닌 경우 항상 여기로 리디렉션됩니다. 사이트 기본 페이지인 경우 로그인 규칙이 적용됩니다. 이 값이 null이면 시스템은 navpage.do 항목 페이지로 사용합니다. 여기에 로그인 페이지를 입력하지 마십시오. 그렇지 않으면 사용자는 두 번 로그인해야 합니다.

   기록에 액세스하기 위해 인스턴스에 로그인:

   사용자가 인스턴스에 로그인하여 http://{instance}.service-now.com/incident.do?sys_id={sys_id}와 같은 sys_id(전역 고유 식별자)로 기록에 액세스하면 시스템은 다음을 수행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 아직 로그인하지 않은 경우 사용자를 로그인 페이지로 안내합니다.

b. 사용자가 액세스할 수 있는 경우 해당 기록으로 안내합니다. 사용자에게 기록에 대한 액세스 권한이 없는 경우 액세스 거부 메시지가 나타납니다.

Service Portal 또는 CMS 사이트에 로그인:

사용자가 서비스 포털 또는 CMS 사이트(예: http://<instance>.service-now.com/site-name/page.do)에 로그온하면 시스템은 다음을 수행합니다.

- Service Portal 또는 CMS 사이트 양식의 로그인 페이지 필드에 값이 있으면 사용자를 해당 로그인 페이지로 안내하고 로그인 규칙(있는 경우)을 사용자에게 적용합니다.
- 로그인 페이지가 지정되지 않은 경우 사용자는 Service Portal 또는 CMS 사이트 양식의 홈페이지 필드에 있는 값으로 리디렉션됩니다.

기록에 액세스하기 위해 Service Portal 또는 CMS 사이트에 로그인:

사용자가 http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident,{sys_id}와 같은 기록에 액세스하기 위해 Service Portal 또는 CMS 사이트에 로그온하면 시스템은 동일한 절차를 따르고 최종적으로 사용자를 기록으로 안내합니다. 사용자에게 기록에 대한 액세스 권한이 없는 경우 액세스 거부 메시지가 나타납니다.

로그인 및 직원 셀프 서비스 포털

시스템은 사용자가 직원 셀프 서비스 포털에 로그인하려는 경우에도 사용자가 액세스하려는 첫 번째 시작 페이지를 추적합니다.

다음과 같은 시나리오를 생각해 볼 수도 있습니다.

예 1:

1. 사용자가 로그인하지 않은 상태에서 URL의 특정 SYS ID를 사용하여 기록에 액세스하려고 합니다.
2. 시스템이 사용자를 로그인 페이지로 리디렉션합니다.
3. 사용자는 로그인하는 대신 직원 셀프 서비스(/ess) 포털과 같은 다른 사이트에 액세스하려고 합니다.
4. 시스템이 사용자를 로그인 페이지로 다시 리디렉션합니다.
5. 사용자가 로그인하면 직원 셀프 서비스 포털이 아닌 사용자가 처음 접근을 시도했던 기록으로 리디렉션됩니다.

예 2:

1. 사용자가 로그인하지 않은 상태에서 직원 셀프 서비스(/ess) 포털을 통해 URL의 특정 SYS ID를 사용하여 기록에 액세스하려고 합니다.
2. 시스템이 사용자를 로그인 페이지로 리디렉션합니다.
3. 사용자는 로그인하는 대신 직원 셀프 서비스 포털을 통해 다른 기록에 액세스하려고 합니다.
4. 시스템이 사용자를 로그인 페이지로 다시 리디렉션합니다.
5. 사용자가 로그인하면 두 번째가 아닌 첫 번째 기록으로 리디렉션됩니다.

로그인 방문 페이지 지정

기본적으로 사용자는 로그인 시 홈페이지를 볼 수 있습니다. 시스템 속성 또는 컨텐츠 관리 시스템을 사용하여 다른 로그인 방문 페이지를 지정할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
모든 사용자에 대한 로그인 방문 페이지를 지정하려면 sys_properties 테이블의 속성 값을 변경합니다.

프로시저
1. 탐색 필터에 `sys_properties.list` 를 입력합니다.
2. **glide.login.home** 시스템 속성을 찾습니다.
3. 값 필드에 로그인 시 모든 사용자에게 표시되는 페이지의 이름을 입력합니다.

   `<### ##>.do`를 사용하십시오. URL의 `http://''instance''.service-now.com/` 부분을 생략할 수 있습니다. 시스템에 있는 페이지의 페이지 이름 또는 URL을 판별하려면 링크를 가리킬 수 있습니다. 일부 가능한 페이지는 `welcome.do` 되고 `incident.do`.

   대시보드 방문 페이지를 지정하려면 속성을 `$dashboards.do?dashboard=<SYS_ID>`로 설정합니다. <SYS_ID> 대시보드의 sys_id로 바꿉니다.

   사용자를 서비스 포털로 안내하려면 속성을 `/sp`로 설정합니다.

   > **주:** 이 속성은 시스템 전체에 적용되므로 이 속성을 설정하면 모든 사용자에게 영향을 줍니다. 역할이 없는 사용자에 대해서만 로그인을 설정하려면 동일한 단계를 적용하고 **glide.entry.loggedin.page_ess** 속성을 사용할 수 있습니다.

   콘텐츠 관리 시스템을 사용하여 로그인 방문 페이지를 지정할 수도 있습니다.

실패한 로그인 시도에 대한 잠금 지정
시스템은 사용자 계정이 잠기기 전에 실패한 로그인 시도 횟수를 지정하고 로그인에 성공한 후 횟수를 재설정할 수 있는 비활성 스크립트 작업을 제공합니다.

시작하기 전에
필요한 역할: 관리자

프로시저
다음으로 이동 모두 > 시스템 정책 > 스크립트 작업 스크립트를 보거나 활성화합니다.

> **주:** 릴리스부터 Kingston zBoot 후 자동 잠금 해제로 **SNC** 사용자 잠금 확인 및 **SNC** 사용자 지우기 스크립트 작업이 활성화됩니다.

실패한 로그인 시도에 영향을 미치는 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정의 실패한 로그인 시도 관리(인스턴스 보안 강화) 를 참조하십시오.

스크립트 작업	설명
자동 잠금 해제로 SNC 사용자 잠금 확인	• *glide.user.max_unlock_attempts* 속성 값을 사용하여 실패한 로그인 시도 한도를 설정합니다. • *glide.user.unlock_timeout_in_mins* 속성에 지정된 기간 이후에 사용자 계정의 잠금을 해제합니다. 값을 지정하지 않으면 기본 기간인 15분 후에 시스템이 사용자 계정의 잠금을 해제합니다.
SNC 사용자 잠금 확인	실패한 로그인 시도 횟수를 추적하고 지정된 로그인 시도 실패 횟수(기본값: 5)가 지나면 사용자 계정을 잠급니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트 작업	설명
SNC 사용자 지우기	로그인에 성공한 후 사용자 기록을 업데이트합니다. 실패한 로그인 시도 횟수를 재설정하고 마지막 로그인 날짜를 업데이트합니다.

다음에 수행할 작업

사용자가 로그인을 시도할 때마다 작업이 이벤트 로그에 기록됩니다. 실패한 로그인 시도에 대한 로그를 볼 수 있습니다.

1. 다음으로 이동 시스템 정책 > 이벤트 로그.
2. 이름 필드에서 **login.failed**를 필터링합니다. 시도된 로그인 시도 이름, 날짜 및 시도에 대해 기록된 IP 주소를 볼 수 있습니다.

UI 페이지를 공개 또는 비공개로 설정

사용자가 로그인하지 않고 페이지를 보도록 하려면 페이지를 공개할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

대부분의 페이지는 로그인한 사용자만 볼 수 있습니다. 시작 페이지, 첫 페이지, 로그인 및 로그아웃 페이지와 같이 사용자가 로그인하지 않고도 볼 수 있도록 제한된 수의 페이지가 공개됩니다.

⚠ 경고: 많은 기능의 기능을 위해서는 여러 기본 시스템 공용 페이지가 필요합니다. 기본 시스템 공용 페이지를 사용하지 않도록 설정하지 마십시오.

프로시저

1. 애플리케이션 네비게이터 필터에 `sys_public.list`를 입력합니다.
2. 새로 만들기를 클릭합니다.
3. sys_public 테이블에서 다음 값을 사용하여 기록을 생성합니다.

필드	설명
페이지	페이지의 이름입니다. 예: $sp
활성	선택하면 페이지에 공개적으로 액세스할 수 있습니다. 페이지를 비공개로 설정하려면 활성 옵션의 선택을 취소합니다.

4. 저장을 클릭합니다.
   활성을 true로 설정하면 페이지가 공개되므로 `<instance_name>/sp` 또는 `<instance_name>/$sp.do` 방문하는 모든 사용자가 페이지에 액세스할 수 있습니다.

암호 복잡성 요구 사항

인스턴스의 암호는 ServiceNow® 복잡성 요구 사항을 충족해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색



암호 복잡성 요구 사항의 기능 및 비즈니스 가치를 알아봅니다.

사용



암호 복잡성 요구 사항을 활성화하는 방법을 이해합니다.

구성



암호 복잡성 요구 사항을 구성합니다.

참조 - 지원되지 않는 암호 문자입니다



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

지원되지 않는 암호 문자에 대해 알고 있습니다.

암호 복잡성 요구 사항 살펴보기

인스턴스의 암호는 ServiceNow® 복잡성 요구 사항을 충족해야 합니다.

암호 복잡성 요구 사항 정책 설정은 암호가 일련의 강력한 암호 지침을 충족해야 하는지 여부를 결정합니다.

암호 복잡성 요구 사항은 암호를 변경하거나 만들 때 적용됩니다.

암호 복잡성 요구 사항은 다음을 준수하고 작동합니다.

- *glide.apply.password_policy.on_login* 속성이 활성화되면 로그인하는 동안 사용자에 대해 암호 정책 검사가 적용됩니다. 로그인하는 동안 사용자는 암호 정책을 준수하고 인스턴스의 암호를 변경해야 합니다.
- 암호 정책 요구 사항은 모든 최신 언어에 대한 문자가 포함된 BMP(Basic Multilingual Plane)를 기반으로 합니다. ServiceNow 인스턴스는 약 10,000자의 BMP와 함께 제공됩니다.
- 허용 가능한 BMP 내의 암호를 인스턴스에 대해 설정할 수 있습니다. 이러한 BMP 내에서 준수하지 않는 암호는 허용되지 않습니다.

필요한 경우 비밀번호를 최소 90일마다 정기적으로 변경하도록 요구할 수 있습니다.

요구 사항 및 금지 문자

안전한 네트워크 환경을 사용하려면 사용자가 문자, 숫자 및 기호의 조합을 포함하는 강력한 암호를 사용해야 합니다. 이러한 조합은 일반적으로 수동 또는 자동 방법을 사용하여 취약한 암호를 추측하는 권한이 없는 사용자를 방지하는 데 도움이 됩니다.

인스턴스 암호는 다음 요구사항을 충족해야 합니다.

- 최소 8자.
- 최대 100자까지 입력할 수 있습니다.
- 소문자와 대문자를 포함합니다.
- 특수 문자를 포함합니다.
- 자릿수를 포함합니다.

다음과 같은 일반적인 잘못된 암호 목록을 금지할 수 있습니다.

- "123456", "qwerty", "!@#$%^", "aaaaa" 등과 같은 예측 가능하고 반복되는 시퀀스입니다.
- 직원 이름 또는 사용자 이름입니다.
- 관련 브랜드 또는 제품 이름입니다.
- 회사 본사, 도시, 국가 등의 위치입니다.
- 회사별 내부 용어 또는 약어입니다.
- 이모티콘.

주: 암호에 사용할 수 없는 사용자, 브랜드 또는 회사별 문자는 암호 정책 또는 암호 제외 페이지에서 구성할 수 있습니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인스턴스에서 암호 정책 사용

로그인 시 암호 정책 통제를 구현합니다. 암호가 암호 정책 기준에 맞지 않으면 사용자가 암호를 변경하도록 강제합니다.

시작하기 전에

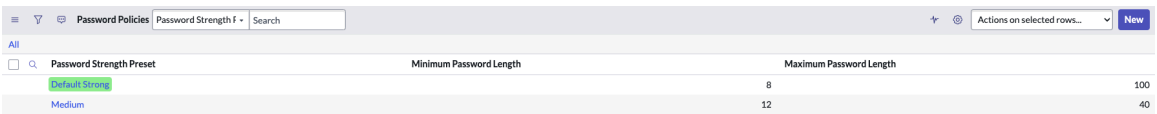
필요한 역할: 관리자

이 태스크 정보

Password Policy 플러그인(com.glide.password_policy)은 기본적으로 활성화되어 있습니다. 이 정책은 사용자가 암호를 변경하거나 재설정할 때 적용됩니다.
암호 강도 사전 설정 필드가 자동으로 기본 강력으로 설정됩니다. 새 기준을 추가하려면 다음 절차를 수행할 수 있습니다.

설치 종료 또는 암호 재설정 자격 증명 스토어 *pwd_cred_store* 속성을 통해 *ValidatePasswordStronger* 인스턴스를 사용자 지정한 경우 암호 정책 속성을 참조하여 인스턴스에 대한 암호 정책을 구현하는 방법을 알아보십시오.

주: 표시된 대로 인스턴스에 대한 활성 암호 정책이 강조 표시됩니다.



암호 정책을 변경하려면 다음으로 이동하십시오. 모두 > 암호 재설정 > 자격 증명 스토어에서 자격 증명을 선택하고 암호 정책 필드를 필요한 정책 입력으로 변경합니다.

프로시저

1. 다음으로 이동 모두 > 암호 정책 > 암호 정책.
2. 새로 만들기를 클릭합니다.
   암호 정책 양식이 나타납니다.
3. 암호 정책의 이름을 지정합니다.
4. 암호 정책 기준 섹션의 암호 강도 사전 설정 필드에서 다음 사전 설정 중 하나를 선택합니다.

암호 강도 사전 설정	설명
기본값	다음과 같이 필수 암호 문자의 필드를 자동으로 채웁니다. ◦ 최소 대문자를 1로 설정합니다. ◦ 최소 소문자를 1로 설정합니다. ◦ 최소 숫자를 1로 설정합니다. ◦ 최소 특수 문자를 0으로 설정합니다. 암호의 최소 길이는 8자이고 최대 암호는 100자입니다.
보통	다음과 같이 필수 암호 문자의 필드를 자동으로 채웁니다. ◦ 최소 대문자를 1로 설정합니다. ◦ 최소 소문자를 1로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호 강도 사전 설정	설명
	◦ 최소 숫자를 1로 설정합니다. ◦ 최소 특수 문자를 1로 설정합니다. 암호의 최소 길이는 12자이고 최대 암호는 40자입니다.
높음	다음과 같이 필수 암호 문자의 필드를 자동으로 채웁니다. ◦ 최소 대문자를 1로 설정합니다. ◦ 최소 소문자를 2로 설정합니다. ◦ 최소 숫자를 1로 설정합니다. ◦ 최소 특수 문자를 3으로 설정합니다. 암호의 최소 길이는 8자이고 최대 암호는 100자입니다.
기본 강력함	다음과 같이 필수 암호 문자의 필드를 자동으로 채웁니다. ◦ 최소 대문자를 1로 설정합니다. ◦ 최소 소문자를 1로 설정합니다. ◦ 최소 숫자를 1로 설정합니다. ◦ 최소 특수 문자를 1로 설정합니다. 암호의 최소 길이는 8자이고 최대 암호는 100자입니다.
사용자 지정	다음과 같이 필수 암호 문자의 필드를 자동으로 채웁니다. ◦ 최소 대문자를 1로 설정합니다. ◦ 최소 소문자를 1로 설정합니다. ◦ 최소 숫자를 1로 설정합니다. ◦ 최소 특수 문자를 1로 설정합니다. 암호의 최소 길이는 8자이고 최대 암호는 100자입니다. 표시되는 암호 정책 스크립트를 사용자 지정할 수도 있습니다.
고급	고급을 선택하면 암호 규칙 스크립트와 암호 강도 스크립트가 표시됩니다. 요구 사항에 따라 이러한 스크립트를 사용자 지정할 수 있습니다.

ⓘ 주: 선택한 사전 설정에 따라 암호 정책이 적용됩니다.

5. 양식의 나머지 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호 정책 양식

필드	설명
최소 암호 길이	암호의 최소 길이입니다. 이 옵션은 고급을 제외한 모든 사전 설정에 대해 표시됩니다. 이 필드를 최소 8-10자로 설정합니다.
최대 암호 길이	암호의 최대 길이입니다. 이 옵션은 고급을 제외한 모든 사전 설정에 대해 표시됩니다. 이 필드는 최대 100자로 설정합니다.
최소 대문자	암호의 최소 대문자 수(0~10자)입니다.
최소 소문자	암호의 최소 소문자(0~10자)입니다.
최소 숫자	암호의 최소 숫자(0~10자)입니다.
최소 특수 문자	암호의 최소 특수 문자 수(0~10자)입니다.
포함된 특수 문자	구분 기호 없이 제한된 특수 문자 집합을 허용합니다. 예를 들어 `$,!`를 입력하면 사용자는 암호에 "$" 및 "!"만 특수 문자로 사용할 수 있습니다. 다른 특수 문자는 사용할 수 없습니다. 다른 특수 문자가 포함된 암호는 허용되지 않습니다.
제외된 특수 문자	구분 기호 없이 제한된 특수 문자 집합을 허용합니다. 예를 들어 `@$!`를 입력하면 사용자는 암호에 '@', '$' 및 '!'를 특수 문자로 사용할 수 없습니다. 주: 이 옵션은 속성이 활성화된 경우에 사용할 수 있습니다 *glide.password_policy.use_excluded_special_ch*
사용자 데이터 허용 안 함	인증과 관련된 사용자 데이터를 허용하지 않는 옵션입니다.
시퀀스 길이 임계치	암호의 시퀀스 길이입니다.
반복 길이 임계치	암호의 반복 길이입니다. 주: ◦ 시퀀스 길이 임계치와 반복 길이 임계치는 모두 최대 8자를 가질 수 있습니다. 이러한 필드를 사용하면 "123456", "qwerty", "!@#$%^", "aaaaa" 등과 같이 시퀀스가 예측 가능하고 반복되는 취약한 암호 조합을 제한할 수 있습니다. ◦ 암호 강도 사전 설정이기본 강력함으로 설정된 경우 시퀀스 길이 임계치와 반복 길이 임계치의 길이가 모두 4자로 설정됩니다.
암호 테스트	이 필드에 실제 암호를 지정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 암호 테스트를 클릭합니다.
7. 암호가 유효한 것으로 테스트되면 제출 을 클릭하여 암호를 제출합니다.

주: 제출하기 전에 항상 암호를 테스트하십시오.

암호 정책 속성

암호 정책 속성을 사용하면 암호 정책을 관리하고, 암호 목록을 제외하고, 로그인하는 동안 암호 정책을 적용할 수 있습니다.

다음으로 이동 암호 정책 > 속성 암호 정책 속성을 보고 편집합니다.

속성	설명
glide.enable.password_policy	인스턴스에 대한 암호 정책을 활성화합니다. 이 정책은 사용자가 암호를 변경하거나 재설정할 때 적용됩니다. 이 속성은 **true**로 자동 설정됩니다. 주: • 설치 종료 또는 암호 재설정 자격 증명 스토어 (pwd_cred_store)를 통해 *ValidatePasswordStronger* 인스턴스가 사용자 지정된 경우에는 이 속성을 생성하여 시스템 속성에 추가해야 합니다. • Orlando 릴리스 이전에는 설치 종료를 사용하여 *ValidatePasswordStronger* 인스턴스가 사용자 지정된 경우 암호 정책이 작동하도록 암호 정책 속성을 만들어야 했습니다. • 릴리스부터 Orlando 는 설치 종료 사용자 지정이 없습니다. 암호 정책 속성은 기본적으로 작동합니다. 이러한 속성은 수동으로 끌 수 있습니다.
glide.enable.blacklist_password	특정 암호 사용을 금지합니다. 관리자는 제외된 암호 테이블에 암호를 삽입할 수 있습니다. 이 속성은 **true**로 자동 설정됩니다.
glide.apply.password_policy.on_login	기존 암호가 현재 암호 정책을 준수하지 않을 경우 사용자가 다음 로그인 시 암호를 변경해야 합니다. 이 속성은 **false**로 자동 설정됩니다. 값을 **true**로 설정하면 로그인하는 동안 암호 정책이 적용됩니다. 주: 이 속성을 활성화하면 새 암호 정책을 준수하지 않는 많은 수의 사용자가 암호를 변경해야 할 수 있습니다.
glide.password_policy.user_excluded_special_chars	사용자가 암호 정책 양식에서 제외된 특수 문자 옵션을 사용할 수 있도록 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
glide.validate.sys_user.password.field	관리자가 sys_user 양식 또는 목록 뷰를 편집할 때 암호 정책에 대해 사용자 암호를 확인할 수 있습니다.
glide.password.policy.generate.password.field.sys_user	sys_user 양식의 암호 설정 팝업에서 암호 필드를 비활성화합니다.
glide.user.show.password.field	sys_user 양식에서 암호 필드를 활성화합니다.
glide.password_policy.debug	암호 정책에 대한 디버그 로깅을 사용하도록 설정합니다.

암호 정책 구성

암호 정책 기준을 사용하면 암호를 보호하고 최소 암호 복잡성 요구 사항을 준수할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Password Policy [com.glide.password_policy] 플러그인은 기본적으로 활성화되어 있습니다. 사용자가 암호를 변경하거나 재설정할 때 적용됩니다. ValidatePasswordStronger 설치 종료 또는 암호 재설정 자격 증명 스토어 (pwd_cred_store)를 통해 인스턴스를 사용자 지정한 경우 암호 정책 속성을 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 암호 정책 > 암호 정책.

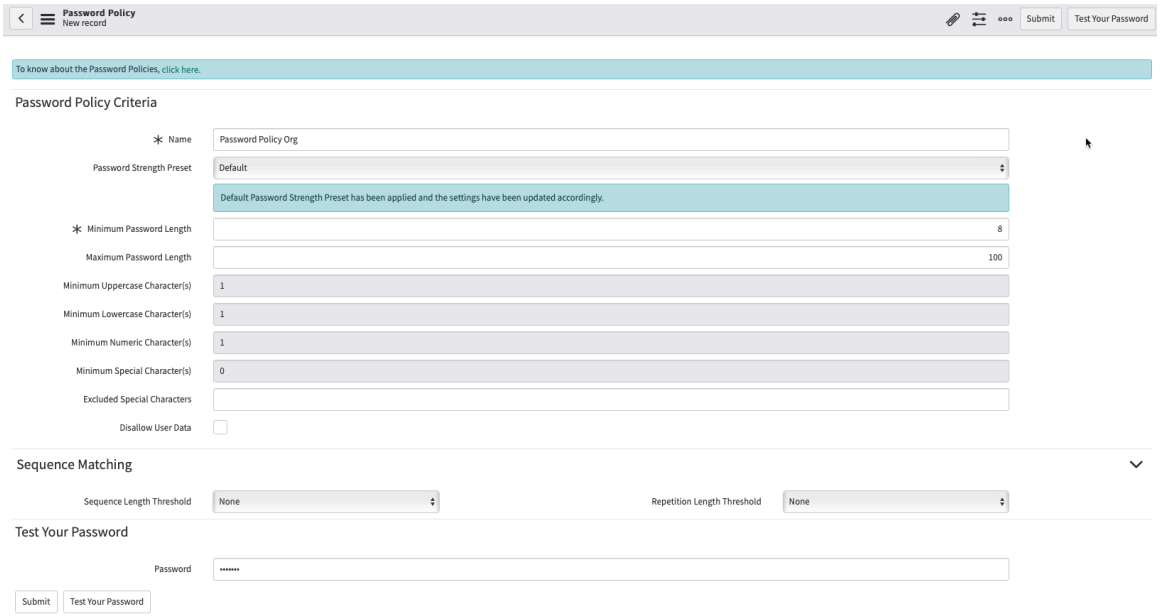
> 주: 기본 암호 수용 기준으로 활성화되어 있는 기본 강력한 사전 설정입니다. 새 기준을 추가하려는 경우 다음 단계를 수행할 수 있습니다.

2. 새로 만들기를 클릭합니다.

암호 정책 새 기록 페이지에는 암호를 설정하기 위해 지정해야 하는 다음 섹션이 있습니다.

- 암호 정책 기준
- 시퀀스 일치
- 암호 테스트

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 암호 정책의 이름을 지정합니다.
4. 암호 정책 기준 섹션의 암호 강도 사전 설정에서 사전 설정을 선택합니다. 사용 가능한 사전 설정은 다음과 같습니다.

암호 강도 사전 설정 및 설명

암호 강도 사전 설정	설명
기본값	기본값을 선택하면 다음과 같이 필요한 암호 문자가 자동으로 채워집니다. ◦ 최소 대문자 1개 ◦ 최소 소문자 1개 ◦ 최소 숫자 1개
보통	중간을 선택하면 다음과 같이 문자에 따라 필요한 암호 문자가 자동으로 채워집니다. ◦ 최소 대문자 1개 ◦ 최소 소문자 1개 ◦ 최소 숫자 1개 ◦ 최소 특수 문자 1개
높음	높음을 선택하면 암호 문자가 다음과 같이 자동으로 채워집니다. ◦ 최소 대문자 1개 ◦ 최소 소문자 2개 ◦ 최소 숫자 1개 ◦ 최소 특수 문자 3개
기본 강력함	기본 강력함을 선택하면 다음과 같이 문자에 따라 필요한 암호 문자가 자동으로 채워집니다. ◦ 최소 대문자 1개 ◦ 최소 소문자 1개

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호 강도 사전 설정	설명
	◦ 최소 숫자 1개 ◦ 최소 특수 문자 1개
사용자 지정	사용자 지정을 선택하면 다음과 같이 문자에 따라 필요한 암호 문자가 자동으로 채워집니다. ◦ 최소 대문자 1개 ◦ 최소 소문자 1개 ◦ 최소 숫자 1개 ◦ 최소 특수 문자 1개 표시되는 암호 정책 스크립트를 사용자 지정할 수도 있습니다.
고급	고급을 선택하면 암호 규칙 스크립트와 암호 강도 스크립트가 표시됩니다. 요구 사항에 따라 이러한 스크립트를 사용자 지정할 수 있습니다.

주: 선택한 사전 설정에 따라 암호 정책이 적용됩니다.

5. 테이블에 설명된 필드를 지정합니다.

암호 정책 양식

필드	설명
최소 암호 길이	암호의 최소 길이입니다. 이 옵션은 고급을 제외한 모든 사전 설정에 대해 표시됩니다. 주: 최소 암호 길이는 필수 필드이며 최소 8-10자로 설정하는 것이 좋습니다.
최대 암호 길이	암호의 최대 길이입니다. 이 옵션은 고급을 제외한 모든 사전 설정에 대해 표시됩니다. 주: 최대 암호 길이는 선택적 필드이며 최대 100자로 설정하는 것이 좋습니다.
최소 대문자	암호의 최소 대문자 수(0~10자)입니다.
최소 소문자	암호의 최소 소문자(0~10자)입니다.
최소 숫자	암호의 최소 숫자(0~10자)입니다.
최소 특수 문자	암호의 최소 특수 문자 수(0~10자)입니다.
포함된 특수 문자	구분 기호 없이 제한된 특수 문자 집합을 허용합니다. 예를 들어 "$,!"를 입력하면 사용자는 암호에 "$" 및 "!"만 특수 문자로 사용할 수 있습니다. 다른 특수 문자는 사용할 수 없으며 다른 특수 문자가 포함된 암호는 허용되지 않습니다.
제외된 특수 문자	구분 기호 없이 제한된 특수 문자 집합을 허용합니다. 예를 들어 '@$!'를 입력할 때

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	사용자는 암호에 '@', '$' 및 '! ' 를 특수 문자로 사용할 수 없습니다. 주: 이 옵션은 glide.password_policy.use_excluded_special_char 속성이 활성화된 경우에 사용할 수 있습니다.
사용자 데이터 허용 안 함	사용자 데이터를 허용하지 않도록 설정되어 있습니다.

6. 시퀀스 일치 섹션에서 시퀀스 길이 임계치 및 반복 길이 임계치를 지정합니다.

   주:
   - 시퀀스 길이 임계치와 반복 길이 임계치는 모두 최대 8자를 가질 수 있습니다. 이러한 필드를 사용하면 "123456", "qwerty", "!@#$%^", "aaaaa" 등과 같이 시퀀스가 예측 가능하고 반복되는 취약한 암호 조합을 제한할 수 있습니다.
   - 기본 강함의 경우 시퀀스 길이 임계값과 반복 길이 임계값의 길이가 모두 4자로 선택됩니다.

7. 암호 테스트 섹션에서 암호를 지정합니다.
8. 암호 테스트를 클릭합니다.
9. 암호가 유효하면 제출 을 클릭하여 암호를 제출합니다.

   주: 제출하기 전에 항상 암호를 테스트하십시오.

사용자에 대한 암호 구성

구성된 암호 정책에 따라 인스턴스의 사용자 암호를 설정합니다.

시작하기 전에

첫 번째 로그인 암호를 설정하기 위해 생성된 사용자입니다. 자세한 내용은 사용자 생성 을 참조하십시오.

사용자 양식에서 직접 암호 필드를 채우려면 활성화를 활성화하여 sys_user 양식 (glide.user.show.password.field)에 암호 필드를 표시합니다 . 속성에 대한 자세한 내용은 문서를 참조하십시오 암호 정책 속성.

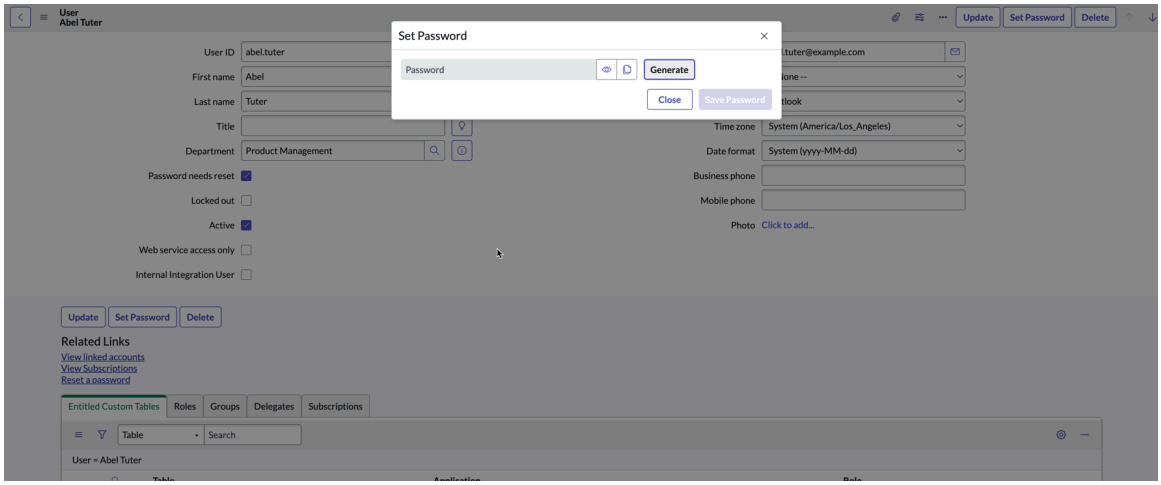
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 사용자 관리 > 사용자.
2. 사용자 페이지의 목록에서 사용자를 선택합니다.
3. 암호 정책에 따라 암호를 설정하려면 암호 설정을 클릭합니다.

   암호 설정 팝업이 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

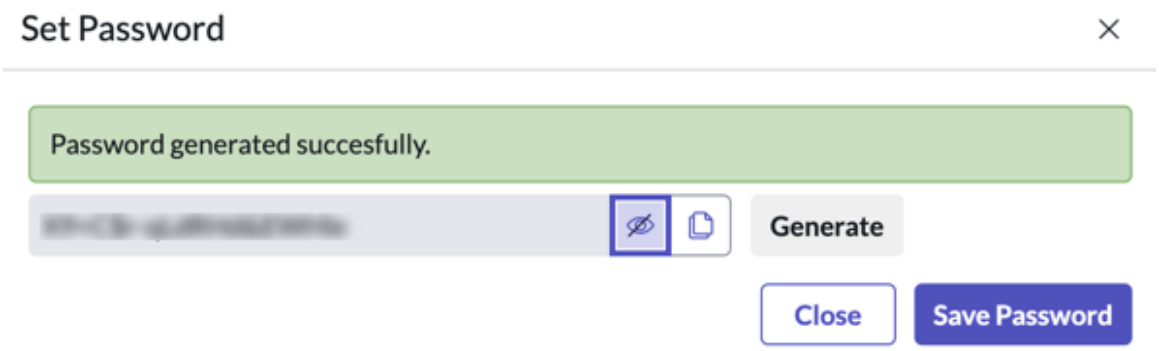


4. 암호 설정에서 다음을 수행합니다.

   a. 생성을 클릭하여 암호를 생성합니다.

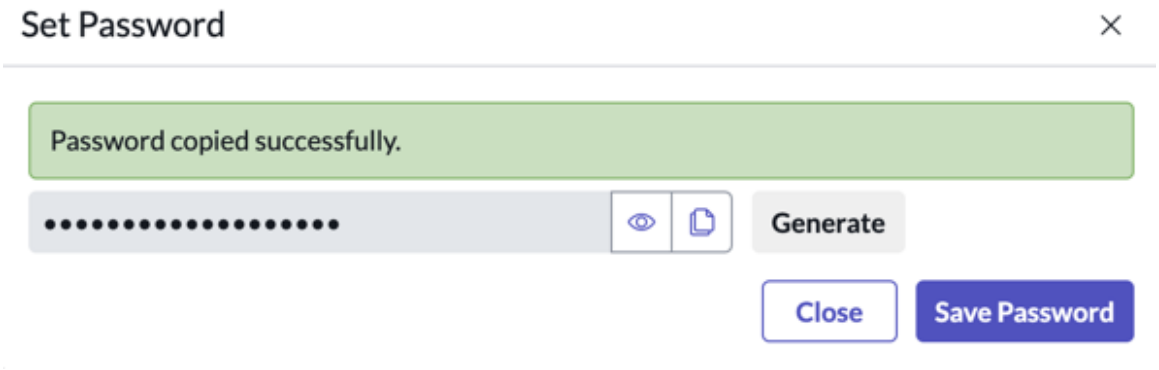


   b. 암호를 보려면 보기 아이콘을 클릭합니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

c. 복사 아이콘을 클릭하여 사용자와 공유할 암호를 복사합니다.



5. **Save** Password(암호 저장)를 클릭합니다.

사용자에 대한 암호가 설정됩니다. 또한 암호에 REST 필요 확인란이 자동으로 활성화됩니다.

처음 로그인할 때 사용자는 로그인 시 동일한 비밀번호를 사용해야 하며, 관리자가 구성한 비밀번호 정책에 따라 로그인 시 비밀번호를 변경해야 합니다.

인스턴스의 암호 정책을 통한 암호 제외

제외된 암호 테이블에 암호를 추가하여 인스턴스에서 사용자가 특정 암호를 사용하지 못하게 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
필요한 만큼 암호를 금지할 수 있습니다. 몇 가지 예는 다음과 같습니다.

- "123456", "qwerty", "!@#$%^", "aaaaa" 등과 같은 예측 가능하고 반복되는 시퀀스입니다.
- 직원 이름 또는 사용자 이름입니다.
- 관련 브랜드 또는 제품 이름입니다.
- 회사 본사, 도시, 국가 등의 위치입니다.
- 회사별 내부 용어 또는 약어입니다.
- 이모티콘.

프로시저

1. 다음으로 이동 모두 > 암호 정책 > 제외된 암호.
2. 제외 목록에 암호를 추가하려면 새로 만들기를 클릭하고 암호를 입력합니다.
3. 다음으로 이동 암호 정책 > 제외 목록 관리 사용자의 암호를 관리하고 사용자가 인스턴스에 잘못된 암호를 사용하지 못하게 합니다.

   제외 목록 관리에는 일반적으로 사용되는 약 5000개의 암호가 있습니다.

지원되지 않는 암호 문자

지원되지 않는 암호 문자가 있습니다. 암호 복잡도 요구 사항에 따라 ServiceNow 사용자는 이러한 문자를 사용할 수 없습니다.

안전한 네트워크 환경을 사용하려면 사용자가 문자, 숫자 및 기호의 조합을 포함하는 강력한 암호를 사용해야 합니다. 이러한 조합은 일반적으로 수동 또는 자동 방법을 사용하여 취약한 암호를 추측하는 권한이 없는 사용자를 방지하는 데 도움이 됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 암호 정책 요구 사항은 모든 최신 언어에 대한 문자가 포함된 BMP(Basic Multilingual Plane)를 기반으로 합니다. ServiceNow 인스턴스는 약 10000자의 BMP와 함께 제공됩니다.
- 이 허용 가능한 BMP 내의 암호 문자는 인스턴스에 대해 설정할 수 있으며, 이 BMP 내에서 준수하지 않는 암호 문자는 허용되지 않습니다.

주: 비밀번호에 사용할 수 없는 사용자 또는 회사별 문자는 비밀번호 제외 목록에서 구성할 수 있습니다.

암호 정책 특성에 대한 자세한 정보는 암호 정책 특성의 내용을 참조하십시오.

암호 재설정

기본 셀프 서비스 암호 재설정 프로세스를 사용하면 사용자가 서비스 데스크 에이전트의 도움 없이 암호를 재설정할 수 있습니다.

Example: 기본 셀프 서비스 암호 재설정 플로우

1. 암호를 기억하지 못하는 사용자는 로그인 화면에서 암호를 잊으셨습니까? 링크를 클릭할 수 있습니다.
2. 암호 재설정 애플리케이션이 시작됩니다. **ID** 페이지에서 사용자는 사용자 이름을 입력하여 자신을 식별합니다.
3. 확인 페이지에서 사용자는 사용자 이름과 연관된 사용자임을 증명합니다. 이 예에서 사용자는 사용자 프로파일과 연결된 이메일 주소를 입력합니다. 관리자는 다른 검증 방법을 구성하거나 추가 검증(예: 사용자만 대답할 수 있는 개인 질문)을 요구할 수 있습니다.
4. 재설정 페이지에서는 사용자에게 지침을 위해 이메일을 확인하라는 메시지를 표시합니다.
5. 사용자가 이메일을 열고 여기 링크를 클릭하여 암호를 재설정합니다. 링크는 지정한 기간 동안 유효합니다(**password_reset.request.expiry** 속성 사용).
6. 암호 재설정 페이지에서는 사용자에게 암호를 재설정하도록 안내합니다.

기본 셀프 서비스 암호 재설정####(`com.glideapp.password_reset`)는 다음을 정의합니다.

- 사용자가 암호를 잊으셨습니까?를 클릭할 때 리디렉션되는 위치를 지정하는 URI입니다. 기본적으로 이 값은 **/$pwd_reset.do?sysparm_url=ss_default**이며, 이는 속성에 사용되는 *glide.security.password_reset.uri* 값과 동일합니다. 이전 릴리스에서는 이 값이 **/reset_password.do**로 설정되었습니다.
- 암호 재설정 **URL** 사용 옵션은 사용자가 '암호를 잊으셨습니까?'를 클릭한 후 암호를 재설정할 수 있는 링크가 포함된 이메일을 받도록 지정합니다.
- 개인 데이터 - 이메일 주소 입력 검증 플로우는 3단계 암호 재설정 플로우를 지정합니다.

이 양식에 액세스하고 필드를 구성하는 방법은 암호 재설정 프로세스 구성을 참조하십시오.

주:

- 이 기능은 사용자 기록에 지정된 사용자 이름과 암호를 입력하는 로컬 인증 사용자에 대해 작동합니다. SSO 솔루션 또는 LDAP 통합을 통해 인스턴스에 로그인하는 사용자는 예시 셀프 서비스 암호 재설정 프로세스를 사용하여 암호를 재설정할 수 없습니다.
- 최종 사용자는 알림 기본 설정을 활성화하고 구성해야 합니다. 구독 기반 알림을 참조하십시오. 관리자는최종 사용자에게 전송되는 이메일을 수정할 수 있습니다.

암호 재설정 알림 이메일 텍스트 수정

셀프 서비스 암호 재설정 프로세스 사용자는 암호 재설정을 요청하면 이메일 알림을 받습니다. 이메일 텍스트 및 알림의 다른 측면을 수정할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
이 프로세스는 사용자가 구독 기반 알림 인 경우에만 관련이 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 통보 > 알림.
2. 암호 재설정 **URL** 알림을 선택합니다.
3. 포함될 내용 섹션에서 이메일 텍스트를 수정합니다.
   알림의 다른 측면을 구성하는 방법에 대한 자세한 내용은 이메일 알림 만들기를 참조하십시오.

속성 구성 암호 재설정

최종 사용자의 경험을 구성하는 암호 재설정 속성을 지정할 수 있습니다.

시작하기 전에
필요한 역할: password_reset_admin

이 태스크 정보
속성에 대해 입력할 수 있는 값의 범위 제한은 없지만 1부터 시작하는 양의 정수 값만 사용하는 것이 좋습니다. 속성의 상한 범위에 대한 제한을 결정할 때는 사용자가 수행하는 작업을 고려합니다.

예를 들어 사용자가 ID를 확인하는 데 100번의 시도를 허용하지 않을 수 있습니다. 더 일반적인 값은 3회입니다. 마찬가지로 등록 프로세스를 완료하는 사용자가 30개의 보안 질문을 선택하고 답변하는 데 시간을 소비하도록 강요하지 않을 수 있습니다. 가장 일반적으로 사용되는 보안 질문의 수는 5개에서 7개 사이입니다.

프로시저

1. 다음으로 이동 모두 > 암호 재설정 > 속성.
   속성에 대한 암호 재설정 자세한 내용은 다음을 참조하십시오. 암호 재설정 전역 속성 .
2. 필요에 따라 설정을 업데이트하고 저장을 클릭합니다.

메일 주소 저장

로그인 시 메일 주소 저장 확인란을 선택하면 쿠키가 사용자의 컴퓨터에 저장됩니다. 이 쿠키는 후속 방문 시 사용자를 자동으로 인증합니다.

사용자가 로그아웃하면 쿠키가 삭제됩니다. 메일 주소 저장 확인란의 기본값은 한 속성에 의해 제어되며, 로그인 페이지에 확인란이 표시되는지 여부는 다른 속성에 의해 제어됩니다.

두 개의 속성과
glide.ui.user_cookie.life_span_in_daysglide.ui.user_cookie.max_life_span_in_days
glide_user 시스템에서 생성한 쿠키 만료 값을 제어합니다. 사용자가 "메일 주소 저장"을 사용하도록 설정된 인스턴스에 액세스하면 최대 수명 제한(glide.ui.user_cookie.max_life_span_in_days)에 도달할 때까지 쿠키 만료 기간이 재설정됩니다.

주: 이러한 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정의 다음 주제를 참조하십시오.

- 절대 세션 시간 제한 기간 최소화[Security Center 1.3에서 업데이트됨]
- 세션 시간 제한 기간 최소화[Security Center 1.3에서 업데이트됨]

메일 주소 저장 확인란의 기본값 변경

메일 주소 저장 확인란의 기본값을 변경할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 속성 > **UI** 속성.
2. 속성()*glide.ui.remember.me.default*을 *Default value of "Remember me" checkbox on login page* 찾습니다.
3. 메일 주소 저장 확인란의 기본값을 아니요로 설정하려면 속성 확인란의 선택을 취소합니다.
4. 메일 주소 저장 확인란의 기본값을 예로 복원하려면 속성 확인란을 선택합니다.

메일 주소 저장 확인란 제거

사용자가 이 기능에 액세스할 수 없도록 메일 주소 저장 확인란을 제거할 수 있습니다.

시작하기 전에
필요한 역할: security_admin

주: 이 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 내용 저장하기 제거 .

프로시저

1. 당신의 역할을 security_admin로 승격시키십시오.
2. 다음으로 이동 시스템 속성 > **UI** 속성.
3. 속성()*glide.ui.forgetme*을 *Remove "Remember me" checkbox from login page* 찾습니다.
4. 속성 확인란을 선택합니다.
   이 설정은 메일 주소 저장 확인란을 제거하고, 기존 쿠키를 무효화하고, 메일 주소 저장 기능을 완전히 사용하지 않도록 설정합니다.
5. 로그인 페이지에 대한 메일 주소 저장 확인란을 복원하려면 속성 확인란의 선택을 취소합니다.

로그아웃 확인 프롬프트 구성

로그아웃 확인 프롬프트를 활성화하여 사용자가 실수로 로그아웃하는 것을 방지할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보

주: 다음 절차는 가장 최신의 가장 일반적으로 사용되는 UI 이전 버전 코어 UI에서만 작동합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 속성 > 시스템.
2. 로그아웃 요청을 확인하라는 메시지 사용자에게 메시지 표시 속성을 찾아 확인란을 선택합니다.
3. 사용자가 로그아웃 버튼을 클릭하면 확인 대화 상자가 표시됩니다.

nonce 구현

SSO(Single Sign-On) 다이제스트 인증과 함께 사용할 nonce를 구현할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Single Sign-On의 암호화되지 않은 토큰 또는 암호화된 토큰 메서드와 함께 nonce를 사용하려면 이러한 단계가 몇 가지 사소한 변경만으로 적용됩니다.

주: nonce는 로그인 요청에만 사용되며 다른 유형의 요청에는 사용되지 않습니다. 시스템이 로그인 후 nonce 값을 수신하면 nonce가 사용되지 않습니다.

복지

nonce를 사용하면 악의적인 사용자가 시스템에 로그인하기 위해 재생 공격을 수행하는 것이 금지됩니다.

Nonce 프로세스 흐름

고객이 다이제스트된 토큰 Single Sign-on을 구현하고 nonce의 보안을 추가하려는 경우 특정 프로세스 흐름을 따릅니다.

1. 사용자가 고객의 포털에 로그인합니다.
2. 고객은 필요한 SSO 매개변수를 생성하고 끝에 임의의 nonce를 추가합니다. 예를 들어 고객이 쿼리 문자열을 통해 인증 응답을 전달하는 경우 다음과 같이 표시될 수 있습니다.

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

인스턴스가 이 요청을 수신하고 인증 변수를 검색합니다. 인증 응답의 무결성을 확인하기 전에 인스턴스는 내부 테이블(u_authentication_nonce)에 대해 nonce를 검사하여 아직 존재하지 않는지 확인합니다. 해당 테이블 내에 nonce가 없는 경우 nonce가 테이블에 추가되고 인증 프로세스를 계속할 수 있습니다. 그러나 해당 nonce 값이 테이블 내에 이미 있는 경우 인증 시도가 취소되고 `## ## failed_missing_requirement` 가 반환되어 일반적으로 사용자가 로그인 페이지로 돌아갑니다.

nonce 구현

인증 헤더에 암호화 nonce를 추가하여 한 번만 사용할 수 있도록 합니다.

- 호출 *glide.authenticate.header.nonce_key* 된 시스템 속성을 만들고 해당 값을 NONCE에 사용 중인 변수 이름(예: NONCE 또는 NCE)으로 설정합니다.
- `u_authentication_nonce`라는 새 테이블을 만듭니다. `u_nonce`라는 테이블에 필드를 추가합니다.
- 이동 시스템 속성 > 설치 종료 ExternalAuthentication()*glide.authenticate.external_property*을 재정의하는 `DigestSingleSignOnNonce`라는 항목을 만듭니다.
- 새로 만든 DigestSingleSignOnNonce의 스크립트 부분에 다음 코드를 추가합니다.

```
gs.include("PrototypeServer");

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");
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
 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);
     if (userLoad == null)
      return "failed_authentication";

     ugr.initialize();
     ugr.addQuery(fieldName, data);
     ugr.query();
     if (!ugr.next())
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
      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();
 gs.log("Inserted new nonce: " + sentNonce);
 return true;
}
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
};
```

- 새 설치 종료를 저장한 후 DigestSingleSignOn 설치 종료로 이동하여 Active=false로 설정되어 있는지 확인합니다.

이제 nonce를 구현하도록 인스턴스를 구성해야 합니다.

다단계 인증**(MFA)**

MFA(다단계 인증)를 활성화, 사용 및 구성하는 방법을 알아봅니다.

탐색



MFA의 기능 및 비즈니스 가치에 대해 알아봅니다.

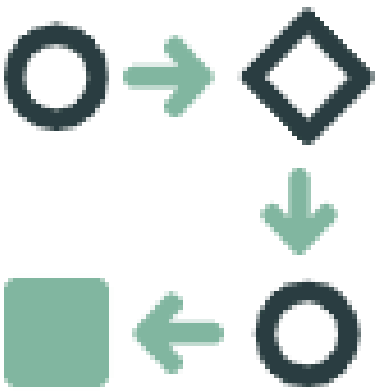
활성화



MFA를 활성화하는 방법을 이해합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용



MFA를 구성하고 사용합니다.

1회 사용자 인증(SSO)을 통한 MFA



SSO(Single Sign-On)를 사용하여 MFA를 구성하는 방법에 대해 알아봅니다.

다단계 인증**(MFA)** 적용

Yokohama 릴리스부터 SSO가 아닌 로그인에 대한 MFA 적용.ServiceNow

MFA는 사용자가 로그인 시 ID를 증명하기 위해 두 개 이상의 증거를 제공하도록 요구하여 보안을 강화합니다. MFA는 피싱 및 계정 탈취와 같은 위협으로부터 계정을 보호합니다.

MFA는 다양한 ID 탈취 관련 공격에 대한 중요한 보안 도구입니다. ServiceNow Yokohama 업그레이드 이후 기본적으로 MFA를 적용하고 비 SSO 로그인(사용자 이름과 암호만 사용하여 로그인을 수행하는 사용자 또는 LDAP 기반 인증)에 대해 의무화하여 보안 태세를 강화하고 위반 위험을 줄입니다.

MFA 적용은 기본적으로 Yokohama에서 활성화되거나 Yokohama로 업그레이드되는 MFA 정책을 통해 수행됩니다.

주:

- 이 정책은 로컬(사용자 이름 및 암호) 또는 LDAP 기반 인증을 수행하는 모든 비**snc_external** 사용자에 대해 활성화됩니다.
- 인스턴스 관리자는 MFA 컨텍스트 정책, 정책 기준 또는 정책 조건을 변경하여 적용 범위를 수정할 수 있습니다.

MFA 적용에 대한 자세한 내용은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 모든 프로덕션 및 비프로덕션 인스턴스에 적용됩니다.
- 모든 비**snc_external** 사용자 및 비**SSO** 로그인에 적용됩니다.
- 기본 인증 및 OAuth와의 통합 리소스 소유자 암호 자격 증명 부여에는 Yokohama의 MFA가 필요하지 않습니다.

시행으로 인한 변경 사항에 대한 자세한 내용은 을 참조하십시오 MFA 적용으로 인한 변경.

MFA에 대한 자세한 내용은 을 참조하십시오 Multi-factor Authentication 살펴보기.

관련 정보

다단계 인증 구성

다단계 인증(MFA) 사용

MFA 적용 속성

MFA 적용 문제 해결

자주 묻는 질문 - MFA 적용

MFA 적용으로 인한 변경

MFA 적용으로 인해 예상되는 변경에 대한 정보입니다.

다음과 같이 예상되는 MFA 적용 변경:

- 통합에 영향을 미치지 않습니다.
- MFA를 이미 등록한 사용자는 로컬 로그인 중에 MFA에 대한 문제가 계속 발생합니다.
- 사용자가 아직 MFA를 설정하지 않은 경우 Yokohama 업그레이드 후 MFA를 등록할 수 있는 일정 기간 동안 MFA를 받지 않아도 됩니다.
- 사용자가 자체 등록에 실패하면 면제 기간(기본 30일)이 완료되면 MFA가 적용되며 MFA를 설정해야 합니다.
- 90일 후에는 MFA가 기본적으로 적용됩니다. 90세 이후 최초 로그인에 대한 자가 등록 기간은 없습니다. 관리자는 이 기간을 구성할 수 있습니다.

관리자는 다음을 기반으로 MFA 적용을 준비할 수 있습니다.

- MFA 컨텍스트 정책 구성을 검토하고 비즈니스 요구 사항에 따라 정책 조건을 조정합니다.
- 면제해야 하는 다른 사용자가 있는 경우 기본적으로 제공된 면제된 그룹을 추가합니다.
- MFA 적용 속성을 검토하고 요구 사항에 따라 조정합니다. 자세한 내용은 MFA 적용 속성 문서를 참조하십시오.

Example: **MFA** 적용 30일 후의 **MFA** 적용 시나리오

- **Acme** Corp의 시나리오 **1**: 인스턴스에서 사용자에게 활성 MFA 정책이 없는 경우입니다. Sarah가 로컬 인증을 사용하여 인스턴스에 액세스한다고 상상해 보십시오. 로그인 시 Yokohama 릴리스로 업그레이드하면 MFA에 등록하라는 메시지가 표시됩니다. 이 설정을 완료하는 데 30일이 걸립니다. Sarah가 설정을 완료하지 않으면 30일 후에 계정에 로그인하려면 MFA가 필요하며 MFA가 설정될 때까지 액세스할 수 없습니다.
- **Acme** Corp의 시나리오 **2**: 인스턴스에서 Anita는 이미 로컬 인증과 함께 MFA였습니다. Anita는 30일의 자가 등록 기간이 없는 MFA를 계속 요구합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- **Acme** Corp의 시나리오 **3**: 이 인스턴스에서 Olivia는 인증에 SSO(Single Sign-On)를 사용합니다. 로그인 환경에는 영향을 주지 않으며 Olivia는 MFA에 적용되지 않습니다.
- **Globex** Corp의 시나리오 **4**: 인스턴스에서 사용자가 회사의 신뢰할 수 있는 네트워크 외부의 모든 로컬 로그인 시도에 대해 MFA를 요구하는 MFA 정책을 이미 가지고 있는 경우. Yokohama 또는 이후 릴리스로 업그레이드할 때 사용자 로그인에 대한 MFA 적용 동작은 동일하게 유지됩니다.

MFA 적용 속성

Yokohama에서 MFA 적용을 위한 속성을 구성하고 Yokohama로 업그레이드합니다.

MFA 적용 속성을 설정하려면 **sys_properties.list** 로 이동하여 MFA 적용 속성을 확인하거나 변경합니다.

MFA 적용 속성

필드	설명
glide.authenticate.multifactor.setup.bypass.max	사용자가 다단계 인증 설정을 바이패스할 수 있는 횟수입니다(가능한 최대 바이패스 수는 3이며 그 이상은 3으로 처리됨).
glide.authenticate.multifactor.self_enrollment.days	사용자에게 MFA에 자체 등록할 수 있는 옵션이 제공되는 일수를 나타내며, 이 기간이 지나면 사용자에게 자동으로 MFA가 적용됩니다. 90을 초과하는 값은 90일로만 처리됩니다.
glide.authenticate.multifactor.enforcement.days	새 사용자에게 MFA에 자체 등록할 수 있는 옵션이 제공되는 최대 일수를 나타내며, 이 기간이 지나면 SSO가 아닌 로그인을 수행하는 모든 새 사용자에게 자동으로 MFA가 적용됩니다. 270을 초과하는 값은 270일로만 처리됩니다.
glide.authenticate.multifactor.enforcement.debug	MFA 적용 디버그 로거 MFA 로그인을 위한 플로우 디버깅을 지원합니다. 주: 이 속성은 인스턴스에 없습니다. 필요한 경우 속성을 작성하고 사용하도록 설정해야 합니다.
glide.authenticate.hybrid_user_tracking.enabled	하이브리드 사용자를 추적하기 위한 속성입니다. 해당 sys_user 기록에 "웹 서비스 액세스 전용"으로 표시되지 않았지만 사용자 이름과 암호를 사용하여 통합(예: API 로그인)을 수행하는 사용자 계정은 이 속성을 활성화하면 "사용자 로그인 정보" 테이블에서 추적됩니다. 주: 이 속성은 인스턴스에 없습니다. 필요한 경우 속성을 작성하고 사용하도록 설정해야 합니다.
glide.authenticate.hybrid_user_tracking.debug	하이브리드 사용자 API 로그인을 추적하기 위한 디버그 로거입니다. 쪽

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MFA 적용 속성

필드	설명
	주: 이 속성은 인스턴스에 없습니다. 필요한 경우 속성을 작성하고 사용하도록 설정해야 합니다.

MFA 적용 문제 해결

MFA 적용으로 인한 문제 해결 정보입니다.

ServiceNow Yokohama 업그레이드 이후 기본적으로 MFA를 적용하고 비 SSO 로그인(사용자 이름과 암호만 사용하여 로그인을 수행하는 사용자 또는 LDAP 기반 인증)에 대해 의무화하여 보안 태세를 강화하고 위반 위험을 줄입니다.

MFA 적용은 기본적으로 Yokohama에서 활성화되거나 Yokohama로 업그레이드되는 MFA 정책을 통해 수행됩니다. 다음은 MFA 동작이 변경된 경우 수행할 수 있는 몇 가지 문제 해결 작업입니다.

- 문제 해결 도구를 사용하여 디버그
- 로그 위치 및 디버그 속성으로 이동합니다.
- MFA를 사용하는 동안 사용자 경험에 따라 MFA 시나리오 이해
- 이전 릴리스에서 업그레이드로 인한 MFA 문제 이해

MFA 디버그

디버그 정보를 이해하려면 다음 도구 중 하나 또는 조합을 사용하십시오.

- **Splunk** - 디버그 로그를 확인합니다.
- 시스템 로그 또는 노드 로그입니다.
- **MFA** 에 대한 디버그 로그를 분석하기 위한 HAR 로그입니다.

로그 위치 및 디버그 속성

로그에 대한 자세한 내용을 보려면 다음 위치로 이동합니다.

- 시스템 로그를 보려면 다음으로 이동하십시오. 모두 > 시스템 로그 > 시스템 로그.
- 노드 로그의 경우 다음으로 이동 모두 > 시스템 로그 > 공공 서비스 > 노드 로그 파일 브라우저.

디버그 목적으로 시스템 디버그 로그와 인스턴스 노드 로그가 필요합니다. 다음은 사용하도록 설정해야 하는 디버그 속성입니다.

- `glide.webauthn.debug.enabled`
- `glide.log.default_log_debug`
- `glide.authenticate.policy.debug`
- `glide.authenticate.hybrid_user_tracking.debug`

시나리오 기반 **MFA** 문제

시나리오 1: 사용자가 두 번째 요소를 사용하여 로그인할 수 없음

사용자에 대한 MFA를 재설정하고 다음 테이블에서 이전 사용자 기록을 삭제합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- `user_multifactor_auth`
- `sys_user_public_credential`
- `sys_user_multi_factor_setup`

시나리오 2: 관리자가 두 번째 요소를 사용하여 로그인할 수 없음

관리자 액세스 권한이 있는 다른 사용자는 차단된 관리자 사용자에 대한 MFA를 재설정할 수 있습니다. 여전히 문제가 존재하는 경우 지원 팀에 ServiceNow 문의하십시오.

시나리오 3: MFA 설정 또는 확인 중 오류가 관찰됨

"관련 오류 코드/경고: 6자리 검증 코드가 잘못되었습니다. 올바른 코드로 다시 시도하십시오.".

다음 단계를 수행합니다.

- TOTP 인증자 앱의 경우 인증자 MFA 장치와 인스턴스의 날짜 및 시간이 동기화되지 않으면(±30초) TOTP 코드가 허용되지 않습니다. 장치 및 인스턴스 날짜 및 시간을 확인합니다.
- 이메일의 경우 `sys_user` 테이블에서 사용자 수준 알림, 아웃바운드 이메일 구성 및 사용자를 올바르게 구성합니다.
- SMS의 경우 Twilio 또는 다른 SMS 서비스 제공자 통합을 올바르게 구성하고 활성으로 설정합니다. 사용자의 휴대폰 번호가 `sys_user` 테이블에서 올바르게 구성되어 있는지 확인합니다.

업그레이드로 인한 문제

TBD.

자주 묻는 질문 - **MFA** 적용

MFA 시행으로 인한 일부 FAQ에 대한 상세 정보입니다.

MFA는 다양한 ID 탈취 관련 공격에 대한 중요한 보안 도구입니다. ServiceNow Yokohama 업그레이드 이후 기본적으로 MFA를 적용하고 비 SSO 로그인(사용자 이름과 암호만 사용하여 로그인을 수행하는 사용자 또는 LDAP 기반 인증)에 대해 MFA를 필수로 설정합니다.

MFA 적용은 기본적으로 Yokohama에서 활성화되거나 Yokohama로 업그레이드되는 MFA 정책을 통해 수행됩니다. 다음 링크를 확인하여 MFA 적용 관련 질문에 대해 자세히 알아볼 수 있습니다.

- MFA 적용 예외
- MFA 적용 요구 사항 – 무엇 및 이유
- MFA 적용 범위
- MFA 적용 타임라인
- MFA 메트릭
- MFA 유형
- MFA 재설정

MFA 적용 요구 사항 **–** 무엇 및 이유

MFA 적용 및 MFA 적용이 중요한 이유와 관련된 FAQ입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

1. MFA란 무엇입니까?

   다단계 인증(MFA)은 계정 또는 시스템에 액세스하기 전에 두 가지 이상의 검증 양식을 제공해야 하는 보안 프로세스입니다. 자세한 내용은 Multi-factor Authentication 살펴보기 문서를 참조하십시오.

2. MFA 시행이 의무화된 이유는 무엇인가요?

   MFA는 귀하의 계정 및 데이터 보안을 보호하기 위해 의무화되어 있습니다. 사이버 위협은 끊임없이 변화하고 있으며 암호만으로는 더 이상 무단 액세스에 대한 충분한 보호를 제공할 수 없습니다.

   - MFA를 활성화하면 공격자가 암호를 알고 있더라도 공격자는 여전히 두 번째 형태의 확인이 필요합니다. 이 추가 계층은 대부분의 무단 시도를 크게 차단하여 정보를 보다 안전하게 유지합니다.
   - MFA를 기본값으로 설정하면 보안 침해 위험을 최소화하고 계정을 자동으로 보호할 수 있습니다. 즉, 추가 보안 결정을 내릴 필요 없이 마음의 평화를 얻을 수 있습니다.

3. MFA를 활성화하는 것이 중요한 이유는 무엇인가요?

   MFA를 활성화하면 계정 보안이 강화됩니다. 비밀번호는 데이터 침해에 노출될 수 있으므로 비밀번호만으로는 충분하지 않습니다. MFA를 사용하면 누군가가 귀하의 암호를 알고 있더라도 두 번째 확인 단계가 없으면 귀하의 계정에 액세스할 수 없습니다.

4. MFA가 ServiceNow 필요한 이유는 무엇입니까?

   ServiceNow 는 이러한 위협으로부터 사용자를 보호하기 위해 MFA를 의무화하고 있습니다. 무단 액세스를 줄이는 간단하면서도 효과적인 방법입니다. MFA를 요구함으로써 모든 계정에 강력한 보호 계층이 있어 귀하와 모든 사용자의 보안 위험을 줄일 수 있습니다.

5. 기존 고객에 대한 MFA 요구 사항은 무엇인가요?

   인스턴스를 Yokohama 이상 릴리스로 업그레이드하는 기존 고객의 경우:

   - 인스턴스에 적응형 인증MFA(다단계 인증) 컨텍스트 이 아직 켜져 있지 않으면 자동으로 기본 MFA 정책으로 활성화됩니다.
   - 로컬 또는 LDAP 인증을 사용하여 로그인하는 모든 내부 사용자(snc_external 역할이 없는 사용자)는 첫 번째 로그인 성공 후 30일 이내에 MFA를 설정해야 합니다. 이 시간 동안에는 정상적으로 로그인할 수 있지만 로그인 시 MFA에 등록하라는 메시지가 표시됩니다.
   - 30일 후에는 기본적으로 MFA가 필요하며 사용자는 MFA 설정을 완료하지 않으면 로그인할 수 없습니다.

6. 신규 고객에 대한 MFA 요구 사항은 무엇인가요?

   Yokohama 릴리스 이상을 사용하는 모든 인스턴스의 경우 모든 내부 사용자에 대해 MFA가 기본적으로 활성화됩니다. `## snc_external` 역할이 없고 로컬 또는 LDAP 인증을 사용하여 로그인하는 사용자에게도 적용됩니다. 사용자는 처음 로그인할 때부터 MFA를 설정하고 사용해야 합니다.

MFA 적용 범위

MFA 적용 범위 및 중요한 이유와 관련된 FAQ입니다.

1. MFA가 필요한 사용자, 로그인 및 환경 유형은 무엇입니까?

   Yokohama 릴리스부터 새로운 기본 보안 MFA 정책 MFA가 다음 시나리오에 적용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- **snc_external** 역할이 있는 사용자를 제외한 모든 사용자
- 로컬 또는 LDAP(Lightweight Directory Access Protocol) 인증을 기반으로 사용자 이름 및 암호를 수행하는 모든 사용자.
- 프로덕션, 하위 프로덕션 및 테스트 인스턴스를 포함하여 업그레이드 전에 아직 활성 MFA 정책이 없는 모든 고객 인스턴스입니다.

인스턴스 관리자는 MFA 컨텍스트 정책, 정책 기준 또는 정책 조건을 변경하여 적용 범위를 수정할 수 있습니다.

2. 1회 사용자 인증(SSO) 로그인에 MFA가 필요합니까?

아니요. 기본 보안 MFA 정책을 사용하면 SSO(SAML, OIDC, 인증서 기반 인증) 로그인에 MFA가 필요하지 않습니다.

고객은 SSO(Single Sign-On) 공급자(ID 공급자 또는 IdP)와 협업하여 IdP 측에서 MFA(Multi-factor Authentication)를 적용할 수 있습니다. IdP 측에서 MFA를 적용할 수 없는 경우 고객은 다음에 SSO(Single Sign-On)를 사용하여 다단계 인증 구성제공된 지침에 따라 SSO 로그인에 대해 플랫폼의 MFA를 활성화할 ServiceNow 수도 있습니다.

3. 외부 사용자에 대해 MFA가 필요합니까?

아니요. 기본 보안 MFA 정책을 사용하면 snc_external 역할을 가진 사용자에게 MFA가 필요하지 않습니다.

- 관리자는 MFA 정책 조건을 업데이트하여 이 동작을 수정하고 외부 사용자에 대해 MFA를 적용할 수 있습니다.
- Yokohama 또는 이후 릴리스로 업그레이드하기 전에 이미 MFA를 진행 중인 외부 사용자는 계속 MFA를 사용할 수 있습니다.
- 외부 사용자는 자신의 프로파일을 방문하여 MFA에 직접 등록할 수 있습니다.

4. 모바일 앱 로그인에 MFA가 필요합니까?

예. MFA 정책은 SSO가 아닌 로그인을 기반으로 사용자 이름과 암호를 사용하여 웹 및 모바일 앱 모두에 적용됩니다.

5. 비프로덕션 및 테스트 환경에 MFA가 필요합니까?

예. Yokohama 이상 버전으로 업그레이드하기 전에 인스턴스에 활성 MFA 정책이 없는 경우 프로덕션, 비프로덕션, 개발 및 테스트 환경을 포함한 모든 고객 인스턴스에 MFA가 적용됩니다.

6. 개발자 인스턴스에 MFA가 필요합니까?

예. MFA는 Yokohama 이상의 릴리스 버전에 있는 모든 개발자 인스턴스에 적용됩니다.

7. API 인증에 MFA가 필요합니까?

아니요. Yokohama 이상 릴리스에서는 사용자 이름 및 암호 기반 대화형 사용자 로그인에만 MFA가 필요합니다. 즉, MFA 없이 작동하는 기본 인증을 사용하는 API 인증을 의미합니다. 고객은 OAuth 또는 mTLS와 같은 대체 보안 API 인증 방법을 사용하는 것이 좋습니다. 자세한 내용은 여기를 참조하세요.

a. 클론

b. 업데이트 세트 검색

c. RPA

8. MFA로 인해 클론 설정 프로세스에 영향이 있습니까?

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

아니요, 클론 설정 프로세스는 사용자 이름 및 암호로 계속 작동하며 MFA가 필요하지 않습니다.

9. MFA로 인해 업데이트 세트 검색에 미치는 영향이 있습니까?

   아니요, 업데이트 세트 검색은 사용자 이름 및 암호로 계속 작동하며 MFA가 필요하지 않습니다.

10. 인스턴스에 액세스하는 ServiceNow RPA 봇에 영향이 있습니까?

    예. RPA 봇이 대화형 사용자 이름 및 암호 로그인을 사용하여 인스턴스에 액세스하는 ServiceNow 경우 MFA를 수행해야 합니다. 관리자는 RPA 봇 계정에 대한 MFA를 완화하려는 경우 **RPA** 봇 계정을 **MFA** 면제 사용자 그룹에 추가할 수 있습니다.

11. OAuth 기반 통합에 MFA가 필요합니까?

    OAuth ROPC(리소스 소유자 암호 자격 증명)는 MFA 없이 사용자 이름 및 암호로 작동합니다. 인증 코드 권한 부여 유형의 경우 OAuth 동의를 제공하기 전에 사용자 로그인 플로우의 일부로 MFA가 필요합니다.

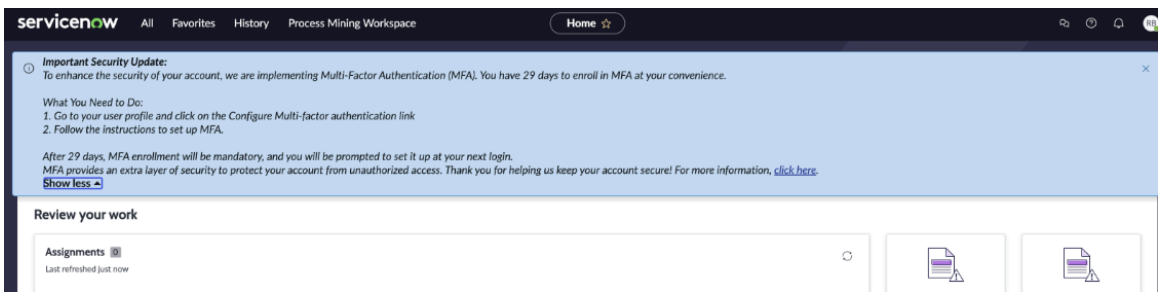
MFA 적용 타임라인

MFA 적용 타임라인 및 MFA 적용 타임라인이 중요한 이유와 관련된 FAQ입니다.

1. MFA는 언제 적용됩니까?

   MFA 정책에 따라 MFA 설정을 완료하지 않은 적격 사용자는 30일의 자체 등록 기간이 있습니다. 동작은 시스템 속성 `glide.authenticate.multifactor.self_enrolment_period`를 사용하여 제어됩니다. 속성의 기본값은 30일입니다. 최대 90일까지 업데이트할 수 있습니다.

   로컬 또는 LDAP 인증을 사용하여 로그인하는 모든 내부 사용자(`snc_external` 역할이 없는 사용자)는 첫 번째 로그인 성공 후 30일 이내에 MFA를 설정해야 합니다. 이 시간 동안에는 정상적으로 로그인할 수 있지만 로그인 시 MFA에 등록하라는 메시지가 표시됩니다.

   Yokohama 또는 이후 릴리스로 업그레이드한 후 90일 후에 내부 사용자(`snc_external` 역할이 없는 사용자)가 처음으로 로컬 또는 LDAP 인증을 사용하여 로그인하는 경우 즉시 MFA를 사용해야 합니다. 30일의 MFA 자체 등록 기간이 없습니다. 이 기간은 시스템 속성인 `glide.authenticate.multifactor.enforcement.max_relaxation_period`에 의해 관리됩니다. 이 속성의 최대값은 270일입니다.

2. MFA 적용 타임라인은 어떻게 조정할 수 있나요?

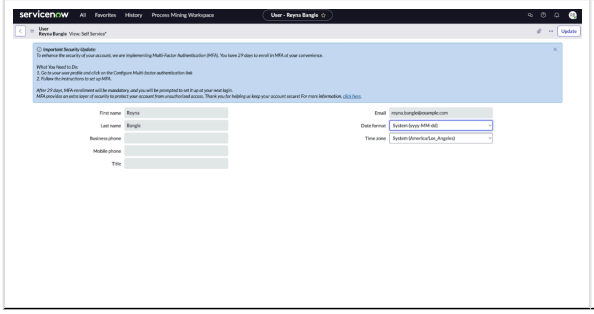
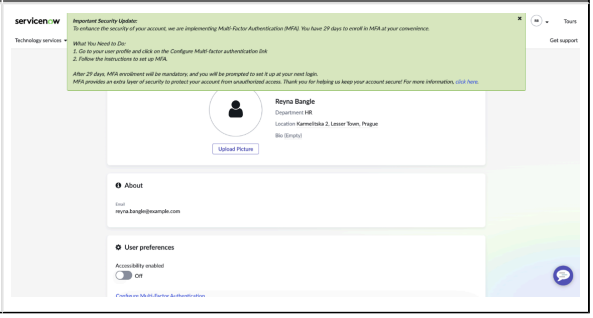
   - 관리자는 속성 `glide.authenticate.multifactor.self_enrolment_period` 값을 업데이트하여 더 작거나 더 긴 자체 등록 기간을 제공할 수 있습니다. 속성 값을 0으로 설정합니다. 사용자는 Yokohama 이상 릴리스로 업그레이드한 후 로컬 또는 LDAP 로그인으로 첫 번째 로그인을 시도한 후 MFA 설정을 완료해야 합니다. 자체 등록 기간의 최대 기간은 90일입니다. 90보다 높게 설정된 속성 값은 90으로 처리됩니다.
   - 관리자는 `glide.authenticate.multifactor.enforcement.max_relaxation_period` 속성 값을 업데이트하여 Yokohama 또는 이후 릴리스로 업그레이드한 후 MFA 자체 등록 기간을 얻는 일수를 결정할 수 있습니다.

3. 최종 사용자는 이 예정된 변경에 대해 어떻게 알 수 있습니까?

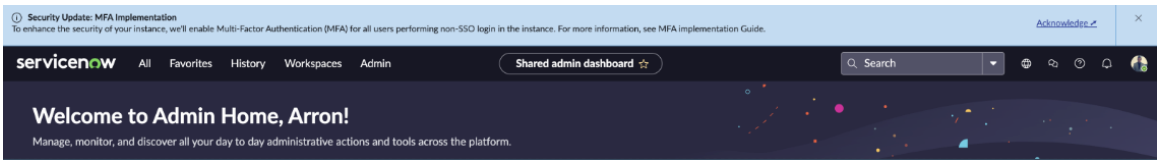
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MFA를 적용할 로컬 또는 LDAP 인증을 수행하는 최종 사용자는 로그인한 후 정보 메시지를 볼 수 있습니다. 사용자가 프로파일을 방문할 때 동일한 메시지를 사용할 수 있습니다.

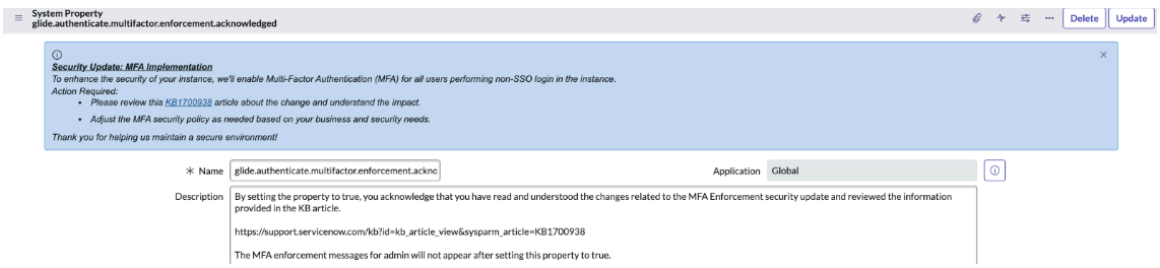
적용 메시지

사용자 프로파일	**Employee Service** Center에서
	

SSO 로그인을 수행하는 비관리자 사용자에게는 이 메시지가 표시되지 않습니다. 로그인에 사용된 인증 방법에 관계없이 로그인에 성공하면 관리자 역할에 다른 정보 메시지가 표시됩니다.



이 메시지는 관리자 중 한 명이 `glide.authenticate.multifactor.enforcement.acknowledged` 속성 값을 예로 설정하여 업데이트를 승인할 때까지 계속 표시됩니다.



4. 최종 사용자가 로그인할 때 MFA 설정 완료에 대해 표시되는 메시지를 끄는 방법은 무엇입니까?

관리자는 `glide.authenticate.multifactor.enforcement.show_user_info_message` 시스템 속성의 값을 false로 업데이트하여 로그인 후 최종 사용자에게 표시되는 MFA 등록 정보 메시지를 끌 수 있습니다.

5. MFA 적용에 대해 관리자에게 표시되는 메시지를 끄는 방법은 무엇입니까?

로그인 후 관리자에게 표시되는 MFA 적용에 대한 정보 메시지는 관리자 중 한 명이 `glide.authenticate.multifactor.enforcement.acknowledged` 시스템 속성의 값을 예로 업데이트하여 이를 승인하면 더 이상 표시되지 않습니다.

6. 인스턴스에 있는 조직의 보안 요구 사항에 따라 적응형 인증을 사용하여 정의된 MFA 정책이 이미 있습니다. 정책이 위임의 영향을 받습니까?

아니요, 인스턴스에 이미 활성 적응형 인증 MFA 컨텍스트 정책이 있는 경우 새로운 기본 보안 MFA 정책이 적용되지 않습니다. 인스턴스에 MFA 속성이 활성화되어 있지만 (`glide.authenticate.multifactor`) MFA 정책이 활성화되지 않은 경우 사용자 이름 및 암호 기반 로컬 또는 LDAP 로그인을 수행하는 모든 내부 사용자(역할이 없는 사용자) `snc_external` MFA를 적용하기 위한 기본 보안 MFA 정책이 활성화됩니다.

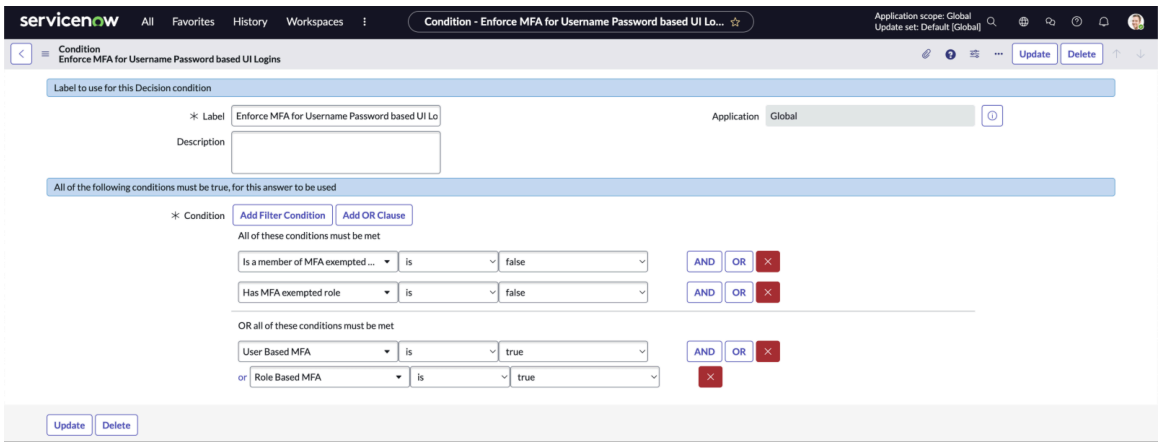
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MFA 적용 예외

MFA 적용 예외 및 MFA 적용 예외가 중요한 이유와 관련된 FAQ입니다.

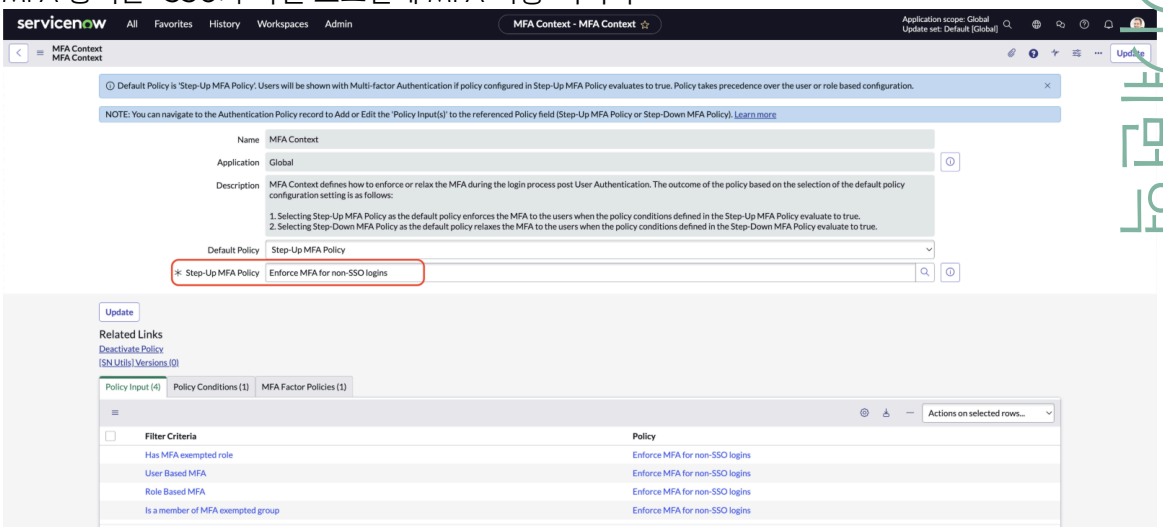
1. 특정 사용자에 대한 MFA 의무를 어떻게 완화할 수 있습니까?

Yokohama 릴리스에서는 새 사용자 그룹인 MFA 면제 사용자 그룹 기록이 추가됩니다. 기본 조건에 따라 MFA 정책이 추가되며, 이 그룹의 구성원인 모든 사용자에게 MFA가 적용됩니다.



특정 사용자에 대한 MFA를 완화하려면 다음 절차를 따르십시오.

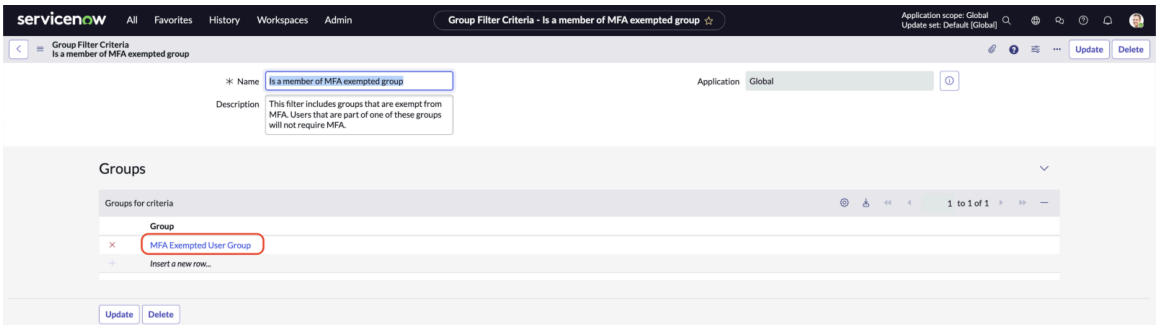
- **MFA** 컨텍스트로 이동합니다. MFA 컨텍스트 기록과 연결된 스텝업 MFA 정책은 "SSO가 아닌 로그인에 MFA 적용"이어야 합니다.



- 정책 입력 관련 목록에서 **MFA** 면제 그룹의 구성원 여부 필터 기준 기록을 선택합니다.

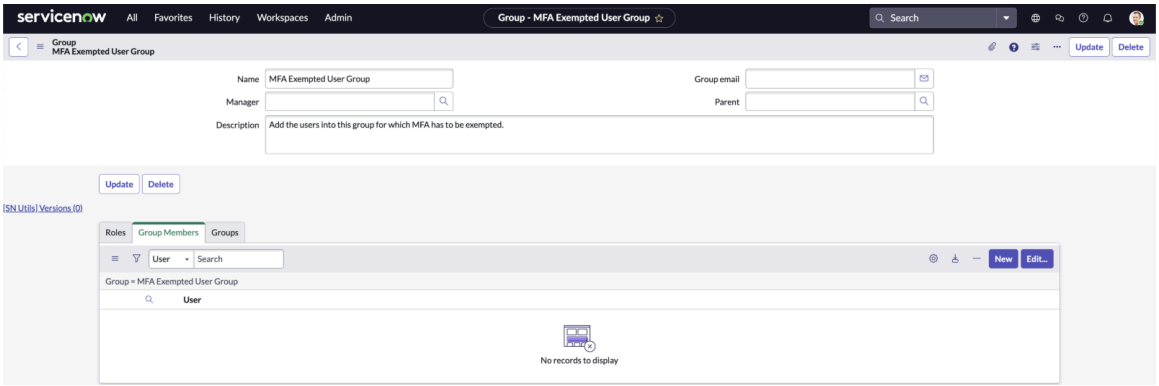
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ **MFA** 면제 사용자 그룹을



선택합니다.

◦ 이 그룹에 사용자를 구성원으로 추가하여 MFA 적용에서

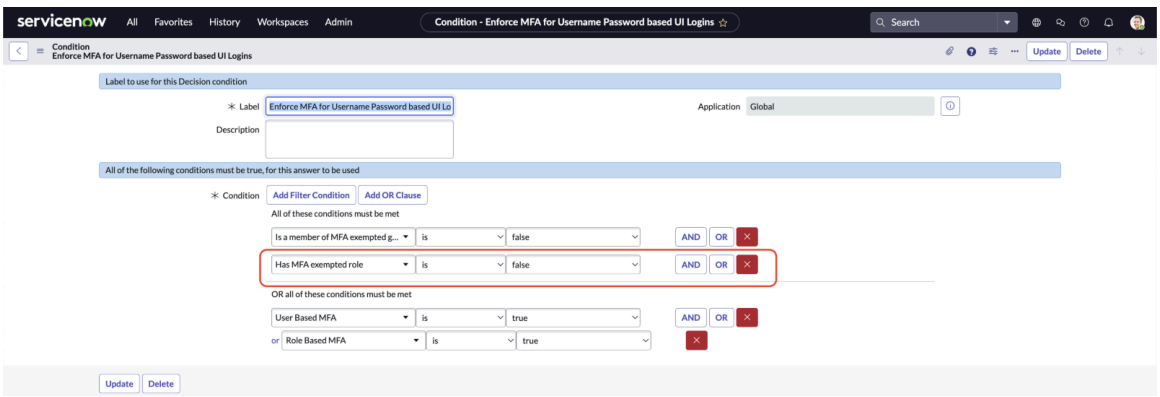


제외합니다.

주: MFA 컨텍스트와 연결된 다른 정책이 있는 경우 정책에 "MFA 면제 그룹의 구성원임" 필터 기준을 추가하고 정책 조건을 수정하여 이 그룹의 사용자를 MFA 적용에서 제외할 수 있습니다.

2. 특정 역할에 대한 MFA 의무를 어떻게 완화할 수 있습니까?

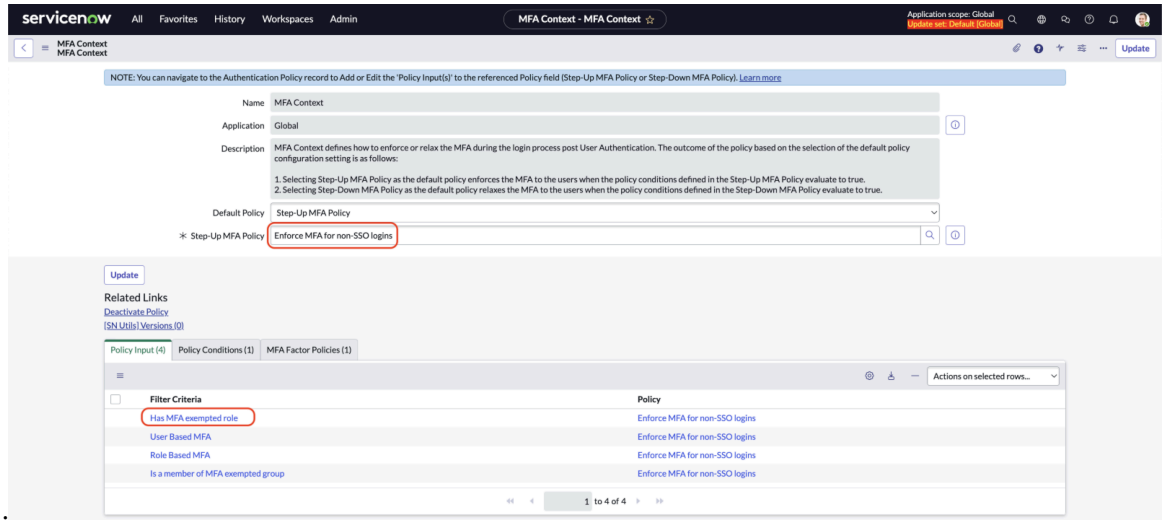
Yokohama 릴리스에서는 비어 있는 새 역할 **MFA** 면제 역할 있음 필터 기준이 추가됩니다. MFA 정책에는 예외 역할 기준의 역할 부분을 가진 사용자를 MFA 적용에서 제외하는 조건이 추가되었습니다.



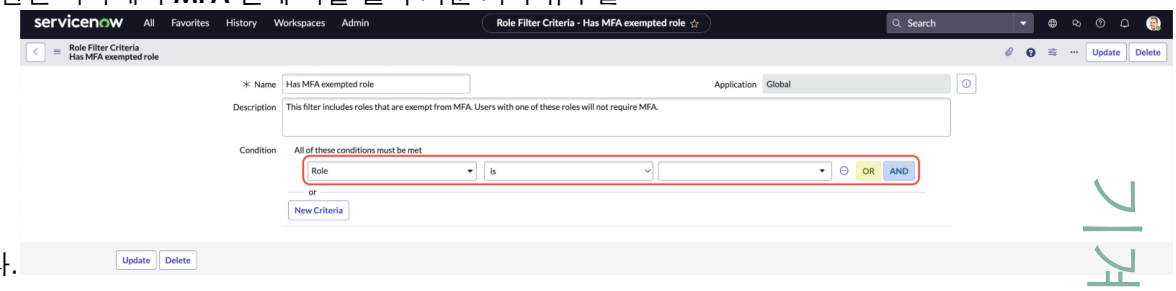
특정 역할에 대한 MFA를 완화하려면 다음 절차를 따르십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ **MFA** 컨텍스트로 이동합니다. MFA 컨텍스트 기록과 연결된 스텝업 MFA 정책은 SSO가 아닌 로그인에 **MFA** 적용이어야 합니다.



◦ 정책 입력 관련 목록에서 **MFA** 면제 역할 필터 기준 기록 유무를 선택합니다.

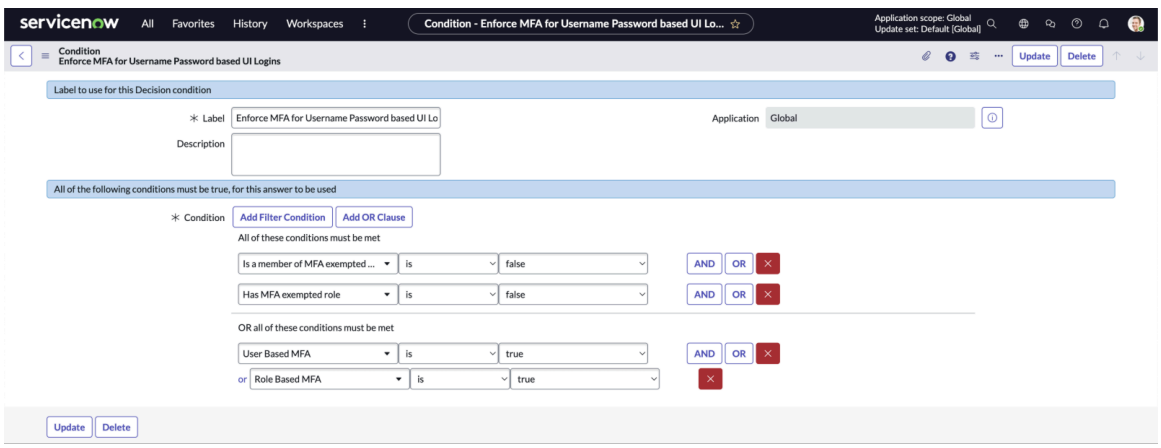


◦ 조건에 추가하려는 역할을 추가합니다. OR 연산자를 사용하여 여러 역할을 추가할 수 있습니다.

ⓘ 주: MFA 컨텍스트와 연결된 다른 정책이 있는 경우 **MFA** 면제 역할 있음 필터 기준을 정책에 추가할 수 있습니다. 면제된 역할이 있는 사용자를 MFA 적용에서 제외하도록 정책 조건을 수정합니다.

3. 특정 그룹에 대한 MFA 의무를 어떻게 완화할 수 있습니까?

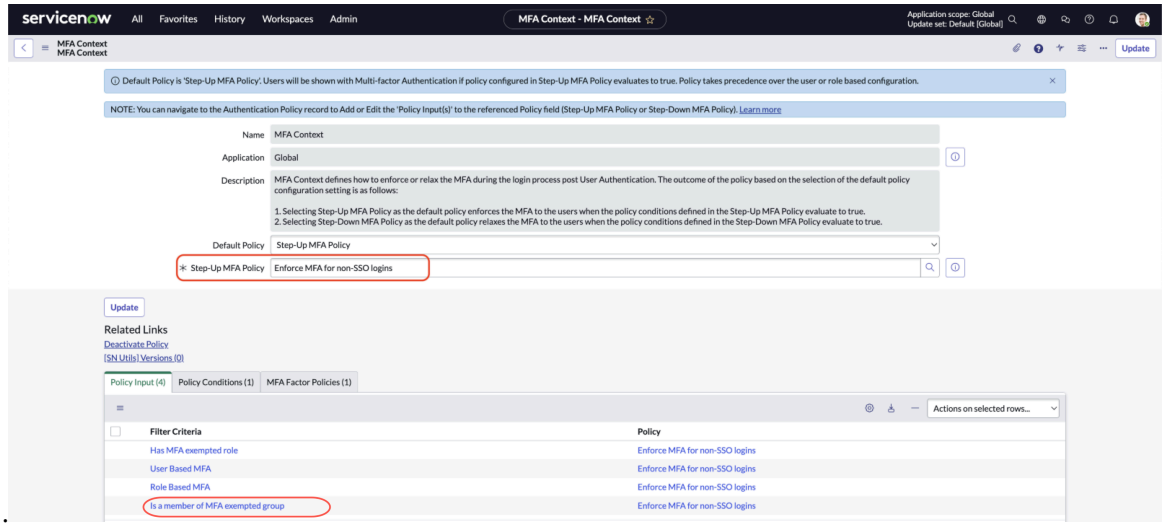
Yokohama 릴리스에서는 사용자 그룹 **MFA** 면제 사용자 그룹이 추가되었습니다. MFA 정책에 추가된 기본 조건에 따라 이 그룹의 구성원인 사용자 또는 그룹에는 MFA가 적용되지 않습니다.



특정 그룹에 대한 MFA를 완화하려면 다음 절차를 따르십시오.

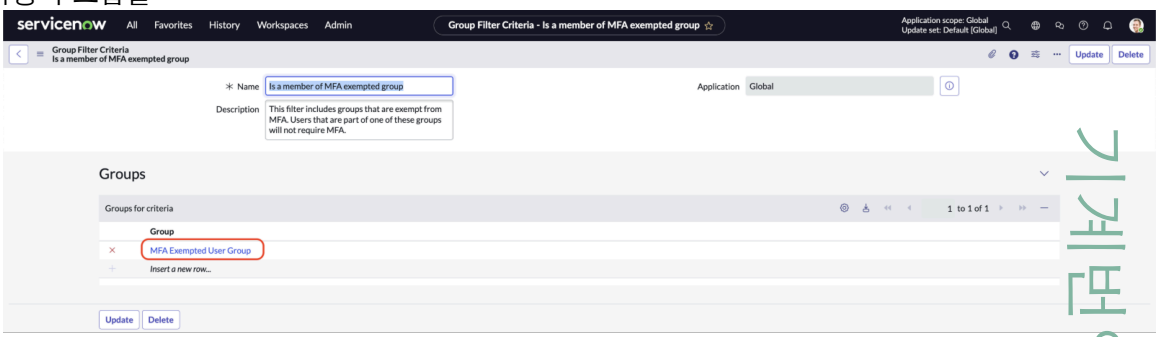
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ **MFA** 컨텍스트로 이동합니다. MFA 컨텍스트 기록과 연결된 스텝업 MFA 정책은 SSO가 아닌 로그인에 **MFA** 적용이어야 합니다.

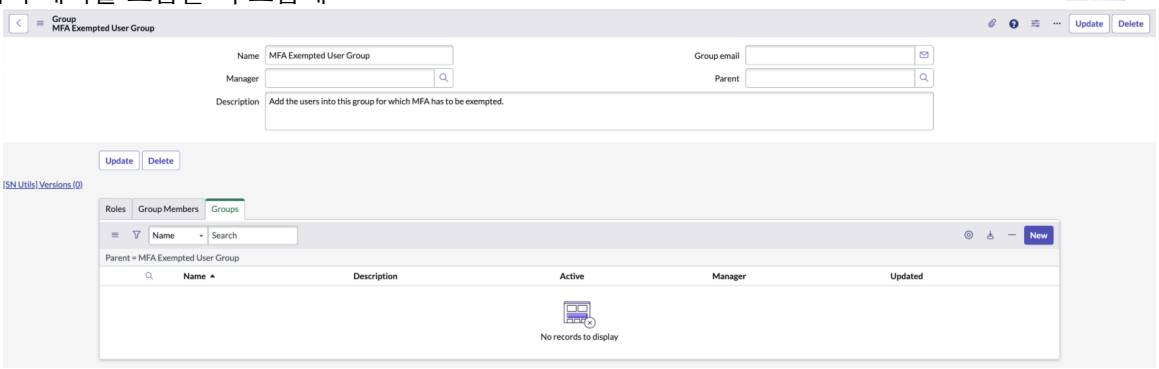


◦ 정책 입력 관련 목록에서 **MFA** 면제 그룹의 구성원 여부 필터 기준 기록을 선택합니다.

◦ **MFA** 면제 사용자 그룹을 선택합니다.



◦ MFA 적용에서 제외할 그룹을 이 그룹에 추가합니다.

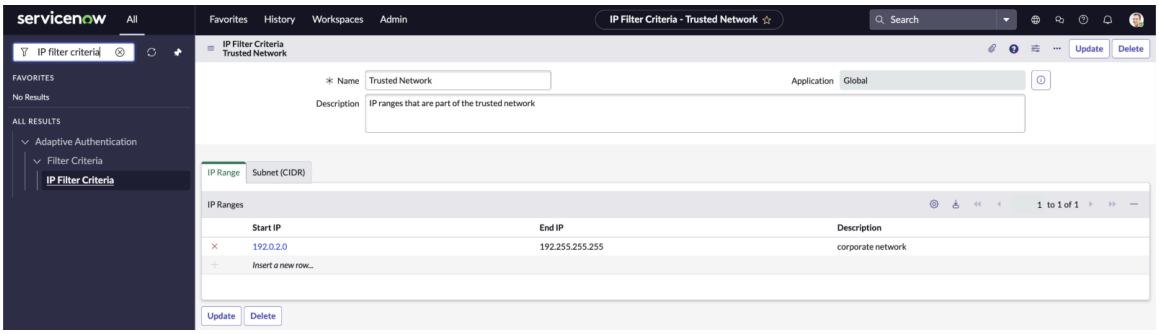


4. 신뢰할 수 있는 네트워크에 대한 MFA 의무를 어떻게 완화할 수 있습니까?

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

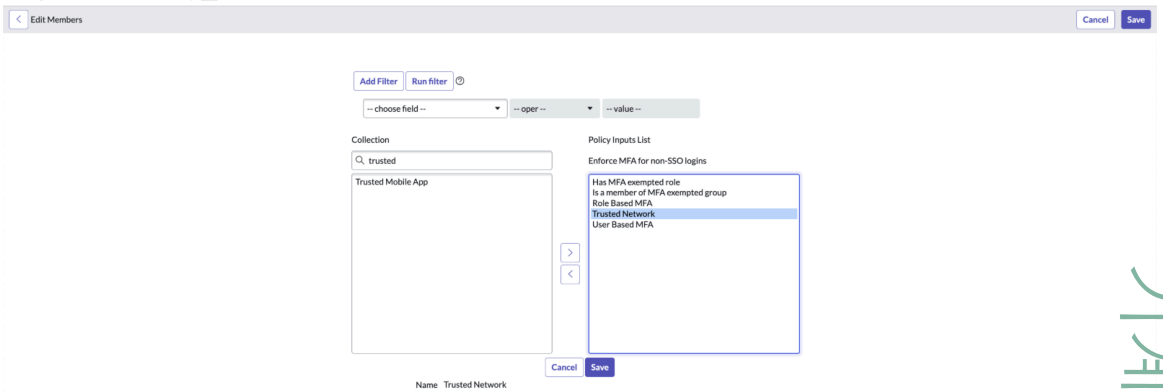
◦ 다음으로 이동 적응형 인증 > 필터 기준 > **IP** 필터 기준.

◦ 신뢰할 수 있는 네트워크를 지정하는 기준을 만듭니다. 신뢰할 수 있는 네트워크의 일부로 IP 범위 또는 서브넷 목록을 지정할 수 있습니다.



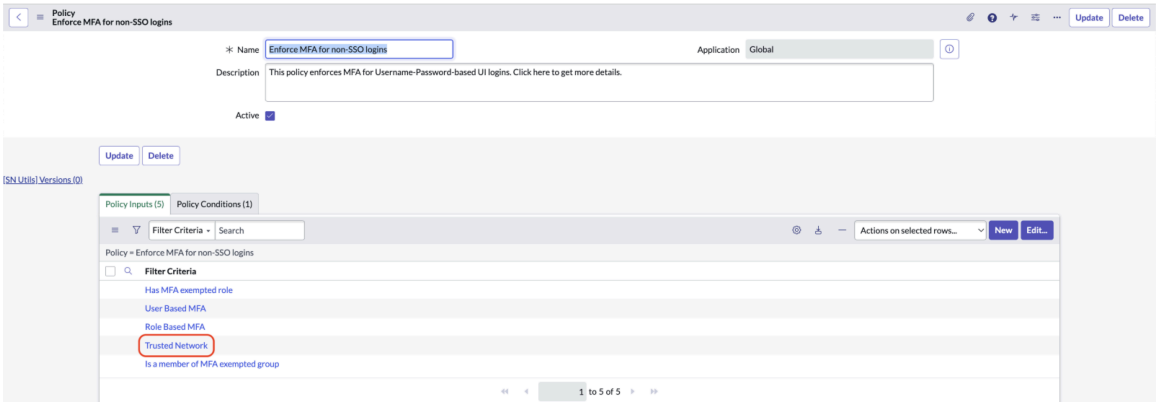
◦ 다음으로 이동 적응형 인증 > 인증 정책 컨텍스트 > **MFA** 컨텍스트.

◦ 컨텍스트와 연결된 정책을 엽니다.



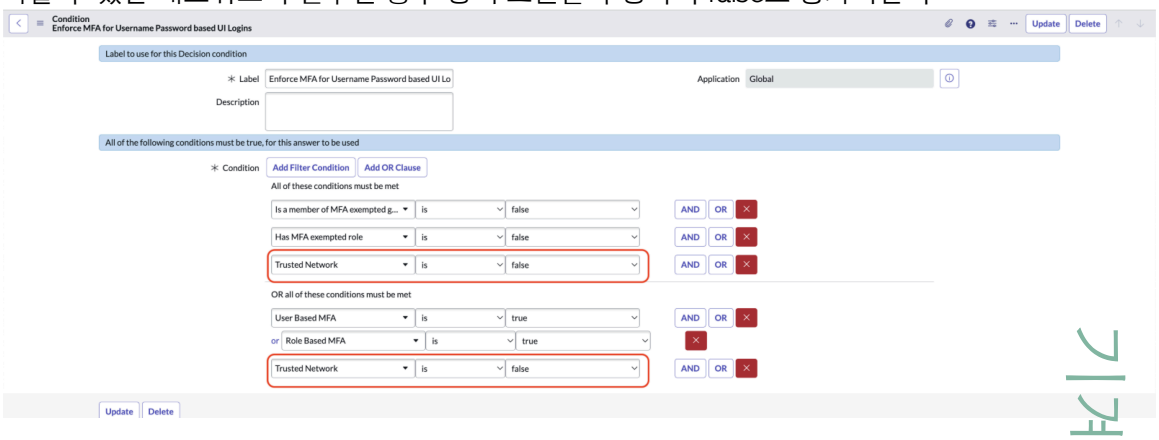
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ 편집을 선택하여 생성한 **IP** 필터 기준을정책 입력 관련 목록에



추가합니다.

◦ 사용자가 신뢰할 수 있는 네트워크의 일부인 경우 정책 조건을 수정하여 false로 평가되는지



확인합니다.

> 주: MFA 컨텍스트와 연결된 다른 정책이 있는 경우 1단계의 일부로 생성된 IP 필터 기준을 정책에 추가하고 정책 조건을 수정하여 신뢰할 수 있는 네트워크에서 MFA 적용을 면제할 수 있습니다.

5. 신뢰할 수 있는 위치에 대해 MFA 의무를 완화하려면 어떻게 해야 합니까?

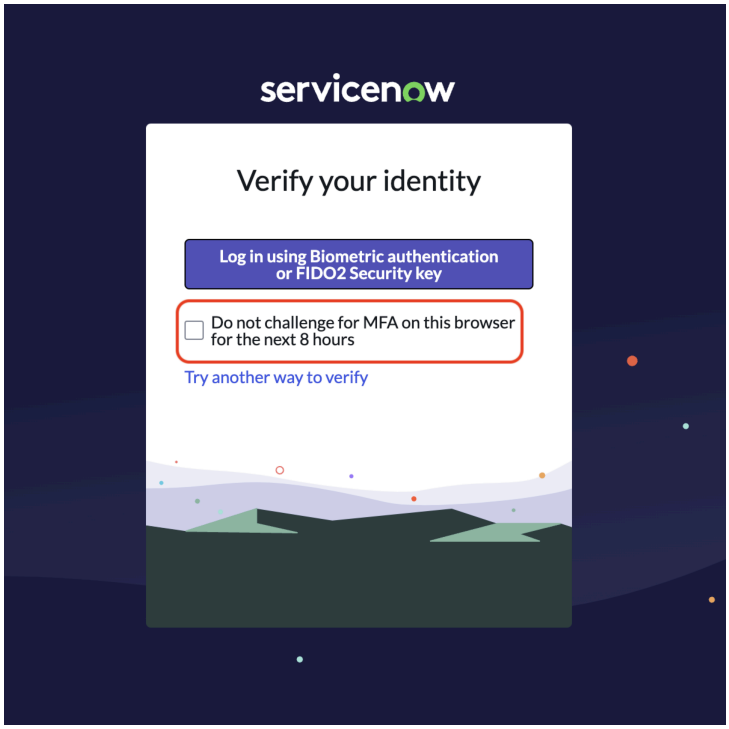
Zero Trust – 위치 기반 액세스(추가 구독 필요) 플러그인에서 사용할 수 있는 위치 필터 기준을 사용할 수 있습니다.

6. 빈번한 MFA 적용을 제어하는 방법은 무엇입니까?

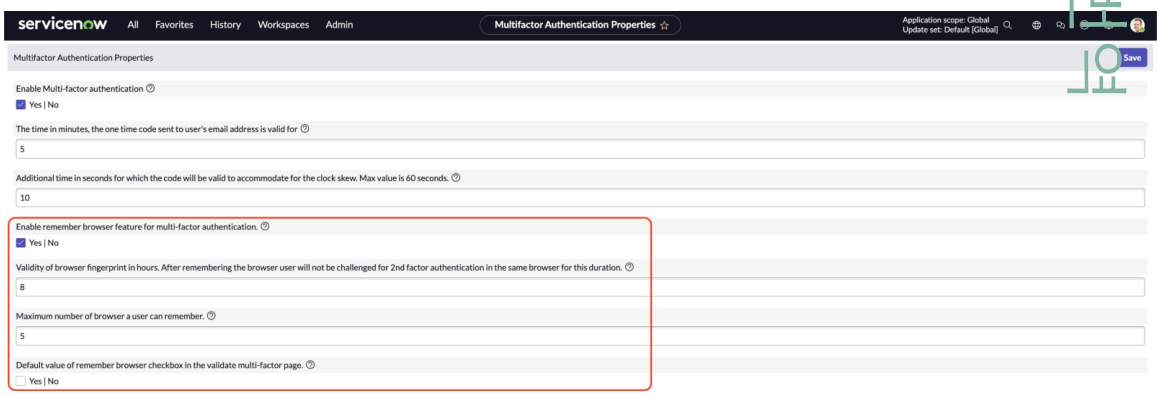
Zero Trust – 위치 기반 액세스(추가 구독 필요) 플러그인에서 사용할 수 있는 위치 필터 기준을 사용합니다.

MFA 유효성 검사 페이지에는 브라우저를 기억하는 확인란이 있습니다. MFA는 기억된 브라우저에 적용되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



- 이 시스템 속성에 의해 지정된 기간입니다. `glide.authenticate.multifactor.browser.fingerprint.validity`. 속성의 기본값은 8시간입니다. 이 지속 시간은 최대 24시간까지 늘릴 수 있습니다. 마찬가지로 `glide.authenticate.multifactor.remember.browser.default` 시스템 속성을 사용하여 확인란의 기본값을 true로 설정할 수 있습니다.
- 다음으로 이동 다단계 인증 > 속성 그리고 이러한 네 가지 속성을 조정하여 기억된 브라우저 기능을



제어합니다.

7. 사용자가 공유하는 계정에 대해 MFA는 어떻게 작동하나요?

여러 사용자가 공유하는 단일 계정은 보안 위험이 있습니다. 여러 사용자와 계정을 공유하는 것은 권장되지 않습니다.

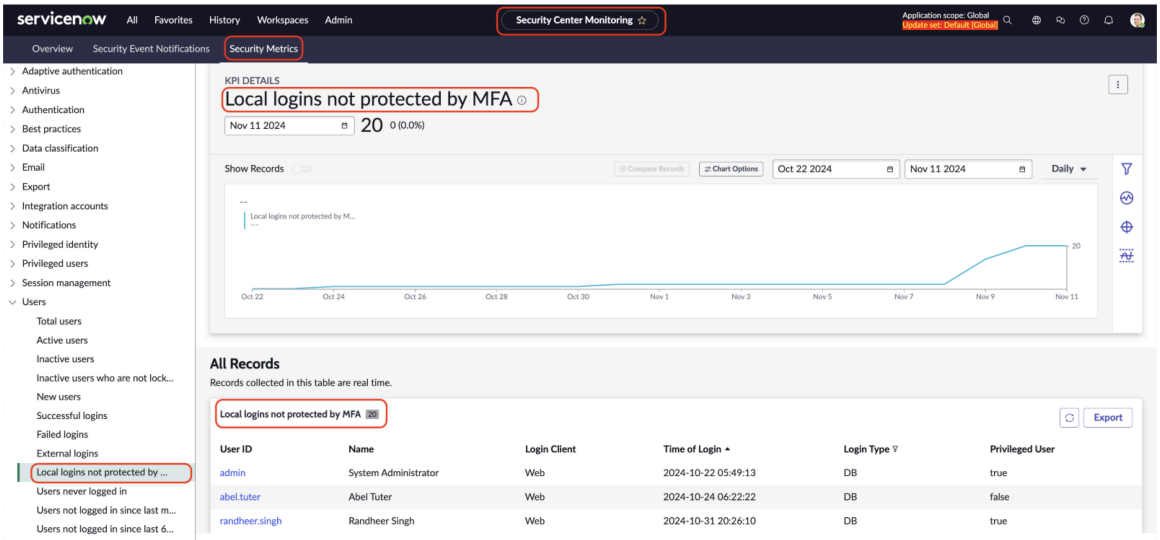
MFA 메트릭

MFA 메트릭 이해와 관련된 FAQ입니다.

1. MFA가 진행되지 않는 로컬 로그인 수를 어떻게 확인할 수 있습니까?

다음으로 이동할 수 있습니다. 보안 센터 > 보안 콘솔 > 보안 메트릭. 사용자에 대한 메트릭에서 MFA의 보호를 받지 않는 로컬 로그인을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. MFA 설정을 완료해야 하고 로컬 로그인을 수행하는 사용자 수를 확인하려면 어떻게 해야 합니까?

다음으로 이동할 수 있습니다. 보안 센터 > 보안 콘솔 > 보안 메트릭. 사용자에 대한 메트릭에서 MFA의 보호를 받지 않는 로컬 로그인을 클릭합니다.

MFA 유형

MFA 유형 및 MFA 유형이 중요한 이유와 관련된 FAQ입니다.

1. MFA에서 ServiceNow사용할 수 있는 검증 방법의 유형은 무엇입니까?

ServiceNow 기본 시스템은 이러한 검증 방법을 지원합니다.

a. 암호

b. Google Authenticator, Okta verify, Microsoft Authenticator, Authy, DUO와 같은 TOTP 인증기 앱

c. Windows Hello, Apple Touch ID, Face ID, Android 지문 센서와 같은 FIDO2(생체 인식 인증기).

d. YubiKey, Thetis와 같은 하드웨어 보안 키(FIDO2)

e. 이메일 일회용 암호(OTP)

f. SMS OTP - SMS OTP 기반 MFA를 사용하려면 SMS를 사용한 다단계 인증 com.snc.authentication.sms_mfaplugin 설치 및 요소 구성이 필요합니다.

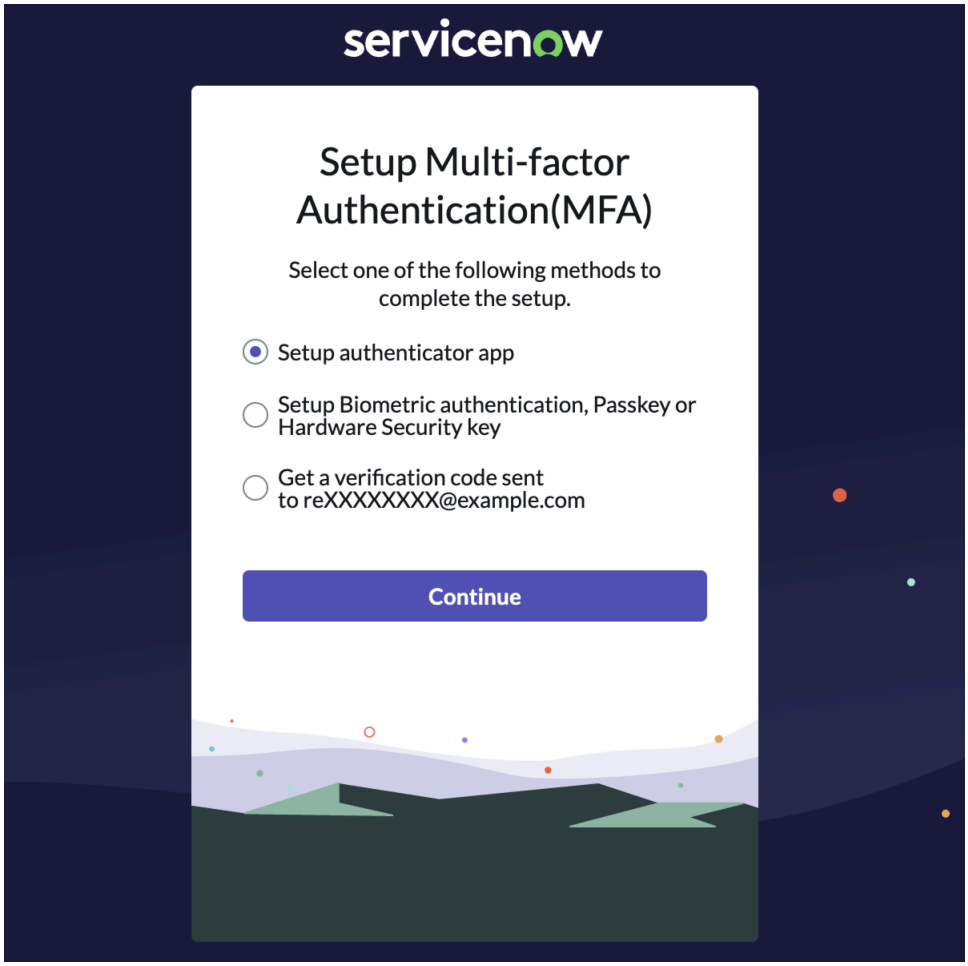
2. 사용자가 여러 MFA 요소 또는 검증 방법을 구성할 수 있습니까?

예. 사용자 프로필을 방문하여 여러 MFA 요소를 등록할 수 있습니다. 예를 들어 생체 인식 인증기가 있는 노트북을 등록하고, 통과 키로 휴대폰을 사용하고, 인증기 앱을 설정할 수 있습니다.

3. MFA 설정을 완료하려면 사용자가 수행해야 하는 단계는 무엇입니까?

사용자는 다음 MFA 옵션 중 하나를 수행할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다단계 인증(MFA) MFA 설정에 대한 자세한 내용은 설명서를 참조하십시오.

4. SMS 및 이메일 OTP 기반 MFA를 특정 사용자로 제한할 수 있습니까?

관리자는 이메일 및 SMS OTP 기반 MFA 요소에 대한 MFA 요소 정책을 설정하여 이러한 요소를 특정 사용자 그룹 또는 역할로 제한할 수 있습니다.

5. 사용자에게 인증자 앱을 설정할 수 있는 휴대폰이 없습니다. 이러한 사용자는 MFA를 어떻게 활성화할 수 있습니까?

Xanadu 릴리스 이후부터는 휴대폰에서 인증기 앱을 설정할 필요 없이 생체 인식 인증기, 패스키, FIDO2 하드웨어 보안 키 및 이메일 OTP 기반 MFA를 사용할 수 있습니다.

6. 최종 사용자로서 MFA를 설정하는 방법은 무엇입니까?

다단계 인증(MFA) 사용 MFA 설정에 대한 자세한 내용은 설명서를 참조하십시오.

MFA 재설정

MFA 재설정 및 MFA 재설정이 중요한 이유와 관련된 FAQ입니다.

1. 인증자 앱 설정이 손실되었습니다. 재설정하려면 어떻게 해야 합니까?

사용자가 MFA로 인해 잠기지 않도록 여러 요인에 등록하는 것이 좋습니다. 예를 들어 TOTP 인증자 앱, 암호 키 및 이메일 OTP 기반 MFA를 사용할 수 있습니다.

사용자가 등록된 MFA 요소를 사용할 수 없는 경우 관리자는 다음 단계에 따라 MFA를 재설정할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 인증자 앱 설정 지우기:
   - 다음으로 이동 모두 > 다단계 인증 > 사용자 다단계 설정.
   - 테이블에서 사용자를 검색합니다.
   - 사용자와 연결된 기록 삭제

b. FIDO2 인증기 및 패스키 지우기:
   - 다음으로 이동 모두 > 다단계 인증 > 웹 인증 > 사용자 공개 자격 증명.
   - 테이블에서 사용자를 검색합니다
   - 사용자와 연결된 기록 삭제

c. 사용자와 관련된 다른 다단계 설정 지우기
   - 다음으로 이동 모두 > 다단계 인증 > 사용자 다단계 설정.
   - 테이블에서 사용자를 검색합니다
   - 사용자와 연결된 기록 삭제

관리자를 포함하여 아무도 인스턴스에 액세스할 수 없는 경우. 관리자는 Now Support 에서 사용할 수 있는 카탈로그 항목을 사용하여 셀프 서비스 MFA 재설정을 수행할 수 있습니다.

2. MFA로 인한 관리자 잠금을 방지하는 방법은 무엇입니까?

관리자는 인스턴스에 액세스하는 것이 차단되지 않도록 여러 MFA 요소에 등록합니다.

관리자를 포함하여 아무도 인스턴스에 액세스할 수 없는 경우. 관리자는 Now Support 에서 사용할 수 있는 카탈로그 항목을 사용하여 셀프 서비스 MFA 재설정을 수행할 수 있습니다.

Multi-factor Authentication 살펴보기

다단계 인증(MFA)은 사용자가 기본 자격 증명 이외의 정보를 제공하도록 요구하는 인증 방법입니다.

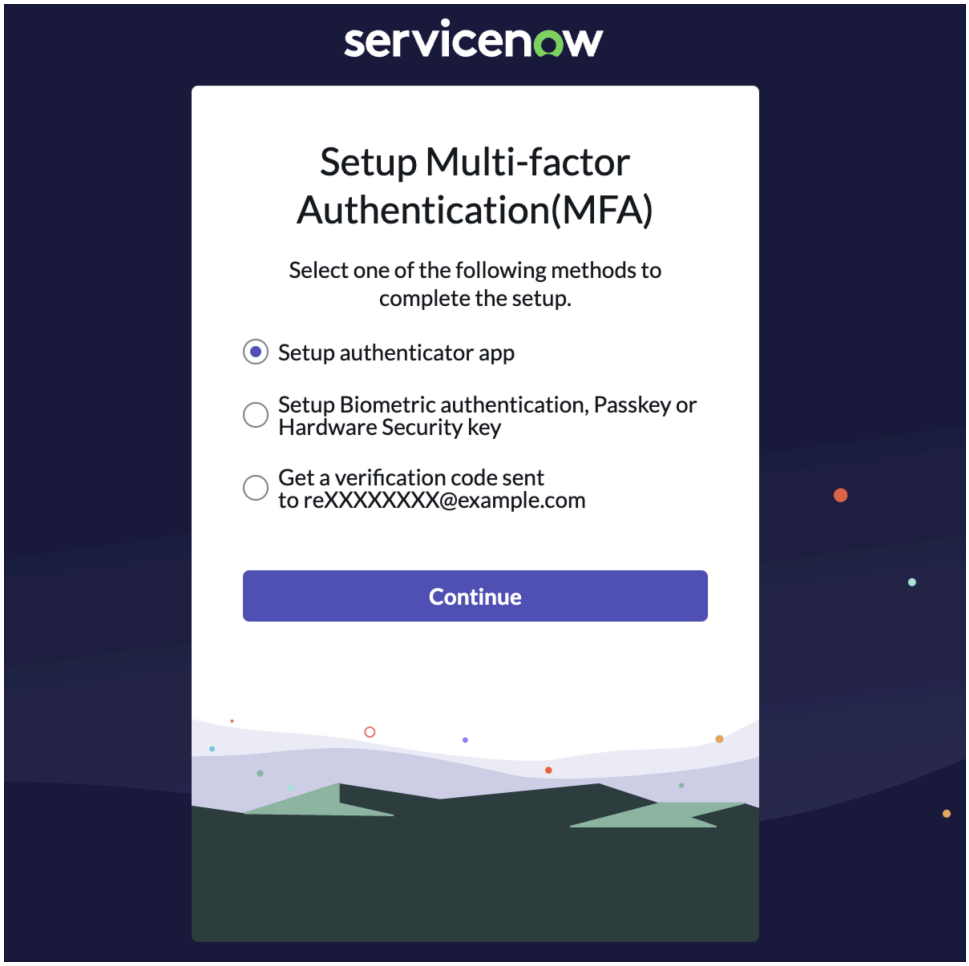
MFA는 사용자가 서비스 또는 계정에 액세스하기 위해 두 가지 이상의 서로 다른 확인 요소를 제공하도록 요구하는 보안 프로세스입니다. 비밀번호뿐만 아니라 서비스에 추가 보안 보호 계층을 추가하여 권한이 없는 개인이 액세스하는 것을 더 어렵게 만듭니다.

MFA는 여러 요소를 요구함으로써 보안을 크게 강화하고 피싱 및 신원 도용을 비롯한 다양한 사이버 위협으로부터 보호하는 데 도움이 됩니다. 다음은 MFA의 작동 방식에 대한 몇 가지 인사이트입니다.

- 첫 번째 요소: 사용자가 로그인에 사용자 이름과 암호를 사용합니다.
- 두 번째 단계: 사용자에게 사용자와 관련된 두 번째 요소(인증자 앱 또는 보안 키와 같은 ID 확인 방법)를 묻는 메시지가 표시됩니다.

주:
- MFA는 기본적으로 에서 ServiceNow활성화됩니다.
- MFA는 속성을 사용하여 *glide.authenticate.multifactor* 활성화됩니다. 이 속성을 사용하지 않으려면 MFA를 사용하지 않도록 설정하려는 이유에 대한 비즈니스 정당성을 제공해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



ServiceNow의 MFA는 Authenticator App, FIDO2(Fast Identity Online 2), Passkey 및 OTP(Time-based One-Time Password)와 같은 확인 방법을 지원합니다. 사용 가능한 검증 방법의 세부 정보는 다음과 같습니다.

- 인증자 앱: 고유한 임시 검증 코드를 생성하는 앱입니다. 예: Otka, Google Authenticator, Microsoft Authenticator 등
- **FIDO2**: 공개 키 암호화를 사용하여 사용자 ID의 유효성을 검사하는 물리적 디바이스입니다. 예: 하드웨어 키(YubiKey), 생체 인식 스캐너(Apple의 Touch ID).
- 통과 키: 생체 인식 센서, PIN 또는 패턴으로 장치를 잠금 해제하여 통과 키로 로그인합니다.
- **OTP:** 짧은 기간 동안만 유효한 고유한 암호를 생성하기 위한 비밀 키 및 현재 시간입니다. 예: SMS(OTP) 및 이메일(OTP).

MFA는 다음과 함께 사용할 수 있습니다.

- 로컬 데이터베이스 인증(기본 ServiceNow 인증) 또는 LDAP 통합
- SSO SAML 또는 SSO OIDC. 자세한 내용은 다중 제공자 1회 사용자 인증(SSO) 문서를 참조하십시오.

관련 정보

MFA 검증 방법

다단계 인증 시스템 속성

다단계 인증 구성

를 사용할 ServiceNow때 사용자 보안 태세를 개선하도록 MFA(다단계 인증)를 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

첫째, MFA를 구현하려면 비즈니스 및 사용자 요구에 따라 MFA 검증 방법을 결정합니다.

의 MFA를 사용하여 ServiceNow요구 사항을 식별한 후 사용자에게 적합한 방법 또는 그 조합을 선택할 수 있습니다. 또한 다양한 다단계 인증 속성을 사용하여 MFA를 활성화, 비활성화 및 구성하여 인증 기준에 따라 사용자의 MFA 환경을 더욱 향상시킬 수도 있습니다.

다음은 MFA 구성과 관련된 몇 가지 중요한 주제입니다.

- MFA 검증 방법
- 다단계 인증 시스템 속성
- 다단계 인증 기준

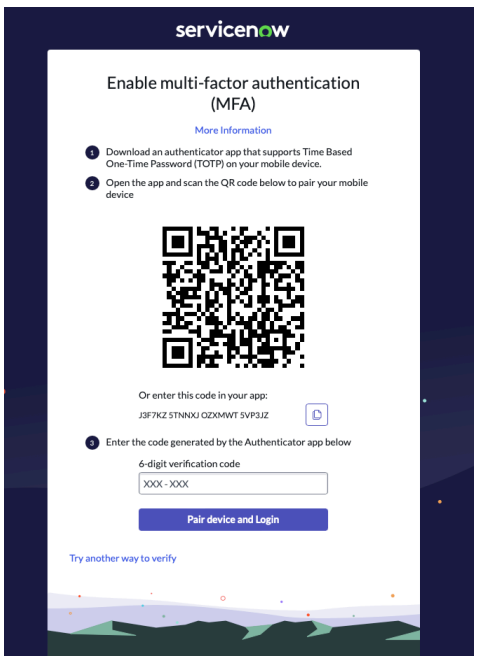
MFA 검증 방법

ServiceNow의 MFA는 인증자 앱, FIDO2(Fast Identity Online 2) 및 TOTP(시간 기반 일회성 암호)와 같은 확인 방법을 지원합니다.

사용자는 사용자 이름 및 암호 외에 다음 옵션을 사용하여 다단계 인증 요구 사항을 충족할 수 있습니다. 사용자는 인증자 애플리케이션, 생체 인식 스캐너, 하드웨어 키 및 SMS와 같은 MFA 요소를 독립적으로 설정할 수 있습니다.

인증 애플리케이션

인증자 애플리케이션은 임시 암호를 생성하는 타사 소프트웨어입니다. 사용자는 암호와 함께 이러한 암호를 사용하여 다단계 인증(MFA)이 필요한 인스턴스에 로그인할 수 있습니다. 이러한 애플리케이션에 대한 자세한 내용은 을 참조하십시오 인증 애플리케이션.



하드웨어 키 및 생체 인식 스캐너(웹 인증)

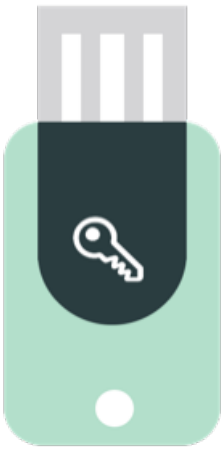
Integration - Web Authentication (com.snc.integration.webauthn) 플러그인을 사용하면 인스턴스에서 하드웨어 키 또는 생체 인식 판독기 인증을 사용할 수 있습니다.

생체 인식 인증기는 지문 또는 얼굴 인식을 사용하여 사용자를 식별합니다. 사용자는 장치에서 이러한 인증기를 다단계 로그인 프로세스의 일부로 사용할 수 있습니다. 생체 인식 인증기 등록에 대한 자세한 내용은 을 참조하십시오 생체 인식 인증기 등록.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



하드웨어 키는 인증에 사용할 수 있는 물리적 하드웨어입니다. 하드웨어 키는 인증을 제공하기 위해 장치의 포트에 삽입됩니다. 하드웨어 키 등록에 대한 자세한 내용은 문서를 참조하십시오 하드웨어 보안 키 등록.



암호

암호 키 인증은 사용자가 생체 인식 센서, PIN 또는 패턴으로 장치의 잠금을 해제하여 암호를 사용하는 안전한 로그인 방법입니다.

SMS

관리자는 SMS 기반 OTP를 사용하여 인스턴스에 로그인을 시도하는 사용자에게 요구하도록 인스턴스를 구성할 ServiceNow 수 있습니다.

사용자가 로그인을 ServiceNow시도하면 sys_user 기록과 연결된 휴대폰 번호로 SMS OTP가 전송됩니다. 사용자는 모바일 장치로 전송된 6자리 검증 코드를 입력하고 ID를 확인할 수 있습니다. 자세한 내용은 SMS를 사용한 다단계 인증 문서를 참조하십시오.



이메일

관리자는 이메일 기반 OTP를 사용하여 인스턴스에 로그인을 시도하는 사용자에게 요구하도록 인스턴스를 구성할 ServiceNow 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자가 로그인을 ServiceNow시도하면 사용자의 이메일 주소로 이메일 OTP가 전송됩니다. 사용자는 이메일 주소로 전송된 6자리 검증 코드를 입력하고 ID를 확인할 수 있습니다. 자세한 내용은 이메일을 사용한 다단계 인증 문서를 참조하십시오.



관련 정보

- 웹 인증 - MFA
- MFA 검증 방법
- 이메일을 사용한 다단계 인증

웹 인증 **- MFA**

통합 **-** 웹 인증**(com.snc.integration.webauthn)**을 사용하여 인스턴스에서 하드웨어 키 또는 생체 인식 판독기 인증을 허용합니다.



하드웨어 키는 인증에 사용할 수 있는 물리적 하드웨어입니다. 하드웨어 키는 인증을 제공하기 위해 장치의 포트에 삽입됩니다. 하드웨어 키 등록에 대한 자세한 내용은 문서를 참조하십시오 하드웨어 보안 키 등록.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



생체 인식 인증기는 지문 또는 얼굴 인식을 사용하여 사용자를 식별합니다. 사용자는 장치에서 이러한 인증기를 다단계 로그인 프로세스의 일부로 사용할 수 있습니다. 생체 인식 인증기 등록에 대한 자세한 내용은 을 참조하십시오 생체 인식 인증기 등록.

생체 인식을 사용하여 **MFA** 구성

관리자는 사용자 공개 자격 증명 목록을 사용하여 사용자가 생성한 자격 증명을 보고 관리할 수 있습니다.

사용자가 인증자 애플리케이션, 생체 인식 인증 또는 하드웨어 키를 등록하면 사용자 공개 자격 증명[sys_user_public_credential] 테이블에 기록이 생성됩니다. 이 테이블을 사용하여 인증자를 등록한 사용자와 인증자 유형, 등록 및 사용 시기를 확인합니다. 또한 이러한 기록을 비활성으로 표시하여 자격 증명이 사용자가 해당 자격 증명을 사용하지 못하도록 할 수 있습니다.

웹 인증(FIDO2)을 위해서는 통합 **-** 웹 인증**(com.snc.integration.webauthn)** 플러그인을 활성화해야 합니다.

주: 통합 **-** 웹 인증**(com.snc.integration.webauthn)** 플러그인이 기본적으로 설치됩니다.

사용자 공개 자격 증명 양식

필드	설명
자격 증명 별명	자격 증명의 별명입니다. 이 별칭은 사용자가 인증자를 등록할 때 선택합니다.
사용자	자격 증명과 연결된 사용자
활성	자격 증명이 활성 상태인지 여부입니다. 관리자는 기록을 비활성으로 설정하여 사용자가 이 자격 증명으로 인증하지 못하도록 할 수 있습니다.
인증자	사용자가 등록한 인증자의 유형입니다.
등록 시간	사용자가 이 자격 증명을 생성한 날짜 및 시간입니다
최종 사용 시간	사용자가 이 자격 증명으로 로그인한 마지막 날짜 및 시간입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제한된 인증자 유형

생체 인식 인증기와 같은 인증 방법을 제한한 경우 사용자는 해당 유형의 새 자격 증명을 만들 수 없습니다. 그러나 이 제한을 만들기 전에 만든 자격 증명은 계속 작동합니다. 사용자 공개 자격 증명 테이블에서 기록을 비활성화하여 이러한 자격 증명이 생성된 후 사용되지 않도록 할 수 있습니다.

인증기 구성 옵션

인증자 구성 페이지를 사용하여 인스턴스의 인증기 옵션을 관리합니다.

다음으로 이동 다단계 인증 > 웹 인증 > 인증기 구성 을 클릭하여 기본 구성 옵션을 보고 편집합니다.

인증자 구성 양식

필드	설명
허용된 인증자 유형	등록할 수 있는 인증자의 유형입니다. 다음 중에서 선택합니다. • 플랫폼 인증자는 장치에 연결되거나 통합됩니다. 모바일 장치에서 사용할 수 있는 지문 판독기 또는 얼굴 인식(예: Apple FaceID 또는 TouchID)이 이 범주에 속합니다. • 로밍 인증기는 컴퓨터 또는 다른 클라이언트 장치에서 제거되어 다른 곳에서 사용될 수 있습니다. 하드웨어 키는 이 범주에 속합니다.
증명 유형	값을 직접 또는 간접으로 설정하면 등록 중 인증기의 출처를 증명하기 위해 인증기 메타데이터를 임포트해야 합니다. • 안 함 • 직접 • 간접
플랫폼 자체 증명	플랫폼 인증자에 대해 자체 증명을 사용할 수 있는지 여부입니다.
교차 플랫폼 자체 증명	로밍 인증기에 대해 자체 증명을 사용할 수 있는지 여부입니다.
사용자 검증	선호 또는 필수 중에서 선택합니다. 필요한 경우 웹 인증 플로우는 PIN 또는 생체 인식을 사용하여 사용자에게 검증을 요청하는 메시지를 표시합니다.
사용자 현재 상태 검증	웹 인증 플로우에 사용자 현재 상태 확인이 필요한지 여부입니다.
상주 키	선호 또는 필수 중에서 선택합니다. 필요한 경우 인증자는 인증기 스토리지 내에 공개 키 자격 증명을 유지합니다.
시간 제한(ms)	웹 인증 등록 및 인증을 완료하기 위한 최대 시간 제한입니다. 시간은 밀리초 단위입니다.

SMS를 사용한 다단계 인증

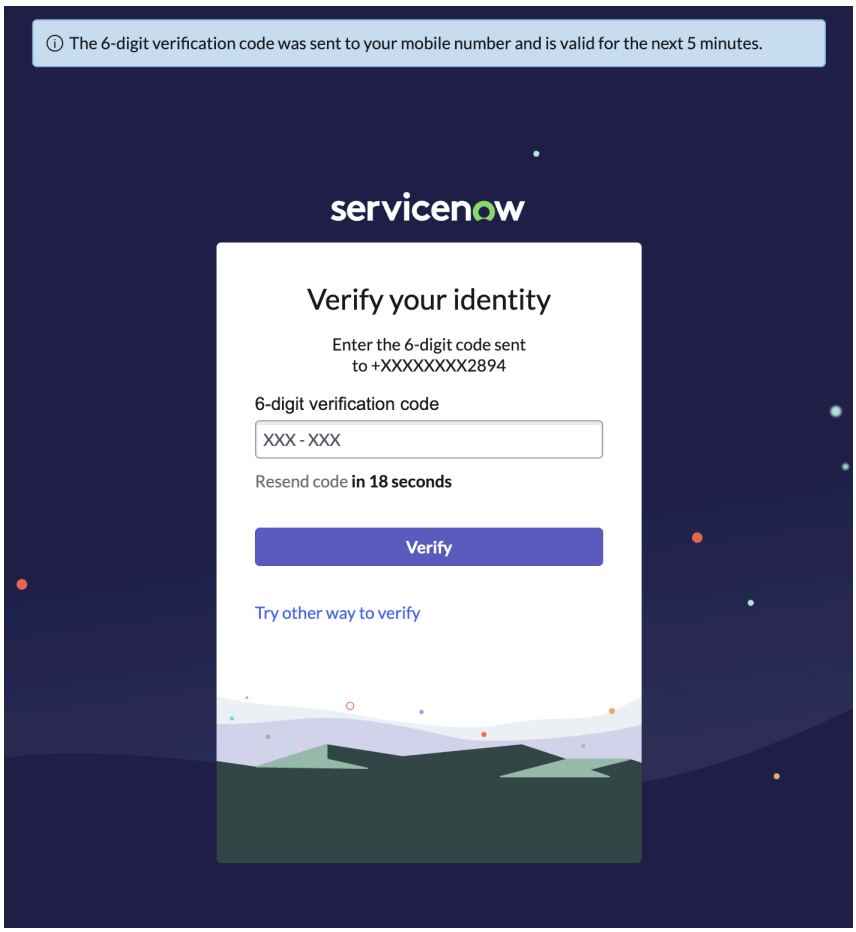
SMS를 인증 요소로 사용하는 다단계 인증(MFA).

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관리자는 SMS 기반 OTP를 사용하여 인스턴스에 로그인을 시도하는 사용자에게 요구하도록 인스턴스를 구성할 ServiceNow 수 있습니다.

사용자가 로그인을 ServiceNow시도하면 sys_user 기록과 연결된 휴대폰 번호로 SMS OTP가 전송됩니다. 사용자는 모바일 장치로 전송된 6자리 검증 코드를 입력하고 ID를 확인할 수 있습니다.

바로 사용 가능한 Twilio SMS를 사용하여 MFA를 구성할 수도 있습니다. 자세한 내용은 다단계 인증 제공자 문서를 참조하십시오.



또한 SMS를 통한 MFA는 필터 기준을 사용하여 정책 입력 및 조건에 따라 제어할 수 있습니다. 필터 기준의 유형은 다음과 같습니다.

- IP 필터 기준
- 역할 필터 기준
- 그룹 필터 기준

SMS 플러그인으로 MFA 활성화

SMS를 사용하는 MFA의 경우 SMS를 사용한 다단계 인증(com.snc.authentication.sms_mfa) 플러그인을 설치합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
SMS를 사용한 다단계 인증과 함께 다음 항목이 설치됩니다.

- 적응형 인증(com.snc.adaptive_authentication
- 알림 - Twilio Direct 드라이버(com.snc.notify.twilio_direct)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

종속 플러그인: Integration - Multifactor Authentication(`com.snc.integration.multifactor.authentication`)

주: SMS를 생성하기 위한 사용자 지정 제공자를 구성하는 경우 플러그인을 설치할 때 데모 데이터를 로드할 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 SMS 플러그인(`com.snc.authentication.sms_mfa`)을 통한 다단계 인증을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

SMS를 **MFA** 요소로 구성

SMS OTP를 인증을 위한 MFA 요소 정책으로 표시하도록 정책 입력 및 조건을 구성합니다.

시작하기 전에

필요한 플러그인: SMS를 사용한 다단계 인증(`com.snc.authentication.sms_mfa`).

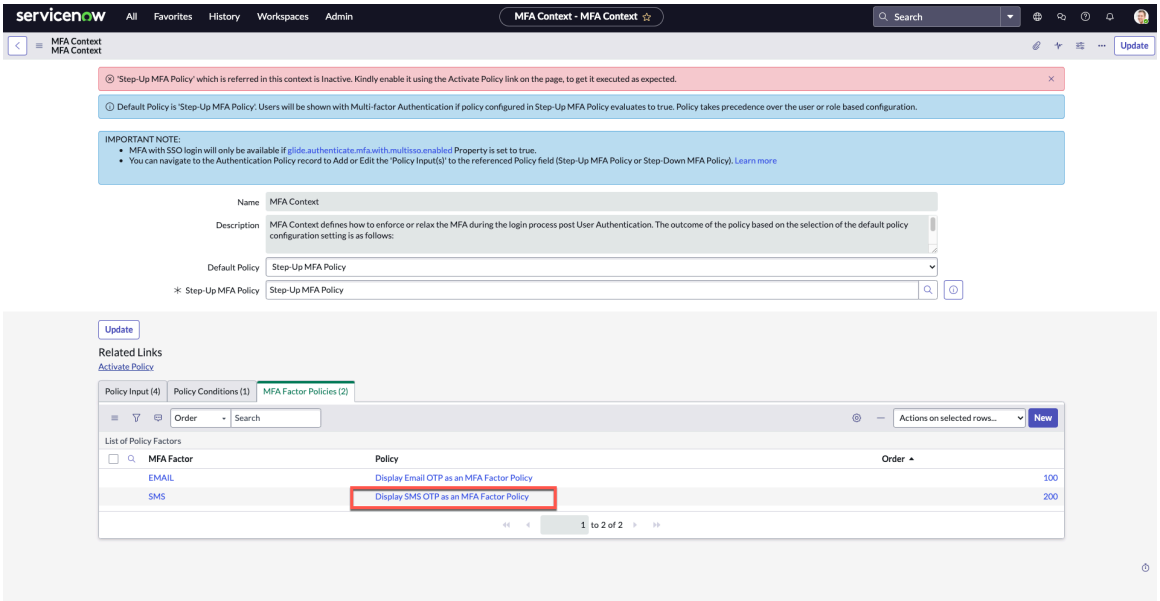
필요한 역할: 관리자

주: SMS 요소 정책을 적용하려면 MFA 컨텍스트 정책을 `true` 로 평가해야 합니다.

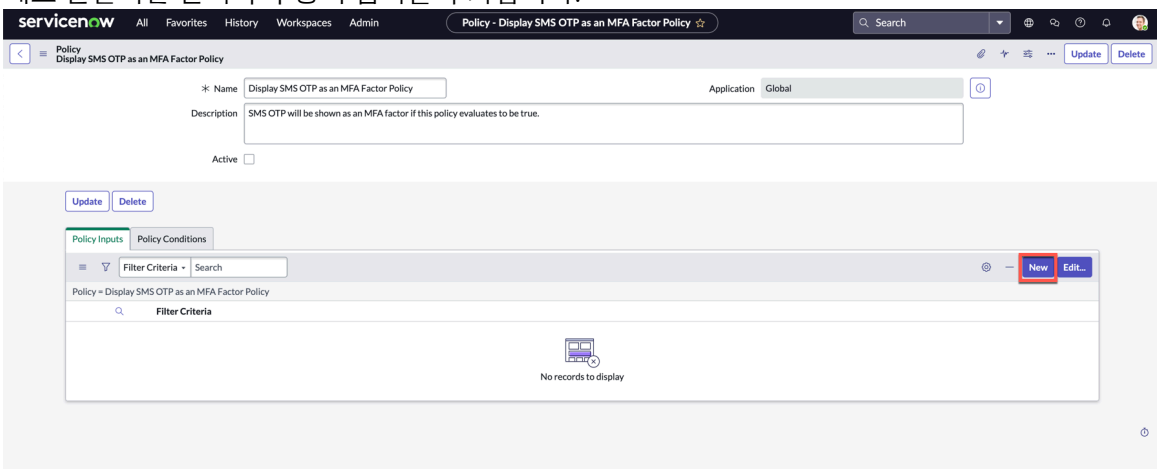
프로시저

1. 다음으로 이동 모두 > 다단계 인증 > **MFA** 컨텍스트.
2. **MFA** 요소 정책 탭을 클릭합니다.
3. **SMS** OTP를 **MFA** 요소 정책으로 표시를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 새로 만들기를 클릭하여 정책 입력을 추가합니다.

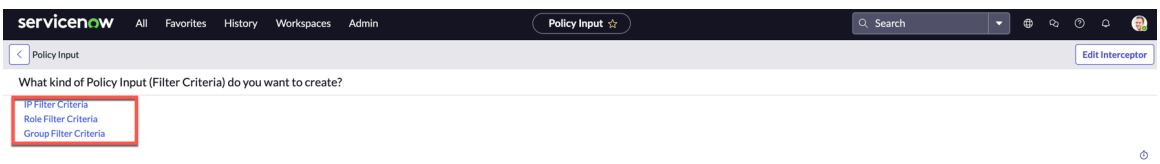


5. 생성하려는 필터 기준을 선택합니다.

필터 기준의 유형은 다음과 같습니다.

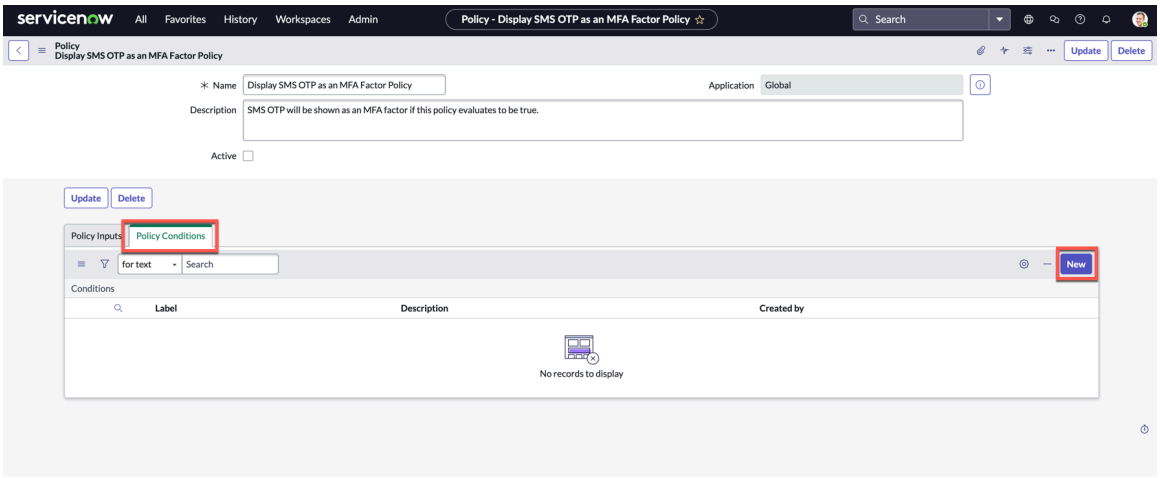
- IP 필터 기준
- 역할 필터 기준
- 그룹 필터 기준

예를 들어, 역할 필터 기준입니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 역할 필터 기준을 클릭하고 역할 필터 기준의 필드를 입력한 후 기록을 제출합니다.
새 정책이 생성됩니다. 자세한 내용은 역할 필터 조건을 참조하십시오.
7. 정책 - SMS OTP를 MFA 요소 정책으로 표시 페이지에서 정책 조건을 클릭합니다.



8. 새로 만들기를 클릭하여 정책 조건을 추가합니다.
9. 양식의 필드에 내용을 입력합니다.

조건 양식

필드	설명
레이블	조건을 식별하는 이름입니다.
설명	조건에 대한 설명입니다.
조건	인증 요청을 평가하는 데 사용되는 여러 정책 입력(필터 기준)의 논리적 조합입니다. 조건에 대해 생성된 역할 기반 필터 기준 정책을 선택합니다.

10. 제출을 클릭합니다.
11. 옵션: 8단계를 반복하여 추가 정책 조건을 생성합니다.

> **주:** 여러 정책 조건을 생성하는 경우 액세스 정책의 최종 출력은 모든 정책 조건의 논리적 OR 출력에 따라 달라집니다. 즉, 정책 조건 중 하나라도 충족되면 정책이 true로 평가됩니다.

역할 필터(사용자) 정책에 따라 역할에 지정된 조건이 일치하면 MFA 요소로서의 SMS가 사용자에 대한 인증 옵션으로 표시됩니다.

다단계 인증 제공자

MFA 공급자를 사용하여 모든 사용자가 안전하게 로그인할 수 있도록 SMS 및 이메일 기반 인증을 구성합니다.

에서 Now Platform이메일 및 SMS와 같은 다단계 인증을 사용하는 메커니즘으로 MFA 제공자를 구성할 수 있습니다.

다음 내에서 MFA에 사용할 수 있는 다음 제공자 구성을 사용할 수 있습니다.Now Platform

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 이메일 제공자 구성
- Twilio 제공자 구성
- Infobip 제공자 구성입니다.

주: SMS(`com.snc.authentication.sms_mfa`) 및 알림 - Twilio Direct 드라이버(`com.snc.notify.twilio_direct`) 플러그인을 사용한 다단계 인증 설치 시 데모 데이터 로드를 활성화하여 Twilio 및 Infobip 제공자 구성이 자동으로 채워집니다.

SMS 및 이메일을 통한 다단계 인증을 활성화하기 위한 고유한 제공자 구성을 생성할 수도 있습니다.

주: Infobip 제공자 구성은 데모 데이터의 일부로 제공되며, 자체 제공자 구성에 대한 요구 사항에 따라 필드를 편집할 수 있습니다.

MFA 제공자 구성

모든 사용자가 안전하게 로그인할 수 있도록 제공자와 함께 SMS 및 이메일을 구성합니다.

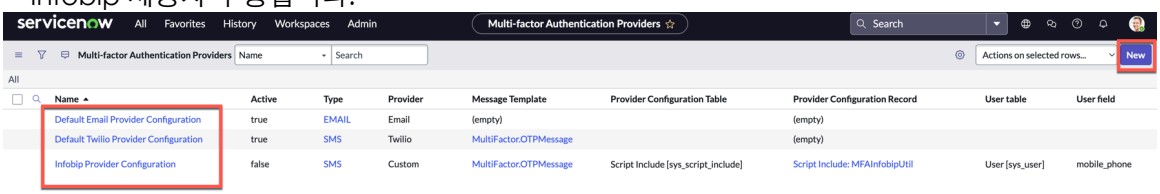
시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 다단계 인증 > 제공자.

   다음 제공자 구성을 MFA에서 사용할 수 있습니다.Now Platform

   - 이메일 제공자 구성
   - Twilio 제공자 구성
   - Infobip 제공자 구성입니다.



2. 새 제공자를 만들려면 새로 만들기를 클릭합니다.
3. 양식에서 필드를 채웁니다.

   조건 양식

필드	설명
이름	기록의 이름입니다.
유형	기록에 대한 설명입니다.
제공자	**Twilio** 또는 사용자 지정을 선택합니다. 주: Twilio를 구성하려면 Twilio로 알림 구성을 참조하십시오. 사용자 지정을 선택할 때 다음 필드를 지정해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	◦ 제공자 구성 테이블 ◦ 제공자 구성 기록 ◦ 스크립트 ◦ 사용자 테이블 ◦ 사용자 필드
메시지 템플릿	기록에 대한 메시지 템플릿입니다.
활성	제공자 구성을 활성화하는 옵션입니다.

4. 제출을 클릭합니다.

   메시지 템플릿 및 제공자 구성에 따라 로그인 프로세스 중에 인증 요소로 SMS 또는 이메일이 사용자에게 전송됩니다.

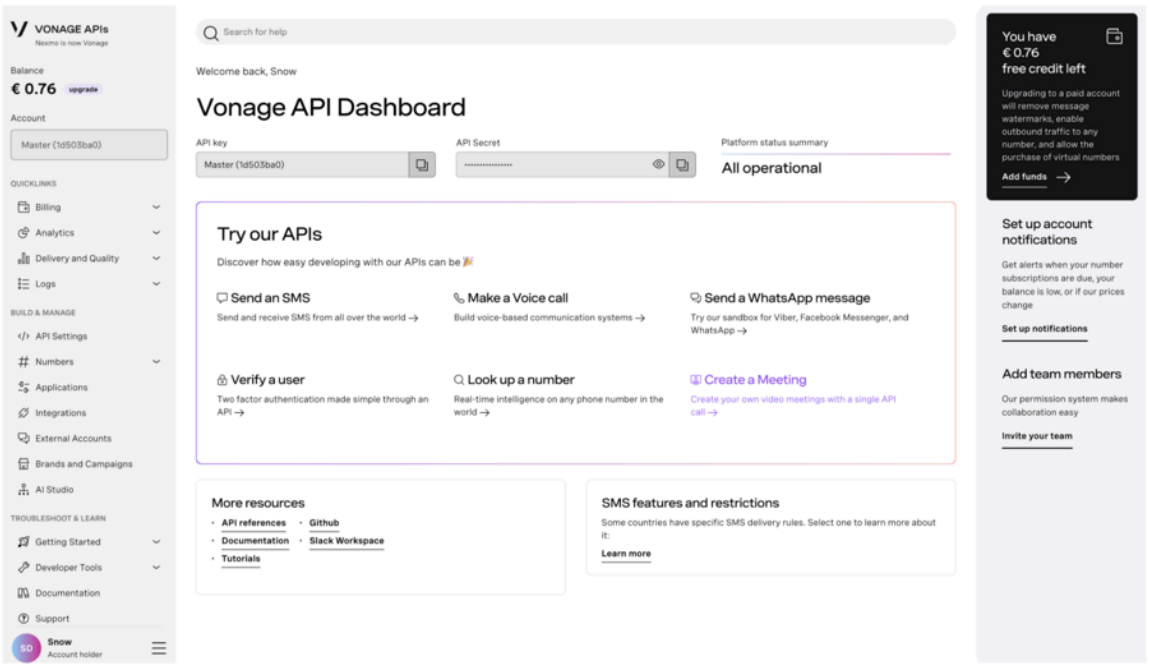
Vonage Provider 사용자 지정 구성(자습서)

모든 사용자가 안전하게 로그인할 수 있도록 Vonage Provider를 통한 SMS를 구성합니다.

시작하기 전에
필요한 역할: 관리자

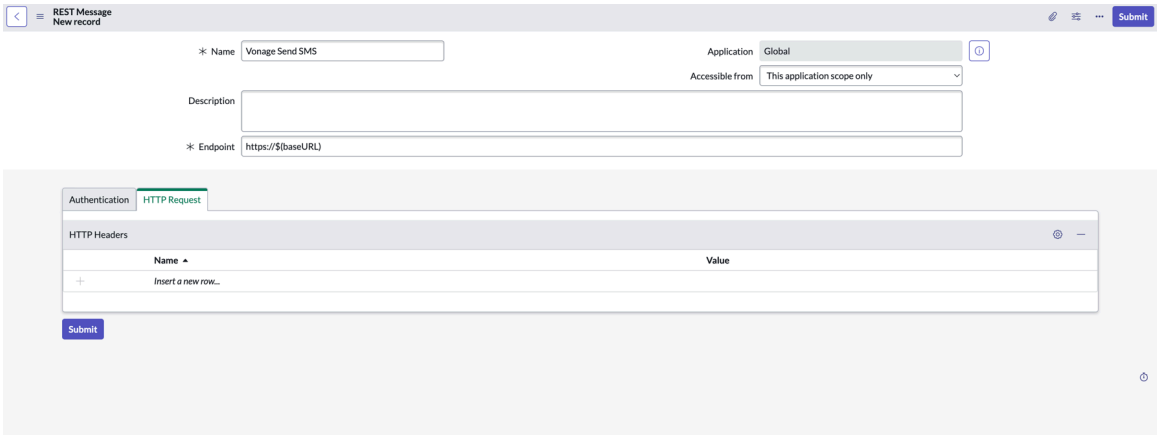
프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > 아웃바운드 > **REST** 메시지 Vonage API 대시보드의 정보를 기반으로 REST 메시지 구성을 수행합니다.

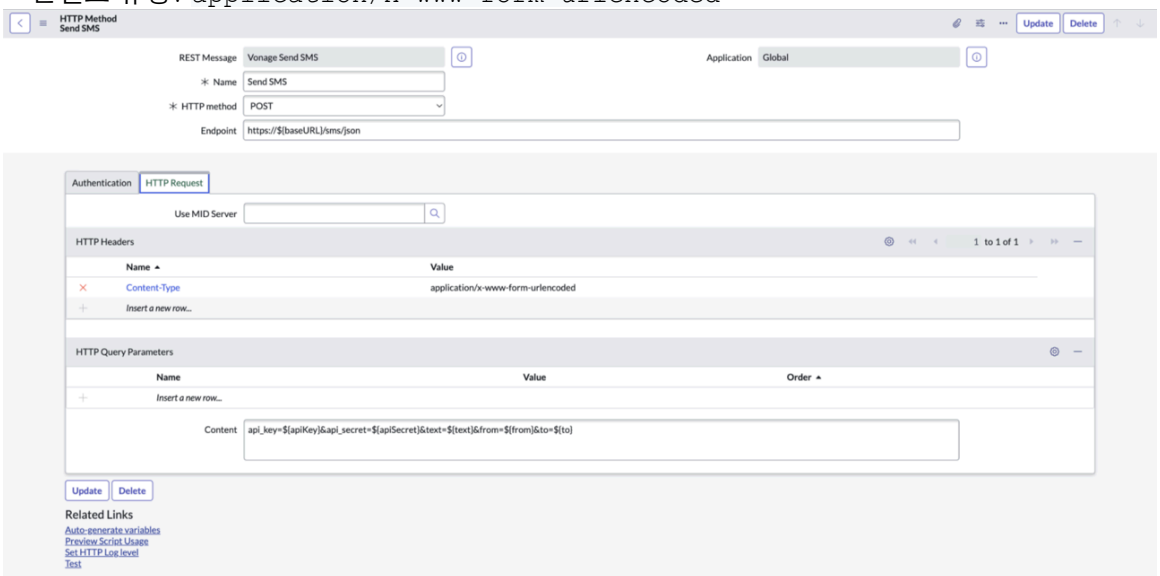


2. 새로 만들기를 클릭하여 새 **REST** 메시지를 만듭니다.
3. 이름과엔드포인트를 제공합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



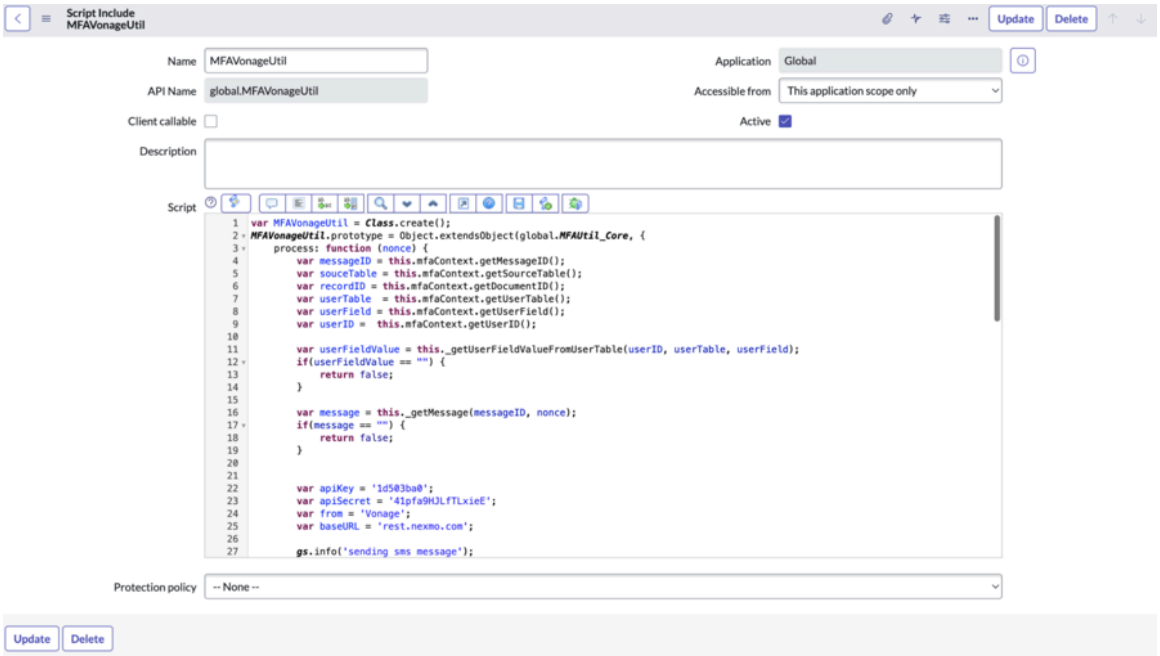
4. 제출을 클릭합니다.
5. 생성된 기록을 열고 **HTTP** 메서드 관련 목록에서 새로 만들기를 클릭한 다음 HTTP 메서드를 **POST**로 선택합니다.
6. 다음 필드를 채웁니다.
   - 엔드포인트: `https://${baseURL}/sms/json`
   - 콘텐츠: `api_key=${apiKey}&api_secret=${apiSecret}&text=${text}&from=${from}&to=${to}`
   - 콘텐츠 유형: `application/x-www-form-urlencoded`



7. 기록을 업데이트합니다.
8. 관련 링크 섹션에서 변수 자동 생성을 클릭합니다.
9. 폴더에서 공유된 SI를 임포트하고 Vonage API 대시보드에서 apiKey와 암호를 복사합니다.

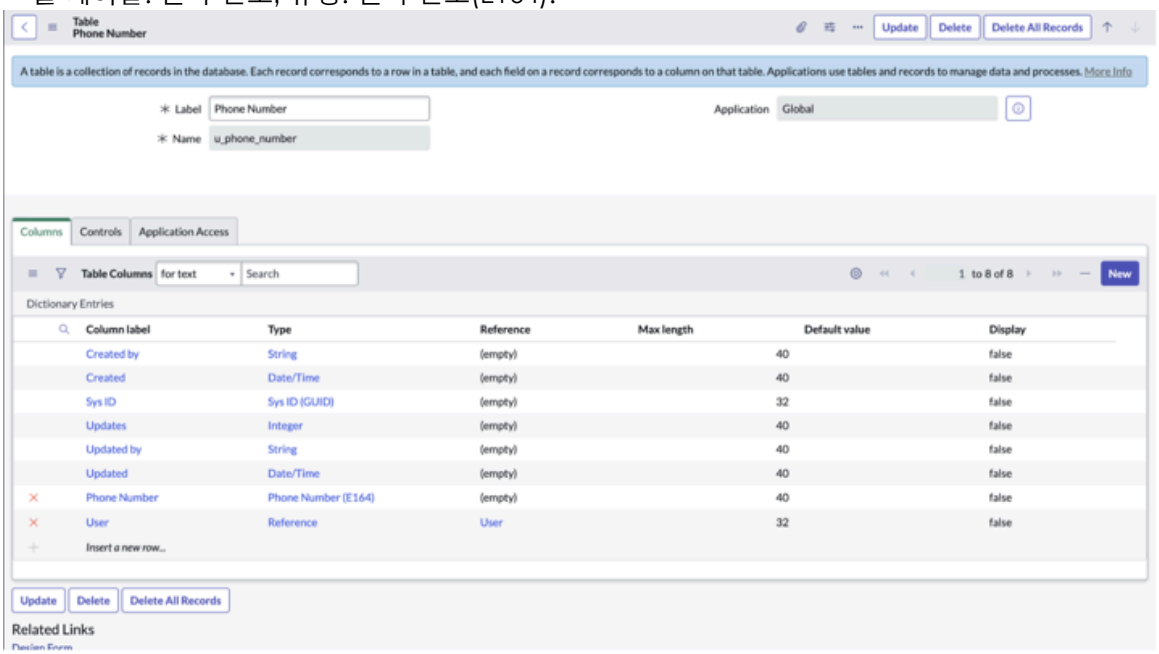
> **주:**
>
> apiKey와 암호는 Vonage 대시보드의 Vonage 계정 설정에 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



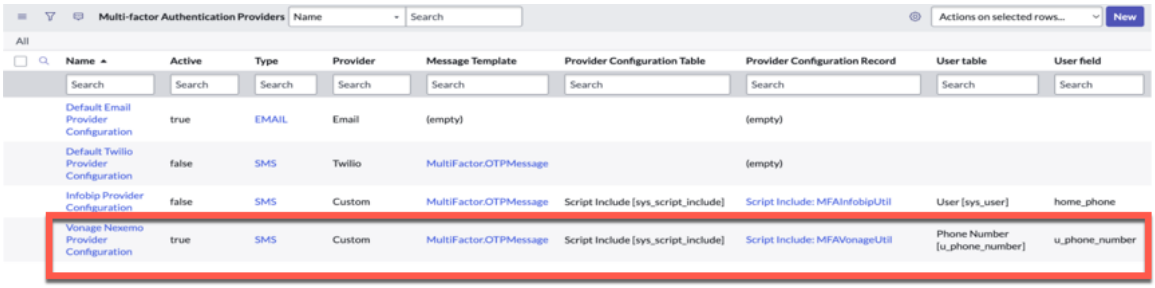
10. 두 개의 열이 있는 사용자 지정 테이블 전화 번호를 생성합니다. 예를 들면 다음과 같습니다.

- 열 레이블: 사용자, 유형: 참조, 참조: 사용자(sys_user).
- 열 레이블: 전화 번호, 유형: 전화 번호(E164).



11. 다단계 제공자 테이블에서 사용자 지정 제공자를 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



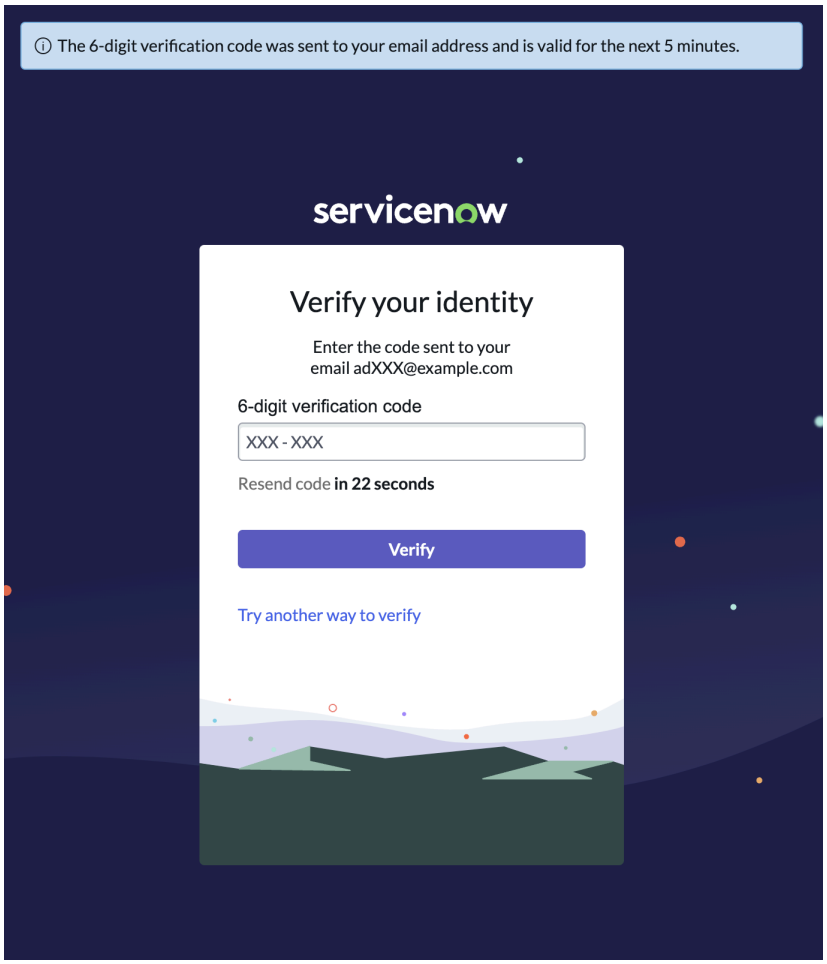
제공자 구성에 대한 자세한 내용은 문서를 참조하십시오 MFA 제공자 구성.

이메일을 사용한 다단계 인증

이메일을 인증 요소로 사용하는 다단계 인증(MFA).

관리자는 이메일 기반 OTP를 사용하여 인스턴스에 로그인을 시도하는 사용자에게 요구하도록 인스턴스를 구성할 ServiceNow 수 있습니다.

주: 이메일을 포함한 MFA는 기본적으로 통합 - 사용자 다단계 인증 (`com.snc.integration.multifactor.authentication`) 플러그인을 사용하여 활성화됩니다. 정책 입력 및 조건을 구성해야 합니다.



사용자가 로그인을 ServiceNow시도하면 연결된 이메일 주소로 이메일 OTP가 전송됩니다. 사용자는 이메일 주소로 전송된 6자리 검증 코드를 입력하고 ID를 확인할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일을 **MFA** 요소로 구성

이메일 OTP를 인증을 위한 MFA 요소 정책으로 표시하도록 정책 입력 및 조건을 구성합니다.

시작하기 전에
필요한 역할: 관리자

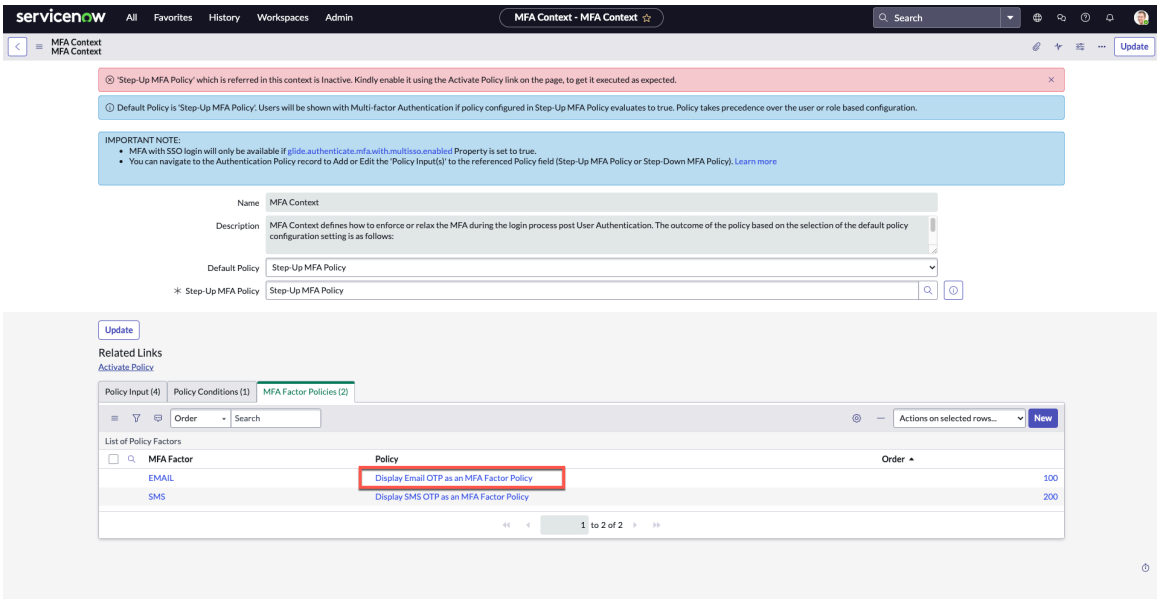
프로시저

1. 다음으로 이동 모두 > 다단계 인증 > **MFA** 컨텍스트.

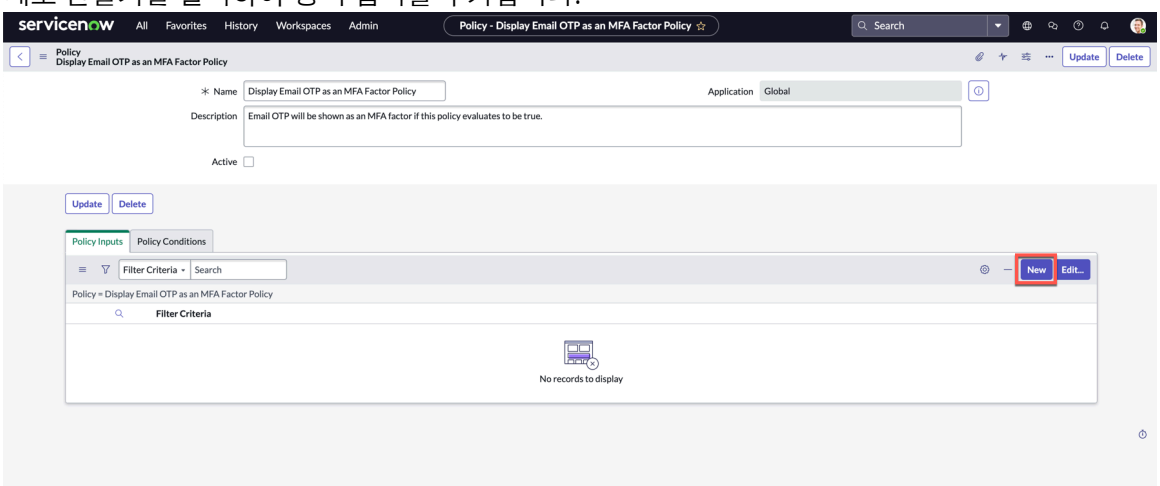
2. **MFA** 요소 정책 탭을 클릭합니다.

> 주: 정책이 포함된 **MFA** 요소로서의 이메일은 기본적으로 사용할 수 있습니다. 정책을 편집하고 정책 입력 및 조건을 지정할 수 있습니다.

3. 이메일 OTP를 **MFA** 요소 정책으로 표시를 선택합니다.



4. 새로 만들기를 클릭하여 정책 입력을 추가합니다.



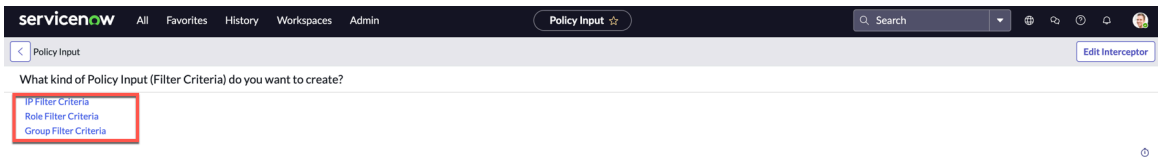
5. 생성하려는 필터 기준을 선택합니다.

필터 기준의 유형은 다음과 같습니다.

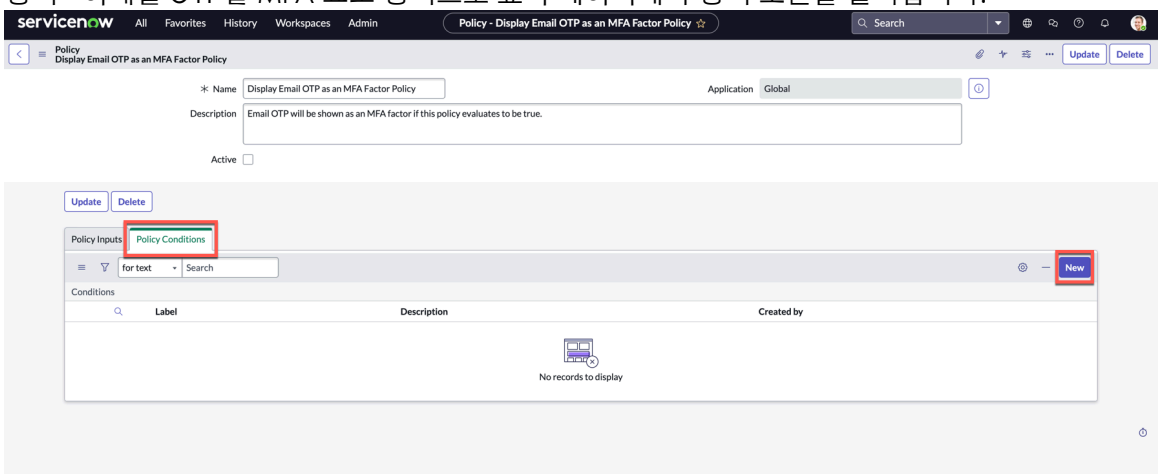
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- IP 필터 기준
- 역할 필터 기준
- 그룹 필터 기준

예를 들어, 역할 필터 기준입니다.



6. 역할 필터 기준을 클릭하고 역할 필터 기준의 필드를 입력한 후 기록을 제출합니다. 새 정책이 생성됩니다. 자세한 내용은 역할 필터 조건을 참조하십시오.
7. 정책 - 이메일 OTP를 MFA 요소 정책으로 표시 페이지에서 정책 조건을 클릭합니다.



8. 새로 만들기를 클릭하여 정책 조건을 추가합니다.
9. 양식의 필드에 내용을 입력합니다.

조건 양식

필드	설명
레이블	조건을 식별하는 이름입니다.
설명	조건에 대한 설명입니다.
조건	인증 요청을 평가하는 데 사용되는 여러 정책 입력(필터 기준)의 논리적 조합입니다. 조건에 대해 생성된 역할 기반 필터 기준 정책을 선택합니다.

10. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

11. 옵션: 8단계를 반복하여 추가 정책 조건을 생성합니다.

> **주:** 여러 정책 조건을 생성하는 경우 액세스 정책의 최종 출력은 모든 정책 조건의 논리적 OR 출력에 따라 달라집니다. 즉, 정책 조건 중 하나가 충족되면 정책이 true로 평가됩니다.

역할 필터(사용자) 정책에 따라 역할에 지정된 조건이 일치하면 이메일 MFA 요소가 사용자에 대한 인증 옵션으로 표시됩니다.

다단계 인증 시스템 속성

시스템 속성을 사용하여 보안 요구 사항에 맞게 MFA를 활성화하고 사용자 지정합니다.

다단계 인증 속성

속성	설명
glide.authenticate.multifactor.setup.bypass.count	사용자가 MFA 설정을 건너뛰도록 선택할 수 있는 횟수입니다. 기본값은 0입니다.
glide.multifactor.onetime.code.validity	재설정 코드가 유효한 시간(분)입니다. 다단계 인증으로 로그인 문서를 참조하십시오. 기본값은 5입니다. **주:** 이 속성은 이메일 OTP 확인 시간용입니다.
glide.authenticate.multifactor.clock_skew	재설정 코드가 유효한 추가 시간(초)입니다. 최대값은 `60`입니다. 기본값은 `10`입니다. 인스턴스는 사용자가 입력한 코드를 `## ###` 생성된 단일 앱 생성 코드와 비교하여 확인합니다. 이 속성을 사용하여 시간 창을 조정하고 시간 창 동안 하나 이상의 코드를 생성하여 유효한 것으로 간주할 수 있습니다. 속성 값은 `## ## - X/2` 및 `## ## + X/2`의 계산에 사용되며, 여기서 `X` 는 이 속성의 값입니다. 예를 들어 값 `10`을 사용하는 경우 인스턴스는 앱이 `## ## [## ## - 5#]` 및 `[## ## + 5#]` 내에서 생성하는 모든 코드를 유효한 것으로 간주합니다. 이 속성을 사용하면 할당된 기본 시간에 사용자가 올바른 코드를 입력할 수 없는 로그인 문제를 방지할 수 있습니다.
glide.authenticate.multifactor.remember.browser.instance	사용자가 새 장치 또는 브라우저에서 로그인할 때 MFA 메시지를 표시하도록 인스턴스를 설정합니다. 기본값은 yes입니다.
glide.authenticate.multifactor.browser.MFA.expiration.interval	MFA가 브라우저를 기억한 후에는 이 기간 동안 동일한 브라우저에서 MFA에 대한 질문이 사용자에게 표시되지 않습니다. 기본값은 8시간입니다.
glide.authenticate.multifactor.remember.browser.max.count	MFA가 이 사용자에 대해 기억하는 브라우저 수입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다단계 인증 속성

속성	설명
glide.authenticate.multifactor.remember.browser.default	다단계 확인 페이지에 있는 remember-browser 확인란의 기본값입니다.
glide.webauthn.enabled	하드웨어 키 및 생체 인식 인증과 같은 암호 없는 인증(FIDO2 기반 MFA) 방법을 활성화하는 옵션입니다.
glide.authenticate.multifactor.email.otp.enable	이메일 기반 OTP를 MFA의 요소로 활성화하는 옵션입니다.
glide.auth.mfa.ui.v2.enabled	인증자 앱을 설정하지 않고 사용자에 대해 독립적으로 MFA 요소를 활성화하는 옵션입니다.

다단계 인증 기준

다중요인 기준을 사용하여 2단계 다단계 인증을 사용해야 하는 사용자와 역할을 결정합니다.

다중요인 기준

다중요인 기준을 사용하여 2단계 다단계 인증을 사용해야 하는 사용자와 역할을 결정합니다. 비즈니스 요구에 맞게 이러한 기준 중 하나를 사용하거나 여러 기준을 조합할 수 있습니다. 비즈니스 요구에 맞게 이러한 기준 중 하나를 사용하거나 여러 기준을 조합할 수 있습니다.

주: 적응형 인증 정책 기반 MFA를 사용하는 것이 좋습니다.

사용자 기반 다중요인 기준

사용자 기반 다중요인 기준을 사용하여 MFA를 사용해 로그인해야 하는 개별 사용자를 선택합니다. 관리자는 사용자 기록의 **Multifactor Authentication** 사용 필드를 업데이트하여 사용자에 대한 MFA 요구 사항을 사용하거나 사용하지 않도록 설정합니다. 이 프로세스에 대한 자세한 내용은 사용자 기반 다중요인 기준 구성 문서를 참조하십시오.

역할 기반 다중요인 기준

역할 기반의 다중요인 기준을 사용하여 특정 역할에 할당된 모든 사용자에 대해 MFA 로그인을 요구합니다. 다중요인 기준 [multi_factor_criteria] 테이블의 역할 기반 다단계 인증 기록에는 MFA 로그인이 필요한 역할 목록이 포함되어 있습니다. 이 목록을 유지 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 역할 기반 다중요인 기준 구성.

적응형 인증 정책 기반 다중요인 기준

적응형 인증을 사용하여 인스턴스에 MFA가 필요한 시기를 결정합니다. 적응형 인증은 인증 정책을 사용하여 사용자의 IP 주소 또는 사용자 그룹과 같은 기준을 평가합니다. 적응형 인증 기능에 대한 자세한 내용은 문서를 참조하십시오 적응형 인증.

사용자 기반 다중요인 기준 구성

사용자 기반 다중요인 기준을 사용하여 사용자에 대해 MFA를 활성화합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 사용자 관리 > 사용자.
2. **Multifactor Authentication** 사용 열을 표시하도록 목록을 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 선택한 사용자에 대한 **Multifactor Authentication** 사용 열의 값을 **true**로 변경합니다.

   사용자가 사용자 이름과 암호로 로그인하면 다단계 인증을 설정하라는 메시지가 표시됩니다.

역할 기반 다중요인 기준 구성

역할 기반의 다중요인 기준을 사용하여 특정 역할에 할당된 모든 사용자에 대해 다단계 인증을 적용합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 다단계 인증 > 다중요인 기준.
2. 다중요인 기준 목록에서 역할 기반 다단계 인증 기록을 엽니다.
3. 다단계 역할 목록을 사용하여 역할을 추가하거나 제거합니다.

옵션	설명
역할 추가	새 행 삽입...을 두 번 클릭하고 역할 이름을 입력하거나 선택합니다. 저장 아이콘( )을 클릭하여 항목을 저장합니다.
역할 제거	목록에서 역할을 제거하려면 삭제 아이콘( )을 클릭합니다.

4. 업데이트를 클릭합니다.

결과
인스턴스가 다단계 역할 목록에 나열된 역할의 구성원인 모든 사용자에 대해 다단계 인증을 적용합니다.

중요사항: 역할 기반 다단계 인증을 적용하려면 기록이 활성 상태여야 합니다.

적응형 인증 정책 기반 다중요인 기준 구성

적응형 정책을 사용하여 2단계 MFA(다단계) 검증을 사용해야 하는 사용자를 결정합니다.

시작하기 전에
필요한 역할: 관리자

주:

- 기본 정책이 스텝업 **MFA** 정책인 경우 스텝업 **MFA** 정책에 구성된 정책이 예로 평가되면 사용자가 다단계 인증으로 표시됩니다. 정책은 사용자 또는 역할 기반 구성보다 우선합니다.
- SSO 로그인을 통한 MFA는 `glide.authenticate.mfa.with.multisso.enabled` 속성이 예로 설정된 경우에만 사용할 수 있습니다.
- 인증 정책 기록으로 이동하여 참조된 정책 필드(스텝 업 **MFA** 정책 또는 스텝 다운 **MFA** 정책)에 "정책 입력"을 추가하거나 편집할 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 컨텍스트 > **MFA** 컨텍스트.
   MFA 컨텍스트 정책 컨텍스트 기록이 열립니다.
2. 기본 정책 필드에서 기본 정책을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 선택에 따라 인스턴스에서 정책 조건을 사용하여 MFA를 요구할지 여부를 결정하는 방법이 결정됩니다.

기본 정책

기본 정책	정의
스텝업 MFA 정책	스텝업 **MFA** 정책에 정의된 정책 조건이 true로 평가될 때 MFA를 적용하려면 선택합니다.
스텝다운 MFA 정책	스텝다운 **MFA** 정책에 정의된 정책 조건이 예로 평가될 때 MFA를 바이패스하려면 선택합니다.

3. 스텝업 **MFA** 정책 필드에서 이 컨텍스트에 사용할 정책을 선택합니다.
4. 업데이트를 클릭합니다.
   기록을 저장하면 정책 입력 및 정책 조건 목록이 업데이트되어 스텝업 **MFA** 정책 필드에서 선택한 정책과 연결된 정책 입력 및 조건이 표시됩니다.

SSO(Single Sign-On)를 사용하여 다단계 인증 구성

인스턴스에 대해 1회 사용자 인증(SSO) 제공자를 사용하여 다단계 인증(MFA)을 ServiceNow 구성합니다.

조직의 많은 사용자가 회사 네트워크에 로그인하고 인스턴스에 액세스하기 ServiceNow 때문에 보안 인증에 대한 필요성이 더욱 커집니다.

SSO를 조합한 MFA는 인스턴스에 향상된 보안을 제공합니다. 이 기능은 사용자에 대해 조건부로 MFA를 활성화할 수 있는 유연성을 제공합니다.

주:

- ServiceNow MFA는 ID 제공자에서 인증에 성공한 후 사용자가 리디렉션된 후에 적용됩니다.
- San Diego 릴리스 이전에는 SSO에 MFA가 적용되지 않았습니다.

예를 들어 외부 사용자에게 추가 보안 프로토콜을 제공하려는 경우 해당 사용자에게만 MFA를 적용할 수 있습니다. 이러한 방식으로 추가 인증 기능을 추가하고 사용자 액세스를 제어할 수 있습니다.

SAML, OpenID Connect, 다이제스트와 같은 SSO 기반 로그인의 경우 인증에 MFA를 적용할 수 있습니다.

SSO를 사용하는 MFA는 요구 사항에 따라 주문형으로 구성할 수 있습니다. 인증 체계 및 ID 공급자의 도움을 받아 특정 로그인 메커니즘을 사용하여 특정 사용자에 대해 MFA를 적용할 수 있습니다.

다음 조건에 대해 MFA를 적용할 수 있습니다.

- 인증 체계
- ID 제공자

SSO를 통한 MFA는 적응형 인증 플러그인(com.snc.adaptive_authentication)의 일부로 제공됩니다. 적응형 인증을 설정하는 방법에 대한 자세한 내용은 문서를 참조하십시오 적응형 인증.

SSO로 **MFA** 구성

조직 내부 또는 외부의 사용자에 대해 SSO를 통해 MFA를 적용합니다.

시작하기 전에

SSO를 통한 MFA 기능은 적응형 인증 플러그인(com.snc.adaptive_authentication)의 일부로 제공됩니다. SSO 기능과 함께 MFA를 사용하려면 적응형 인증 속성을 활성화해야 합니다. 적응형 인증을 설정하는 방법에 대한 자세한 내용은 문서를 참조하십시오 적응형 인증.

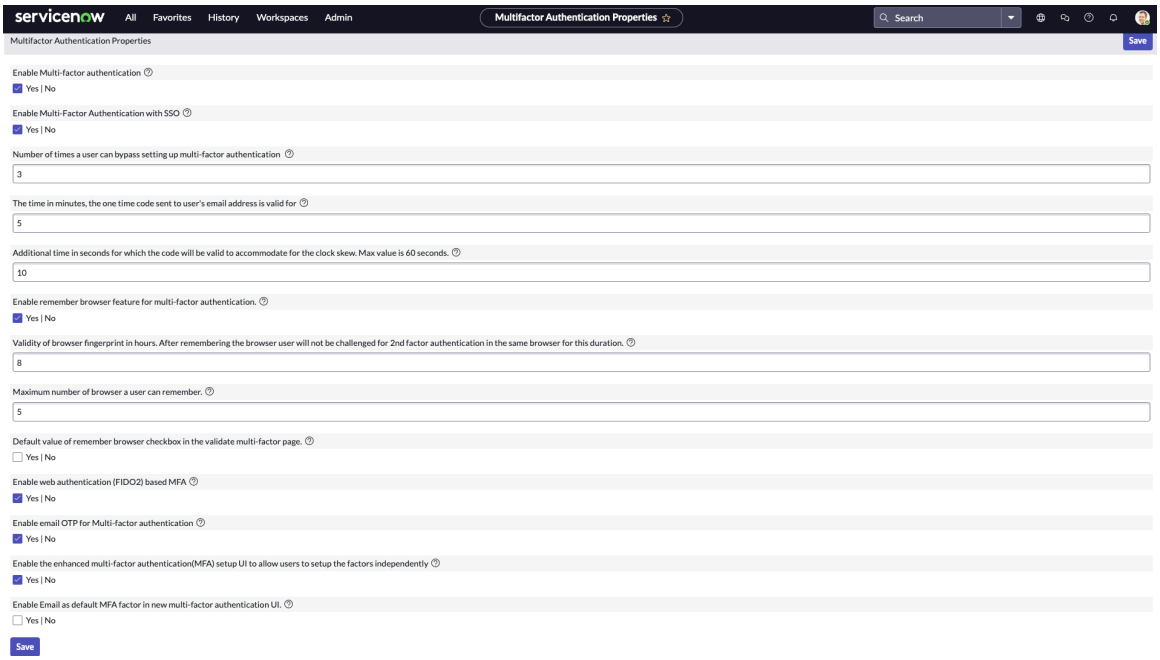
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 속성이 예로 설정된 경우 SSO 로그인을 통한 MFA를 사용할 수 *glide.authenticate.mfa.with.multisso.enabled*있습니다.

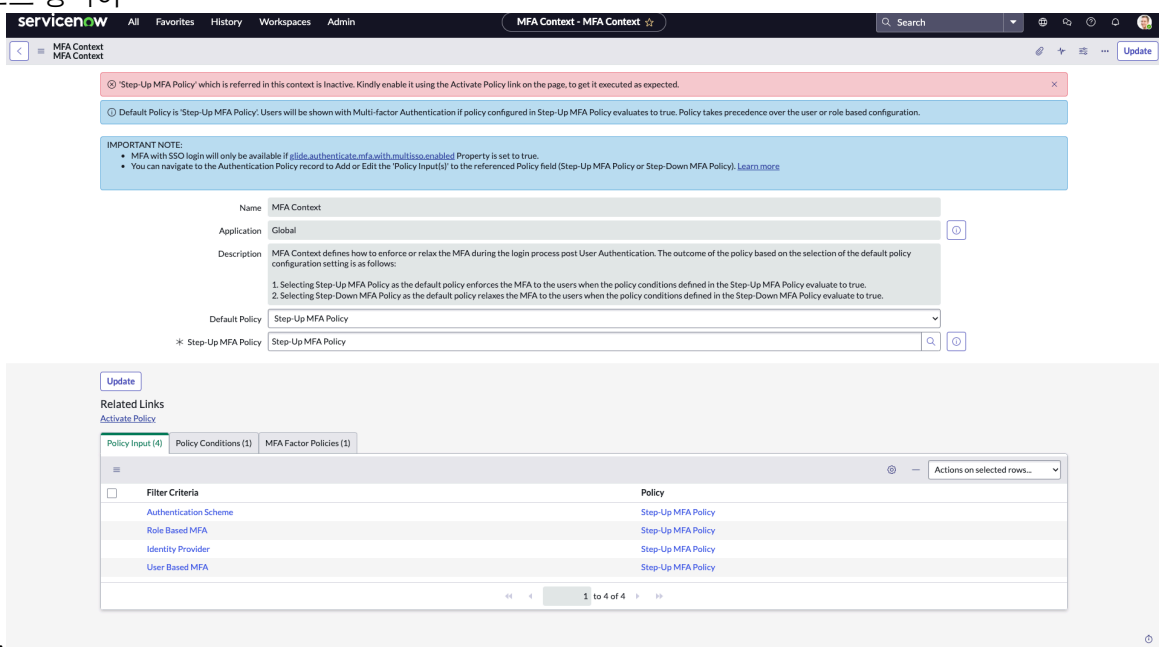
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 다단계 인증 > 속성.
2. **Multi-factor Authentication** 사용 및 SSO를 통한 **Multi-factor Authentication** 사용 확인란을 활성화합니다.



3. 저장을 클릭합니다.
4. 다음으로 이동 다단계 인증 > **MFA** 컨텍스트.
   MFA 컨텍스트 양식이



나타납니다.

기계번역

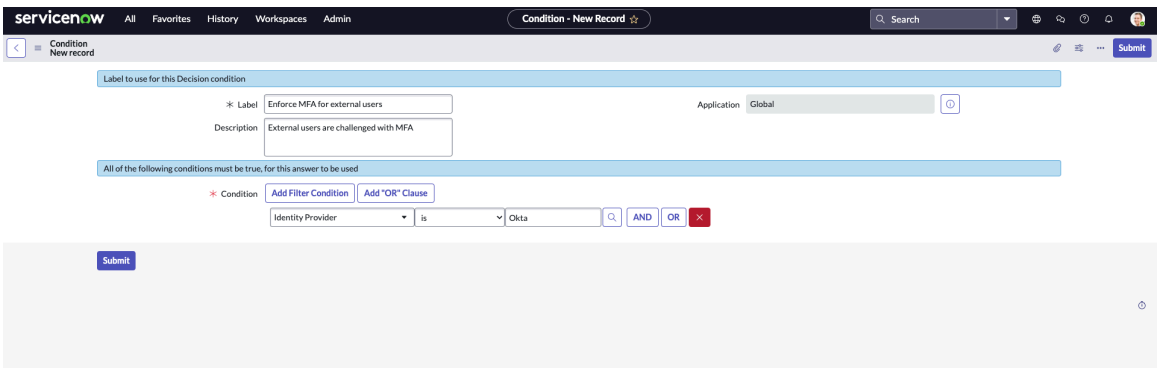
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 기본적으로 정책은 스텝업 **MFA** 정책입니다. 스텝업 **MFA** 정책에 구성된 조건이 **true**로 평가되면 사용자가 다단계 인증으로 표시됩니다. 정책은 사용자 또는 역할 기반 구성보다 우선합니다.

5. 옵션: 정책을 편집하려면 인증 정책 기록으로 돌아가서 조건을 변경한 후 다시 돌아오십시오. 인증 정책 기록으로 이동하면 참조된 정책 필드, 스텝업 **MFA** 정책 또는 스텝다운 **MFA** 정책에 "정책 입력"을 추가하거나 편집할 수 있습니다.
6. 새 정책 조건을 설정하려면 정책 조건을 클릭합니다.
7. 새로 만들기를 클릭합니다.
8. 양식의 필드에 내용을 입력합니다.

조건 양식

필드	설명
레이블	레이블에 대해 생성하려는 조건의 고유한 이름입니다.
설명	정책 조건 설명입니다.
조건	정책에 적용할 조건의 유형입니다. 필터 조건과 'OR' 절을 추가할 수 있습니다. 주: 다양한 필터 조건과 절을 추가하면 특정 사용자에 대해 MFA에 이의를 제기할 수 있습니다.



Example
조건을 설정하려면 다음 예를 고려하십시오. 외부 사용자에 대한 조건으로 ID 제공자를 사용하는 인증 체계를 사용한다고 가정합니다. 다음과 같이 조건을 설정할 수 있습니다.

a. 인증 체계를 선택하고 기준을 **Single Sign-On** 또는 사용자 이름 및 암호로 설정합니다.

이 선택 항목에 따라 사용자에게 SSO 기반 로그인 또는 사용자 이름과 암호를 지정하는 로그인 양식이 제공됩니다.

b. **ID** 제공자를 선택하고 MFA를 활성화할 IDP 기록으로 제공자를 지정합니다. 예: **Okta**.

이 선택 항목에 따라 사용자가 SSO를 사용하여 로그인하면 사용자에게 MFA가 적용되지 않습니다. 반대로 사용자가 를 사용하여 Okta로그인하면 MFA가 적용됩니다.

9. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 정보

적응형 인증

SSO(Single Sign-On)를 사용하여 다단계 인증 구성

사용자에 대한 MFA(다단계 인증) 재설정

관리자는 앱을 삭제했거나, 디바이스에 대한 액세스 권한을 잃었거나, 디바이스와 연결된 대체 MFA가 없는 사용자에 대해 MFA를 재설정할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

다음 절차에서는 ServiceNow® 관리자가 MFA 확인을 재설정하여 사용자 차단을 해제하고 사용자가 MFA를 다시 등록할 수 있도록 하는 방법을 설명합니다.

프로시저

1. 다음으로 이동 모두 > 다단계 인증 > 사용자 다단계 설정.
2. 차단을 해제하려는 사용자를 검색합니다.
3. 유효성 검사를 **false**로 설정합니다.
4. 다음으로 이동 모두 > 다단계 인증 > 웹 인증 > 사용자 공개 자격 증명**(sys_user_public_credential**.
5. 차단을 해제하려는 사용자를 검색합니다.
6. 이 사용자에 대한 모든 기록을 삭제합니다.
7. 다음으로 이동 모두 > 다단계 인증 > 사용자 최근 사용자 요인.
8. 동일한 사용자를 검색합니다.
9. 이 사용자에 대한 모든 기록을 삭제합니다.

결과

차단이 해제된 사용자가 자격 증명을 입력하고 로그인하면 MFA(다단계 인증) 사용 페이지가 표시됩니다. 사용자는 페이지의 단계에 따라 MFA를 다시 등록할 수 있습니다.

참조 주제 - 다단계 인증

다단계 인증 구성과 관련된 참조 주제입니다.

사용자 다단계 인증

사용자의 다단계 인증에 대한 세부 정보에 액세스하려면 다음으로 이동합니다. 모두 > 다단계 인증 > 사용자 다단계 설정.

사용자 다단계 인증

필드	설명
사용자	사용자의 사용자 이름
남은 항목 바이패스	사용자에 대해 남아 있는 총 바이패스 수입니다.
다단계 비밀	다단계 암호의 세부 정보입니다.
확인됨	다단계 확인 여부입니다. 값을 **false** 로 변경하면 기존 인증자 앱 설정이 무효화됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 사용자가 최근에 사용한 MFA 요인은 사용자 최근 사용한 요인 모듈에서 사용할 수 있습니다. 다음으로 이동 모두 > 다단계 인증 > 사용자 최근 사용자 요인. 자세한 내용은 사용자가 최근에 사용한 요인 문서를 참조하십시오.

다중 요소 브라우저 지문

사용자의 브라우저 지문에 대한 세부 정보에 액세스하려면 다음으로 이동하십시오. 모두 > 다단계 인증 > 다중 요소 브라우저 지문.

다중 요소 브라우저 지문

필드	설명
사용자	사용자의 사용자 이름
브라우저	사용자가 사용한 브라우저입니다.
브라우저 지문	브라우저 지문 상세 정보입니다.
브라우저 지문 쿠키	브라우저 지문 쿠키 세부 정보입니다.
브라우저 지문 쿠키 만료	브라우저 지문 쿠키 만료 상세 정보입니다.

사용자가 최근에 사용한 요인

사용자가 최근에 사용한 요인에 대한 세부 정보에 액세스하려면 다음으로 이동하십시오. 모두 > 다단계 인증 > 사용자 최근 사용자 요인.

사용자 다단계 설정

필드	설명
사용자	사용자의 사용자 이름
다단계 유형	사용자가 로그인에 사용한 다단계 유형입니다.
다단계 여부	사용자의 최근 다단계 상세 정보입니다.

다단계 인증(MFA) 사용

다단계 인증 도구를 사용하여 인스턴스에 안전하게 액세스하는 방법을 알아봅니다.

MFA로 로그인

ServiceNow 에는 TOTP(시간 기반 일회성 암호)를 지원하는 인증자 애플리케이션이 필요합니다. ServiceNow 는 다음 인증자로 MFA를 테스트합니다.

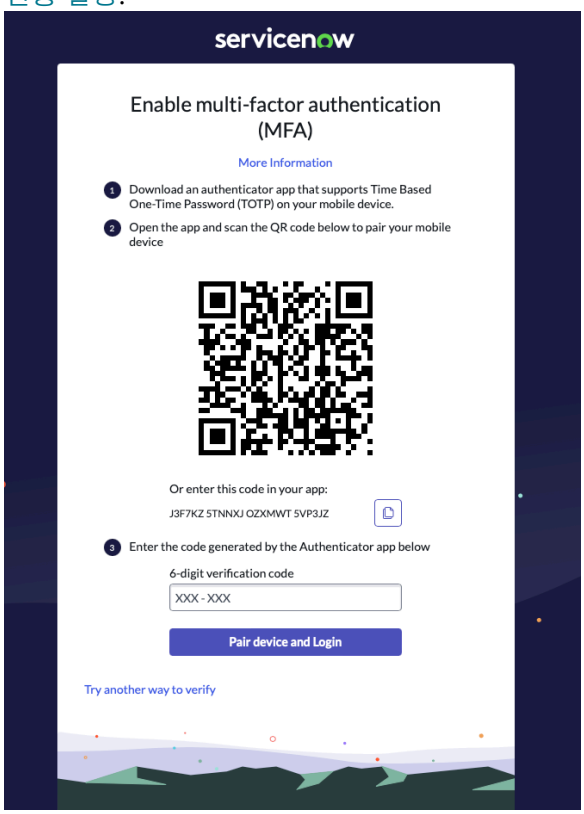
- Google 인증자
- Microsoft 인증자
- LastPass 인증기
- 인증
- 프리OTP
- 듀오
- Okta 확인

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 나열되지 않은 다른 인증자도 호환 가능할 수 있지만 에서 테스트 ServiceNow하지 않습니다.
- 브라우저별 동작 변경과 관련된 자세한 내용은 이 KB 문서를 참조하십시오.

인증 앱 등록

인증자 앱 인증자 앱을 사용하여 두 번째 인증 단계를 사용할 수 있습니다.	관리자가 인스턴스에서 MFA(다단계 인증)를 활성화한 경우 사용자 이름과 암호를 입력한 후 두 번째 인증을 요청하는 메시지가 표시됩니다. MFA 로그인 프로세스에 대한 자세한 내용은 문서를 참조하십시오 다단계 인증으로 로그인.
인증자 앱으로 확인 인증자 앱에 표시된 코드를 입력하여 로그인합니다.	두 번째 인증 양식을 구성하지 않은 경우 로그인 후 인증 앱 설정 프로세스를 안내하는 구성 페이지가 표시됩니다. 이 설정에 대한 자세한 내용은 문서를 참조하십시오 처음으로 다단계 인증 설정. 

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인증 장치 등록

인증 앱을 구성한 후 다른 인증 방법을 등록할 수 있습니다.



생체 인식 인증기

지문 또는 얼굴 인식과 같은 생체 인식 인증기를 두 번째 MFA 인증으로 사용할 수 있습니다. 관리자가 이 옵션을 허용하는 경우에는 다음의 생체 인식 인증기 등록단계를 사용하여 생체 인식 인증기를 구성할 수 있습니다.

하드웨어 키 인증기

하드웨어 키는 인증에 사용할 수 있는 물리적 보안 장치입니다. 다음 하드웨어 보안 키 등록의 단계를 사용하여 인스턴스에 사용할 하드웨어 장치를 등록할 수 있습니다.



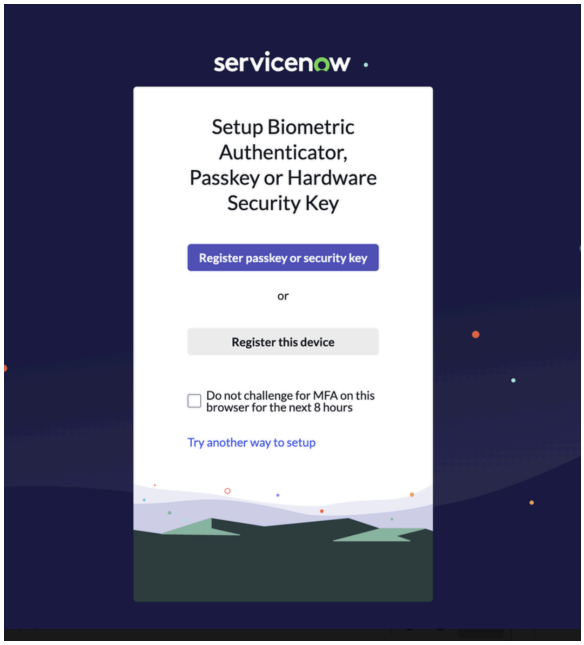
생체 인식 또는 하드웨어 키를 사용한 확인

생체 인식 또는 하드웨어 키를 사용하여 로그인합니다.

생체 인식 또는 보안 키를 사용하여 로그인합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



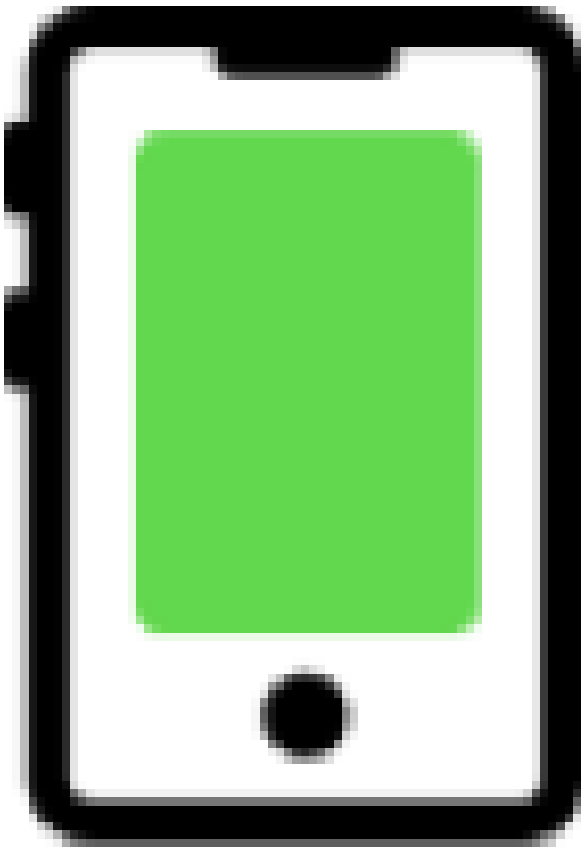
OTP용 전화번호 등록

SMS

SMS 기반 OTP를 사용하여 로그인을 시도하는 사용자에게 요구합니다.

사용자가 로그인을 ServiceNow시도하면 sys_user 기록과 연결된 휴대폰 번호로 SMS OTP가 전송됩니다. 사용자는 모바일 장치로 전송된 6자리 검증 코드를 입력하고 ID를 확인할 수 있습니다.

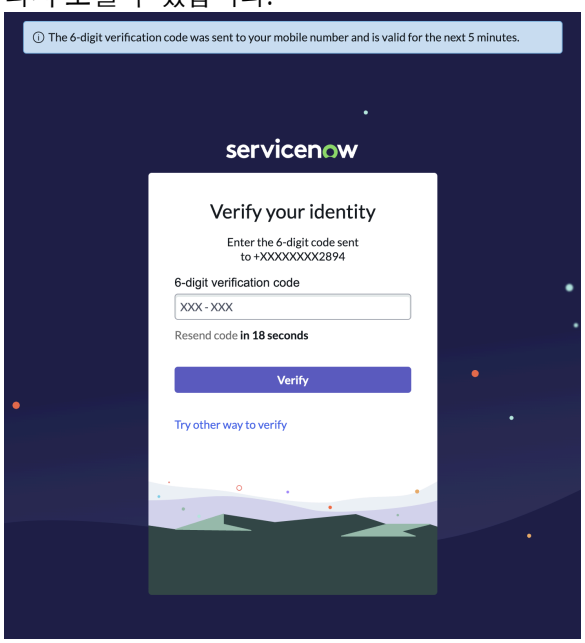
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



SMS를 사용한 확인

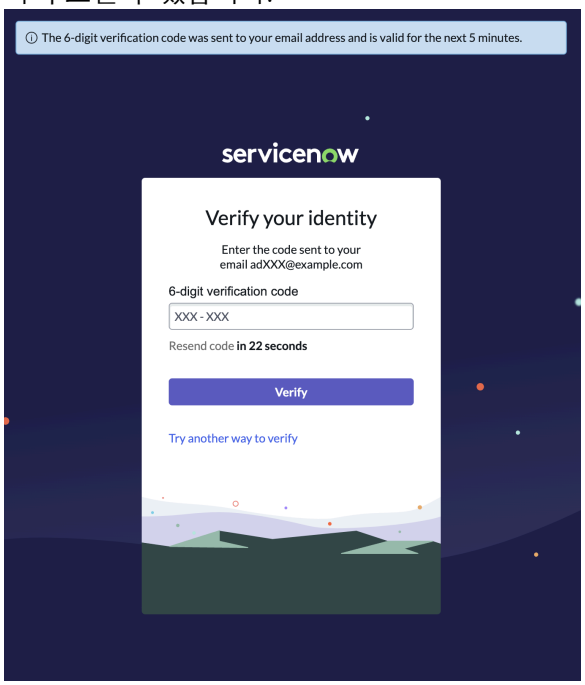
생성된 OTP를 기반으로 로그인하려면 SMS로 확인을 사용합니다.

휴대폰 번호로 전송된 6자리 코드를 입력하여 로그인합니다. 전송된 코드는 다음 5분 동안 유효합니다. 코드 다시 보내기를 사용하여 코드를 다시 보낼 수 있습니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OTP용 이메일 주소 등록

이메일 주소 이메일 기반 OTP를 사용하여 로그인을 시도하는 사용자에게 요구합니다.	사용자가 로그인을 ServiceNow시도하면 사용자와 연결된 이메일 주소로 이메일 OTP가 전송됩니다. 사용자는 모바일 장치로 전송된 6자리 검증 코드를 입력하고 ID를 확인할 수 있습니다. 
이메일로 확인 생성된 OTP를 기반으로 로그인하려면 이메일로 확인을 사용합니다.	이메일 주소로 전송된 6자리 코드를 입력하여 로그인합니다. 전송된 코드는 다음 5분 동안 유효합니다. 코드 다시 보내기를 사용하여 코드를 다시 보낼 수 있습니다. 

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

처음으로 다단계 인증 설정

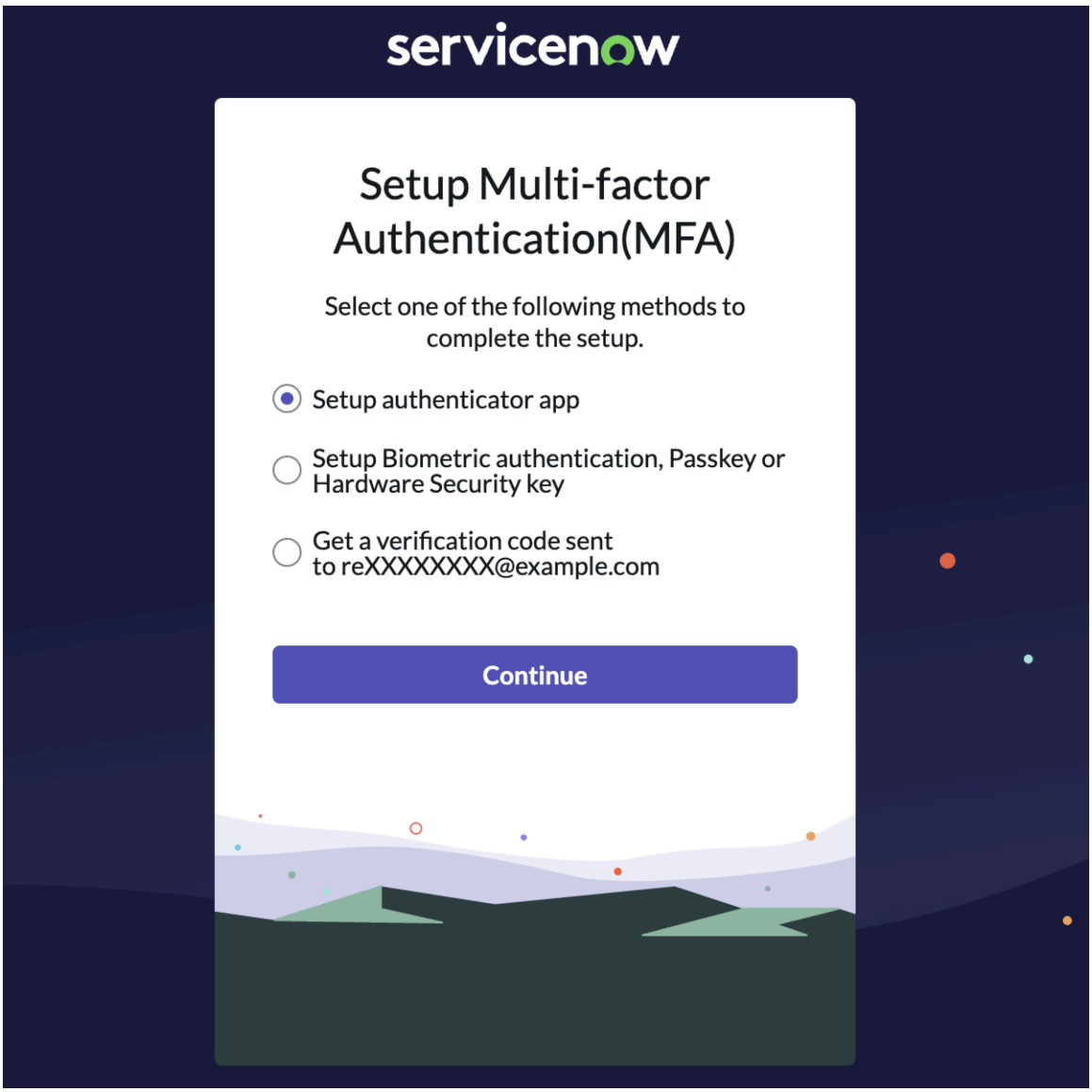
관리자가 프로파일에서 다단계 인증을 활성화했지만 아직 애플리케이션을 설정하지 않은 경우 로그인 시 설정할 수 있습니다.

시작하기 전에
필요한 역할: 없음

프로시저

1. 사용자 이름과 암호를 사용하여 인스턴스에 로그인합니다.

   다단계 인증 설정 화면이 로그인을 가로챕니다.



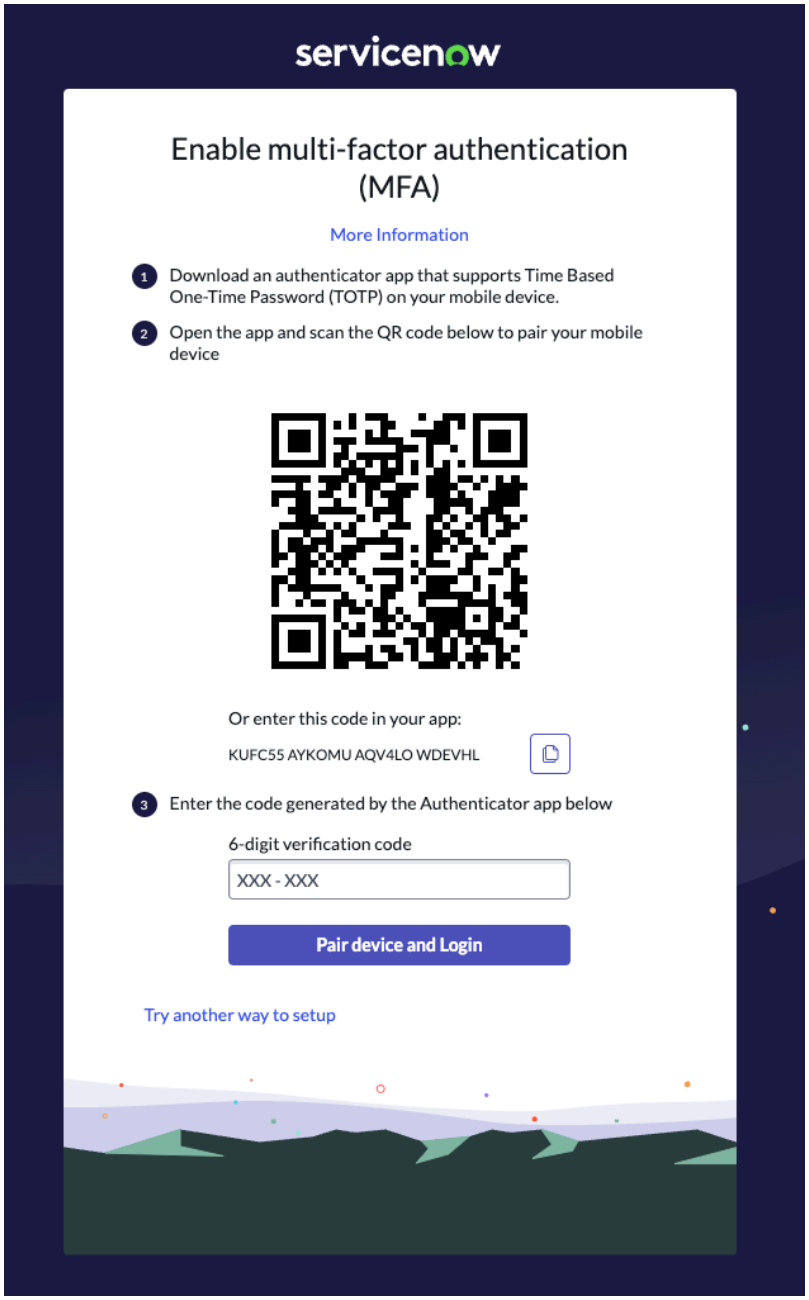
   주: 지금 설정된 인증 설정을 건너뛰려면 바이패스 설정을 클릭합니다. 관리자가 허용하는 제한된 횟수만큼 다단계 인증을 바이패스할 수 있습니다. 결국 다단계 인증을 구성해야 합니다.

2. MFA 설정을 완료하려면 다음 방법 중 하나를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 인증기 앱 설정

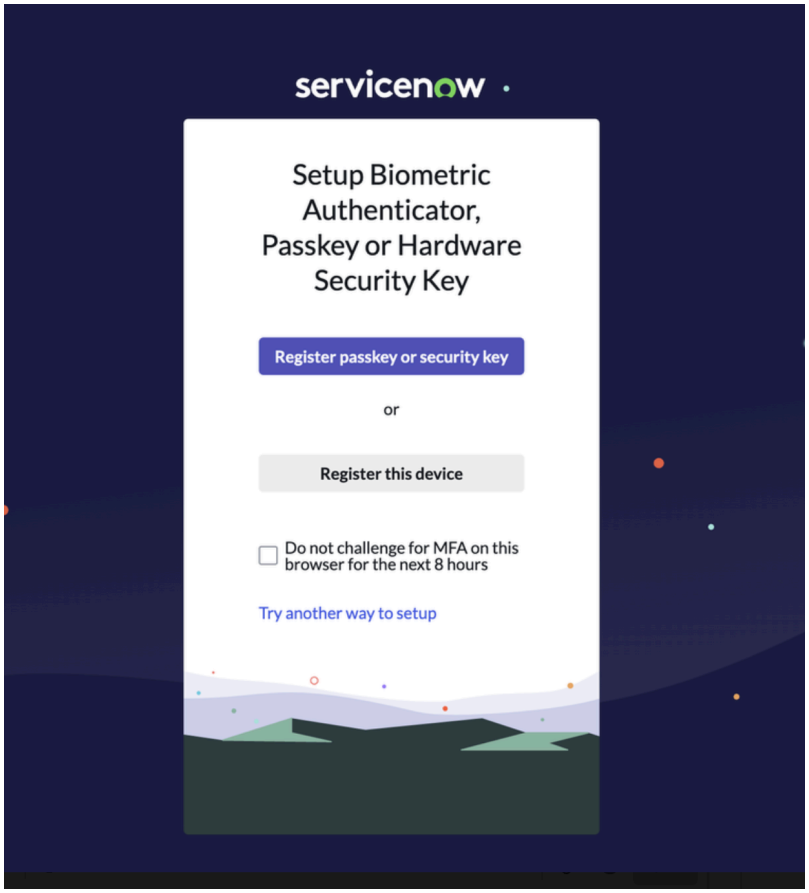
화면의 지시에 따라 장치를 페어링하고 로그인합니다.



b. 생체 인식 인증기, 통과 키 또는 하드웨어 보안 키 설정

옵션 중 하나를 선택하여 설정을 완료합니다.

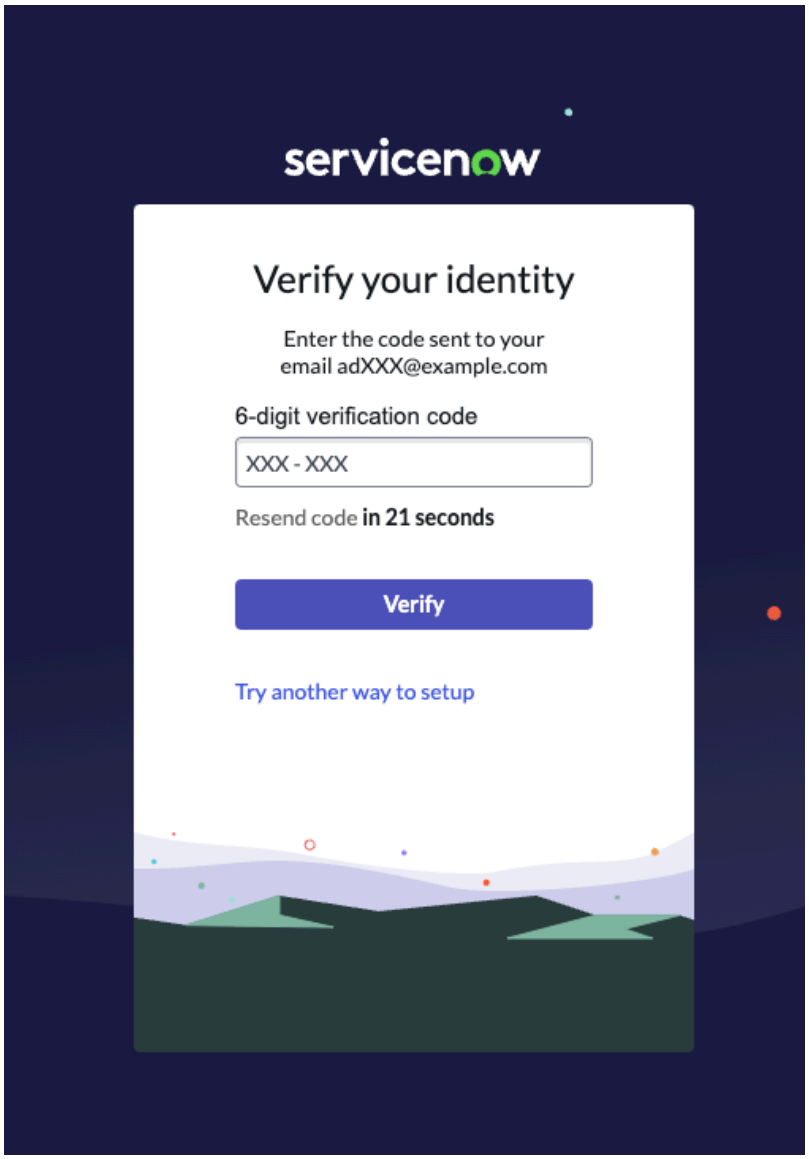
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



c. 이메일로 전송된 검증 코드 받기

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이메일로 전송된 검증 코드를 입력합니다.



두 설정 중 하나가 성공적으로 완료되면 인스턴스에 로그인됩니다.

사용자 프로파일에 다단계 인증 설정

사용자 프로파일 설정에서 계정에 대한 다단계 인증을 활성화합니다.

시작하기 전에

필요한 역할: 없음

인스턴스에서 다단계 인증을 사용하도록 설정해야 합니다.

주: 관리자가 다단계 인증을 사용하도록 요구할 수 있습니다. 이 경우 로그인할 때 자동으로 메시지가 표시됩니다. 처음으로 다단계 인증 설정 문서를 참조하십시오. 관리자가 다단계 인증에 옵트인할 수 있도록 허용하는 경우 아래 프로세스를 사용합니다.

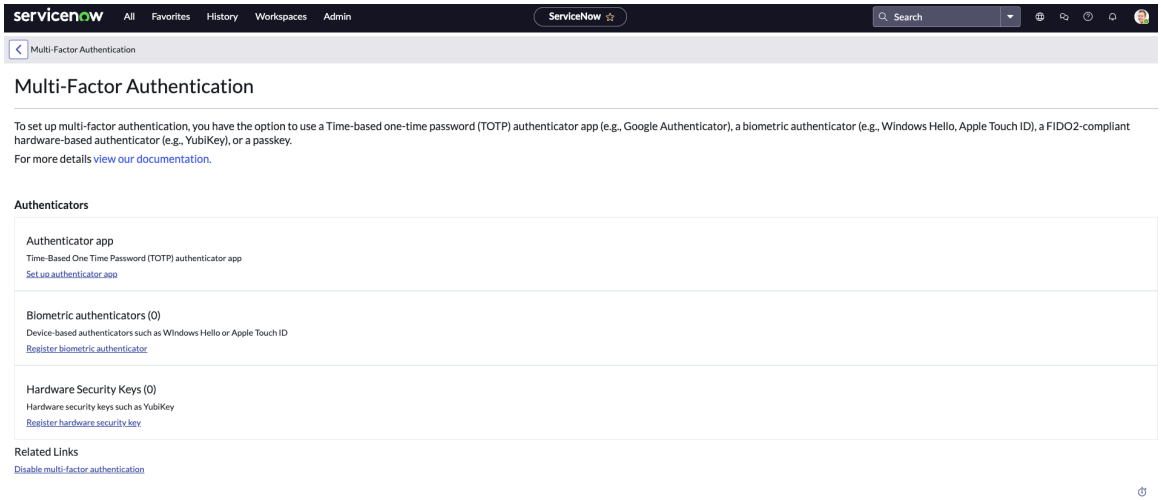
프로시저

1. 다음으로 이동 모두 > 셀프 서비스 > 내 프로필.

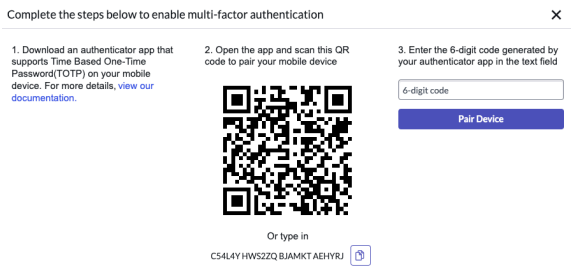
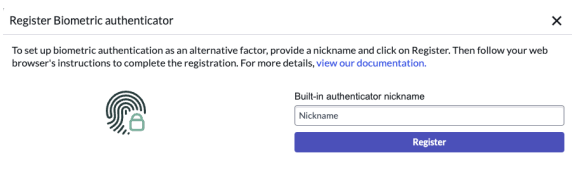
주: 인스턴스 헤더에서 사용자 이름을 클릭하여 프로필에 액세스할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

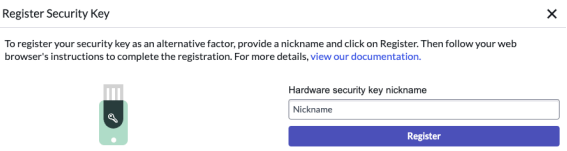
2. 사용자 프로파일의 관련 링크 섹션에서 **Multi-factor Authentication**을 클릭합니다.
3. 사용할 MFA 인증자 유형을 선택합니다.



MFA 인증자

MFA 인증자	설명
인증자 앱	TOTP(시간 기반 일회성 암호) 기반 인증기 앱 인증기 앱 설정을 선택하고 화면의 지침에 따라 인증을 위한 두 번째 단계로 인증자 앱을 등록합니다. 
생체 인식 인증기	Windows Hello 또는 Apple Touch ID와 같은 장치 기반 인증기 생체 인식 인증 등록을 선택하고 화면의 지침에 따라 인증을 위한 두 번째 단계로 인증자 앱을 등록합니다. 
하드웨어 보안 키	YubiKey와 같은 하드웨어 보안 키

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MFA 인증자	설명
	하드웨어 보안 키 등록을 선택하고 화면의 지침에 따라 인증을 위한 두 번째 단계로 인증자 앱을 등록합니다. 

결과
사용자 계정에 대해 다단계 인증이 활성화되어 있습니다. 다음에 로그인할 때 Multi-factor Authentication을 사용할 것을 요청합니다.

주: Multi-factor Authentication(다단계 인증)을 활성화한 후에는 계정에서 비활성화할 수 없습니다. 다단계 인증을 사용하지 않도록 설정해야 하는 경우 관리자에게 문의하십시오.

다단계 인증으로 로그인

인스턴스에서 관리자가 활성화한 경우 다단계 인증으로 로그인합니다.

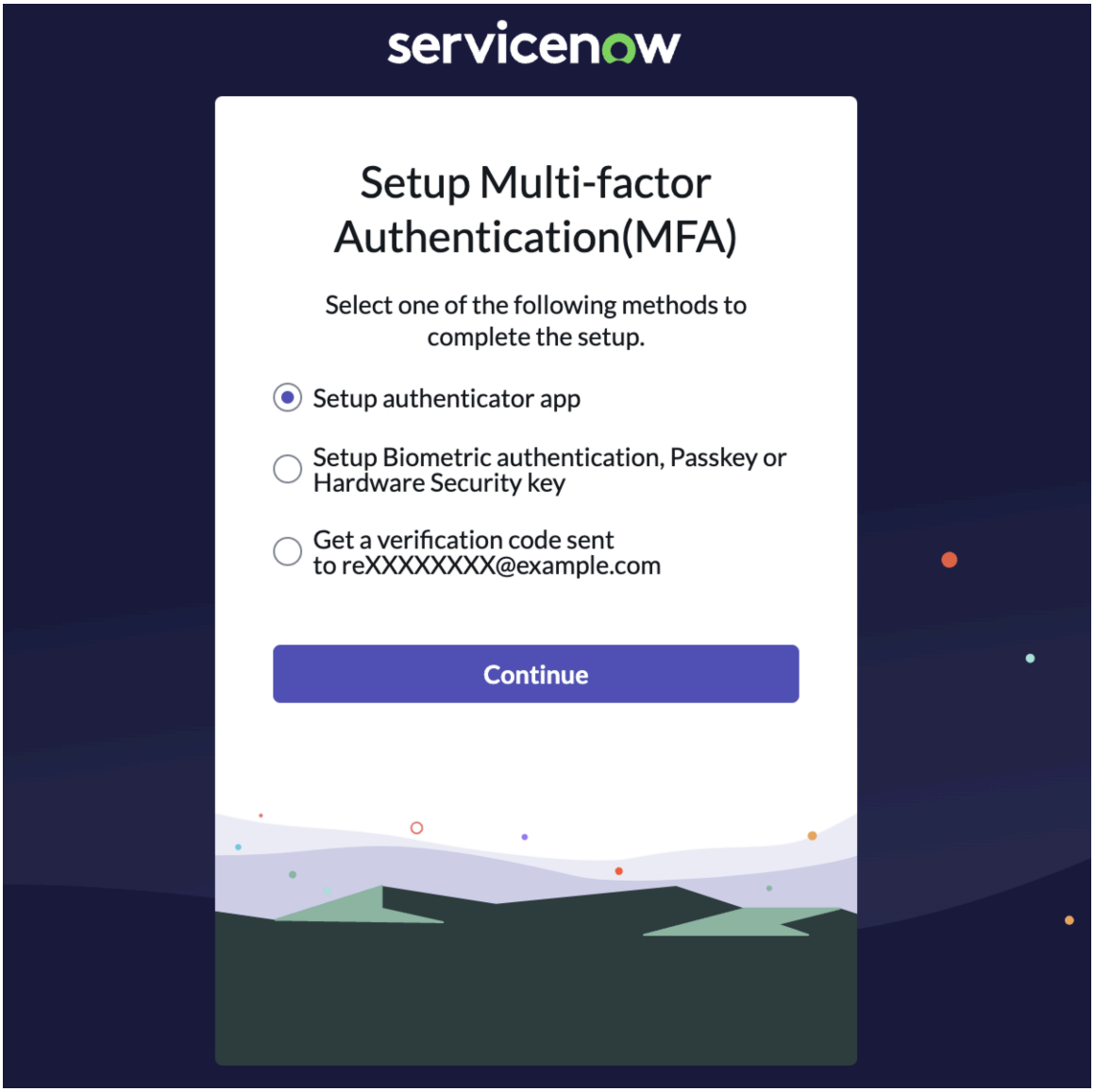
시작하기 전에
프로파일에 Multi-factor Authentication(다단계 인증)을 사용하도록 설정해야 합니다. 사용자 프로파일에서 직접 활성화하거나 관리자가 활성화할 수 있습니다.
필요한 역할: 없음

주: 마지막으로 사용한 MFA 검증 요소가 후속 로그인 시 사용자에게 자동으로 표시됩니다.

프로시저

1. 인스턴스의 URL로 이동하여 로그인 화면을 엽니다.
2. 사용자 이름과 암호를 입력합니다.
3. 로그인을 클릭합니다.
   다단계 인증 화면이 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. MFA 설정을 완료하는 방법 중 하나를 선택합니다.
   각 설정에 대한 자세한 내용은 다음 문서를 참조하십시오 처음으로 다단계 인증 설정.

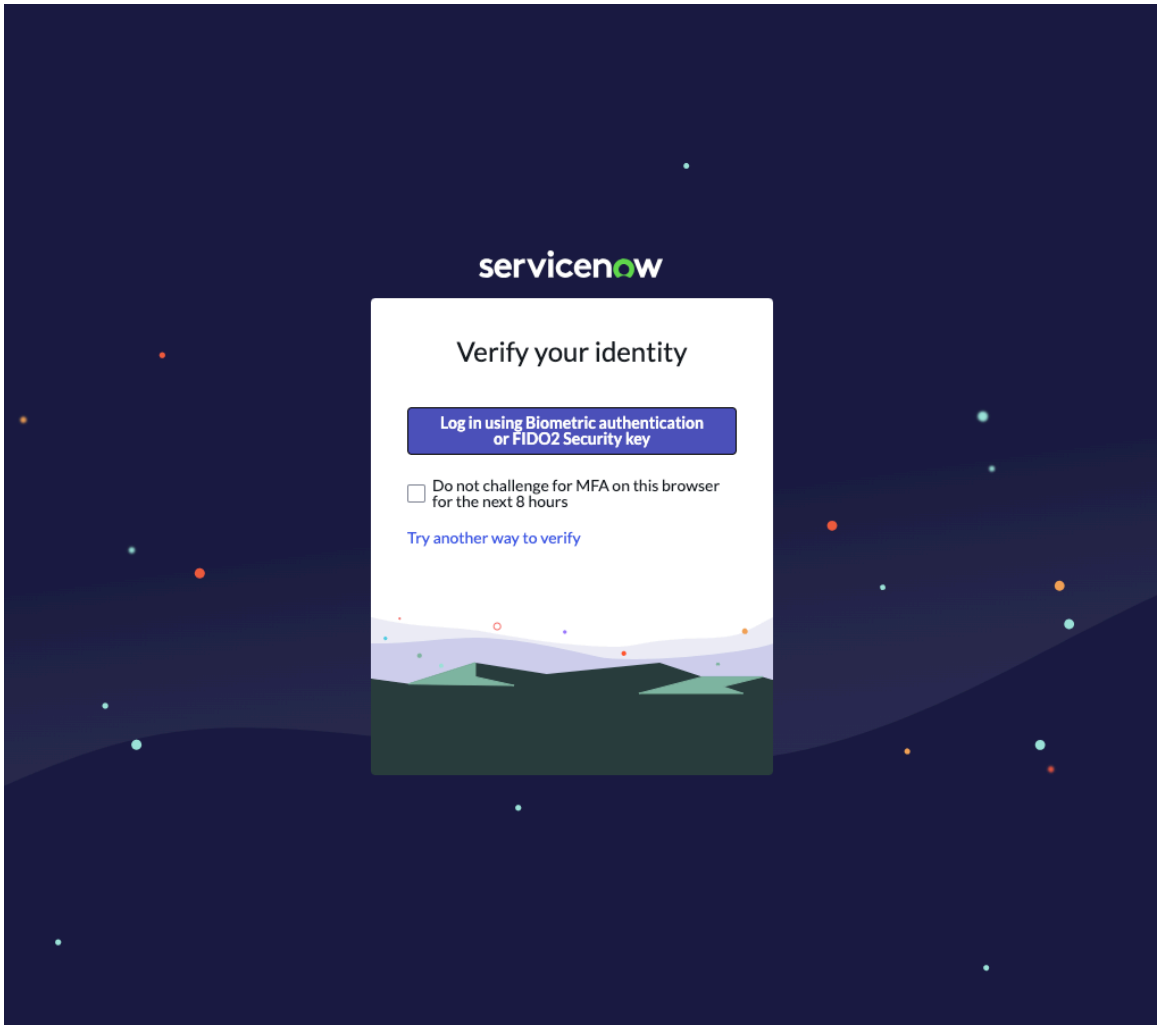
   설정을 연기하려면 설정 연기를 선택합니다. 설정을 연기할 수 있는 최대 시간 수가 화면에 표시되며 이 값은 관리자가 구성합니다.

결과
MFA를 이미 설정한 경우 사용자 이름과 암호를 입력한 후 인스턴스에 로그인할 때 최근에 사용한 요소가 표시됩니다.

Example: 최근에 사용한 **MFA** 요소

최근에 사용한 요소가 생체 인식 로그인인 경우 사용자 이름과 암호를 사용하여 로그인하면 생체 인식 MFA 설정 화면이 직접 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

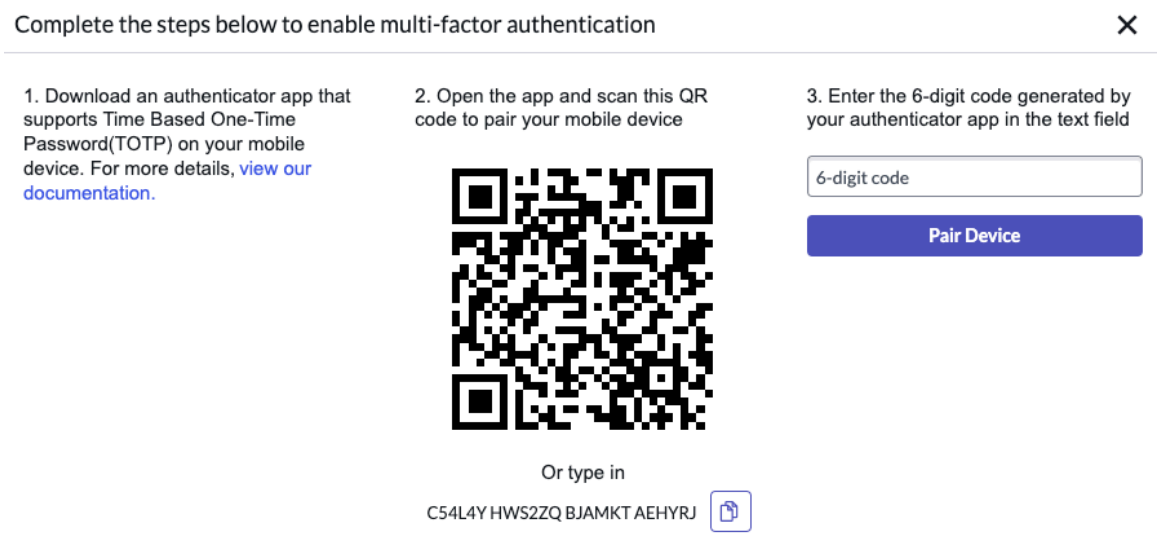


인증 애플리케이션

외부 공급업체 인증자 애플리케이션을 사용하여 임시 MFA 패스 코드를 생성합니다.

인증자 애플리케이션은 임시 암호를 생성하는 타사 소프트웨어입니다. 이러한 암호를 암호와 함께 사용하여 다단계 인증(MFA)이 필요한 인스턴스에 로그인할 수 있습니다.

관리자가 인스턴스에서 MFA를 활성화한 경우 로그인 시 사용자와 암호를 입력한 후 암호를 입력하라는 메시지가 표시됩니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow 에는 TOTP(시간 기반 일회성 암호)를 지원하는 인증자 애플리케이션이 필요합니다.

ServiceNow 는 다음 인증자로 MFA를 테스트합니다.

- Google 인증자
- Microsoft 인증자
- LastPass 인증기
- 인증
- 프리OTP
- 듀오
- Okta 확인

주: 나열되지 않은 다른 인증자도 호환 가능할 수 있지만 에서 테스트 ServiceNow하지 않습니다.

인증자 앱 변경

장치에서 인증자 앱을 변경하는 새 코드를 생성합니다.

시작하기 전에

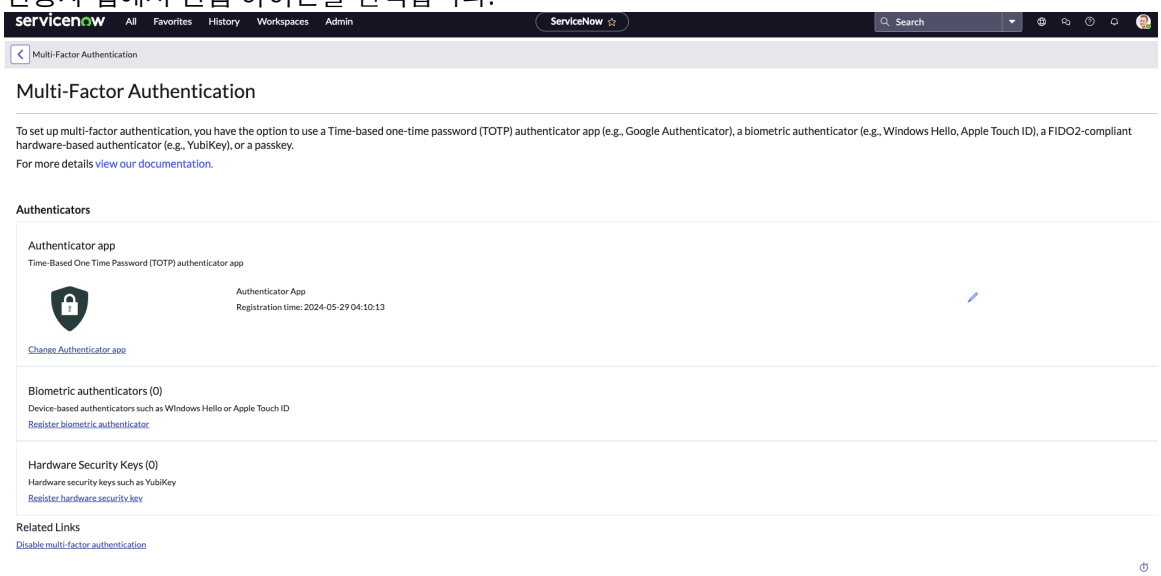
프로파일에 Multi-factor Authentication(다단계 인증)을 사용하도록 설정해야 합니다. 사용자 프로파일에서 직접 활성화하거나 관리자가 활성화할 수 있습니다.
필요한 역할: 없음

프로시저

1. 다음으로 이동 모두 > 셀프 서비스 > 내 프로필.

   주: 인스턴스 헤더에서 사용자 이름을 클릭하여 프로필에 액세스할 수도 있습니다.

2. 사용자 프로파일의 관련 링크 섹션에서 **Muti-factor Authentication**을 클릭합니다.
3. 인증자 앱에서 편집 아이콘을 선택합니다.



4. 인증기 코드 변경 창에서 변경을 클릭합니다.
5. 화면의 지시에 따라 인증자 앱을 장치에 등록합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

웹 인증

사용자는 하드웨어 키 또는 장치의 생체 인식 판독기(FIDO2)를 사용하여 인스턴스에 인증할 수 있습니다.

하드웨어 키



하드웨어 키는 인증에 사용할 수 있는 물리적 하드웨어입니다. 하드웨어 키는 인증을 제공하기 위해 장치의 포트에 삽입됩니다. 하드웨어 키 등록에 대한 자세한 내용은 문서를 참조하십시오 하드웨어 보안 키 등록.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

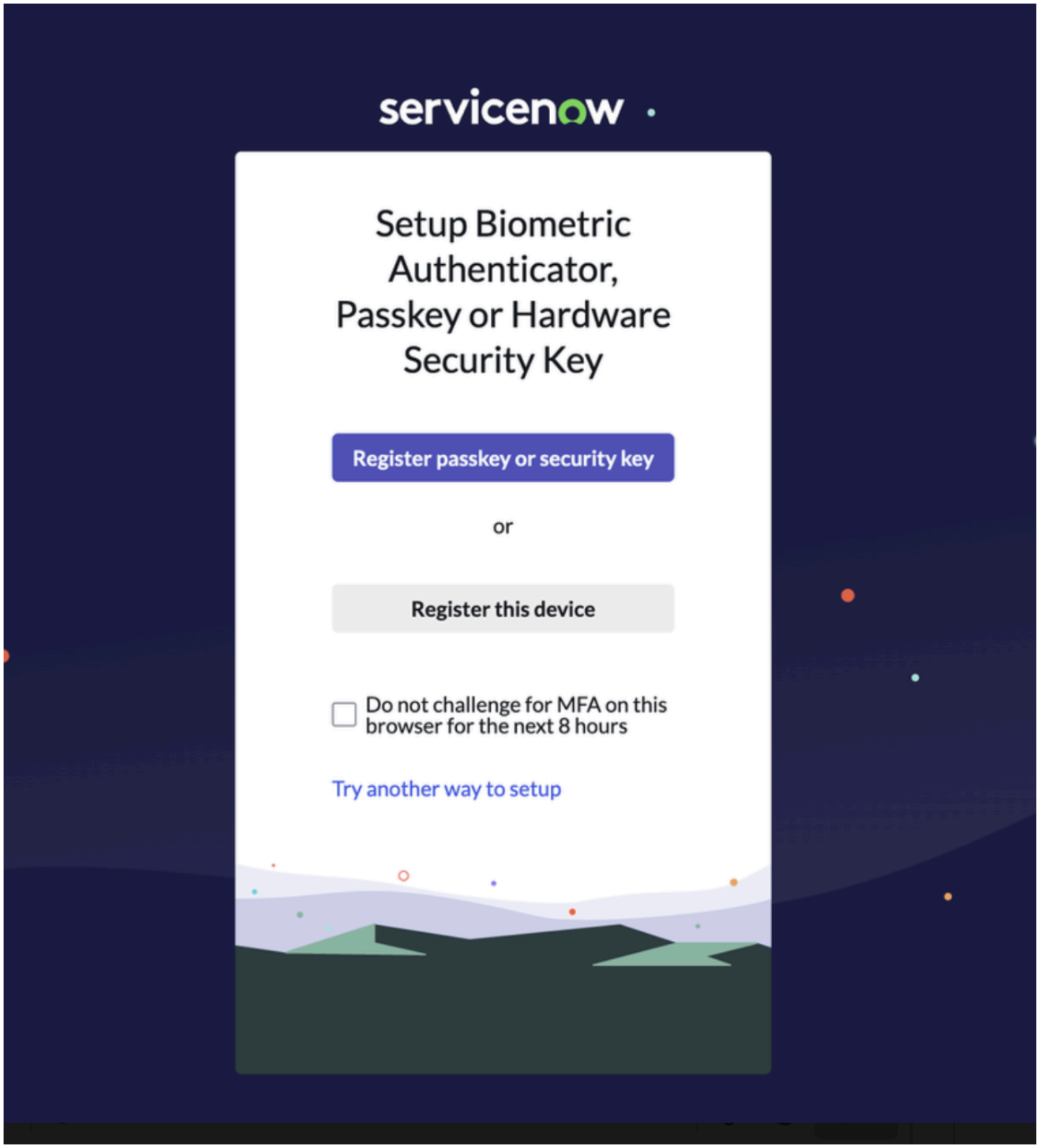
생체 인식



생체 인식 인증기는 지문 또는 얼굴 인식을 사용하여 사용자를 식별합니다. 사용자는 장치에서 이러한 인증기를 다단계 로그인 프로세스의 일부로 사용할 수 있습니다. 생체 인식 인증기 등록에 대한 자세한 내용은 을 참조하십시오 생체 인식 인증기 등록.

인스턴스를 인증하고 인증할 두 번째 요소를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



생체 인식 인증기 등록

다단계 인증 로그인의 일부로 사용할 생체 인식 인증기를 등록합니다.

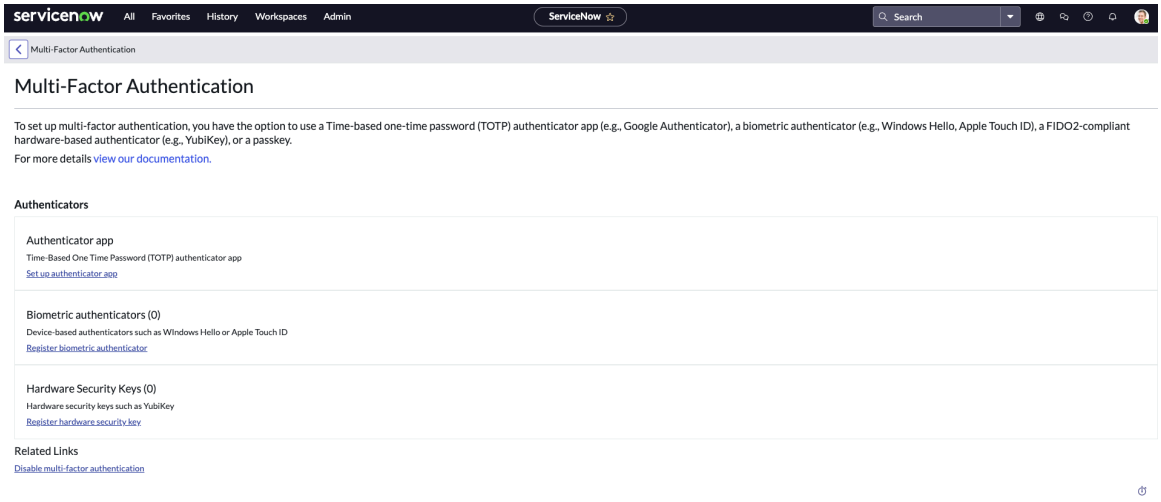
시작하기 전에

필요한 역할: 없음

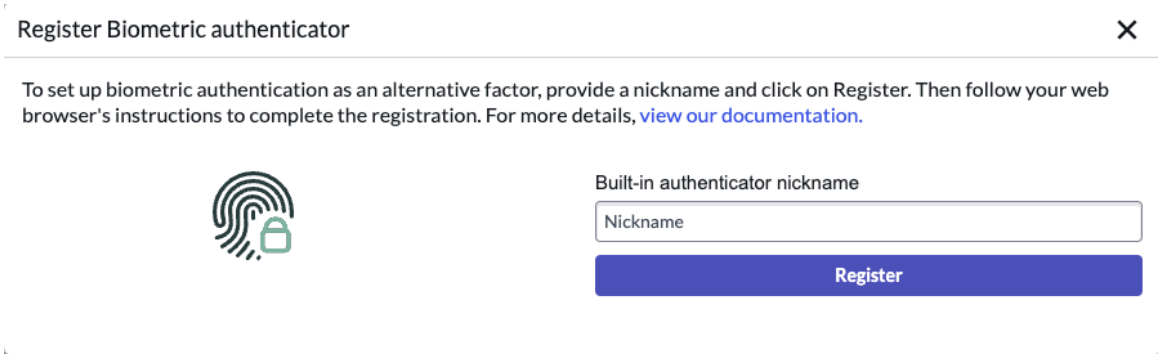
프로시저

1. 다음으로 이동 모두 > 셀프 서비스 > 내 프로필.
2. 관련 링크 아래에서 **Multi-factor Authentication**을 클릭합니다.
   다단계 인증 페이지가 열립니다.
3. 생체 인식 인증 등록을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

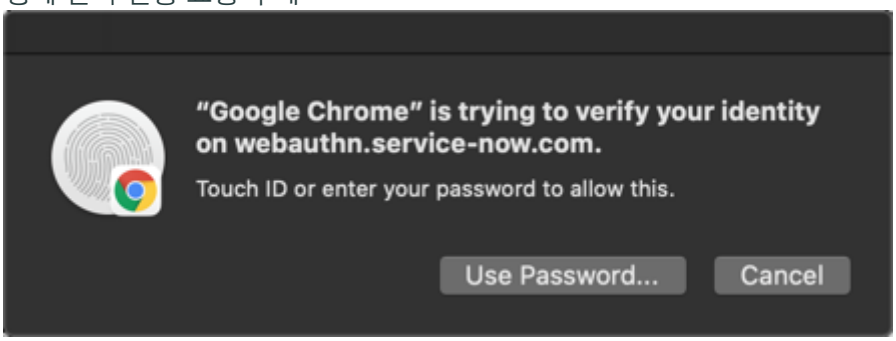


4. 인증자의 닉네임을 입력하고 등록을 클릭합니다.



5. 메시지가 표시되면 화면의 지시에 따라 생체 인식 인증기로 인증합니다.
이 메시지는 특정 인증자에 따라 달라집니다.

생체 인식 인증 요청의 예



성공적으로 인증되면 확인 창이 표시됩니다. X를 클릭하여 확인을 닫습니다.

결과
생체 인식 인증기가 등록되었습니다. 다단계 인증 페이지에서 생체 인식 인증기가 나열된 것을 볼 수 있습니다.

하드웨어 보안 키 등록

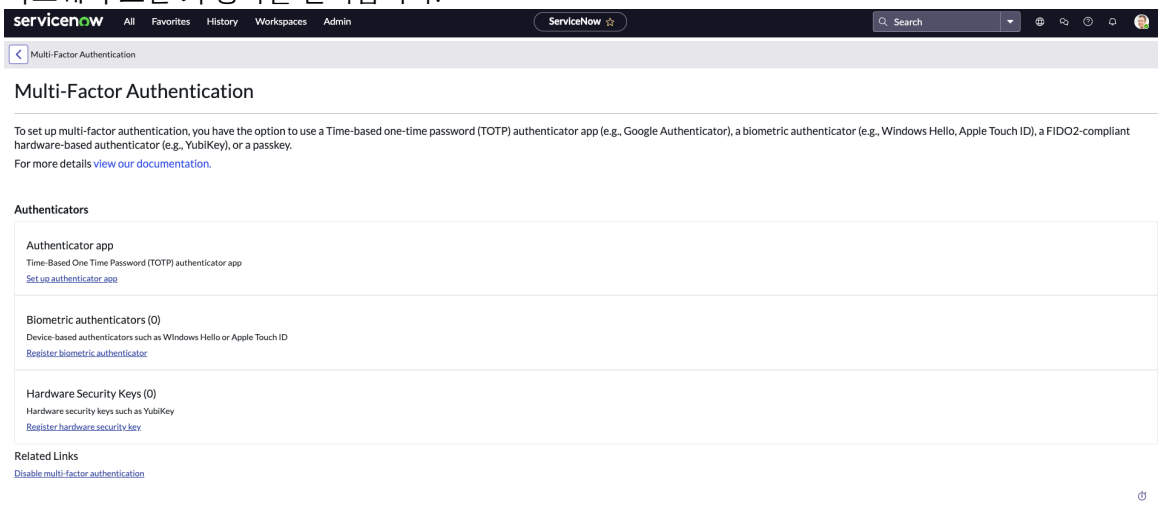
다단계 인증 로그인의 일부로 사용할 하드웨어 키를 등록합니다.

시작하기 전에
필요한 역할: 없음

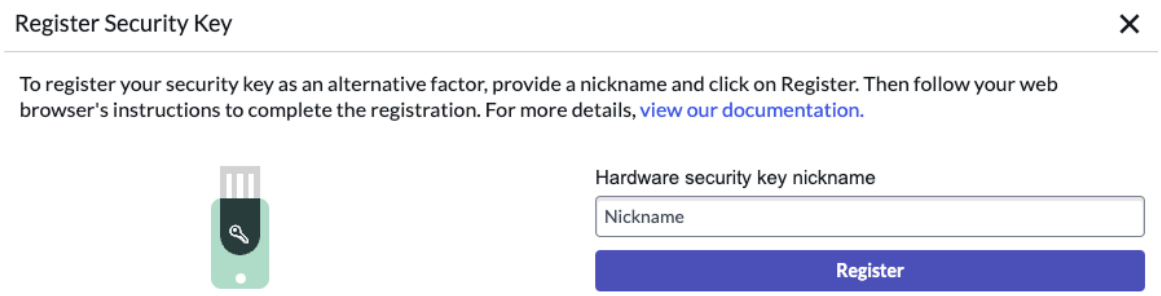
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 셀프 서비스 > 내 프로필.
2. 관련 링크 아래에서 **Multi-factor Authentication**을 클릭합니다.
   Multi-factor Authentication(다단계 인증) 페이지가 열립니다.
3. 하드웨어 보안 키 등록을 클릭합니다.



4. 하드웨어 키의 닉네임을 입력하고 등록을 클릭합니다.



5. 메시지가 표시되면 하드웨어 보안 키를 삽입하고 활성화합니다.
   성공적으로 인증되면 확인 창이 표시됩니다. X를 클릭하여 확인을 닫습니다.

결과
하드웨어 키가 등록되었습니다. Multi-factor Authentication(다단계 인증) 페이지에 나열된 하드웨어 키를 볼 수 있습니다.

MFA 메트릭

다양한 MFA 메트릭을 보고 MFA 채택 및 사용을 이해합니다.

MFA 관련 메트릭은 Security Center에서 사용할 수 있습니다. Security Center는 스토어에서 다운로드할 수 있는 무료 애플리케이션입니다 ServiceNow . Security Center에 대한 자세한 내용은 을 참조하십시오 보안 센터 방문.

Security Center에서 페이지 맨 위에 있는 표시줄을 사용하여 보안 모니터링 콘솔 섹션 사이를 이동하고 보안 메트릭 탭을 선택합니다.

MFA 메트릭은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- MFA에 등록된 사용자: MFA를 사용하기 위해 등록된 총 사용자 수입니다.
- MFA 바이패스를 사용하는 사용자: 다단계 인증을 바이패스하는 총 사용자 수입니다.
- 높은 권한의 비 MFA 사용자: MFA를 사용하지 않는 높은 권한의 총 사용자 수입니다.
- 활성 MFA 사용자: 인스턴스에서 활성 상태인 총 MFA 사용자 수입니다.
- 잠긴 MFA 사용자: 인스턴스에서 잠긴 MFA 사용자의 총 수입니다.
- MFA의 보호를 받지 않는 로컬 로그인: MFA 없이 로그인한 사용자입니다.

보안 메트릭에 대한 자세한 내용은 다음 문서를 참조하십시오 보안 메트릭.

다중 제공자 1회 사용자 인증(SSO)

외부 SSO를 통해 조직은 여러 SSO IdP(ID 공급자)를 사용하여 인증을 관리할 뿐만 아니라 로컬 데이터베이스(기본) 인증을 유지할 수 있습니다.

통합은 단일 인스턴스에서 로컬 및 외부 인증 방법의 모든 조합을 지원합니다.

- SAML 2.0
- 다이제스트 인증
- OpenID 커넥트

다중 제공자 SSO를 설정하려면 속성 구성, IdP(자격 증명 제공자) 생성, SSO를 사용하도록 사용자 구성 등 여러 단계를 수행해야 합니다.

예를 들어 전 세계에 분산된 기업은 직원에 대해 하나의 SSO 제공자, 벤더에 대해 다른 SSO 제공자, 관리자에게는 로컬 데이터베이스 인증이 필요할 수 있습니다. 또는 회사에서 동일한 인스턴스에 SAML 2.0 및 다이제스트 토큰 인증 솔루션을 구현할 수 있습니다.

복수 제공자 SSO 플러그인 활성화

이러한 통합에는 통합 - 다중 제공자 1회 사용자 인증 설치 관리자 (com.snc.integration.sso.multi.installer) 플러그인이 필요합니다.

시작하기 전에
필요한 역할: admin.

com.snc.integration.sso.multi.installer 플러그인은 OIDC, SAML 및 다이제스트에도 사용할 수 있습니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 통합 - 다중 제공자 1회 사용자 인증 설치 관리자 (com.snc.integration.sso.multi.installer) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

> 주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

복수 제공자 SSO 속성, 테이블 및 스크립트

통합 - 다중 제공자 1회 사용자 인증(SSO) 설치 관리자 플러그인에는 다음과 같은 시스템 속성, 테이블 및 스크립트가 포함됩니다.

속성

복수 제공자 SSO는 다음 시스템 속성을 추가합니다.

복수 제공자 **SSO** 속성

이름	설명
glide.authenticate.multisso.debug	복수 제공자 SSO 통합에 대한 디버그 로깅을 활성화(true) 또는 비활성화(true)합니다. • 유형: true | false • 기본값: false
glide.authenticate.multisso.enabled	복수 제공자 SSO를 활성화(true) 또는 비활성화(false)합니다. • 유형: true | false • 기본값: false 주: 인스턴스에서 계정 복구(ACR)도 활성화되어 있는 경우 이 속성을 아니오로 설정해도 다중 제공자 SSO가 비활성화되지 않습니다. 사용자 이름 및 암호로 로그인하려면 속성을 사용하여 *glide.sso.acr.enabled* ACR도 사용하지 않도록 설정해야 합니다. 이 속성에 대한 자세한 내용은 계정 복구 속성 문서를 참조하십시오.
glide.authenticate.multissov2_feature.enabled	이 속성은 인스턴스에서 MultiSSOv2 버전을 사용할 수 있는지 여부를 결정합니다.

테이블

복수 제공자 SSO는 다음 테이블을 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

복수 제공자 **SSO** 테이블

이름	설명
SSO 속성 [sso_properties]	각 IdP, 스키마, 공통 SSO 데이터 등에 대한 데이터를 저장합니다.
SAML 2 업데이트 1 속성 [saml2_update1_properties]	SAML 인증서와 같은 SAML 2.0 업데이트 1 구성에 대한 데이터를 저장합니다.
다이제스트 속성 [digest_properties]	다이제스트 토큰 인증 구성에 대한 데이터를 저장합니다.
SSO 페더레이션 [sso_federation]	각 SSO 페더레이션에 대한 데이터를 저장합니다.
OIDC ID 제공자 [oidc_identity_provider]	Open ID 커넥트 기반 ID 제공자에 대한 데이터를 저장합니다.

스크립트

복수 제공자 SSO는 다음 스크립트를 추가합니다.

복수 제공자 **SSO** 스크립트

이름	설명
MultiSSO	고객이 회사 단위로 정의된 SSO 유형을 가질 수 있도록 합니다.
MultiSSOLogin	각 도메인이 고유한 로그인 스크립트를 가질 수 있도록 허용합니다.
MultiSSOLogout	각 도메인이 자체 로그아웃 스크립트를 가질 수 있도록 허용합니다.
MultiSSO_OIDC_custom	사용자가 OIDC 연결을 위한 사용자 지정 1회 사용자 인증(SSO) 스크립트를 정의할 수 있습니다.
MultiSSO_OIDC_logout_custom	사용자가 OIDC 연결에 대한 사용자 지정 로그아웃 스크립트를 정의할 수 있습니다.
MultiSSO_Abstract_Core	모든 다중 제공자 SSO 클래스에 대한 기본 클래스를 제공합니다.
MultiSSO_ClientHelper	복수 제공자 SSO를 위한 클라이언트 호출 가능 유틸리티 함수를 제공합니다.
MultiSSO_DigestedToken	다이제스트된 토큰 인증을 위한 기본 시스템 논리를 제공합니다.
MultiSSO_SAML2_Update1	멀티 테넌트 Single Sign-On에 대한 SAML 2.0 업데이트 1 인증을 처리하는 논리를 제공합니다.

복수 제공자 **SSO** 구성

다중 제공자 SSO를 설정하려면 속성 구성, IdP(자격 증명 제공자) 생성, SSO를 사용하도록 사용자 구성 등 여러 단계를 수행해야 합니다.

각 구성에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 복수 제공자 SSO(SAML) IdP 인증 플로우
- 복수 제공자 SSO 속성 구성
- 외부 ID 제공자 생성
- 복수 제공자 SSO에 대한 사용자 구성

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

복수 제공자 SSO 속성 구성

SSO 속성을 구성하고 시스템 속성 테이블에 속성을 추가하여 IdP 포함 목록을 구성합니다.

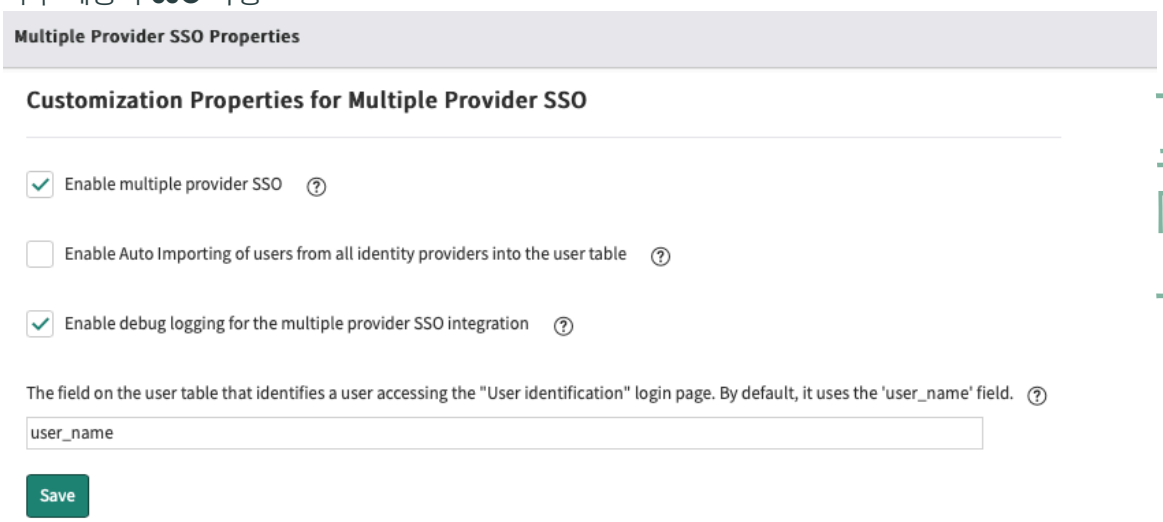
시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > 관리 > 속성.
2. 복수 제공자 **SSO** 사용 확인란을 선택합니다.
   이 선택은 로그인 페이지에 외부 로그인 사용 링크를 추가합니다.
3. IdP의 사용자로 사용자 테이블을 업데이트하려면 자동 임포트 사용 옵션을 선택합니다.
4. 디버그 메시지가 컨텐츠 프레임 하단에 표시되도록 하려면 복수 제공자 **SSO** 통합에 대한 디버그 로깅 사용 확인란을 선택합니다.
   디버그 로깅 기능을 활성화하면 성능이 저하되고 디스크 공간을 사용하여 로그를 생성합니다.
5. 사용자 **ID** 로그인 페이지에 액세스하는 사용자를 식별하는 사용자 테이블의 필드 속성에 IdP가 사용자를 식별하는 데 사용하는 값이 포함된 사용자 테이블의 필드를 입력합니다. 기본값은 **user_name**입니다.

   기본값은 **user_name**입니다.

   복수 제공자 **SSO** 속성

6. 저장을 클릭합니다.
7. 사용자에게 인스턴스에 로그인할 때 외부 로그인 사용 링크를 클릭하도록 지시합니다.

관련 정보

SAML 사용자 프로비저닝

외부 ID 제공자 생성

복수 제공자 SSO 속성을 구성한 후 새 SAML 2.0 또는 다이제스트 토큰 신원 확인 제공자를 업데이트하거나 작성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. ID 제공자 기록을 편집하려면 기록을 클릭합니다.
   - 다이제스트 토큰 구성의 경우 속성을 수동으로 업데이트합니다.
   - SAML2 업데이트 1 구성의 경우 **ID** 제공자 메타데이터 임포트 관련 링크를 사용하여 ID 제공자 메타데이터를 자동으로 업데이트하거나 속성을 수동으로 업데이트합니다.
   - OpenID Connect 구성의 경우 속성을 수동으로 업데이트합니다.
3. 새 ID 공급자를 만들려면 새로 만들기를 클릭합니다.
   - 다이제스트 토큰 구성의 경우: 다이제스트 **SSO** 를 클릭하고 다중 제공자 SSO(Single Sign-On)에 대한 다이제스트 속성을 입력합니다.
   - SAML2 구성의 경우: **MultiSSOV2_SAML2_custom** 클릭하고 URL에서 신원 확인 제공자 메타데이터를 XML로 가져오거나 ID 제공자 정보를 수동으로 입력합니다.



   - OpenID Connect의 경우: **OpenID Connect** 를 클릭하고 클라이언트 ID, 클라이언트 비밀 및 잘 알려진 구성 URL을 입력합니다.
4. 기본 IdP를 사용할 수 없을 때 사용되는 장애 조치 IdP로 IdP를 설정하려면 기본 확인란을 선택합니다.

   SAML 2 업데이트 1이 활성화되어 있는 경우 Fuji 릴리스로 업그레이드하면 SAML 2 업데이트 1 IdP가 기본 페일오버로 선택됩니다. 새 인스턴스에 대해 또는 SAML 2 업데이트 1이 활성화되지 않은 릴리스에서 업그레이드하는 경우 기본 페일오버 IdP가 선택되지 않습니다.

   주: 메타데이터 임포트 프로세스는 ID 제공자에 대한 인증서 기록을 자동으로 생성합니다. **x509** 인증서 모듈로 이동하여 인증서를 확인합니다.

   주: Single Sign-On에 대한 인증서는 SAML 인증서와 함께 작동하도록 항상 PEM 형식이어야 합니다.

5. 전자 서명이 활성 상태이면 ID 제공자 양식을 구성하고 전자 서명 인증용 **Assertion Consumer URL** 필드를 추가합니다.
   대부분의 경우 이 URL은 `https://YOURINSTANCE.service-now.com/consumer.do` 입니다. 그러나 전자 서명에 대한 SAML 인증을 처리하는 사용자 지정 방법을 사용하는 경우 고유한 소비자 URL을 설정할 수 있습니다. SAML 2.0 업데이트 1만 사용하고 다중 제공자 1회 사용자 인증(SSO)을 사용하지 않는 경우 전자 서명 SAML 속성으로 어설션 소비자 URL을 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SAML에 대한 인스턴스 서비스 제공자(SP) 메타데이터 작성

SSO 구성의 일부로 IdP에 제공할 인스턴스 SP 메타데이터를 생성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
IdP에서 요청을 인증하고 전달하려면 인스턴스 SP 메타데이터가 필요합니다.

프로시저

1. 설치된 SSO 플러그인을 선택합니다.

옵션	설명
복수 제공자 SSO	다음으로 이동 복수 제공자 **SSO** > **ID** 제공자. IdP를 선택하고 메타데이터 생성 버튼을 클릭합니다. 통합은 시스템 속성 설정에서 인스턴스의 SP 메타데이터를 자동으로 생성합니다.
SAML 2 SSO	다음으로 이동 **SAML 2** 1회 사용자 인증 **(SSO)** > 메타데이터. 통합은 시스템 속성 설정에서 인스턴스의 SP 메타데이터를 자동으로 생성합니다.

2. 텍스트 상자에서 SP 메타데이터를 복사합니다.

예:

```
<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:emailAddres
s</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. 인스턴스 SP 메타데이터를 IdP에 제공합니다.
예를 들어 SSOCircle을 사용하면 사용자가 SP 메타데이터를 온라인으로 제공할 수 있습니다.

복수 제공자 SSO에 대한 사용자 구성

관리자는 개별 사용자 또는 회사에 속한 모든 사용자에 대해 복수 제공자 SSO를 구성할 수 있습니다. 그룹에 대해 복수 제공자 SSO를 구성할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. 신원 확인 제공자 기록을 마우스 오른쪽 버튼으로 클릭하고 **sys_id** 복사를 선택합니다.
3. 데이터를 클립보드에 복사합니다.
4. 사용자 기록 또는 회사 기록으로 이동합니다.
5. 양식을 구성하고 **SSO** 소스 필드를 추가합니다.
6. **SSO** 소스 필드에 다음 중 하나를 입력합니다.
   - **SAML** 사용자: **sso:** 와 ID 제공자 기록의 sys_id를 차례로 입력합니다.
   - **SSO** 페더레이션 사용자: 페더레이션 입력: 페더레이션 기록 sys_id 차례입니다.
7. 업데이트를 클릭합니다.

IdP 연결 테스트

IdP에 대한 연결을 테스트하면 외부 인증을 활성화하기 전에 설정의 유효성을 검사합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Jakarta 릴리스는 팝업 창 내에서 연결 테스트를 지원합니다. 이 옵션을 사용해도 IdP가 제대로 작동하지 않으면 이 기본 설정을 해제할 수 있습니다.
MultiSSO IDP 메타데이터 새로 고침 작업은 연결을 작성, 업데이트 또는 테스트하는 동안 IdP에 대한 인증서를 가져오고 업데이트합니다.

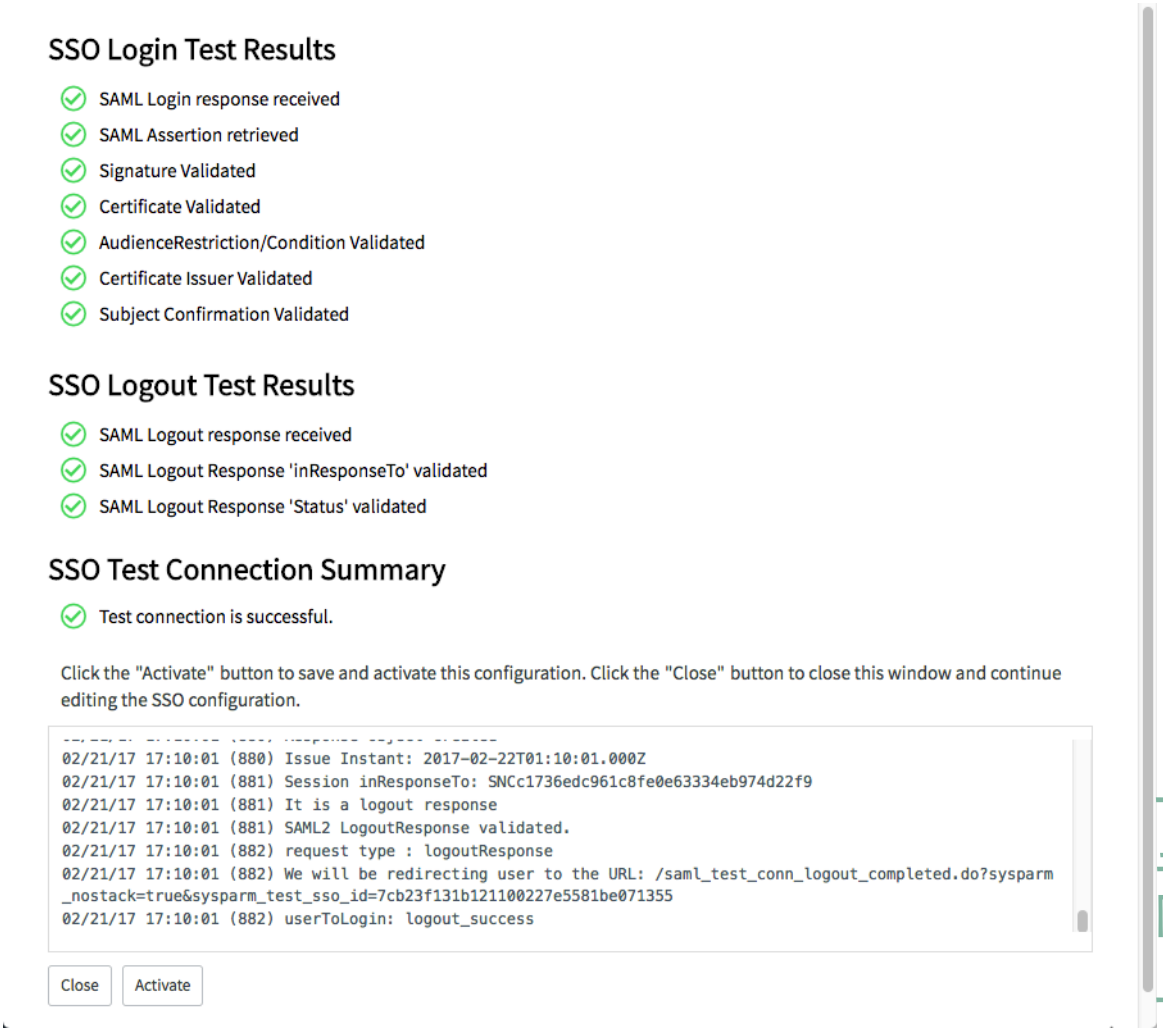
> 주: 일부 IdP 케이스의 경우 연결 테스트가 실패하면 값이 false인 glide.authenticate.multisso.test.connection.mandatory를 생성해야 하며 연결 테스트 없이 IdP를 활성화할 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. 정의된 IdP를 선택하거나 신규 를 클릭하여 새 IdP를 정의합니다.
3. 옵션: 새 IdP를 설정하는 경우 ID 제공자를 구성합니다.
4. 연결 테스트를 클릭하고 IdP에 대한 로그인 자격 증명을 입력하여 로그인을 확인합니다.
   연결 테스트가 성공적으로 완료될 때까지 IdP를 활성화할 수 없습니다. 테스트에 실패하면 업데이트하여 구성 정보를 저장할 수 있지만 이 구성을 활성화할 수는 없습니다.
5. 로그 메시지를 보려면 **SSO** 테스트 결과/요약 또는 **SSO** 테스트 로그 섹션을 사용하여 결과를 확인합니다.
   오류가 있는 경우 다음을 참조하십시오. 다중 SSO(SAML 2.0) 오류 및 수정

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 테스트가 완료되면 취소 를 클릭합니다.



일반 **IdP** 연결 오류

다음 표에서는 몇 가지 일반적인 IdP 연결 오류와 해결 방법에 대해 설명합니다.

IdP 테스트 연결 문제 해결

오류 메시지	솔루션
사용자 필드 확인에 실패했습니다. 잘못된 사용자 필드 "〈필드 이름〉"은(는) 테이블의 필드가 아닙니다sys_user.	선택한 사용자 테이블 필드의 내용이 SAML NameID 토큰과 일치하는지 확인합니다.
어설션 발급자가 잘못되었습니다.	**ID** 제공자 **URL**에 IdP에 대한 유효한 URL이 포함되어 있는지 확인합니다. 각 IdP URL은 고유해야 합니다.
AudienceRestriction 확인에 실패했습니다.	대상 **URI**에 인스턴스에 대한 유효한 URL이 포함되어 있는지 확인합니다.
IdP의 세션에서 로그아웃할 수 없습니다.	**SingleLogoutRequest** URL에 IdP의 로그아웃 서비스에 대한 유효한 URL이 포함되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

IdP 테스트 연결 문제 해결

오류 메시지	솔루션
자격 증명 키에 대해 서명이 확인되지 않았습니다.	IdP에 유효한 인증서가 설치되어 있는지 확인합니다.

SAML 관련 스크립트 문제 해결

SAML과 관련된 스크립트 문제를 해결합니다. 다중 Single Sign-On을 활성화할 때 SAML이 이미 활성화되어 있고 설치 종료를 이미 사용자 지정한 경우 스크립트 문제가 발생할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 수정된 설치, 종료 SAML2SingleSignon_update1 및 스크립트 포함 SAML2_update1 백업합니다.
2. 설치 종료 및 스크립트 포함을 모두 기준선 시스템에서 사용할 수 있는 버전으로 되돌립니다.
3. 통합 - 다중 제공자 1회 사용자 인증**(SSO)** 설치 관리자 플러그인을 활성화하거나 업그레이드합니다.
   시스템은 SAML 및 필요한 모든 파일을 SAML 2 업데이트 1로 업그레이드합니다.
4. 복수 SSO 속성 페이지를 열고 복수 제공자 **SSO** 사용 확인란을 선택하여 사용하도록 설정합니다.
5. 설치 종료 SAML2SingleSignon_update1 변경 사항을 베이스라인 스크립트 포함 MultiSSO_SAML2_Update1에 넣 고, **SAML2_update1** 스크립트 포함 변경 사항을 베이스라인 SAML2_update1 스크립트 포함에 넣습니다.

복수 제공자 SSO를 사용하여 로그인

복수 제공자 SSO를 사용하여 로그인하는 사용자에게 권장되고 가장 효율적인 방법은 특별히 구성된 URL을 사용하는 것입니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
복수 제공자 SSO가 구성되면 매개변수 문자열에 올바른 IdP를 사용하여 사용자에게 URL을 보낼 수 있습니다. 예:

/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>

사용자가 IdP 페이지에 성공적으로 로그인하면 IdP sys_id 포함된 쿠키가 브라우저에 추가됩니다. 다음에 사용자가 로그인을 시도할 때 시스템은 사용자를 IdP 서버에 로그인하도록 리디렉션하며, 자동으로 인스턴스에 로그인합니다.

URL 매개변수가 설정되지 않았거나 브라우저 캐시가 지워진 경우 사용자는 다음을 수행할 수도 있습니다.

프로시저

1. 로그인 페이지에서 외부 로그인 사용 링크를 클릭합니다.

   외부 로그인 페이지가 나타납니다. 사용자는 로컬 로그인 사용을 클릭하여 표준 로그인 페이지로 돌아갈 수 있습니다.

2. 복수 제공자 SSO 속성에서 구성한 사용자 테이블에 지정된 필드의 값을 입력합니다.

   사용자는 IdP 서버로 리디렉션되어 로그인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과
사용자가 IdP에 성공적으로 로그인하면 인스턴스에 액세스하려고 할 때마다 해당 IdP로 자동으로 리디렉션됩니다. 사용자가 다른 IdP에 액세스하도록 하려면 매개변수에 새 IdP 정보가 포함된 URL을 사용자에게 보냅니다. 사용자가 성공적으로 로그인하면 새 IdP가 쿠키의 이전 IdP를 덮어씁니다. 사용자가 성공적으로 로그인하지 않으면 이전 IdP 정보가 쿠키에 유지됩니다.

사용자가 로그인에 필요한 **ID** 제공자를 선택할 수 있도록 합니다.

SSO 페더레이션 지원을 사용하면 사용자가 로그인할 IdP를 선택할 수 있습니다.

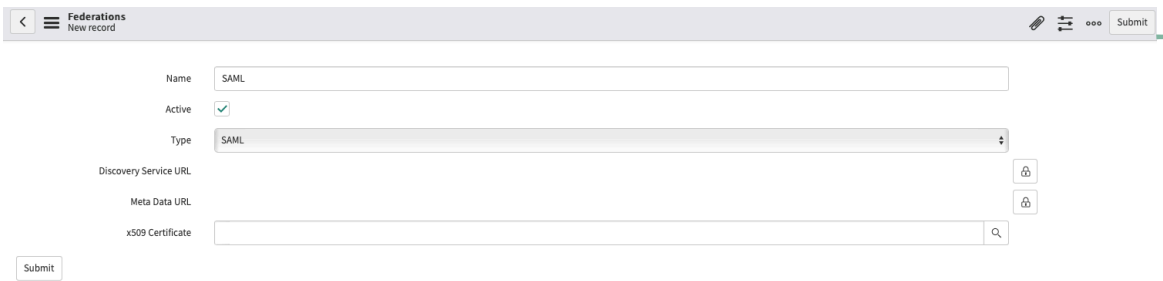
시작하기 전에
필요한 역할: 관리자

이 태스크 정보
SSO 연동은 인스턴스를 포함하여 여러 IdP 및 서비스 제공자의 메타데이터를 집계합니다. 그런 다음 페더레이션은 메타데이터를 IdP 이름 및 IdP 인증서와 같은 정보가 포함된 XML 파일로 게시합니다. 그런 다음 관리자는 XML 파일을 읽도록 인스턴스에 지시하고 필요한 모든 IdP 정보로 SSO 속성 테이블을 자동으로 채울 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > 페더레이션.
2. 새로 만들기를 클릭합니다.
3. 필드에 적절한 정보를 입력합니다(표 참조).
4. 제출을 클릭합니다.
5. 페더레이션을 구성한 후 SSO 메타데이터 새로 고침 예약된 작업을 사용하도록 설정한 다음 페더레이션 IdP에 액세스할 사용자를 구성합니다. 방금 생성한 페더레이션 기록의 sys_ID 사용합니다.

   방금 생성한 페더레이션 기록의 sys_ID 사용합니다.



   인스턴스가 SSO 속성 테이블을 IdP 정보로 채웁니다. 연합을 사용하도록 구성된 사용자가 로그인하면 구성한 검색 서비스 URL로 리디렉션됩니다. 그런 다음 IdP를 선택하고 필요한 자격 증명을 제공합니다. 또는 매개변수에 IdP가 포함된 URL을 사용자에게 보낼 수 있습니다.

사용자가 로그인에 필요한 **ID** 제공자를 선택할 수 있도록 허용

필드	설명
이름	페더레이션을 설명하는 이름을 입력합니다.
활성	인스턴스가 페더레이션에서 XML 파일을 끌어올 수 있도록 하려면 확인란을 선택합니다.
유형	이 페더레이션이 지원하는 인증 유형을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
디스커버리 서비스 URL	이 페더레이션에 대한 검색 서비스의 URL을 입력합니다. 이 사이트에서는 사용자가 IdP를 선택하고 로그인하도록 안내됩니다.
메타데이터 URL	페더레이션 메타데이터를 포함하는 XML 파일의 URL을 입력합니다.
x509 인증서	페더레이션 인증서를 선택합니다.
도메인	데이터가 속한 도메인을 선택합니다.

주: InCommon 페더레이션 ID 관리 IdP가 미리 구성되어 있습니다.

복수 제공자 SSO와 함께 사용하여 서비스 포털 **URL** 리디렉션

서비스 포털 는 시스템 속성과 스크립트 포함의 조합을 사용하여 포털에서 로그인하는 사용자의 URL 리디렉션을 시스템에서 처리하는 방법을 결정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
시스템 속성을 사용하여 기본 IdP 서비스 포털 (신원 확인 제공자)로 자동으로 리디렉션하는 경우 해당 IdP로 자동으로 리디렉션됩니다. IdP가 여러 개인 경우 서비스 포털 로그인 페이지에 외부 로그인 사용 링크를 표시합니다.

프로시저

1. Service Portal 로그인 페이지 구성
2. 로그인 후 서비스 포털로 리디렉션

계정 복구**(ACR)**

관리자는 SSO 구성 오류 또는 만료된 인증서 해결과 같은 복구 활동을 수행하도록 계정 복구(ACR)를 구성할 수 있습니다.

주: ACR을 사용하면 인스턴스에 SSO가 활성화된 경우 로컬 대화형 로그인(사용자 이름 또는 암호 기반)이 비활성화됩니다.

ACR은 다음과 같은 기능을 제공합니다.

- 1회 사용자 인증(SSO) 로그인을 바이패스하여 관리자로서 SSO 구성과 관련된 문제를 해결합니다.
- 계정 복구로 구성된 관리자 계정으로 작업을 수행하려면 SSO를 사용하여 로그인하십시오.
- ACR 흐름을 사용하면 관리자가 셀프 서비스 기능을 사용하여 복구가 필요한 경우(예: SSO 잘못된 구성, 만료된 인증서) 계정 복구 문제를 해결할 수 있습니다.
- 인스턴스에 대한 무단 액세스를 줄이고 SSO 사용 사례 외부에서 ACR을 사용할 수 있는 강력한 기반을 제공합니다.

새로운 인스턴스

새 인스턴스에서 ACR을 사용하려면 다음을 수행해야 합니다.

- 다중 SSO 플러그인(`com.snc.integration.sso.multi.installer`) 활성화
- ACR 사용(`glide.sso.acr.enabled`) - 새로운 인스턴스의 경우 기본적으로 활성화됩니다.
- SSO 속성(`glide.authenticate.multisso.enabled`)을 활성화하기 전에 관리자가 ACR 사용자로 등록해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 인스턴스에서 계정 복구(ACR)도 활성화되어 있는 경우 이 속성을 아니오로 설정해도 다중 제공자 SSO가 비활성화되지 않습니다. 사용자 이름 및 암호로 로그인하려면 속성을 사용하여 *glide.sso.acr.enabled* ACR도 사용하지 않도록 설정해야 합니다. 이 속성에 대한 자세한 내용은 계정 복구 속성 문서를 참조하십시오.

- 관리자는 ACR 사용자로 등록하기 전에 로컬 로그인을 위한 암호를 설정하고 MFA를 등록해야 합니다.

업그레이드된 인스턴스

업그레이드된 인스턴스에서 ACR을 사용하려면 다음을 수행해야 합니다.

- 다중 SSO 플러그인(`com.snc.integration.sso.multi.installer`) 활성화
- ACR 사용(`glide.sso.acr.enabled`)

주: 업그레이드된 인스턴스의 경우 관리자가 ACR을 활성화해야 합니다.

- SSO 속성(`glide.authenticate.multisso.enabled`)을 활성화하기 전에 관리자가 ACR 사용자로 등록해야 합니다.
- 관리자는 ACR 사용자로 등록하기 전에 로컬 로그인을 위한 암호를 설정하고 MFA를 등록해야 합니다.

계정 복구 사용자 구성

계정 복구를 사용하려면 하나 이상의 관리자 계정을 계정 복구 사용자로 등록해야 합니다. 하나 이상의 계정이 구성될 때까지 인스턴스에서 Single Sign-On을 활성화할 수 없습니다. 이 프로세스에 대한 자세한 내용은 계정 복구 속성 페이지에서 계정 복구 사용자 구성 문서를 참조하십시오.

주: 이미 SSO(Single Sign-On)를 사용 중인 인스턴스를 이후 릴리스로 Rome 업그레이드하는 경우, 복구 사용자가 구성되지 않아도 SSO가 계속 작동합니다.

계정 복구 구성

계정 복구 기능은 **Integration - Multiple Provider Single Sign-On Installer(com.snc.integration.sso.multi.installer)** 플러그인에 포함되어 있습니다. 이 기능은 기본적으로 사용하도록 설정됩니다. 시스템 속성을 사용하여 이 설정과 다른 계정 복구 설정을 변경할 수 있습니다. 이러한 속성에 대한 자세한 내용은 문서를 참조하십시오 계정 복구 속성.

계정 복구 정책 컨텍스트

계정 복구 사용자를 등록하고 SSO(Single Sign-On)를 활성화한 후에는 인스턴스가 모든 로컬 로그인을 제한합니다. 이 제한은 **SSO - ACR** 컨텍스트 인증 정책 컨텍스트에 정의됩니다. 컨텍스트에 대한 자세한 내용은 다음 문서를 참조하십시오 계정 복구 컨텍스트.

인증 정책 및 정책 컨텍스트의 방식과 인스턴스에서 작동하는 방식에 대한 자세한 내용은 다음 문서를 참조하십시오 적응형 인증.

계정 복구 사용자 구성

인스턴스에서 계정 복구 작업을 수행하도록 계정 복구 사용자를 구성합니다.

계정 복구 사용자는 관리자가 잘못된 SSO 구성 해결 또는 만료된 인증서 해결과 같은 계정 복구 작업을 수행하는 데 사용할 수 있는 사용자 계정입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 인스턴스에서 계정 복구를 사용하는 경우 계정 복구 사용자를 구성해야 합니다. 이 단계는 인스턴스에서 복수 제공자 SSO(Single Sign-On)를 사용하도록 설정하기 전에 필요합니다.

계정 복구 속성 페이지에서 계정 복구 사용자 구성

계정 복구 속성 페이지에서 계정 복구를 구성합니다.

시작하기 전에
필요한 역할: 관리자

새 인스턴스에서 ACR을 구성하려면 다음을 수행해야 합니다.

- 다중 SSO 플러그인(`com.snc.integration.sso.multi.installer`) 활성화
- ACR 사용(`glide.sso.acr.enabled`) - 새로운 인스턴스의 경우 기본적으로 활성화됩니다.
- SSO 속성(`glide.authenticate.multisso.enabled`)을 활성화하기 전에 관리자가 ACR 사용자로 등록해야 합니다.
- 관리자는 ACR 사용자로 등록하기 전에 로컬 로그인을 위한 암호를 설정하고 MFA를 등록해야 합니다.

업그레이드된 인스턴스에서 ACR을 사용하려면 다음을 수행해야 합니다.

- 다중 SSO 플러그인(`com.snc.integration.sso.multi.installer`) 활성화
- ACR 사용(`glide.sso.acr.enabled`)

  주: 업그레이드된 인스턴스의 경우 관리자가 ACR을 활성화해야 합니다.

- SSO 속성(`glide.authenticate.multisso.enabled`)을 활성화하기 전에 관리자가 ACR 사용자로 등록해야 합니다.

  주: 인스턴스에서 계정 복구(ACR)도 활성화되어 있는 경우 이 속성을 아니오로 설정해도 다중 제공자 SSO가 비활성화되지 않습니다. 사용자 이름 및 암호로 로그인하려면 속성을 사용하여 *`glide.sso.acr.enabled`* ACR도 사용하지 않도록 설정해야 합니다. 이 속성에 대한 자세한 내용은 계정 복구 속성 문서를 참조하십시오.

- 관리자는 ACR 사용자로 등록하기 전에 로컬 로그인을 위한 암호를 설정하고 MFA를 등록해야 합니다.

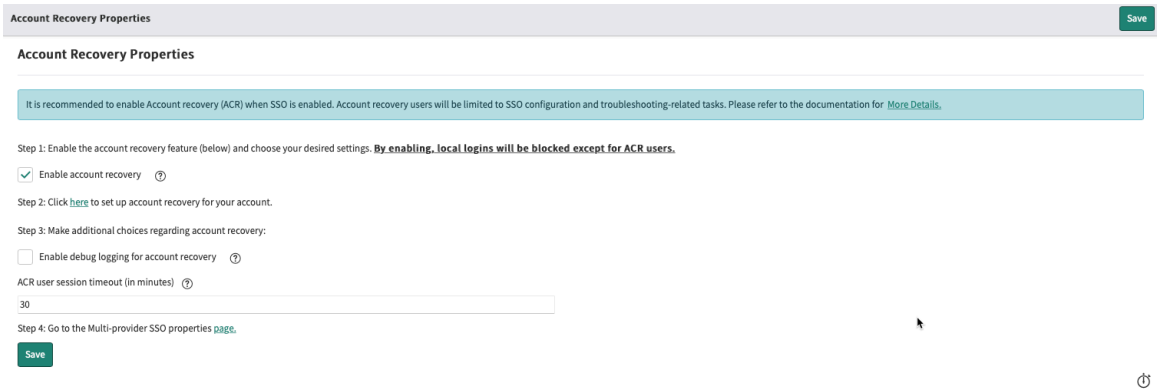
프로시저

1. 다음으로 이동 모두 > 계정 복구 > 속성.
2. 계정 복구 사용을 클릭합니다.

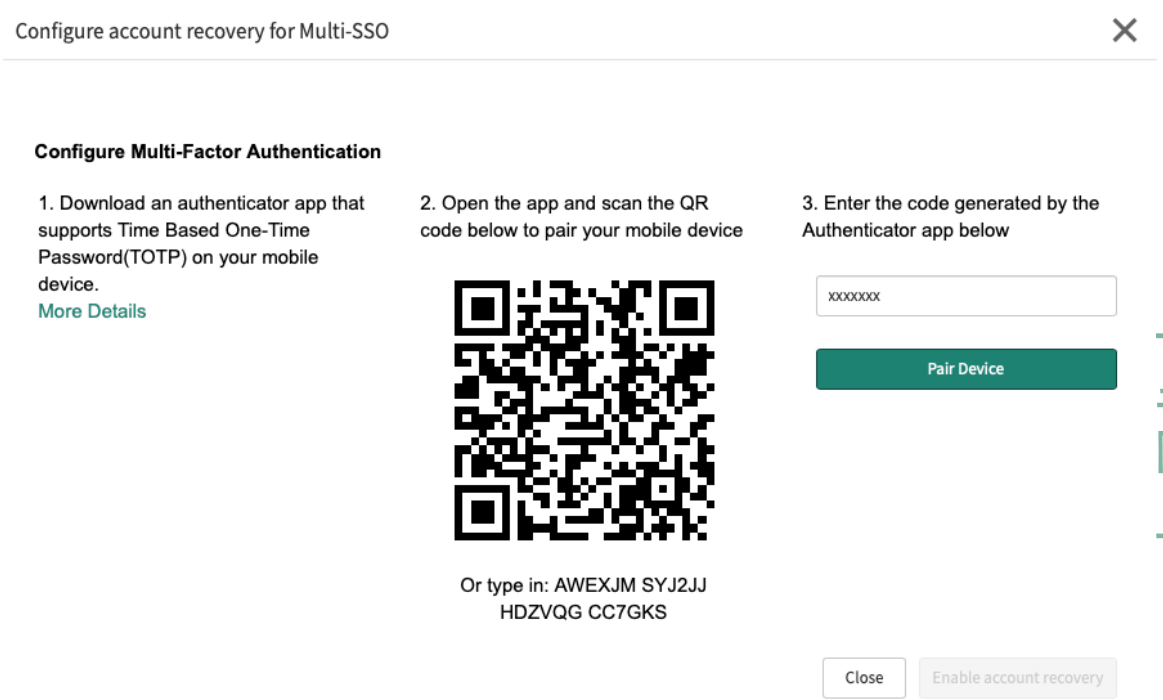
   주: SSO를 사용하는 경우 계정 복구를 활성화해야 합니다. 계정 복구 사용자는 SSO 구성 및 문제 해결 관련 작업으로 제한됩니다.

3. 클릭 **here** 의 텍스트 2 단계.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 다중 SSO에 대한 계정 복구 구성 모달의 화면 지침을 따릅니다.



화면의 단계를 완료하면 계정 복구 활성화 가 활성화됩니다.

5. 계정 복구 사용을 클릭합니다.

결과
사용자 계정을 계정 복구 사용자로 구성했습니다. 이 계정을 확인하고 다음으로 이동하여 구성된 다른 계정 복구 사용자를 볼 수 있습니다. 복수 제공자 **SSO** > 계정 복구 > 사용자.

관리자 사용자 프로파일에서 계정 복구 사용자 구성

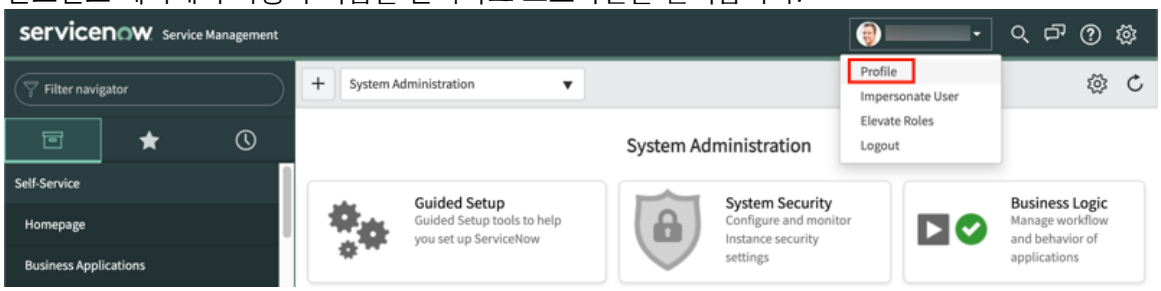
관리자 사용자 프로파일에서 관리자를 계정 복구 사용자로 구성합니다.

시작하기 전에
필요한 역할: 관리자

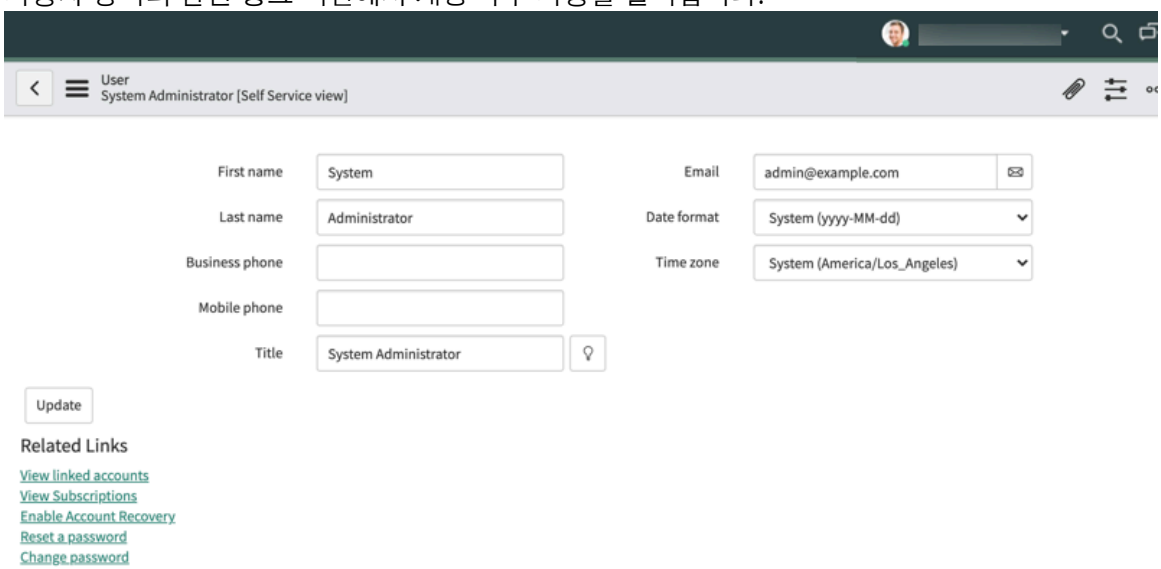
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 관리자 계정을 사용하여 인스턴스에 로그인합니다.
2. 인스턴스 헤더에서 사용자 이름을 클릭하고 프로파일을 선택합니다.



3. 사용자 양식의 관련 링크 섹션에서 계정 복구 사용을 클릭합니다.

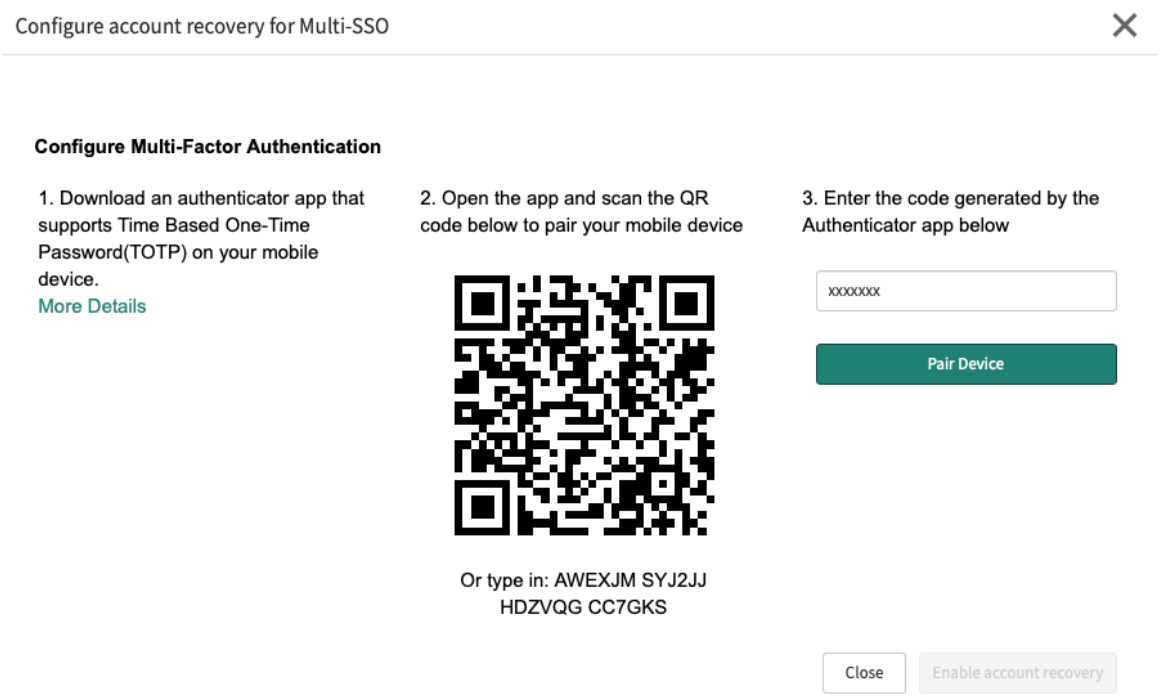


주:

선택한 사용자가 이미 계정 복구를 활성화한 경우, 계정 복구 활성화 가 관련 링크에 나타나지 않습니다. 대신 계정 복구 비활성화 옵션이 있습니다.

4. 다중 SSO에 대한 계정 복구 구성 모달의 화면 지침을 따릅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



화면의 단계를 완료하면 계정 복구 활성화 가 활성화됩니다.

5. 계정 복구 사용을 클릭합니다.

결과
사용자 계정을 계정 복구 사용자로 구성했습니다. 이 계정을 확인하고 다음으로 이동하여 구성된 다른 계정 복구 사용자를 볼 수 있습니다. 복수 제공자 **SSO** > 계정 복구 > 사용자.

계정 복구 속성

시스템 속성을 사용하여 인스턴스에서 계정 복구(ACR)를 구성합니다.

다음으로 이동하여 인스턴스의 계정 복구 속성에 액세스합니다. 복수 제공자 **SSO** > 계정 복구 > 속성.

계정 복구 시스템 속성

속성	설명
계정 복구 기능 활성화 [glide.sso.acr.enabled]	인스턴스에서 계정 복구 기능을 사용할 수 있는지 여부입니다. 이 속성은 기본적으로 사용하도록 설정됩니다.
계정 복구용 디버그 로깅 사용 [glide.sso.acr.debug.log.enabled]	인스턴스의 디버그 로깅에 계정 복구 정보가 포함되어 있는지 여부입니다. 기본적으로 이 속성은 사용되지 않습니다.
ACR 사용자 세션 시간 제한(분) [glide.sso.acr.ui.session.timeout]	인스턴스가 계정 복구 사용자 세션을 종료하기 전 비활성 시간(분)입니다. 이 속성의 기본값은 30입니다.

복수 제공자 SSO에 대한 전자 서명

복수 제공자 SSO를 통한 전자 서명을 사용하면 인증에 SAML 또는 OIDC 속성 대신 전자 서명 속성을 사용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인증 중 1회 사용자 인증(SSO)을 확인하고 사용자가 전자 서명을 제출하기 전에 자격 증명을 제공하도록 요구하기 위해 서명을 제출하기 전에 사용자 자격 증명을 묻는 메시지를 표시하도록 인증을 구성할 수 있습니다.

SSO 로그인에 대한 전자 서명 구성을 갖도록 전자 서명(`com.glide.e_signature_approvals`) 플러그인을 설치할 수 있습니다.

주: 전자 서명 플러그인을 설치하려면 코드 서명 서명 (`com.glide.code_signing.signatures`)을 설치해야 합니다.

전자 서명 플러그인으로 승인 활성화

전자 서명을 사용한 승인 플러그인(com.glide.e_signature_approvals)을 사용하면 사용자가 로그인 자격 증명을 다시 입력하여 요청을 승인할 수 있습니다.

시작하기 전에

필요한 역할: 관리자

주: 전자 서명 플러그인을 설치하려면 코드 서명 서명 (`com.glide.code_signing.signatures`)을 설치해야 합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 조건과 검색 창을 사용하여 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

다중 제공자 SSO를 사용하여 **SAML 2.0** 인증에 대한 **SSO** 승인을 설정합니다.

전자 서명이 있는 SSO 승인에는 ServiceNow SAML IdP 및 인스턴스에 대한 구성이 필요합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

SAML IdP는 SAML 어설션 요청에서 forceAuthn 속성을 지원하고 승인해야 합니다. 이 IdP 설정이 없으면 전자 서명이 작동하지 않습니다. SAML 2.0 인증의 자격 증명을 사용하여 전자 서명으로 승인을 설정합니다.

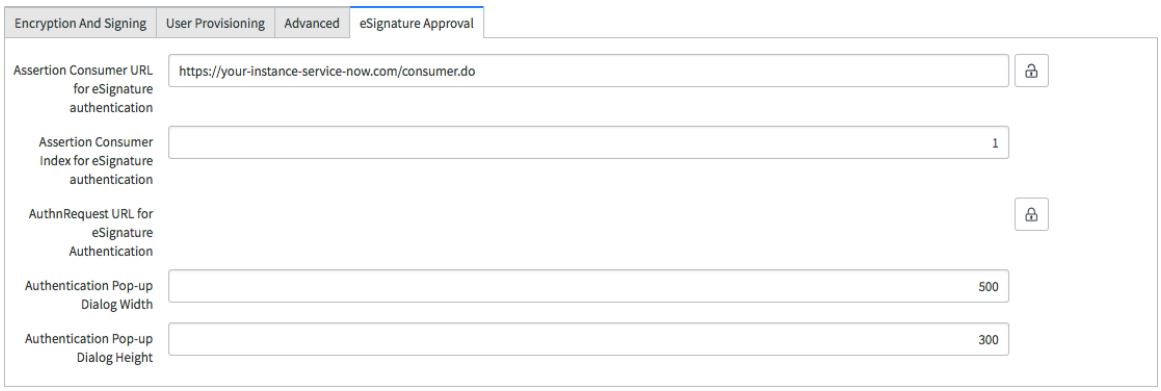
프로시저

1. 복수 제공자 SSO 활성화 플러그인을 사용하여 SAML 2.0을 활성화하거나 SAML 2.0으로 업그레이드합니다.
2. Approval with E-Signature 플러그인을 활성화합니다.
3. 다음으로 이동 복수 제공자 **SSO** > **ID** 제공자 을 클릭하고 2.0 SAML IdP 구성을 확인하십시오. 고급 탭에 강제 **AuthnRequest** 속성이 선택되어 있는지 확인합니다.
   SAML 2.0 IdP가 강제 **AuthnRequest** 속성을 지원해야 하며, 그렇지 않으면 전자 서명이 지원되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 전자 서명 승인 탭에서 다음 전자 서명 SAML 속성을 입력합니다.

옵션	설명
전자 서명 인증용 Assertion Consumer URL	이 속성은 기본적으로 적절한 URL로 설정됩니다. 이 속성을 구성하려면 이 필드를 편집할 수 있도록 하려면 잠금 아이콘을 선택합니다. 편집 후 아이콘을 선택하여 필드를 잠급니다.
전자 서명 인증용 Assertion Consumer Index	서비스 제공자기에 AssertionConsumerURL용으로 설정된 URL이 두 개 이상 있는 경우 인덱스 1 이상으로 시작하는 전자 서명에 사용할 인덱스를 설정할 수 있습니다.
전자 서명 인증용 AuthnRequest URL	전자 서명 인증을 위해 SAML 2.0 IdP AuthnRequest URL을 가리키는 URL을 입력할 수 있습니다. URL이 Assertion Consumer URL과 같으면 이 설정을 비워 둘 수 있습니다.
인증 팝업 대화 상자 너비	사용자가 전자 서명을 사용하여 요청을 승인하면 대화 상자가 열리고 사용자는 자격 증명을 입력할 수 있습니다. 이 설정은 해당 대화 상자의 너비를 제어합니다. 기본값은 500입니다.
인증 팝업 대화 상자 높이	사용자가 전자 서명을 사용하여 요청을 승인하면 대화 상자가 열리고 사용자는 자격 증명을 입력할 수 있습니다. 이 설정은 해당 대화상자의 높이를 조정합니다. 기본값은 300입니다.



5. 탭 아래에 있는 메타데이터 생성 버튼을 선택하여 서비스 제공자 메타데이터를 다시 생성합니다.

6. 서비스 제공자 메타데이터를 복사하여 SAML IdP에서 업데이트합니다.

복수 제공자 SSO를 사용하여 **OIDC** 인증에 대한 **SSO** 승인을 설정합니다.

전자 서명이 있는 SSO 승인에는 ServiceNow SAML IdP 및 인스턴스에 대한 구성이 필요합니다.

시작하기 전에
필요한 역할: 관리자

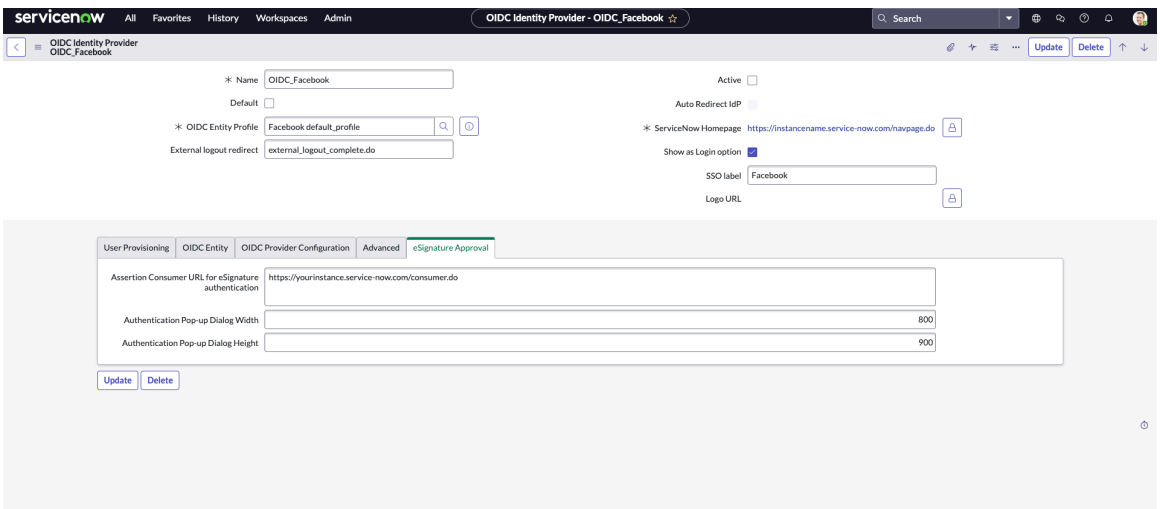
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
SAML IdP는 SAML 어설션 요청에서 forceAuthn 속성을 지원하고 승인해야 합니다. 이 IdP 설정이 없으면 전자 서명이 작동하지 않습니다. SAML 2.0 인증의 자격 증명을 사용하여 전자 서명으로 승인을 설정합니다.

프로시저

1. Approval with E-Signature 플러그인을 활성화합니다.
2. 다음으로 이동 복수 제공자 **SSO** > **ID** 제공자 OIDC 제공자 구성을 검증합니다.
3. 전자 서명 승인 탭에서 다음 전자 서명 SAML 속성을 입력합니다.

옵션	설명
전자 서명 인증용 Assertion Consumer URL	이 속성은 기본적으로 적절한 URL로 설정됩니다. 이 속성을 구성하려면 이 필드를 편집할 수 있도록 하려면 잠금 아이콘을 선택합니다. 편집 후 아이콘을 선택하여 필드를 잠급니다.
인증 팝업 대화 상자 너비	사용자가 전자 서명을 사용하여 요청을 승인하면 대화 상자가 열리고 사용자는 자격 증명을 입력할 수 있습니다. 이 설정은 해당 대화 상자의 너비를 제어합니다. 기본값은 800입니다.
인증 팝업 대화 상자 높이	사용자가 전자 서명을 사용하여 요청을 승인하면 대화 상자가 열리고 사용자는 자격 증명을 입력할 수 있습니다. 이 설정은 해당 대화상자의 높이를 조정합니다. 기본값은 900입니다.



4. 초기 OIDC 설정 중에 전자 서명을 구성하는 경우 제출 을 선택하고 전자 서명의 세부 정보를 업데이트하려면 업데이트를 선택합니다.

1회 사용자 인증(SSO)으로 **OIDC(OpenID Connect) IdP(ID** 제공자)

OIDC(OpenID Connect)는 OAuth 프로토콜을 기반으로 구축된 ID 계층으로, 사용자와 최종 사용자에게 현대적이고 직관적인 SSO(Single Sign-On) 환경을 제공합니다. 또한 OIDC는 사용자가 소셜 ID 제공자를 사용하여 애플리케이션에 로그인할 ServiceNow 수 있도록 함으로써 모바일 애플리케이션의 로그인 환경을 개선합니다. 예를 들어 관리자는 OpenID Connect를 지원하는 타사 ID 제공자를 사용하여 Single Sign-On을 구성할 수 있습니다. 그러면 사용자는 신원 확인 제공자 자격 증명을 사용하여 사용자 지정 ServiceNow 애플리케이션에 로그인할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

B2C(business-to-customer) 사용자와 같은 Google 소셜 ID 제공자 및 business-to-business(business-to-business) 사용자의 경우 와 Microsoft Azure AD 같은 Okta 엔터프라이즈 ID 제공자를 사용하도록 선택할 수 있습니다.

1회 사용자 인증(SSO)에 대한 **OIDC(OpenID Connect)** 구성 만들기

복수 제공자 SSO 플러그인을 사용하여 OIDC(OpenID Connect) 구성을 생성하거나 업데이트합니다.

1회 사용자 인증(SSO)에 대한 OIDC(OpenID Connect) 구성

시작하기 전에

- IdP(ID 제공자)에 OIDC 애플리케이션을 등록하고 클라이언트 ID, 클라이언트 비밀 및 잘 알려진 구성 URL을 기록해 둡니다.
- 복수 제공자 SSO 플러그인 활성화
- 복수 제공자 SSO 속성 구성
- 전자 서명 플러그인을 사용하여 승인을 활성화 하여 OIDC IdP에 대한 전자 서명을 활성화합니다.
- 필요한 역할: 관리자

클라이언트 ID, 클라이언트 비밀 및 ID 제공자의 잘 알려진 구성 URL이 있는 경우 SSO에 대한 OIDC 구성을 직접 임포트할 수 있습니다.

주: 도메인 분리 플러그인이 설치된 경우 OIDC IdP를 사용하는 로그인 옵션이 지원되지 않습니다.

ID 제공자에 대한 필요한 정보가 없는 경우 SSO에 대해 OIDC를 수동으로 구성할 수 있습니다. 구성을 완료한 후 사용자는 와 같은 Google Okta타사 소셜 ID 공급자를 사용하여 애플리케이션에 로그인할 ServiceNow 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. 다음 옵션 중 하나를 선택합니다.
   - 기존 구성을 업데이트하려면 OIDC ID 제공자 기록을 클릭합니다.
   - 새 구성을 만들려면 새로 만들기를 클릭하고 **OpenID Connect**를 선택합니다.
3. 새 구성의 경우 다음 방법 중 하나로 OIDC 구성 정보를 입력합니다.

옵션	설명
OpenID 커넥트 잘 알려진 구성 임포트	연결된 클라이언트 자격 증명과 함께 잘 알려진 구성 URL이 있는 경우 OIDC 구성을 직접 임포트할 수 있습니다. 주: OIDC의 잘 알려진 구성을 임포트하면 모든 관련 필드가 자동으로 채워집니다.
OIDC ID 제공자 양식 수동 구성	기존 OAuth OIDC 엔터티가 없는 경우 OpenID Connect의 잘 알려진 구성 임포트 팝업을 닫고 OIDC ID 제공자 양식의 필드를 수동으로 채웁니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OpenID 커넥트의 잘 알려진 구성 필드 임포트

속성	설명
이름	OIDC ID 제공자 구성의 고유한 이름입니다.
클라이언트 ID	타사 OIDC ID 제공자에 등록된 애플리케이션의 클라이언트 ID입니다.
클라이언트 비밀	타사 OIDC ID 제공자에 등록된 애플리케이션의 클라이언트 비밀입니다.
잘 알려진 구성 URL	타사 OIDC ID 제공자에 대한 메타데이터가 포함된 URL입니다.

모든 필수 필드는 OIDC ID 제공자 양식에 입력해야 합니다.

OIDC ID 제공자 양식을 수동으로 작성하기 전에 OIDC IdP에 대한 OAuth 엔터티 프로파일이 이미 있는지 확인합니다.

OAuth 엔터티 프로파일이 없는 경우 Okta, Azure 등과 같은 기본 외부 OIDC 제공자 템플릿을 사용하여 만들 수 있습니다.

OAuth 엔터티 프로파일의 권한 부여 유형에는 인증 코드가 있어야 합니다. 자세한 내용은 Now Platform에서 OAuth OIDC 제공자 구성을 참조하십시오.

주: 타사 ID 공급자의 템플릿을 사용할 수 있으며, Auth0, Azure AD, Google 및 Okta는 다중 공급자 SSO(Single Sign-On) 설치 관리자 플러그인의 데모 데이터에서 사용할 수 있습니다.

OIDC ID 제공자 필드

속성	설명
이름	OIDC ID 제공자 기록의 이름입니다.
활성	OIDC IdP 구성을 활성화하는 옵션입니다. 주: 이 옵션은 연결 테스트가 성공한 후에만 활성으로 설정할 수 있습니다.
기본값	OIDC 구성이 두 개 이상인 경우 OIDC IdP 구성을 기본값으로 설정하는 옵션입니다.
IDP 자동 리디렉션	ID 제공자의 로그인 페이지로 사용자 자동 리디렉션을 활성화하는 옵션입니다. 이 필드는 관련 링크 섹션 아래에 자동 리디렉션 IdP로 설정 옵션이 설정된 경우에 표시됩니다. 주: 새 자동 리디렉션 IdP 구성을 활성화하면 쿠키가 *glide_sso_id*자동으로 새 자동 리디렉션 IdP로 업데이트됩니다. *glide.authenticate.sso.update.idp.cookie* 시스템 속성이 이 기능을 제어합니다.
OIDC 엔터티 프로파일	OIDC 구성에 대한 OAuth 엔터티 프로파일입니다.
ServiceNow 홈페이지	인증에 사용되는 로그인 페이지의 URL입니다. 이 필드는 인스턴스 URL로 자동 설정됩니다. URL 형식은 다음과 같습니다. `https://yourinstance.service-now.com/navpage.do`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
외부 로그아웃 리디렉션	사용자가 로그아웃한 후 통합이 사용자를 리디렉션하는 URL입니다. 일반적으로 SSO에 사용되는 포털입니다. 이 필드는 `external_logout_complete.do` 로 자동 설정됩니다. 예: `https://yourinstance.service-now.com/external_logout_complete.do`
로그인 옵션으로 표시	로그인 페이지에서 OIDC IdP를 로그인 옵션으로 표시하는 옵션입니다. 로그인 옵션이 **ID** 제공자를 통한 로그인 버튼으로 나타납니다.
SSO 라벨	로그인 페이지에 표시되는 OIDC IdP의 레이블입니다. 이 필드는 로그인 옵션으로 표시 가 활성화된 경우에만 나타납니다.
로고 URL	OIDC IdP 제공자의 로고가 포함되어 있으며 공개적으로 사용 가능한 URL입니다. 이 필드는 로그인 옵션으로 표시 가 활성화된 경우에만 나타납니다.

4. 옵션: 사용자 프로비저닝 탭>사용자 프로비저닝 탭에서 자동 사용자 프로비저닝을 활성화합니다.

   (Optional) 사용자가 로그인하는 동안 자동 사용자 프로비저닝을 사용하도록 선택할 수 있습니다. 자동 사용자 프로비저닝이 활성화되면 해당 사용자 기록이 없으면 ServiceNow 인스턴스에 사용자 기록이 자동으로 생성됩니다.

   사용자 프로비저닝 필드

속성	설명
자동으로 사용자 프로비저닝	자동 사용자 프로비저닝을 활성화하는 옵션입니다. 이 속성은 사용자가 IdP에서 종료하지만 사용자 테이블에 없는 경우 인스턴스 사용자(sys_user) 테이블에 사용자를 작성합니다.
다음을 사용하여 프로비저닝	ServiceNow 사용자에 대한 ID `##`, `### ##` 엔드포인트 또는 `ID ### ### ## ###` 변환하는 데 사용할 데이터 소스입니다. 조회 목록을 사용하여 사전 정의된 데이터 소스 템플릿을 선택한 다음 기록을 열어 변환 테이블 매핑을 구성합니다.
데이터 소스 프로비저닝	사용자 프로비저닝에 사용되는 ID 토큰 데이터 소스입니다.
사용자 정보 데이터 소스	사용자 프로비저닝에 사용되는 사용자 정보 엔드포인트 데이터 소스입니다. 이 필드는 프로비저닝 사용 필드에 `## ### ##` 또는 `ID ### ### ## ###` 선택한 경우에 표시됩니다.
다음 로그인 시 사용자 업데이트	다음 로그인 시 사용자 업데이트를 활성화하는 옵션입니다.
사용자 간격 시간 업데이트(초)	후속 로그인 간에 사용자 기록을 업데이트하기 위한 최소 시간 간격(초)입니다. 이 필드는 3,600초로 자동 설정됩니다. 예를 들어, 사용자가 로그인한 후 3,600초 후에 다음 로그인까지 사용자 기록이 업데이트됩니다. 이 필드는 다음 로그인 시 사용자 업데이트 필드가 활성화된 경우에만 사용할 수 있습니다.
프로비저닝된 사용자에게 적용되는 사용자 역할	새로 프로비저닝된 사용자에게 적용되는 역할 목록입니다.

5. OIDC 엔터티 탭
   엔터티 기록을 사용하여 OIDC 클라이언트 구성 및 OIDC 연결 플로우를 보고 수정할 수 있습니다.
6. OIDC 제공자 구성 탭
   OIDC IdP 또는 ID 토큰 클레임 확인의 잘 알려진 구성 URL을 보고 수정할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 옵션: 고급 탭

(Optional) Single Sign-On 및 로그아웃 중에 실행되는 스크립트입니다.

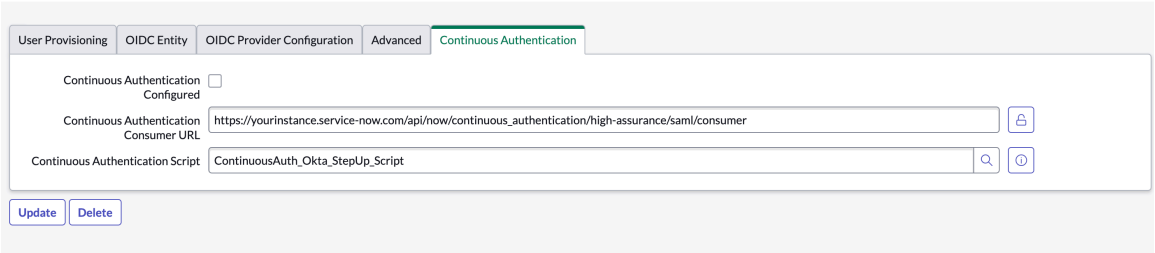
고급 필드

속성	설명
1회 사용자 인증 (SSO) 스크립트	Single Sign-On 중에 실행되는 스크립트입니다. 이 필드는 `MultiSSO_OIDC_custom`로 자동 설정됩니다.
로그아웃 스크립트	사용자가 로그아웃한 후에 실행되는 스크립트입니다. 이 필드는 `MultiSSO_OIDC_logout_custom`로 자동 설정됩니다.

8. 옵션: Continuous Authentication(연속 인증) 탭에서 다음 필드를 구성합니다.

주:

- 연속 인증 탭은 라이센스가 필요한 제로 트러스트 -`com.snc.zero_trust_continuous_authentication`(연속 인증) 플러그인을 설치할 때만 나타납니다.
- 연속 인증 정책을 사용하여 테이블 또는 데이터 클래스에 대한 액세스를 보호하는 경우 을 참조하십시오 연속 인증.



연속 인증

필드	설명
연속 인증 구성됨	구성을 활성화하려면 확인란을 선택합니다.
연속 인증 소비자 URL	ID 제공자의 소비자 URL을 제공합니다.
연속 인증 스크립트	(Optional) 조회 아이콘을 선택하여 플랫폼에서 제공되는 스크립트를 선택합니다. 이 구성에서 OIDC Okta의 경우: **ContinuousAuth_Okta_StepUp_Script**

9. 옵션: 전자 서명 승인 탭에서 OIDC IdP에 대한 전자 서명을 구성합니다.

주: 전자 서명 승인 탭은 com.glide.e_signature_approvals(전자 서명으로 승인) 플러그인을 설치할 때만 나타납니다.

전자 서명 승인 필드

속성	설명
전자 서명 인증용 Assertion Consumer URL	전자 서명에 대한 OIDC 인증을 처리하는 사용자 지정 방법을 사용하는 경우 고유한 소비자 URL을 설정할 수 있습니다. 예를

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
	들어 다중 제공자 SSO를 사용하는 경우에는 이 속성을 사용할 필요가 없습니다. 이 URL 형식은 `https://yourinstance.service-now.com/consumer.do`
인증 팝업 대화 상자 너비	인증 팝업 대화 상자의 너비입니다. 이 필드는 `800`으로 자동 설정됩니다.
인증 팝업 대화 상자 높이	인증 팝업 대화 상자의 높이입니다. 이 필드는 `900`으로 자동 설정됩니다.

10. 옵션: 인스턴스의 로그인 페이지로 이동하여 IdP가 로그인 옵션으로 나타나는지 확인합니다. URL은 `https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP` 형식이어야 합니다.

    주: 로그인 옵션으로 선택을 활성화한 경우 인스턴스의 로그인 URL로 이동할 수 있습니다.

Facebook 기반 SSO(Single Sign-On) 사용

ServiceNow Facebook 기반 SSO의 자격 증명을 사용하여 Facebook 인스턴스에 로그인합니다.

시작하기 전에
Facebook 기반 SSO가 인스턴스 ServiceNow 와 함께 제공됩니다.

OIDC_Facebook IdP에 대한 신원 확인 제공자(IdP) 구성을 신원 확인 제공자로 정의할 수 있습니다. IDP 구성에 대한 자세한 내용은 다음 문서를 참조하십시오 Facebook 기반 SSO(Single Sign-On) 구성.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. **OIDC_Facebook** 선택합니다.
3. OIDC_Facebook 페이지에서 다음 필드를 지정합니다.

    주:

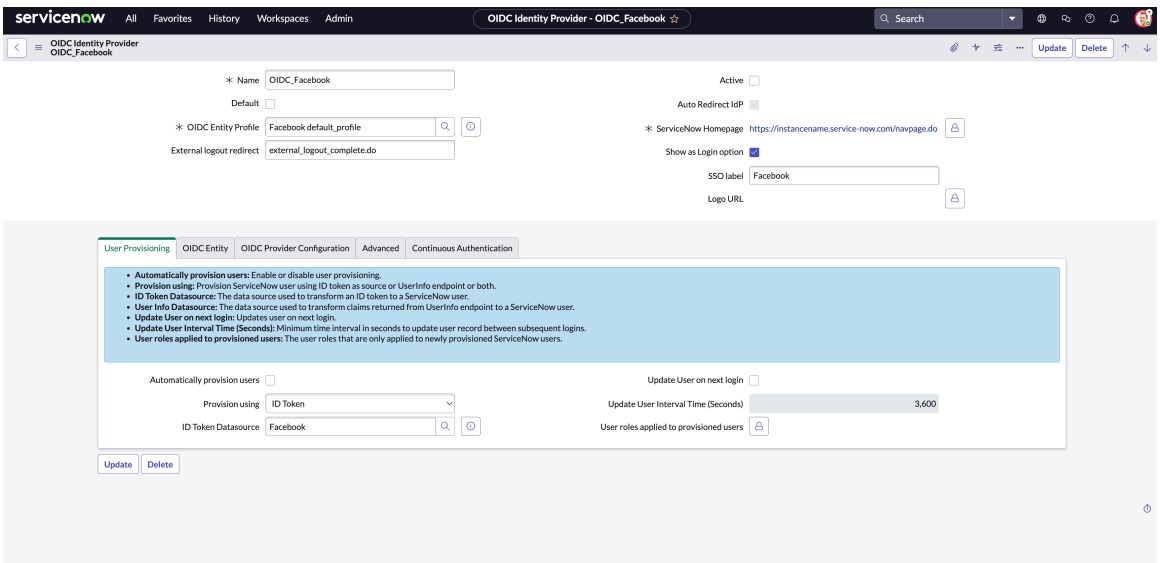
    - 기본 IdP를 사용하면 대부분의 필드가 자동으로 채워집니다.
    - 홈페이지의 ServiceNow 세부 정보를 제공해야 합니다.
    - 클라이언트 ID 및 클라이언트 암호와 Facebook 같은 사용자 관련 세부 정보는 IdP 내에 제공되어야 합니다.

ID 제공자 상세 정보 **OIDC_Facebook**

필드	설명
이름	OIDC IdP 기록의 이름입니다. `OIDC_Facebook` 입력합니다.
기본값	OIDC IdP 구성을 기본값으로 설정하는 옵션입니다.
OIDC 엔터티 프로파일	OIDC 구성에 대한 OAuth 엔터티 프로파일입니다. `Facebook default_profile`를 입력하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
외부 로그아웃 리디렉션	사용자가 로그아웃한 후 통합이 사용자를 리디렉션하는 URL입니다. 일반적으로 이 URL은 SSO에 사용되는 포털입니다. 이 필드는 **external_logout_complete.do**로 자동 설정됩니다. 예: `https://<####>.service-now.com/external_logout_complete.do`.
활성	OIDC IdP 구성을 활성화하는 옵션입니다. 주: 이 옵션은 연결 테스트가 성공한 후에만 활성으로 설정할 수 있습니다.
IDP 자동 리디렉션	ID 제공자의 로그인 페이지로 사용자를 자동으로 리디렉션할 수 있도록 하는 옵션입니다.
ServiceNow 홈페이지	인증에 사용되는 로그인 페이지의 URL입니다. 이 필드는 인스턴스 URL로 자동 설정됩니다. URL의 형식은 `https://<####>.service-now.com/navpage.do` 입니다.
로그인 옵션으로 표시	로그인 페이지에서 OIDC IdP를 로그인 옵션으로 표시하는 옵션입니다. 이 경우 로그인 옵션은 Facebook으로 로그인 버튼으로 표시됩니다.
SSO 라벨	로그인 페이지에 표시되는 OIDC IdP의 레이블입니다. 이 필드는 로그인으로 표시 옵션이 활성화된 경우에만 나타납니다.
로고 URL	OIDC IdP 제공자의 로고가 포함되어 있는 공개적으로 사용 가능한 URL입니다. 이 필드는 로그인으로 표시 옵션이 활성화된 경우에만 나타납니다.



4. 옵션: 사용자 프로비저닝 탭을 열고 필드를 채웁니다.

   주: 에서 Facebook사용자의 클라이언트 ID 및 클라이언트 암호와 같은 OIDC 관련 정보를 구성해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 프로비저닝 탭

필드	설명
자동으로 사용자 프로비저닝	자동 사용자 프로비저닝을 활성화하는 옵션입니다. 이 속성은 사용자가 IdP에 있지만 사용자 테이블에는 없는 경우 인스턴스 사용자 [sys_user] 테이블에 사용자를 작성합니다. 주: 사용자가 로그인하는 동안 자동 사용자 프로비저닝을 사용하도록 선택할 수 있습니다. 자동 사용자 프로비저닝이 활성화되면 해당 사용자 기록이 없는 경우 인스턴스에 사용자 기록이 ServiceNow 자동으로 생성됩니다.
다음을 사용하여 프로비저닝	사용자로 변환하는 데 사용할 데이터 소스입니다 ServiceNow . 선택 항목은 다음과 같습니다. ◦ **ID** 토큰 ◦ 사용자 정보 엔드포인트 ◦ **ID** 토큰 및 사용자 정보 모두 조회 목록을 사용하여 사전 정의된 데이터 소스 템플릿을 선택한 다음 기록을 열어 변환 테이블 매핑을 구성합니다.
데이터 소스 프로비저닝	사용자 프로비저닝에 사용되는 ID 토큰 데이터 소스입니다.
사용자 정보 데이터 소스	사용자 프로비저닝에 사용되는 사용자 정보 엔드포인트 데이터 소스입니다. 이 필드는 다음을 사용하여 프로비저닝 필드에서사용자 정보 또는 **ID** 토큰과 사용자 정보를 모두 선택한 경우에만 표시됩니다.
다음 로그인 시 사용자 업데이트	다음 로그인 시 사용자 업데이트를 활성화하는 옵션입니다.
사용자 간격 시간 업데이트(초)	후속 로그인 간에 사용자 기록을 업데이트하는 최소 시간 간격(초)입니다. 이 필드는 3600초로 자동 설정됩니다. 예를 들어, 사용자가 로그인한 후 3,600초 후에 다음 로그인까지 사용자 기록이 업데이트됩니다. 이 필드는 다음 로그인 시 사용자 업데이트 필드가 활성화된 경우에만 사용할 수 있습니다.
프로비저닝된 사용자에게 적용되는 사용자 역할	새로 프로비저닝된 사용자에게 적용되는 역할 목록입니다.

5. **OIDC** 엔터티 탭에서 엔터티 기록을 사용하여 OIDC 클라이언트 구성 및 OIDC 연결 플로우를 보고 수정합니다.
   OIDC 기반 구성과 관련된 자세한 내용은 다음을 참조하십시오. 외부 공급업체 토큰을 수락하도록 OAuth OIDC 제공자 구성
6. **OIDC** 제공자 구성 탭에서 OIDC IdP의 잘 알려진 구성 URL을 보고 수정합니다.
7. 옵션: 고급 탭을 열고 필드를 채웁니다.

고급 탭

속성	설명
1회 사용자 인증(SSO) 스크립트	Single Sign-On 중에 실행되는 스크립트입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
로그아웃 스크립트	사용자가 로그아웃한 후 실행되는 스크립트입니다.

주: 스크립트는 Single Sign-On 및 로그아웃 중에 실행됩니다.

8. 구성을 활성화하고 테스트하려면 활성을 클릭합니다.
9. 기록을 업데이트하려면 업데이트를 클릭합니다.
   Facebook 기반 로그인 옵션이 로그인 양식에 표시됩니다.
10. 로그인 양식에 로그인할 때 다음을 수행합니다.
    a. 옵션을 Facebook 선택합니다.
    b. 인스턴스에 로그인 ServiceNow 하려면 자격 증명을 지정합니다 Facebook .

Facebook 기반 SSO(Single Sign-On) 구성

인스턴스에 대한 Facebook 기반 SSO를 ServiceNow 구성합니다.

시작하기 전에
에서 IdP Facebook로 구성된 유효한 클라이언트 ID가 있어야 합니다.

다음 속성을 활성화합니다.

- 복수 제공자 SSO를 활성화합니다.
- 복수 제공자 SSO 통합에 디버그 로깅을 사용합니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. 새 Facebook ID 공급자를 만들려면 새로 만들기를 클릭합니다.
3. **OpenID Connect**를 클릭합니다.
4. 양식의 필드에 내용을 입력합니다.

OpenID 커넥트 잘 알려진 구성 임포트 양식

필드	설명
이름	OIDC ID 제공자 구성의 고유한 이름입니다.
클라이언트 ID	타사 OIDC ID 제공자에 등록된 애플리케이션의 클라이언트 ID입니다.
클라이언트 비밀	타사 OIDC ID 제공자에 등록된 애플리케이션의 클라이언트 비밀입니다.
잘 알려진 구성 URL	타사 OIDC ID 제공자에 대한 메타데이터가 포함된 URL입니다.

5. 임포트를 클릭합니다.
   Facebook 기반 IdP가 생성됩니다.
6. IdP를 Facebook 선택합니다.
7. Facebook idP에서 다음을 수행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 이름, **OIDC** 엔터티 프로파일, 외부 로그아웃 리디렉션 및 **ServiceNow** 홈페이지와 같은 모든 필드를 확인합니다.

b. **SSO** 레이블을 입력합니다.

8. 사용자 프로비저닝 탭에서 사용자를 특정 사용자 프로비저닝 및 역할에 구성하는 데 필요한 필드를 지정합니다.

   필수 필드만 필요합니다. 필요에 따라 나머지 필드를 지정할 수 있습니다.

9. **OIDC** 엔터티 탭에서 다음을 수행합니다.

   a. 엔터티를 클릭합니다.

   b. 리디렉션 **URL** 필드를 리디렉션 URL로 Facebook 설정합니다.

10. **OAuth** 엔터티 프로파일 탭에서 다음을 수행합니다.

    a. 프로파일 상세 정보에서 프로파일을 클릭합니다.

    b. 범위를 선택하고 상세 정보를 확인합니다.
    예를 들어 **scope-1**을 선택합니다

11. **OAuth** 엔터티 범위 탭에서 범위-1 링크를 클릭하고 범위를 `####` 추가합니다.
12. 구성을 저장하려면 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 클릭합니다.
13. 구성을 활성으로 설정하려면 활성을 선택합니다.

결과
사용자는 로그인 양식에 SSO 옵션과 함께 Facebook 표시됩니다.

SAML

SAML(Security Assertion Markup Language)은 보안 도메인 간에 인증 및 권한 부여 데이터를 교환하기 위한 XML 기반 표준입니다.

SAML은 ID 제공자(어설션 작성자)와 서비스 제공자(어설션 소비자) 간에 보안 정보를 교환합니다. SAML은 OASIS 보안 서비스 기술 위원회의 제품입니다. SAML을 올바르게 구현하면 가장 안전한 SSO(Single Sign-On) 방법 중 하나가 됩니다.

SAML 2.0 통합은 외부 IdP(신원 확인 제공자)와 XML 토큰을 교환함으로써 SSO를 가능하게 합니다. IdP는 사용자를 인증하고 NameID 토큰을 시스템에 전달합니다. 시스템에서 일치하는 NameID 토큰(예: 이메일 주소)이 있는 사용자를 찾으면 인스턴스에서 해당 사용자를 로그인합니다.

SSO 인증을 위해 SAML 2.0 플러그인을 사용하는 경우 glide.ui.rotate_sessions 속성을 false로 설정해야 합니다. 그렇지 않으면 인스턴스와 ID 제공자 간에 수행되는 세션 정보 공유에 방해가 됩니다. security_admin 상승된 권한을 가진 사용자는 이 속성에 액세스할 수 있습니다.

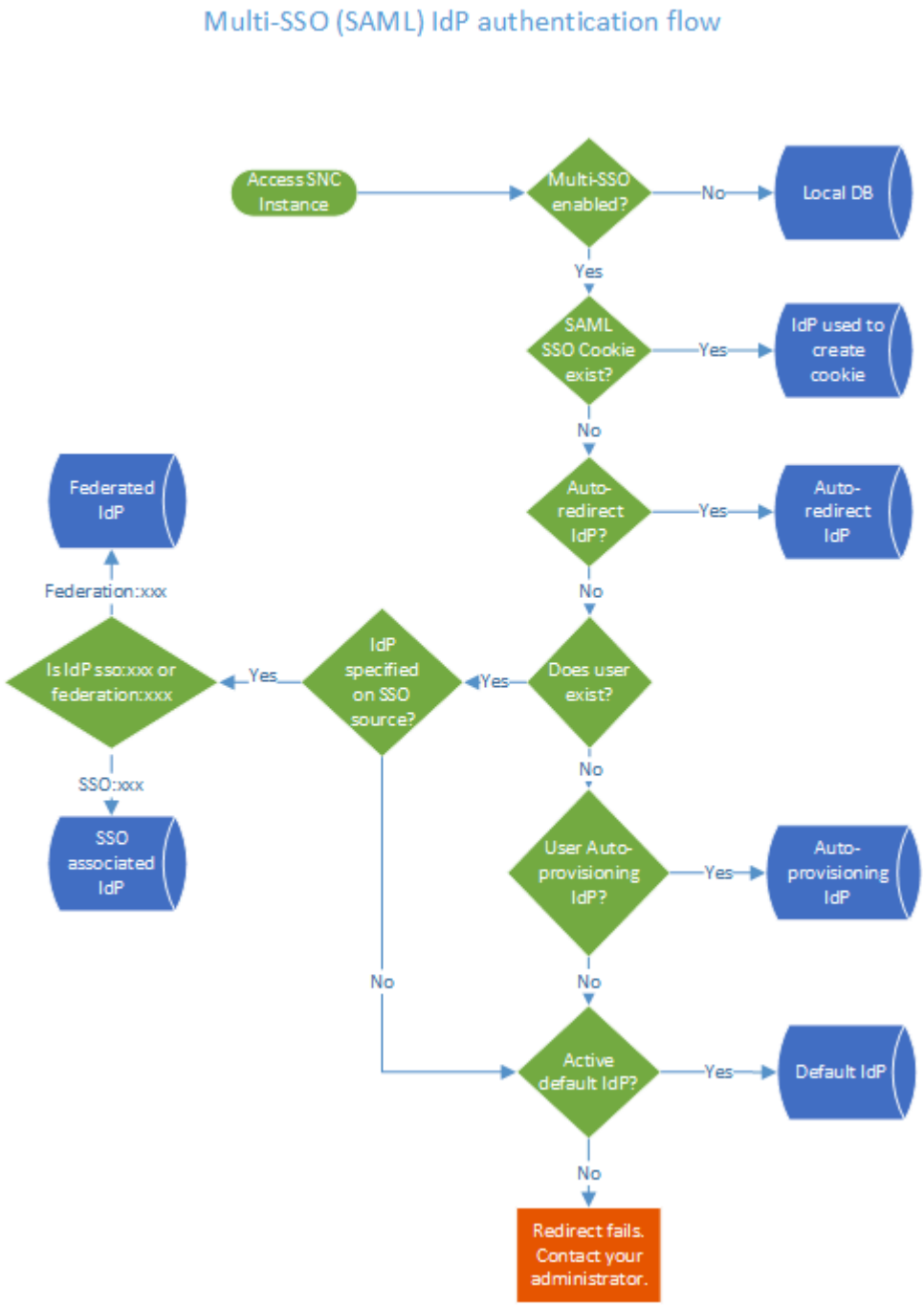
주: 기존 SAML 2.0 통합을 사용하는 고객은 복수 제공자 SSO 플러그인으로 업그레이드하는 것이 좋습니다.

복수 제공자 **SSO(SAML) IdP** 인증 플로우

SAML 다중 SSO를 통해 사용자를 인증할 수 있는 다양한 엔터티에 대해 설명합니다.

인증 플로우를 따라 엔터티가 다중 SSO를 사용하여 사용자를 인증하는 시기를 이해할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



로컬 DB

다중 SSO가 활성화되지 않은 경우 인증은 로컬 DB로 전달됩니다.

SAML SSO 쿠키 IdP

SAML SSO 쿠키가 존재하는 경우 이 쿠키로 지정된 IdP가 사용자를 인증합니다.

IDP 자동 리디렉션

자동 리디렉션 IdP가 활성화된 경우 이 IdP가 사용자를 인증합니다.

페더레이션 IDP

사용자 브라우저가 외부 인증(login_locate_sso.do) 로그인 화면으로 리디렉션되고 사용자가 **SSO** 소스 필드에 페더레이션: xxx로 설정된 IdP를 사용하여 사용자 테이블에 존재하는 경우, 페더레이션 IdP가 사용자를 인증합니다.

연결된 IdP

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 브라우저가 외부 인증(login_locate_sso.do) 로그인 화면으로 리디렉션되고 사용자가 **SSO** 소스 필드에 IdP가 sso: xxx로 설정된 사용자 테이블에 있는 경우 연결된 IdP가 사용자를 인증합니다.

자동 프로비저닝 IdP

사용자 브라우저가 외부 인증(login_locate_sso.do) 로그인 화면으로 리디렉션되고 사용자가 사용자 테이블에 없지만 자동 프로비저닝이 활성화된 경우 자동 프로비저닝 IdP가 사용자를 인증합니다.

주: 자동 프로비저닝 IdP가 두 개 이상 활성화된 경우 사용자는 사용할 수 있는 자동 프로비저닝 IdP를 선택할 수 있습니다.

기본 IdP

사용자 브라우저가 외부 인증(login_locate_sso.do) 로그인 화면으로 리디렉션되고 사용자가 다음 중 하나를 수행하는 경우:

- 사용자 테이블에 없고, 자동 프로비저닝을 사용할 수 없으며, 활성 기본 IdP가 있습니다.
- 사용자 테이블에 있고, IdP가 SSO 소스 사용자 또는 회사 기록에 지정되지 않았으며, 활성 기본 IdP가 있습니다.

그런 다음 기본 IdP가 사용자를 인증합니다.

ID 제공자(IdP) 시스템 속성

IdP는 일반적으로 인증 및 로그아웃 메타데이터가 포함된 XML 문서를 제공합니다.

예를 들어 SSOCircle 은 메타데이터를 온라인에 게시합니다.

IdP 메타데이터를 탐색하여 다음 항목을 찾습니다.

- `HTTP-Redirect` 값을 포함하는 `Binding` 특성이 있는 `SingleSignOnService` 요소입니다. `##` 속성은 통합에서 AuthnRequest 서비스에 필요한 URL을 나열합니다.
- `HTTP-Redirect` 값을 포함하는 `Binding` 특성이 있는 `SingleLogoutService` 요소입니다. `##` 속성은 통합에서 SingleLogoutRequest 서비스에 필요한 URL을 나열합니다.

주: SAML 2.0 통합은 HTTP 리디렉션을 통한 IdP 서비스에 대한 바인딩만 지원합니다.

예:

```
<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"/>
```

IdP 발급자 URL 설정

보안 토큰을 발급할 IdP에 URL을 제공합니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
통합은 각 SAML 응답에 발급자 요소에 나열된 URL과 동일한 URL이 이 시스템 속성에 포함되어 있는지 확인합니다. 예:

```
<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>
```

프로시저

1. 다음으로 이동 모두 > **SAML 2** 1회 사용자 인증**(SSO)** > 속성.
2. 사용자 정보가 포함된 *SAML2* 보안 토큰을 발급할 *ID* 제공자 *URL* 속성에 IdP의 URL을 입력합니다.

   각 IdP URL은 고유해야 합니다. 기본적으로 통합에는 SSOCircle에 대한 URL이 포함되어 있습니다. 자세한 내용은 http://idp.ssocircle.com 문서를 참조하십시오.

AuthnRequest 서비스 **URL** 설정

IdP의 메타데이터를 사용하여 통합의 IdP에 대한 요청 서비스 URL을 설정합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 속성 *ID* 제공자의 *AuthnRequest* 서비스에 대한 기본 URL입니다. AuthnRequest가 이 URL에 *SAMLRequest* 매개변수로 게시됩니다. `SingleSignOnService` 요소에서 가져온 HTTP-Redirect 바인딩에 대한 URL을 입력하십시오.
2. ID 제공자의 SSO(Single Sign-On) 서비스가 서명된 AuthnRequest를 받을 수 있도록 하려면 *Sign AuthnRequest* 옆 의 확인란을 선택합니다.
3. 속성이 세션이 인증되지 않았기 때문에 *SAML 2.0* 1회 사용자 인증(SSO)이 실패하거나 최초 로그인인 경우 이 URL로 리디렉션합니다. 이 URL은 *SAMLRequest* 매개변수를 사용하여 최초 SAML 2.0 AuthnRequest가 전송되는 기본 URL이며, `SingleSignOnService` 요소에서 가져온 HTTP-Redirect 바인딩에 대한 URL을 입력하십시오.

   기본적으로 통합에는 SSOCircle 서비스에 대한 URL이 포함되어 있습니다.

SingleLogoutRequest 서비스 **URL** 설정

IdP의 메타데이터를 사용하여 통합의 IdP에 대한 요청 서비스 URL을 설정합니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. *ID* 제공자의 *SingleLogoutRequest* 서비스에 대한 기본 URL입니다. LogoutRequest가 이 URL에 *SAMLRequest* 매개변수 속성으로 게시되며, `SingleLogoutService` 요소에서 가져온 URL을 입력하십시오.
   LogoutRequest는 이 URL에 SAMLRequest 매개변수로 게시됩니다. 기본적으로 통합에는 SSOCircle 서비스에 대한 URL이 포함되어 있습니다.
2. 로그아웃한 사용자를 리디렉션할 URL(일반적으로 SSO(예: *http://portal.companya.com/logout)* 속성을 활성화한 포털로 돌아가 는 경우)에 사용자가 성공적으로 로그아웃한 후 사용자를 리디렉션할 URL을 입력합니다.

   IdP가 양식 기반 인증을 사용하는 경우 IdP의 로그인 양식에 대한 URL을 입력합니다. IdP가 Kerberos와 같은 양식 기반이 아닌 인증 방법을 사용하는 경우 URL을 정적 로그아웃 페이지로 설정해야 합니다. 이렇게 하면 로그아웃한 사용자가 즉시 IdP로 리디렉션되지 않고 다시 로그인할 수 있습니다. 기본적으로 통합에는 정적 UI 페이지 `external_logout_complete.do`에 대한 URL이 포함되어 있습니다.

(선택 사항) 서명된 로그아웃 요청 사용

일부 IdP에서는 서비스 제공자가 인증서로 로그아웃 요청에 서명해야 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
IdP에서 서명된 로그아웃 요청을 요구하는 경우 IdP의 메타데이터 데이터를 사용하여 다음 시스템 속성을 설정합니다.

프로시저

1. 고급 탭의 Sign LogoutRequest 속성에서. *ID* 제공자의 *SingleLogoutRequest* 서비스에서 서명된 *LogoutRequest*를 요구할 경우 이 속성을 예로 설정하거나, IdP에서 서명된 로그아웃 요청을 요구하도록 지정하려면 예를 선택하고, 서명되지 않은 로그아웃 요청을 사용하려면 아니요 를 선택합니다.
2. LogoutRequest에 서명하기 위해 예를 선택한 경우 ID 제공자의 *SingleLogoutRequest* 서비스에 대한 프로토콜 바인딩 (값은 *"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"* 또는 *"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-*POST*"*일 수 있습니다.) 속성에 `SingleLogoutService` 요소의 `###` 특성에 나열된 지원되는 값 중 하나를 입력합니다.

   기본적으로 통합은 HTTP-Redirect 바인딩을 사용합니다.
3. 업데이트를 클릭합니다.
4. SP(서비스 제공자) 키 스토어를 설치합니다.

서비스 제공자**(SP)** 시스템 속성

이러한 시스템 속성은 인스턴스가 서비스 제공자로서 IdP와 상호작용하는 방법을 정의합니다.

순차 프로세스에 따라 IdP를 서비스 제공자로 정의합니다.

SAML에 대한 인스턴스 **URL** 설정

IdP에서 사용자를 인증할 수 있도록 인스턴스별 URL을 설정합니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. *Service-now* 인스턴스(일반적으로 이 인스턴스)의 *URL* 속성에 IdP가 인증되는 인스턴스의 URL(로그인 페이지 포함)을 입력합니다.
   예: https://yourinstance.service-now.com/navpage.do
2. 엔터티 *ID* 또는 발급자 속성에 IdP가 인증되는 인스턴스의 기본 URL(로그인 페이지 제외)을 입력합니다.
   예: https://yourinstance.service-now.com/

SAML에 대한 대상 **URL** 설정

Audience 속성을 사용하여 인스턴스가 SAML 응답의 의도된 수신자인지 확인할 수 있도록 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
통합은 각 SAML 응답에 *Audience* 요소에 나열된 URL과 동일한 URL이 이 시스템 속성에 포함되어 있는지 확인합니다. 예:

```
<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:Audi
ence>https://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:C
onditions>
...
</samlp:Response>
```

프로시저

1. 다음으로 이동 모두 > **SAML 2** 1회 사용자 인증**(SSO)** > 속성.
2. 속성 에서 *SAML2* 토큰을 수락하는 대상 그룹 URI입니다. (일반적으로 인스턴스 URI입니다. 예: *https://*<인스턴스 이름>*.service-now.com)*인 경우 인스턴스의 URL을 입력합니다.
   예: https://demoi2.service-now.com. 이 URL은 SAML 응답의 *Audience* 요소 값과 일치해야 합니다.
3. 업데이트를 클릭합니다.

SAML에 대한 **NameID** 정책 설정

SAML에 대한 NameID 정책을 설정합니다. SAML 2.0에서는 IdP가 NameID 토큰을 서비스 제공자와 교환해야 합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
SAML 2.0 통합의 경우 NameID 토큰은 사용자 테이블의 특정 필드에 매핑되어야 합니다. 통합은 NameID 토큰의 값을 사용하여 IdP가 인증하는 사용자를 결정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. IdP 메타데이터를 탐색하여 `emailAddress` 값을 포함하는 `NameIDFormat` 요소를 찾습니다. 이 요소의 값은 통합에서 사용하는 기본 형식입니다.
2. 다른 `NameIDFormat` 요소를 검토하여 User 테이블의 다른 필드와 일치하는 형식이 있는지 확인합니다.

NameID 토큰과 일치하는 사용자 테이블 필드를 결정합니다.

ID 제공자는 `NameID` 토큰의 형식을 지정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
SAML 2.0을 설정하려면 `### ##### NameID` 토큰의 형식과 일치하는 필드를 선택해야 합니다. 일반적으로 IdP는 이메일 주소를 `NameID` 토큰으로 사용하는 옵션을 제공합니다. 사용자 테이블에는 이메일 필드가 포함되어 있으므로 이 필드는 `NameID` 토큰으로 사용하기 위한 논리적 선택입니다. 사용자 테이블의 다른 필드를 `NameID` 토큰으로 사용하려면 먼저 IdP가 사용자 테이블 필드의 값과 일치하는 `NameID` 형식을 제공하는지 확인합니다. 이렇게 하려면 사용자 테이블에 필드를 추가해야 할 수 있습니다.

프로시저

1. IdP의 `NameIDFormat` 요소에서 사용 가능한 형식을 사용자 테이블의 필드와 비교합니다.
2. 사용자 테이블에 일치하는 값이 있는 `NameID` 형식을 선택합니다.
3. *SAMLResponse* 필드의 제목의 *NameID* 요소와 일치할 사용자 테이블 필드에 사용자 테이블 필드의 이름을 입력하여 `NameID` 토큰에서 일치하는 값을 검색합니다.

   기본적으로 통합에서는 이메일 필드를 사용합니다.

IdP NameID 정책 설정

IdP에서 `NameID` 토큰에 사용하는 형식을 지정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
이 형식은 IdP 메타데이터의 일부로 나열됩니다.

프로시저

1. 속성 에서 SAMLResponse에서 제목의 NameID를 리턴하기 위해 사용할 *NameID* 정책입니다. *SAML* 자격 증명 공급자는 메타데이터에서 정책을 선언하여 이를 지원해야 합니다. *NameID* 값은 사용자를 조회하기 위해 사용자 테이블의 지정된 필드와 일치시키는 데 사용됩니다. 통합에서 사용하는 `NameIDFormat` 요소의 값을 입력합니다.

   기본적으로 통합은 이메일 주소에 SSOCircle `NameIDFormat` 을 사용합니다.

2. 저장을 클릭합니다.

SAML에 대한 사용자 테이블 필드의 값

통합의 사용자 테이블 필드에 적절한 일치 값이 포함되어 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예를 들어 통합에서 이메일 필드를 `NameID` 토큰으로 사용하는 경우 인스턴스가 IdP와 동일한 이메일 주소를 나열하는지 확인합니다. 통합은 `NameID` 토큰에 대해 일치하는 값이 없는 사용자를 인증하지 못합니다.

(선택 사항) SAML에 대한 인증 컨텍스트 클래스 제공 사용

인스턴스가 인스턴스의 기본 인증 요청 형식을 포함하는 IdP에 인증 컨텍스트 클래스 요청을 보내도록 설정할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
AuthContextClass 메시지 작성을 사용하는 경우 인증 컨텍스트 클래스 참조 형식도 지정해야 합니다.

> **주:** 일부 IdP에서는 서비스 제공자가 인증 컨텍스트 클래스를 설정하는 것을 허용하지 않습니다. 이 설정을 사용하지 않도록 설정하면 IdP가 인증 컨텍스트 클래스를 선택할 수 있습니다.

프로시저

1. 속성에서 AuthnRequest문에 *AuthnContextClass* 요청 작성을 입력하고, 예를 선택하여 비밀번호로 보호된 전송과 같은 특정 컨텍스트 클래스를 지정하거나, IdP가 가장 적합한 컨텍스트 클래스를 선택하도록 하려면 아니요를 선택합니다.
2. *AuthnRequest* 문에서 *AuthnContextClass* 요청을 만들기 위해 예를 선택한 경우 *ID* 제공자 속성에 대한 *SAML 2.0* AuthnRequest에서 요청할 *AuthnContextClassRef* 메서드에서 인증에 사용할 컨텍스트 클래스의 URN을 입력합니다(표 참조).

AuthnContextClass URN 옵션

인증 유형	인증 컨텍스트 클래스 **URN**
폼 기반 인증	`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
Kerberos 기반 인증	`urn:#####:##:Windows`

기본적으로 통합은 암호로 보호된 전송 인증 방법을 사용합니다.

3. 업데이트를 클릭합니다.

(선택 사항) SAML에 대한 로그아웃 요청에 서명하기 위한 키 스토어 속성 설정

키 스토어 속성을 설정하여 통합에서 서명된 서버와 서명된 CA 인증을 사용하여 로그아웃 요청에 서명할 수 있도록 합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. *SAML 2* 요청 서명에 사용되는 *SAML 2.0 SP* 키 스토어에 저장되는 키 입력의 별칭 속성에서 SAML 2.0 키 스토어에 대해 작성한 별칭 이름을 입력하십시오.
   기본적으로 통합은 별칭 *saml2sp*를 찾습니다.
2. *SAML 2* 요청 서명에 사용되는 *SAML 2.0 SP* 키 스토어에 저장되는 키 입력의 비밀번호 속성에 SAML 2.0 키 스토어의 비밀번호를 입력하십시오.
   기본적으로 암호는 기본 별칭 이름과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 업데이트를 클릭합니다.
4. SP 메타데이터를 재생성합니다.
   자세한 내용은 SP 메타데이터를 참조하십시오.

SAML에 대한 서비스 제공자 키 스토어 생성

로그아웃 요청에 서명하기 위해 인스턴스에 대해 다음 항목을 포함하는 Java 키 스토어를 생성합니다.

시작하기 전에
필요한 역할: admin

이 태스크 정보

- 인스턴스에 대해 서명된 서버 인증서
- 서명된 CA 인증서
- 공개 및 개인 키 페어

사설 인증 기관을 통해 서명된 인증서를 직접 생성하거나 공용 인증 기관에서 구매할 수 있습니다.

다음 단계에서는 새 Java Keytool 키 저장소 파일을 생성하고, CSR(인증서 서명 요청)을 만들고, 인증서를 임포트하는 방법을 보여줍니다. 도메인의 기본 인증서를 임포트하기 전에 루트 인증서 또는 중간 인증서를 임포트해야 합니다. 명령줄 인터페이스에 다음 명령을 입력합니다.

주: 이러한 지침은 플랫폼에 국한되지 않으며 작성하려면 보안 인증서에 대한 기술 지식이 필요합니다. 기술 지원에서는 인증서 생성을 지원할 수 없습니다.

프로시저

1. Java 키 스토어와 키 페어를 생성합니다.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. 기존 Java 키 스토어에 대한 CSR을 생성합니다.

```
keytool -certreq -alias mydomain -keystore my.keystore -file
 mydomain.csr
```

3. 루트 또는 중간 인증 기관 CA 인증서를 기존 Java 키 스토어로 임포트합니다.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
 my.keystore
```

4. 서명된 기본 인증서를 기존 Java 키 스토어로 임포트합니다.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt
 -keystore my.keystore
```

SAML 요청 서명을 위한 서비스 제공자 키 스토어 설치

다음 단계를 사용하여 기존 예제 키 스토어를 제거하고 퍼블릭 및 프라이빗 키 페어가 포함된 고유한 서비스 제공자 키 스토어를 설치합니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 서비스 제공자 키 스토어를 생성합니다.
2. 다음으로 이동 **SAML 2** 1회 사용자 인증**(SSO)** > 인증서 또는 다중 제공자 > 관리자 > **x509** 인증서.
3. **SAML 2.0 Keystore_Key2048_SHA256** 클릭합니다.
4. 첨부 파일 관리**(Manage Attachments)** 링크를 누릅니다.
5. *saml2sp_key2048withsha256.jks* 옆에 있는 삭제 확인란을 선택합니다.
6. 제거를 클릭합니다.
7. 파일 선택을 클릭하고 서명된 인증서가 포함된 키 저장소를 선택합니다.
8. 연결을 클릭합니다.
9. 첨부 파일 팝업을 닫습니다.

   주: 새로 첨부된 인증서에는 다른 이름을 제공하는 것이 좋습니다.

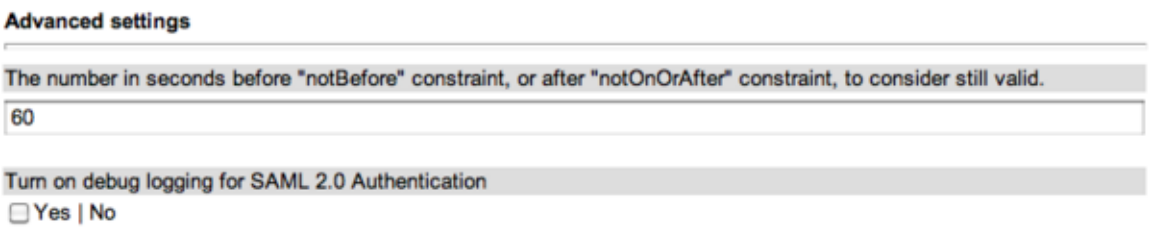
10. 키 스토어 암호*(Key store password)*에 SAML 2 별칭에 액세스하기 위한 암호를 입력합니다.
11. 업데이트를 클릭합니다.

(선택 사항) 고급 **SAML** 속성

다음 고급 설정을 사용하면 보안을 더욱 강화하고 통합을 디버깅할 수 있습니다.

고급 설정

다음으로 이동 모두 > **SAML 2** 1회 사용자 인증**(SSO)** > 속성.



고급 시스템 속성 테이블

속성	설명
"notBefore" 제약 조건 또는 "notOnOrAfter" 제약 조건 후에도 유효한 것으로 간주되는 시간(초)	IdP 클럭과 SP 클럭 간의 시간 차이를 고려하도록 *NotBefore* 및 *NotOnOrAfter* 제약 조건에 추가할 시간(초)을 입력합니다. 이러한 제약 조건은 지정된 시간 범위 내에 이루어지지 않은 요청을 거부하여 재생 공격을 방지합니다. IdP 클럭과 SP 클럭이 크게 다른 경우 네트워크 대기 시간이 발생하면 SAML 요청이 무단으로 처리될 수 있습니다. 이 속성은 SAML 요청 및 응답이 여전히 유효한 것으로 간주되는 유예 기간을 추가합니다.
SAML 2.0 인증에 대한 디버그 로깅을 켭니다.	SAML 2.0 이벤트에 대한 추가 로깅 정보를 사용하려면 예를 선택합니다.

ID 제공자 인증서 설치

식별 제공자가 서비스 제공자와의 통신을 확인할 수 있도록 PEM 인증서를 X.509 인증서 양식에 붙여 넣을 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

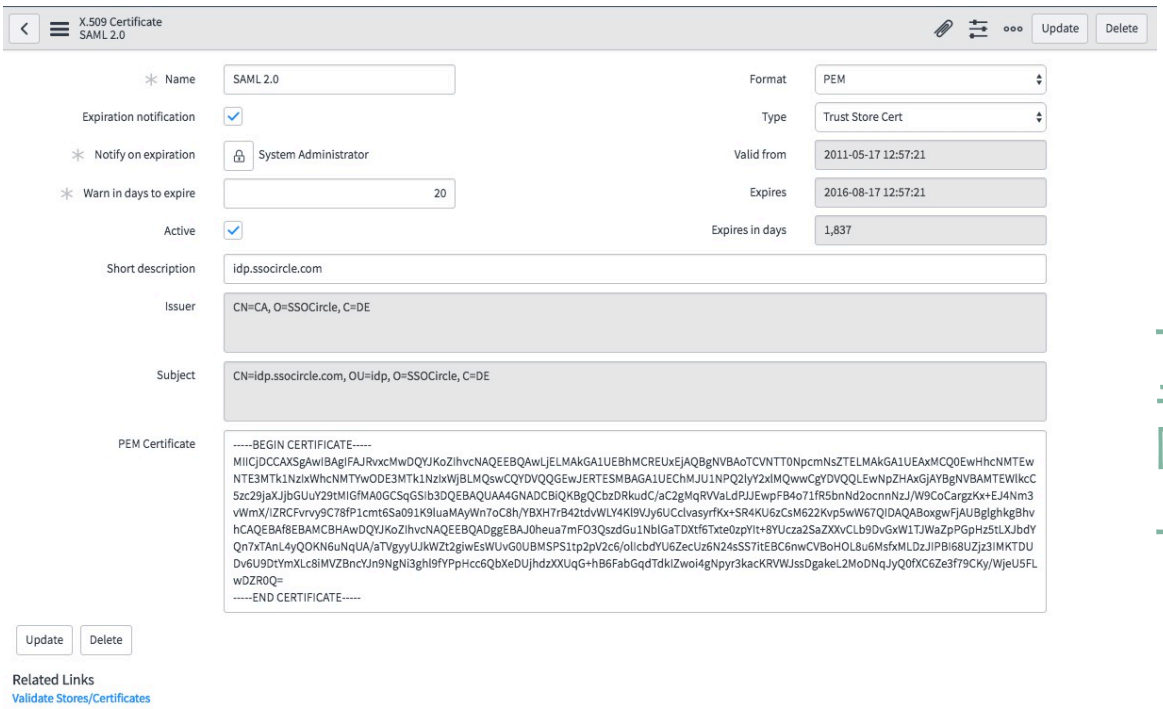
시작하기 전에
필요한 역할: 관리자

이 태스크 정보
IdP의 인증서는 IdP의 메타데이터 내에 있습니다. IdP 개발자는 로컬 IdP를 만들 때 인증서 메타데이터가 있는 위치를 결정합니다.

주: Single Sign-On에 대한 인증서는 SAML 인증서와 함께 작동하도록 항상 PEM 형식이어야 합니다.

프로시저

1. 다음으로 이동 모두 > **SAML** 1회 사용자 인증**(SSO)** > 인증서.
2. 양식 필드를 입력합니다(표 참조).
3. 저장을 클릭합니다.



주: 통합은 현재 인스턴스와 IdP 간의 통신에서 인증서에 서명하지 않습니다.

필드	설명
이름	인증서 이름입니다. 이름 항목을 변경하지 마십시오. 통합에서 X.509 인증서를 사용하려면 X.509 인증서의 이름이 *SAML 2.0* 이어야 합니다. 이 요구 사항은 를 사용하지 다중 제공자 1회 사용자 인증(SSO)않는 경우에만 적용됩니다.
만료 알림	만료 시 알림 필드에서 선택한 사용자에게 알림을 보내려면 이 옵션을 선택합니다. 기본적으로 이 기능은 사용 설정되어 있습니다.
만료 시 알림	인증서 만료와 관련된 알림을 되살릴 사용자를 선택합니다. 선택한 사용자가 없으면 기본적으로 관리자 역할을 가진 마지막 로그인한 사용자 두 명과 함께 로그인한 사용자가 추가됩니다.
만료되기 전 경고	인스턴스가 알림을 보내는 만료 전 일수입니다. 20 이상의 값을 입력합니다. Istanbul 및 이후 릴리스로 업그레이드된 인스턴스에서는 더 큰 값을 지정하지 않는 한 이 값이 20으로 설정됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
활성	이 인증서가 활성 상태임을 나타내는 확인란입니다.
형식	인증서의 형식입니다. SAML은 PEM 형식을 사용합니다.
유형	인증서 컨테이너입니다. 인스턴스는 신뢰 스토어, Java 키 스토어 및 PKCS#12 키 스토어의 인증서를 인식합니다.
유효 기간 (시작)	인스턴스가 이 필드에 유효한 인증 시작일을 자동으로 추가합니다. 인증서를 X.509 인증서 기록에 첨부하여 이 필드를 채웁니다.
만료	인스턴스가 이 필드에 인증서 만료 날짜를 자동으로 추가합니다. 인증서를 X.509 인증서 기록에 첨부하여 이 필드를 채웁니다.
며칠 후 만료	만료까지 계산된 일수입니다.
간단한 설명	인증서에 대한 설명입니다.
문제	인스턴스가 이 필드에 인증서 발급자를 자동으로 추가합니다. 인증서를 X.509 인증서 기록에 첨부하여 이 필드를 채웁니다.
제목	인스턴스는 이 필드에 제목의 인증서를 자동으로 추가합니다. 인증서를 X.509 인증서 기록에 첨부하여 이 필드를 채웁니다.
PEM 인증서	X509 인증서의 값을 입력합니다.

다음에 수행할 작업
Validate Stores/Certificates(저장소/인증서 확인)를 클릭하여 신뢰 저장소와 인증서를 테스트합니다.

SAML에 대해 누락된 인증서 교체

인증서 모듈에 빈 페이지가 표시되면 SAML 2.0 인증서 기록이 삭제된 것입니다. 인증서 기록을 수동으로 생성하여 누락된 인증서를 교체할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 인증서.
2. `SAML 2.0`이라는 새 레코드를 만듭니다.

> **중요사항:** 이 이름을 사용해야 합니다. 이 요구 사항은 를 사용하지 다중 제공자 1회 사용자 인증(SSO)않는 경우에만 적용됩니다.

3. Click **SAML 2** 1회 사용자 인증**(SSO)** > 인증서.
4. *PEM* 인증서 필드에 IdP의 메타데이터에서 `ds:X509Certificate` 요소의 값을 입력합니다.
5. 저장을 클릭합니다.

SAML 통합 테스트

다른 모든 설정 작업을 완료한 후 SAML 통합을 테스트합니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 관리자 역할을 가진 사용자로 인스턴스에 로그인합니다.
2. 다음으로 이동 **SAML 2** 1회 사용자 인증**(SSO)** > 속성.
3. 외부 인증 사용 속성에서 예를 선택합니다.

   주:

   외부 인증을 사용하려면 모든 사용자가 SAML 2.0 SSO(Single Sign-On)를 사용해야 합니다. 누군가 인증되지 않은 상태에서 애플리케이션에 액세스하려고 하면 인스턴스가 자동으로 (IdP)에 인증 요청을 전송하고 사용자를 SAML IdP 인증 페이지로 리디렉션합니다.

4. 저장을 클릭합니다.
5. 인스턴스에서 로그아웃합니다.
6. 인스턴스 URL로 이동합니다.
   통합이 제대로 작동하는 경우 IdP에서 사용자의 자격 증명을 요청해야 합니다.

관련 정보

다중 SSO(SAML 2.0) 오류 및 수정

다중 **SSO(SAML 2.0)** 오류 및 수정

다중 SSO(SAML 2.0) 설정 및 구성에 대한 일반적인 오류 및 관련 수정 사항 목록입니다.

다중 **SSO(SAML 2.0)** 설정 중 오류 발생

인스턴스 로그의 오류	연결 테스트 메시지	**SAML** 속성	진단	고정
NotAfter: <Thu Jun 05 22:57:44 PDT 2014>.	IDP x509 인증서가 있고 유효하며 활성 상태인지 확인하십시오.	해당 사항 없음	현재 인증서 또는 SAML 어설션이 만료되었습니다.	• SNC 시계를 SAML IdP 서버 시계와 동기화합니다. • SAML 2.0 인증서 기록을 업데이트합니다.
• SAML 2.0 인증서를 찾을 수 없습니다. • ServiceNow 인스턴스에 저장된 디지털 서명을 찾을 수 없습니다.	IDP x509 인증서가 있고 유효하며 활성 상태인지 확인하십시오.	PEM 형식 문자열을 PEM 인증서 필드에 입력해야 합니다.	SAML 인증서가 없습니다. 비활성 상태일 수 있습니다.	올바른 PEM 형식 인증서가 인스턴스에 업로드되었는지 확인합니다.
인증서가 일치하지 않습니다. 예상: <certStr>, 실제: <inboundCert>.	IDP x509 인증서가 있고 유효하며 활성 상태인지 확인하십시오.	해당 사항 없음	SNC에서 사용할 수 있는 인증서가 어설션의 인증서와 일치하지 않습니다. 원인은 다음과 같습니다. • 인증서가 IdP에서는 업데이트되지만 ServiceNow	SAML 2.0 인증서 기록의 PEM 형식 문자열이 사용자 IdP에 대한 SAMLResponse의 X509 인증서와 일치하는지 확인합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다중 **SSO(SAML 2.0)** 설정 중 오류 발생

인스턴스 로그의 오류	연결 테스트 메시지	**SAML** 속성	진단	고정
			인스턴스에서는 업데이트되지 않습니다. • 인증서의 형식이 잘못되었습니다.	
인증서의 유효성을 검사하지 못했습니다.	IDP x509 인증서가 있고 유효하며 활성 상태인지 확인하십시오.	해당 사항 없음	현재 인증서가 만료되었을 수 있습니다.	SAML 2.0 인증서 기록을 업데이트합니다.
서명 프로파일을 확인하지 못했습니다.	IDP x509 인증서가 있고 유효하며 활성 상태인지 확인하십시오.	해당 사항 없음	어설션이 다른 인증서로 서명될 수 있습니다.	IdP에 SNC 인스턴스와 동일한 인증서가 있는지 확인합니다.
SubjectConfirmationData 제목 확인 InResponseTo 특성이 일치하지 않습니다. 예상: <inResponseTo>, 실제: <inResponseTo>.	제목 확인 유효성 확인 실패함	해당 사항 없음	이 오류는 다음 상황 중 하나가 발생할 때 나타납니다. • IdP는 다른 SAMLRequest에 대한 SAMLResponse를 반환합니다. • 사용자가 인스턴스 URL 대신 SAMLRequest로 URL에 책갈피를 지정합니다. • null 값이 필요한 경우 인스턴스에 여러 노드가 있을 때 응답이 다른 노드로 전송될 수 있습니다.	IdP 관리자는 예상된 SAMLReponse가 반환되고 있는지 확인해야 합니다. 이 상황은 부하 분산 장치 또는 인프라 문제일 수 있습니다.
SessionIndex 값을 찾을 수 없음: <message>...	SessionIndex가 잘못되었습니다.	해당 사항 없음	SNC 인스턴스에는 SessionIndex가 필요합니다. IdP가 SAML 응답에 이를 반환하여 성공적으로 인증합니다.	IdP 관리자는 SessionIndex가 SAMLResponse에 정의되어 있는지 확인해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다중 **SSO(SAML 2.0)** 설정 중 오류 발생

인스턴스 로그의 오류	연결 테스트 메시지	**SAML** 속성	진단	고정
올바른 SubjectConfirmation이 없습니다.	제목 확인 유효성 확인 실패함	해당 사항 없음	IdP의 오류로 인해 조건이 누락될 수 있습니다. 응답의 StatusCode에는 예상되는 Success 대신 Responder가 포함됩니다.	조건이 SAMLResponse에 포함되어 있는지 확인하려면 SAMLResponse를 검토하십시오. 유효한 제목 확인 데이터가 만료되거나 올바른 대상에 대해 만료되지 않을 수 있습니다.
어설션 대상이 일치하지 않습니다. 예상: <propAudience>, 실제: <audienceUri>. 또는 AudienceRestriction 확인에 실패했습니다. 일치하는 대상을 찾을 수 없습니다.	"대상 URI" 필드가 올바로 설정되어 있는지 확인하십시오.	SAML2 토큰을 수락하는 대상 그룹 URI입니다. (일반적으로 인스턴스 URI입니다. 예: `https://demo.service-now.com`.)	SNC 인스턴스 구성 대상 그룹 URI는 IdP의 값과 일치해야 합니다.	로그의 SAMLResponse에서 〈saml2:Audience〉를 찾아 인스턴스의 값과 일치하는지 확인합니다.
어설션 발급자가 잘못되었습니다. 예상: 〈인스턴스의 값〉, 실제: 〈IdP에서 반환된 값〉	어설션 발급자가 잘못되었습니다.	사용자 정보를 포함하는 SAML2 보안 토큰을 발급하는 ID 제공자 URL입니다.	IdP 엔터티 ID(발급자)가 SNC 인스턴스에 정의된 값과 일치하지 않습니다.	• IdP 또는 SP가 제대로 구성되지 않았는지 확인합니다. • SAML 속성 (사용자 정보가 포함된 SAML2 보안 토큰을 발급하는 ID 제공자 URL)이 올바르게 설정되었는지 확인합니다.
제목은 나중에 유효합니다. Now: <now>, NotBefore: <notBefore> 또는 제목이 만료되었습니다. Now: <now>,	제목 확인 확인에 실패했습니다.	notBefore 제약 조건 또는 notOnOrAfter 제약 조건 후에 유효한 것으로 간주되는 시간(초)입니다.	IdP 클럭이 SP 클럭과 동기화되지 않습니다.	SAML 속성 glide.authenticate.sso.saml2.clockskew 더 큰 값으로 업데이트합니다. 기본값은 180초입니다. 경우에 따라 300 이상으로 설정해야 합니다. IdP 서버에서 시간을 확인해야 할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다중 **SSO(SAML 2.0)** 설정 중 오류 발생

인스턴스 로그의 오류	연결 테스트 메시지	**SAML** 속성	진단	고정
notOnOrAfter: <notOnOrAfter>				
어셜션은 미래, 현재: <now>, notBefore: <notBefore> 또는 어셜션이 만료됨: 지금: <now>, notOnOrAfter: <notOnOrAfter>	어설션이 잘못되었습니다.	notBefore 제약 조건 전이나 notOnOrAfter 제약 조건 후에 유효한 것으로 간주되는 시간(초)입니다.	IdP 시계가 SP 시계와 동기화되어 있지 않습니다.	SAML 속성을 더 큰 값으로 업데이트합니다. 기본값은 60초입니다. 경우에 따라 300 이상으로 설정해야 합니다. IdP 서버에서 시간을 확인해야 할 수도 있습니다.

일반적인 로그인 및 **IdP** 오류

오류 또는 증상	진단	고정
로그인 요청은 높은 보안이 활성 상태일 때 시스템과 IdP 간에 무한 루프를 생성합니다.	• 일반적으로 URL 엔드포인트는 오류 페이지 또는 로그아웃 페이지입니다. • logout_redirect.do는 IdP 호스트 이름을 속성 값에 추가하지 않고 정의할 *glide.security.url.whitelist* 때 이 루프를 만들 수 있습니다. 주: 이 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 URL 허용 목록 검사 강제 적용[Security Center 1.3, 1.5 및 2.0에서 업데이트됨〕.	실패한 인증 요청을 이 URL로 리디렉션하도록 시스템 속성 glide.authenticate.failed_redirect 설정(또는 생성)합니다.
사용자 또는 요청을 인증하는 데 사용되는 토큰이 예상되는 서명 알고리즘 http://www.w3.org/2000/09/xmldsig#rsa-sha1 이 아닌 서명 알고리즘 http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 로 서명됩니다.	이벤트 상세 정보는 경보 컨텍스트 탭을 확인하십시오.	신뢰 당사자 트러스트 구성 대화 상자의 고급 탭으로 이동하여 알고리즘이 SHA-256이 아닌 SHA-1로 설정되어 있는지 확인합니다.
시스템 로그(syslog) 테이블에 `## ###`	IdP(예: ADFS)가 `oasis:names:tc:SAML:2.0:status:Requester` 상태로 응답하면 IdP에서 전송된	IDP로 전송된 SAML 요청을 검토하고 IDP 관리자와 협력하여 인스턴스 SAML

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

일반적인 로그인 및 **IdP** 오류

오류 또는 증상	진단	고정
`urn:oasis:names:tc:SAML:2.0:status:Requester` 가 나타납니다.	요청에 문제가 있어 로그인을 거부했음을 의미합니다. 안타깝게도 대부분의 경우 IdP에서 받은 SAML 응답은 오류에 대한 자세한 정보를 제공하지 않습니다.	설정을 업데이트하여 오류를 방지하십시오. 로그인 실패의 이유를 이해하려면 IDP 공급자에게 문의해야 할 수도 있습니다.

1회 사용자 인증**(SSO)** 로그인 리디렉션

SSO가 활성화되면 사용자를 특정 페이지로 리디렉션하거나 사용자가 로컬로 로그인하도록 지시할 수 있습니다.

예를 들어 사용자가 `https://customerX.service-now.com` 로 이동하려고 하면 기본 로그인 페이지 대신 내부 회사 포털이 표시될 수 있습니다. 또는 사용자가 애플리케이션에서 로그아웃하면 브라우저에서 특정 내부 페이지로 리디렉션할 수 있습니다. 인스턴스 내에서 리디렉션 속성을 설정하여 사용자에게 기본 로그인 페이지가 아닌 SSO 로그인 페이지가 표시되도록 할 수 있습니다.

주: 다음 속성은 SSO를 강제 적용하지 않습니다. login.do 페이지에는 계속 액세스할 수 있으며 사용자는 로컬 암호를 설정한 경우 시스템에 로그인할 수 있습니다.

리디렉션 속성

사용자가 로그아웃하거나 SSO를 사용한 사인 온 시도가 실패한 경우 기본 포털 페이지 또는 SSO 로그인 정보가 있는 지식베이스 문서와 같이 사용자를 다음으로 이동할 위치를 정의할 수 있습니다. 다음 속성을 사용하여 URL을 지정합니다. 이러한 속성 중 하나가 인스턴스에 없는 경우 속성을 만들 수 있습니다.

glide.authenticate.failed_requirement_redirect

사용자가 비공개 페이지(예: 인시던트 보기)에 액세스하려고 할 때 SSO 자격 증명을 제공하지 않을 때 리디렉션할 URL입니다. 이 속성은 일반적으로 고객의 로그인 포털(예: `http://portal.companya.com/`)로 설정됩니다.

glide.authenticate.failed_redirect

실패한 SSO 시도 후 사용자를 리디렉션할 URL. 오류를 설명하고 유용한 링크(예: `http://portal.companya.com/error`)가 있는 퍼블릭 지식 문서로 리디렉션할 수 있습니다.

glide.authenticate.external.logout_redirect

로그아웃한 사용자를 리디렉션할 URL로, 일반적으로 Single Sign-On 로그인을 활성화한 포털(예: `http://portal.companya.com/logout`)로 돌아갑니다.

glide.authentication.external.disable_local_login

예로 설정할 경우 메인 로그인 페이지에 대한 SSO 자격 증명이 필요합니다. 기본값은 false입니다. 이 속성은 속성과 함께 사용해야 합니다 *`glide.authenticate.failed_requirement_redirect`*.

다음 표에서는 설치 종료 반환 값, 속성 및 예상 동작 간의 관계를 보여 줍니다.

SSO만 사용하여 로그인 강제 적용

값 반환	속성	동작
`failed_missing_requirement`	*`glide.authenticate.failed_requirement_redirect`*	이 값이 반환되면 세션에 없음을 나 실패하고 세션이

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SSO만 사용하여 로그인 강제 적용

값 반환	속성	동작
		리디렉션됩니다. 시도되고 자격 증 제공자의 URL입
failed_authentication	*glide.authenticate.failed_redirect*	이 값이 반환되면 인증에 실패했거 사용자가 잠겼음 실패하고 세션이 리디렉션됩니다. 시도되고 자격 증 제공자의 URL입
<*user_id*>	해당 사항 없음	<*user_id*>에서 인증된 로그인입 *glide.authen* 정의된 필드 이름 인스턴스의 필드

로컬 로그인 제한

보안 예방 조치로 리디렉션 속성에 의존하여 로컬 로그인을 금지하는 것 이상의 작업을 수행해야 합니다. 사용자가 절대로 로컬에 로그인할 수 없고 항상 내부의 Single Sign-On 시스템에서 인증을 받는 경우, 인스턴스로 가져온 각 사용자에게 임의의 암호를 할당해야 합니다. 임의 암호는 사용자 임포트 시 가장 쉽게 설정할 수 있습니다. 임포트 세트를 통해 사용자 데이터를 시스템으로 임포트하는 경우 다음 코드를 사용하여 onBefore 변환 스크립트를 만들 수 있습니다.

```
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
```

SAML 통합으로 인스턴스 복제

SAML 통합으로 인스턴스를 복제합니다. SAML 2.0을 사용하는 인스턴스를 복제하기 전에 대상 인스턴스에서 SAML SSO 관련 설정을 유지하거나 대상 인스턴스에 액세스할 수 없게 만들 수 있습니다.

시작하기 전에

필요한 역할: 관리자

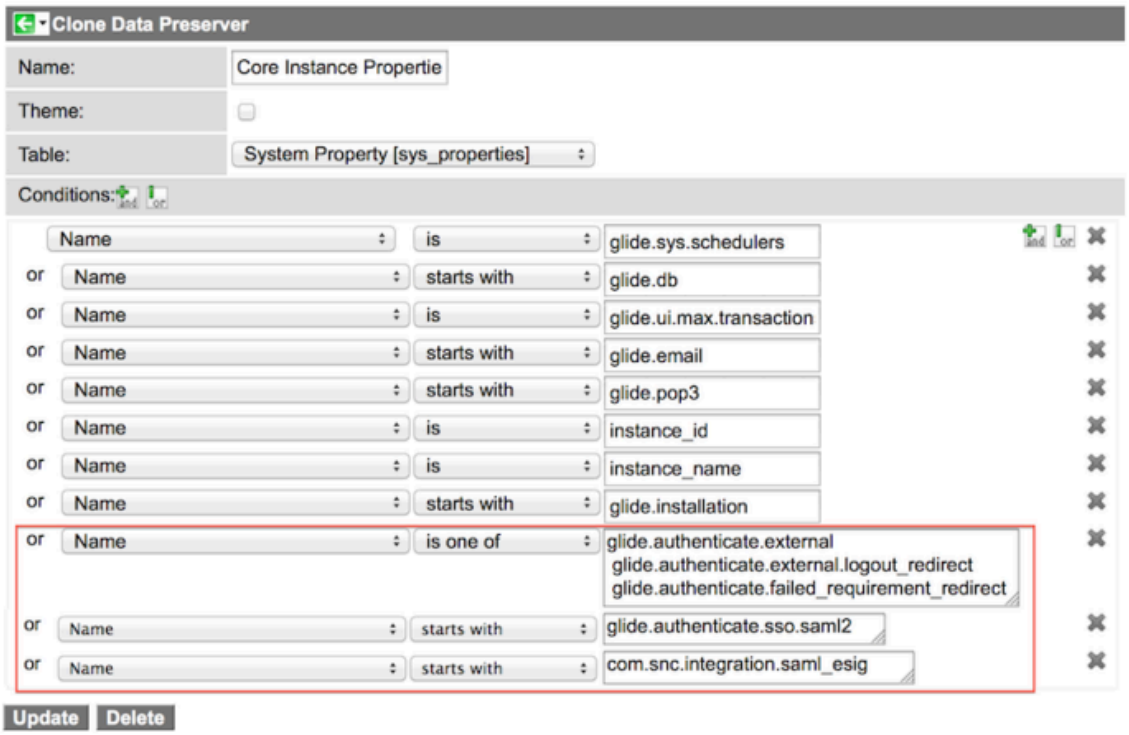
프로시저

1. 소스 인스턴스에서 다음으로 이동합니다. 시스템 클론 > 데이터 보관 > 코어 인스턴스 속성.
2. 조건을 사용하여 다음 SAML SSO 관련 속성이 유지되는지 확인합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- glide.authenticate
- glide.보안
- glide.entry
- glide.script
- glide.session
- glide.saml2
- com.glide.communications
- com.snc.integration.saml_esig



주: 클론을 만들 때 인증서가 대상 인스턴스로 전달되도록 첨부 파일을 포함합니다. 또한 인스턴스 테마를 유지하는지 여부에 관계없이 이러한 속성이 보존되도록 테마 확인란의 선택을 취소합니다.

3. 소스 인스턴스에서 다음으로 이동합니다. 시스템 클론 > 데이터 보관 SAML/SSO/다중 SSO와 관련된 sys_user sys_certificate SAML 인증서와 SAML 사용자를 보존합니다.

   필요한 경우 XML로 내보낸 다음 대상에서 수동으로 가져옵니다.

   경고: 한 시스템에서 다른 시스템으로 SAML/SSO/다중 SSO 설정을 복제하지 마십시오. 대부분의 SAML/SSO 또는 다중 SSO 설정 전송은 ID 제공자에서 구성해야 하므로 작동하지 않습니다. 작업 설정을 덮어쓰면 대상 인스턴스가 인증에 실패하여 대상 인스턴스에 액세스할 수 없게 됩니다. 또한 다중 SSO 제공자 기록의 sys_id 변경하지 마십시오. 이렇게 하면 사용자가 쿠키를 플러시해야 합니다. 복제 예방 조치에 대한 자세한 내용은 인스턴스 복제 전 검사 목록을 참조하십시오.

4. 다중 SSO 테이블sso_properties, digest_properties 및 saml2_update1_properties 제외합니다.
5. 각 인스턴스에서 독립적으로 SAML/SSO/다중 SSO 기록을 수동으로 생성하고 ID 제공자에서도 기록을 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

6. 대상 인스턴스의 sys_user(LDAP 또는 SAML에 없음) 기록과 소스 인스턴스에 없는 sys_id 사용하여 로컬 관리자 계정을 수동으로 생성해야 합니다.
7. 업데이트를 클릭합니다.

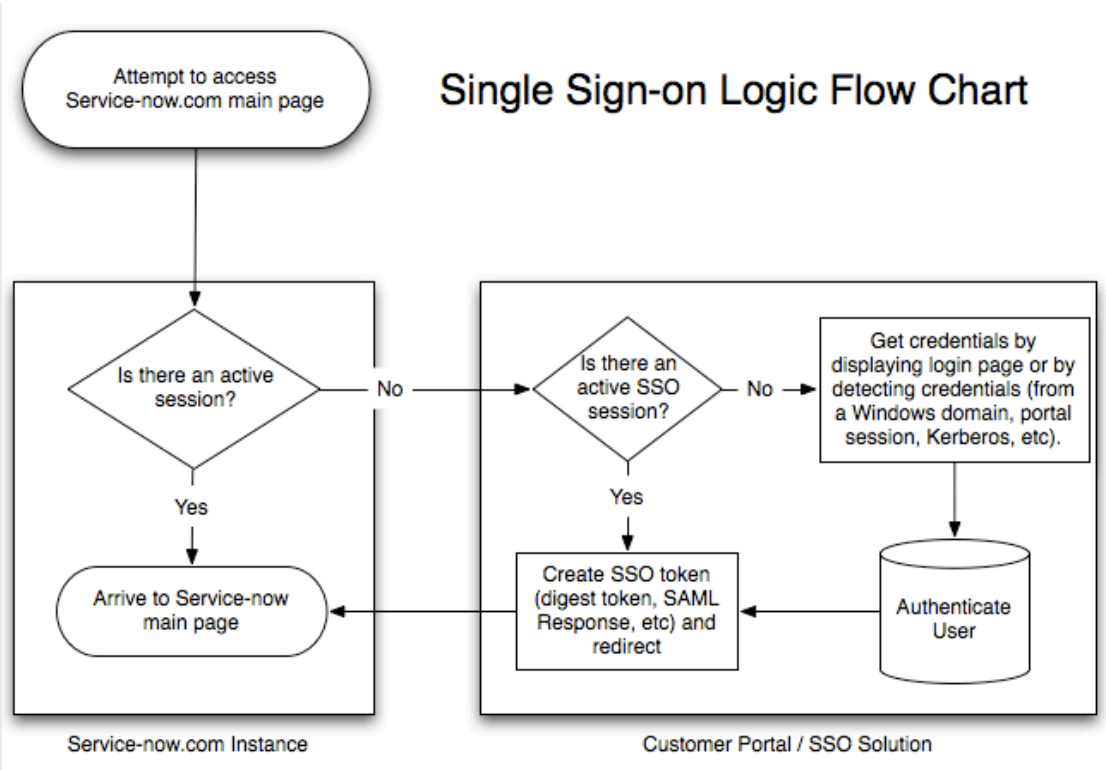
SAML 2.0 개념

이러한 SAML 개념을 숙지하십시오.

일반적인 SAML 프로세스 흐름(다이어그램)

일반적인 SSO 논리 플로우에는 활성 세션을 찾고, 사용자 자격 증명을 확인하고, 필요한 토큰을 만드는 작업이 포함됩니다.

SSO 표준



로그인(AuthnRequest) 프로세스 흐름

SAML 2.0은 웹 브라우저에서 IdP(ID 공급자), SP(서비스 공급자) 및 보안 주체(사용자) 간에 정보를 교환하는 웹 브라우저 SSO 프로필을 지정합니다.

ID 제공자는 SAML 인증 서비스를 제공하는 모든 SSO 서비스(예: SSOCircle)일 수 있습니다. 서비스 제공자는 항상 인스턴스입니다. 메시지 플로우는 서비스 제공자의 보안 자원에 대한 요청으로 시작됩니다.

SP에서 대상 자원 요청

보안 주체는 서비스 제공자에서 대상 자원을 요청합니다.

https://instance.service-now.com/

인스턴스는 요청을 검사하여 SAMLRequest 및 RelayState URL 매개변수가 있는지 확인합니다. 존재하는 경우 사용자는 이미 IdP로 검증되었으므로 2-6단계를 건너뛸 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ID 제공자에게 AuthnRequest 발급

인스턴스는 SAMLRequest 값을 사용하여 IdP로 전송될 AuthnRequest를 구성합니다. 또한 인스턴스는 ### ## URL 매개변수 값을 생성하고 전송합니다.

토큰은 서비스 제공자가 유지 관리하는 상태 정보에 대한 불투명 참조입니다. SAMLRequest 매개변수의 값은 <samlp:AuthnRequest> 요소의 수축된 base64 인코딩 값입니다.

```
<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:Au
thnRequest>
```

그러면 통합에서 <samlp:AuthnRequest> 요소를 URL 인코딩하여 SAMLRequest URL 매개변수로 전송합니다.

SSO 서비스는 URL 디코딩, base64 디코딩 및 요청 팽창을 통해 <samlp:AuthnRequest> 요소를 순서대로 처리합니다. 그런 다음 보안 검사를 수행합니다. 사용자에게 유효한 보안 컨텍스트가 없는 경우 IdP는 로그인 자격 증명을 묻는 메시지를 표시하여 사용자를 식별합니다. 사용자가 이미 로그인한 경우 IdP는 SAMLResponse<tt> # <tt>### ## URL 매개변수로 응답합니다(3단계 참조).

SAMLResponse 및 릴레이 상태로 응답

필요한 로그인 자격 증명을 수집한 후 SSO 서비스는 요청의 유효성을 검사하고 XHTML 양식이 포함된 문서로 응답합니다.

```
<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>
```

매개변수의 값은 이 단계에서 가져옵니다. SAMLResponse 매개변수의 값은 다음 <samlp:Response> 요소의 base64 인코딩입니다.

```
<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#">
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
...
      </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:NameI
D><saml:SubjectConfirmation
 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmation
Data              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:Audi
ence>https://
dloomac.service-now.com</saml:Audience></saml:AudienceRestriction></saml:
Conditions><saml:AuthnStatement AuthnInstant="2010-04-29T23:21:51Z"

 SessionIndex="s2dbf89ab99001e0e8cdaed67266d9d4b21b968a04"><saml:AuthnCon
text><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Pa
sswordProtectedTransport</saml:AuthnContextClassRef></saml:AuthnContext
></saml:AuthnStatement></saml:Assertion></samlp:Response>
```

SAMLResponse 확인

`SAMLResponse` 값은 base64로 디코딩되고 팽창되어 3단계에서 XML 문서를 표시합니다. 로그인 스크립트는 `Subject/NameID` 요소에서 XML 값을 추출하여 사용자 테이블에서 기존 사용자를 조회하는 데 사용합니다.

또한 `### ##### AuthnStatement/@SessionIndex` 요소에서 세션 ID를 추출하여 `LogoutRequest`에 저장합니다.

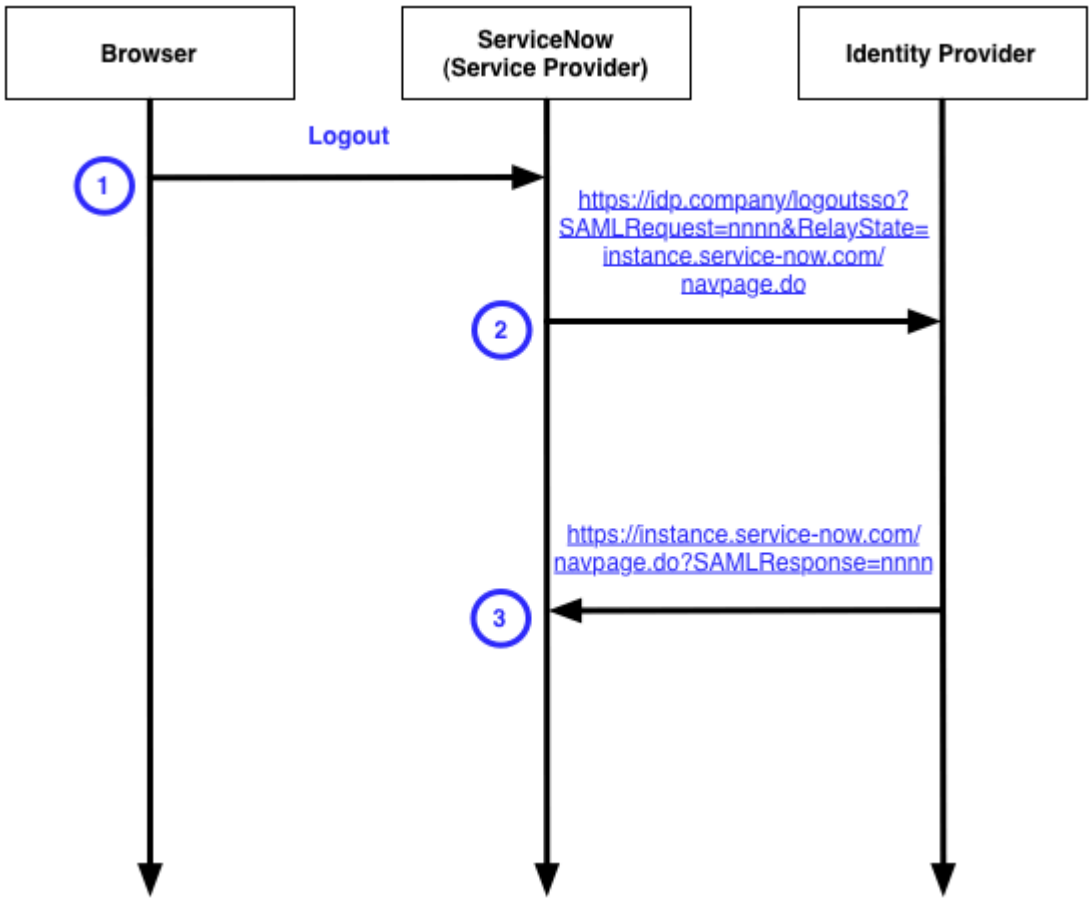
로그아웃**(LogoutRequest)** 프로세스 흐름

로그아웃 시 인스턴스는 IdP에 SAML 2.0 *LogoutRequest* 서비스 호출을 발행합니다.

이 서비스는 사용자를 로그아웃한 후 지정된 로그아웃 URL로 다시 리디렉션합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SAML 2 로그아웃



사용자가 로그아웃 버튼을 클릭합니다.

사용자가 로그아웃 버튼을 클릭하면 인스턴스가 로그아웃 스크립트를 실행합니다.

LogoutRequest 발급됨

로그아웃 스크립트는 SAML 2.0 `LogoutRequest` 를 구성하고 이를 IdP에서 미리 구성된 SingleLogoutRequest SAML 2.0 서비스에 게시합니다. IdP는 요청을 축소한 다음 base64로 인코딩합니다. `LogoutRequest`의 예는 다음과 같습니다.

```
<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:Name
ID><saml2p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104
 </saml2p:SessionIndex></saml2p:LogoutRequest>
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

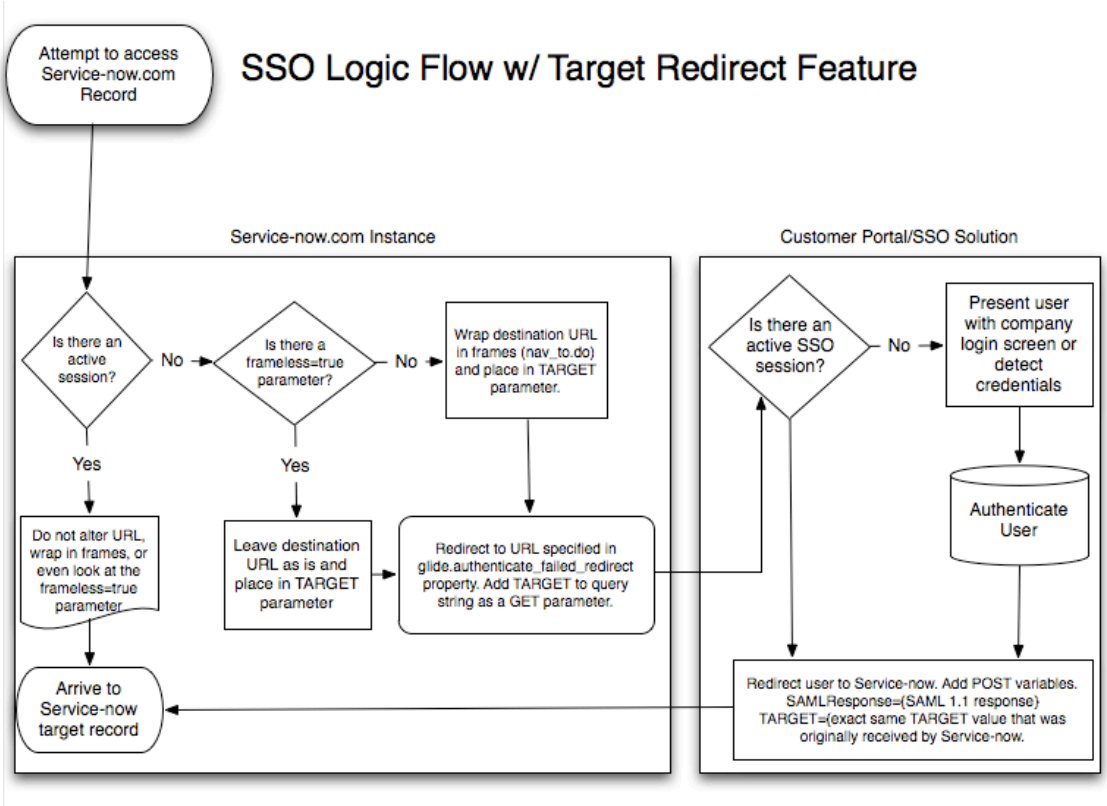
사용자 로그아웃

사용자가 IdP에서 로그아웃합니다. IdP가 인스턴스로 다시 리디렉션되고, 사용자가 로그인하지 않았으므로 인스턴스가 다시 IdP로 리디렉션됩니다.

SSO 제공자에 대한 URL 정보

SSO 세션이 필요한 인스턴스로 연결되는 URL 링크에서 발생하는 로그인 챌린지가 진행되는 동안, 인증 후 URL이 인스턴스로 다시 전달되고 올바른 자원에 링크될 수 있도록 참조 URL을 SSO 제공자에게 제공해야 할 수 있습니다.

SSO 대상 리디렉션



설치 종료 반환 값이 속성으로 정의된 URL 대신 또는 URL에 추가로 URL을 전달하도록 개선되었습니다. 일반적으로 사용자 이름 또는 미리 정의된 문자열 값을 반환하여 SSO 세션을 제어, 권한 부여 또는 이의를 제기합니다. 다음 예제에서는 URL을 전달하는 확장된 동작을 보여 줍니다.

```
return
 "failed_missing_requirement:%26amp;TARGET=https://
instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

위의 예시는 URL `https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345` TARGET이라는 URL 매개변수의 형태로 SSO 제공자에게 전달합니다.

주: SSO 제공자는 사용자 자격 증명이 수집되고 인증이 통과되면 TARGET 매개변수의 해당 정보를 사용하여 인스턴스로 다시 리디렉션한다고 가정합니다.

콜론: 두 반환 값을 구분하고 인코딩된 & (%26amp;)는 속성 *glide.authenticate.failed_missing_requirement* 과 TARGET 매개변수에 정의된 URL을 연결합니다.

다중 제공자 SSO를 사용하는 SAML 2.0 구성

복수 제공자 SSO 기능에서 SAML 2.0 SSO 구성을 생성하거나 업데이트할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보

주: 릴리스에 새로 추가된 Jakarta 릴리스에서는 IdP 구성을 활성화하기 전에 연결 테스트 기능을 사용하여 구성의 유효성을 확인해야 합니다. 업데이트 기능을 사용하여 구성 데이터를 저장할 수 있지만 연결 테스트가 성공하지 않으면 활성 구성이 아닙니다.

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. 다음 옵션 중 하나를 수행합니다.
   - 구성을 업데이트하려면 SSO 구성 기록을 클릭합니다.
   - 새 구성을 만들려면 다음을 클릭합니다. 신규 > **SAML**.
3. 다음 방법 중 하나로 IdP 정보를 입력합니다.

옵션	설명
메타데이터 설명자 URL 사용	URL 확인란을 클릭하고 사용 중인 IdP의 URL을 입력합니다.
메타데이터 설명자 XML 파일 사용	XML 확인란을 클릭하고 사용 중인 IdP에서 작성된 XML 데이터를 붙여넣습니다.
수동으로 메타데이터 입력	팝업 창을 닫고 속성 필드에 데이터를 수동으로 입력합니다.

주: ID 제공자 양식에 모든 필수 필드를 작성해야 합니다.

다중 제공자 **SSO(Single Sign-On)** 필드

속성	필수	설명
이름	예	IdP의 이름을 입력합니다. 이 IdP는 자동 리디렉션 시스템 ID입니다.
활성	예	인증에 사용할 IdP에 대해 Active를 true로 설정해야 합니다. 주: 이 속성을 설정하는 옵션은 연결 테스트가 성공한 후에만 제공됩니다.
기본값	아니요	자동 리디렉션 IdP(이전의 기본 IdP)는 사용자를 기본 인스턴스 URL에 액세스하도록 자동으로 리디렉션합니다. 이 속성은 이 IdP 구성을 기본값으로 설정합니다.
IDP 자동 리디렉션	아니요	이 IdP 구성을 자동 리디렉션 IdP로 설정합니다. 주: 새 자동 리디렉션 IdP 구성을 활성화하면 쿠키가 *glide_sso_id* 새 자동 리디렉션 IdP로 업데이트됩니다. *glide.authenticate.sso.update.idp.cookie* 자동으로 활성화된 시스템 속성이 이 기능을 제어합니다.
ID 제공자 URL	예	IdP의 URL을 입력합니다. 각 IdP URL은 고유해야 합니다.
ID 제공자의 AuthnRequest	예	SingleSignOnService 요소에서 가져온 HTTP-Redirect 바인딩에 대한 URL을 입력합니다.

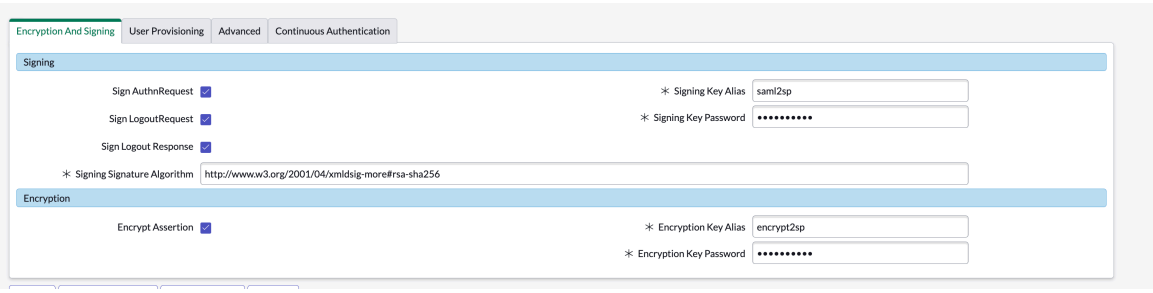
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	필수	설명
ID 제공자의 SingleLogoutRequest	아니요	SingleLogoutService 요소에서 가져온 URL을 입력합니다.
ServiceNow 홈페이지	예	IdP가 인증되는 인스턴스의 URL을 입력합니다(로그인 페이지 포함). 예: https://yourinstance.service-now.com/navpage.do
엔터티 ID/발급자	예	로그인 페이지를 제외한 기본 URL을 입력합니다. IdP가 인증하는 인스턴스의 예: https://yourinstance.service-now.com/
대상 그룹 URI	예	로그인 페이지를 제외한 기본 URL을 입력합니다. IdP가 인증하는 인스턴스의 예: https://yourinstance.service-now.com/
NameID 정책	예	통합에서 사용하는 NameIDFormat 요소의 값을 입력합니다.
외부 로그아웃 리디렉션	아니요	사용자가 로그아웃한 후 통합이 사용자를 리디렉션하는 URL을 입력합니다.
실패한 요구 사항 리디렉션	아니요	실패한 인증 요청을 리디렉션하기 위한 URL을 입력합니다. 기본적으로 IdP에서 구성한 오류 페이지 또는 로그아웃 페이지의 URL 엔드포인트입니다. glide.authenticate.failed_requirement_redirect 필드에 이 값을 채울 수 있습니다.
클라이언트 유형	아니요	클라이언트 유형에 따라 클라이언트 유형을 선택합니다. 옵션: **Iframe** 임베디드. 주: 구성에 클라이언트 유형 필드가 필요한 경우 양식을 편집하고 필드를 추가할 수 있습니다. 자세한 내용은 를 참조하십시오 OAuth 및 SSO 기록에 대한 클라이언트 유형 구성.

4. 옵션: 암호화 및 서명 탭

주:

- 암호화 및 서명에 사용자 고유의 인증서를 사용하는 것이 좋습니다.
- **FIPS** 승인 모드에는 암호화 및 서명을 위해 다른 인증서가 필요합니다.
- 인증서를 사용하는 동안 다음 시스템 속성을 인증서의 sys_id(x.509 인증서)으로 업데이트해야 합니다.
  - 서명 (`glide.authenticate.sso.saml2.keystore`)
  - 암호화 (`glide.authenticate.sso.saml2.encryption.keystore`)
- ID 제공자 기록에서 서명 및 암호화 키 저장소의 키 별칭 및 키 암호를 업데이트하고 메타데이터를 생성해야 합니다(메타데이터 생성 선택).
- 생성된 메타데이터(XML)에 있는 서명 및 암호화 인증서를 ID 제공자에게 업로드합니다.



기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 및 서명 필드

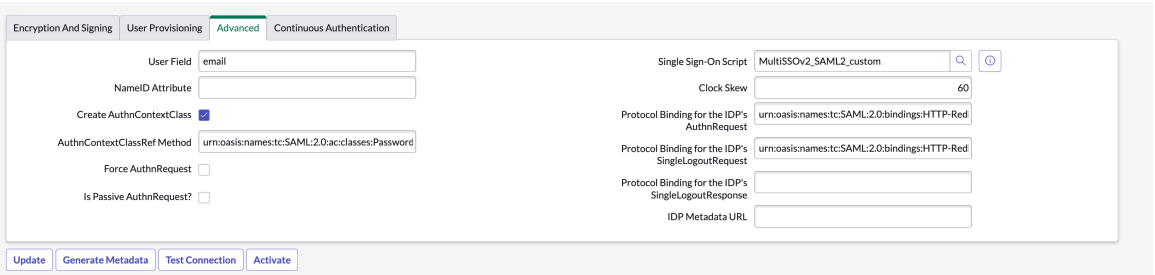
속성	설명
서명 키 별칭	SAML 2.0 SP 키 스토어에 저장되는 키 입력의 서명 별칭을 입력합니다.
서명 키 암호	SAML 2.0 SP 키 스토어에 저장되는 키 입력의 서명 암호를 입력하십시오.
암호화 키 별칭	SAML 2.0 SP 키 스토어에 저장된 키 항목의 암호화 별칭을 입력합니다.
암호화 키 암호	SAML 2.0 SP 키 스토어에 저장된 키 입력의 암호화 암호를 입력합니다.
어설션 암호화	SAML 응답에서 어설션을 암호화하려면 확인란을 선택합니다. IDP에 대해 생성된 메타데이터에는 x509 인증서가 포함되며, IDP는 이 인증서를 생성하여 생성되는 SAML 응답의 어설션을 암호화하는 데 사용합니다.
서명 알고리즘	전자 서명을 인증을 위해 SAML 2.0 ID 제공자 AuthnRequest 소비자를 가리키는 URL을 입력합니다.
AuthnRequest에 서명	IdP SSO(Single Sign-On) 서비스가 서명된 AuthnRequest를 수신할 수 있도록 하려면 이 확인란을 선택합니다.
LogoutRequest에 서명	IdP SSO(Single Sign-On) 서비스가 서명된 LogoutRequest를 수신할 수 있도록 하려면 확인란을 선택합니다.
로그아웃 응답 서명	IdP SSO(Single Sign-On) 서비스가 서명된 로그아웃 응답을 수신할 수 있도록 하려면 이 확인란을 선택합니다.

5. 옵션: 사용자 프로비저닝 탭

사용자 프로비저닝 필드

속성	설명
자동 프로비저닝 사용자	자동 사용자 프로비저닝을 활성화하고 IdP에서 제공한 정보를 기반으로 인스턴스 사용자 테이블에 사용자가 없을 때 사용자를 작성합니다.
각 로그인 시 사용자 기록 업데이트	사용자가 SAML을 사용하여 로그인할 때마다 인스턴스 사용자 테이블의 사용자 정보를 IdP의 정보로 업데이트합니다.

6. 옵션: 고급 탭



고급 필드

속성	설명
사용자 필드	IdP가 사용자를 식별하는 데 필요한 값이 포함된 필드를 사용자 테이블에 입력합니다. 응답의 일부로 지정된 고유 ID입니다. 예를 들어 사용자 이름, 직원 ID 등이 있습니다. 시스템 사용자 테이블에서 이 고유 ID는 사용자 상세 정보와 일치합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

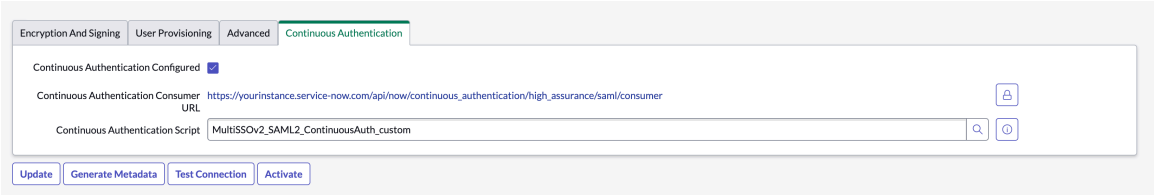
속성	설명
NameID 속성	새 NameID 정책을 구성하지 않는 한 이 필드를 비워 둡니다. 새 정책을 구성하는 경우 시스템은 로그인하는 사용자를 식별하는 데 사용해야 하는 사용자 테이블이 필요합니다. 시스템은 NameID 토큰을 여기에서 해당 사용자 테이블 필드의 이름과 일치시킵니다.
AuthnContextClass 작성	암호 보호 전송과 같은 특정 컨텍스트 클래스를 지정하려면 확인란을 선택합니다. 확인란의 선택을 취소하면 IdP는 가장 적합한 컨텍스트 클래스를 선택합니다.
AuthnContextClassRef 메서드	IdP에서 사용자를 인증하는 데 사용할 로그인 메커니즘의 URN을 입력합니다.
AuthnRequest 강제 적용	AuthnRequest를 강제로 실행하려면 확인란을 선택합니다.
소극적 AuthnRequest임	AuthnRequest가 수동인 경우 확인란을 선택합니다.
1회 사용자 인증(SSO) 스크립트	Single Sign-On 스크립트를 선택합니다. 기본값은 *MultiSSOV2_SAML2_custom*입니다.
로그아웃 응답 서명	이 필드에 로그아웃 응답 상세 정보를 입력합니다.
클럭 오차	SAMLResponse nonce를 구성하는 두 속성 사이의 시간(초)을 입력합니다. 기본값은 60입니다. 올바른 SAMLResponse는 *notBefore* 와 *notOnOrAfter* 날짜-시간 값 사이에 있어야 합니다. 샘플 SAMLResponse 메시지는 SubjectConfirmation 및 SubjectConfirmationData 요소가 포함된 샘플 SAML 2 응답 및 AudienceRestrictions 및 Audience 요소가 포함된 샘플 SAML 2 응답을 참조하십시오.
IDP의 SingleLogoutReuqest에 대한 프로토콜 바인딩	SingleLogoutService 요소의 Binding 특성에 나열된 지원되는 값 중 하나를 입력합니다.
IDP 속성을 임포트하는 메타데이터 URL	IdP 속성은 이 URL에서 임포트됩니다. 설정하면 이전 인증서가 만료된 경우 IdP에서 SAML 인증서를 자동으로 임포트할 수 있습니다. **주:** SAML2 업데이트 1에서 다중 제공자 SSO로 업그레이드하거나 SSO 연결을 수동으로 설정하는 경우 IdP 메타데이터 URL이 자동으로 채워지지 않습니다.
요청	요청의 일부인 고유 ID이며 ID는 사용자 이름, 직원 ID 등이 될 수 있습니다. **주:** 요청에 대해 리디렉션 및 사후 바인딩이 모두 지원됩니다. 이 필드를 설정하는 옵션은 연결 테스트가 성공한 후에만 나타납니다. 자세한 내용은 IdP 연결 테스트 문서를 참조하십시오.
응답	응답의 일부인 고유 ID이며 ID는 사용자 이름, 직원 ID 등이 될 수 있습니다. **주:** 응답에는 리디렉션 및 사후 바인딩이 모두 지원됩니다. 이 필드를 설정하는 옵션은 연결 테스트가 성공한 후에만 나타납니다. 자세한 내용은 IdP 연결 테스트 문서를 참조하십시오.

7. 옵션: Continuous Authentication(연속 인증) 탭에서 다음 필드를 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 연속 인증 탭은 라이센스가 필요한 제로 트러스트 -com.snc.zero_trust_continuous_authentication(연속 인증) 플러그인을 설치할 때만 나타납니다.
- 연속 인증 정책을 사용하여 테이블 또는 데이터 클래스에 대한 액세스를 보호하는 경우 을 참조하십시오 연속 인증.



연속 인증

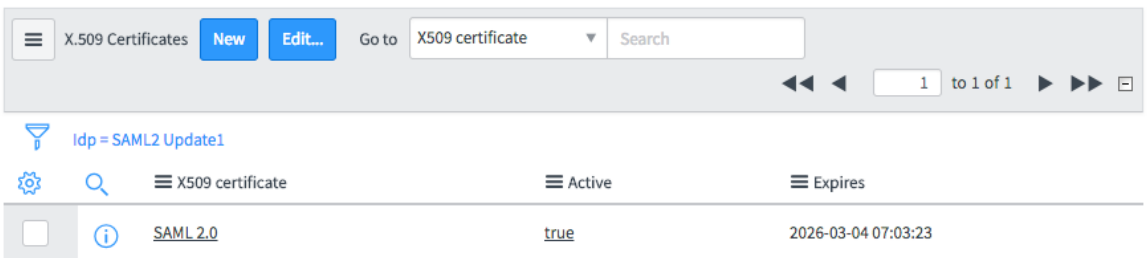
필드	설명
연속 인증 구성됨	구성을 활성화하려면 확인란을 선택합니다.
연속 인증 소비자 URL	ID 제공자의 소비자 URL을 제공합니다.
연속 인증 스크립트	(Optional) 조회 아이콘을 선택하여 플랫폼에서 제공되는 스크립트를 선택합니다. 이 구성에서 SAML의 경우: **MultiSSOv2_SAML2_ContinuousAuth_custom**

SAML에 대한 **X.509** 인증서

SAML 구성에 필요한 IdP 인증서를 저장하고 활성화합니다.

X.509 인증서는 SAML 구성에서 사용하는 IdP 인증서입니다. 인증서를 설치한 후 필요한 만큼 인증서를 추가할 수 있습니다. 인증이 여러 개 있는 경우 시스템은 발견된 첫 번째 활성 인증을 사용합니다. **IDP** 속성을 임포트하는 메타데이터 URL의 URL을 설정하면 인증서가 더 이상 유효하지 않을 때 시스템에서 자동으로 IdP에 현재 유효한 인증서를 폴링합니다. 이 인증서가 인스턴스에 추가되고 활성 SAML 구성에 사용됩니다.

주: 폴링은 네트워크 외부에서 IdP에 액세스할 수 있는 경우에 발생합니다.



SAML 가이드가 있는 둘러보기

SAML 가이드가 있는 둘러보기를 사용하여 1회 사용자 인증(SSO)에 대한 SAML을 구성합니다.

SAML 가이드가 있는 둘러보기는 교육을 받고 인스턴스에 대한 SSO를 구성하는 데 도움이 됩니다 ServiceNow® . 관리자는 가이드가 있는 둘러보기를 선택하여 인스턴스에 대한 SSO를 구성할 때 필요한 작업을 빠르게 파악할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

가이드가 있는 둘러보기를 사용하기 전에 선호하는 신원 확인 제공자(예: Okta, Microsoft Azure, ADFS 등)에서 SAML 애플리케이션을 구성해야 합니다. SAML 애플리케이션을 구성하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오.

- Okta: Okta의 경우 다음을 수행해야 합니다.
  - Okta SAML 애플리케이션 추가
  - 용 SAML 2.0 구성 ServiceNow®
- Microsoft Azure: 와 1회 사용자 인증(SSO) 통합 ServiceNow®
- 핑: 를 사용하여 SAML SSO 구성 ServiceNow®
- ADFS: SAML 2.0과 통합

SAML 가이드가 있는 둘러보기를 사용하려면 통합 - 다중 제공자 1회 사용자 인증(SSO) 설치 관리자 플러그인을 활성화하십시오. 자세한 내용은 복수 제공자 SSO 플러그인 활성화 문서를 참조하십시오.

SAML 가이드가 있는 둘러보기를 사용하려면 다음 단계를 따르세요.

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. 새로 만들기를 클릭합니다.
3. **SAML**을 선택합니다.
4. 도움말 아이콘을 클릭합니다.
5. 둘러보기를 클릭합니다.

SAML 가이드가 있는 둘러보기: 둘러보기의 일부로 제공된 단계와 지침에 따라 여러 페이지에 걸쳐 일련의 단계를 사용하여 구성을 완료하고 둘러보기를 완료합니다. SAML 구성에 대한 자세한 내용은 문서를 참조하십시오 다중 제공자 SSO를 사용하는 SAML 2.0 구성.

SAML 2.0과 다른 기능 통합

SAML 2.0 솔루션을 전자 서명, 딥 링크 및 ADFS와 같은 다른 기능과 통합할 수 있습니다.

SAML에 대한 딥링크 지원 추가

딥링크를 사용하면 인스턴스가 시스템의 특정 기록에 대한 직접 이메일 링크를 지원할 수 있습니다.

SAML 2.0 통합을 활성화하면 IdP가 사용자를 원래 요청한 URL로 리디렉션하기 전에 딥 링크 URL이 인증 검사를 통과해야 합니다. 예를 들어 다음 URL이 포함된 이메일이 있다고 가정해 보겠습니다.
`https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`

인스턴스는 IdP에 인증 요청을 보내고 `### ##` URL 매개변수를 사용하여 원래 요청된 자원을 보존합니다(이 경우 `uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`). IdP가 사용자를 인증한 후 인스턴스는 릴레이 상태 URL 매개변수의 값을 읽고 사용자를 요청된 자원(인스턴스에 있는 경우)으로 리디렉션합니다.

딥 링크에 대한 지원을 추가하려면 ID 제공자가 `### ##` URL 매개변수를 지원하는지 확인합니다.

SAML 2.0과 **ADFS** 통합

복수 제공자 SSO 플러그인은 ServiceNow SAML 2를 지원합니다. Microsoft ADFS와의 1회 사용자 인증(SSO) 통합.

ADFS 설치 및 구성에 대한 자세한 내용은 ADFS(Active Directory Federation Services) 개요를 참조하십시오. ADFS 2.0, 3.0, Azure AD와의 SAML 2.0 SSO 통합으로 구성 및 테스트된 다중 공급자 SSO 플러그인은 다음에서 SAML 응답을 지원하지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SAML에 대한 **ADFS** 설정

SAML용 ADFS를 설정합니다. 이 절차에서는 ADFS 2.0을 사용하며 ADFS 웹 사이트로 samportal.example.com 보여 줍니다. 이 주소를 ADFS 웹 사이트 주소로 바꾸십시오.

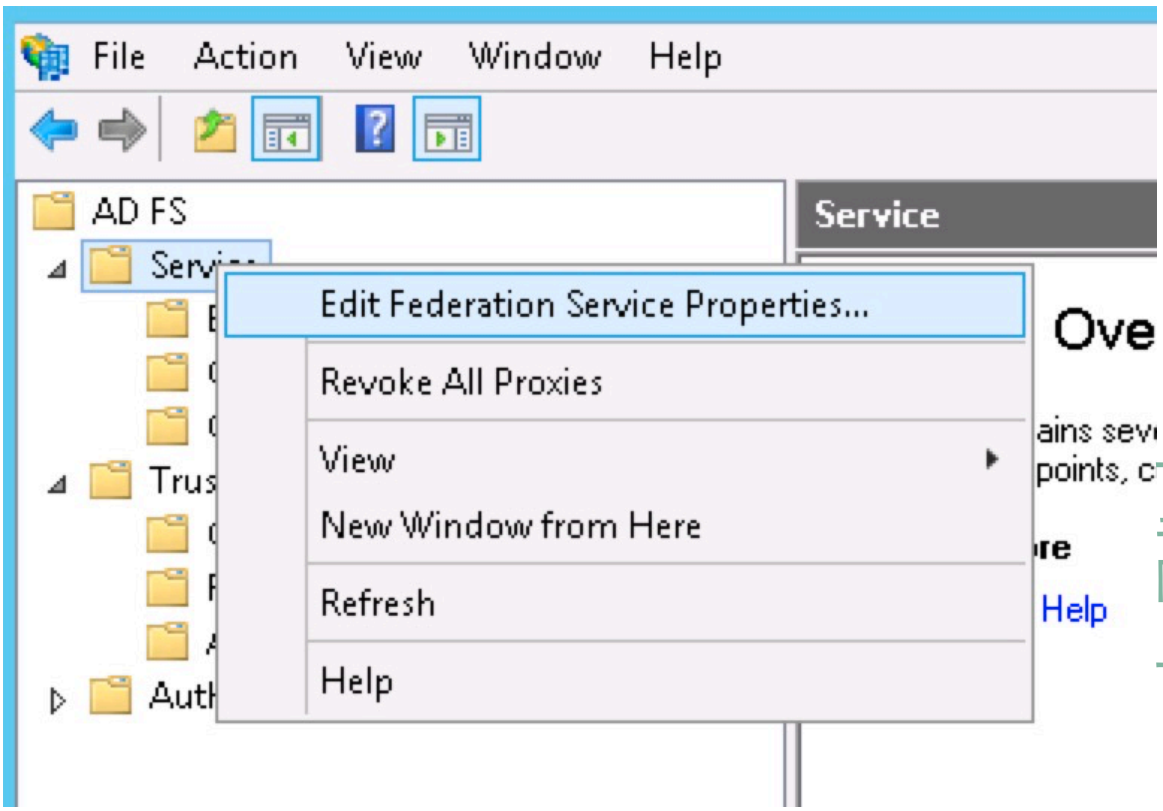
시작하기 전에

필요한 역할: 관리자

프로시저

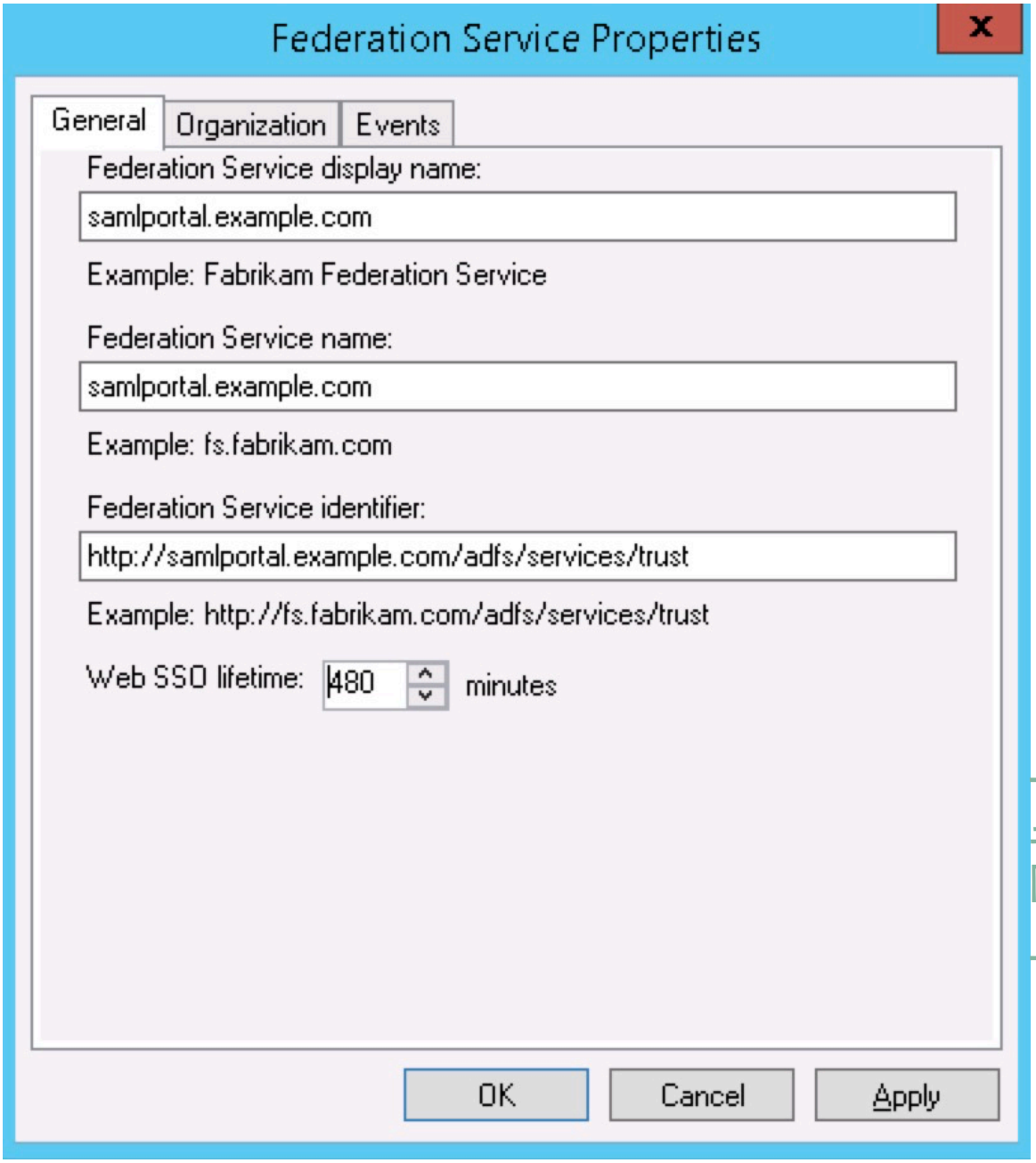
1. ADFS 3.0 서버에 로그인하고 관리 콘솔을 엽니다.

2. 서비스를 마우스 오른쪽 단추로 클릭하고 페더레이션 서비스 속성 편집을 선택합니다.



3. 일반 설정이 DNS 항목 및 인증서 이름과 일치하는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 인증서를 찾아 토큰 서명 인증서를 익스포트합니다.

a. 인증서를 마우스 오른쪽 버튼으로 클릭하고 인증서 보기를 선택합니다.

b. 상세정보 탭을 선택합니다.

c. 파일에 복사를 클릭합니다.
인증서 내보내기 마법사가 열립니다.

d. 다음을 선택합니다.

e. 아니요, 개인 키를 내보내지 않습니다 옵션이 선택되어 있는지 확인하고 다음을 클릭합니다.

f. DER로 인코딩된 이진 **X.509(.cer)**를 선택하고 다음을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

g. 파일을 저장할 위치를 선택하고 이름을 지정한 후 다음을 클릭합니다.

h. 마침을 선택합니다.
인스턴스를 사용하려면 이 인증서가 PEM 형식이어야 합니다. 클라이언트 도구 또는 SSL Shoppers와 같은 온라인 도구를 사용하여 이 인증서를 변환할 수 있습니다.

5. 방금 만든 DER/이진 인증서를 사용하고 표준 PEM 형식으로 익스포트합니다.

ADFS에 대한 인스턴스 설정

ADFS와 함께 작동하도록 인스턴스 및 SAML 2.0 설정을 구성합니다.

시작하기 전에

SAML에 대해 ADFS를 설정한 후에만 이러한 단계를 수행합니다. 이 프로세스에 대한 자세한 내용은 SAML에 대한 ADFS 설정을 참조하세요.

필요한 역할: 관리자

프로시저

1. 아직 활성화되지 않은 경우 복수 제공자 SSO 플러그인 활성화.
2. 를 구성 SAML하되 IdP 인증서를 설치할 때 에서 생성한 SAML에 대한 ADFS 설정PEM 인증서를 첨부합니다.
3. 저장을 클릭합니다.
4. 문제 및 제목 필드에 값이 있고 오류가 없는지 확인합니다.
오류가 발생하면 메모장에 저장된 PEM 형식 인증서를 열고 인증서를 복사하여 PEM 인증서 필드에 붙여넣습니다.
5. SAML2SingleSignon_update1 설치 종료가 활성 상태인지 확인하십시오.
6. SAML 2.0 구성을 계속합니다.

> 주: ADFS 서버에서 인증서가 업데이트되면 업데이트된 인증서도 인스턴스에 업로드해야 합니다.

ADFS 신뢰 당사자 구성

인스턴스 메타데이터를 가져와서 ADFS 서버로 임포트합니다. 그러나 신뢰 당사자의 수동 구성은 구현하기가 더 쉬운 것으로 보입니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자 > **SAML2** 업데이트**1** > 암호화 및 서명 SAML 속성 Sign AuthnRequest(*glide.authenticate.sso.saml2.require_signed_authnrequest*)가 활성 상태가 아닌지 확인합니다.
ADFS 관리자가 서명된 요청이 필요한지 확인할 수 있는 경우에만 이 속성을 활성 상태로 유지합니다.
2. SAML 2 메타데이터 링크를 통해 생성된 메타데이터를 복사하여 파일에 저장합니다.
3. ADFS 서버에 로그인하고 관리 콘솔을 엽니다.
4. 신뢰 당사자 트러스트를 선택합니다.
5. 창의 오른쪽 위 모서리에서 신뢰 당사자 트러스트 추가를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

추가 마법사가 나타납니다.

6. 시작을 클릭하여 시작합니다.
7. 파일 가져오기 옵션을 사용하여 메타데이터 파일을 가져옵니다.
8. 표시 이름(예: `ServiceNow`)을 지정하고 원하는 메모를 입력합니다.
9. **ADFS 3.0** 프로파일을 선택합니다.
10. 토큰 암호화 인증서는 선택하지 마십시오.
    이미 내보낸 서비스에 정의된 인증서를 사용합니다. 인증서를 정의하면 인스턴스와의 적절한 통신이 차단됩니다.
11. **URL** 구성에서 설정을 활성화하지 마십시오.
12. 연결한 인스턴스 사이트를 신뢰 당사자 트러스트 식별자로 입력합니다.
    이 경우 `https://company.service-now.com` 사용하고 추가를 클릭합니다.
13. 모든 사용자가 이 신뢰 당사자에 액세스할 수 있도록 허용합니다.
14. 다음**(Next)**을 클릭하고 완료 시 클레임 열기**(Open the Claims when this finishes)** 확인란의 선택을 취소합니다.
15. 이 페이지를 닫습니다.
    새 신뢰 당사자 트러스트가 창에 나타납니다.
16. 신뢰 당사자 트러스트를 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
17. 고급 탭으로 이동하여 보안 해시 알고리즘을 SHA-256 또는 SHA-1로 설정합니다.
18. 엔드포인트 탭으로 이동하여 **Post** 바인딩과 `https://company.service-now.com/navpage.do` URL을 사용하여 **SAML Assertion Consumer**를 추가합니다.

ADFS 신뢰 당사자 클레임 규칙 구성

클레임 규칙을 편집하여 인스턴스와 적절한 통신을 가능하게 합니다.

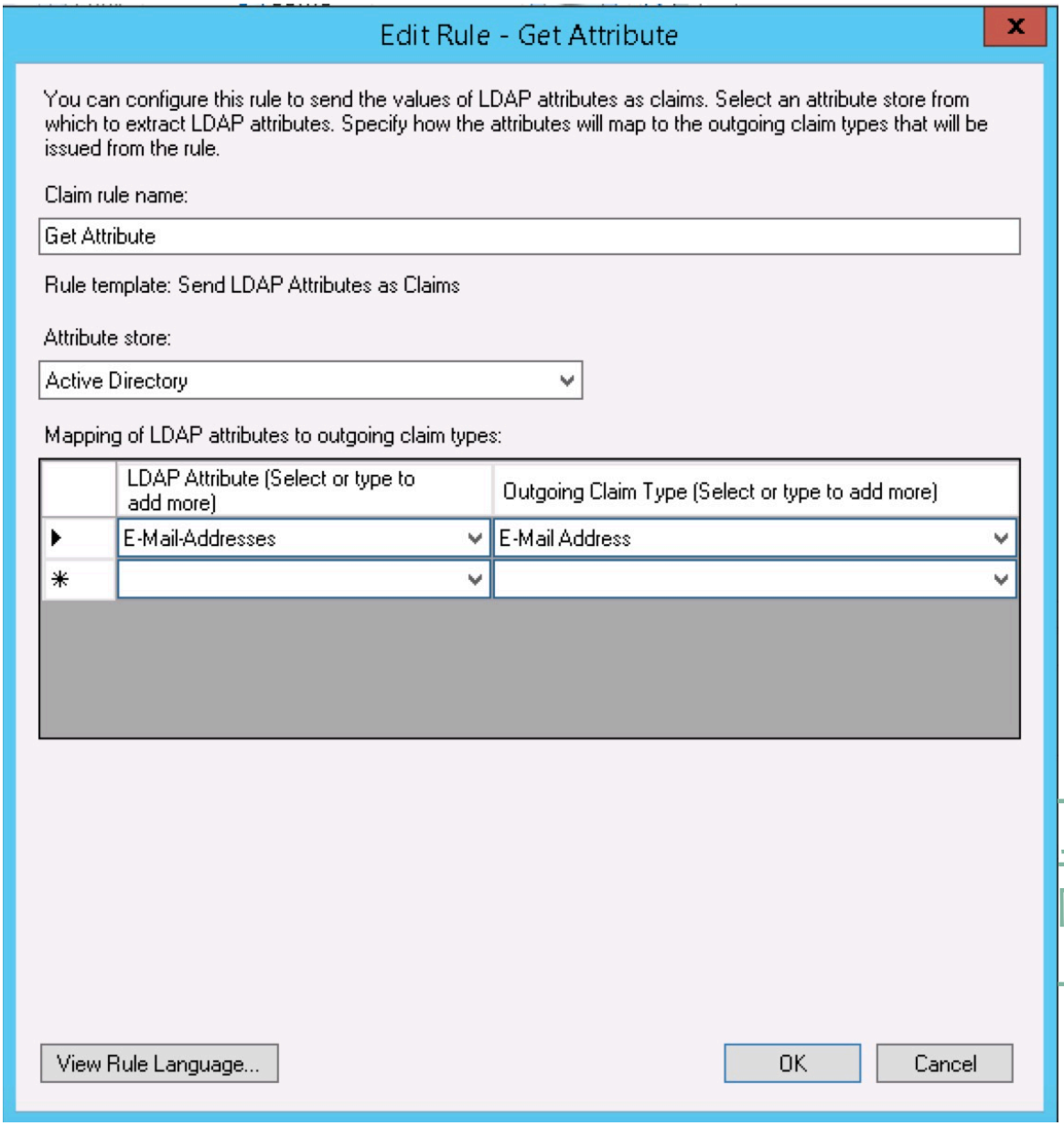
시작하기 전에

필요한 역할: 관리자

프로시저

1. ADFS 서버에 로그인하고 관리 콘솔을 엽니다.
2. 신뢰 당사자 트러스트를 마우스 오른쪽 단추로 클릭하고 클레임 규칙 편집을 선택합니다.
3. 발급 변환 규칙 탭을 클릭합니다.
4. 규칙 추가를 선택합니다.
5. 사용할 클레임 규칙 템플릿으로 **LDAP** 속성을 클레임으로 보내기를 선택합니다.
6. 클레임에 `LDAP ## ####`와 같은 이름을 지정합니다.
7. 특성 저장소를`Active Directory`로 설정하고, **LDAP** 특성을`## ## ###` 설정하고, 보내는 클레임 유형을`## ## ###` 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



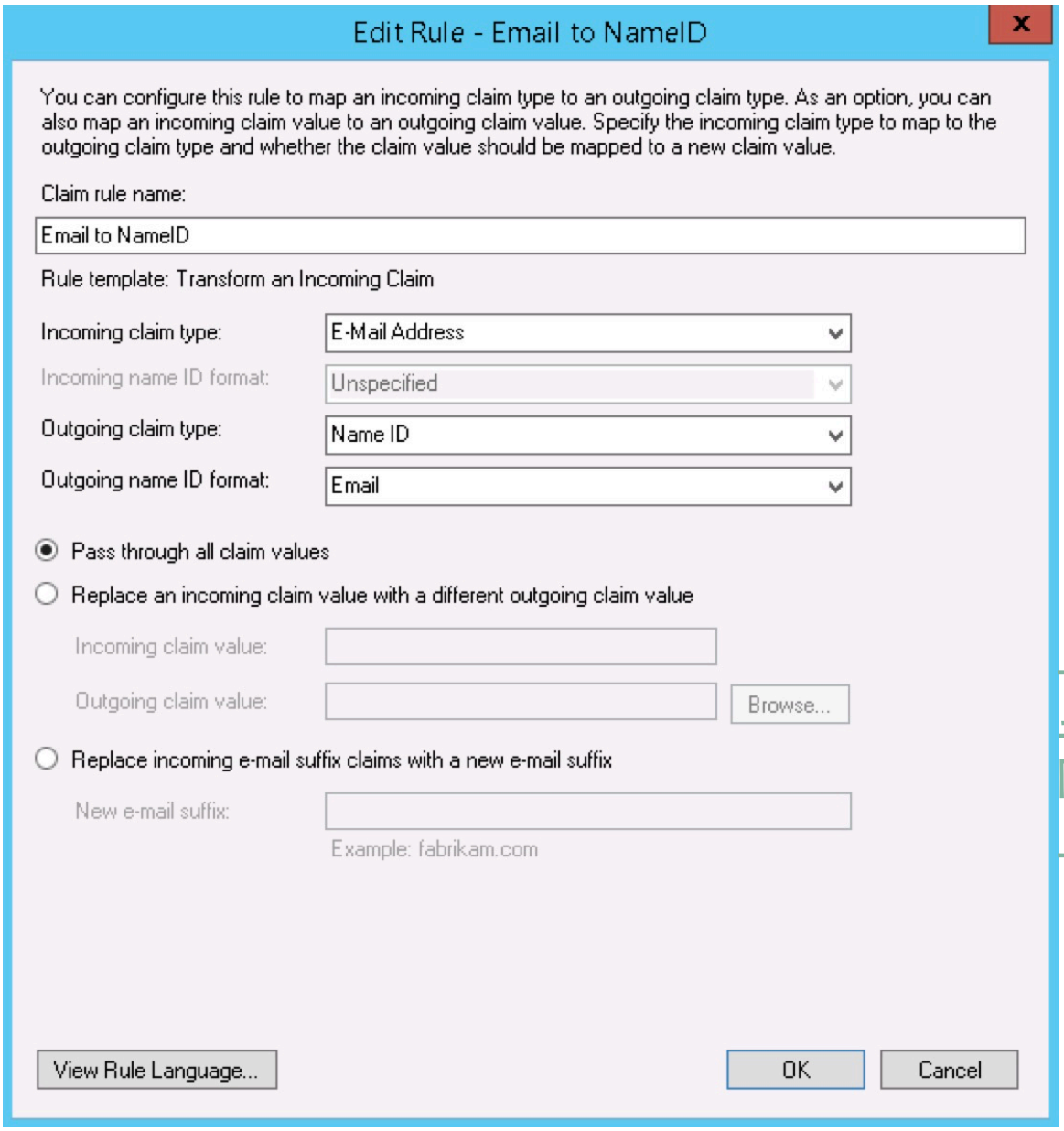

```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccoun
tname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory",
types =
 ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
"),
query = ";mail;{0}", param = c.Value);
```

8. 마침을 선택합니다.
9. 규칙 추가를 선택합니다.
10. 사용할 클레임 규칙 템플릿으로 수신 클레임 변환을 선택합니다.
11. `#### ### ## ID`와 같은 이름을 지정합니다.
12. 수신 클레임 유형을 이전 규칙의 나가는 클레임 유형으로 설정합니다.
    예: `## ## ##`.
13. 발신 클레임 유형을`## ID`로 설정하고 발신 이름 **ID** 형식을`####` 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 이러한 값은 SAML 2.0 구성 중에 정의한 이름 ID 정책 과 일치해야 합니다.

14. 모든 클레임 값 통과를 선택합니다.



이 클레임 규칙은 다음 규칙 언어와 유사해야 합니다.

```
c:[Type ==
 "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type =
 "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifie
r",
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. 마침을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SAML 로그아웃 엔드포인트 작성

단일 로그아웃을 허용하는 SAML 로그아웃 엔드포인트를 작성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
자세한 내용은 ADFS 로그아웃에 대한 이 문서를 참조하세요.

프로시저

1. 이동 **ADFS** 관리자 > 신뢰 관계 > 신뢰 당사자 트러스트 > 속성.
2. 엔드포인트 탭에서 **SAML** 추가를 클릭합니다.
3. 설정을 구성합니다.
   - 엔드포인트 유형: SAML 로그아웃
   - 제본: POST
   - 신뢰할 수 있는 **URL**: ADFS 서버의 URL입니다. 예:

     ```
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
     ```

   - 응답 **URL**: 애플리케이션 로그아웃 URL입니다. 예:

     ```
     https://{instancename}.service-now.com/external_logout_complete.do
     ```

ADFS 구성 테스트

ADFS 구성을 테스트하여 ID 공급자로 제대로 작동하는지 확인합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. Internet Explorer 브라우저를 엽니다.
2. ADFS 포털로 이동합니다.

   예: `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx`. 이 페이지에는 구성된 모든 신뢰 당사자 트러스트의 드롭다운 목록이 포함되어 있습니다.

3. 인스턴스와 연결된 신뢰 당사자를 선택합니다.
4. 계속을 클릭하여 로그인합니다.

   SAML 2.0 외부 인증을 올바르게 구성한 경우에는 인스턴스에 자동으로 로그인됩니다.

5. `https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://company.service-now.com` 로 이동하여 직접 로그인 URL을 테스트합니다.

(임시 해결책) 서비스 제공자 시작 인증 사용

SAML 2.0 업데이트 1이 없기 때문에 인증이 실패할 경우 이 임시 해결책을 사용합니다. 이 문제는 사용자가 IdP 인증을 건너뛰고 인스턴스로 직접 이동하려고 할 때 발생할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
이 오류는 인스턴스가 SAMLResponse의 SPNameQualifier 속성에 필요한 정의 및 의미 체계를 ADFS에 제공하지 않을 때 발생합니다.

다음 작업 중 하나를 수행하여 서비스 제공자가 시작한 인증을 활성화합니다.

프로시저
- SAML 2.0 업데이트 1로 업그레이드하고 AuthnContextClass 요청을 생성하는 옵션을 선택 취소합니다.
- SAML 2.0이 활성화된 경우(SAML 2.0 업데이트 1이 아님) `SPNameQualifier` 속성의 정의를 주석으로 처리하도록 **SAML2** 스크립트 포함을 수정합니다.

  createNameID 및 createNameIDPolicy 함수에서 다음 줄을 주석으로 처리합니다.

```
//nid.setSPNameQualifier (serviceURL ) ;

 //nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

다음에 수행할 작업
인스턴스에 액세스할 때 ADFS 서버의 로그인 프롬프트가 표시되지 않도록 하려면 다음 SAML 2.0 업데이트 1 속성을 false로 설정합니다. AuthnRequest 문 ()*glide.authenticate.sso.saml2.createrequestedauthncontext*에서 **AuthnContextClass** 요청을 생성합니다.

(임시 해결책) **Kerberos** 인증 지원

SAML 2.0 통합에서 인증 컨텍스트를 폼 기반 인증에서 Windows 기반 인증으로 변경하는 임시 해결책이 제공됩니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
현재 SAML 2 통합은 PasswordProtectedTransport 또는 "양식 기반 인증" 인증 컨텍스트를 사용합니다. 이 인증 컨텍스트를 사용하려면 IdP가 사용자에게 인증 자격 증명 양식을 제공해야 합니다. Kerberos를 사용하면 설정된 Windows 로그인을 통해 SAML 세션이 이미 활성화되어 있으므로 사용자는 IdP로 인증할 필요가 없습니다.

프로시저
1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. **SAML2** 업데이트**1** IdP 기록을 엽니다.
3. **ID** 제공자에 대한 **SAML 2.0** AuthnRequest에 포함될 **AuthnContextClassRef** 메서드를 다음 중 하나로 설정합니다.

AuthnContextClassRef 메서드 값
`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` (기본값)
`urn:#####:##:Windows`

4. 업데이트를 클릭합니다.

SAML 2.0과 **Azure AD** 통합

Azure AD(Azure Active Directory)와 통합합니다 ServiceNow .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Azure AD와 통합 ServiceNow 하면 다음을 수행할 수 있습니다.

- 에 액세스할 ServiceNow수 있는 Azure AD의 제어
- 사용자가 Azure AD 계정으로 자동으로 로그인할 ServiceNow 수 있도록 합니다.
- Azure Portal에서 계정을 관리합니다.

필수 구성요소

시작하려면 다음을 수행해야 합니다.

- Azure AD 구독. 구독이 없는 경우 무료 계정을 얻을 수 있습니다.
- SSO(Single Sign-On)를 ServiceNow 사용할 수 있습니다.
- San Diego 버전 이상을 지원하는 인스턴스 또는 테넌트 ServiceNow 입니다ServiceNow.
- ServiceNow 테넌트에서 복수 제공자 SSO(Single Sign On) 플러그인을 사용하도록 설정해야 합니다.
- 자동 구성의 경우 에 대한 ServiceNow다중 제공자 플러그인을 활성화합니다.

구성에 대한 작업 세트

다음은 Azure AD를 구성하기 위해 수행해야 하는 작업 집합입니다.

- 갤러리에서 Azure AD에 추가합니다 ServiceNow .
- Azure AD SSO 구성
- Azure AD 테스트 사용자 만들기
- Azure AD 테스트 사용자 할당
- ServiceNow 구성

갤러리에서 추가 **ServiceNow**

갤러리에서 Azure AD의 관리되는 SaaS 앱 목록에 추가합니다 ServiceNow .

시작하기 전에

필요한 역할: Azure 관리자

프로시저

1. Microsoft 계정을 사용하여 Azure Portal에 로그인합니다.
2. 왼쪽 창에서 **Azure Active Directory** 서비스를 선택합니다.
3. 다음으로 이동 엔터프라이즈 애플리케이션 > 모든 애플리케이션.
4. 새 애플리케이션을 추가하려면 새 애플리케이션을 선택합니다.
5. 갤러리에서 추가 섹션에서 검색 상자에 입력합니다 ServiceNow .
6. 결과 패널에서 선택한 ServiceNow 다음, 앱을 추가합니다.
7. 앱이 테넌트에 추가되는 동안 몇 초 정도 기다립니다.

Azure AD SSO 구성

Azure Portal에서 Azure AD SSO를 구성합니다.

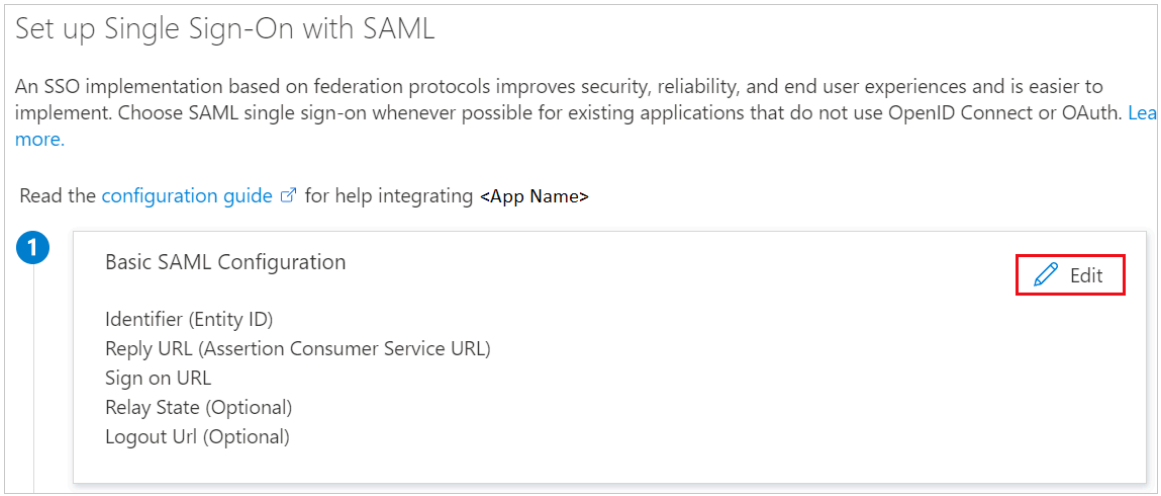
시작하기 전에

필요한 역할: Azure 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. Azure Portal ServiceNow 의 애플리케이션 통합 페이지에서 관리 섹션을 찾습니다.
2. Single Sign-On을 선택합니다.
   Single Sign-On 방법 선택 페이지에서 SAML을 선택합니다.
3. SAML을 사용하여 Single Sign-On 설정 페이지에서 기본 SAML 구성에 대한 펜 아이콘을 선택하여 설정을 편집합니다.



4. 기본 SAML 구성 섹션에서 다음을 수행합니다.

   a. 로그온 **URL**에 다음 URL 패턴 중 하나를 입력합니다.

   ```
   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>
   ```

   주: 이 URL 내에 sys_id 제공해야 합니다.

   b. 식별자(엔터티 ID)에 `https://<instance-name>.service-now.com` 패턴의 URL을 입력합니다.

   c. 회신 **URL**에 다음 URL 패턴 중 하나를 입력합니다.

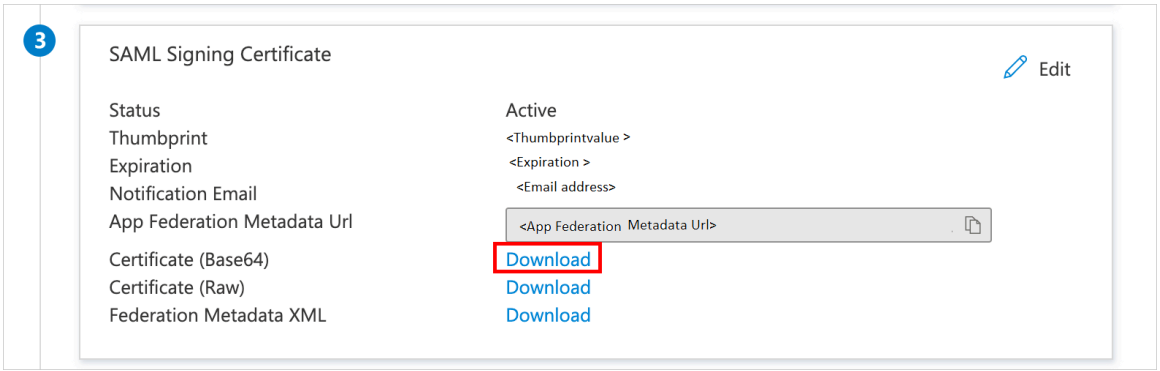
   ```
   https://<instancename>.service-now.com/navpage.do
   https://<instancename>.service-now.com/customer.do
   ```

   d. 로그아웃 URL에 `https://<instancename>.service-now.com/navpage.do` 패턴의 URL을 입력합니다.

   주: 실제 로그온 URL, 회신 URL, 로그아웃 URL 및 식별자를 업데이트해야 합니다. 이러한 URL에 표시된 값은 데모 목적입니다.

5. SAML로 Single Sign-On 설정 페이지의 SAML 서명 인증서 섹션에서 인증서**(Base64)**를 찾습니다.

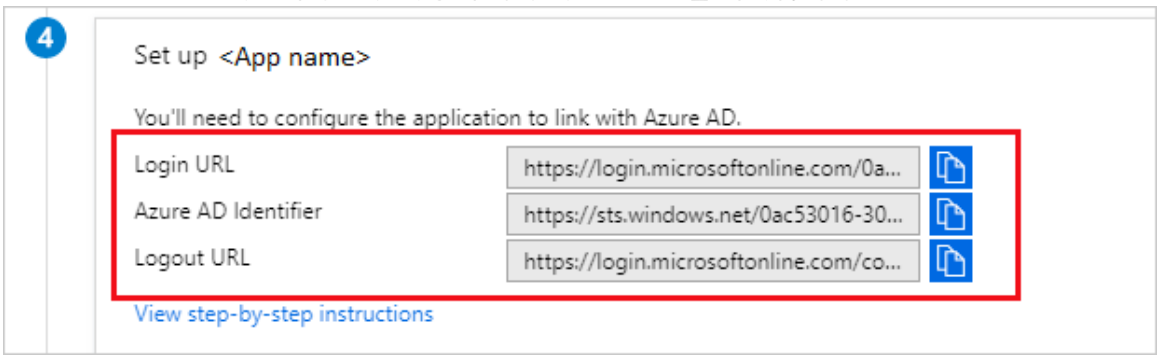
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



a. 복사 단추를 선택하여 앱 페더레이션 메타데이터 **URL**을 복사하고 메모장에 붙여넣습니다. 추가 구성에 이 URL이 필요합니다.

b. 다운로드를 선택하여 인증서(Base64)를 다운로드합니다.

6. 설정 ServiceNow 섹션에서 요구 사항에 따라 적절한 URL을 복사합니다.



Azure AD 테스트 사용자 만들기

Azure AD에서 테스트 사용자를 만듭니다.

시작하기 전에
필요한 역할: Azure 관리자

프로시저

1. Azure Portal에서 모두 > **Azure Active Directory** > 사용자 > 모든 사용자.
2. 새 사용자를 선택합니다.
3. 사용자 속성에서 다음 정보를 제공합니다.
   - 이름
   - 사용자 이름
   - 암호
4. 생성을 클릭합니다.

Azure AD 테스트 사용자 할당

에 ServiceNow대한 액세스 권한을 부여하여 Azure Single Sign-On을 사용하도록 생성된 Azure AD 테스트 사용자를 할당합니다.

시작하기 전에
필요한 역할: Azure 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. Azure Portal에서 모두 > 엔터프라이즈 애플리케이션 > 모든 애플리케이션.
2. 애플리케이션 목록에서 을 선택합니다 ServiceNow.
3. 앱 페이지의 관리 섹션에서 사용자 및 그룹을 선택합니다.
4. 사용자 추가를 선택합니다.
5. 할당 추가 창에서 사용자 및 그룹을 선택합니다.
6. 사용자 및 그룹 창의 사용자 목록에서 생성된 `### ####` 선택합니다.
7. 필요한 경우 역할 선택 드롭다운에서 할당된 사용자의 역할을 선택합니다.
8. 할당 추가 창에서 할당을 선택합니다.

ServiceNow 구성

SSO를 사용하도록 Azure AD 세부 정보로 구성합니다 ServiceNow .

시작하기 전에
플러그인: `## - ## ### SSO(Single Sign-On) ## ###`

복수 제공자 SSO 속성을 활성화합니다.

- ◦ 복수 공급업체 **SSO** 사용을 선택합니다.
  ◦ 모든 **ID** 제공자로부터 사용자 테이블로 사용자 자동 임포트 활성화를 선택합니다.
  ◦ 복수 공급업체 **SSO** 통합에 디버그 로깅 사용을 선택합니다.
  ◦ 이메일을 입력합니다.....

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. ID 공급자 페이지에서 새로 만들기를 선택합니다.
3. ID 공급자 창에서 **SAML**을 선택합니다.
4. ID 제공자 메타데이터 임포트에서 다음 중 하나를 수행할 수 있습니다.
   ◦ **URL**: ID 제공자 구성 페이지의 세부 정보를 자동으로 채우는 앱 페더레이션 메타데이터 URL입니다.
   ◦ 임포트: XML을 임포트하여 ID 제공자 구성 페이지의 상세 정보를 임포트합니다.
5. 화면 위쪽을 마우스 오른쪽 단추로 클릭하고 **sys_id** 복사를 클릭한 다음 이 값을 기본 **SAML** 구성 섹션에서 로그온 **URL**에 사용합니다.
6. 양식의 필드에 내용을 입력합니다.

다중 제공자 **SSO(Single Sign-On)** 필드

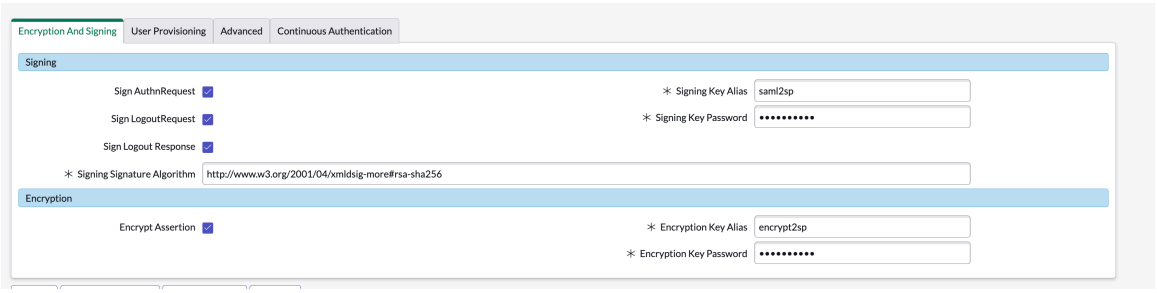
속성	필수	설명
이름	예	IdP의 이름입니다. 이 IdP는 자동 리디렉션 시스템 ID입니다.
활성	예	인증에 사용할 IdP에 대해 Active를 true로 설정해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	필수	설명
		주: 이 속성을 설정하는 옵션은 연결 테스트가 성공한 후에만 제공됩니다.
기본값	아니요	자동 리디렉션 IdP(이전의 기본 IdP)는 사용자를 기본 인스턴스 URL에 액세스하도록 자동으로 리디렉션합니다. 이 속성은 이 IdP 구성을 기본값으로 설정합니다.
IDP 자동 리디렉션	아니요	자동 리디렉션 IdP로 설정할 수 있는 IdP 구성입니다. 주: 새 자동 리디렉션 IdP 구성을 활성화하면 쿠키가 *glide_sso_id* 새 자동 리디렉션 IdP로 업데이트됩니다. *glide.authenticate.sso.update.idp.cookie* 자동으로 활성화된 시스템 속성이 이 기능을 제어합니다.
ID 제공자 URL	예	IdP의 URL입니다. 각 IdP URL은 고유해야 합니다.
ID 제공자의 AuthnRequest	예	SingleSignOnService 요소에서 가져온 HTTP-Redirect 바인딩에 대한 URL입니다.
ID 제공자의 SingleLogoutRequest	아니요	SingleLogoutService 요소에서 가져온 URL입니다.
ServiceNow 홈페이지	예	IdP가 인증하는 인스턴스의 URL입니다(로그인 페이지 포함). 예: https://yourinstance.service-now.com/navpage.do
엔터티 ID/발급자	예	IdP가 인증하는 인스턴스의 로그인 페이지를 제외한 기본 URL입니다. 예: https://yourinstance.service-now.com/
대상 그룹 URI	예	IdP가 인증하는 인스턴스의 로그인 페이지를 제외한 기본 URL입니다. 예: https://yourinstance.service-now.com/
NameID 정책	예	통합에서 사용하는 NameIDFormat 요소의 값입니다.
외부 로그아웃 리디렉션	아니요	사용자가 로그아웃한 후 통합이 사용자를 리디렉션하는 URL입니다.
실패한 요구 사항 리디렉션	아니요	실패한 인증 요청을 리디렉션하기 위한 URL입니다. 기본적으로 IdP에서 구성한 오류 페이지 또는 로그아웃 페이지의 URL 엔드포인트입니다. glide.authenticate.failed_requirement_redirect 필드에 이 값을 채울 수 있습니다.

7. 옵션: 암호화 및 서명 탭

주: 암호화 및 서명에 사용자 고유의 인증서를 사용합니다.

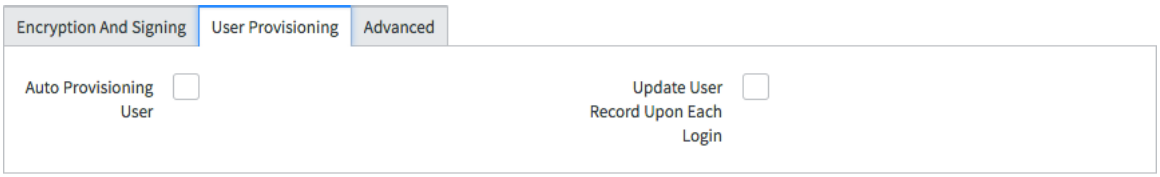


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

암호화 및 서명 필드

속성	설명
서명/암호화 키 별칭	SAML 2.0 SP 키 스토어에 저장되는 키 입력의 별칭.
서명 키 암호	SAML 2.0 SP 키 스토어에 저장되는 키 입력의 암호.
어설션 암호화	SAML 응답의 어설션을 암호화하는 확인란입니다. IDP에 대해 생성된 메타데이터에는 x509 인증서가 포함되며, IDP는 이 인증서를 생성하여 생성되는 SAML 응답의 어설션을 암호화하는 데 사용합니다.
서명 알고리즘	전자 서명을 인증을 위해 SAML 2.0 ID 제공자 AuthnRequest 소비자를 가리키는 URL입니다.
AuthnRequest에 서명	IdP SSO(Single Sign-On) 서비스가 서명된 AuthnRequest를 수신할 수 있도록 하는 확인란입니다.
LogoutRequest에 서명	IdP SSO(Single Sign-On) 서비스가 서명된 LogoutRequest를 수신할 수 있도록 하는 확인란입니다.

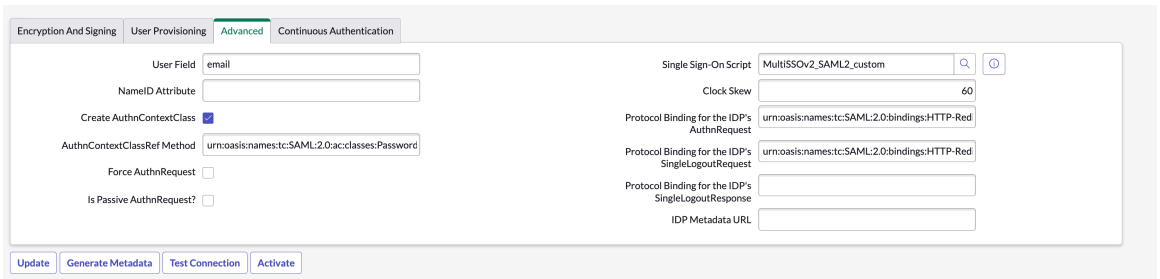
8. 옵션: 사용자 프로비저닝 탭



사용자 프로비저닝 필드

속성	설명
자동 프로비저닝 사용자	자동 사용자 프로비저닝, IdP에서 제공한 정보를 기반으로 인스턴스 사용자 테이블에 사용자가 없을 때 사용자를 작성합니다.
각 로그인 시 사용자 기록 업데이트	사용자가 SAML을 사용하여 로그인할 때마다 IdP의 정보로 인스턴스 사용자 테이블의 사용자 정보를 업데이트합니다.

9. 옵션: 고급 탭



고급 필드

속성	설명
사용자 필드	IdP가 사용자를 식별하는 데 필요한 값을 포함하는 사용자 테이블의 필드입니다. 이 고유 ID는 응답의 일부입니다. 예를 들어 사용자 이름, 직원 ID 등이 있습니다. 시스템 사용자 테이블에서 이 고유 ID는 사용자 상세 정보와 일치합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	설명
NameID 속성	새 NameID 정책을 구성하지 않는 한 비워 두는 필드입니다. 새 정책을 구성하는 경우 시스템은 로그인하는 사용자를 식별하는 데 사용해야 하는 사용자 테이블이 필요합니다. 시스템이 NameID 토큰을 해당 사용자 테이블 필드의 이름과 일치시킵니다.
AuthnContextClass 작성	암호로 보호된 전송과 같은 특정 컨텍스트 클래스를 지정하는 확인란입니다. 확인란의 선택을 취소하면 IdP는 가장 적합한 컨텍스트 클래스를 선택합니다.
AuthnContextClassRef 메서드	IdP에서 사용자를 인증하는 데 사용할 로그인 메커니즘의 URN입니다.
AuthnRequest 강제 적용	AuthnRequest를 강제로 발생시키는 확인란입니다.
소극적 AuthnRequest임	AuthnRequest가 수동인 경우의 확인란입니다.
1회 사용자 인증(SSO) 스크립트	1회 사용자 인증(SSO) 스크립트. 기본값은 *MultiSSOV2_SAML2_custom*입니다.
로그아웃 응답 서명	이 필드의 로그아웃 응답 상세 정보입니다.
클럭 오차	SAMLResponse nonce를 구성하는 두 속성 사이의 N수(초)입니다. 기본값은 60입니다. 올바른 SAMLResponse는 *notBefore* 와 *notOnOrAfter* 날짜-시간 값 사이에 있어야 합니다. 샘플 SAMLResponse 메시지는 SubjectConfirmation 및 SubjectConfirmationData 요소가 포함된 샘플 SAML 2 응답 및 AudienceRestrictions 및 Audience 요소가 포함된 샘플 SAML 2 응답을 참조하십시오.
IDP의 SingleLogoutReuqest에 대한 프로토콜 바인딩	SingleLogoutService 요소의 Binding 특성에 나열된 지원되는 값 중 하나입니다.
IDP 속성을 임포트하는 메타데이터 URL	이 URL에서 IdP 속성을 임포트합니다. 설정하면 이전 인증서가 만료된 경우 IdP에서 SAML 인증서를 자동으로 임포트할 수 있습니다. 주: SAML2 업데이트 1에서 다중 제공자 SSO로 업그레이드하거나 SSO 연결을 수동으로 설정하는 경우 IdP 메타데이터 URL이 자동으로 채워지지 않습니다.
요청	요청의 일부인 고유 ID입니다. ID는 사용자 이름, 직원 ID 등이 될 수 있습니다. 주: 요청에 대해 리디렉션 및 사후 바인딩이 모두 지원됩니다. 이 필드를 설정하는 옵션은 연결 테스트가 성공한 후에만 나타납니다. 자세한 내용은 IdP 연결 테스트 문서를 참조하십시오.
응답	응답의 일부인 고유 ID입니다. ID는 사용자 이름, 직원 ID 등이 될 수 있습니다. 주: 응답에는 리디렉션 및 사후 바인딩이 모두 지원됩니다. 이 필드를 설정하는 옵션은 연결 테스트가 성공한 후에만 나타납니다. 자세한 내용은 IdP 연결 테스트 문서를 참조하십시오.

10. 페이지의 오른쪽 위 모서리에서 연결 테스트를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

11. 자격 증명을 입력하십시오.
    SSO 로그아웃 테스트 결과가 표시됩니다.
12. 활성화를 선택하여 구성을 활성화합니다.

외부 인증을 사용하는 이메일 링크

다이제스티브 토큰 외부 인증을 사용할 때 이메일 링크를 사용할 수 있지만 이메일 알림에서 링크를 처리하는 방법을 설정해야 합니다.

기본 링크에는 SSO 자격 증명이 포함되지 않은 경우 인시던트나 변경 요청과 같은 인스턴스의 특정 위치로 안내하는 URL이 포함되어 있습니다. 다음은 인스턴스 로그인 페이지에 로그인하지 않고 사용자를 인스턴스의 위치로 안내하는 예입니다.

- /demo 인스턴스에 연결하는 암호화되지 않은 HTTP 기술(특정 기록으로 이동하지 않음):

```
https://<instance
 name>.service-now.com/?SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vg
U24tbE=
```

- 사용자가 먼저 회사의 자체 로그인 포털로 이동할 수 있도록 특정 기록에 대한 링크(이메일 알림에서):

```
https://login.company_portal_page.com/nav_to.do?uri=incident.do?sys_id=
009f8eda0a0a0b2b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsys
parm_query=active=true
```

  회사 포털 페이지의 URL을 포함하도록 인스턴스에서 속성을 설정해야 *glide.email.override.url* 합니다. 이 속성이 없으면 생성할 수 있습니다.

- 그런 다음 회사 포털은 해당 URL을 사용하여 인스턴스에 대한 리디렉션 URL을 생성하여 특정 레코드에 액세스하는 데 필요한 세그먼트를 유지하고 URL 끝에 SSO 자격 증명을 추가해야 합니다.

```
https://<instance
 name>.service-now.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2
b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=acti
ve=true&SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vgU24tbE=
```

SAML에 대한 전자 서명 지원 추가

SAML(Security Assertion Markup Language) 2.0 업데이트 1을 사용하는 전자 서명에 대해 다음 속성을 구성합니다.

다중 SSO에서 전자 서명이 활성 상태인 경우 SAML 속성이 사용되지 않습니다. 시스템이 SAML2 업데이트1 속성 [saml2_update1_properties] 테이블에 전자 서명 속성을 추가합니다.

속성	설명	기본값
전자 서명 인증용 Assertion Consumer Index	엔드포인트를 식별하는 인덱스 번호입니다.	1
전자 서명 인증용 Assertion Consumer URL	소비자를 식별하는 URL입니다.	`https://yourinstance.service-now.com/consumer.do`
전자 서명 인증용 AuthnRequest URL	인증을 위한 URL	안 함

SAML 1.0 또는 SAML 2.0(업데이트 1 제외)과 함께 전자 서명을 사용하는 경우 특수 구성 지침을 복수 제공자 SSO에 대한 전자 서명참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 전자 서명을 사용하는 생명과학 고객인 경우 사용자 자체 잠금 방지 비즈니스 규칙을 비활성화합니다.

기존 **SAML 1.1** 통합을 **SAML** 2.0으로 마이그레이션

SAML 1.1 통합에서 SAML 2.0 통합으로 마이그레이션하려면 고객 지원에 문의하십시오.

기존 **SAML 2.0** 통합 업데이트

기존 SAML 2.0 통합을 업데이트합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
SAML 2.0 업데이트 1 플러그인을 요청합니다. *SAML 2.0* 1회 사용자 인증*(SSO)* - 업데이트 *1:* 보안 강화 플러그인을 요청하려면 연락처로 문의하십시오고객 서비스 및 지원. 플러그인은 *SAML2SingleSignon* 설치 종료(로그인 스크립트), *SAML2Logout* 설치 종료(로그아웃 스크립트) 및 *SAML2* 스크립트 포함(스크립트 객체)의 업데이트된 버전을 적용합니다.

기존 설치 종료 스크립트의 사용자 지정을 새 스크립트로 병합합니다. 업데이트는 통합의 원래 설치 종료 스크립트의 비활성 복사본을 저장합니다. 이러한 사본을 사용하여 로그인 및 로그아웃 스크립트에 작성한 사용자 조정을 이러한 설치 종료의 새 버전에 병합할 수 있습니다.

기존 설치의 사용자 지정 병합 스크립트 종료 후 새 스크립트로

원본 설치 종료 스크립트 이름	원래 스크립트 상태	새 설치 종료 스크립트 이름	새 스크립트 상태
SAML2싱글 사인온	비활성	SAML2SingleSignon_update1	활성
SAML2	비활성	SAML2_update1	활성
SAML2로그아웃	비활성	SAML2Logout_update1	활성

다음 경로를 사용하여 SAML 2.0 로그인 및 로그아웃 설치 종료 스크립트로 이동할 수 있습니다.

- **SAML 2** 1회 사용자 인증**(SSO)** > 로그인 스크립트.
- **SAML 2** 1회 사용자 인증**(SSO)** > 로그아웃 스크립트.
- 시스템 정의 > 설치 종료.

다음 경로를 사용하여 SAML 2.0 업데이트 1 스크립트 포함으로 이동할 수 있습니다.

- **SAML 2** 1회 사용자 인증**(SSO)** > 스크립트 객체.
- 시스템 정의 > 스크립트 포함.

업데이트를 테스트합니다.

프로시저

1. *true* 값을 사용하여 `glide.authenticate.sso.saml2.debug`라는 시스템 속성을 추가합니다.
2. SAML 2.0 로그인을 시도합니다.
3. 시스템 로그를 검토합니다.
   SAML2 유효성 검사 오류는 *SAML2ValidationError* 텍스트로 시작합니다.
4. 일반적인 로그인 오류를 식별하고 수정합니다.
   자세한 내용은 다중 SSO(SAML 2.0) 오류 및 수정 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

업데이트 후 샘플 **SAML 2** 응답

다음 섹션에서는 IdP가 SAML 응답에서 제공해야 하는 새로운 필수 요소 및 속성을 설명합니다.

발급자 요소가 포함된 샘플 **SAML 2** 응답

다음 SAML 2 응답은 *Issuer* 요소를 사용합니다.

```
<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>
```

SubjectConfirmation 및 **SubjectConfirmationData** 요소가 포함된 샘플 **SAML 2** 응답

다음 SAML 2 응답은 *NotOnOrAfter* 및 *Recipient* 속성과 함께 *SubjectConfirmation* 및 *SubjectConfirmationData* 요소를 사용합니다.

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><
saml:SubjectConfirmationData
 InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
     NotOnOrAfter="2012-01-30T20:17:10Z"
 Recipient="https://
demoi2.service-now.com/navpage.do"/></saml:SubjectConfirmation>
```

AudienceRestrictions 및 **Audience** 요소가 포함된 샘플 **SAML 2** 응답

다음 SAML 2 응답은 *NotBefore* 및 *NotOnOrAfter* 특성과 함께 *AudienceRestrictions* 및 *Audience* 요소를 사용합니다.

```
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audi
ence>https://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:C
onditions>
```

SAML 사용자 프로비저닝

사용자가 IdP에 있지만 인스턴스에 없는 경우 SAML 사용자 프로비저닝을 통해 인스턴스의 사용자 [sys_user] 테이블에 사용자를 자동으로 생성할 수 있습니다.

다중 SSO를 사용하는 경우 SAML 2.0 업데이트 1에 대해 SAML 사용자 프로비저닝이 지원됩니다.

SAML 사용자 프로비저닝 작동 방식

SAML 사용자 프로비저닝이 활성화되고 시스템에 인스턴스에 없는 새 사용자가 발견되면 인스턴스는 자동으로 `u_imp_saml_user_<###>`라는 이름의 임시 테이블에 기록을 생성합니다. 여기서 `<###>`는 자동으로 생성된 텍스트 식별자입니다. 시스템은 임포트 테이블과 사용자 테이블 간의 데이터

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관계를 지정하는 변환 맵도 생성합니다. 시스템에서 식별된 각 IdP에는 자체 변환 맵이 있습니다. 변환 맵은 각 IdP에 대해 한 번씩 만들어집니다. 관리자는 필요에 따라 업데이트할 수 있습니다.

사용자가 로그인하면 IdP에 액세스하여 로그인합니다.

- 시스템은 SAML 사용자 프로비저닝을 사용할 수 있는 모든 IdP의 목록을 제공합니다. SAML 사용자 프로비저닝을 사용할 수 있는 IdP가 하나만 있는 경우 해당 IdP가 자동으로 사용됩니다.
- 위 조건 중 어느 것도 true가 아닌 경우 시스템은 자동 리디렉션 IdP를 사용합니다.

SAML 사용자 프로비저닝 관리

먼저 필드 매핑을 설정한 다음 다중 SSO IdP 설정을 통해 사용자 프로비저닝을 사용하도록 설정하여 IdP의 사용자로 사용자 테이블을 업데이트합니다.

시작하기 전에

사용자 테이블의 올바른 필드에 매핑되는 IdP의 필드를 식별하도록 IdP 매핑을 설정합니다.

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > 속성.
2. 이 기능을 활성화하려면 모든 **ID** 제공자로부터 사용자 테이블 (*glide.authenticate.multisso.user.autoprovision*)로 사용자 자동 임포트 활성화를 선택합니다.
3. 저장을 클릭합니다.
4. 다음으로 이동 복수 제공자 **SSO** > **ID** 제공자.
5. 사용할 ID 제공자 기록을 엽니다.
6. 사용자가 아직 없는 경우 사용자 자동 프로비저닝을 선택하여 사용자 테이블에 기록을 생성합니다. 이 릴리스로 업그레이드한 경우 양식을 구성하고 이 필드를 추가해야 합니다.
7. 각 로그인 시 사용자 기록 업데이트를 선택하여 사용자가 IdP에 로그인하고 IdP의 정보가 사용자 테이블의 정보로 만료될 때 사용자 기록을 업데이트할 수 있도록 합니다. 이 릴리스로 업그레이드한 경우 양식을 구성하고 이 필드를 추가해야 합니다.
8. 사용자 프로비저닝 변환 맵을 클릭하여 시스템이 자동으로 생성하는 맵을 확인합니다.
9. 필요에 따라 맵을 변경합니다.

결과

알 수 없는 첫 번째 사용자가 로그인을 시도하면 시스템은 metadata.xml 파일에서 임포트 세트 테이블의 필드를 생성합니다.

주: 이 첫 번째 사용자가 로그인할 때까지 IdP 테이블에서 필드를 매핑할 수 없습니다.

SAML 2.0 문제 해결

지원 팀에 문의하기 전에 Hi의 지식베이스에서 사용할 수 있는 문제 해결 솔루션을 시도해 보십시오.

주: 인스턴스는 외부 사이트에서 제공하는 솔루션을 지원하지 않습니다.

지식베이스 문서 KB0540617 "'SAML 오류 매트릭스'''를 참조하십시오.

기타 일반적인 문제

오류 또는 증상	솔루션
오류 메시지: "is not a function."	이 오류는 플러그인이 활성 상태가 아니어서 .jar 파일을

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기타 일반적인 문제

오류 또는 증상	솔루션
이 문제는 다중 노드 환경에서 발생할 수 있습니다. 플러그인이 모든 노드에서 활성화되지 않으면 다음과 같은 오류가 나타납니다. org.mozilla.javascript.EcmaError: *[JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder]* is not a function.	로드하지 않았기 때문에 발생합니다. 따라서 코드가 누락된 것으로 보입니다. 기술 지원에 문의하여 플러그인이 누락된 노드를 다시 시작합니다.
SAML은 CMS 페이지에 액세스하는 사용자를 인증하지 않습니다.	기본적으로 CMS 페이지는 공개되어 있으므로 인증이 필요하지 않습니다. SAML에서 CMS 페이지를 인증하려면 *view_content.do* 공개 페이지를 *active=true* 에서 *active=false*로 변경합니다.
SAML 인증 후에는 사용자를 CMS 페이지로 다시 리디렉션할 수 없습니다.	기본적으로 SSO 통합은 *URI* 라는 URL 매개변수를 사용하여 IdP에서 인증 후 사용자가 전달되는 위치를 제어합니다. SSO는 상대 URL을 무시합니다. 예를 들어, SSO는 사용자를 */ess* 상대 URL로 리디렉션할 수 없습니다. 대신 사용자는 딥 링크 구문을 사용하는 */nav_to.do?uri=/ess*와 같은 URL로 이동해야 합니다. 그러나 이렇게 하면 ESS 포털이 메인 탐색 콘텐츠 IFrame 내에 배치됩니다. 즉, 사이트는 전체 페이지를 차지하지 않고 인스턴스에서 페이지로 로드됩니다. 자세한 내용은 CMS 사이트 및 Single Sign-On을 참조하십시오. *view_content.do*를 *active=false*로 설정하여 CMS 항목 페이지를 비공개로 변경하는 경우 딥 링크 동작에 따라 설치 종료 로그인 스크립트에 대한 사용자 지정이 필요합니다. URL의 *URI* 부분을 찾고 IdP에서 인증한 후 사용자를 리디렉션할 상대 URL 경로가 포함된 릴레이 상태 URL 매개변수를 구성하는 스크립트를 만듭니다.
SAML은 인증 후 사용자를 적절한 페이지로 리디렉션하지 않습니다.	릴레이 상태가 IdP로 전달된 다음 인증 중에 다시 전달되는지 여부를 결정합니다. HTTP 요청 헤더와 POST 정보를 저장할

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기타 일반적인 문제

오류 또는 증상	솔루션
	수 있는 브라우저(예: 내장된 개발자 도구가 있는 Chrome 또는 HTTPfox라는 추가 기능이 있는 Firefox)에서 이 작업을 수행할 수 있습니다. Internet Explorer의 경우 Fiddler와 같은 타사 애플리케이션을 사용합니다. 목표는 요청이 클라이언트(브라우저)에서 인스턴스로, 클라이언트에서 IdP로 전달되는 것을 지켜보는 것입니다.

로그인 활동에 대한 이벤트 큐 모니터링

모든 Single Sign-On 통합은 로그인 활동에 대한 이벤트를 생성합니다.

이러한 이벤트를 사용하여 로그인 실패를 모니터링하고 해결해야 할 보안 문제가 있는지 확인할 수 있습니다.

로그인 실패에 대한 이벤트 큐 모니터링

이벤트 이름	설명	기록	매개변수 **1**	매개변수 **2**
external.authentication.succeeded	외부 인증에 성공했고 사용자가 인스턴스 URL에 액세스했습니다.	세션 ID	성공적으로 로그인한 사용자의 사용자 ID	사용자가 접근한 URL(딥 링크일 수 있음)
external.authentication.failed	1회 사용자 인증(SSO) 요구 사항이 없거나 누락되었습니다.		세션 ID	누락된 인증 요구 사항
external.authentication.failed	사용자가 사용자 `[sys_user]` 테이블에 없습니다.		사용자 ID	"User does not exist" 문자열
external.authentication.failed	사용자가 잠깁니다.		사용자 ID	"User locked out"이라는 문자열입니다.

이벤트 큐 로그인 이벤트

SAML 2.0 통합은 로그인 활동에 대한 이벤트를 생성합니다.

이러한 이벤트를 사용하여 로그인 실패를 모니터링하고 해결해야 할 보안 문제가 있는지 확인할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

로그인 활동 이벤트

이벤트 이름	설명	이벤트와 함께 사용된 ID	이벤트 문자열
saml2.logout.validation.failed	IdP의 로그아웃 응답이 로그아웃 요청에 대한 확인에 실패했습니다. 이 이벤트는 세션 ID(<saml2p:LogoutRequest>> 요소의 ID 특성)에 대해 <inResponseTo 요소의 유효성을 검사합니다. 예를 들어, 발행된 로그아웃 요청에 대한 워크플로우를 참조하십시오.	세션 ID	"SAML2 LogoutResponse 확인에 실패했습니다." 문자열
external.authentication.succeeded	외부 인증에 성공했습니다.		'Authentication Successed' 문자열
external.authentication.succeeded	외부 인증에 성공했고 사용자가 인스턴스 URL에 액세스했습니다.	성공적으로 로그인한 사용자의 세션 ID 및 사용자 ID	사용자가 접근한 URL(딥 링크일 수 있음)
external.authentication.failed	1회 사용자 인증(SSO) 요구 사항이 없거나 누락되었습니다.	세션 ID	누락된 인증 요구 사항
external.authentication.failed	사용자가 사용자 [sys_user] 테이블에 없습니다.	사용자 ID	'User does not exist' 문자열
external.authentication.failed	사용자가 잠깁니다.	사용자 ID	'User locked out' 문자열

OAuth 인바운드 및 아웃바운드 인증

OAuth 기반 인증은 인증 프로토콜을 사용하여 시스템에서 신뢰를 설정하려고 시도하는 클라이언트의 ID를 확인합니다.

OAuth 2.0 - Open Authorization은 웹 애플리케이션, 데스크톱 애플리케이션 및 모바일 장치에 대한 특정 권한 부여 흐름을 제공하면서 클라이언트 개발자의 단순성을 유지하는 업계 표준 권한 부여 프로토콜입니다.

웹 사이트 또는 애플리케이션이 사용자를 대신하여 다른 웹앱에서 호스트하는 리소스에 액세스할 수 있도록 설계된 표준입니다.

리소스 사용자의 자격 증명을 사용하여 보호된 리소스에 액세스하는 대신 클라이언트는 액세스 토큰을 얻습니다. 액세스 토큰은 사용자의 승인을 받아 타사 클라이언트에 발급되며, 클라이언트는 액세스 토큰을 사용하여 보호된 리소스에 액세스합니다.

인바운드

인스턴스에 액세스하려는 외부 클라이언트에 대한 엔드포인트를 생성합니다. 이렇게 하면 OAuth 클라이언트 애플리케이션 레코드가 생성되고 클라이언트가 인스턴스의 제한된 자원에 액세스하는 데 필요한 클라이언트 ID 및 클라이언트 비밀이 생성됩니다. 자세한 내용은 OAuth 인바운드 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

아웃바운드

인스턴스에 대한 액세스 권한을 제공하는 타사 OAuth 제공자를 사용합니다. 다른 OAuth 제공자에 연결할 때 OAuth 프로파일 및 OAuth 범위를 지정합니다. 자세한 내용은 OAuth 아웃바운드 문서를 참조하십시오.

OAuth 2.0

OAuth 2.0을 사용하면 사용자가 각 자원 요청과 함께 로그인 자격 증명을 입력하는 대신 토큰을 얻어 외부 클라이언트를 통해 인스턴스 자원에 액세스할 수 있습니다.

OAuth 통합을 관리하려면 security_admin 역할이 있어야 합니다. 다음 시나리오에 대해 OAuth 2.0을 구성합니다.

- **OAuth** 외부 클라이언트 시나리오 (인바운드): 인스턴스는 타사 클라이언트가 인스턴스에서 데이터를 끌어올 수 있는 엔드포인트를 제공합니다.
- **OAuth** 제공자 시나리오 (아웃바운드): 인스턴스가 외부 공급업체 제공자로부터 데이터를 가져옵니다.

주: 토큰 게시물을 가져오려면 처음으로 사용자 인증을 해야 하며, 토큰이 만료되기 전에 사용자 계정을 사용하여 인증할 필요가 없습니다.

단순 보안과 높은 보안 프레임워크 모두 OAuth 2.0을 지원합니다. 높은 보안을 권장합니다. 높은 보안이 이미 활성화된 버전과 높은 보안을 활성화하는 방법에 대한 자세한 내용은 을 참조하십시오.

OAuth 2.0 구현의 핵심 개념

개념	설명
자원 소유자	보호된 자원에 대한 액세스 권한을 부여할 수 있는 엔터티입니다. 사람인 자원 소유자를 최종 사용자라고 합니다. 자원 소유자는 항상 사용자 계정입니다.
클라이언트	자원 소유자의 권한 부여를 받아 자원 소유자를 대신하여 보호된 자원을 요청하는 애플리케이션입니다.
자원 서버	보호된 자원을 호스팅하는 서버로, 보호된 자원에 대한 요청을 수락하고 응답할 수 있습니다.
권한 부여 서버	자원 소유자를 성공적으로 인증하고 권한 부여를 얻은 후 클라이언트에 액세스 토큰을 발급하는 서버입니다.
인증 요청	클라이언트가 보호된 리소스에 액세스하는 데 필요한 권한입니다. 권한 부여 요청은 항상 리소스 소유자를 대신하여 작동하는 클라이언트의 ID와 요청에 권한을 부여하는 자격 증명을 포함하는 HTTP POST 메시지입니다.
권한 부여	자원에 액세스할 수 있는 자원 소유자의 권한 부여를 나타내는 자격 증명입니다. 권한 부여 권한은 사용자 로그인 자격 증명 또는 새로 고침 토큰입니다.
접근 토큰	클라이언트가 보호된 리소스에 액세스하는 데 사용하는 보안 문자열입니다. 인스턴스는 유효한 권한 부여 권한이 있는 클라이언트에 액세스 토큰을 발급합니다. 각 액세스 토큰에는 특정 범위, 수명 및 기타 속성이 있습니다. 기본적으로 인스턴스는 인스턴스가 OAuth 제공자인 시나리오에서 30분 수명의 액세스 토큰을 발급합니다. 타사 토큰의 경우 30일입니다.
새로 고침 토큰	클라이언트가 추가 사용자 권한 부여 없이 새 액세스 토큰을 얻기 위해 사용하는 자격 증명입니다. 인스턴스는 액세스 토큰을 가질 수 있는 첫 번째 권한이 부여될 때 클라이언트에 새로 고침 토큰을 발행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개념	설명
	기본적으로 인스턴스는 인스턴스가 OAuth 제공자인 시나리오에서 수명이 100일인 새로 고침 토큰을 발급합니다. 제3자 토큰의 경우 365일입니다.
자체 서명된 인증서	Now Platform 자체 서명된 인증서를 지원하지 않습니다. OAuth 클라이언트는 인증서 신뢰 저장소를 활용하지 않거나 자체 서명된 인증서를 통합하는 OAuth 엔드포인트에 대한 연결을 허용하지 않습니다.
사용자 에이전트	클라이언트 애플리케이션(주로 웹 사이트)에 대한 액세스 권한을 위임하는 사용자입니다. 액세스 권한을 통해 클라이언트 애플리케이션 또는 웹 사이트는 사용자에게 액세스 권한이 있는 인스턴스의 데이터에 액세스할 수 있습니다. 이 시나리오에서는 사용자 에이전트가 사용됩니다.

OAuth 권한 유형

권한 부여 유형은 클라이언트가 액세스 토큰을 얻는 방법입니다. 다음과 같은 권한 부여 유형이 지원됩니다.

- 권한 부여 코드: 소비자는 먼저 권한 부여 코드를 받은 다음 이를 사용하여 액세스 토큰을 가져옵니다. OAuth 프로파일을 지정하고 이 권한 부여 유형을 지정할 수 있습니다. 인증 코드를 사용하는 프로세스를 인증 코드 플로우 또는 인증 코드 플로우라고도 합니다.
- 리소스 소유자 암호 자격 증명: 리소스 소비자에게 액세스 토큰을 가져올 수 있는 사용자 자격 증명이 이미 있습니다. 이 프로세스를 암호 플로우라고도 합니다.
- 클라이언트 자격 증명: 자원의 소비자는 애플리케이션 레지스트리에 이미 구성된 클라이언트 ID와 클라이언트 비밀을 사용합니다.

인증 자격 증명 스토리지

OAuth 클라이언트 암호는 KMF로 *password2* 암호화된 유형 필드로 저장됩니다. 수신 엔드포인트 요청을 확인하는 데 사용되는 사용자 암호는 유형 필드(SHA 256)의 *password* 사용자 테이블에 해시 값으로 저장됩니다. 이 암호화에 대한 자세한 내용은 KMF를 사용한 Password2 암호화 섹션을 참조하세요

OAuth 설정

OAuth 설정 및 활성화하고, OAuth 시스템 속성을 사용하도록 설정하고, 외부 클라이언트 애플리케이션이 인스턴스에 액세스할 수 있도록 OAuth 애플리케이션 엔드포인트를 생성하고, OAuth 매개변수를 설정합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. OAuth 플러그인이 활성 상태이고 OAuth 활성화 속성이 true로 설정되어 있는지 확인합니다.
2. 다음 방법 중 하나를 사용하여 OAuth 애플리케이션 레지스트리를 생성합니다.
   - 인스턴스에 액세스하려는 외부 클라이언트에 대한 엔드포인트를 생성합니다. 이렇게 하면 **OAuth** 클라이언트 애플리케이션 레코드가 생성되고 클라이언트가 인스턴스의 제한된 자원에 액세스하는 데 필요한 클라이언트 ID 및 클라이언트 비밀이 생성됩니다.
   - 인스턴스에 대한 액세스 권한을 제공하는 타사 OAuth 제공자를 사용합니다 .

     다른 OAuth 제공자에 연결할 때 OAuth 프로파일을 지정하고 OAuth 범위를 지정하십시오 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. OAuth 토큰을 요청하는 HTTP POST를 만들도록 클라이언트 응용 프로그램을 구성합니다. 또한 애플리케이션은 반환된 액세스 토큰 및 새로 고침 토큰을 사용하기 위해 JSON 응답을 구문 분석할 수 있어야 합니다.

OAuth 활성화

기본적으로 **OAuth 2.0(com.snc.platform.security.oauth)** 플러그인은 새 인스턴스와 업그레이드된 인스턴스에서 활성화되어 있습니다. 플러그인이 인스턴스에서 활성화되어 있지 않은 경우 활성화할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 조건과 검색 창을 사용하여 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.

3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

OAuth 속성 설정

등록된 애플리케이션에 OAuth 2.0 토큰을 생성하려면 인스턴스에 대해 `com.snc.platform.security.oauth.is.active` 속성이 활성 상태여야 합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. OAuth 2.0을 사용하려면 탐색기에 **sys_properties.list** 를 입력하고 새로 만들기를 선택합니다. 다음으로 이동하여 시스템 속성 목록을 열 수도 있습니다. 모두 > 시스템 속성 > 모든 속성 > .
2. 다음 설정으로 양식을 작성합니다.

   - 이름: com.snc.platform.security.oauth.is.active
   - 유형: true | false
   - 값: true

OAuth 암호 매개변수 변경

이 속성을 사용하여 POST 본문 매개변수만 지원되는 모든 권한 유형에 대한 입력으로 허용되도록 합니다.

URI 쿼리 매개 변수를 통해 중요한 정보를 보내면 클라이언트, 서버 또는 요청 사이의 호스트에서 중요한 정보가 노출될 수 있습니다. Madrid 릴리스부터 이 새 속성은 POST 본문 매개변수만 지원되는 모든 권한 유형에 대한 입력으로 허용되도록 합니다. 지원되는 권한 유형은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 인증 코드
- 암호
- 클라이언트 자격 증명
- 새로 고침 토큰

OAuth 암호 매개변수 속성

속성	설명
`glide.oauth.allow.parameters.in.post.body.only`	이 특성은 OAuth 2.0 플러그인의 일부로 zBoots에 대해서만 true로 설정됩니다. 인스턴스에 이 설정이 필요한 경우 속성을 생성하고 true로 설정합니다.

OAuth 인바운드

OAuth 인바운드는 타사 클라이언트가 인스턴스에서 데이터를 끌어올 수 있는 엔드포인트를 제공합니다.

OAuth 통합을 관리하려면 `security_admin` 역할이 있어야 합니다.

인스턴스가 타사 클라이언트가 인스턴스에서 데이터를 끌어올 수 있도록 엔드포인트를 제공하도록 하려는 경우 **OAuth** 외부 클라이언트 시나리오 (인바운드) 통합을 구성할 수 있습니다.

주: 토큰 게시물을 가져오려면 처음으로 사용자 인증을 해야 하며, 토큰이 만료되기 전에 사용자 계정을 사용하여 인증할 필요가 없습니다.

다음 유형의 권한 유형에 따라 OAuth 인바운드 구성을 수행할 수 있습니다.

- 인증 코드 부여 플로우: 사용자가 사용자 이름이나 암호를 입력할 필요 없이 액세스 토큰을 통해 인증을 위해 승인된 URL을 구성할 수 있는 사용자 시작 권한 부여 플로우의 경우. 자세한 내용은 OAuth 인증 코드 부여 플로우 문서를 참조하십시오.
- 암호 부여 플로우: 인증을 위해 사용자 상호 작용이 필요한 사용자 시작 권한 부여 플로우의 경우. 자세한 정보는 암호 부여 흐름 구성을 참조하십시오.

  주: 인증 코드 플로우의 경우 사용자는 로컬 로그인, SSO 또는 MFA를 통한 인증을 완료한 다음 동의를 제공해야 합니다.

- **JWT** 전달자 권한 플로우: 사용자 개입이 필요하지 않은 시스템 대 시스템 통합의 경우. 자세한 내용은 JWT 전달자 권한 부여 플로우 구성을 참조하세요.
- **ID** 토큰 플로우: Okta, Azure와 같은 타사 OIDC 제공자가 발급한 ID 토큰을 사용합니다. 자세한 내용은 인증을 위한 ID 토큰 플로우 를 참조하세요.
- **OAuth** 암시적 권한 부여: 일반적으로 웹 브라우저 또는 모바일 장치인 사용자 에이전트를 통해 클라이언트 애플리케이션에 직접 액세스 토큰을 제공할 수 있도록 합니다. 자세한 내용은 OAuth 암시적 부여 문서를 참조하십시오.
- 클라이언트 자격 증명: 외부 공급업체 OAuth 클라이언트에서 플랫폼으로의 ServiceNow® 인바운드 통합에 OAuth 클라이언트 자격 증명 부여 유형을 사용합니다. 자세한 내용은 클라이언트 자격 증명 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OAuth 범위

REST API에 대한 OAuth 인증 범위 지원의 범위를 지정할 수 있습니다. OAuth 범위는 특정 REST API에 대한 액세스만 제공합니다. 자세한 내용은 REST API 인증 범위 문서를 참조하십시오.

OAuth 인증 코드 부여 플로우

인증 코드 부여 플로우를 사용하면 사용자 이름/암호 자격 증명으로 인증하는 것과는 반대로 사용자가 자원을 신뢰하는 OAuth 서버로 직접 인증하여 자원에 액세스할 수 있습니다.

이 OAuth 인증 코드 플로우를 구현하면 REST를 통해 자원에 액세스할 수 있습니다. 인증 코드 프레임워크는 사용자에게 사용자 이름/암호를 입력하도록 요구하지 않고 사용자가 구성하는 인증된 URL을 통해 액세스 토큰을 가져옵니다. 사용자 이름/암호는 자원에 대한 액세스를 요청하는 클라이언트에 노출되지 않습니다.

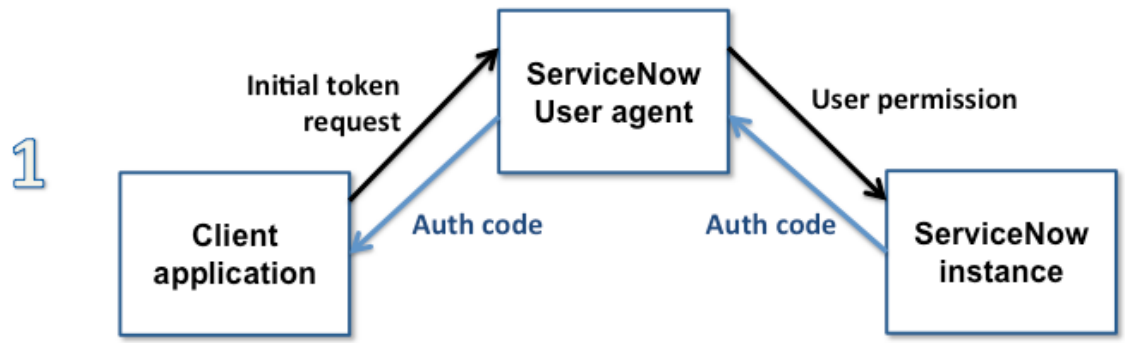
ServiceNow 권한 부여 서버로서의 인스턴스

OAuth 서버는 일반적으로 외부 공급업체 권한 부여 서버입니다. 권한 부여 코드 플로우에 대한 토큰을 발급하는 권한 부여 서버로 인스턴스를 지정할 ServiceNow 수도 있습니다.

제한된 자원을 소유한 사용자는 액세스 권한을 부여해야 합니다. 또한 사용자는 언제든지 발급된 액세스 토큰을 해지하여 액세스를 종료할 수 있습니다.

인증 코드 부여 플로우 프로세스

인증 코드 부여 플로우 프로세스는 다음 세 단계로 구성됩니다.



1단계에서 클라이언트 애플리케이션 또는 웹 사이트는 사용자 에이전트를 통해 인스턴스에 대한 GET 요청 형식으로 REST API 호출을 시작합니다. 일반적으로 REST 호출은 최종 사용자가 클라이언트 애플리케이션 또는 웹 사이트의 단추 또는 링크를 클릭하여 액세스 토큰을 요청할 때 시작됩니다. 또한 클라이언트 애플리케이션에서 최종 사용자는 권한 부여 URL, 토큰 URL, 클라이언트 ID 및 클라이언트 비밀을 지정해야 합니다. 이러한 항목에 대한 설명은 외부 공급업체 OAuth 제공자 사용 주제의 필드 설명을 참조하십시오. 클라이언트가 권한 부여 유형을 요청하는 경우 최종 사용자는 권한 부여 코드를 선택해야 합니다.

클라이언트 애플리케이션에서 인스턴스로의 GET 요청 예시:

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redir
ect_uri={the_redirect_url}&client_id={the_client_identifier}
```

주: **response_type**는 표준 OAuth 코드 부여 플로우를 사용하는 코드여야 합니다.

최종 사용자는 인스턴스의 제한된 자원에 대한 액세스를 수동으로 허용해야 합니다. 구현에서 ServiceNow 최종 사용자는 인스턴스에 로그인해야 합니다. 이 인스턴스는 허용 및 거부 버튼이 있는 UI 페이지를 최종 사용자에게 표시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라이언트 애플리케이션이 실제로 토큰을 요청하는 항목은 권한 부여 엔드포인트라고도 하는 사용자가 만든 OAuth 제공자 애플리케이션 레지스트리 레코드입니다(외부 공급업체 OAuth 제공자 사용 참조). 인증 코드는 권한 부여 엔드포인트에서 클라이언트로 전송됩니다. 클라이언트로 직접 이동하지 않고 인증 끝점 양식에서 지정한 리디렉션 **URL** 로 이동합니다. 이 URL을 콜백 URL이라고도 합니다. 클라이언트 응용 프로그램 또는 웹 사이트에서 이 URL을 가져올 수 있습니다.

인증 코드를 제공하는 인스턴스의 클라이언트 애플리케이션 응답 예시:

```
https/http://{callbackURL}?code={the actual auth code}
```



이제 클라이언트 애플리케이션에 인증 코드가 있으므로 클라이언트는 이 코드를 사용하여 액세스 토큰을 요청합니다. 인증 코드는 사용자가 1단계에서 동의했음을 증명합니다.

클라이언트 애플리케이션에서 인증 코드를 제공하고 접근 토큰을 요청하는 인스턴스로의 ServiceNow POST 요청 예:

```
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}
```

인스턴스의 엔드포인트는 액세스 토큰과 새로 고침 토큰을 반환합니다. 새로 고침 토큰을 사용하여 추가 액세스 토큰을 요청할 수 있습니다.

인스턴스에서 토큰 해지를 포함하여 토큰을 관리할 수 있습니다. OAuth 토큰 관리를 참조하세요.



클라이언트 애플리케이션은 액세스 토큰을 사용하여 REST API에 인증합니다. 클라이언트 애플리케이션을 인증한 후 REST API는 요청된 데이터를 JSON 페이로드로 반환합니다.

인시던트 [incident] 테이블에 대한 데이터의 JSON 페이로드에 대한 GET 요청 예시:

```
https://myinstance.service-now.com/api/now/table/incident?access_token={the_token}
```

주: 시스템은 암시적 허용 코드 흐름이라고도 하는 OAuth 암시적 부여도 지원합니다.

통합 지원

인증 코드 플로우는 인스턴스에서 다음 통합을 지원합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 다중 SSO
- SAML 2.0 업데이트 1
- Multifactor Authentication

모바일 인터페이스도 지원됩니다.

인증 코드 플로우를 사용하여 **OAuth** 엔드포인트에 대한 액세스 권한 부여

인스턴스에서 보호된 자원을 ServiceNow 소유한 최종 사용자는 먼저 자원에 대한 액세스 권한을 부여해야 인스턴스가 액세스 토큰을 제공할 수 있습니다.

시작하기 전에

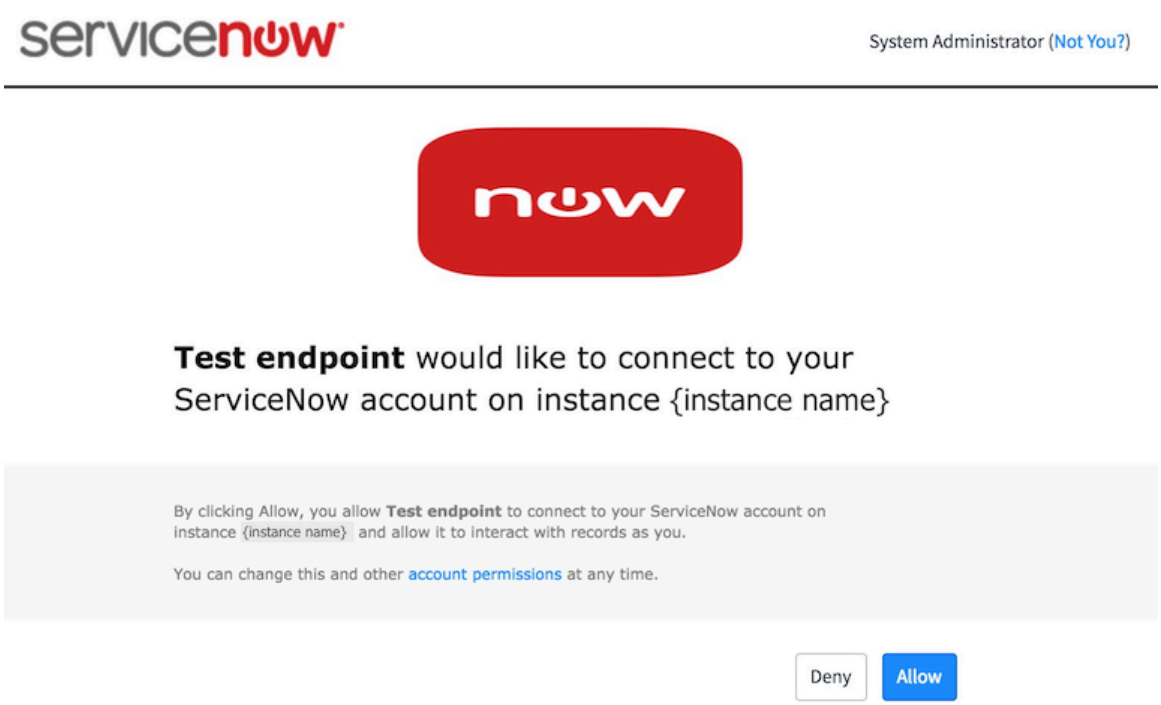
필요한 역할: 없음. 보호된 자원을 보유한 인스턴스에 이미 로그인되어 있어야 합니다. 또는 관리자가 이미 설정한 인증 방법(예: 다단계 인증 또는 SAML)을 사용하여 로그인할 수 있습니다 ServiceNow .

프로시저

1. 인스턴스의 보호된 자원에 대한 액세스를 요청하는 클라이언트 애플리케이션에서 링크 또는 버튼을 클릭합니다.
   그러면 토큰 요청이 시작됩니다. 한 인스턴스에서 다른 인스턴스로 REST 호출을 수행하는 경우 이 링크는 REST 메시지 양식에서 **OAuth** 토큰 가져오기 입니다.
2. 로그인하지 않은 경우 지금 로그인하십시오.
   오른쪽 위 모서리에 지정된 사용자와 같은 사용자가 아닌 경우 본인이 아닙니까? 를 클릭하고 로그인합니다.
3. 계정 권한을 클릭하여 이미 발급한 액세스 토큰 목록을 엽니다.
   이것은 셀프 서비스 > 내 연결됨 앱 토큰 목록입니다.
4. 허용을 클릭하여 액세스를 허용하고 인스턴스가 인증 코드(인증 코드 플로우를 사용하는 경우) 또는 접근 토큰(암시적 권한 부여 유형을 사용하는 경우)을 발급하도록 합니다.

   거부를 클릭하면 인증이 허용되지 않지만 인스턴스에서 로그아웃되지는 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



액세스를 확인하는 메시지가 나타납니다. 인스턴스의 REST 메시지 양식에서 액세스를 요청하는 경우 양식 맨 위에 다음 메시지가 나타납니다. OAuth 새로 고침 토큰을 사용할 수 있으며 {date}에 만료됩니다.

인증 코드 플로우 상태 매개변수 요구 사항

glide.oauth.state.paramater.required 시스템 속성을 사용하면 인증 코드 플로우에 대한 OAuth 요청에 상태 매개변수를 요구할 수 있습니다.

상태 매개변수

필요한 역할: 없음.

Madrid 릴리스부터 시스템 속성은 *glide.oauth.state.parameter.required*OAuth 요청에 대한 상태 매개변수를 추가합니다. zbooted 인스턴스의 경우 속성은 true입니다. 업그레이드된 인스턴스의 경우 속성이 없으므로 상태 매개변수를 사용할 수 없습니다. State 매개변수는 문자열 값이며 특수 문자를 포함해서는 안 됩니다. 상태 매개변수는 비워 두거나 ""일 수 없습니다.

상태 매개변수 확인

클라이언트가 인스턴스에 액세스할 수 있는 엔드포인트를 만듭니다. oauth_auth.do에 대한 인증 코드 플로우를 시작합니다. 예:

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code
```

요청에서 state 매개변수를 지정하지 않으면 오류가 발생하고 인증 코드가 반환되지 않습니다.### ## ##### ####.

요청에 State 매개 변수를 추가합니다.

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code&state=123
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상태 매개변수를 추가하면 로그인 화면으로 리디렉션되고 일반 인증 코드 플로우는 인증 코드를 반환합니다.

주: 응답 URL에는 요청에 전달된 상태 매개변수가 포함되어 있습니다. 이 예에서 추가된 매개변수는 `state=123`입니다.

인증 코드 플로우가 oauth_initiator.do에서 시작되는 경우:

```
http://myinstance.service-now.com/oauth_initiator.do?oauth_requestor_context=sys_rest_message&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fec0d1300964f214a2c2fcf51&response_type=code
```

State 매개 변수는 oauth_auth.do에 의해 리디렉션될 때 자동으로 추가됩니다.

```
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
```

인증 코드 플로우 예시: **ServiceNow** 인증 서버로서의 인스턴스

인스턴스를 인증 서버로 사용하여 인증 코드 플로우를 사용하여 클라이언트에 토큰을 발행할 수 있습니다.

시작하기 전에
필요한 역할: 없음.

이 예에서는 두 개의 인스턴스, 즉 하나는 권한 부여 서버로, 다른 하나는 클라이언트로 사용합니다. 한 인스턴스는 REST 호출을 사용하여 다른 인스턴스에서 토큰을 요청합니다.

두 경우 모두 해야 합니다 OAuth 활성화 .

프로시저

1. 권한 부여 서버 인스턴스(Istanbul 이상 릴리스 실행 중)에서 시스템 **OAuth** > 애플리케이션 레지스트리 을 클릭한 다음 새로 만들기를 클릭합니다.
2. 외부 클라이언트용 **OAuth API** 엔드포인트 작성을 클릭합니다.
3. 설명된 클라이언트가 인스턴스에 액세스할 수 있는 엔드포인트 만들기대로 OAuth 애플리케이션 기록의 양식 필드를 입력합니다.
   이 단계를 완료하면 권한 부여 서버가 설정됩니다. 다음 단계에 따라 클라이언트 서버를 설정합니다.
4. 클라이언트 인스턴스에서 다음으로 이동 시스템 **OAuth** > 애플리케이션 레지스트리 을 클릭한 다음 새로 만들기를 클릭합니다.
5. 외부 공급업체 **OAuth** 공급자에 연결을 클릭합니다.
6. 설명된 대로 OAuth 애플리케이션 기록의 양식 필드를 입력합니다.
   다음 필드 값을 참고하십시오.
   - 이름: OAuth 액세스가 필요한 애플리케이션을 식별하는 고유 이름입니다.
   - 클라이언트 **ID**: 권한 부여 서버에 대해 생성한 애플리케이션 레지스트리 기록의 클라이언트 ID입니다.
   - 클라이언트 비밀: (읽기 전용) 애플리케이션의 자동 생성 고유 ID입니다. 인스턴스는 액세스 토큰을 요청할 때 클라이언트 ID를 사용합니다.
   - 기본 부여 유형: 인증 코드를 선택합니다.
   - 권한 부여 **URL**: 권한 부여 서버인 인스턴스의 URL입니다. URL 끝에 `oauth_auth.do` 를 추가하는 것을 잊지 마십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 로고 **URL**: 애플리케이션 로고로 사용할 이미지가 포함된 URL입니다. 로고는 사용자가 인스턴스의 제한된 자원에 대한 클라이언트 애플리케이션 액세스 권한을 부여해 달라는 요청을 받으면 승인 페이지에 나타납니다.
- 토큰 **URL**: 권한 부여 서버인 인스턴스의 URL입니다. URL 끝에 `oauth_token.do` 를 추가해야 합니다.
- 리디렉션 **URL**: 인스턴스의 URL: 클라이언트 서버 인스턴스입니다. URL 끝에 `oauth_redirect.do` 를 추가해야 합니다.

7. 인증 코드 권한 유형을 사용하여 기록에 대한 프로파일을 생성합니다.
클라이언트 서버가 설정됩니다. 이제 아웃바운드 REST 메시지를 생성하고 OAuth 토큰을 가져올 수 있습니다.

클라이언트가 인스턴스에 액세스할 수 있는 엔드포인트 만들기

외부 클라이언트 애플리케이션이 인스턴스에 액세스할 ServiceNow 수 있도록 OAuth 애플리케이션 엔드포인트를 생성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 **OAuth** > 애플리케이션 레지스트리 을 클릭한 다음 새로 만들기를 클릭합니다.
2. 인터셉터 페이지에서 외부 클라이언트용 **OAuth API** 엔드포인트 작성을 클릭한 후 양식을 채웁니다.

필드	설명
이름	OAuth 액세스가 필요한 애플리케이션을 식별하는 고유 이름입니다.
클라이언트 ID	〔읽기 전용〕 애플리케이션의 자동 생성 고유 ID입니다. 인스턴스는 액세스 토큰을 요청할 때 클라이언트 ID를 사용합니다.
클라이언트 비밀	〔필수〕 인스턴스와 클라이언트 애플리케이션 또는 웹 사이트 둘 다에서 서로에 대한 통신을 승인하는 데 사용하는 공유 비밀 문자열입니다. 인스턴스는 액세스 토큰을 요청할 때 클라이언트 암호를 사용합니다. 인스턴스가 클라이언트 비밀을 자동으로 생성하려면 이 필드를 비워 두십시오. 기존 클라이언트 암호를 표시하려면 잠금 아이콘을 클릭합니다.
리디렉션 URL	권한 부여 서버가 리디렉션하는 콜백 URL입니다. 자원에 대한 액세스를 요청하는 클라이언트의 전체 URL을 `/oauth_redirect.do`에 추가하여 입력합니다. 예: `http://token_consumer:port/oauth_redirect.do`. 가능한 모든 토큰 소비자에 대해 필요한 만큼 URL을 입력합니다. 인스턴스는 수신 요청의 URL을 리디렉션 URL 중 하나와 일치시킵니다. 일치하는 항목이 없으면 인스턴스가 첫 번째 리디렉션 URL을 사용합니다.
로고 URL	애플리케이션 로고로 사용할 이미지가 포함된 URL입니다. 로고는 사용자가 인스턴스의 제한된 자원에 대한 클라이언트 애플리케이션 액세스 권한을 부여해 달라는 요청을 받으면 승인 페이지에 나타납니다.
활성	애플리케이션 레지스트리를 활성화하려면 확인란을 선택합니다.
새로 고침 토큰 수명	새로 고침 토큰이 유효한 시간(초)입니다. 인스턴스는 새로 고침 토큰을 요청할 때 수명 값을 사용합니다. 기본적으로 새로 고침 토큰은 100일(8640000초) 후에 만료됩니다.
토큰 제한 적용	인증 프로파일을 허용하도록 설정된 API에서만 토큰을 사용할 수 있도록 하려면 선택합니다. 접근 권한 부여는 API 접근 정책을 사용하여 설정할 수 있습니다. 자세한 내용은 REST API 액세스 정책 만들기를 참조하세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	기본값: 선택 취소.
모바일 클라이언트	모바일 앱 또는 웹에 대한 엔터티를 나타냅니다. 이 정보는 모바일 또는 웹으로 로그인 정보를 분석하는 데 사용됩니다.
접근 토큰 수명	접근 토큰이 유효한 시간(초)입니다. 인스턴스는 액세스 토큰을 요청할 때 수명 값을 사용합니다. 기본적으로 액세스 토큰은 30분(1,800초) 후에 만료됩니다.
설명	애플리케이션과 연결할 추가 정보입니다.
클라이언트 유형	클라이언트 유형에 따라 클라이언트 유형을 선택합니다. 옵션: ◦ **Iframe** 임베디드 ◦ 사용자형 통합 ◦ 서비스형 통합 자세한 내용은 를 참조하십시오 OAuth 및 SSO 기록에 대한 클라이언트 유형 구성.

3. 제출을 클릭합니다.

결과
시스템이 OAuth 클라이언트 유형의 애플리케이션 레지스트리 [oauth_entity] 테이블에 기록을 생성합니다. 인스턴스가 실제로 토큰과 권한 부여 코드를 발급하면 테이블에 저장됩니다. 자세한 내용은 OAuth 토큰 관리를 참조하세요.

OAuth API 응답 매개변수

OAuth 2.0 API는 다음 매개변수를 name:value 쌍으로 포함하는 JSON 응답을 생성합니다.

접근 토큰 응답 매개변수

응답 매개변수	설명
scope	액세스 토큰으로 부여된 액세스 권한의 양입니다. 범위는 항상 **useraccount**이며, 이는 액세스 토큰이 토큰에 권한을 부여한 사용자 계정과 동일한 권한을 가짐을 의미합니다. 예를 들어 Abel Tuter가 로그인 자격 증명을 제공하여 애플리케이션에 권한을 부여하면 결과 액세스 토큰은 토큰 전달자에게 Abel Tuter와 동일한 액세스 권한을 부여합니다.
token_type	OAuth RFC에 정의된 대로 요청에 의해 발행된 토큰의 유형입니다. 토큰 형식은 항상 전달자이므로 액세스 토큰을 소유한 모든 사용자가 암호화 키를 제공하지 않고도 보호된 리소스에 액세스할 수 있습니다. OAuth 2.0에서 전달자 토큰을 사용하는 방법에 대한 자세한 내용은 RFC6750 참조하십시오.
expires_in	액세스 토큰의 수명(초)입니다.
refresh_token	새로 고침 토큰의 문자열 값입니다.
access_token	액세스 토큰의 문자열 값입니다. 액세스 토큰 만료 시간 내에 수행된 액세스 요청은 항상 현재 액세스 토큰을 반환합니다.
format	〔선택사항〕 응답의 출력 형식입니다. 이 값은 항상 JSON입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: OAuth 공급자가 응답 본문을 "Content-Type" 대신 "content-type"으로 보내는 경우 OAuth HTTP 클라이언트가 응답을 올바르게 구문 분석하지 못할 수 있습니다. 이 문제를 해결하려면 다음 매개변수를 사용하여 시스템 속성을 생성합니다.

필드	값
이름	glide.oauth.inhouse.httpclient.enabled
유형	true | false
값	거짓

시스템 속성 생성에 대한 자세한 내용은 시스템 속성 추가를 참조하십시오.

다음 예제에서는 액세스 토큰 요청에서 반환되는 JSON 문자열을 보여 줍니다. (가독성을 높이기 위해 공백이 추가되었습니다.)

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,
"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k
1K0FMxHW40H8yOO3Hoe",
"access_token":"F0jh9korTyzd9kaZqZ0SzjKZuS3ut0i4P46Lc52m2JYHiLIcqzFAumpyx
shU9mMQ13gJHtxD2fy"}
```

OAuth API 요청 매개변수

액세스 토큰 요청에서 사용하는 OAuth API 요청 매개변수에 대해 알아봅니다.

주: OAuth API의 콘텐츠 유형은 *application/x-www-form-urlencoded*여야 합니다. *application/json*의 콘텐츠 형식으로 인해 지정되지 않은 오류가 발생합니다.

접근 토큰 요청 매개변수

요청 매개변수	설명
grant_type	〔필수〕 액세스 토큰에 대한 요청을 승인하는 자격 증명의 유형입니다. 이 매개변수에는 다음 값 중 하나가 있어야 합니다. • **password**: 액세스 토큰 요청을 승인하기 위한 사용자 자격 증명 집합입니다. 사용자 이름 및 암호 매개변수에 사용자 자격 증명을 지정합니다. • **refresh_token**: 기존 새로 고침 토큰이 액세스 토큰 요청에 권한을 부여합니다. refresh_token 매개변수에서 새로 고침 토큰을 지정합니다.
client_id	〔필수〕 액세스 토큰을 요청하는 클라이언트 애플리케이션의 고유 ID가 자동 생성됩니다.
client_secret	〔필수〕 인스턴스와 OAuth 애플리케이션이 서로에 대한 통신을 승인하는 데 사용하는 공유 비밀 문자열입니다.
username	액세스 토큰 요청을 승인하는 사용자 계정 이름입니다. 이 매개변수는 암호**grant_type** 있는 액세스 토큰 요청에 필요합니다.
암호	액세스 토큰 요청을 승인하는 사용자 계정의 암호입니다. 이 매개변수는 암호**grant_type** 있는 액세스 토큰 요청에 필요합니다.
refresh_token	액세스 토큰 요청을 승인하는 기존 새로 고침 토큰입니다. 이 매개변수는 **grant_type refresh_token**인 액세스 토큰 요청에 필요합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 자격 증명을 사용한 요청

인스턴스는 클라이언트가 처음 인증할 때 또는 새 새로 고침 토큰 생성을 인증할 때 사용자 로그인 자격 증명을 제공할 것을 요구합니다. 이 유형의 요청은 항상 다음 두 개의 토큰을 반환합니다.

- 접근 토큰
- 새로 고침 토큰

인스턴스는 사용자가 활성 상태인지, 현재 잠겨 있지 않은지, 대화형 세션이 있는지 확인합니다. 이러한 조건 중 하나라도 false이면 인스턴스가 액세스 토큰을 생성하지 않습니다. 액세스 토큰의 만료 시간 내에 수행된 액세스 요청은 항상 현재 액세스 토큰을 반환합니다.

주: 이 유형의 권한 부여 권한은 TLS 암호화를 사용하여 전송 중에 사용자 자격 증명을 보호합니다.

다음 예시에서는 사용자 자격 증명 세트를 사용하여 액세스 토큰을 요청하는 방법을 보여줍니다 (가독성을 높이기 위해 공백이 추가됨).

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&username=admin&password=admin"
https://instancename.service-now.com/oauth_token.do
```

새로 고침 토큰을 사용한 요청

인스턴스는 기존 새로 고침 토큰을 사용하여 새 접근 토큰을 만들 수 있습니다. 이 유형의 요청은 액세스 토큰만 반환합니다. 인스턴스는 새 액세스 토큰을 생성하기 전에 새로 고침 토큰이 만료되지 않았음을 확인합니다. 새로 고침 토큰 만료 시간 내에 수행된 액세스 요청은 항상 현재 새로 고침 토큰을 반환합니다. 새로 고침 토큰을 전송하는 것은 일반적으로 사용자 자격 증명을 전송하는 것보다 더 안전합니다. 다음 예제에서는 기존 새로 고침 토큰을 사용하여 액세스 토큰을 요청하는 방법을 보여줍니다(가독성을 높이기 위해 공백이 추가됨).

```
$ curl
 -d"grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K
0FMxHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

외부 클라이언트용 **OAuth JWT API** 엔드포인트 생성(컴퓨터 대 컴퓨터 통합)

OAuth JWT 전달자 토큰을 사용하면 최종 사용자가 수동으로 로그인하거나 암호를 공유하지 않고도 클라이언트 웹 애플리케이션이 인바운드 JWT 권한 유형을 사용하여 인스턴스로 원활하게 인증할 수 있습니다.

시작하기 전에

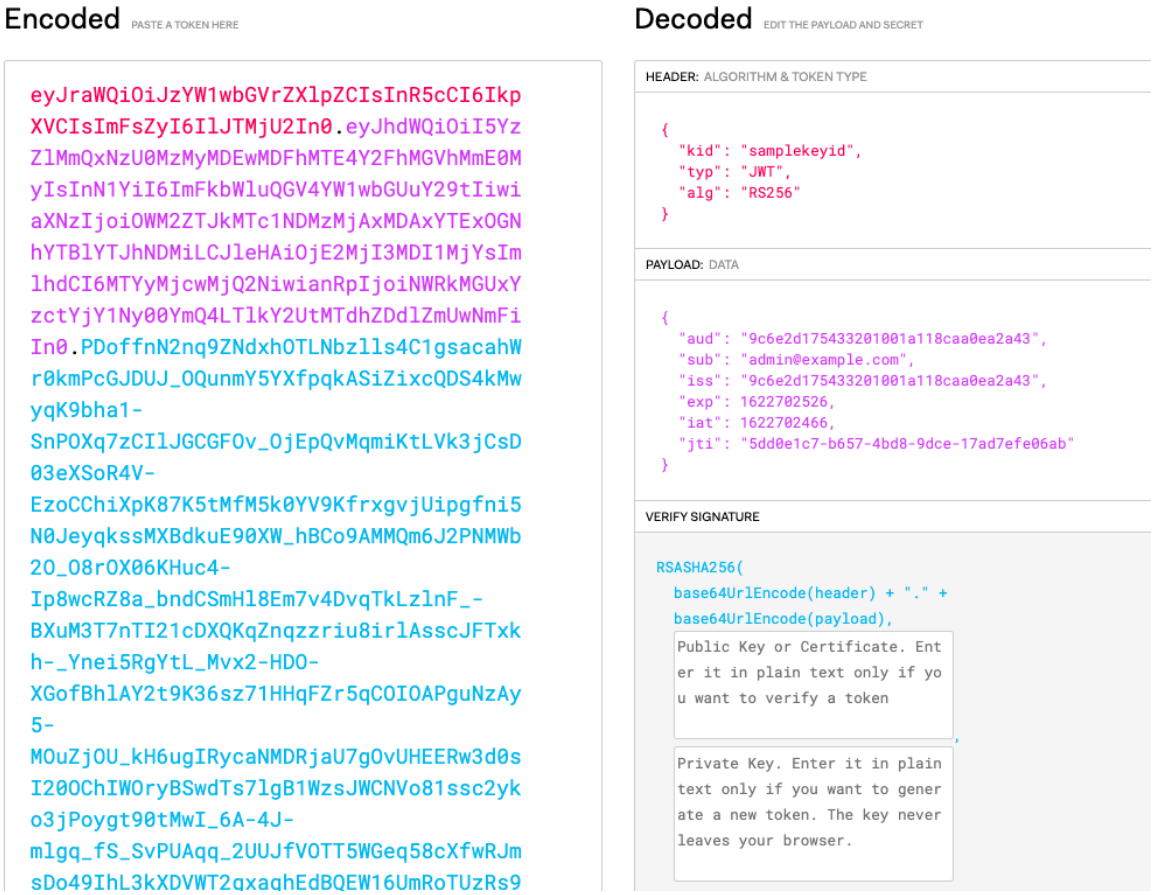
클라이언트 측에서 다음 클레임을 사용하여 JWT(JSON Web Token)를 생성합니다.

- `aud`: 클라이언트 ID의 값과 일치해야 합니다.
- `sub`: 토큰을 연결하려는 사용자의 메일과 같은 사용자 식별자여야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- `iss`: 클라이언트 ID의 값과 일치하는 것이 좋습니다. `aud`와 `iss`가 일치하지 않는 경우 클레임 유효성 검사에 `iss` 값을 추가합니다.
- `exp`: 원하는 만료입니다.

디코딩된 **JSON** 웹 토큰 예제



의 구성 **ServiceNow**

이 태스크 정보

JWT 권한 부여 유형을 사용하면 요청에 암호가 포함되지 않으므로 웹 서비스 간의 보안을 강화할 수 있습니다. 예를 들어, 외부 애플리케이션을 개발하고 토큰을 사용하여 인스턴스에 대한 인바운드 요청을 인증할 수 있습니다 ServiceNow .

필요한 역할: 관리자

JSON 웹 토큰에 대한 자세한 내용은 다음을 참조하십시오 https://jwt.io/ .

프로시저

1. 클라이언트 앱의 공개 키를 **sys_certificate** 테이블에 추가합니다.
2. 수신 JWT를 확인하도록 인스턴스에 구성을 ServiceNow 설정합니다.

   a. 다음으로 이동 시스템 **OAuth** > 애플리케이션 레지스트리.

   b. 외부 클라이언트용 **OAuth JWT API** 엔드포인트 작성을 선택합니다.

   c. 토큰에 대한 정보로 양식을 작성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OAuth JWT 테이블

필드	설명
이름	JWT OAuth 액세스가 필요한 애플리케이션을 식별하는 고유 이름입니다.
클라이언트 ID	애플리케이션의 자동 생성 고유 ID입니다. 시스템은 이 필드의 값을 사용하여 공개 또는 공유 키를 검색하고 JWT를 확인합니다. 이 필드의 값은 JWT의 발급자 및 대상 클레임의 값과 일치해야 합니다.
클라이언트 비밀	인스턴스와 클라이언트 애플리케이션 또는 웹 사이트 둘 다에서 서로에 대한 통신을 승인하는 데 사용하는 공유 비밀 문자열입니다. 인스턴스가 클라이언트 비밀을 자동으로 생성하려면 이 필드를 비워 두십시오. 기존 클라이언트 암호를 표시하려면 잠금 아이콘을 선택합니다. 주: 공용 클라이언트를 선택한 경우 클라이언트 암호를 생략할 수 있습니다.
사용자 필드	시스템이 JWT의 주체 클레임 값을 일치시키기 위해 사용하는 사용자(sys_user) 테이블의 필드입니다. 예를 들어 주체 클레임 값이 user.name@example.com 인 토큰을 추가하는 경우 사용자 필드를이메일로 설정합니다. 이 필드는 이메일 필드에서 user.name@example.com 값을 검색하고 인바운드 요청에서 일치하는 사용자 기록을 사용하도록 시스템에 지시합니다.
JTI 검증 사용	토큰 교환마다 새 토큰을 요구하려면 선택합니다. 기본값: 선택됨.
애플리케이션	읽기 전용 애플리케이션 범위입니다. 이 필드는 자동으로 채워집니다.
다음에서 접근 가능	교차 범위 접근 정책입니다. 자세한 내용은 애플리케이션 액세스 설정을 참조하세요.
접근 토큰 수명	토큰이 유효한 시간입니다. 단위: 초
클럭 오차	JWT에서 `exp` 및 `nbf` 클레임의 유효성을 검사할 때 서버와 클라이언트 클록 간에 허용되는 시간 차이입니다. 단위: 초 기본값: 300
토큰 제한 적용	인증 프로파일을 사용하도록 설정된 API에서만 토큰을 사용할 수 있도록 하려면 선택합니다. 접근 권한 부여는 API 접근 정책을 사용하여 설정할 수 있습니다. 자세한 내용은 REST API 액세스 정책 만들기를 참조하세요. 기본값: 선택 취소.
설명	애플리케이션과 연결할 추가 정보입니다.
공용 클라이언트	JWT 클라이언트가 공용이면 이 필드를 양식에 추가합니다. 이 옵션을 선택하면 클라이언트 암호를 포함할 필요가 없습니다. 기본값: 선택 취소.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
클라이언트 유형	클라이언트 유형에 따라 클라이언트 유형을 선택합니다. 옵션: ▪ **iframe** 임베디드 ▪ 사용자형 통합 ▪ 서비스형 통합 자세한 내용은 를 참조하십시오 OAuth 및 SSO 기록에 대한 클라이언트 유형 구성.

d. 양식을 저장합니다.

e. JWT 검증기 맵 관련 목록에 기록을 추가하여 JWT 서명을 확인합니다.

JWT 검증기 맵 테이블

필드	설명
이름	JWT 매핑 기록의 이름입니다.
아이	JWT의 키 ID입니다.
공유 키	지정된 키 ID의 공유 키입니다.
애플리케이션	읽기 전용 애플리케이션 범위입니다.
시스템 인증서	X.509 인증서(sys_certificate) 테이블의 인증서 기록. 1단계에서 업로드된 인증서입니다.

f. JWT와 연결된 사용자 지정 클레임을 OAuth JWT 클레임 확인 관련 목록에 추가합니다.

다음 필수 클레임에 대한 기록을 추가할 필요가 없습니다.

- ISS는
- aud
- 하위
- 특급

주:

- `aud`와 `iss`가 일치하지 않는 경우 클레임 유효성 검사에 `iss` 값을 추가합니다.
- 인증서의 경우 여러 키와 연결된 여러 검증기 맵을 추가할 수 있습니다.

OAuth JWT 클레임 확인 테이블

필드	설명
내 외부 클라이언트	OAuth JWT 기록으로 자동으로 채워집니다.
클레임 값 유형	클레임 값의 데이터 유형입니다.
클레임 이름	추가할 클레임의 이름입니다.
클레임 값	클레임의 값입니다.
애플리케이션	읽기 전용 애플리케이션 범위입니다.

3. 인스턴스에서 액세스 토큰을 가져오려면 JWT 토큰이 포함된 cURL 요청을 보냅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example

다음은 액세스 토큰을 요청하는 샘플 cURL 명령입니다.

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdW
QiOiI5YzZlMmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4Y
W1wbGUuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJl
eHAiOjE2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny0
0YmQ4LTlkY2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0k
mPcGJDUJ_OQunmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvM
qmiKtLVk3jCsD03eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0Jeyqkss
MXBdkuE90XW_hBCo9AMMQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4D
vqTkLzlnF_-BXuM3T7nTI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-H
DO-XGofBhlAY2t9K36sz71HHqFZr5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7g
OvUHEERw3d0sI20OChIWOryBSwdTs7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-
4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16
UmRoTUzRs9A9sOm18y3skmOVtnEOm-MlJMFQZ754UMzbiH0ZsMmk1ivCGIjex5J0_lDjKEl
WF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqPdS2vzg2m1eKGUwr3m6uNs_HflcDystwVd
MZ7nLlBG4"
https://instancename.service-now.com/oauth_token.do
```

JWT 클라이언트가 Mobile SDK와 같은 공용 클라이언트인 경우 요청에서 client_id 및 client_secret 매개변수를 생략할 수 있습니다. 다음은 client_id 및 client_secret 생략하는 액세스 토큰을 요청하는 샘플 cURL 명령입니다.

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdW
QiOiI5YzZlMmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4Y
W1wbGUuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJl
eHAiOjE2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny0
0YmQ4LTlkY2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0k
mPcGJDUJ_OQunmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvM
qmiKtLVk3jCsD03eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0Jeyqkss
MXBdkuE90XW_hBCo9AMMQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4D
vqTkLzlnF_-BXuM3T7nTI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-H
DO-XGofBhlAY2t9K36sz71HHqFZr5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7g
OvUHEERw3d0sI20OChIWOryBSwdTs7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-
4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16
UmRoTUzRs9A9sOm18y3skmOVtnEOm-MlJMFQZ754UMzbiH0ZsMmk1ivCGIjex5J0_lDjKEl
WF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqPdS2vzg2m1eKGUwr3m6uNs_HflcDystwVd
MZ7nLlBG4"
https://instancename.service-now.com/oauth_token.do
```

인스턴스는 응답에 액세스 토큰을 반환합니다.

```
{
    "access_token":
 "KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaa
FijqQzq2kcABNJxNA",
    "scope": "useraccount",
    "token_type": "Bearer",
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
    "expires_in": 1799
}
```

주: 인바운드 JWT 권한 부여 유형에는 새로 고침 토큰이 포함되지 않습니다.

4. REST API를 호출하여 액세스 토큰을 사용하여 자원에 액세스합니다.

Example

다음은 토큰을 사용하여 인시던트 테이블에 액세스하는 cURL 명령입니다.

```
$ curl -H "Authorization: Bearer
 KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaF
ijqQzq2kcABNJxN"
https://instancename.service-now.com/api/now/v1/table/incident
```

결과
시스템은 REST 호출에서 액세스 토큰을 검색하고 요청된 자원에 대한 액세스를 활성화합니다.

외부 공급업체 토큰을 수락하도록 **OAuth OIDC** 제공자 구성

SSO(Single Sign-On) 옵션(복수 제공자 SSO)을 사용하는 인바운드 API 호출을 사용하여 타사 OIDC 제공자가 생성한 ID 토큰을 수락하도록 OAuth OIDC 제공자를 구성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
는 Now Platform 인바운드 API 호출 외에도 외부 1회 사용자 인증(SSO) 구현을 통해 OIDC를 지원합니다. OIDC 공급자 구성의 예는 Azure AD 설정을 참조하세요. OIDC 공급자 구성의 SSO 관련 예제는 SSO(Single Sign-On)에 대한 OIDC(OpenID Connect) 구성 만들기를 참조하세요.

프로시저

1. 다음으로 이동 모두 > 시스템 **OAuth** > 애플리케이션 레지스트리.
   - 새로 만들기를 선택하고, **ID** 토큰을 확인하도록 **OIDC** 공급자 구성을 선택한 다음, 양식을 작성합니다.
   - OIDC 제공자(ADFS, Auth0, Azure AD, Google, Okta)에 대한 기존 템플릿을 선택한 다음, 양식을 작성합니다.

     주: OAuth 2.0 플러그인으로 데모 데이터를 로드한 후에는 OIDC 제공자 템플릿을 사용할 수 있습니다.

필드	설명
이름	OAuth OIDC 엔터티를 식별하는 고유 이름입니다.
클라이언트 ID	타사 OAuth OIDC 서버에 등록된 애플리케이션의 클라이언트 ID입니다. 이 값은 JWT 토큰의 `aud` 클레임 값과 같아야 합니다.
OAuth API 스크립트	외부 OAuth 제공자에 대한 요청 및 응답을 사용자 지정하는 데 사용할 수 있는 스크립트입니다.
OAuth OIDC 제공자 구성	OIDC 공급자(ADFS, Auth0, Azure AD, Google, Okta)를 사용하여 JWT 토큰의 유효성을 검사할 수 있습니다. OIDC 제공자 구성의 기록을 선택하여 사용자 클레임 및 사용자 필드가 적절하게 설정되었는지 확인합니다. 또한 다음 필드를 채워야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	◦ **JTI** 클레임 검증 사용: 사용 가능한 경우 JWT 토큰 유효성 검증은 ServiceNow 제공자가 보낸 JTI도 유효성 검증합니다. ◦ **OIDC** 메타데이터 **URL**: OIDC 공급자의 잘 알려진 구성에 대한 상세 정보입니다. 주: 유효성 검사를 검사하지 않으면 jti가 JWT 토큰에 있는지 여부에 관계없이 `jti` 의 유효성을 검사할 수 없습니다. 토큰의 클레임 이름은 `jti`여야 합니다.
클럭 오차	제약 조건이 유효한 것으로 간주되는 숫자(초)입니다. 기본값은 300입니다.
토큰 제한 적용	인증 프로파일을 사용하도록 설정된 API에서만 토큰을 사용할 수 있도록 하려면 선택합니다. 접근 권한 부여는 API 접근 정책을 사용하여 설정할 수 있습니다. 자세한 내용은 REST API 액세스 정책 만들기를 참조하세요. 기본값: 선택 취소.
활성	OAuth 애플리케이션을 활성화하려면 확인란을 선택합니다.
클라이언트 유형	클라이언트 유형에 따라 클라이언트 유형을 선택합니다. 옵션: ◦ **Iframe** 임베디드 ◦ 사용자형 통합 ◦ 서비스형 통합 자세한 내용은 를 참조하십시오 OAuth 및 SSO 기록에 대한 클라이언트 유형 구성.

2. 제출을 선택합니다.
   기록은 애플리케이션 레지스트리 [oauth_entity] 테이블에 저장됩니다.
   인스턴스가 토큰 및 인증 코드를 발급하면 외부 **OIDC** 제공자 유형의 애플리케이션 레지스트리 [oauth_entity] 테이블에 기록이 생성됩니다. 자세한 내용은 문서를 참조하십시오.
3. 옵션: OAuth 엔터티 프로파일 기록의 관련 목록으로 이동하여 범위 없이 새 OAuth 제공자에 대해 시스템에서 생성된 기본 프로파일을 확인합니다.
   이름, 권한 부여 유형 및 OAuth 범위를 포함하여 OAuth 제공자 프로파일을 변경하거나 추가할 수 있습니다.
4. 옵션: 이 OAuth 제공자에 대해 사용 가능한 모든 OAuth 범위를 정의하려면 기록 OAuth 엔터티 범위의 관련 목록으로 이동합니다.
   정의된 범위는 프로파일을 만들거나 업데이트할 때 선택할 수 있습니다. 정의된 각 OAuth 범위에는 제공자 스펙에서 가져와야 하는 이름 및 범위(예: 읽기 범위 또는 쓰기 범위)가 포함됩니다. 각 범위는 별도로 정의해야 합니다.
5. 옵션: 자동 사용자 프로비저닝을 활성화하려면 사용자 프로비저닝 기록의 관련 목록으로 이동합니다.

옵션	설명
자동으로 사용자 프로비저닝	사용자에 대해 강제 인증을 활성화하는 옵션입니다.
데이터 소스 프로비저닝	OIDC 토큰을 사용자로 변환하는 데 사용할 데이터 소스입니다 ServiceNow . 조회 목록을 사용하여 사전 정의된 데이터 소스 템플릿을 선택한 다음 기록을 열어 변환된 테이블 매핑을 구성합니다. 변환 매핑을 구성할 때 소스 필드의

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	출처는 이고 대상 필드는 *JWT token*테이블의 출처입니다 *sys_user*.
프로비저닝된 사용자에게 적용되는 사용자 역할	새로 프로비저닝된 ServiceNow 사용자에게 적용되는 사용자 역할입니다.

Example: 다음은 **REST API** 호출을 호출하는 **cURL** 요청의 예입니다
REST API 호출을 호출합니다.

다음 단계를 수행합니다.

- OpenID Connect 제공자에 앱을 등록합니다.
- OAuth OIDC 엔터티를 구성합니다.
- OIDC 제공자를 구성합니다.

OIDC 제공자

OIDC 제공자	OIDC 제공자의 이름입니다.
OIDC 메타데이터 URL	OIDC 메타데이터 URL(잘 알려진 구성 URL)을 지정합니다. 이 정보는 `jwks` 엔드포인트를 통해 토큰의 유효성을 검증하기 위해 공개 키를 가져오는 데 사용됩니다.
사용자 클레임	사용자 테이블에 대해 확인된 클레임입니다.
사용자 필드	사용자 기록을 식별하는 사용자 클레임입니다.
JTI 클레임 검증 사용	이 옵션을 사용하면 ServiceNow JWT 토큰 유효성 검사에서 제공자가 보낸 JTI도 유효성을 검증합니다. 주: 유효성 검사를 검사하지 않으면 jti가 JWT 토큰에 있는지 여부에 관계없이 `jti` 의 유효성을 검사할 수 없습니다. 토큰의 클레임 이름은 `jti`여야 합니다. 이 정보는 재생 공격을 방지하는 데 사용됩니다.

- JWT 토큰을 가져옵니다.
- REST API 호출을 호출합니다.
  - 테이블 API 또는 스크립트 기반 웹 서비스에 액세스하기 위한 인증 헤더의 ID 토큰입니다.

```
curl -X GET --header "Accept:application/json"
 https://<instance_name>.service-now.com/api/now/table/incident/897b04
f2dbd4a300a135364e9d961952 -k
--header "Authorization: Bearer
 eyJraWQiOiJjNTZtZTlXU0xPVnY3UFMwcTg4Qzl1b0lzNjFQYTdmUG4yZFVFOW9RNUg4I
iwiYWxnIjoiUlMyNTYifQ.eyJzdWIiOiIwMHVnZDg1OD
VkczI1WXpUSjBoNyIsIm5hbWUiOiJpbXJhbiBhbGkiLCJsb2NhbGUiOiJlbi1VUyIsImVt
YWlsIjoiaW1yb241NDNAZ21haWwuY29tIiwidmVyIjoxLCJpc3MiOiJodHRwczovL2Rldi
05MzQ
xMjEub2t0YXByZXZpZXcuY29tIiwiYXVkIjoiMG9hZ2Q4bzk3a2lCT3dwd0IwaDciLCJpY
XQiOjE1Mzc5MzMzMjYsImV4cCI6MTUzNzkzNjkyNiwianRpIjoiSUQueThVdXpWNUg2bm1
6SzRs
```

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
OTI1RFVrQnJoR1o1MmJzVVpGVHRVTEphQjg3ayIsImFtciI6WyJwd2QiXSwiaWRwIjoiMD
BvZ2Q4NTgycEFqZDZTemcwaDciLCJub25jZSI6InNub3ciLCJwcmVmZXJyZWRfdXNlcm5h
bWUiO
iJpbXJvbjU0M0BnbWFpbC5jb20iLCJnaXZlbl9uYW1lIjoiaW1yYW4iLCJmYW1pbHlfbmF
tZSI6ImFsaSIsInpvbmVpbmZvIjoiQW1lcmljYS9Mb3NfQW5nZWxlcyIsInVwZGF0ZWRfY
XQiOj
E1Mzc5MzAxOTcsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJhdXRoX3RpbWUiOjE1Mzc5Mjk2
NjF9.OG87SYxWFgHGlhBYby2H79diRm9rlYZTeEkIINRUatwg-p4739htB8xEY-5_t6yU_
6k5w1
0pdgtt5M5QFZRPXVbQZNoGtY-Bxn0BjaimcFgoWfhY_0ldnGTkzN2RYyIHvrf9-yhxg347
zvczmLrgMMa_VwG4rxrtE6rUXaIpIeIK5b-Deq8ADz8UTUTKpF_5RWk4X-oh5xK6BLniFH
k4ShO
Zq2v_mjproXwKk5euJKrVrar2lQ4adZCOSTRuTf3ThMO5WDh0sel-82LngXtLzRJJ51Iqx
AsXns0kJHLLqLtH1hXNRKfwT1ScQoE_OfWm4t0KryI2j4wSMEanFtLXIw"
```

◦ 사용자가 인증되면 유효한 애플리케이션/json 응답이 반환됩니다. 그렇지 않으면 인증되지 않은 사용자 오류 메시지가 반환됩니다.

```
User Not Authenticated
{"error":{"message":"User Not Authenticated","detail":"Required to
 provide Auth information"},"status":"failure"}
```

OAuth 및 SSO 기록에 대한 클라이언트 유형 구성

OAuth 및 SSO 기록 관련 구성에 대한 클라이언트 유형 필드를 구성합니다.

웹 UI(대화형 로그인), Iframe 내장, 포함 또는 통합과 같은 다양한 로그인 유형에 대한 세션을 설정할 때 다양한 로그인에 사용되는 ODC(OAuth 엔터티), SAML 및 다이제스트 레코드에 대한 클라이언트 유형을 구성할 수 있습니다.

클라이언트 유형 선택 항목은 다음과 같습니다.

- **Iframe Embedded**: 외부 공급업체 웹 사이트의 Iframe에 상주하는 대화형 ServiceNow 인스턴스에 사용할 수 있습니다. 예를 들어 중요한 테이블(sys_user 테이블 - 사용자의 전화 번호)이 있는 경우 관리자는 사용자가 외부 공급업체의 Iframe Embedded 세션에서 데이터(테이블 정보)에 액세스하지 못하도록 sec 속성(Iframe Embedded)을 false로 설정하여 ACL을 구성할 수 있습니다.
- 사용자로 통합: Slack, Teams 등과 같은 데스크톱 앱에 설치된 가상 에이전트 채팅 봇에 사용할 수 있습니다.
- 서비스형 통합: 기계 간 통합(서비스 간 통신)에 사용할 수 있습니다.

주:

- OIDC(OAuth 엔터티)의 경우: 모든 선택 항목을 사용할 수 있습니다.
- SAML 및 다이제스트의 경우: Iframe만 임베디드되었습니다. 양식을 편집하고 클라이언트 유형 필드를 기록에 추가한 후 **Iframe** 내장 클라이언트 유형을 선택해야 합니다.
- 선택한 클라이언트 유형이 없음이면 세션 분류가 없습니다.

OIDC(OAuth 엔터티), SAML 및 다이제스트에 대해 생성된 모든 기록에는 클라이언트 유형 필드를 사용하는 것이 좋습니다. 이렇게 하면 구성은 동일하지만 클라이언트 유형과 구별되는 각 로그인 방법을 보다 효과적으로 제어할 수 있습니다.

필드를 구성한 후 사용자가 해당 구성(OAuth 또는 SSO)에서 로그인할 때마다 인증이 성공하면 구성된 클라이언트 유형에 따라 세션이 고려되고 그에 따라 세션 시간 제한이 활용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

현재 세션의 경우 해당 보안 속성이 포함되거나 사용자가 선택한 클라이언트 유형 내에서 테이블 특정 정보에 액세스하지 못하도록 활용할 수 있습니다. 자세한 내용은 OOB(바로 사용 가능) 보안 속성 문서를 참조하십시오.

클라이언트 유형에 대한 세션 시간 제한

다음은 다양한 클라이언트 유형에 대한 세션 시간 제한과 관련된 시스템 속성입니다.

- `glide.session_timeout.iframe_embedded`
- `glide.session_timeout.integration_as_a_user`
- `glide.session_timeout.integration_as_a_service`

OAuth 암시적 부여

ServiceNow 인스턴스는 액세스 토큰의 암시적 부여를 지원합니다.

내재적 권한 부여 유형(라고도 함 *implicit grant code flow*)을 사용하면 일반적으로 웹 브라우저 또는 모바일 장치인 사용자 에이전트를 통해 클라이언트 애플리케이션에 직접 액세스 토큰을 제공할 수 있습니다. 새로 고침 토큰은 부여되지 않습니다. 최종 사용자는 표준과 마찬가지로 인스턴스에서 보호된 리소스에 대한 액세스 권한을 계속 부여해야 합니다.

OAuth 암시적 승인 플로우 프로세스

표준 인증 코드 플로우 프로세스와 마찬가지로 클라이언트 애플리케이션이 인스턴스에서 제한된 자원을 사용하도록 요청하고 최종 사용자가 이를 승인합니다. 요청은 인스턴스로 전송되는 URL 형식입니다. URL에는 다음 매개변수가 포함되어야 합니다.

- `client_id=<### ##### ID>###`. 이는 클라이언트 애플리케이션이 액세스하려는 보호된 자원을 식별하기 위한 필수 사항입니다.
- `response_type=##`입니다. 이는 액세스 토큰을 직접 요청하기 위한 필수 사항입니다(인증 코드를 요청하는 것과는 반대). 값은 암시적 부여에 대한 `##` 이어야 합니다. 표준 인증 코드 플로우 예시에서 응답 유형은 `code`입니다.
- `redirect_uri=<a URL>`: 토큰이 전송되는 위치입니다.

권한 부여 서버는 권한 부여 코드가 아닌 액세스 토큰을 사용자 에이전트를 통해 클라이언트 애플리케이션으로 보냅니다.

다음은 인시던트 [incident] 테이블에 대한 데이터의 JSON 페이로드를 수신하기 위한 GET 요청의 예입니다.

```
https://myinstance.servicenow.com/oauth_auth.do?response_type=token&redir
ect_uri={the_redirect_url}&client_id={the_client_identifier}
```

사용자가 액세스 권한을 부여하면 토큰이 리디렉션(콜백) URL에 포함됩니다.

```
https/http://{callbackURL}?access_token={the_token}
```

OAuth 토큰 관리

OAuth 토큰을 열어 제한된 자원에 대한 액세스를 제공합니다.

시작하기 전에
필요한 역할: 모든 사용자 또는 관리자

이 태스크 정보
인스턴스 및 외부 공급업체 OAuth 제공자가 발급한 OAuth 토큰oauth_credential 테이블에 저장됩니다.

이 테이블의 중요한 열 중 일부는 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 토큰: 인스턴스에서 발급한 ServiceNow 토큰의 값입니다.
- 유형: 토큰이 접근 토큰인지 새로 고침 토큰인지를 결정합니다.
- 만료: 접근 또는 새로 고침 토큰이 만료되는 데이터/시간입니다.
- 받은 토큰: 외부 공급업체 OAuth 제공자가 발행한 토큰의 값입니다. 이 값은 암호화된 형식입니다.

토큰 만료 및 유효 기간은 다음과 같습니다.

- 접근 토큰: 인스턴스가 OAuth 제공자인 시나리오에서 기본적으로 인스턴스는 수명이 30분인 접근 토큰을 발급합니다.
- 새로 고침 토큰: 인스턴스가 OAuth 제공자인 시나리오에서 기본적으로 인스턴스는 수명이 100일인 새로 고침 토큰을 발급합니다.

프로시저

1. 다음 메뉴 옵션 중 하나로 이동합니다.
   - 셀프 서비스 > 내 연결 앱 인스턴스의 자원에 대한 액세스 권한을 부여했을 때 인스턴스가 생성한 토큰을 보려면 다음을 수행합니다.
   - 시스템 **OAuth** > 토큰 관리 모든 토큰을 볼 수 있습니다. 관리자만 이 모듈에 액세스할 수 있습니다.
2. 이름을 클릭하여 토큰을 엽니다.
3. 제한된 자원에 대한 접근을 차단하려면 접근 취소 를 클릭하십시오.

   액세스가 허용되는 범위와 만료 날짜를 포함하여 토큰에 대한 다른 정보도 볼 수 있습니다.

   일정 페이지(`sys.trigger.list`)에서 만료된 **OAuth** 자격 증명 기록 정리를 선택하고 다음을 구성할 수 있습니다.

   - **com.snc.platform.security.oauth.is.active**: 기본적으로 값은 true로 설정됩니다.
   - **com.snc.platform.security.oauth.hours.expired.credential.is.kept**: 요구 사항에 따라 값을 설정하여 시스템에서 만료된 `OAuth` 자격 증명을 유지할 시간을 결정합니다.
   - **com.snc.platform.security.oauth.day.old.credential.is.kept**: 요구 사항에 따라 값을 설정하여 만료된 `OAuth` 자격 증명을 시스템에 보관할 일 수를 결정합니다.

OAuth 토큰 해지

보안상의 이유로 OAuth 액세스 또는 새로 고침 토큰을 취소할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
토큰 해지 상황은 인스턴스가 OAuth 자원 서버 역할을 하는 상황과 관련이 있습니다. URL 또는 를 통해 토큰을 해지할 수 있습니다.

프로시저

`oauth_revoke_token.do`를 사용하여 인스턴스에 액세스하고 접근 또는 새로 고침 토큰을 추가합니다.

예: 대괄호 `[ ]`가 없는 `https://[Your_ServiceNow_Instance]:[port]/oauth_revoke_token.do?token=[access or refresh token]`

결과
이 엔드포인트 액세스에는 인증이 필요하지 않습니다. 이 요청의 토큰은 만료된 것으로 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라이언트 자격 증명

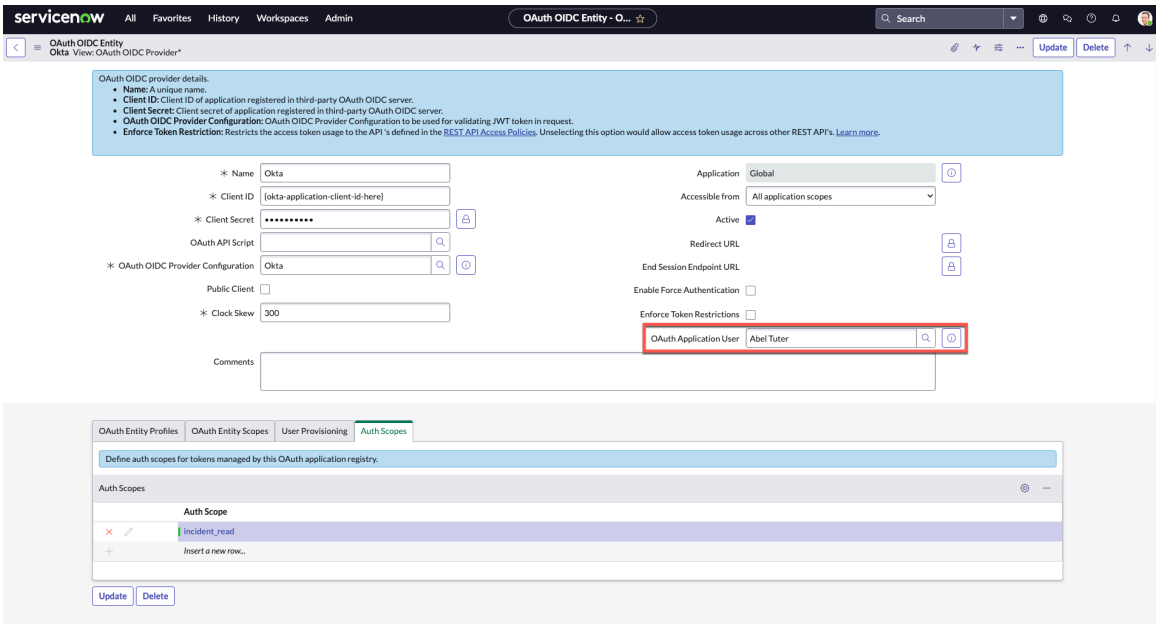
외부 공급업체 OAuth 클라이언트에서 플랫폼으로의 ServiceNow® 인바운드 통합에 OAuth 클라이언트 자격 증명 부여 유형을 사용합니다.

관리자는 CC(클라이언트 자격 증명) 부여 유형을 사용하여 외부 공급업체 OAuth 클라이언트에서 플랫폼으로 통합을 활성화할 수 있습니다 ServiceNow .

인바운드 클라이언트 자격 증명 부여 유형은 시스템 속성을 통해 제어할 수 있는 기능입니다. 기본적으로 시스템 속성은 false입니다.

클라이언트 자격 증명 부여 유형을 사용하려면 다음 단계를 수행해야 합니다.

- `glide.oauth.inbound.client.credential.grant_type.enabled` 시스템 속성을 생성합니다.
- **OAuth** 엔터티 양식에 **OAuth** 애플리케이션 사용자 필드를 추가합니다.



클라이언트 자격 증명 시스템 속성 생성

OAuth 인바운드 통합에 클라이언트 자격 증명 부여 유형을 사용하려면 `glide.oauth.inbound.client.credential.grant_type.enabled` 시스템 속성을 생성합니다.

시작하기 전에

필요한 역할: 관리자

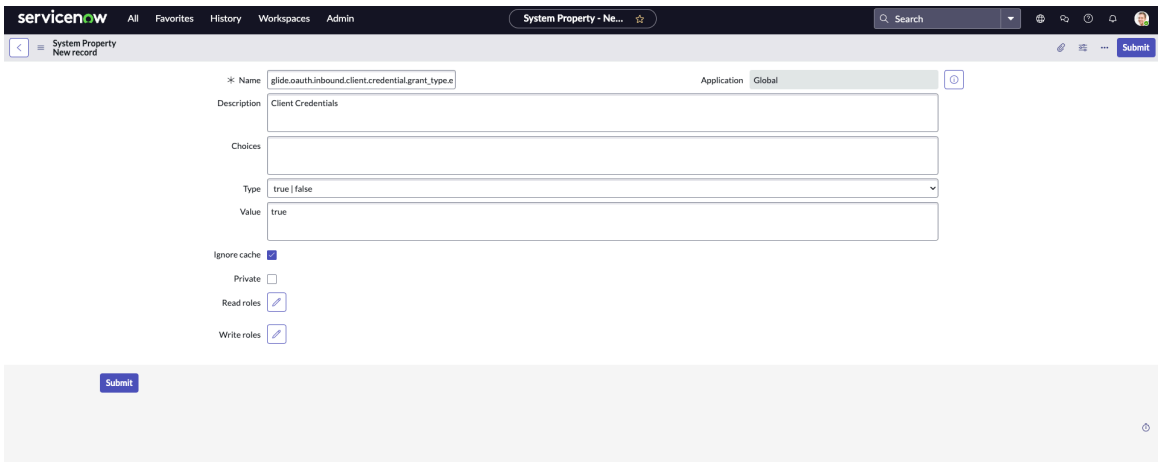
필요한 플러그인: OAuth 2.0.

프로시저

1. 탐색 필터에 `sys_properties.list`를 입력합니다.
   시스템 속성 [sys_properties] 테이블에 전체 속성 목록이 나타납니다.
2. 새로 만들기를 선택합니다.
3. 양식에서 다음 필드를 채웁니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
이름	만들고 있는 속성의 이름입니다. 이 경우 `glide.oauth.inbound.client.credential.grant_type`
설명	속성의 기능을 설명하는 간략한 설명이 포함된 구문을 입력합니다.
유형	목록에서 적절한 데이터 유형을 선택합니다. 이 경우, `true| false`입니다.
값	속성에 원하는 값을 설정합니다. 이 경우, OAuth 인바운드 통합에 클라이언트 자격 증명 부여 유형을 사용하려면 `####` .



주: 선택 사항, 캐시 무시, 비공개, 읽기 역할 및 쓰기 역할과 같은 양식의 다른 필드는 요구 사항에 따라 구성할 수 있습니다.

4. 제출을 선택합니다.

주: 캐시 무시 확인란을 선택하면 매개변수가 변경될 때 시스템에서 서버 캐시를 플러시합니다.

다음으로 OAuth 클라이언트(외부 클라이언트용 OAuth API 엔드포인트)를 생성하고 OAuth 클라이언트 기록에 OAuth 애플리케이션 사용자 필드를 추가해야 합니다.

OAuth 애플리케이션 사용자 추가

OAuth 엔터티 양식에 OAuth 애플리케이션 사용자 필드를 추가하여 OAuth 인바운드 통합에 클라이언트 자격 증명 부여 유형을 사용합니다.

시작하기 전에
필요한 역할: 관리자

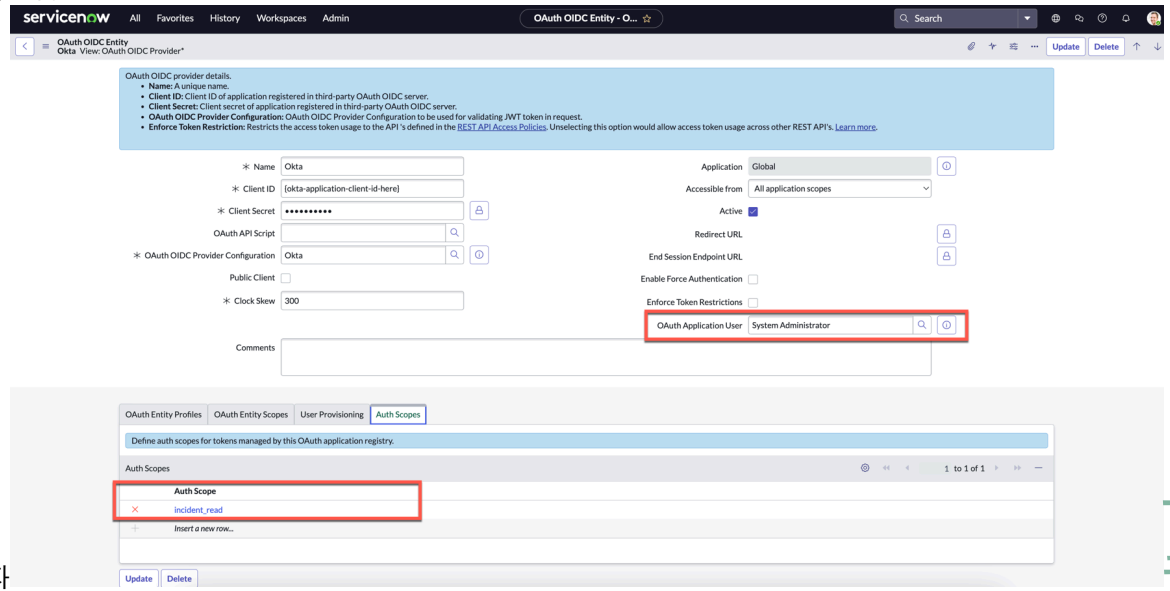
필요한 플러그인: OAuth 2.0.

OAuth 클라이언트를 생성해야 합니다. 자세한 내용은 클라이언트가 인스턴스에 액세스할 수 있는 엔드포인트 만들기 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 생성된 OAuth 클라이언트 레코드를 엽니다.
2. 페이지 헤더에서 추가 옵션 아이콘을 선택합니다.
3. 선택 구성 > 양식 설계.
4. 양식 설계 페이지의 필드 목록에서 **OAuth** 애플리케이션 사용자를 추가합니다.
5. 양식을 저장 또는 업데이트합니다.
6. **OAuth** 애플리케이션 사용자에 대한 사용자를 선택합니다.
   예: 시스템 관리자



> **주:** 클라이언트 자격 증명 부여 유형과 함께 REST API 인증 범위를 사용하여 외부 공급업체 클라이언트에 제공되는 액세스를 제어해야 합니다.

7. 양식을 저장 또는 업데이트합니다.

   부여 유형이클라이언트 자격 증명, 클라이언트 **ID** 및 비밀인 모든 권한 부여 요청은 의 ServiceNow®연결된 OAuth 애플리케이션 사용자에 대해 전달됩니다.

> **주:** OAuth 애플리케이션 사용자가 OAuth 클라이언트 기록에서 선택되지 않았거나 클라이언트 자격 증명 속성이 `false`로 설정된 경우 권한 부여 요청이 전달되지 않습니다.

OAuth 아웃바운드

OAuth 아웃바운드를 사용하면 외부 공급업체 제공자의 데이터를 인스턴스로 끌어올 수 있습니다.

OAuth 통합을 관리하려면 security_admin 역할이 있어야 합니다.

다음 권한 유형에 대해 아웃바운드 OAuth 2.0을 구성할 수 있습니다.

- 외부 공급업체 제공자에 연결: 클라이언트 ID와 비밀을 사용하여 OAuth 제공자에게 보냅니다. 자세한 내용은 외부 공급업체 OAuth 제공자에 연결 문서를 참조하십시오.
- **JWT** 전달자: 권한 부여 서버는 보안 도메인 간에 ID 및 보안 정보를 공유할 수 있도록 JWT 토큰의 유효성을 검증합니다. 자세한 내용은 JWT 전달자 권한 유형으로 OAuth 제공자 설정 문서를 참조하십시오.
- **SAML2** 전달자: SAML2 어설션을 작성한 다음 접근 토큰에 대한 어설션을 제공자와 교환합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 아웃바운드 요청 SuccessFactors 에서 **SAML2** 전달자를 기본 부여 유형으로 사용하는 경우. **SAML2** 전달자를 구성하는 방법에 대한 자세한 내용은 의 v4.x.x 설정 예를 참조하십시오.

- 권한 부여 코드: 액세스 토큰을 얻기 위해 클라이언트에 부여된 코드로, 리소스에 대한 액세스 권한을 얻는 데 사용됩니다. 이 옵션을 선택하는 경우 권한 부여 URL(권한 부여 서버의 URL)이 필요합니다.
- 자원 소유자 암호 자격 증명: 자원에 액세스하려는 사용자의 사용자 이름과 암호입니다.
- 클라이언트 자격 증명: 액세스 토큰을 가져오는 데 사용되는 클라이언트 ID 및 클라이언트 암호입니다. 이 메서드는 새로 고침 토큰을 제공하지 않습니다.
- **MID** 서버: MID 서버는 단일 ServiceNow® 인스턴스와 외부 애플리케이션, 데이터 소스 및 서비스 간의 통신 및 데이터 이동을 용이하게 합니다. MID 서버를 통한 아웃바운드 통합 요청에 OAuth의 인증 코드, 자원 소유자 암호 자격 증명, SAML 전달자 및 JWT 전달자 OAuth 권한 유형을 사용합니다. 개인 인증도 MID 서버를 통해 지원됩니다.

OAuth 제공자 시나리오를 구성할 수 있습니다(아웃바운드): 인스턴스가 외부 공급업체 제공자로부터 데이터를 가져옵니다.

주: 토큰 게시물을 가져오려면 처음으로 사용자 인증을 해야 하며, 토큰이 만료되기 전에 사용자 계정을 사용하여 인증할 필요가 없습니다.

외부 공급업체 **OAuth** 제공자에 연결

클라이언트 ID 및 비밀을 OAuth 제공자에게 보내는 방법을 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 **OAuth** > 애플리케이션 레지스트리 을 클릭한 다음 새로 만들기를 클릭합니다.
2. 인터셉터 페이지에서 외부 공급업체 **OAuth** 제공자에 연결을 클릭한 다음 양식을 작성합니다.

필드	설명
이름	외부 공급업체 OAuth 연결의 고유한 이름입니다.
클라이언트 ID	타사 OAuth 서버에 등록된 애플리케이션의 클라이언트 ID입니다.
클라이언트 비밀	타사 OAuth 서버에 등록된 애플리케이션의 클라이언트 비밀입니다.
OAuth API 스크립트	외부 OAuth 제공자에 대한 요청 및 응답을 사용자 지정하는 데 사용되는 스크립트입니다.
로고 URL	OAuth 애플리케이션 로고 URL입니다.
기본 부여 유형	토큰을 설정하는 데 사용되는 기본 부여 유형입니다. 선택 항목은 다음과 같습니다. ◦ 권한 부여 코드: 액세스 토큰을 얻기 위해 클라이언트에 부여된 코드로, 리소스에 대한 액세스 권한을 얻는 데 사용됩니다. 이 옵션을 선택하는 경우 권한 부여 URL(권한 부여 서버의 URL)이 필요합니다. ◦ 자원 소유자 암호 자격 증명: 자원에 액세스하려는 사용자의 사용자 이름과 암호입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	◦ 클라이언트 자격 증명: 액세스 토큰을 가져오는 데 사용되는 클라이언트 ID 및 클라이언트 암호입니다. 이 메서드는 새로 고침 토큰을 제공하지 않습니다. ◦ **JWT** 전달자: 권한 부여 서버는 보안 도메인 간에 ID 및 보안 정보를 공유할 수 있도록 JWT 토큰의 유효성을 검증합니다. ◦ **SAML2** 전달자: SAML2 어설션을 작성한 다음 접근 토큰에 대한 어설션을 제공자와 교환합니다. 주: 아웃바운드 요청 SuccessFactors 에서 **SAML2** 전달자를 기본 부여 유형으로 사용하는 경우.
새로 고침 토큰 수명	새로 고침 토큰이 유효한 시간(초)입니다. 기본 시간은 8,640,000초입니다.
공용 클라이언트	공용 클라이언트가 권한 부여를 위해 PKCE를 요구할 수 있도록 합니다. 주: PKCE *Default Grant type*가 활성화된 경우 인증 코드만 사용할 수 있습니다.
코드 챌린지 메서드	OAuth PCKE 워크플로에 사용되는 코드 챌린지 메서드입니다. 선택 항목은 다음과 같습니다. ◦ s256 〔기본값〕 ◦ 일반 ◦ 안 함
설명	OAuth 앱에 대한 의견을 추가합니다.
애플리케이션	이 기록이 포함된 애플리케이션 및 범위입니다.
다음에서 접근 가능	모든 애플리케이션 범위 또는 이 범위에서만 이 앱에 액세스할 수 있도록 합니다.
활성	앱을 활성화하려면 확인란을 선택합니다.
인증 URL	OAuth 인증 코드 엔드포인트입니다.
토큰 URL	OAuth 서버 토큰 엔드포인트입니다.
토큰 해지 URL	OAuth 서버 토큰 해지 엔드포인트입니다.
리디렉션 URL	OAuth 콜백 엔드포인트입니다. 비어 있으면 인스턴스가 항목을 자동으로 생성합니다.
상호 인증 사용	토큰 요청 및 해지에 상호 인증을 사용하려면 확인란을 선택합니다. 이 기능을 사용하려면 상호 인증 프로파일을 지정해야 합니다.
자격 증명 보내기	OAuth 클라이언트는 요청에 클라이언트 자격 증명을 채웁니다. ◦ 요청 본문 내(URL 인코딩 형식) ◦ 기본 권한 부여 헤더 ◦ 개인 키 JWT로
클라이언트 유형	클라이언트 유형에 따라 클라이언트 유형을 선택합니다. 옵션: ◦ **Iframe** 임베디드 ◦ 사용자형 통합 ◦ 서비스형 통합

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	자세한 내용은 를 참조하십시오 OAuth 및 SSO 기록에 대한 클라이언트 유형 구성.

시스템이 OAuth 제공자 유형의 애플리케이션 레지스트리 [oauth_entity] 테이블에 기록을 생성합니다.

3. 옵션: OAuth 엔터티 프로파일 기록의 관련 목록으로 이동하여 범위 없이 새 OAuth 제공자에 대해 시스템에서 생성된 기본 프로파일을 확인합니다.
이름, 권한 부여 유형 및 OAuth 범위를 포함하여 OAuth 제공자 프로파일을 변경하거나 추가할 수 있습니다.
4. 옵션: 이 OAuth 제공자에 대해 사용 가능한 모든 OAuth 범위를 정의하려면 기록 OAuth 엔터티 범위의 관련 목록으로 이동합니다.
프로파일을 만들거나 업데이트할 때 범위를 선택할 수 있습니다. 각 OAuth 범위에는 읽기 범위 또는 쓰기 범위와 같이 제공자의 사양에서 가져와야 하는 이름과 범위가 포함되어 있습니다. 각 범위는 별도로 정의해야 합니다.

JWT 전달자

JWT(JSON 웹 토큰)를 사용하면 사용자 개입 없이 외부 API 공급자와 서버 간 API 상호작용 ServiceNow 을 구성할 수 있습니다.

JWT(JSON Web Token) 전달자 권한 부여는 액세스 토큰을 발급하기 전에 권한 부여 서버 측의 JWT 부여 핸들러에서 평가하고 유효성을 검사하는 클레임 값이 포함된 JSON 문자열입니다.

JWT 전달자 권한 유형을 사용하여 아웃바운드 REST 메시지에 대해 OAuth 2.0 JWT 전달자 권한 플로우를 구성할 수 있습니다.

JWT 전달자 권한 유형으로 **OAuth** 제공자 설정

JWT(JSON 웹 토큰)를 사용하면 사용자 개입 없이 외부 API 공급자와 서버 간 API 상호작용 ServiceNow 을 구성할 수 있습니다. 이 지원을 통해 JWT를 사용하는 또는 다른 자동화 작업을 통해 통합 허브 다른 제공자와의 API 및 서비스 통합을 구성할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
다음 태스크는 OAuth 2.0 클라이언트 인증 및 권한 부여에 JWT를 사용하도록 설정하는 방법을 ServiceNow 보여줍니다. ServiceNow 는 OAuth 클라이언트이며 Box 또는 Docusign과 같은 OAuth 제공자를 구성할 수 있습니다.

프로시저

1. Java 키 스토어 인증서 업로드
JWT 클라이언트 인증을 사용하도록 설정하는 데 사용할 JKS 인증서를 인스턴스에 연결합니다.
2. JWT 서명 키 구성
JKS(Java KeyStore) 인증서에 할당할 JWT 서명 키를 생성합니다.
3. JWT 서명 키를 사용하여 JWT 제공자 작성
인스턴스에 JWT 제공자 ServiceNow 를 추가합니다.
4. 외부 공급업체 OAuth 제공자에 연결
애플리케이션 레지스트리에서 JWT 전달자를 기본 부여 유형으로 사용하여 타사 OAuth 제공자를 ServiceNow 생성합니다.
5. OAuth 프로파일 지정
OAuth 제공자의 OAuth 엔터티 프로파일을 열고 JWT 제공자를 할당합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Java 키 스토어 인증서 업로드

Java KeyStore(JKS) 인증서를 인스턴스에 첨부하여 JWT 클라이언트 인증을 활성화하는 데 사용할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **x509** 인증서.
2. 필요에 따라 양식을 작성합니다.

옵션	설명
이름	인증서의 고유 이름입니다.
만료 시 알림	인증서가 만료될 때 알림을 보낼 대상을 지정합니다.
만료되기 전 경고	인증서가 만료되기 전에 인증서 관리자에게 이메일 알림을 보냅니다.
활성	인증서를 토큰 요청에 사용할 수 있도록 합니다.
유형	업로드하려는 인증서의 유형입니다.
며칠 후 만료	인증서가 만료될 때까지의 일 수입니다.
키 스토어 암호	인증서와 연결된 암호입니다.
간단한 설명	

3. 제출을 클릭합니다.

JWT 서명 키 구성

Java KeyStore(JKS) 인증서에 할당할 JSON 웹 토큰(JWT) 서명 키를 생성합니다.

시작하기 전에
필요한 역할: 관리자

주: **X.509** 인증서 **SHA-1** 지문 **int(x5t)**를 JWT 키의 일부로 헤더에 추가하려면 양식을 구성하고 **X.509** 인증서 **SHA-1** 지문 **int(x5t)** 필드를 추가해야 합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 **OAuth** > **JWT** 키.
2. 필요에 따라 양식을 작성합니다.

옵션	설명
이름	JWT 키 서명 구성의 고유한 이름입니다.
서명 키 스토어	JWT에 서명할 때 지정된 키 저장소입니다.
키 ID	키 ID(kid)는 토큰에 서명하는 데 여러 키를 사용할 때 사용되는 키를 식별하는 데 도움이 됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
	주: 이 필드를 구성하면 키 ID 클레임이 JWT에 포함됩니다. 이 필드를 구성하지 않으면 JWT에 키 ID 클레임이 없습니다.
서명 알고리즘	JWT 키로 서명하는 데 사용할 알고리즘입니다. RSA 256은 사용할 수 있는 유일한 알고리즘입니다.
서명 키 암호	서명 키와 연결된 암호입니다.
활성	JWT 키 별명이 JWT 제공자로부터 능동적으로 참조되도록 지정하십시오.

3. 제출을 클릭합니다.

JWT 서명 키를 사용하여 JWT 제공자 작성

인스턴스에 JSON 웹 토큰(JWT) 제공자를 추가합니다 ServiceNow .

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 **OAuth** > **JWT** 제공자.
2. 양식을 작성하고 제출을 클릭합니다.

옵션	설명
이름	JWT 제공자 구성의 고유한 이름입니다.
만료 간격(초)	JWT 제공자가 작성한 토큰의 수명(초)입니다.
서명 구성	적용할 JWT 서명 키 구성입니다 ServiceNow .

JSON 웹 토큰(JWT) 작성

에서 두 당사자 간의 클레임을 안전하게 나타내기 위한 JWT(JSON Web Token)를 Now Platform생성합니다.

GlideJWT API는 JWT를 생성하는 범위가 지정되고 스크립트 가능한 API입니다. JWT를 생성하기 전에 필요한 세 가지 인수가 있습니다.

- JWT 제공자의 Sys_id
- JSON 직렬화된 헤더
- JSON 직렬화된 페이로드

JWT 제공자를 구성할 때 사용할 수 있는 두 개의 JWT API 스크립트(JWTTokenInternal 및 JWTTokenRestricted)가 있습니다. 관리자는 JWTTokenRestricted 스크립트를 사용하여 JWT를 생성할 수 있는 사용자를 구성할 수 있습니다. JWTTokenInternal 스크립트는 읽기 전용이며 로그인한 사용자만 JWT를 생성할 수 있습니다.

JWT를 생성하려면 다음을 수행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 공유 키(HMAC) 또는 서명 키 스토어(RSA)를 사용하여 JWT 키 생성
- JWT 키를 참조하는 서명 구성과 JWT 제공자를 연결합니다.

API를 사용하여 토큰을 생성할 수 있습니다.

JWT 공급자를 구성할 때 표준 및 사용자 지정 클레임 을 사용할 수 있습니다. generateJWT API 서명의 일부로 동적 헤더 및 페이로드 클레임을 전달할 수 있습니다.

API를 테스트할 샘플 스크립트:

```
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 클라이언트 API

OAuth 클라이언트 API는 OAuth 토큰을 요청하고 취소하는 메서드를 제공합니다.

OAuth 클라이언트는 다음 클래스를 제공합니다.

- GlideOAuthClient : 새로 고침 및 액세스 토큰을 요청하고 취소하는 메서드입니다.
- GlideOAuthClientRequest : 클라이언트 요청을 처리하는 메서드입니다.
- GlideOAuthClientResponse : 클라이언트 응답을 처리하는 메서드입니다.
- GlideOAuthToken : 액세스 토큰 및 액세스 토큰에 대한 정보를 검색하는 메서드입니다.

OAuthUtil 스크립트 포함을 사용자 지정하여 요청 매개변수를 가로채고 외부 OAuth 제공자의 응답을 구문 분석할 수도 있습니다.

범위가 지정된 스크립트에서 OAuth 클래스를 사용하는 경우 `sn_auth` 네임스페이스 식별자를 사용합니다.

기본 프로파일 지원을 위한 OAuth 매개변수

기본 프로파일 기능에는 *`setParameter()`* API와 함께 OAuth 요청자, 요청에 대한 컨텍스트 및 제공자 프로파일을 지정하는 데 사용할 수 있는 매개변수 세트가 필요합니다.

OAuth 제공자 시나리오에서는 기본적으로 사용할 OAuth 프로파일을 OAuth 제공자에 알려주는 세 개의 매개변수를 설정해야 합니다. 이러한 세 개의 매개변수가 설정되면 액세스 토큰이 인스턴스 데이터베이스에 저장됩니다. *`GlideOAuthClientRequest`*와 함께 매개변수를 사용합니다.

기본 프로파일 지원을 위한 **OAuth** 매개변수

매개변수	설명
`oauth_requestor`	객체의 sys_id로, 사용자 기록 또는 이메일 계정일 수 있습니다.
`oauth_requestor_context`	OAuth 요청자에 대한 컨텍스트를 제공하는 설명자입니다. `oauth_requestor` 객체가 저장되는 테이블의 이름을 사용하는 것이 좋습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 프로파일 지원을 위한 **OAuth** 매개변수

매개변수	설명
`oauth_provider_profile`	기본값인 OAuth 프로파일 기록의 sys_id입니다(OAuth 프로파일 지정 참조).

값이 OAuth 프로파일 레코드에 구성되어 있으므로 매개변수를 사용하여 권한 부여 유형 및 범위를 설정할 필요가 없습니다. 매개변수를 사용하지 않는 경우 GlideOAuthClientRequest API 메서드 *`setScope`* 및 *`setGrantType`*을 사용할 수 있습니다. 자세한 내용은 setScope 및 setGrantType 을 참조하십시오.

OAuth 2.0 클라이언트 인증을 위한 개인 키 **JWT** 지원

OAuth 2.0 클라이언트 인증에 대한 JWT 지원을 지원합니다.

개인 키 JWT 클라이언트 인증은 토큰 엔드포인트를 사용할 때 클라이언트가 권한 부여 서버에 인증하는 데 사용할 수 있는 인증 방법입니다.

이 인증 메커니즘에서는 공개 키를 등록하고 해당 키를 사용하여 JWT에 서명한 클라이언트만 인증할 수 있습니다.

JWT는 필수 클레임 값을 포함해야 하며 선택적 클레임 값을 포함할 수 있습니다. `private_key_jwt` 인증을 위해 JWT에 필요한 클레임 값에 대한 자세한 내용은 OpenID Connect 코어 설명서의 클라이언트 인증 섹션을 참조하십시오.

주: 인증 토큰을 client_assertion 매개변수의 값으로 보내야 합니다. **client_assertion_type** 매개변수의 값은 `urn:ietf:params:oauth:client-assertion-type:jwt-bearer`여야 합니다.

JWT 토큰을 사용하는 OAuth 2.0 클라이언트 인증에 필요한 플러그인:

- **OAuth 2.0(com.snc.platform.security.oauth):** 이 플러그인은 새 인스턴스와 업그레이드된 인스턴스에서 활성화됩니다. 플러그인이 인스턴스에서 활성화되어 있지 않은 경우 활성화할 수 있습니다.
- **Integration - Multiple Provider** 1회 사용자 인증**(SSO)** 설치 관리자 **(com.snc.integration.sso.multi.installer):** OIDC 기반 1회 사용자 인증(SSO) 사용 사례에 사용됩니다.

다음을 위해 개인 키 JWT를 사용하는 OAuth 2.0 클라이언트 인증을 사용할 수 있습니다.

- OIDC 기반 1회 사용자 인증(SSO)
- 아웃바운드 OAuth 통합

OIDC 기반 SSO에 대한 개인 키 **JWT** 구성

OIDC 기반 SSO 통합을 위해 개인 키 JWT를 구성합니다.

시작하기 전에
필요한 역할: 관리자

OIDC 기반 SSO에 대한 개인 키 JWT를 선택하기 전에 다음 작업을 수행해야 합니다.

- Java 키 스토어 인증서 업로드: JWT 클라이언트 인증을 활성화하는 데 사용할 JKS 인증서를 인스턴스에 첨부합니다.
- JWT 서명 키 구성: JKS(Java KeyStore) 인증서에 할당할 JWT 서명 키를 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: **X.509** 인증서 **SHA-1** 지문 **int(x5t)**를 JWT 키의 일부로 헤더에 추가하려면 양식을 구성하고 **X.509** 인증서 **SHA-1** 지문 **int(x5t)** 필드를 추가해야 합니다.

- JWT 서명 키를 사용하여 JWT 제공자 작성: 인스턴스에 JWT 제공자 ServiceNow 를 추가합니다.

OIDC 기반 ID 제공자에 대한 JWT 키를 포함하려면 다음을 수행해야 합니다.

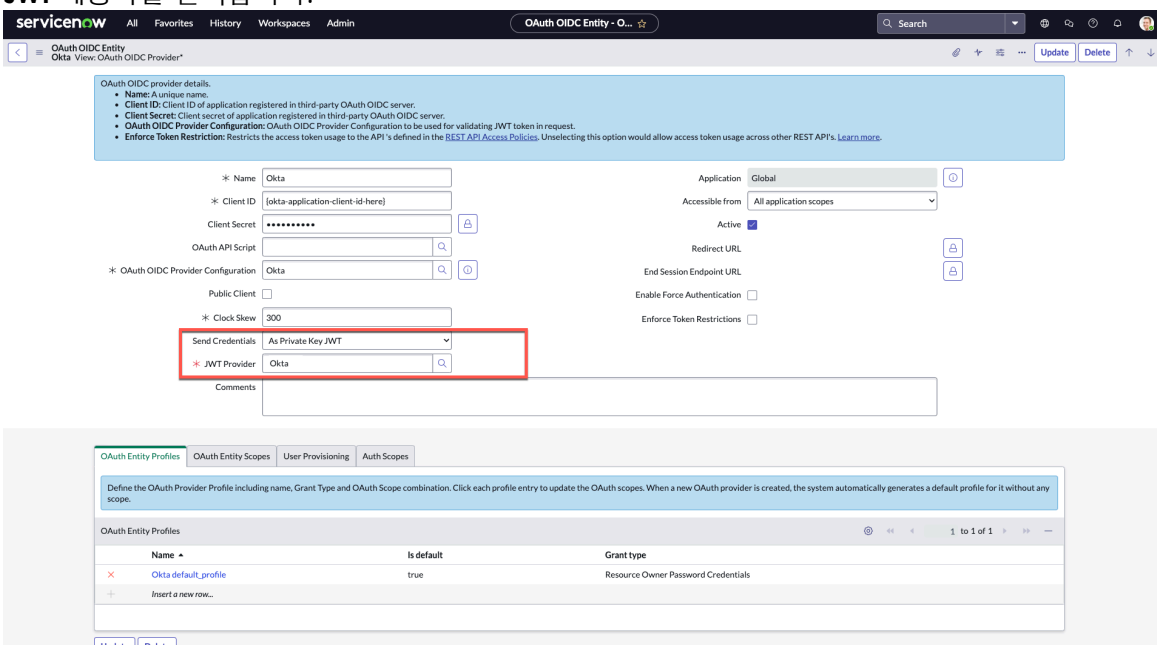
- 통합 - 다중 제공자 1회 사용자 인증 설치 관리자(`com.snc.integration.sso.multi.installer`) 플러그인을 설치합니다.
- 복수 제공자 **SSO** 속성에 속성을 사용합니다. 자세한 내용은 복수 제공자 SSO 속성, 테이블 및 스크립트 문서를 참조하십시오.
- OIDC ID 제공자를 생성합니다. 자세한 내용은 1회 사용자 인증(SSO)에 대한 OIDC(OpenID Connect) 구성 만들기 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 시스템 **OAuth** > 애플리케이션 레지스트리.
2. 생성한 OIDC ID 제공자를 선택합니다.
3. 양식 상단에서 구성 > 양식 설계.

주: OIDC 기반 ID 제공자 인증 요청에 개인 키 JWT를 사용하려면 자격 증명 보내기 및 **JWT** 제공자 필드를 양식에 추가해야 합니다.

4. 자격 증명 보내기를 위해 개인 키로 JWT를 선택합니다.
5. **JWT** 제공자를 선택합니다.



사용자가 인증하면 인증 페이지에 Okta를 통해 로그인하는 옵션이 있습니다.

아웃바운드 OAuth에 대한 개인 키 **JWT** 구성

아웃바운드 OAuth 통합에 대한 개인 키 JWT를 구성합니다.

시작하기 전에

필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

아웃바운드 OAuth 통합에 대해 개인 키 JWT를 구성하기 전에 다음 작업을 수행해야 합니다.

- Java 키 스토어 인증서 업로드: JWT 클라이언트 인증을 활성화하는 데 사용할 JKS 인증서를 인스턴스에 첨부합니다.
- JWT 서명 키 구성: JKS(Java KeyStore) 인증서에 할당할 JWT 서명 키를 생성합니다.

  주: **X.509** 인증서 **SHA-1** 지문 **int(x5t)**를 JWT 키의 일부로 헤더에 추가하려면 양식을 구성하고 **X.509** 인증서 **SHA-1** 지문 **int(x5t)** 필드를 추가해야 합니다.

- JWT 서명 키를 사용하여 JWT 제공자 작성: 인스턴스에 JWT 제공자 ServiceNow 를 추가합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 **OAuth** > 애플리케이션 레지스트리 을 클릭한 다음 새로 만들기를 클릭합니다.
2. 인터셉터 페이지에서 외부 공급업체 **OAuth** 제공자에 연결을 클릭한 다음 양식을 작성합니다.

   주: 아웃바운드 OAuth 인증 요청에 개인 키 JWT를 사용하려면 자격 증명 보내기 및 **JWT** 제공자 필드를 양식에 추가해야 합니다.

필드	설명
이름	외부 공급업체 OAuth 연결의 고유한 이름입니다.
클라이언트 ID	타사 OAuth 서버에 등록된 애플리케이션의 클라이언트 ID입니다.
클라이언트 비밀	타사 OAuth 서버에 등록된 애플리케이션의 클라이언트 비밀입니다.
OAuth API 스크립트	외부 OAuth 제공자에 대한 요청 및 응답을 사용자 지정하는 데 사용되는 스크립트입니다.
로고 URL	OAuth 애플리케이션 로고 URL입니다.
기본 부여 유형	선택: 클라이언트 자격 증명: 클라이언트 ID 및 클라이언트 암호로, 둘 다 액세스 토큰을 가져오는 데 사용됩니다. 이 메서드는 새로 고침 토큰을 제공하지 않습니다.
새로 고침 토큰 수명	새로 고침 토큰이 유효한 시간(초)입니다. 기본 시간은 8,640,000초입니다.
공용 클라이언트	공용 클라이언트가 권한 부여를 위해 PKCE를 요구할 수 있도록 합니다. 주: PKCE *Default Grant type*가 활성화된 경우 인증 코드만 사용할 수 있습니다.
설명	OAuth 앱에 대한 의견을 추가합니다.
애플리케이션	이 기록이 포함된 애플리케이션 및 범위입니다.
다음에서 접근 가능	모든 애플리케이션 범위 또는 이 범위에서만 이 앱에 액세스할 수 있도록 합니다.
활성	앱을 활성화하려면 확인란을 선택합니다.
인증 URL	OAuth 인증 코드 엔드포인트입니다.
토큰 URL	OAuth 서버 토큰 엔드포인트입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
토큰 해지 URL	OAuth 서버 토큰 해지 엔드포인트입니다.
리디렉션 URL	OAuth 콜백 엔드포인트입니다. 비어 있으면 인스턴스가 항목을 자동으로 생성합니다.
상호 인증 사용	토큰 요청 및 해지에 상호 인증을 사용하려면 확인란을 선택합니다. 이 기능을 사용하려면 상호 인증 프로파일을 지정해야 합니다.
자격 증명 보내기	선택: 개인 키 JWT로
JWT 제공자	JWT 제공자 상세 정보. 조회를 사용하여 JWT 제공자를 선택할 수 있습니다.

시스템은 개인 JWT 키 인증에 사용할 수 있는 유형 OAuth 제공자로 애플리케이션 레지스트리 [oauth_entity] 테이블에 기록을 작성합니다.

아웃바운드 **REST** 메시지 작성

아웃바운드 REST 메시지를 생성하여 인스턴스를 인증 서버로 인증합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 시스템 웹 서비스 > 아웃바운드 > **REST** 메시지 을 클릭한 다음 새로 만들기를 클릭합니다.
2. 설명된 대로 OAuth 애플리케이션 기록의 양식 필드를 입력합니다.
   다음 필드 값을 참고하십시오.
   - 엔드포인트: 권한 부여 서버인 인스턴스의 URL입니다.
   - 인증 유형: **OAuth 2.0**.
   - **OAuth** 프로파일: 클라이언트 서버에 대해 생성한 OAuth 프로파일입니다.
3. REST 메시지 기록에서 **OAuth** 토큰 가져오기를 클릭합니다.
4. 토큰을 제공하는 인스턴스로 인증합니다. 방법은 SSO(Single Sign-On) 통합에 따라 다릅니다.
   다음을 사용할 수 있습니다.
   - 인스턴스를 인증하는 데 사용하는 사용자 이름과 암호입니다.
   - IDP의 사용자 이름 및 암호입니다(활성화된 경우). **Use External** Login(외부 로그인 사용)을 클릭하여 IdP 로그인 화면에 액세스합니다.

     주: IdP 로그인 페이지로 자동 리디렉션되려면 glide.authenticate.external 시스템 속성을 설정해야 합니다.

   - MFA가 활성화된 경우 코드입니다.
5. 허용 또는 거부를 클릭하여 권한 부여를 완료하고 토큰을 발급합니다.
   다음 프로세스는 에 설명되어 있습니다 OAuth 인증 코드 부여 플로우.

인스턴스에 자체 등록 **ServiceNow**

외부 사용자 자체 등록을 사용하여 대량의 외부 사용자를 인스턴스에 온보딩합니다. 이 기능은 ID 검증을 강화하여 고객 경험을 개선하고 일반적으로 사용되는 등록 플로우를 지원합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색



셀프 레지스터의 기능 및 비즈니스 가치에 대해 알아봅니다.

활성화



외부 자가 등록을 활성화하는 방법을 이해합니다.

구성



자체 등록을 구성합니다.

사용



자체 등록의 속성에 대해 알고 있습니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

셀프 레지스터 살펴보기

외부 사용자 자체 등록을 사용하여 대량의 외부 사용자를 인스턴스에 온보딩합니다. 이 기능은 ID 검증을 강화하여 고객 경험을 개선하고 일반적으로 사용되는 등록 플로우를 지원합니다.

외부 사용자 셀프 등록을 사용하면 관리자의 도움 없이 많은 사용자 그룹이 앱에 등록할 ServiceNow 수 있습니다. 예를 들어, 캠퍼스 내 주차가 필요한 학생 그룹이 많은 대학은 캠퍼스 주차 앱에 등록할 수 있습니다. 각 학생은 주차와 관련된 제한된 특권을 부여받고 자동 등록 절차를 완료하게 됩니다. 이 시스템은 각 학생에게 고유한 주차 번호를 생성하고 주차 공간이 있는지 확인할 수 있습니다.

자체 등록 플로우는 사용자 지정 ServiceNow 앱(이 경우 캠퍼스 주차 앱)으로 구성됩니다. 필요한 테이블이 있는 앱을 구성한 후 관리자는 사전 등록 플로우, 필드 매핑, 사후 등록 매핑, captcha, 역할 매핑 및 사후 등록 플로우를 포함한 등록을 구성합니다.

외부 사용자 자가 등록 활성화

관리자 역할이 있는 경우 외부 사용자 셀프 등록 플러그인(com.snc.external_user_self_registration)을 활성화할 수 있습니다.

시작하기 전에
필요한 역할: admin

이 태스크 정보

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 조건과 검색 창을 사용하여 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.

3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

자체 등록의 외부 역할

실수로 외부 사용자에게 액세스 권한을 제공하는 것을 방지하기 위해 모든 외부 사용자에게 snc_external 역할을 할당할 수 있습니다.

자체 등록하는 외부 사용자에게는 최소 권한을 가진 snc_external 역할이 할당되어야 합니다. snc_external 역할은 사용자가 조직 외부에 있음을 나타내며 ACL을 통해 snc_external 역할을 상속하는 추가 역할 또는 snc_external 역할을 명시적으로 허락받지 않는 한, 자원에 대한 액세스 권한을 가질 수 없습니다.

기본적으로 snc_external 역할이 있는 사용자는 다음에 접근할 수 없습니다.

- external로 표시되지 않은 스크립팅된 REST API 자원입니다.
- snc_external 역할이나 public 역할을 상속하는 역할이 없는 테이블
- snc_external 역할 또는 snc_external 역할을 상속하는 역할이 없는 프로세서와 UI 페이지와 같은 기록이 아닌 형식의 리소스입니다.
- 플랫폼 분석 대시보드.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Paris 릴리스부터는 exclude-list 속성을 활성화하여 snc_external 역할의 명시적 할당을 적용해야 합니다. 속성을 사용하도록 설정하는 방법에 대한 자세한 내용은 외부 사용자에 대한 향후 내부 역할 할당 방지 를 참조하세요.

외부 사용자에 대한 사용자 등록 구성 구성

사용자 등록 구성 기록을 생성하여 사용자 지정 ServiceNow 애플리케이션에 대한 외부 사용자의 온보딩 프로세스를 부트스트랩합니다. 이 양식은 외부 사용자에게 자체 등록 프로세스를 안내합니다.

시작하기 전에

- 필요한 역할: 관리자
- 외부 사용자 자가 등록 활성화

프로시저

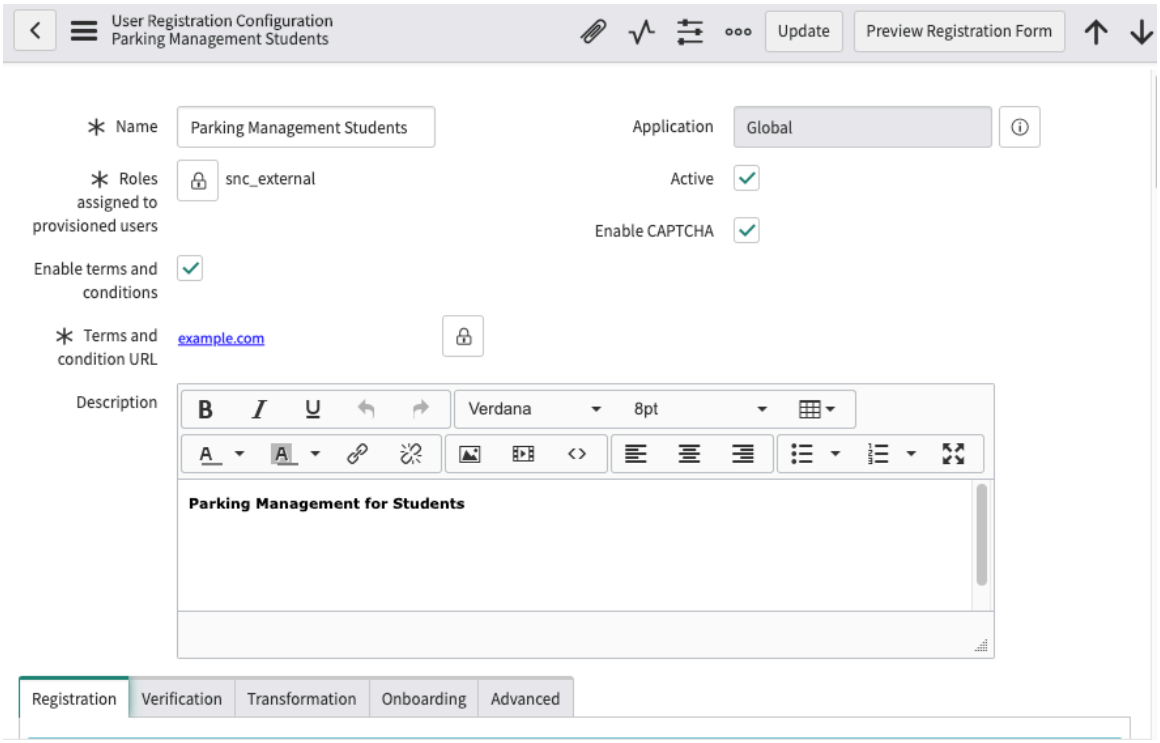
1. 다음으로 이동 모두 > 외부 사용자 셀프 등록 > 사용자 등록 구성 을 클릭하고 신규를 클릭합니다.
2. 양식의 필드에 내용을 입력합니다.

사용자 등록 구성 양식

필드	설명
이름	등록 양식의 이름입니다 . 예를 들어, 학생 주차 등록은 Parking Management Students일 수 있습니다.
프로비저닝된 사용자에게 할당된 역할	프로비저닝된 사용자에게 할당된 역할입니다. 지정된 역할은 `snc_external` 역할을 확장하거나 포함해야 합니다. 지정된 역할은 `snc_external` 역할일 수도 있습니다. 외부 사용자의 경우 각 역할에는 외부 사용자를 알리는 `snc_external` 있어야 합니다. 미리 구성된 역할이 있는 경우 역할의 잠금을 해제하고 사용자를 검색할 때 역할에 접근할 수 있어야 합니다.
사용 약관 사용	등록 페이지에 사용 약관 URL을 추가하는 옵션입니다.
사용 약관 URL	등록 양식의 사용 약관을 포함하는 공개적으로 접근 가능한 URL입니다. 이 필드는 사용 약관 사용이 선택된 경우에만 나타납니다.
설명	등록 양식에 대한 설명입니다. 이 필드는 구성을 저장하거나 제출할 때만 나타납니다. 이 필드에 등록 양식에 대한 추가 정보를 추가할 수 있습니다. 주: 사용자 등록 구성을 저장하거나 업데이트한 후에만 설명을 추가할 수 있습니다.
애플리케이션	이 기록이 포함된 애플리케이션입니다. 애플리케이션은 `##`으로 자동 설정됩니다.
활성	사용자 등록 구성을 활성화하는 옵션입니다. 이 옵션은 기본적으로 선택됩니다.
CAPTCHA 사용	등록 양식에 CAPTCHA를 추가하는 옵션입니다. 기본 CAPTCHA 제공자는 Google reCAPTCHA입니다. 주: 사용자 등록에 CAPTCHA를 활성화하려면 다음 외부 사용자 셀프 등록을 위한 구성 Google reCAPTCHA의 단계를 수행하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 제출을 클릭합니다.
   기본 설정이 포함된 사용자 등록 구성이 생성됩니다.



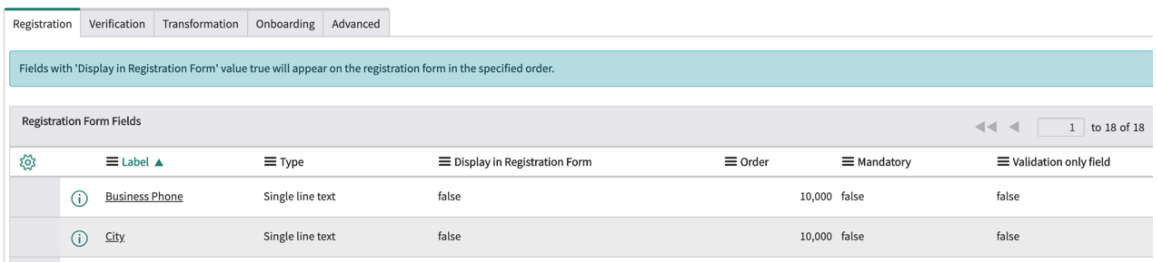
4. 옵션: 필드와 표시되는 순서를 표시하도록 등록 탭을 구성합니다.

등록 양식 필드

열	설명
등록 양식에 표시	True로 표시하려는 필드를 #####.
순서	양식에 필드를 표시할 순서 번호를 설정합니다.
필수	필수로 설정하려는 필드를 #로 설정합니다.
확인 전용 필드	확인에만 사용하려는 필드를 설정합니다. 예를 들면 등록 코드입니다.

기본 양식 필드를 표시하도록 선택하거나 등록 양식에 사용자 지정 양식 필드를 추가할 수 있습니다. 자세한 내용은 기본 등록 양식 필드 문서를 참조하십시오.

등록 탭



사용자 지정 등록 양식 필드를 추가할 수도 있습니다. 자세한 내용은 사용자 지정 등록 양식 필드 추가 문서를 참조하십시오.

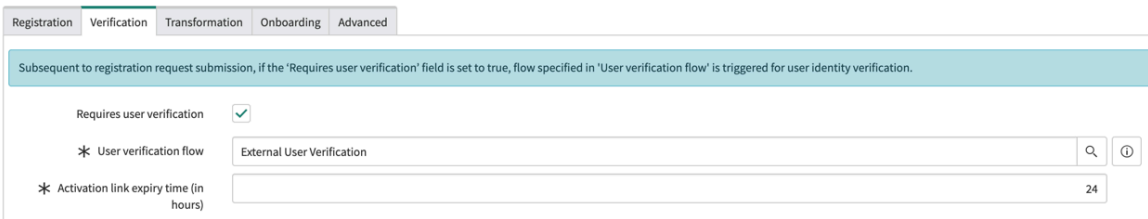
5. 옵션: 등록된 사용자의 신원을 확인하도록 검증 탭을 구성합니다. 사용자 검증 플로우가 트리거되면 사용자의 등록된 이메일 주소로 활성화 링크가 전송됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검증 탭 필드

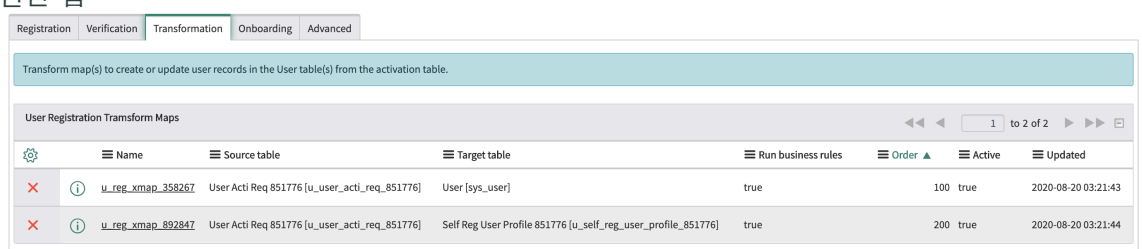
필드	설명
사용자 검증 필수	사용자 등록 후 실행되는 사용자 검증 하위 플로우를 트리거하는 옵션입니다. 하위 플로우는 사용자 ID 확인을 위한 것입니다.
사용자 검증 플로우	사용자의 ID를 확인하는 데 사용되는 하위 플로우입니다. 사용자 검증을 활성화한 경우에만 하위 플로우가 트리거됩니다. (Optional) 기본적으로 외부 사용자 검증 하위 플로우를 사용할 수 있습니다. 에서 플로우 디자이너 기본 하위 플로우의 사본을 생성하고 요구 사항에 따라 수정할 수 있습니다. 자세한 내용은 다음 문서를 참조하십시오플로우 디자이너 . 주: 새 탭에서 외부 사용자 검증 하위 플로우를 미리 보려면 다음 바로 가기를 사용합니다. ◦ Macintosh: Command + 클릭 ◦ Windows: Control + 클릭
활성화 링크 만료 시간(시간 단위)	활성화 링크가 만료되기까지 남은 시간입니다. 기본값은 24입니다.

검증 탭



6. 옵션: 자체 등록 사용자와 활성화된 사용자를 매핑하도록 변환 탭을 구성합니다.
사용자 활동 요청 [number] 테이블에서 자체 등록 사용자 [number] 테이블로 등록된 사용자를 자동으로 매핑하는 두 개의 변환 맵(u_reg_xmap_〔number〕)이 있습니다. 이러한 기본 변환 맵의 사본을 만들고 요구 사항에 따라 맵을 수정할 수 있습니다. 자세한 내용은 변환 맵을 참조하십시오.

변환 탭

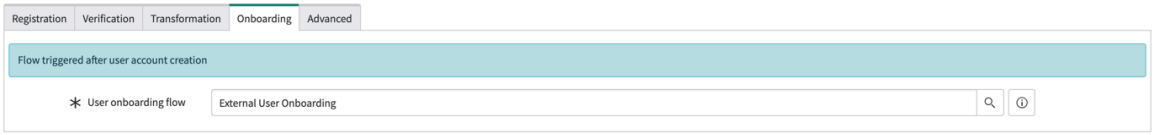


7. 온보딩 활성화 사용자에 대한 하위 플로우를 트리거하도록 온보딩 탭을 구성합니다.
기본 외부 사용자 온보딩 하위 플로우는 암호를 재설정하는 링크가 포함된 이메일을 사용자에게 보냅니다. 기본 하위 플로우의 사본을 생성하고 요구 사항에 따라 수정할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

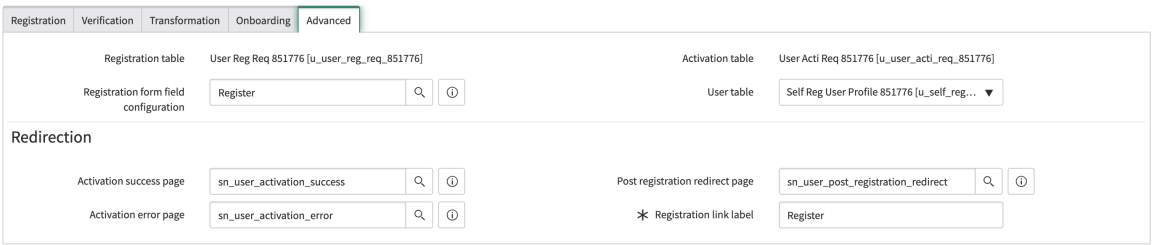
주: 외부 사용자 온보딩 하위 플로우가 트리거되면 하위 플로우는 암호를 재설정하는 링크가 포함된 이메일을 사용자에게 보냅니다.

온보딩 탭



8. 옵션: 고급 탭을 구성하여 등록 양식의 사용자 테이블과 리디렉션 페이지를 매핑합니다.

고급 탭



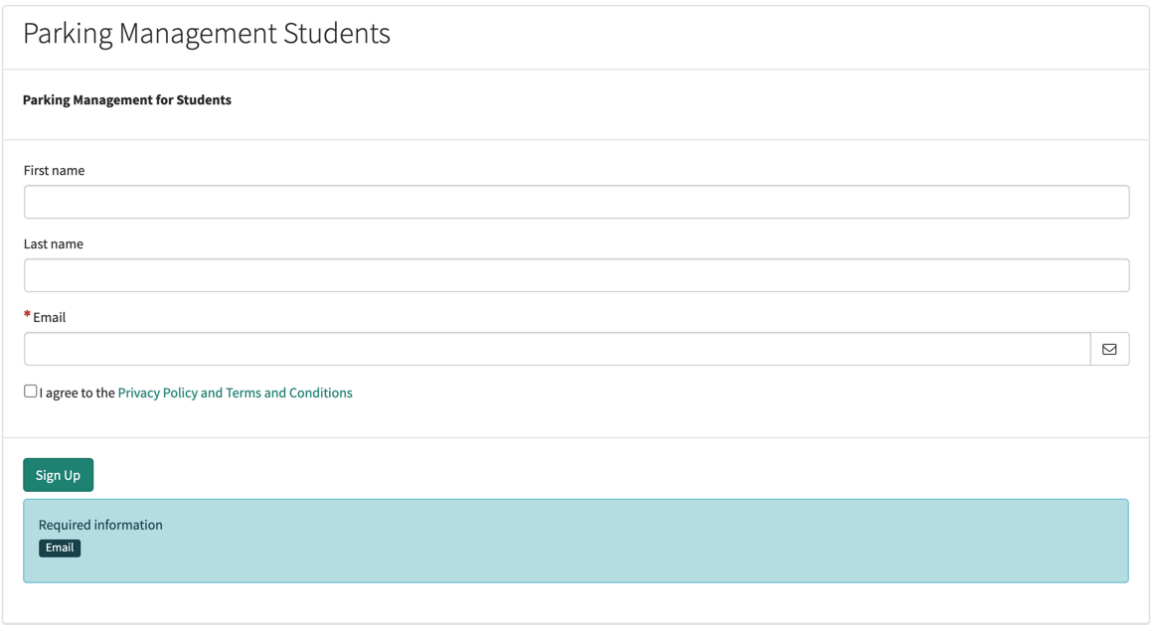
고급 탭

필드	설명
등록 테이블	등록 양식 정보가 저장되는 테이블의 이름입니다.
등록 양식 필드 구성	기록 생성자의 등록 양식과 연결된 기록입니다.
활성화 테이블	사용자 활성화에 사용되는 테이블의 레이블 및 이름입니다. 활성화 테이블에는 검증을 완료한 사용자의 기록이 포함되어 있습니다.
사용자 테이블	사용자 프로파일 테이블의 레이블 및 이름입니다.
활성화 성공 페이지	활성화에 성공한 후 사용자가 리디렉션하는 페이지입니다.
활성화 오류 페이지	활성화가 실패할 때 사용자가 리디렉션하는 페이지입니다.
게시물 등록 리디렉션 페이지	등록 후 사용자가 리디렉션되는 페이지입니다.
등록 링크 레이블	서비스 포털에서 등록하는 데 사용되는 버튼 이름입니다. 기본값은 Register입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

변경하는 동안 또는 사용자 등록 구성의 모든 변경을 완료한 후 등록 양식 미리 보기 버튼을 사용하여 등록 양식의 변경 내용을 미리 볼 수 있습니다.

등록 양식 미리 보기



외부 사용자 셀프 등록을 위한 구성 **Google reCAPTCHA**

서비스를 사용하려면 Google reCAPTCHA 에서 API 키 페어를 Google 요청한 후 관련 시스템 속성을 구성해야 합니다.

시작하기 전에

- at https://www.google.com/recaptcha 에서 Google API 키 쌍(사이트 키 및 암호)을 요청합니다.
- 필요한 역할: 관리자

이 태스크 정보

프로시저

1. 다음으로 이동 모두 > 시스템 속성 > 모든 속성.
2. 다음 속성을 검색하고 값을 설정합니다.

속성	값
glide.user.registration.google.recaptcha.secret	비밀은 애플리케이션과 reCAPTCHA 서버 간의 통신을 승인합니다. 유형: password2
glide.user.registration.google.recaptcha.site_key	등록 페이지에서 reCAPTCHA 서비스를 호출하는 데 사용되는 사이트 키입니다. 유형: string

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성	값
glide.user.registration.captcha.widget	Captcha 위젯의 Sys_ID입니다. 유형: 문자열

기본 등록 양식 필드

기본 등록 양식 필드를 사용하거나 사용자 지정 등록 양식 필드를 만들 수 있습니다.

등록 양식 필드

기본적으로 등록 양식에 다음 양식 필드가 추가됩니다.

필드 레이블	유형
직장 전화번호	1줄 텍스트
구/군/시	1줄 텍스트
국가	선택 상자
EDU 상태 직원, 학생 및 방문자를 구별하는 데 사용됩니다. 주: 이 필드는 등록 양식이 교육 기관에 대한 경우 유용합니다.	선택 상자
이메일	이메일
이름	1줄 텍스트
성별	1줄 텍스트
집 전화 번호	1줄 텍스트
언어	선택 상자
성	1줄 텍스트
중간 이름	1줄 텍스트
휴대폰	1줄 텍스트
이름	1줄 텍스트
프리픽스 사용자의 직함입니다. 예를 들어, Mr. , Dr. 등입니다.	선택 상자
시/도	1줄 텍스트
주소	넓은 1줄 텍스트
직함 - 직함	선택 상자
우편 번호	1줄 텍스트

주: 기본 등록 양식 필드는 삭제할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사용자 지정 등록 양식 필드 추가

사용자 자가 등록 양식에 사용자 지정 필드를 추가할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 외부 사용자 셀프 등록 > 사용자 등록 구성.
2. 필요한 사용자 등록 구성에 대한 기록을 엽니다.
3. Registration Form Fields 섹션의 끝으로 이동하여 **Insert a new row...**를 클릭합니다.
4. 레이블 열 아래에 필드 이름을 입력하고 확인 표시를 클릭합니다.
   새 행이 기본값으로 추가됩니다. 요구 사항에 따라 사용자 지정 등록 양식 필드를 구성할 수 있습니다.

   등록 양식 필드 열

열	설명
레이블	등록 양식에 나타나는 필드 이름입니다.
유형	사용자 인터페이스 요소의 유형입니다. 지원되는 유형은 다음과 같습니다. ◦ 1줄 텍스트 ◦ 이메일 ◦ 날짜 ◦ 날짜/시간 ◦ 예/아니요 ◦ 넓은 1줄 텍스트 ◦ 복수 선택 ◦ 선택 상자
등록 양식에 표시	등록 양식에 필드를 표시하는 옵션입니다.
순서	등록 양식에서 양식 필드가 나타나는 순서입니다. 순서 값이 가장 낮은 필드가 먼저 나타나고 순서 값이 가장 높은 필드가 마지막에 나타납니다. 기본값은 10,000입니다.
필수	등록 양식에서 필드를 필수 필드로 만드는 옵션입니다.
확인 전용 필드	확인 목적으로만 필드를 사용하는 옵션입니다. 예를 들면 등록 코드입니다. true로 설정하면 이 필드가 사용자 테이블(sys_user)에 저장되지 않습니다.

5. 변경 내용을 저장하거나 업데이트합니다.

에 대한 외부 사용자 셀프 등록 사용 서비스 포털

외부 사용자가 서비스 포털을 통해 ServiceNow 앱에 등록할 수 있도록 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 서비스 포털 > 포털.
2. 포털 기록을 엽니다.
3. 양식의 외부 사용자 등록 구성 필드에 내용을 입력합니다.

   사용자 등록 구성을 선택합니다.

4. 업데이트를 클릭합니다.

결과
로그인 위젯에는 이전에 구성한 등록 양식에 대한 링크가 포함됩니다.

사용자 셀프 등록 요청 검증

사용자가 에서 등록하면 서비스 포털 사용자 기록이 등록 요청 모듈에 추가됩니다. 에 서비스 포털 성공적으로 등록한 등록된 사용자 목록을 볼 수 있습니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 외부 사용자 셀프 등록 > 등록 요청.
   사용자 기록 목록이 표시됩니다.
2. (선택 사항) 개별사용자 기록을 검토하고 요구 사항에 따라 수정합니다. 예를 들어 사용자 기록 양식의 상태를 보류 중 에서 처리됨으로 변경할 수 있습니다.

토큰 기반 인증(사용자 로그인)

토큰 기반 인증을 사용하여 사용자가 네트워크에 액세스할 수 있도록 보안 메커니즘을 개선합니다.

시간 제한 인증



다이제스트 토큰 인증



기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

토큰 기반 인증은 사용자가 자신의 ID를 확인하고 그 대가로 고유한 액세스 토큰을 받을 수 있도록 하는 프로토콜입니다.

사용자가 네트워크에 액세스할 수 있도록 보안 메커니즘을 강화하는 데 도움이 됩니다.

다이제스트 토큰 인증은 암호화 되지 않은 HTTP 헤더 내에서 사용자 자격 증명과 다이제스트 토큰을 전달합니다.

시간 제한 인증

인스턴스에 대해 ServiceNow 시간 제한 인증을 지원합니다.

탐색



시간 제한 인증의 기능 및 비즈니스 가치에 대해 알아봅니다.

활성화



시간 제한 인증을 활성화하는 방법을 이해합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자습서: 시간 제한 인증



제로 트러스트 액세스의
속성에 대해 알아봅니다.

시간 제한 인증 탐색

인스턴스에 대해 ServiceNow 시간 제한 인증을 지원합니다.

주: 시간 제한 인증은 인스턴스에 따라 매우 다르 ServiceNow 며, 사용자에 대한 사용자 지정 링크는 다음 내에서만 ServiceNow작성할 수 있습니다.

관리자는 인스턴스에서 링크 기반 인증을 구성할 수 있습니다 ServiceNow . 구성된 링크는 이메일 또는 SMS를 통해 사용자와 공유할 수 있으며 사용자는 이러한 링크를 사용하여 인스턴스에 로그인할 수 있습니다.

이 인증 체계를 사용하여 인스턴스에 로그인하는 것은 인스턴스에 구성된 ServiceNow 적응형 인증 정책을 통해 제어됩니다.

시간 기반 인증을 사용하면 다음을 수행할 수 있습니다.

- 관리자는 만료 시간 내에 사용하도록 링크 기반 인증을 구성할 수 있습니다.
- 애플리케이션 팀은 노출된 스크립트 가능한 API를 사용하여 특정 구성 항목에 대한 링크와 함께 사용할 nonce를 가져올 수 있습니다. 링크 작성은 애플리케이션 팀에서 처리합니다.
- 애플리케이션 팀은 링크를 생성하고 기존 채널을 통해 사용자에게 보낼 수 있습니다.
- 링크가 있는 사용자는 구성의 일부로 지정된 만료 시간 내에 인스턴스에 한 번 로그인할 수 있습니다.
- 관리자는 인증 체계에 대해 낮은 권한의 역할을 구성할 수 있습니다.
- 관리자는 TLA 링크를 통한 인증의 두 번째 단계로 인증 체계에 MFA를 적용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시간 제한 인증 활성화

시간 제한 인증은 통합 - 복수 제공자 1회 사용자 인증(SSO) 설치 관리자 플러그인을 통해 활성화됩니다.

시작하기 전에
필요한 역할: 관리자

> 주: 시간 제한 인증은 인스턴스에 따라 매우 다르 ServiceNow 며, 사용자에 대한 사용자 지정 링크는 다음 내에서만 ServiceNow작성할 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 *##*제한 인증 (com.snc.authenticate.time_limited_authentication) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   > 주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

SMS를 사용한 시간 제한 인증 - **Twilio** 자습서

를 사용하여 TwilioSMS와 같은 MFA 요소로 시간 제한 인증을 설정합니다.

시작하기 전에
필요한 역할: 관리자

필요한 플러그인:

- *com.snc.authenticate.time_limited_authentication* (시간 제한 인증)
- *com.snc.authentication.sms_mfa* (SMS를 사용한 다단계 인증)

> 주: TLA(시간 제한 인증)는 인스턴스에 따라 매우 다르 ServiceNow 며, 사용자에 대한 사용자 지정 링크는 다음 내에서만 ServiceNow생성할 수 있습니다.

제공된 튜토리얼 지침을 통해 관리자는 특정 역할을 가진 사용자에게 SMS를 MFA(2단계)로 사용하는 링크 기반 로그인을 제공할 수 있습니다.

구성이 성공하면 시스템에서 링크를 생성한 다음 알림(이메일/SMS) 채널을 통해 사용자와 링크를 공유합니다. 링크를 클릭하면 사용자 역할(구성)에 따라 이메일 또는 SMS로 전송되는 OTP 요소를 지정하라는 메시지가 사용자에게 표시됩니다.

> 주:
>
> - TLA 뒤에는 항상 MFA가 뒤따라야 하며, TLA 로그인에 적응형 인증을 사용하여 관리자가 MFA를 활성화해야 합니다. 적응형 인증을 사용하여 MFA를 구성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 MFA(다단계 인증) 컨텍스트.
> - TLA는 권한이 제한된 사용자에 대해 사용해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. Twilio 구성을 생성합니다.

a. Twilio 테스트 계정을 생성합니다. 자세한 내용은 다음을 참조하십시오. Twilio .

b. 다음으로 이동 모두 > 알림 > 관리 > **Twilio** 직접 구성.

c. 계정 **SID** 및 인증 토큰(에서 Twilio생성됨)을 입력하고 기록을 저장합니다.

주: 고유한 제공자 구성을 생성하여 TLA에 사용할 수 있습니다. 이 예에서는 Twilio입니다. MFA 제공자 구성을 생성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 MFA 제공자 구성.

2. TLA(시간 제한 인증) 기록 구성 및 사용.

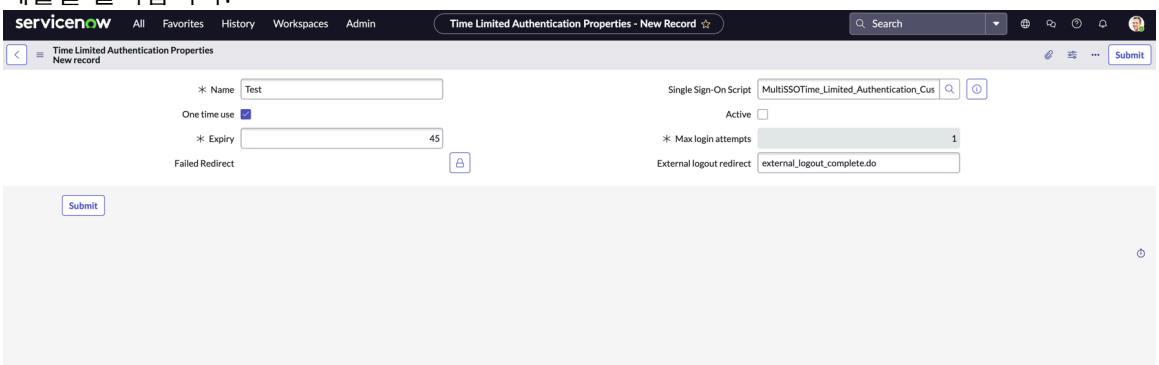
a. 다음으로 이동 모두 > 시간 제한 인증 구성 기록 을 클릭하고 신규를 클릭합니다.

b. 양식에서 필드를 채웁니다.

시간 제한 인증 속성

필드	설명
이름	기록의 이름입니다.
1회용	TLA 링크를 한 번 사용하도록 설정합니다.
만료	링크 만료 시간(초)을 지정합니다. 기본값은 45분입니다.
실패한 리디렉션	인증 실패 후 사용자를 리디렉션할 URL을 입력합니다.
1회 사용자 인증(SSO) 스크립트	사용할 SSO 스크립트의 상세 정보입니다.
활성	구성을 활성화하는 옵션입니다.
최대 로그인 시도	생성된 TLA 링크에 허용되는 로그인 시도 횟수를 지정합니다. 1회용 확인란의 선택을 취소하여 최대 시도 횟수를 제공합니다.
외부 로그아웃 리디렉션	로그아웃한 사용자를 리디렉션할 URL을 입력합니다.

c. 제출을 클릭합니다.



d. 다음으로 이동 모두 > 복수 제공자 **SSO** > 관리 > 속성 을 클릭하고 복수 제공자 **SSO** 사용 속성을 활성화하고 저장합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

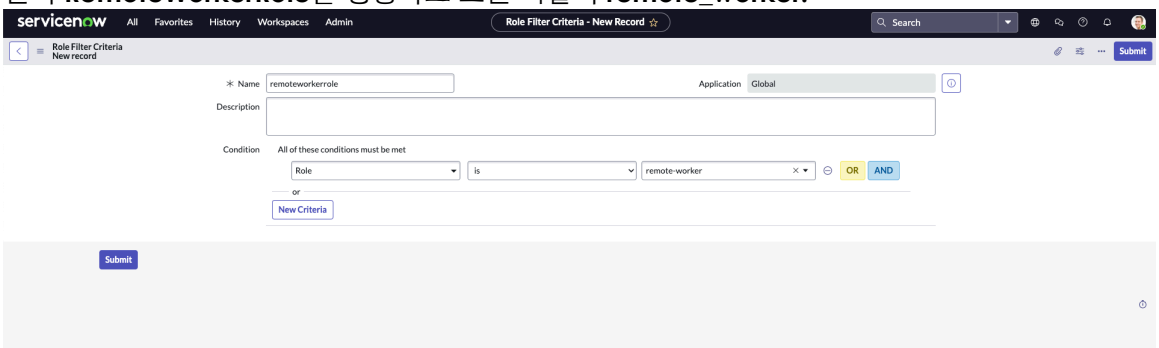
3. TLA가 사후 인증 컨텍스트 정책을 사용하여 특정 사용자 가상 사용자에게만 허용.

   a. 역할로 이동하여 역할을 생성합니다. 예: remote_worker.

   b. 유효한 이메일 ID와 휴대폰 번호로 사용자를 생성합니다. 사용자를 만드는 방법을 알아보려면 사용자 만들기를 참조하십시오.

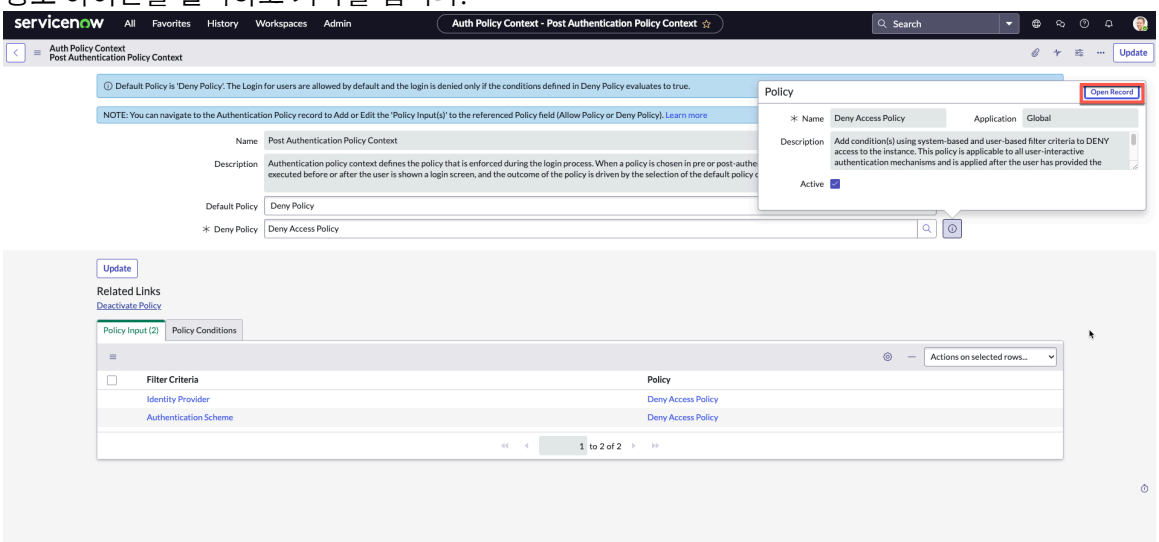
   c. 사용자에게 역할을 할당합니다. 사용자에게 역할을 할당하는 방법을 알아보려면 사용자에게 역할 할당을 참조하세요.

   d. 역할 필터 기준을 작성하려면 다음으로 이동하십시오. 모두 > 적응형 인증 > 역할 필터 기준, 새 필터 **RemoteWorkerRole**을 생성하고 조건 역할이 **remote_worker.**



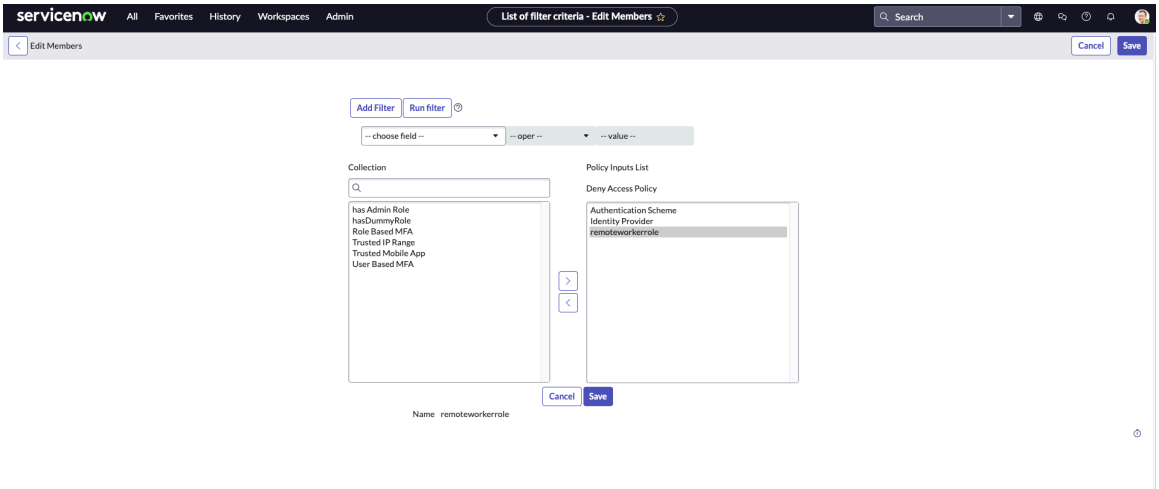
   e. IdP 및 역할 필터 기준에 따라 거부 정책 컨텍스트를 기반으로 정책 조건을 추가하려면 다음으로 이동합니다. 모두 > 적응형 인증 > 사후 인증 컨텍스트.

   f. 정보 아이콘을 클릭하고 기록을 엽니다.



   g. 정책 입력에서 편집을 클릭하고 역할(remoteworkerrole)을 추가하고 저장합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

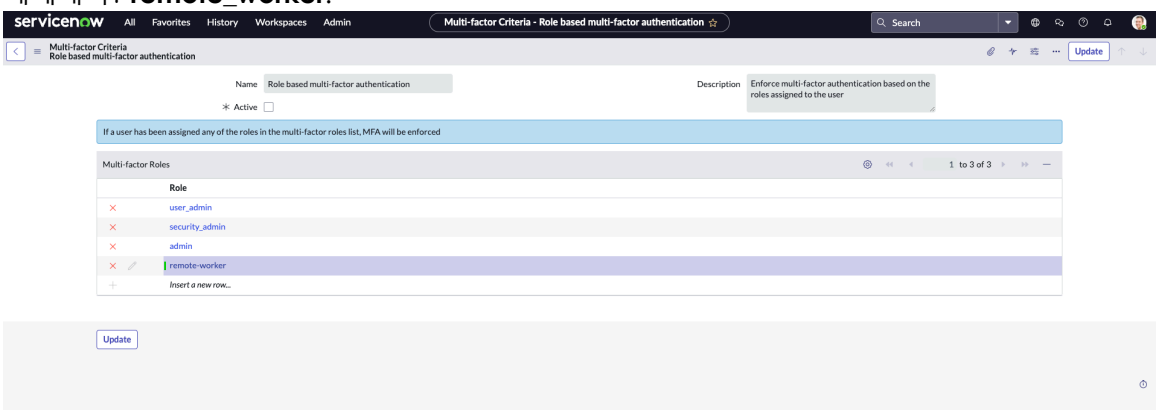


h. 정책 조건에서 정책 입력에 대한 조건을 추가하고 기록을 제출 합니다.

4. 스텝업 인증 정책 구성 - MFA 컨텍스트.

a. 다음으로 이동 모두 > 다중요인 기준.

b. 역할 기반 다단계 인증을 선택하고 다단계 역할 섹션 및 업데이트에서 역할을 추가합니다. 이 예제에서: **remote_worker**.



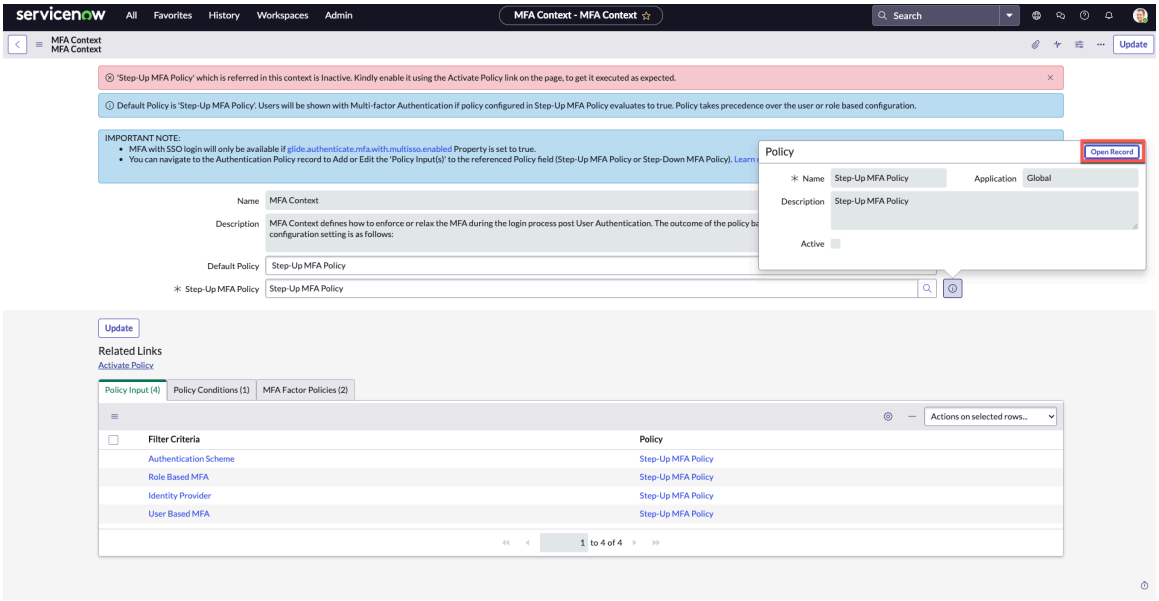
c. 다음으로 이동 모두 > 적응형 인증 > **MFA** 컨텍스트.

d. 다음 사항을 확인하십시오.

- 기본 정책 필드는 스텝업 **MFA** 정책입니다.
- 스텝업 MFA 정책은 스텝업 **MFA** 정책입니다.

e. 정보 아이콘을 클릭하고 기록을 엽니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



f. Step-Up MFA Policy(스텝업 MFA 정책) 양식의 Policy Inputs(정책 입력)에서 Edit(편집)를 클릭합니다.

g. 역할 기반 다단계 인증을 목록에 추가하고 저장합니다. 이 예시에서는 **remoteworkerrole**입니다.

h. 정책 조건에서 역할 기반 또는 사용자 기반 **MFA** 설정이 true인 경우 **MFA** 적용을 클릭합니다.

i. 역할 기반 또는 사용자 기반 MFA 설정이 예인 경우 MFA 적용 페이지에서 역할 기반 **MFA** 가 예인지 확인합니다.

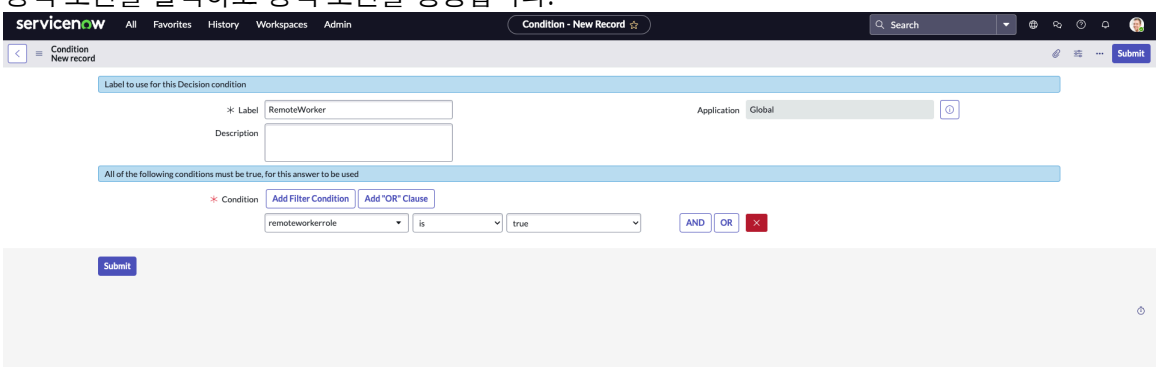
5. SMS를 MFA 요소 정책으로 사용하도록 MFA 적용.

a. 다음으로 이동 모두 > 적응형 인증 > **MFA** 컨텍스트.

b. MFA 컨텍스트 페이지에서 **MFA** 요소 정책을 클릭하고 정책을 클릭합니다. **SMS** OTP를 **MFA** 요소 정책으로 표시합니다.

c. Edit(편집)를 클릭하고 **Policy** Inputs(정책 입력)에서 **remoteworkerrole**을 추가합니다.

d. 정책 조건을 클릭하고 정책 조건을 생성합니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

e. 제출을 클릭합니다.

원격 작업자 역할을 역할로 하여 사용자에게 생성 및 공유된 TLA 링크는 SMS 코드를 인스턴스에 로그인하기 위한 두 번째 단계로 사용하도록 승격됩니다.

6. 다른 필수 속성을 활성화합니다.

a. 다음으로 이동 모두 > 다단계 인증 > 속성.

b. 다음 확인란을 활성화합니다.

- **Multi-Factor Authentication** 사용
- SSO를 통한 다단계 인증 사용

c. 레코드를 저장합니다.

d. 다음으로 이동 모두 > 적응형 인증 > 인증 정책 > 속성.

e. 인증 정책 사용 확인란을 활성화합니다.

f. 레코드를 저장합니다.

7. TLA 링크 생성 – 예.

a. 다음으로 이동 모두 > 시스템 정의 > 스크립트 – 백그라운드.

b. 사용자 sysid 및 구성 ID를 제공하여 다음 API를 사용합니다.

```
var tla=new ##. TimeLimitedAuthentication();
gs.info(tla.generateNonce("user_sysid", "config1_sys_id","IAR2"));
```

주: 소스(IAR2)는 필수 매개변수가 아닙니다.

c. 쿼리 매개변수가 다음과 같이 반환됩니다.

```
nonce=VCeinfboDt0M&glide_sso_id=b3277f1b44351110f8779b5a2d9909f3&user=3b0277d3443511
```

d. 아래 형식으로 URL을 만듭니다.

```
https://<instance-url> /login_with_sso.do?uri=<encoded url>&
nonce=2olIQSxdgkjs&glide_sso_id=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf0371020
```

8. URL을 클릭하면 로그인을 위한 다음 MFA 화면이 표시됩니다.

다이제스트 토큰 인증

다이제스트 토큰 인증은 암호화 되지 않은 HTTP 헤더 내에서 사용자 자격 증명과 다이제스트 토큰을 전달합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색	구성
	
다이제스트 토큰 인증의 기능 및 비즈니스 가치에 대해 알아봅니다.	다이제스트 토큰 인증을 구성하는 방법을 이해합니다.

다이제스트 토큰 인증 탐색

인스턴스는 HTTP 헤더 값을 읽고 다이제스트 토큰의 계산된 해시 값을 비교합니다. 계산된 해시 값이 다이제스트 토큰 값과 일치하면, 인스턴스는 사용자 테이블에서 일치하는 값을 검색합니다. 사용자 테이블에 일치하는 값이 있는 경우, 인스턴스는 사용자가 사전 인증된 것으로 간주하고 사용자를 로그인합니다.

다이제스트 토큰 인증은 암호화되지 않은 HTTP 헤더에 대한 우발적이거나 의도적인 변경으로 인해 다른 해시 값이 생성되기 때문에 암호화되지 않은 단순한 HTTP 헤더보다 더 안전합니다. 해시 값이 일치하지 않으면 인스턴스는 요청된 인스턴스에 대한 사용자 액세스를 거부합니다. 이렇게 하면 사용자가 다른 사용자의 자격 증명으로 로그인을 시도할 수 없습니다.

다이제스트 링크 만료에 대한 자세한 내용은 이 KB 문서를 참조하세요.

주: TLA(시간 제한 인증)를 사용하여 시간 기반 만료 링크를 구성합니다. 자세한 내용은 를 참조하십시오 시간 제한 인증.

통합 요구 사항

다이제스트 토큰 인증 통합에는 다음이 필요합니다.

- 웹 서버
- 로컬 네트워크에서 사용자를 사전 인증하기 위한 SiteMinder 또는 다른 1회 사용자 인증(SSO) 애플리케이션
- 이러한 형식 중 하나로 대상 인스턴스에 사용자 자격 증명을 전달하는 웹 페이지 또는 포털

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- HTTP 헤더
- URL 매개변수
- 쿠키

- 이러한 인코딩 기술 중 하나를 사용하여 다이제스트 토큰을 생성하고 대상 인스턴스에 전달하는 웹 페이지 또는 포털입니다
  - SHA1
  - MD5
  - SHA 256(권장)

다중 제공자 **SSO(Single Sign-**On)에 대한 다이제스트 속성 구성

다이제스트 설치 기존 스크립트를 활성화한 후 다중 제공자 SSO에 대한 속성을 구성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
다중 제공자 Single Sign-On을 사용하지 않는 경우 표준 Single Sign-On 속성을 구성합니다.

프로시저
1. 다음으로 이동 모두 > 복수 제공자 **SSO** > **ID** 제공자.
2. 다이제스트 속성 양식의 필드에 내용을 입력합니다.

옵션	설명
이름	다이제스트 토큰의 이름을 입력합니다.
사용자	수신 헤더에 대해 일치하는 데이터가 포함된 sys_user 필드를 입력합니다.
HTTP 다이제스트 헤더 이름	생성한 HTTP 헤더를 입력합니다. 예: `DE_USER`.
HTTP 헤더 이름	작성된 다이제스트 토큰에 대해 작성한 HTTP 헤더를 입력합니다. 예를 들어 `SM_USER`.
비밀 암호	다이제스트 키를 인코딩하는 데 사용할 비밀 키를 입력합니다. 예를 들어 `32# ##`입니다.
실패한 **SSO** 리디렉션 필드	인증 실패 후 사용자를 리디렉션할 URL을 입력합니다.
외부 로그아웃 리디렉션	로그아웃한 사용자를 리디렉션할 URL을 입력합니다.
1회 사용자 인증**(SSO)** 스크립트	**MultiSSO_DigestedToken** 선택합니다.
클라이언트 유형	클라이언트 유형에 따라 클라이언트 유형을 선택합니다. 옵션: **Iframe** 임베디드. 주: 구성에 클라이언트 유형 필드가 필요한 경우 양식을 편집하고 필드를 추가할 수 있습니다. 자세한 내용은 를 참조하십시오 OAuth 및 SSO 기록에 대한 클라이언트 유형 구성.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 업데이트를 클릭합니다.
4. 다이제스트된 토큰 기본값을 true로 설정합니다.
   기본값을 true로 설정하면 SSO에 연결된 시스템 기본 다이제스트 토큰 기록을 덮어씁니다. 첫 번째 복수 제공자 SSO 관련 IdP 기록이 활성화되면 복수 제공자 SSO와 관련된 기록만 사용됩니다.

   다이제스트 속성 테이블에 있는 다이제스트 토큰 기록은 IdP의 Sys_ID 추가하여 개별적으로 호출할 수 있습니다. 예를 들어 인증 URL의 다이제스트 토큰 기록:
   `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_tok`

샘플 다이제스트 토큰 구현

다음은 다이제스트 토큰을 만드는 몇 가지 샘플입니다.

샘플 다이제스트 인증 구현

로 빌드된 다이제스트	비밀 키 값	해시 방법	예제
Java	32자 이상	SHA256	암호화를 위한 샘플 Java 다이제스트 알고리즘
C	sharedKey 매개변수의 값	strEncryptionMethod 매개변수의 값(SHA256 또는 MD5)	샘플 C

암호화를 위한 샘플 **Java** 다이제스트 알고리즘

이 Java 알고리즘은 HTTP 헤더에서 다이제스트 토큰을 만드는 방법을 보여줍니다.

이 샘플에서는 다음을 가정합니다.

- 웹 서버는 Java를 지원합니다.
- 해시 계산 메서드는 SHA1입니다.
- 비밀 키 값은 abc123입니다.
- 암호화되지 않은 HTTP 헤더 이름이 user_name

다른 해시 계산 메커니즘(예: MD5)을 사용하도록 Java 코드를 변경하거나 비밀 키 값 또는 HTTP 헤더 이름을 변경합니다.

```
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);
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
            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();
        String userName = "user_name";
        System.out.println("base 64 digest username: " +
 encoder.encode(test.getDigest(userName)));
    }
}
```

샘플 **C**

이 C 클래스는 세 개의 입력 매개 변수에서 다이제스트 토큰을 만드는 방법을 보여줍니다.

- strEncryptionMethod – 해시 계산 방법(SHA1, SHA256 또는 MD5)을 나열합니다.
- message – 다이제스트 토큰으로 변환할 값을 나열합니다.
- sharedKey – 비밀 키를 나열합니다.

주: 다이제스트 토큰 작성을 위해 SHA256과 같은 더 강력한 보안 해시 알고리즘을 사용합니다.

이 샘플에서는 다음을 가정합니다.

- 웹 서버는 C를 지원합니다.
- 다른 코드는 이 클래스를 호출하고 예상 매개 변수를 전달합니다

샘플 코드

```
 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 ( ) ;
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
                    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 ;

                default :

                    b64SHA1Message  = "Unknown Encryption Method" ;
break ;

            }


          TextBoxBase64. Text = b64SHA1Message ; return
b64SHA1Message ;

        }
```

웹 서비스 보안

기본 인증, 상호 인증 또는 WS-보안을 사용하여 보안을 적용합니다.

웹 보안 살펴보기	상호 인증 구성
	

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

웹 서비스 보안의 기능 및 비즈니스 가치를 학습합니다.	상호 인증을 사용하여 SSL(Secure Sockets Layer) 인증서를 교환하여 신뢰를 설정합니다.

웹 서비스 보안 탐색

기본 인증, 상호 인증 또는 WS-보안을 사용하여 보안을 적용합니다.

기본 인증

WSDL 문서 또는 SOAP 메시지 게시에 대한 각 요청에 대해 기본 인증을 적용하려면 속성을 *glide.basicauth.required*`true`로 설정할 수 있습니다. 이렇게 하면 각 WSDL 또는 SOAP 요청에 기본 인증 프로토콜에 지정된 대로 "Authorization" 헤더가 포함되어야 합니다. 요청이 비대화형이므로 요청 중에 항상 **Authorization** 헤더가 필요합니다.

필수 여부에 관계없이 기본 인증 정보를 제공하면 웹 서비스 호출의 결과로 작성되거나 업데이트된 데이터가 기본 인증 자격 증명에 제공된 사용자를 대신하여 수행된다는 추가 이점이 있습니다. 예를 들어, 인시던트 기록을 만들 때 저널 필드에는 기본 게스트 사용자 대신 기본 인증 사용자의 사용자 ID가 있습니다.

권한 부여 헤더가 대문자 사용 규칙을 무시하도록 하려면 해당 *glide.security.script.include.name.case.insensitive.list* 속성을 사용합니다. 시스템 속성 [sys_properties] 테이블에서 이 속성을 수정하고 인증을 처리하는 데 필요한 스크립트 포함을 추가할 수 있습니다. 기본적으로 이 속성에는 다음 값이 있습니다.

- BasicAuth
- 사용자 지정 인증

필요에 따라 다른 스크립트 포함을 추가합니다.

Perl 및 SOAP::Lite 라이브러리를 사용할 때 기본 인증을 제공하기 위해 다음 함수를 구현할 수 있습니다.

```
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return
 'user_name' => 'password' ; }
```

- C# .NET VS 2005 또는 이전 버전을 사용하는 경우 다음과 같이 Credentials 개체를 활용할 수 있습니다.

```
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 ) { }
```

- C# .NET VS 2008을 사용하는 경우 다음과 같은 ClientCredentials 개체를 활용할 수 있습니다.

```
Demo_Incident. ServiceNowSoapClient client  = new Test08WebService .
 Demo_Incident . ServiceNowSoapClient ( ) ;
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
client . ClientCredentials . UserName . UserName = "admin" ;
client . ClientCredentials . UserName . Password = "admin" ;
```

그런 다음 app.config 파일에서 다음을 찾아 `None` 을 `Basic` 으로 변경하십시오.

```
<transport clientCredentialType= "None" proxyCredentialType= "None"
 realm= "" />
```

- NET을 사용할 때 Credentials 개체를 활용하는 것은 다음과 같습니다.

```
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
```

기본 인증이 켜져 있고 자격 증명이 제공되지 않은 경우 결과 응답은 다음과 같습니다.

```
<html> <head > <title >Apache Tomcat/5.0.28
 - Error report </ title > <style > <!--H1
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;font-size:22px;}    H2
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;font-size:16px;}    H3
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;font-size:14px;}    BODY
 {font-family:Tahoma,Arial,sans-serif;color:black;background-color:whit
e;}    B
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525
D76;}    P
 {font-family:Tahoma,Arial,sans-serif;background:white;color:black;fo
nt-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 >
```

상호 인증 구성

상호 인증은 SSL(Secure Sockets Layer) 인증서를 교환하여 신뢰를 설정합니다.

SSL 핸드셰이크 중에 서버는 클라이언트에 인증서를 제공합니다. 이후 서버 구성에 따라 클라이언트로부터 인증서를 요청할 수 있습니다. 서버와 클라이언트 모두 인증서 유효성 검사 절차를 수행하여 제공된 인증서의 신뢰성과 무결성을 보장합니다.

확인에 성공하면 HTTPS 연결을 시작하기 전에 승인이 교환됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관리자는 인증 요청이 이행되기 전에 클라이언트 키 저장소를 설정하고 인증서를 생성하는 예비 작업을 수행합니다.

⚠ 경고: 이 기능은 아웃바운드 https 연결에서만 상호 인증을 사용하도록 설정합니다.

키 스토어 생성

인스턴스는 현재 개인 키와 공용 인증서 쌍이 포함된 Java 키 스토어 파일 업로드를 지원하며, 공용 인증서에는 루트 인증서를 포함한 전체 체인이 포함됩니다.

클라이언트 키 스토어를 설정하려면 다음을 수행합니다.

- 신뢰할 수 있는 CA(인증 기관)에서 서명한 인증서가 필요합니다.
- API 엔드포인트 제공자가 키 스토어 생성을 지원할 수 있습니다.

키 스토어를 생성해야 하는 경우 프로세스에는 명령줄 인터페이스 명령을 사용하여 새 키 스토어 파일을 생성하고, CSR(인증서 서명 요청)을 생성하고, 서명된 인증서를 임포트하는 여러 단계가 포함됩니다. 도메인의 기본 인증서를 임포트하기 전에 루트 또는 중간 인증서를 먼저 임포트해야 합니다. 다음은 단계별 지침입니다.

1. Java 키 스토어와 키 페어를 생성합니다.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. 기존 Java 키 스토어에 대한 CSR을 생성합니다.

```
keytool -certreq -alias mydomain -keystore my.keystore -file
 mydomain.csr
```

3. CSR을 CA 서명 기관으로 보내 서명된 인증서와 함께 중간 및 루트 인증서를 포함하는 인증서 파일에 서명하고 반환합니다.
4. 루트 또는 중간 인증 기관 CA 인증서를 기존 Java 키 스토어로 임포트합니다.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore
 my.keystore
```

ⓘ 주: 모든 인증서를 하나의 파일에 묶어서 임포트할 수 있습니다. 이 옵션이 바람직합니다. 이렇게하면 5를 건너 뛸 수 있습니다.

```
keytool -import -alias mydomain -file merged.crt -keystore
 my.keystore
```

5. 서명된 기본 인증서를 기존 Java 키 스토어로 임포트합니다.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt
 -keystore my.keystore
```

키 스토어 설정

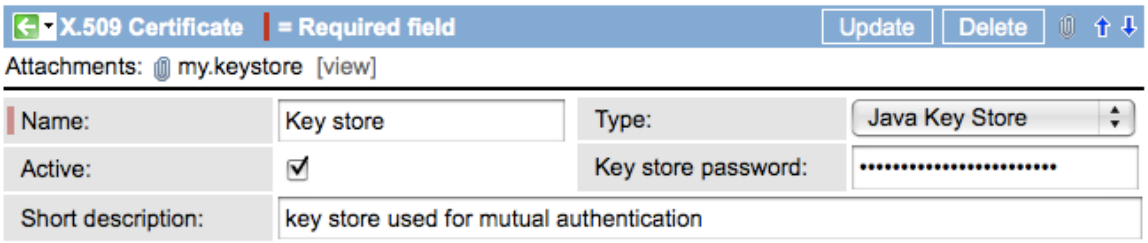
이제 키 스토어가 생성되었으므로 인증서 테이블에 업로드할 수 있습니다. 대상 시스템 정의 > 인증서 페이지에서 새로 만들기를 클릭하고 다음 필드를 설정합니다.

- 인증서 이름을 입력합니다.
- 키 스토어를 활성으로 저장합니다.
- 유형 = **Java** 키 스토어를 설정합니다.
- 키 스토어 암호를 입력합니다. 키 스토어를 작성하는 데 사용된 암호입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

제출을 클릭하여 Java 키 스토어 항목을 만듭니다.

키 스토어



신뢰할 수 있는 서버 인증서 지정

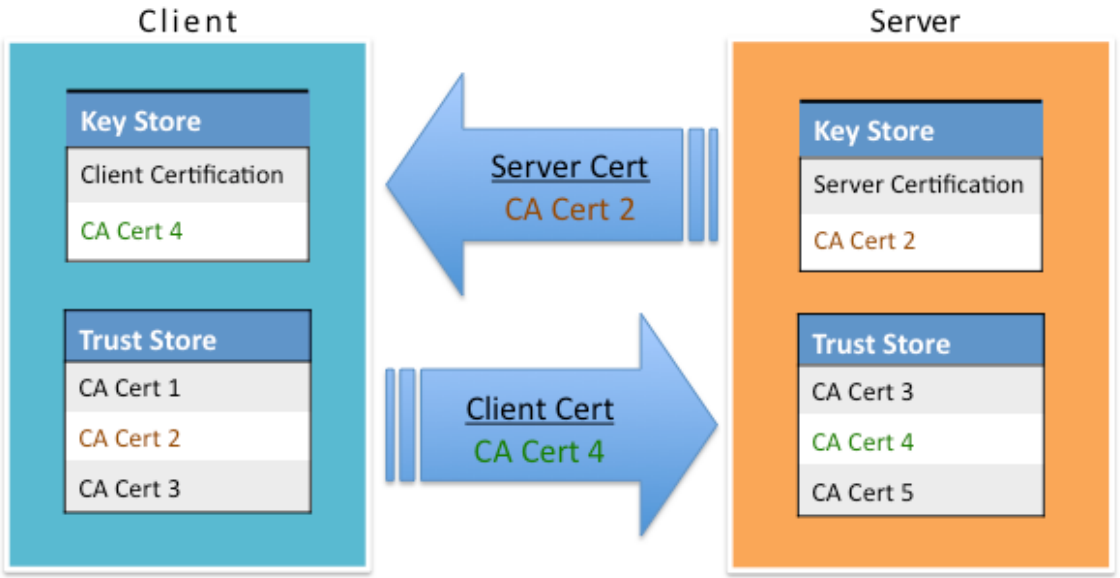
HTTPS 웹 서비스 호출인 아웃바운드 SSL 연결 중에 SSL 연결 중에 서비스 제공자의 유효성을 보장하는 서비스 제공자가 제공하는 인증서를 지정할 수 있습니다. 예를 들어 인증서로 자신을 식별하는 보안 서비스에 연결하려고 시도하는 브라우저가 있습니다.

신뢰할 수 있는 서버 인증서를 ServiceNow 업로드하면 연결 중인 서비스가 유효하고 안전한지 확인할 수 있습니다.

"믿을 수 있는 스토어 인증서" 유형의 새 인증서 항목을 만들고 DER 형식의 인증서를 첨부하거나 PEM 형식을 복사하여 **PEM** 인증서 필드에 붙여넣습니다.

프로토콜 프로파일

인증서 교환



- 클라이언트가 인증을 위해 서버 인증서를 요청하면 인증서 서명 요청(CSR)이 생성됩니다.
- CSR에 응답하기 위해 서버는 두 개의 고유한 암호화 키, 즉 서버에 대한 메시지를 암호화하는 데 사용되는 공개 키와 메시지를 해독하는 데 사용되는 개인 키를 생성합니다. 두 키는 모두 키 스토어에 보관됩니다.
- 키는 서버에서 읽을 수 있도록 클라이언트 보안 메시지의 암호를 해독하는 데 사용됩니다. HTTPS가 될 모든 발신 연결은 키 스토어를 확인하고 공용 인증서를 제공하여 인증을 검증하며, 신뢰 스토어 인증서를 사용하여 상호 신뢰를 다시 확인합니다.
- 클라이언트와 서버 간의 보안 링크를 완료하기 위해 서버는 인증서를 해당 개인 키와 일치시킵니다. 서버만 개인 키에 액세스할 수 있기 때문에 서버는 클라이언트의 데이터를 해독할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음은 포트 443에서 `com.glide.certificates.DBKeyStoreSocketFactory` 소켓 팩토리를 사용하여 MYHTTPS를 등록하는 명령의 예입니다. 데이터베이스 키 저장소 팩토리는 SSL 교환 프로세스 중에 상호 인증을 위한 클라이언트 인증서를 제공하는 데 사용됩니다.

```
glide.httpclient.protocol.myhttps.class =
 "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "443"
```

위의 구성을 사용하면 SSL 중에 사용자 지정 소켓 팩터리 및 교환 인증서를 사용하는 모든 아웃바운드 `myhttps://host.domain.com/target` URL에 영향을 줍니다.

주: 기본 HTTPS 프로토콜 소켓 팩터리를 재정의하면 모든 아웃바운드 HTTPS 연결에 영향을 줍니다. 이것은 일반적으로 바람직하지 않습니다.

서버는 인증서를 전송하여 응답합니다. 클라이언트가 수락하는 인증서입니까? 그렇다면 인증서를 승인하는 서버로 메시지가 전송되고 보안 채널이 시작됩니다. 인증서가 수락되지 않으면 인증을 위해 루트 기관이 필요함을 의미할 수 있습니다.

접근 제어 목록 규칙

접근 제어 목록(ACL)에 대한 규칙은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 액세스를 제한합니다.

탐색	구성
	
ACL에 대해 자세히 알아보십시오.	ACL을 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

참조



상황별 보안 관리자에 대한 상세 정보를 가져옵니다.

고급



고급 ACL에 대해 자세히 알아보십시오.

접근 제어 목록 탐색

접근 제어 목록(ACL)을 탐색합니다.

모든 접근 제어 목록 규칙에는 다음과 같은 사항이 명시되어 있습니다.

- ACL을 정의하는 결정 유형, 규칙 유형 및 작업
- 보호 중인 객체
- 객체에 접근하는 데 필요한 조건

ACL의 구성요소

결정 유형은 조건이 충족될 경우 사용자의 객체 접근을 허용할지 또는 조건이 충족되지 않을 경우 객체 접근을 거부할지 여부를 정의합니다.

결정 유형	설명
거부-미포함	조건이 전달되지 않는 한 접근을 명시적으로 거부하여 자원에 대한 접근을 제한합니다. 자세한 내용은 #unique_1349_Connect_42_section_qnd_snl_zbc 문서를 참조하십시오.
허용-If	조건이 전달되면 자원에 대한 액세스를 허용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

객체는 접근에 대한 제어가 필요한 대상입니다. 각 객체는 특정 테이블, 필드 또는 기록을 고유하게 식별하는 유형과 이름으로 구성됩니다. 적용 대상 필드를 사용하면 사용자가 이 ACL을 적용할 특정 기록을 세부적으로 제어할 수 있습니다.

예를 들어, 이러한 모든 항목은 객체를 지정합니다.

유형	이름	객체 보안
기록	〔인시던트〕. 〔--없음--〕	인시던트 테이블입니다.
기록	〔인시던트〕.〔활성〕	인시던트 테이블의 활성 필드입니다.
기록	[incident] 적용 대상: 우선순위 = P1	인시던트 테이블의 우선순위 1 인시던트만.
REST_Endpoint	user_role_inheritance	user_role_inheritance 스크립트 기반 REST API에 대한 기록입니다.

각 작업은 시스템이 지정된 객체에 대해 수행할 수 있는 유효한 동작을 설명합니다. 기록과 같은 일부 객체는 여러 작업을 지원하지만 REST_Endpoint 등의 다른 객체는 하나의 작업만 지원합니다.

예를 들어, 이러한 모든 항목은 작업을 지정합니다.

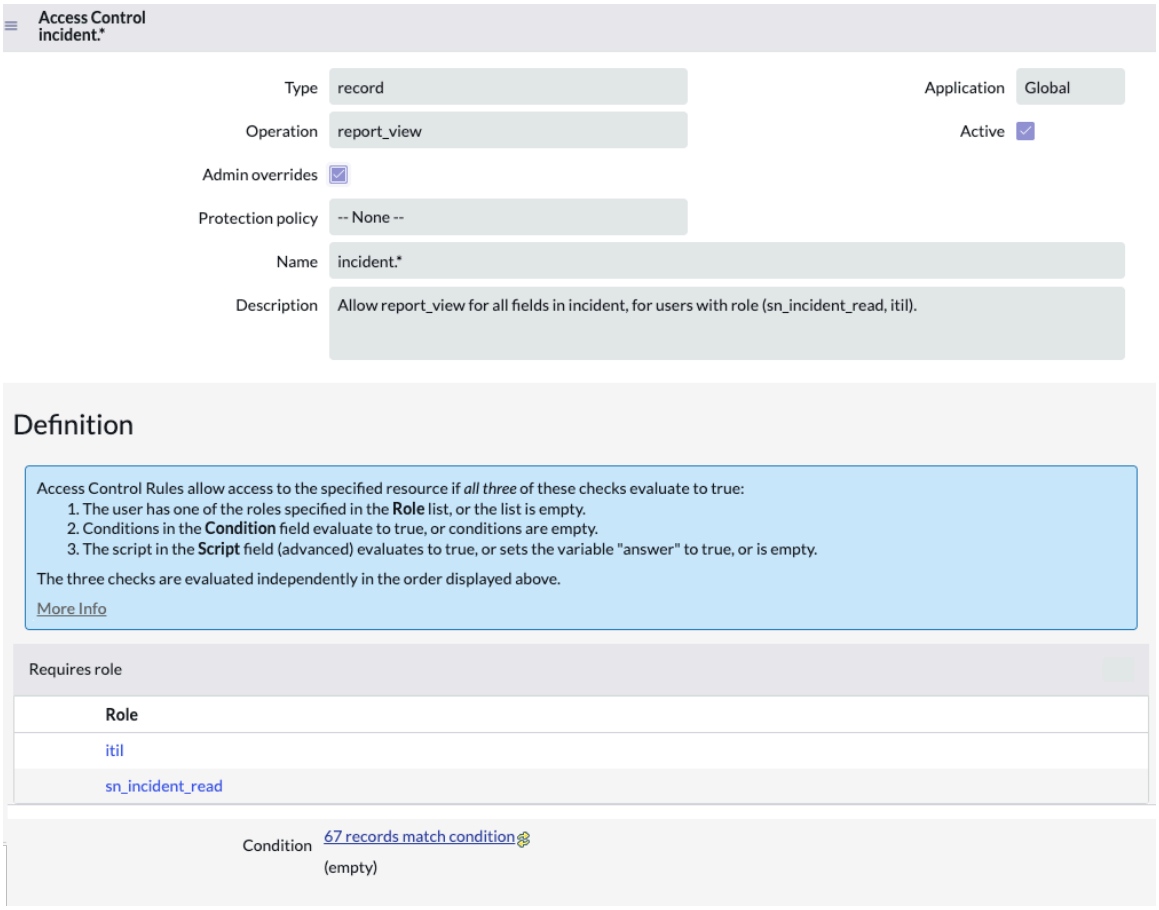
유형	이름	운영	운영 보안
기록	〔인시던트〕. [-- 없음 --]	생성	인시던트 테이블에서 기록을 생성합니다.
기록	〔인시던트〕.〔활성〕	쓰기	인시던트 테이블의 활성 필드를 업데이트합니다.
REST_Endpoint	user_role_inheritance	실행	user_role_inheritance 스크립트 기반 REST API 실행

조건은 누군가가 명명된 객체 및 작업에 접근할 수 있는 시기를 지정합니다. 보안 관리자는 다음을 추가하여 조건 요구 사항을 지정할 수 있습니다.

- 역할 필요 목록에 하나 이상의 사용자 역할.
- 하나 이상의 보안 속성을 true로 평가해야 합니다.
- 하나 이상의 데이터 조건.
- true 또는 false로 평가하거나 `##` 변수를 true 또는 false로 설정하는 스크립트

객체 및 작업에 액세스하려면 사용자는 액세스 제어에 나열된 모든 조건을 통과해야 합니다. 예를 들어, 이 접근 제어는 인시던트 테이블에서 작업을 볼 수 있도록 액세스를 제한합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



인시던트 테이블의 기록을 업데이트하려면 사용자에게 나열된 역할이 있어야 하고 기록이 조건을 충족해야 합니다.

조건 유형	요구 사항	설명
역할 필요	필요한 역할:itil	itil 역할을 가진 사용자만 인시던트를 업데이트할 수 있도록 허용합니다.
보안 속성	UserIsAuthenticated	인증된 사용자만 인시던트를 업데이트할 수 있습니다.
데이터 조건	〔인시던트 상태〕〔일치하지 않음〕〔정기휴일〕	활성 인시던트 기록에 대한 업데이트만 허용합니다.

적용 동작

적용 대상 필드는 ACL이 기록에 적용되는지 여부를 결정하는 반면, 데이터 조건은 이미 적용된 ACL을 평가합니다. 적용 대상 은 ACL이 특정 기록에 영향을 주는지 여부를 지정합니다. 비어 있는 경우 ACL이 모든 기록에 적용됩니다. 적용-대상 은 세분화된 ACL 적용에 사용할 수 있는 반면 "데이터 조건"은 평가 기준입니다.

주: 적용-대상 은 대/소문자를 구분합니다.

기본적으로 거부 동작

기본적으로 ACL 엔진은 ACL이 비어 있거나 유효하지 않은 경우 액세스를 완전히 거부합니다. 빈 ACL은 다음 구성 요소 중 하나 이상이 없는 ACL로 정의됩니다.

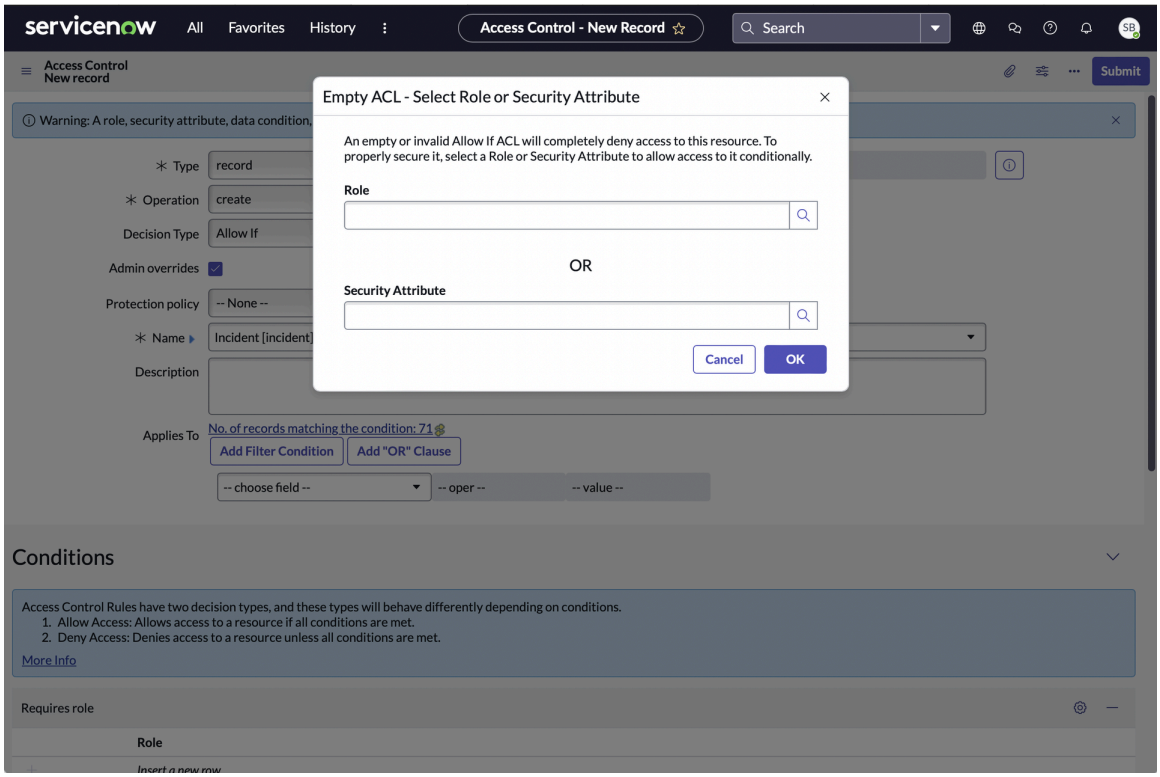
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 정의된 역할
- 보안 속성
- 데이터 조건
- 스크립트

잘못된 ACL은 다음과 같이 정의합니다.

- 존재하지 않는 역할이 있는(예: 데이터베이스에 행이 없는 경우) ACL
- 존재하지 않는 보안 속성이 있는(예: 데이터베이스에 행이 없는 ACL)
- "answer=true" 또는 "true"가 포함된 스크립트가 있는 ACL

시스템이 ACL을 만드는 사용자를 탐지하면 사용자에게 역할 또는 기존 보안 속성을 선택하라는 메시지를 표시합니다.



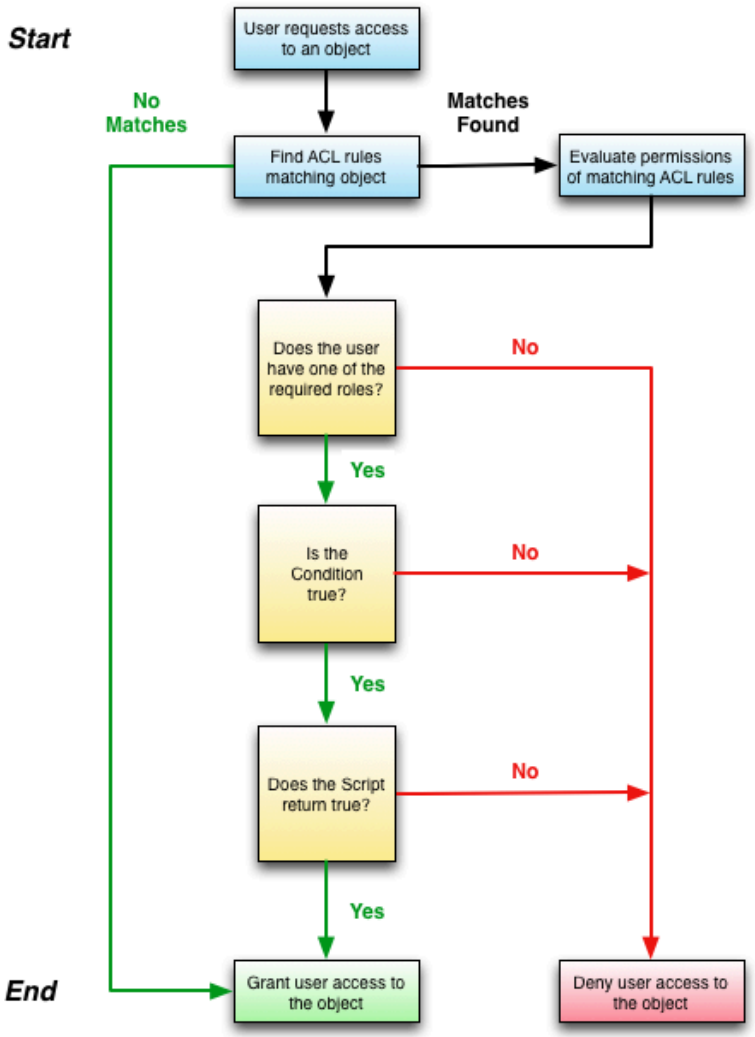
ACL 평가 프로세스

ACL 규칙은 사용자가 일치하는 ACL 규칙에 필요한 모든 조건을 충족하는 경우에만 객체에 대한 사용자 액세스 권한을 부여합니다.

- 조건은 *true*로 평가되어야 합니다.
- 스크립트는 *true* 로 평가하거나 *true* 값을 가진 응답 변수를 반환해야 합니다.
- 사용자에게 필수 역할 목록에 있는 역할 중 하나가 있어야 합니다. 목록이 비어 있으면 이 조건은 *true*로 평가됩니다.
- 〔기록 ACL 규칙만〕 일치하는 테이블 수준 및 필드 수준 ACL 규칙은 모두 *true*로 평가되어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ACL 평가 조건



하나의 세션이 데이터를 요청할 때마다 시스템은 요청된 객체 및 운영과 일치하는 접근 제어 규칙을 검색합니다. 일치하는 접근 제어 규칙이 있는 경우 시스템은 사용자가 해당 객체 및 운영에 접근하는 데 필요한 조건을 갖추고 있는지 평가합니다. 접근 제어 규칙이 둘 이상의 조건을 지정할 경우, 사용자는 객체 및 운영에 접근하기 위한 모든 조건을 충족해야 합니다. 한 가지 조건 검사를 통과하지 못할 경우, 사용자는 일치하는 객체 및 운영에 접근할 수 없습니다.

사용자가 첫 번째로 일치하는 규칙의 조건을 충족하지 않을 경우, 시스템은 접근 제어 처리 순서에 따라 지정된 바와 같이 그 다음으로 일치하는 접근 제어 규칙의 조건을 평가합니다. 사용자가 일치하는 접근 제어 규칙의 조건을 충족하지 못하면 시스템은 요청된 객체 및 운영에 대한 접근을 거부합니다.

주: 요청된 객체 및 작업에 대해 일치하는 접근 제어 규칙이 없는 경우 시스템은 사용자에게 액세스 권한을 부여합니다. 실제로 시스템에는 모든 기록 작업을 보호하는 기본 접근 제어 규칙 세트가 있기 때문에 시스템에서 일치하는 규칙을 찾지 못하는 경우는 드뭅니다.

개체에 대한 액세스가 거부되는 결과는 사용자가 실패한 ACL 규칙에 따라 달라집니다. 예를 들어, 읽기 작업 ACL 규칙에 실패하면 사용자가 객체를 볼 수 없습니다. ACL 규칙은 보안된 객체에 따라 양식의 필드와 목록에서 행을 숨기거나 사용자가 UI 페이지에 액세스하지 못하도록 합니다. 다음 테이블에는 지정된 작업 및 객체 유형에 대한 ACL 규칙 실패 결과의 전체 목록이 포함되어 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

사전 및 사후 쿼리 **ACL** 검사

인스턴스는 사용자가 쿼리를 하기 전과 후에 ACL 규칙을 확인합니다. 쿼리 전후에 서로 다른 정보를 사용할 수 있으므로 결과가 다를 수 있습니다.

사전 쿼리 ACL 검사

인스턴스가 데이터베이스 쿼리를 실행하기 전에 쿼리된 테이블의 각 필드에 대한 ACL 규칙을 검사하여 사용자가 액세스할 수 있는 필드를 결정합니다. 이 검사는 사용자의 역할만 확인하고 이러한 역할이 필드에 대한 액세스를 허용하는지 확인합니다. 이 검사는 쿼리 전에 실행되므로 ACL은 테이블의 기록에 액세스할 수 없으므로 해당 데이터를 고려할 수 없습니다. 기록의 내용을 알고 있어야 하는 스크립트와 조건은 평가되지 않습니다.

이 시점에서 사용자에게 읽기 액세스 권한이 없는 경우 필드 값이 사용자에게 표시되지 않습니다.

쿼리 후 ACL 검사

쿼리 후 인스턴스는 쿼리에서 반환된 각 레코드를 확인합니다. 이 검사 중에 ACL에 대한 컨텍스트가 있으므로 ACL의 역할, 조건 및 스크립트 부분이 평가됩니다. 이 시점에서 사용자에게 읽기 액세스 권한이 없는 경우 필드 값이 사용자에게 표시되지 않지만 자신의 역할이 필드에 대한 액세스를 허용하는 경우 사용자에게 필드 레이블이 표시됩니다.

운영	객체에 대한 **ACL** 규칙 실패의 결과
실행	사용자는 기록 또는 UI 페이지에서 스크립트를 실행할 수 없습니다.
생성	사용자는 양식에서 새 UI 작업을 볼 수 없습니다. 또한 사용자는 웹 서비스와 같은 API 프로토콜을 사용하여 테이블에 기록을 삽입할 수 없습니다. 필드에 특정 값을 포함해야 한다는 조건을 가진 **ACL** 생성 은 false로 평가될 수 있습니다. 새 기록의 필드는 기록이 저장될 때까지 비어 있는 것으로 간주됩니다.
읽음	사용자는 양식이나 목록에서 객체를 볼 수 없습니다. 또한 사용자는 웹 서비스와 같은 API 프로토콜을 사용하여 레코드를 검색할 수 없습니다.
쓰기	사용자는 양식 및 목록에서 읽기 전용 필드를 볼 수 있으며 웹 서비스와 같은 API 프로토콜을 사용하여 기록을 업데이트할 수 없습니다.
삭제	사용자는 양식에서 **UI** 삭제 작업을 볼 수 없습니다. 또한 사용자는 웹 서비스와 같은 API 프로토콜을 사용하여 테이블에서 기록을 제거할 수 없습니다.
edit_task_relations	사용자는 작업 테이블 간의 관계를 정의할 수 없습니다.
edit_ci_relations	사용자는 구성 항목 [cmdb_ci] 테이블 간의 관계를 정의할 수 없습니다.
save_as_template	템플릿을 생성할 때 저장해야 하는 필드를 제어하는 데 사용됩니다.
add_to_list	사용자는 정비사 목록의 특정 열을 보거나 개인화할 수 없습니다.
list_edit	사용자는 목록에서 기록(행)을 업데이트할 수 없습니다.
report_on	사용자는 ACL 테이블에서 보고서를 생성할 수 없습니다. 자세한 내용은 ACL 규칙으로 보고서 생성 제한을 참조하십시오.
report_view	사용자는 ACL 테이블이나 ACL 필드에서 보고서 내용을 볼 수 없습니다. 자세한 내용은 Reporting 문서를 참조하십시오.
personalize_choices	사용자는 목록 필드를 마우스 오른쪽 단추로 클릭하고 선택 사항 구성을 선택할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

객체에 대한 **ACL** 일치 요구 사항

객체 유형	객체에 접근하는 데 필요한 일치 **ACL** 규칙	기존 와일드카드 **ACL** 규칙
클라이언트 호출 가능 스크립트 포함 프로세서	사용자는 다음 두 가지 ACL 규칙의 조건을 충족해야 합니다. **1.** 객체에 대한 모든 와일드카드 ACL 규칙(작업에 대한 ACL 규칙이 있는 경우). **2.** 객체의 이름과 일치하는 첫 번째 ACL 규칙(운영에 대한 ACL 규칙이 있는 경우).	기본적으로 이러한 객체 유형에 대한 와일드카드(*) 규칙은 없습니다. 이러한 개체 중 하나에 대해 와일드카드 ACL 규칙을 만들면 이 유형의 모든 개체에 ACL 규칙이 적용됩니다.
UI 페이지 기록	사용자는 다음 두 가지 ACL 규칙의 조건을 충족해야 합니다. **1.** 기록의 필드와 일치하는 첫 번째 ACL 규칙(운영에 대한 ACL 규칙이 존재하는 경우). **2.** 기록의 테이블과 일치하는 첫 번째 ACL 규칙(운영에 대한 ACL 규칙이 존재하는 경우).	기본적으로 생성, 읽기, 쓰기 및 삭제 작업에 대한 와일드카드 테이블 규칙(*)과 personalize_choices, 생성 및 save_as_template 작업에 대한 와일드카드 필드 규칙(*.*)이 있습니다. 제공된 와일드카드 ACL 규칙을 사용하지 않고 테이블을 생성할 때 테이블에 대한 ACL 규칙을 생성합니다.

주: 보안 관리자 기본 동작(*glide.sm.default_mode*) 속성은 사용자가 와일드카드 테이블 ACL 규칙에 대해서만 일치하는 객체에 액세스할 수 있는지 여부를 결정합니다. 이 속성이 접근 거부로 설정되면 관리자만 와일드카드 테이블 ACL 규칙과 일치하는 객체에 액세스할 수 있습니다.

주: 만들기 작업에 대한 와일드카드 필드 ACL 규칙(*.*)은 쓰기 작업과 동일한 조건을 다시 사용합니다. 즉, 명시적 생성 작업 ACL 규칙을 정의하지 않는 한 생성 조건은 쓰기 조건과 동일합니다.

처리 순서에서 동일한 지점에 있는 여러 **ACL** 규칙

처리 순서에서 두 개 이상의 규칙이 동일한 지점에서 일치하는 경우 사용자는 ACL 규칙 조건 중 하나를 통과해야 객체에 액세스할 수 있습니다. 예를 들어, 에 대해 *incident.number*두 개의 필드 ACL 규칙을 만드는 경우 한 규칙을 통과한 사용자는 처리 순서의 동일한 지점에서 다른 필드 ACL 규칙을 실패했는지 여부에 관계없이 번호 필드에 액세스할 수 있습니다.

필요한 역할

일반 관리자 사용자는 접근 제어 규칙을 보고 디버그할 수 있습니다. 그러나 기존 접근 제어 규칙을 만들거나 업데이트하려면 관리자가 security_admin 역할에 대한 권한을 상승시켜야 합니다. 지침은 권한 있는 역할로 상승 문서를 참조하십시오.

범위가 지정된 애플리케이션의 **ACL** 규칙

ACL 규칙과 동일한 범위에 있는 객체에 대해 ACL 규칙을 만들 수 있습니다. ACL 규칙과 동일한 범위에 있는 필드가 하나 이상 있는 테이블에 대한 ACL 규칙을 생성할 수도 있습니다.

ACL 규칙 기록과 범위가 다른 테이블의 경우에는 규칙 유형이 제한됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- ACL 규칙과 동일한 범위에 있는 모든 테이블, UI 페이지 또는 기타 객체에 대해 ACL 규칙을 만들 수 있습니다.
- ACL 규칙과 동일한 범위에 있는 필드에 대한 ACL을 만들 수 있습니다.
  - 테이블이 동일한 범위에 있으면 스크립트를 사용하여 조건을 평가할 수 있습니다.
  - 테이블이 다른 범위에 있으면 스크립트를 사용하여 조건을 평가할 수 없습니다.
- 다른 범위의 ACL에 역할을 추가하는 것을 포함하여 애플리케이션 선택기에서 선택한 애플리케이션과 다른 범위에 있는 객체에 대해서는 ACL 규칙을 생성하거나 수정할 수 없습니다.
- 전역 범위에서만 와일드카드 테이블 규칙(*)을 생성할 수 있습니다.
- ACL 규칙과 동일한 범위에 있는 테이블에 대해서만 와일드카드 필드 규칙(*)을 생성할 수 있습니다.

ACL 규칙 유형

시스템의 다양한 구성요소에 ACL 규칙을 생성합니다.

기록 ACL 규칙

기록 ACL 규칙은 테이블 및 필드 이름으로 구성됩니다.

- 테이블 이름은 보호하려는 테이블입니다. 이 테이블에서 다른 테이블이 확장되면 해당 테이블은 상위 테이블로 간주됩니다. 상위 테이블에 대한 ACL 규칙은 상위 테이블을 확장하는 모든 테이블에 적용됩니다.
- 필드 이름은 보호하려는 필드입니다. 테이블 확장으로 인해 일부 필드가 여러 테이블의 일부입니다. 상위 테이블의 필드에 대한 ACL 규칙은 상위 테이블을 확장하는 모든 테이블에 적용됩니다.

ACL 규칙은 다음 기록 작업에 보안을 유지할 수 있습니다.

운영	설명
생성	사용자가 테이블에 새 기록(행)을 삽입할 수 있습니다.
읽음	사용자가 테이블의 기록을 표시할 수 있습니다.
쓰기	사용자가 테이블의 기록을 업데이트할 수 있습니다.
삭제	사용자가 테이블에서 기록을 제거하거나 테이블을 삭제할 수 있습니다.
edit_task_relations	사용자가 작업 [task] 테이블을 확장할 수 있습니다.
edit_ci_relations	사용자가 구성 항목 [cmdb_ci] 테이블을 확장할 수 있습니다.
save_as_template	사용자가 기록을 템플릿으로 저장할 수 있습니다.
add_to_list	사용자가 목록 정비사의 특정 열을 보거나 개인화하지 못하도록 합니다. 주: 조건 및 스크립트는 지원되지 않습니다.
list_edit	사용자가 목록에서 기록(행)을 업데이트할 수 있습니다.
report_on	사용자가 테이블에 대해 보고할 수 있습니다.
report_view	사용자가 필드 ACL에 대해 보고할 수 있습니다.
personalize_choices	사용자가 테이블 또는 필드를 구성할 수 있습니다.
query_exact	사용자가 일치 쿼리("is", "is not", "is empty" 등)를 제출할 수 있도록 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

운영	설명
query_range	사용자가 범위 쿼리("starts with", "ends with", "contains" 등)를 제출할 수 있으며 정렬이 제한되지 않습니다.

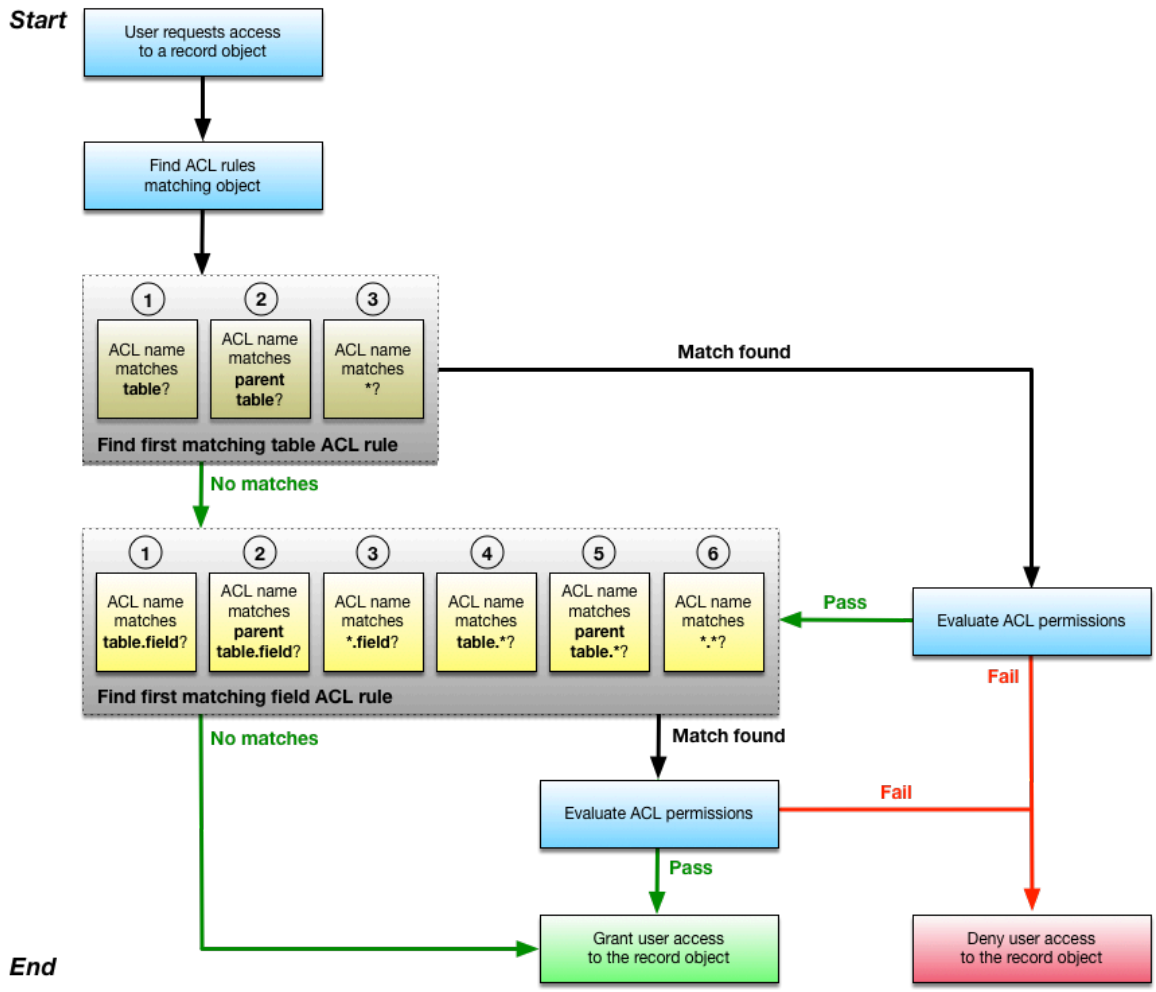
기록 ACL 규칙은 다음 순서로 처리됩니다.

- 테이블 ACL 규칙에 대해 객체를 일치시킵니다.
- 필드 ACL 규칙에 대해 객체를 일치시킵니다.

이러한 처리 순서를 따르면 사용자는 보다 일반적인 객체에 접근하기 전에 보다 구체적인 객체에 접근할 수 있습니다. 하나의 기록 객체에 접근하려면 테이블 및 필드 ACL 규칙을 모두 통과해야 합니다.

- 테이블 ACL 규칙을 통과하지 못할 경우, 필드 ACL 규칙을 통과하더라도 테이블의 모든 필드에 대한 접근이 거부됩니다.
- 테이블 ACL 규칙을 통과했지만 필드 ACL 규칙을 통과하지 못할 경우, 사용자는 필드 ACL 규칙에 따라 설명된 필드에 접근할 수 없습니다.

ACL 일치



프로세서 ACL 규칙

프로세서 ACL 규칙은 보안할 프로세서를 지정합니다. 사용 가능한 프로세서 목록을 보려면 다음으로 이동하십시오. 시스템 정의 > 프로세서.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본적으로 EmailClientProcessor에 대한 ACL 규칙이 포함되어 이메일 클라이언트를 itil 역할을 가진 사용자로 제한합니다.

프로세서 ACL 규칙은 해당 자원에 대한 보다 구체적인 ACL을 찾을 수 없는 경우 STAR(*) 규칙을 따릅니다.

테이블 **ACL** 규칙

사용자는 먼저 테이블 ACL 규칙을 통과해야 합니다. 기본 시스템에는 모든 테이블과 일치하는 STAR(*) 테이블 ACL 규칙이 포함되어 있으므로 사용자는 항상 하나 이상의 테이블 ACL 규칙을 통과해야 합니다. 기본 시스템에서는 특정 테이블에 대한 접근을 제어하는 추가 테이블 ACL 규칙을 제공합니다.

테이블 ACL 규칙은 다음 순서로 처리됩니다.

1. 테이블 이름과 일치합니다. 예: 인시던트.
2. 상위 테이블 이름과 일치합니다. 예: 작업
3. 임의의 테이블 이름(*)과 일치합니다. 예를 들어*.

사용자가 모든 테이블 ACL 규칙을 통과하지 못할 경우, 사용자는 테이블의 모든 필드에 접근할 수 없습니다. 사용자가 테이블 ACL 규칙을 통과하면 시스템은 필드 ACL 규칙을 평가합니다.

필드 **ACL** 규칙

사용자가 테이블 ACL 규칙을 통과하면 필드 ACL 규칙은 다음 순서로 처리됩니다.

1. 테이블 및 필드 이름을 일치시킵니다. 예: incident.number
2. 상위 테이블과 필드 이름을 일치시킵니다. 예: task.number
3. 테이블(*)과 필드 이름을 일치시킵니다. 예: *.number.
4. 테이블과 임의의 필드(*)를 일치시킵니다. 예: incident.*.
5. 상위 테이블과 모든 필드(*)를 일치시킵니다. 예: task.*.
6. 모든 테이블(*) 및 모든 필드(*)를 일치시킵니다. 예를 들어*.*.

사용자는 테이블 ACL 규칙을 통과해야 테이블의 필드에 대한 액세스 권한을 부여받을 수 있습니다. 예를 들어 인시던트 테이블의 번호 필드에 액세스하려면 먼저 인시던트 테이블의 테이블 ACL 규칙을 통과해야 합니다.

첫 번째 성공한 필드 ACL 평가는 필드 수준에서 ACL 규칙 처리를 중지합니다. 사용자가 필드 ACL 규칙을 전달하면 시스템은 일치하는 다른 필드 ACL 규칙에 대한 검색을 중지합니다. 예를 들어 사용자가 incident.number에 대한 필드 ACL 규칙을 통과하면 시스템은 인시던트 테이블의 번호 필드를 보호하는 다른 ACL 규칙 검색을 중지합니다.

보호된 필드에는 유추된 데이터의 쿼리 정보에 대한 액세스가 제한되어 예측 정보가 반환되지 않습니다.

UI 페이지 **ACL** 규칙

UI 페이지 ACL 규칙은 보안할 UI 페이지를 지정합니다. 사용 가능한 UI 페이지 목록을 보려면 다음으로 이동하십시오. 시스템 **UI** > **UI** 페이지. UI 페이지의 ACL 규칙을 정의할 때는 전체 범위의 페이지 이름을 사용합니다. 예: **x_myapp_mypage**.

주: **ui_page** 유형 ACL의 이름 필드에 STAR(*) 문자를 사용하여 모든 UI 페이지와 일치시킬 수 있습니다.

UI 페이지 ACL 규칙은 해당 자원에 대한 보다 구체적인 ACL을 찾을 수 없는 경우 STAR(*) 규칙을 따릅니다. 예를 들어 `mysecretpage` 라는 UI 페이지가 있지만 이 UI 페이지에 대한 ACL을 정의하지 않은 경우 UI 페이지 프로세서에 대한 STAR(*) 규칙이 액세스 검사에 사용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ACL 규칙은 다음 UI 페이지 작업을 보호할 수 있습니다.

운영	설명
읽음	사용자가 UI 페이지를 표시할 수 있습니다.

클라이언트 호출 가능 스크립트 포함 **ACL** 규칙

스크립트 포함 ACL 규칙은 보안을 유지할 클라이언트 호출 가능 스크립트 포함을 지정합니다. 사용 가능한 스크립트 포함 목록을 보려면 다음으로 이동하십시오. 시스템 정의 > 스크립트 포함. 클라이언트 호출 가능 열을 표시하도록 목록을 개인화할 수 있습니다.

기본 시스템에는 클라이언트 호출 가능 스크립트 포함에 대한 ACL 규칙이 포함되어 있지 않습니다.

클라이언트 호출 가능 스크립트 포함 ACL 규칙은 해당 자원에 대한 보다 구체적인 ACL을 찾을 수 없는 경우 STAR(*) 규칙을 따릅니다.

기능 필드의 **ACL** 통제

함수 필드에 대한 액세스를 평가할 때 시스템은 함수 필드 자체에 대한 액세스를 확인하는 것 외에도 함수의 기여 필드에 대한 액세스도 확인합니다. 기여 필드는 지정된 기능 정의에서 인수로 사용되는 필드입니다.

함수 필드에 대한 자세한 내용은 함수 필드를 참조하십시오.

이전 버전에서 Rome 시스템은 단순히 함수 필드 자체에 대한 액세스를 확인합니다(다른 필드와 마찬가지로). 해당 필드의 ACL이 액세스를 허용하는 경우, 사용자는 기여 필드에 대한 액세스 권한이 있는지 여부에 관계없이 결과 값을 받습니다.

또한 Yokohama 시스템 및 그 이후에는 함수 필드에 대한 액세스를 허용하기 위해 모든 기여 필드에 대한 액세스 권한이 필요합니다. 하나 이상의 기여 필드 ACL이 액세스를 거부하는 경우 함수 필드도 액세스를 거부합니다.

새 요구 사항의 영향을 받는 유일한 작업은 읽기 및 report_view입니다. Report_view에는 자체 추가 요구 사항이 있습니다.

운영	설명
읽기 작업	사용자는 다음 두 가지 모두에 해당하는 경우에만 함수 필드에 대한 읽기 권한을 갖습니다. • 사용자에게 함수 필드에 대한 읽기 권한이 있습니다. • 사용자에게 기능에 사용되는 모든 기여 필드에 대한 읽기 권한이 있습니다.
report_view 작업	사용자는 다음 report_view 모두 참일 경우에만 함수 필드에 액세스할 수 있습니다. • 사용자에게 함수 필드에 대한 report_view 액세스 권한이 있습니다. • 사용자는 각 기여 필드에 액세스할 report_view 있습니다. • 조건이나 스크립트가 없는 역할 전용 읽기 ACL이 있으며 사용자가 해당 역할을 갖습니다. • 사용자는 기여 필드에 대한 읽기 권한만 역할 수행하므로 조건 또는 스크립트가 없는 ACL만 허용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

예제

주어진:

- 테이블: 급여
- 열: base, bonus, total(이 예에서는 모두 정수임)
- 함수 필드: 전체 열은 `## ## glidefunction:add(base, bonus)`와 함께 함수 필드로 표시됩니다.
- 기여 필드: 기본 및 보너스(함수 정의에 사용되기 때문)
- 역할: salary_admin, bonus_admin

예시 **1:** 모든 필드에 접근이 허용됨

ACL	결과
합계, 기본, 보너스: 조건이나 스크립트 없이 역할 salary_admin에 대한 읽기 및 report_view	salary_admin 역할이 있는 사용자에게는 필요한 역할이 있으므로 합계에 대한 읽기 및 report_view 권한이 부여됩니다.

예제 **2:** 기여 필드가 읽기 액세스를 거부함

ACL	결과
• 합계, 기본: 조건 또는 스크립트 없이 역할 salary_admin에 대한 읽기 및 report_view • 보너스: 조건이나 스크립트가 없는 역할 salary_admin에 대한 report_view • 보너스: 조건이나 스크립트 없이 역할 bonus_admin 읽기	보너스가 해당 역할에 대한 읽기 권한을 거부하기 때문에 salary_admin 역할을 가진 사용자는 합계에 대한 읽기 및 report_view 액세스가 거부됩니다.

예시 **3:** 기여 필드 ACL에 스크립트가 있음

ACL	결과
• 합계, 기본: 조건 또는 스크립트 없이 역할 salary_admin에 대한 읽기 및 report_view • 보너스: 조건이나 스크립트가 없는 역할 bonus_admin 대한 report_view • 보너스: 스크립트와 함께 역할 salary_admin 읽기(스크립트에 무엇이 있는지는 중요하지 않으며 거기에 있다는 것만 유의하십시오)	salary_admin 역할을 가진 사용자에게는 모든 필드에 필요한 역할이 있으므로 합계에 대한 읽기 권한이 부여됩니다. 그러나 salary_admin 있는 동일한 사용자는 필요한 역할이 있더라도 이 경우 스크립트가 있는 읽기 ACL이 기본적으로 액세스를 거부하기 때문에 액세스가 거부됩니다report_view.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 점프 시작 - ACL 규칙 플러그인

보안 점프 시작 접근 제어 수준(ACL 규칙) 플러그인은 모든 새 인스턴스에 자동으로 설치됩니다. 이 플러그인을 사용하여 여러 시스템 테이블을 빠르게 보호하고 조직의 프로덕션 시작 프로세스를 신속하게 처리할 수 있습니다.

프로덕션 환경에서 이미 사용 중인 테이블에 대한 보안 액세스를 변경할 수 있으므로 이 플러그인은 기존 인스턴스를 위한 것이 아닙니다. 관리자가 기존 인스턴스에 이 플러그인을 설치하려는 경우 먼저 테스트 인스턴스에서 철저히 테스트해야 합니다. 이렇게 하면 조직의 현재 구현과의 호환성을 확인하는 데 도움이 됩니다.

관리자가 이 플러그인에서 제공하는 새 ACL 규칙에 관심이 있는 경우 ACL 목록을 지침으로 사용하여 기존 인스턴스에 하나 이상을 수동으로 생성할 수 있습니다.

이 플러그인에는 다음 ACL이 포함되어 있습니다. 헤더 행에서 아이콘을 선택하여 열을 오름차순 또는 내림차순으로 정렬합니다. 운영 키는 다음과 같습니다.

- R=읽기
- W=쓰기
- D=삭제
- C=작성

이름	운영	설명
cmdb_ci	WCD	구성 항목 기록을 쓰기/생성/삭제하는 데 필요한 asset 또는 itil 역할
cmn_department	백색 왜성	부서 기록을 쓰고 삭제하는 데 필요한 user_admin 역할
cmn_location	화장실	위치 기록을 쓰고 생성하는 데 필요한 user_admin 역할
core_company	백색 왜성	회사 기록을 쓰고 삭제하는 데 필요한 user_admin 역할
kb_knowledge	생성	지식 기록을 작성하는 데 필요한 지식 역할
ldap_ou_config	RWCD	LDAP OU 정의 기록을 읽기/쓰기/생성/삭제하는 데 필요한 user_admin 역할
ldap_server_config	RWCD	LDAP 서버 기록 읽기/쓰기/작성/삭제에 필요한 user_admin 역할
process_guide	WCD	프로세스 가이드 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
process_step	WCD	프로세스 단계 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sc_category	생성	서비스 카탈로그 범주 기록을 만드는 데 필요한 catalog_admin 역할
sc_category	삭제	서비스 카탈로그 범주 기록을 삭제하는 데 필요한 catalog_admin 역할
sc_category	쓰기	서비스 카탈로그 범주 기록에 쓰는 데 필요한 catalog_admin 역할
sc_cat_item	쓰기	카탈로그 항목 기록에 쓰는 데 필요한 catalog_admin 역할

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	운영	설명
sc_cat_item	삭제	카탈로그 항목 기록을 삭제하는 데 필요한 catalog_admin 역할
sc_cat_item	생성	카탈로그 항목 기록을 만드는 데 필요한 catalog_admin 역할
sysevent_email_action	읽음	모든 사용자는 이메일 알림 기록을 읽을 수 있습니다(구독 목적인).
sysevent_register	RWCD	이벤트 레지스트리 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자 역할
sysevent_script_action	RWCD	스크립트 작업 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자 역할
Syslog	RWCD	로그 항목 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자
sysrule	RWCD	규칙 기록(이메일 알림, 인바운드 이메일 작업, 승인 규칙 등)을 읽기/쓰기/생성/삭제하는 데 필요한 관리자
sysrule	읽음	모든 사용자가 (구독 기반 알림)에 대한 이메일 알림 기록을 읽을 수 있습니다.
sys_app_application	WCD	애플리케이션 기록을 쓰기/생성/삭제하는 데 필요한 관리자
sys_app_category	WCD	애플리케이션 범주 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_app_module	WCD	모듈 기록을 쓰기/생성/삭제하는 데 필요한 관리자
sys_audit	RWCD	감사 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자
sys_dictionary	RWC	딕셔너리 기록을 읽기/쓰기/작성하는 데 필요한 personalize_dictionary 역할
sys_dictionary.*	읽음	personalize_dictionary 역할이 읽을 수 있음 딕셔너리 필드
sys_documentation	삭제	필드 레이블 기록을 삭제하는 데 필요한 personalize_dictionary 역할
sys_documentation	생성	필드 레이블 기록을 만드는 데 필요한 personalize_dictionary 역할
sys_documentation	쓰기	필드 레이블 기록에 쓰는 데 필요한 personalize_dictionary 역할
sys_gauge	RWCD	게이지 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_gauge_count	RWCD	게이지 카운트 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_group_has_role	읽음	그룹 역할 기록을 보는 데 필요한 itil 역할
sys_home	WCD	시작 페이지 섹션 기록을 쓰기/작성/삭제하는 데 필요한 itil_admin 역할
sys_installation_exit	WCD	설치 종료 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	운영	설명
sys_job	WCD	시스템 작업 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_nav_link	WCD	탐색 링크 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_perspective	WCD	메뉴 목록 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_portal	RWCD	포털 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_portal_page	RWCD	홈페이지 기록을 읽기/쓰기/작성/삭제하는 데 필요한 관리자 역할
sys_portal_preferences	RWCD	포털 기본 설정 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_processor	화장실	프로세서 기록을 쓰고 만드는 데 필요한 관리자 역할
sys_properties	화장실	시스템 속성 기록을 쓰고 생성하는 데 필요한 관리자 역할
sys_properties_category	WCD	속성 범주 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_report	삭제	보고서 기록을 삭제할 수 있는 역할(보고서 UI를 통한 삭제를 제한하지 않음)
sys_report	쓰기	보고서 기록에 쓸 수 있는 역할(보고서 UI를 통한 편집을 제한하지 않음)
sys_report	읽음	사용자는 자체 보고서 기록, 그룹의 기록 및 전역 기록(보고서 UI를 통한 보기와 관계 없음)을 읽을 수 있습니다.
sys_report	읽음	보고서 기록을 읽을 수 있는 역할(보고서 UI를 통한 보기를 제한하지 않음)
sys_reportroles	읽음	보고서 역할 기록을 읽는 데 필요한 관리자 역할
sys_script	WCD	비즈니스 규칙 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_script_ajax	WCD	AJAX 스크립트 기록을 쓰기/작성/삭제하는 데 필요한 관리자 역할
sys_script_client	WCD	클라이언트 스크립트 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_script_include	WCD	스크립트 포함 기록을 쓰기/생성/삭제하는 데 필요한 관리자 역할
sys_security_acl	쓰기	접근 제어 기록에 쓰는 데 필요한 관리자 역할
sys_security_acl_role	생성	접근 역할 기록을 만드는 데 필요한 관리자 역할
sys_security_acl_role	삭제	접근 역할 기록을 삭제하는 데 필요한 관리자 역할
sys_security_acl_role	쓰기	액세스 역할 기록에 쓰는 데 필요한 관리자 역할
sys_security_operation	삭제	보안 운영 기록을 삭제하는 데 필요한 관리자 역할
sys_security_operation	생성	보안 운영 기록을 생성하는 데 필요한 관리자 역할

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	운영	설명
sys_security_operation	쓰기	보안 운영 기록에 쓰는 데 필요한 관리자 역할
sys_security_operation	query_range	
sys_security_operation		
sys_security_type	쓰기	보안 유형 기록에 쓰는 데 필요한 관리자 역할
sys_security_type	생성	보안 유형 기록을 만드는 데 필요한 관리자 역할
sys_security_type	삭제	보안 유형 기록을 삭제하는 데 필요한 관리자 역할
sys_status	생성	시스템 상태 기록을 만드는 데 필요한 관리자 역할
sys_status	삭제	시스템 상태 기록을 삭제하는 데 필요한 관리자 역할
sys_status	쓰기	시스템 상태 기록에 쓰는 데 필요한 관리자 역할
sys_template	쓰기	템플릿 기록에 쓰는 데 필요한 template_editor 역할
sys_template	생성	템플릿 기록을 만드는 데 필요한 emplate_editor 역할
sys_template	삭제	템플릿 기록을 삭제하는 데 필요한 template_editor 역할
sys_template	읽음	템플릿 역할 기록을 읽는 데 필요한 template_editor 역할
sys_ui_action	생성	UI 작업 기록을 만드는 데 필요한 관리자 역할
sys_ui_action	삭제	UI 작업 기록을 삭제하는 데 필요한 관리자 역할
sys_ui_action	쓰기	UI 작업 기록에 쓰는 데 필요한 관리자 역할
sys_ui_action_view	쓰기	UI 뷰 작업 기록에 쓰는 데 필요한 관리자 역할
sys_ui_action_view	생성	UI 뷰 작업 기록을 만드는 데 필요한 관리자 역할
sys_ui_action_view	삭제	UI 뷰 작업 기록을 삭제하는 데 필요한 관리자 역할
sys_ui_policy	생성	UI 정책 기록을 만드는 데 필요한 관리자 역할
sys_ui_policy	삭제	UI 정책 기록을 삭제하는 데 필요한 관리자 역할
sys_ui_policy	쓰기	UI 정책 기록에 쓰는 데 필요한 관리자 역할
sys_ui_policy_action	생성	UI 정책 작업 기록을 만드는 데 필요한 관리자 역할
sys_ui_policy_action	삭제	UI 정책 작업 기록을 삭제하는 데 필요한 관리자 역할
sys_ui_policy_action	쓰기	UI 정책 작업 기록에 쓰는 데 필요한 관리자 역할
sys_ui_script	쓰기	UI 스크립트 기록에 쓰는 데 필요한 관리자 역할
sys_ui_script	삭제	UI 스크립트 기록을 삭제하는 데 필요한 관리자 역할
sys_ui_script	생성	UI 스크립트 기록을 만드는 데 필요한 관리자 역할
sys_user	쓰기	역할이 없는 사용자는 자신의 기록 외에는 어떤 사용자 기록도 업데이트할 수 없습니다.
sys_user_grmember	삭제	그룹 구성원 기록을 삭제하는 데 필요한 user_admin 역할

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이름	운영	설명
sys_user_grmember	쓰기	그룹 구성원 기록에 쓰는 데 필요한 user_admin 역할
sys_user_group	생성	itil 이상만 그룹 기록을 생성할 수 있습니다.
sys_user_group	쓰기	itil 이상만 그룹 기록에 쓸 수 있습니다.
sys_user_has_role	읽음	사용자 역할 기록을 보는 데 필요한 itil 역할
sys_user_role	생성	역할 기록을 만드는 데 필요한 관리자 역할
sys_user_role	삭제	역할 기록을 삭제하는 데 필요한 관리자 역할
sys_user_role	쓰기	역할 기록에 쓰는 데 필요한 관리자 역할
sys_user_role_contains	읽음	포함된 역할 기록을 보는 데 필요한 itil 역할
sys_user_role_contains	쓰기	포함된 역할 기록에 쓰는 데 필요한 관리자 역할
sys_user_token	RWCD	사용자 토큰 기록을 읽기/쓰기/생성/삭제하는 데 필요한 관리자 역할

주: 이 플러그인에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 보안 점프 시작 플러그인(ACL 규칙) 사용〔보안 센터 1.3에서 업데이트됨〕.

ACL 규칙 구성

사용자 지정 ACL(접근 제어 목록) 규칙을 구성하여 새 객체에 대한 액세스를 보호하거나 기본 보안 동작을 변경합니다.

시작하기 전에
필요한 역할: security_admin

이 태스크 정보
ACL 규칙을 생성하려면 security_admin 역할에 대한 권한을 상승시켜야 합니다.

ACL 규칙 기록과 범위가 다른 테이블의 경우 규칙 유형이 제한됩니다. 범위 마스터 테이블에서 범위를 파생시키고 범위 지정 ACL을 실행하려면 속성을 **true**로 설정합니다*glide.enforce_security_scope.<scope_name>*. 이렇게 하면 관련 테이블에 생성된 범위별 ACL이 있는 경우 전역 범위의 ACL이 일치하지 않습니다. 예를 들어 sys_attachment 또는 sys_question_answer 테이블과 같은 전역 범위의 공유 애플리케이션 테이블 내에서 데이터를 보호하는 경우를 들 수 있습니다.

프로시저
1. 권한 역할이 security_admin 역할로 상승되었습니다.
2. 다음으로 이동 시스템 보안 > 접근 제어**(ACL)**.
3. 새로 만들기를 클릭합니다.

   팁: 새 ACL을 만들 때 를 거부-미포함 ACL검토하는 것이 좋습니다.

4. 양식을 작성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 제어 필드

필드	설명
유형	이 ACL 규칙이 보호하는 개체의 종류를 선택합니다. 개체의 형식은 개체의 이름을 지정하는 방법과 사용 가능한 작업을 결정합니다. 이 필드는 ACL 규칙이 생성된 후에 읽기 전용이 됩니다. 유형을 변경하려면 ACL을 삭제하고 올바른 유형으로 새 ACL을 만들어야 합니다.
운영	이 ACL 규칙이 보호하는 작업을 선택합니다. 각 개체 형식에는 고유한 작업 목록이 있습니다. ACL 규칙은 하나의 작업만 보호할 수 있습니다. 여러 작업을 보호하려면 각각에 대해 별도의 ACL 규칙을 생성합니다. report_view 작업에 대한 규칙을 만드는 경우 도 Report_view 접근 제어 참조하십시오 .
결정 유형	ACL의 결정 유형을 선택합니다. 평가 성공 시 액세스를 허용하는 경우 허용. 미충족 거부 는 평가에 성공하지 못한 경우 접근을 거부합니다. 자세한 내용은 을 참조하십시오 거부-미포함 ACL .
관리자 재정의	관리자 역할을 가진 사용자가 이 ACL 규칙에 대한 권한 검사를 자동으로 통과하도록 하려면 이 확인란을 선택합니다. admin 사용자는 적용되는 스크립트 또는 역할 제한에 관계없이 통과합니다. 그러나 직원만 ServiceNow 할당할 수 있는 **nobody** 역할이 admin 재정의 옵션보다 우선합니다. ACL에 아무도 역할이 할당된 경우 관리자 재정의 를 선택한 경우에도 관리자 사용자는 자원에 액세스할 수 없습니다. 기본 시스템 역할을 참조하십시오. 관리자가 보안 개체에 접근하기 위해 이 ACL 규칙에 정의된 권한을 충족해야 하는 경우 이 확인란의 선택을 취소합니다. 관리자는 항상 역할 검사를 통과하므로(필수 역할 필드에 대한 설명 참조) 조건 작성기 또는 스크립트 필드를 사용하여 관리자가 통과해야 하는 권한 검사를 만듭니다.
보호 정책	ACL에 보호 정책을 설정하려면 이 항목을 선택합니다.
이름	보안이 유지되는 객체의 이름(기록 이름 또는 테이블 및 필드 이름)을 입력합니다. 이름이 구체적일수록 ACL 규칙도 더 구체적입니다. 기록, 테이블 또는 필드 이름 대신 와일드카드 문자 별표(*)를 사용하여 기록 유형, 모든 테이블 또는 모든 필드와 일치하는 모든 객체를 선택할 수 있습니다. 와일드카드 문자와 텍스트 검색을 결합할 수 없습니다. 예를 들어, inc*는 유효한 ACL 규칙 이름이 아니지만 incident.* 및 *.number는 유효한 ACL 규칙 이름입니다. 주: 파란색 삼각형을 클릭하여 보호 중인 객체의 기록 이름 또는 테이블 및 필드 이름을 수동으로 입력합니다. 드롭다운에 나타나지 않는 개체를 보호하려면 이 옵션을 사용합니다.
설명	이 ACL 규칙이 보호하는 개체 또는 권한에 대한 설명을 입력합니다.
활성	이 ACL 규칙을 적용하려면 이 확인란을 선택합니다.
고급	고급 조건 필드를 표시하려면 이 확인란을 선택합니다. 6단계를 참조하십시오.

5. 옵션: ACL의 범위를 좁히려면 필요에 따라 조건 필드를 채웁니다.

역할 필요	이 목록을 사용하여 사용자가 객체에 액세스하는 데 필요한 역할을 지정합니다. 여러 역할을 나열하는 경우 나열된 역할 중 하나를 가진 사용자가 객체에 액세스할 수 있습니다. 역할 필요 목록이 관련 목록으로 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 관리자 역할이 사용자에게 다른 모든 역할을 자동으로 부여하기 때문에 관리자 역할을 가진 사용자는 항상 이 권한 검사를 통과합니다.

데이터 조건	이 조건 작성기 를 사용하여 사용자가 객체에 액세스하는 데 예여야 하는 필드와 값을 선택합니다. 주: 조건 필드는 대/소문자를 구분합니다

6. 옵션: 고급 상자가 선택되어 있으면 필요에 따라 고급 조건 필드를 채웁니다

참조에 의해 제어됨	관련 기록에 ACL을 적용합니다. 자세한 내용은 관련 기록 접근 문서를 참조하십시오.
스크립트	객체에 접근하는 데 필요한 권한을 설명하는 사용자 지정 스크립트를 입력합니다. 스크립트는 비즈니스 규칙과 시스템 속성의 현재 및 이전 전역 변수 값을 사용할 수 있습니다. 스크립트는 다음 두 가지 방법 중 하나로 true 또는 false 응답을 생성해야 합니다. ◦ true 또는 false 값으로 설정된 응답 변수를 반환합니다. ◦ True 또는 False로 평가 두 경우 모두 스크립트가 true로 평가되고 사용자가 ACL 규칙의 조건을 충족하는 경우에만 객체에 액세스할 수 있습니다. 사용자가 객체에 액세스하려면 조건과 스크립트가 모두 true로 평가되어야 합니다. 스크립트 필드에 스크립트가 있는 경우 이 스크립트는 필드가 양식에 표시되지 않아도 실행됩니다. 주: 평가된 항목이 관련 목록에 있으면 현재 는 ACL이 대상인 현재 항목이 아니라 관련 목록이 있는 항목을 가리킵니다. 그러나 ACL을 평가 중인 항목이 관련 목록에 없는 경우 현재 가 실제 항목을 가리킵니다.

7. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택합니다.

거부-미포함 ACL

거부-미포함 ACL에 대해 자세히 알아보십시오.

거부-미충족 ACL은 "거부-미충족" 접근 방식으로 평가됩니다. ACL은 거부되지 않을 사용자를 정의합니다. 달리 말하면 역할, 조건 및 스크립트 요구 사항이 충족 되지 않으면 사용자의 액세스가 거부됩니다.

중요사항: 거부-미사용 ACL은 ACL 평가에서 Allow-If ACL보다 우선합니다.

거부-미사용 ACL은 두 가지 결과를 생성합니다.

평가 결과	결과
성공	정의된 역할, 데이터 조건, 보안 속성 및 스크립트 요구 사항이 충족됩니다. ACL이 추가 평가를 진행합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

평가 결과	결과
	중요사항: Allow-If ACL은 주체가 자원에 액세스할 수 있도록 액세스 권한을 계속 부여해야 합니다.
실패	거부-미포함 ACL이 실패로 표시되고 액세스가 거부됩니다.

다음은 Deny-Unless ACL의 설명 된 예입니다.

- ACL에 `sn_hr_core.manager` 및 `itil` 역할이 있습니다.
- 조건 활성 = `#`
- 스크립트에 응답이 있음 = `gs.isLoggedIn();`

이 ACL에 대한 세 가지 요구 사항이 모두 충족되지 않으면 사용자의 액세스가 거부됩니다. 이 예외 거부 ACL을 통과하려면 사용자에게`sn_hr_core.manager` 또는 `itil` 역할이 있어야 하며, 활성 필드 = `true`인 기록에 액세스하고, 로그인해야 합니다. 세 가지 요구 사항 중 하나라도 충족되지 않으면 거부 ACL이 실패합니다.

ACL 허용

ACL(접근 제어 목록) 허용에 대해 알아봅니다.

ACL 허용은 특정 규칙에서 거부하지 않는 한 기본적으로 자원에 대한 액세스 권한을 부여하도록 설계되었습니다. 이것은 "Deny-Unless" 모델의 반대입니다.

쿼리 ACL

쿼리 ACL을 사용하면 데이터를 쿼리할 수 있는 사용자를 명시적으로 정의하여 보다 세분화된 액세스 제어를 정의할 수 있습니다.

쿼리 ACL이란 무엇입니까?

쿼리 ACL 의 작업은 `query_range` 또는 `query_match`로 설정됩니다. 쿼리 ACL을 사용하면 사용자 쿼리를 보다 구체적으로 제어하여 설정에 따라 액세스를 제한하거나 활성화할 수 있습니다. 쿼리 ACL은 공격자가 값을 볼 수 없는 경우에도 데이터를 맹목적으로 쿼리하여 결과에서 정보를 추출하는 블라인드 쿼리 공격 에 대한 강력한 도구입니다.

쿼리 ACL을 사용하는 경우

열에 중요한 값이 포함되어 있고 데이터에 대한 부분/조건부 액세스를 허용하는 경우 쿼리 ACL은 데이터의 민감도에 따라 필요에 따라 고려되고 구현되어야 합니다. 테이블의 행과 해당 열에 대한 부분/조건부 액세스가 있는 경우, 특히 데이터 필터에 의해 액세스가 적용되지 않는 경우 쿼리 ACL은 데이터의 민감도에 따라 필요에 따라 구현되어야 합니다.

주: 일부 사용자가 일부 행이나 열에는 액세스할 수 있고 다른 행이나 열에는 액세스할 수 없는 경우 쿼리 ACL을 고려하십시오.

Example: 급여 쿼리 통제

급여 테이블에서 내 급여와 함께 한 행을 볼 수 있지만 2개의 경계 내에 포함된 급여를 가진 사용자를 쿼리하기 위해 범위 쿼리를 실행할 수 있을 이유가 없습니다. 급여에 대한 `query_range` ACL로 인해 해당 쿼리를 실행할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example: HR 쿼리 제어

모든 hr_profiles 볼 수 있지만 SSN은 직접 볼 수 있습니다. SSN을 쿼리하는 비즈니스가 없으며 쿼리 ACL은 SSN 매핑을 추출하기 위해 다른 HR 프로필의 SSN에 대해 쿼리를 실행하지 못하게합니다.

쿼리 ACL 동작

쿼리 ACL은 안전하고 세분화된 테이블 쿼리 동작을 위해 `query_match` 및 `query_range` 작업을 사용합니다. 그들의 행동은 아래에 설명되어 있습니다.

`query_match`

`query_match` 는 EQUALS, NOT_EQUALS, IN, NOT_IN, SAMEAS, NSAMEAS, ANYTHING, ISEMPTYSTRING, ISEMPTY, ISNOTEMPTY, ISNULL, ISNOTNULL로 구성됩니다. `query_match` 는 특정 기록을 가져오도록 구축되었으며 다른 기록을 반환하기 위해 악용할 수 없다는 의미에서 "안전한 연산자"로 구성됩니다.

평가 결과	결과
성공	사용자는 일치 쿼리를 제출할 수 있습니다.
실패	사용자는 일치 쿼리를 제출할 수 없습니다. • 같음 • NOT_EQUALS • IN • NOT_IN • 동일 • 은사메스 • 아무것도 • ISEMPTY문자열 • 비어 있음 • ISNOTEMPTY • ISNULL • ISNOTNULL

`query_range`

`query_range` 는 다른 모든 항목(STARTS_WITH, CONTAINS, >=, <= 등)으로 구성되며, 이는 사용자가 경계 값을 조정하여 더 많은 레코드를 쿼리할 수 있도록 하므로 더 위험합니다.

평가 결과	결과
성공	사용자는 범위 쿼리를 제출할 수 있으며 정렬은 무제한입니다.
실패	사용자는 (STARTS_WITH, CONTAINS, >=, <= 등을 사용하여 범위 쿼리를 제출할 수 없습니다. 열별 정렬이 제한됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항:

쿼리 ACL(query_match 및 query_range 모두)은 기본적으로 읽기 권한을 위임하는 star.star ACL로 설정됩니다. 즉, ACL이 쿼리에 적용되는 경우 쿼리 ACL이 생성되지 않은 경우 열에 대한 읽기 권한이 평가됩니다. 쿼리 ACL이 정의된 경우 기본 동작을 재정의합니다.

포함된 목록에서 기록 보호

포함된 목록의 기록에 보안을 적용하려면 포함된 목록의 기록 편집 및 삭제를 특정 역할로 제한합니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 접근 제어**(ACL)**.
2. 해당 테이블에 대한 쓰기 또는 삭제 기록을 엽니다.
3. 양식의 역할 필요 섹션에서 해당 테이블에 대한 쓰기 또는 삭제 권한이 있는 역할을 추가합니다.
4. 변경 내용을 저장합니다.
   연결된 테이블의 기록이 포함된 목록에 나타나는 경우 지정된 역할을 가진 사용자만 편집 및 삭제 옵션을 사용할 수 있습니다.

관련 기록 접근

관련 기록 액세스를 통해 사용자가 관련 테이블 간에 액세스할 수 있는 기록을 일관되게 제어할 수 있습니다.

관련 기록 접근 상세 정보

관련 기록 액세스를 사용하면 관련 기록에 대한 액세스를 구성하고, ACL에서 액세스가 허용된 데이터에 관련 상위 테이블의 ACL을 적용해야 하는지 여부를 결정할 수 있습니다. 다음 사용 사례를 고려할 때, 사용자는 ACL을 통해 기록에 액세스할 수 있고, 관련 기록 액세스를 사용하면 참조 또는 양방향 관계를 통해 관련된 다른 모든 기록에 액세스할 수 있습니다.

상황별 보안 관리자

상황별 보안 관리자는 읽기, 쓰기, 생성 및 삭제 권한 부여를 제어하여 데이터를 보호합니다.

주요 이점

상황별 보안 관리자는 시스템 테이블 계층 구조를 인식하므로 계층 구조에서 필드가 표시되는 위치에 따라 필드에 대한 특정 보안 규칙을 만들 수 있습니다. 상황별 보안 관리자의 이점은 다음과 같습니다.

- 상황별 보안: 기록의 내용을 기반으로 기록을 보호합니다.
- 계층적 보안: 개체 계층 구조의 모든 수준에 보안 규칙을 적용합니다.

필드 및 테이블 보안

레거시 Simple Security Manager를 사용하면 적절한 딕셔너리 항목에 역할을 추가하여 필드와 테이블을 보호할 수 있습니다. 상황별 보안 관리자를 사용하면 이러한 딕셔너리 역할이 더 이상 테스트되지 않습니다. 대신 시스템은 필드와 테이블에서 ACL 규칙을 찾습니다.

경고: 상황별 보안 관리자를 설치한 후에는 ACL 규칙을 통해 필드와 테이블을 보호해야 합니다. 양식 레이아웃, 딕셔너리 양식을 구성하고 딕셔너리 항목에 역할을 추가하더라도 권한은 변경되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상황별 보안 및 역할

사용자 또는 그룹에 역할을 부여할 수 있습니다. 그러나 상황별 보안 관리자를 설치한 후에는 사용자 기록의 역할 필드가 더 이상 선택되지 않으며 사용자 및 그룹 양식에 나타나지 않습니다. 대신, 사용자 또는 그룹 기록 대신 역할 관련 목록에 역할을 추가해야 합니다.

애플리케이션 및 모듈에는 이를 보는 데 필요한 역할 목록이 포함되어 있습니다. 예를 들어 시스템 정의 애플리케이션을 보려면 관리자 역할이 필요합니다. 애플리케이션 및 모듈에 대한 보안 권한은 여전히 역할 배열을 사용하여 정의됩니다.

카탈로그 항목과 카탈로그 변수 모두 이를 확인하는 데 필요한 역할 목록이 포함되어 있습니다. 카탈로그 항목 및 카탈로그 변수에 대한 보안 권한은 여전히 이러한 역할 배열을 통해 정의됩니다.

상황별 보안 관리자에서 역할은 역할에 대한 상속 플래그가 예로 설정된 경우에도 그룹에 부여된 모든 역할을 자동으로 상속합니다.

상황별 보안 관리자 활성화

상황별 보안 관리자가 기본 시스템에서 활성 상태입니다. 사용자 역할 테이블에 중복 항목이 많은 경우 중복 역할을 제거하기 위해 상황별 보안: 역할 관리 V2로 업그레이드해야 할 수 있습니다. 플러그인은 다음과 같습니다.

상황별 보안: 역할 관리[com.glide.role_management]

상황별 보안 기능을 제공합니다. 이 플러그인은 자동으로 설치됩니다.

상황별 보안: Role Management V2 [com.glide.role_management.inh_count]

사용자 역할 [sys_user_has_role] 테이블에서 상속된 역할로 인한 중복 항목을 방지합니다. 이 플러그인은 새 인스턴스에 자동으로 설치되며 업그레이드를 위해 활성화할 수 있습니다. 상황별 보안: 역할 관리 개선 사항 플러그인은 이 플러그인의 이전 버전입니다. Role Management Enhancements 플러그인에는 RoleManagementVerify() 스크립트가 포함되어 있지 않습니다. 이 스크립트는 플러그인의 변경 내용을 모니터링할 수 있도록 업그레이드에서 수행할 변경 목록을 반환합니다.

주: 역할 관리 V2를 활성화한 후에는 감사 역할 테이블이 사용자 역할과 관련된 감사 기록을 생성할 수 있도록 glide.role_management.v2.audit_roles 시스템 속성을 설정해야 합니다. 이 속성 설정 및 역할 감사 테이블에 대한 자세한 내용은 다음을 참조하십시오.

- 상황별 보안과 함께 역할 감사 사용: 역할 관리 V2.
- 강화 설정 인스턴스 보안 강화 설정에서.
- 사용자 역할 감사

상황별 보안으로 중복 항목 방지: 역할 관리 **V2**

다른 역할에서 상속된 역할은 사용자 역할 테이블 (sys_user_has_role)에 개별 항목으로 추가되며, 이로 인해 한 역할이 중복 항목을 가질 수 있습니다. 상황별 보안: 역할 관리 V2는 이러한 중복 항목을 제거하고 향후 중복을 방지합니다.

상속 횟수를 통해 중복 항목 제거

상황별 보안: 역할 관리 V2는 상속 수(inh_count) 열을 사용하여 역할이 다른 역할 또는 그룹에서 상속되는 횟수를 추적합니다. 사용자 역할 [sys_user_has_role] 테이블에서 사용자는 특정 역할을 한 번만 상속할 수 있으므로 중복 항목이 제거됩니다. 상속 수(inh_count) 열은 읽기 전용이며 사용자가 역할을 상속하는 횟수를 계산합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

활성화 변경

상황별 보안: 역할 관리 V2는 새 인스턴스에 자동으로 설치되며 업그레이드를 위해 활성화할 수 있습니다. 활성화되면 상황별 보안: 역할 관리 V2가 상황별 보안과 상황별 보안: 역할 관리 개선 사항을 모두 대체합니다.

상황별 보안: 역할 관리 V2가 활성화되면 다음 열은 더 이상 사용되지 않지만 이전 버전과의 호환성을 위해 사용자 역할 테이블에 남아 있습니다.

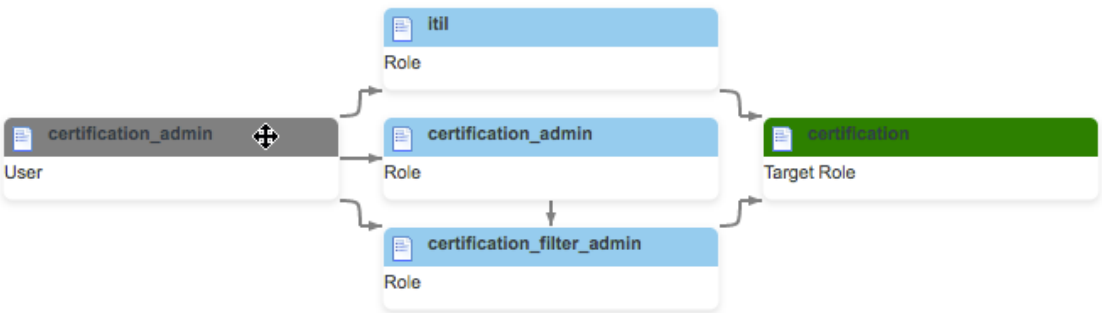
- granted_by(역할 위임에 의해서만 사용됨)
- included_in_role
- included_in_role_instance

경고: 이러한 열이 인스턴스의 사용자 지정 스크립트에서 사용 중인 경우 역할 관리 V2로 업그레이드하지 마십시오.

역할 상속 맵을 통해 역할 상속 시각화

역할 상속 맵은 상속된 역할의 시각적 표현을 표시합니다. 이 맵을 사용하여 상속 수(inh_count) 열에 표시되는 역할을 이해할 수 있습니다. 역할 상속 맵을 보려면 역할 상속 맵 열을 표시하도록 사용자 역할 [sys_user_has_role] 테이블을 구성합니다.

역할 상속 맵



상황별 보안: 역할 관리 V2로 업그레이드

상황별 보안: 역할 관리 V2는 새 인스턴스에 자동으로 설치됩니다. 상황별 보안: 역할 관리에서 상황별 보안: 역할 관리 V2로 업그레이드하여 사용자 역할 테이블에서 중복 역할을 제거하고 향후 중복을 방지할 수 있습니다.

시작하기 전에

필요한 역할: admin, security_admin
관리자 역할이 있어야 하며 권한 있는 역할로 상승 유효 security_admin 역할을 얻어야 합니다.

주: 상황별 보안: 역할: 관리 V2로 업그레이드하기 전에 감사 역할 테이블을 활성화하여 사용자 역할과 관련된 감사 기록을 생성해야 합니다. 필수 시스템 속성을 설정하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 상황별 보안과 함께 역할 감사 사용: 역할 관리 V2.

이 태스크 정보

이 절차에서는 상황별 보안 역할을 업그레이드하는 방법과 다음 표에 설명된 관련 플러그인을 활성화하는 방법을 설명합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

상황별 보안용 플러그인: 역할 관리 **V2**

플러그인	설명
상황별 보안: 역할 관리 V2 [com.glide.role_management.inh_count]	사용자 역할 [sys_user_has_role] 테이블에 중복 항목을 방지합니다. 플러그인 또는 연락처를 고객 서비스 및 지원활성화하려면 security_admin 역할 또는 상승된 권한이 있는 사용자가 필요합니다.
상황별 보안: 역할 관리 V2 REST API [com.glide.role_management.inh_count.rest_api]	역할 관리를 위해 API 기능을 활성화합니다.

상황별 보안: 역할 관리에서 상황별 보안: 역할 관리 V2로 업그레이드하기 전에 스크립트를 실행하여 업그레이드 결과를 테스트합니다. 스크립트는 업그레이드가 수행할 변경 내용 목록을 반환합니다. 변경 내용이 허용되는 경우 상황별 보안: 역할 관리 V2 플러그인을 설치합니다. 변경 내용이 허용되지 않는 경우 상황별 보안: 역할 관리 V2 플러그인을 설치하지 마십시오. 또는 업그레이드를 수행한 다음 필요한 사항을 수동으로 변경할 수 있습니다.

프로시저

1. 다음 스크립트를 실행하여 업그레이드에 앞서 업그레이드의 영향을 테스트합니다.

a. 다음으로 이동 시스템 정의 > 스크립트 **-** 백그라운드.

b. 전역 범위에서 다음 스크립트를 실행합니다.

```
new RoleManagementVerify().verifyInheritedRoles();
```

큰 sys_user_has_role 테이블의 경우 실행을 완료하는 데 최대 몇 시간이 걸릴 수 있습니다. 이 시간 동안에는 사용자 역할을 편집하거나 추가하지 마십시오.
테스트 데이터를 기반으로 한 예제 결과:

```
*** 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. 스크립트 결과를 평가하여 제안된 변경 내용이 수용 가능한지 여부를 결정합니다.

2. 상황별 보안: 역할 관리 V2 플러그인을 활성화합니다.

중요사항: 플러그인 또는 연락처를 고객 서비스 및 지원활성화하려면 security_admin 역할 또는 상승된 권한이 있는 사용자가 필요합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 시스템 정의 > 플러그인.

b. 플러그인 이름을 찾아서 클릭합니다.

c. 시스템 플러그인 양식에서 플러그인 상세 정보를 검토한 다음 활성화/업그레이드 관련 링크를 클릭합니다.

d. 활성화를 클릭합니다.

결과
역할 관리 V2를 활성화하면 스크립트 결과에 설명된 변경 내용이 적용됩니다. 사용자 역할 테이블의 inh_count(상속 수) 열은 읽기 전용이며 사용자가 역할을 상속한 횟수를 자동으로 반영합니다.

상황별 보안과 함께 역할 감사 사용: 역할 관리 **V2**

감사 역할 테이블이 사용자 역할과 관련된 감사 기록을 생성할 수 있도록 시스템 속성을 설정합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
사용하도록 설정하면 역할 감사 [sys_audit_role] 테이블에서 사용자 기록에 대한 변경 내용을 유지합니다. 역할 감사에 대한 자세한 내용은 사용자 역할 감사 를 참조하십시오. 상황별 보안: 역할 관리 V2 [com.glide.role_management.inh_count] 플러그인이 설치된 경우 역할 감사를 사용하려면 시스템 속성을 **true** 로 설정해야 합니다.

프로시저

1. 시스템 속성 [sys_properties] 테이블로 이동합니다.
2. *glide.role_management.v2.audit_roles* 시스템 속성을 추가하고 **true**로 설정합니다.

   상황별 보안: 역할 관리 V2 [com.glide.role_management.inh_count] 플러그인이 설치된 경우 이 속성을 **true** 로 설정하면 사용자 역할이 변경될 때 역할 감사 [sys_audit_role] 테이블에서 기록을 만들 수 있습니다.

양식 제출 재확인

시스템에서 현재 사용자가 특정 필드(예: task.number)를 기록해서는 안 된다고 결정하면 시스템은 해당 필드를 읽기 전용 모드로 렌더링하므로 대부분의 인시던트에서 번호 필드를 쓸 수 없습니다.

수신 필드의 값에 쓰기 가능성을 다시 확인하도록 시스템을 설정하면 시스템은 트랜잭션의 인바운드 레그에 동일한 보안 규칙 집합을 적용합니다. 예를 들어 인시던트를 제출할 때 시스템은 변경 사항을 게시하기 전에 번호 필드를 쓸 수 있는지 다시 확인합니다.

인바운드 트랜잭션을 다시 확인하지 않도록 시스템에 지시하면 클라이언트가 다시 보내는 트랜잭션인 경우 명목상 읽기 전용 필드에 쓸 수 있습니다. 예를 들어 클라이언트 스크립트를 사용하여 쓰기 가능한 다른 필드의 사용자 선택에 대한 응답으로 명목상 읽기 전용 필드를 설정하는 경우와 같이 많은 배포에서 이는 실제로 바람직한 동작입니다.

속성	위치	기본값
양식을 제출하는 동안 인바운드 트랜잭션의 보안을 다시 한 번 확인하십시오(양식 작성 시 권한을 항상 확인합니다).	시스템 속성 > 보안	사용 안 함(이중 확인 없음)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기본 거부 속성

기본 거부 속성(`glide.sm.default_mode`)은 유일하게 일치하는 ACL 규칙이 와일드카드 테이블 ACL 규칙인 경우 보안 관리자의 기본 동작을 제어합니다.

가장 일반적인 기록 기반 작업에 대한 와일드카드 테이블 ACL 규칙 세트인 읽기, 쓰기, 생성 및 삭제를 사용할 수 있습니다. 시스템 테이블에 대한 역할 기반 액세스를 제공하기 위해 많은 수의 ACL도 사용할 수 있습니다. 예를 들어 business_rule_admin 역할이 비즈니스 규칙을 관리할 수 있는 것으로 문서화되어 있기 때문에 해당 역할에 대한 sys_script 액세스 권한을 부여하는 ACL이 있습니다.

`glide.sm.default_mode` 속성을 사용하여 모든 테이블에서 이러한 작업을 거부하거나 허용합니다.

- 접근 거부: 와일드카드 테이블 ACL 규칙은 사용자에게 관리자 역할이 있거나 다른 테이블 ACL 규칙의 요구 사항을 충족하지 않는 한 모든 테이블에서 읽기, 쓰기, 생성 및 삭제 작업을 제한합니다. report_on 및 personalize_choices와 같은 다른 작업은 이 설정의 영향을 받지 않습니다.
- 접근 허용: 와일드카드 테이블 ACL 규칙은 작업을 제한하는 특정 테이블 ACL 규칙이 없는 한 모든 테이블에서 읽기, 쓰기, 생성 및 삭제 작업을 허용합니다.

glide.sm.default_mode 액세스 거부로 설정된 후에는 액세스 허용으로 재설정할 수 없습니다.

주: 기본적으로 와일드카드 테이블 ACL 규칙은 `glide.sm.default_mode` 속성의 값을 확인하는 유일한 ACL 규칙입니다. 이 설정으로 다른 작업을 제어하려면 이 속성 값을 확인하는 고유한 ACL 규칙을 생성합니다.

이 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 빈 ACL을 사용하여 기본적으로 거부 〔보안 센터 1.3에서 업데이트됨〕 .

고급 **ACL** 구성

새 ACL을 만들거나 기존 ACL을 수정하는 것 외에도 ACL 기능의 다른 측면을 구성할 수 있습니다.

거부 **ACL** 규칙

거부-미포함

쿼리 **ACL** 규칙

작업	설명
참조 필드에 ACL 스크립트 조건 적용	참조 필드가 양식이나 목록에 표시하는 데이터에 대한 액세스를 제어하려면 스크립트 조건을 참조 필드에 적용할 수 있도록 속성을 활성화합니다. 이를 활성화하면 인스턴스 성능에 영향을 미칠 수 있습니다.
AJAXGlideRecord에 ACL 적용 (클라이언트 측 Glide 기록)	시스템이 현재 연결된 사용자에게 액세스 권한이 있는 데이터만 쿼리할 수 있도록 *GlideAjax* API 호출에 ACL을 적용합니다.
접근 수준에서 관리자 재정의 평가	접근 수준에서 관리자 재정의에 대한 ACL 평가를 강제 적용합니다. 기본적으로 ACL 규칙 양식에서 관리자 재정의 옵션을 선택하면 관리자 역할이 있는 사용자는 이 ACL 규칙에 대한 권한 검사를 자동으로 전달합니다.
ACL 디버깅 및 문제 해결 도구 사용	ACL 감시자, 필드 수준 디버깅 및 액세스 ACL 규칙 출력 메시지와 같은 도구를 사용하여 ACL 문제를 해결하고 디버그할 수 있습니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

외부 사용자에게 테이블 접근 권한 제공

snc_external 역할만 가진 사용자가 테이블의 목록 뷰에 접근할 수 있도록 하려면 일련의 ACL을 만들어야 합니다.

시작하기 전에

필요한 역할: security_admin

프로시저

1. 권한 있는 역할로 승격합니다.
2. 다음 설정을 사용하여 ACL 규칙을 만듭니다.
   - 유형: ui_page
   - 작업: 읽기
   - 이름: {table_name}_list
   - 필요한 역할: snc_external
3. 테이블의 기본 읽기 ACL에서 필요한 역할 목록에 **snc_external**을 추가합니다. ACL이 아직 없으면 새로 만듭니다.
4. 다음 설정을 사용하여 다른 ACL을 만듭니다.
   - 유형: ui_page
   - 작업: 읽기
   - 이름: {table_name}
   - 필요한 역할: snc_external
5. 이 설정을 사용하여 사용자에게 테이블의 필드에 대한 쓰기 권한을 부여하는 다른 ACL을 만들 수 있습니다.
   - 유형: 기록
   - 작업: 만들기
   - 이름: {table_name} {column_name}
   - 필요한 역할: snc_external

   사용자에게 쓰기 권한을 부여할 모든 필드에 대해 이 단계를 반복합니다. 모든 필드에 대한 접근 권한을 한 번에 제공하려면 열 이름 대신 별표*를 사용합니다.

참조 필드에 **ACL** 스크립트 조건 적용

glide.sys_reference_row_check 시스템 속성을 사용하여 참조 필드에 스크립팅된 조건을 활성화합니다.

기본 동작은 인스턴스 성능을 향상시키기 위한 것입니다. 참조 필드에 대한 스크립트 조건을 활성화하려면 다음 시스템 속성을 추가합니다.

주: 시스템 속성 생성에 대한 자세한 내용은 다음 문서를 참조하십시오 시스템 속성 추가.

시스템 속성

속성	설명
glide.sys_reference_row_check	접근 제어 규칙의 스크립트 조건이 테이블의 참조 필드에 적용되는지 여부를 통제합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 속성

속성	설명
	• 유형: true | false • 기본값: **false** • 위치: 시스템 속성 [sys_properties] 테이블에 시스템 속성 추가

주: *glide.sys_reference_row_check* 시스템 속성이 없거나 false로 설정된 경우 접근 제어 규칙에 대한 스크립트 조건이 적용되지 않습니다. 즉, 스크립팅된 조건을 포함하는 ACL은 다른 ACL 기준(예: 역할 요구 사항)이 충족되는 한 검사를 통과합니다.

AJAXGlideRecord에 **ACL** 적용(클라이언트 측 **Glide** 기록)

클라이언트 스크립트 내에서 GlideAjax API를 사용하여 서버 측 기록(예: 테이블)에 액세스할 때 시스템 속성을 사용하여 ACL(접근 제어 목록) 규칙 확인을 수행합니다.

GlideAjax API 호출에 ACL(접근 제어 목록)을 적용하기로 선택한 경우 현재 연결된 사용자에게 액세스 권한이 있는 데이터만 쿼리할 수 있습니다. 예를 들어 사용자가 `cmn_location` 테이블을 읽을 수 있는 권한이 없는 ESS 사용자로 로그인한 경우 사용자가 *GlideAjax* API를 호출하면 실패합니다.

Now Platform GlideAjax ACL 호출 검사 없이 실행 중인 경우 API는 현재 로그인한 사용자가 액세스할 수 없는 정보를 반환할 수 있습니다.

데이터를 쿼리할 때 GlideRecordSecure를 사용하여 최고 수준의 보안을 보장합니다. GlideRecord는 구성을 통한 ACL 시행에 의존하는 반면 GlideRecordSecure는 더 엄격한 보안 통제를 적용합니다. GlideRecordSecure는 중요한 데이터를 처리하기 위한 보다 안전하고 즉시 사용 가능한 솔루션을 제공합니다.

주: 다음 위치에서 이 속성 설정 시스템 속성 > 보안.

속성	기본값
AJAXGlideRecord 호출에 표준 보안 ACL 적용	ACL 검사 적용됨

경고: `sys_class_name`, `sys_id`, `sys_domain`는 ACL 검사에서 무시됩니다.

이 속성에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 AJAXGlideRecord ACL 검사 필요[Security Center 1.3에서 업데이트됨] .

접근 수준에서 관리자 재정의 평가

접근 수준에서 관리자 재정의에 대한 ACL 평가를 강제 적용하려면 시스템 속성을 추가할 수 있습니다.

시작하기 전에
필요한 역할: security_admin

이 태스크 정보
ACL은 누적 평가됩니다. 지정된 필드에 ACL 수가 있고 그 중 하나에서 **Admin Overrides**(관리자 재정의) 옵션이 **false** (선택되지 않음)인 경우 모든 ACL에 대한 유효한 관리자 재정의는 **false**로 간주됩니다. 이렇게 하면 관리자가 재정의가 적용되어야 하는 ACL도 전달할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

시스템 속성 테이블에 다음 속성을 추가합니다.

속성	설명
glide.security.admin.override.accessterm	접근 조건 수준에서 관리자 재정의 조건을 평가합니다. • 유형: true | false • 기본값: 새 인스턴스의 경우 **True**, 업그레이드의 경우 **False** • 위치: 시스템 속성 *[sys_properties]* 테이블에 추가 주: 인스턴스에 속성이 정의되어 있지 않으면 값이 false로 평가됩니다.

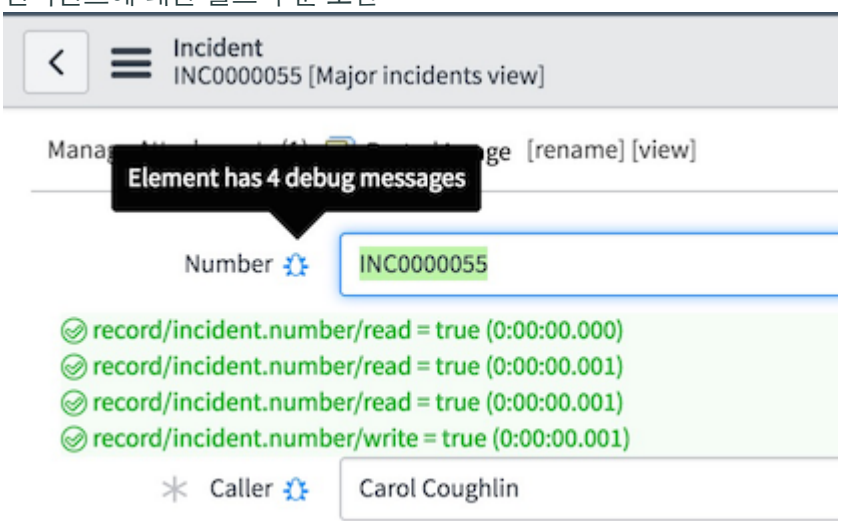
ACL 디버깅 도구

필드 레벨 디버깅 및 액세스 ACL 규칙 출력 메시지를 사용하여 ACL 문제를 해결하고 디버깅할 수 있습니다. ACL 구성 감시자를 사용하면 하나를 수정할 때 어떤 관련 ACL이 있는지 알 수 있습니다.

필드 수준 디버깅

디버깅을 사용하도록 설정하면 각 필드 옆에 작은 버그 아이콘(디버그)이 ACL 규칙이 있는 표시됩니다. 아이콘을 클릭하면 필드에 적용되는 ACL 규칙과 평가 결과가 나열됩니다. 로 이동하여 디버깅 활성화 시스템 보안 > 디버깅 > 보안 규칙 디버그.

인시던트에 대한 필드 수준 보안



ACL 디버깅을 활성화한 후 다른 사용자를 가장하여 사용자가 통과 및 실패하는 ACL 규칙을 확인할 수 있습니다. 다른 사용자로 전환하면 해당 사용자에게 허용된 내용만 볼 수 있습니다. 예를 들어, ACL이 사용자에게 표시하지 않는 기록은 볼 수 없습니다. 디버깅을 쉽게 하기 위해 테이블에 대한 읽기 권한이 없는 사용자를 가장하는 경우에도 특정 ACL 관련 테이블에 대한 읽기 전용 액세스가 기본적으로 활성화됩니다. 이 기능을 변경하려면 다음 속성을 **false**로 설정합니다.

ACL 규칙 디버깅을 활성화하려면 다음으로 이동하십시오. 시스템 보안 > 보안 규칙 디버그.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시스템 속성	설명	기본 설정
glide.security.access_acl_has_impersonator	사용자를 가장하는 동안 sys_security_acl, sys_security_operation, sys_security_type, sys_user_role 테이블에 대한 읽기 권한을 허용합니다. 따라서 가장한 사용자는 가장한 사용자가 읽을 수 없는 데이터를 읽을 수 있습니다.	예 주: 속성이 false로 설정되면 가장된 사용자가 ACL 관련 데이터를 읽지 못할 수 있습니다. 이 경우 ACL을 디버깅하기 위해 관리자 또는 security_admin로 로그인한 두 번째 세션이 필요할 수 있습니다.

ACL 규칙 출력 메시지

ACL 디버깅은 각 목록 및 양식의 맨 아래에 ACL 규칙 출력 메시지를 표시합니다. 출력 메시지에는 다음이 표시됩니다.

Message 요소	설명
시간	이 ACL 규칙을 처리하는 데 사용된 총 시간입니다.
경로	<ACL ## ##>/<ACL ## ##>/<##> 형식으로 각 ACL 규칙을 고유하게 식별하는 정보입니다.
문맥	ACL 규칙에 의해 평가되는 객체입니다.
RC(영어)	ACL 규칙의 반환 코드입니다. true 값은 ACL 규칙을 통과합니다. False 값은 ACL 규칙을 통과하지 못합니다.
규칙	프로세서 및 스크립트에 대한 간략한 요약과 함께 각 테이블 수준 및 필드 수준 ACL 평가에 대한 ACL 결과가 표시됩니다. 대부분의 ACL 평가는 전체 합격 또는 불합격 결과와 각 ACL 기준 유형에 대한 결과 분석을 보여줍니다. • iAccessHandler: 플랫폼에서 숨겨진 소스 코드를 사용하는 내부 시스템 검사입니다. 수정할 수 없는 시스템 보안 검사입니다. IAccessHandler는 ACL을 평가하지 않고 리소스에 대한 액세스 권한을 부여하거나 거부할 수 있습니다. IAccessHandler를 무시하면 ACL이 평가됩니다. 어떤 식으로든 IAccessHandler 검사를 수정할 수 없습니다. 예를 들어, IAccessHandler 구현은 응용 프로그램 리소스에 대한 액세스 검사에 사용되며 변경할 수 없습니다. 릴리스부터 Istanbul 사용할 수 있습니다. • 역할: 사용자에게 올바른 역할이 있는지 확인합니다. • 조건: 사용자가 ACL 규칙에 지정된 조건을 통과했다는 검증(있는 경우). • 스크립트: 사용자가 ACL 규칙에 지정된 스크립트를 통과했는지 확인합니다 (있는 경우).

표시되는 아이콘은 ACL이 평가된 방식을 보여줍니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

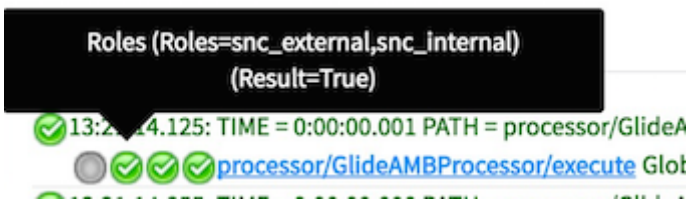
아이콘	설명
그린 체크 표시 ( )	테이블 또는 필드가 기준을 통과했음을 나타냅니다.
빨강 × 아이콘 ( )	테이블 또는 필드가 통과하지 못했음을 나타냅니다.
빈 회색 원 아이콘( )	ACL 평가를 수행할 필요가 없었음을 나타냅니다.
파란색 확인 표시, x 또는 빈 원	이전 ACL 검사의 캐시된 결과에서 ACL을 가져왔음을 나타냅니다. 아이콘의 의미는 위와 같습니다.

ACL 디버그 출력에서 다음 작업을 수행할 수 있습니다.

- 디버그 출력 상단에 있는 다음 확인란을 선택하거나 선택을 취소합니다.
  - 보안 규칙: ACL 검사 결과를 표시하거나 숨깁니다.
  - 기타: 다른 경고 또는 메시지를 표시하거나 숨깁니다.
- 출력 메시지 옆에 있는 ACL 이름을 클릭하여 해당 ACL 기록을 엽니다.



- 4개의 ACL 검사에 대한 아이콘 위에 커서를 올려놓으면 자세한 정보가 표시됩니다.



ACL 문제 해결 참조

일반적인 ACL 규칙 오류 및 해결 방법의 목록입니다.

디버깅을 사용하면 문제 해결에 도움이 됩니다.

문제 해결

오류 또는 증상	솔루션
사용자 지정 테이블의 기록에는 액세스할 수 없습니다.	사용자에게 테이블에 대한 접근 권한을 부여하는 사용자 지정 테이블에 대한 테이블 ACL 규칙을 생성합니다. 명시적 테이블 ACL 규칙이 없을 경우, 사용자는 테이블 와일드카드(*) ACL 규칙으로 권한을 전달해야 하며, 이 규칙은 기본적으로 관리자에게만 접근을 제한합니다. 디버깅을 활성화하고 사용자 지정 테이블에 대해 평가할 ACL 규칙을 결정합니다.
제대로 작동하지 않는 사용자 지정 ACL 규칙을 만듭니다.	가장 가능성이 높은 문제는 처리 순서에서 다른 규칙이 사용자 지정 규칙보다 우선하거나 사용자가 개체 유형에 대한 모든 권한 요구 사항을 충족하지 않는 것입니다. 디버깅을 사용하도록 설정하고 ACL 규칙이 평가되고 있는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

문제 해결

오류 또는 증상	솔루션
필드 ACL 규칙이 제대로 작동하지 않습니다.	사용자가 충족하지 못한 테이블 ACL 규칙이 있을 수 있습니다. 디버깅을 활성화하고 필드에 대해 평가할 ACL 규칙을 결정합니다. 상충하는 테이블 ACL 규칙 또는 중복 필드 ACL 규칙이 없는지 확인합니다.
테이블 ACL 규칙이 제대로 작동하지 않습니다.	처리 순서에서 더 높은 ACL 규칙 또는 테이블 ACL 규칙을 방해하는 중복 테이블 ACL 규칙이 있습니다. 디버깅을 활성화하고 테이블에 대해 평가할 ACL 규칙을 결정합니다.
목록에서는 필드를 볼 수 있지만 양식에서는 볼 수 없습니다.	ACL 규칙 조건 또는 스크립트가 목록에서는 트리거되지만 양식에서는 트리거되지 않을 수 있습니다. 디버깅을 활성화하고 ACL 규칙이 예로 평가되는 시기를 결정합니다. 목록 및 양식에서 동일하게 작동하도록 조건 또는 스크립트를 업데이트합니다.
프로세서 또는 클라이언트 호출 가능 스크립트 포함을 실행하려고 할 때 오류 메시지가 나타납니다.	사용자가 충족하지 않은 프로세서 또는 클라이언트 호출 가능 스크립트 포함에 대한 ACL 규칙이 있습니다. 사용자에게 개체에 대한 액세스 권한이 있어야 하는 경우 디버깅 을 사용하도록 설정하고 프로세서 또는 스크립트 포함에 대해 평가할 ACL 규칙을 결정합니다. 객체에 접근하는 데 필요한 대로 ACL 규칙 또는 사용자 역할을 업데이트합니다.

ACL 구성 감시자

ACL 구성 감시자를 사용하면 동일한 테이블에서 ACL을 삽입, 업데이트 또는 삭제할 때 테이블에 어떤 관련 ACL이 있는지 알 수 있습니다.

ACL 구성 감시자는 액세스 제어 [sys_security_acl] 테이블에서 중요한 변경 사항이 있을 때마다 표시되는 인터셉터 창입니다. 수정 중인 ACL과 관련된 ACL을 볼 수 있는 보안 규칙 요약 창이 표시됩니다. 보안 규칙 창에서 ACL을 수정할 수 없습니다. 수정하려면 감시자 창을 닫고 해당 ACL로 이동합니다.

ACL 구성 감시자는 다음과 같은 상황에서는 나타나지 않습니다.

- 실제로 변경하지 않고 ACL 기록을 저장 또는 업데이트하는 경우
- 스크립트, 조건 및 admin-overrides 옵션 업데이트와 같은 사소한 업데이트(삽입 또는 삭제 아님)를 수행하는 경우.
- ACL 기록이 활성 상태가 아닌 경우

ACL 보안 규칙 창

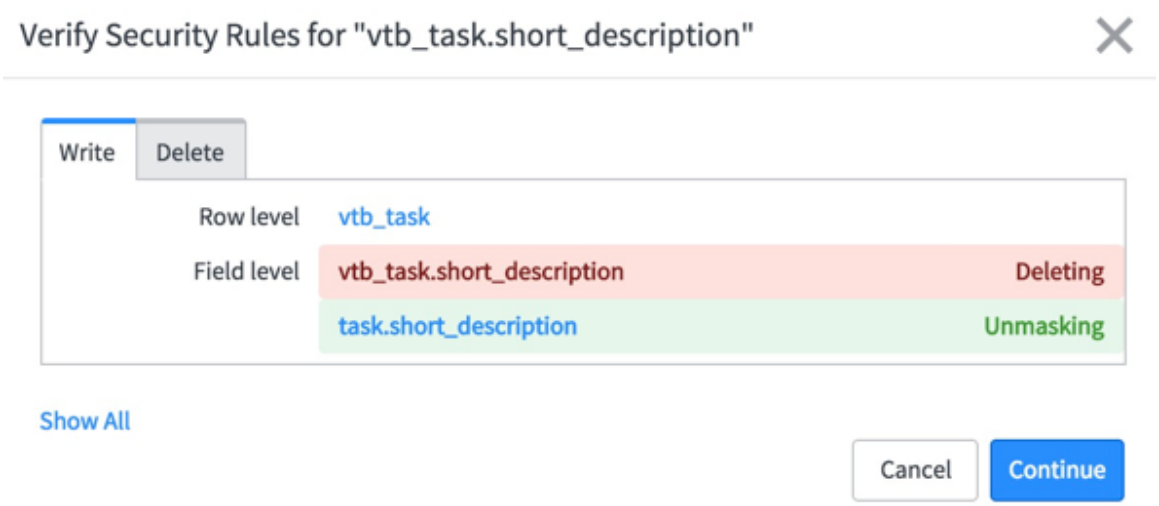
구성 감시자에는 ACL 실행 계획이 표시됩니다. 실행 계획이 보안 규칙 팝업 창에 표시됩니다. 이러한 종류의 정보를 볼 수 있습니다.

ACL 구성 창 요소

항목	설명
빨간색 강조 표시	삭제되거나 비활성화된 ACL입니다.
파란색 강조 표시	수정된 ACL입니다.
녹색 강조 표시	추가되거나 활성화되는 ACL
마스킹됨	변경하기 전까지 유효한 ACL입니다.
마스크	변경했을 때 방금 발효된 ACL입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

구성 감시자 예시



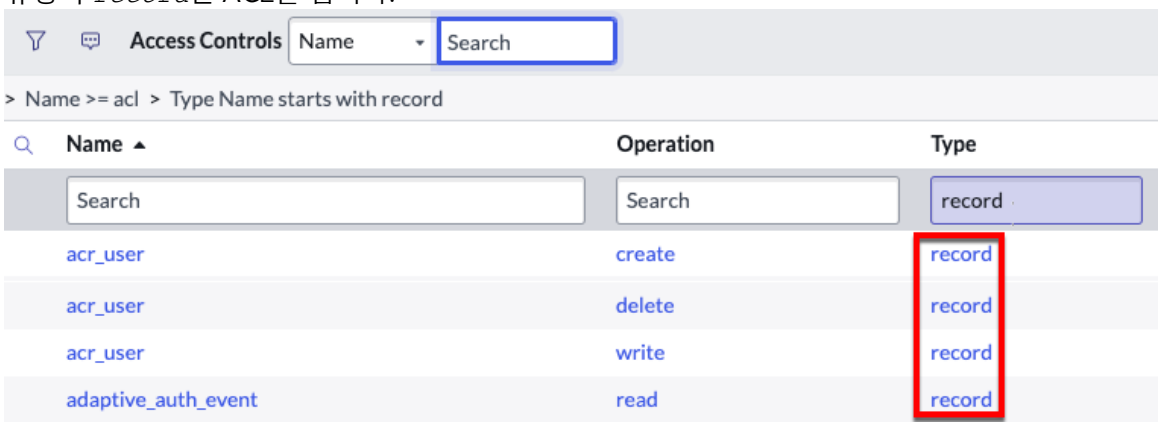
ACL 실행 계획 표시

관리자는 인스턴스의 모든 ACL에 대한 실행 계획을 보고 ACL이 서로 어떻게 관련되어 있는지 볼 수 있습니다.

시작하기 전에
필요한 역할: security_admin

프로시저

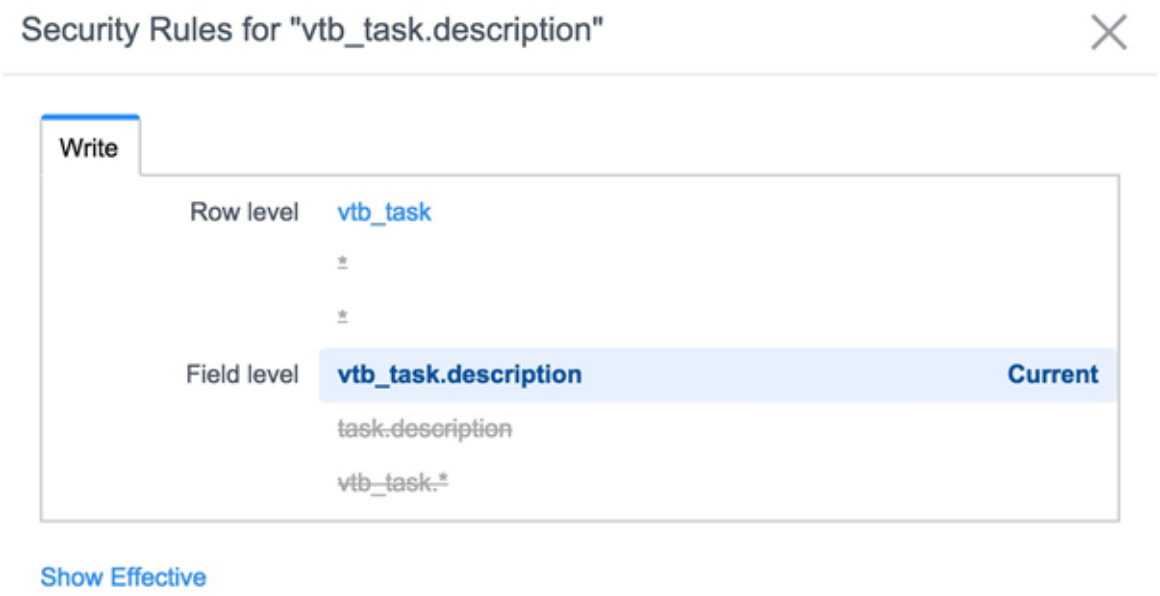
1. 권한 있는 역할로 상승.
2. 다음으로 이동 시스템 보안 > 접근 제어**(ACL)**.
3. 유형이 *record*인 ACL을 엽니다.



4. 관련 링크 섹션에서 **ACL** 실행 계획 표시를 클릭합니다.

   ACL에 대한 보안 규칙 창이 나타납니다. 이 예에서는 "vtb_task"에 대한 실행 계획을 표시합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



ACL 실행 계획 창

UI 항목	설명
제목	ACL의 이름입니다.
탭 이름	ACL이 생성, 읽기, 쓰기 또는 삭제인지 여부
행 수준	이 테이블에서 실행되는 행 수준 ACL입니다.
필드 수준	이 필드(또는 테이블의 열)에서만 실행되는 필드 수준 ACL입니다.

5. 모두 표시를 클릭하여 재정의된 ACL 및 모든 기록에 적용되는 일반 ACL을 포함한 모든 관련 ACL을 표시합니다.
   재정의된 ACL은 이름에 한 줄이 있고 일반 ACL에는 이름에 와일드카드 문자 별표(*)가 있습니다.
6. 현재 보고 있는 ACL과 관련된 바로 옆 ACL만 표시하고 **ACL** 테이블이 확장된 테이블의 ACL 및 일반 와일드카드(*) ACL을 숨깁니다.

ACL 구성 감시자 사용

security_admin 역할로 승격한 후 ACL 구성 감시자를 사용합니다.

시작하기 전에
필요한 역할: security_admin
권한 있는 역할로 상승

프로시저

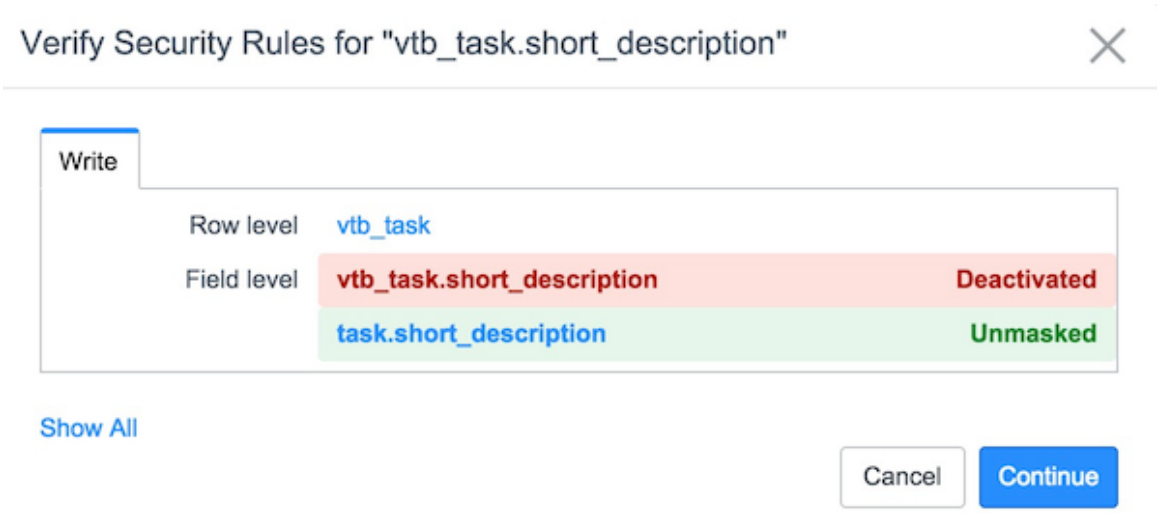
1. 기록 유형 ACL인 ACL을 엽니다.
2. ACL을 수정하거나 상황에 맞는 메뉴에서 삽입과 같은 옵션을 선택하는 등의 작업을 수행합니다.
3. 접근 제어 양식에서 값을 수정한 경우 헤더를 마우스 오른쪽 버튼으로 클릭하고 저장을 선택하거나 업데이트 또는 삭제를 클릭합니다.

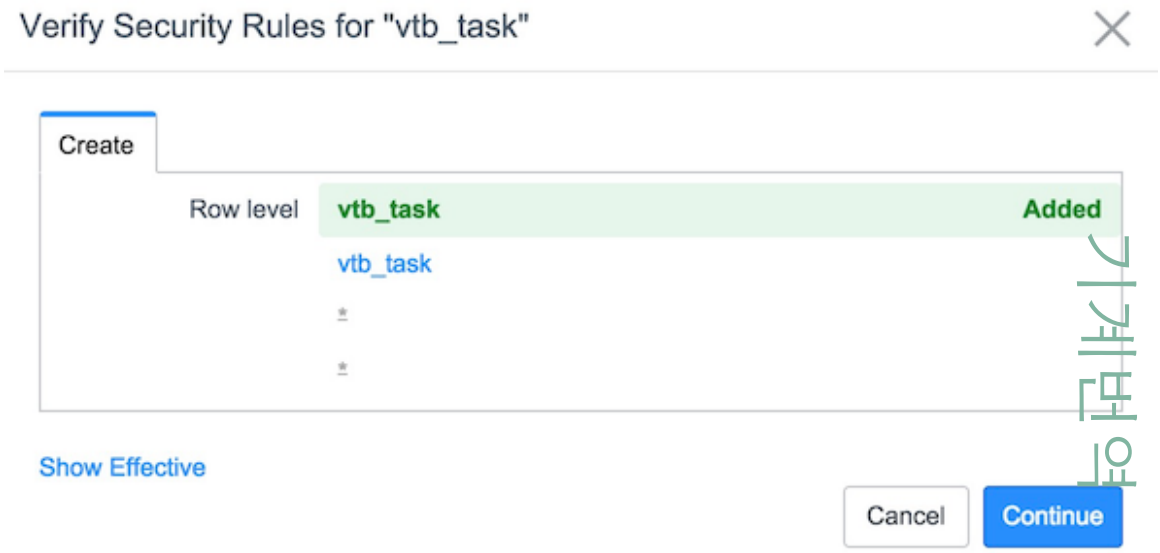
   보안 규칙 창이 나타납니다. 시스템이 ACL에서 데이터베이스 작업을 아직 수행하지 않았으므로 변경 내용이 아직 저장되지 않았습니다.

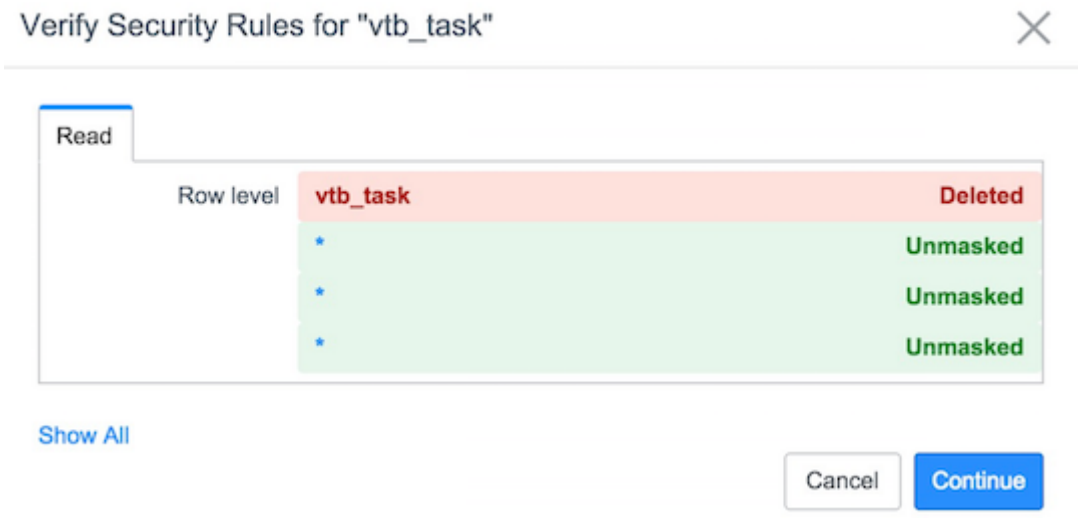
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

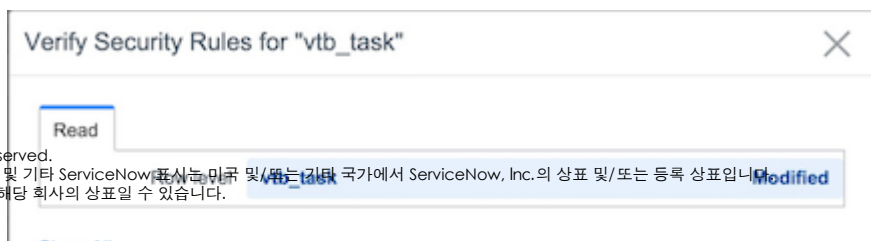
다음은 시각적 작업 보드 애플리케이션의 개인 작업 [vtb_task] 테이블에 있는 보안 규칙의 예입니다. 이 창의 항목에 대한 설명은 을 참조하십시오 ACL 구성 감시자 .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.









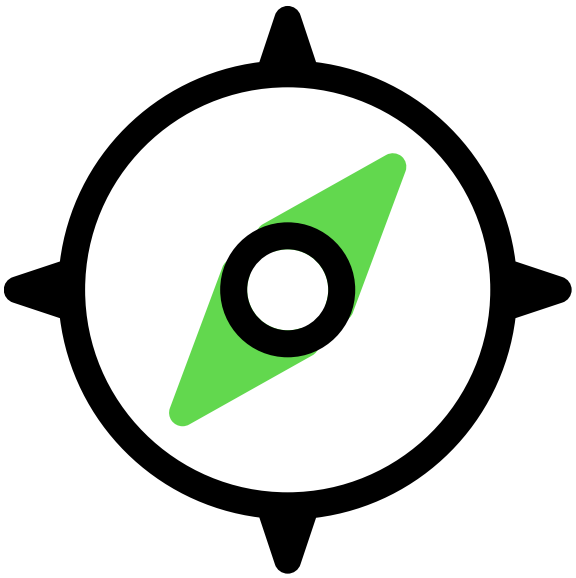
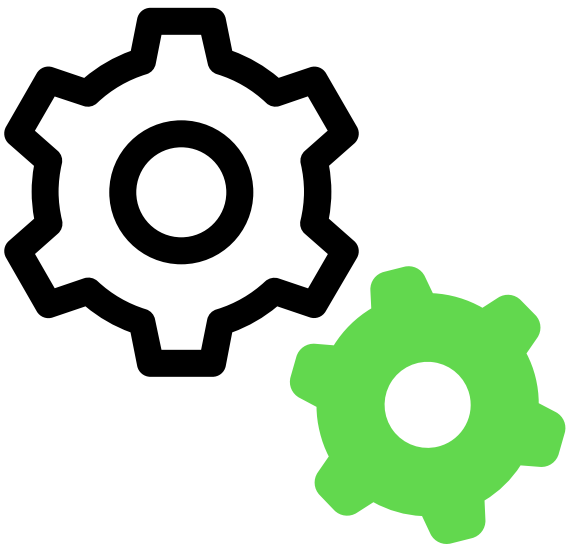
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 실행 계획과 마찬가지로 모두 표시를 클릭하여 재정의된 ACL 및 모든 레코드에 적용되는 일반 ACL을 포함한 모든 관련 ACL을 표시하거나 유효 표시를 클릭하여 보고 있는 ACL과 관련된 바로 옆에 있는 ACL만 표시할 수 있습니다.
5. 설명을 보려면 ACL 위에 마우스를 올려놓으십시오.

보안 속성

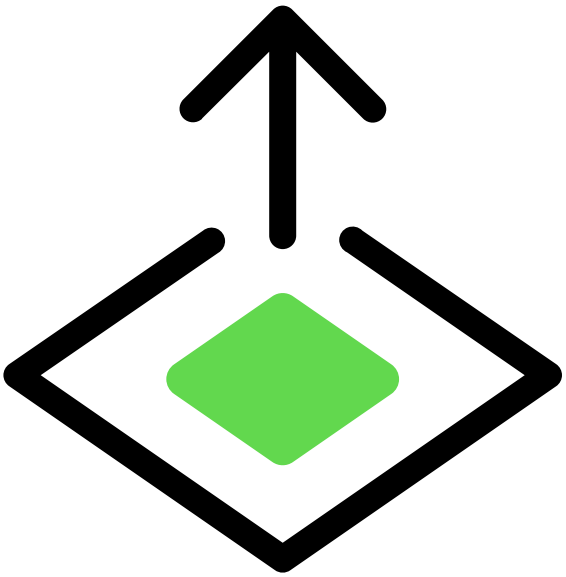
보안 속성은 접근 제어 목록에 대한 유연한 대안을 제공합니다.

시작하기

보안 속성 탐색	보안 속성 생성
	
보안 속성의 기본 사항 알아보기	새 보안 속성 생성

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OOB(바로 사용 가능) 보안 속성



OOB 보안 속성 설명

보안 속성 로깅



보안 속성 로깅 검토

보안 속성 기본

보안 속성은 주체 또는 해당 환경에 대한 구성 가능성이 높은 정보로, 액세스 제어에 사용될 때 복잡하지 않은 방식으로 세분화된 보안 구성을 가능하게 합니다.

개요

보안 속성은 역할 정의를 통해 현재 실행되는 ACL(액세스 제어 목록) 구성에 대한 액세스 제어를 위한 대체 방법을 제공합니다. 보안 속성은 ACL 기반 구성에 다음과 같은 몇 가지 이점을 제공합니다.

보안 강화

향상된 권한 평가 난독 처리로 조직의 보안을 유지할 수 있습니다.

사람이 읽을 수 있음

보안 속성은 보안 권한의 작성 및 사용 용이성을 단순화하도록 설계되었습니다.

유연한 보안

고객이 정의한 가상 사용자와 함께 바로 사용 가능한 구성에서 가상 사용자 정의를 빌드합니다.

로깅 및 감사

보안 속성은 자세한 감사 및 로깅을 제공하여 보안 조치 및 이론에 대한 더 많은 통찰력을 제공합니다.

보안 속성 생성

단계별 가이드로 새 보안 속성을 생성합니다.

시작하기 전에
필요한 역할: security_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 시스템 보안 > 보안 속성.
2. 보안 특성 목록에서 새로 만들기를 선택합니다.
3. 보안 속성 필드 양식에서 필드에 내용을 입력합니다.

보안 속성 필드

필드	설명
레이블	보안 속성의 레이블입니다.
이름	보안 속성의 이름입니다.
유형	보안 속성의 유형입니다. ◦ 화합물 주: 복합 보안 속성에 대한 자세한 내용은 다음을 참조하십시오. 복합 보안 속성 ◦ 정수 ◦ 목록 ◦ 문자열 ◦ 부울(예|아니오)
동적 여부	보안 속성 값을 각각마다 재평가해야 하는 경우
설명	보안 속성에 대해 사용자가 생성한 설명
애플리케이션	정적 필드, 애플리케이션 범위입니다.
조회 테이블	평가를 위해 외부 테이블을 참조합니다.
조회 테이블 열	평가를 위해 테이블 열을 참조합니다.
스크립트	스크립트에서 값을 파생시킵니다.

OOB(바로 사용 가능) 보안 속성

일반적으로 사용되는 일반화된 보안 속성 역할을 사용할 준비가 되었습니다.

개요

OOB(바로 사용 가능) 보안 속성은 미리 구성된 일련의 보안 속성 역할로 보안 속성의 기능을 사용하고 학습할 수 있는 쉬운 방법입니다. OOB 보안 속성 역할은 일반적으로 사용되는 접근 제어 역할입니다.

고유한 보안 속성을 만들거나 OOB 보안 속성 기능을 확장하려면 다음을 참조하십시오. 복합 보안 속성

OOB 보안 속성

속성	설명
그룹	사용자는 지정된 그룹의 구성원입니다.
GroupExplicit	사용자가 특정 그룹의 명시적 구성원입니다.
HasAdminRole	사용자에게 관리자 가상 사용자가 있음

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OOB 보안 속성

속성	설명
가장 중	사용자가 가장되었습니다.
대화형 세션	현재 대화형 세션
로그인됨	사용자가 로그인 및 인증됨
네트워크 기준	추가 네트워크 기준
역할	사용자에게 특정 역할이 있습니다.
RoleExplicit	사용자에게 명시적으로 정의된 특정 역할이 있습니다.

클라이언트 세션의 보안 속성

클라이언트 세션에 대해 다음 보안 속성이 추가됩니다(플러그인: `com.glide.client_session_security_attributes`).

- **IsIframeEmbeddedSession**: 이 특성은 외부 공급업체 포털의 포함된 iframe에 사용됩니다. 예를 들어 참여 메신저, 가상 에이전트 웹 클라이언트, 포함된 세션 등이 있습니다.
- **IsIntegrationAsAServiceSession**: 이 속성은 팀의 가상 에이전트, Slack의 가상 에이전트, whatapp의 가상 에이전트와 같은 메시징 앱에서 사용됩니다.
- **IsIntegrationAsAUserSession**: 이 특성은 통합 계정 사용자 또는 웹 서비스 사용자에게 사용됩니다.
- **ServiceNow** 웹 세션임: 이 속성은 모바일 대화형 세션에서 사용됩니다.
- 모바일 앱 세션 여부: **oauth_entity** 기록에서 **mobile_client** 속성이 true이면 속성이 사용됩니다.

비명시적 및 명시적 동작 설명

보안 속성은 역할 권한에 대한 명시적 대 비명시적(상속된) 평가를 통해 미묘한 권한 요구를 해결합니다.

복합 보안 속성

복합 보안 속성을 사용하면 비즈니스 요구에 맞는 일관되고 재사용 가능한 보안 속성 프로파일을 만들 수 있습니다.

개요

복합 보안 속성은 하나 이상의 기존 보안 속성에서 정의되어 권한 평가를 위한 보안 속성의 단일 참조 조합을 만듭니다.

복합 보안 속성 생성

쉽게 재사용할 수 있도록 복합 보안 속성을 생성합니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 다음으로 이동 시스템 보안 > 보안 속성.
2. 보안 특성 목록에서 새로 만들기를 선택합니다.
3. 유형 필드에서 ##을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 보안 속성 필드 양식에서 필드에 내용을 입력합니다.

보안 속성 필드

필드	설명
레이블	보안 속성의 레이블입니다.
이름	보안 속성의 이름입니다.
설명	보안 속성에 대해 사용자가 생성한 설명
조건	보안 속성 평가를 정의하는 데 사용되는 특정 보안 속성 조건입니다.
새 기준	평가를 위해 추가 **Or** 조건 세트를 추가합니다.

보안 속성 범위

보안 속성은 범위 지정 기능을 지원합니다.

보안 속성 범위 지정

보안 속성 범위가 지정된 동작은 플랫폼의 범위 지정 동작과 일치합니다. 범위 내에서 생성된 보안 속성은 동일한 범위의 액세스 제어에서만 사용할 수 있습니다.

로컬 및 기존 보안 속성

기존 및 로컬 보안 속성을 사용하면 고객이 보안 속성 조건 세트를 재사용할 수 있습니다.

로컬 및 기존 속성

고객은 ACL 보안 속성 조건 작성기를 사용하여 보안 속성이 기존 속성인지 로컬인지 지정할 수 있습니다.

주: 보안 속성 조건은 기본적으로 로컬로 설정됩니다.

로컬 정의 보안 속성은 생성된 단일 ACL에만 저장됩니다.

기존 옵션을 사용하면 사용자가 기존 보안 속성 조건을 조건 작성기에 참조할 수 있습니다.

필드 쿼리 역할 및 제한 사항

필드 쿼리 역할 및 필드 쿼리 제한속성을 사용하면 테이블에서 사용자가 사용할 수 있는 정보를 보다 효과적으로 제어할 수 있습니다.

개요

필드 쿼리 역할 및 필드 쿼리 제한 속성을 사용하면 사용자가 테이블에서 수행할 수 있는 작업을 보다 세부적으로 제어할 수 있습니다.

필드 쿼리 역할

사용자 역할에 따라 중요한 필드를 쿼리하지 못하게 차단합니다.

필드 쿼리 제한

해당 필드에 대한 액세스가 거부된 경우 기록에 대한 액세스를 제한합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드 쿼리 역할 구성

필드 쿼리 역할 속성을 활성화하고 구성하는 방법에 대해 알아봅니다.

시작하기 전에
필요한 역할: 관리자

프로시저
1. 다음으로 이동 모두 > 시스템 정의 > 테이블.
2. 테이블을 선택합니다.
3. 열 레이블을 선택하여 딕셔너리 항목을 봅니다.
4. 속성 탭을 선택합니다.
5. 팁: 필드 쿼리 역할 필드가 없으면 새로 만들기를 선택하여 하나 만듭니다

   필드 쿼리 역할 속성을 선택합니다.
6. 값의 이 테이블 열을 보는 데 필요한 역할을 입력하십시오.
7. 업데이트를 선택합니다.

결과
테이블 열은 필드 쿼리 역할 속성에 정의된 역할로만 쿼리할 수 있습니다. 정의된 역할이 없는 사용자가 테이블 열을 쿼리하면 작업에 대한 액세스가 거부됩니다.

필드 쿼리 제한 구성

필드 쿼리 제한을 구성하는 방법 알아보기

시작하기 전에
필요한 역할: 관리자

프로시저
1. 다음으로 이동 모두 > 시스템 정의 > 테이블.
2. 테이블을 선택합니다.
3. 열 레이블을 선택하여 딕셔너리 항목을 봅니다.
4. 속성 탭을 선택합니다.
5. 팁: 필드 쿼리 기록 접근 제한 필드가 없으면 새로 만들기를 선택하여 새로 만듭니다

   필드 쿼리 기록 접근 제한 속성을 선택합니다.
6. 필드를 볼 수 있는 사용자만 기록 액세스를 제한하려면 값 필드에 `true`를 입력하고, 그렇지 않으면 `false`를 입력합니다.
7. 업데이트를 선택합니다.

결과
테이블 열은 쿼리 결과를 제한합니다. 제한된 사용자에게는 쿼리가 반환된 결과 수가 표시되지만 추가 정보는 표시되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 필터링(레거시)

데이터 필터링을 사용하여 읽기 쿼리를 수행할 때 제목 속성을 기반으로 테이블 및 기록에 대한 액세스를 제어합니다.

데이터 필터링 살펴보기



데이터 필터링에 대해 자세히 알아보세요.

데이터 필터링 규칙 생성



필요에 맞게 고유한 데이터 필터링 규칙을 생성합니다.

데이터 디버그



데이터 필터링 결과를 디버그하는 방법을 알아보세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

⚠ 경고: Yokohama 릴리스부터 데이터 필터링은 향후 사용 중단 예정입니다. 이 항목은 숨겨지고 새 인스턴스에서 더 이상 활성화되지 않습니다.

데이터 필터링 탐색

데이터 필터링을 사용하여 읽기 쿼리를 수행할 때 제목 속성을 기반으로 테이블 및 기록에 대한 액세스를 제어합니다.

데이터 필터링은 인스턴스의 기존 접근 통제 규칙(ACL)과 함께 작동하도록 설계된 별도의 접근 제어 형식입니다. 데이터 필터링은 관리자가 정의한 제목 속성과 일치하지 않는 테이블 및 기록에 대한 접근을 거부합니다. 데이터 필터링은 감사, 보고 및 문제 해결을 더 쉽게 수행할 수 있도록 설계되었습니다.

관리자가 인스턴스에서 활성화할 수 있는 선택적 기능입니다.

데이터 필터링 기능

데이터 필터 데이터 필터를 사용하여 기록 내 정보를 기반으로 액세스 권한을 부여합니다. 데이터 필터는 테이블 필드의 데이터를 사용하여 사용자가 기록을 사용할 수 있는지 여부를 결정합니다.
제목 속성 기반 조건 작성기 제목 속성을 사용하여 사용자 역할, 그룹, 제목 기준 또는 IP 네트워크 주소를 평가합니다.
데이터 필터링은 거부 기반 모델을 사용합니다. 데이터 필터링은 거부 기반 모델을 사용하여 기록에 대한 액세스를 제어합니다. 데이터 필터링을 사용하면 기록이 데이터 필터링에 정의된 기준을 충족하지 않는 한 인스턴스가 기록에 대한 액세스를 거부합니다.
데이터 필터링 적용 데이터 필터링 규칙은 READ 작업에 대한 데이터베이스 쿼리 후에 실행되며 ACL 전에 평가됩니다. 데이터 필터링 규칙에 의해 거부된 기록은 진행되지 않으며 ACL 규칙에 의해 평가됩니다. • 데이터 필터링 규칙 적용은 READ ACL의 적용과 일치합니다. • ACL과 같은 데이터 필터링은 기존 *Report_view access control list* 동작과 함께 작동합니다. 이러한 보고서 통제 구성에 대한 자세한 내용은 Report_view 접근 제어를 참조하십시오.
세션 디버깅 데이터 필터링은 세션 디버깅을 지원합니다. 세션 디버깅을 사용하여 지정된 쿼리에 적용되는 데이터 필터링 기록을 확인합니다. 관리자는 이 정보를 사용하여 기록에 대한 사용자 액세스 문제를 해결할 수 있습니다.

데이터 필터링의 구성요소

데이터 필터링은 다음 기록 유형을 사용하여 작동합니다.

데이터 필터링 기록

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 필터링 [sys_df_data_filtration] 레코드를 생성하여 인스턴스에 대한 테이블 액세스 권한을 부여합니다. 데이터 필터링 기록에는 규칙의 범위와 영향을 받는 사용자를 제한하기 위해 위에서 설명한 데이터 필터 및 제목 속성 조건이 포함되어 있습니다.

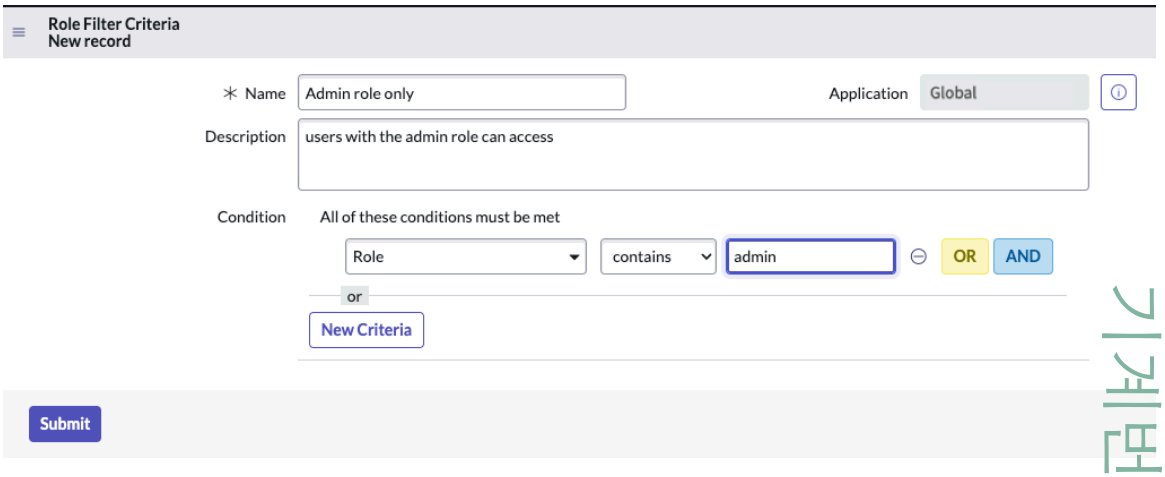
제목 기준 기록

제목 기준 [sys_df_subject_criteria] 기록은 데이터 필터링 규칙으로 액세스 권한을 부여할지 여부를 결정하는 데 사용할 수 있는 특정 사용자 속성을 나타냅니다. 이러한 속성은 사용자 그룹, 역할 또는 IP 주소일 수 있습니다. 제목 기준을 생성하려면 제목 기준 기록과 기준 입력 및 기준 조건 기록을 생성해야 합니다. 이 프로세스에 대한 자세한 내용은 제목 기준 생성 문서를 참조하십시오.

제목 기준 기록을 생성한 후 규칙에 적용할 수 있습니다. 이 작업은 데이터 필터링 규칙의 제목 조건 탭에서 수행됩니다.

기준 입력 기록 예시

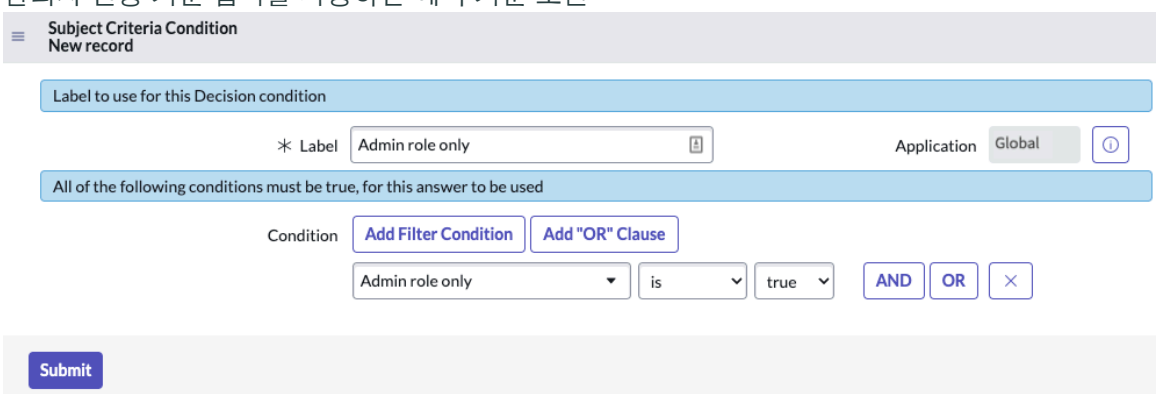
관리자를 포함하는 모든 역할에 대한 예시 기준 입력



기준 입력 [sys_df_subject_filter_criteria_m2m]은 사용자와 비교할 기준이 포함된 기록입니다. 사용자 그룹 또는 역할 목록, IP 주소 범위 또는 IP 주소 서브넷일 수 있습니다. 이러한 기록은 제목 기준 조건 기록과 함께 사용되어 사용자의 그룹, 역할 또는 IP 주소에 대해 평가하여 테이블 또는 해당 기록에 대한 액세스를 결정합니다.

제목 기준 조건 기록

관리자 전용 기준 입력을 사용하는 예시 기준 조건



제목 기준 조건 [sys_df_subject_criteria_condition] 기록을 사용하여 사용자 속성을 기준 입력에 정의된 역할, 그룹 또는 IP 주소와 비교하는 방법을 정의합니다. 단일 제목 기준 조건에서 여러 기준 입력을 사용하여 기록에 대한 액세스 범위를 더 좁힐 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 필터링 활성화

인스턴스에서 데이터 필터링을 활성화하는 방법에 대해 알아봅니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 시스템 정의 > 플러그인.
2. 검색 필드를 사용하여 데이터 필터링(com.glide.data_filtration) 플러그인을 찾습니다.
3. 설치를 클릭한 다음 플러그인 활성화 대화 상자에서 활성화를 클릭합니다.

데이터 필터링 규칙 생성

사용자에게 테이블에 대한 액세스 권한을 부여하는 데이터 필터링 규칙을 만드는 방법에 대해 알아봅니다.

시작하기 전에
필요한 역할: security_admin

> 주: 데이터 필터링 규칙을 만들거나 수정하려면 권한 있는 역할로 격상해야 합니다. 이 프로세스에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 데이터 필터링 > 데이터 필터링 기록.
2. 데이터 필터링 목록에서 새로 만들기를 클릭합니다.
   새 데이터 필터링 양식이 표시됩니다.
3. 양식의 필요에 따라 필드에 내용을 입력합니다.

데이터 필터링 양식

필드	설명
테이블	이 데이터 필터링 규칙이 적용되는 테이블입니다. 주: 유지 관리가 아닌 사용자는 일부 테이블에서 데이터 필터링을 만들 수 없습니다. 이 문제를 해결하려면 tableChoicesScript=DataFiltrationTableList 특성을 제거하지만 sys_df_xxx 테이블이나 sys_df_table_exclusion의 테이블에 필터가 만들어지지 않도록 합니다.
활성	데이터 필터링 규칙을 활성으로 설정합니다. 주: 의도치 않게 사용자를 기록에서 잠그지 않도록 테스트할 준비가 될 때까지 데이터 필터링 규칙을 비활성으로 유지합니다.
설명	데이터 필터링 규칙에 대한 설명입니다.
계단식	확장된 테이블에 적용할 데이터 필터링 규칙을 설정하려면 선택합니다. 예를 들어 Task[task] 테이블을 선택하고 계단식을 활성화합니다. 이 경우 데이터 필터링 규칙은 인시던트[incident] 및 변경 요청〔change_request〕과 같이

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	작업에서 확장된 모든 테이블에도 적용됩니다. 테이블 확장에 대한 자세한 내용은 다음을 참조하십시오. 테이블 확장 및 클래스 주: 이 필드는 기본적으로 활성화됩니다.

4. 옵션: 규칙의 범위를 좁히려면 필요에 따라 조건 필드를 채웁니다.

필드	설명
제목 조건	액세스하려면 모든 조건이 충족되어야 합니다.
보안 속성 조건	액세스하려면 모든 조건이 충족되어야 합니다. 로컬 이 속성은 데이터 필터링 규칙의 범위 내에서만 정의됩니다. 기존 이 속성은 이미 존재하는 보안 속성을 참조하여 정의됩니다.
데이터 조건	데이터가 규칙의 적용을 받는 조건을 정의합니다. 주: 빈 데이터 조건이 선택한 테이블의 모든 기록에 적용됩니다.

5. 양식 메뉴에서 저장을 선택합니다.
데이터 필터링 규칙을 저장한 후에는 데이터 조건에서 달리 지정하지 않는 한 이 규칙이 선택한 테이블의 모든 기록에 자동으로 적용됩니다.

데이터 필터링 규칙에 대한 데이터 필터 추가

선택적으로 데이터 필터를 사용하여 테이블의 특정 기록에만 적용되도록 데이터 필터링 규칙의 범위를 좁힐 수 있습니다.

시작하기 전에
필요한 역할: 관리자

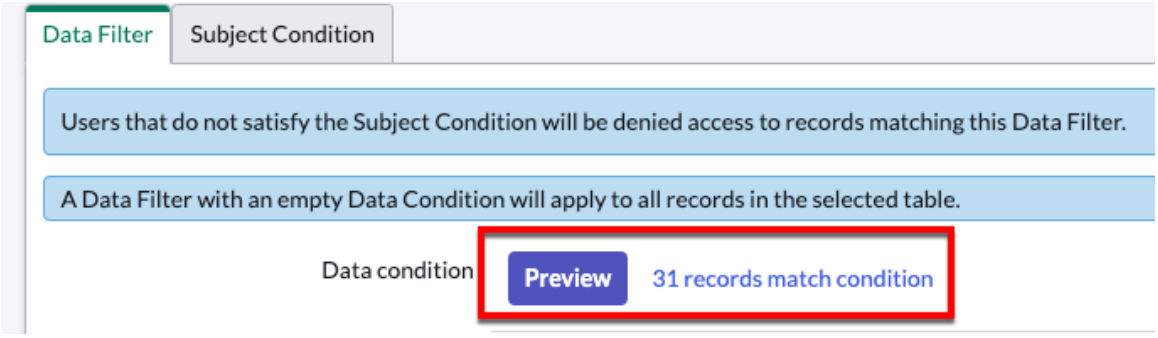
프로시저

1. 데이터 필터링 기록에서 데이터 필터 탭을 엽니다.
2. 조건 작성기를 사용하여 테이블 기록과 필드 값을 필터링합니다.
데이터 필터는 플랫폼의 다른 부분에서 사용되는 것과 동일한 조건 작성기를 사용합니다. 이 인터페이스 사용에 대한 자세한 내용은 조건 작성기 를 참조하십시오.

   중요사항: 데이터 필터 탭은 테이블 필드에서 테이블을 선택할 때까지 비어 있는 상태로 나타납니다.

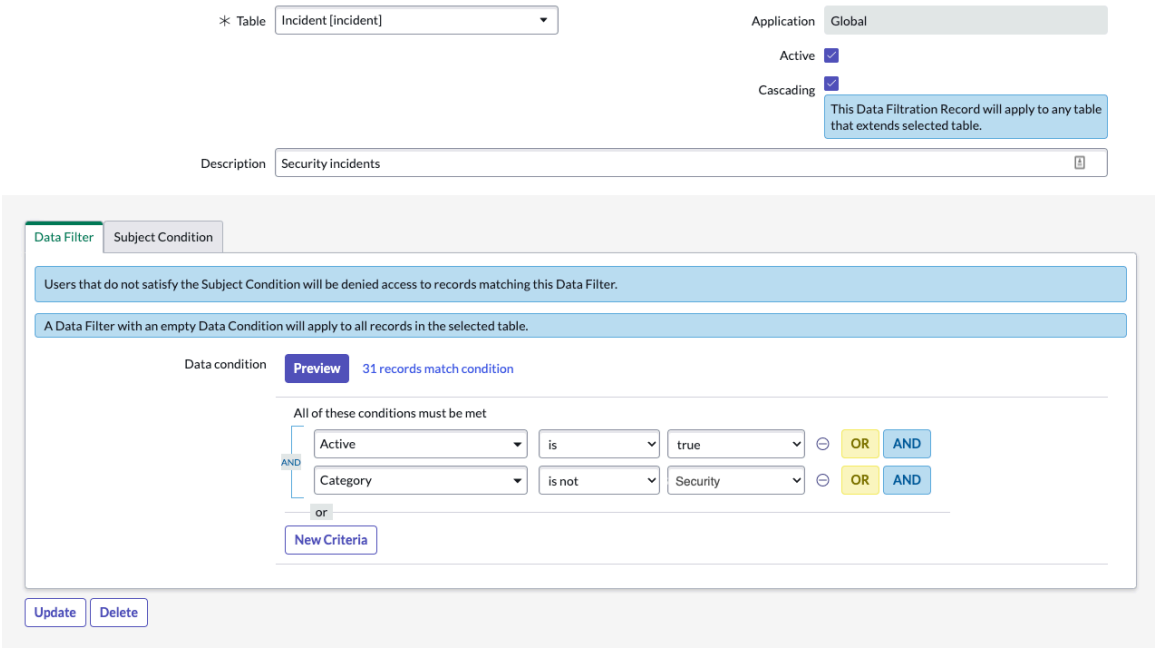
3. 미리 보기 버튼을 사용하여 데이터 필터와 일치하는 기록 수를 확인합니다.
4. 기록 수를 선택하여 일치하는 기록 목록을 엽니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



5. 저장을 선택합니다.

Example:
이 예에서는 Incident[incident] 테이블에 대한 데이터 필터링 규칙을 보여줍니다. 데이터 필터는 보안 범주에 없는 모든 활성 기록을 선택하도록 설정됩니다. 이 규칙을 활성화하면 사용자가 이러한 기록을 볼 수 있습니다. 기록 내용 이외의 기준을 추가로 사용하려면 아래 섹션을 참조하십시오.



중요사항:

조건에서 **not** 작업을 수행하면 인스턴스에서 사용하는 데이터베이스 유형에 따라 예기치 않은 결과가 반환될 수 있습니다. 예를 들어 다음 조건을 가정합니다.

이 조건의 경우 결과 세트는 회사가 `ServiceNow`가 아닌 모든 기록과 회사 필드에 값이 없는 모든 기록이 될 것으로 예상됩니다. MySQL 및 Maria 이외의 데이터베이스를 사용하는 인스턴스는 회사 필드가 비어 있는 값 레코드를 반환하지 않습니다. 이러한 인스턴스에 **not** 쿼리를 사용하는 경우 빈 값이 반환되도록 조건을 포함합니다.

데이터 필터링 규칙에 제목 속성 추가

필요에 따라 제목 속성을 사용하여 IP 네트워크 주소, 사용자 그룹 및 역할 또는 제목 기준과 같은 속성을 기반으로 데이터 필터링 규칙의 범위를 좁힐 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 데이터 필터링 기록에서 제목 기준 탭을 엽니다.
2. 조건 작성기를 사용하여 다음 기준 중 하나 이상을 기준으로 테이블 기록을 필터링합니다.

제목 기준 옵션

옵션	설명
네트워크 기준	네트워크 IP 범위 또는 IP 서브넷을 기준으로 기록에 액세스할 수 있습니다.
제목 기준	제목 기준에 따라 기록에 액세스할 수 있습니다. 제목 기준 기록을 선택하여 데이터 필터링 규칙에 해당 조건을 적용합니다. 제목 기준 기록 생성에 대한 자세한 내용은 다음 문서를 참조하십시오 제목 기준 생성.
제목 그룹	사용자가 특정 그룹의 구성원인 경우 액세스를 허용합니다. 그룹[sys_user_group] 테이블에서 그룹을 선택합니다.
대상 역할	사용자가 특정 그룹의 구성원인 경우 액세스를 허용합니다. 역할[sys_user_role] 테이블에서 그룹을 선택합니다.

중요사항: 제목 기준 조건은 **is** 연산자만 지원합니다.

3. 제목 기준을 추가한 후 저장을 클릭합니다.

제목 기준 생성

데이터 필터링 규칙에 사용할 제목 기준 기록을 생성합니다.

시작하기 전에
필요한 역할: security_admin

중요사항: 데이터 필터링 규칙을 만들거나 수정하려면 권한 있는 역할로 격상해야 합니다. 이 프로세스에 대한 자세한 내용은 권한 있는 역할로 상승을 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 데이터 필터링 > 제목 기준.
2. 제목 기준 목록에서 새로 만들기 버튼을 클릭합니다.
   새 주제 기준 양식이 표시됩니다.
3. 양식의 필요에 따라 필드에 내용을 입력합니다.

제목 기준 필드

필드	설명
이름	제목 기준의 이름입니다.
애플리케이션	제목 기준에 대해 범위가 지정된 애플리케이션입니다. 이 필드는 읽기 전용이며 현재 범위가 지정된 애플리케이션으로 자동으로 채워집니다.
설명	제목 기준에 대한 설명입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 양식 헤더를 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 저장을 클릭합니다.
   저장하면 기준 입력 및 기준 조건 필드가 나타납니다.

제목 기준 입력 생성

제목 기준 입력을 생성하여 데이터 필터링 규칙이 필터링하는 기준을 정의합니다.

시작하기 전에

필요한 역할: security_admin

프로시저

1. 제목 기준 기록에서 기준 입력 탭을 엽니다.
2. 조건 입력 목록에서 새로 만들기를 클릭합니다.
3. 생성하려는 기준에 대한 정책 입력을 선택합니다.

정책 입력

정책 입력	설명
IP 필터 기준	IP 주소를 기준으로 정책 입력 작성
역할 필터 기준	사용 역할에 따라 정책 입력 만들기
그룹 필터 기준	사용자 그룹을 기반으로 정책 입력 작성

이 단계에서 선택한 항목에 따라 **IP** 필터 기준, 역할 필터 기준 또는 그룹 필터 기준 양식이 표시됩니다.

4. 필터 기준 양식에서 필요에 따라 필드에 내용을 입력합니다.

필터 기준 필드

필드	설명
이름	필터 기준의 이름
애플리케이션	제목 기준에 대해 범위가 지정된 애플리케이션입니다. 이 필드는 읽기 전용이며 현재 범위가 지정된 애플리케이션으로 자동으로 채워집니다.
설명	필터 기준 설명

5. 양식 필드 아래에는 필터 기준 입력에 대한 IP 주소, 그룹 또는 역할을 정의하는 데 사용되는 탭이 있습니다.

특정 입력 유형에 대한 필터 기준 필드

정책 입력 유형	설명	작성
IP 필터 기준	IP 주소의 범위 또는 서브넷을 작성하기 위한 사용자 IP 필터 기준입니다. 그런 다음 제목 기준을 이 범위 또는 서브넷에 대해 사용자의 IP 주소와 비교할 수 있습니다.	**IP** 범위 또는 서브넷**(CIDR)**을 사용하여 입력에 대한 IP 주소를 정의합니다. IP 범위 **IP** 범위 목록에서 새 행 삽입을 두 번 클릭하고 시작 **IP**에 시작 IP 주소를 입력합니다. 그런 다음

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

정책 입력 유형	설명	작성
		Tab 키를 누르고 끝 **IP** 필드에 끝 IP 주소를 입력합니다. 마지막으로 Enter 키를 눌러 목록 항목을 저장합니다. 서브넷(CIDR) 서브넷 목록에서 새 행 삽입을 두 번 클릭하고 네트워크 **IP** 필드에 네트워크 IP를 입력합니다. 그런 다음 Tab 키를 누르고 넷마스크 필드에 넷마스크를 입력합니다. 마지막으로 Enter 키를 눌러 목록 항목을 저장합니다. 주: 스케줄러에 의해 트리거되는 예약된 작업은 요청 클라이언트 IP의 컨텍스트가 없으므로 네트워크 기준을 사용하여 데이터를 필터링하기 위한 것이 아닙니다. 더 적절한 여과 유형은 역할/그룹 대상 조건일 수 있습니다.
역할 필터 기준	역할 필터 기준을 사용하여 선택한 역할을 생성합니다. 그런 다음 제목 기준을 이 선택 항목에 대해 사용자에게 할당된 역할과 비교할 수 있습니다.	조건 필드의 조건 작성기를 사용하여 입력에 대한 역할을 선택합니다.
그룹 필터 기준	그룹 필터 기준을 사용하여 선택한 사용자 그룹을 생성합니다. 그런 다음 제목 기준을 이 선택 항목에 대해 사용자에게 할당된 그룹과 비교할 수 있습니다.	기준 그룹 테이블에서 새 행 삽입을 두 번 클릭하고 사용자 그룹을 선택합니다. Enter 키를 누르거나 녹색 확인 표시 아이콘을 클릭하여 그룹을 저장합니다. 첫 번째 항목 아래에 새 행 삽입**(Insert a new row)** 텍스트를 클릭하여 추가 항목을 생성합니다.

6. 입력을 정의한 후 제출을 클릭합니다.

주: 제목 기준에 대한 기준 입력을 생성하는 것 외에도 기존 입력을 추가할 수도 있습니다. 기준 입력 탭에서 편집을 클릭하고 기존 입력에서 선택합니다.

제목 기준 조건 생성

사용자 정보를 기존 제목 기준 입력과 비교하는 조건을 만듭니다.

시작하기 전에
필요한 역할: security_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기준 조건은 사용자 속성을 기존 기준 입력과 비교하여 기록에 대한 액세스를 허용할지 여부를 결정합니다. 기준 조건을 생성하려면 제목 기준을 생성해야 합니다. 해당 프로세스에 대한 자세한 내용은 제목 기준 입력 생성를 참조하십시오.

프로시저

1. 제목 기준 기록에서 기준 조건 탭을 엽니다.
2. 조건 목록에서 새로 만들기를 클릭합니다.
3. 제목 기준 조건 양식에서 필요에 따라 필드에 내용을 입력합니다.

제목 기준 조건 양식

필드	설명
레이블	조건에 대한 설명이 포함된 레이블
애플리케이션	제목 기준에 대해 범위가 지정된 애플리케이션입니다. 이 필드는 읽기 전용이며 현재 범위가 지정된 애플리케이션으로 자동으로 채워집니다.

4. 다음 조건 옵션에서 선택하여 조건 작성기를 사용하여 제목 기준 조건에 대한 조건을 생성합니다. 이러한 조건 옵션에는 생성한 모든 제목 기준 입력이 포함됩니다.
5. 옵션: 필터 조건 추가 또는 **"OR"** 절 추가 버튼을 클릭하여 더 많은 조건을 생성합니다.

   주: 조건이 **OR** 절로 구분되지 않는 한 모든 조건이 true로 평가되어야 대상 기준 조건이 true로 평가됩니다.

6. 제출을 클릭하여 제목 기준 조건을 저장합니다.

다음에 수행할 작업

데이터 필터링 규칙의 제목 기준을 사용하여 테이블 및 기록에 대한 액세스를 제한합니다. 데이터 필터링 규칙에서 제목 기준을 사용하는 방법에 대한 자세한 내용은 문서를 참조하십시오 제목 기준 생성.

데이터 필터링 디버깅

세션 로그를 사용하여 데이터 필터링이 기록에 어떤 영향을 미치는지 확인하고 사용자 액세스 문제를 디버깅합니다.

시작하기 전에

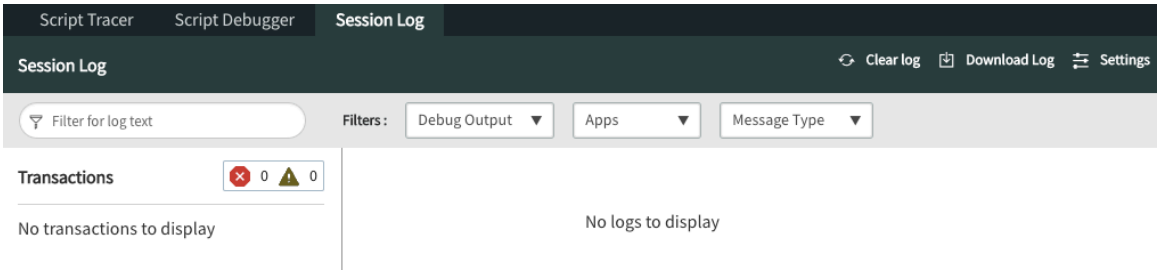
필요한 역할: 관리자

출력 정보는 사용자가 기록에 액세스할 때 세션 로그에 나타납니다. 이 로깅 정보를 가장과 함께 사용하면 사용자가 기록을 보거나 못하는 이유를 파악할 수 있습니다. 그런 다음 해당 정보를 사용하여 데이터 필터링 규칙을 조정하고 사용자가 의도한 내용만 볼 수 있도록 할 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 디버깅 > 모든 보안 디버그.
   스크립트 디버거가 새 브라우저 탭이나 창에서 열립니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



2. 스크립트 디버거 창에서 세션 로그 탭을 선택합니다.
3. 다른 브라우저 탭이나 창에서 사용자를 가장하여 해당 사용자의 액세스 문제를 해결합니다.

   주: 가장을 사용하면 관리자가 다른 사용자 설정 및 액세스 권한이 있는 인스턴스를 볼 수 있습니다. 다른 사용자로 전환에 관한 자세한 내용은 다른 사용자로 전환을 참고하세요.

4. 다른 사용자로 전환하는 동안 예기치 않은 동작이 표시되는 목록이나 기록에 액세스합니다.
   이 동작은 사용자에게 표시되지만 확인해서는 안 되는 기록 또는 사용자에게 예상대로 표시되지 않는 기록 목록일 수 있습니다.
   가장된 사용자로 레코드에 액세스한 후 세션 디버거에 출력이 표시되기 시작해야 합니다.
5. 세션 디버거에서 데이터 필터링 정보를 찾습니다.



   이 예에서는 데이터 필터가 레코드에 대한 액세스를 거부한 두 개의 로그 메시지를 보여 줍니다. 로그 항목은 빨간색 텍스트로 나타나며 데이터 필터의 액세스 거부 이유와 데이터 필터의 sys_id 포함합니다. 이 sys_id 클릭하여 데이터 필터링 기록을 열 수 있습니다.



   이 예는 데이터 필터가 기록에 대한 액세스를 허용한 로그 메시지를 보여줍니다. 이러한 로그 항목은 녹색 텍스트로 나타납니다. 첫 번째 메시지와 마찬가지로 이 sys_id 클릭하여 데이터 필터링 기록을 열 수 있습니다.

6. 이 정보를 사용하여 데이터 필터링 규칙을 조정합니다.
   이 단계를 반복하여 규칙을 구체화하고 사용자에게 필요한 액세스 권한을 부여합니다.

데이터 필터 베스트 프랙티스

테스트용 스텁 문서

테스트용 스텁 문서

보안 데이터 필터

보안 데이터 필터는 역할 또는 보안 속성 관련 어설션을 기준으로 기록에 대한 액세스를 제한합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 데이터 필터 탐색

보안 데이터 필터를 사용하면 사용자 역할 또는 기타 보안 속성 관련 어설션을 기준으로 기록에 대한 액세스를 제한할 수 있습니다. 보안 데이터 필터는 데이터 액세스 방식에 관계없이 권한 있는 사용자만 기록을 볼 수 있도록 합니다.

보안 데이터 필터는 쿼리가 실행되기 전에 적용되므로 제한된 데이터가 데이터베이스를 벗어나지 않습니다. 반면 조건부 ACL은 쿼리가 실행된 후 데이터를 필터링하여 데이터가 유출될 수 있습니다.

주: 보안 데이터 필터와 거부-미포함 ACL 페어링하여 일관된 보안을 보장합니다.

보안 데이터 필터의 기능

보안 데이터 필터의 주요 기능은 다음과 같습니다.

- 보안 데이터 필터는 쿼리 내에서 적용됩니다.
- 보안 데이터 필터 조건 # 대상 테이블의 쿼리에 대한 조건과 상호 작용합니다.
- 보안 데이터 필터는 `canRead`에 의해 확인되지 않습니다. 자세한 내용은 다음을 참조하십시오 보안 데이터 필터를 사용하는 경우 .
- 데이터 필터 범위 지정 규칙은 테이블의 범위를 기반으로 하며, 데이터 필터는 ScopeMaster 또는 sys_scope 범위 규칙을 따르지 않습니다.

보안 데이터 필터 애플리케이션 및 적용

일반적으로 보안 데이터 필터는 절대 ACL(테이블 수준 ACL이라고도 함) 뒤와 행 ACL 뒤에 적용됩니다. 보안 데이터 필터는 기본적으로 적용되며 신중하게 사용하지 않을 경우 시스템 동작에 영향을 미칩니다. 기본 보안 데이터 필터 목록은 을 참조하십시오 기본 보안 필터 .

보안 데이터 필터는 기본적으로 GlideRecordSecure, GlideRecordSandbox 및 GlideAggregateSandbox 쿼리에만 적용됩니다. Java 및 서버 측 스크립트에서 특정 쿼리에 대한 데이터 필터를 활성화하거나 비활성화하는 데 사용할 수 있는 두 가지 새로운 GlideRecord API인 `enableSecurityFeature` 및 `disableSecurityFeature`가 있습니다.

중요사항: GlideRecordSecure를 사용하지 않는 사용자용 쿼리에 대해 데이터 필터를 명시적으로 활성화해야 합니다.

보안 데이터 필터를 사용하는 경우

보안 데이터 필터는 다음에 가장 적합합니다.

- 민감한 데이터가 데이터베이스를 벗어나지 않도록 방지
- "보안으로 숨겨진 행" 메시지 표시 안 함
- 보고서를 통해 민감한 데이터가 유출되지 않도록 방지

보안 데이터 필터를 사용하지 않는 경우

보안 데이터 필터는 다음과 같이 사용하면 안 됩니다.

- 가시성 제어로
- ACL의 대체로
- 많은 수의 필터 조건이 있는 경우
- 인덱싱되지 않은 열에서

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 데이터 필터 동작

AND가 피연산자를 결합하는 것처럼 여러 보안 데이터 필터가 평가를 위해 함께 결합됩니다. 예를 들어 다음과 같은 세 가지 보안 데이터 필터가 있습니다.

- 필터 1: 'active=true
- 필터 2: `priority=1`
- 필터 3: `state=open`

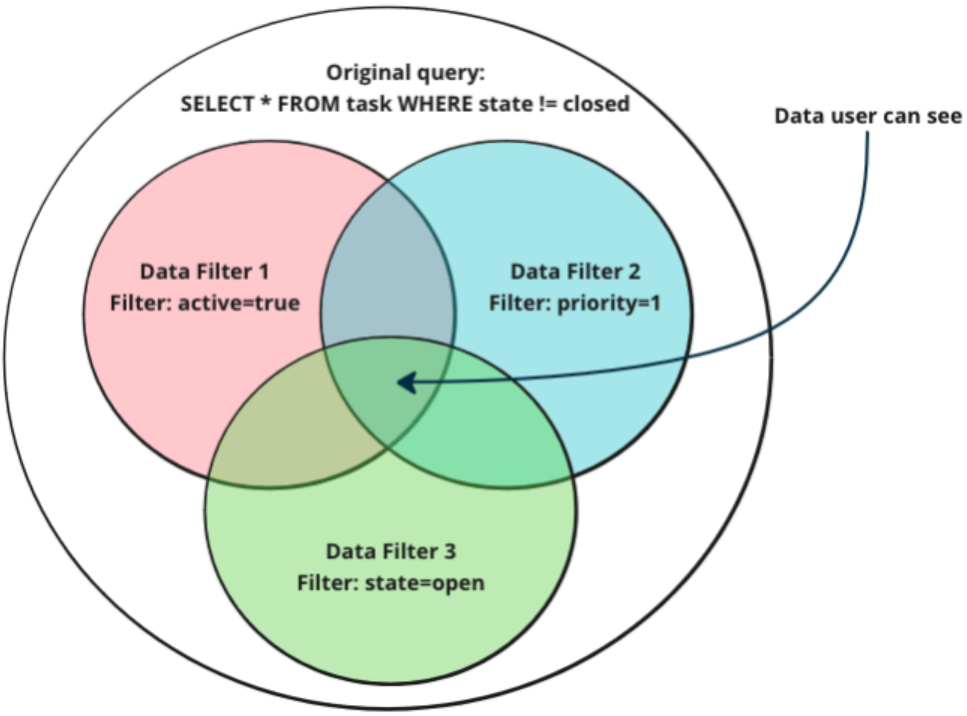
그리고 초기 쿼리 :

```
SELECT * FROM task WHERE state != closed AND active = true AND
        priority = 1
```

마지막 쿼리는 다음과 같습니다.

```
SELECT * FROM task WHERE state != closed
        AND active = true AND priority = 1 AND state = open
```

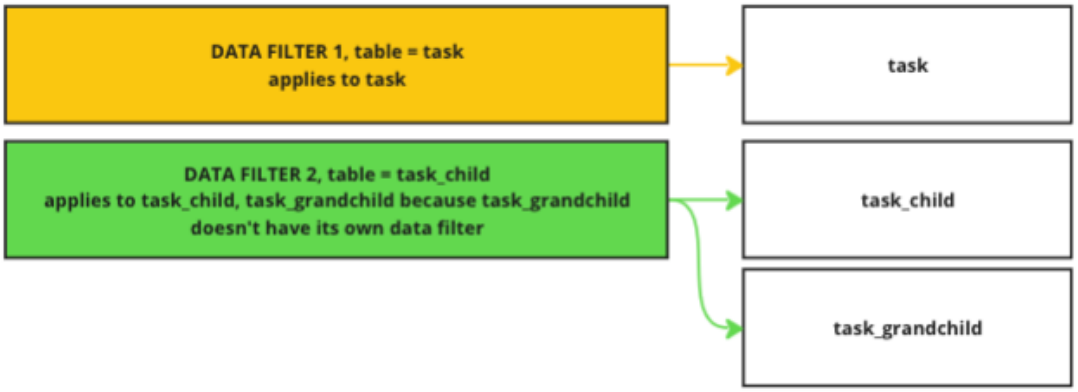
이 예제의 시각적 표현은 아래 다이어그램을 참조하십시오.



보안 데이터 필터와 ACL이 적용되는 방식에서 한 가지 중요한 차이점은 상위 테이블에서 데이터를 쿼리할 때 하위 테이블의 데이터 필터가 상위 테이블에 적용되지 않는다는 것입니다. 하위 테이블과 상위 테이블 모두에 데이터 필터를 추가하여 상위 테이블의

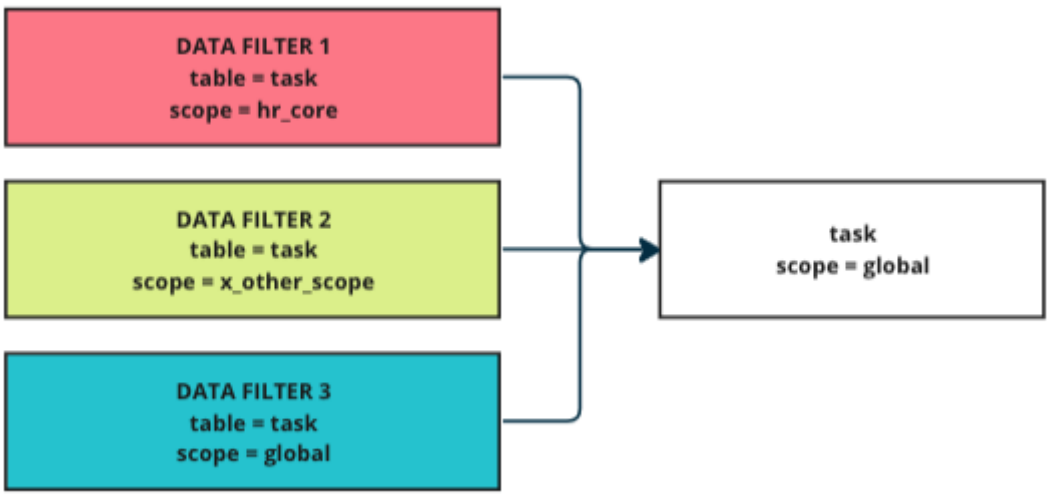
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

기록에 대한 액세스를 제한합니다. 아래 다이어그램은 계층 구조를 강조 표시합니다.



주: 이에 대한 일반적인 해결 방법은 상위 테이블에서 하위 기록을 완전히 숨기는 상위에 데이터 필터를 추가하는 것입니다.

데이터 필터는 ACL과 유사한 범위 지정 규칙으로 적용되지만,
데이터 필터가 쿼리 전에 적용되기 때문에 몇 가지 주요 차이점이



있습니다.

보안 데이터 필터 생성

사용자에게 테이블에 대한 액세스 권한을 부여하는 보안 데이터 필터 규칙을 만드는 방법에 대해 알아봅니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > 보안 데이터 필터.
2. 보안 데이터 필터 목록에서 새로 만들기를 클릭합니다.
3. 양식의 필요에 따라 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

데이터 필터링 양식

필드	설명
테이블 이름	보안 데이터 필터가 적용되는 테이블입니다.
설명	보안 데이터 필터 규칙에 대한 설명입니다.
활성	보안 데이터 필터 규칙을 활성으로 설정합니다. 주: 의도치 않게 사용자를 기록에서 잠그지 않도록 테스트할 준비가 될 때까지 보안 데이터 필터 규칙을 비활성으로 유지합니다.
UI에 표시	보안 데이터 필터가 쿼리에 적용되는 경우 UI에 알림을 표시할지 여부를 결정합니다.
애플리케이션	보안 데이터 필터의 애플리케이션 범위입니다.
모드	데이터 필터의 모드입니다.
필터	데이터 필터가 적용되는 기록을 결정하는 필터 조건
보안 속성	데이터 필터의 적용 여부를 제어하는 보안 속성

4. 양식 메뉴에서 저장을 선택합니다.

결과
보안 데이터 필터 규칙을 저장한 후에는 데이터 조건에서 달리 지정하지 않는 한 이 규칙이 선택한 테이블의 모든 기록에 자동으로 적용됩니다.

기본 보안 필터

일반적으로 데이터 필터는 절대 ACL(테이블 수준 ACL이라고도 함) 뒤와 행 수준 ACL 뒤에 적용됩니다. 이는 기본적으로 적용되며 신중하게 사용하지 않으면 시스템 동작에 영향을 줄 수 있습니다.

기본 적용된 보안 데이터 필터

보안 데이터 필터는 기본적으로 다음 위치에 적용됩니다.

범주	애플리케이션
목록 및 양식	• UI16 • 작업 공간 • 서비스 카탈로그 • 서비스 포털 • 모바일
보고서 및 대시보드	• 레거시 대시보드 • 현대식 대시보드

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

범주	애플리케이션
데이터 익스포트	• XML 익스포트 • CSV • Excel • JSON • PDF
플로우 엔진	기록 조회 단계
검색	• AI 검색 • 텍스트 검색
GlideRecord	• GlideRecordSecure • GlideRecordSandbox • GlideAggregateSandbox
REST 및 GraphQL API	• REST 테이블 API • REST 통계 API • GraphQL 테이블 및 통계 API와 상응하는 항목

보안 역할

보안 역할은 추가 보안을 제공하며, 인스턴스가 내부 및 외부 사용자를 구분할 수 있도록 모든 사용자에게 하나 이상의 역할이 있어야 합니다.

명시적 역할 탐색



상승된 권한 탐색



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

명시적 역할의 주요 기능 및 비즈니스 가치에 대해 알아봅니다.

상승된 권한 역할이 세션 기반 권한을 사용하도록 설정하는 방법을 알아봅니다.

명시적 역할

내부 사용자와 외부 사용자 모두에게 인스턴스에 액세스할 수 있도록 권한을 부여할 수 있습니다. 그러나 두 유형의 사용자가 모두 같은 수준의 액세스 권한을 갖는 것을 원하지 않을 수도 있습니다. 추가 보안을 제공하려면 인스턴스에서 내부 및 외부 사용자를 구분할 수 있도록 모든 사용자에게 적어도 하나의 역할이 있어야 합니다.

Paris 릴리스에서는 사용자가 명시적 역할(snc_internal 및 snc_external)을 모두 사용할 수 없습니다. 그룹 및 역할 포함에는 두 역할을 모두 포함할 수 없습니다. 이는 이러한 그룹이나 역할에 할당된 그룹 구성원 또는 사용자가 자동으로 두 역할을 가질 수 있기 때문입니다. Now Platform에서는 이러한 시나리오를 생성하는 모든 운영을 중단합니다.

외부 사용자는 최소한 snc_external 역할을 얻어야 합니다. snc_external 역할은 사용자가 조직 외부에 있다는 것을 나타냅니다. ACL을 통해 snc_external 역할을 상속하는 추가 역할 또는 snc_external 역할을 명시적으로 허락받지 않는 한, 자원에 대한 액세스 권한을 가질 수 없습니다. 기본적으로 snc_external 역할이 있는 사용자는 다음에 접근할 수 없습니다.

- external로 표시되지 않은 스크립팅된 REST API 자원입니다.
- snc_external 역할이나 public 역할을 상속하는 역할이 없는 테이블
- snc_external 역할 또는 snc_external 역할을 상속하는 역할에 접근 권한을 부여하지 않는 프로세서, UI 페이지와 같은 기록이 아닌 형식의 자원.
- 플랫폼 분석 대시보드.

snc_internal 역할을 상승된 것으로 표시하지 마십시오. 표시할 경우 내부 사용자가 인스턴스에 액세스할 수 없습니다.

Explicit Roles 플러그인

Explicit Roles 플러그인이 활성화되는 경우:

- 모든 사용자가 내부 자원에 액세스하려면 snc_internal 역할을 가지고 있거나 외부 자원에 액세스하려면 snc_external 역할을 가지고 있어야 합니다. 위의 명시적인 역할 중 하나라도 없는 사용자는 public 자원에만 액세스할 수 있습니다.
- 기존의 모든 사용자에게는 snc_internal 역할이 자동으로 할당됩니다. 이 역할은 기존 액세스 수준이나 시스템 동작을 변경하지 않습니다. 대신 외부 사용자와 내부 사용자를 구분할 수 있는 범주를 제공합니다. 모든 내부 사용자는 플러그인이 활성화되기 전과 동일한 수준의 액세스 권한을 유지합니다.

  팁: 사용자가 기존 기능을 변경하지 못하도록 하려면, Explicit Roles 플러그인을 활성화하여 인스턴스의 모든 기존 사용자에게 snc_internal 사용자 역할을 할당합니다. 여기에는 Explicit Roles 플러그인을 활성화하기 전에 추가된 모든 외부 사용자가 포함됩니다. Explicit Roles 플러그인이 활성화된 후에는 Explicit Roles 플러그인이 활성화되기 전에 추가된 모든 외부 사용자에 대해 다음을 수행합니다.

  - snc_internal 역할을 제거합니다.
  - snc_external 역할을 추가합니다.

  이전 작업을 수행하면 Explicit Roles 플러그인을 활성화하기 전에 추가한 외부 사용자는 내부 사용자만 사용할 수 있는 내부 자원에 액세스할 수 없습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 새로 만든 사용자가 snc_external 역할을 명시적으로 할당받지 않는 한, 처음 인스턴스에 로그인할 때 자동으로 snc_internal 역할이 할당됩니다. 새 사용자가 처음 인스턴스에 로그인하기 전에 새 사용자에게 snc_external 역할을 추가하여 외부 사용자 권한을 제공할 수 있습니다.

  중요사항:

  유지관리 기간 동안 또는 로그인한 사용자가 거의 없는 경우 이 플러그인을 활성화합니다. 플러그인이 활성화됐을 때 로그인한 상태의 사용자에게는 snc_internal 역할이 동적으로 할당되지 않습니다. 로그아웃했다가 다시 로그인했을 때 사용자는 snc_internal 역할을 할당받을 수 있습니다. 플러그인이 활성화되면 언제든지 snc_internal 및 snc_external 역할을 추가하거나 제거하여 사용자 권한을 변경할 수 있습니다.

  플러그인이 활성화되면 사용자가 로그인할 때마다 계정에 해당 역할 또는 snc_external 역할이 없는 경우 사용자에게 snc_internal 역할이 부여됩니다. 여기에는 가장을 통해 로그인한 사용자가 포함됩니다.

- 필요한 역할이 없는 기존의 모든 ACL에는 snc_internal 역할이 자동으로 할당됩니다. 기존의 ACL과 사용자 모두 snc_internal 역할이 할당되었기 때문에 기존 액세스 수준은 변경되지 않습니다.
- 필요한 역할이 없는 새로 만든 ACL에는 snc_internal 역할이 자동으로 할당됩니다. 역할이 할당된 새로 만든 ACL에는 이 역할 할당이 적용되지 않습니다.
- 모든 기존 프로세서[sys_processor] 기록 또는 **Type=script**를 사용하여 새롭게 생성된 프로세서[sys_processor] 기록의 경우, 필드가 비어 있으면 snc_internal 역할이 자동으로 역할 필드에 추가됩니다.
- UI 페이지에 대한 액세스를 내부 사용자로 제한하기 위해 플러그인에서 snc_internal 역할을 ***ui_page** 유형의 ACL로 자동 할당합니다.
- 프로세서에 대한 액세스를 내부 사용자로 제한하기 위해 플러그인에서 snc_internal 역할을 ***processor** 유형의 ACL로 자동 할당합니다.
- 외부 사용자는 최소한 snc_external 역할을 얻어야 인스턴스에 액세스할 수 있습니다. 이 역할은 외부 사용자에게 수동으로 부여해야 합니다. 레코드에 대한 액세스는 ACL을 통해 부여됩니다.

Explicit Roles 플러그인이 활성화되거나 활성화되지 않은 인스턴스 간에 시스템 업데이트 세트를 이동하지 마십시오. 자세한 내용은 시스템 업데이트 세트 를 참조하십시오.

주: 이 플러그인을 사용하려면 상황별 보안 관리자 플러그인도 필요합니다.

glide.security.explicit_roles.do_not_fix 동작

릴리스부터 Xanadu`glide.security.explicit_roles.do_not_fix` 가 snc_internal 변경되어 조정되었습니다. snc_internal 역할은 이제 메모리와 sys_user_has_role 모두 동일합니다. `glide.security.explicit_roles.do_not_fix`의 새로운 동작은 다음과 같습니다.

glide.security.explicit_roles.do_not_fix 새 동작

값	결과
아니요	메모리와 sys_user_has_role 모두에서 snc_internal 역할 추가
예	메모리나 sys_user_has_role에 snc_internal 역할을 추가하지 마십시오.

특정 사용자의 snc_internal 역할을 제외하려면 `glide.security.explicit_roles.ignore.snc_internal.exclude_role_list` 속성을 사용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

팁: 이전 `glide.security.explicit_roles.do_not_fix` 동작으로 되돌리려면 `glide.security.explicit_roles.do_not_fix_in_memory` 속성을 사용합니다.

외부 사용자에게 테이블 액세스 권한 제공

snc_external 역할을 상속하는 테이블에 역할을 추가하여 외부 사용자에게 테이블에 대한 액세스 권한을 제공할 수 있습니다. 자세한 내용은 외부 사용자에게 테이블 접근 권한 제공 문서를 참조하십시오.

HasRoles() 메서드

`Hasroles()` 메서드는 그대로 사용할 수 있지만 이 Geneva 릴리스에서는 사용하지 않습니다. 대신 `hasRole(## ##)` 메서드를 사용하십시오.

`hasRoles()` 메서드를 사용하는 경우 다음 변경 사항에 유의하십시오.

- 이 메서드는 역할을 확인할 때 기본 snc_internal 역할을 자동으로 제외합니다. 즉, 사용자에게 snc_internal 역할만 있으면 `hasRoles()` 메서드는 그대로 **false**를 반환합니다.
- 사용자에게 snc_external 역할이 있는 경우 인스턴스가 외부 사용자에 게 역할이 없는 것으로 간주하므로 이 메서드는 **false**를 반환합니다.

상호 배제: snc_external과 **snc_internal** 비교

Now Platform에서는 사용자가 snc_external 역할과 snc_internal 역할을 모두 가질 수 없습니다. Now Platform 시스템의 모든 곳에서 이 상호 배제를 적용하여 각 상충에 대한 오류 메시지를 로그에 기록합니다.

주: 모든 사용자가 ACL 자원에 접근할 수 있어야 하는 경우 ACL에는 두 역할 모두 있을 수 있습니다.

예시: 사용자에게 명시적 역할을 모두 추가합니다(직접 충돌).

1. snc_internal 역할을 사용자 Abel Tuter에게 할당합니다.
2. snc_external 역할을 사용자 Abel Tuter에게 할당합니다.

결과: Abel Tuter에게 snc_internal 역할이 있으므로 snc_external 역할을 추가하지 못합니다.

예시: 그룹에 명시적 역할을 모두 추가합니다(직접 충돌).

1. 테스트 그룹이라는 그룹에는 현재 그룹에 할당된 명시적 역할이 없는 것으로 고려합니다.
2. 테스트 그룹에 Abel Tuter를 추가합니다.
3. snc_external 역할을 테스트 그룹에 추가합니다.

결과: Abel Tuter에게 이미 snc_internal 역할이 있고 두 역할 모두 가질 수 없으므로 snc_external 역할을 추가하지 못합니다.

예시: 그룹 구성원에게 상충하는 명시적 역할이 있는 그룹에 명시적 역할을 추가합니다(간접 충돌).

1. snc_internal 역할을 사용자 Abel Tuter에게 할당합니다.
2. 테스트 그룹이라는 그룹에는 현재 그룹에 할당된 명시적 역할이 없는 것으로 고려합니다.
3. 테스트 그룹에 Abel Tuter를 추가합니다.
4. snc_external 역할을 테스트 그룹에 추가합니다.

결과: Abel Tuter가 그룹 구성원 자격을 통해 snc_external 역할을 상속하므로 그룹에 snc_external 역할을 추가할 수 없습니다. 명시적 역할 모두 허용되지 않은 동일한 사용자에게 할당됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다른 예시의 경우 다음 테이블을 참조하십시오.

역할	시도한 동작	결과
직접 충돌		
사용자에게 snc_internal 역할이 있습니다.	snc_external 역할을 추가합니다.	동작이 중단되었습니다.
사용자에게 snc_external 역할이 있습니다.	snc_internal 역할을 추가합니다.	동작이 중단되었습니다.
사용자에게 명시적 역할이 없습니다.	snc_internal 또는 snc_external 역할을 추가합니다.	역할이 추가되었습니다.
사용자에게 명시적 역할이 모두 있습니다 (기존 충돌).	역할이 없는 그룹에 사용자를 추가합니다.	동작이 중단되었습니다.
사용자와 관련되지 않은 역할에는 snc_internal 역할이 포함되어 있습니다.	snc_external 역할을 추가합니다.	동작이 중단되었습니다.
사용자와 관련되지 않은 역할에는 snc_external 역할이 포함되어 있습니다.	snc_internal 역할을 추가합니다.	동작이 중단되었습니다.
역할에 명시적 역할이 모두 있습니다 (기존 충돌).	사용자, 역할 또는 그룹에 역할을 추가합니다.	동작이 중단되었습니다.
구성원이 없는 그룹에 snc_internal 역할이 포함되어 있습니다.	snc_external 역할을 추가합니다.	동작이 중단되었습니다.
구성원이 없는 그룹에 snc_external 역할이 포함되어 있습니다.	snc_internal 역할을 추가합니다.	동작이 중단되었습니다.
구성원이 없는 그룹에는 역할이 없습니다.	snc_internal 또는 snc_external 역할을 추가합니다.	역할이 추가되었습니다.
간접 충돌		
충돌이 포함된 역할 포함	**1.** snc_internal 역할이 있는 사용자에게 테스트 역할이라는 역할을 부여합니다. **2.** snc_external 역할을 테스트 역할에 추가합니다.	동작이 중단되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할	시도한 동작	결과
충돌이 포함되지 않은 역할 포함	**1.** 역할이 없는 사용자에게 테스트 역할이라는 역할을 부여합니다. **2.** snc_external 역할을 테스트 역할에 추가합니다.	역할이 사용자와 테스트 역할 모두에 추가됩니다.
충돌이 포함된 그룹 포함	**1.** snc_internal 역할이 있는 사용자를 테스트 그룹 2(테스트 그룹 1의 하위)라는 그룹에 추가합니다. **2.** snc_external 역할을 테스트 그룹 2에 추가합니다. **3.** 테스트 그룹 1(테스트 그룹 2의 상위)이라는 상위 그룹에 snc_external 역할을 추가합니다.	동작이 중단되었습니다.
충돌이 포함되지 않은 그룹 포함	**1.** 역할이 없는 사용자를 테스트 그룹 2(테스트 그룹 1의 하위)라는 그룹에 추가합니다. **2.** 테스트 그룹 1(테스트 그룹 2의 상위)에 snc_external 또는 snc_internal 역할을 추가합니다.	역할이 상위 그룹, 하위 그룹 및 사용자에 추가됩니다.
그룹 포함에 충돌이 있는 역할 포함 추가	테스트 그룹 1(테스트 그룹 2의 상위)에 contains_external을 추가합니다.	테스트 그룹 1과 테스트 그룹 2는 모두 contains_external을 사용할 수 있지만 snc_external 역할을 명시적으로 사용하지는 않습니다.
	테스트 그룹 2(테스트 그룹 1의 하위)에 snc_internal 역할을 추가합니다.	동작이 중단되었습니다.
그룹 상위 변경에 그룹 포함 추가	**1.** 테스트 그룹 1(테스트 그룹 2의 상위)을 제거합니다. **2.** snc_internal 역할을 테스트 그룹 1에 추가합니다. **3.** snc_external 역할을 테스트 그룹 2에 추가합니다. **4.** 테스트 그룹 2에서 테스트 그룹 1을 상위 그룹으로 설정하고 저장합니다.	동작이 중단되었습니다. 동일한 결과가 되는 이미 중첩된 그룹에 대해 반복합니다.

중단된 동작에 대한 원인이 오류 메시지에 나타나며 다른 시도하여 성공하려면 먼저 해결되어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개별 사용자에게 명시적 역할을 추가하는 등의 직접적인 케이스에는 사용자에게 명시적인 역할이 있는지 확인하십시오. 사용자에게 잘못된 명시적 역할이 있는 경우, 먼저 제거한 다음 올바른 명시적 역할을 추가해야 합니다.

명시적 역할을 그룹에 추가하는 것과 같은 간접적 케이스의 경우, 그룹 구성원에게 명시적인 역할이 모두 할당되도록 하려면 해당 사용자가 그룹에 있어야 하는지 여부를 평가하십시오. 그룹 계층 구조와 역할 포함을 통한 상속을 비롯하여 그룹에 명시적 역할을 지정해야 하는지 여부도 결정합니다.

Now Platform에서는 발생한 첫 번째 잠재적 충돌만 보고된다는 점에 유의하십시오. 매번 새로운 근본 원인이 있어 정정 이후에도 반복적인 시도 작업이 계속 실패하면 관련 사용자/그룹/역할 상호 의존성을 보다 폭넓게 다시 평가하십시오. 그룹 및 역할 포함을 구성하는 방식을 다시 생각해 볼 수 있습니다.

명시적 역할 요청

Service Catalog를 통해 Now Support Explicit Roles 플러그인(com.glide.explicit_roles)을 요청하여 명시적 역할을 활성화합니다.

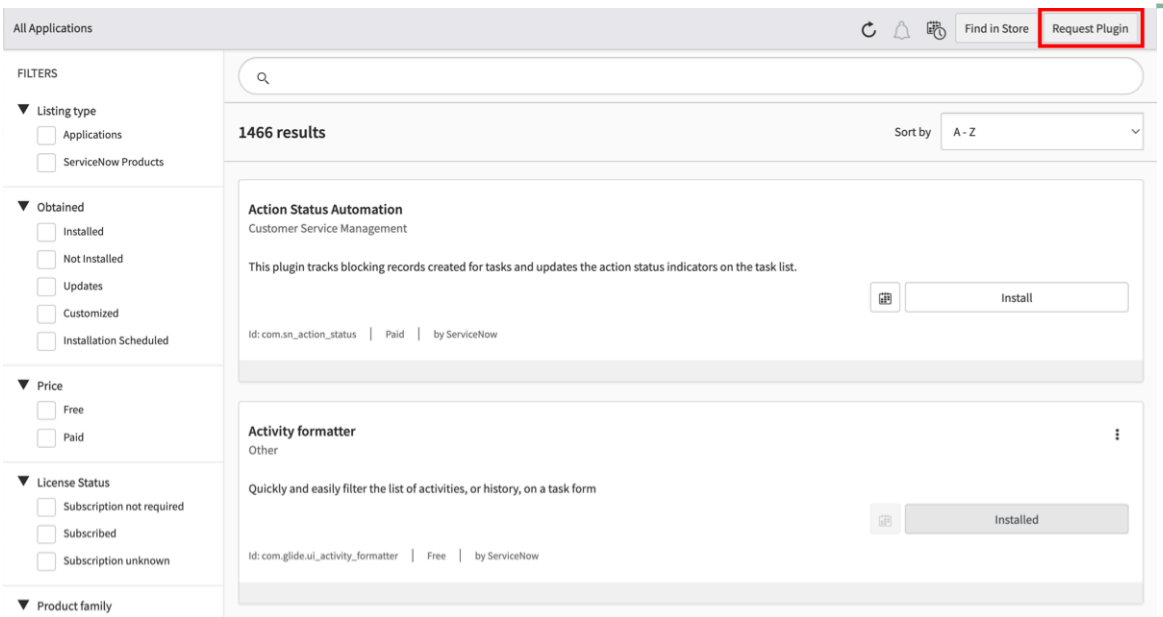
시작하기 전에

필요한 역할: 관리자

중요사항: 유지관리 기간 동안 또는 로그인한 사용자가 거의 없는 경우 이 플러그인을 활성화합니다. 플러그인이 활성화됐을 때 로그인한 상태의 사용자에게는 snc_internal 역할이 동적으로 할당되지 않습니다. 로그아웃했다가 다시 로그인했을 때 사용자는 snc_internal 역할을 할당받을 수 있습니다. 플러그인이 활성화되면 언제든지 snc_internal 및 snc_external 역할을 추가하거나 제거하여 사용자 권한을 변경할 수 있습니다.

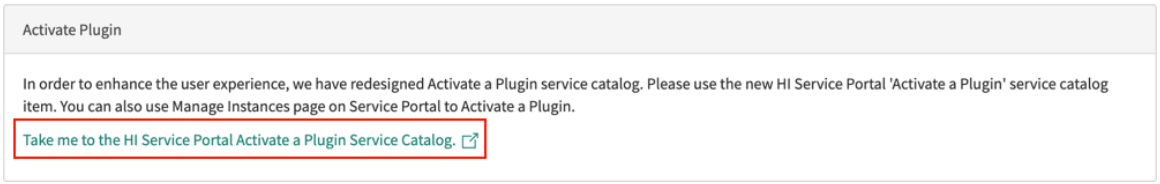
프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 모든 애플리케이션 페이지에서 플러그인 요청을 선택하여 Now Support의 플러그인 활성화 양식을 엽니다.



3. Now Support에서 Now Support 서비스 포털 서비스 카탈로그에 액세스하는 링크를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 인스턴스를 선택합니다.
5. 작업 > 플러그인 활성화를 선택합니다.
6. 플러그인 활성화 양식에서 다음 정보를 입력합니다.

플러그인 활성화 양식

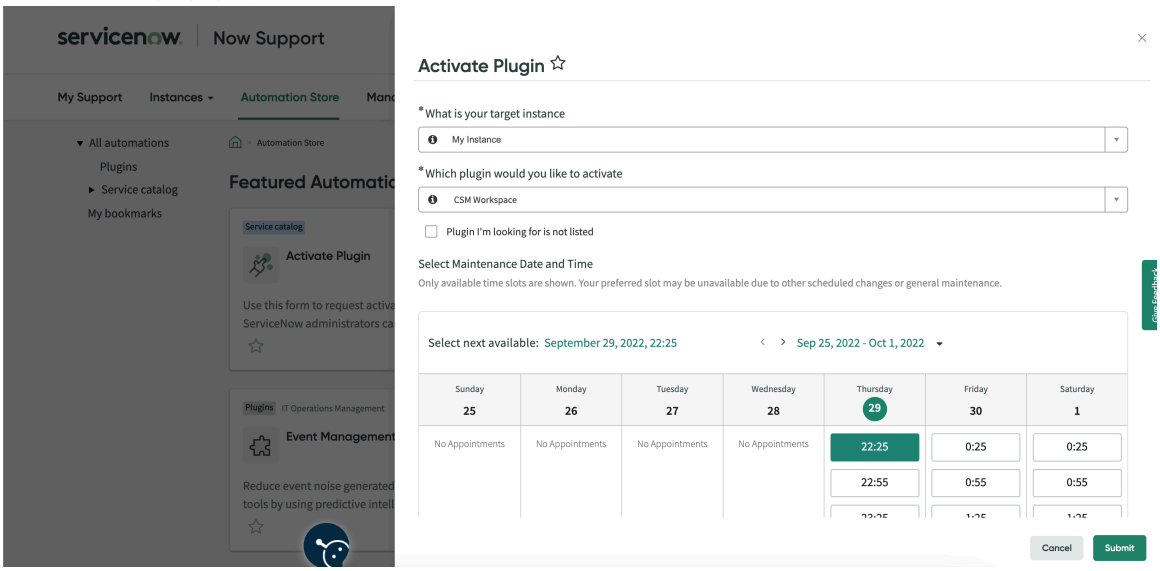
필드	설명
대상 인스턴스는 무엇입니까?	플러그인을 활성화할 인스턴스입니다.
어떤 플러그인을 활성화하시겠습니까?	활성화할 플러그인의 이름입니다. 주: 시스템에서 원하는 플러그인을 나열하지 않거나 OEM 또는 온프레미스 인스턴스에서 플러그인을 활성화하는 경우 찾고 있는 플러그인이 목록에 없음 확인란을 선택한 다음 플러그인 이름을 입력합니다.
유지관리 날짜 및 시간 선택	플러그인을 활성화하는 날짜 및 시간입니다. 주: 플러그인은 미국 태평양 시간대의 모든 영업일에 두 번(오전과 저녁에 각각 한 번씩) 활성화됩니다. 특정 시간에 플러그인을 활성화해야 하는 경우 이유/설명 필드에 요청을 입력합니다.

Example

예를 들어, 내 인스턴스라는 인스턴스에서 CSM Workspace 플러그인을 활성화하는 다음 양식을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플러그인 활성화 양식



7. 제출을 선택합니다.
   플러그인 요청에 대한 자세한 내용은 다음을 참조하십시오. 의 서비스 카탈로그 [KB0751715] 문서에서 플러그인 요청 Now Support 지식베이스.

상승된 권한 역할

상승된 권한 역할을 사용하려면 먼저 역할 사용에 대한 책임을 수동으로 수락해야 역할의 기능에 액세스할 수 있습니다.

기본적으로 로그인 시 상승된 권한 역할은 없습니다. 수동으로 해당 역할의 권한으로 상승시켜야 합니다. 상승된 권한 역할은 사용자 세션 기간 동안만 지속됩니다. 세션 제한 시간 또는 로그아웃은 역할을 제거합니다.

어떤 역할이든 상승된 권한 역할로 지정한 다음 한 명 이상의 사용자에게 해당 역할을 할당할 수 있습니다. 사용자가 로그인 직후 역할이 제공하는 권한에 액세스하지 못하도록 제한하려면 이 작업을 수행합니다. 역할 양식에서 권한 역할을 지정할 수 있습니다. 지침은 역할 생성을 참조하세요.

상승된 역할을 사용하려면 다음 조건을 충족해야 합니다.

- 상승된 역할이 사용자에게 할당되어야 합니다.
- 첫 번째 상승된 역할을 포함하는 두 번째 상승된 역할로 이미 상승된 경우에도 권한을 얻으려면 수동으로 상승된 특정 역할로 상승해야 합니다.

  예를 들어 상승된 역할 A에 상승된 역할 B가 포함된 경우 역할 A로 승격하더라도 해당 권한을 얻으려면 역할 B로 승격해야 합니다.

관리자 역할

사용자에게 관리자 역할을 부여하려면 권한을 부여하는 사용자에게 관리자 역할도 있어야 합니다. 예를 들어, user_admin 역할만 있는 사용자는 다른 사용자에게 관리자 역할을 부여할 수 없습니다.

- 관리자가 아닌 사용자는 관리자 역할이 포함된 그룹에 사용자를 추가할 수 없습니다.
- 사용자에게 security_admin 역할을 부여하려면 권한을 부여하는 사용자에게 관리자 역할도 있어야 하며 다른 사용자에게 security_admin 역할을 부여하기 전에 security_admin 역할로 격상해야 합니다. 관리자 역할만 있는 사용자는 다른 사용자에게 security_admin 역할을 부여할 수 없습니다.
- security_admin 역할이 없는 사용자는 security_admin 역할이 포함된 그룹에 사용자를 추가할 수 없습니다.

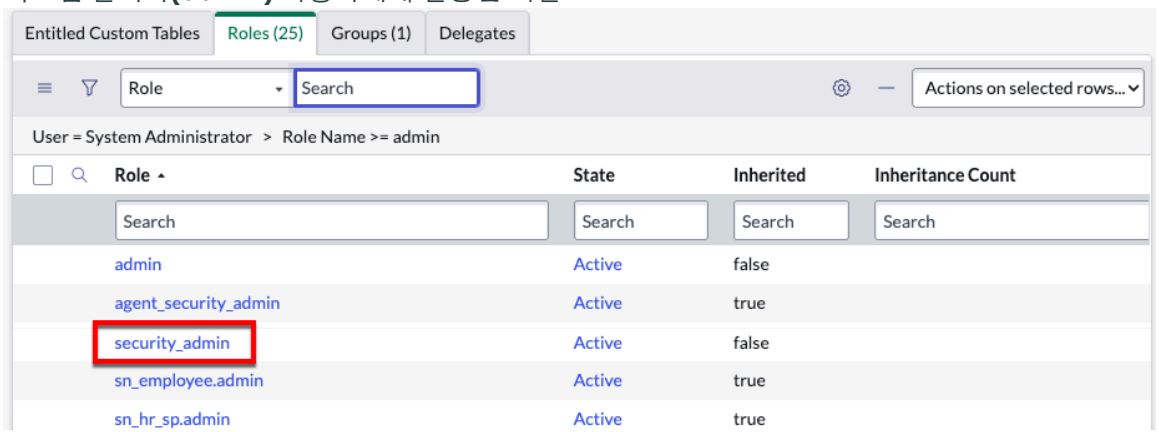
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

⚠ 경고: 관리자 역할에 대한 상승된 권한의 사용은 지원되지 않습니다. 대신 관리자가 수동으로 상승시키도록 요구하십시오. 관리자가 수동으로 상승하도록 강제 설정

security_admin 역할

기본 시스템에서 security_admin 역할은 상승된 권한을 가진 유일한 역할입니다. 이 역할은 기본 시스템 관리자(admin) 사용자인 사용자에게 자동으로 할당됩니다. ACL 및 높은 보안 설정에 대한 액세스를 제공합니다.

시스템 관리자**(admin)** 사용자에게 할당된 역할



ⓘ 주: 이 역할을 보려면 먼저 security_admin 역할로 승격해야 합니다. 시스템 관리자(admin) 사용자로만 로그인한 경우 역할 목록에 security_admin 기록을 볼 수 없습니다.

Security_admin 역할

security_admin 역할은 사용자가 접근 제어를 생성 및 변경하고 높은 보안 설정을 변경할 수 있는 높은 보안 설정과 함께 제공되는 상승된 권한 역할입니다.

기본 시스템에서는 기본 시스템 관리자(admin) 사용자만 security_admin 역할을 가집니다. 권한 상승이 필요하므로 admin 사용자는 로그인 시 이 역할을 갖지 않습니다. 권한을 상승시킨 후 admin 사용자는 사용자 세션 기간 동안 security_admin 역할을 가집니다. 자세한 내용은 권한 있는 역할로 상승 문서를 참조하십시오.

높은 보안을 유지하려면 security_admin 역할에 상승된 권한이 필요합니다. 이 역할을 할당할 사용자와 그룹을 제한합니다.

권한 있는 역할로 상승

기본 시스템 관리자의 역할을 상승시켜 권한이 있는 역할을 부여하면 고급 보안 설정의 기능을 이용할 수 있게 됩니다.

시작하기 전에
필요한 역할: 관리자

ⓘ 주: 다른 사용자에게 관리자 역할을 부여하면, 이러한 사용자는 특권 역할로 격상할 수 없습니다. 기본 시스템 관리자만 상승할 수 있습니다.

프로시저

1. 배너 프레임에서 이미지를 클릭하거나, 업로드된 이미지가 없는 경우 이니셜을 클릭합니다.
2. 역할 상승을 선택합니다.
   권한 상승에 사용할 수 있는 역할이 포함된 대화상자가 나타납니다.
3. 할당할 상승된 역할을 선택하고 확인을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 역할은 세션의 나머지에 대해 역할로 제어되는 모든 자원에 대한 사용자 상승 권한을 부여합니다. 사용자가 로그아웃하면 상승된 권한이 세션과 함께 종료되지만 다음 로그인 시 다시 설정될 수 있습니다.

4. 2단계의 대화 상자로 돌아가 역할 선택을 취소하여 역할 상승을 종료합니다.

관리자가 수동으로 상승하도록 강제 설정

관리자 역할을 가진 모든 사용자가 격상시키려는 역할을 수동으로 선택하도록 강제하는 속성이 있습니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 관리자로 로그인합니다.
2. 당신의 역할을 security_admin로 승격시키십시오.
3. **sys_properties.list**로 이동합니다.
4. 속성을 검색하여 선택합니다 *glide.security.strict_elevate_privilege*.
5. 값 필드를 **true** 로 설정하고 제출을 클릭합니다.

결과
사용자가 로그인하면 승격할 수 있는 역할을 선택할 수 있는 대화 상자 창이 나타납니다.

연결 및 자격 증명

검색, 서비스 매핑 및 클라우드 관리를 위해 컴퓨터나 네트워크 장치에 접근 권한을 획득하거나 오케스트레이션을 사용하여 작업을 수행하려면 자격 증명과 연결 정보가 필요합니다. 콘텐츠를 Share 또는 AppStore에 추가할 때 빌드된 콘텐츠를 수정하지 않고도 환경과 관련된 연결 및 자격 증명을 구성할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색



자격 증명에 대해 자세히 알아보십시오.

구성



자격 증명을 구성합니다.

참조



자격 증명에 대한 상세 정보를 얻습니다.

문제 해결



연결 및 자격 증명 문제를
해결하는 방법에 대해 알아봅니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자격 증명, 연결 및 별칭 탐색

의 모든 애플리케이션 통합은 Now Platform 연결, 자격 증명 및 별칭을 사용하여 애플리케이션이 자원에 액세스할 수 있도록 합니다.

에서 Now Platform애플리케이션 통합을 실행하려면 먼저 연결 정보와 해당 자격 증명을 생성 및 구성하고 별칭을 추가해야 합니다. 이러한 용어를 정의하는 방법을 ServiceNow 이해하려면 다음을 수행합니다.

연결

연결은 프로토콜이 있는 IP 주소 또는 엔드포인트와 같은 시스템과의 통합입니다. 여기에는 데이터베이스와 통합할 때 데이터베이스 세부 사항과 같은 특정 세부 정보가 포함됩니다.

자격 증명

자격 증명은 ID 및 암호와 같이 연결에 필요한 인증 데이터입니다.

별칭

별칭은 인스턴스의 연결 또는 자격 증명 세트와 관련된 명명 규칙 또는 태그입니다. 별칭에는 애플리케이션을 통합하는 데 필요한 연결 및 자격 증명 정보가 포함되어 있습니다. 통합할 때마다 해당 정보를 입력하는 대신 별칭을 사용할 수 있습니다. 예를 들어 동일한 애플리케이션 통합에 대한 QA, 개발 및 프로덕션 자격 증명을 보관할 별칭을 지정할 수 있습니다. 별칭은 각 환경에 대한 애플리케이션 통합을 해결합니다.

는 Now Platform 다양한 유형의 별칭을 구별합니다.

자격 증명 별칭

이 별칭은 자격 증명 데이터에만 연결되고 런타임 중에 확인됩니다.

연결 및 자격 증명 별칭

이 별칭은 통합을 완료하는 데 필요한 연결 정보 및 자격 증명 데이터에 연결되고 런타임 중에 해결됩니다.

연결 및 자격 증명 별칭 내에서 하위 별칭이라는 추가 별칭을 생성할 수도 있습니다. 하위 별칭을 사용하면 동일한 애플리케이션 통합 내에서 여러 연결을 만들 수 있습니다. 하위 별칭을 생성하면 이를 생성한 별칭이 상위 별칭이 됩니다. 하위 별칭은 상위 별칭에서 속성을 상속하지만 하위 별칭은 고유한 연결 및 자격 증명 정보를 전달합니다.

연결, 자격 증명 및 별칭 사용의 이점

- 외부 서비스에 대한 자격 증명을 저장하고 관리할 중앙 위치
- 한 번 정의하여 여러 플랫폼 기능에 재사용
- 다른 플랫폼 기능의 구성 최소화
- 관리자가 아닌 사용자가 미리 정의된 연결 및 자격 증명을 사용할 수 있도록 허용
- 보안 강화

연결, 자격 증명 및 별칭을 사용하는 기능

다음 기능에서 연결, 자격 증명 및 별칭을 사용합니다.

- 플로우 디자이너
- 통합 허브
- 클라우드 관리
- 디스커버리

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Orchestration
- 서비스 매핑

다음 Now Platform 두 가지 방법 중 하나로 별칭을 설정할 수 있습니다.

- 연결 및 자격 증명 모듈 사용. 연결 및 자격 증명 별칭 생성 문서를 참조하십시오.
- 의 연결 대시보드 통합 허브에서 . 연결 추가를 참조하세요.

> 주: 통합 허브 별도의 구독이 필요합니다. 자세한 내용은 다음을 참조하십시오. 요청 통합 허브 .

MID 서버에서 자격 증명 동기화

인스턴스와 동기화된 네트워크의 각 MID 서버는사용자가 생성한 모든 자격 증명의 복사본을 보관합니다. MID(Management, Instrumentation, Discovery) Server는 ServiceNow 인스턴스와 외부 애플리케이션, 데이터 소스 및 서비스 간에 데이터의 통신과 이동을 가능하게 하는 Java 애플리케이션입니다. 이 동기화는 애플리케이션이 네트워크의 여러 장치와 같 디스커버리 거나 서비스 매핑 액세스해야 할 때 자격 증명 읽기 속도를 높입니다. MID Server는 ECC 큐에서 작업을 찾으면 *credentials_reload* 동기화됩니다. 다시 로드 작업은 인스턴스에 대한 SOAP 호출을 수행하여 자격 증명 [discovery_credentials] 테이블에 있는 모든 필드 값을 포함한 전체 자격 증명 목록을 가져오도록 MID 서버에 지시합니다. 자세한 내용은 MID 서버를 참조하십시오.

인스턴스가 각 MID 서버에 보내는 SOAP 응답에는 사용자 지정한 자격 증명 양식에 추가한 사용자 지정 필드도 포함됩니다. 참조 필드를 추가한 경우 참조된 테이블의 데이터도 SOAP 응답의 일부로 전송됩니다. 이로 인해 여러 MID Server와 자격 증명 동기화가 발생할 때 성능 문제가 발생할 수 있습니다. 이를 제어하려면 시스템 속성 [sys_properties] 테이블에 다음 속성을 수동으로 추가합니다.

> 주: 이러한 속성의 값을 변경하려면 시스템 속성 [sys_properties] 테이블에 추가합니다. 추가하지 않으면 시스템이 기본값을 사용합니다.

속성	설명
`com.snc.credentials_user_fields`	자격 증명 동기화에 모든 사용자 지정 필드를 포함합니다. 자격 증명 양식에 추가한 필드를 포함하지 않으려면 이 속성을 False로 설정합니다. • 유형: true | false • 기본값: true
`com.snc.credentials_recursion_depth`	자격 증명 동기화 메커니즘이 참조 테이블에서 필드를 수집할 때 통과할 테이블 수를 정의합니다. 성능 문제가 발생하고 참조 필드가 있는 테이블에 대한 참조 필드를 포함하는 자격 증명 양식을 사용자 지정한 경우 이 수를 낮추십시오. • 유형: 정수 • 기본값: 3

자격 증명 및 연결에 대한 범위 보호

특정 유형의 연결 및 자격 증명 기록을 범위에 속하는 것으로 분류하고 범위 보호를 해당 범위로 확대할 수 있습니다. 이러한 범위 정책은 테이블에 생성하는 기록을 보호하고 다른 범위에 공개되지 않는 기록과의 상호작용을 방지합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 필드는 연결 [sys_connection] 및 검색 자격 증명 [discovery_credentials] 테이블에서 사용할 수 있으며, 이 유형의 기록을 특정 범위에 연결할 수 있습니다. 의 YokohamaUI 양식에는 표시되지 않지만 쉽게 추가할 수 있습니다. 이러한 기록 유형에 대해 자세히 알아보고 UI 양식에 필드를 추가하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 연결 시작하기
- 자격 증명으로 시작
- 검색에 대한 자격 증명 별칭
- 양식 레이아웃 구성

연결 및 자격 증명 기록의 사용을 특정 범위로 제한하는 것은 강력한 보안이 필요한 애플리케이션 관리에 중요합니다. 이러한 애플리케이션에는 HR 서비스 제공 또는 보안 운영 범위가 지정된 관리 애플리케이션에서 생성된 연결 및 자격 증명 기록은 관리 사용자에게 표시되지 않습니다. 연결 및 자격 증명 기록을 특정 애플리케이션 범위에 연결하면 다음과 같은 보호를 받을 수 있습니다.

- 제한된 범위에 ACL(접근 제어 목록) 규칙을 적용합니다. 범위가 지정된 ACL에 대한 자세한 내용은 접근 제어 목록 규칙을 참조하세요.

  주: 범위 관리 및 적용된 보안을 사용하는 일부 애플리케이션에는 추가 설정이 필요할 수 있습니다. 자세한 내용은 HR 역할 관리를 참조하십시오.

- 스크립트를 사용하여 쿼리할 때 기록을 보호합니다. 전역 범위에서 쿼리를 수행하고 연결 및 자격 증명 기록이 보호된 범위에 있는 경우 액세스 권한이 부여되지 않는 한 쿼리에 표시되지 않습니다.

제한된 호출자 액세스를 사용하여 쿼리 제한된 기록을 사용자 지정하고 액세스 권한을 부여할 수 있습니다. 자세한 내용은 제한된 호출자 접근 권한 설정을 참조하세요. 범위 지정 제한은 연결 [sys_connection] 및 검색 자격 증명 [discovery_credentials] 테이블의 모든 하위 테이블에도 적용됩니다. 빈 필드와 기타 범위는 제한되지 않습니다.

주: 범위 보호는 새 기록을 설정할 때 혼동을 피하기 위해 보안된 특정 범위에 대해서만 활성화됩니다. 누군가가 범위가 지정된 애플리케이션 범위에서 연결을 만드는 경우 자동 범위 제한이 없습니다.

도메인 분리와 자격 증명 및 연결

도메인 분리는 자격 증명 및 연결에서 지원됩니다. 도메인 분리를 사용하여 데이터, 프로세스 및 관리 작업을 도메인이라는 논리적 그룹으로 분할할 수 있습니다. 어떤 사용자가 데이터를 보고 액세스할 수 있는지를 포함하여 이러한 분리의 여러 측면을 제어할 수 있습니다.

지원 수준: 표준

- 기본 수준 지원의 모든 측면을 포함합니다.
- 애플리케이션 속성이 필요에 따라 도메인을 인식합니다.
- 비즈니스 논리: 서비스 제공자(SP)가 고객별로 프로세스를 만들거나 수정합니다. 사용 사례는 여러 SP 고객이 단일 인스턴스에서 애플리케이션을 올바르게 사용하는 것을 반영합니다.
- 인스턴스 소유자는 특정 애플리케이션에 필요한 대로 테넌트별 최소 실행 가능한 제품(MVP) 비즈니스 논리 및 데이터 매개변수를 구성해야 합니다.

샘플 사용 사례: 관리자가 한 테넌트에 대해서는 기록이 닫히지만 다른 테넌트에 대해서는 기록이 닫히지 않는 경우 설명이 필요하도록 설정할 수 있어야 합니다.

지원 수준에 대한 자세한 내용은 도메인 분리를 위한 애플리케이션 지원을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

개요

자격 증명은 인스턴스 외부의 시스템에 액세스하는 다양한 ServiceNow 기능에 연결됩니다. 자격 증명은 자격 증명을 사용하는 기능에 연결된 도메인 분리를 따릅니다.

연결은 인스턴스 외부의 대상 호스트를 참조하는 프로토콜별 정보입니다. 연결을 통해 활동을 실행할 도메인을 지정할 수 있습니다.

자격 증명 및 연결에서 도메인 분리가 작동하는 방식

자격 증명은 인스턴스 외부의 자원에 액세스하며 Discovery , Orchestration 및 서비스 매핑 , 및 클라우드 프로비저닝 및 거버넌스 응용 프로그램. 이러한 자격 증명은 특정 도메인에 연결되지 않고 애플리케이션에 바인딩된 다음 애플리케이션이 사용하는 도메인 분리를 따를 수 있습니다. 자격 증명을 MID 서버에 할당한 다음 구성에 지정된 MID 서버 도메인 분리를 따를 수도 있습니다.

연결은 JMS, JDBC 또는 HTTP(s) 연결을 사용하여 대상 호스트에 액세스합니다. 연결이 속한 전역 또는 특정 도메인을 지정할 수 있습니다.

관련 정보

서비스 제공자용 도메인 분리

연결 및 자격 증명 구성 템플릿

admin 및 flow_designer 역할을 가진 사용자가 사용자 지정이 가능한 단일 양식을 사용하여 타사 시스템과 함께 스포크 통합을 설정할 수 있도록 합니다.

예를 들어 OAuth 제공자를 등록하고, 토큰을 생성하고, 연결 및 자격 증명 기록을 생성하는 OAuth 통합을 설정할 수 있습니다. 작업 디자이너 또는 개발자는 구성 템플릿을 사용하여 한 곳에서 스포크를 설정할 수 있으며 시스템은 관련 기록을 생성합니다.

혜택

구성 템플릿을 사용하면 다음을 수행할 수 있습니다.

- 관리자 또는 플로우 디자이너는 단일 양식을 사용하여 복잡한 통합을 설정할 수 있습니다.
- 개발자가 통합에서 정적 값을 설정하여 관리자 및 플로우 디자이너의 설정 프로세스를 단순화할 수 있습니다.

지원되는 자격 증명 유형

다음 자격 증명 유형과의 통합을 위한 구성 템플릿을 생성할 수 있습니다.

- 기본 인증
- API 키
- OAuth JWT 전달자 권한 유형
- OAuth 인증 코드 권한 유형
- 사용자 지정 인증

구성 템플릿 구성요소

기본 데이터 템플릿

모든 통합에 적용되는 정적 정보를 설정합니다. 예를 들어 값이 모든 통합에 적용되는 경우 API 및 토큰 URL을 설정할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

동적 데이터 템플릿

통합을 설정하기 위해 사용자가 완료해야 하는 정보를 정의합니다. 예를 들어 사용자 이름 및 암호 키-값 쌍을 추가하여 사용자 정의 값을 수집할 수 있습니다.

후처리 중인 스크립트

통합에 필요한 추가 레코드를 생성합니다. 예를 들어 스포크에 사용자 지정 테이블이 포함되어 있는 경우 구성 템플릿의 사용자 입력을 기반으로 해당 테이블에 레코드를 만들 수 있습니다. 이 스크립트는 연결 및 자격 증명 레코드가 만들어진 후에 실행 됩니다.

스크립트 사전 편집

기존 연결을 편집할 때 추가 정보 섹션의 사용자 지정 필드를 미리 채웁니다. 사용자 지정 필드를 미리 채우면 사용자 지정 필드와 연결된 현재 값을 볼 수 있습니다.

데모 데이터

연결 및 자격 증명 템플릿 [sys_alias_templates] 테이블에는 공통 인증 유형에 대한 템플릿을 설정하는 방법을 보여주는 예제 템플릿이 포함되어 있습니다. 직접 만들 때 이러한 예시를 가이드로 사용하십시오.

OAuth JWT 전달자 권한 유형에 대한 템플릿 구성

이 예제 구성 템플릿은 Docusign에 대한 요청을 인증하기 위해 JWT 전달자 권한 유형을 사용하여 자격 증명 및 연결 기록을 설정합니다.

기본 데이터 템플릿

기본 데이터 템플릿의 각 최상위 항목은 연결된 기록을 생성합니다. 템플릿에는 다음 섹션이 포함되어 있습니다.

- `## ##`: 자격 증명 테이블에 기록을 작성합니다.
- `##`: 연결 [sys_connection] 테이블과 관련된 모든 연결 기록에 기록을 작성합니다.
- `##`: 선택적으로 사용자 지정 테이블에 기록을 작성합니다. 후처리 스크립트는 이러한 기록으로 수행할 작업을 시스템에 알려줍니다.

다음 예에서는 OAuth JWT 전달자 권한 유형 인증에 필요한 레코드를 생성합니다.

```
{
  "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"
        }
      ],
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
      "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,
        "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":{
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
    "docusign_account_name": "<docusign-account-name>",
    "docusign_account_email": "<docusign-account-email>"
}
}
```

동적 데이터 스키마

동적 데이터 스키마는 사용자가 연결 및 자격 증명 별칭을 생성하고 입력을 수집할 때 표시되는 내용을 정의합니다. 닷워킹 구문을 사용하여 기본 데이터 템플릿에서 생성된 필드에 사용자 입력을 매핑합니다. 예를 들어 `connection_fields`는 기본 데이터 템플릿으로 만든 `##` 객체의 `connection_url` 필드에 사용자 입력을 매핑합니다.

```
{
  "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"
    },
    {
      "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"
    },
 {
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
      "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"
    }
  ]
}
```

후처리 중인 스크립트

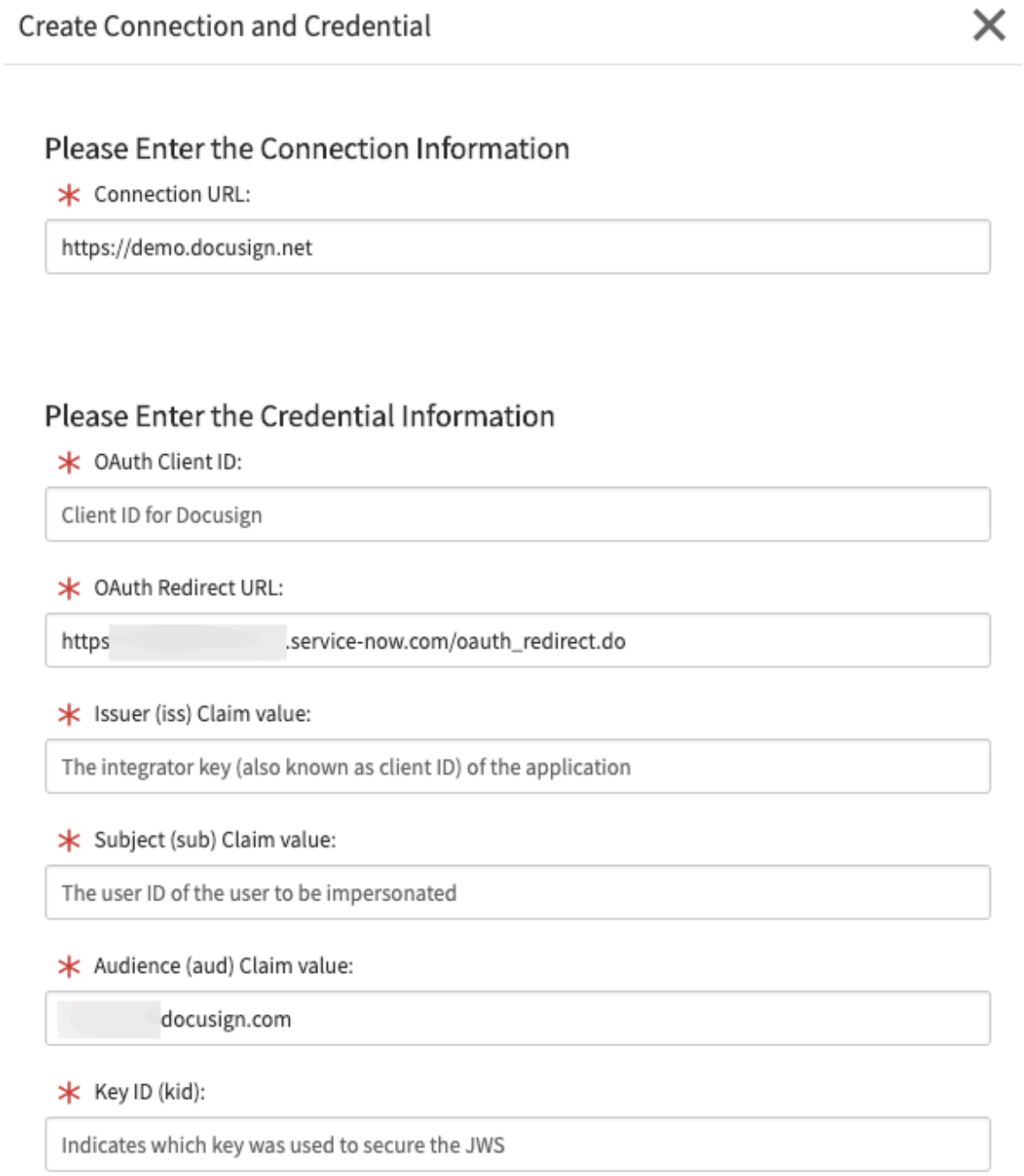
다음 후처리 스크립트는 사용자 입력을 sn_docusign_spoke_accounts 테이블의 필드에 매핑합니다.

```
(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);
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

결과 **Docusign** 연결 및 자격 증명 구성 양식

사용자가 연결된 Docusign 연결 및 자격 증명 별칭으로 이동하여 새 연결 및 자격 증명 작성을 선택하면 다음 대화 상자가 나타납니다.



구성 템플릿 생성

스포크를 설정하는 데 필요한 입력을 정의하는 템플릿을 생성합니다. 정적 키-값 쌍을 설정하여 기록을 생성하고 모든 통합에 적용되는 값을 설정합니다. 동적 키-값 쌍을 설정하여 사용자 입력을 수집하고 다를 수 있는 필드 값을 설정합니다. 이 템플릿을 사용하여 관리자와 플로우 디자이너는 단일 양식에서 스포크를 설정할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 통합 허브 > 연결 및 자격 증명 > 구성 템플릿.
2. 새로 만들기를 선택합니다.
3. 만들려는 구성 템플릿의 유형을 선택합니다.

구성 유형	설명
OAuth 인증 코드 권한 유형을 사용하는 HTTP 연결	인증 코드를 사용하여 타사 시스템을 OAuth 제공자로 등록하기 위한 템플릿을 생성합니다.
OAuth JWT 전달자 권한 유형을 사용하는 HTTP 연결	JSON 웹 토큰을 사용하여 외부 공급업체 시스템을 OAuth 제공자로 등록하는 템플릿을 작성합니다.
클라이언트 자격 증명을 사용하는 HTTP OAuth 권한 유형	클라이언트 자격 증명 부여 유형을 사용하는 OAuth 2.0 인증을 통해 외부 공급업체 애플리케이션과 통합하는 템플릿을 생성합니다.
OAuth 클라이언트 자격 증명을 사용하는 HTTP 연결 부여 유형 (외부 스토리지)	외부 저장소에 저장된 클라이언트 자격 증명으로 구성된 OAuth 토큰 요청을 MID 서버를 통해 OAuth 서버로 보낼 수 있는 템플릿을 작성합니다.
기본 인증 자격 증명을 사용하는 HTTP 연결	기본 인증을 사용하여 외부 공급업체 시스템과 통합하는 템플릿을 만듭니다.
API 키 자격 증명을 사용하는 HTTP 연결	API 키를 사용하여 외부 공급업체 시스템과 통합하는 템플릿을 만듭니다.
기타 구성	사용자 지정 인증을 위한 템플릿을 설정할 수 있는 빈 템플릿을 작성합니다.

4. 이름 필드에 템플릿을 식별하는 이름을 추가합니다.
5. 기본 데이터 템플릿 필드에서 필요한 사항을 변경합니다.

   이 필드는 모든 통합에 적용되는 정적 정보를 설정합니다. 예를 들어 값이 모든 통합에 적용되는 경우 API 및 토큰 URL을 설정할 수 있습니다.

   기본 데이터 템플릿의 다음 객체는 필수입니다.

   - `## ##`: 필수 필드가 있는 자격 증명 기록을 생성합니다.
   - `##`: 필수 필드가 있는 연결 기록을 생성합니다. `extended_attributes` 자식 개체를 사용하여 연결 속성에 액세스합니다. 예:

```
"connection": {
            "extended_attributes": {
                "api_version": "v1"

             },
        "connection_url": "https://<provider-domain-name>.com",
        "name": "Spoke Connection",
        "table": "http_connection"
    }
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

`##` 객체를 사용하여 사용자 지정 테이블에 대한 데이터를 설정하고 후처리 스크립트를 사용하여 테이블에 데이터를 삽입할 수 있습니다.

주: OAuth 인증 코드 권한 유형에 대한 기본 데이터 템플릿에서 `oauth_entity_profile_scope` 및 `oauth_entity_scope` 키의 값이 일치해야 합니다. 다음 예에서 두 키 모두 `## #### ###` 값을 갖습니다.

```
"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. **Dynamic Data Schema** 필드에서 필요한 사항을 변경합니다.

   이 필드 통합을 설정하기 위해 사용자가 완료해야 하는 정보를 정의합니다. 예를 들어 사용자 이름 및 암호 키-값 쌍을 추가하여 사용자 정의 값을 수집할 수 있습니다.

   동적 데이터 스키마의 필드에는 다음 속성이 포함됩니다.

   - `name`: 사용자의 입력이 매핑되는 필드입니다. 예를 들어 사용자 입력을 연결 기록의 연결 URL 필드에 매핑하려면 `connection.connection_url#` 입력합니다.
   - `label`: 템플릿을 작성할 때 사용자에게 표시되는 필드 레이블입니다.
   - `type`: 필드 유형입니다. 이 데이터 유형이 값을 매핑하는 필드의 데이터 유형과 일치하는지 확인하십시오.
   - `defaultValue`: 선택 사항입니다. 필드의 기본값입니다. 기본값이 제공되지 않으면 힌트가 표시됩니다.
   - `hint`: 선택 사항입니다. 기본값이 없을 때 표시할 힌트 텍스트입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: OAuth JWT 전달자 권한 유형 인증을 위한 템플릿을 설정하는 경우 `jwt_claim_validation` 배열의 단일 키-값 쌍에 대한 사용자 입력을 원할 수 있습니다. 배열의 인덱스를 참조하여 동적 데이터 스키마의 단일 키-값 쌍을 참조할 수 있습니다. 예를 들어 기본 데이터 템플릿에 이 스니펫이 포함될 수 있습니다.

```
"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"
      } ],
```

항목의 0부터 시작하는 인덱스 (`credential.jwt_provider.jwt_claim_validation[0].value`)를 사용하여 `iss` 키-값 쌍을 참조합니다.

7. 옵션: 후처리 중인 스크립트 필드에서, 다음과 같은 스크립트를 추가합니다.통합에 필요한 추가 레코드를 생성합니다. 예를 들어 스포크에 사용자 지정 테이블이 포함되어 있는 경우 구성 템플릿의 사용자 입력을 기반으로 해당 테이블에 레코드를 만들 수 있습니다. 이 스크립트는 연결 및 자격 증명 레코드가 만들어진 후에 실행 됩니다.
후처리 스크립트는 이러한 전역 객체에 액세스할 수 있습니다.

전역 객체	설명
aliasId	연결 및 자격 증명 별칭 [sys_alias] 테이블의 별칭 기록 Sys_id.
connectionSysId	템플릿에서 만든 연결 기록의 Sys_id입니다.
jsonDefaultData	기본 데이터 템플릿 필드의 JSON 컨텐츠(문자열 형식)입니다.
json동적 데이터	동적 데이터 템플릿 필드의 JSON 컨텐츠(문자열 형식)

8. 스크립트 사전 편집 필드에 스크립트를 추가하여 연결을 편집할 때 추가 필드를 미리 채웁니다.

이 스크립트는 객체 배열을 반환합니다. 각 객체에는 추가 필드를 채우기 위한 이름-값 쌍이 있습니다. 예를 들어, 연결에 사용자 지정 테이블에 있는 필드가 필요한 경우 이러한 필드를 사용자 지정 테이블에 매핑할 수 있습니다.

편집 전 스크립트는 다음과 같은 전역 객체에 액세스할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

전역 객체	설명
aliasId	연결 및 자격 증명 별칭 [sys_alias] 테이블의 별칭 기록 Sys_id.
connectionSysId	템플릿에서 만든 연결 기록의 Sys_id입니다.
jsonDefaultData	기본 데이터 템플릿 필드의 JSON 컨텐츠(문자열 형식)입니다.
json동적 데이터	동적 데이터 템플릿 필드의 JSON 컨텐츠(문자열 형식)

스크립트의 각 객체에는 다음과 같은 속성이 있습니다.

- `name`: 연결의 값을 지정하는 사용자 지정 필드의 이름입니다.
- `#`: 사용자 지정 필드를 채우기 위해 매핑하려는 값입니다. 함수, 변수를 사용하거나 하드 코딩하여 필드를 매핑할 수 있습니다.

필드에 지원되는 데이터 형식은 다음과 같습니다.

필드에 지원되는 데이터 유형

유형	설명
텍스트	문자열 값입니다.
부울	선택 상자. 선택은 true 값을 나타내고 비선택은 false 값을 나타냅니다.
번호	숫자 값입니다.
날짜	yyyy-mm-dd 형식의 날짜 값입니다. GlideDate 객체를 사용할 수도 있습니다.
선택	동적 데이터 스키마필드에 정의된 유효한 선택 목록입니다.
참조	유효한 GlideRecord입니다.
라디오 그룹	다른 필드 집합을 포함하는 그룹입니다. 이러한 그룹은 연결을 편집할 때 드롭다운 목록에서 선택 항목으로 사용할 수 있습니다. 드롭다운 목록에서 필요한 그룹을 선택하면 각 그룹의 필드가 나타납니다. 예를 들어, 동적 데이터 스키마 필드에 정의된 라디오 그룹의 다음 구조를 고려하십시오. `{ "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",`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

유형	설명

	<pre>"label": "Radio Group 2",
	"fields": [{
	"name": "radio_field2",
	"label": "Radio Field 2",
	"type": "text",
	"defaultValue": "abcd",
	"mandatory": true
	}],
	"default_group": true
	}</pre>
	이 예제에서는 다음 코드 조각을 사용하여 닷워킹을 통해 스크립트에서 라디오 그룹이 사용되는 방식을 이해할 수 있습니다.
	<pre>{
	name:
	"radio_field.first_radio_group.radio_field1",
	value: "radio field 1"
	}, {
	name:
	"radio_field.second_radio_group.radio_field 2",
	value: "radio field 2"
	}, {
	name: “radio_groups”,
	value:
	gr.getValue(‘radio_groups’)
	}</pre>
	닷워킹을 사용하는 방법에 대한 자세한 내용은 닷워킹을 참조하세요.

팁: 연결을 편집하는 동안 미리 채워진 값이 필드에 표시되지 않으면 다음으로 이동하십시오. 시스템 진단 > 세션 디버그 > 디버그 로그 문제를 진단합니다.

9. 연결 및 자격 증명 별칭에 템플릿을 추가합니다.

a. 다음으로 이동 통합 허브 > 연결 및 자격 증명 > 연결 및 자격 증명 별칭.

b. 스포크의 별칭 기록을 엽니다.

c. 구성 템플릿 필드에서 조회 아이콘을 클릭합니다.

d. 목록에서 생성한 템플릿을 선택합니다.

e. 업데이트를 클릭합니다.

결과
사용자가 연결된 연결 및 자격 증명 별칭으로 이동하여 새 연결 및 자격 증명 작성을 선택하면 입력을 수집하는 대화 상자가 나타납니다. OAuth 인증 코드 권한 부여 유형에 대한 템플릿을 생성한 경우 이 대화 상자에서 OAuth 토큰을 검색할 수도 있습니다.

다음에 수행할 작업
연결된 연결 및 자격 증명 별칭으로 이동하고 새 연결 및 자격 증명 생성을 선택하여 템플릿을 테스트합니다. 대화가 예상 데이터를 수집하고 시스템에 필요한 기록을 생성하는지 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연결 시작하기

연결 테이블을 사용하여 대상 호스트에 대한 기본, JMS, JDBC 또는 HTTP(s) 연결을 설정합니다.

연결 테이블

연결 테이블(sys_connection)은 모든 연결 테이블의 기본 테이블입니다. 다음 프로토콜에 대한 연결을 설정할 수 있습니다.

- PowerShell 및 SSH에 대한 기본 연결
- JDBC
- JMS
- HTTP(s)

연결 테이블은 연결 별칭 테이블을 참조하며, 테이블은 연결 별칭을 연결 정보에 연결합니다. 모든 연결은 다음 정보를 기록합니다.

기본 연결 속성

필드	설명
이름	연결의 이름입니다. 이 필드는 테이블에서 고유해야 합니다.
자격 증명	이 연결에 사용할 자격 증명을 지정합니다. 선택 사항입니다.
연결 별칭	연결 별칭은 런타임에 연결 및 자격 증명을 확인합니다. 한 번에 연결 별칭당 하나의 연결만 활성화됩니다.
활성	현재 연결을 활성화하려면 선택합니다.
도메인	연결이 속한 도메인입니다.

자격 증명은 비어 있지 않은 경우 활성 연결에서 고유합니다.

연결 정보 업그레이드

- JDBC 연결 [jdbc_connection] 및 JMS 연결 [orch_jms_ds] 테이블은 현재 연결 [sys_connection] 테이블에서 확장된 기존 Orchestration 연결 테이블입니다. 테이블은 원래 sys_metadata에서 확장되었습니다. sys_metadata 관련 데이터가 제거됩니다.
- 테이블은 오케스트레이션 런타임 플러그인 〔com.snc.runbook_automation.runtime〕에서 자격 증명 및 연결 플러그인으로 이동합니다.
- 업그레이드 프로세스는 JDBC 및 JMS 연결 정보를 가져오고 해당 연결 별칭을 작성하고 해당 연결에 별칭을 할당합니다.
- JDBC 필드 이름 변경:
  - JDBC 서버 이름이 호스트로 변경되었습니다.
  - 데이터베이스 포트의 이름이 포트로 변경되었습니다.
  - JDBC 서버 및 데이터베이스의 데이터는 업그레이드 중에 호스트 및 포트로 마이그레이션됩니다

PowerShell 및 SSH에 대한 기본 연결 만들기

PowerShell 또는 SSH(Secure Shell) 프로토콜을 사용하는 사용자 지정 활동 또는 작업에 사용할 연결 정보를 구성합니다.

시작하기 전에
필요한 역할: admin 또는 connection_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 자격 증명 및 연결 > 연결.
2. 새로 만들기를 클릭합니다.
3. **PowerShell &** SSH에 대한 기본 연결을 선택합니다.
4. 양식을 작성하십시오.

필드	설명
이름	연결 기록의 고유한 이름입니다.
자격 증명	연결 권한을 부여하는 데 사용할 자격 증명 레코드를 선택합니다.
연결 별칭	이 연결과 연결할 레코드 별칭을 선택합니다. 별칭을 사용하면 별칭을 사용하는 작업이나 활동을 재구성하지 않고도 연결 기록을 업데이트할 수 있습니다.
호스트	시스템에서 활동 또는 작업을 실행하는 대상 호스트의 전체 주소 도메인 이름입니다. 예를 들어 host.domain.com.
활성	이 연결을 활성화하려면 선택하십시오.
도메인	활동이 실행되는 도메인을 결정합니다. Flow Designer는 도메인 분리를 지원하지 않으며 이 필드를 무시합니다.
기본 포트 무효화	연결에 사용되는 대상 포트입니다. 이 필드를 비워 두면 시스템에서 기본 포트 값을 사용합니다.
MID 서버 사용	를 MID 서버통해 대상 호스트에 연결하려면 선택합니다. 선택하는 경우 고급 MID 서버 구성 섹션의 필드를 정의합니다. 주: PowerShell에는 .MID 서버
MID 선택	특정 MID 서버 또는 MID 클러스터를 선택하는 옵션입니다. ◦ **MID** 서버 자동 선택: MID 서버를 자동으로 선택합니다. ◦ 특정 **MID** 서버: 선택한 MID 서버를 사용합니다. ◦ 특정 **MID** 클러스터: 선택한 MID 클러스터를 사용합니다. 이 필드는 **MID** 서버 사용이 선택된 경우에 사용할 수 있습니다. 주: 통합 허브 연결 기록이 아니라 오케스트레이션 연결 기록이 참조되었는지 확인합니다.
역량	MID 서버가 선택 자격을 갖추려면 지원해야 하는 기능입니다. 시스템은 선택한 애플리케이션을 지원하는 MID 서버에서 작업을 실행합니다. **MID** 서버 사용이 선택된 경우에만 표시됩니다. 필수 기능에 따라 런타임 시 선택되는 항목이 결정됩니다 MID 서버 . 런타임 중에 a MID 서버 를 선택하는 방법에 대한 자세한 내용은 MID 서버 선택을 참조하십시오. 이 필드는 MID 선택 목록에서 **MID** 서버 자동 선택을 선택한 경우에만 표시됩니다.
MID 애플리케이션	MID 서버가 선택 자격을 갖추려면 지원해야 하는 애플리케이션입니다. 시스템은 선택한 애플리케이션을 지원하는 MID 서버에서 작업을 실행합니다. **MID** 서버 사용이 선택된 경우에만 표시되며, **MID** 선택 목록에서 **MID** 서버 자동 선택을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	런타임 중에 MID 서버가 선택되는 방법에 대한 자세한 내용은 MID Server 선택 문서를 참조하십시오.
MID 서버	단계가 실행되는 특정 MID 서버 단계입니다. 이 필드는 MID 선택 목록에서 특정 **MID** 서버를 선택한 경우에만 표시됩니다.
MID 클러스터	사용할 특정 MID 클러스터입니다. 이 필드는 **MID** 서버 사용이 선택되고 MID 선택 목록에서 특정 **MID** 클러스터를 선택한 경우에 사용할 수 있습니다.

5. 제출을 클릭합니다.

HTTP 연결 작성

HTTP 연결은 사용자 지정 HTTP 작업 또는 활동이 연결에 사용하는 정보를 제공합니다.

시작하기 전에

필요한 역할: connection_admin

프로시저

1. 다음으로 이동 모두 > 자격 증명 및 연결 > 연결을 클릭하고 새로 만들기를 클릭한 다음 **HTTP(s)** 연결을 선택합니다.
2. 다음 연결 정보를 추가하고 제출을 클릭합니다.

필드	설명
이름	이 HTTP 연결의 고유한 이름입니다.
자격 증명	연결 권한을 부여하는 데 사용할 자격 증명 레코드를 선택합니다.
연결 별칭	이 연결과 연결할 레코드 별칭을 선택합니다. 별칭을 사용하면 별칭을 사용하는 작업이나 활동을 재구성하지 않고도 연결 기록을 업데이트할 수 있습니다.
URL 작성기	연결 URL을 수동으로 입력하거나 시스템을 사용하여 입력을 기반으로 URL을 작성합니다. 기본값은 선택 취소되어 있습니다. 선택 시 연결 URL은 다음 필드에서 계산됩니다. ◦ 상호 인증 — 상호 인증이 사용되는 경우 확인란입니다. ◦ 프로토콜 — 상호 인증을 사용하지 않는 경우 protocol을 입력합니다. 기본값은 HTTPs입니다. ◦ 프로토콜 프로파일 — 상호 인증을 사용하는 경우 sys_protocol_profile에서 프로토콜 프로파일을 입력합니다. ◦ 호스트 ◦ 포트 ◦ 기본 경로 — 연결 문자열의 경로입니다. 주: 상호 인증을 선택하면 연결 URL이 구축됩니다: 프로토콜 + :// + 호스트:포트 + URL입니다. 상호 인증을 선택하지 않으면 연결 URL이 빌드됩니다. 프로토콜 프로파일 + :// + 호스트:포트 +URL

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
연결 URL	URL 작성기가 선택되어 있지 않은 경우 이 필드에 연결 URL을 입력합니다. 주: 상호 인증을 선택하면 연결 URL이 구축됩니다: 프로토콜 + :// + 호스트:포트 + URL입니다. 상호 인증을 선택하지 않으면 연결 URL이 빌드됩니다. 프로토콜 프로파일 + :// + 호스트:포트 +URL
활성	이 연결을 활성화하려면 확인란을 선택합니다.
도메인	작업 또는 활동이 실행되는 도메인을 확인합니다.
MID 서버 사용	이 작업 또는 활동에 MID 서버를 사용하려면 선택합니다. 선택하는 경우 고급 MID 서버 구성 섹션의 필드를 정의합니다.
MID 선택	특정 MID 서버 또는 MID 클러스터를 선택하는 옵션입니다. ◦ **MID** 서버 자동 선택: MID 서버를 자동으로 선택합니다. ◦ 특정 **MID** 서버: 선택한 MID 서버를 사용합니다. ◦ 특정 **MID** 클러스터: 선택한 MID 클러스터를 사용합니다. 이 필드는 **MID** 서버 사용이 선택된 경우에 사용할 수 있습니다. 주: 통합 허브 연결 기록이 아니라 오케스트레이션 연결 기록이 참조되었는지 확인합니다.
역량	MID 서버가 선택 자격을 갖추려면 지원해야 하는 기능입니다. 시스템은 선택한 애플리케이션을 지원하는 MID 서버에서 작업을 실행합니다. **MID** 서버 사용이 선택된 경우에만 표시됩니다. 필수 기능에 따라 런타임 시 선택되는 항목이 결정됩니다 MID 서버 . 런타임 중에 a MID 서버 를 선택하는 방법에 대한 자세한 내용은 MID 서버 선택을 참조하십시오. 이 필드는 MID 선택 목록에서 **MID** 서버 자동 선택을 선택한 경우에만 표시됩니다.
MID 애플리케이션	MID 서버가 선택 자격을 갖추려면 지원해야 하는 애플리케이션입니다. 시스템은 선택한 애플리케이션을 지원하는 MID 서버에서 작업을 실행합니다. **MID** 서버 사용이 선택된 경우에만 표시되며, **MID** 선택 목록에서 **MID** 서버 자동 선택을 선택합니다. 런타임 중에 MID 서버가 선택되는 방법에 대한 자세한 내용은 MID Server 선택 문서를 참조하십시오.
MID 서버	단계가 실행되는 특정 MID 서버 단계입니다. 이 필드는 MID 선택 목록에서 특정 **MID** 서버를 선택한 경우에만 표시됩니다.
MID 클러스터	사용할 특정 MID 클러스터입니다. 이 필드는 **MID** 서버 사용이 선택되고 MID 선택 목록에서 특정 **MID** 클러스터를 선택한 경우에 사용할 수 있습니다.
연결 시간 제한	호스트가 성공적으로 연결되기까지 시스템에서 기다리는 시간(밀리초)입니다. 이 시간 동안 연결에 성공하지 못하면 연결 요청이 시간 초과됩니다. 시스템 기본 연결 시간 제한 값을 사용하려면 이 필드를 비워두십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 연결 시간 제한 값을 0으로 설정하면 연결이 부실해질 수 있으므로 0으로 설정하지 마십시오.
additional_http_headers(속성 탭)	필요한 추가 헤더(예: sap-client=100)를 포함합니다. 헤더를 여러 개 추가하는 경우 세미콜론으로 구분합니다.
odata_ping_url(속성 탭)	기본 OData ping URL은 /sap/bc/ping입니다. OData 하트비트에 대한 ping URL을 편집하려면 잠금 아이콘을 선택하고 URL을 편집한 다음 잠금 아이콘을 다시 선택합니다.

3. 제출을 클릭합니다.
   사용자 지정 HTTP 작업 또는 활동을 생성할 준비가 되었습니다.

JDBC 연결 생성

JDBC 연결은 사용자 정의 JDBC 조치 또는 활동이 다양한 대상 데이터베이스에 연결하는 데 사용하는 정보를 제공합니다.

시작하기 전에

인스턴스와 함께 제공되는지 또는 사용자 지정 JAR 파일과 함께 제공되는지 여부에 관계없이 적절한 JAR 파일이 있어야 합니다.

주: 이 ServiceNow 인스턴스는 MySQL, SQLServer 및 Oracle 데이터베이스를 지원하는 현재 릴리스의 일부로 `mysql-connector-java-5.1.21.jar`, `sql-server-jdbc-4.0.jar` 및 `ojdbc6.jar` 파일을 제공합니다. Sybase 또는 DB2 Universal과 같은 다른 데이터베이스는 JDBC 연결을 설정하기 전에 인스턴스에 업로드해야 하는 사용자 정의 JAR 파일을 사용해야 합니다.

필요한 역할: connection_admin

이 태스크 정보

JDBC 자격 증명은 활동 디자이너 템플릿에 의해 별도로 검색되며 CyberArk와 같은 외부 자격 증명 스토리지를 지원합니다.

프로시저

1. 다음으로 이동 모두 > 자격 증명 및 연결 > 연결에서 새로 만들기를 클릭하고 **JDBC** 연결을 선택합니다.
2. 테이블의 필드를 사용하여 양식을 작성합니다.
   형식 필드의 데이터베이스 선택에 따라 사용 가능한 필드가 결정됩니다.

JDBC 연결 필드

필드	데이터베이스 형식	설명
이름	모두	이 JDBC 연결의 고유한 이름. 예를 들어 **JDBC MySQLProd**를 입력할 수 있습니다.
자격 증명	모두	JDBC 제공자에 대한 자격 증명을 추가합니다.
연결 별칭	모두	이 연결과 연결할 레코드 별칭을 선택합니다. 별칭을 사용하면 별칭을 사용하는 작업이나 활동을 재구성하지 않고도 연결 기록을 업데이트할 수 있습니다.
쿼리 제한 시간	모두	JDBC 쿼리가 응답 없이 실행될 수 있는 최대 경과 시간입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	데이터베이스 형식	설명
연결 시간 제한	모두	JDBC 연결 또는 연결 요청을 닫기 전에 시스템에서 대기하는 시간(초)입니다. 예를 들어 연결 시간 제한 값이 10초인 경우 시스템은 성공적으로 연결될 때까지 10초를 기다립니다. 이 시간 동안 연결에 성공하지 못하면 연결 요청이 시간 초과됩니다. 연결에 성공하면 10초 동안 비활성 상태가 될 때까지 연결이 열린 상태로 유지됩니다. 연결이 10초 동안 비활성 상태이면 연결이 닫힙니다. 주: 연결 시간 제한 값을 0으로 설정하면 연결이 부실해질 수 있으므로 0으로 설정하지 마십시오.
활성	모두	이 연결을 활성 상태로 만들려면 확인란을 선택합니다.
도메인	모두	이 테이블의 도메인입니다. 기본적으로 JDBC 연결 [jdbc_connection] 테이블은 전역 도메인에서 실행됩니다.
형식	모두	이 연결에 대한 데이터베이스 유형입니다. 기본 선택 항목은 다음과 같습니다. ◦ **MySQL** ◦ **Oracle** ◦ **SQLServer** ◦ 없음 적절한 JDBC 드라이버 JAR 파일을 인스턴스에 업로드하여 **Sybase** 또는 **DB2 Universal** 을 선택 목록에 추가할 수 있습니다. 오케스트레이션 는 이러한 드라이버가 시스템에 로드될 때 자동으로 인식하여 이 목록에 추가합니다.
호스트	Oracle, MySQL, SQLServer	데이터베이스 서버의 호스트 이름 또는 IP 주소입니다.
Oracle SID	Oracle	Oracle 데이터베이스 사이트 식별자입니다. 기본값은 **orcl**입니다.
Oracle 포트	Oracle	Oracle 데이터베이스에서 사용 중인 포트입니다. 기본값은 **1521**입니다.
데이터베이스 이름	내 SQL, SQLServer	데이터베이스의 이름입니다.
포트	MySQL, SQLServer	선택한 데이터베이스가 사용 중인 포트입니다.
인스턴스 이름	SQLServer	선택한 SQLServer의 인스턴스 이름
연결 URL	모두	MID 서버가 지정된 데이터베이스에 연결하는 데 사용하는 URL입니다. URL은 양식을 저장할 때 자동으로 생성되며 기본 데이터베이스의 경우 읽기 전용입니다. 주: 선택한 형식이 기본 데이터베이스 중 하나가 아닌 경우 MID 서버가 연결을 만드는 방법을 알 수 있도록 연결 URL을 수동으로 만들어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	데이터베이스 형식	설명
JDBC 드라이버	없음, DB2 유니버설, Sybase	기본 데이터베이스가 아닌 경우 이 연결에 사용할 JDBC 드라이버입니다. 주: Sybase 또는 DB2 유니버설 데이터베이스를 추가하는 경우 이 필드에 드라이버 이름을 입력하고 드라이버 JAR 파일을 인스턴스에 업로드해야 합니다.
MID 서버 사용	모두	이 작업 또는 활동에 MID 서버를 사용하려면 선택합니다. 선택하는 경우 고급 MID 서버 구성 섹션의 필드를 정의합니다.
MID 선택	모두	특정 MID 서버 또는 MID 클러스터를 선택하는 옵션입니다. ◦ **MID** 서버 자동 선택: MID 서버를 자동으로 선택합니다. ◦ 특정 **MID** 서버: 선택한 MID 서버를 사용합니다. ◦ 특정 **MID** 클러스터: 선택한 MID 클러스터를 사용합니다. 이 필드는 **MID** 서버 사용이 선택된 경우에 사용할 수 있습니다. 주: 통합 허브 연결 기록이 아니라 오케스트레이션 연결 기록이 참조되었는지 확인합니다.
역량	모두	MID 서버가 선택 자격을 갖추려면 지원해야 하는 기능입니다. 시스템은 선택한 애플리케이션을 지원하는 MID 서버에서 작업을 실행합니다. **MID** 서버 사용이 선택된 경우에만 표시됩니다. 필수 기능에 따라 런타임 시 선택되는 항목이 결정됩니다 MID 서버 . 런타임 중에 a MID 서버 를 선택하는 방법에 대한 자세한 내용은 MID 서버 선택을 참조하십시오. 이 필드는 MID 선택 목록에서 **MID** 서버 자동 선택을 선택한 경우에만 표시됩니다.
MID 애플리케이션	모두	MID 서버가 선택 자격을 갖추려면 지원해야 하는 애플리케이션입니다. 시스템은 선택한 애플리케이션을 지원하는 MID 서버에서 작업을 실행합니다. **MID** 서버 사용이 선택된 경우에만 표시되며, **MID** 선택 목록에서 **MID** 서버 자동 선택을 선택합니다. 런타임 중에 MID 서버가 선택되는 방법에 대한 자세한 내용은 MID Server 선택 문서를 참조하십시오.
MID 서버	모두	단계가 실행되는 특정 MID 서버 단계입니다. 이 필드는 MID 선택 목록에서 특정 **MID** 서버를 선택한 경우에만 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	데이터베이스 형식	설명
MID 클러스터	모두	사용할 특정 MID 클러스터입니다. 이 필드는 **MID** 서버 사용이 선택되고 MID 선택 목록에서 특정 **MID** 클러스터를 선택한 경우에 사용할 수 있습니다.

3. 제출을 클릭합니다.

관련 정보

JDBC 자격 증명

JMS 연결 작성

사용자 정의 JMS 활동 또는 조치와 함께 JMS(Java Messaging Service)를 사용하도록 시스템을 구성하십시오.

시작하기 전에
필요한 역할: connection_admin

이 태스크 정보
MID 서버에는 조직에 맞는 JMS 연결 팩토리가 있어야 합니다. 속성에 있는 속성에서 *mid.property.jms.command.allowed_factory_names* 해당 값을 구성합니다. **MID** 서버 > 속성. 이 특성의 기본값은 써드파티 JMS 제공자가 알리는 값 또는 쉼표로 구분된 값 목록으로 변경할 수 있습니다.

프로시저
1. 다음으로 이동 자격 증명 및 연결 > 연결.
2. 새로 만들기를 클릭하고 **JMS** 연결을 선택한 다음 양식을 작성한 다음 제출을 클릭하십시오.

옵션	설명
이름	이 연결 팩토리의 고유한 이름입니다.
자격 증명	JMS 제공자에 대한 자격 증명을 추가합니다.
연결 별칭	이 연결과 연결할 레코드 별칭을 선택합니다. 별칭을 사용하면 별칭을 사용하는 작업이나 활동을 재구성하지 않고도 연결 기록을 업데이트할 수 있습니다.
초기 컨텍스트 팩토리	InitialContext를 만드는 데 사용되는 JNDI 클래스의 이름입니다. 주: 예를 들어 ActiveMQ V5.10(JMS 제공자)에 연결하려면 이 값은 `org.apache.activemq.jndi.ActiveMQInitialConte`
제공자 URL	실행 중인 JMS 제공자 설치의 위치입니다. 주: 예를 들어 ActiveMQ V5.1에 연결하려면 다음을 수행합니다. `tcp://ipAddressOrHostName:61616`.
활성	이 연결을 활성 상태로 만들려면 확인란을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

옵션	설명
도메인	작업 또는 활동이 실행되는 도메인을 확인합니다.
MID 서버 사용	이 작업 또는 활동에 MID 서버를 사용하려면 선택합니다. 선택하는 경우 고급 MID 서버 구성 섹션의 필드를 정의합니다.
MID 선택	특정 MID 서버 또는 MID 클러스터를 선택하는 옵션입니다. ◦ **MID** 서버 자동 선택: MID 서버를 자동으로 선택합니다. ◦ 특정 **MID** 서버: 선택한 MID 서버를 사용합니다. ◦ 특정 **MID** 클러스터: 선택한 MID 클러스터를 사용합니다. 이 필드는 **MID** 서버 사용이 선택된 경우에 사용할 수 있습니다.
MID 클러스터	사용할 특정 MID 클러스터입니다. 이 필드는 **MID** 서버 사용이 선택되고 MID 선택 목록에서 특정 **MID** 클러스터를 선택한 경우에 사용할 수 있습니다.
역량	MID 서버가 선택 자격을 갖추려면 지원해야 하는 기능입니다. 시스템은 선택한 애플리케이션을 지원하는 MID 서버에서 작업을 실행합니다. **MID** 서버 사용이 선택된 경우에만 표시됩니다. 런타임 중에 MID 서버가 선택되는 방법에 대한 자세한 내용은 MID Server 선택 문서를 참조하십시오.
MID 애플리케이션	MID 서버가 선택 자격을 갖추려면 지원해야 하는 애플리케이션입니다. 시스템은 선택한 애플리케이션을 지원하는 MID 서버에서 작업을 실행합니다. **MID** 서버 사용이 선택된 경우에만 표시되며, **MID** 선택 목록에서 **MID** 서버 자동 선택을 선택합니다. 런타임 중에 MID 서버가 선택되는 방법에 대한 자세한 내용은 MID Server 선택 문서를 참조하십시오.

3. 다음으로 이동 연결 및 자격 증명 > 자격 증명.
4. 새로 만들기를 클릭하고 **JMS** 자격 증명을 선택한 다음 MID가 JMS 제공자와 통신하는 데 사용해야 하는 사용자 이름과 암호를 제공합니다.
   자세한 내용은 JMS 자격 증명을(를) 참조하십시오.
5. 제출을 클릭합니다.
   사용자 정의 JMS 조치 또는 활동을 작성할 준비가 되었습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통합 허브에 대한 연결 속성 생성

통합 허브 통합 단계에서 사용할 수 있는 연결별 변수를 정의합니다.

시작하기 전에

필요한 역할:

- 연결 속성을 만들려면 관리자 역할이 필요합니다.
- 속성 값을 할당하려면 connection_admin 또는 관리자 역할이 필요합니다.
- 사용자 지정 작업에서 속성을 사용하려면 action_designer 또는 관리자 역할이 필요합니다.

연결 속성은 에 대한 구독 통합 허브이 필요한 통합 단계에서만 사용됩니다. 활성화 통합 허브에 대한 자세한 내용은 다음을 참조하십시오. 요청 통합 허브 플러그인 .

이 태스크 정보

통합 단계를 사용하려면 외부 시스템과의 연결을 설정해야 합니다. 연결 인라인을 정의하는 대신 연결 및 자격 증명 별칭을 사용합니다. 별칭을 사용하면 모든 작업을 다시 구성할 필요 없이 연결 정보를 한 번 업데이트할 수 있습니다. 별칭을 사용하는 모든 작업 단계는 관련된 속성을 물려받습니다. 플로우 디자이너는 작업 단계로 드래그할 수 있는 속성을 데이터 알약으로 표시합니다. 예를 들어 REST 단계 쿼리 매개변수가 되는 페이지 크기 속성을 만들 수 있습니다.

사용자 지정 플로우 디자이너 작업을 빌드하는 방법에 대한 자세한 내용은 다음을 참조하십시오. 작업 디자이너 .

프로시저

1. 다음으로 이동 모두 > 자격 증명 및 연결 > 연결 및 자격 증명 별칭.
2. 별칭 기록을 생성하거나 선택합니다.
3. 연결 속성 관련 목록에서 새로 만들기를 클릭합니다.
4. 속성 레이블과 필드 유형을 정의합니다.
   필드 유형 목록은 필드 유형을 참조하십시오.
5. 고급 뷰 관련 링크를 클릭하여 속성에 대한 고급 딕셔너리 기본 설정을 설정합니다.
   예를 들어 동적으로 계산된 값을 갖는 속성을 만들 수 있습니다. 딕셔너리 입력 양식 문서를 참조하십시오.
6. 제출을 클릭합니다.
7. 연결 기록의 속성 값을 정의합니다.

   a. 다음으로 이동 자격 증명 및 연결 > 연결.

   b. 별칭과 동일한 연결 유형으로 연결 기록을 만들거나 선택합니다.

   c. 연결 별칭에서 연결 속성이 있는 별칭을 선택합니다.

   d. 레코드를 저장합니다.
      속성 탭은 별칭 기록에 정의된 연결 속성으로 채워집니다.

   e. 속성 값을 설정합니다.
      별칭에 다중 활성 연결 지원이 활성화되어 있는 경우 둘 이상의 연결 기록을 별칭과 연결하고 각 연결 기록에서 속성 값을 정의할 수 있습니다. 동일한 별칭에 대한 속성 값을 가진 연결 기록이 여러 개 있는 경우, 플로우 실행 시 사용되는 연결에 따라 속성 값이 결정됩니다. 예를 들어 두 개의 활성 연결 엔드포인트인 프로덕션과 테스트를 가지고 있으며 별칭을 사용하는 하나의 작업이 있다고 가정합니다. 이 속성은 런타임에 사용되는 연결에 의해 정의된 값을 해결합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

8. 의 작업 디자이너통합 단계에 별칭을 추가합니다.
   a. 플로우 디자이너 작업으로 이동하여 작업을 만들거나 선택합니다.
   b. 작업에 통합 단계를 추가합니다.
   c. 연결 세부 정보에서 속성을 생성한 별칭을 추가합니다.

   별칭과 연결된 연결 속성이 데이터 창에 데이터 알약으로 표시됩니다.

   주: 별칭을 단계에 연결한 후에는 연결 속성 레이블 및 데이터 유형에 대한 변경 사항이 추적되지 않습니다. 연결 속성 레이블 또는 데이터 유형을 새로 고치려면 단계에서 별칭을 삭제하고 다시 추가합니다.

자격 증명으로 시작

MID 서버는 자격 증명 [discovery_credentials] 테이블에서 만든 자격 증명을 사용하여 검색, 오케스트레이션, 서비스 매핑 및 클라우드 관리를 위한 자원에 액세스합니다.

MID Server에서 자격 증명을 사용하는 방법

기본적으로 Windows MID 서버는 호스트 시스템에서 MID 서버 서비스의 로그인 자격 증명을 사용하여 네트워크에서 장치를 검색합니다 Windows . 최소한 로컬 관리자 권한을 갖도록 Windows MID Server 서비스 자격 증명을 구성해야 합니다. 머신 UNIX 및 네트워크 장치의 경우 Linux MID 서버는 다음 인스턴스의 SSH 및 SNMP 자격 증명을 사용합니다 디스커버리 > 자격 증명.

사용하는 MID Server 오케스트레이션 는 워크플로우 활동 에서 지정한 대로 네트워크의 컴퓨터에서 명령을 실행하는 데 필요한 자격 증명에 액세스할 수 있어야 합니다. 오케스트레이션은 와 동일한 디스커버리SSH 및 SNMP 자격 증명을 사용할 수 있지만 특정 워크플로우 활동 Windows 용으로 설계된 두 가지 추가 자격 증명인 (PowerShell 활동의 경우) 및 VMware가 있습니다.

암호화 및 암호 해독

플랫폼은 자격 증명 [discovery_credentials] 테이블의 암호화된 필드에 자격 증명을 저장합니다. 일단 입력하면 볼 수 없습니다.

MID 서버가 자격 증명을 요청하면 다음 Now Platform 프로세스를 사용하여 자격 증명을 해독합니다.

1. 자격 증명은 password2 고정 키를 사용하여 인스턴스에서 해독됩니다.
2. 자격 증명은 MID 서버의 공개 키를 사용하여 인스턴스에서 다시 암호화됩니다.
3. 자격 증명은 SSL을 사용하여 부하 분산 장치에서 암호화됩니다.
4. 자격 증명은 SSL을 사용하여 MID 서버에서 해독됩니다.
5. 자격 증명은 MID 서버의 개인 키를 사용하여 MID 서버에서 다시 해독됩니다.

주: 플랫폼에는 다중 테넌트 인스턴스에 대한 별도의 암호화 키가 없습니다.

자격 증명 순서

자격 증명은 자격 증명 양식에서 순서 값을 할당할 수 있으며, 이를 통해 응용 프로그램은 특정 순서로 원하는 대로 모든 자격 증명을 시도할 수 있습니다. 순서 값을 지정하지 않으면 애플리케이션은 작동하는 자격 증명을 찾을 때까지 Credentials [discovery_credential] 테이블의 자격 증명을 임의로 시도합니다. 예를 들면 다음과 같습니다.

- 오케스트레이션이 Linux 또는 UNIX 컴퓨터와 같은 SSH 서버에서 명령을 실행하려고 합니다.
- 검색은 프린터, 라우터 또는 UPS와 같은 SNMP 장치를 쿼리하려고 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

장치에 대한 자격 증명을 식별한 디스커버리 후 오케스트레이션은 자격 증명 선호도 `[dscy_credentials_affinity]` 테이블을 사용하여 자격 증명과 장치 간의 선호도를 만듭니다. 이후의 모든 검색 또는 오케스트레이션 활동은 이 테이블의 자격 증명 정보를 선호도가 있는 장치와 일치시키려고 합니다. 장치의 자격 증명이 변경되면 디스커버리 Orchestration은 새로운 선호도를 만들 때까지 사용 가능한 모든 자격 증명을 다시 시도합니다.

주: 오케스트레이션 및(와 디스커버리)이 설치되고 자격 증명 별칭이 활성화된 경우 여러 선호도가 존재할 수 있습니다. 이 경우 플랫폼은 각 선호도에 대한 자격 증명을 조회하고 순서가 가장 낮은 선호도에 대한 자격 증명을 프로브에 삽입합니다.

자격 증명 순서는 다음과 같은 경우에 유용합니다.

- 자격 증명 테이블에는 많은 자격 증명이 포함되어 있으며 일부는 다른 자격 증명보다 더 자주 사용됩니다. 예를 들어 테이블에는 150개의 SSH 자격 증명이 포함되어 있으며 이러한 자격 증명 중 5개는 장치의 90%에 로그인하는 데 사용됩니다. 이러한 5개의 자격 증명을 낮은 순서 번호로 구성하여 실행 목록의 맨 위에 배치하는 것이 좋습니다. 디스커버리 및 Orchestration은 이러한 공통 자격 증명을 먼저 시도할 때 더 빠르게 작동합니다. 첫 번째 연결에 성공한 Now Platform 후에는 각 장치에 다음에 사용할 자격 증명을 알 수 있습니다.
- 공격적인 로그인 보안이 Now Platform 있습니다. 예를 들어, 네트워크의 Solaris 데이터베이스 서버가 MID 서버를 잠그기 전에 실패한 로그인 시도를 세 번만 제공하는 경우 낮은 순서 값으로 데이터베이스 자격 증명을 구성합니다.

자격 증명 별칭

자격 증명 별칭은 Discovery 및 Orchestration에 사용할 수 있습니다.

Discovery에 대한 별칭을 사용하면 관리자가 다음을 수행할 수 있습니다.

- 구성 가능한 준수 수준으로 자격 증명 필터링 동작을 사용합니다.
- 검색 일정에 여러 자격 증명 별칭을 할당합니다.
- 부적절하거나 민감한 자격 증명을 사용하는 자격 증명 선호도 생성을 방지합니다. 자세한 내용은 자격 증명 선호도를 참조하세요.

워크플로우 작성자는 오케스트레이션에 대한 별칭을 사용하여 다음을 수행할 수 있습니다.

- 오케스트레이션 워크플로우의 모든 활동에 개별 자격 증명 할당
- 플로우 디자이너의 모든 작업에 개별 자격 증명 할당
- 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당합니다.
- 디자이너 플로우에서 동일한 작업의 각 항목에 서로 다른 자격 증명을 할당합니다.

외부 자격 증명 스토어

인스턴스에 자격 증명을 저장하지 않으려면 외부 자격 증명 리포지토리를 사용할 수 있습니다. 외부 자격 증명 스토어는 인스턴스가 액세스할 수 있는 외부 사이트에 자격 증명을 저장합니다. CyberArk는 유일하게 지원되는 외부 자격 증명 저장소입니다. 그러나 다른 외부 저장소는 ServiceNow API를 사용하여 구성할 수 있습니다.

연결 및 자격 증명 별칭 생성

자격 증명 또는 연결 기록에 레이블을 지정하는 별칭을 정의합니다.

시작하기 전에

필요한 역할:

- 별칭을 만들려면 관리자 역할이 필요합니다.
- credential_admin 및 connection_admin 역할에는 별칭 기록에 대한 읽기 권한이 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보
연결 및 자격 증명 별칭은 자격 증명 또는 연결 기록에 레이블을 지정하는 별칭을 정의합니다.
별칭에는 다음 필드가 포함됩니다.

프로시저

1. 다음으로 이동 모두 > 연결 및 자격 증명 > 연결 및 자격 증명 별칭.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

연결 및 자격 증명 별칭

필드	설명
이름	별칭의 이름입니다. 별칭에는 알파, 숫자 및 밑줄 문자만 사용할 수 있습니다. 업그레이드 중에 자격 증명 기록의 태그는 연결 및 자격 증명 별칭으로 마이그레이션됩니다. 자격 증명 태그에 알파벳, 숫자 및 밑줄 이외의 특수 문자가 포함되어 있으면 업그레이드 후에도 태그 이름이 유지됩니다. 마이그레이션된 이 별칭을 계속 사용할 수 있지만 명명 제한을 충족하도록 이름을 변경할 때까지 별칭을 업데이트할 수 없습니다.
ID	연결 및 자격 증명 별칭의 고유 식별자로, `scope_name.alias_name` 형식을 기반으로 합니다. ◦ 범위가 전역인 경우 ID는 별칭 이름입니다. 예를 들어 전역 범위에서 Workday 별칭을 만들면 ID가 `Workday`로 설정됩니다. ◦ HR 앱 범위에서 Workday 별칭을 만들면 ID가 `x_hr_app.Workday`로 설정됩니다.
유형	자격 증명 또는 연결 및 자격 증명을 선택합니다. 기본값은 연결 및 자격 증명입니다.
애플리케이션	연결 및 자격 증명 별칭이 할당되는 애플리케이션 범위입니다. 애플리케이션 선택기에서 마지막으로 선택한 현재 세션 범위가 나타납니다. ◦ 예를 들어 이 세션의 현재 범위인 경우 전역 이 표시됩니다. ◦ 별칭을 생성하기 전에 애플리케이션 선택기에서 범위를 변경할 수 있습니다. 애플리케이션 범위와 선택 방법에 대한 자세한 내용은 다음을 참조하십시오. ▪ 애플리케이션 범위 ▪ 애플리케이션 선택기에서 애플리케이션 선택
연결 유형	연결 유형의 이름으로, 기본, HTTP, JDBC, JMS 또는 Kafka 중 하나입니다. 기본값은 HTTP입니다.
다중 활성 연결 지원	별칭이 여러 활성 연결을 지원하는지 여부를 나타내는 지정자입니다. 연결 테이블을 사용하여 연결을 추가하고 연결 관련 목록을 사용하여 별칭에 연결합니다.
기본 재시도 정책	별칭에 대한 재시도 정책입니다. 자세한 내용은 재시도 정책을 참조하세요.
구성 템플릿	연결 및 자격 증명 기록을 생성하는 데 사용할 구성 템플릿입니다.

4. 저장을 클릭합니다.
연결 및 연결 속성 관련 목록이 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

관련 목록	설명
연결	이 별칭과 연결된 관련 연결 기록입니다. 별칭을 생성한 후에는 연결 기록을 정의하고 별칭에 연결할 수 있습니다. 다중 활성 연결 지원을 선택하면 둘 이상의 연결을 별칭에 연결할 수 있습니다.
연결 속성	연결에 대한 속성입니다. 연결에 특정한 데이터를 정의하고 통합 단계에서 통합 허브 사용합니다. 자세한 내용은 통합 허브에 대한 연결 속성 생성 문서를 참조하십시오.
하위 별칭	상위 별칭과 연결된 하위 별칭입니다. 연결 및 자격 증명 별칭을 생성한 후에는 하위 별칭 을 생성하여 동일한 애플리케이션 통합에 대한 다중 연결을 구성할 수 있습니다.

관련 목록	설명
연결	이 별칭과 연결된 관련 연결 기록입니다. 별칭을 생성한 후에는 연결 기록을 정의하고 별칭에 연결할 수 있습니다. 다중 활성 연결 지원을 선택하면 둘 이상의 연결을 별칭에 연결할 수 있습니다.
연결 속성	연결에 대한 속성입니다. 연결에 특정한 데이터를 정의하고 통합 단계에서 통합 허브 사용합니다. 자세한 내용은 통합 허브에 대한 연결 속성 생성 문서를 참조하십시오.

5. 옵션: 자격 증명 별칭 *Related Links*과 관련된 새 자격 증명 및 연결을 작성하려면 아래에서 새 연결 및 자격 증명 작성을 클릭하십시오.
   결과로 생성되는 연결 및 자격 증명 기록은 미리 정의된 구성 템플릿을 기반으로 합니다. 연결 및 자격 증명 구성 템플릿을 참조하십시오.
6. 옵션: 연결 및 자격 증명 별칭에 대한 하위 별칭을 생성하려면 하위 별칭 관련 목록에서 새로 만들기를 선택합니다.

   a. 하위 별칭의 이름을 입력하고 제출을 선택합니다.
      하위 별칭은 상위 별칭에서 속성을 상속합니다. 그런 다음 고유한 연결 및 자격 증명 정보 집합을 포함하도록 하위 별칭을 구성할 수 있습니다.

다음에 수행할 작업
별칭 또는 하위 별칭과 연결할 하나 이상의 연결 기록을 생성합니다. 연결 생성에 대한 자세한 내용은 다음 문서를 참조하십시오 연결 시작하기. 별칭에 연결 속성을 추가하여 의 플로우 플로우 디자이너에서 연결 메타데이터를 사용할 수 있도록 합니다.

다음을 통해 **OAuth** 통합 설정 **MID** 서버

를 통해 MID 서버외부 공급업체 서버에 OAuth 토큰 요청을 보낼 수 있는 연결 기록을 생성합니다.

시작하기 전에
ServiceNow 통합 허브 표준 팩 설치 관리자를 구독했는지 확인합니다. 자세한 내용은 https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf 문서를 참조하십시오.

필요한 역할: admin

프로시저

구성 템플릿으로 연결을 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

a. 다음으로 이동 모두 > 통합 허브 > 구성 템플릿.

b. 새로 만들기를 선택합니다.

c. **OAuth** 클라이언트 자격 증명을 사용하는 **HTTP** 연결 부여 유형을 선택합니다.

d. 필요에 따라 양식을 업데이트합니다.
예를 들어 기본 데이터 템플릿 섹션의 `oauth_entity_profile_scope` 및 `oauth_entity_scope` 필드에 범위를 제공할 수 있습니다. 구성 템플릿을 만드는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 구성 템플릿 생성.

e. 제출을 선택합니다.
구성 템플릿을 생성했습니다.

f. 다음으로 이동 모두 > 통합 허브 > 연결 및 자격 증명 별칭.

g. 양식을 업데이트합니다.

연결 및 자격 증명 별칭

필드	설명
이름	별칭의 이름입니다. 별칭에는 알파, 숫자 및 밑줄 문자만 사용할 수 있습니다. 업그레이드 중에 자격 증명 기록의 태그는 연결 및 자격 증명 별칭으로 마이그레이션됩니다. 자격 증명 태그에 알파벳, 숫자 및 밑줄 이외의 특수 문자가 포함되어 있으면 업그레이드 후에도 태그 이름이 유지됩니다. 마이그레이션된 이 별칭을 계속 사용할 수 있지만 명명 제한을 충족하도록 이름을 변경할 때까지 별칭을 업데이트할 수 없습니다.
애플리케이션	연결 및 자격 증명 별칭의 고유 식별자로, `scope_name.alias_name` 형식을 기반으로 합니다. ◦ 범위가 전역인 경우 ID는 별칭 이름입니다. 예를 들어 전역 범위에서 Workday 별칭을 만들면 ID가 `Workday`로 설정됩니다. ◦ HR 앱 범위에서 Workday 별칭을 만들면 ID가 `x_hr_app.Workday`로 설정됩니다.
상위 별칭	이 연결 및 자격 증명 별칭을 생성하는 데 사용할 별칭을 선택하는 옵션입니다. 생성하려는 연결 및 자격 증명 별칭은 하위 별칭입니다. 하위 별칭은 상위 연결 및 자격 증명 별칭 페이지의 하위 별칭 탭 아래에 나열됩니다. 
유형	생성 중인 별칭의 유형을 나타내는 옵션입니다. 다음 옵션 중에서 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	◦ 자격 증명: 자격 증명 기록이 포함된 별칭입니다. ◦ 연결 및 자격 증명: 연결 및 자격 증명 기록을 모두 포함하는 별칭입니다. 이 옵션은 기본적으로 선택됩니다. 연결 및 자격 증명이 선택되었는지 확인합니다.
다중 활성 연결 지원	별칭이 여러 활성 연결을 지원하는지 여부를 나타내는 지정자입니다. 연결 테이블을 사용하여 연결을 추가하고 연결 관련 목록을 사용하여 별칭에 연결합니다.
기본 재시도 정책	별칭에 대한 재시도 정책입니다. 자세한 내용은 재시도 정책을 참조하세요.
구성 템플릿	연결 및 자격 증명 별칭을 생성하는 데 기반이 되는 구성 템플릿을 선택하는 옵션입니다. 생성한 **OAuth** 클라이언트 자격 증명을 사용하는 **HTTP** 연결 권한 유형 유형의 템플릿을 선택합니다.

h. 제출을 선택합니다.
연결 및 자격 증명 별칭 기록을 생성했습니다.

i. 다음으로 이동 모두 > 통합 허브 > 연결 대시보드.

j. 모든 연결 검색 필드에 생성한 연결 및 자격 증명 별칭 기록의 이름을 입력합니다.

k. 연결 및 자격 증명 별칭 기록에서 상세 정보 보기를 선택합니다.

l. 구성을 선택합니다.

m. 양식을 작성합니다.

연결 기록

필드	설명
연결 이름	연결 기록의 이름입니다. 이름을 업데이트할 수 없습니다.
연결 URL	외부 공급업체 서버와 연결하는 URL을 제공하는 옵션입니다.
MID 사용	MID 서버를 통해 OAuth 토큰 요청을 보내도록 지정하는 옵션입니다. 중요사항: 옵션이 선택되어 있는지 확인합니다.
MID 선택	특정 MID 서버를 사용할지, MID 서버의 자동 선택을 활성화할지, MID 클러스터를 사용할지

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	지정하는 옵션입니다. 다음 옵션 중 하나를 선택합니다. ◦ MID 서버 자동 선택 ◦ 특정 MID 서버 ◦ 특정 MID 클러스터
역량	하나 이상의 MID 서버 역량을 선택하는 옵션입니다. 기능은 IP 주소 범위 내에서 MID 서버의 특정 기능을 정의하며, 애플리케이션이 가장 적합한 MID 서버를 선택할 수 있도록 합니다. MID 기능 아이콘( )을 선택하여 하나 이상의 기능을 선택합니다. 주: 이 옵션은 MID 선택 필드에서 **MID** 서버 자동 선택을 선택한 경우 나타납니다.
MID 애플리케이션	MID 애플리케이션을 지정하거나 기본 애플리케이션 선택을 수락하는 옵션입니다. 주: 이 옵션은 MID 선택 필드에서 **MID** 서버 자동 선택을 선택한 경우 나타납니다. 기본적으로 **ALL** 옵션이 선택되어 있습니다.
MID 서버	MID 서버를 선택하는 옵션입니다. 주: 이 옵션은 MID 선택 필드에서 특정 **MID** 서버를 선택한 경우 나타납니다.
MID 클러스터	MID 클러스터를 선택하는 옵션입니다. 주: 이 옵션은 MID 선택 필드에서 특정 **MID** 클러스터를 선택한 경우 나타납니다.
OAuth 클라이언트 ID	클라이언트 ID를 지정하는 옵션입니다.
OAuth 클라이언트 비밀	클라이언트 암호를 지정하는 옵션입니다.
MID 서버를 통해 인증 서버에 연결	ServiceNow 인스턴스와 인증 서버 간의 연결이 MID 서버를 통해 발생하도록 지정하는 옵션입니다. 중요사항: 옵션이 선택되어 있는지 확인합니다.
OAuth 토큰 URL	OAuth 토큰을 요청하는 데 사용되는 OAuth 토큰 URL을 지정하는 옵션입니다.

n. OAuth 토큰 구성 및 가져오기를 선택합니다.
연결 및 자격 증명 기록이 생성됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

검색에 대한 자격 증명 별칭

에 대한 디스커버리 자격 증명 별칭을 사용하면 관리자가 검색 일정에 따라 특정 자격 증명을 사용할 수 있습니다. 시스템에서 별칭 사용을 얼마나 엄격하게 적용할지를 결정하는 별칭에 대한 동작을 구성할 수 있습니다.

자격 증명 별칭이 없으면 Discovery 일정에서 인스턴스에 정의된 모든 자격 증명에 액세스할 수 있습니다. 이 동작은 일부 상황, 특히 상승된 권한이 있는 자격 증명의 경우 바람직하지 않을 수 있습니다. 자격 증명 별칭은 Discovery 일정에서 사용할 수 있는 자격 증명을 보다 효과적으로 제어하고 상승된 권한으로 자격 증명이 불필요하게 노출되는 것을 방지합니다.

자격 증명 별칭의 작동 방식

검색 선호도 및 자격 증명 별칭 삽입(이전에는 *Discovery* 선호도 삽입)이라는 비즈니스 규칙은 기록이 ECC 큐에 삽입될 때 실행됩니다. 비즈니스 규칙은 MID 서버가 자격 증명 필터링을 수행할 수 있도록 검색 일정에 정의된 자격 증명 별칭을 프로브에 첨부합니다. MID Server의 첫 번째 작업은 검색할 자격 증명 목록을 만드는 것입니다. 선호도별로 자격 증명을 필터링한 다음 태그(있는 경우)별로 자격 증명을 필터링합니다. 선호도는 목록의 맨 위로 이동하고 일치하는 태그는 목록의 맨 아래로 이동합니다. MID 서버는 작동하는 자격 증명을 찾을 때까지 목록을 반복합니다. 그런 다음 MID 서버는 이 자격 증명에 대한 선호도를 생성합니다.

주: 자격 증명은 모든 자격 증명 태그와 일치해야 합니다.

비즈니스 규칙에서 장치에 대한 선호도가 존재한다고 판단하면 규칙은 사용할 적절한 *credential_id* 식별합니다. 자격 증명 `[discovery_credentials]` 테이블에 있는 기록의 *sys_id*입니다. 플랫폼에서 비즈니스 규칙에 *credential_alias* 것으로 정의된 자격 증명 별칭 값을 가진 선호도가 발견되면 비즈니스 규칙은 선호도에서 참조하는 자격 증명에 지정된 별칭이 있는지 여부를 결정합니다. 이 경우 비즈니스 규칙은 별칭 *credential_id* 선택하고 해당 값을 MID 서버에 전달합니다. 자격 증명에 지정된 자격 증명 별칭이 없는 경우 대상 시스템에 대해 존재하는 다른 선호도가 검사됩니다.

검색 자격 증명 별칭 생성

별칭을 생성한 다음 자격 증명 기록의 자격 증명에 해당 별칭을 추가합니다. 여러 별칭에 자격 증명을 추가하고 단일 별칭에 여러 자격 증명을 추가할 수 있습니다.

시작하기 전에

필요한 역할: admin, credential_admin(읽기 액세스 전용), connection_admin(읽기 액세스 전용)

이 태스크 정보

Discovery 일정은 해당 일정에 대해 정의된 별칭에 포함된 자격 증명만 사용합니다.

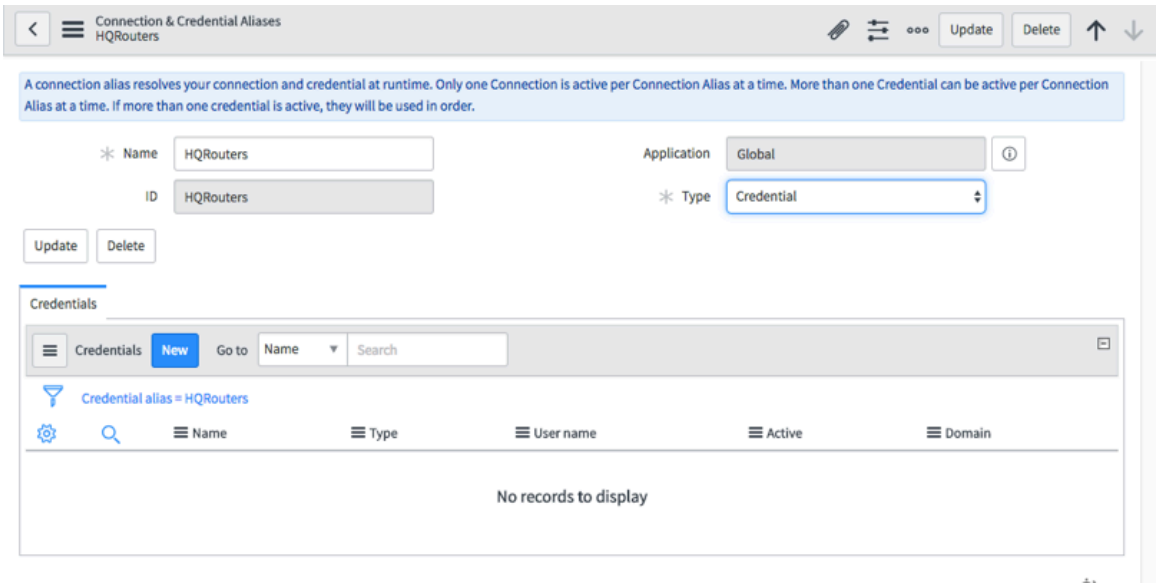
주: 일정에 대해 자격 증명 별칭이 정의된 경우 이 별칭은 해당 자격 증명 별칭을 사용하도록 설정된 일정에서 검색된 자격 증명과 대상 간의 기존 자격 증명 선호도를 무시합니다.

프로시저

1. 별칭을 생성합니다.
   a. 다음으로 이동 연결 및 자격 증명 > 연결 및 자격 증명 별칭.
   b. 새로 만들기를 클릭합니다.
   c. 별칭에 대한 고유 이름을 입력하고 별칭 유형에 대한 자격 증명을 선택합니다.
   d. 제출을 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자격 증명 관련 목록이 나타납니다. 이 별칭에 대한 새 자격 증명을 이 목록에서 추가할 수 있지만 기존 자격 증명은 추가할 수 없습니다.

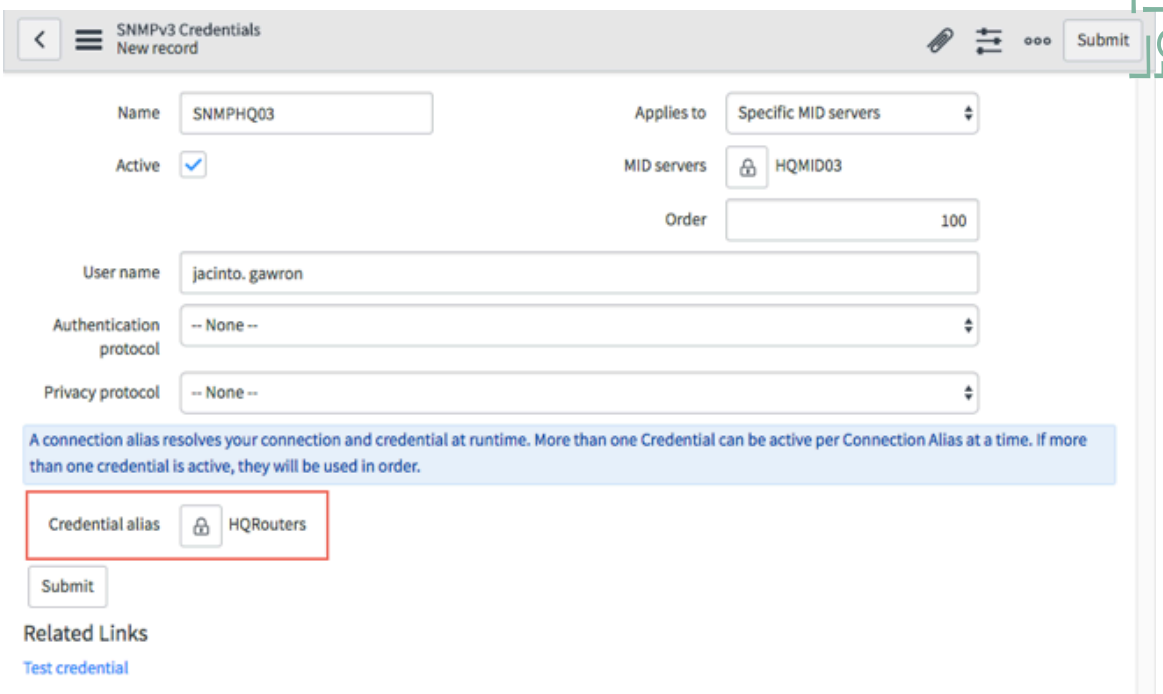


2. 새 별칭에 대한 자격 증명을 구성합니다.

a. 다음으로 이동 연결 및 자격 증명 > 자격 증명.

b. 목록에서 기존 자격 증명을 선택하거나 새로 만들기를 클릭하여 새 자격 증명을 생성합니다.

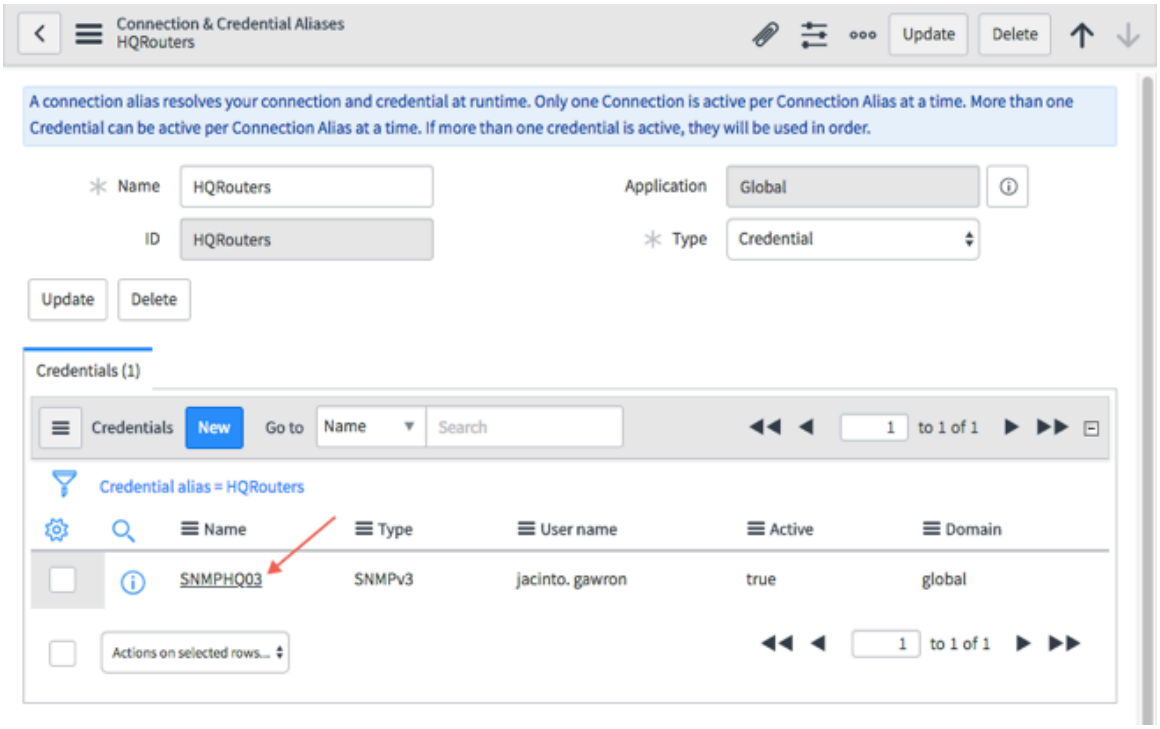
c. 자격 증명 기록에서 자격 증명 별칭 필드의 잠금을 해제하고 생성한 별칭을 선택합니다.



d. 기록을 저장하거나 제출합니다.

3. 반환 대상 연결 및 자격 증명 > 연결 및 자격 증명 별칭 을 클릭하고 새 별칭을 엽니다.
별칭에 연결한 자격 증명이 관련 목록에 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 이 별칭에 대한 추가 자격 증명을 생성하려면 관련 목록에서 새로 만들기를 클릭하고 자격 증명 유형을 선택합니다.
   별칭 이름은 자격 증명 기록의 자격 증명 별칭 필드에 미리 채워집니다.
5. 양식의 필드를 모두 채우고 기록을 제출합니다.

오케스트레이션 활동에 대한 자격 증명 별칭

자격 증명 별칭을 통해 관리자는 오케스트레이션 활동에 사용되는 자격 증명을 보다 잘 제어할 수 있습니다.

이 기능은 활동에 작업을 수행하기 위해 특정 자격 증명이 필요한 경우에 유용합니다. 자격 증명 태그를 사용하여 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있습니다.

자격 증명 별칭은 자격 증명 선호도 와 상호 작용하여 오케스트레이션 활동에 사용해야 하는 자격 증명을 결정합니다.

자격 증명 별칭의 작동 방식

검색 선호도 삽입(Geneva 릴리스에서는 자격 증명 선호도 삽입에서 이름이 변경됨)이라는 비즈니스 규칙은 기록이 ECC 큐에 삽입될 때 실행됩니다. 이 규칙은 장치에 대한 자격 증명 선호도가 있는지 여부를 확인하고 사용할 적절한 *credential_id*(자격 증명 `[discovery_credentials]` 테이블의 레코드 *sys_id*)를 식별합니다. 플랫폼에서 비즈니스 규칙에 *credential_alias* 자격 증명 별칭 값이 정의된 선호도가 발견되면 비즈니스 규칙은 선호도에서 참조하는 자격 증명에 지정된 별칭이 있는지 여부를 결정합니다. 이 경우 비즈니스 규칙은 자격 증명 별칭의 *credential_id* 선택하고 해당 값을 MID 서버에 전달합니다. 자격 증명에 지정된 자격 증명 별칭이 없는 경우 대상 시스템에 대해 존재하는 다른 모든 선호도가 확인됩니다. 적절하게 태그가 지정된 자격 증명을 참조하는 선호도가 없는 경우 MID 서버는 자격 증명 *[discovery_credentials]* 테이블을 반복하고 적절한 태그가 있는 자격 증명을 선택합니다. 그런 다음 MID 서버는 이 자격 증명에 대한 새 선호도를 만듭니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자격 증명 작성 및 테스트

검색, 서비스 매핑, 클라우드 관리 및 오케스트레이션이 네트워크의 하드웨어 및 소프트웨어에 액세스하는 데 필요한 자격 증명을 생성하고 테스트합니다.

시작하기 전에

필요한 역할: 관리자

조직의 보안 팀과 함께 보안 정책 및 옵션을 검토합니다.

이 태스크 정보

이 작업에는 자격 증명을 생성하는 일반적인 절차가 포함되어 있습니다. 특정 필드 및 요구 사항에 대한 자세한 내용은 자격 증명 유형에 대한 설명서를 참조하십시오.

지원되는 자격 증명 유형

애플리케이션 자격 증명	기본 인증 자격 증명	Chef 서버 자격 증명
CIM 자격 증명	클라우드 자격 증명	Infoblox 자격 증명
JDBC 자격 증명	JMS 자격 증명	OAuth 2.0 자격 증명
SAP 자격 증명	SNMP 자격 증명	SSH 자격 증명
VMware 자격 증명	Windows 자격 증명	컨테이너 이미지 리포지토리 자격 증명

주: 보안을 향상시키려면 자격 증명의 범위를 특정 MID 서버로 제한하거나 불필요한 자격 증명을 피하도록 예약합니다.

프로시저

1. 다음 모듈 중 하나로 이동합니다.
   - 디스커버리 > 자격 증명
   - 서비스 매핑 > 자격 증명
   - 오케스트레이션 > 자격 증명
2. 새로 만들기를 클릭합니다.
3. 자격 증명 페이지에서 자격 증명 유형에 대한 링크를 클릭하고 양식을 작성합니다.

   자세한 내용은 선택한 자격 증명 유형의 설명서를 참조하십시오.

   자격 증명 기록을 먼저 제출한 다음 나중에 테스트하거나 저장하기 직전에 자격 증명을 테스트할 수 있습니다.

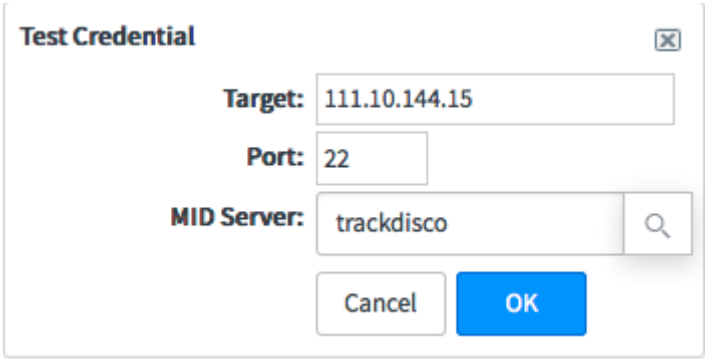
   다음 자격 증명 유형에 대해 자격 증명 테스트가 지원됩니다.
   - SSH 개인 키
   - 기간
   - SNMP v3
   - VMWare
   - JDBC
   - JMS
4. 관련 링크에서 자격 증명 테스트를 클릭합니다.

   주: 자격 증명은 테스트 중에 항상 암호화됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

5. 자격 증명 테스트 대화 상자의 필드를 작성합니다.

자격 증명 테스트 대화 상자



자격 증명 테스트 필드

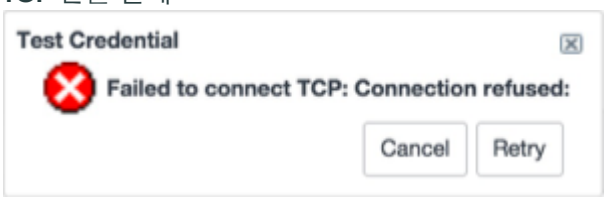
필드	설명	자격 증명 유형
대상	이러한 자격 증명이 실행되는 대상 호스트입니다. 이 값은 호스트 URL이 될 수 있는 VMware를 제외한 모든 자격 증명 유형의 IP 주소여야 합니다. MID 서버를 대상으로 지정할 수 없습니다. 주: JMS의 경우 제공자 URL입니다. 이 URL의 정보는 JNDI에 JMS 제공자를 찾고 액세스하는 방법을 알려줍니다. ActiveMQ V5.1에 연결하는 값의 예는 `tcp://ipAddressOrHostName:61616` 입니다.	모두
포트	이 테스트에 사용할 대상의 포트입니다. 시스템은 이 필드를 선택된 자격 증명 유형의 기본 포트로 미리 채웁니다.	모두
MID 서버	이 테스트에 사용할 MID 서버입니다. Windows 자격 증명을 테스트하려면 Windows MID 서버를 사용해야 합니다. 사용 가능 및 확인됨 MID Server만 사용할 수 있습니다.	모두
DB 유형	이 자격 증명을 테스트할 데이터베이스 유형입니다.	JDBC
DB 이름	이 자격 증명을 테스트할 데이터베이스의 이름입니다.	JDBC
초기 컨텍스트 팩토리	InitialContext를 만드는 데 사용되는 JNDI 클래스의	JMS

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명	자격 증명 유형
	이름입니다. 이 초기 컨텍스트 팩토리를 사용하여 JMS Connection과 같은 다양한 JMS 오브젝트가 생성됩니다. 예를 들어 ActiveMQ V5.10(JMS 제공자)에 연결하려면 이 필드의 값이 `org.apache.activemq.jndi.ActiveMQInitialContextFactory`여야 합니다.	

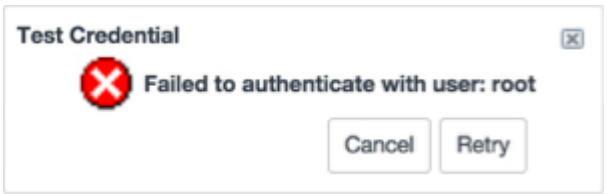
6. 확인을 클릭하여 테스트를 시작합니다.
   시스템이 제공한 자격 증명을 사용하여 대상에 연결을 시도하고 있음을 나타내는 표시기가 나타납니다. 인스턴스가 대상에 연결되면 성공 메시지가 표시됩니다. 제공한 테스트 입력에 문제가 발생하면 인스턴스에 적절한 오류 메시지가 표시됩니다. 다음은 몇 가지 일반적인 오류 메시지입니다.
   - 잘못된 대상 또는 포트 번호:

     TCP 연결 실패

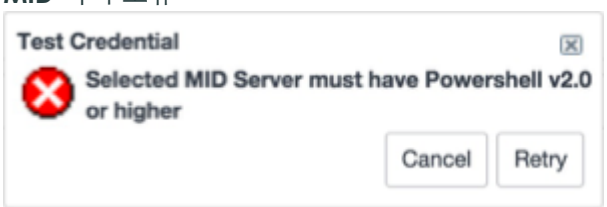
   - 잘못된 사용자 이름 또는 암호:

     인증 실패

   - Windows용 MID 서버 자격 증명이 올바르지 않음:

     MID 서버 오류

7. 재시도를 클릭하여 자격 증명 테스트 대화 상자를 열고 입력 오류를 수정합니다.
8. 자격 증명 테스트가 성공하면 제출 을 클릭하여 기록을 저장합니다.

중요사항: 자격 증명을 테스트한다고 해서 해당 자격 증명에 의도한 Discovery 또는 오케스트레이션 워크플로우 작업에 필요한 권한이 있는지 확인할 수 있는 것은 아닙니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Ansible Tower 자격 증명

Ansible 구성 관리 계정에 접근하려면 Ansible Tower 자격 증명이 필요합니다. 이러한 자격 증명을 사용하여 애플리케이션을 통해 클라우드 관리 Ansible 자원을 관리합니다.

클라우드 프로비저닝 및 거버넌스를 Ansible 구성 관리 계정과 통합하려면 Ansible에서 관리자 계정의 사용자 이름과 암호를 구성해야 합니다.

Ansible Tower 자격 증명을 위한 양식 필드

필드	설명
이름	설명적인 이름을 입력합니다.
사용자 이름/암호	관리자 권한이 있는 Ansible Tower 사용자의 인증 자격 증명을 입력하십시오.

주: 다른 필드는 구성할 필요가 없습니다.

API 키 자격 증명

API 키는 호출 애플리케이션 또는 사용자를 식별하기 위해 API에 전달되는 고유한 코드입니다.

API 키 자격 증명

API 키 자격 증명 양식 필드

필드	입력 값
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
API 키	API 키를 입력합니다.
자격 증명 별칭	플로우 및 워크플로우 작성자가 플로우 또는 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 플로우 또는 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.

애플리케이션 자격 증명

일부 애플리케이션에는 해당 호스트 머신에 필요한 자격 증명 외에 자격 증명이 필요합니다. 이러한 애플리케이션에 액세스하는 데 필요한 자격 증명을 애플리케이션 자격 증명이라고 합니다.

일반적인 자격 증명에는 장치 또는 애플리케이션에 로그인하기 위한 사용자 이름과 암호가 포함됩니다. 대부분의 애플리케이션에는 액세스를 위한 자격 증명이 하나만 필요하지만 일부 호스트와 애플리케이션에는 추가 보안을 위해 별도의 자격 증명이 있습니다. 예를 들어 ABAP SAP Central Services(ASCS)에서는 ASCS를 호스트하는 서버의 경우 SSH 또는 Windows 호스트 자격 증명 외에도 애플리케이션 자격 증명이 필요합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: ServiceNow 애플리케이션은 CI(구성 항목)로 서비스 인스턴스를 구성하는 장치 및 애플리케이션을 말합니다.

호스트 자격 증명과 마찬가지로 MID 서버에 애플리케이션 자격 증명을 할당합니다.

CI 유형별로 애플리케이션 자격 증명을 생성할 수 있습니다. 예를 들어 ASCS의 CI 유형은 SAP ASCS 애플리케이션(cmdb_ci_appl_sap_ascs)입니다. 이 CI 유형에 속한 CI를 검색하기 위한 미리 구성된 패턴에는 MID 서버가 이 CI 유형에 애플리케이션 자격 증명을 사용할 것을 요청하는 명령이 포함되어 있습니다. 이 CI 유형에 대해 구성된 자격 증명이 두 개 이상 있는 경우 MID 서버는 적합한 자격 증명을 찾을 때까지 정의된 순서대로 해당 자격 증명을 사용하려고 합니다.

ServiceNow 설명서의 디스커버리 요구 사항 정보를 확인하여 특정 애플리케이션 CI에 대해 애플리케이션 자격 증명을 구성해야 하는지 여부를 판단합니다. 디스커버리 필요 조건에 언급되지 않은 경우에는 애플리케이션 자격 증명을 구성할 필요가 없습니다.

애플리케이션 자격 증명 양식 필드

필드	설명
이름	자격 증명의 이름입니다. Oracle DB 또는 London Oracle DB(Oracle 데이터베이스의 경우)와 같은 설명적인 이름을 사용합니다. 자격 증명 이름에 공백이나 특수 문자를 사용하지 않아야 합니다.
활성	이 자격 증명을 사용하려면 확인란을 선택하십시오.
사용자 이름	애플리케이션 자격 증명의 실제 사용자 이름을 입력합니다.
암호	애플리케이션 자격 증명의 실제 암호를 입력하십시오. 자격 증명 이름에 공백이나 특수 문자를 사용하지 않아야 합니다.
CI 유형	CI가 속한 CI 유형을 선택하십시오.
자격 증명 별칭	별칭을 만들어 특정 검색 일정에 대한 특정 자격 증명을 할당합니다. 별칭을 할당할 때, 애플리케이션이 애플리케이션 자격 증명을 사용하는 CI 유형의 테이블 이름을 지정해야 합니다. 애플리케이션은 자체 CI 유형과는 다른 애플리케이션 자격 증명을 사용할 수 있습니다. 특정 애플리케이션의 경우, 적합한 테이블에 대한 목록을 참조하십시오. • ABAP SAP Central Services(ASCS): cmdb_ci_appl_sap_ascs • IBM Security Access Manager 어플라이언스: cmdb_ci_app_server_webseal • SAP Central Instance: 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 (for Microsoft Exchange): cmdb_ci_exchange_mailbox • Microsoft SQL Database: cmdb_ci_db_mssql_instance • MySQL Server: cmdb_ci_db_mysql_instance • Oracle Advanced Queue Queue: cmdb_ci_db_ora_instance • Oracle Database: cmdb_ci_db_ora_instance • Oracle E-Business Suite: cmdb_ci_db_ora_instance

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

애플리케이션 자격 증명 양식 필드

필드	설명
	• Oracle WebLogic Module: cmdb_ci_app_server_weblogic • Tibco Enterprise Message Service (EMS): cmdb_ci_appl_tibco_message
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.

기본 인증 자격 증명

기본 인증 자격 증명 유형은 기본 인증 자격 증명을 저장하는 액세스를 관리합니다.

이러한 필드는 기본 인증을 위해 자격 증명 양식에서 사용할 수 있습니다.

기본 인증 자격 증명 양식

필드	입력 값
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다. 예를 들어 기본 인증이라고 할 수 있습니다.
사용자 이름	사용자 이름을 입력합니다.
암호	암호를 입력합니다.
자격 증명 ID	CyberArk 외부 자격 증명 스토리지 시스템에서 이러한 자격 증명에 대해 구성된 고유 키를 입력합니다. 여러 안전 장치가 사용 중일 때 자격 증명 ID를 안전 재정의로 사용할 수 있습니다. 기본적으로 자격 증명 **ID** 필드의 구문은 다음과 같습니다 *<safe name>:<Credential ID>*. 안전한 이름이 생략된 경우 `config.xml` 파일에 정의된 안전한 이름이 있어야 합니다. 구분 기호 문자를 기본 콜론에서 다른 문자로 변경하려면 선택적 *ext.cred.safe_name* 매개 변수로 값을 재정의합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 저장소 확인란이 선택된 경우에만 표시됩니다.
외부 자격 증명 스토어	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Chef 서버 자격 증명

Chef 서버 자격 증명은 인스턴스와 Chef 통합에 액세스합니다.

이러한 필드는 Chef 서버 유형 자격 증명에 대한 자격 증명 양식에서 사용할 수 있습니다. 이 정보는 Chef 서버 설치를 수행할 때 구성한 설정에서 가져옵니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
관리자 이름	Chef 서버 설치 중에 만든 관리자 이름을 제공합니다.
관리자 키	관리자를 만들 때 Chef 서버에서 생성한 RSA 개인 키를 입력합니다.
확인 도구 이름	유효성 검사기를 입력합니다.
확인 도구 키	조직을 작성할 때 Chef 서버에서 생성한 RSA 개인 키를 입력하십시오.
인증서 이름	인증 이름을 입력합니다.
인증서 키	인증 키를 입력합니다.

CIM 자격 증명

CIM 자격 증명 유형은 VMware ESX 서버에 대한 정보를 위해 CIM 서버(CIMOM(Common Information Model Object Manager)이라고도 함)에 대한 접근을 관리합니다. 이 자격 증명 유형은 검색에 사용할 수 있습니다.

이러한 필드는 CIM의 자격 증명 양식에서 사용할 수 있습니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
사용자 이름	자격 증명 테이블에 생성할 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다. CIM 검색의 경우 사용자에게 관리자 역할이 있어야 합니다.
암호	암호를 입력합니다.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다. 서비스 매핑 및 디스커버리 패턴을 사용하여 이 CI 유형에 속하지 않는 CI를 검색하는 데 자격 증명을 사용하려면 CI가 속한 CI 유형의 테이블 이름(예: cmdb_ci_apache_web_server)을 입력하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
외부 자격 증명 스토리지	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화된 경우에만 사용할 수 있습니다. 주: 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다. 주: 특정 **MID** 서버를 선택해도 MID 서버 선택에 영향을 주지 않습니다. 이는 자격 증명에 대한 가시성을 확보해야 하는 MID Server를 결정하는 데만 사용됩니다. 오케스트레이션 활동에서는 특정 **MID Server**가 지원되지 않습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
Windows MID 서버 서비스 계정	활성 상태인 경우 정의된 자격 증명은 MID 서버 서비스 계정을 표현합니다.

CIM 자격 증명에 대한 **NetApp** 스토리지 장치 구성

NetApp 저장소 장치를 탐색하려면 추가 구성이 디스커버리 필요합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 저장소 장치 호스트에 SMI-S 에이전트를 설치합니다.

   을 참조하십시오 " 데이터 ONTAP SMI-S 에이전트 5.2 설치 및 구성 가이드 " 지침 및 요구 사항은 을 참조하십시오.

   주:

   ServiceNow 는 이 사이트의 문서를 유지관리하지 않습니다. 이 문서는 예고 없이 변경될 수 있습니다.

2. SMI-S 에이전트에 대한 사용자 계정 및 암호를 생성합니다.
3. SMI-S 에이전트 자격 증명에 대한 자격 증명 기록을 생성합니다.
   자격 증명 유형을 **CIM**으로 설정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라우드 자격 증명

클라우드 자격 증명 유형은 Amazon Web Services 및 Microsoft Azure 클라우드를 포함한 클라우드 기반 애플리케이션에 대한 액세스를 관리합니다.

AWS Identity and Access Management(IAM) 역할

AWS 클라우드의 Amazon EC2에 MID Server가 설치되어 있고 해당 MID Server가 클라우드 내에서 자원을 검색하도록 구성되어 있는 경우, 인스턴스에서 관리되는 자격 증명 대신 AWS Identity and Access Management(IAM) 역할이 제공하는 보안 자격 증명을 사용할 수 있습니다. 이러한 AWS 자격 증명은 역할에 따라 인스턴스 프로파일을 통해 클라우드에서 권한을 부여합니다. 이러한 자격 증명은 일시적이며 구성 가능한 간격으로 자동 순환됩니다. IAM 역할이 MID 서버에 정의된 경우. 자세한 내용은 AWS IAM 역할에 대한 MID 서버 구성 섹션을 참조하세요.

검색은 인스턴스 프로파일에서 역할에 의해 부여된 자격 증명을 위해 인스턴스에 저장된 자격 증명을 무시합니다. AWS 인스턴스 프로파일에 대한 자세한 내용은 Amazon EC2의 IAM 역할을 참조하십시오.

AWS 자격 증명

AWS 자격 증명 양식 필드

필드	입력 값
이름	AWS 자격 증명에 대한 고유하고 설명적인 이름입니다.
활성	자격 증명을 사용하는 옵션입니다.
접근 키 ID	AWS 관리 콘솔에서 생성한 접근 키 **ID**(예: APIAIOSFODNN7EXAMPLE)입니다.
비밀 접근 키	AWS 관리 콘솔에서 생성한 비밀 접근 키(예: wPalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)입니다.

Azure 서비스 주체 자격 증명 양식 필드

필드	값
이름	인스턴스에 등록할 서비스 주체의 이름을 입력합니다.
테넌트 ID 및	Azure Portal의 Azure 디렉터리 **ID** 값을 클라우드 관리 테넌트 **ID** 필드에 붙여넣습니다.
클라이언트 ID	Azure에서 등록한 애플리케이션의 Azure 애플리케이션 **ID** 값을 클라우드 관리 클라이언트 **ID** 필드에 붙여넣습니다.
인증 방법	클라이언트 비밀을 선택합니다. 주: 클라이언트 어설션은 지원되지 않습니다.
비밀 키	Azure 서비스 주체를 만드는 동안 생성된 비밀 키를 붙여넣습니다. 이 필드는 인증 방법이 클라이언트 비밀인 경우 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Azure Enterprise 계약 자격 증명

Azure 엔터프라이즈 계약 자격 증명은 Cloud Management 애플리케이션에서 제공하는 청구 기능에 필요합니다.

Azure Enterprise 계약 자격 증명 양식 필드

필드	설명
이름	설명적인 이름을 입력합니다.
등록 번호	Azure의 등록 번호를 입력합니다.
접근 키	Azure에서 제공하는 접근 키를 붙여넣습니다.

클라우드 관리 자격 증명

이 자격 증명 유형은 오케스트레이션에 사용할 수 있습니다.

클라우드 관리 자격 증명 양식 필드

필드	입력 값
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다. 예를 들어 클라우드 애틀랜타라고 할 수 있습니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
유형	**AWS**를 지정합니다.
사용자 이름	자격 증명 테이블에 생성할 CIM 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다.
암호	CIM 암호를 입력합니다.
SSH 암호 구문	키 생성을 위해 기억에 남는 문구를 입력합니다. 예를 들어 **Friday is a good** day를 입력할 수 있습니다.
SSH 개인 키	SSH 개인 키를 입력합니다.
인증 프로토콜	인증 키를 생성하는 데 사용된 **MD5**또는 **SHA** 인증 프로토콜을 선택합니다.
인증 키	SSH 생성 인증 키를 입력합니다.
개인 프로토콜	개인 키에 대한 암호화를 설명하는 다음 개인 프로토콜 중 하나를 입력합니다. • 3중 데이터 암호화 표준(DES)을 위한 **3DES** • 128비트 암호화를 사용하는 AES(Advanced Encryption Standard)용 **AES128** • **AES192** (192비트 암호화를 사용하는 AES용 AES) • AES256비트 암호화를 사용하는 **AES256** • 레거시 DES 암호화를 위한 **DES**
추가 개인 키를 입력합니다.	
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

클라우드 관리 자격 증명 양식 필드

필드	입력 값
외부 자격 증명 저장소	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
분류	CI 검색을 위한 애플리케이션 분류를 입력합니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.

클라우드 관리**(CMP)** 노드 자격 증명

클라우드 관리(CMP) 노드 자격 증명은 클라우드 관리가 프로비저닝하는 가상 서버의 자격 증명을 연결합니다. 클라우드 관리 애플리케이션에서 이러한 자격 증명을 자동으로 생성합니다.

주: 더 이상 사용하지 않으려는 경우 이러한 자격 증명을 비활성화하거나, 순서 우선순위를 변경하거나, 액세스가 허용된 MID 서버를 선택해야 할 수도 있습니다. 그렇지 않으면 이 유형의 자격 증명을 수동으로 만들거나 수정할 필요가 없습니다.

CMP 노드 자격 증명 양식 필드

필드	설명
이름	가상 머신이 있는 데이터센터를 기반으로 자동 생성된 이름입니다.
활성	자격 증명이 활성 상태인 경우입니다.
적용 대상	특정 MID 서버 또는 모든 MID 서버에서 이 자격 증명을 사용할 수 있는지 여부를 선택합니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
사용자 이름 및 암호	가상 서버 사용자 이름 및 암호입니다.
SSH 암호 구문 및 SSH 개인 키	가상 서버에서 필요로 할 경우 키를 보호하는 개인 키와 암호 구문입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CMP 노드 자격 증명 양식 필드

필드	설명
인증 프로토콜 및 인증 키	가상 서버에서 필요로 할 경우 키를 보호하는 개인 키와 암호 구문입니다.
개인 프로토콜 및 개인 키	가상 서버와 함께 사용하는 암호화 프로토콜로, 개인 키를 입력합니다.
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다.

클라우드 관리**(CMP) SSH** 키 쌍 자격 증명

클라우드 관리(CMP) SSH 키 쌍은 사용자가 스택 자원을 프로비저닝할 때 클라우드 관리 애플리케이션이 자동으로 생성하는 키를 저장합니다.

주: 더 이상 사용하지 않으려면 이러한 자격 증명을 비활성화해야 할 수 있습니다. 그렇지 않으면 이 유형의 자격 증명을 수동으로 만들거나 수정할 필요가 없습니다.

CMP SSH 키 페어 자격 증명 양식 필드

필드	설명
이름	자동으로 생성된 이름입니다.
활성	자격 증명이 활성 상태인 경우입니다.
SSH 공개 키	공개 키입니다.
SSH 개인 키	SSH 로그인에 대한 암호 대신 사용할 수 있는 보안 개인 키입니다.

Infoblox 자격 증명

클라우드 관리 애플리케이션에서 IPAM(IP 풀)을 설정하려면 Infoblox 자격 증명이 필요합니다.

이러한 필드는 Infoblox 유형 자격 증명에 대한 자격 증명 양식에서 사용할 수 있습니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
적용 대상	특정 MID 서버 또는 모든 MID 서버에서 이 자격 증명을 사용할 수 있는지 여부를 선택합니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
wAPI 버전	사용 중인 wAPI 버전을 입력합니다.
사용자 이름 및 암호	InfoBlox 사용자 이름 및 암호를 입력합니다.

JDBC 자격 증명

JDBC 자격 증명 유형은 JDBC(Java Database Connectivity) 연결에 대한 액세스를 관리합니다. 이 자격 증명 유형은 검색 및 오케스트레이션에 사용할 수 있습니다.

이러한 필드는 JDBC 유형 자격 증명에 대한 자격 증명 양식에서 사용할 수 있습니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
사용자 이름	자격 증명 테이블에 생성할 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다. CIM 검색의 경우 사용자에게 관리자 역할이 있어야 합니다.
암호	암호를 입력합니다.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다. 서비스 매핑 및 디스커버리 패턴을 사용하여 이 CI 유형에 속하지 않는 CI를 검색하는 데 자격 증명을 사용하려면 CI가 속한 CI 유형의 테이블 이름(예: cmdb_ci_apache_web_server)을 입력하십시오.
외부 자격 증명 스토리지	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화된 경우에만 사용할 수 있습니다. 주: 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다. 주: 특정 **MID** 서버를 선택해도 MID 서버 선택에 영향을 주지 않습니다. 이는 자격 증명에 대한 가시성을 확보해야 하는 MID Server를 결정하는 데만 사용됩니다. 오케스트레이션 활동에서는 특정 **MID Server**가 지원되지 않습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
Windows MID 서버 서비스 계정	활성 상태인 경우 정의된 자격 증명은 MID 서버 서비스 계정을 표현합니다.

JMS 자격 증명

JMS 신임 정보 유형은 JMS(Java Message Service)에 대한 액세스를 관리합니다. 이 자격 증명 유형은 검색 및 오케스트레이션에 사용할 수 있습니다.

이러한 필드는 JMS의 자격 증명 양식에서 사용할 수 있습니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
사용자 이름	자격 증명 테이블에 생성할 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다. CIM 검색의 경우 사용자에게 관리자 역할이 있어야 합니다.
암호	암호를 입력합니다.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	서비스 매핑 및 디스커버리 패턴을 사용하여 이 CI 유형에 속하지 않는 CI를 검색하는 데 자격 증명을 사용하려면 CI가 속한 CI 유형의 테이블 이름(예: cmdb_ci_apache_web_server)을 입력하십시오.
외부 자격 증명 스토리지	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화된 경우에만 사용할 수 있습니다. 주: 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다. 주: 특정 **MID** 서버를 선택해도 MID 서버 선택에 영향을 주지 않습니다. 이는 자격 증명에 대한 가시성을 확보해야 하는 MID Server를 결정하는 데만 사용됩니다. 오케스트레이션 활동에서는 특정 **MID Server**가 지원되지 않습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
Windows MID 서버 서비스 계정	활성 상태인 경우 정의된 자격 증명은 MID 서버 서비스 계정을 표현합니다.

OAuth 2.0 자격 증명

ServiceNow는 OAuth 2.0 자격 증명을 사용하여 HTTP 서비스의 사용자 계정에 액세스할 수 있습니다.

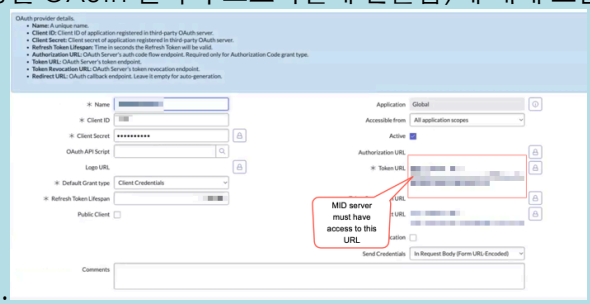
이러한 필드는 OAuth 2.0의 자격 증명 양식에서 사용할 수 있습니다.

OAuth 2.0 자격 증명 양식

필드	입력 값
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다. 예를 들어 **OAuth2** 자격 증명이라고 할 수 있습니다.
활성	이 자격 증명이 활성 상태인지 여부를 지정합니다.
OAuth 엔터티 프로파일	OAuth 프로파일은 권한 부여 유형과 하나 이상의 범위를 조합한 것입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OAuth 2.0 자격 증명 양식

필드	입력 값
MID 서버를 통해 인증 서버에 연결	를 MID 서버통해 방화벽 뒤에 상주하는 온프레미스 OAuth 서버에 인스턴스를 연결합니다ServiceNow. 또한 MID 서버를 통해 인스턴스를 클라우드 기반 OAuth 서버에 연결할 ServiceNow 수 있습니다. 이 옵션을 사용하면 OAuth 토큰 MID 서버에 대한 요청이 . **중요사항:** • 이 옵션은 OAuth 엔터티 프로파일의 부여 유형 필드 값이 클라이언트 자격 증명으로 설정된 경우에 나타납니다. 타사 OAuth 제공자에 대한 OAuth 엔터티 프로파일을 설정하는 방법을 알아보려면 문서를 참조하십시오 외부 공급업체 OAuth 제공자에 연결. • **MID** 서버를 통해 인증 서버에 연결 확인란을 선택하는 경우 필수 MID 서버MID 서버 항목을 식별하거나 적용 대상 목록에서 식별해야 합니다.
적용 대상	자격 증명 기록이 모든 MID 서버 또는 특정 MID 서버에 적용 가능한지 지정합니다. 특정 경우 필요에 따라 MID Server를 추가합니다. **중요사항:** **MID** 서버를 통해 인증 서버에 연결 확인란을 선택한 경우 이러한 고려 사항에 유의해야 합니다. • 적용 대상에서 선택한 모든 항목이 MID 서버 인증 서버와 통신할 수 있는지 확인합니다. 이는 OAuth 제공자 기록에 언급된 토큰 **URL** (OAuth 2.0 자격 증명 기록에 지정된 OAuth 엔터티 프로파일에 연결됨)에 대해 토큰 요청을 실행하는 데 필요합니다.  • 적용 대상에서 선택한 항목에 다음 구성이 하나 이상 MID 서버MID 서버 있는지 확인합니다. ◦ 상태 필드의 값은 **Up**입니다. ◦ 확인됨 필드의 값은 예입니다. ◦ 의 MID 서버 기능은 **REST** 또는 **ALL**로 설정됩니다. MID 서버를 구성하는 방법에 대한 자세한 내용은 문서를 참조하십시오 https://docs.servicenow.com/csh?topicname=t_ConfigureCapabilities&version=yokohama&pubname=yokohama-integrate-applications .  이러한 상태에 대한 자세한 내용은 다음 문서를 참조하십시오 MID 서버 대시보드 .
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OAuth 2.0 자격 증명 양식

필드	입력 값
	시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
자격 증명 별칭	OAuth 2.0 자격 증명에 연결할 자격 증명 별칭을 지정합니다.
통합 유형	자격 증명의 통합 유형을 나타냅니다. 시스템 또는 사용자별 OAuth 토큰을 생성하는 OAuth 요청을 사용하여 타사의 API를 호출합니다. 통합 유형은 다음과 같습니다. • 시스템: 요청자 프로파일을 기반으로 토큰 정보를 끌어옵니다. • 개인: 사용자별 토큰 정보를 가져옵니다. 세션을 시작하는 사용자입니다. OAuth 요청자 프로파일 페이지에서 이 개인 을 선택하면 개인 이라는 추가 플래그가 표시됩니다. 주: • 사용자와 관련된 모든 정보는 통합 유형이 개인인 사용자별 OAuth 토큰으로만 액세스할 수 있습니다. • 세션 사용자 관련 토큰을 사용하려면 플로우 속성에서 세션을 시작하는 사용자로 다른 이름으로 실행을 선택해야 합니다.

SAP 자격 증명

SAP 자격 증명 유형은 SAP JCo 시스템에 대한 액세스를 관리합니다. 이 자격 증명 유형은 Discovery 및 Orchestration에 사용할 수 있습니다.

이러한 필드는 SAP 유형 자격 증명에 대한 자격 증명 양식에서 사용할 수 있습니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
사용자 이름	자격 증명 테이블에 생성할 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다. CIM 검색의 경우 사용자에게 관리자 역할이 있어야 합니다.
암호	암호를 입력합니다.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	서비스 매핑 및 디스커버리 패턴을 사용하여 이 CI 유형에 속하지 않는 CI를 검색하는 데 자격 증명을 사용하려면 CI가 속한 CI 유형의 테이블 이름(예: cmdb_ci_apache_web_server)을 입력하십시오.
외부 자격 증명 스토리지	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화된 경우에만 사용할 수 있습니다. 주: 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다. 주: 특정 **MID** 서버를 선택해도 MID 서버 선택에 영향을 주지 않습니다. 이는 자격 증명에 대한 가시성을 확보해야 하는 MID Server를 결정하는 데만 사용됩니다. 오케스트레이션 활동에서는 특정 **MID Server**가 지원되지 않습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
Windows MID 서버 서비스 계정	활성 상태인 경우 정의된 자격 증명은 MID 서버 서비스 계정을 표현합니다.

SNMP 자격 증명

디스커버리는 SNMP 프로토콜을 사용하여 많은 종류의 장치(스위치, 라우터, 프린터 등)를 탐색합니다. SNMP용 자격 증명에는 사용자 이름이 포함되지 않고 *#### ###*이라는 암호만 포함됩니다.

많은 SNMP 장치의 기본 읽기 전용 커뮤니티 문자열은 공용 디스커버리 이며 자동으로 시도합니다. *##* 커뮤니티 문자열과 다른 경우 적절한 SNMP 자격 증명 정보를 입력합니다.

SNMP를 검색하면 구성된 모든 커뮤니티 문자열이 사용됩니다. 이 동작은 SNMPv3 검색에는 적용되지 않습니다.

기본 오케스트레이션 활동인 SNMP 쿼리는 장치의 객체 식별자(OID)를 반환하며 SNMP 자격 증명이 필요합니다.

SNMP 커뮤니티 자격 증명

SNMP 커뮤니티 자격 증명 유형은 SNMP 프로토콜을 사용하여 다양한 종류의 장치(스위치, 라우터, 프린터 등)를 검색하기 위한 액세스를 관리합니다. 이 자격 증명 유형은 , 서비스 매핑, 및 에 사용할 디스커버리수 있습니다오케스트레이션.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SNMP 자격 증명에는 사용자 이름이 아니라 암호(커뮤니티 문자열)만 포함됩니다. 많은 SNMP 장치의 기본 읽기 전용 커뮤니티 문자열은 공용이며 시스템은 이를 자동으로 시도합니다. 공용 커뮤니티 문자열과 다른 경우 적절한 SNMP 자격 증명 정보를 입력합니다.

이러한 필드는 SNMP 커뮤니티의 자격 증명 양식에서 사용할 수 있습니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
사용자 이름	자격 증명 테이블에 생성할 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다. CIM 검색의 경우 사용자에게 관리자 역할이 있어야 합니다.
암호	암호를 입력합니다.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다. 서비스 매핑 및 디스커버리 패턴을 사용하여 이 CI 유형에 속하지 않는 CI를 검색하는 데 자격 증명을 사용하려면 CI가 속한 CI 유형의 테이블 이름(예: cmdb_ci_apache_web_server)을 입력하십시오.
외부 자격 증명 스토리지	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화된 경우에만 사용할 수 있습니다. 주: 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다. 주: 특정 **MID** 서버를 선택해도 MID 서버 선택에 영향을 주지 않습니다. 이는 자격 증명에 대한 가시성을 확보해야 하는 MID Server를 결정하는 데만 사용됩니다. 오케스트레이션 활동에서는 특정 **MID Server**가 지원되지 않습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
Windows MID 서버 서비스 계정	활성 상태인 경우 정의된 자격 증명은 MID 서버 서비스 계정을 표현합니다.

SNMPv3 자격 증명

SNMPv3 자격 증명은 개인 프로토콜 및 추가 개인 키를 허용하며 검색 및 오케스트레이션에 사용할 수 있습니다. CyberArk의 외부 저장소의 경우 개인 계정 키를 선택할 수 있습니다.

이러한 필드는 SNMPv3의 자격 증명 양식에서 사용할 수 있습니다.

SNMPv3 자격 증명 필드

필드	입력 값
이름	이 자격 증명에 대한 고유하고 설명적인 이름입니다. 예를 들어 **SNMP** 커뮤니티 애틀랜타로 부를 수도 있습니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID Server**에 적용할지 아니면 하나 이상의 특정 **MID Server**에 적용할지 선택하십시오. **MID Server** 필드에 이러한 자격 증명을 사용해야 하는 MID Server를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
사용자 이름	SNMP 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다.
인증 프로토콜	이 자격 증명에 사용할 인증 유형을 선택하십시오. 선택 항목은 다음과 같습니다. • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
인증 키	이 자격 증명에 사용할 인증 키를 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SNMPv3 자격 증명 필드

필드	입력 값
개인 프로토콜	이 자격 증명에 대한 암호화 프로토콜을 선택하십시오. 선택 항목은 다음과 같습니다. • 3DES • AES128 • AES192 • AES256 • DES
개인 키	선택한 개인 정보 프로토콜에 연결된 키를 입력합니다.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
개인 자격 증명 ID	CyberArk에서 SNMPv3 자격 증명에 대해 구성된 개인 계정 키를 입력하십시오. CyberArk에서 개인 프로토콜을 사용하는 경우 이 필드의 값은 CyberArk SNMPv3 개인 계정의 이름 필드와 같아야 합니다. 이 필드는 자격 증명 저장소 유형 필드에서 **CyberArk**를 선택할 때만 SNMPv3에 표시됩니다. CyberArk에 개인 키를 사용하지 않는 경우에는 이 필드를 비워 둡니다.
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다.
외부 자격 증명 저장소	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 외부 저장소가 활성화되면 자격 증명 **ID** 필드가 나타납니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화되고 외부 저장소 보기가 선택된 경우에만 사용할 수 있습니다.
자격 증명 저장소 유형	외부 저장소 제공자를 선택하십시오. CyberArk SNMPv3 개인 키를 사용하는 경우에만 **CyberArk**를 선택하십시오. 키 항목을 입력할 수 있도록 개인 정보 자격 증명 **ID** 필드가 표시됩니다.
컨텍스트 사용	이 자격 증명에 대한 컨텍스트 값을 추가하려면 이 확인란을 선택합니다. 이 필드는 검색 뷰에 표시됩니다. 외부 자격 증명 스토리지에는 현재 컨텍스트가 지원되지 않습니다. **주:** 컨텍스트는 특정 OID를 참조하는 SNMPv3 자격 증명에서 액세스하는 관리 정보의 모음입니다. 일반 자격 증명으로 액세스할 수 없는 장치에 대한 정보를 수집하는 컨텍스트를 참조하는 경우도 있습니다. 컨텍스트는 제조업체에서 제공하거나 별도로 구성할 수 있습니다. 사용자 이름과 키가 같은 여러 개의 SNMPv3 자격 증명이 있지만 일부 장치에는 컨텍스트가 필요하지 않은 경우에는 각 장치마다 별도의 레코드를 만들어야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SNMPv3 자격 증명 필드

필드	입력 값
컨텍스트 이름	이 자격 증명에 대한 컨텍스트 이름 값을 입력하십시오. 모든 액세스에 이 값을 필요로 하는 장치가 있는 경우에만 사용해야 합니다. 이 필드는 컨텍스트 사용 확인란이 선택된 경우에만 표시됩니다.

SSH 자격 증명

디스커버리, 오케스트레이션 및 통합 허브는 SSH(Secure Shell)를 통해 명령을 실행하기 위해 SSH 자격 증명을 사용하여 UNIX 및 Linux 장치를 탐색합니다. SSH 명령은 루트 자격 증명 또는 sudo 사용을 통해 루트 권한으로 실행되어야 합니다. SSH 개인 키 자격 증명은 추가 보안을 제공합니다.

루트 권한 부여

루트 권한을 부여하기 전에 조직의 보안 팀과 함께 보안 정책 및 옵션을 검토하십시오.

다음 방법 중 하나를 사용하여 사용자가 루트 권한으로 SSH 명령을 실행할 수 있도록 합니다.

- 디스커버리, 오케스트레이션, 또는 통합 허브에 다른 자격 증명을 주고 해당 자격 증명의 sudo 를 사용하여 루트 권한으로 특정 명령을 실행할 수 있는 권한을 사용자에게 부여합니다. 이것은 제한된 권한을 부여하는 안전한 방법입니다. 디스커버리, 오케스트레이션 또는 통합 허브는 `must_sudo` 매개변수를 **True** 로 설정한 모든 프로브에서 sudo를 사용합니다(기본값은 **False**). 그러나 sudo가 작동할 수 있도록 각 시스템을 구성해야 합니다. 이 작업을 수행하려면 **visudo** 명령을 사용하여 **/etc/sudoers** 파일을 편집합니다.
- 루트 자격 증명을 제공합니다. 이것은 확실히 가장 강력한 자격 증명이지만 보안 측면에서는 바람직하지 않을 수 있습니다. 만약 디스커버리, 오케스트레이션 또는 통합 허브가 UNIX 또는 Linux 시스템에 대한 루트 자격 증명을 갖고 있는 경우 추가 구성이 필요하지 않습니다.

권한 있는 명령

플랫폼은 MID 서버에서 사용할 수 있는 기본적인 권한 있는 명령과 시스템에 명령을 추가하는 기능을 제공합니다. sudo 및 기타 권한 있는 명령 사용에 대한 자세한 내용은 MID 서버 권한 있는 명령 을 참조하십시오.

SSH 개인 키 자격 증명 형식

주: 대부분의 경우 SSH 개인 키 자격 증명을 사용해야 합니다. 두 당사자 간의 통신을 가로채는 MitM(메시지 가로채기) 공격을 포함하여 SSH 암호 자격 증명보다 더 나은 보안을 제공합니다.

필드	입력 값
이름	이 자격 증명에 대한 고유하고 설명적인 이름입니다. 예를 들어 **SSH** 애틀랜타로 부를 수도 있습니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
사용자 이름	UNIX 또는 Linux 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다.
암호	UNIX 또는 Linux 암호를 입력합니다. **SSH** 개인 키 유형 자격 증명의 경우 사용자 이름에 필요한 경우 sudo 암호를 입력 합니다.
SSH 암호	보안 SSH 암호를 입력합니다. 이 필드는 **SSH** 개인 키 자격 증명에 대해서만 사용할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	입력 값

SSH 개인 키	안전한 RSA, DSA, ECDSA 또는 ED25519 개인 키를 입력합니다.
	
	개인 키는 올바르게 암호화되도록 적절한 형식으로 입력해야 합니다. 개인 키는 `-----BEGIN` 문자열로 시작해야 합니다.
	
	다음은 올바른 형식의 RSA 개인 키 예시입니다.
	
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3IWz+x`
	`...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END RSA PRIVATE KEY-----`
	
	DSA 키의 예:
	
	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3IWz+x`
	`...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END DSA PRIVATE KEY-----`
	
	ECDSA 키의 예:
	
	`-----BEGIN EC PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3IWz+x`
	`...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END EC PRIVATE KEY-----`
	
	ED25519 개인 키의 예:
	
	`-----BEGIN OPENSSH PRIVATE KEY-----`
	`b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2`
	`gtZW`
	`QyNTUxOQAAACAlYlqhcdwx8VQzZ5XaIC5ltQpjRr3lIlq/aE66mufmiwAAAKDQUtxZ`
	`0FLc`
	`WQAAAAtzc2gtZWQyNTUxOQAAACAlYlqhcdwx8VQzZ5XaIC5ltQpjRr3lIlq/aE66mu`
	`fmiw`
	`AAAECuvsTkFUPdpTh0kw23i8TYx19qsFOZ3TRgowkkHBh6wSViWqFx3DHxVDNnldog`
	`LmW1`
	`CmNGveUiWr9oTrqa5+aLAAAAGmFiaGluYXYuc3V0YXJATVJFTUE3OTAzMkI3AQID`
	`-----END OPENSSH PRIVATE KEY-----`
	
	주: ED25519 개인 키의 경우 OpenSSH SSH-keygen 유틸리티를 사용하여 생성되는 OpenSSH 키 형식만 지원됩니다.
	
	Now Platform은 OpenSSH ssh-keygen 유틸리티에서 생성된 PEM 형식의 개인 키를 지원합니다. PuTTY에 의해 생성된 PPK 키를 변환하려면 다음을 수행합니다.
	
	• PuTTYGen에서 개인 키를 엽니다.
	• 메뉴에서 OpenSSH 형식으로 익스포트 변환 > **OpenSSH** 키 익스포트.
	• 새 OpenSSH 키를 저장합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	입력 값
SSH 인증서	RSA 또는 ED25519 기반 OpenSSH 인증서를 입력합니다. 인증서를 입력하면 인증서 기반 인증에 개인 키가 사용됩니다. 이 인증은 OpenSSH 7.8 이상에서 지원됩니다.
자격 증명 별칭	• Flow Designer가 별칭을 사용하여 연결 및 자격 증명 정보를 관리할 수 있도록 합니다. 별칭을 사용하면 여러 환경을 사용할 때 여러 자격 증명과 연결 정보 프로파일을 구성하지 않아도 됩니다. 연결 또는 자격 증명 정보가 변경되면 연결을 사용하는 작업을 업데이트할 필요가 없습니다. 자세한 내용은 연결 및 자격 증명 문서를 참조하십시오. • 워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다.
외부 자격 증명 저장소	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID Server**에 적용할지 아니면 하나 이상의 특정 **MID Server**에 적용할지 선택하십시오. **MID Server** 필드에 이러한 자격 증명을 사용해야 하는 MID Server를 지정하십시오.
순서	플랫폼에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 검색 또는 오케스트레이션에서 임의의 순서로 자격 증명을 시도합니다.

SSH 자격 증명 유형

이러한 필드는 SSH 자격 증명 양식에서 사용할 수 있습니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
사용자 이름	자격 증명 테이블에 생성할 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다. CIM 검색의 경우 사용자에게 관리자 역할이 있어야 합니다.
암호	암호를 입력합니다.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
자격 증명 별칭	• Flow Designer가 별칭을 사용하여 연결 및 자격 증명 정보를 관리할 수 있도록 합니다. 별칭을 사용하면 여러 환경을 사용할 때 여러 자격 증명과 연결 정보 프로파일을 구성하지 않아도 됩니다. 연결 또는 자격 증명 정보가 변경되면 연결을 사용하는 작업을 업데이트할 필요가 없습니다. 자세한 내용은 연결 및 자격 증명 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	• 워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다. 서비스 매핑 및 디스커버리 패턴을 사용하여 이 CI 유형에 속하지 않는 CI를 검색하는 데 자격 증명을 사용하려면 CI가 속한 CI 유형의 테이블 이름(예: cmdb_ci_apache_web_server)을 입력하십시오.
외부 자격 증명 스토리지	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화된 경우에만 사용할 수 있습니다. 주: 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.

검색, 오케스트레이션 및 통합 허브에 대한 루트 권한이 필요한 명령

이 예시에서는 사용자 이름을 **Disco**로 가정합니다. 실제 사용자 이름을 대체하여 명령의 경로가 시스템의 경로와 일치하는지 확인합니다.

주: Sudo 명령은 sudo 명령에 제공할 암호가 없기 때문에 개인 키 자격 증명과 함께 사용할 수 없습니다. 해결 방법은 sudo 구성에 *NOPASSWD* 옵션을 추가하는 것입니다. 예를 들어 다음과 같이 입력 합니다. `disco ALL = (root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

루트 권한이 필요한 **UNIX** 및 **Linux** 명령

명령	목적
HP-UX	
adb	CPU 속도와 메모리를 수집합니다. • **/etc/sudoers** 라인 예: Disco ALL = (root)/usr/bin/adb • 검색에서 사용
모든 **Linux** 및 **UNIX** 버전	
chage	암호 변경 간격 및 마지막 암호 변경 날짜 사이의 일 수를 변경 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

루트 권한이 필요한 **UNIX** 및 **Linux** 명령

명령	목적
	• **/etc/sudoers** 라인 예: Disco ALL = (root)/usr/bin/chage • 오케스트레이션 및 통합 허브에서 사용
chpasswd	사용자 암호를 변경합니다. • **/etc/sudoers** 라인 예: Disco ALL = (root)/etc/chpasswd • 오케스트레이션 및 통합 허브에서 사용
모든 **Linux**	
dmidecode	마더보드에 내장된 일련 번호를 포함하여 하드웨어에 대한 여러 가지 정보를 수집합니다. • **/etc/sudoers** 라인 예: Disco ALL = (root)/sbin/dmidecode • 검색에서 사용
fdisk	시스템에서 디스크와 크기 정보를 수집합니다. • **/etc/sudoers** 라인 예: Disco ALL = (root)/usr/bin/fdisk-l • 검색에서 사용
다중 경로	MPIO에 대한 장치 매핑을 수집합니다. • **/etc/sudoers** 라인 예: Disco ALL = (root)/usr/bin/multipath-ll • 검색에서 사용
Linux 및 **Solaris**	
dmsetup	낮은 레벨의 볼륨을 검사합니다. • **/etc/sudoers** 라인 예: ◦ Disco ALL = (root)/usr/bin/dmsetup 테이블 * ◦ Disco ALL = (root)/usr/bin/dmsetup ls • 검색에서 사용
모든 **UNIX** 버전	
lsof	프로세스와 시스템 간의 연결 관계를 결정합니다. • **/etc/sudoers** 라인 예: Disco ALL = (root)/sbin/lsof • 검색에서 사용
oratab	Oracle 홈 및 pfile을 찾기 위해 oratab 파일에 대한 읽기 권한을 부여합니다. • **/etc/sudoers** 줄 예: 해당 없음 • 검색에서 사용

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

루트 권한이 필요한 **UNIX** 및 **Linux** 명령

명령	목적
Solaris	
iscsiadm	ISCSI IQNs 가져오기 • **/etc/sudoers** 라인 예: $ {sudo: iscsiadm 목록 대상-S} • 검색에서 사용
fcinfo	포트에 대한 WWPN을 가져옵니다. • **/etc/sudoers** 라인 예: ${sudo:fcinfo remote-port -sl -p $port} • 검색에서 사용
prtvtoc	디스크 파티션에 대한 정보를 보고합니다. • **/etc/sudoers** 라인 예: Disco ALL = (root)/usr/bin/prtvtoc • 검색에서 사용
pfiles	TCP 연결 정보를 수집하는 데 사용됩니다. • **/etc/sudoers** 줄 예시: Disco ALL=(root) /usr/bin/pfiles • 검색에서 사용
pgrep	pfiles를 실행할 특정 지역의 프로세스 ID를 나열하는 데 사용됩니다. • **/etc/sudoers** 줄 예시: Disco ALL=(root) /usr/bin/pgrep • 검색에서 사용
/usr/bin/ps	실행 중인 프로세스를 나열합니다. 루트 액세스를 실행하는 대신 proc_owner 역할을 추가합니다. • **/etc/sudoers** 라인 예: Disco ALL = (root)/usr/bin/ps • 검색에서 사용
/usr/ucb/ps	실행 중인 프로세스를 나열합니다. 루트 액세스를 실행하는 대신 proc_owner 역할을 추가합니다. `/Usr/ucb/ps` 명령은 Solaris 11에서 사용되지 않습니다. 디스커버리, 오케스트레이션 및 통합 허브는 모든 Solaris 버전에 대해 해당 명령을 사용해야 하므로 solaris 11 시스템에서 ucb 유틸리티를 수동으로 설치해야 합니다. 자세한 내용은 KB0564262 를 참조하십시오. • **/etc/sudoers** 라인 예: Disco ALL = (root)/usr/ucb/ps • 검색에서 사용

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Discovery 및 서비스 매핑에 필요한 권한 있는 명령 목록을 보려면 권한이 있는 사용자를 필요로 하는 서비스 매핑 명령 문서를 참조하여 조직 내에서 UNIX 기반 호스트를 검색 및 매핑하기 위해 승격된 권한을 필요로 하는 명령 목록을 확인합니다.

루트가 아닌 자격 증명에 대한 액세스 요구 사항

루트 액세스 자격 증명에 디스커버리를 제공하지 않으면 다음 액세스 요구 사항이 있는 자격 증명을 제공해야 합니다.

애플리케이션	파일 또는 디렉터리	액세스 필수
Apache	httpd.conf	읽기
Hbase	hbase-site.xml	읽기
JBoss	jboss-service	읽기
	JBoss 홈 디렉터리	읽기
	web.xml	읽기
MySQL	my.cnf	읽기
NGINX	nginx.conf	읽기
Oracle	oratab	읽기
	연결된 (s) pfiles	읽기
Oracle Listener	lsnrctl	실행
	ora	읽기
Tomcat	catalina.jar	읽기
	server.xml	읽기
	web.xml	읽기
Unix	/etc/*release	읽기
	/etc/bashrc	읽기
	/etc/profile	읽기
	/proc/cpuinfo	읽기
	/proc/vmware/sched/ncpus	읽기
	/var/log/dmesg	읽기
	APD 디렉터리	읽기
WebSphere	cell.xml	읽기
	server.xml	읽기
	serverindex.xml	읽기

VMware 자격 증명

VMware 자격 증명 유형은 vCenter 자격 증명에 대한 접근을 관리합니다.

VMware Cloud 자원에 액세스하는 애플리케이션은 VMware 자격 증명에 액세스할 수 있어야 합니다. 예를 들어 VMware 자격 증명 유형을 사용하면 Discovery는 Windows 컴퓨터에서 실행 중인 VMware의 vCenter를 탐색하여 ESX 컴퓨터, 가상 머신, 자원 풀을 검색할 수 있습니다. VMware

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

디스커버리 및 자동화 API(vCenter API)에서 컴퓨터 CI에 대해 전역적으로 고유한 일련 번호를 제공합니다. 각 VMware 호스트에 대한 액세스를 허용하는 데 CIM 자격 증명이 필요하지 않습니다.

주: 유효한 VMware 자격 증명이 사용되는 경우 vCenter 디스커버리에 Windows 자격 증명은 필요하지 않습니다.

중요사항: vCenter에 의해 클론된 개별 가상 머신에서 작업을 수행하는 Orchestration 활동에는 **VMware** 유형 자격 증명을 사용하지 마십시오(예: Linux VM 다시 시작). 이러한 활동의 경우 자격 증명 유형은 가상 머신의 운영 체제(**SSH** 또는 **Windows**)에 따라 다릅니다.

VMware 자격 증명 양식

필드	설명
이름	VMware 자격 증명에 대해 고유하고 설명적인 이름을 입력 하십시오.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
사용자 이름	VMware 계정에 사용할 사용자 이름을 입력하십시오. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다. VMware 자격 증명은 vCenter에서 읽기 전용 역할을 수행해야 합니다.
암호	VMware 계정에 대한 암호를 입력하십시오.
적용 대상	사용 가능한 MID 서버 목록에서 MID 서버 하나 이상을 선택합니다. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID 서버에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.

Windows 자격 증명

Windows 자격 증명은 Windows 컴퓨터에 대한 접근 권한을 제공합니다. 이 자격 증명 유형은 Discovery 및 Orchestration에 사용할 수 있습니다.

자격 증명 요구 사항

디스커버리 및 Orchestration에는 다음과 같은 Windows 자격 증명 요구 사항이 있습니다.

- Windows 호스트에 MID Server를 서비스로 설치합니다.
- 다음 위치 중 하나에 Windows 자격 증명을 추가합니다.
  - 자격 증명 `[windows_credentials]` 테이블의 항목
  - 특정 Windows 사용자 또는 도메인 계정으로 실행할 MID Server 서비스 계정입니다.

적절한 권한 부여

충분한 권한을 제공하려면 Windows 자격 증명이 다음 중 하나여야 합니다.

- 대상 Windows 호스트에 대한 로컬 관리자 액세스 권한이 있는 도메인 사용자
- 동일한 대상 호스트에서 관리자 권한과 UAC(사용자 접근 제어)가 비활성화된 로컬 계정입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- Windows 프로브 및 권한 요구 사항을 충족하는 사용자입니다(디스커버리전용).
- 실행할 Orchestration 활동의 요구 사항을 충족하는 사용자입니다(Orchestration만 해당).

주: 로그온 권한은 필요하지 않습니다. 계정이 대화형일 필요는 없습니다.

JEA 프로필을 사용하여 디스커버리를 실행함으로써 권한 있는 액세스 권한 부여에 대한 보안을 강화할 수 있습니다. 자세한 내용은 Microsoft JEA(Just Enough Administration) for Discovery를 참조하십시오.

작업 그룹 컴퓨터

Powershell 명령을 실행하여 작업 그룹 컴퓨터를 검색하려면 다음 사용자 중 하나에 대한 MID Server 자격 증명을 구성합니다.

- 작업 그룹 컴퓨터의 기본 관리자 계정입니다.
- 작업 그룹 컴퓨터의 도메인 사용자입니다.

다중 도메인 구성

Windows 자격 증명이 여러 도메인에서 작동하려면 올바른 이름 형식과 MID Server 구성을 사용해야 합니다.

디스커버리 및 Orchestration은 사용자 계정 이름 및 다운레벨 로그온 이름 사용자 이름 형식의 Windows 도메인 자격 증명을 지원합니다. 예를 들어 **Domain\UserName** 또는 **UserName@example.domain.com**입니다. WORKGROUP\UserName 형식으로 Windows 작업 그룹 자격 증명을 제공할 수 있습니다.

주: .\ 사용자 이름을 사용하여 로컬 계정을 제공할 수도 있습니다.

자격 증명이 여러 Windows 도메인에서 작동하려면 이러한 추가 작업이 필요합니다.

조건	필요한 추가 조치
Windows 대상과 동일한 도메인의 MID Server 호스트입니다.	없음
Windows 대상과 다른 도메인의 MID Server 호스트입니다.	MID Server 호스트에 PowerShell 3.0 이상(최대 5.1)이 설치되어 있는지 확인합니다.
Microsoft SQL Server 대상과 다른 도메인의 MID Server 호스트입니다.	MSSQL 서버 검색을 참조하십시오 .

Windows 자격 증명 유형

이러한 필드는 Windows용 자격 증명 양식에서 사용할 수 있습니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
사용자 이름	자격 증명 테이블에 생성할 사용자 이름을 입력합니다. 사용자 이름에 선행 또는 후행 공백을 넣지 않도록 합니다. 플랫폼이 사용자 이름에서 선행 또는 후행 공백을 탐지하면 경고가 표시됩니다. CIM 검색의 경우 사용자에게 관리자 역할이 있어야 합니다.
암호	암호를 입력합니다.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 자격 증명 **ID** 필드에는 40자 제한이 있습니다. 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
자격 증명 별칭	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다. 서비스 매핑 및 디스커버리 패턴을 사용하여 이 CI 유형에 속하지 않는 CI를 검색하는 데 자격 증명을 사용하려면 CI가 속한 CI 유형의 테이블 이름(예: cmdb_ci_apache_web_server)을 입력하십시오.
외부 자격 증명 스토리지	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화된 경우에만 사용할 수 있습니다. 주: 현재 유일하게 지원되는 외부 저장소 시스템은 CyberArk입니다.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID** 서버에 적용할지 아니면 하나 이상의 특정 **MID** 서버에 적용할지 선택하십시오. **MID** 서버 필드에 이러한 자격 증명을 사용해야 하는 MID 서버를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다. 주: 특정 **MID** 서버를 선택해도 MID 서버 선택에 영향을 주지 않습니다. 이는 자격 증명에 대한 가시성을 확보해야 하는 MID Server를 결정하는 데만 사용됩니다. 오케스트레이션 활동에서는 특정 **MID Server**가 지원되지 않습니다.
순서	디스커버리에서 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)입니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 인스턴스에서 임의의 순서로 자격 증명을 시도합니다.
Windows MID 서버 서비스 계정	활성 상태인 경우 정의된 자격 증명은 MID 서버 서비스 계정을 표현합니다.

MID Server에 대한 **Windows** 자격 증명 구성

자체 Windows 서비스의 자격 증명 또는 자격 증명 [discovery_credentials] 테이블의 자격 증명을 사용하도록 MID 서버를 구성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에
필요한 역할: admin

프로시저

1. MID 서버 서비스 계정의 자격 증명을 사용하도록 MID 서버를 구성합니다.
   a. 권한 요구 사항을 충족하는 사용자에 대한 Windows MID 서버 구성 서비스 자격 증명을 설정합니다.
   b. 사용자 이름이 이름 형식 요구 사항을 충족하는지 확인합니다.
   c. 양식의 필드에 적절히 입력합니다.
   d. 자격 증명이 도메인 요구 사항을 충족하는지 확인합니다.
2. 자격 증명 [discovery_credentials] 테이블의 자격 증명을 사용하여 MID 서버를 구성합니다.
   a. 자격 증명 `[windows_credentials]` 테이블에 개별 Windows 자격 증명을 추가합니다.
      - 각 자격 증명이 권한 요구 사항을 충족하는지 확인합니다.
      - 각 사용자 이름이 이름 형식 요구 사항을 충족하는지 확인합니다.
      - 각 자격 증명이 Windows 도메인 요구 사항을 충족하는지 확인합니다.
   b. 옵션: `mid.use_powershell` 매개변수를 **true**로 설정하여 Powershell을 사용하도록 MID 서버를 구성합니다.
      MID Server 구성을 참조하십시오.
   c. 특정 Windows 사용자 또는 도메인 계정으로 실행할 Windows MID 서버 서비스 계정을 나타내는 자격 증명을 작성하려면 Windows MID 서버 서비스 계정 확인란을 선택합니다.

컨테이너 이미지 리포지토리 자격 증명

컨테이너 이미지 리포지토리 자격 증명은 컨테이너 이미지 스캔을 위해 프라이빗 리포지토리에 대한 액세스를 관리합니다. 이 자격 증명 유형은 에 사용할 디스커버리수 있습니다.

이러한 필드는 자격 증명 이미지 리포지토리 유형 자격 증명에 대한 자격 증명 양식에서 사용할 수 있습니다.

컨테이너 이미지 리포지토리 자격 증명 양식

필드	설명
이름	사용자가 할당한 자격 증명 이름입니다.
사용자 이름	리포지토리에 대한 읽기 권한이 있는 사용자 이름입니다.
암호	리포지토리에 대한 읽기 권한이 있는 암호입니다.
리포지토리	리포지토리의 전체 주소 도메인 이름입니다. 예: `docker.io/snow_images`.

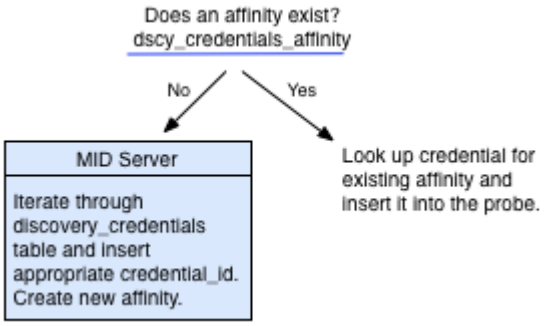
Discovery 및 Orchestration에 대한 자격 증명 선호도

자격 증명 선호도는 자격 증명 집합과 네트워크의 장치 간의 연결입니다.

디스커버리 또는 Orchestration이 처음 장치에 액세스하려고 하면 올바른 자격 증명을 찾을 때까지 사용 가능한 모든 자격 증명을 시도합니다. 장치에 대한 자격 증명을 식별한 디스커버리 후 오케스트레이션은 자격 증명 선호도 `[dscy_credentials_affinity]` 테이블을 사용하여 자격 증명과 장치 간의 선호도를 만듭니다. 이후의 모든 검색 또는 오케스트레이션 활동은 이 테이블의 자격 증명 정보를 선호도가 있는 장치와 일치시키려고 합니다. 장치의 자격 증명이 변경되면 디스커버리 Orchestration은 새로운 선호도를 만들 때까지 사용 가능한 모든 자격 증명을 다시 시도합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자격 증명 선호도 다이어그램



주: 오케스트레이션 및(와 디스커버리)이 설치되고 자격 증명 별칭이 활성화된 경우 여러 선호도가 존재할 수 있습니다. 이 경우 플랫폼은 각 선호도에 대한 자격 증명을 조회하고 순서가 가장 낮은 선호도에 대한 자격 증명을 프로브에 삽입합니다.

자격 증명 문제 해결

자격 증명 관련 문제를 해결하려면 ECC 큐 페이로드의 `<credentials_debug>` 섹션을 검토합니다.

특정 프로브는 자격 증명 디버깅을 지원합니다. 자격 증명 디버깅은 MID 서버가 인스턴스 ECC 큐에 반환하는 페이로드에 `<credentials_debug>` 섹션을 삽입합니다. `<credentials_debug>` 섹션에서 자격 증명 조회에 대한 자세한 정보를 볼 수 있습니다.

다음과 같은 경우 `##### <credentials_debug>` 섹션이 나타납니다.

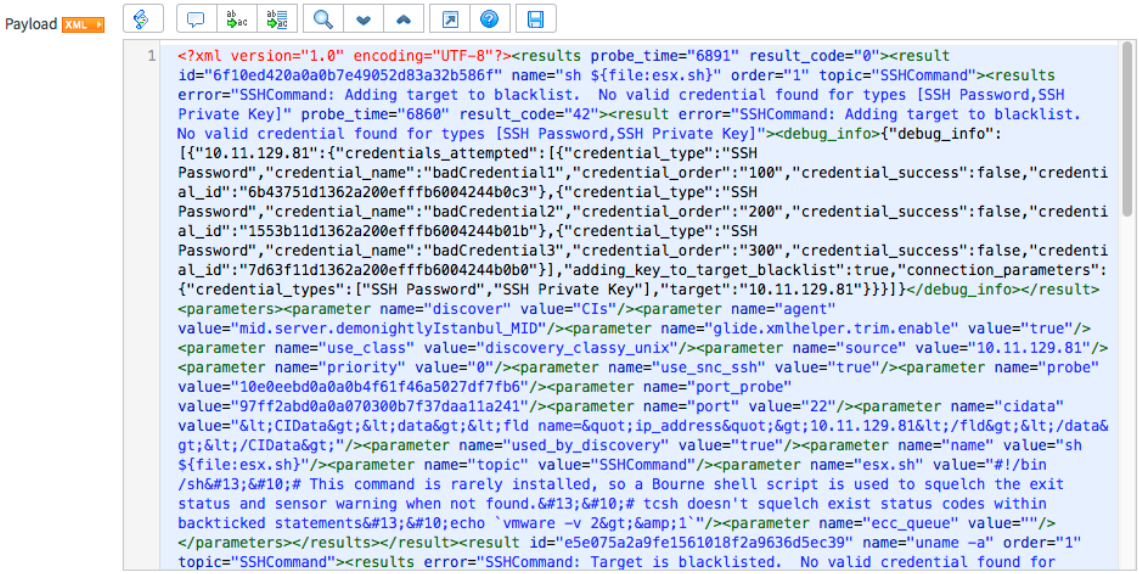
- WMIRunner 프로브 , PowerShell 프로브 , JMS 또는 SSHCommand 프로브 에 대한 자격 증명에 실패했습니다.
- WMIRunner, PowerShell 또는 SSHCommand 프로브에 대해 매개변수를 **true**로 설정합니다*credentials_debug*. 매개변수를 true로 설정하면 자격 증명 조회에 성공해도 `<credentials_debug>` 섹션이 나타납니다.

`<credentials_debug>` 섹션에는 다음이 표시됩니다.

- 자격 증명 유형, 태그 및 선호도와 같은 자격 증명 검색에 대한 정보입니다.
- 대상 IP 주소입니다.
- 유형, 분류, 태그, 이름, 시스템 ID 및 외부 자격 증명 ID(있는 경우)를 포함하여 MID 서버에서 사용한 각 자격 증명에 대한 순서대로인 정보입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

잘못된 자격 증명을 보여주는 샘플 페이로드



PowerShell 매개변수에 대한 상세 정보가 표시됩니다.

- 모든 Windows 자격 증명이 실패한 후에 로컬 MID 서버 자격 증명을 사용한 경우.
- MID 서버가 있는 동일한 컴퓨터를 검색하려고 하기 때문에 자격 증명을 건너뛴 경우.
- mid.powershell.use_credentials 매개변수가 `true`로 설정된 경우.

SSHCommand에 대한 상세 정보가 표시됩니다.

- 대상 IP가 제외되어 자격 증명 검색을 건너뛴 경우.
- 대상 IP가 제외 목록에 추가된 경우

주: MID 서버는 실패한 자격 증명 검색의 IP 주소를 캐시 메모리의 제외 목록에 저장합니다. 이 제외 목록은 MID 서버가 액세스 시도를 중지해야 하는 장치를 지정합니다. 모든 자격 증명이 실패하면 IP 주소가 제외 목록에 추가됩니다. 5분 후, MID 서버가 다시 시작되거나 인스턴스의 자격 증명 레코드가 업데이트되면 제외 목록 캐시에서 IP 주소가 지워집니다.

외부 자격 증명 스토리지

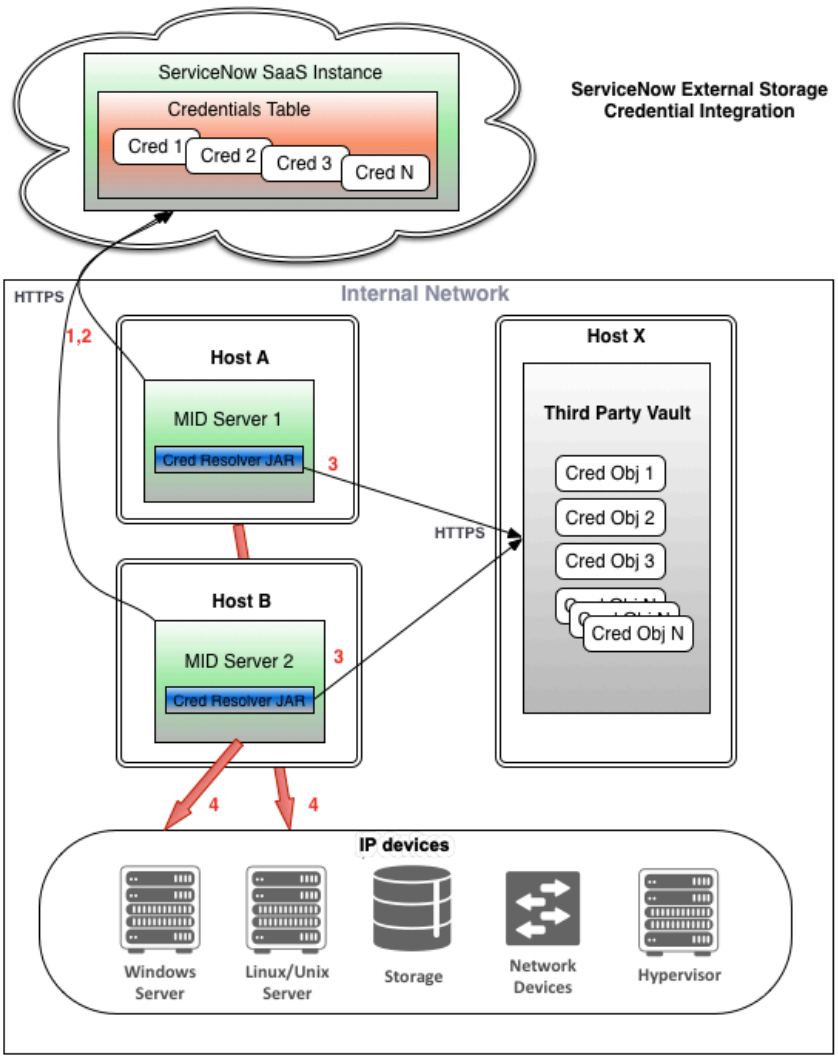
인스턴스는 , 오케스트레이션 서비스 매핑 에서 디스커버리사용하는 자격 증명을 자격 증명 기록에 직접 ServiceNow 저장하지 않고 외부 자격 증명 리포지토리에 저장할 수 있습니다.

인스턴스는 각 자격 증명, 자격 증명 유형(예: SSH, SNMP 또는 Windows) 및 자격 증명 선호도에 대한 고유 식별자를 유지관리합니다. MID 서버는 인스턴스에서 자격 증명 식별자를 얻은 다음 고객 제공 JAR 파일을 사용하여 리포지토리의 식별자를 사용 가능한 자격 증명으로 확인합니다. 현재 플랫폼은 ServiceNow® 외부 자격 증명 스토리지에 CyberArk 볼트 또는 BeyondTrust의 사용을 지원합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

외부 자격 증명 스토리지 아키텍처

외부 자격 증명 스토리지 아키텍처



자격 증명 프로세스 흐름

MID 서버는 다음 프로세스를 사용하여 외부 저장소에서 자격 증명을 검색합니다.

1. MID 서버는 대상 저장소의 해당 자격 증명 ID를 포함하는 자격 증명 [discovery_credentials] 테이블에서 자격 증명 객체를 ServiceNow 다운로드합니다.
2. 각 프로브 또는 패턴이 또는 오케스트레이션 작업에서 실행될 디스커버리 때 MID 서버는 자격 증명 ID, 대상 IP 주소 및 자격 증명 유형과 같은 정보를 자격 증명 해석기 Java Jar 파일에 전달하여 자격 증명을 요청합니다. 자격 증명 모음에서 검색할 올바른 자격 증명 객체에 대한 세부 정보는 자격 증명 확인자에 의해 결정됩니다.

   CyberArk와 같은 많은 자격 증명 확인자는 MID 서버와 동일한 시스템에서 실행되는 타사 저장소 벤더가 제공한 애플리케이션을 호출합니다. 해당 애플리케이션은 종종 자격 증명을 캐시하도록 구성될 수 있으며 Vault에서 자격 증명이 변경될 때 캐시를 업데이트하는 것을 알고 있습니다. 이는 MID Server가 자격 증명을 요청할 때마다 Vault에 대한 불필요한 네트워크 호출을 방지하는 데 매우 중요합니다. 자격 증명 확인자(있는 경우 선택적 벤더 애플리케이션 사용)는 Vault를 호출하여 실제 사용자 이름, 암호 등을 가져옵니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

바로 사용 가능한 자격 증명 확인자(현재 CyberArk만 해당)의 경우 MID 서버는 MID 서버 프로세스 메모리에서 암호화를 사용하여 자격 증명을 최대 몇 초 동안만 캐시합니다. 즉, MID 서버는 단일 장치를 검색할 때에도 동일한 자격 증명에 대해 자격 증명 확인자에게 여러 요청을 할 수 있습니다. 다른 자격 증명 해결자의 캐싱 구현에 대한 자세한 내용은 외부 공급업체 공급업체에 문의하십시오.

3. MID 서버는 적절한 자격 증명을 사용하여 프로브를 실행합니다.

주: 자격 증명 선호도는 여전히 적용됩니다. MID Server의 관점에서 실제 자격 증명 세부 정보(사용자 이름 및 암호)가 외부 공급업체 저장소에서 제공된다는 것만 다르기 때문에 메커니즘은 동일하게 유지됩니다.

외부 자격 증명 스토리지 로깅

MID 서버는 외부 자격 증명 스토리지에 대한 로그 메시지를 게시합니다.

자격 증명 요청을 해결하는 동안 리포지토리에 오류가 발생하면 MID 서버는 다음 접두사를 사용하여 로그 메시지를 게시합니다. `###### CredentialResolver# ## ##:`

외부 자격 증명 스토리지와 함께 설치되는 구성요소

비즈니스 규칙

외부 자격 증명 스토리지 비즈니스 규칙은 관리자가 외부 자격 증명 스토리지 속성을 변경할 때 다음 작업을 수행합니다.

- 자격 증명 기록 목록 및 양식의 보기를 외부 저장소 보기로 변경합니다. 이 보기를 사용하면 사용자가 목록에서 자격 증명 **ID** 열을 볼 수 있습니다.
- 자격 증명을 가져오는 방식의 변경을 준비하는 동안 MID 서버에서 자격 증명 캐시를 새로 고치도록 지시합니다.

속성

외부 자격 증명 스토리지 사용 [com.snc.use_external_credentials] 속성은 활성화된 외부 자격 증명 스토리지 플러그인을 사용하거나 사용하지 않도록 설정합니다. 숙소는 다음 위치에 있습니다. 디스커버리 정의 > 속성 및 오케스트레이션 > **MID** 서버 속성이며 플러그인을 활성화하면 활성화됩니다.

시스템 속성을 사용하여 외부 자격 증명 스토리지를 사용하지 않도록 설정하면, 시스템은 자동으로 모든 외부 자격 증명을 비활성화된 인스턴스로 설정합니다. 이 속성을 사용하여 기능을 다시 활성화하면 시스템은 외부 자격 증명 기록을 활성으로 재설정하지 않습니다. 각 자격 증명 기록을 수동으로 다시 활성화해야 합니다.

Discovery 및 Orchestration을 위한 외부 자격 증명 저장소 요청

요청에 따라 External Credential Storage 플러그인을 사용할 수 있습니다.

시작하기 전에
필요한 역할: admin

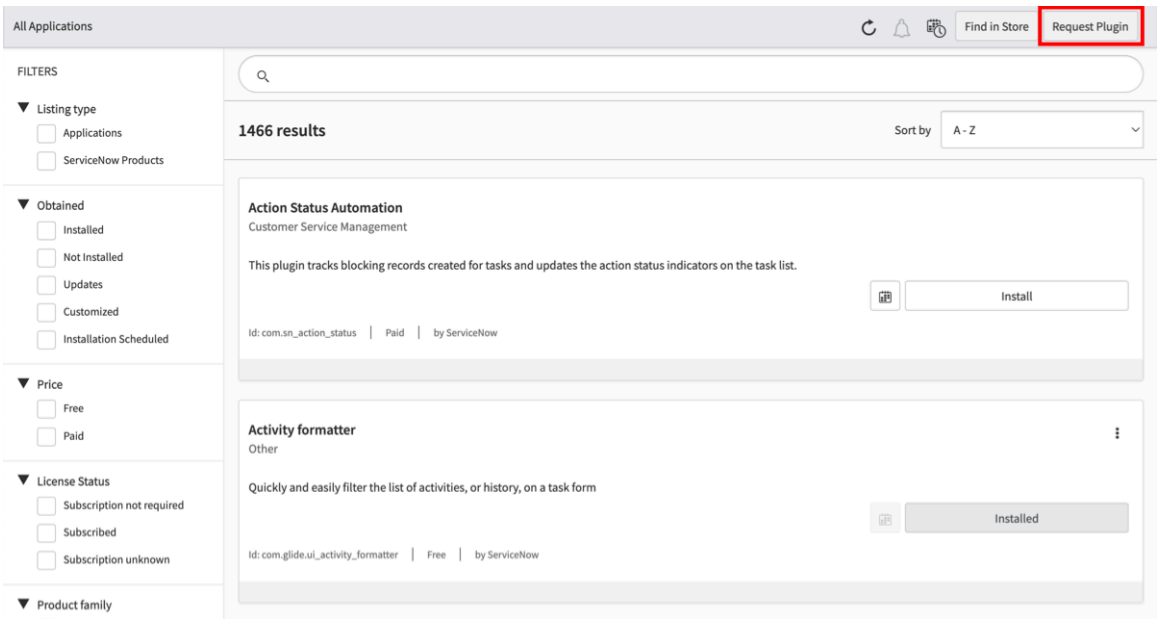
이 태스크 정보
플러그인을 요청하는 방법은 두 가지가 있습니다.

- 을(를) 선택하여 Service Catalog에 Now Support 직접 액세스합니다. 모두 > 서비스 카탈로그 > 플러그인 활성화 에 Now Support.
- 다음 단계에 따라 인스턴스의 모든 애플리케이션 페이지에서 Now Support 서비스 카탈로그에 액세스합니다.

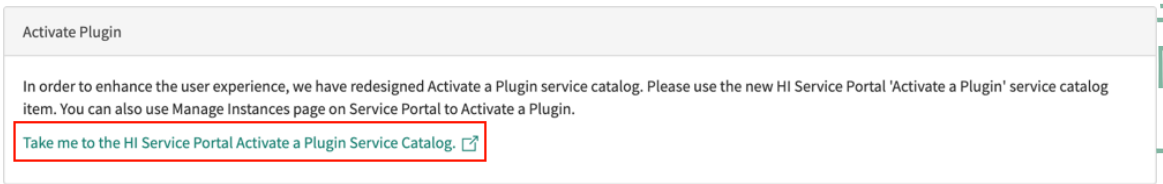
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 모든 애플리케이션 페이지에서 플러그인 요청을 선택하여 Now Support의 플러그인 활성화 양식을 엽니다.



3. Now Support에서 Now Support 서비스 포털 서비스 카탈로그에 액세스하는 링크를 선택합니다.



4. 인스턴스를 선택합니다.
5. 작업 > 플러그인 활성화를 선택합니다.
6. 플러그인 활성화 양식에서 다음 정보를 입력합니다.

플러그인 활성화 양식

필드	설명
대상 인스턴스는 무엇입니까?	플러그인을 활성화할 인스턴스입니다.
어떤 플러그인을 활성화하시겠습니까?	활성화할 플러그인의 이름입니다. 주: 시스템에서 원하는 플러그인을 나열하지 않거나 OEM 또는 온프레미스 인스턴스에서 플러그인을 활성화하는 경우 찾고 있는 플러그인이 목록에 없음 확인란을 선택한 다음 플러그인 이름을 입력합니다.

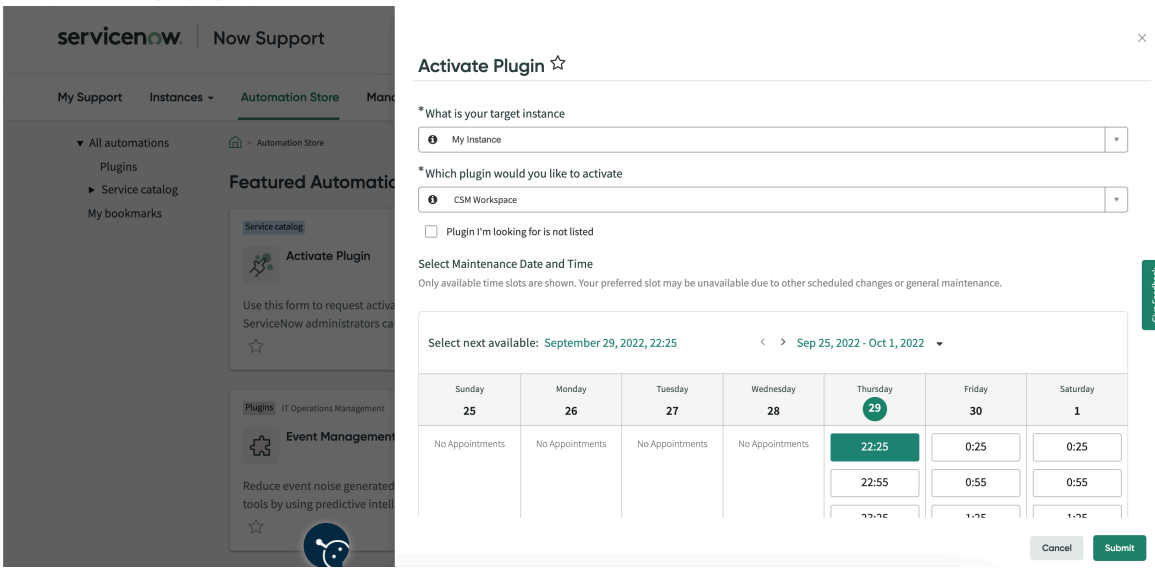
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
유지관리 날짜 및 시간 선택	플러그인을 활성화하는 날짜 및 시간입니다. 주: 플러그인은 미국 태평양 시간대의 모든 영업일에 두 번(오전과 저녁에 각각 한 번씩) 활성화됩니다. 특정 시간에 플러그인을 활성화해야 하는 경우 이유/설명 필드에 요청을 입력합니다.

Example

예를 들어, 내 인스턴스라는 인스턴스에서 CSM Workspace 플러그인을 활성화하는 다음 양식을 참조하십시오.

플러그인 활성화 양식



7. 제출을 선택합니다.
플러그인 요청에 대한 자세한 내용은 다음을 참조하십시오. 의 서비스 카탈로그 [KB0751715] 문서에서 플러그인 요청 Now Support 지식베이스.

외부 자격 증명 스토리지 구성

원격 리포지토리에서 자격 증명을 가져오도록 인스턴스를 구성합니다.

이러한 절차에서는 보호하려는 자격 증명으로 구성된 외부 리포지토리가 이미 있다고 가정합니다. 인스턴스에 구성된 ServiceNow 자격 증명 식별자는 JAR 파일을 통해 리포지토리의 실제 자격 증명에 매핑되어야 합니다.

주: ServiceNow는 한 번에 두 개의 외부 저장소(기본 CyberArk 자격 증명 확인자 1개와 사용자 지정 외부 자격 증명 확인자 1개)를 지원합니다. 사용자 지정 CyberArk 자격 증명 확인자를 생성해도 두 번째 사용자 지정 외부 저장소가 계속 사용되며 추가 사용자 지정 외부 저장소를 사용할 수 없습니다.

외부 자격 증명 스토리지를 구성하려면 다음 작업을 순서대로 완료하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자격 증명을 해결하기 위한 **JAR** 파일 생성

MID 서버에서 보낸 자격 증명 식별자를 리포지토리의 실제 자격 증명으로 확인하려면 JAR 파일을 만드십시오.

시작하기 전에
필요한 역할: agent_admin 또는 admin

개인 키와 같이 인스턴스에 필요한 모든 자격 증명 요소를 포함해야 합니다.

자격 증명을 해결하기 위해 JAR 파일을 생성하려면 다음과 같이 하십시오.

프로시저

github에 ServiceNow 제공된 템플릿 또는 샘플 Java 파일을 사용합니다.

⚠ 경고: 이러한 샘플은 템플릿으로만 사용됩니다. 사용자 환경에 맞게 수정하지 않고 프로덕션에서 이 코드를 사용하지 마십시오 .

a. github의 지침에 따라 오픈 소스 JAR 파일을 다운로드합니다.ServiceNow
- HashiCorp 외부 자격 증명 해결자
- CyberArk 외부 자격 증명 해결자

b. 다음 샘플 Java 파일을 템플릿으로 사용하고 환경에 맞게 수정합니다.

Example

```
package com.snc.discovery;

import java.util.*;
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";
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
// 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";


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()) {
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
    System.err.println("Can't open "+propFile.getAbsolutePath());
   }
   else {
    InputStream propsIn = new FileInputStream(propFile);
    fProps.load(propsIn);
   }

 //fProps.load(CredentialResolver.class.getClassLoader().getResourceAsS
tream("dummycredentials.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));

  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();
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
  System.err.println("I spy the following credentials: ");
  for(Object key: obj.fProps.keySet()) {
   System.err.println(key+": "+obj.fProps.get(key));
  }

 }
}
```

자격 증명을 해결하기 위해 **JAR** 파일 임포트

MID 서버에서 보낸 자격 증명 식별자를 확인하기 위해 생성된 JAR 파일을 리포지토리의 실제 자격 증명으로 임포트합니다.

시작하기 전에
필요한 역할: agent_admin 또는 admin

JAR 파일을 생성한 후 MID 서버에서 액세스할 수 있는 인스턴스로 임포트합니다.

프로시저

1. JAR 및 속성 파일을 생성한 후 속성 파일을 MID 서버에 복사합니다.
2. 다음으로 이동 **MID** 서버 > **JAR** 파일.
3. 새로 만들기를 클릭합니다.
4. 다음 필드를 작성합니다.

필드	설명
이름	인스턴스에서 파일을 식별하기 위한 고유하고 설명적인 이름입니다.
버전	파일의 버전 번호입니다(사용 가능한 경우).
소스	참조를 위한 JAR 파일의 위치입니다. 소스 정보는 시스템에서 사용되지 않습니다.
설명	JAR 파일 및 인스턴스에서의 목적에 대한 짧은 설명입니다.

5. 배너에서 클립 아이콘을 클릭하고 JAR 파일을 기록에 첨부합니다.

Example

JAR 파일 첨부

6. 제출을 클릭합니다.
7. MID 서버 서비스를 다시 시작합니다.
   플랫폼은 인스턴스와 통신하도록 구성된 모든 MID 서버에서 JAR 파일을 사용할 수 있게 합니다.

자격 증명 식별자 구성

인스턴스에서 자격 증명 식별자를 구성합니다.

시작하기 전에
필요한 역할: 관리자
다음 항목을 확인합니다.

- 외부 자격 증명 스토리지 플러그인이 활성 상태여야 합니다.
- 외부 자격 증명 스토리지 검색 사용 속성이 활성화됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 디스커버리 > 자격 증명 또는 오케스트레이션 > 자격 증명.
2. 새로 만들기를 클릭합니다.
3. 자격 증명 유형을 선택합니다.
4. 외부 자격 증명 저장소 확인란을 선택합니다.
   사용자 이름 및 암호 필드가 사라지고 자격 증명 **ID** 필드 및 자격 증명 스토리지 **Vault** 메뉴가 나타납니다.
5. 자격 증명 스토리지 저장소 메뉴에서 없음, CyberArk 저장소 또는 사용자 지정 외부 자격 증명 저장소 저장소 저장소 중 하나를 선택합니다.

   주:

   CyberArk Vault를 선택하면 자격 증명 ID, IP 주소, FQDN, 위의 네 가지 조회 키 선택 항목이 있는 조회 키 메뉴가 나타납니다. 위의 모든 항목을 선택하면 Vault에 여러 번 액세스해야 하므로 성능이 저하될 수 있습니다.

   a. 사용자 지정 외부 자격 증명 스토리지 Vault를 사용하려면 인스턴스에서 Vault 구성〔vault_configuration.list〕으로 이동하십시오.

   b. 사용자 지정 자격 증명 해결자를 위해 임포트한 JAR 파일을 연결한 이름을 사용하여 새 기록을 생성합니다.

   사용자 지정 외부 자격 증명 스토리지 Vault 생성에 대한 절차 자격 증명을 해결하기 위한 JAR 파일 생성 및 자격 증명을 해결하기 위해 JAR 파일 임포트 정보를 참조하십시오.

6. 다음 테이블의 필드를 사용하여 자격 증명 양식을 작성합니다.

필드	설명
이름	이 자격 증명을 설명하는 고유한 이름을 입력합니다.
활성	사용하는 자격 증명을 활성화하거나 비활성화하십시오.
자격 증명 ID	외부 자격 증명 시스템용 MID 서버로 업로드된 JAR 파일의 외부 자격 증명에 대해 구성된 고유 키를 입력합니다. 매개변수 맵의 Java 클래스에 전달된 ID입니다. `public static final String ARG_ID = "id";` MID 서버는 이 식별자를 사용하여 리포지토리의 실제 자격 증명을 확인합니다. 주: 이 필드는 외부 자격 증명 저장소 확인란이 선택된 경우에만 표시됩니다.
태그	워크플로우 작성자가 오케스트레이션 워크플로우에서 모든 활동에 개별 자격 증명을 할당하거나, 오케스트레이션 워크플로우에서 동일한 활동 유형의 각 항목에 서로 다른 자격 증명을 할당할 수 있도록 허용합니다.
외부 자격 증명 저장소	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 이 옵션을 선택하면 사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다. 외부 자격 증명 스토리지는 외부 자격 증명 스토리지 플러그인이 활성화된 경우에만 사용할 수 있습니다.
자격 증명 스토리지 Vault	사용 가능한 자격 증명 모음 목록에서 외부 자격 증명 스토리지 Vault를 선택합니다. 메뉴는 Vault 구성〔vault_configuration.list〕의 기록으로

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	구성됩니다. 새 기록을 추가하고 사용자 지정 자격 증명 확인자 JAR 파일과 관련된 이름을 사용할 수 있습니다. 사용자 지정 외부 자격 증명 스토리지 Vault 생성에 대한 절차 자격 증명을 해결하기 위한 JAR 파일 생성 및 자격 증명을 해결하기 위해 JAR 파일 임포트 정보를 참조하십시오.
적용 대상	이러한 자격 증명을 네트워크의 모든 **MID Server**에 적용할지 아니면 하나 이상의 특정 **MID Server**에 적용할지 선택하십시오. **MID Server** 필드에 이러한 자격 증명을 사용해야 하는 MID Server를 지정하십시오.
MID Server	사용 가능한 MID Server 목록에서 MID Server를 하나 이상 선택하십시오. 이 레코드에 구성된 자격 증명은 해당 리스트의 MID Server에서 사용 가능합니다. 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택했을 때만 사용할 수 있습니다.
순서	플랫폼이 장치에 로그인하려고 할 때 이 자격 증명을 시도하는 순서(시퀀스)를 입력합니다. 숫자가 작을수록 이 자격 증명이 목록에서 더 위에 나타납니다. 많은 수의 자격 증명을 사용하거나 로그인 시도가 3회 실패하여 보안상 사용자가 잠기는 경우 자격 증명 순서를 설정하십시오. 모든 자격 증명의 순서 번호가 같거나 없으면 검색 또는 오케스트레이션에서 임의의 순서로 자격 증명을 시도합니다.

7. 제출을 클릭합니다.

AWS에 대한 자격 증명 식별자 구성

원격 리포지토리에서 자격 증명을 가져오도록 인스턴스를 구성합니다.

시작하기 전에

필요한 역할: cloud_admin

다음 플러그인이 활성 상태이고 MID 서버가 설치되었는지 확인합니다.

- 검색 [com.snc.discovery]
- 클라우드 프로비저닝 및 거버넌스 [com.snc.cloud.mgmt]
- 외부 자격 증명 스토리지 [com.snc.discovery.external_credentials]

이 태스크 정보

이러한 절차에서는 보호하려는 자격 증명으로 구성된 외부 리포지토리가 이미 있다고 가정합니다. ServiceNow 인스턴스에 구성된 자격 증명 식별자는 JAR 파일을 통해 리포지토리의 실제 자격 증명에 매핑되어야 합니다.

프로시저

1. 다음으로 이동 모두 > 디스커버리 > 자격 증명.

2. 외부 자격 증명 스토리지 제공자가 지원하는 자격 증명을 선택합니다.

3. 테이블의 필드를 사용하여 양식을 작성합니다.

필드	설명
이름	이 자격 증명에 대한 고유하고 설명적인 이름입니다. 예로는 Amazon Web Services가 있습니다.
활성	자격 증명을 활성화하거나 비활성화하는 확인란입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
자격 증명 ID	외부 자격 증명 스토리지 제공자에 이 자격 증명이 저장되는 이름을 입력합니다.
MID 서버	이러한 자격 증명을 사용할 수 있는 MID Server를 하나 이상 선택하십시오.
외부 자격 증명 스토어	외부 자격 증명 스토리지 시스템을 사용하려면 이 확인란을 선택합니다. 외부 저장소가 활성화되면 자격 증명 **ID** 필드가 나타납니다. 이 확인란이 표시되지 않으면 헤더 막대에서 메뉴 아이콘을 누르고 뷰 > 외부 스토리지 컨텍스트 메뉴에서.
자격 증명 스토리지 Vault	CyberArk를 선택합니다.

4. 제출을 클릭합니다.

CyberArk 자격 증명 스토리지 통합

볼트ServiceNow® 오케스트레이션와 CyberArk 통합하면 MID 서버 인스턴스에 자격 증명을 저장하지 않고도 , ServiceNow® 디스커버리및 ServiceNow® 서비스 매핑 실행할 수 있습니다.

소개 CyberArk

CyberArk AIM(Application Identity Management) 제품은 권한 있는 계정 보안 솔루션을 사용하여 애플리케이션, 스크립트 또는 구성 파일에 포함된 애플리케이션 암호를 저장할 필요가 없으며 이러한 매우 중요한 암호를 자격 증명 모음 내에서 중앙에서 저장, 기록 및 관리할 수 있도록 CyberArk 합니다. 이 방법을 통해 조직은 주기적인 암호 교체에 대한 내부 및 규정 요구 사항을 준수하고 온-프레미스 또는 클라우드에 관계없이 모든 유형의 권한 있는 ID와 연결된 활동을 모니터링할 수 있습니다.

인스턴스는 각 자격 증명, 자격 증명 유형(예: SSH, SNMP 또는 Windows) 및 자격 증명 선호도에 대한 고유 식별자를 유지 관리합니다. MID 서버 인스턴스에서 자격 증명 식별자, 자격 증명 유형 및 IP 주소를 얻은 다음 자격 증명 모음을 CyberArk 사용하여 이러한 요소를 사용 가능한 자격 증명으로 확인합니다. 자격 증명 확인자는 호스트 이름, fqdn을 조회하고 역방향 DNS 조회를 사용하여 fqdn을 가져올 수도 있습니다.

통합하려면 CyberArk 다음에서 사용할 수 있는 ServiceNow® 외부 자격 증명 스토리지 플러그인이 필요합니다. 시스템 정의 > 플러그인. MID 서버 및 CyberArk AIM/API 클라이언트를 동일한 머신에 설치해야 합니다. CyberArk Application Access Manager(AAM) 자격 증명 공급자 버전 12.0.1 이상이 지원됩니다.

CyberArk 앱과 함께 설치되는 구성요소

- 비즈니스 규칙: 외부 자격 증명 스토리지 비즈니스 규칙은 관리자가 외부 자격 증명 스토리지 속성을 변경할 때 다음 작업을 수행합니다.
  - 자격 증명 기록 목록 및 양식의 보기를 외부 저장소 보기로 변경합니다. 이 뷰를 사용하면 사용자가 목록에서 자격 증명 ID 열을 볼 수 있습니다.
  - 자격 증명을 가져오는 방식의 변경을 준비하는 동안 외부가 아닌 자격 증명 캐시를 새로 고치도록 지시 MID 서버 합니다.
- 시스템 속성: 외부 자격 증명 스토리지 사용〔com.snc.use_external_credentials〕이라는 속성은 활성화된 외부 자격 증명 스토리지 플러그인을 활성화하거나 비활성화합니다. 이 숙박 시설은

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음 지역에 위치해 있습니다.디스커버리 정의 > 속성그리고오케스트레이션 > **MID** 서버 속성이며 플러그인을 활성화하면 활성화됩니다.

주: 시스템 속성을 사용하여 외부 자격 증명 스토리지를 사용하지 않도록 설정하면, 시스템은 자동으로 모든 외부 자격 증명을 비활성화된 인스턴스로 설정합니다. 이 속성을 사용하여 기능을 다시 활성화하면 시스템은 외부 자격 증명 기록을 활성으로 재설정하지 않습니다. 각 자격 증명 기록을 수동으로 다시 활성화해야 합니다.

지원되는 자격 증명 유형

통합은 다음과 같은 ServiceNow 자격 증명 유형을 지원합니다.CyberArk

- GCP
- Azure
- CIM
- JMS
- SNMP 포럼
- SNMPv3
- 기본 인증
- SSH 키 페어
- SSH 개인 키(키, 암호, 암호)
- VMware
- Windows
- 애플리케이션 자격 증명

주: GCP 자격 증명 유형과의 통합을 사용하려면 CyberArk 외부 자격 증명 스토리지 jar를 수정해야 합니다. 자세한 내용은 CyberArk를 사용하는 ServiceNow GCP 자격 증명 확인자를 참조하십시오.

Now Platform 이러한 네트워크 프로토콜을 사용하는 기능은 자격 증명 모음에 CyberArk 저장된 자격 증명 사용도 지원합니다.

네트워크 프로토콜에서 지원하는 자격 증명

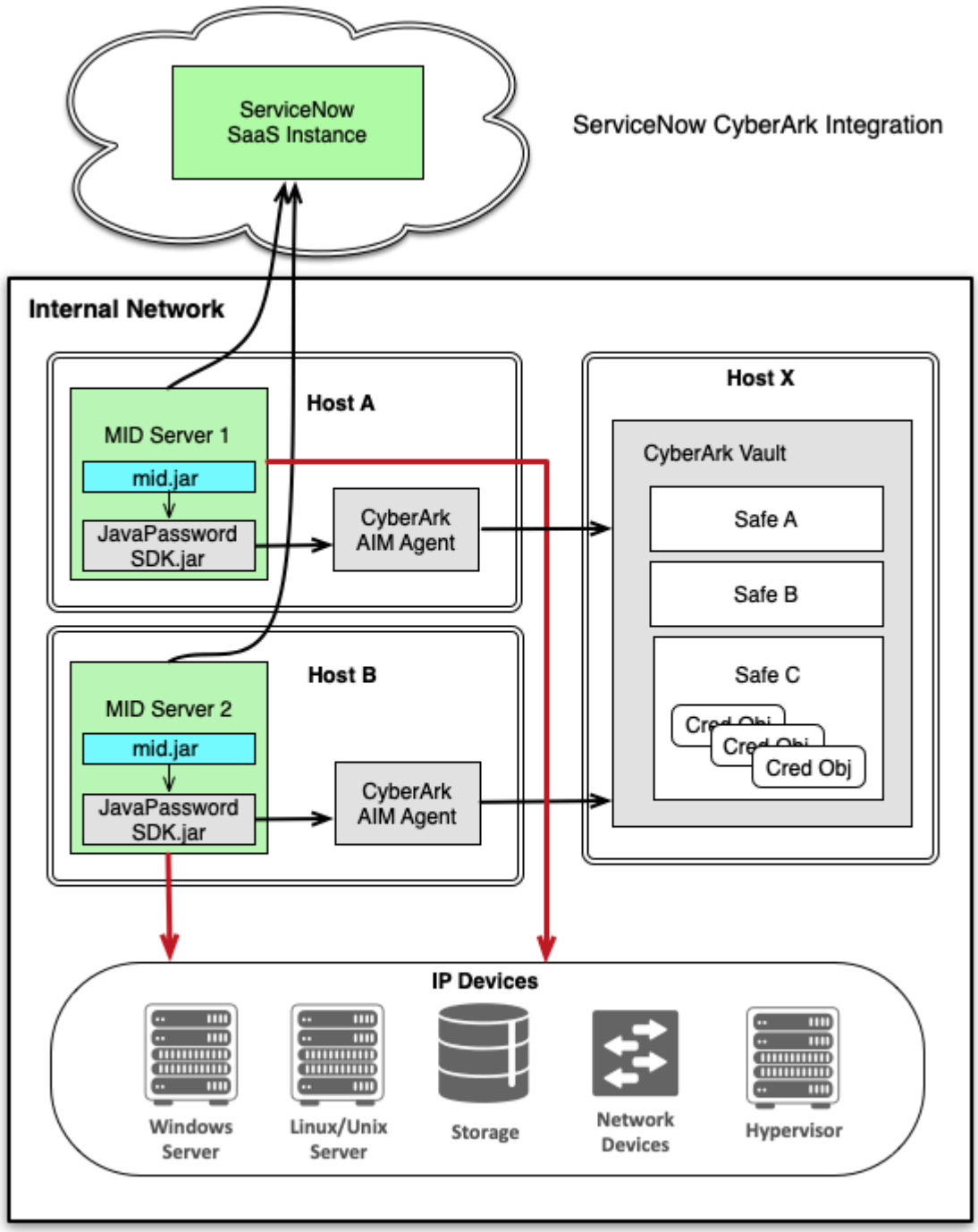
네트워크 프로토콜	ServiceNow® 플로우 디자이너 지원	오케스트레이션 지원
SOAP	SOAP 단계	기본 인증 무효화로 SOAP 웹 서비스 활동 작성
REST	REST(Representational State Transfer) 단계	기본 인증 무효화로 REST 웹 서비스 활동 작성
JDBC	JDBC 단계	JDBC 활동
SSH	SSH 단계	SSH 활동
PowerShell	PowerShell 단계	PowerShell 활동
SFTP	SFTP 단계	SFTP 활동
JMS		JMS 활동

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

중요사항: 자격 증명 모음 및 사용자 지정 외부 자격 증명 스토리지 시스템에 저장된 CyberArk 자격 증명은 동일한 MID 서버. MID 서버 및 CyberArk AIM/API 클라이언트를 동일한 머신에 설치해야 합니다.

CyberArk 아키텍처

CyberArk 스토리지 아키텍처



주: CyberArk 는 자격 증명을 해결하기 위해 기본 시스템 `mid.jar` 파일을 사용합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

계정을 **MID** 서버 처리하는 **Windows** 방법

자격 증명 조회는 처음에 지정된 자격 증명 ID를 볼트 이름 필드의 기존 값과 CyberArk 일치시키려고 시도합니다. 일치하는 항목이 발견되면 해당 자격 증명이 반환됩니다. 일치하는 항목이 없으면 자격 증명 조회에서 IP 주소를 사용하여 일치하는 항목을 찾습니다. IP 주소 조회가 둘 이상의 자격 증명(예: WindowsTomcat 동일한 서버)과 일치하는 경우 조회가 실패합니다. 이 문제를 방지하려면 config.xml 파일의 매개 변수를 MID 서버**true**로 설정하여 *ext.cred.type_specifier* 자격 증명 유형과 IP 주소 모두 일치하는 자격 증명을 강제로 반환하도록 합니다CyberArk. 예를 들어, IP 주소가 and 에 의해 Windows 공유되는 경우 자격 Windows 증명 유형의 경우 자격 증명만 반환합니다Windows.Tomcat

CyberArk 라이브러리 업그레이드

보안 구성 매개변수가 필요한 경우 라이브러리를 업그레이드할 CyberArk 수 있습니다.

config.xml에서 다음 구성 매개변수를 확인하십시오. `<parameter name="mid.secure_config.provider" value="com.service_now.mid.services.config.CyberArkSecuredConfigProvider"/>`

보안 구성 매개변수 제공자가 구성된 경우 업그레이드를 수행하려면 다음 단계를 수행합니다.

1. 클라이언트 버전의 이름을 `JavaPasswordSDK_MajorVersion_minorVersion_patchNum.jar`로 바꿉니다CyberArk.
2. `ecc_agent` 테이블에 이름 바꾸기 jar를 첨부할 수 있는 새 jar 항목을 작성합니다. 이 새 항목은 MID 서버. 이 단계를 수행하면 두 개의 jar (Passworsdk.jar 및 JavaPasswordSDK _12_X_X.jar)가 생성됩니다.
3. 인스턴스에서 이전 ecc_agent 항목을 삭제합니다. 이 단계에서는 에서 MID 서버Passworsdk.jar 삭제하고 JavaPasswordSDK _12_X_X.jar 시스템에 남아 있습니다.

CyberArk 통합 구성

이러한 절차에는 적절한 CyberArk 설명서에 대한 참조를 포함하여 CyberArk 및 ServiceNow 구성 작업이 모두 포함됩니다.

인스턴스에 구성된 ServiceNow 자격 증명 식별자는 CyberArk 볼트의 자격 증명 이름에 매핑되어야 합니다. 자격 증명을 조회할 때 MID 서버는 자격 증명 식별자를 Vault의 이름과 일치시켜 자격 증명을 찾습니다. 이름은 고유해야 합니다. 자격 증명 식별자가 비어 있으면 MID 서버는 IP 주소로 자격 증명을 찾습니다. IP 주소로 자격 증명을 식별하기 위해 시스템은 자격 증명 유형을 조사하여 해당 주소에 해당 유형의 자격 증명이 하나만 있는지 확인합니다. 예를 들어 Windows 서버와 vCenter가 모두 동일한 IP 주소에서 실행되는 경우를 들 수 있습니다. SSH 환경에서 이와 같은 엄격한 자격 증명 요구 사항을 지원하기 위해 MID Server 구성 매개 변수를 사용하면 요청된 자격 증명 유형이 CyberArk에서 반환되는 유형과 일치하도록 요구할 수 있습니다.

> **주:** 자격 증명 **ID** 필드는 SNMPv3를 제외한 모든 경우에 자격 증명을 CyberArk에 매핑하는 데 필요한 유일한 필드입니다. 개인 자격 증명 **ID** 필드는 선택 사항이며 SNMPv3 자격 증명을 사용하고 자격 증명에 개인 프로토콜을 사용하는 경우에만 필요합니다. 자세한 내용은 CyberArk 자격 증명 식별자 구성 문서를 참조하십시오.

CyberArk 볼트에서 자격 증명을 가져오도록 인스턴스를 구성하려면 아래에 나타나는 순서대로 작업을 완료하십시오.

CyberArk 저장소 구성 및 **AIM API** 설치

MID 서버 액세스를 허용하도록 CyberArk 볼트를 구성하고 MID 서버 머신에 CyberArk AIM API를 설치합니다.

시작하기 전에
필요한 역할: 관리자

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 절차를 시작하기에 앞서 외부 자격 증명 스토리지 플러그인 이 활성화되어 있는지 확인하십시오. CyberArk Application Access Manager(AAM) 자격 증명 공급자 버전 12.0.1 이상이 지원됩니다.

프로시저

1. 자격 증명을 요청하는 모든 MID 서버에서 사용할 애플리케이션 ID 및 인증 세부 정보로 CyberArk Vault를 구성합니다.
   자세한 내용은 CyberArk 자격 증명 공급자 및 ASCP 구현 가이드를 참조하십시오.

   a. CyberArk에서 라는 *ServiceNow_MID_Server*App-ID를 생성하여 MID Server가 볼트에 액세스할 수 있도록 CyberArk가 구성되어 있는지 확인하십시오.

   b. MID 서버에 필요한 모든 자격 증명에 App-ID에 대한 *ServiceNow_MID_Server* 액세스 권한이 부여되어 있는지 확인하십시오.

      주: ext.cred.app_id 매개변수를 사용하여 MID 서버 `config.xml` 파일의 기본 **ServiceNow_MID_Server** App-ID를 무효화할 수 있습니다. 이 매개변수의 값을 변경하는 경우 볼트에서 일치하는 값을 구성해야 합니다.

2. 자격 증명 스토어에 액세스하는 데 사용되는 MID 서버 서비스를 호스팅하는 각 머신에 AIM API를 포함한 CyberArk 자격 증명 제공자를 설치합니다.
3. CyberArk 계정을 프로비저닝하고 애플리케이션 액세스 권한을 설정합니다.
   자세한 내용은 CyberArk 권한 있는 계정 보안 구현 가이드를 참조하십시오.
   a. CyberArk 암호 금고에서 검색, 오케스트레이션 또는 서비스 매핑에 필요한 권한 있는 계정을 생성하여 다른 장치에 액세스하고 이러한 계정이 필요한 자격 증명이 저장된 금고의 구성원인지 확인합니다.
   b. 자격 증명 제공자 및 애플리케이션 사용자를 애플리케이션 암호가 저장되는 암호 세이프의 구성원으로 추가합니다.

CyberArk JAR 파일 임포트

MID 서버에서 액세스할 수 있도록 CyberArk JavaPasswordSDK.jar 파일을 인스턴스로 임포트합니다.

시작하기 전에
필요한 역할: agent_admin 또는 admin
이 절차를 시작하기에 앞서 MID 서버가 자격 증명에 액세스할 수 있도록 CyberArk가 구성되어 있는지 확인하십시오. Vault에 액세스하는 데 사용되는 MID Server를 호스팅하는 각 서버에 CyberArk AIM API가 설치되어 있는지 확인합니다.

주: 별도의 두 CyberArk 통합은 MID 서버에서 지원되지 않습니다. 동일한 인스턴스에 연결된 모든 MID Server에 동일한 버전의 CyberArk AIM API가 설치되어 있어야 합니다.

이 태스크 정보
JavaPasswordSDK.jar 파일이 MID 서버에 이미 있는 경우에도 이 프로세스를 사용합니다.

프로시저

1. 다음으로 이동 모두 > **MID** 서버 > **JAR** 파일.
2. 새로 만들기를 클릭합니다.
3. 테이블의 필드를 사용하여 양식을 작성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

JAR 파일 양식 필드

필드	설명
이름	인스턴스에서 파일을 식별하기 위한 고유하고 설명적인 이름입니다.
버전	파일의 선택적 버전 번호입니다(있는 경우).
소스	JAR 파일의 제공자입니다. 소스 정보는 시스템에서 사용되지 않습니다.
설명	JAR 파일 및 인스턴스에서의 목적에 대한 선택적 짧은 설명입니다.

4. 이 기록에 JAR 파일을 첨부합니다.
   AIM `JavaPasswordSDK.jar` 파일은 AIM SDK 설치 파일과 함께 제공되며 일반적으로 MID Server의 AIM 설치 디렉터리(`<install_dir>/CyberArk/ApplicationPasswordSdk`)에 있습니다.

   주: 첨부된 AIM JavaPasswordSDK.jar은 설치된 CyberArk AIM API 버전과 일치해야 합니다. JavaPasswordSDK.jar 파일이 일치하지 않으면 예기치 않은 동작과 잠재적인 기능 문제가 발생할 수 있습니다.

5. 제출을 클릭합니다.
6. MID 서버 서비스를 다시 시작합니다.
   플랫폼은 인스턴스와 통신하도록 구성된 모든 MID 서버에서 JAR 파일을 사용할 수 있게 합니다.

CyberArk에 대한 **MID** 서버 구성

MID 서버에 CyberArk 볼트에 대한 액세스 권한을 부여하도록 `config.xml` 파일을 구성합니다.

시작하기 전에

필요한 역할: 관리자

이 절차를 시작하기 전에 `JavaPasswordSDK.jar` 파일을 인스턴스로 임포트합니다.

프로시저

수동으로 MID 서버 구성 다음 매개변수를 사용하여 MID 서버 매개변수 파일을 추가합니다 .

이 구성은 인스턴스에서 수행할 수 없습니다.

필수 구성 매개변수

매개변수	값	설명
ext.cred.safe_folder	폴더 이름	모든 자격 증명 조회에 사용할 폴더입니다. 예를 들어 루트입니다.
ext.cred.use_cyberark	참	이 MID 서버가 CyberArk와 통합되었음을 나타내는 부울 매개변수입니다.

선택적 구성 매개변수

매개변수	값	설명
ext.cred.safe_timeout	5(초)	자격 증명 모음의 각 자격 증명 조회에 소요되는 시간 제한(초)입니다.
ext.cred.safe_name	안전한이름의이름	모든 자격 증명 조회에 사용되는 기본 안전 이름입니다. 매개변수가 여러

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

매개변수	값	설명
		SAF에 있는 경우 자격 증명 ID를 . *<safeName>:<CredentialID>*형식으로 지정할 수 있습니다. 이렇게 구성하면 **NameOfSafe** 필드가 무시됩니다. 모든 외부 자격 증명의 자격 증명 ID가 이 형식으로 지정된 경우 **NameOfSafe** 필드를 생략합니다. 주: 기본적으로 이 형식의 구분 기호는 콜론입니다. 구분 기호로 원하는 문자를 할당하려면 `CredMap.properties` 파일에 `safe.cred.split.string=<string>` 줄을 추가합니다.
ext.cred.app_id	ServiceNow_MID_Server	MID 서버에 CyberArk 볼트에 접근할 수 있는 권한을 부여하는 데 사용되는 앱 ID를 지정합니다. 기본값인 **ServiceNow_MID_Server**은 CyberArk 볼트에 정의되어야 합니다. 이 매개변수를 사용하여 기본값을 재정의하고 고유한 App-ID를 지정할 수 있습니다. 이 매개변수에서 App-ID를 편집하는 경우 일치하도록 CyberArk를 구성해야 합니다.
ext.cred.type_specific	참	CyberArk 플랫폼 ID 및 IP 주소와 모두 일치하는 자격 증명을 반환하기 위해 IP 주소 조회를 강제 실행합니다. 예를 들어, IP 주소가 Windows와 Tomcat 모두에서 공유되는 경우 플랫폼 ID가 **Win** 으로 시작하는 자격 증명은 Windows 자격 증명만 반환합니다. 이 매개변수가 true로 설정되면 CyberArk는 다음으로 시작하는 플랫폼 ID를 찾습니다. • Win: Windows • Unix: SSH • VMWare : VM웨어
ext.cred.check_ssh_type	거짓	true로 설정하면 CyberArk에서 반환된 SSH 자격 증명 유형이 요청된 자격 증명 유형과 일치해야 합니다. 예를 들어 일반 SSH 사용자 이름/암호 자격 증명이 요청되고 SSH 키만 사용할 수 있는 경우 자격 증명 조회가 실패합니다.

SNMPv2 자격 증명에 대한 **CyberArk** 구성

시스템에서 SNMPv2를 사용하는 경우 특수 파일을 생성하여 자격 증명의 속성을 커뮤니티 문자열에 매핑할 수 있습니다.

시작하기 전에
필요한 역할: 관리자
이 절차를 시작하기 전에 CyberArk 볼트에 액세스할 수 있도록 MID 서버를 구성하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

이 태스크 정보

주: 커뮤니티 문자열이 CyberArk 자격 증명의 암호 필드에 나타나는 경우에는 이 절차를 수행할 필요가 없습니다.

SNMPv2는 CyberArk에서 기본적으로 지원되지 않습니다. 조직에서 자격 증명의 암호 필드에 커뮤니티 문자열이 나타나지 않는 사용자 지정 SNMPv2 자격 증명을 만든 경우 다음 절차를 사용하여 자격 증명의 속성을 커뮤니티 문자열에 매핑합니다.

프로시저

1. 텍스트 편집기에서 다음 코드를 포함하는 `CredMap.properties`라는 파일을 만듭니다.
   `SNMPv2.Community=attribute_name`
2. MID Server 설치의 `/agent` 디렉터리에 파일을 저장합니다.
   자격 증명 조회 시 MID 서버는 자격 증명에 대해 이 속성을 찾으려고 시도합니다. 속성을 찾을 수 없는 경우 MID 서버는 암호 필드를 조회합니다. 암호 필드가 비어 있으면 자격 증명 조회에 실패합니다.

CyberArk 자격 증명 식별자 구성

CyberArk가 외부 리포지토리에서 특정 자격 증명을 식별하는 데 사용할 수 있는 고유 키를 생성합니다.

시작하기 전에

필요한 역할: 관리자

이 절차를 시작하기 전에 외부 자격 증명 스토리지 플러그인이 활성화되어 있고 com.snc.use_external_credentials 시스템 속성이 true로 설정되어 있는지 확인합니다.

프로시저

1. 다음으로 이동 모두 > 디스커버리 > 자격 증명 또는 오케스트레이션 > 자격 증명.
2. 새로 만들기를 클릭합니다.
3. 자격 증명 유형 목록에서 CyberArk 외부 스토리지를 지원하는 유형을 선택합니다.
4. 자격 증명 유형의 필드를 사용하여 양식을 작성합니다.
5. 외부 자격 증명 저장소 확인란을 선택합니다.
   사용자 이름 및 암호 필드가 자격 증명 **ID** 필드로 바뀝니다.

   주: 확인란이 표시되지 않으면 헤더 표시줄에서 메뉴 아이콘을 클릭하고 뷰 > 외부 스토리지.

6. 자격 증명 **ID** 필드에 다음 형식 중 하나를 사용하여 식을 입력합니다.
   - 모든 자격 증명이 동일한 금고에 있는 경우 ext.cred.safe_name 매개변수를 사용하여 MID 서버 `config.xml` 파일에서 이 안전 이름을 구성한 다음 자격 증명 ID를 〈자격 증명 **ID>**로 이름으로만 지정합니다.
   - 특정 금고에 있는 특정 플랫폼에 대한 자격 증명의 이름을 지정하려면 자격 증명 ID를 **<safe>:<credential** ID〉:〈플랫폼 **ID>**로 정의합니다.
   - 자격 증명이 여러 안전에 있는 경우 **<safe>:<credential ID>** 형식으로 자격 증명 ID를 지정합니다.
   - CyberArk가 대체 금고를 사용하여 IP 주소로 자격 증명을 조회하도록 하려면 **<safe>:** 형식으로 자격 증명 ID를 지정합니다.
   - CyberArk가 동일한 금고에서 대체 플랫폼 ID에 대한 자격 증명을 조회하도록 하려면 ::〈플랫폼 **ID** 형식을 사용하십시오>

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ CyberArk가 자격 증명 ID가 아닌 IP 주소로 구성된 금고에서 자격 증명을 조회하도록 하려면 이 필드를 비워 두십시오. 이는 각 서버에 고유한 자격 증명이 있는 설치를 처리하는 가장 좋은 방법입니다. 이러한 유형의 조회가 없으면 환경의 모든 서버에 대해 인스턴스에 자격 증명 ID 기록을 만들어야 합니다.

주: 자격 증명 ID는 CyberArk 계정의 이름 필드 값과 일치해야 합니다. 자격 증명 **ID** 필드는 180자로 제한됩니다.

7. CyberArk에 SNMPv3 자격 증명을 저장하고 개인 프로토콜 및 개인 키를 사용하는 경우 다음과 같이 ID를 구성합니다.

   a. 자격 증명 스토어 유형 필드에서 **CyberArk**를 선택합니다.
   개인 자격 증명 **ID** 필드가 나타납니다.

   b. 개인 정보 자격 증명 **ID** 필드에 CyberArk SNMPv3 개인 계정의 이름을 입력합니다.

8. 제출을 클릭합니다.

CyberArk Vault에서 **AWS** 자격 증명 구성

인스턴스에서 사용하기 위해 검색할 AWS 자격 증명으로 CyberArk 볼트를 구성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
자격 증명을 CyberArk Vault에 계정으로 저장합니다. 인스턴스에서 볼트에 대한 액세스를 구성할 때 계정에 지정한 이름도 자격 증명 ID로 사용해야 합니다.

주: 다음 절차는 CyberArk Password Vault v14.2.1을 참조합니다. 다른 버전을 사용하는 경우 공식 CyberArk Password Vault 설명서에 따라 구성을 설정하십시오.

프로시저

1. CyberArk에서 계정 > 계정 및 요청 > 계정 뷰 > 계정 추가.
2. 시스템 유형: 클라우드 서비스를 선택합니다.
3. 플랫폼에 할당: **Amazon Web Services - AWS -** 접근 키.
4. 금고에 저장: 목록에서 금고를 선택합니다.
5. 속성 정의: 다음 정보를 입력합니다.

CyberArk 자격 증명

필드	값
AWS IAM 사용자 이름	AWS에서 제공하는 AWS 접근 키를 입력합니다.
AWS 접근 키 비밀(선택 사항)	AWS에서 제공하는 대로 AWS 비밀 접근 키를 입력합니다.
계정 이름 사용자 지정	슬라이더를 전환하여 이 키의 사용자 지정 이름을 입력합니다.
AWS 접근 키 ID	AWS에서 제공한 대로 AWS 접근 키를 다시 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	값
AWS 계정 ID 번호	AWS에서 제공한 대로 AWS 접근 키를 다시 입력합니다.
AWS 계정 별칭 이름(선택 사항)	계정의 별칭 이름을 입력합니다.

6. 추가**(Add)**를 선택합니다.

다음에 수행할 작업
아직 인스턴스에 자격 증명 식별자를 생성하여 CyberArk 볼트에 대한 액세스를 구성하지 않은 경우 인스턴스에 자격 증명 식별자를 생성합니다. 자세한 내용은 AWS에 대한 외부 자격 증명 스토리지에 대한 액세스 구성을 참조하세요.

클래식 UI를 사용하여 **CyberArk** Vault에서 **AWS** 자격 증명 구성
인스턴스에서 사용하기 위해 검색할 AWS 자격 증명으로 CyberArk 볼트를 구성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
CyberArk Password Vault v14.2.1에는 자격 증명을 계정으로 저장하는 계정 뷰 및 계정 뷰(클래식 UI) 구성 옵션이 모두 포함되어 있습니다. 인스턴스에서 볼트에 대한 액세스를 구성할 때 계정에 지정한 이름도 자격 증명 ID로 사용해야 합니다.

주: 다음 절차는 CyberArk Password Vault v14.2.1을 참조합니다. 다른 버전을 사용하는 경우 공식 CyberArk Password Vault 설명서에 따라 구성을 설정하십시오.

프로시저
1. CyberArk에서 계정 > 계정 및 요청 > 계정 뷰(클래식 **UI)** > 계정 추가.
2. 다음 정보를 입력합니다.

CyberArk 자격 증명

필드	값
장치 유형	클라우드 서비스를 선택합니다.
플랫폼 이름	**Amazon Web Services - AWS -** 접근 키를 선택합니다.
AWS IAM 사용자 이름	AWS에서 제공하는 AWS 접근 키를 입력합니다.
AWS 접근 키 ID	AWS에서 제공한 대로 AWS 접근 키를 다시 입력합니다.
AWS 계정 ID 번호	AWS에서 제공한 대로 AWS 접근 키를 다시 입력합니다.
AWS 접근 키 비밀	AWS에서 제공하는 대로 AWS 비밀 접근 키를 입력합니다.
이름	이 키의 사용자 지정 이름을 입력합니다.

3. 저장**(Save)**을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

다음에 수행할 작업
아직 인스턴스에 자격 증명 식별자를 생성하여 CyberArk 볼트에 대한 액세스를 구성하지 않은 경우 인스턴스에 자격 증명 식별자를 생성합니다. 자세한 내용은 AWS에 대한 외부 자격 증명 스토리지에 대한 액세스 구성을 참조하세요.

CyberArk Vault에서 **Azure** 자격 증명 구성

인스턴스에서 사용하기 위해 검색할 Azure 자격 증명으로 CyberArk Vault를 구성합니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
Azure 자격 증명을 저장하려면 먼저 CyberArk Vault에 Azure 자격 증명 템플릿을 생성합니다. 이 프로세스는 Vault에 대해 한 번만 완료하면 됩니다.

프로시저

1. 관리 모드에서 CyberArk에 로그인하십시오.
2. 관리 탭으로 이동합니다.
3. 시스템 구성에서 플랫폼 관리를 편집합니다.
4. 클라우드 제공자 템플릿으로 이동하여 복제합니다.
5. Azure 자격 증명에 대한 템플릿을 편집합니다.
6. 다음 두 속성을 추가합니다.
   - *Name* As *Username* 및 *Display Name* As *Client ID*
   - *Name* As *Address* 및 *DisplayName* As *Tenant ID*
7. 변경 내용을 적용합니다.
8. 계정 섹션으로 이동하여 계정 추가를 선택합니다.
9. 안전을 선택합니다.
10. 장치 유형을클라우드 서비스로 설정합니다.
11. 이전에 편집한 Azure 템플릿을 선택합니다.
12. 클라이언트 **ID**, 테넌트 **ID** 및 암호 필드에 대한 정보를 입력합니다.
13. 저장을 선택합니다.

외부 자격 증명 저장소를 사용한 **MID** 서버 **OAuth 2.0** 인증

OAuth 2.0 자격 증명(클라이언트 ID 및 클라이언트 비밀)을 ServiceNow 인스턴스 대신 볼트에 CyberArk 저장합니다. MID 서버 OAuth 토큰을 가져오는 데 필요한 경우 자격 증명을 볼트에서 CyberArk 가져옵니다. 토큰은 MID Server에 저장되고 만료 시 자동으로 새로 고쳐집니다.

CyberArk AIM(Application Identity Management) 제품은 권한 있는 계정 보안 솔루션을 사용하여 애플리케이션, 스크립트 또는 구성 파일에 포함된 애플리케이션 암호를 저장할 필요가 없으며 이러한 매우 중요한 암호를 자격 증명 모음 내에서 CyberArk 중앙에서 저장, 기록 및 관리할 수 있도록 합니다. 자격 증명 레코드에 직접 저장하지 않고 OAuth 2.0 자격 증명을 저장하도록 Vault를 ServiceNow 구성할 CyberArk 수 있습니다. CyberArk에 대한 자세한 내용은 CyberArk 자격 증명 스토리지 통합 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요청의 **OAuth 2.0** 인증 **MID** 서버 아키텍처

아키텍처는 인스턴스와 AIM(Application Identity Manager) 클라이언트 및 MID 서버가 구성되는 환경의 두 부분으로 ServiceNow 구성됩니다. 환경의 예로는 클라우드 또는 고객 환경이 있습니다.

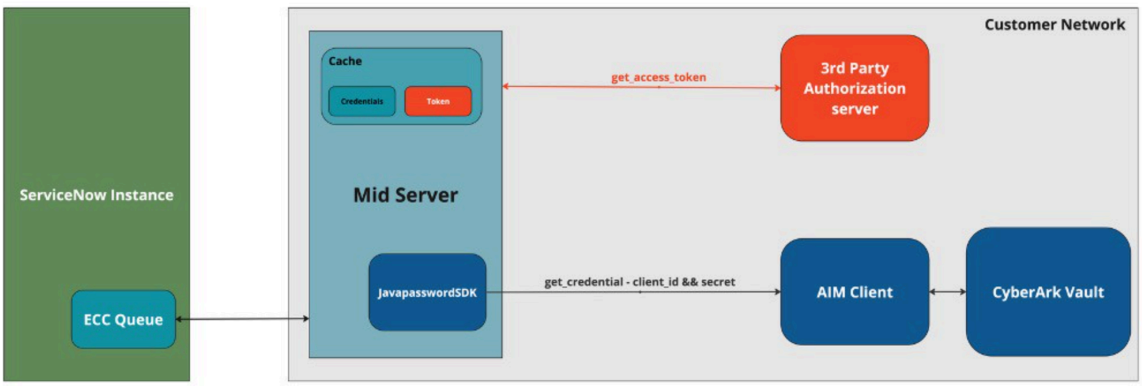
MID 서버 및 Application Identity Manager(AIM) 클라이언트는 동일한 환경에서 구성되어야 하며 Application Identity Manager(AIM)는 외부 저장소와 CyberArk 상호 작용하도록 구성되어야 합니다. 외부 저장소는 CyberArk MID Server 및 Application Identity Manager(AIM)와 동일한 환경 또는 다른 환경에서 호스팅될 수 있습니다.

인스턴스는 ServiceNow 볼트에 저장된 특정 OAuth 2.0 자격 증명에 매핑되는 자격 증명 식별자를 CyberArk 유지 관리합니다. OAuth 토큰 요청을 보내기 전에 MID 서버는 인스턴스에서 자격 증명 식별자를 얻은 다음 고객 제공 JAR 파일을 사용하여 식별자를 AIM 클라이언트로 보냅니다. AIM 클라이언트는 요청을 보관소로 CyberArk 보냅니다. Vault는 CyberArk AIM 클라이언트를 통해 OAuth 2.0 자격 증명을 MID 서버로 다시 보냅니다. OAuth 2.0 자격 증명을 받은 후 MID 서버는 외부 공급업체 인증 서버로 OAuth 토큰 요청을 보냅니다. 토큰 요청은 저장하는 클라이언트 및 클라이언트 암호 CyberArk , OAuth 범위, 인스턴스가 저장하는 토큰 URL 등의 정보로 구성됩니다. 권한 부여 서버에서 OAuth 토큰을 발급하면 MID 서버에서 해당 토큰을 캐시 메모리에 저장합니다.

주: 이 기능은 클라이언트 자격 증명 부여 유형을 지원합니다.

이미지는 MID Server 요청 인증 프로세스를 보여줍니다.

주: 타사 권한 부여 서버와 CyberArk 자격 증명 모음이 고객 네트워크에서 호스트된다고 가정합니다.



JAR 파일 및 자격 증명 식별자 구성

JAR 파일이 외부 저장소에서 실제 자격 증명으로 자격 증명 식별자를 확인할 수 있도록 JAR 파일 및 자격 증명 식별자를 CyberArk 구성합니다. 이 프로세스를 통해 MID 서버는 OAuth 토큰 요청에 OAuth 2.0 자격 증명을 가져와 포함할 수 있습니다.

시작하기 전에

필요한 역할: agent_admin 또는 admin

외부 저장소는 CyberArk 중요한 자격 증명을 ServiceNow 저장하고 인스턴스는 자격 증명 모음이 저장하는 특정 자격 증명 이름에 매핑되는 자격 증명 식별자를 저장합니다. JAR 파일을 사용하면 자격 증명 식별자를 외부 저장소의 특정 자격 증명 이름으로 매핑할 수 있습니다. 매핑을 통해 MID 서버 OAuth 토큰 요청에 필요한 자격 증명을 획득하고 포함할 수 있습니다. ServiceNow 인스턴스와 MID 서버에서 각각 자격 증명 식별자와 JAR 파일을 구성해야 합니다.

프로시저

1. CyberArk JAR 파일 임포트.
2. 외부 저장소 사용을 통해 MID 서버 OAuth 요청을 보내도록 연결 구성.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

CyberArk 구성

CyberArk OAuth 2.0 자격 증명을 MID 서버저장하고 .

시작하기 전에

ServiceNow 통합 허브 표준 팩 설치 관리자를 구독했는지 확인합니다. 자세한 내용은 https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf 문서를 참조하십시오.

필요한 역할: agent_admin 또는 admin

프로시저

1. CyberArk 저장소 구성 및 AIM API 설치.
2. CyberArk JAR 파일 임포트.
3. CyberArk에서 OAuth 2.0 자격 증명 구성.
4. 외부 저장소 사용을 통해 MID 서버 OAuth 요청을 보내도록 연결 구성.

CyberArk에서 **OAuth 2.0** 자격 증명 구성

인스턴스가 요청하는 OAuth 2.0 자격 증명으로 CyberArk 볼트를 ServiceNow 구성합니다.

시작하기 전에

필요한 역할: admin

이 태스크 정보

OAuth 2.0 자격 증명을 저장하려면 먼저 CyberArk Vault에 OAuth 2.0 자격 증명 템플릿을 생성합니다. Vault에 대해 이 프로세스는 한 번만 완료해야 합니다.

프로시저

1. OAuth 2.0 자격 증명을 처음 구성하는 경우 다음 단계를 수행합니다.

   a. 관리 모드에서 CyberArk에 로그인하십시오.

   b. 관리 탭으로 이동합니다.

   c. 플랫폼 관리를 선택합니다.
   플랫폼 관리 페이지의 대상 탭 아래에 플랫폼이 표시됩니다.

   d. 플랫폼 유형을 확장합니다.

   e. 플랫폼 템플릿에 해당하는 설정 아이콘(...)을 선택하고 복제를 선택합니다.

   f. Duplicate Platform 창에서 템플릿의 이름을 입력하고 **Create**를 선택합니다.

   > 주: 중복 템플릿을 만든 시스템 유형을 기록해 둡니다. 예를 들어 클라우드 서비스는 시스템 유형입니다.

   g. 생성한 중복 플랫폼 템플릿에 해당하는 설정 아이콘(...)을 선택하고 편집을 선택합니다.

   h. 속성을 추가합니다.
   이름을 사용자 이름으로 하고 표시 이름을 클라이언트 ID로 지정합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

i. 다른 속성의 이름을 바꿉니다.

팁: OAuth 2.0과 관련된 속성 이름을 선택합니다.

j. 적용을 선택합니다.
업데이트가 적용됩니다.

k. 확인을 선택합니다.

l. 왼쪽 패널에서 계정으로 이동합니다.

m. 계정 추가를 선택합니다.

n. 시스템 유형 제목 아래에서 플랫폼 템플릿을 생성한 시스템 유형을 선택합니다.
시스템 유형에 플랫폼 템플릿이 표시됩니다.

o. Select Platform(플랫폼 선택) 제목에서 생성한 플랫폼 템플릿을 선택합니다.

p. 안전을 선택합니다.
나중에 사용할 수 있도록 안전 값을 저장합니다.

q. 클라이언트 ID, 암호(클라이언트 암호를 값으로 제공) 및 필요에 따라 기타 필드에 대한 정보를 입력합니다.

r. 추가를 선택합니다.
계정이 추가됩니다.

s. 계정 뷰 페이지에서 계정을 엽니다.

t. 상세정보 탭을 선택합니다.

u. 계정 이름 섹션에 저장된 값을 복사하고 나중에 사용할 수 있도록 저장합니다.
복사 및 저장한 값은 ServiceNow 인스턴스에서 자격 증명 식별자로 사용됩니다.

2. OAuth 2.0 자격 증명을 처음 구성하지 않는 경우 다음 단계를 수행합니다.

a. 관리 모드에서 CyberArk에 로그인하십시오.

b. 계정 섹션으로 이동하여 계정 추가를 선택합니다.

c. OAuth 2.0을 저장하기 위한 템플릿이 있는 시스템 유형 에서 시스템 유형을 선택합니다.

d. 생성한 필수 플랫폼 템플릿을 선택하고 안전을 선택합니다.
나중에 사용할 수 있도록 안전 값을 저장합니다.

e. 클라이언트 ID, 암호(클라이언트 암호를 값으로 제공) 및 필요에 따라 기타 필드에 대한 정보를 입력합니다.

f. 추가를 선택합니다.
계정이 추가됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

g. 계정 뷰 페이지에서 계정을 엽니다.

h. 상세정보 탭을 선택합니다.

i. 계정 이름 섹션에 저장된 값을 복사하고 나중에 사용할 수 있도록 저장합니다.
복사하여 저장한 값은 인스턴스에서 자격 증명 식별자 ServiceNow 로 사용됩니다.

외부 저장소 사용을 통해 **MID** 서버 **OAuth** 요청을 보내도록 연결 구성

를 MID 서버통해 OAuth 2.0 토큰에 대한 요청을 외부 공급업체 인증 서버로 보내도록 연결을 구성합니다. MID 서버 외부 저장소의 OAuth 2.0 자격 증명(클라이언트 ID 및 클라이언트 암호), CyberArk 인스턴스에서 OAuth 범위 및 토큰 URL을 요청에 추가하고 타사 인증 서버로 보냅니다.

시작하기 전에
다음 항목을 검증합니다.

- ServiceNow 통합 허브 표준 팩 설치 관리자를 구독했는지 확인합니다. 자세한 내용은 https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf 문서를 참조하십시오.
- MID 서버가 외부 저장소로 CyberArk 자격 증명을 확인할 수 있는 JAR 파일을 생성했습니다. 자격 증명을 해결하기 위한 JAR 파일 생성 문서를 참조하십시오.
- JAR 파일을 MID 서버로 임포트했습니다.
- MID Server는 CyberArk용으로 설정되어 있습니다. CyberArk에 대한 MID 서버 구성 문서를 참조하십시오.
- OAuth 2.0은 CyberArk 외부 스토리지에 구성됩니다. CyberArk에서 OAuth 2.0 자격 증명 구성 문서를 참조하십시오.

필요한 역할: 없음

이 태스크 정보
구성 템플릿을 사용하거나 수동으로 연결 및 자격 증명을 구성할 수 있습니다. 구성 템플릿은 연결 기록 양식 구성요소를 정의하며 다른 연결 기록에 다시 사용할 수 있습니다. 수동으로 이 용도로만 연결을 구성할 수 있습니다. 이 항목에서는 두 가지 방법을 모두 보여 줍니다.

프로시저

1. 구성 템플릿으로 연결을 구성합니다.

   a. 다음으로 이동 모두 > 통합 허브 > 구성 템플릿.

   b. 새로 만들기를 선택합니다.

   c. **OAuth** 클라이언트 자격 증명 부여 유형을 사용하는 **HTTP** 연결(외부 스토리지)을 선택합니다.

   d. 필요에 따라 양식을 업데이트합니다.
   예를 들어 기본 데이터 템플릿 섹션의 `oauth_entity_profile_scope` 및 `oauth_entity_scope` 필드에 범위를 제공할 수 있습니다. 구성 템플릿을 만드는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 구성 템플릿 생성.

   e. 제출을 선택합니다.
   구성 템플릿을 생성했습니다.

   f. 다음으로 이동 모두 > 통합 허브 > 연결 및 자격 증명 별칭.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

g. 양식을 업데이트합니다.

연결 및 자격 증명 별칭

필드	설명
이름	별칭의 이름입니다. 별칭에는 알파, 숫자 및 밑줄 문자만 사용할 수 있습니다. 업그레이드 중에 자격 증명 기록의 태그는 연결 및 자격 증명 별칭으로 마이그레이션됩니다. 자격 증명 태그에 알파벳, 숫자 및 밑줄 이외의 특수 문자가 포함되어 있으면 업그레이드 후에도 태그 이름이 유지됩니다. 마이그레이션된 이 별칭을 계속 사용할 수 있지만 명명 제한을 충족하도록 이름을 변경할 때까지 별칭을 업데이트할 수 없습니다.
애플리케이션	연결 및 자격 증명 별칭의 고유 식별자로, `scope_name.alias_name` 형식을 기반으로 합니다. ▪ 범위가 전역인 경우 ID는 별칭 이름입니다. 예를 들어 전역 범위에서 Workday 별칭을 만들면 ID가 `Workday`로 설정됩니다. ▪ HR 앱 범위에서 Workday 별칭을 만들면 ID가 `x_hr_app.Workday`로 설정됩니다.
상위 별칭	이 연결 및 자격 증명 별칭을 생성하는 데 사용할 별칭을 선택하는 옵션입니다. 생성하려는 연결 및 자격 증명 별칭은 하위 별칭입니다. 하위 별칭은 상위 연결 및 자격 증명 별칭 페이지의 하위 별칭 탭 아래에 나열됩니다. 
유형	생성 중인 별칭의 유형을 나타내는 옵션입니다. 다음 옵션 중에서 선택합니다. ▪ 자격 증명: 자격 증명 기록이 포함된 별칭입니다. ▪ 연결 및 자격 증명: 연결 및 자격 증명 기록을 모두 포함하는 별칭입니다. 이 옵션은 기본적으로 선택됩니다. 연결 및 자격 증명이 선택되었는지 확인합니다.
다중 활성 연결 지원	별칭이 여러 활성 연결을 지원하는지 여부를 나타내는 지정자입니다. 연결 테이블을 사용하여 연결을 추가하고 연결 관련 목록을 사용하여 별칭에 연결합니다.
기본 재시도 정책	별칭에 대한 재시도 정책입니다. 자세한 내용은 재시도 정책을 참조하세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
구성 템플릿	연결 및 자격 증명 별칭을 생성하는 데 기반이 되는 구성 템플릿을 선택하는 옵션입니다. 생성한 **OAuth** 클라이언트 자격 증명 부여 유형(외부 저장소)을 사용하는 **HTTP** 연결 유형의 템플릿을 선택합니다.

h. 제출을 선택합니다.
연결 및 자격 증명 별칭 기록을 생성했습니다.

i. 다음으로 이동 모두 > 통합 허브 > 연결 대시보드.

j. 모든 연결 검색 필드에 생성한 연결 및 자격 증명 별칭 기록의 이름을 입력합니다.

k. 연결 및 자격 증명 별칭 기록에서 상세 정보 보기를 선택합니다.

l. 구성을 선택합니다.

m. 양식을 작성합니다.

연결 구성 양식

필드	설명
연결 이름	연결의 이름입니다. 이름을 업데이트할 수 없습니다.
연결 URL	외부 공급업체 서버에 대한 URL입니다.
MID 사용	MID 서버를 활성화하는 옵션입니다. 중요사항: 옵션이 선택되어 있는지 확인합니다.
MID 선택	연결에 대한 MID 구성을 지정하는 옵션입니다. ▪ 특정 **MID** 서버: 특정 MID 서버의 수동 선택을 나타내는 옵션입니다. ▪ **MID** 서버 자동 선택: MID 서버를 자동으로 선택할지 여부를 나타내는 옵션입니다. ▪ 특정 **MID** 클러스터: MID Server의 MID 클러스터 수동 선택을 나타내는 옵션입니다. 중요사항: 선택한 MID 서버가 CyberArk 볼트에 액세스하도록 구성된 CyberArk AIM 클라이언트와 동일한 컴퓨터에 있는지 확인합니다. CyberArk 저장소 구성 및 AIM API 설치 문서를 참조하십시오.
MID 서버	MID 서버를 수동으로 지정하는 옵션입니다. 이 옵션은 **MID** 선택 필드에서 특정 **MID** 서버를 선택한 경우 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
MID 클러스터	MID 클러스터를 수동으로 지정하는 옵션입니다. 이 옵션은 **MID** 선택 필드에서 특정 **MID** 클러스터를 선택한 경우 나타납니다.
외부 자격 증명 스토어	CyberArk 외부 자격 증명 스토리지를 사용하는 옵션입니다. 이 옵션을 선택하면 MID 서버가 외부 자격 증명 스토리지에서 OAuth 2.0 자격 증명(클라이언트 ID 및 클라이언트 비밀)을 가져옵니다. 중요사항: 옵션이 선택되어 있는지 확인합니다.
자격 증명 ID	클라이언트 ID 및 클라이언트 비밀 상세 정보를 포함하는 CyberArk 계정의 식별자입니다. 자격 증명 식별자를 가져오는 절차를 보려면 다음 문서를 CyberArk에서 OAuth 2.0 자격 증명 구성참조하십시오. 자격 증명 ID 필드에 다음 형식 중 하나를 사용하여 식을 입력합니다. ▪ 모든 자격 증명이 동일한 금고에 있는 경우 ext.cred.safe_name 매개변수를 사용하여 MID 서버 `config.xml` 파일에서 이 안전 이름을 구성한 다음 자격 증명 ID를 〈자격 증명 **ID>**로 이름으로만 지정합니다. ▪ 특정 금고에 있는 특정 플랫폼에 대한 자격 증명의 이름을 지정하려면 자격 증명 ID를 **<safe>:<credential** ID〉:〈플랫폼 **ID>**로 정의합니다. ▪ 자격 증명이 여러 안전에 있는 경우 **<safe>:<credential ID>** 형식으로 자격 증명 ID를 지정합니다.
OAuth 토큰 URL	OAuth 서버에서 액세스 토큰을 가져올 엔드포인트를 지정하는 URL입니다.

n. 연결 구성을 선택합니다.

2. 연결을 수동으로 구성합니다.

a. 다음으로 이동 모두 > 시스템 **OAuth** > 애플리케이션 레지스트리.

b. 새로 만들기를 선택합니다.

c. 외부 저장소를 사용하여 외부 공급업체 **OAuth** 공급자에 연결을 선택합니다.

d. 양식을 작성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

새 애플리케이션 레지스트리 상세 정보

필드	설명
이름	애플리케이션 레지스트리 기록을 식별하기 위한 이름입니다. 예를 들어 MID 앱을 통한 OAuth 2.0 토큰 요청을 입력합니다.
애플리케이션	이 애플리케이션 레지스트리에 액세스할 수 있는 애플리케이션의 이름을 지정하는 옵션입니다. 필드는 읽기 전용입니다.
기본 부여 유형	OAuth 서버에서 클라이언트 애플리케이션으로 액세스 토큰을 가져오는 기본 방법입니다. 기본 및 읽기 전용 권한 부여 유형은 클라이언트 자격 증명입니다.
다음에서 접근 가능	이 애플리케이션 레지스트리에 액세스할 수 있는 애플리케이션을 지정하는 옵션입니다.
토큰 URL	OAuth 서버에서 액세스 토큰을 가져올 엔드포인트를 지정하는 URL입니다.
자격 증명 보내기	요청 본문에 OAuth 2.0을 보내는 방법을 지정하는 옵션입니다.
설명	관련 의견을 입력합니다.

e. **OAuth** 범위 열에서 다음 단계를 수행하여 하나 이상의 OAuth 범위를 생성합니다.

i. 이름 열에서 필드를 두 번 클릭하고 OAuth 범위의 이름을 입력합니다.

ii. OAuth 범위 열에서 필드를 두 번 클릭하고 범위를 입력합니다.

f. 제출을 선택합니다.
OAuth 엔터티 프로파일과 애플리케이션 레지스트리를 생성했습니다.

g. 다음으로 이동 모두 > 통합 허브 > 연결 및 자격 증명 > 자격 증명.

h. 새로 만들기를 선택합니다.

i. **OAuth 2.0** 자격 증명을 선택합니다.

j. 외부 저장소 보기를 선택합니다.

중요사항: 뷰가 OAuth 2.0 자격 증명 외부 스토리지 양식의 뷰와 다른 경우에만 외부 스토리지 뷰를 선택합니다.

k. 양식을 작성합니다.

OAuth 2.0 자격 증명

필드	설명
이름	자격 증명 기록의 이름입니다.
적용 대상	자격 증명 기록을 모든 MID 서버 또는 특정 MID 서버에 적용할 수 있는지 여부를 지정하는 옵션입니다. 특정 경우 MID Server를 추가합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	다음 옵션 중 하나를 선택합니다. ▪ 모든 MID 서버: MID 서버는 MID 서버 컬렉션에서 자동으로 선택됩니다. ▪ 특정 MID 서버: 하나 이상의 MID 서버를 지정하는 옵션입니다.
MID 서버	하나 이상의 MID 서버를 지정하는 옵션입니다. 주: 이 필드는 적용 대상 필드에서 특정 **MID** 서버를 선택한 경우에 나타납니다.
활성	자격 증명 기록을 사용할 수 있는지 여부를 지정하는 옵션입니다. 기본적으로 사용할 수 있습니다.
OAuth 엔터티 프로파일	자격 증명에서 사용하는 OAuth 엔터티 프로파일을 지정하는 옵션입니다. 위에서 만든 OAuth 엔터티 프로파일을 선택합니다. OAuth 엔터티 프로파일 구성의 내용을 참조하십시오.
외부 자격 증명 스토어	자격 증명이 ServiceNow 인스턴스가 아닌 외부 저장소에 저장되도록 지정하는 옵션입니다. 중요사항: 옵션이 선택되어 있는지 확인합니다.
자격 증명 ID	클라이언트 ID와 클라이언트 비밀을 보유한 CyberArk 계정의 자격 증명 식별자를 지정하는 옵션입니다. 자격 증명 식별자를 가져오는 절차를 보려면 다음 문서를 CyberArk에서 OAuth 2.0 자격 증명 구성참조하십시오.
자격 증명 스토리지 Vault	외부 자격 증명 스토리지 Vault의 이름을 지정하는 옵션입니다. 을 선택 CyberArk했는지 확인합니다.

l. 제출을 선택합니다.
자격 증명 기록이 생성되었습니다.

m. 연결 및 자격 증명 별칭을 생성합니다.
단계를 알아보려면 문서를 참조하십시오 연결 및 자격 증명 별칭 생성.

n. 다음으로 이동 모두 > 통합 허브 > 연결.

o. 새로 만들기를 선택합니다.

p. HTTP(s) 연결을 선택합니다.

q. 양식을 작성합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

연결 양식

필드	설명
이름	이 HTTP 연결의 고유한 이름입니다.
활성	생성 중인 연결을 활성으로 설정하는 옵션입니다. 이 옵션은 기본적으로 선택되어 있습니다.
자격 증명	연결 권한을 부여하는 데 사용할 자격 증명 레코드를 선택합니다. 위에서 생성한 자격 증명을 선택합니다.
연결 별칭	이 연결과 연결할 레코드 별칭을 선택합니다. 별칭을 사용하면 별칭을 사용하는 작업이나 활동을 재구성하지 않고도 연결 기록을 업데이트할 수 있습니다.
URL 작성기	연결 URL을 수동으로 입력하거나 시스템을 사용하여 입력을 기반으로 URL을 작성합니다. 기본값은 선택 취소되어 있습니다. 선택 시 연결 URL은 다음 필드에서 계산됩니다. ▪ 상호 인증 — 상호 인증이 사용되는 경우 확인란입니다. ▪ 프로토콜 — 상호 인증을 사용하지 않는 경우 protocol을 입력합니다. 기본값은 HTTPs입니다. ▪ 프로토콜 프로파일 — 상호 인증을 사용하는 경우 sys_protocol_profile에서 프로토콜 프로파일을 입력합니다. ▪ 호스트 ▪ 포트 ▪ 기본 경로 — 연결 문자열의 경로입니다. 주: 상호 인증을 선택하면 연결 URL이 구축됩니다: 프로토콜 + :// + 호스트:포트 + URL입니다. 상호 인증을 선택하지 않으면 연결 URL이 빌드됩니다. 프로토콜 프로파일 + :// + 호스트:포트 +URL
연결 URL	URL 작성기가 선택되어 있지 않은 경우 이 필드에 연결 URL을 입력합니다. 주: 상호 인증을 선택하면 연결 URL이 구축됩니다: 프로토콜 + :// + 호스트:포트 + URL입니다. 상호 인증을 선택하지 않으면 연결 URL이 빌드됩니다. 프로토콜 프로파일 + :// + 호스트:포트 +URL
MID 서버 사용	MID 서버를 통해 OAuth 토큰 요청을 보내도록 지정하는 옵션입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	중요사항: 옵션이 선택되어 있는지 확인합니다.
연결 시간 제한	호스트가 성공적으로 연결되기까지 시스템에서 기다리는 시간(밀리초)입니다. 이 시간 동안 연결에 성공하지 못하면 연결 요청이 시간 초과됩니다. 시스템 기본 연결 시간 제한 값을 사용하려면 이 필드를 비워두십시오.
MID 선택	다음 옵션 중 하나를 지정하는 옵션입니다. ▪ MID 서버 자동 선택: 클러스터의 구성원인지 여부에 관계없이 MID 서버 기준에 따라 MID 서버에서 선택합니다. ▪ 특정 MID 서버: MID 서버를 수동으로 선택합니다. ▪ 특정 MID 클러스터: 다른 MID 서버에 대한 자동 재할당은 지정된 클러스터의 구성원에서만 선택합니다. **중요사항:** 선택한 MID 서버가 CyberArk 볼트에 액세스하도록 구성된 CyberArk AIM 클라이언트와 동일한 컴퓨터에 있는지 확인합니다. CyberArk 저장소 구성 및 AIM API 설치 문서를 참조하십시오.
역량	하나 이상의 MID 서버 역량을 선택하는 옵션입니다. 기능은 IP 주소 범위 내에서 MID 서버의 특정 기능을 정의하며, 애플리케이션이 가장 적합한 MID 서버를 선택할 수 있도록 합니다. MID 기능 아이콘( )을 선택하여 하나 이상의 기능을 선택합니다. **주:** ▪ 선택한 MID 서버가 CyberArk 볼트에 액세스하도록 구성된 CyberArk AIM 클라이언트와 동일한 컴퓨터에 있는지 확인합니다. CyberArk 저장소 구성 및 AIM API 설치 문서를 참조하십시오. ▪ 이 옵션은 MID 선택 필드에서 **MID 서버 자동 선택**을 선택한 경우 나타납니다.
MID 서버	MID 서버를 수동으로 선택합니다. 이 옵션은 MID 선택 필드에서 특정 MID 서버를 선택한 경우 나타납니다.
MID 클러스터	MID 클러스터를 수동으로 선택합니다. 이 옵션은 MID 선택 필드에서 특정 MID 클러스터를 선택하는 경우 나타납니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

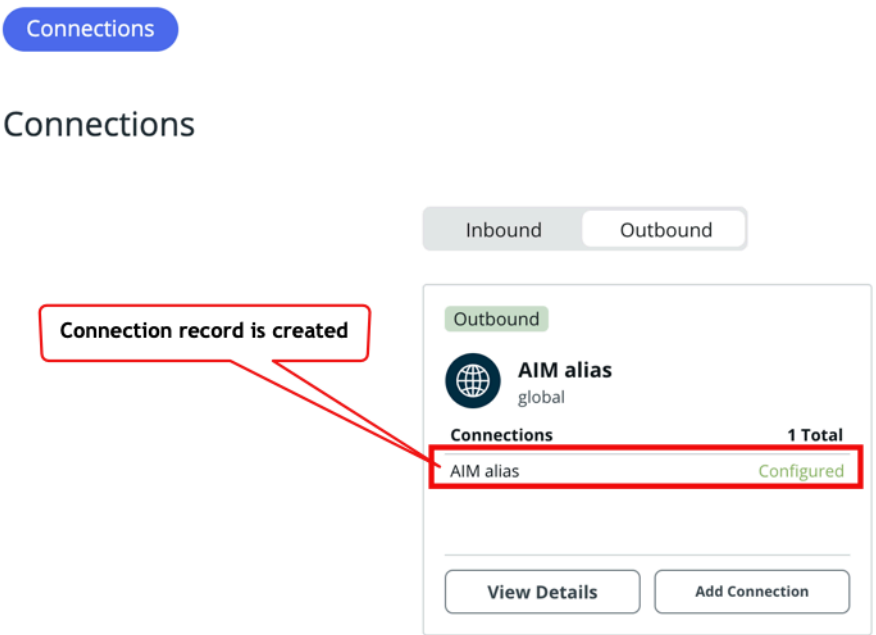
필드	설명
MID 애플리케이션	MID 애플리케이션을 지정하거나 기본 애플리케이션 선택을 수락하는 옵션입니다. 주: 이 옵션은 MID 선택 필드에서 **MID** 서버 자동 선택을 선택한 경우 나타납니다. 기본적으로 **ALL** 옵션이 선택되어 있습니다.

r. 제출을 선택합니다.
HTTP 연결 기록을 생성했습니다.

s. 다음으로 이동 모두 > 프로세스 자동화 > 통합 허브 > 연결 대시보드.

t. 모든 연결 검색 필드에 생성한 연결 기록의 이름을 입력합니다.
연결 별칭 기록이 나타납니다.

OAuth 2.0 연결 기록이 생성됨



인증 알고리즘

인증 알고리즘을 사용하여 보낸 사람의 신원 확인

복잡하거나 비표준 연결 또는 자격 증명 메커니즘이 필요한 웹 서비스를 인증하기 위한 통합 단계를 허용합니다. 인증 알고리즘을 자격 증명 및 연결 별칭에 연결하면 통합 단계를 수동으로 구성할 필요성을 줄이거나 없앨 수 있습니다.

인증 알고리즘을 사용하여 통합 단계에 대한 사용자 지정 인증 데이터를 생성할 수 있습니다. 통합 단계에서는 이 동적 데이터를 사용하여 대상 웹 서비스로 인증하는 데 필요한 사용자 지정 아티팩트를 만들 수 있습니다. 예를 들어 REST 단계에서는 인증 헤더, 쿼리 매개변수 또는 토큰을 만들 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

인증 알고리즘은 다음 단계를 지원합니다.

- 연결 정보 가져오기 단계
- REST(Representational State Transfer) 단계
- SOAP 단계

자세한 내용은 통합 단계를 참조하십시오.

인증 알고리즘 유형

- **Amazon** 서명 버전 **4**: Amazon Web Services에 연결하기 위한 사전 구축된 인증 알고리즘입니다.
- 사용자 지정 인증: 개발자가 자체 인증 알고리즘을 만드는 데 사용할 수 있는 템플릿입니다.

인증 알고리즘을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오 인증 알고리즘을 구성합니다..

스크립트

인스턴스 인증 스크립트는 인스턴스 스크립트의 테이블에 있습니다 *sys_script_include*.

인스턴스 인증 스크립트

RequestAuthInternal	아웃바운드 요청과 함께 전송되는 AWS V4 서명 또는 사용자 지정 인증 생성을 지원하는 인스턴스의 읽기 전용 스크립트입니다.
RequestAuthAWSV4Signer	AWS V4 서명을 생성하기 위해 서명자를 구현하도록 RequestAuthInternal을 확장하는 스크립트입니다.
RequestAuthTwitterSigner	OAuth 1.0a를 사용하여 Twitter 서명을 생성하는 서명자를 구현하도록 RequestAuthInternal을 확장하는 스크립트입니다.
RequestAuthSampleCustomSigner	인스턴스에 사용자 지정 서명자를 작성하는 방법을 이해하기 위해 RequestAuthInternal을 확장하는 샘플 스크립트입니다.

MID 인증 스크립트는 테이블의 MID 스크립트 부분에 *ecc_agent_script_include* 있습니다.

MID 인증 스크립트

RequestAuthInternal	아웃바운드 요청과 함께 전송되는 AWS V4 서명 또는 사용자 지정 인증 생성을 지원하는 MID의 읽기 전용 스크립트입니다.
RequestAuthAWSV4MID시그너	AWS V4 서명을 생성하기 위해 서명자를 구현하도록 RequestAuthInternal을 확장하는 스크립트입니다.
RequestAuthTwitterSigner	OAuth 1.0a를 사용하여 Twitter 서명을 생성하는 서명자를 구현하도록 RequestAuthInternal을 확장하는 스크립트입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

MID 인증 스크립트

RequestAuthSampleMidCustomSigner	MID에서 사용자 지정 서명자를 작성하는 방법을 이해하기 위해 RequestAuthInternal을 확장하는 샘플 스크립트입니다.

JavaScript API의

다음은 인증 알고리즘을 위한 JavaScript API입니다.

- AuthCredential
- HttpRequestAuthed데이터
- HttpRequestData
- 요청AuthAPI

인증 알고리즘을 구성합니다.

아웃바운드 HTTP 요청에 서명할 수 있도록 인증 알고리즘을 구성합니다.

시작하기 전에

인증 알고리즘을 구성하기 전에 스크립트 포함을 구성해야 합니다.
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 자격 증명 및 연결 > 인증 알고리즘를 클릭하고 새로 만들기를 클릭합니다.
2. 양식의 필드에 내용을 입력합니다.
   형식 필드의 데이터베이스 선택에 따라 사용 가능한 필드가 결정됩니다.

   인증 양식

필드	설명
이름	이 알고리즘의 고유한 이름입니다.
알고리즘	아웃바운드 요청 유형입니다.
설명	알고리즘이 수행하는 작업에 대한 설명입니다.
애플리케이션	애플리케이션이 실행되는 범위입니다.
인스턴스 인증 스크립트	스크립트 포함 테이블에서 선택하는 스크립트입니다.
MID 인증 스크립트	MID 서버 스크립트 포함 [검색 뷰] 테이블에서 선택하는 스크립트입니다.

3. 제출을 클릭합니다.

Amazon 서명 기반 사용자 지정 알고리즘 구성

Amazon 스크립트를 실행하여 웹 서비스에 인증하는 데 필요한 서명 기반 데이터를 생성합니다.

시작하기 전에

- JavaScript 지식
- REST 지식

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 대상 웹 서비스 API 지식
- 연결, 자격 증명 및 별칭 지식
- 필요한 역할: 개발자

이 태스크 정보

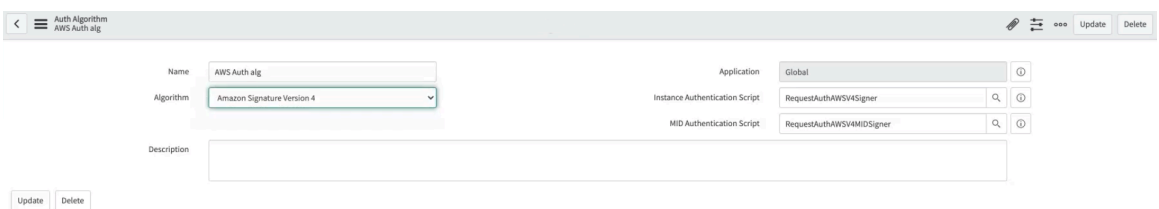
인증에 연결 및 자격 증명 별칭과 Amazon 서명 버전 4 기반 알고리즘을 사용합니다.

프로시저

1. 다음으로 이동 모두 > 자격 증명 및 연결 > 인증 알고리즘를 클릭하고 새로 만들기를 클릭합니다.
2. 양식의 필드에 내용을 입력합니다.
   형식 필드의 데이터베이스 선택에 따라 사용 가능한 필드가 결정됩니다.

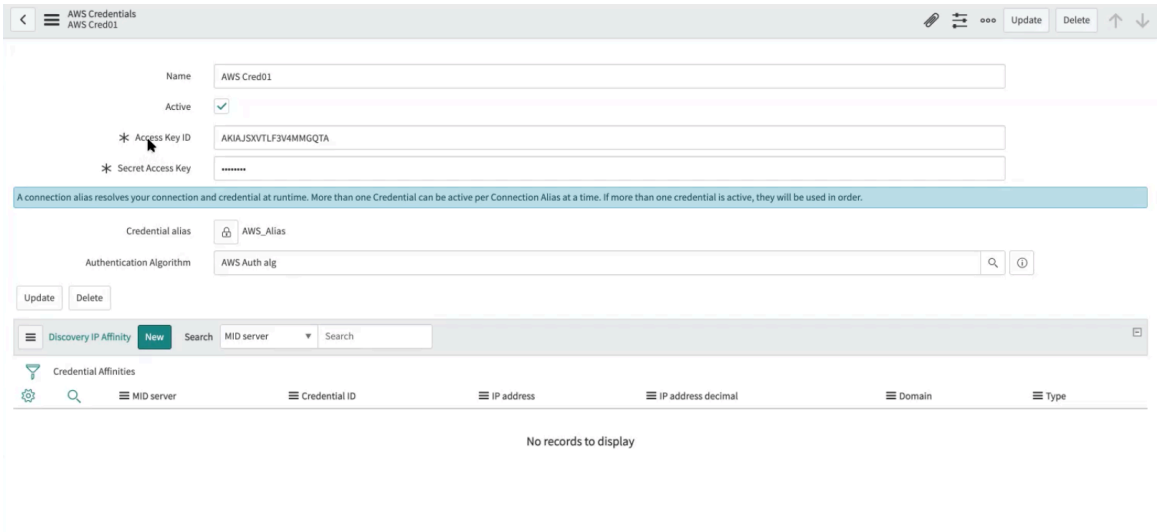
인증 양식

필드	설명
이름	이 알고리즘의 고유한 이름입니다.
알고리즘	아웃바운드 요청 유형입니다. **Amazon** 서명 버전 **4**를 선택합니다.
설명	알고리즘이 수행하는 작업에 대한 설명입니다.
애플리케이션	애플리케이션이 실행되는 범위입니다.
인스턴스 인증 스크립트	스크립트 포함 테이블에서 선택하는 스크립트입니다. **Amazon** 서명 버전 **4** 알고리즘의 경우 **[RequestAuthAWSV4Signer]**를 선택합니다. 사용 가능한 스크립트는 다음과 같습니다. ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner 주: 스크립트에 대한 자세한 내용을 보려면 필드 옆에 있는 정보 아이콘을 클릭하십시오. 이름, API 이름, 애플리케이션, 다음에서 접근 가능, 스크립트 등과 같은 스크립트의 상세 정보가 표시됩니다.
MID 인증 스크립트	MID 서버 스크립트 포함 [검색 뷰] 테이블에서 선택하는 스크립트입니다. 사용 가능한 스크립트는 다음과 같습니다. ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 업데이트를 클릭합니다.
4. 다음으로 이동 모두 > 연결 및 자격 증명 > 자격 증명.
5. 새로 만들기를 클릭합니다.
6. 인증 알고리즘을 사용하여 자격 증명을 생성합니다 AWS .
   이 경우 **AWS Auth alg**입니다.
7. 다음을 지정합니다.
   - 이름
   - 활성
   - 접근 키 ID
   - 비밀 접근 키
   - 자격 증명 별칭
   - 인증 알고리즘



8. 업데이트를 클릭합니다.

결과
선택한 스크립트 및 인증 알고리즘을 기반으로 구성된 자격 증명(액세스 키 **ID** 및 비밀 액세스 키) 또는 사용자의 자격 증명(액세스 키 **ID**, 비밀 액세스 키 및 세션 토큰)은 제공자(ServiceNow이 경우AWS)에게 아웃바운드 요청으로 전송되는 V4 서명을 생성합니다Amazon.

Example: AWS를 사용한 **REST** 단계

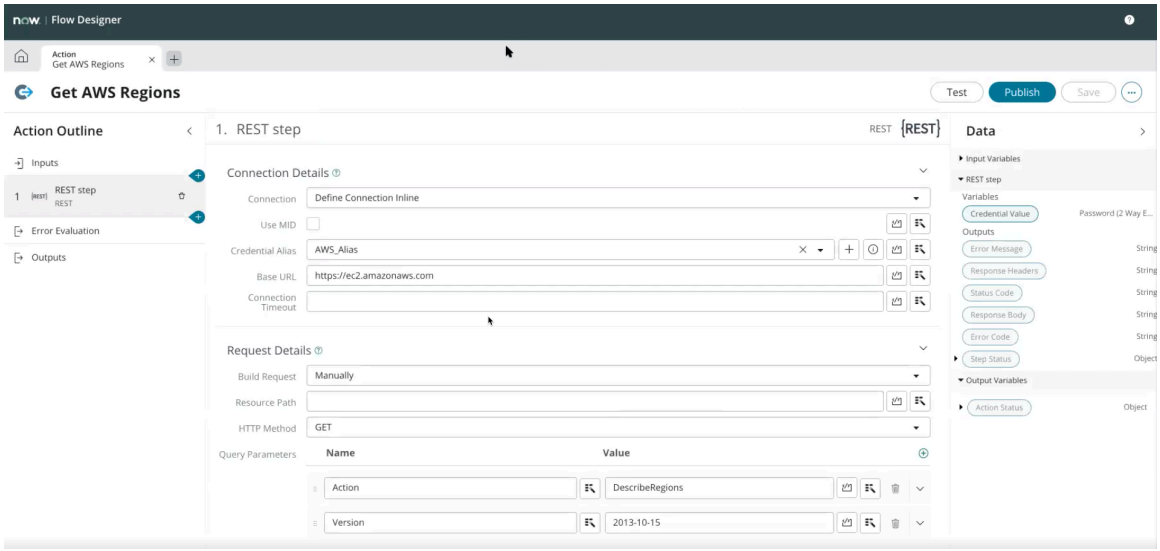
주: Amazon V4 서명 기반 인증은 스크립트 백그라운드에서도 사용할 수 있습니다.

작업: 지역 가져오기 AWS

다음과 같이 REST 단계를 입력합니다.AWS

- 자격 증명 별칭: 에 대해 AWS작성된 별칭입니다.
- 기본 **URL**: 의 AWS기본 URL 상세 정보입니다.
- **HTTPS** 메서드: 이 경우 GET 메서드입니다.
- 쿼리 파라미터: **DescribeRegions**로 작업합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



작업을 테스트할 수 있으며 연결된 지역이 표시됩니다. 응답 본문은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



Amazon V4는 인증 메커니즘을 지원하는 표준 알고리즘 세트로 정의됩니다. 이 알고리즘을 사용하면 REST 단계를 사용하여 인증(HTTP 요청)에 대한 권한 부여 헤더로 서명을 추가합니다.

사용자 지정 인증 알고리즘 구성

스크립트를 실행하여 웹 서비스에 인증하는 데 필요한 사용자 지정 데이터를 생성합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

시작하기 전에

- JavaScript 지식
- REST 지식
- 대상 웹 서비스 API 지식
- 연결, 자격 증명 및 별칭 지식
- 필요한 역할: 개발자

이 태스크 정보

인증에 연결 및 자격 증명 별칭과 사용자 지정 인증 기반 알고리즘을 사용합니다.

프로시저

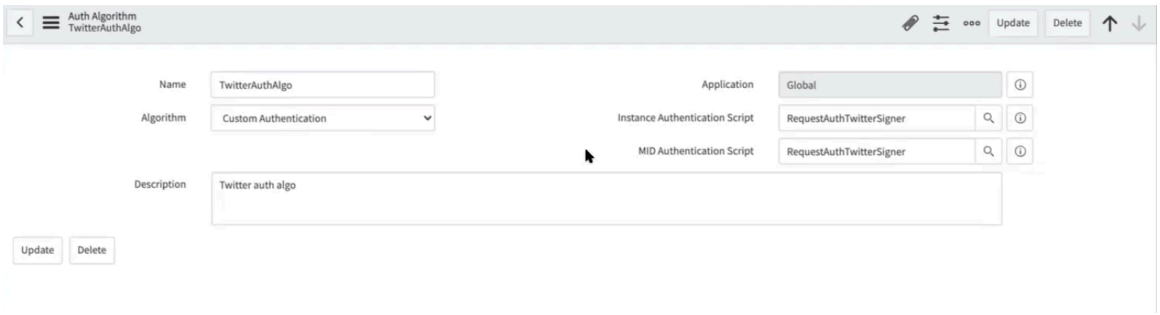
1. 다음으로 이동 모두 > 자격 증명 및 연결 > 인증 알고리즘를 클릭하고 새로 만들기를 클릭합니다.
2. 양식의 필드에 내용을 입력합니다.
   형식 필드의 데이터베이스 선택에 따라 사용 가능한 필드가 결정됩니다.

인증 양식

필드	설명
이름	이 알고리즘의 고유한 이름입니다.
알고리즘	아웃바운드 요청 유형입니다. 사용자 지정 인증을 선택합니다.
설명	알고리즘이 수행하는 작업에 대한 설명입니다.
애플리케이션	애플리케이션이 실행되는 범위입니다.
인스턴스 인증 스크립트	스크립트 포함 테이블에서 선택하는 스크립트입니다. 사용 가능한 스크립트는 다음과 같습니다. ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal ◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner **주:** ◦ 스크립트에 대한 자세한 내용을 보려면 필드 옆에 있는 정보 아이콘을 클릭하십시오. 이름, API 이름, 애플리케이션, 다음에서 접근 가능, 스크립트 등과 같은 스크립트의 상세 정보가 표시됩니다. ◦ Twitter를 사용한 사용자 지정 인증의 경우 OAuth 1.0a 인증 방법을 사용하므로 **RequestAuthTwitterSigner**를 선택할 수 있습니다. 이를 위해서는 권한 부여 헤더에 전달할 서명을 만드는 데 사용할 수 있는 **API** 키 및 비밀 , 액세스 토큰 및 비밀 과 같은 정보가 필요합니다. 자세한 내용은 Twitter의 인증을 참조하세요.
MID 인증 스크립트	MID 서버 스크립트 포함 [검색 뷰] 테이블에서 선택하는 스크립트입니다. 사용 가능한 스크립트는 다음과 같습니다. ◦ RequestAuthAWSV4Signer ◦ RequestAuthInternal

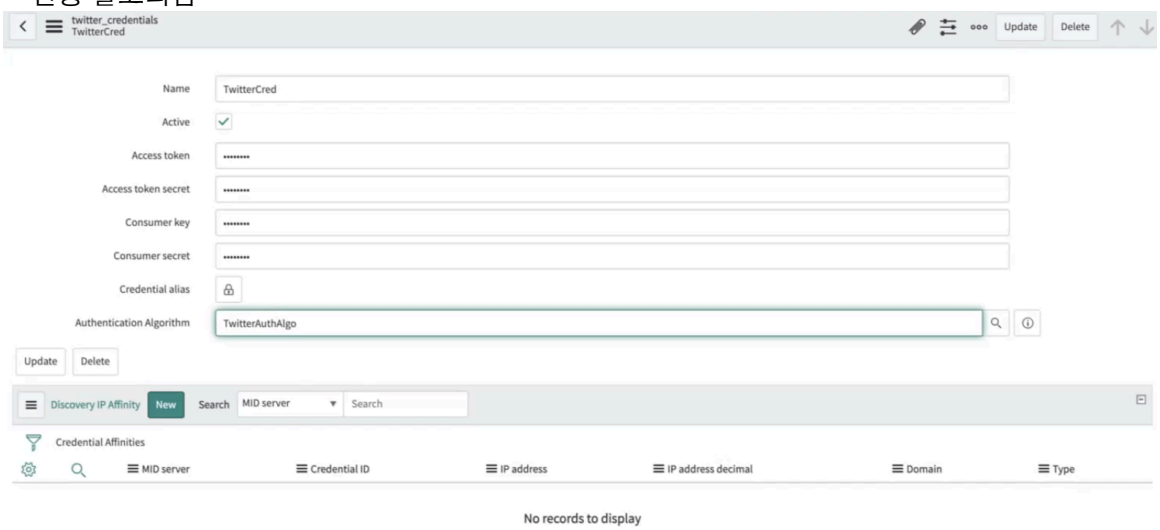
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	◦ RequestAuthSampleCustomSigner ◦ RequestAuthTwitterSigner



선택한 스크립트와 인증 알고리즘에 따라 구성된 자격 증명이 제공자의 ServiceNow 아웃바운드 요청으로 전송됩니다.

3. 업데이트를 클릭합니다.
4. 다음으로 이동 모두 > 연결 및 자격 증명 > 자격 증명.
5. 새로 만들기를 클릭합니다.
6. 인증 알고리즘을 사용하여 자격 증명을 생성합니다 Twitter .
   이 경우 **TwitterAuthAlgo**입니다.
7. 다음 필드를 지정합니다.
   - 이름
   - 활성
   - 접근 토큰
   - 접근 토큰 비밀
   - 소비자 키
   - 소비자 비밀
   - 자격 증명 별칭
   - 인증 알고리즘



8. 업데이트를 클릭합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Example: REST 단계 Twitter

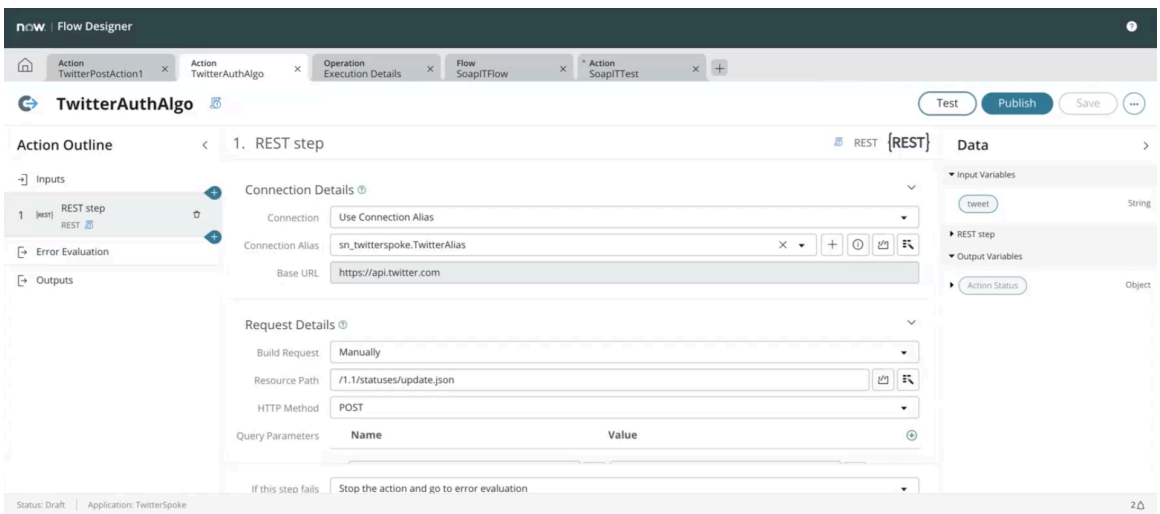
의 Twitter경우 다음 스포크 또는 자격 증명을 사용할 수 있는지 확인해야 합니다.

- 접근 토큰
- 접근 토큰 비밀
- 소비자 키
- 소비자 비밀
- 인증 알고리즘

작업: TwitterAuthAlgo.

다음과 같이 REST 단계를 입력합니다.Twitter

- 자격 증명 별칭: 에 대해 Twitter작성된 별칭입니다.
- 기본 **URL**: 의 Twitter기본 URL 상세 정보입니다.
- **HTTPS** 방법: 이 경우 POST 방법입니다. 트윗 게시.
- 쿼리 매개변수: 트윗으로 작업합니다.



작업을 테스트할 수 있습니다. 트윗이 페이지에 게시 Twitter 됩니다.

검색 및 오케스트레이션의 IP 서비스 동질 관계 검사

IP 서비스 테이블에서 프로토콜과 관련된 IP 주소 목록을 확인할 수 있습니다.

시작하기 전에
필요한 역할: 관리자

이 태스크 정보
IP 서비스 테이블은 프로토콜에 포트를 매핑합니다. HTTP용 포트 80, SSH용 포트 22 및 SNMP용 포트 161과 같이 일반적으로 사용되는 포트-프로토콜 조합에는 몇 가지 매핑이 기본적으로 제공됩니다. 디스커버리는 *glide.discovery.ip_service_affinity*라는 시스템 속성을 사용하여 검색된 IP 주소의 마지막 포트를 기억할 수 있습니다. 이 속성은 기본적으로 **false**로 설정됩니다.

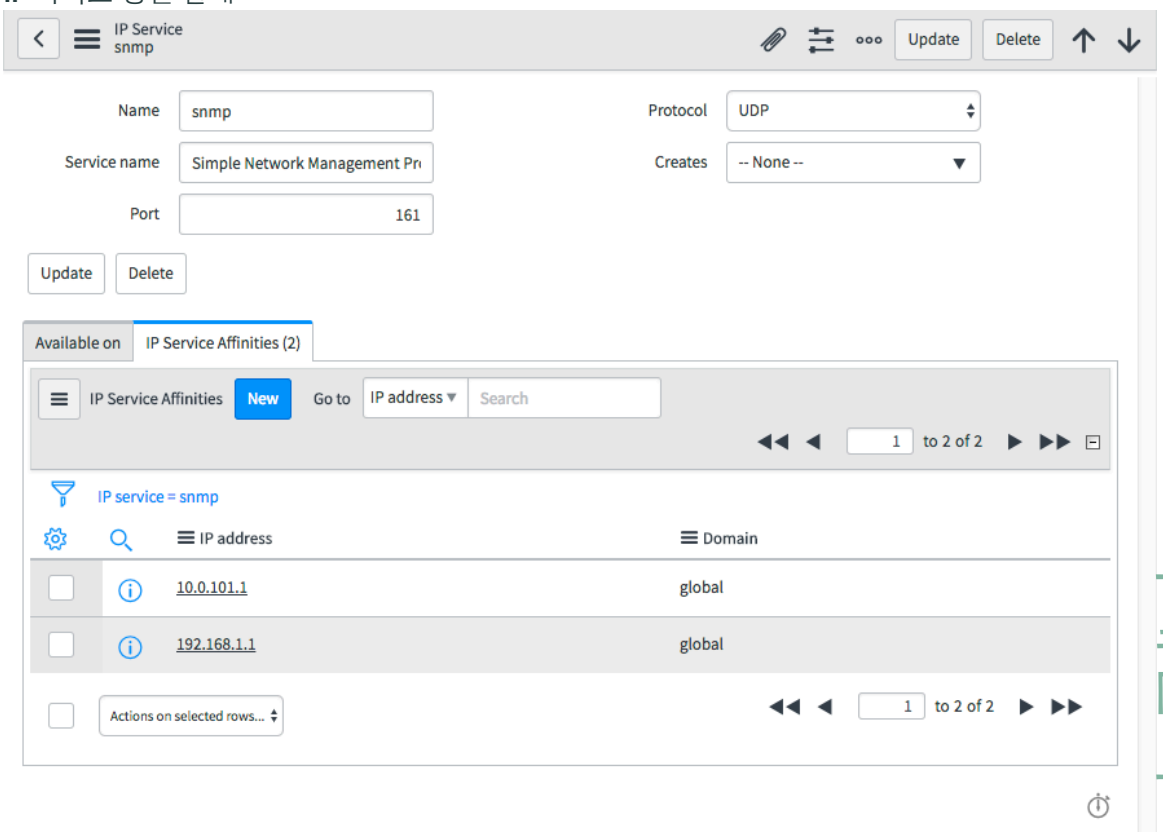
중요사항: 조직에서 사용자 지정 포트를 사용하는 경우를 제외하고는 IP 서비스를 수정하지 않아야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 디스커버리 정의 > **IP** 서비스.
2. 목록을 필터링하여 적절한 IP 서비스를 찾습니다.
3. 서비스 이름을 클릭하여 해당 IP 서비스 페이지로 이동합니다.
4. 해당 서비스와 연결된 IP 주소 목록에 대한 **IP** 서비스 동질 관계 탭을 클릭합니다.

IP 서비스 동질 관계



기계번역

ServiceNow® 접근 제어

SNC 접근 제어 플러그인(com.snc.snc_access_control)을 사용하면 인스턴스에 액세스할 수 있는 고객 서비스 및 지원 직원과 시기를 제어할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow 접근 제어 살펴보기



접근 제어의 ServiceNow® 기능에 대해 알아봅니다.

ServiceNow 액세스 제어 활성화



활성 ServiceNow® 액세스 제어.

ServiceNow 액세스 제어 구성



접근 제어를 구성하는 ServiceNow® 방법을 이해합니다.

감사 로깅



접근 제어 감사 로깅에 대해 ServiceNow® 알아보고 검토합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 제어 살펴보기 ServiceNow®

SNC 접근 제어 플러그인(com.snc.snc_access_control)을 사용하면 인스턴스에 액세스할 수 있는 고객 서비스 및 지원 직원과 시기를 제어할 수 있습니다.

플러그인을 고객 서비스 및 지원 처음 활성화하면 직원이 인스턴스에 로그인할 수 없습니다. 현재 로그인한 고객 서비스 및 지원 직원은 모두 로그인된 상태로 유지됩니다. SNC 액세스 제어 테이블에서 특정 SNC 직원 또는 모든 직원에게 액세스 권한을 부여하는 기록을 생성합니다.

이 플러그인을 사용하면 고객 서비스 및 지원 사용자가 사용자의 명시적 허가 없이 인스턴스에 액세스할 수 없습니다. 그러나 제품을 지원 및 관리하고 사용 현황을 확인할 수 있는 다른 공인 ServiceNow 운영 담당자가 기본 인프라에서 관리 작업을 수행해야 합니다. 이 인프라에는 SaaS 솔루션을 구성하는 다른 인프라 구성 요소 중에서 서버와 데이터베이스가 포함됩니다. 이 액세스 방법은 완전히 감사 및 추적이 가능합니다.

이 플러그인을 사용하면 명시적 허가 없이 인스턴스에 대한 액세스를 제한할 수 있으므로 지원 서비스 수준 및 가용성 SLA에 영향을 줄 수 있습니다. 그런 다음 가용성 SLA는 지원 담당자가 인스턴스에 대한 액세스 권한을 부여받은 시간부터 측정됩니다.

로그인 보안

인스턴스에 대한 승인된 고객 서비스 및 지원 직원 로그인에 대한 보안은 보안 서버에서 생성된 암호화된 토큰을 사용합니다. 적절하게 인증된 고객 서비스 및 지원 직원에게만 인스턴스에 대한 액세스 권한이 부여됩니다. SNC 액세스 제어 플러그인이 없으면 보안 서버는 액세스 권한이 hi.service-now.com 에 적용되도록 합니다. 플러그인이 활성화되면 암호화된 로그인 토큰은 해당 기록에 정의된 기준을 사용하여 플러그인 제공 액세스 목록의 이름과 일치해야 합니다. 이 인증 방법을 사용하면 인스턴스에 액세스할 수 있는 직원 및 해당 직원이 액세스할 수 있는 시기를 정확하게 고객 서비스 및 지원 결정할 수 있습니다.

이 시스템에 선택된 아키텍처에는 인스턴스의 보안을 강화하기 위해 설계된 몇 가지 기능이 있습니다.

보안 서버

보안 서버는 보안 담당자만 액세스할 수 있는 잠긴 Linux 호스트입니다 ServiceNow . 이 서버는 로그인 토큰을 생성하는 데 필요한 중요한 개인 암호화 키에 액세스할 수 있는 유일한 시스템입니다. 이 구획화(표준 보안 관행)를 사용하면 공격자가 HI 인스턴스를 손상시키는 드문 경우에도 개인 키가 보호됩니다.

합성 사용자

권한 있는 고객 서비스 및 지원 직원이 인스턴스에 로그인할 수 있는 인스턴스의 기능은 해당 인스턴스에서 계정을 프로비저닝할 필요가 없습니다. 프로비저닝된 사용자 기록이 없으며 영구 또는 영구 자격 증명이 없습니다. 대신 각 고객 서비스 및 지원 직원 로그온에 대해 가상 사용자가 만들어집니다. 이 사용자는 메모리에만 존재하며 지속적인 권한을 제공하지 않습니다. SNC 액세스 제어 플러그인이 활성화된 경우 언제든지 직원의 권한을 고객 서비스 및 지원 해제할 수 있습니다.

토큰

보안 토큰은 인스턴스 및 특정 고객 서비스 및 지원 직원에만 해당됩니다. 또한 토큰을 생성하는 메커니즘은 가장된 사용자가 아닌 HI에 대한 실제 고객 서비스 및 지원 직원 로그인에서만 작동합니다. 보안 토큰이 생성되면 특정 고객 서비스 및 지원 직원만 이를 사용하여 인스턴스에 로그인할 수 있습니다.

시간 제한

보안 토큰은 생성된 후 4시간 후에 만료됩니다. 이 만료는 하이재킹된 토큰의 유용성을 제한하며, 이 짧은 기간 동안에만 사용할 수 있습니다.

로깅

직원이 인스턴스에 로그인 고객 서비스 및 지원 하면 로그인 이벤트로 기록됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 로그인한 고객 서비스 및 지원 직원이 수행한 모든 작업은 데이터베이스의 트랜잭션 로그에 추가됩니다.
- 또한 대부분의 ServiceNow 직원이 액세스할 수 없는 파일 시스템의 인스턴스 로그에도 추가됩니다.
- 고객 서비스 및 지원 사용자 이름이 모두 @snc(예: frodo.baggins@snc)으로 끝나므로 직원 로그인 및 작업을 쉽게 식별할 수 있습니다.

이러한 작업은 비직원의 액세스에 대해 사용하기 쉽고 강력하며 신뢰할 수 있는 보안 로깅을 제공합니다.

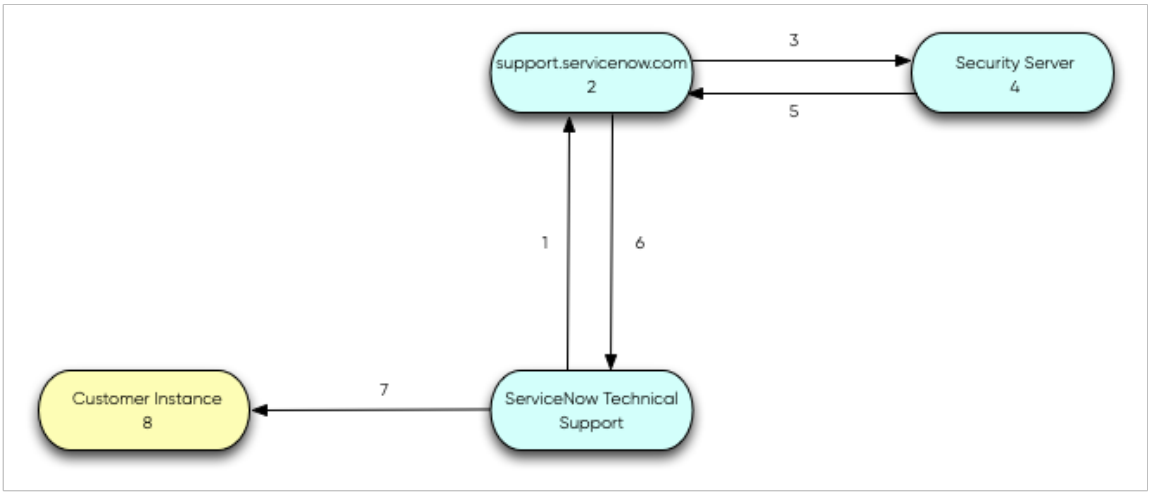
보안 처리 플로우

고객 서비스 및 지원 직원이 인스턴스에 로그인하려는 경우, 보안 처리 플로우는 다음과 같습니다.

1. 기술자는 고객 서비스 및 지원 hi.service-now.com 를 통해 인스턴스에 대한 로그인을 요청합니다.
2. HI는 기술자에게 인스턴스에 대한 액세스 권한을 부여하는 적절한 역할이 있는지 확인합니다.
3. 사용자에게 적절한 역할이 있는 경우 HI는 보안 서버에 대한 접근 요청을 보냅니다.
4. 보안 서버는 요청이 HI IP 주소에서 왔는지 확인하고 요청(요청자의 사용자, 역할 및 IP 주소)을 평가합니다. 요청이 유효하면 보안 서버가 이를 승인하고 토큰을 구성합니다. 이 토큰에는 사용자 이름, 역할, 인스턴스 ID 및 시간(4시간의 토큰 수명 시작)이 포함됩니다. 마지막으로 보안 서버는 개인 암호화 키를 사용하여 토큰을 암호화합니다.
5. 보안 서버는 암호화된 토큰을 HI로 보냅니다.
6. Hi는 토큰을 지원 기술자의 브라우저로 보냅니다.
7. 지원 기술자의 브라우저가 `@snc`로 끝나는 특수 사용자 이름을 사용하여 인스턴스에 로그인을 시작합니다.
8. 인스턴스는 공개 키를 사용하여 토큰을 해독합니다. 토큰을 확인하기 위해 인스턴스는 토큰을 이전 단계에서 제공된 사용자 이름, 인스턴스 ID 및 승인된 기간과 일치시킵니다. SNC 액세스 제어 플러그인이 활성화된 경우 인스턴스는 사용자가 다음 중 어떤 사람인지 확인합니다.
   - 나열됨
   - 활성
   - 현재 시간대의 인스턴스에 액세스하도록 구성
9. 사용자가 인증되면 인스턴스는 지정된 역할로 메모리에 합성 사용자를 생성합니다. 이 사용자는 시간 제한이 만료되거나, 사용자가 로그오프하거나, 인스턴스가 다시 시작된 후에도 유지되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ServiceNow 보안 접근 프로세스 흐름



감사 로깅

다음 로깅은 직원의 로그인 및 활동을 고객 서비스 및 지원 추적합니다.

- 이벤트 로그: 이벤트 로그에는 인스턴스에 대한 모든 고객 서비스 및 지원 로그인이 표시됩니다.
- 트랜잭션 로그: 트랜잭션 로그에는 로그 삭제 작업을 포함하여 인스턴스의 모든 활동이 표시됩니다.

주: 이 플러그인에 대한 자세한 내용은 인스턴스 보안 강화 설정을 참조하십시오 ServiceNow 접근 제어 .

접근 통제 활성화 **ServiceNow**®

SNC 접근 제어 플러그인(com.snc.snc_access_control)의 활성화를 요청합니다.

시작하기 전에
필요한 역할: admin

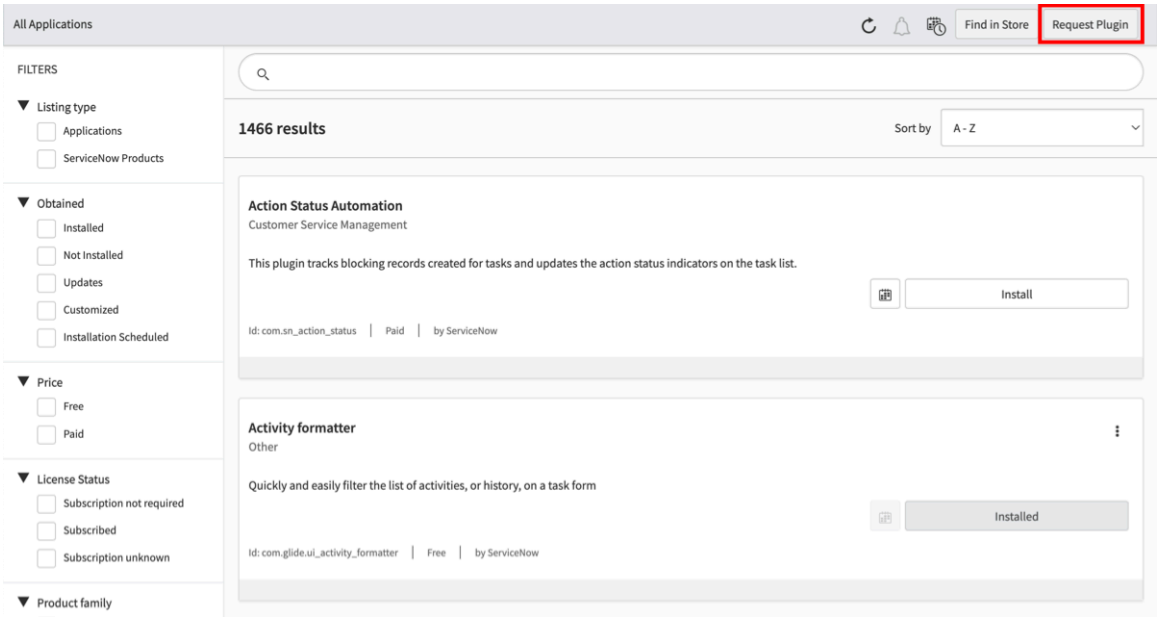
이 태스크 정보
플러그인을 요청하는 방법은 두 가지가 있습니다.

- 을(를) 선택하여 Service Catalog에 Now Support 직접 액세스합니다. 모두 > 서비스 카탈로그 > 플러그인 활성화 에 Now Support.
- 다음 단계에 따라 인스턴스의 모든 애플리케이션 페이지에서 Now Support 서비스 카탈로그에 액세스합니다.

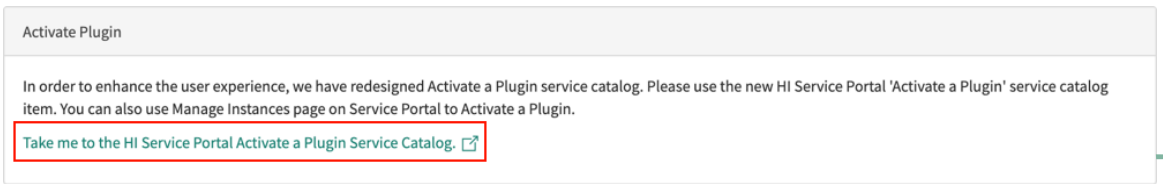
프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 모든 애플리케이션 페이지에서 플러그인 요청을 선택하여 Now Support의 플러그인 활성화 양식을 엽니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. Now Support에서 Now Support 서비스 포털 서비스 카탈로그에 액세스하는 링크를 선택합니다.



4. 인스턴스를 선택합니다.

5. 작업 **>** 플러그인 활성화를 선택합니다.

6. 플러그인 활성화 양식에서 다음 정보를 입력합니다.

플러그인 활성화 양식

필드	설명
대상 인스턴스는 무엇입니까?	플러그인을 활성화할 인스턴스입니다.
어떤 플러그인을 활성화하시겠습니까?	활성화할 플러그인의 이름입니다. 주: 시스템에서 원하는 플러그인을 나열하지 않거나 OEM 또는 온프레미스 인스턴스에서 플러그인을 활성화하는 경우 찾고 있는 플러그인이 목록에 없음 확인란을 선택한 다음 플러그인 이름을 입력합니다.
유지관리 날짜 및 시간 선택	플러그인을 활성화하는 날짜 및 시간입니다.

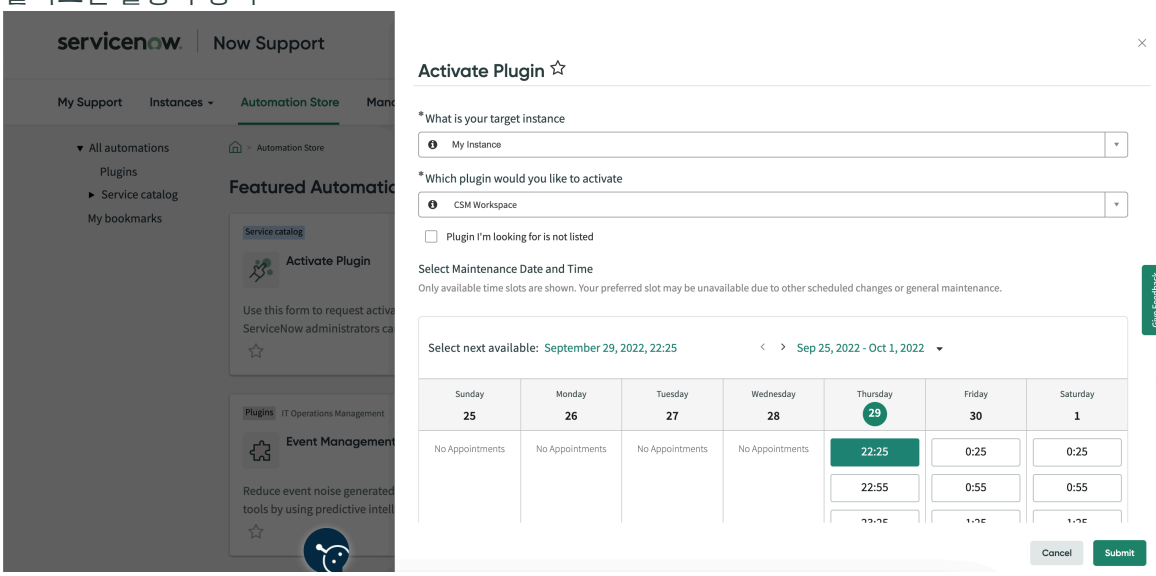
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 플러그인은 미국 태평양 시간대의 모든 영업일에 두 번(오전과 저녁에 각각 한 번씩) 활성화됩니다. 특정 시간에 플러그인을 활성화해야 하는 경우 이유/설명 필드에 요청을 입력합니다.

Example

예를 들어, 내 인스턴스라는 인스턴스에서 CSM Workspace 플러그인을 활성화하는 다음 양식을 참조하십시오.

플러그인 활성화 양식



7. 제출을 선택합니다.
   플러그인 요청에 대한 자세한 내용은 다음을 참조하십시오. 의 서비스 카탈로그 [KB0751715] 문서에서 플러그인 요청 Now Support 지식베이스.

접근 제어 구성 ServiceNow®

인스턴스에 로그인할 권한을 가진 한 명 이상의 고객 서비스 및 지원 직원을 지정하도록 접근 제어 기록을 구성합니다.

시작하기 전에

필요한 역할: 관리자

이 태스크 정보

주: SNC 접근 제어(com.snc.snc_access_control) 플러그인은 사용자가 사용자의 명시적 허가 없이 인스턴스에 액세스하지 못하도록 합니다 고객 서비스 및 지원 . 그러나 제품을 지원하고 관리할 수 있는 다른 승인된 ServiceNow 운영 담당자는 기본 인프라에 대한 관리 작업을 수행해야 합니다. 이 인프라에는 SaaS 솔루션을 구성하는 다른 인프라 구성 요소 중에서 서버와 데이터베이스가 포함됩니다. 이 액세스 방법은 완전히 감사 및 추적이 가능합니다.

이 플러그인을 사용하면 명시적 허가 없이 인스턴스에 대한 액세스를 제한할 수 있으므로 지원 서비스 수준 및 가용성 SLA에 영향을 줄 수 있습니다. 그런 다음 가용성 SLA는 지원 담당자가 인스턴스에 대한 액세스 권한을 부여받은 시간부터 측정됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > **SNC** 접근 통제.
2. 새로 만들기를 클릭합니다.
3. 양식 필드를 입력합니다(표 참조).
4. 제출을 클릭합니다.

SNC 접근 통제

양식 필드	설명
이름	이 인스턴스에 로그인할 수 있는 권한이 있는 각 고객 서비스 및 지원 직원의 이름을 지정합니다. ◦ 이름을 소문자로 이름.성으로 표시하고 마침표로 구분합니다(예: `john.smith`). 각 이름에는 에 해당 사용자 기록이 *support.servicenow.com*있어야 합니다. ◦ 두 고객 서비스 및 지원 명 이상의 직원이 이 인스턴스에 로그인할 수 있는 권한을 가지고 있는 경우, 여러 이름을 입력하고 쉼표로 구분합니다. ◦ 모든 고객 서비스 및 지원 직원 로그인 권한이 인스턴스에 액세스할 수 있도록 하려면 이름 대신 별표() *를 입력합니다. ◦ 인스턴스에 대한 직원 액세스를 제한 고객 서비스 및 지원 하려면 이름 필드의 필드에 별표(*)가 없어야 합니다.
이유	액세스 권한을 부여하는 이유를 설명하는 사람이 읽을 수 있는 필드입니다. 이 필드는 선택 사항입니다.
시작	지정된 고객 서비스 및 지원 직원이 로그인 액세스 권한을 갖는 기간의 시작 날짜 및 시간을 지정합니다. 이 필드는 필수입니다.
종료	지정된 고객 서비스 및 지원 직원이 로그인 액세스 권한을 갖는 기간의 종료 날짜 및 시간을 지정합니다. 이 필드는 필수입니다.
활성	이 권한 기록이 활성 상태인지 여부를 통제합니다. 기본값은 활성입니다.

감사 로깅

다음 로깅은 직원의 로그인 및 활동을 ServiceNow 추적합니다.

이벤트 로그	이벤트 로그에는 고객 인스턴스에 대한 모든 ServiceNow 로그인이 표시됩니다.
트랜잭션 로그	트랜잭션 로그에는 로그 삭제 작업을 포함하여 인스턴스의 모든 활동이 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

신원

인스턴스의 ID에 대해 자세히 알아봅니다.

액세스 분석기



액세스 분석기는 ServiceNow® 액세스 권한 도구인 스토어 앱입니다. 자원에 액세스할 수 있는 사용자를 결정하는 데 도움이 됩니다.

전역 ID



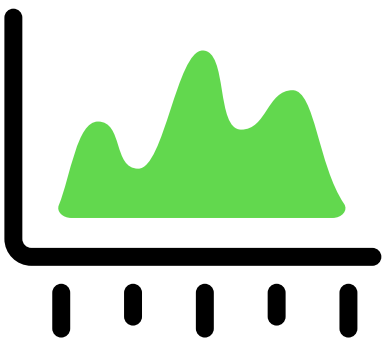
Global Identity는 ServiceNow® 한 인스턴스에서 인스턴스로 (예: 인스턴스) 사용자 속성을 업데이트할 수 있는 스토어 앱입니다.

ID 센터



Identity Center를 사용하면 ID 기반 위험 및 보안 격차를 모니터링, 관리 및 최소화할 수 있습니다.

SCIM(교차 도메인 ID 관리 시스템)



SCIM(System for Cross-domain Identity Management) API는 SCIM 프로토콜을 사용하여 사용자 및 그룹에 대한 작업을 만들고, 읽고, 업데이트하고, 삭제할 수 있는 엔드포인트를 제공합니다.

ID 및 액세스 감사



ID 및 액세스 감사를 사용하여 사용자, 그룹, 역할 및 ACL의 변경 내용을 파악합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

액세스 분석기

ServiceNow® 액세스 분석기는 리소스에 대한 ID 권한을 볼 수 있는 액세스 진단 도구입니다.

탐색



Access Analyzer의 기능 및 비즈니스 가치에 대해 알아봅니다.

사용



Access Analyzer 사용 방법을 이해합니다.

권한 평가



권한이 평가되는 방식을 알고 있습니다.

자주 묻는 질문



기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

액세스 분석기 살펴보기

인스턴스의 ID를 분석합니다 ServiceNow .

ServiceNow 액세스 분석기는 관리자가 선택한 사용자, 역할 또는 그룹에 대한 권한을 볼 수 있는 애플리케이션입니다.

주:

- 액세스 분석기는 ServiceNow 스토어 제품입니다. 사용 가능한 모든 앱을 보고 스토어에 요청을 제출하는 방법을 확인하려면 ServiceNow Store 웹 사이트를 방문하십시오.
- 액세스 분석기는 ID 레코드를 가장하여 사용 권한에 대한 세부 정보를 검색하며 ID의 개인 데이터나 중요한 데이터를 읽거나 저장하지 않습니다.
- 액세스 분석기 평가 결과는 제로 트러스트 액세스(ZTA)와 같이 사용자에 대해 정의된 액세스 정책에 관계없이 동일합니다. 정책은 실제 사용자 로그인 중에만 평가되며 액세스 분석기 플로우 중에는 평가되지 않습니다.
- 액세스 분석기는 관리 범위 자원 및 위임된 개발자와 관련된 자원의 액세스를 정확하게 평가하는 데 제한이 있습니다.

액세스 평가

액세스 평가는 관리자가 선택한 사용자, 역할 또는 그룹에 대한 권한을 볼 수 있도록 도와주는 액세스 분석기의 기능입니다 ServiceNow .

이를 통해 테이블, 클라이언트 호출 가능 스크립트 포함, UI 페이지 및 REST 엔드포인트에 대한 사용자, 그룹, 역할의 권한을 분석하고 볼 수 있습니다.

Access Analyzer를 사용하여 조직은 보안 태세, ID 거버넌스, 위험 관리를 개선하고, 규정 준수 목표를 달성하고, 누가(ID) 무엇(리소스)에 액세스할 수 있는지 파악할 수 있습니다.

액세스 비교

액세스 비교는 관리자가 사용자 액세스를 비교하고 인스턴스의 사용자에 ServiceNow 대한 적절한 액세스 수준을 결정할 수 있는 액세스 분석기 V2의 기능입니다ServiceNow.

사용자 기록 및 접근 제어를 위해 사용자 간에 접근을 비교할 수 있습니다.

Access 비교를 사용하여 다음 분석을 수행할 수 있습니다.

- 수준 1: 사용자 기록을 비교하여 속성, 역할 및 그룹을 이해합니다.
- 수준 2: 접근 제어를 비교하여 접근 문제를 찾아 근본 원인 분석을 실행합니다.

복지

다음은 Access Analyzer를 사용할 때의 몇 가지 이점입니다.

- 자원(테이블)에 대한 액세스를 분석합니다.
- 사용자 2명의 액세스를 비교합니다.
- 사용자 2명의 역할과 그룹을 비교합니다.
- ID가 자원(테이블)에 액세스할 수 있는지 여부를 보여주는 보고서를 생성합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 중요한 보안 예방 조치에 대한 액세스 권한이 있는 사용자를 파악합니다.
- 과도한 권한 프로비저닝을 방지하는 데 도움이 됩니다.
- 접근 제어를 구현할 때 최소 권한 원칙을 달성합니다.
- 애플리케이션, 테이블, 행 또는 열, 기타 자원을 포함하는 특정 데이터에 대한 액세스를 제한합니다.
- 분석기 결과에 대한 보고 기능을 제공합니다.
- 사용자 기록과 액세스 제어 간의 액세스를 비교합니다.
- 인스턴스의 사용자에게 ServiceNow 적절한 액세스 수준을 결정합니다.

액세스 분석기 사용

ID와 인스턴스에 대한 액세스를 분석합니다 ServiceNow® .

시작하기 전에

필요한 역할: admin, AA_admin

다음 절차에서는 Access Analyzer에 액세스하고 Access Analyzer 내의 다양한 기능을 사용하는 단계를 설명합니다.

주: 액세스 분석기는 ServiceNow® 스토어 제품입니다.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.

   액세스 분석기에는 다음과 같은 기능이 있습니다.

   - 액세스 평가
   - 사용자 기록 비교
   - 접근 제어 비교

2. 요구 사항에 따라 Access Analyzer를 사용하려면 해당 탭을 선택합니다.

액세스 평가 사용

인스턴스의 ID를 분석합니다 ServiceNow® .

시작하기 전에

필요한 역할: admin, AA_admin

다음 절차에서는 액세스 분석기에서 액세스 평가에 액세스하고 다양한 기능을 사용하는 단계를 설명합니다.

주: 액세스 분석기는 ServiceNow Store 제품입니다.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.
2. 액세스 평가 탭을 선택합니다.
3. 다음과 같이 기준을 선택합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

액세스 및 권한을 분석하기 위한 기준을 선택합니다.

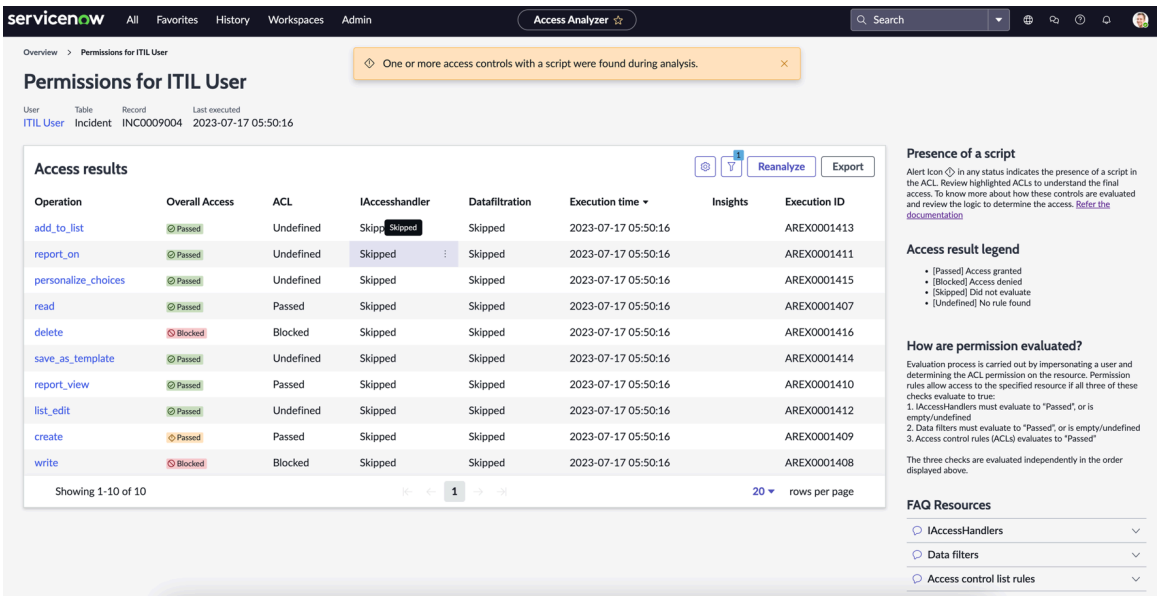
필드	설명
분석 단위 *	사용자, 역할 또는 그룹에 대한 액세스 분석
사용자 선택 *	목록에서 선택할 사용자 이름을 지정합니다.
규칙 유형 *	테이블, UI 페이지, REST 엔드포인트 또는 클라이언트 호출 가능 스크립트 포함에 대한 액세스를 분석합니다.
테이블 선택 *	목록에서 선택할 테이블 이름을 지정합니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다.
필드 선택	목록에서 선택할 필드 이름을 지정합니다.

4. 설명 필드에 설명을 지정합니다.
5. 권한 분석을 선택합니다.

사용자에 대한 액세스 결과가 표시됩니다. 마찬가지로 다음 규칙 유형에 대한 그룹 또는 역할의 권한을 분석할 수 있습니다.

- 테이블(기록)
- 클라이언트 호출 가능 스크립트에는 다음이 포함됩니다.
- REST 엔드포인트

액세스 결과가 표시됩니다.



액세스 결과 테이블에는 다음 필드가 포함됩니다.

액세스 결과

필드	설명
운영	사용자, 그룹 또는 역할이 선택한 테이블, 기록 또는 필드에 대해 수행할 수 있는 작업의 유형입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
전체 액세스	전체 액세스의 결과입니다. 결과는 다음과 같습니다. ◦〔통과됨〕 액세스 권한 부여됨 ◦〔차단됨〕 접근 거부됨 ◦〔건너뜀〕 평가하지 않음 ◦〔정의되지 않음〕 규칙을 찾을 수 없음
ACL	선택한 작업에 대해 ACL이 정의되어 있는지 여부입니다.
액세스 핸들러	플랫폼에서 숨겨진 소스 코드를 사용하는 내부 시스템 검사입니다. IAccessHandler는 ACL을 평가하지 않고 리소스에 대한 액세스 권한을 부여하거나 거부할 수 있습니다. IAccessHandler를 무시하면 ACL이 평가됩니다.
데이터 필터링	데이터 필터는 인스턴스의 기존 접근 통제 규칙(ACL)과 함께 작동하도록 설계된 접근 제어의 한 형태입니다.
실행 시간	액세스 결과가 실행된 시간입니다.
인사이트	선택한 운영에 대한 자세한 정보입니다.
실행 ID	각 액세스 결과 실행에 대한 고유 ID입니다.

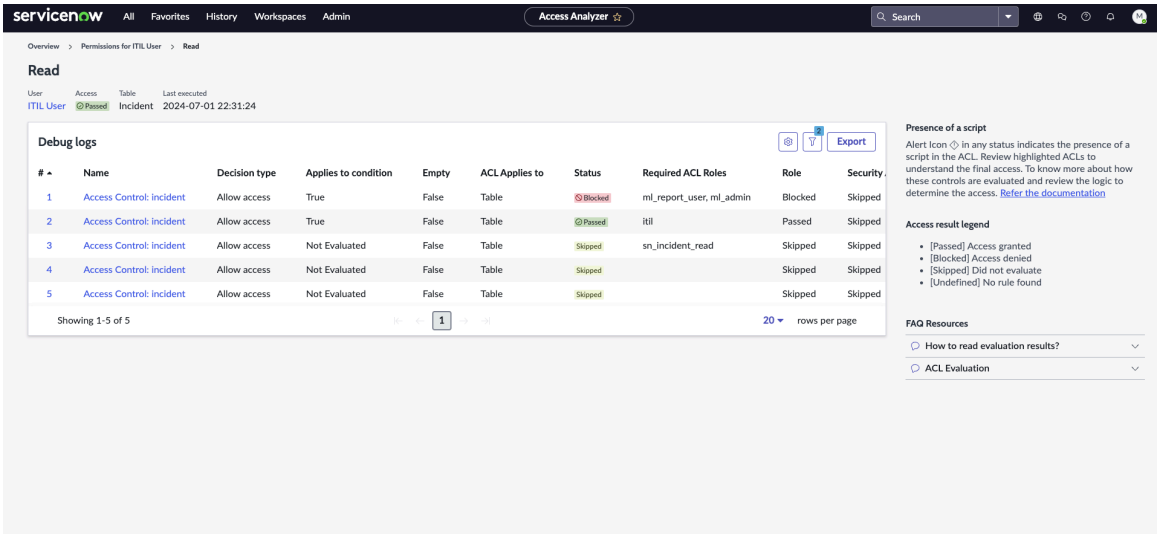
6. ACL에 대한 자세한 내용을 보려면 작업을 선택합니다.
예를 들어 읽기를 선택하면 읽기와 관련된 접근 제어가 표시됩니다.

ACL 상세 정보

필드	설명
이름	ACL의 이름입니다.
결정 유형	ACL에 대해 구성된 결정 유형입니다. 접근 허용 또는 접근 거부
조건에 적용	ACL이 조건에 적용되는지 여부입니다.
ACL 적용 대상	ACL이 적용되는 자원에 대한 상세 정보입니다.
상태	ACL 또는 액세스 결과의 상태입니다.
필수 ACL 역할	자원에 액세스하는 데 필요한 역할의 상세 정보입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
역할	역할의 상태입니다. 통과, 건너뜀 또는 차단되었습니다.



사용자의 권한 보기

액세스 분석기를 사용하여 선택한 사용자의 권한을 봅니다.

시작하기 전에

필요한 역할: admin, AA_admin

다음 절차에서는 선택한 사용자(**ITIL** 사용자)가 액세스 분석기의 액세스 평가를 사용하여 인시던트 테이블의 권한을 볼 수 있는 권한을 보는 샘플 단계를 설명합니다.

주: 액세스 분석기는 ServiceNow® 스토어 제품입니다.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.
2. 다음과 같이 기준을 선택합니다.

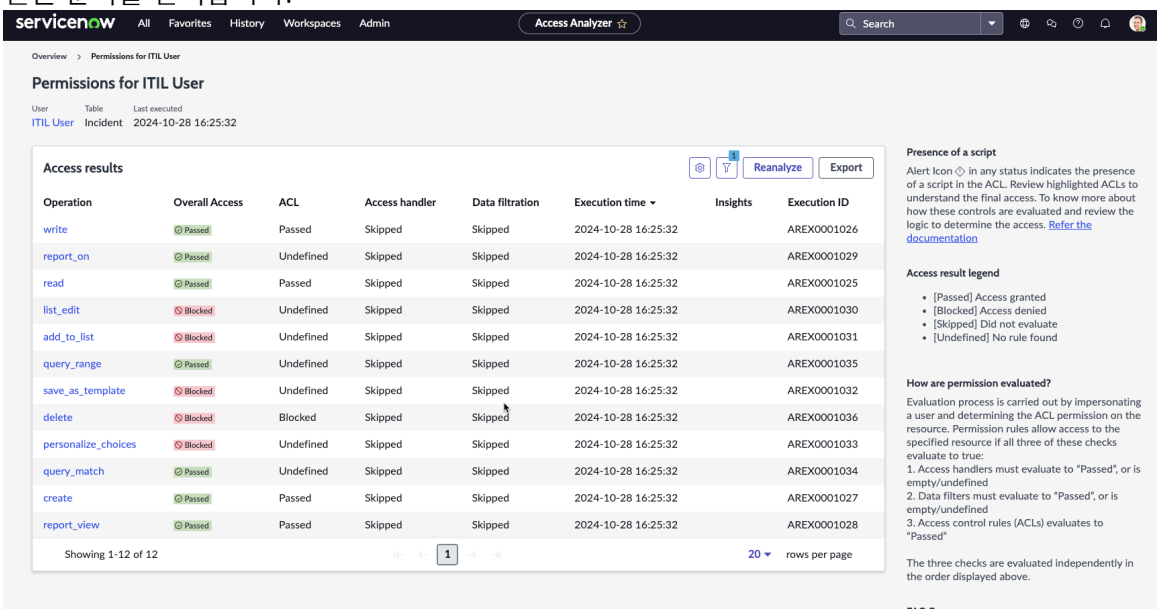
액세스 및 권한을 분석하기 위한 기준을 선택합니다.

필드	설명
분석 단위 *	사용자를 선택합니다.
사용자 선택 *	목록에서 선택할 사용자 이름을 지정합니다. 이 예에서는 **ITIL** 사용자입니다.
규칙 유형 *	테이블, **UI** 페이지, **REST** 엔드포인트 또는 클라이언트 호출 가능 스크립트 포함에 대한 액세스를 분석합니다. 이 예에서는 ###입니다.
테이블 선택 *	목록에서 선택할 테이블 이름을 지정합니다. 이 예시에서는 인시던트입니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다. 이 예에서는 **INC0000001**.

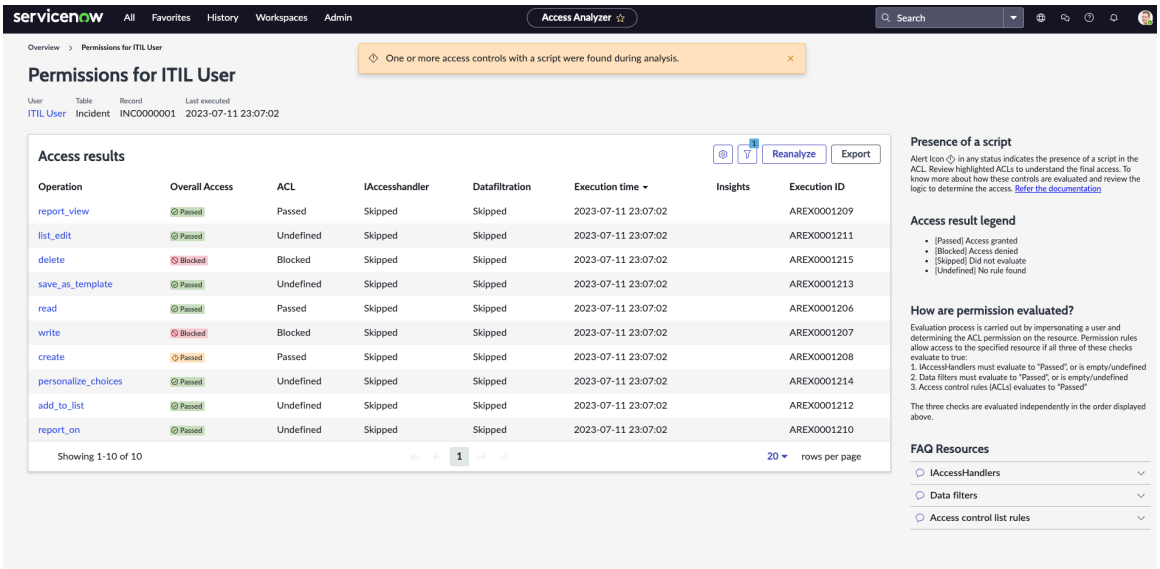
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
필드 선택	목록에서 선택할 필드 이름을 지정합니다. 이 필드는 필드 수준에서도 권한을 분석하는 데 사용할 수 있습니다. 예를 들어 활성, 작성자 등이 있습니다.

3. 설명 필드에 설명을 지정합니다.
4. 권한 분석을 선택합니다.



ITIL 사용자에 대한 액세스 결과가 표시됩니다.



범례, ACL(액세스 제어 목록), IAccesshandler 및 데이터 필터를 참조하여 결과를 읽을 수 있습니다.

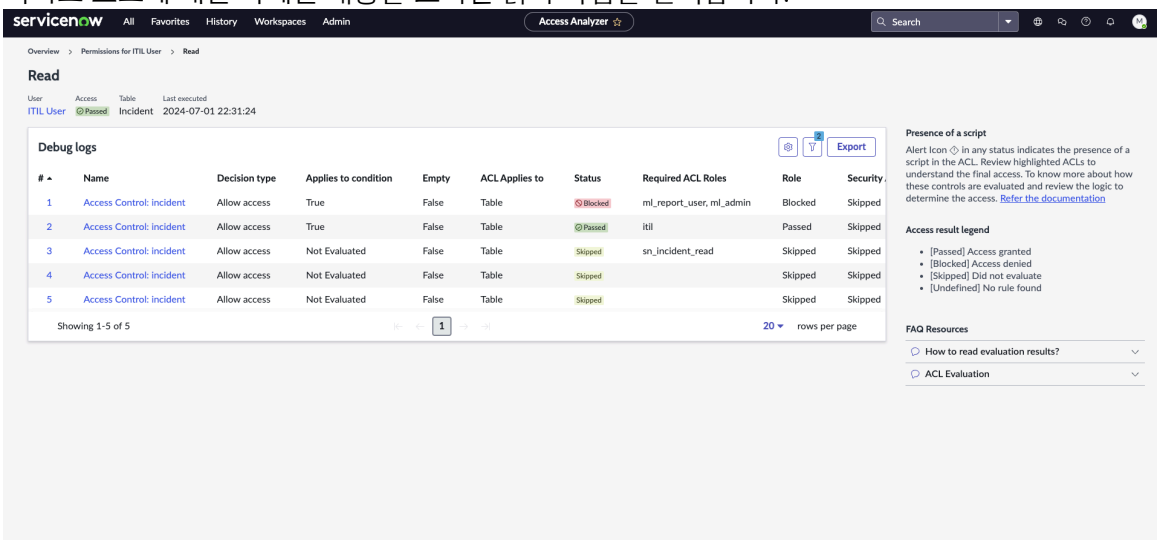
읽기 작업의 예를 들어 보겠습니다. **ITIL** 사용자의 경우 전체 액세스가 전달되며, 이는 사용자가 올바른 권한(ACL)으로 기록을 읽을 수 있음을 의미합니다.

만들기 작업의 경우와 마찬가지로 전체 액세스 권한은 경보 아이콘과 함께 전달되며, 이는 ACL 평가를 위한 스크립트가 있을 수 있음을 의미합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 이 예에서는 선택한 사용자에 대한 쓰기 및 삭제 작업이 차단되고 사용자는 선택한 기록을 편집하거나 삭제할 수 없습니다(INC0000001).

5. 디버그 로그에 대한 자세한 내용을 보려면 읽기 작업을 선택합니다.

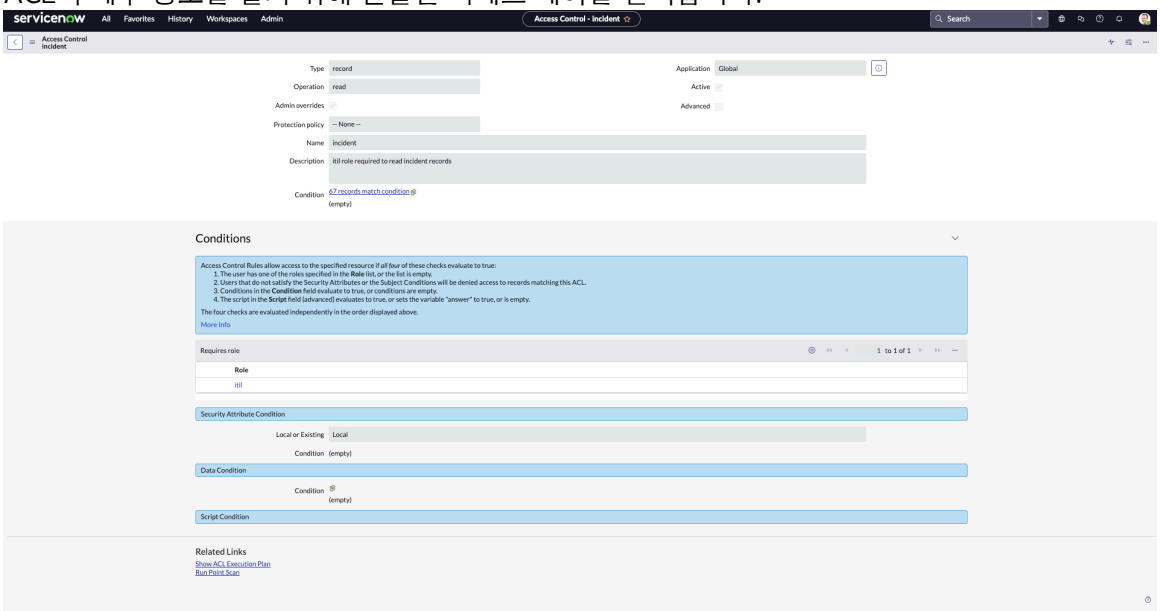


디버그 로그 페이지에는 기록에 대한 읽기 작업을 수행하는 데 필요한 비즈니스 규칙 및 관련 ACL이 표시되었습니다.

디버그 로그는 읽기 작업과 관련된 비즈니스 규칙과 4개의 ACL이 있음을 보여줍니다.

ACL 중 하나에 대해 통과 상태가 있습니다. 이는 선택한 기록을 읽는다는 의미이며, 사용자에게 필요한 ACL이 있으며 기록을 읽을 수 있습니다. ACL 중 하나가 전달되었으므로 다른 ACL 평가는 건너뜁니다.

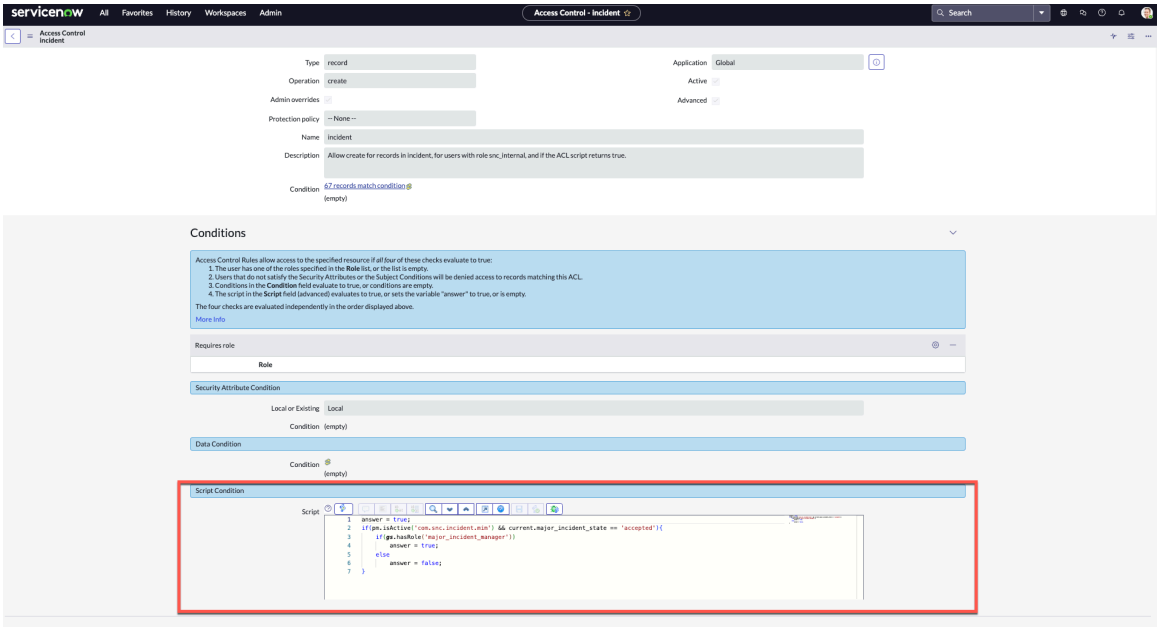
6. ACL의 세부 정보를 알기 위해 전달된 액세스 제어를 선택합니다.



선택한 ACL에 대한 액세스 제어의 세부 정보가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통과했고 스크립트가 있는 선택한 작업의 경우. 접근 제어 페이지에는 기록에 연결된 스크립트가 표시됩니다.



역할에 대한 권한 보기

액세스 분석기를 사용하여 선택한 역할에 대한 권한을 봅니다.

시작하기 전에

필요한 역할: admin, AA_admin

다음 절차에서는 Access Analyzer의 액세스 평가를 사용하여 REST API 엔드포인트에 대한 권한을 보기 위해 선택한 역할(**user_admin**)에 대한 권한을 보는 샘플 단계를 설명합니다.

주: 액세스 분석기는 ServiceNow® 스토어 제품입니다.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.
2. 다음과 같이 기준을 선택합니다.

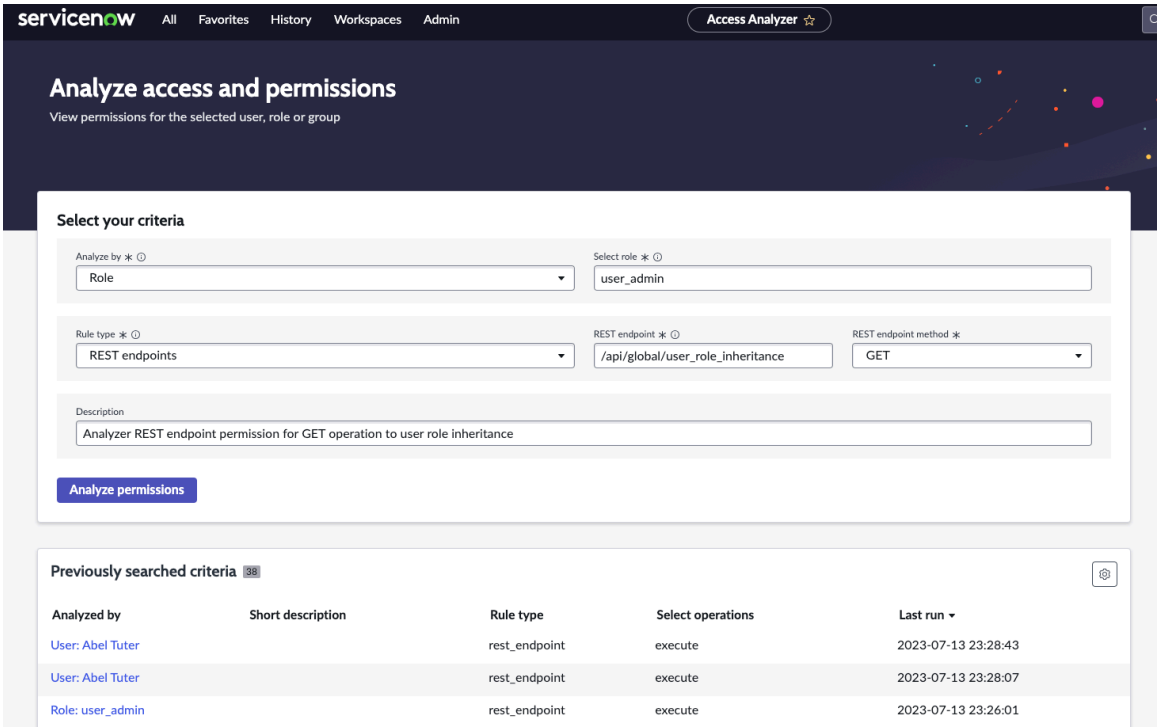
액세스 및 권한을 분석하기 위한 기준을 선택합니다.

필드	설명
분석 단위 *	역할을 선택합니다.
사용자 선택 *	목록에서 선택할 역할을 지정합니다. 예: **user_admin**.
규칙 유형 *	테이블, UI 페이지, REST 엔드포인트 또는 클라이언트 호출 가능 스크립트 포함에 대한 액세스를 분석합니다. 예를 들어 **REST** 엔드포인트입니다.
REST 엔드포인트*	REST 엔드포인트를 지정합니다. 예: `/api/global/user_role_inheritance`.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	주: 선택한 필드를 사용할 때는 전체 REST 엔드포인트를 사용해야 합니다.
REST 엔드포인트 메서드 *	REST 엔드포인트 메서드를 지정합니다. 예를 들어 GET.

3. 설명 필드에 설명을 지정합니다.
4. 권한 분석을 선택합니다.



user_admin 역할에 대한 액세스 결과가 표시됩니다.

범례, ACL(액세스 제어 목록), IAccesshandler 및 데이터 필터를 참조하여 결과를 읽을 수 있습니다.

역할에 대한 전체 액세스 권한이 전달되며, 이는 역할(**user_admin**)이 선택한 **GET** 메서드의 **REST** 엔드포인트에 액세스할 수 있음을 의미합니다.

그룹의 권한 보기

액세스 분석기를 사용하여 선택한 그룹에 대한 권한을 봅니다.

시작하기 전에

필요한 역할: admin, AA_admin

다음 절차는 액세스 분석기의 액세스 평가를 사용하여 선택한 그룹(인시던트 관리)이 인시던트 **UI** 페이지의 권한을 볼 수 있는 권한을 보는 샘플 단계를 설명합니다.

주: 액세스 분석기는 ServiceNow® 스토어 제품입니다.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.

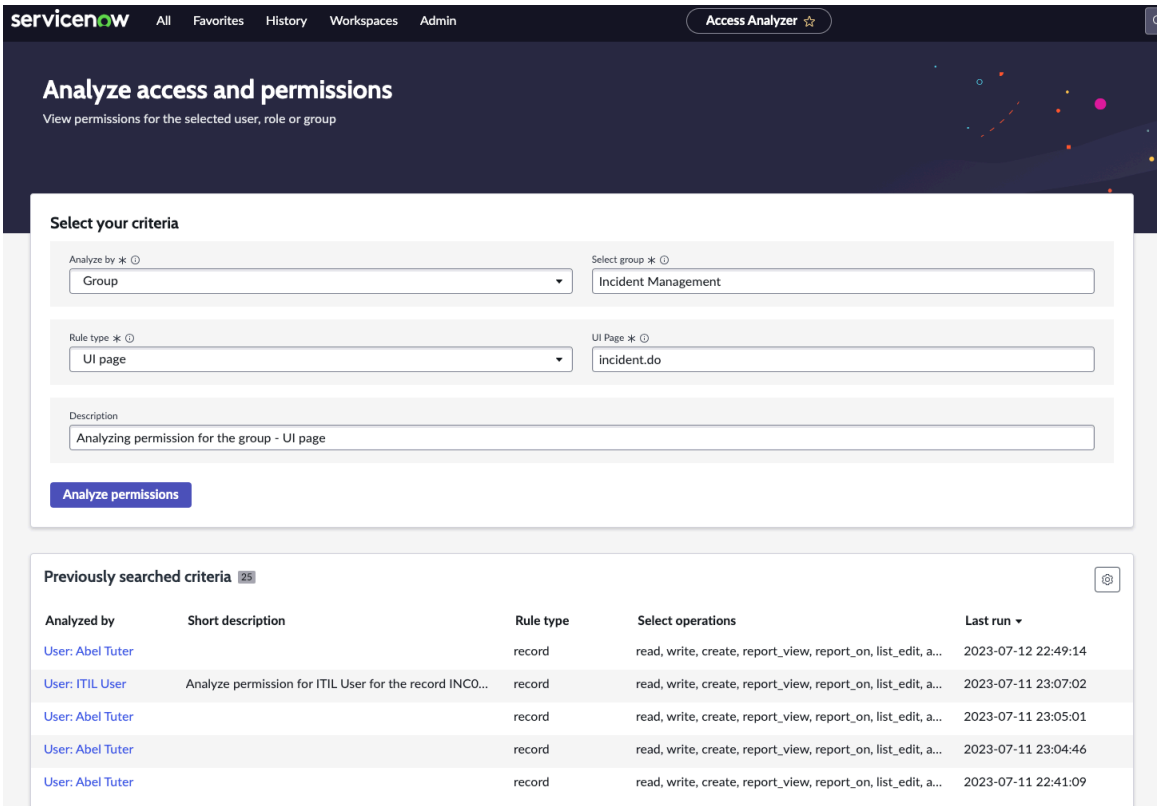
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

2. 다음과 같이 기준을 선택합니다.

액세스 및 권한을 분석하기 위한 기준을 선택합니다.

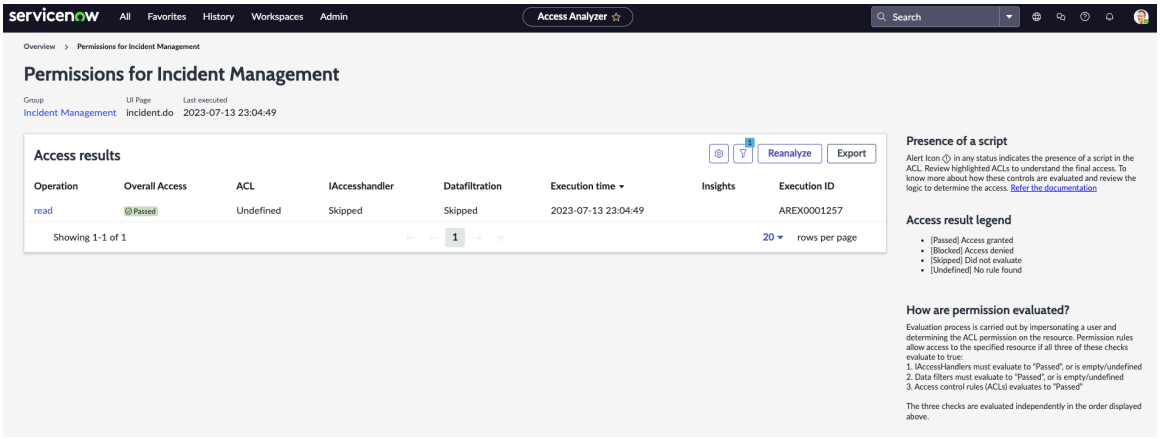
필드	설명
분석 단위 *	그룹을 선택합니다.
사용자 선택 *	목록에서 선택할 사용자 이름을 지정합니다. 인시던트 관리를 예로 들 수 있습니다.
규칙 유형 *	테이블, UI 페이지, REST 엔드포인트 또는 클라이언트 호출 가능 스크립트 포함에 대한 액세스를 분석합니다. 예: **UI** 페이지
UI 페이지 *	UI 페이지를 지정합니다. 예: **incident.do**.

3. 설명 필드에 설명을 지정합니다.
4. 권한 분석을 선택합니다.



인시던트 관리 그룹에 대한 액세스 결과가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



범례, ACL(액세스 제어 목록), IAccesshandler 및 데이터 필터를 참조하여 결과를 읽을 수 있습니다.

그룹에 대한 전체 액세스 권한이 전달되었으므로 그룹(**Incident Management**) 내의 사용자가 인시던트 기록에 액세스할 수 있습니다.

액세스 분석기 쿼리 익스포트

Access Analyzer를 사용하여 분석된 쿼리를 익스포트합니다.

시작하기 전에
필요한 역할: admin, AA_admin

다음 절차에서는 Access Analyzer에 액세스하고 Access Analyzer 내의 다양한 기능을 사용하는 단계를 설명합니다.

주: 액세스 분석기는 ServiceNow® 스토어 제품입니다.

프로시저

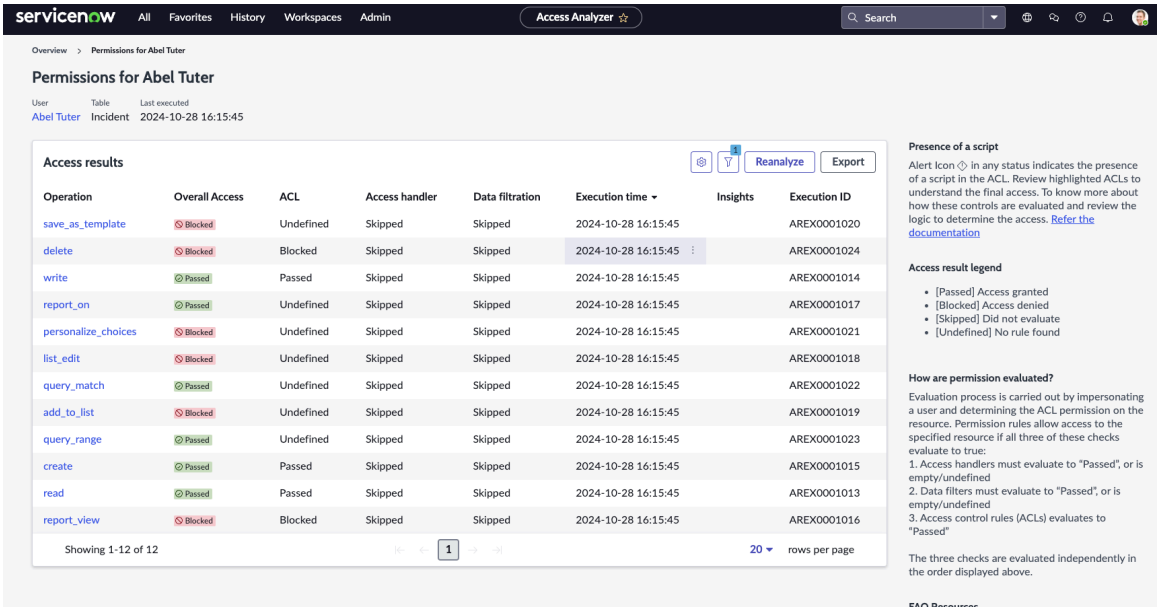
1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.
2. 다음과 같이 기준을 선택합니다.

   액세스 및 권한을 분석하기 위한 기준을 선택합니다.

필드	설명
분석 단위 *	사용자, 역할 또는 그룹에 대한 액세스 분석
사용자 선택 *	목록에서 선택할 사용자 이름을 지정합니다.
규칙 유형 *	테이블, UI 페이지, REST 엔드포인트 또는 클라이언트 호출 가능 스크립트 포함에 대한 액세스를 분석합니다.
테이블 선택 *	목록에서 선택할 테이블 이름을 지정합니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다.
필드 선택	목록에서 선택할 필드 이름을 지정합니다.

3. 설명 필드에 설명을 지정합니다.
4. 권한 분석을 선택합니다.

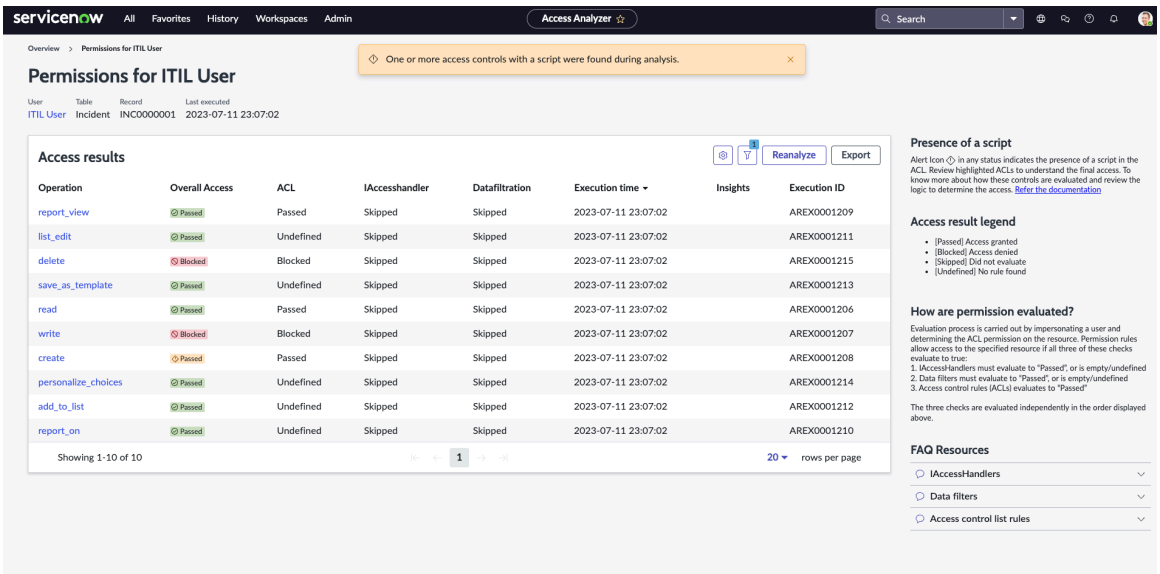
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



사용자에 대한 액세스 결과가 표시됩니다. 마찬가지로 다음 규칙 유형에 대한 그룹, 역할의 권한을 분석할 수 있습니다.

- 테이블(기록)
- 클라이언트 호출 가능 스크립트 포함
- REST 엔드포인트

선택한 규칙 유형에 대한 액세스 결과가 표시됩니다.

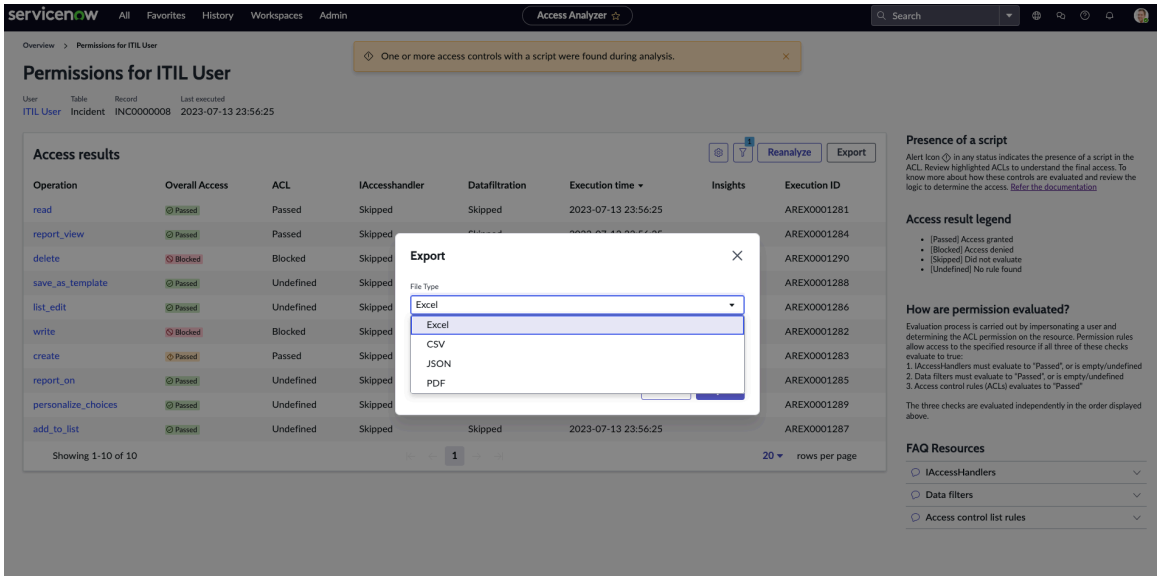


5. 익스포트를 클릭합니다.

a. 파일 유형을 선택합니다.

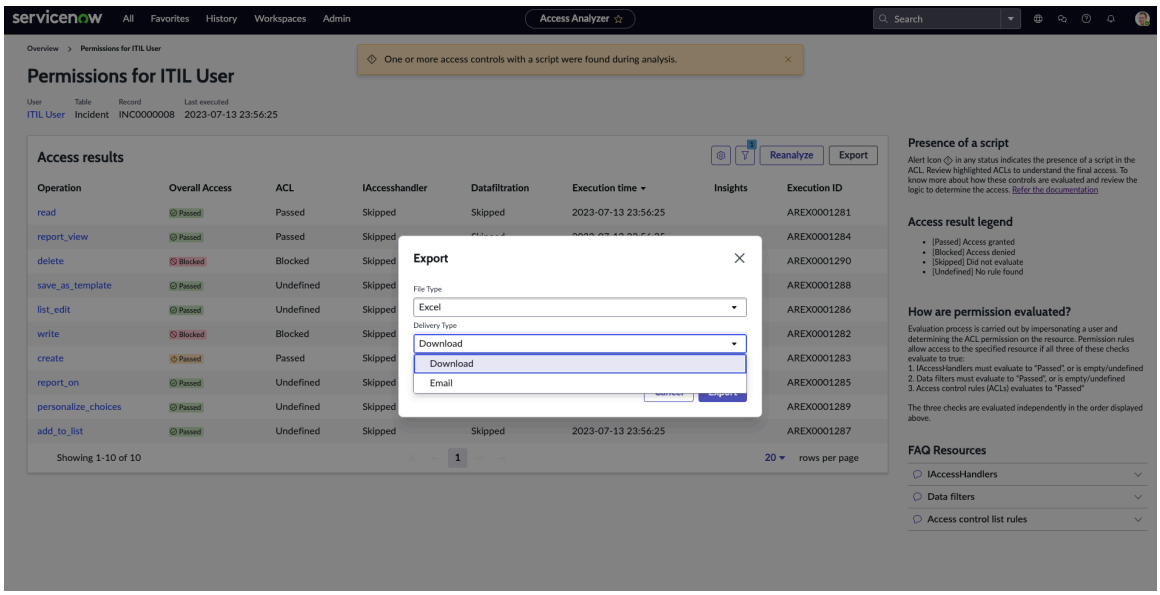
사용 가능한 파일 형식은 Excel, CSV, JSON, PDF.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



b. 제공 유형을 선택합니다.

사용 가능한 제공 유형은 다운로드 및 이메일입니다.



사용자 기록 비교

사용자 기록을 비교하여 두 사용자 간의 액세스를 이해합니다.

시작하기 전에

필요한 역할: admin, AA_admin

다음 절차는 Access Analyzer를 사용하여 사용자 레코드를 비교하는 단계를 설명합니다.

주: 액세스 분석기는 ServiceNow® Store 제품입니다.

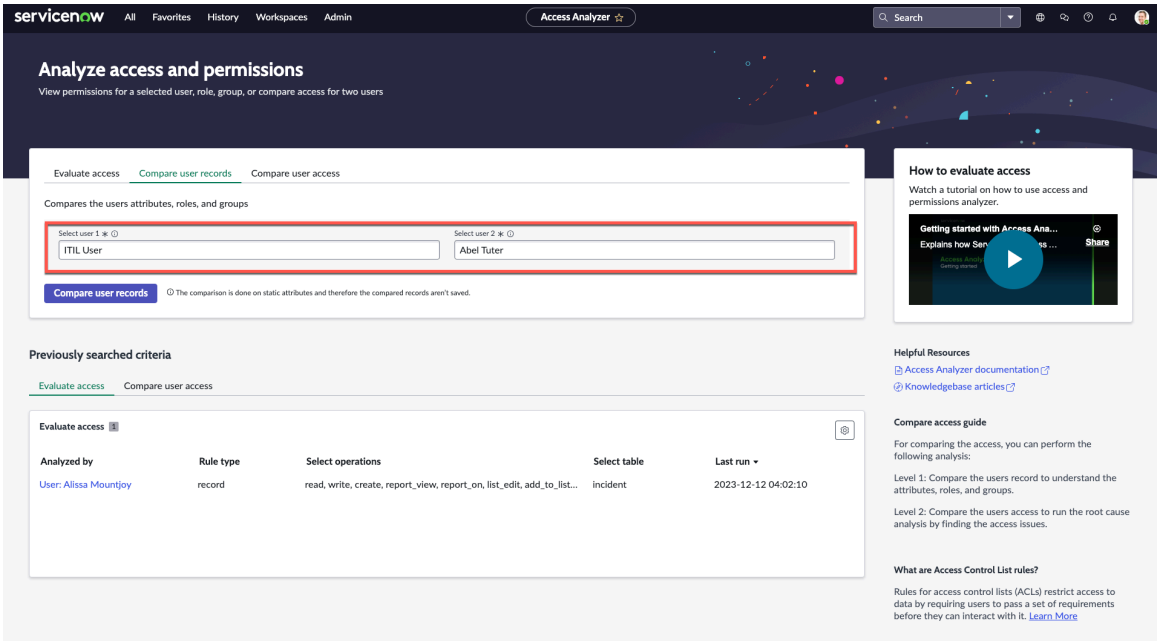
프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.
2. 사용자 기록 비교 탭을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 비교할 사용자 **1** 과 사용자 **2** 를 선택합니다.

   예를 들어, 사용자 **1**은 `ITIL ###`이고 사용자 **2**는 `Abel Tuter`입니다.

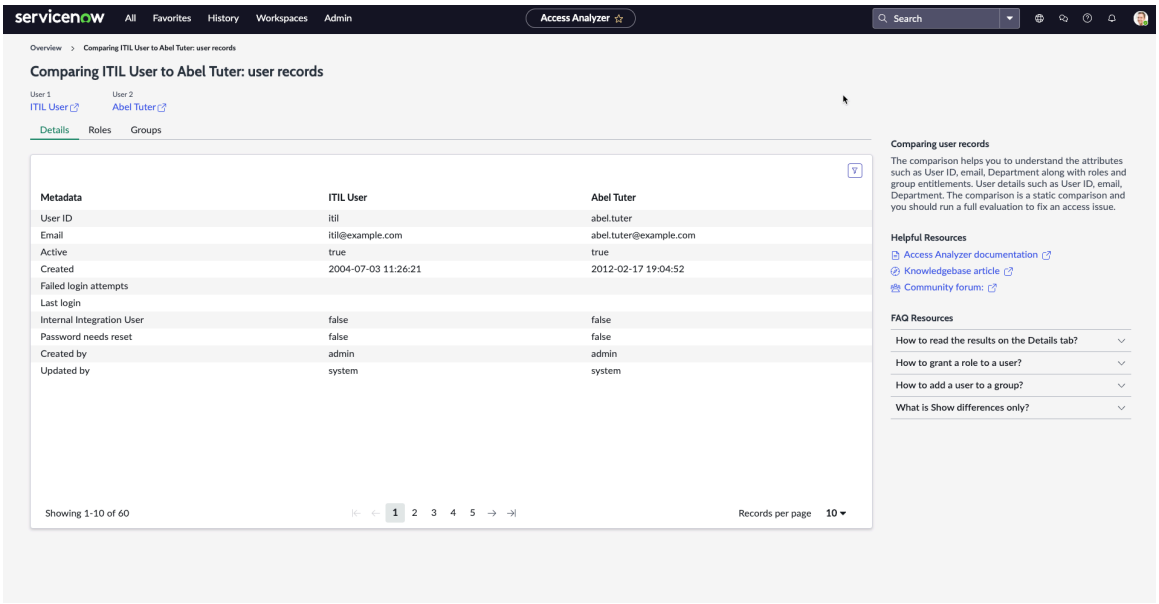


4. 사용자 기록 비교를 선택합니다.

   결과는 다음 탭과 함께 표시됩니다.

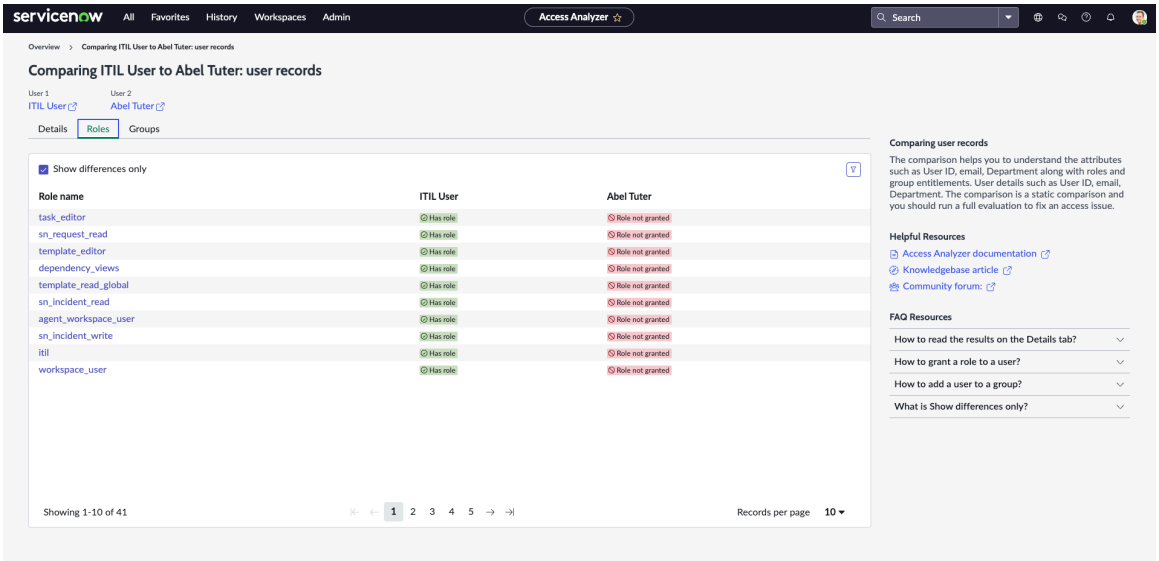
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ 상세 정보: 사용자의 메타데이터를



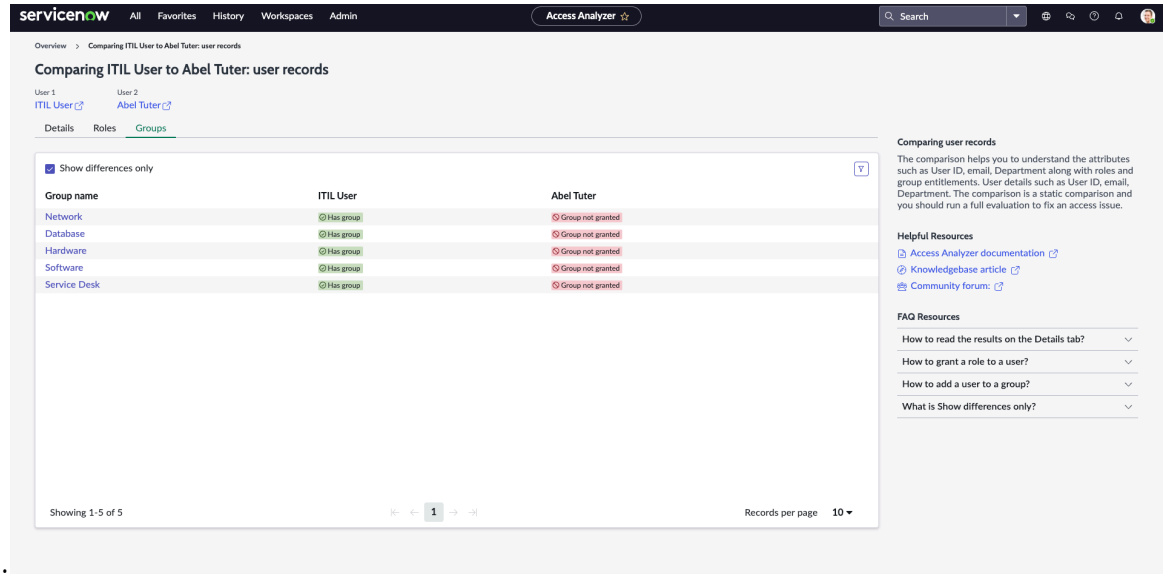
표시합니다.

◦ 역할: 사용자에게 할당된 역할을 표시합니다. 역할을 선택하여 역할 및 해당 권리에 대해 자세히 알아볼 수 있습니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

◦ 그룹: 사용자에게 할당된 그룹을 표시합니다. 그룹을 선택하여 그룹 및 해당 권리에 대해 자세히 알아볼 수



있습니다.

마찬가지로 인스턴스의 여러 사용자를 ServiceNow 비교하여 사용자에게 할당된 액세스 권한을 파악할 수 있습니다.

사용자 액세스 비교

액세스 분석기를 사용하여 사용자의 액세스 제어를 비교합니다.

시작하기 전에

필요한 역할: admin, AA_admin

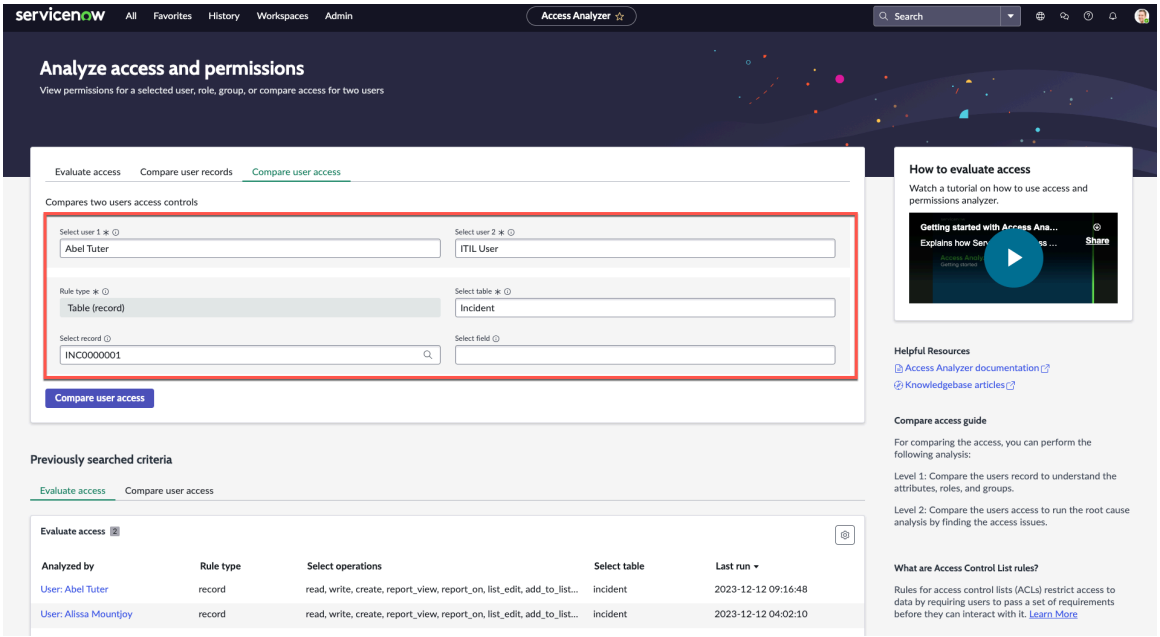
다음 절차에서는 Access Analyzer를 사용하여 사용자 간의 액세스 제어를 비교하는 단계를 설명합니다.

주: 액세스 분석기는 ServiceNow® Store 제품입니다.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.
2. 사용자 액세스 비교 탭을 선택합니다.
3. 다음 필드를 채웁니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



사용자 액세스 비교

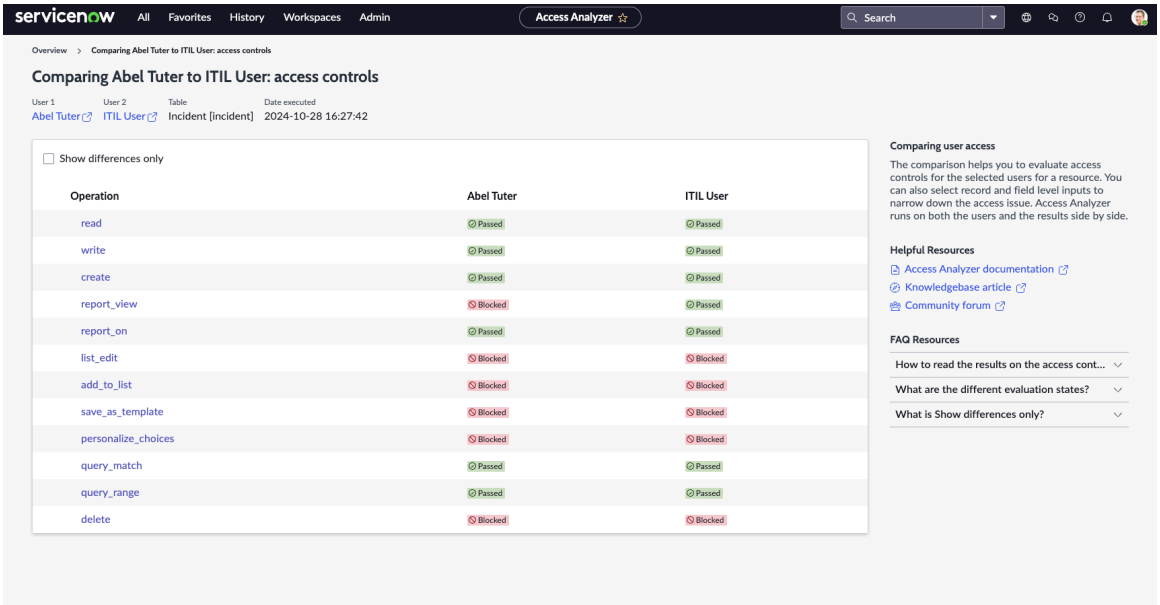
필드	설명
사용자 1* 선택	비교할 목록에서 선택할 사용자 이름을 지정합니다.
사용자 2* 선택	목록에서 선택하여 사용자와 비교할 사용자 이름을 지정합니다 1.
규칙 유형*	테이블에 대한 액세스 권한을 분석합니다. 주: 테이블에 대한 액세스 권한만 사용자 비교 액세스에 사용할 수 있습니다.
테이블 선택*	목록에서 선택할 테이블 이름을 지정합니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다.
필드 선택	목록에서 선택할 필드 이름을 지정합니다.

4. 사용자 액세스 비교를 선택합니다.

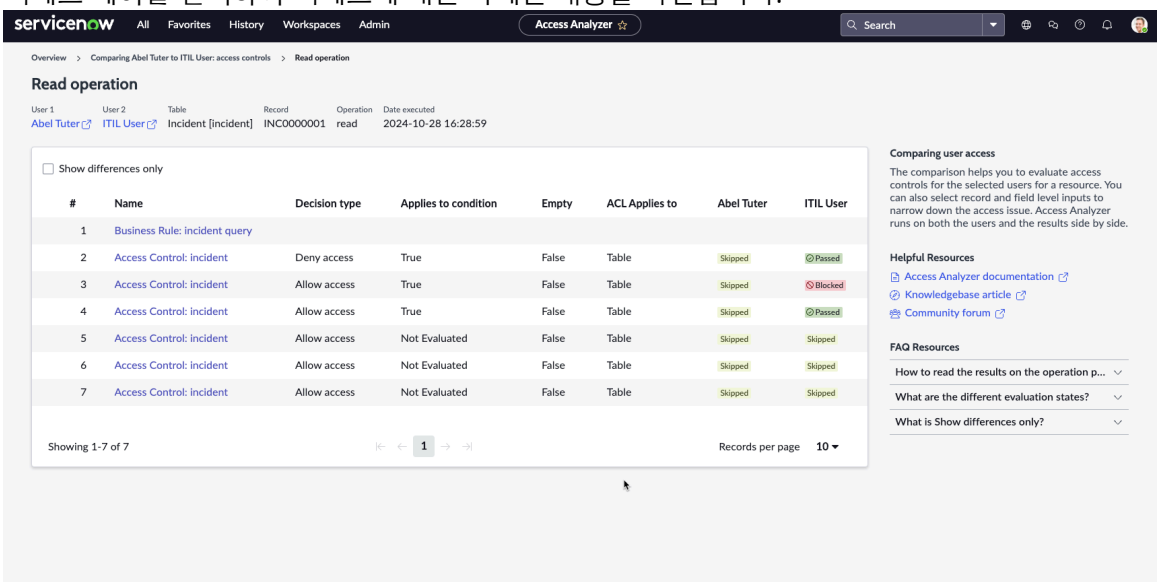
   선택한 사용자에 대한 사용자 액세스 비교 결과가 표시됩니다.

   사용자 액세스 비교 결과에는 사용자에 대한 작업 및 액세스 평가 상태가 표시됩니다. 예를 들어 Abel Tuter 및 ITIL 사용자가 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

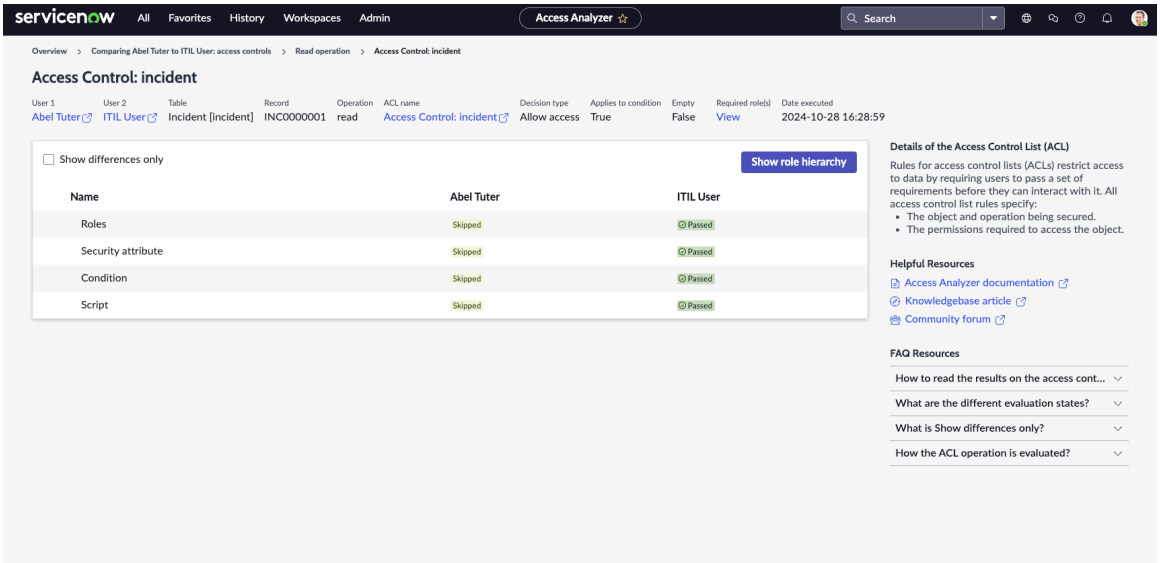


5. 권한 평가 및 사용자에게 할당된 역할에 대해 자세히 알아보려면 작업을 선택하십시오. 예를 들어 읽기 작업입니다.
6. 액세스 제어를 선택하여 액세스에 대한 자세한 내용을 확인합니다.



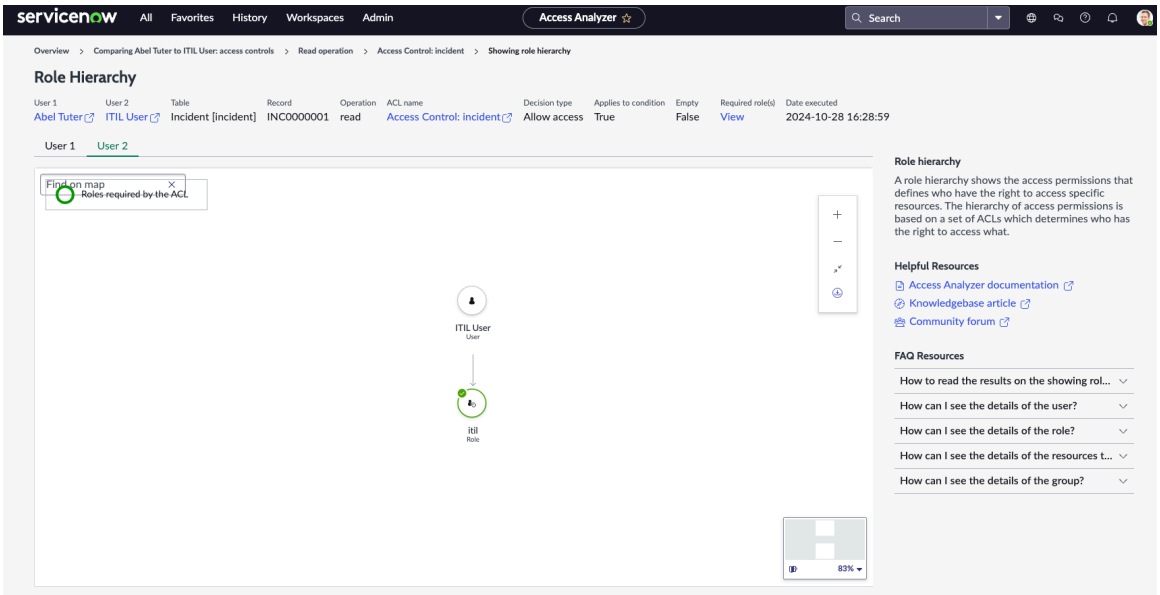
역할, 보안 속성, 조건 및 스크립트 평가 상태와 같은 접근 제어 상세 정보가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



7. 역할 계층 구조 표시를 선택하여 사용자에게 할당된 역할과 그룹에 대해 자세히 알아보고 두 사용자를 비교합니다.

   역할 계층 구조에 따라 자원(테이블)에 액세스할 수 있도록 사용자에게 필요한 역할 및 그룹 할당을 할당할 수 있습니다.



   이 예에서 **Abel Tuter** 에는 `itil` 이 할당되어 있지 않습니다. 역할 계층 구조를 살펴보고 사용자에게 필요한 역할 및 그룹 할당을 결정할 수 있습니다.

   노드를 선택하여 역할, 역할이 액세스할 수 있는 자원 또는 그룹화에 대해 자세히 알아볼 수 있습니다.

액세스 분석기 쿼리 보기 - 이전에 검색된 기준

이전에 검색한 액세스 분석기 기준을 봅니다.

시작하기 전에
필요한 역할: admin, AA_admin

> 주: 액세스 분석기는 ServiceNow® Store 제품입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

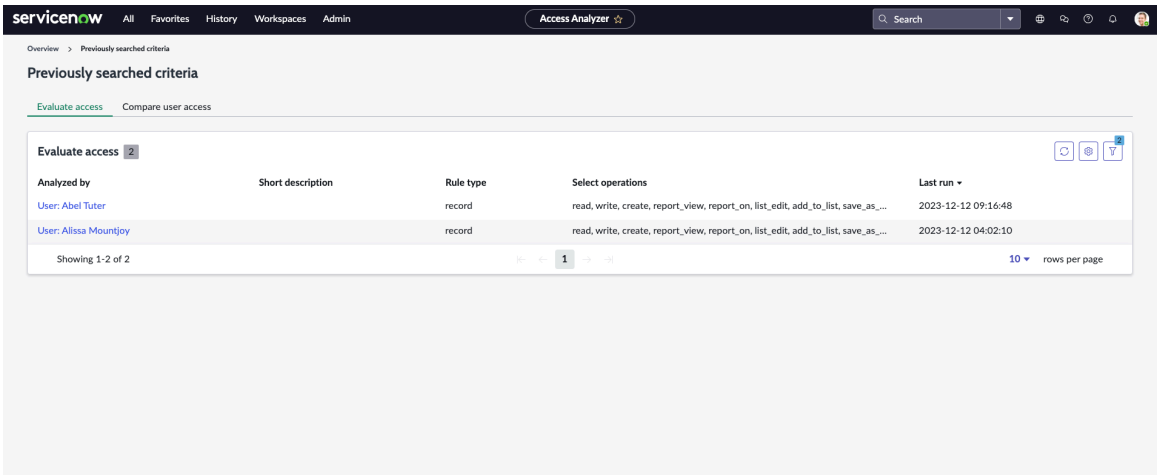
프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 액세스 분석기 쿼리.

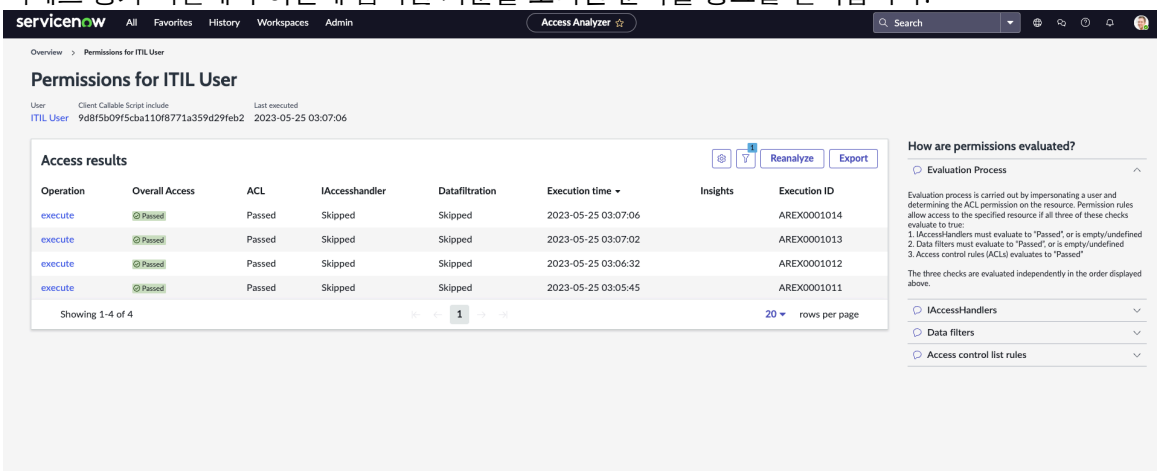
   이전에 검색된 기준에는 다음 섹션이 있습니다.

   - 액세스 평가: 액세스 평가 기능을 통해 수행된 쿼리를 기반으로 결과를 표시합니다.
   - 사용자 액세스 비교: 사용자 액세스 비교 기능을 통해 수행된 쿼리를 기반으로 결과를 표시합니다.

   주: 사용자 기록 비교 기능을 사용할 때 이전에 검색한 기준은 저장되지 않습니다.



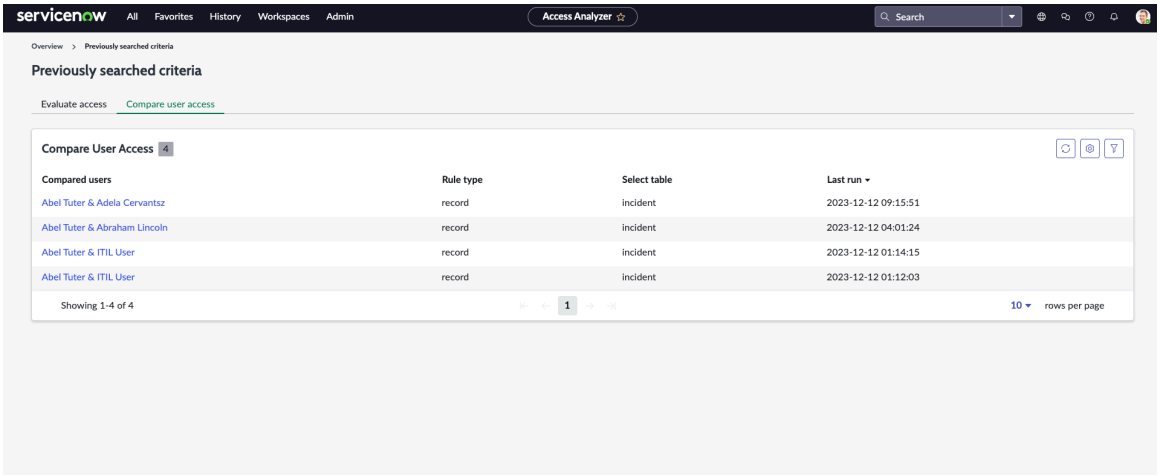
2. 액세스 평가 섹션에서 이전에 검색된 기준을 보려면 분석별 링크를 선택합니다.



사용자에 대한 액세스 재분석을 선택할 수 있습니다. 익스포트 옵션을 사용하여 상세 정보를 익스포트합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 사용자 액세스 비교 섹션에서 이전에 검색된 기준을 보려면 비교된 사용자 링크를 선택합니다.



권한 평가

액세스 분석기를 사용하는 경우 권한 평가 기준입니다.

평가 계층 구조

선택한 사용자, 그룹 또는 역할에 대한 권한은 다음 계층 구조에서 평가됩니다.

- 비즈니스 규칙: 비즈니스 규칙은 기록이 표시, 삽입, 업데이트 또는 삭제되거나 테이블이 쿼리될 때 실행되는 서버 측 스크립트입니다.
- 액세스 핸들러: 플랫폼에서 숨겨진 소스 코드를 사용하는 내부 시스템 검사입니다.
- 데이터 필터링: 데이터 필터는 인스턴스의 기존 접근 통제 규칙(ACL)과 함께 작동하도록 설계된 접근 제어의 한 형태입니다. 데이터 필터는 읽기 작업만 지원합니다.
- ACL(접근 제어 목록): ACL(접근 제어 목록)에 대한 규칙은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 액세스를 제한합니다. ACL 내에서 다음과 같은 계층이 평가됩니다.
  - 역할
  - 보안 속성
  - 조건
  - 스크립트

액세스 분석기를 사용하여 선택한 사용자, 역할 또는 그룹에 대한 액세스 및 권한을 분석할 수 있습니다. 권한은 다음 규칙 유형에 따라 평가됩니다.

- 테이블 수준 평가: 역할 및 보안 속성 ACL은 테이블 수준 평가에 사용됩니다.
- 기록 또는 필드 수준 평가: 역할, 보안 속성, 조건 및 스크립트 수준 ACL은 기록 또는 필드 수준 평가에 사용됩니다.
- **UI** 페이지: 지원 전용 준비된 작업. 읽기 수준 ACL만 평가됩니다.
- **REST** 엔드포인트: 실행 작업만 지원합니다. 실행 수준 ACL만 평가됩니다.

액세스 결과의 중요 필드에 대한 세부 정보는 다음과 같습니다.

- 스크립트의 존재
- 액세스 결과 범례

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 평가 프로세스
- IAccessHandlers
- 데이터 필터
- 접근 제어 목록 규칙

스크립트의 존재

모든 상태의 경보 아이콘은 ACL에 스크립트가 있음을 나타냅니다. 강조 표시된 ACL을 검토하여 최종 액세스 권한을 파악합니다. 이러한 컨트롤을 평가하고 액세스 권한을 결정하는 논리를 검토하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오 액세스 분석기 디버그 로그.

액세스 분석기의 범례

액세스 및 권한을 분석할 때 범례가 평가 프로세스의 일부로 표시됩니다. 다음은 범례입니다.

- 〔통과됨〕 액세스 권한 부여됨
- 〔차단됨〕 접근 거부됨
- 〔건너뜀〕 평가하지 않음
- 〔정의되지 않음〕 규칙을 찾을 수 없음

평가 프로세스

평가 프로세스는 사용자를 가장하고 자원에 대한 ACL(접근 제어 목록) 권한을 결정하여 수행됩니다. 권한 규칙을 사용하면 다음 검사가 true로 평가될 경우 지정된 자원에 액세스할 수 있습니다.

- IAccessHandlers는 "통과"로 평가되어야 하거나 비어 있거나 정의되지 않았습니다.
- 데이터 필터는 "통과"로 평가되어야 하거나, 비어 있거나 정의되지 않았습니다.
- 접근 통제 규칙(ACL)은 "통과"로 평가됩니다.

IAccessHandlers

플랫폼에서 숨겨진 소스 코드를 사용하는 내부 시스템 검사입니다. IAccessHandler는 ACL을 평가하지 않고 리소스에 대한 액세스 권한을 부여하거나 거부할 수 있습니다. IAccessHandler를 무시하면 ACL이 평가됩니다.

IAccessHandler 검사를 변경할 수 없습니다. 예를 들어 IAccessHandler 구현은 읽기 액세스와 같은 애플리케이션 자원에 대한 액세스 검사에 사용됩니다.

데이터 필터

데이터 필터는 인스턴스의 기존 접근 통제 규칙(ACL)과 함께 작동하도록 설계된 접근 제어의 한 형태입니다.

접근 제어 목록 규칙

접근 제어 목록(ACL)에 대한 규칙은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 액세스를 제한합니다.

자주 묻는 질문

액세스 분석기를 사용하는 동안 자주 묻는 질문입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

액세스 평가

다음은 Access Analyzer에서 액세스 평가 기능을 사용할 때 자주 묻는 질문입니다.

자주 묻는 질문

질문	설명
액세스 분석기에 의해 표시된 평가 결과를 읽는 방법은 무엇입니까?	각 행은 개별 ACL(접근 제어 목록)을 나타냅니다. 결과의 시퀀스(#)는 ACL이 평가되는 순서입니다. 상태에는 전체 액세스 권한이 부여되었는지(통과) 또는 거부되었는지(차단됨)가 표시됩니다.
ACL은 어떻게 평가됩니까?	테이블 수준에서 ACL은 역할 및 보안 속성에 대해서만 평가되며, 조건 및 스크립트는 평가되지 않습니다. 역할이 먼저 평가됩니다. 역할이 차단되면 조건과 스크립트를 건너뜁니다. 자세한 내용은 ACL 규칙 구성 문서를 참조하십시오.
Access Analyzer의 범례는 무엇입니까?	액세스 및 권한을 분석할 때 범례가 평가 프로세스의 일부로 표시됩니다. 다음은 범례입니다. • 〔통과됨〕 액세스 권한 부여됨 • 〔차단됨〕 접근 거부됨 • 〔건너뜀〕 평가하지 않음 • 〔정의되지 않음〕 규칙을 찾을 수 없음
Access 결과의 경고 아이콘은 무엇을 의미합니까?	모든 상태의 경보 아이콘은 ACL에 스크립트가 있음을 나타냅니다. 강조 표시된 ACL을 검토하여 최종 액세스 권한을 파악합니다. 이러한 컨트롤을 평가하고 액세스 권한을 결정하는 논리를 검토하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오 액세스 분석기 디버그 로그.
IAccesshandler란 무엇입니까?	플랫폼에서 숨겨진 소스 코드를 사용하는 내부 시스템 검사입니다. 수정할 수 없는 시스템 보안 검사입니다. **IAccessHandler** 는 ACL을 평가하지 않고 리소스에 대한 액세스 권한을 부여하거나 거부할 수 있습니다. 이 **IAccessHandler** 를 무시하면 ACL이 평가됩니다. 어떤 식으로든 **IAccessHandler** 검사를 수정할 수 없습니다. 예를 들어 **IAccessHandler** 구현은 읽기 전용 액세스와 같은 응용 프로그램 리소스에 대한 액세스 검사에 사용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자주 묻는 질문

질문	설명
데이터 필터란 무엇입니까?	데이터 필터는 인스턴스의 기존 접근 통제 규칙(ACL)과 함께 작동하도록 설계된 접근 제어의 한 형태입니다.
ACL 규칙이란 무엇입니까?	접근 제어 목록(ACL)에 대한 규칙은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 액세스를 제한합니다.

결과에 영향을 줄 수 있는 사용자에 대한 시간 제한 역할 할당이 발견되었습니다. 여기에서 사용자에게 할당된 시간 제한 역할을 검토할 수 있습니다.

사용자 기록 비교

다음은 Access Analyzer에서 사용자 기록 비교 기능을 사용할 때 자주 묻는 질문입니다.

자주 묻는 질문

질문	설명
세부 정보 탭에서 결과를 읽는 방법은 무엇입니까?	상세 정보 탭에는 사용자 1 및 사용자 2와 연결된 메타데이터가 표시됩니다
사용자에게 역할을 부여하는 방법은 무엇입니까?	사용자 탭에서 사용자에게 부여해야 하는 역할을 확인하고 해당 역할을 할당할 수 있습니다.
그룹에 사용자를 추가하는 방법은 무엇입니까?	그룹 탭에서 사용자를 추가해야 하는 그룹을 확인하고 사용자를 그룹에 추가할 수 있습니다.
차이만 표시란 무엇입니까?	차이점만 표시 확인란을 선택하면 사용자 1과 사용자 2 간 다른 역할 또는 그룹만 표시됩니다.

사용자 액세스 비교

다음은 Access Analyzer에서 사용자 액세스 비교 기능을 사용할 때 자주 묻는 질문입니다.

자주 묻는 질문

질문	설명
접근 제어 비교 페이지에서 결과를 읽는 방법은 무엇입니까?	접근 제어 비교 페이지에는 다른 ACL 작업에 대한 평가 상태가 표시됩니다.
다른 평가 상태는 무엇입니까?	사용자 간 접근 제어를 비교할 때 다른 평가 상태는 다음과 같습니다. • 통과 • 차단됨
차이만 표시란 무엇입니까?	차이점만 표시 확인란을 선택하면 사용자 1과 사용자 2 간 다른 작업 평가 상태만 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자주 묻는 질문

질문	설명
ACL 작업이 어떻게 평가됩니까?	접근 제어 목록(ACL)은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 접근을 제한하는 접근 제어 목록(ACL) 규칙입니다. ACL 내에서 다음과 같은 계층이 평가됩니다. • 역할 • 보안 속성 • 조건 • 스크립트
역할 계층 구조 표시 페이지에서 결과를 읽는 방법은 무엇입니까?	역할 계층 구조 표시 페이지에는 사용자 1과 사용자 2에 할당된 역할이 표시됩니다. 특정 ACL 작업을 위해 사용자에게 요구되는 역할을 이해할 수 있습니다.
사용자의 세부 정보는 어떻게 볼 수 있습니까?	다음을 선택할 수 있습니다. 사용자(노드) > 추가 작업 > 사용자 뷰 사용자에 대한 자세한 내용을 확인할 수 있는 세부 정보입니다.
역할의 세부 정보는 어떻게 볼 수 있습니까?	다음을 선택할 수 있습니다. 역할(노드) > 추가 작업 > 역할 보기 역할에 대한 자세한 내용은 세부 정보를 참조하십시오.
역할이 액세스할 수 있는 자원의 세부 정보는 어떻게 볼 수 있습니까?	다음을 선택할 수 있습니다. 역할(노드) > 추가 작업 > 역할이 액세스할 수 있는 모든 자원 보기 역할이 액세스할 수 있는 자원을 파악합니다.
그룹 세부 정보는 어떻게 볼 수 있습니까?	다음을 선택할 수 있습니다. 그룹(노드) > 추가 작업 > 그룹 뷰 그룹에 대한 자세한 내용을 확인할 수 있는 세부 정보입니다.

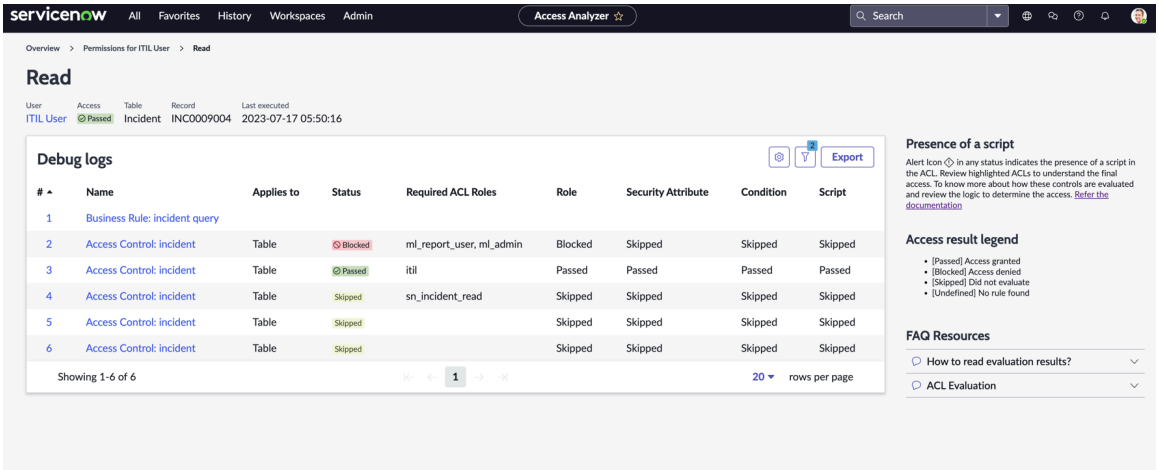
액세스 분석기 디버그 로그

디버그 로그에 액세스 결과 선택 작업의 세부 정보가 표시됩니다.

디버그 로그의 필드

액세스 분석기의 디버그 로그에는 작업과 관련된 권한, 비즈니스 규칙 및 ACL을 이해하기 위해 선택한 작업에 대한 정보가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



다음은 디버그 로그의 필드와 해당 설명입니다.

디버그 로그

필드	설명
이름	비즈니스 규칙 또는 ACL에 대한 상세 정보입니다. 자세한 내용은 ACL의 비즈니스 규칙을 선택할 수 있습니다.
적용 대상	필드, 기록 또는 테이블 수준에서의 ACL 적용에 대한 상세 정보입니다.
상태	관련 역할 및 권한에 대한 ACL의 상태입니다.
ACL 필요	필드, 기록 또는 테이블에 액세스하는 데 필요한 역할입니다.
역할	접근 제어에 대해 차단, 통과, 건너뛴 역할에 대한 상세 정보입니다.
보안 속성	접근 제어에 대해 차단, 통과, 건너뛴 보안 속성에 대한 상세 정보입니다.
조건	액세스 제어에 대해 차단, 통과, 건너뛴 조건에 대한 상세 정보입니다.
스크립트	접근 제어에 대해 차단, 통과, 건너뛴 스크립트에 대한 상세 정보입니다.
사용자 지정됨	액세스 제어에 대해 사용자 지정된 ACL에 대한 상세 정보입니다(있는 경우).
애플리케이션	애플리케이션의 상태입니다. 전역 또는 스토어.

평가 계층 구조

선택한 사용자, 그룹 또는 역할에 대한 권한은 다음 계층 구조에서 평가됩니다.

- 비즈니스 규칙: 비즈니스 규칙은 기록이 표시, 삽입, 업데이트 또는 삭제되거나 테이블이 쿼리될 때 실행되는 서버 측 스크립트입니다.
- 액세스 핸들러: 플랫폼에서 숨겨진 소스 코드를 사용하는 내부 시스템 검사입니다.
- 데이터 필터링: 데이터 필터는 인스턴스의 기존 접근 통제 규칙(ACL)과 함께 작동하도록 설계된 접근 제어의 한 형태입니다. 데이터 필터는 읽기 작업만 지원합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- ACL(접근 제어 목록): ACL(접근 제어 목록)에 대한 규칙은 사용자가 데이터와 상호작용하기 전에 일련의 요구 사항을 통과하도록 요구하여 데이터에 대한 액세스를 제한합니다. ACL 내에서 다음과 같은 계층이 평가됩니다.
  - 역할
  - 보안 속성
  - 조건
  - 스크립트

접근 제어 목록 평가

작업에 대한 ACL은 다음과 같은 순서대로 평가됩니다.

- 역할
- 보안 속성
- 조건
- 스크립트

스크립트의 존재

모든 상태의 경보 아이콘은 ACL에 스크립트가 있음을 나타냅니다. 강조 표시된 ACL을 검토하여 최종 액세스 권한을 파악합니다.

주: 액세스 분석기 쿼리 중에는 비즈니스 규칙이 먼저 실행된 다음 액세스 제어 목록이 실행됩니다.

실행 시퀀스

다양한 시나리오에서 액세스 결과 실행 순서는 다음과 같습니다.

- 상속된 **ACL** 또는 와일드카드 ACL의 존재: 실행 시퀀스 중에 상속된 ACL이 먼저 평가된 다음 와일드카드 ACL이 평가됩니다.
- 하나의 ACL이 전달되고 다른 ACL은 건너뜁니다. 권한을 실행하고 평가하는 동안 하나의 ACL이 전달되면 다른 ACL 실행 및 평가를 건너뜁니다. 선택한 작업에 대한 전체 권한에서 ID의 필드, 기록 또는 테이블에 액세스하려면 하나의 ACL이 필요하기 때문입니다.
- 필드 수준 **ACL** 및 테이블 수준 **ACL** 실행: 실행 중에 필드 수준 ACL이 먼저 실행된 다음 테이블 수준 ACL이 실행되어 ID에 대한 액세스를 분석할 때 보다 세부적인 결과를 제공합니다.
- 스크립팅된 ACL이 있는 경우 평가: 스크립트가 있는 경우 작업에 대한 전체 액세스 권한은 ACL의 스크립트를 나타내는 경고 아이콘과 함께 전달됩니다.

액세스 시뮬레이터

액세스 시뮬레이터를 사용하면 역할 또는 그룹이 할당되거나 사용자에게서 제거되었을 때 지정된 테이블에 대한 액세스가 어떻게 변경되는지 시뮬레이션할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색



액세스 시뮬레이터의 기능 및 비즈니스 가치에 대해 알아봅니다.

사용



액세스 시뮬레이터 사용 방법을 이해합니다.

구성



액세스 시뮬레이터 구성 방법을 알아봅니다.

자주 묻는 질문



액세스 시뮬레이터에 대해 자주 묻는 질문에 대해 자세히 알아보세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Access 시뮬레이터 살펴보기

액세스 시뮬레이터를 사용하면 역할 또는 그룹이 할당되거나 사용자에게서 제거되었을 때 지정된 테이블에 대한 액세스가 어떻게 변경되는지 시뮬레이션할 수 있습니다.

관리자는 액세스 시뮬레이터를 사용하여 지정된 테이블에서 사용자의 액세스 요구 사항을 시뮬레이션하고 사용자에 대한 액세스 제어가 어떻게 변경되는지 이해할 수 있습니다. 이는 사용자의 현재 액세스를 빠르게 이해하고 사용자에게 역할을 제공하거나 제거할 때의 영향을 이해하는 데 도움이 됩니다.

https://player.vimeo.com/video/988627830?badge=0&autopause=0&player_id=0&app_id=58479

액세스 시뮬레이터는 다음 시나리오에서 사용자에 대한 액세스를 시뮬레이션하는 데 사용할 수 있습니다.

- 사용자에게 역할 추가
- 사용자로부터 역할 제거
- 그룹에 사용자 추가
- 그룹에서 사용자 제거

액세스 시뮬레이터 설정에 대한 자세한 내용을 보고 작업 수행을 활성화하려면 다음 문서를 참조하십시오 액세스 시뮬레이터 구성(작업 수행).

액세스 시뮬레이터 구성(작업 수행)

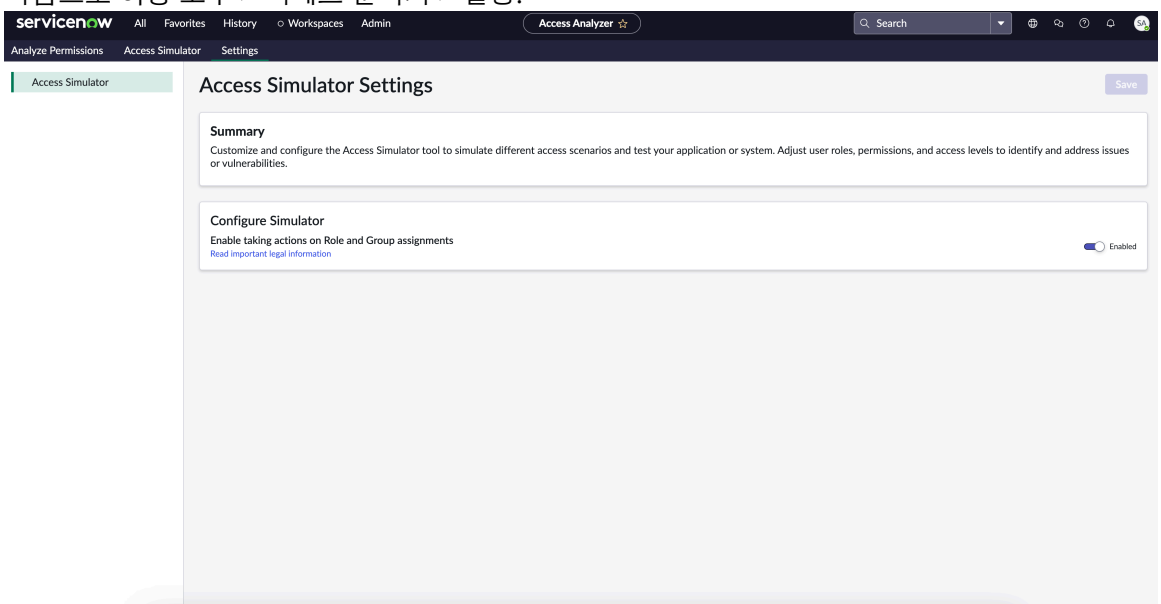
시뮬레이션 후 추가하려는 역할 및 그룹 할당을 완료하도록 작업 수행 옵션을 구성합니다.

시작하기 전에

필요한 역할: admin, AA_admin

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 설정.



2. 활성화하려면 토글 스위치를 선택합니다.
   액세스 시뮬레이터를 활성화하기 전에 법무 정보를 읽어보십시오(조치하기).
3. 수락을 선택합니다.
4. 저장을 선택하여 구성을 저장합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

액세스 시뮬레이터 사용

액세스 시뮬레이터를 사용하면 역할 또는 그룹이 할당되거나 제거되었을 때 지정된 테이블에 대한 사용자의 액세스가 변경될 수 있음을 시뮬레이션할 수 있습니다.

시작하기 전에

필요한 역할: admin, AA_admin

수행 작업을 활성화합니다. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 액세스 시뮬레이터.
2. 다음 시나리오를 기준으로 각 섹션 아래에서 시뮬레이션 옵션을 선택합니다.
   - 사용자에게 역할 추가
   - 사용자로부터 역할 제거
   - 그룹에 사용자 추가
   - 그룹에서 사용자 제거

사용자에게 역할 추가

자원(테이블)에 대한 사용자의 접근 변경을 시뮬레이션하려면 역할 추가 시뮬레이션 을 사용합니다.

시작하기 전에

필요한 역할: admin, AA_admin

수행 작업을 활성화합니다. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.

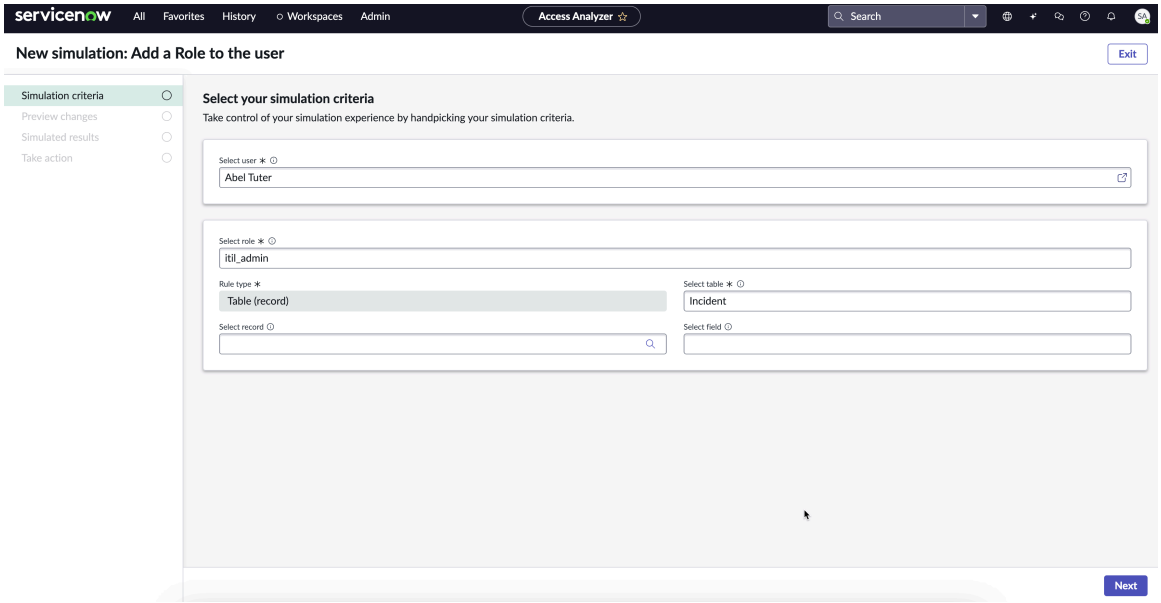
프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 액세스 시뮬레이터.
2. Add a Role to the user 섹션에서 **Simulate** 를 선택합니다.
3. 시뮬레이션 기준에 대해 다음 필드를 지정합니다.

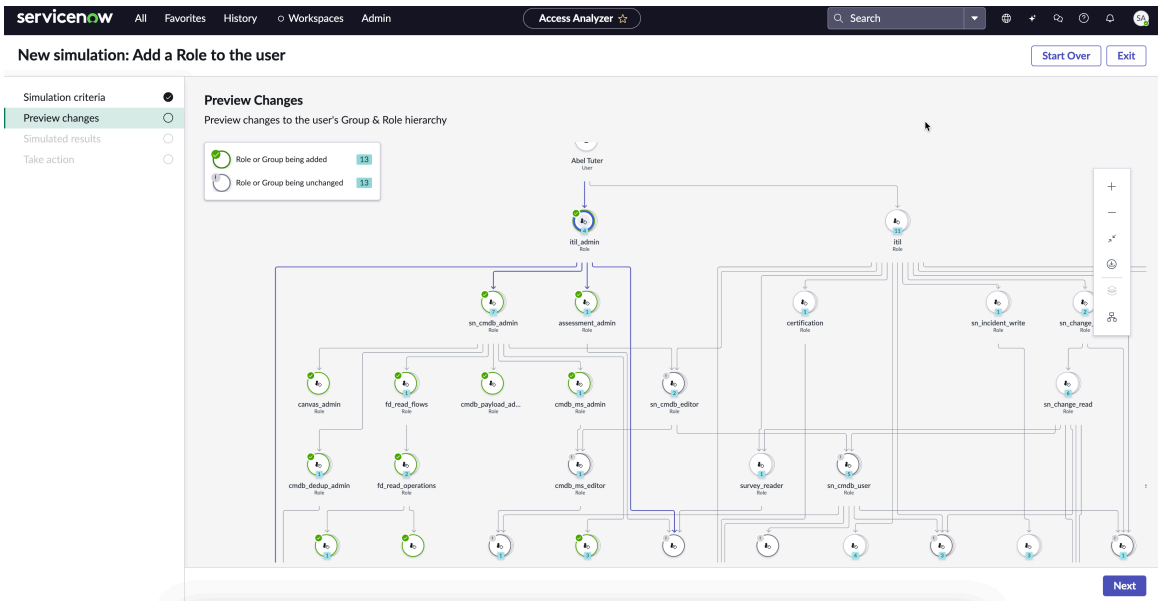
사용자에게 역할 추가

필드	설명
사용자 선택 *	목록에서 선택할 사용자 이름을 지정합니다. 이 예에서는 **Abel Tuter**입니다.
역할 선택 *	목록에서 선택할 역할을 지정합니다. 이 예에서는 **itil_admin**.
규칙 유형 *	규칙 유형은 자동으로 채워지며 변경할 수 없습니다.
테이블 선택 *	목록에서 선택할 테이블 이름을 지정합니다. 이 예시에서는 인시던트입니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다 (선택 사항).
필드 선택	목록에서 선택할 필드 이름을 지정합니다. 이 필드는 필드 수준에서도 권한을 분석하는 데 사용할 수 있습니다. 예를 들어 활성, 작성자 등이 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



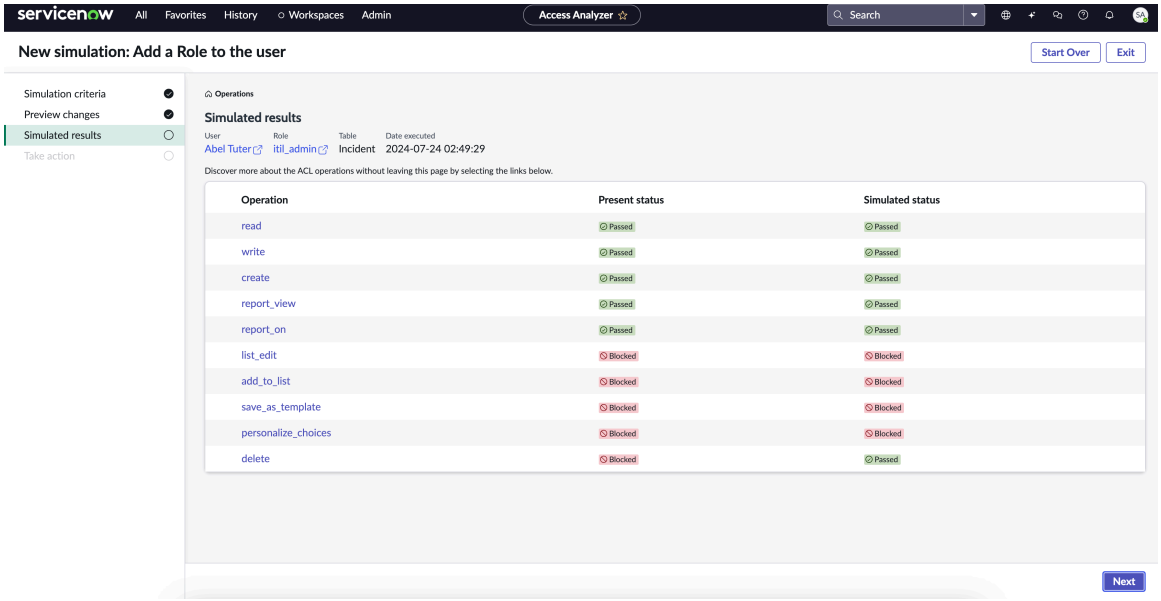
4. 다음을 선택합니다.
5. 변경 내용을 미리 봅니다.
   새로 할당된 역할은 변경 내용 미리 보기에서 시뮬레이션됩니다. 다음 단계로 이동하기 전에 사용자에게 추가되는 역할 및 하위 역할의 유효성을 확인할 수 있습니다.



역할의 일부로 추가되는 새 역할이 사용자의 기존 역할과 함께 표시되는 것을 볼 **itil_admin** .

6. 다음을 선택합니다.
7. 현재 상태 및 시뮬레이션됨 상태의 유효성을 검사하여 시뮬레이션된 사용자에게 전달되거나 차단된 액세스를 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

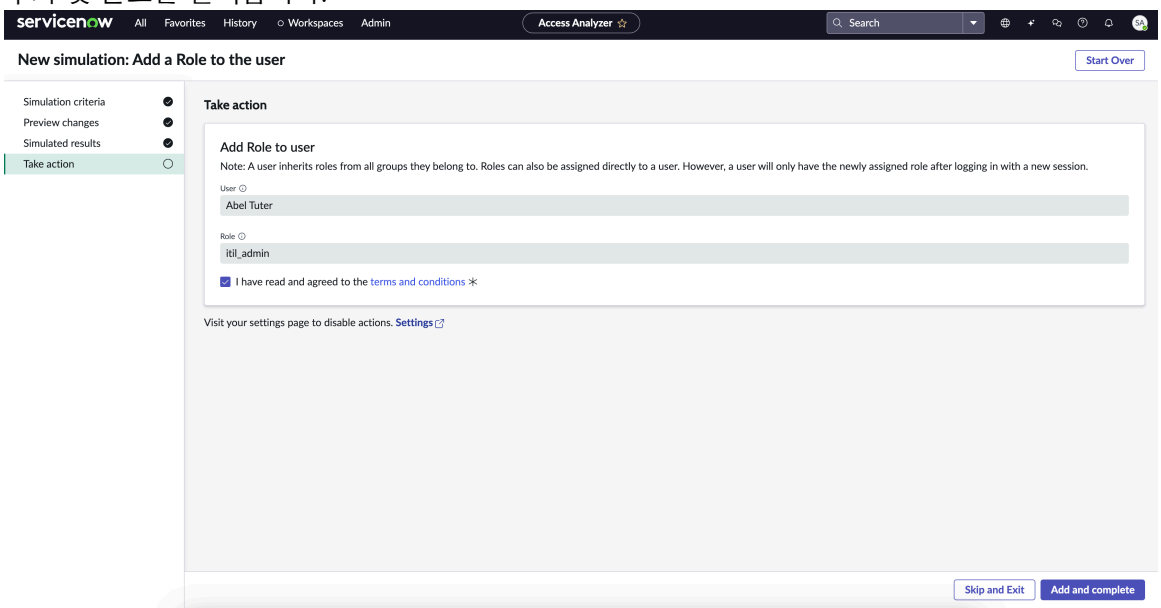


itil_admin 추가하면 사용자가 테이블(인시던트)에서 삭제 작업을 수행할 수 있습니다.

주:

- ACL(작업)에 대해 자세히 알아보려면 각 기록에 대한 작업 링크를 선택합니다.
- 다른 역할에 대해 시뮬레이션을 다시 시작하려면 다시 시작을 선택합니다.
- 시뮬레이션을 종료하려면 종료를 선택합니다.

8. 다음을 선택합니다.
9. 추가 및 완료를 선택합니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 액세스 시뮬레이터를 사용하도록 설정하지 않으면 시뮬레이션을 완료할 수 없습니다. 사용하려면 작업 사용을 선택하고 법무 정보를 수락합니다.
- 시뮬레이션을 숨기려면 작업 숨기기를 선택합니다. 숨기기를 해제하고 작업을 활성화하려면 설정으로 이동하십시오. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.
- 시뮬레이션을 종료하려면 건너뛰기 및 종료를 선택합니다.

역할이 사용자에게 성공적으로 추가됩니다. 액세스 분석기를 사용하여 액세스 권한을 확인할 수 있습니다. 사용자의 액세스를 확인하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 액세스 분석기.

사용자로부터 역할 제거

자원(테이블)에 대한 사용자의 접근 변경을 시뮬레이션하려면 역할 제거 시뮬레이션 을 사용합니다.

시작하기 전에

필요한 역할: admin, AA_admin

수행 작업을 활성화합니다. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.

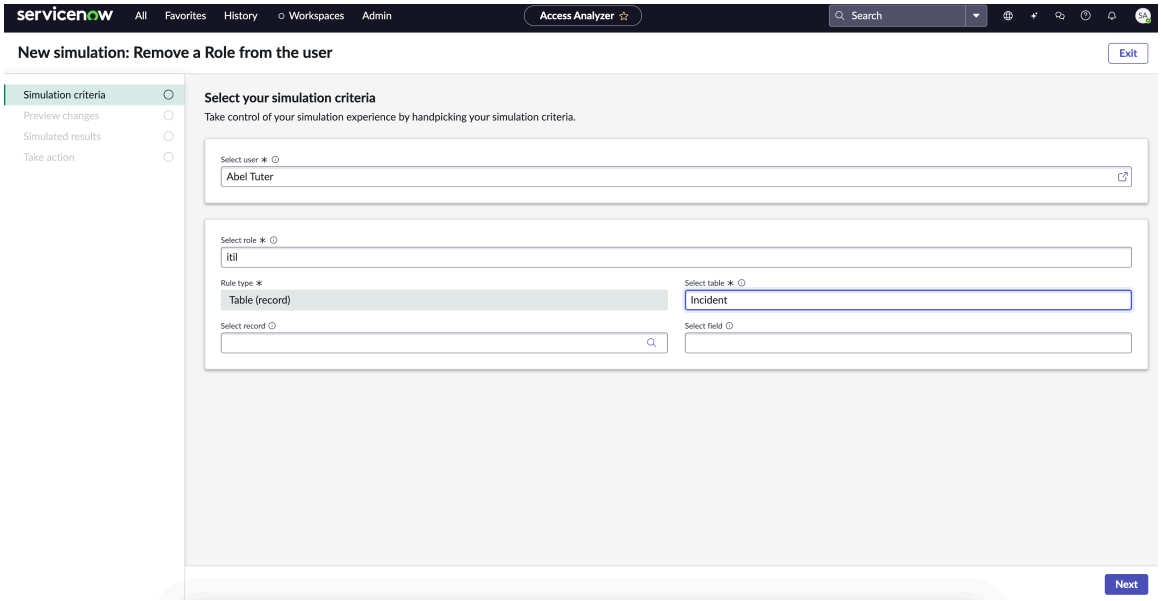
프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 액세스 시뮬레이터.
2. Remove a Role from the user 섹션에서 **Simulate** 를 선택합니다.
3. 시뮬레이션 기준에 대해 다음 필드를 지정합니다.

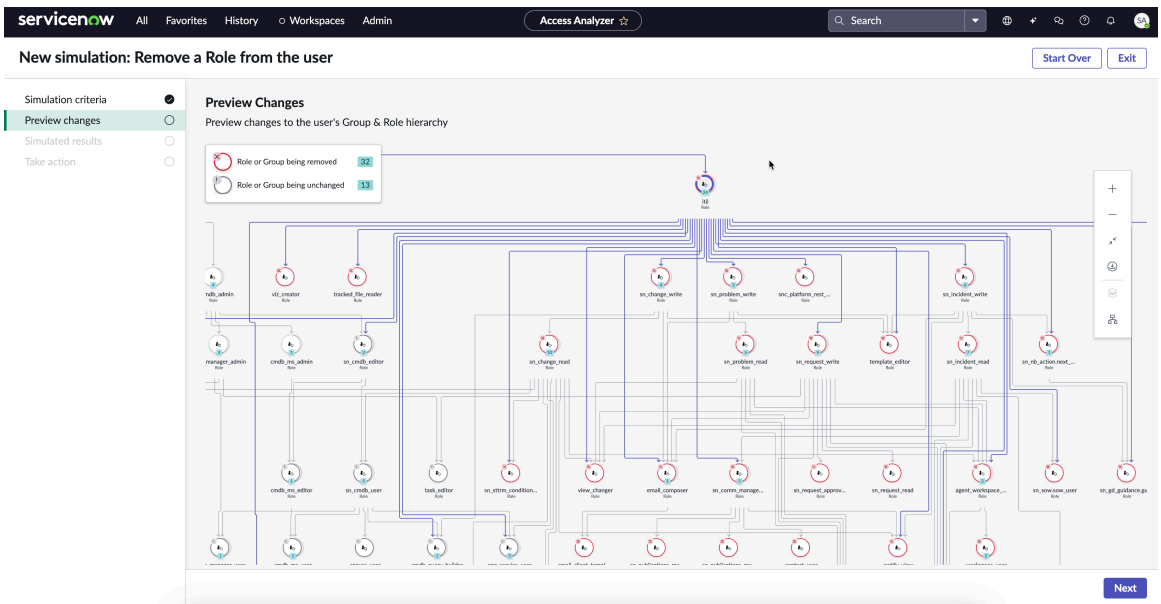
사용자에서 역할 제거

필드	설명
사용자 선택 *	목록에서 선택할 사용자 이름을 지정합니다. 이 예에서는 **Abel Tuter**입니다.
역할 선택 *	목록에서 선택할 역할을 지정합니다. 이 예에서는 **itil**입니다.
규칙 유형 *	규칙 유형은 자동으로 채워지며 변경할 수 없습니다.
테이블 선택 *	목록에서 선택할 테이블 이름을 지정합니다. 이 예시에서는 인시던트입니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다.
필드 선택	목록에서 선택할 필드 이름을 지정합니다. 이 필드는 필드 수준에서도 권한을 분석하는 데 사용할 수 있습니다. 예를 들어 활성, 작성자 등이 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

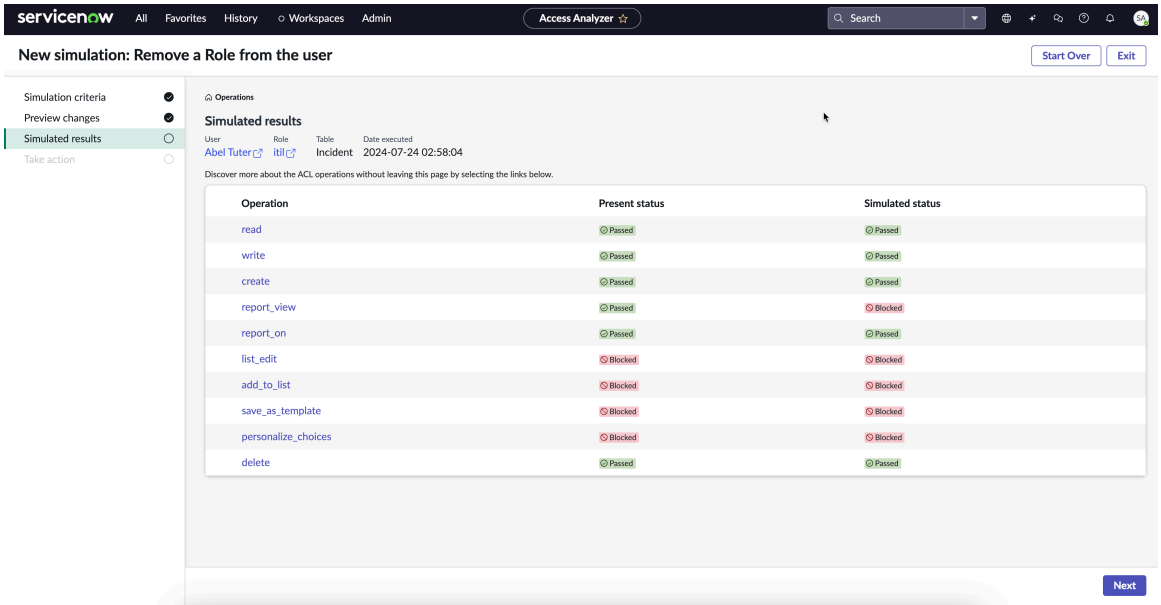


4. 다음을 선택합니다.
5. 변경 내용을 미리 봅니다.
   제거된 역할은 변경 내용 미리 보기에서 시뮬레이션됩니다. 다음 단계로 이동하기 전에 사용자에게 제거되는 역할 및 하위 역할의 유효성을 확인할 수 있습니다.



6. 다음을 선택합니다.
7. 현재 상태 및 시뮬레이션된 상태의 유효성을 검사하여 시뮬레이션된 사용자에게 전달되거나 차단된 액세스를 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:

- ACL(작업)에 대해 자세히 알아보려면 각 기록에 대한 작업 링크를 선택합니다.
- 다른 역할에 대해 시뮬레이션을 다시 시작하려면 다시 시작을 선택합니다.
- 시뮬레이션을 종료하려면 종료를 선택합니다.

8. 다음을 선택합니다.
9. 제거 및 완료를 선택합니다.

주:

- 액세스 시뮬레이터를 사용하도록 설정하지 않으면 시뮬레이션을 완료할 수 없습니다. 사용하려면 작업 사용을 선택하고 법무 정보를 수락합니다.
- 시뮬레이션을 숨기려면 작업 숨기기를 선택합니다. 숨기기를 해제하고 작업을 활성화하려면 설정으로 이동하십시오. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.
- 시뮬레이션을 종료하려면 건너뛰기 및 종료를 선택합니다.

역할이 사용자로부터 성공적으로 제거되었습니다. 액세스 분석기를 사용하여 액세스 권한을 확인할 수 있습니다. 사용자의 액세스를 확인하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오 액세스 분석기.

그룹에 사용자 추가

사용자가 그룹에 추가될 때 자원(테이블)에 대한 사용자의 접근 변경을 시뮬레이션하려면 그룹에 추가 시뮬레이션 을 사용합니다.

시작하기 전에

필요한 역할: admin, AA_admin

수행 작업을 활성화합니다. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.

프로시저

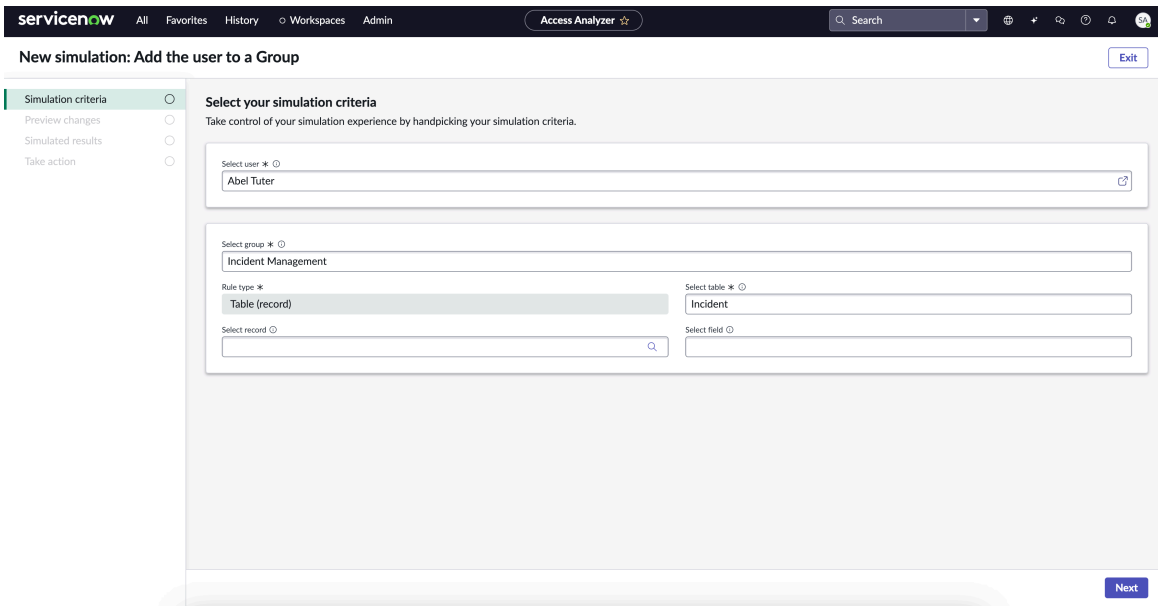
1. 다음으로 이동 모두 > 액세스 분석기 > 액세스 시뮬레이터.
2. 그룹에 사용자 추가 섹션에서 시뮬레이션 을 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

3. 시뮬레이션 기준에 대해 다음 필드를 지정합니다.

그룹에 사용자 추가

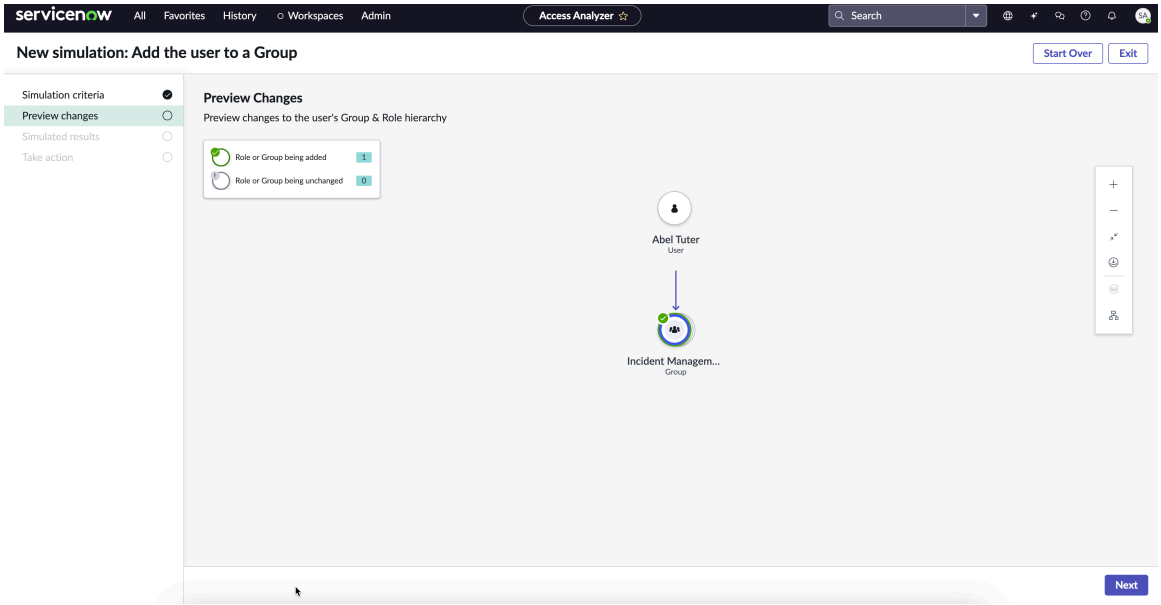
필드	설명
사용자 선택 *	목록에서 선택할 사용자 이름을 지정합니다. 이 예에서는 **Abel Tuter**입니다.
그룹 선택 *	목록에서 선택할 그룹을 지정합니다. 이 예에서는 **Incident Management**입니다.
규칙 유형 *	규칙 유형은 자동으로 채워지며 변경할 수 없습니다.
테이블 선택 *	목록에서 선택할 테이블 이름을 지정합니다. 이 예시에서는 인시던트입니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다.
필드 선택	목록에서 선택할 필드 이름을 지정합니다. 이 필드는 필드 수준에서도 권한을 분석하는 데 사용할 수 있습니다. 예를 들어 활성, 작성자 등이 있습니다.



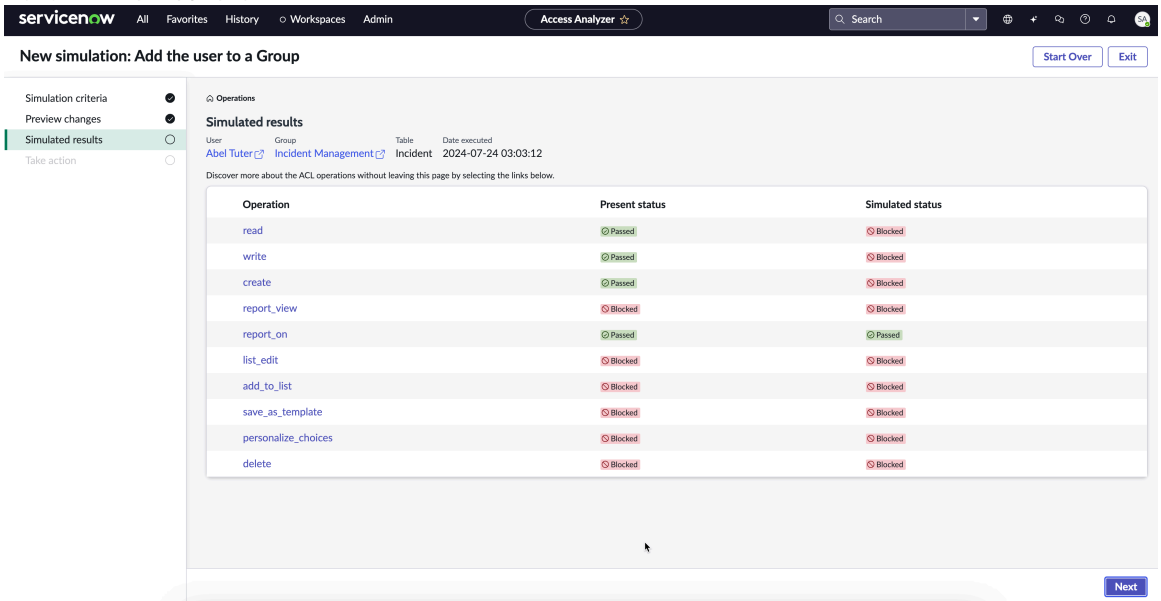
4. 다음을 선택합니다.
5. 변경 내용을 미리 봅니다.

   사용자가 할당된 그룹은 변경 내용 미리 보기에서 시뮬레이션됩니다. 다음 단계로 이동하기 전에 변경 내용을 확인할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 다음을 선택합니다.
7. 현재 상태 및 시뮬레이션된 상태의 유효성을 검사하여 시뮬레이션된 사용자에게 전달되거나 차단된 액세스를 확인합니다.



주:

- ACL(작업)에 대해 자세히 알아보려면 각 기록에 대한 작업 링크를 선택합니다.
- 다른 역할에 대해 시뮬레이션을 다시 시작하려면 다시 시작을 선택합니다.
- 시뮬레이션을 종료하려면 종료를 선택합니다.

8. 다음을 선택합니다.
9. 추가 및 완료를 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 액세스 시뮬레이터를 사용하도록 설정하지 않으면 시뮬레이션을 완료할 수 없습니다. 사용하려면 작업 사용을 선택하고 법무 정보를 수락합니다.
- 시뮬레이션을 숨기려면 작업 숨기기를 선택합니다. 숨기기를 해제하고 작업을 활성화하려면 설정으로 이동하십시오. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.
- 시뮬레이션을 종료하려면 건너뛰기 및 종료를 선택합니다.

사용자가 그룹에 성공적으로 추가되었습니다.

그룹에서 사용자 제거

사용자가 그룹에서 제거될 때 자원(테이블)에 대한 사용자의 접근 변경을 시뮬레이션하려면 그룹에서 제거 시뮬레이션 을 사용합니다.

시작하기 전에

필요한 역할: admin, AA_admin

수행 작업을 활성화합니다. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.

프로시저

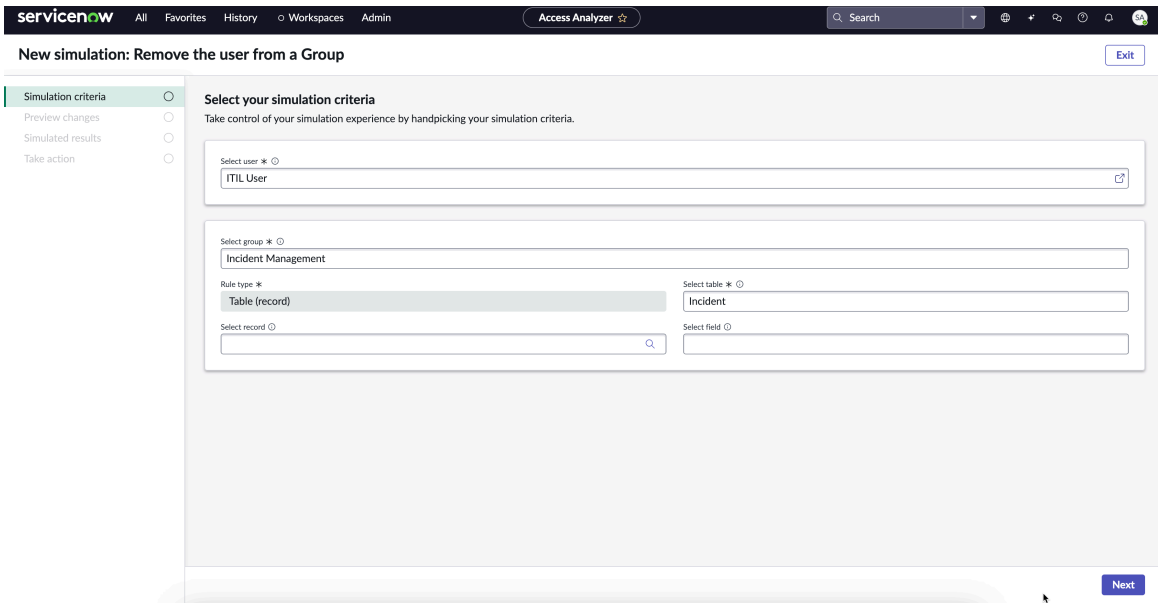
1. 다음으로 이동 모두 > 액세스 분석기 > 액세스 시뮬레이터.
2. 그룹에서 사용자 제거 섹션에서 시뮬레이션 을 선택합니다.
3. 시뮬레이션 기준에 대해 다음 필드를 지정합니다.

그룹에서 사용자 제거

필드	설명
사용자 선택 *	목록에서 선택할 사용자 이름을 지정합니다. 이 예에서는 **ITIL** 사용자입니다.
그룹 선택 *	목록에서 선택할 그룹을 지정합니다. 이 예에서는 **Incident Management**입니다.
규칙 유형 *	규칙 유형은 자동으로 채워지며 변경할 수 없습니다.
테이블 선택 *	목록에서 선택할 테이블 이름을 지정합니다. 이 예시에서는 인시던트입니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다.
필드 선택	목록에서 선택할 필드 이름을 지정합니다. 이 필드는 필드 수준에서도 권한을 분석하는 데 사용할 수 있습니다. 예를 들어 활성, 작성자 등이 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

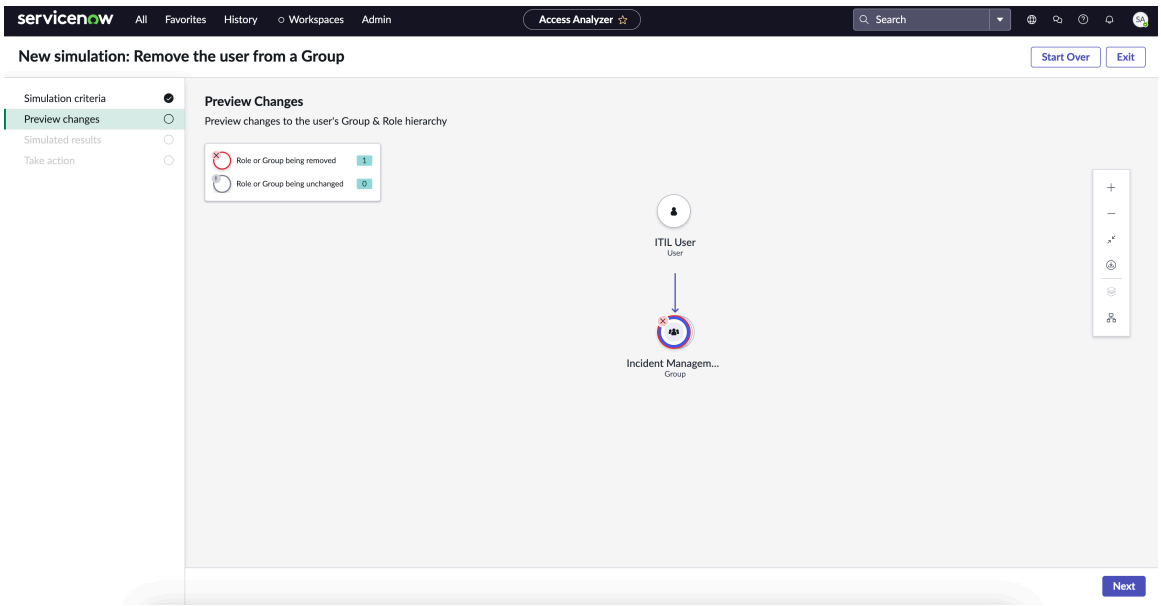
d



4. 다음을 선택합니다.

5. 변경 내용을 미리 봅니다.

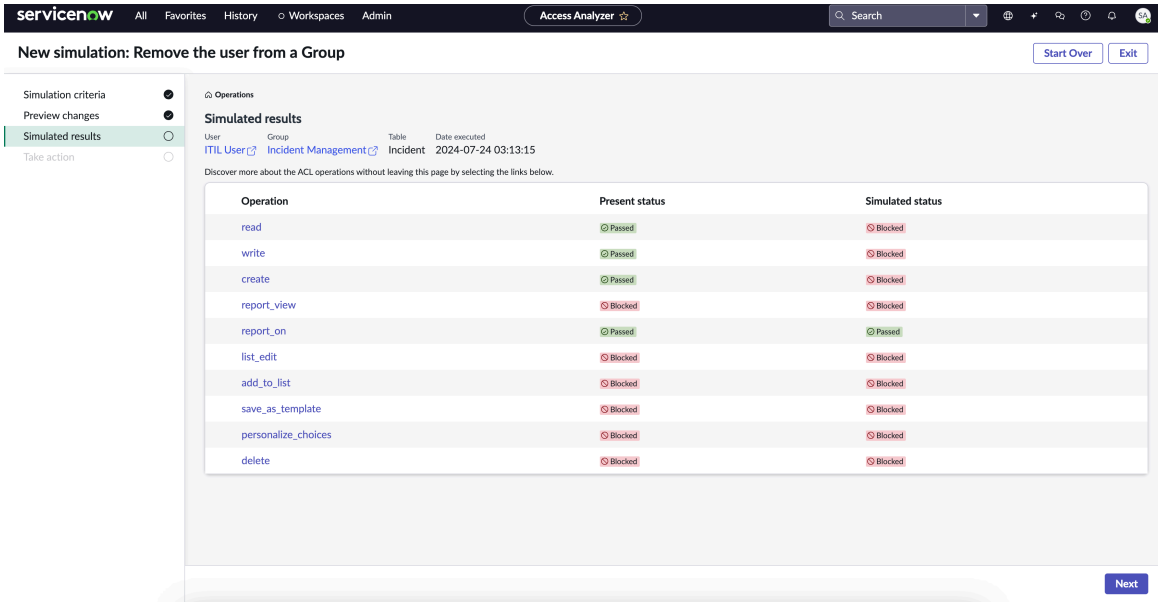
사용자가 제거되는 그룹은 변경 내용 미리 보기에서 시뮬레이션됩니다. 다음 단계로 이동하기 전에 변경 내용을 확인할 수 있습니다.



6. 다음을 선택합니다.

7. 현재 상태 및 시뮬레이션됨 상태의 유효성을 검사하여 시뮬레이션된 사용자에게 전달되거나 차단된 액세스를 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



주:

- ACL(작업)에 대해 자세히 알아보려면 각 기록에 대한 작업 링크를 선택합니다.
- 다른 역할에 대해 시뮬레이션을 다시 시작하려면 다시 시작을 선택합니다.
- 시뮬레이션을 종료하려면 종료를 선택합니다.

8. 다음을 선택합니다.
9. 제거 및 완료를 선택합니다.

주:

- 액세스 시뮬레이터를 사용하도록 설정하지 않으면 시뮬레이션을 완료할 수 없습니다. 사용하려면 작업 사용을 선택하고 법무 정보를 수락합니다.
- 시뮬레이션을 숨기려면 작업 숨기기를 선택합니다. 숨기기를 해제하고 작업을 활성화하려면 설정으로 이동하십시오. 자세한 내용은 액세스 시뮬레이터 구성(작업 수행) 문서를 참조하십시오.
- 시뮬레이션을 종료하려면 건너뛰기 및 종료를 선택합니다.

사용자가 사용자에서 성공적으로 제거되었습니다.

자주 묻는 질문

액세스 시뮬레이터 사용에 대해 자주 묻는 질문입니다.

자주 묻는 질문

질문	설명
시뮬레이터를 시작하려면 어떻게 해야 합니까?	사용자에 대해 시뮬레이션하려는 다양한 시나리오에 대해 시뮬레이션 옵션을 선택하고 단계를 수행할 수 있습니다.
시뮬레이터는 어떻게 작동합니까?	액세스 시뮬레이터는 선택된 사용자에게 지정된 테이블에 대한 액세스를 시뮬레이션하고 액세스 변경을 미리 확인하여 액세스 프로비저닝에 대한 결정을 내릴 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자주 묻는 질문

질문	설명
시뮬레이터에서 작업을 활성화하거나 비활성화하는 방법은 무엇입니까?	설정으로 이동하거나 시뮬레이션 프로세스의 작업 수행 단계에서 액세스 시뮬레이터에서 동작을 활성화 또는 비활성화할 수 있습니다.

액세스 인사이트

액세스 인사이트는 역할 또는 그룹 할당에 대한 확신을 얻는 데 도움이 됩니다.

탐색



액세스 인사이트의 기능 및 비즈니스 가치에 대해 알아봅니다.

구성



액세스 인사이트 구성 방법을 이해합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

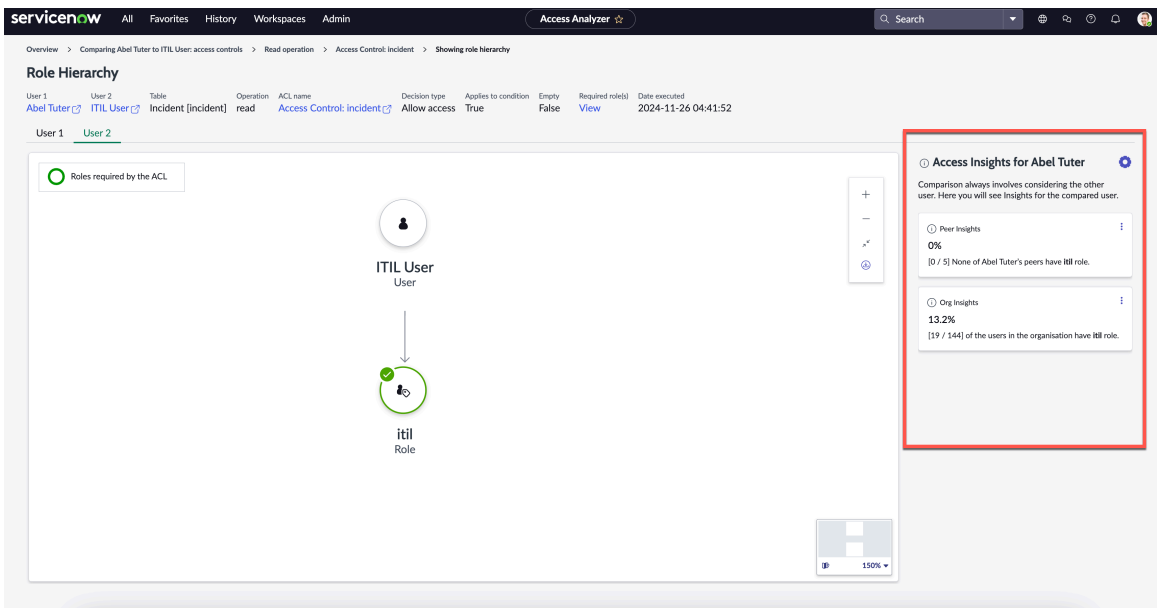
사용	
	
액세스 인사이트 사용 방법을 알고 있습니다.	

액세스 인사이트 탐색

액세스 분석기의 액세스 인사이트는 역할 또는 그룹 할당에 대한 확신을 얻는 데 도움이 됩니다.

액세스 인사이트는 자원에 대한 사용자의 동료 및 조직 수준 액세스 통계를 표시합니다. 이를 통해 현재 추가 권리를 검토하고 있는 사용자에게 역할 또는 그룹을 할당할 수 있는지 확인할 수 있습니다. 이는 동일한 동료 그룹 내에서 역할 및 그룹 할당을 비교하는 데 도움이 됩니다.

액세스 인사이트는 액세스 분석기의 사용자 액세스 비교 기능을 사용하여 사용자의 액세스를 비교하는 동안에만 표시됩니다. 액세스 인사이트 사용에 대한 자세한 내용은 다음 문서를 참조하십시오 액세스 인사이트 사용.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

통계를 기반으로 동료 내에서 비교하는 사용자에게 올바른 역할 또는 그룹 할당을 제공하도록 결정할 수 있습니다.

주:

- 액세스 인사이트는 액세스 분석기 V4에서 사용할 수 있습니다.
- 액세스 인사이트 기능 내에서 통계를 보면서 동료 수준(동일한 조직, 동일한 부서, 동일한 관리자)에서 사용자를 비교해야 합니다.

액세스 분석기에서 액세스 인사이트를 활성화하려면 설정으로 이동해야 합니다. 자세한 내용은 액세스 인사이트 구성 문서를 참조하십시오.

액세스 인사이트 구성

액세스 분석기에서 액세스 인사이트 기능을 활성화합니다.

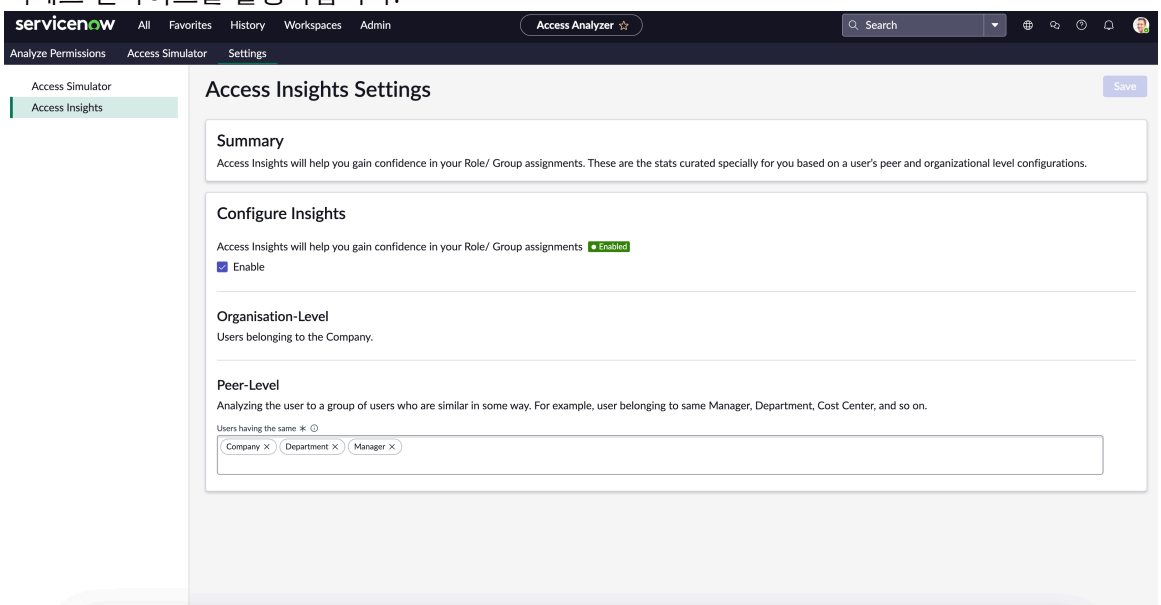
시작하기 전에

필요한 역할: admin, AA_admin

다음 절차에서는 액세스 인사이트를 활성화하는 단계를 설명합니다.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 액세스 분석.
2. 설정 탭을 선택합니다.
3. 액세스 인사이트를 선택합니다.
4. 액세스 인사이트를 활성화합니다.



주: 기본적으로 동료 수준 필드는 회사, 부서, 관리자와 함께 선택됩니다. 비용 센터, 국가 코드, 위치 및 제목과 같은 필드를 더 추가할 수 있습니다.

5. 저장을 선택합니다.

결과

액세스 인사이트 기능은 자원에 대한 사용자 액세스를 비교하는 동안 역할 계층 구조를 볼 때 활성화되고 표시됩니다. 액세스 인사이트 사용에 대한 자세한 내용은 다음 문서를 참조하십시오 액세스 인사이트 사용.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

액세스 인사이트 사용

액세스 인사이트를 사용하여 선택한 자원에 대한 사용자 피어 수준 액세스를 이해합니다.

시작하기 전에

필요한 역할: admin, AA_admin

주: 액세스 인사이트 기능에 대한 자세한 내용을 보려면 사용자 액세스 비교 기능을 사용해야 합니다.

다음 절차에서는 액세스 인사이트 기능 내에서 피어 수준 역할 또는 그룹 할당 통계를 보는 단계를 설명합니다.

프로시저

1. 다음으로 이동 모두 > 액세스 분석기 > 권한 분석.
   액세스 및 권한 분석 홈페이지가 표시됩니다.
2. 사용자 액세스 비교 탭을 선택합니다.
3. 다음 필드를 채웁니다.

사용자 액세스 비교

필드	설명
사용자 1* 선택	비교할 목록에서 선택할 사용자 이름을 지정합니다.
사용자 2* 선택	목록에서 선택하여 사용자와 비교할 사용자 이름을 지정합니다 1.
규칙 유형*	테이블에 대한 액세스 권한을 분석합니다. 주: 테이블에 대한 액세스 권한만 사용자 비교 액세스에 사용할 수 있습니다.
테이블 선택*	목록에서 선택할 테이블 이름을 지정합니다.
기록 선택	목록에서 선택할 기록 이름을 지정합니다.
필드 선택	목록에서 선택할 필드 이름을 지정합니다.

4. 사용자 액세스 비교를 선택합니다.

   선택한 사용자에 대한 사용자 액세스 비교 결과가 표시됩니다.

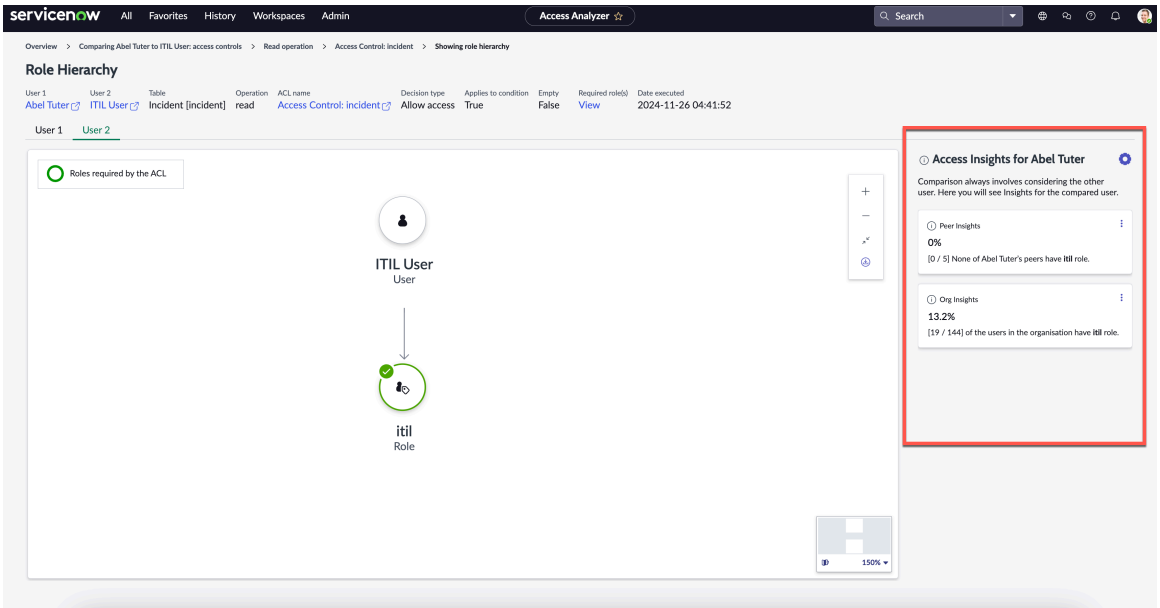
   사용자 액세스 비교 결과에는 사용자에 대한 작업 및 액세스 평가 상태가 표시됩니다. 예를 들어 Abel Tuter 및 ITIL 사용자가 있습니다.

5. 운영을 선택합니다.
   예를 들어 읽기 작업입니다.
6. 액세스 제어를 선택하여 액세스에 대해 자세히 알아보십시오.
7. 역할 계층 구조 표시를 선택하여 피어 수준 액세스에서 액세스 비교를 봅니다.

   액세스 인사이트는 다음과 같이 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 동료 인사이트: 동료(동일한 관리자 또는 부서) 내에서 동일한 역할이 할당된 사용자 수를 표시합니다.
- 조직 인사이트: 조직 내에서 동일한 역할이 할당된 사용자 수를 표시합니다.



이 정보를 기반으로 비교한 사용자에게 액세스 권한을 제공하거나 취소하도록 선택할 수 있습니다.

전역 ID

Global Identity는 ServiceNow® 여러 인스턴스에서 고유 사용자를 식별할 수 있는 제품입니다.

Global Identity는 여러 ServiceNow® 인스턴스에서 사용자, 해당 속성, 기타 기초 데이터를 ServiceNow® 관리하는 데 도움이 됩니다.

페더레이션 ID 탐색



페더레이션 ID 액세스



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Federated ID의 주요 기능 및 비즈니스 가치를 알아봅니다.	페더레이션 ID에 액세스합니다.
ID 필드 업데이트  페더레이션 ID를 업데이트하고 설정합니다.	

페더레이션 **ID** 탐색

사용자 이름과 이메일을 기반으로 여러 인스턴스에서 사용자를 결정하고 여러 인스턴스에서 사용자에게 고유 ID(페더레이션 ID)를 제공합니다.

페더레이션 ID는 여러 ServiceNow® 인스턴스에서 사용자를 식별하는 데 사용됩니다. 페더레이션 ID를 기반으로 사용자를 식별하고 여러 인스턴스에서 정확한 사용자 수를 결정할 수 있습니다. 자세한 내용은 Federated ID를 참조하십시오.

주: 페더레이션 ID를 작성하려면 사용자 이름이 필요합니다.

페더레이션 ID는 여러 인스턴스에서 해시 함수를 사용하는 자격 증명의 고유 식별자입니다 ServiceNow® .

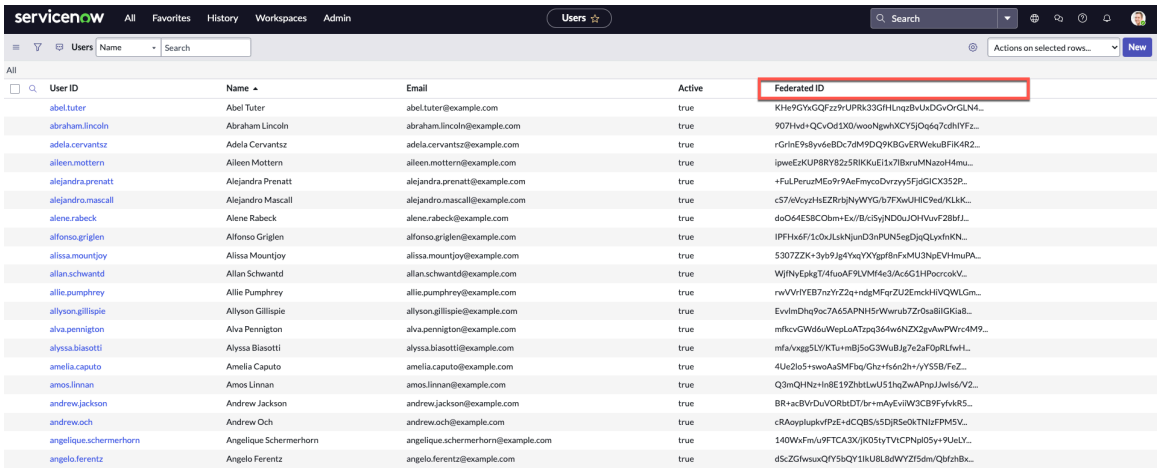
인스턴스 전체에서 사용자의 사용자 **ID** 와 이메일을 사용하여 페더레이션 ID가 생성되어 sys_user 테이블에 표시됩니다.

릴리스로 Yokohama 업그레이드하면 페더레이션 ID 생성(`com.glide.identity.globalid`) 플러그인이 모든 인스턴스에 자동으로 설치됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- 페더레이션 ID를 작성하려면 사용자 이름이 필요합니다.
- 사용자 이름과 이메일은 기본적으로 페더레이션 ID를 생성하는 데 사용됩니다. 요구 사항에 따라 페더레이션 ID를 생성하기 위한 필드를 업데이트하려면 다음 문서를 참조하십시오 ID 필드 업데이트.
- 구성을 업데이트하려면 **Iamsync_admin** 역할이 필요합니다.
- 중복된 사용자 이름과 이메일을 가진 사용자가 있는 경우 한 사용자에 대해서만 페더레이션 ID가 생성됩니다. 사용자 이름이 null이거나 비어 있는 경우 페더레이션 ID는 null입니다.



플러그인 설치 후의 스키마 변경 사항은 다음과 같습니다.

- `sys_user` 테이블에 새 열 federated_id이 생성됩니다.
- 새 테이블 - `iamsync_typesys_user` 테이블의 기본 구성으로 자동으로 채워집니다.

페더레이션 ID는 `sys_user` 테이블과 sys_user 테이블을 확장하는 모든 테이블에 대해서만 지원됩니다.

릴리스로 Yokohama 업그레이드하면 페더레이션 ID 생성(`com.glide.identity.globalid`) 플러그인이 모든 인스턴스에 자동으로 설치됩니다.

페더레이션 ID 기준 액세스

페더레이션 ID 기준에 액세스하여 페더레이션 ID를 생성하는 데 사용되는 ID 필드에 대해 알 수 있습니다.

시작하기 전에
필요한 역할: iamsync_admin

프로시저

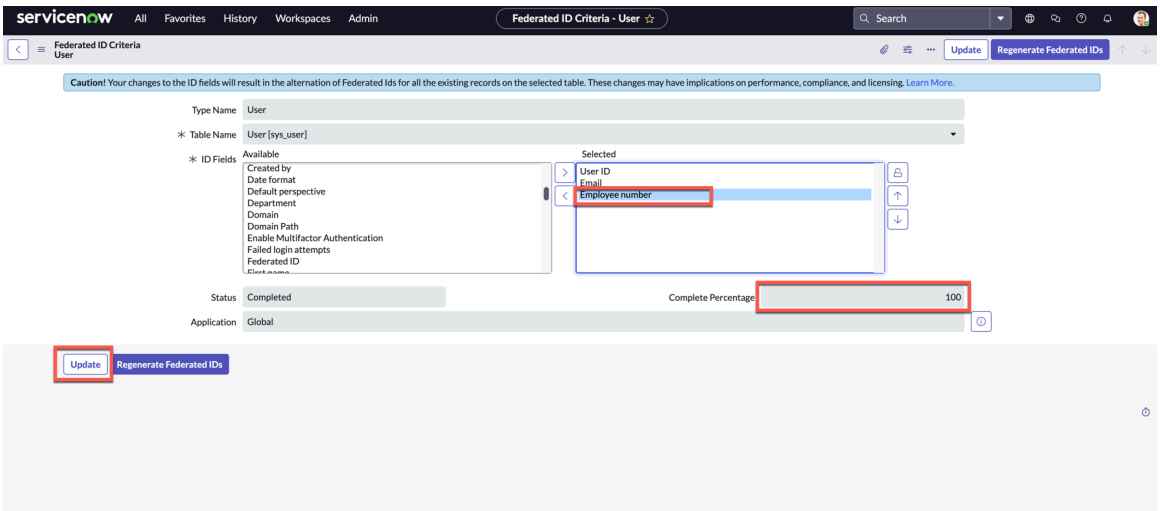
1. 다음으로 이동 모두 > 페더레이션 **ID** 관리 > 페더레이션 **ID** 기준.
2. 페더레이션 ID 기준 페이지에는 다음 상세 정보가 포함된 기록이 표시됩니다.
   - 유형 이름: 사용자
   - 테이블 이름: 사용자 **[sys_user]**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- ID 필드: user_name(사용자 **ID)**, 이메일 (페더레이션 ID 작성에 사용되는 기본 필드).
- 상태: 완료 됨(페더레이션 ID 생성 상태). 사용 가능한 상태: 준비, 실행 중, 완료됨, 오류.

주:

- 페더레이션 ID를 작성하려면 사용자 이름이 필요합니다.
- 사용자 이름과 이메일은 기본적으로 페더레이션 ID를 생성하는 데 사용됩니다.



주: ID 필드만 업데이트하여 기존 기록에 대한 새 페더레이션 ID를 생성할 수 있습니다. 자세한 내용은 를 참조하십시오 ID 필드 업데이트.

ID 필드 업데이트

ID 필드를 업데이트하여 업데이트된 필드를 기반으로 페더레이션 ID를 재생성합니다.

시작하기 전에
필요한 역할: iamsync_admin

주: ID 필드를 변경하면 선택한 테이블의 모든 기존 기록에 대한 페더레이션 ID가 변경됩니다. 이러한 변경 사항은 성능, 규정 준수 및 라이선싱에 영향을 미칠 수 있습니다.

프로시저

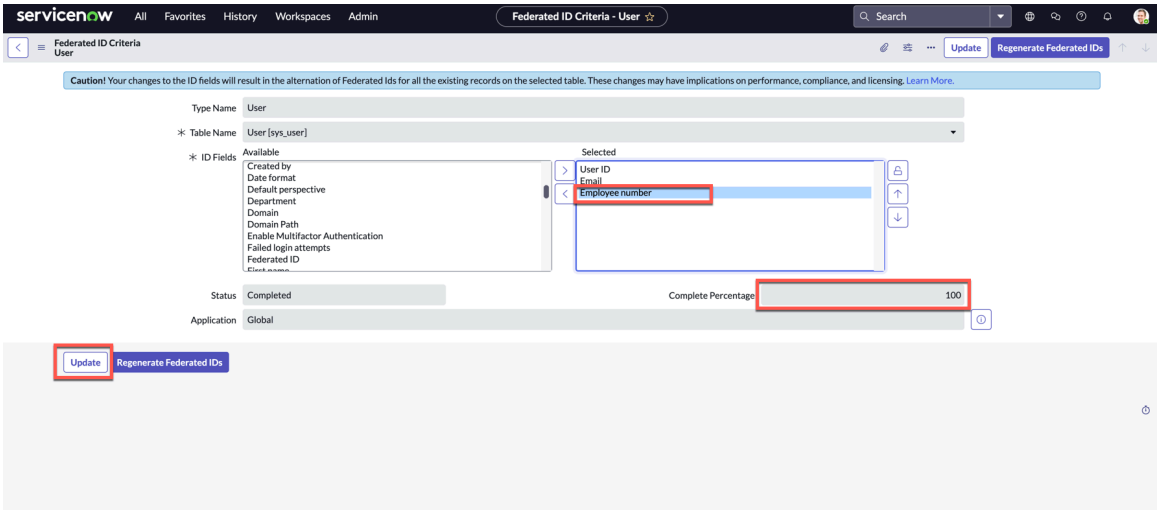
1. 다음으로 이동 모두 > 페더레이션 **ID** 관리 > 페더레이션 **ID** 기준.
2. 유형 이름(사용자)을 선택합니다.
3. 페더레이션 ID 기준 사용자 페이지에서 화살표 버튼을 사용하여 사용 가능 항목에서 선택할 수 있는 항목에서 추가할 새 ID 필드를 선택합니다.

   예: 직원 번호

주:

- 페더레이션 ID를 작성하려면 사용자 이름이 필요합니다.
- 사용자 이름과 이메일은 기본적으로 페더레이션 ID를 생성하는 데 사용됩니다.
- 중복된 사용자 이름과 이메일을 가진 사용자가 있는 경우 한 사용자에 대해서만 페더레이션 ID가 생성됩니다. 사용자 이름이 null이거나 비어 있는 경우 페더레이션 ID는 null입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



이제 선택한 직원 번호는 페더레이션 ID를 생성하기 위한 또 다른 속성이 됩니다.

4. 업데이트를 선택하여 페더레이션 ID를 생성합니다.

   주: 먼저 업데이트를 선택한 다음 다른 업데이트를 시작하기 전에 완료율(100)을 확인합니다.

   상태 백분율은 인스턴스 전반의 모든 ID에 대한 페더레이션 ID 생성을 나타냅니다.

   주:

   - 이전 업데이트 작업이 완료될 때까지 필드를 변경하지 마십시오.
   - 업데이트되는 필드는 문자열 유형이어야 합니다.
   - ID 필드로 선택할 수 없는 필드는 다음과 같습니다.
     - 시스템 수준 필드
     - 에지 암호화 규칙 필드
     - 암호 필드입니다.

5. sys_user 테이블로 이동하여 ID 필드 업데이트로 인해 생성된 새 페더레이션 ID를 확인합니다.

   주: XML 임포트, 하위 수준 데이터베이스 업데이트, 인스턴스가 제대로 작동하지 않는 경우 사용자가 생성되거나 업데이트되는 경우 페더레이션 **ID** 재생성을 선택합니다. 페더레이션 **ID** 재생성을 선택하면 현재 ID 필드 기준을 사용하여 모든 사용자의 ID가 재생성됩니다.

ID 센터

ID 기반 위험 및 보안 격차를 모니터링, 관리 및 최소화할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색



ID 센터의 기능 및 비즈니스 가치에 대해 알아봅니다.

활성화



ID 센터를 활성화하는 방법을 이해합니다.

관리자용 ID 메트릭



권한이 평가되는 방식을 알고 있습니다.

사용자를 위한 ID 센터



액세스 분석기에 대해 자주 묻는 질문에 대한 상세 정보를 확인합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ID 센터 탐색

Identity Center는 사용자 속성, 액세스, 장치, 로그인 기록, 보안 활동 등의 모음입니다.

Identity Center는 ID 기반 위험 및 보안 격차를 모니터링, 관리 및 최소화하는 기능을 제공합니다.

ID 센터는 에서 ID 기반 위험 및 보안 격차를 ServiceNow모니터링, 관리 및 최소화하는 원스톱 서비스입니다.

ID 센터를 활성화하려면 ID 센터(`com.snc.identity_center`) 플러그인을 설치합니다. 최종 사용자는 Identity Center를 사용하여 활성 세션, 로그인 기록 및 신뢰할 수 있는 장치에 대한 세부 정보를 볼 수 있습니다. 자세한 내용은 사용자를 위한 ID 센터 문서를 참조하십시오.

ID 센터 활성화

ID 센터의 경우 ID 센터(`com.snc.identity_center`) 플러그인을 설치합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 Identity Center(`com.snc.identity_center`) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

   주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 `<#### ##># ## #### ### ### ## #### ###### ### ### # ####`라는 오류가 나타납니다.

   설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

사용자를 위한 ID 센터

ID 센터에서 활성 세션, 로그인 기록 및 신뢰할 수 있는 장치에 대한 세부 정보를 봅니다.

Identity Center는 사용자 속성, 장치, 로그인 기록, 보안 활동 등의 모음입니다. 추가 보안 제어 및 알림 기능과 함께 모든 데이터에 대한 단일 창 보기를 제공합니다.

ID 센터를 사용하면 활성 세션, 로그인 기록 및 신뢰할 수 있는 장치에 대한 세부 정보를 볼 수 있습니다.

사용자를 위한 ID 센터에 액세스하려면 다음 중 하나로 이동합니다.

- 에서 Now Platform다음으로 이동 모두 > 셀프 서비스 > 내 프로필 을 클릭하고 관련 링크 섹션에서 **ID 센터 보기**를 선택합니다.

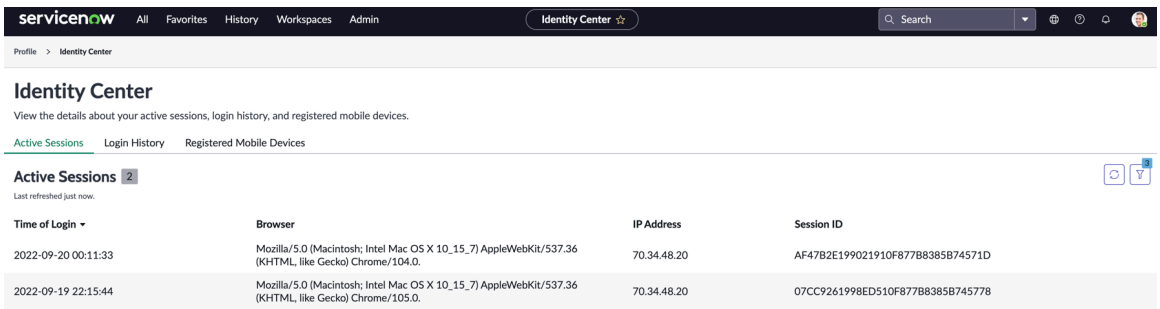
  주: 인스턴스 헤더에서 사용자 이름을 선택하여 프로파일에 액세스할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



- 에서 Now Support프로필을 선택하고 페이지 아래쪽에서 **ID** 센터 보기를 선택합니다.

ID 센터 페이지는 다음과 같이 표시됩니다.



ID 센터에는 다음 탭이 있습니다.

- 활성 세션
- 로그인 이력
- 등록된 모바일 장치

이 탭을 선택하여 브라우저, IP 주소, 세션 관계 정보, 로그인 정보, 등록된 모바일 장치와 같은 세부 정보를 볼 수 있습니다.

활성 세션 보기

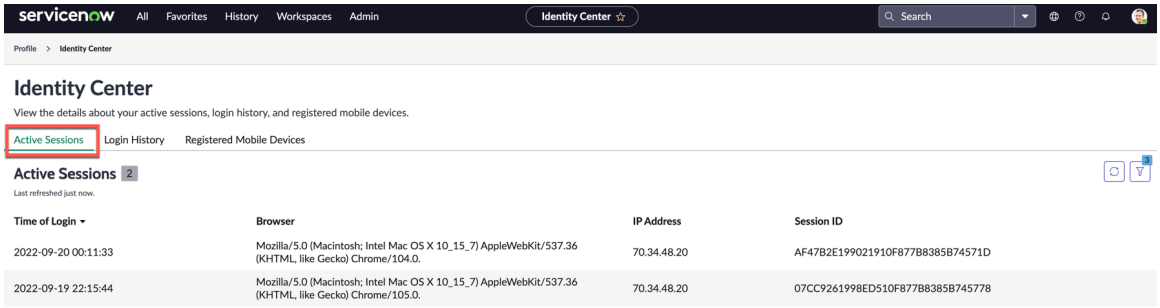
사용자 세션에 대한 정보를 표시합니다.

활성 세션은 현재 ServiceNow® 인스턴스에 여러 브라우저나 장치를 사용하여 열려 있는 세션입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

Identity Center(ID 센터)의 Active Sessions(활성 세션) 탭을 사용하면 브라우저, IP 주소 및 세션 ID를 기반으로 세션을 식별할 수 있습니다. 이 정보를 사용하여 세션 연장 또는 종료와 같은 필요한 작업을 수행할 수 있습니다.

이 정보를 사용하면 세션이 실제이고 보안 문제가 없는지 확인하는 데 도움이 될 수 있습니다.



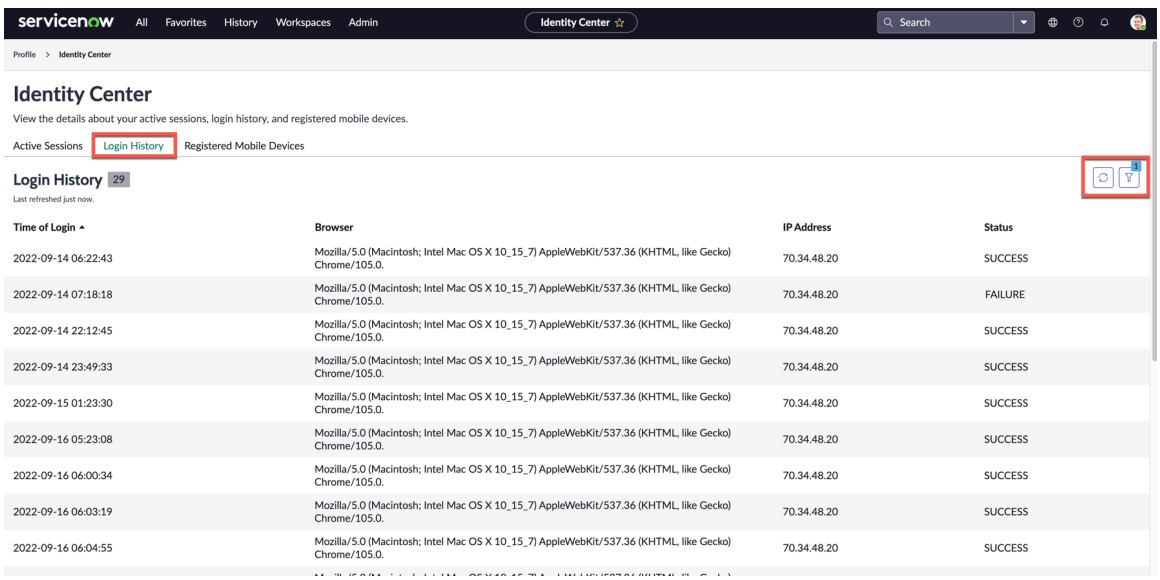
로그인 이력 조회

로그인 이력에 대한 세부 정보를 제공합니다.

Identity Center의 Login History(로그인 기록) 탭에서는 로그인 정보와 로그인 상태를 확인할 수 있습니다.

필터를 사용하여 보안 조사에 도움이 되는 로그인 작업을 지정할 수 있습니다. 필터링을 통해 활동이 진짜인지 의심스러운지 확인하고 관리자에게 정보를 보고할 수 있습니다.

로그인 기록의 페이지 매김은 기본적으로 20이며 최대 100까지 설정할 수 있습니다.



다음은 로그인 기록의 다른 세부 정보 중 일부입니다.

- 로그인 시간은 모바일 장치가 인스턴스에 액세스하는 데 사용될 때 업데이트된 시간입니다.
- 레코드는 30일 동안 ID 센터에 저장됩니다.

등록된 모바일 장치 보기

인스턴스에 등록된 모바일에 ServiceNow 대한 상세 정보를 제공합니다.

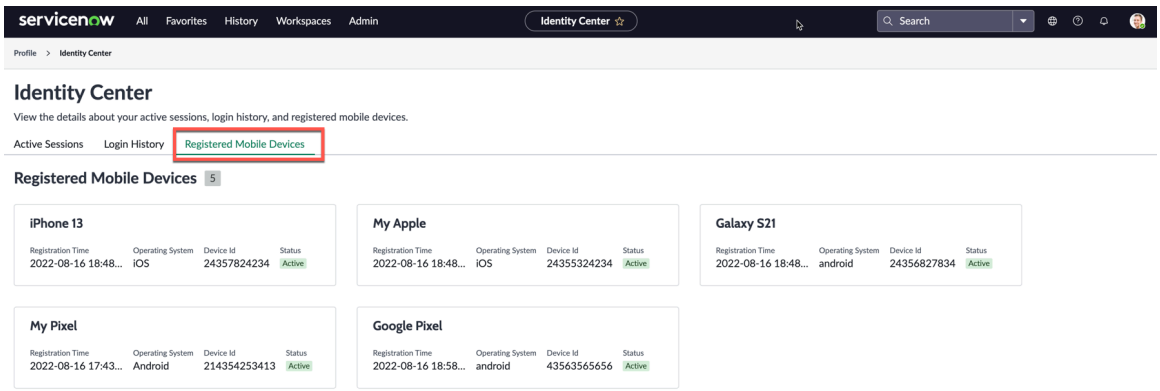
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

ID 센터의 등록된 모바일 장치 탭에는 인스턴스에 액세스하는 ServiceNow 데 사용된 등록된 장치에 대한 세부 정보가 표시됩니다.

적응형 인증 모듈이 활성화되고 등록된 모바일 장치가 등록된 경우 ID 센터에 등록된 장치에 대한 세부 정보가 표시됩니다.

또한 장치의 등록 시간과 함께 운영 체제, 장치 ID 및 장치 상태와 같은 장치의 세부 정보도 표시합니다.

모바일 장치를 등록하려면 적응형 인증(*com.snc.adaptive_authentication*) 플러그인이 설치되어 있고 신뢰할 수 있는 모바일 앱 기능이 활성화되어 있는지 확인해야 합니다. 자세한 내용은 신뢰할 수 있는 모바일 앱 활성화 문서를 참조하십시오.



관리자용 ID 메트릭

인스턴스의 사용자, 권한 있는 사용자, 활성 세션 및 통합 계정의 추세를 ServiceNow 봅니다.

관리자용 ID 메트릭에는 다음에 대한 추세가 있습니다.

- 사용자
- 권한 있는 사용자
- 통합 또는 비인간 계정
- 활성 세션
- 비활성 세션

자세한 내용은 보안 센터 메트릭을 참조하세요.

SCIM(교차 도메인 ID 관리 시스템)

SCIM(System for Cross-domain Identity Management) API는 SCIM 프로토콜을 사용하여 사용자 및 그룹에 대한 작업을 만들고, 읽고, 업데이트하고, 삭제할 수 있는 엔드포인트를 제공합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCIM 제공자



SCIM 제공자는 기록 생성, 업데이트 또는 삭제를 포함하여 IdP의 ID에 대한 변경 내용을 동기화합니다.

SCIM 클라이언트



SCIM 클라이언트는 SCIM 호환 REST 요청을 지원하는 시스템에서 ID 자원을 생성, 업데이트 및 삭제하는 데 사용됩니다.

SCIM 프로토콜은 HTTP(RFC7230) 표준을 기반으로 하는 애플리케이션 수준 HTTP 기반 프로토콜입니다. 이 API를 사용하여 사용자 및 그룹과 같은 ID 데이터를 프로비저닝하고 관리할 수 있습니다. 웹과 도메인 간 환경(예: 엔터프라이즈-클라우드 서비스 제공자 또는 클라우드 간 시나리오)에서 API를 사용합니다.

이 API에 액세스하려면 SCIM v2 - ServiceNow® 도메인 간 ID 관리(com.snc.integration.scim2) 플러그인을 활성화해야 합니다.

SCIM API에 대한 자세한 내용은 SCIM(System for Cross-domain Identity Management) API를 참조하세요.

SCIM 제공자

서비스 제공자는 SCIM API를 사용하여 사용자와 그룹을 프로비저닝합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

탐색



SCIM 제공자에 대해 알아봅니다.

활성화



SCIM을 활성화합니다.

SCIM 커스터마이제이션



SCIM을 사용자 지정하는 방법에 대한 상세 정보를 얻습니다.

소스 정의



SCIM에 대한 소스 정의에 대해 자세히 알아보십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCIM 제공자 탐색

서비스 제공자는 SCIM API를 사용하여 사용자와 그룹을 프로비저닝합니다.

SCIM 제공자로서 스키마는 ServiceNow SCIM API를 지원하여 사용자와 그룹을 프로비저닝합니다.

SCIM 제공자는 기록 생성, 업데이트 또는 삭제를 포함하여 IdP의 ID에 대한 변경 내용을 동기화합니다. 이러한 변경 내용은 SCIM 프로토콜에 따라 공급자와 자동으로 동기화됩니다. 또한 IdP는 제공자의 ID를 읽어 IdP 디렉터리에 추가할 수 있습니다. 그러면 IdP는 보안 취약성을 만들 수 있는 제공자의 잘못된 값을 탐지할 수 있습니다. 동기화를 통해 최종 사용자는 최신 프로필과 권한을 사용하여 자신에게 할당된 애플리케이션에 원활하게 액세스할 수 있습니다.

SCIM 제공자에 대한 구성

SCIM 제공자를 구성하려면 다음 작업을 수행합니다.

- **SCIM v2 - ServiceNow Cross-domain Identity Management** 플러그인을 활성화합니다. 자세한 내용은 다음 문서를 참조하십시오 SCIM 플러그인 활성화.
- SCIM에 필요한 다른 플러그인의 다른 플러그인을 활성화합니다.
  - OAuth 2.0
  - REST API 제공자
  - REST API 접근 정책
- SCIM 서비스의 일부로 scim_admin 역할을 추가합니다.

⚠ 경고: 이 역할은 신중하게 부여해야 합니다. scim_admin 역할은 scmin_admin PII(개인 식별 정보)를 추가하거나 업데이트할 수 있는 관리자 역할을 사용자에게 부여하는 것과 같습니다.

테이블

두 테이블(sys_user 및 sys_group)에는 기존 ServiceNow 테이블에 매핑되지 않는 SCIM 속성이 포함되어 있습니다. 테이블에 대한 자세한 내용은 SCIM 특정 테이블을 참조하세요.

SCIM 플러그인 활성화

SCIM 활성화의 경우 SCIM v2 - ServiceNow 도메인 간 ID 관리(com.snc.integration.scim2) 플러그인을 설치합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 SCIM v2 - ServiceNow 교차 도메인 ID 관리 (com.snc.integration.scim2) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.
3. 설치를 선택하여 설치 프로세스를 시작합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

자습서: 공급자를 통한 사용자 프로비저닝에 대한 **SCIM** 구성

SCIM을 구성하면 제공자 프로비저닝 서비스를 사용하여 사용자 및 그룹을 자동으로 프로비저닝 및 프로비저닝 해제할 수 있습니다 ServiceNow .

시작하기 전에

SCIM 플러그인을 설치합니다.

필요한 역할: scim_admin

경고: 이 역할은 신중하게 부여해야 합니다. scim_admin 역할은 scmin_admin PII(개인 식별 정보)를 추가하거나 업데이트할 수 있는 관리자 역할을 사용자에게 부여하는 것과 같습니다.

이 태스크 정보

다음 인증 방법으로 SCIM을 사용하여 사용자를 프로비저닝할 수 있습니다.

- 기본 인증을 사용하여 사용자 프로비저닝
- OAuth를 사용하여 사용자 프로비저닝

기본 인증을 사용하여 사용자 프로비저닝

SCIM을 구성하면 기본 인증과 함께 제공자의 프로비저닝 서비스를 사용하여 사용자 및 그룹을 자동으로 프로비저닝 및 프로비저닝 해제할 수 ServiceNow 있습니다.

시작하기 전에

필요한 역할: scim_admin

경고: 이 역할은 신중하게 부여해야 합니다. scim_admin 역할은 scmin_admin PII(개인 식별 정보)를 추가하거나 업데이트할 수 있는 관리자 역할을 사용자에게 부여하는 것과 같습니다.

SCIM 플러그인을 활성화해야 합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > **REST API** 접근 정책 REST API 접근 정책에 대한 상세 정보를 확인하려면
2. API 접근 정책 페이지에서 **SCIM API** 정책 기록을 클릭합니다.
3. 인증 프로파일 섹션에서 **SCIM API** 기본 인증 기록을 사용할 수 있는지 확인합니다.
4. 유형으로 기본 인증을 선택합니다.
5. 제공자 측에서 필요한 구성을 생성합니다.
6. 연결을 테스트하여 제공자 ServiceNow가 .

주: 연결에 실패하면 계정에 관리자 권한이 있는지 ServiceNow 확인하고 다시 시도하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

OAuth를 사용하여 사용자 프로비저닝

SCIM에 대한 공급자를 구성하면 OAuth와 함께 공급자 프로비전 서비스를 사용하여 사용자 및 그룹의 프로비전 및 프로비전 해제가 자동으로 프로비전됩니다 ServiceNow .

시작하기 전에
필요한 역할: scim_admin

⚠ 경고: 이 역할은 신중하게 부여해야 합니다. scim_admin 역할은 scmin_admin PII(개인 식별 정보)를 추가하거나 업데이트할 수 있는 관리자 역할을 사용자에게 부여하는 것과 같습니다.

SCIM 플러그인을 활성화해야 합니다.

프로시저

1. 다음으로 이동 모두 > 시스템 **OAuth** > 애플리케이션 레지스트리.
2. 애플리케이션 레지스트리 페이지에서 **SCIM API** 기록을 클릭합니다.
3. **SCIM API** 기록 상세 정보를 검증합니다.

   이러한 세부 정보는 Azure AD에서 응용 프로그램을 구성하는 ServiceNow 동안 제공해야 합니다.
4. 다음으로 이동 모두 > 시스템 웹 서비스 > **REST API** 접근 정책 REST API 접근 정책에 대한 상세 정보를 확인하려면
5. API 접근 정책 페이지에서 **SCIM API** 정책 기록을 클릭합니다.
6. 인증 프로필 섹션에서 **SCIMAPIOAuthOnly** 레코드를 사용할 수 있는지 확인합니다.
7. **OAuth** 엔터티 필드가 이전에 애플리케이션 레지스트리로 구성되거나 확인된 **SCIM API** 기록으로 지정되어 있는지 확인합니다.
8. 제공자 측에서 필요한 구성을 생성합니다.
9. 연결을 테스트하여 제공자 ServiceNow가 .

   ⓘ 주: 연결에 실패하면 계정에 관리자 권한이 있는지 ServiceNow 확인하고 다시 시도하십시오.

SCIM 문제 해결

SCIM과 통합되는 일반적인 오류 시나리오입니다.

잘못된 **REST API URL**

작업: 올바른 API URL을 입력합니다. **REST API** 탐색기에서 REST API URL을 교차 확인할 수 있습니다.

인스턴스에 리디렉션 URL이 설정되지 **ServiceNow** 않음

작업: SCIM OAuth 엔터티에 대한 유효한 리디렉션 URL을 ServiceNow에 입력합니다. 에서 OAuth 엔터티를 구성하는 동안 리디렉션 URL을 ServiceNow입력합니다.

리디렉션 URL이 요청과 다른 경우

작업: "인증 엔드포인트"에 제공된 "**redirect_url**"은(는) 에 ServiceNow구성된 OAuth 엔터티와 같아야 합니다.

ⓘ 주:

이 오류는 Azure '권한 부여 엔드포인트'와 ServiceNow '리디렉션 URL'이 일치하지 않을 때 발생합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

잘못된 클라이언트 암호가 전달될 때

작업: "클라이언트 비밀"에 입력한 값은 에 구성된 ServiceNowOAuth 엔터티와 같아야 합니다.

Azure "인증 엔드포인트"에 잘못된 "ClientId"가 전달된 경우

작업: "인증 엔드포인트"의 "client_id" 매개변수에 대해 입력한 값은 에서 ServiceNow구성한 OAuth 엔터티와 같아야 합니다.

SCIM 커스터마이제이션

ID 관리를 위한 SCIM 프로토콜을 사용자 지정합니다.

SCIM 커스터마이제이션을 통해 다음을 수행할 수 있습니다.

- 동적 확장 스키마 생성을 통해 sys_user 및 sys_user_group 테이블의 사용자 지정 필드를 지원합니다.
- 기본 SCIM 매핑을 재정의하는 기능을 제공합니다.

SCIM 관리자는 사용자 및 그룹 자원에 대한 사용자 지정 확장 스키마를 정의할 수 있습니다. 사용자 지정 확장 스키마에 정의된 속성은 sys_user 또는 sys_user_group 테이블의 필드에 매핑할 수 있습니다.

SCIM 커스터마이제이션을 위한 구성

SCIM 사용자 지정의 경우 다음 작업을 수행해야 합니다.

- SCIM 확장 스키마 테이블에서 사용자 및 그룹에 대한 사용자 지정 확장 스키마를 정의합니다. 자세한 내용은 다음 문서를 참조하십시오 SCIM 확장 스키마 만들기.
- 사용자 지정 스키마 속성에 대한 ETL 정의에서 엔터티를 생성합니다. 엔터티는 sys_user 또는 sys_user_group 속성으로 매핑되는 대상 테이블에 대해 생성됩니다. 자세한 내용은 SCIM ETL 정의 생성 문서를 참조하십시오.
- 이 두 엔터티 간에 RTE 매핑을 생성합니다. 자세한 내용은 의 SCIM ETL 정의 생성단계를 5 참조하십시오.
- SCIM API 요청 페이로드의 데이터가 포함된 사용자 지정 스키마 속성을 보냅니다.

SCIM API는 정의된 매핑을 사용하여 RTE 엔진을 호출합니다. 데이터는 매핑에 정의된 대로 대상 테이블의 각 필드에 저장됩니다.

SCIM 커스터마이제이션 속성 및 스키마

SCIM 커스터마이제이션에는 다음 속성, 지원되는 스키마 및 지원되지 않는 스키마가 포함됩니다.

속성

SCIM 커스터마이제이션은 다음과 같은 시스템 속성을 추가합니다.

속성

이름	설명
com.snc.integration.scim2.max.member.count	SCIM 최대 구성원 수입니다.
com.snc.integration.scim2.resolve.external.domains	외부 ID SCIM 필터를 사용하여 여러 자원을 찾은 경우 요청 클라이언트의 소스 정의에 따라 SCIM 자원을 해결합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성

이름	설명
	주: 단, 여러 소스에서 프로비저닝이 수행되는 경우 SCIM 소스 정의 테이블에 소스를 정의해야 합니다. 소스가 정의되지 않았거나 이 속성이 비활성 상태인 경우 일치하는 모든 자원이 외부 ID 필터 응답과 함께 반환됩니다.
com.snc.integration.scim2.user.etl.definition.id	SCIM 사용자 ETL 정의 ID입니다.
com.snc.integration.scim2.group.etl.definition.id	SCIM 그룹 ETL 정의 ID입니다.
com.snc.integration.scim2.rte.verbose.logging.enabled	SCIM 사용자 및 그룹 RTE 정의에 대한 자세한 로깅 사용.
com.snc.integration.scim2.string.field.length.validation.enabled	필드의 길이 확인입니다. 이 속성을 사용하면 필드를 자르고 저장하는 대신 확인할 수 있습니다.
com.snc.integration.scim2.provider.custom.response.script.id	SCIM 응답을 사용자 지정하기 위한 스크립트 포함의 ID입니다.

지원되는 스키마

SCIM 사용자 지정은 다음과 같이 지원되는 스키마를 추가합니다.

지원되는 스키마

스키마	설명	프리픽스	예제
urn:ietf:params:scim:schemas:core:2.0:User	자원에 대한 핵심 인증 속성을 포함합니다.	없음	이름.중간 이름
urn:ietf:params:scim:schemas:servicenow:2.0:User	외부 ServiceNow 관련된 ServiceNow 속성을 포함합니다.	ServiceNow	servicenow.manager.value
urn:ietf:params:scim:schemas:extension:servicenow:custom:2.0:User	핵심 확장 또는 ServiceNow 확장 스키마의 일부로 매핑되지 않은 사용자 지정 속성을 포함합니다.	사용자 지정	custom.socialId

지원되지 않는 스키마

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: 비즈니스 또는 기업에 속하거나 이를 대신하는 사용자를 나타내는 데 일반적으로 사용되는 속성을 포함합니다.

주: 엔터프라이즈 스키마는 유효한 스키마이지만 해당 속성이 모든 테이블에 매핑됩니다. 데이터베이스 지속성은 지원되지 않으므로 요청 본문에 엔터프라이즈 스키마가 포함된 경우 오류가 표시되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCIM 확장 스키마 만들기

핵심 스키마 또는 ServiceNow 확장 스키마의 일부로 매핑되지 않은 필드에 매핑할 사용자 지정 속성을 만듭니다.

시작하기 전에

필요한 역할: scim_admin

> **경고:** 이 역할은 신중하게 부여해야 합니다. scim_admin 역할은 사용자에게 관리자 역할을 부여하는 것과 같으며, scmin_admin 역할은 비즈니스 논리 또는 ACL 보호를 바이패스할 수 있는 테이블에 새 레코드를 삽입할 수 있습니다.

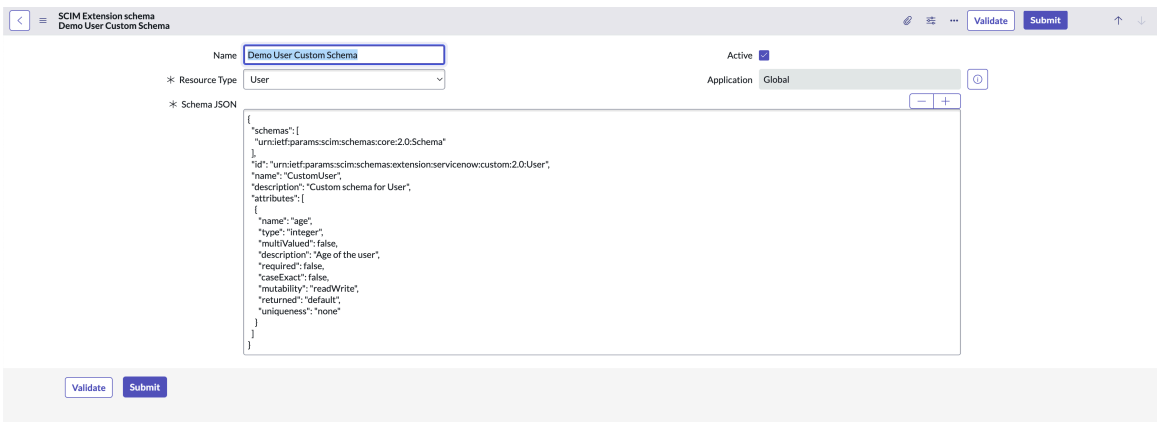
프로시저

1. 다음으로 이동 모두 > **SCIM** > **SCIM** 확장 스키마.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

> **주:** 하나의 확장 스키마만 자원 유형 필드에 매핑할 수 있습니다. 예를 들어 자원 유형인 사용자를 사용자 확장 스키마에 매핑할 수 있습니다.

SCIM 확장 스키마

필드	설명
이름	확장 스키마의 이름입니다.
활성	스키마를 활성화하는 옵션입니다. 기록을 사용자 지정 확장 스키마로 간주해야 하는 경우 이 필드를 선택합니다. 사용자 또는 그룹 유형에 관계없이 특정 자원 유형에 대해 한 번에 하나의 사용자 지정 확장 스키마 기록만 활성화할 수 있습니다.
자원 유형	확장 스키마에 매핑해야 하는 자원 유형입니다. 옵션은 다음과 같습니다. ◦ 사용자 ◦ 그룹
애플리케이션	이 기록에 대한 애플리케이션 범위입니다.
스키마 JSON	JSON 스키마 내의 세부 정보입니다. 특성을 사용하여 확장 스키마를 정의하는 방법에 대한 자세한 내용은 Datatracker 를 참조하세요.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

4. 확인을 클릭하여 속성을 확인합니다.
5. 제출을 클릭합니다.

결과
사용자 또는 그룹 자원 유형과 관련된 사용자 지정 속성이 있는 확장 스키마가 생성됩니다. SCIM ETL 정의를 사용하여 sys_user 및 sys_user_group 테이블의 확장 스키마를 기반으로 자원을 매핑합니다. 자세한 내용은 SCIM ETL 정의 생성 문서를 참조하십시오.

SCIM ETL 정의 생성

SCIM ETL 정의를 사용하여 사용자 지정 속성을 sys_user 또는 sys_user_group 테이블과 매핑합니다.

시작하기 전에
필요한 역할: scim_admin

⚠ 경고: 이 역할은 신중하게 부여해야 합니다. scim_admin 역할은 사용자에게 관리자 역할을 부여하는 것과 같으며, scmin_admin 역할은 비즈니스 논리 또는 ACL 보호를 바이패스할 수 있는 테이블에 새 레코드를 삽입할 수 있습니다.

ⓘ 주:

- SCIM 그룹 및 SCIM 사용자 ETL 정의는 리소스 매핑을 위한 기본 시스템의 일부입니다. 동일한 리소스 매핑을 사용하고 필요에 따라 기준을 변경하거나 새 리소스 매핑을 만들 수 있습니다.
- SCIM 매핑에서는 RTE를 통한 [*] 필드가 지원되지 않습니다.

프로시저

1. ETL(추출 변환 로드) 정의 생성 의 지침을 따릅니다.
2. 새로 만든 기록을 열고 상세 정보를 봅니다.
3. ETL 엔터티 섹션에서 새로 만들기를 클릭하여 엔터티를 생성합니다.
   다음 사용자에 대한 엔터티를 생성해야 합니다.
   - scim-user: SCIM의 필드입니다.
   - 사용자(sys_user) 또는 그룹(sys_user_group) 테이블: 데이터베이스 테이블에서 SCIM을 사용하여 매핑하려는 필드의 경우. 예를 들어 SCIM을 통해 사용자 상세 정보를 커스터마이제이션하려면 sys_user 테이블을 사용할 수 있습니다.

a. 양식의 필드에 내용을 입력합니다.

ETL 엔터티 양식

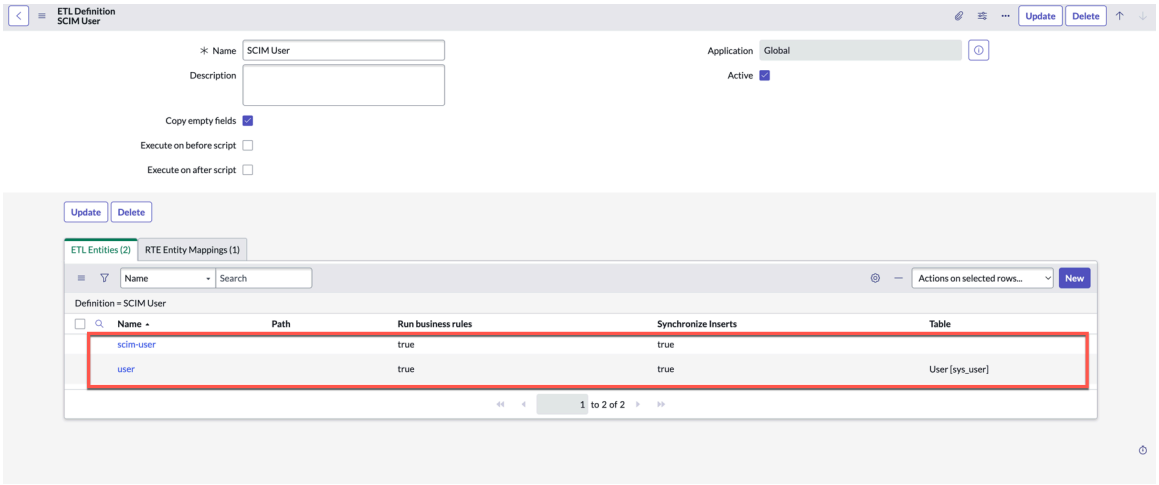
필드	설명
이름	ETL 엔터티의 이름입니다.
애플리케이션	이 기록에 대한 애플리케이션 범위입니다.
테이블	ETL 엔터티의 대상 테이블입니다.
정의	선택한 ETL 엔터티.
경로	이 엔터티의 고유한 경로입니다. 임포트 세트 테이블을 나타내는 엔터티에 대한 경로를 지정하지 마십시오. 엔터티가 컬렉션을 나타내는 경우 경로는 별표(*)로 끝나야 합니다. 이 요구 사항은 중간 항목 및 대상 테이블 엔터티에 적용됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
삽입 동기화	기록 삽입을 동기화하여 고유한 병합 필드 값이 있는 단 하나의 기록만 보장하는 옵션입니다.
비즈니스 규칙 실행	비즈니스 규칙을 실행하는 옵션입니다.

b. 제출을 클릭합니다.

scim-user 및 user 테이블에 대해 ETL 엔터티가 생성됩니다. 이러한 ETL 엔터티 내에 ETL 엔터티 필드를 생성하고 RTE 엔터티 매핑을 생성하여 두 엔터티를 모두 매핑해야 합니다.



4. 엔터티를 생성하고 매핑합니다.

a. 제출된 기록(scim-user 및 사용자)을 엽니다.

b. ETL 엔터티 필드에서 새로 만들기를 클릭하여 필드를 추가합니다.

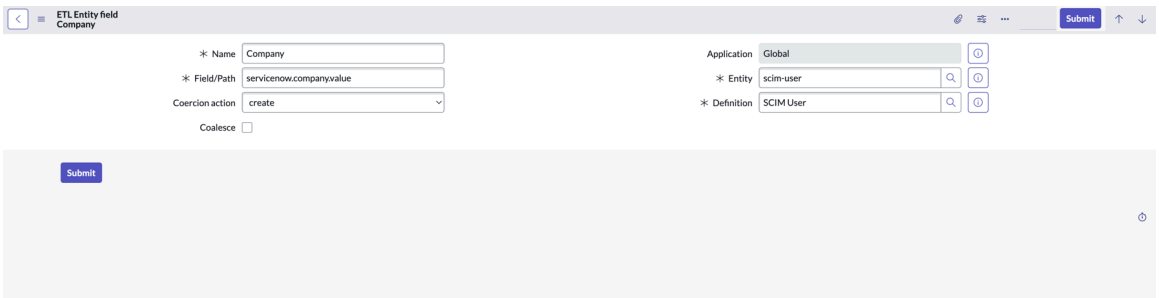
c. 양식의 필드에 내용을 입력합니다.

ETL 엔터티 양식

필드	설명
이름	ETL 엔터티 필드 정의의 이름입니다.
애플리케이션	이 필드 정의가 속한 선택한 ETL 엔터티입니다.
필드/경로	이 필드는 열 또는 경로입니다. ▪ 엔터티가 임포트 또는 대상 테이블인 경우 필드는 열 이름입니다. ▪ 필드에 중첩된 구조가 있는 경우 필드는 경로입니다.
엔터티	이 운영이 적용되는 엔터티입니다. 조회 아이콘을 사용하여 엔터티를 선택합니다.
강제 변환 작업	참조 또는 선택 항목을 찾을 수 없는 경우 시스템에서 수행해야 하는 작업입니다. 옵션은 다음과 같습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

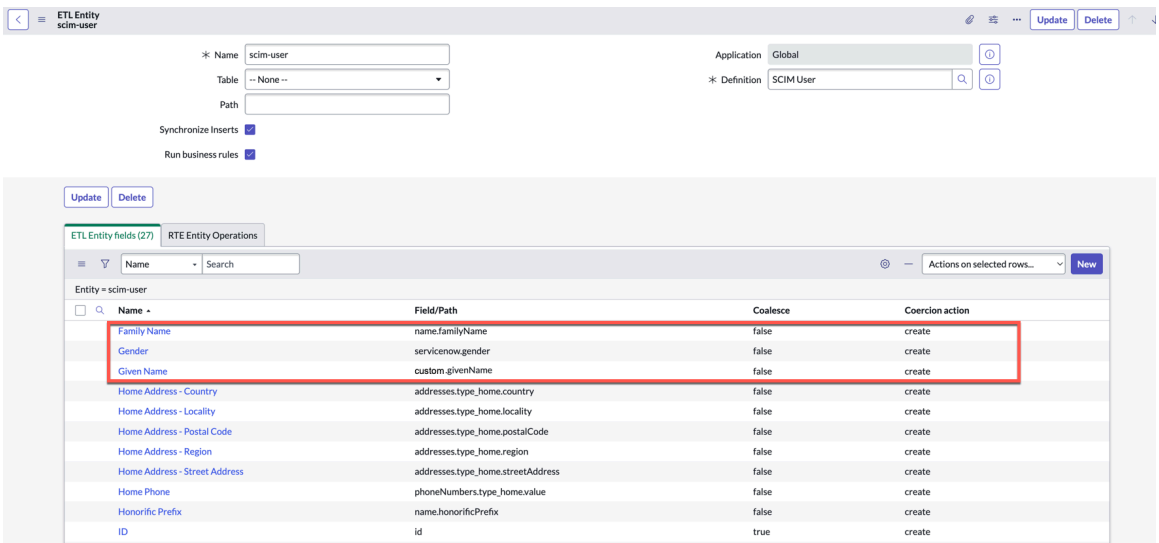
필드	설명
	▪ 생성: 새 참조 또는 선택 항목을 만듭니다. 현재 기록에 참조 또는 선택을 할당합니다. ▪ 거부: 전체 기록을 데이터베이스에 저장하지 않습니다. ▪ 무시: 현재 값을 비어 있음으로 설정합니다.
정의	이 필드 정의가 속한 선택한 ETL 엔터티입니다.
병합	기존 기록을 쿼리하는 옵션입니다.



d. 제출을 클릭하여 항목을 제출합니다.

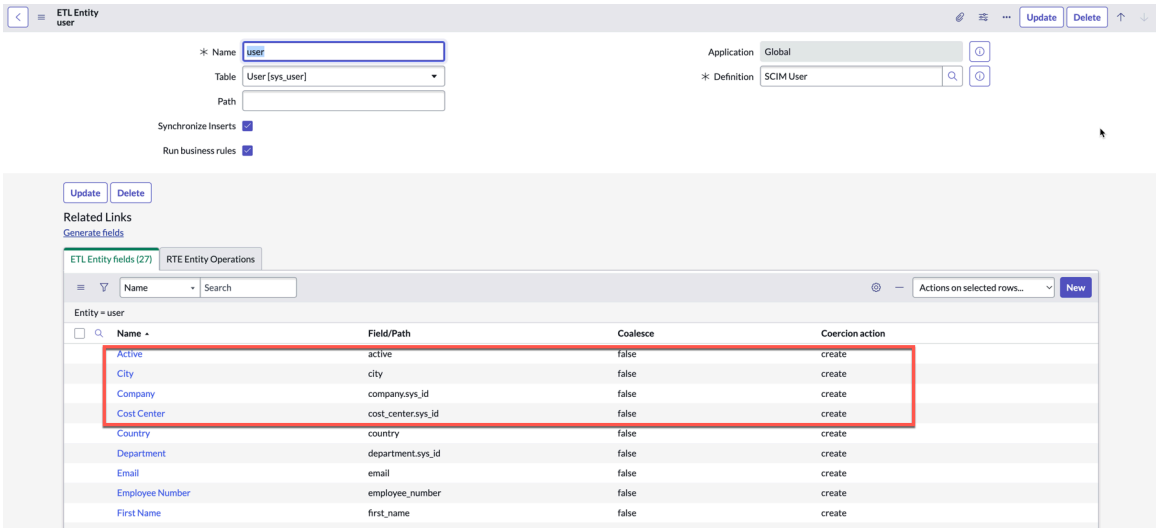
요구 사항에 따라 여러 항목을 ETL 엔터티 필드로 추가할 수 있습니다.

scim-user ETL 엔터티에는 코어 확장(사용자), ServiceNow 확장 또는 사용자 지정 확장이 있는 엔터티가 있을 수 있습니다.



사용자 ETL 엔터티는 데이터베이스 테이블의 엔터티를 가질 수 있습니다. 예를 들어 sys_user 테이블입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



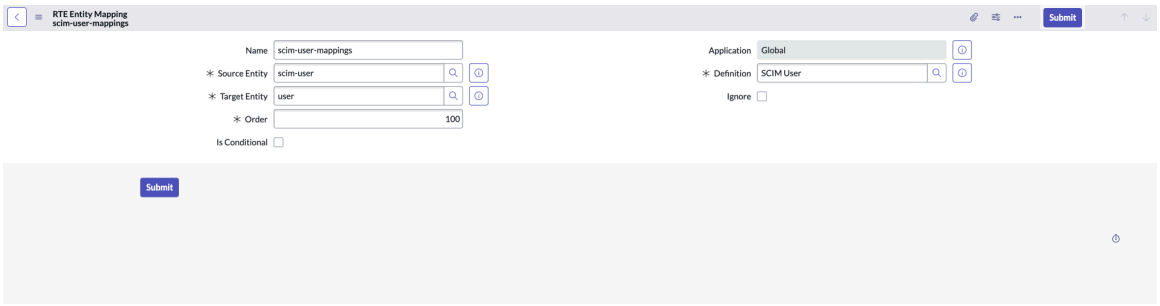
주: 수신 SCIM 필드에 필터를 추가하려면 밑줄(_)을 사용합니다. 이 밑줄은 EQ 필터로 변환됩니다. 예를 들어 이 속성은 *email.type_work.value* 이메일 *[type eq "work"].value*의 SCIM 필터를 적용합니다.

scim-user 및 사용자 ETL 엔터티 기록 모두에서 필드를 만든 후에는 RTE 엔터티 매핑 기록을 만들어야 합니다. 그런 다음 소스와 대상 정의를 지정하여 두 필드를 매핑해야 합니다.

5. RTE 엔터티 매핑 섹션에서 신규를 클릭하여 엔터티 매핑을 생성합니다

6. 양식에서 필드를 채웁니다.

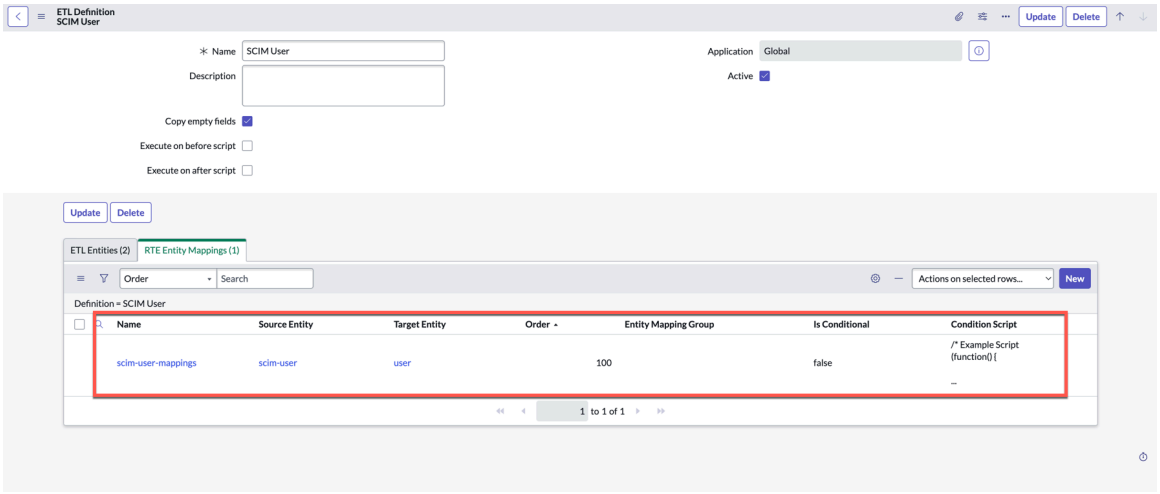
필드	설명
이름	매핑의 이름입니다.
소스 엔터티	매핑에 대한 소스 엔터티입니다.
대상 엔터티	매핑할 대상 엔터티입니다.
순서	매핑을 처리해야 하는 순서입니다.
조건부	매핑을 조건부로 지정하는 옵션입니다.
조건 스크립트	매핑에 대해 충족되어야 하는 조건을 정의하는 스크립트입니다.
애플리케이션	이 기록에 대한 애플리케이션 범위입니다.
정의	이 매핑이 속한 선택한 ETL 엔터티입니다.
무시	강력한 임포트 세트 변환(RTE)을 사용하여 데이터 통합을 수행할 때 이 ETL 엔터티 매핑을 무시해야 하는지 여부를 지정하는 옵션입니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

7. 제출을 클릭합니다.

   다음 예는 scim-user 및 user ETL 엔터티 기록을 모두 매핑하기 위해 생성된 기록을 보여줍니다.



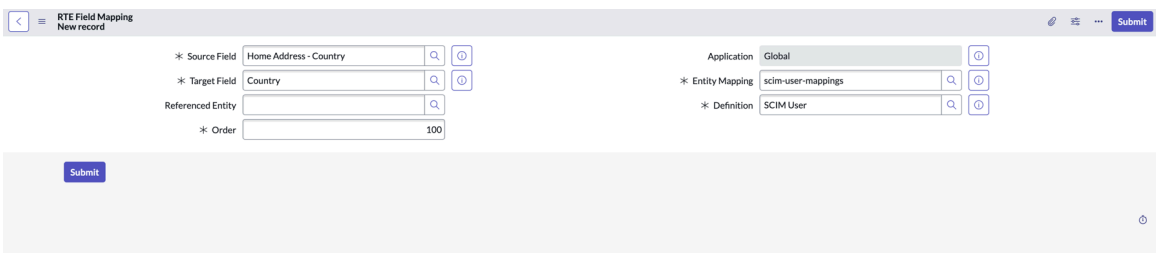
8. 제출된 기록(scim-user-mappings)을 열고 scim-user와 사용자 ETL 엔터티 기록 간에 매핑을 생성합니다.

   a. RTE 필드 매핑 섹션에서 새로 만들기를 클릭합니다.

   b. 양식의 필드에 내용을 입력합니다.

   ETL 엔터티 필드

필드	설명
소스 필드	이 기록에 대한 애플리케이션 범위입니다.
애플리케이션	이 필드 정의가 속한 선택한 ETL 엔터티입니다.
대상 필드	운영이 단일 출력을 사용하는 경우 운영에 대한 출력 ETL 필드입니다.
엔터티 매핑	이 작업이 적용되는 엔터티 매핑입니다.
참조된 엔터티	참조되는 엔터티와 이 엔터티가 적용되는 작업입니다.
정의	이 필드 정의가 속한 선택한 ETL 엔터티입니다.
순서	엔터티에서 작업이 실행되는 순서입니다.

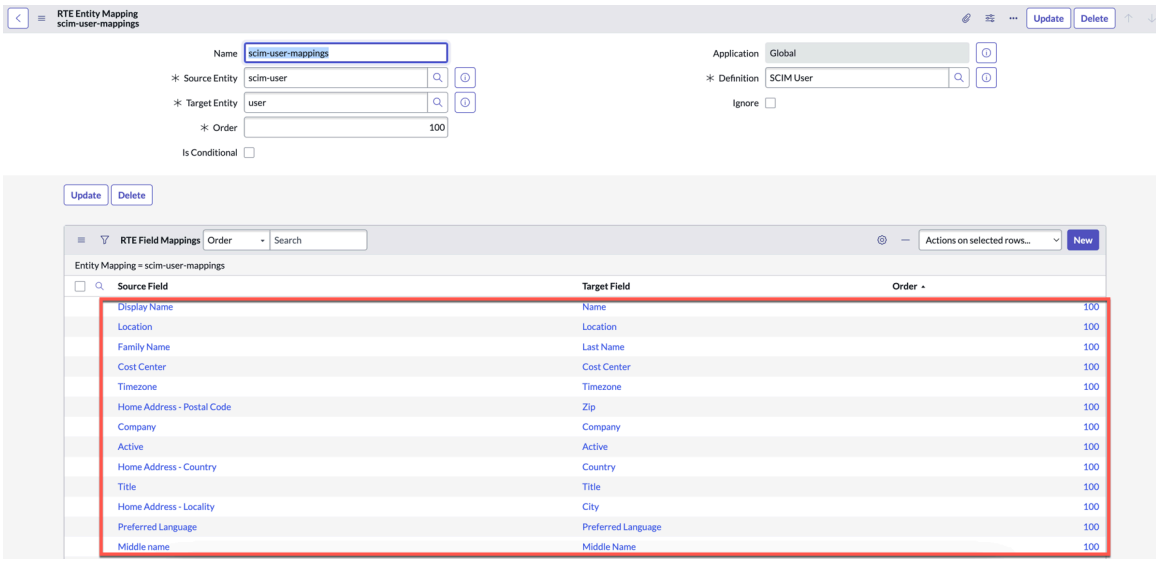


   소스 필드 집 주소 - 국가 (scim-user ETL 엔터티)는 대상 필드를 국가 (사용자 ETL 엔터티)로 매핑합니다.

   c. 제출을 클릭하여 항목을 제출합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

요구 사항에 따라 여러 항목을 RTE 엔터티 매핑으로 추가할 수 있습니다.



소스 필드와 대상 필드는 구성된 대로 매핑됩니다. SCIM을 사용하여 CRUD 작업을 수행하면 해당 테이블에서 사용자 지정된 값이 업데이트됩니다.

결과
이러한 ETL 정의 및 매핑을 사용하면 소스 테이블에서 데이터를 추출하고, 원하는 대로 데이터를 변환하고, 데이터를 대상 테이블에 로드할 수 있습니다.

관련 정보

ETL(추출 변환 로드) 정의 생성

매핑되지 않은 필드 처리

SCIM 커스터마이제이션에서 매핑되지 않은 필드를 다양한 방법으로 처리할 수 있습니다.

SCIM 커스터마이제이션 중에 다음 기능을 수행하여 sys_user 및 sys_user_group 테이블에 속하지 않는 필드를 매핑할 수 있습니다.

SCIM 사용자 지정(만들기 또는 업데이트)

SCIM 클라이언트를 만들거나 업데이트할 수 있습니다.

- SCIM 관리자는 ETL 정의 또는 RTE에 매핑되지 않은 필드에 대한 및 *onAfter* 스크립트에 *onBefore* 사용자 지정 스크립트를 추가할 수 있습니다.
- SCIM 관리자는 및 *onAfter* 스크립트에 사용자 지정 스크립트를 추가하여 RTE 매핑을 *onBefore* 재정의할 수 있습니다.
- RTE *onBefore* 또는 *onAfter* 스크립트에서 스크립트 가능한 API를 호출하여 수신 요청에 액세스하고 다른 테이블, 목록 및 매핑되지 않은 속성에 대한 변환을 수행할 수 있습니다.
- 이 *sn_auth.SCIM2Util.getScimProviderCustomizationContext()* 메서드를 사용하여 객체가 포함된 SCIM 요청 컨텍스트를 제공할 수 있습니다 *scimResource*. in 컨텍스트는 *scimResource* 각 작업에서 다음을 나타냅니다.
  - **POST:** 요청 페이로드로 전송된 SCIM 자원입니다.
  - **PUT**: 데이터베이스의 현재 SCIM 자원이 요청 페이로드에 전송된 SCIM 자원으로 대체됩니다.
  - **PATCH:** 패치 작업을 수행한 후 데이터베이스의 현재 SCIM 자원입니다.

다음은 스크립트의 *onAfter* 예입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
(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();
            }
           }

})(source, target, importLog);
```

SCIM 응답 사용자 지정

GET API 호출의 경우 스크립트를 확장하여 스크립트를 사용하여 SCIM 클라이언트에 대한 응답을 사용자 지정할 수 있습니다 *SCIMProviderCustomization*.

스크립트를 확장하는 동안 작성자는 and *customizeGroupResponse* 메서드를 재정의 *customizeUserResponse* 하여 사용자 및 그룹 자원에 대한 응답을 수정할 수 있습니다.

이 *com.snc.integration.scim2.provider.customization.script.id*속성을 사용하면 SCIM 플러그인이 응답 커스터마이제이션에 사용해야 하는 스크립트를 사용할 수 있습니다.

다음은 기본 스크립트를 확장하는 예시입니다.

```
var SCIMCustomizationScript = Class.create();
SCIMCustomizationScript.prototype =
 Object.extendsObject(SCIMProviderCustomization, {
    initialize: function() {
        SCIMProviderCustomization.prototype.initialize.call(this);
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

```
    },
    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(th
is, "User", context);
                    customExtensionValue.salary = salary;

 SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(th
is, "User", context, customExtensionValue);
                }
            }
        } catch (ex) {
            gs.error("err: " + ex);
        }
        return context;
    },
    customizeGroupResponse: function(context) {
        return context;
    },
    type: 'SCIMCustomizationScript'
});
```


© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주:

- and *customizeGroupResponse* 메서드에 포함된 매개 변수는 *customizeUserResponse* 라는 *scimResource*하나의 속성이 있는 컨텍스트 객체입니다. 이 속성에는 사용자 또는 그룹 자원 개체의 모든 속성이 있습니다.
- 사용자 지정된 스크립트 포함은 관리자만 작성하고 볼 수 있습니다.
- 사용자 또는 그룹 자원이 수정되면 컨텍스트를 다시 반환해야 합니다.
- 리소스 개체에 속성이 수정되지 않은 경우 the를 *com.snc.integration.scim2.provider.customization.script.id*비워 두거나 null로 반환합니다.
- 특정 속성이 스크립트를 통해 *onAfter* 유지되는 경우 사용자 지정된 스크립트 내의 객체에 있는 *scimResource* 데이터베이스 값으로 채워야 합니다. 시스템에서 다음을 수행할 수 있도록 이 작업이 필요합니다.
  - PUT 및 PATCH 작업 중에 스크립트에서 *onAfter* 올바른 *scimResource* 객체를 가져오기 위해.
  - 클라이언트에 대한 응답에 스크립트를 통해 *onAfter* 유지된 속성을 포함합니다.

도우미 함수

다음은 SCIM 사용자 지정을 위한 도우미 함수 중 일부입니다. 이러한 함수를 사용하면 다양한 유형의 정보를 가져오거나 설정할 수 있습니다.

도우미 함수

함수	목적
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");	사용자 지정 확장 스키마의 값을 가져옵니다.
SCIMProviderCustomization.prototype.getServiceNowExtensionUrn.call(this, "User");	확장 스키마의 ServiceNow 값을 가져옵니다.
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User", context);	응답에서 사용자 지정 스키마 노드를 가져옵니다.
SCIMProviderCustomization.prototype.getServiceNowExtensionNodeValue.call(this, "User", context);	응답에서 ServiceNow 스키마 노드를 가져오기
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this, "User", context, customExtensionValue);	응답에서 사용자 지정 스키마 노드를 설정합니다.

다음은 도우미 함수를 사용하는 예제입니다.

```
var customExtensionUrn =
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this,
 "User");
var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(th
is, "User", context);
customExtensionValue.age = "18";
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue
 call(this, "User", context, customExtensionValue);
```

주: RTE는 sys_user 및 sys_user_group 테이블 이외의 테이블에서 데이터를 설정할 수 있도록 지원합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

소스 정의 생성

소스 정의를 생성하여 자원이 프로비저닝되는 ID 소스에 대한 정보를 캡처합니다.

시작하기 전에

필요한 역할: scim_admin

경고: 이 역할은 신중하게 부여해야 합니다. scim_admin 역할은 scmin_admin PII(개인 식별 정보)를 추가하거나 업데이트할 수 있는 관리자 역할을 사용자에게 부여하는 것과 같습니다.

이 태스크 정보

소스 정의를 사용하면 프로비저닝 ID 소스를 프로비저닝하는 동안 인증하는 OAuth 엔터티에 매핑할 수 있습니다.

소스 정의가 생성되면 해당 ID 소스에서 프로비저닝되는 모든 자원이 해당 소스 정의 ID에 매핑됩니다.

소스 정의는 다음을 수행하는 등의 방법으로 필요한 소스 정보를 캡처합니다.

- 자원이 프로비저닝되는 SCIM 클라이언트를 식별합니다.
- 외부 ID에서 제공하는 중복 정보를 해결합니다.
  - 여러 ID 소스가 자원을 프로비저닝하는 경우 외부 ID가 ID 소스에만 고유하기 때문에 둘 이상의 자원이 동일한 외부 ID 값을 가질 수 있습니다.
  - 여러 자원이 외부 ID SCIM 필터와 함께 반환되는 경우, 요청 ID 소스의 소스 정의에 따라 자원을 확인할 수 있습니다.

주: 소스 정의는 OAuth 인증 방법을 사용하는 ID 소스에 대해서만 생성할 수 있습니다.

프로시저

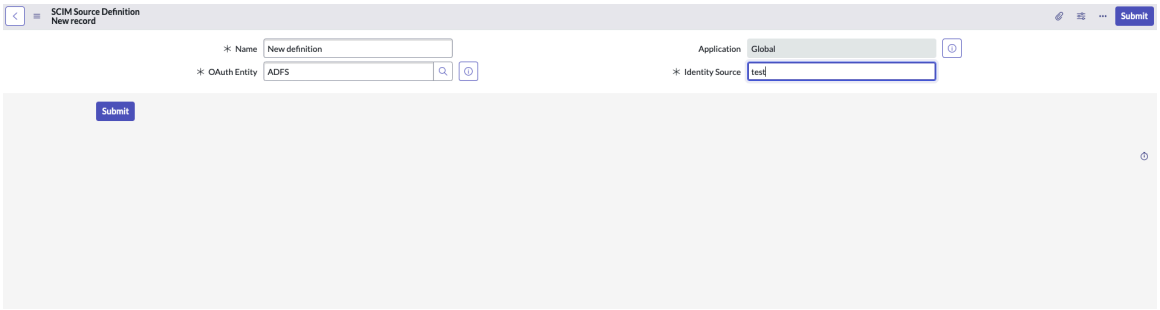
1. 다음으로 이동 모두 > **SCIM** > 소스 정의.
2. SCIM 소스 정의 페이지에서 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

SCIM 소스 정의

필드	설명
이름	소스 정의의 이름입니다.
애플리케이션	이 기록에 대한 애플리케이션 범위입니다.
OAuth 엔터티	통합 사용자의 OAuth 엔터티입니다. 엔터티는 ID 소스 제공자가 사용자를 프로비저닝하는 데 사용됩니다.
ID 소스	ID 소스 제공자의 이름입니다. 예를 들어 Azure AD, Okta 등이 있습니다

주: *com.snc.integration.scim2.resolve.externalid.conflict* 요청 ID 소스에서 생성한 SCIM 자원만 반환하도록 속성을 활성화합니다. 기본적으로 외부 ID 필터가 있는 모든 일치하는 자원이 반환됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



4. 제출을 클릭합니다.

결과
SCIM 소스 정의가 생성됩니다. SCIM ETL 정의를 사용하여 sys_user 및 sys_user_group 테이블의 확장 스키마를 기반으로 자원을 매핑합니다. 자세한 내용은 SCIM ETL 정의 생성 문서를 참조하십시오.

SCIM 클라이언트

SCIM 클라이언트는 외부 시스템의 SCIM 엔드포인트에 의해 노출되는 CRUD 작업을 통해 ID 자원에 대한 프로비저닝 및 업데이트를 용이하게 합니다.

탐색	활성화
	
SCIM 클라이언트에 대해 알아봅니다.	SCIM 클라이언트를 활성화합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

SCIM 클라이언트 속성



SCIM을 사용자 지정하는 방법에 대한 상세 정보를 얻습니다.

문제 해결



SCIM에 대한 소스 정의에 대해 자세히 알아보십시오.

SCIM 클라이언트 탐색

SCIM 클라이언트는 외부 시스템의 SCIM 엔드포인트에 의해 노출되는 CRUD 작업을 통해 ID 자원에 대한 프로비저닝 및 업데이트를 용이하게 합니다.

SCIM 클라이언트는 SCIM 호환 REST 요청을 지원하는 시스템에서 ID 자원을 생성, 업데이트 및 삭제하는 데 사용됩니다. 클라이언트는 ID 수명 주기 관리 및 인스턴스 간 ServiceNow 또는 ServiceNow 다른 SCIM 제공자와의 ID 속성 동기화에 사용됩니다.

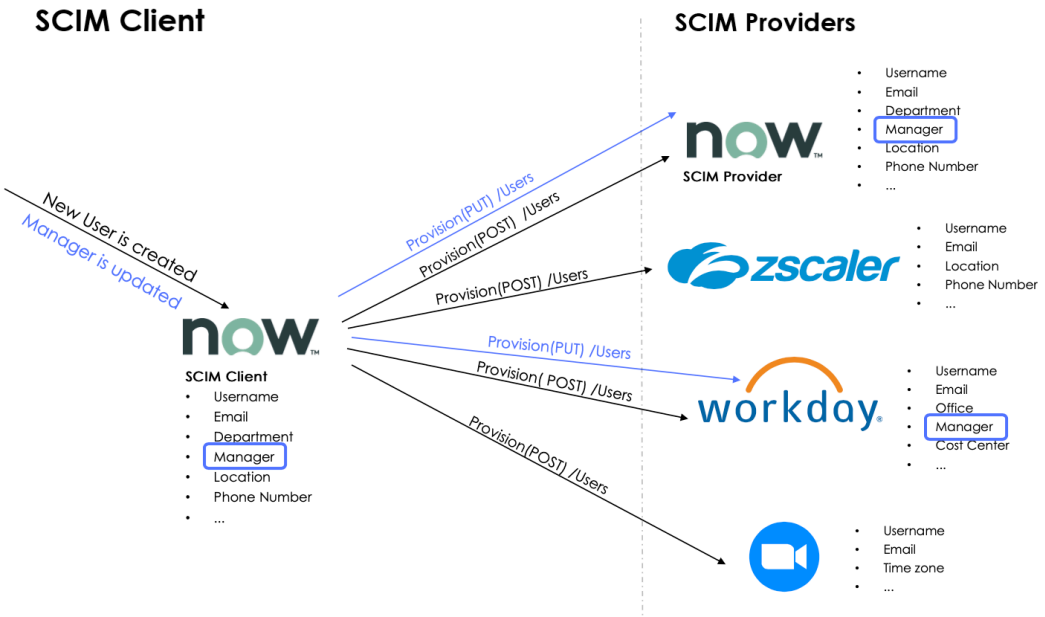
API는 클라이언트에 의해 노출되므로 단일 또는 여러 SCIM 공급자에서 리소스를 생성, 업데이트 또는 삭제하는 프로세스를 자동화할 수 있습니다. 예를 들어 개발자가 조직에 가입하는 경우 Git, 작업 공간 등에 대한 액세스 권한을 제공해야 합니다.

SCIM 클라이언트를 사용하면 다음 작업을 수행할 수 있습니다.

- 사용자 또는 그룹 구성원 자격에 대한 ID 및 액세스 권한을 프로비저닝합니다.
- ID 및 관련 자원을 SCIM 호환 시스템과 동기화합니다.
- 에 SCIM 제공자를 ServiceNow®통합합니다.
- ID 및 액세스 프로비저닝 해제

SCIM 클라이언트는 통합 개발자가 지정된 작업을 수행하기 위한 워크플로우 또는 자동화를 빌드하는 데 사용할 수 있는 스크립트 가능한 API를 제공합니다. 스크립트 가능한 API에 대한 자세한 내용은 SCIM2Client API 를 참조하세요.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



SCIM 클라이언트에 대한 구성

SCIM 클라이언트를 구성하려면 다음 작업을 수행합니다.

- 특정 SCIM 제공자에 대한 모든 아웃바운드 호출에 대한 REST 메시지를 생성합니다. 자세한 내용은 REST 메시지 생성 문서를 참조하십시오.
- SCIM 제공자를 생성하여 REST 메시지와 함께 SCIM 제공자로부터 자원 유형 및 스키마 정보를 가져옵니다. HTTP 메서드(PUT 또는 PATCH)의 구성을 활성화하여 SCIM 제공자의 자원을 업데이트합니다. 자세한 내용은 SCIM 제공자 생성 문서를 참조하십시오.
- 특정 자원 유형 및 SCIM 제공자의 속성에 대한 SCIM 속성의 ServiceNow 매핑을 생성합니다. 자세한 내용은 를 참조하십시오 SCIM 제공자 리소스 매핑 생성.
- 데이터베이스 테이블 및 필드 이름을 사용하여 SCIM 필드의 매핑을 수행합니다. 기본값을 전달하거나 스크립트를 작성하여 값을 가져옵니다. 자세한 내용은 문서를 참조하십시오 SCIM 속성 매핑 생성.

SCIM 클라이언트 플러그인 활성화

SCIM 클라이언트 활성화의 경우 SCIM v2 - ServiceNow 도메인 간 ID 관리 클라이언트 (com.snc.integration.scim2.client) 플러그인을 설치합니다.

시작하기 전에

필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 애플리케이션 > 모든 사용 가능 애플리케이션 > 모두.
2. 필터 기준 및 검색 창을 사용하여 SCIM v2 - ServiceNow 교차 도메인 ID 관리 클라이언트 (com.snc.integration.scim2.client) 플러그인을 찾습니다.

   이름 또는 ID를 기준으로 플러그인을 검색할 수 있습니다. 플러그인을 찾을 수 없으면 ServiceNow 담당자에게 요청해야 할 수 있습니다.

3. 설치를 선택하여 설치 프로세스를 시작합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

주: 인스턴스에서 도메인 분리와 위임된 관리자가 활성화된 경우, 관리자 역할이 있는 사용자가 전역 도메인에 있어야 합니다. 그렇지 않으면 <#### ##># ## #### ### ### ## #### ###### ### ### # ####라는 오류가 나타납니다.

설치가 완료되면 메시지가 표시됩니다. 플러그인과 함께 설치되는 구성요소에 대한 자세한 내용은 애플리케이션과 함께 설치되는 구성요소 찾기 를 참조하십시오.

SCIM 클라이언트 속성, 테이블, 스크립트 가능한 API 및 로그

SCIM v2 - ServiceNow 교차 도메인 ID 관리 클라이언트(com.snc.integration.scim2.client) 플러그인에는 다음과 같은 시스템 속성, 테이블, 스크립트 가능한 API, 로그가 포함됩니다.

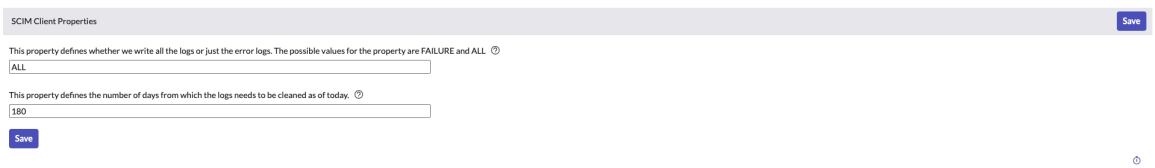
속성

SCIM 클라이언트는 다음 시스템 속성을 추가합니다.

속성

이름	설명
com.snc.integration.scim2.client.log.level	이 속성은 모든 로그 레코드를 쓸지 또는 오류 로그 레코드만 쓸지 여부를 결정합니다. 가능한 값은 **FAILURE** 또는 **ALL**입니다. 기본값: 모두
com.snc.integration.scim2.client.log.clean.up	이 속성은 로그를 자울 일 수를 결정합니다. 기본값: **180**

속성을 설정하려면 다음으로 이동합니다. 모두 > **SCIM** > **SCIM** 클라이언트 속성.



테이블

SCIM 클라이언트는 다음 테이블을 추가합니다.

테이블

이름	설명
SCIM 제공자(sys_scim_provider)	각 SCIM 제공자에 대한 데이터(예: 이름, REST 메시지, 자원 정의 등)를 저장합니다.
SCIM 제공자 리소스 매핑 (sys_scim_provider_resource_mapping)	각 제공자 및 자원 이름에 대한 기본 테이블 정보를 저장합니다.
SCIM 속성 매핑(sys_scim_attribute_mapping)	테이블 필드, 스크립트 등 각 SCIM 속성 값을 가져와야 하는 소스 상세 정보를 저장합니다.
SCIM 클라이언트 로그(sys_scim_client_logs)	SCIM 제공자에 트리거된 각 호출의 상태를 저장합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

스크립트 가능한 API

SCIM2Client API는 SCIM(System for Cross-domain Identity Management) 공급자(서버 역할)를 호출하여 SP(서비스 공급자)에서 데이터를 생성, 업데이트 또는 삭제합니다. SCIM 클라이언트의 스크립트 가능한 API는 시스템 컨텍스트에서 실행 중인 스크립트에서 또는 시스템 관리 사용자가 사용해야 합니다.

예를 들어, 시스템 사용자로 통합 허브 워크플로우를 실행하는 동안, 예약된 작업을 실행하는 동안 스크립트를 사용할 수 있습니다.

다음은 스크립트 가능한 API를 사용하기 위한 몇 가지 사용 사례입니다.

- 관리자는 백그라운드 스크립트, 비즈니스 규칙, 스크립트 포함 호출, 워크플로우 등에서 ID 정보를 프로비저닝합니다.
- 관리자는 ID 프로비저닝을 위해 예약된 작업 또는 요청 시 작업을 실행합니다.
- 스크립트 가능한 프로비저닝 API 호출을 사용하여 스크립트 단계로 워크플로우 또는 하위 워크플로우를 실행합니다.
- 비즈니스 규칙 또는 스크립트 포함에 프로비저닝 스크립트를 직접 추가합니다. 관리자가 아닌 사용자가 스크립트를 트리거할 수 있습니다. 이 사용 사례는 다음과 같은 상황에서 작동합니다.
  - 사용자에게 토큰에 대한 액세스 권한이 있으므로 REST 템플릿에서 토큰을 생성할 수 있는 역할이 사용자에게 있습니다.
  - 사용자는 매핑된 테이블에서 SCIM 속성 값을 검색할 수 있는 액세스 권한을 갖습니다.

스크립트 가능한 API에 대한 자세한 내용은 SCIM2Client API 를 참조하세요.

SCIM 클라이언트 로그

SCIM 클라이언트 로그에는 SCIM API에 대한 프로비저닝 상태가 표시됩니다. 프로비저닝 상태를 보려면 다음으로 이동합니다. 모두 > **SCIM** > **SCIM** 클라이언트 로그.

REST 메시지 생성

특정 SCIM 제공자에 대한 모든 아웃바운드 호출에 대한 REST 메시지를 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 웹 서비스 > 아웃바운드 > **REST** 메시지.
2. 새로 만들기를 클릭합니다.
3. 양식의 필드에 내용을 입력합니다.

SCIM 제공자

필드	설명
이름	이 메시지에 대한 설명이 포함된 이름입니다.
엔드포인트	SCIM 제공자의 기본 URL입니다. 예를 들면 `https://example.service-now.com/api/now/scim`.
인증 유형	외부 SCIM 제공자에 연결하는 데 사용할 인증 유형입니다. 자세한 정보는 아웃바운드 REST 인증을 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
HTTP 헤더	외부 SCIM 공급자에게 필요한 콘텐츠 형식입니다. 예를 들어 헤더 이름은 다음 API 요청 본문의 콘텐츠 `#####. ### ##: application/scim+json`

4. HTTP 메서드 관련 목록에서 새로 만들기를 클릭합니다.
5. 다음 HTTP 메서드를 구성합니다.

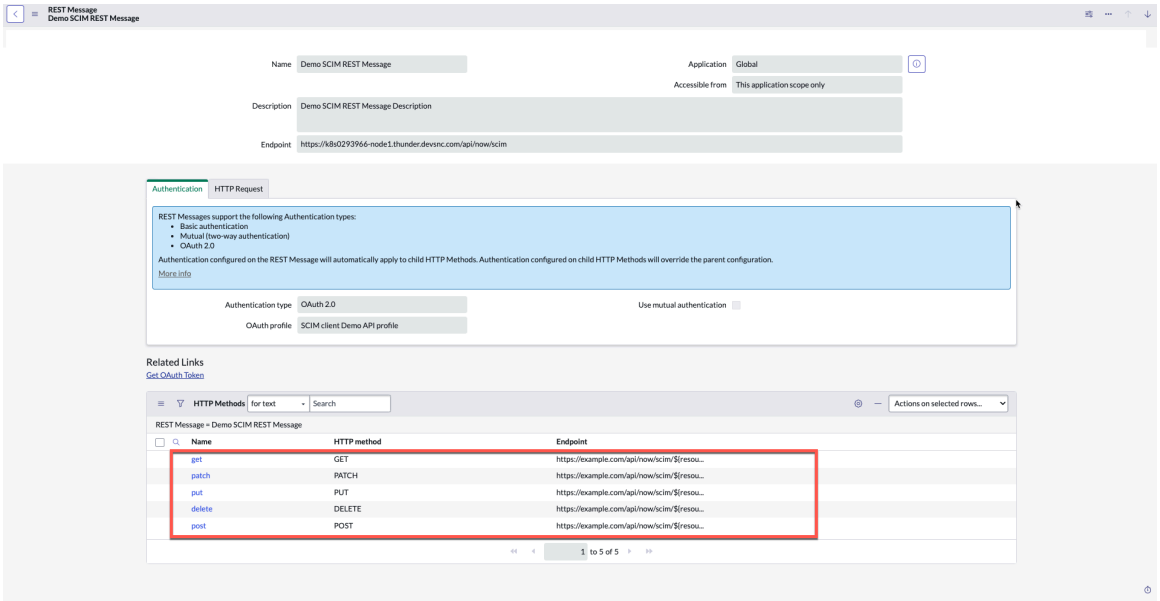
   주: URL에는 바꿔야 하는 변수가 있습니다.

   HTTP 메서드

방법	샘플 **URL**
임포트	`https://example.com/api/now/scim/${resourceName}`
패치	`https://example.com/api/now/scim/${resourceName}/${resourceId}`
넣기	`https://example.com/api/now/scim/${resourceName}/${resourceId}`
삭제	`https://example.com/api/now/scim/${resourceName}/${resourceId}`
게시	`https://example.com/api/now/scim/${resourceName}/${resourceId}`

   주:
   - SCIM 클라이언트 작업을 위한 모든 HTTP 메서드를 만들어야 합니다.
   - 샘플 REST 메시지는 기본 시스템에서 제공됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



6. 제출을 클릭합니다.

결과
REST 메시지 기록이 생성됩니다.

다음에 수행할 작업
REST 메시지를 사용하여 SCIM 제공자를 생성합니다. 자세한 내용은 SCIM 제공자 생성 문서를 참조하십시오.

REST 메시지를 만드는 방법에 대한 자세한 내용은 REST 메시지 만들기를 참조하세요.

SCIM 제공자 생성

SCIM 제공자를 생성하여 REST 메시지와 함께 SCIM 제공자로부터 자원 유형 및 스키마 정보를 가져옵니다. HTTP 메서드(PUT 또는 PATCH)의 구성을 활성화하여 SCIM 제공자의 자원을 업데이트합니다.

시작하기 전에

주: 샘플 SCIM 제공자는 기본 시스템의 일부입니다. 요구 사항에 따라 사용하고 구성하거나 새 기록을 만들 수 있습니다.

필요한 역할: admin

프로시저

1. 다음으로 이동 모두 > **SCIM** 클라이언트 > **SCIM** 제공자.

2. SCIM 제공자 페이지에서 새로 만들기를 클릭합니다.

3. 양식의 필드에 내용을 입력합니다.

SCIM 제공자 양식

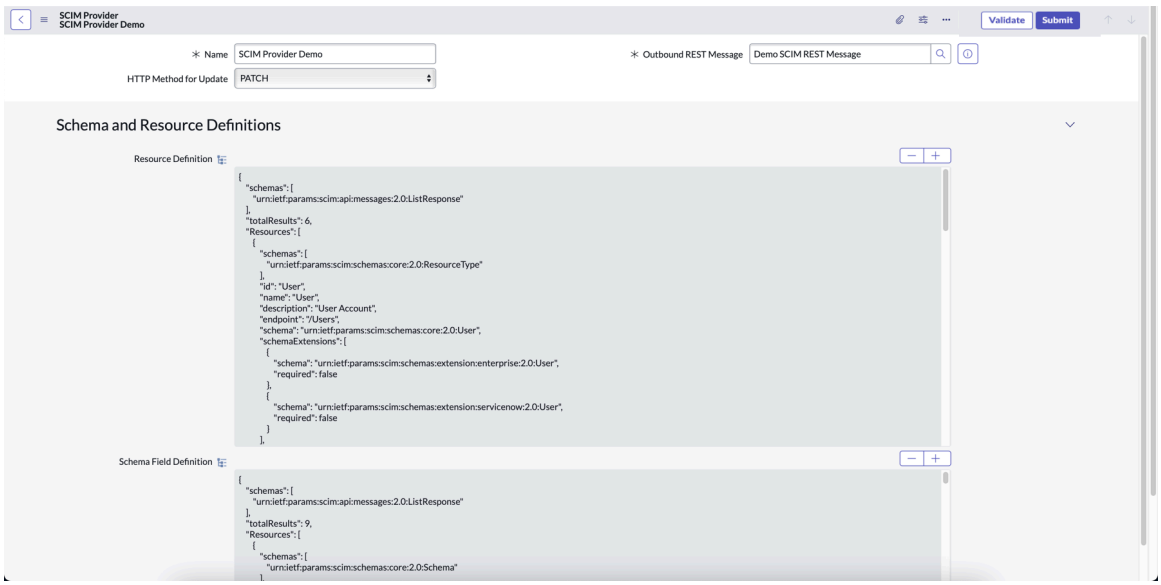
필드	설명
이름	SCIM 제공자의 이름
아웃바운드 REST 메시지	SCIM 제공자의 API를 호출하는 데 사용되는 메시지입니다. 자세한 내용은 REST 메시지 생성 문서를 참조하십시오.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
업데이트를 위한 HTTP 메서드	자원 매핑을 업데이트하는 데 사용되는 HTTPS 방법의 유형입니다. PATCH 또는 PUT 메서드는 이미 존재하는 리소스를 프로비전하는 동안 ID 리소스를 업데이트하는 동안 클라이언트에서 사용할 수 있습니다.

주:

- 자원 정의 및 스키마 필드 정의 필드는 SCIM 제공자의 공개 엔드포인트에서 */ResourceTypes/Schemas* 가져옵니다. 이러한 필드는 나머지 메시지를 선택한 후에 자동으로 채워집니다.
- SCIM 제공자에서 REST 메시지, 스키마 또는 자원 유형이 업데이트된 경우 새로 고침 을 클릭한 다음 업데이트를 클릭하여 자원 정의 및 스키마 필드 정의 필드를 업데이트합니다.



4. 제출을 클릭합니다.

결과
SCIM 제공자 상세 정보가 성공적으로 생성되었습니다. SCIM 제공자 리소스 매핑을 사용하여 SCIM 제공자 상세 정보를 사용자 또는 그룹과 같은 자원에 매핑합니다. 자세한 내용은 SCIM 제공자 리소스 매핑 생성 문서를 참조하십시오.

SCIM 제공자 리소스 매핑 생성

특정 자원 유형 및 SCIM 제공자의 속성에 대한 SCIM 속성의 ServiceNow 매핑을 정의합니다.

시작하기 전에
필요한 역할: admin

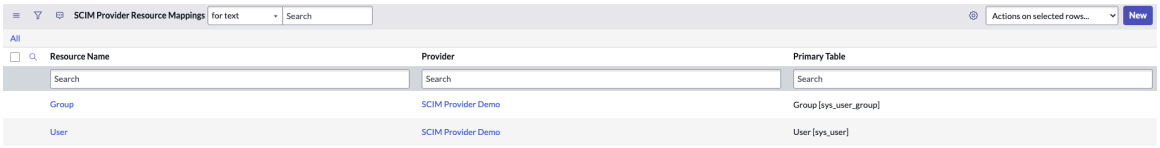
프로시저

1. 다음으로 이동 모두 > **SCIM** 클라이언트 > **SCIM** 제공자 리소스 매핑.

   SCIM 제공자 리소스 매핑은 기본적으로 사용자 및 그룹 매핑과 함께 제공됩니다.

   주: 사용자 또는 그룹 매핑에는 참조로 사용할 수 있는 샘플 매핑이 포함되어 있습니다. 사용자 또는 그룹 자원을 기반으로 매핑을 생성할 수도 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

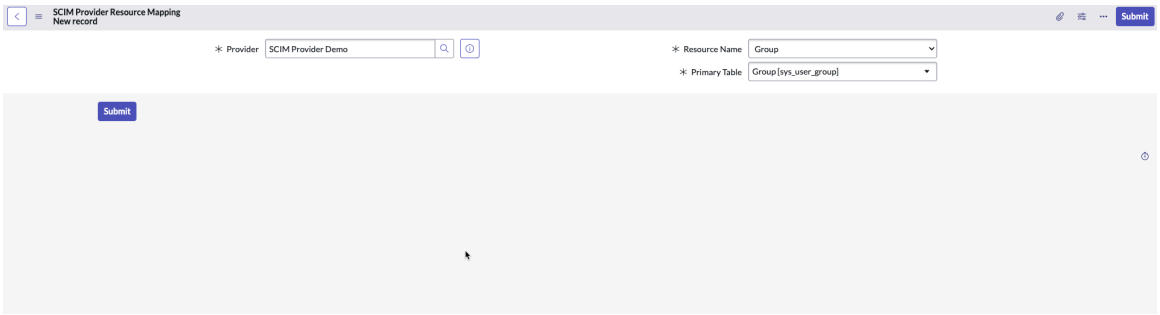


2. 새로 만들기를 클릭하여 리소스 매핑을 생성합니다.

3. 양식의 필드에 내용을 입력합니다.

리소스 매핑

필드	설명
제공자	SCIM 제공자의 이름입니다. SCIM 제공자를 생성할 때 구성된 제공자 이름을 참조하십시오.
자원 이름	매핑을 정의해야 하는 자원입니다.
기본 테이블	매핑되는 자원의 sys_id 포함된 테이블입니다.



4. 제출을 클릭합니다.

결과
기록이 생성되고 SCIM 제공자 리소스 매핑 페이지에 표시됩니다. SCIM 속성 매핑을 사용하여 스키마에서 속성을 추가로 매핑합니다. 자세한 내용은 SCIM 속성 매핑 생성 문서를 참조하십시오.

SCIM 속성 매핑 생성

SCIM 속성 매핑을 생성하고 테이블 필드에 대한 ServiceNow 단일 자원 소스로 사용합니다.

시작하기 전에
필요한 역할: admin

이 태스크 정보
다음은 속성 매핑 유형과 해당 설명입니다.

속성 매핑 유형

속성 매핑 유형	설명
직접	SCIM 속성은 데이터베이스 테이블 이름 및 데이터베이스 필드 이름 필드의 도움말로 채워집니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

속성 매핑 유형

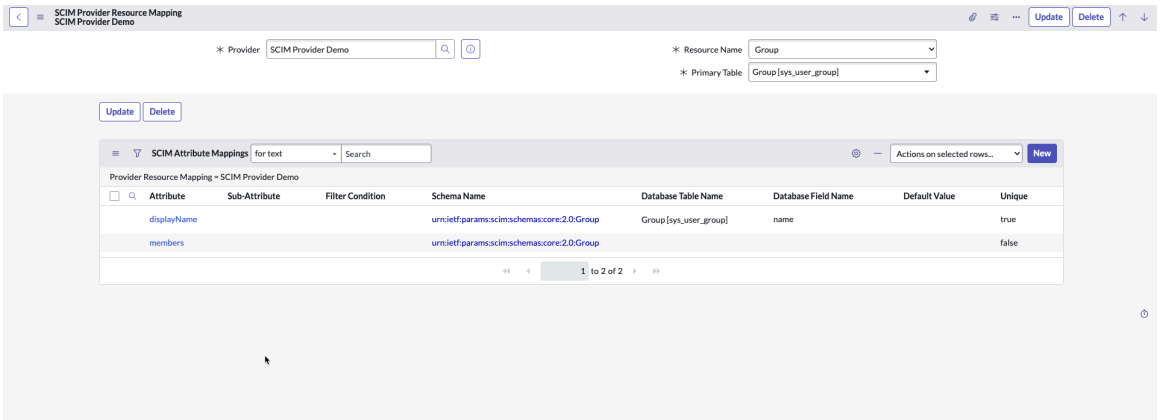
속성 매핑 유형	설명
상수	SCIM 속성은 지정된 기본값의 도움말로 채워집니다.
스크립트/사용자 지정	SCIM 특성은 스크립트의 반환 값 도움말로 채워집니다. 이 속성을 사용하려면 스크립트 실행 옵션을 활성화해야 합니다.

주:

- 암호 속성은 지원되지 않습니다.
- 사용자 및 그룹 자원에 대한 샘플 속성 매핑은 기본 시스템의 일부입니다. 요구 사항에 따라 매핑을 사용하고 구성하거나 새 기록을 만들 수 있습니다.

프로시저

1. 다음으로 이동 모두 > **SCIM** 클라이언트 > **SCIM** 제공자 리소스 매핑.
2. 구성에 대해 작성된 SCIM 리소스 매핑을 선택했습니다.
3. SCIM 속성 매핑 관련 목록에서 새로 만들기를 클릭합니다.



4. 양식의 필드에 내용을 입력합니다.

SCIM 속성 매핑 양식

필드	설명
제공자 리소스 매핑	제공자-자원 조합에 대한 속성 매핑입니다. 이 필드가 자동으로 채워지지 않으면 검색 옵션을 사용합니다. 제공자 리소스 매핑 기록을 선택합니다.
스키마 이름	매핑을 정의해야 하는 SCIM 속성의 스키마 이름입니다. 예를 들어, *urn:ietf:params:scim:schemas:core:2.0:User*을(를) 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
속성	매핑을 정의해야 하는 속성입니다. 예를 들어, *userName*을(를) 선택합니다.
하위 속성	매핑을 정의해야 하는 하위 속성(있는 경우)입니다. 예를 들어 와 같은 *name.familyName*복합 형식 속성이 있는 경우 속성은 **name** 이고 하위 속성은 **familyName**입니다.
필드 유형	SCIM 속성 데이터 유형입니다. 이 필드는 SCIM 제공자가 정의한 스키마에서 자동으로 채워집니다. 예를 들어 부울입니다.
다중 값	속성에 할당된 여러 값입니다. 속성에는 직장 이메일, 집 이메일 또는 다른 이메일과 같은 여러 값이 있을 수 있습니다. 예를 들어, *emails*을(를) 선택합니다. 이 필드는 SCIM 제공자가 정의한 스키마를 사용하여 채워집니다.
필터 조건	일부 다중값 특성에는 필터 조건을 사용하여 지정할 수 있는 추가 정보가 있을 수 있습니다. 필터 조건의 선택 항목은 SCIM 제공자가 정의한 스키마를 사용하여 채워집니다. 예를 들어 속성에는 *phoneNumbers* 직장, 모바일, 집 등의 여러 유형이 있습니다
고유	SCIM 클라이언트와 SCIM 제공자 시스템 간의 자원을 고유하게 식별하는 옵션입니다. 다중값 특성은 고유한 특성으로 표시할 수 없습니다. 예를 들어 사용자 자원의 *username* 경우 속성을 고유하게 만들 수 있습니다.
데이터베이스 테이블 이름	이 필드를 사용하여 속성 테이블 이름을 테이블 이름에 매핑합니다 ServiceNow . 직접 속성 매핑을 선택하는 경우 이 필드를 정의해야 합니다. 예를 들어, *username* SCIM 속성은 데이터베이스 테이블 이름 필드의 사용자 필드에 매핑될 수 있습니다.
데이터베이스 필드 이름	데이터베이스 필드 이름 필드는 SCIM 속성과 매핑할 필드 이름에 SCIM 속성을 ServiceNow

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

필드	설명
	매핑합니다. 직접 속성 매핑을 선택하는 경우 이 필드를 정의해야 합니다. 예를 들어, *username* SCIM 속성은 데이터베이스 필드 이름 필드의 사용자 **ID** 필드에 매핑될 수 있습니다.
기본값	SCIM 제공자에게 전달되는 기본값 에 대한 상세 정보입니다. 필드의 직접 속성 매핑이 null을 반환하거나 기본값을 사용하여 하드 코딩된 값을 반환할 수 있는 경우 사용할 수 있습니다. 하드 코딩된 값의 경우 데이터베이스 테이블 이름과 필드 이름은 **None**이어야 합니다. 예를 들어 업무용 이메일의 기본 하위 속성 값을 **true**로 하드 코딩할 수 있습니다.
스크립트 실행	스크립트를 통해 속성 값을 가져오는 옵션입니다. 이 옵션은 필터 조건이 포함되지 않은 다중값 속성에 필요합니다. 복합 속성 형식의 경우 스크립트는 속성 또는 하위 속성 수준에서 값을 제공할 수 있습니다. 예를 들어 그룹 자원의 구성원 속성에는 필터 조건이 없습니다. 따라서 script 옵션은 **Members** 특성의 부모 특성 수준에서 정의해야 합니다.
스크립트	속성 값을 가져오는 데 사용되는 스크립트입니다. 스크립트의 반환 형식은 문자열이거나 문자열로 변환된 JSON이어야 합니다. 스크립트의 출력은 해당 특성에 대해 공급자가 예상하는 적절한 형식이어야 합니다.

5. 제출을 클릭합니다.

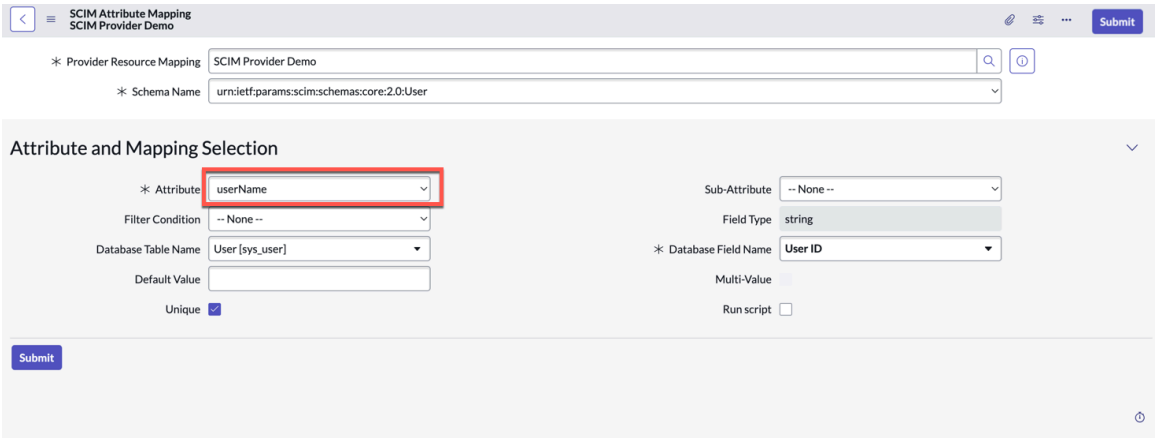
속성 매핑 참조

속성 매핑을 사용하면 속성을 테이블 필드에 대한 단일 자원 소스로 사용할 수 있습니다 ServiceNow .

속성

매핑을 정의해야 하는 속성입니다. 예를 들어, *userName*을(를) 선택합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

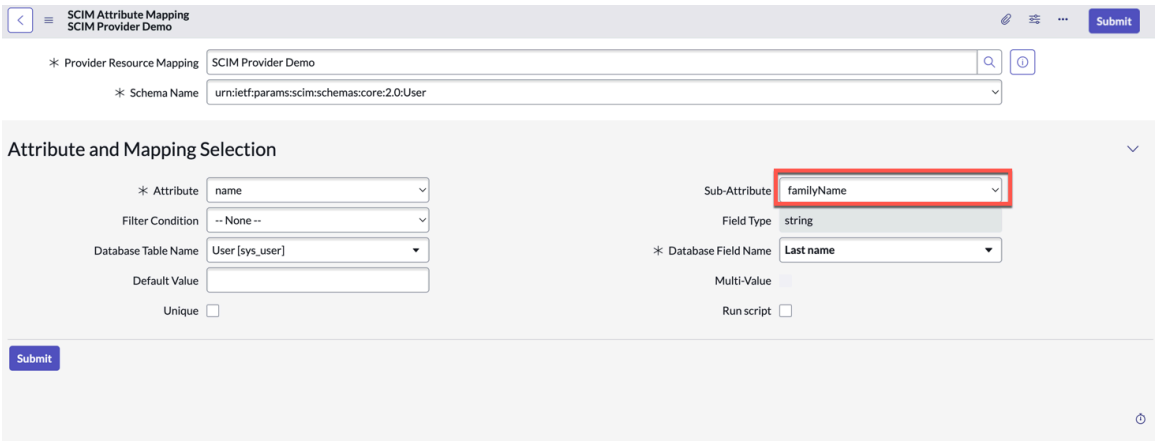


하위 속성

매핑을 정의해야 하는 하위 속성(있는 경우)을 선택합니다.

예를 들어 와 같은 *name.familyName*복합 형식 속성이 있는 경우 속성은 이고 *name* 하위 속성은 입니다 *familyName*.

사용자 이름과 같은 단순 속성의 경우 하위 속성 값은 없음입니다.



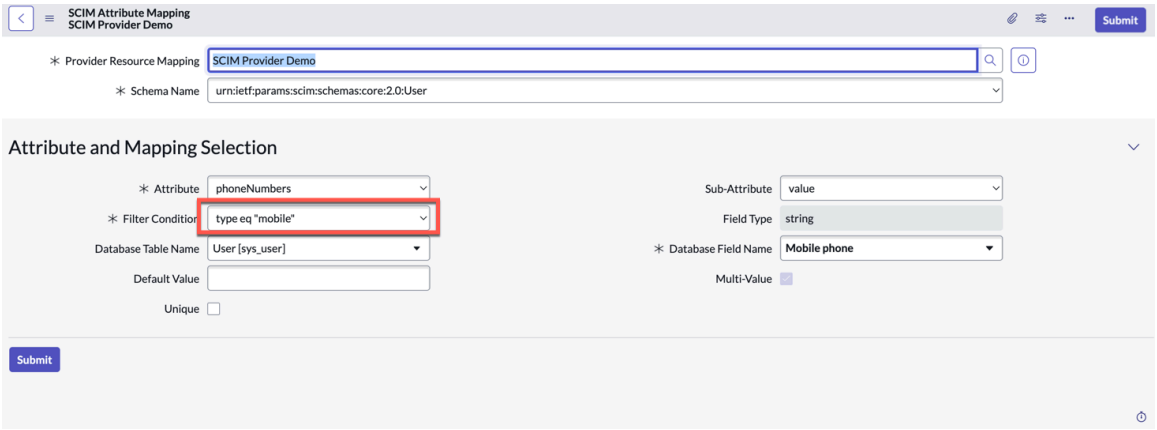
필터 조건

다중값 특성에는 필터 조건을 사용하여 지정할 수 있는 추가 정보가 있을 수 있습니다. 필터 조건에 대한 선택 항목은 SCIM 제공자가 정의한 스키마를 사용하여 채워집니다.

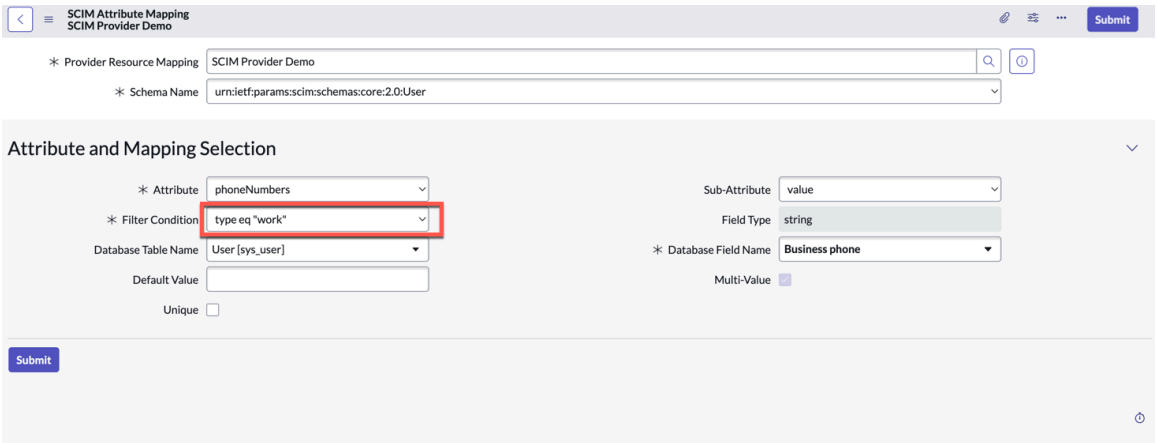
예를 들어 속성에는 *phoneNumbers* 작업, 모바일, 홈 등의 여러 유형이 있습니다.

가능한 값 집합에서 필터 조건을 지정할 수 있습니다. 예를 들어 *phoneNumber* 속성에 필터 조건이 **eq "mobile"** 유형이 있을 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



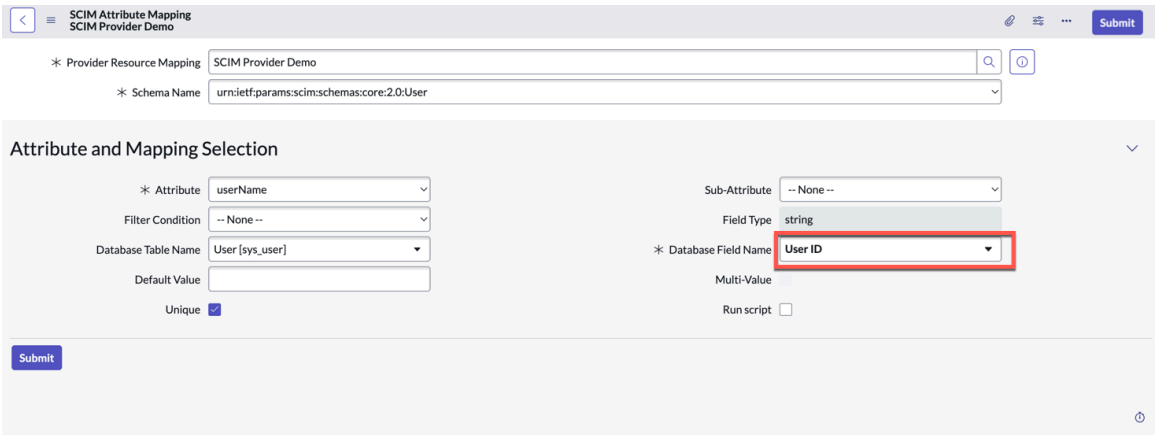
대신 *phoneNumber* 속성에 필터 조건을 **eq "work"** 유형으로 지정할 수 있습니다.



데이터베이스 필드 이름

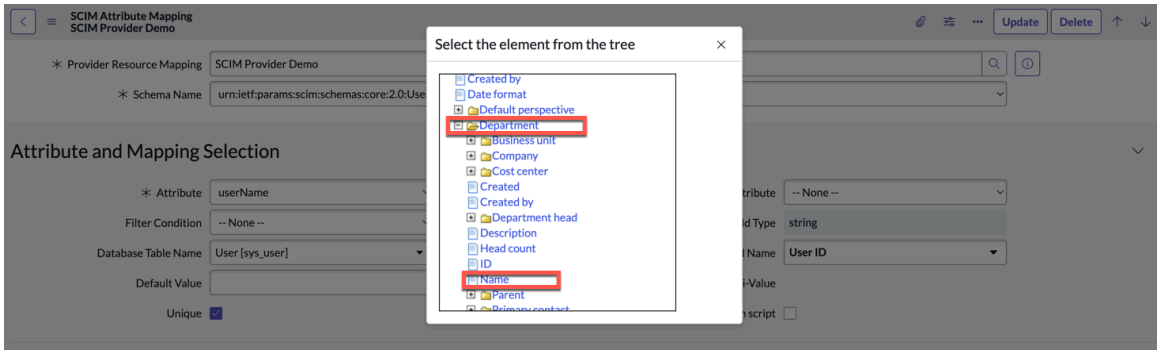
직접 속성 매핑 옵션을 선택한 경우 이 속성을 정의해야 합니다. 데이터베이스 필드 이름 필드는 SCIM 속성으로 매핑되는 필드 이름을 나타냅니다ServiceNow.

예를 들어, *username* SCIM 속성은 데이터베이스 테이블 이름 필드로 사용자에게 매핑되고 데이터베이스 필드 이름 필드로 사용자 ID 필드에 매핑될 수 있습니다.

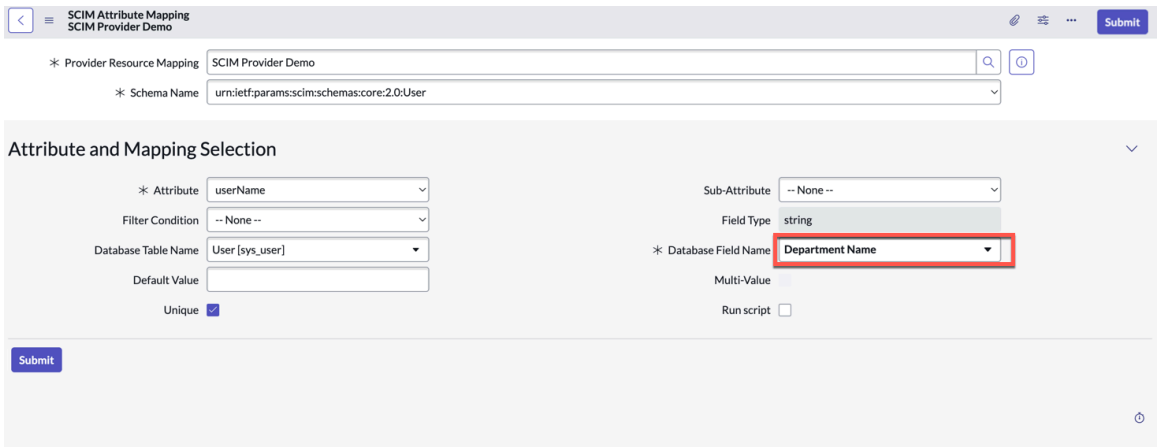


데이터베이스 필드 이름을 사용하여 닷워킹할 수도 있습니다. 예를 들어 부서 SCIM 속성을 부서 이름 필드에 매핑할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



여기서 데이터베이스 테이블은 사용자 이고 데이터베이스 필드 이름은 부서 이름입니다.

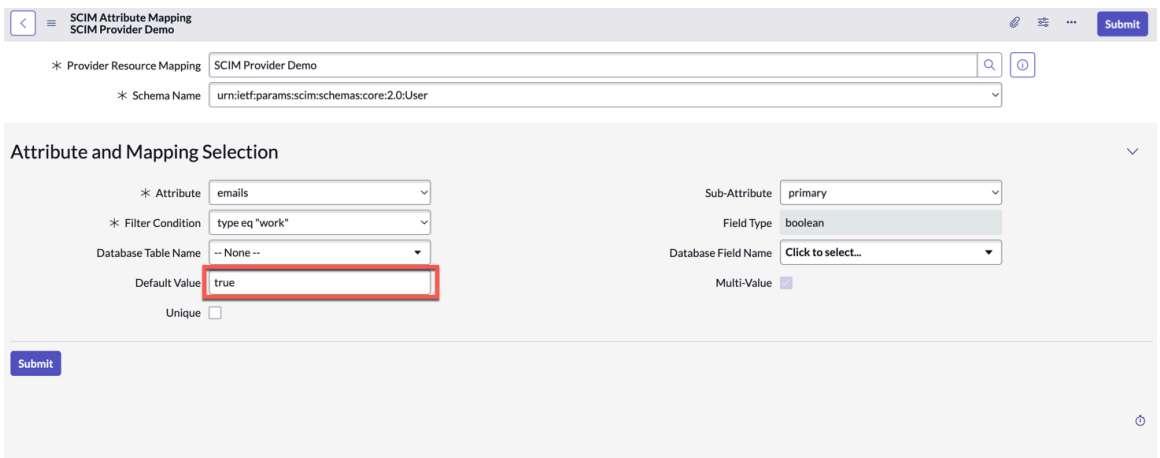


기본값

해당 필드의 직접 속성 매핑이 null을 반환하는 경우 기본값이 SCIM 제공자에게 전달됩니다. 기본값을 사용하여 하드 코딩된 값을 반환할 수도 있습니다.

하드 코딩된 값의 경우 데이터베이스 테이블 이름과 필드 이름은 **None**이어야 합니다.

예를 들어 업무용 이메일의 기본 하위 속성 값을 **true**로 하드 코딩할 수 있습니다.

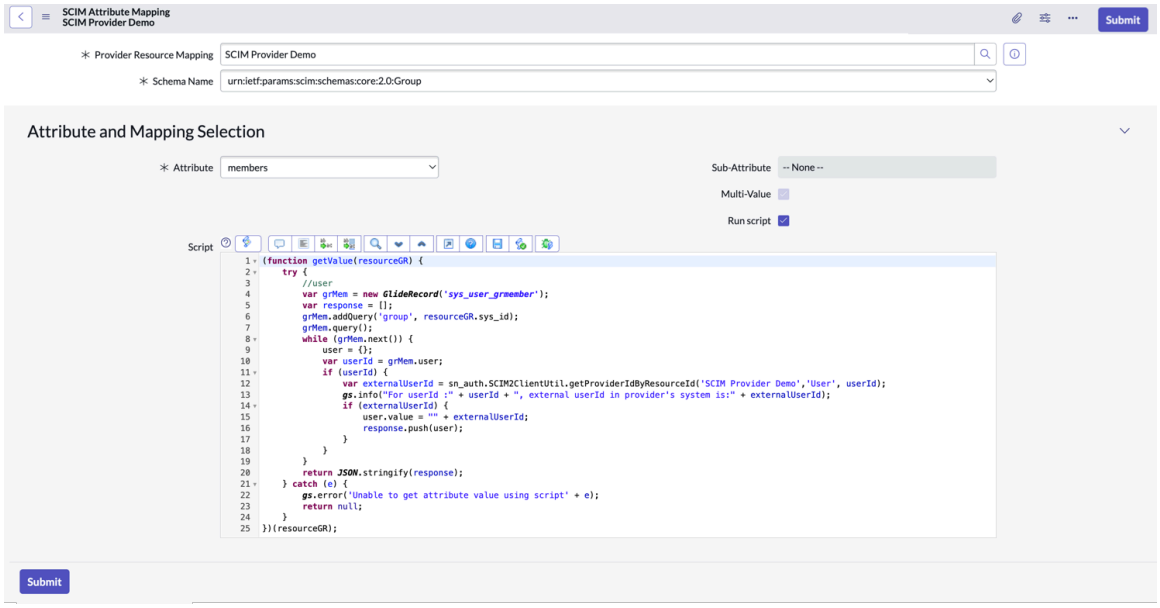


스크립트

스크립트는 속성 값을 가져오는 데 사용됩니다. 스크립트의 반환 형식은 항상 문자열이거나 문자열로 변환된 JSON이어야 합니다. 스크립트의 출력은 해당 특성에 대해 공급자가 예상하는 적절한 형식이어야 합니다.

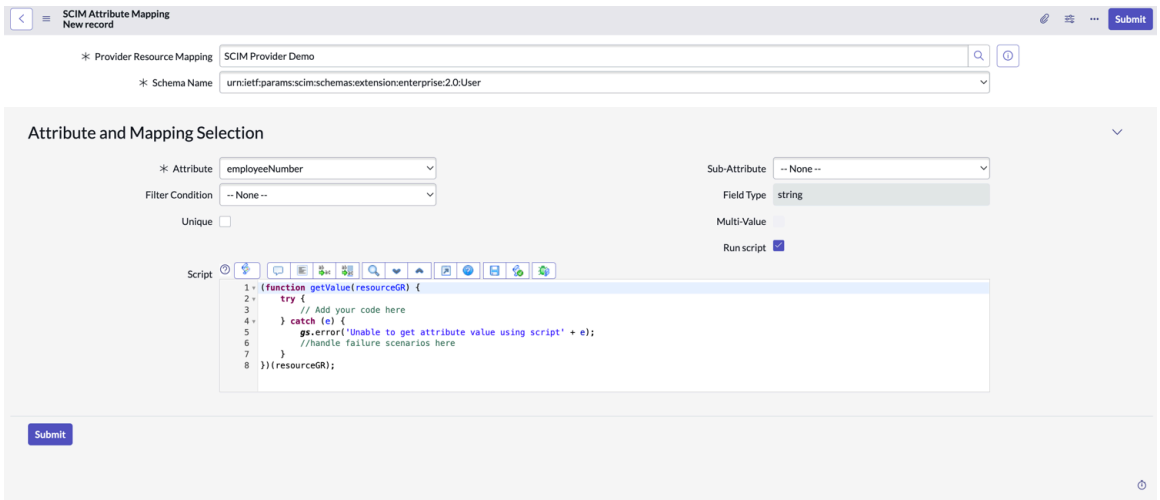
다음은 다중값 속성에 대한 샘플 스크립트입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



스크립트의 출력에는 문자열화된 JSON 배열이 있어야 합니다.

다음은 단순 값 속성의 샘플 스크립트입니다.



스크립트의 출력은 문자열이어야 합니다.

SCIM 클라이언트 문제 해결

문제 해결 작업은 SCIM 클라이언트를 설정하거나 실행할 때 발생하는 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

문제 해결

문제	동작
응답에는 다음 메시지가 포함되어 있습니다. `"message":"Unable to access the table core_company with id: 0c441abbc6112275000025157c651c89, Please cross check the Access control rules"`	사용자 컨텍스트에서 API가 호출되고 사용자에게 테이블에 대한 액세스 권한이 없는 경우 메시지가 표시됩니다. 스크립트 가능한 API가 시스템 컨텍스트에서 호출되었는지 확인해야 합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

문제 해결

문제	동작
응답에는 다음 메시지가 포함되어 있습니다. `{"message":"User Not Authenticated","detail":"Required to provide Auth information”}`	• 토큰이 해당 REST 메시지를 통해 생성되고 유효한지 확인하십시오. • 스크립트 가능한 API가 시스템 컨텍스트에서 호출되었는지 확인합니다.
응답에는 다음 메시지가 포함되어 있습니다. `Script execution failed, the reason is: Cannot cast java.lang.Integer to java.lang.String`	SCIM 속성 매핑에서 이 문제가 있는 스크립트에서 가져오도록 필드가 정의된 경우 반환 유형이 항상 문자열이어야 합니다.
응답에는 다음 메시지가 포함되어 있습니다. `"status": "400", "scimType": "invalidValue", "detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"`	ID가 필요한 SCIM 속성의 경우 해당 ID는 항상 제공자 시스템의 ID입니다. 페이로드에 전달된 ID가 제공자 시스템에서 유효한지 확인합니다.

문제 해결을 위해 확인할 영역

다음은 SCIM 클라이언트를 사용할 때 문제 해결 오류를 확인할 수 있는 몇 가지 영역입니다.

- 스크립트 가능한 API를 실행하는 동안 문제가 발견되면 SCIM 클라이언트 로그 섹션을 참조하십시오.

로그 필드

필드	설명
요청 ID	호출된 스크립트 가능한 API를 나타내는 고유 ID입니다.
SCIM 제공자	API가 호출되는 제공자 이름입니다.
자원	API가 호출되는 자원의 이름입니다.
자원 ID	API가 호출되는 ID입니다. 삭제의 경우 ID는 제공자 시스템의 리소스 ID를 나타내고 ID는 클라이언트 시스템에 있습니다.
동작	호출되는 API
상태	성공 또는 실패로 로그 상태
메시지	성공 또는 오류 메시지입니다. 오류 메시지는 SCIM 제공자로부터 또는 SCIM 클라이언트의 구성 문제로 인해 발생할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 아웃바운드 호출을 구성하고 확인하여 요청 본문을 확인합니다. 자세한 내용은 아웃바운드 웹 서비스 로깅을 참조하세요.
- 콘텐츠 형식을 추가하고, 샘플을 테스트하고, 해당 공급자의 REST 메시지에서 해당 HTTP 메서드 양식으로 이동하여 로그 수준을 업데이트합니다.
- 요청 본문이 잘린 경우 시스템 속성 *glide.outbound_http.content.max_limit*을 사용하여 제한을 늘립니다.

ID 및 액세스 감사

ID 및 액세스 감사를 사용하여 사용자, 그룹, 역할 및 ACL에 대한 변경 내용을 파악합니다.

탐색



ID 및 액세스 감사의 기능과 비즈니스 가치에 대해 알아봅니다.

구성



ID 및 액세스 감사를 구성하는 방법을 이해합니다.

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

감사 결과



ID 및 액세스 감사의 결과를 봅니다.

ID 및 액세스 감사 탐색

ID 및 액세스 감사를 사용하여 사용자, 그룹, 역할 및 ACL에 대한 변경 내용을 파악합니다.

ID 및 액세스 감사는 사용자 계정, 그룹 및 역할에서 누가 무엇을, 어디서, 언제 수정했는지에 대한 중요한 정보를 이해하는 데 도움이 됩니다.

악의적인 사용자를 탐지하고, 인스턴스의 비정상적인 활동을 ServiceNow® 추적하고, 액세스 변경을 추적할 수 있는 규정 준수 표준을 준수하는 데 도움이 됩니다.

ID 및 액세스 감사(ID 보안 감사)는 플러그인(`com.glide.security.audit`)이며 자동으로 설치됩니다.

`glide.identity.security.audit.enabled` 시스템 속성을 전환하여 감사 기능을 켜거나 끌 수 있습니다. 기본적으로 속성은 `true`로 설정됩니다.

ID 및 액세스 감사를 사용하면 다음을 수행할 수 있습니다.

- 사용자, 그룹, 역할 ACL 속성, 역할 구성원 자격, 그룹 구성원 자격 및 ACL 역할에 지난 30일 동안 변경된 내용을 봅니다.
- 인스턴스의 변경 내용을 ServiceNow 추적합니다.
- 잠재적인 보안 및 규제 위험을 완화하는 데 도움이 됩니다.
- 조직 내 여러 그룹에 대한 감사자의 규정 준수를 입증합니다.
- 조직이 사용자 그룹의 가시성 부족 및 역할 변경과 관련된 위협에 취약하지 않음을 보여줍니다.

ID 액세스 및 감사의 가상 사용자

다음은 ID 및 액세스 감사의 다양한 사용자 가상 사용자입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 관리자: 감사 기록과 구성을 봅니다.
- 보안 관리자: 이 감사 추적을 확인합니다. 특정 테이블에 대한 감사를 사용 또는 사용하지 않도록 구성을 수정하거나 감사 중인 필드를 수정합니다.

감사 테이블

ID 및 액세스 감사를 사용하여 다음 테이블을 감사할 수 있습니다.

- 그룹 [sys_user_group]
- 역할 [sys_user_role]
- 접근 제어 [sys_security_acl]
- 사용자 [sys_user]
- 그룹 역할 [sys_group_has_role]
- 사용자 역할 [sys_user_has_role]
- 접근 역할 [sys_security_acl_role]
- 포함된 역할 [sys_user_role_contains]
- 그룹 구성원 [sys_user_grmember]

ID 및 액세스 감사의 모듈

ID 및 액세스 감사에는 인스턴스에 대해 ServiceNow 다음과 같은 모듈이 있습니다.

모듈	설명
감사 결과	인스턴스에서 발생한 감사를 ServiceNow 표시합니다.
테이블 및 필드 구성	ID 및 액세스 감사에서 사용 가능한 필드로 시스템 테이블과 필드를 구성합니다.
보존 기간 구성	감사된 데이터의 보존 기간을 구성합니다. 설정할 수 있는 최대 기간은 30일입니다.
사용자 트레일	사용자에 대한 감사를 표시합니다.
그룹 트레일	그룹의 감사를 표시합니다.
역할 트레일	역할에 대한 감사를 표시합니다.
ACL 트레일	ACL에 대한 감사를 표시합니다.

ID 감사 결과

인스턴스에서 발생한 ServiceNow® 감사를 표시합니다.

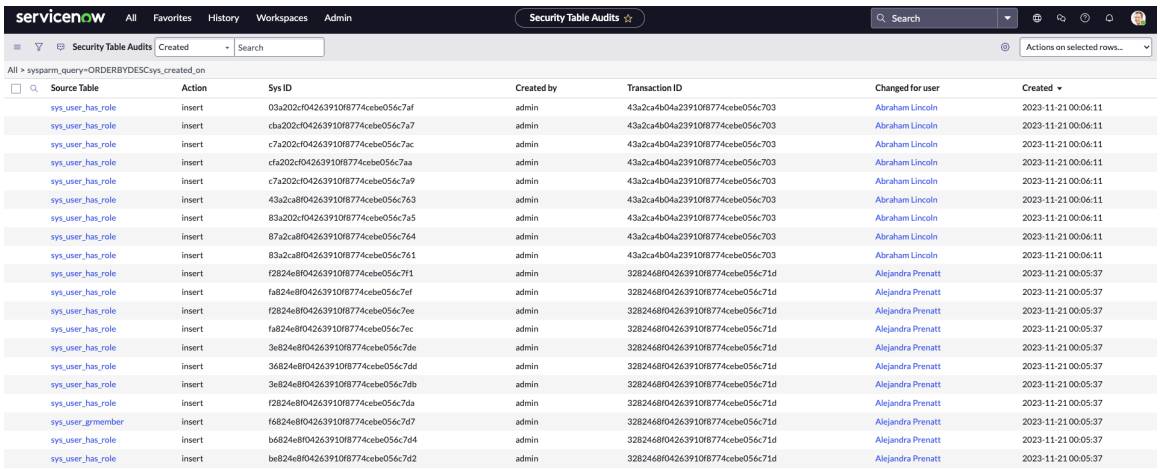
감사 결과에는 인스턴스의 사용자, 그룹, 역할 및 ACL ServiceNow 에 대한 변경 내용이 표시됩니다.

감사 결과에 액세스하려면 다음으로 이동하십시오. 모두 > 시스템 보안 > **ID** 및 액세스 감사 > 감사 결과. 다음 정보와 함께 보안 테이블 감사 페이지가 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

보안 테이블 감사

열 이름	설명
소스 테이블	감사가 발생한 소스 테이블의 상세 정보입니다.
동작	감사 작업을 설명합니다.
Sys_id	감사된 기록의 sys_id 대한 상세 정보입니다.
작성자	작성자가 작성한 감사의 상세 정보입니다.
트랜잭션 ID	수행된 특정 감사에 대한 모든 작업을 나타내는 고유 ID입니다.
사용자를 위해 변경	감사가 수행된 사용자의 이름입니다.
작성됨	감사가 수행된 시간 및 날짜입니다.



사용자 트레일

인스턴스에 있는 사용자에 대한 감사를 ServiceNow® 표시합니다.

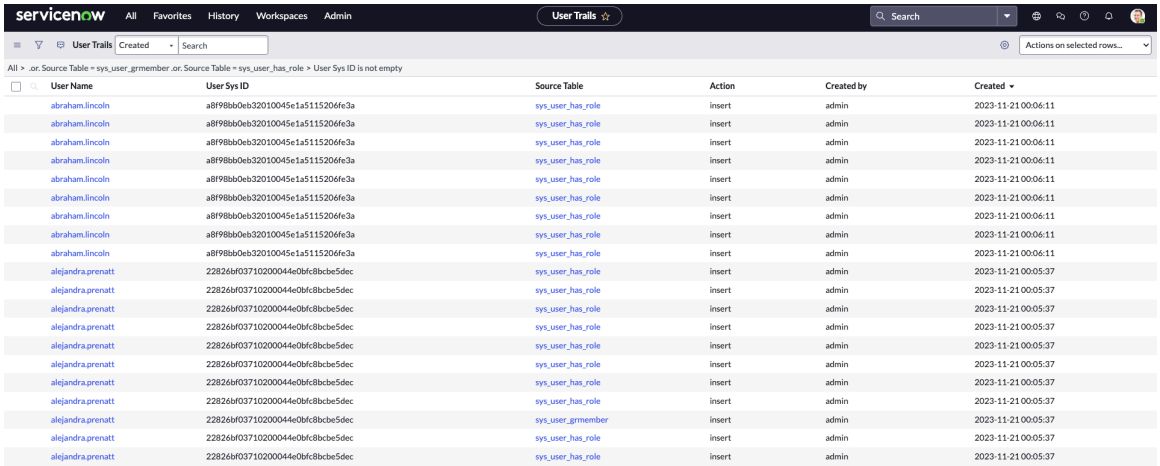
사용자 트레일에는 사용자에 대한 ID 속성 변경, 역할 구성원 자격 변경 및 그룹 구성원 자격 변경 사항이 표시됩니다.

사용자 추적에 액세스하려면 다음으로 이동하십시오. 모두 > 시스템 보안 > **ID** 및 액세스 감사 > 사용자 트레일. 사용자 트레일 페이지에는 다음 정보가 표시됩니다.

사용자 트레일

사용자 이름	사용자의 이름입니다.
사용자 시스템 ID	감사된 기록의 사용자 sys_id 대한 상세 정보입니다.
소스 테이블	감사가 수행된 소스 테이블에 대한 상세 정보입니다.
동작	감사 작업을 설명합니다.
작성자	변경한 사용자입니다.
작성됨	감사가 수행된 시간 및 날짜입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



그룹 트레일

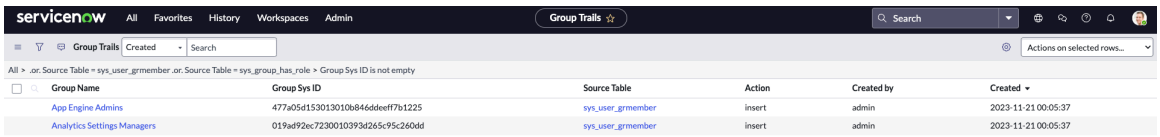
인스턴스에 있는 그룹의 감사를 ServiceNow® 표시합니다.

그룹 트레일에는 그룹의 속성 변경, 구성원 자격 변경 및 역할 변경이 표시됩니다.

그룹 트레일에 액세스하려면 다음으로 이동하십시오. 모두 > 시스템 보안 > **ID** 및 액세스 감사 > 그룹 트레일. 다음 정보와 함께 그룹 트레일 페이지가 표시됩니다.

그룹 트레일

그룹 이름	그룹의 이름입니다.
그룹 시스템 ID	감사된 기록의 그룹 sys_id에 대한 상세 정보입니다.
소스 테이블	감사가 수행된 소스 테이블에 대한 상세 정보입니다.
동작	감사 작업을 설명합니다.
작성자	변경한 사용자입니다.
작성됨	감사가 수행된 시간 및 날짜입니다.



역할 트레일

인스턴스의 역할에 대한 감사를 ServiceNow® 표시합니다.

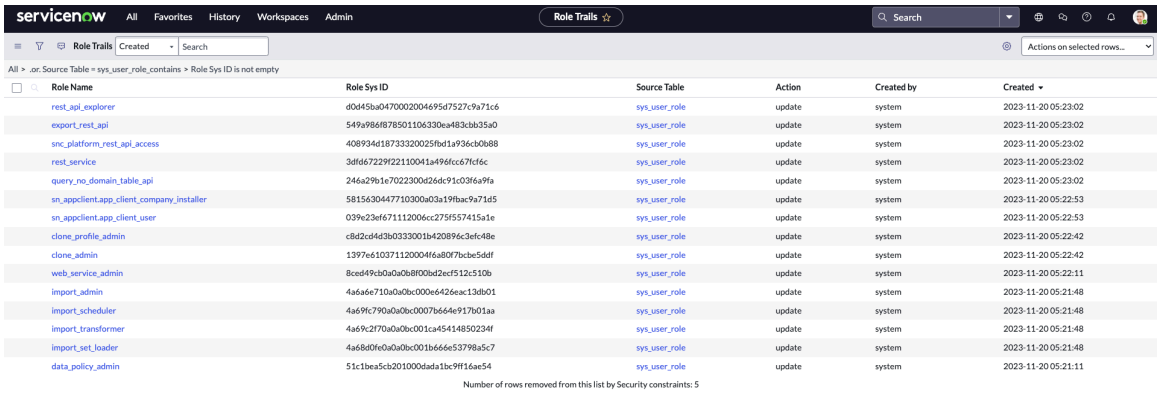
역할 트레일에는 역할의 속성 변경 내용과 상위-하위 관계 변경 내용이 표시됩니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

역할 추적에 액세스하려면 다음으로 이동하십시오. 모두 > 시스템 보안 > **ID** 및 액세스 감사 > 역할 트레일. 역할 트레일 페이지는 다음 정보와 함께 표시됩니다.

역할 트레일

역할 이름	역할의 이름입니다.
역할 시스템 ID	감사된 기록의 역할 sys_id 대한 상세 정보입니다.
소스 테이블	감사가 수행된 소스 테이블에 대한 상세 정보입니다.
동작	감사 작업을 설명합니다.
작성자	변경한 사용자입니다.
작성됨	감사가 수행된 시간 및 날짜입니다.



ACL 트레일

인스턴스의 ACL에 대한 감사를 ServiceNow® 표시합니다.

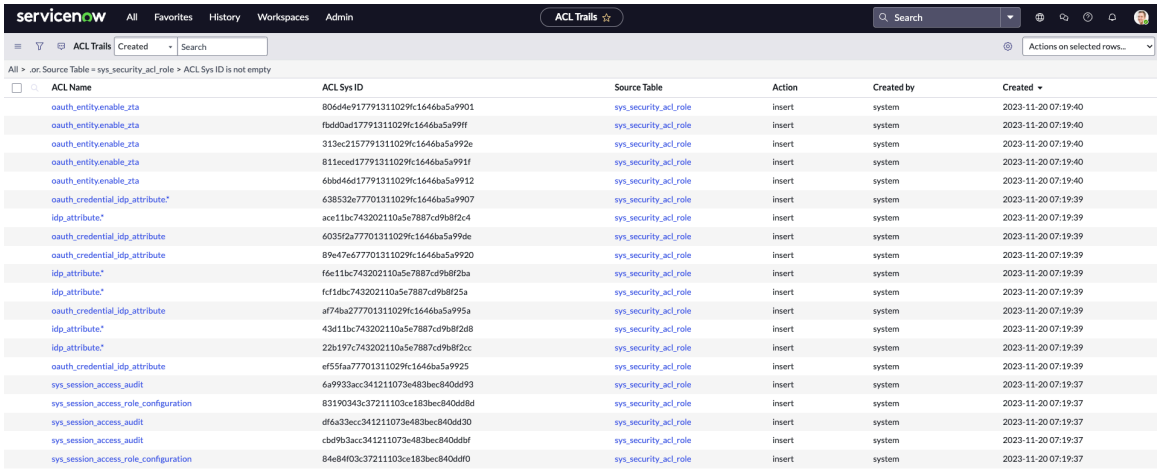
ACL 트레일에는 ACL에 대한 속성 변경 및 필요한 역할 관계 변경 내용이 표시됩니다.

ACL 추적에 액세스하려면 다음으로 이동합니다. 모두 > 시스템 보안 > **ID** 및 액세스 감사 > **ACL** 트레일. ACL 트레일(ACL Trails) 페이지가 다음 정보와 함께 표시됩니다.

ACL 트레일

ACL 이름	ACL의 이름입니다.
ACL 시스템 ID	감사된 기록의 ACL sys_id 대한 상세 정보입니다.
소스 테이블	감사가 수행된 소스 테이블에 대한 상세 정보입니다.
동작	감사 작업을 설명합니다.
작성자	변경한 사용자입니다.
작성됨	감사가 수행된 시간 및 날짜입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



보안 감사 가능 필드

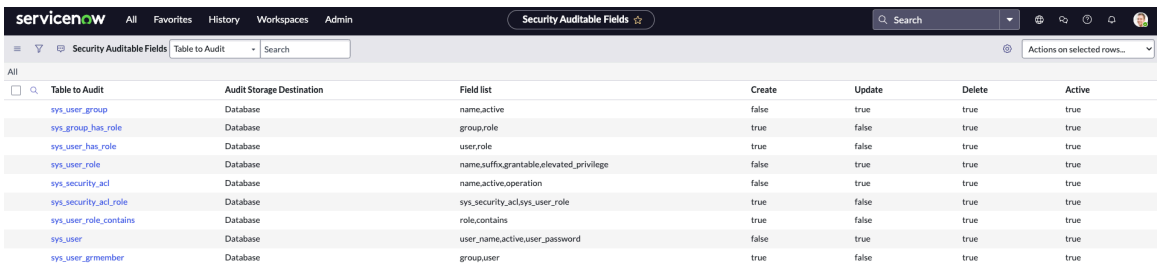
인스턴스에서 감사 ServiceNow® 할 테이블 및 필드 수준 상세 정보를 표시합니다.

보안 감사 가능 필드에는 인스턴스에서 감사 ServiceNow 할 테이블 및 필드의 상세 정보가 표시됩니다.

보안 감사 가능 필드 페이지에 액세스하려면 다음으로 이동하십시오. 모두 > 시스템 보안 > **ID** 및 액세스 감사 > 테이블 및 필드 구성. 보안 감사 가능 필드 페이지가 다음 정보와 함께 표시됩니다.

보안 감사 가능 필드

열 이름	설명
감사할 테이블	감사되는 테이블의 상세 정보입니다.
스토리지 대상 감사	감사 상세 정보가 저장되는 대상의 상세 정보입니다.
필드 목록	목록에 지정된 필드에 대해 감사가 수행됩니다.
작성	만들기 작업과 관련된 변경 내용을 감사합니다.
업데이트	업데이트 작업과 관련된 변경 사항을 감사합니다.
삭제	삭제 작업과 관련된 변경 사항을 감사합니다.
활성	테이블 구성이 활성 상태인 경우에만 감사합니다.



ID 및 액세스 감사를 사용하여 다음 테이블을 감사할 수 있습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

- 그룹 [sys_user_group]
- 역할 [sys_user_role]
- 접근 제어 [sys_security_acl]
- 사용자 [sys_user]
- 그룹 역할 [sys_group_has_role]
- 사용자 역할 [sys_user_has_role]
- 접근 역할 [sys_security_acl_role]
- 포함된 역할 [sys_user_role_contains]
- 그룹 구성원 [sys_user_grmember]

테이블 및 필드 구성

사용자, 그룹, 역할 및 ACL에 대한 변경 사항을 이해하기 위한 ID 및 액세스 감사입니다.

시작하기 전에

필요한 역할: security_admin

ID 및 액세스 감사를 위한 테이블과 필드를 구성하려면 역할을 보안 관리자로 승격해야 합니다.

감사를 위해 다음 테이블을 구성할 수 있습니다.

- 그룹 [sys_user_group]
- 역할 [sys_user_role]
- 접근 제어 [sys_security_acl]
- 사용자 [sys_user]
- 그룹 역할 [sys_group_has_role]
- 사용자 역할 [sys_user_has_role]
- 접근 역할 [sys_security_acl_role]
- 포함된 역할 [sys_user_role_contains]
- 그룹 구성원 [sys_user_grmember]

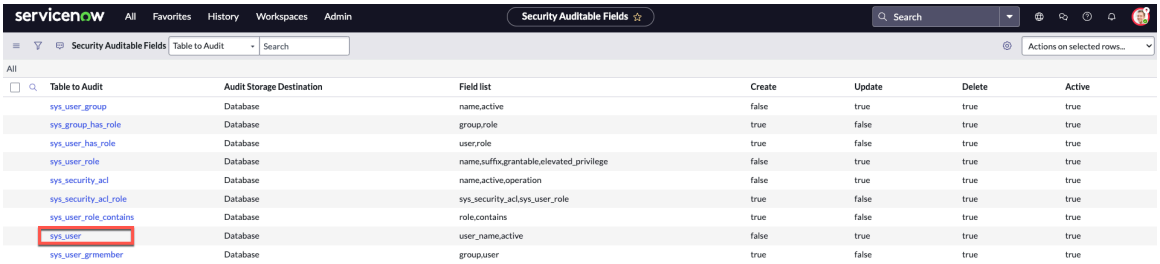
> 주: 테이블에 대해 구성할 수 있는 필드를 이해하려면 다음 문서를 참조하십시오 ID 액세스 및 감사에 대해 지원되는 필드와 지원되지 않는 필드.

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > **ID** 및 액세스 감사 > 테이블 및 필드 구성.
2. 필드를 감사할 테이블을 선택합니다.

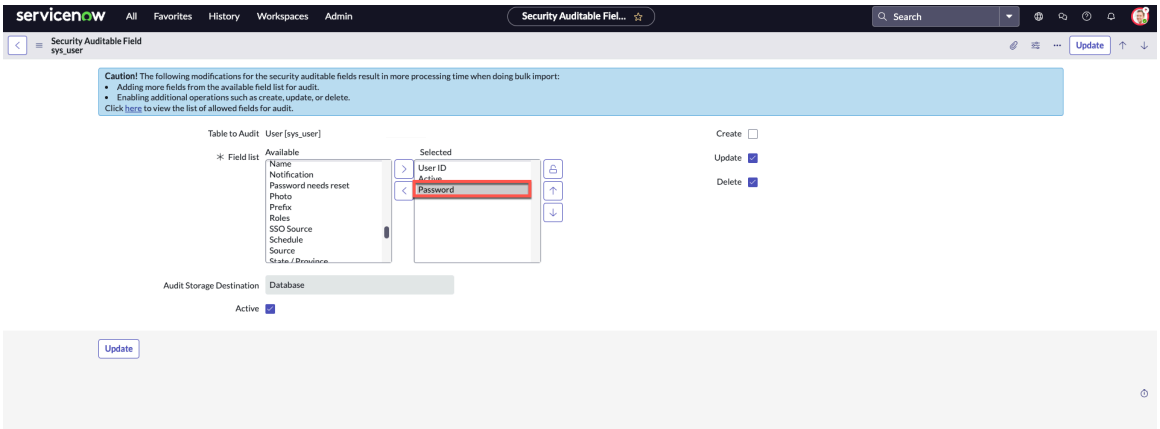
   예: **sys_user**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.



3. 감사할 필드를 추가합니다.

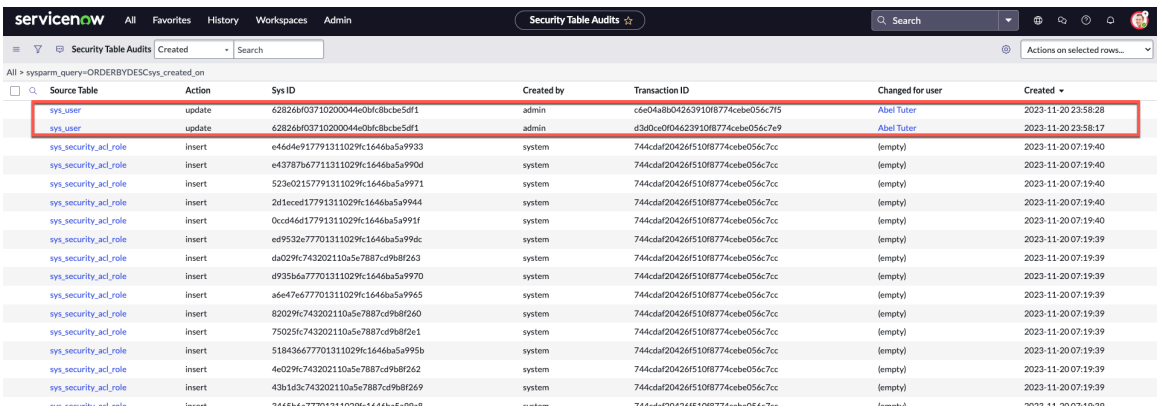
예를 들어 암호입니다.



> **주:** 보안 감사 가능 필드를 다음과 같이 수정하면 대량 임포트를 수행할 때 처리 시간이 더 길어집니다.
>
> - 감사에 사용 가능한 필드 목록에서 필드를 더 추가합니다.
> - 생성, 업데이트, 삭제와 같은 추가 작업을 사용합니다.

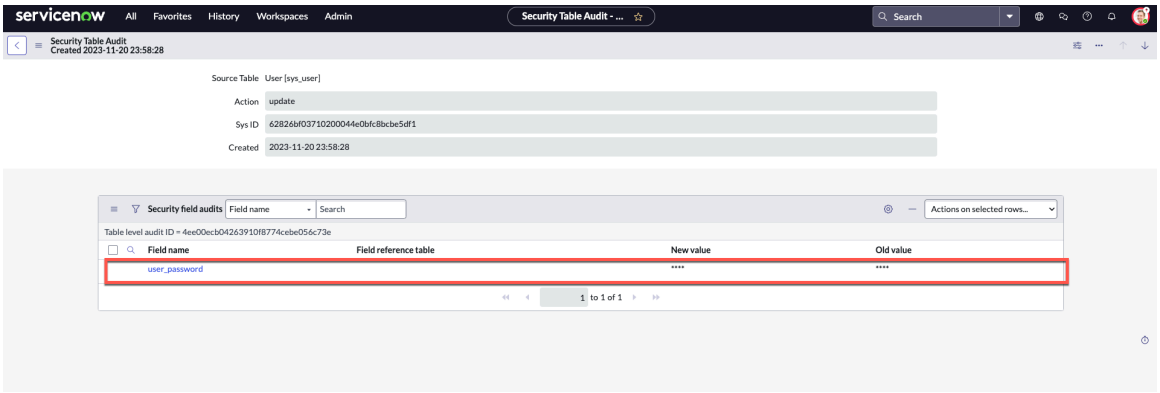
4. 기록을 업데이트합니다.

암호 필드를 변경하면 보안 테이블 감사에 새 기록이 추가됩니다. 이 예에서 감사는 사용자 **Abel Tuter**에 대해 변경된 암호 필드를 보여줍니다.



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

생성된 기록을 선택하면 변경 내용에 대한 상세 정보가 표시됩니다.



보존 기간 구성

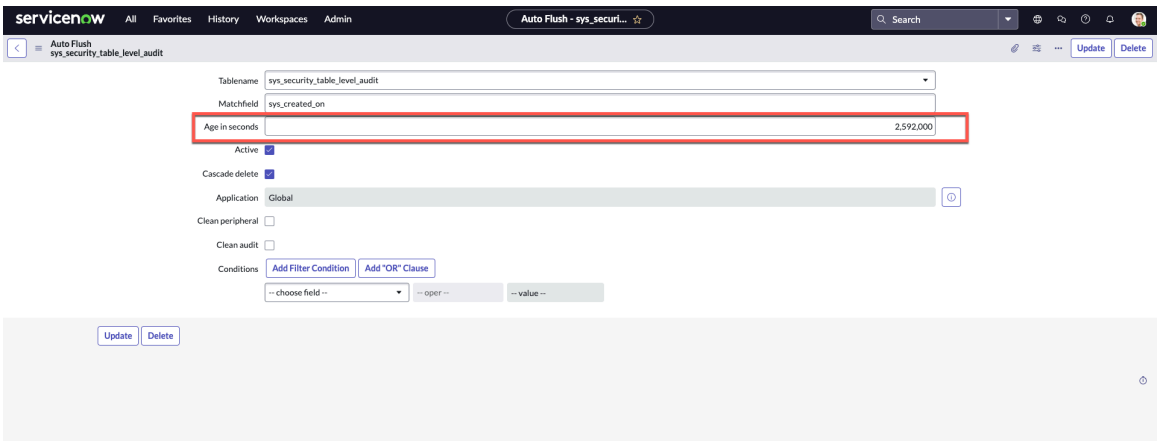
ID 및 액세스 감사의 보존 기간을 구성합니다.

시작하기 전에
필요한 역할: 관리자

프로시저

1. 다음으로 이동 모두 > 시스템 보안 > **ID** 및 액세스 감사 > 보존 기간 구성.
2. 양식에서 기간을 초 단위로 변경할 수 있습니다.

   주: ID 및 액세스 감사의 최대 일수는 30일(2,592,000초)입니다.



3. 기록을 저장하거나 업데이트합니다.

ID 액세스 및 감사에 대해 지원되는 필드와 지원되지 않는 필드

감사가 지원되는 필드와 지원되지 않는 필드 목록입니다.

감사 필드 확인으로 인해 sys_sec_field_audit_config(보안 필드 감사 구성) 테이블의 field_list에서 일부 필드가 선택되지 않습니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

감사에 대해 지원되거나 지원되지 않는 필드

테이블	지원되거나 지원되지 않는 필드
모든 테이블	지원되지 않는 필드: • 작성 날짜(sys_created_on) • 작성자(sys_created_by) • 업데이트한 사람(sys_updated_by) • 업데이트 날짜(sys_updated_on)
사용자에게 역할이 있음**(sys_user_has_role)**	지원되는 필드: • 사용자 • 역할 • 상속됨 • 카운트
사용자**(sys_user)**	지원되지 않는 필드: • 마지막 로그인(last_login) • 마지막 로그인 시간(last_login_time) • 마지막 로그인 장치(last_login_device) • enable_multifactor_authn(Multi-factor Authentication) 사용 • 기본 관점(default_perspective) • 달력 통합(calendar_integration) • 페더레이션 ID(federated_id) • 암호 재설정 필요(password_needs_reset) • 실패한 시도(failed_attempts) • 마지막 암호(last_password) • LDAP 서버(ldap_server) • 잠겨 있음(locked_out) • 알림(notification) • 역할(roles) • 도메인(sys_domain) • 도메인 경로(sys_domain_path) • 시간 형식(time_format) • 해시된 사용자 ID(hashed_user_id) • 클래스 이름(sys_class_name) • 모드 수(sys_mod_count)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

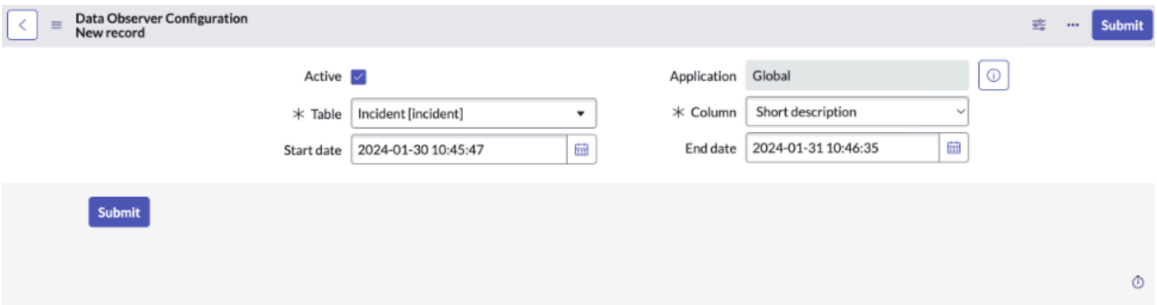
접근 관찰자

접근 관찰자를 사용하여 인스턴스의 사람과 프로세스 액세스 데이터를 이해합니다.

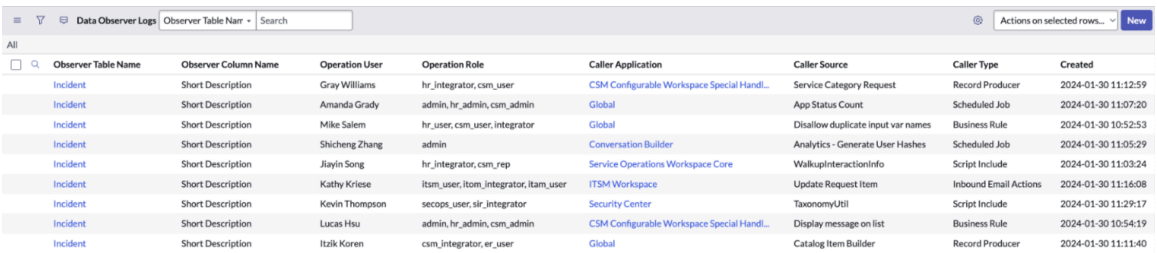
접근 관찰자를 통해 보안 관리자는 다음을 수행할 수 있습니다.

- 데이터에는 액세스하는 사용자, 역할, 범위가 지정된 앱 및 스크립트와 같은 엔터티가 무엇인지 파악합니다.
- 이 예지를 사용하여 데이터에 대한 불필요한 액세스를 제한하기 위해 보안을 적용하는 가장 좋은 방법을 아는 동시에 액세스가 필요하고 여전히 정상적으로 작동하는 것을 확인합니다.
- 보안을 변경하기 전에 데이터에 액세스하는 방법을 명확하게 확인하여 자동화가 중단되는 것을 방지합니다.
- 인스턴스에 암호화를 적용하는 방법에 대한 정보를 제공해야 하는 문제를 해결합니다.

접근 관찰자 구성 기록을 생성하여 접근 관찰자를 구성합니다. 이러한 기록 내에서 관찰할 특정 테이블과 열 및 열을 관찰하는 시간을 정의합니다.



접근 참관인 로그 기록 테이블에서 관찰 결과를 찾습니다. 이 테이블에서 지정된 열에 액세스할 때마다 자세히 설명하는 기록을 볼 수 있습니다.



Observer Table Name	Observer Column Name	Operation User	Operation Role	Caller Application	Caller Source	Caller Type	Created
Incident	Short Description	Gray Williams	hr_integrator, csm_user	CSM Configurable Workspace Special Handl...	Service Category Request	Record Producer	2024-01-30 11:12:59
Incident	Short Description	Amanda Grady	admin, hr_admin, csm_admin	Global	App Status Count	Scheduled Job	2024-01-30 11:07:20
Incident	Short Description	Mike Salem	hr_user, csm_user, integrator	Global	Disallow duplicate input var names	Business Rule	2024-01-30 10:52:53
Incident	Short Description	Shicheng Zhang	admin	Conversation Builder	Analytics - Generate User Hashes	Scheduled Job	2024-01-30 11:05:29
Incident	Short Description	Jiayin Song	hr_integrator, csm_rep	Service Operations Workspace Core	WalkupInteractionInfo	Script Include	2024-01-30 11:03:24
Incident	Short Description	Kathy Kriese	itsm_user, itom_integrator, itam_user	ITSM Workspace	Update Request Item	Inbound Email Actions	2024-01-30 11:16:08
Incident	Short Description	Kevin Thompson	secops_user, sir_integrator	Security Center	TaxonomyUtil	Script Include	2024-01-30 11:29:17
Incident	Short Description	Lucas Hsu	admin, hr_admin, csm_admin	CSM Configurable Workspace Special Handl...	Display message on list	Business Rule	2024-01-30 10:54:19
Incident	Short Description	Itzik Koren	csm_integrator, er_user	Global	Catalog Item Builder	Record Producer	2024-01-30 11:11:40

접근 관찰 구성

접근 관찰 기록을 생성하여 지정된 기간 동안 데이터 열에 대한 액세스를 검토합니다.

시작하기 전에
필요한 역할: security_admin

프로시저

1. 다음으로 이동 모두 > 접근 관찰자 > 접근 관찰자 구성.
2. 새로 만들기를 선택하여 기록을 생성합니다.
3. 양식의 필드에 내용을 입력합니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 관찰자 구성 필드

필드	설명
활성	기록의 활성화 여부입니다. 관찰 기간 동안에는 기록이 자동으로 활성으로 표시되고 그 외에는 비활성화됩니다.
애플리케이션	기록에 대한 범위의 애플리케이션입니다. 이 필드는 읽기 전용입니다.
테이블	관찰할 열이 포함된 테이블
열	관찰할 선택한 테이블 내의 열입니다.
즉시 작업 시작	이 옵션을 선택하면 기록이 생성되는 즉시 관찰이 시작됩니다.
종료 날짜 및 시간	관찰이 종료되는 시간입니다.
시작 날짜 및 시간	관찰이 시작되는 시간입니다. 이 필드는 작업 즉시 시작을 선택하지 않은 경우에만 표시됩니다.

4. 제출을 선택하여 기록을 저장합니다.

다음에 수행할 작업
정의한 관찰 창이 시작되면 접근 관찰자 로그 [sys_data_ob_log] 테이블의 기록에 자세히 설명된 열에 액세스한 각 인스턴스를 볼 수 있습니다.

접근 관찰자 로그 검토

액세스 관찰자 로그 기록의 정보를 사용하여 데이터에 액세스하는 방법에 대한 인사이트를 얻을 수 있습니다.

하나 이상의 접근 관찰 기록을 구성하면 인스턴스가 선택한 열에 대한 액세스에 대한 상세 정보를 포함하는 접근 관찰자 로그 기록을 생성하기 시작합니다. 다음 인스턴스에서 이러한 기록을 찾을 수 있습니다. 모두 > 접근 관찰자 > 접근 관찰자 로그.

접근 관찰자 로그 결과

다음 표를 사용하여 로그에 표시되는 정보를 이해합니다.

접근 관찰자 로그 필드

필드	설명
관찰자 테이블 이름	이 기록을 생성한 접근 관찰 기록에서 선택한 테이블입니다.
관찰자 열 이름	이 기록을 생성한 접근 관찰 기록에서 선택한 열입니다.
운영 사용자	열에 접근한 사용자
운영 역할	열에 접근한 사용자의 역할
호출자 애플리케이션	데이터에 접근한 범위가 지정된 애플리케이션입니다.
호출자 유형	열에 액세스한 요소의 유형(예: 기록 생성자, 예약된 작업 또는 비즈니스 규칙)입니다.
호출자 소스 문서 ID	

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

접근 관찰자 로그 필드

필드	설명
호출자 소스	열에 액세스한 요소입니다. 호출자 유형 필드를 따라 열에 액세스한 구체적인 항목을 확인하는 데 사용됩니다. 예를 들어 호출자 유형이 `#### ##`인 경우 호출자 소스는 열에 액세스한 비즈니스 규칙의 이름입니다.
기본 해시	
반복 횟수	
Java 스택	
JavaScript 스택	
세션 ID	열에 액세스한 세션의 ID입니다.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

플랫폼 보안 제품 및 솔루션에 대한 추가 자원

플랫폼 보안 베스트 프랙티스, 문제 해결 또는 기타 구현 가이드라인을 찾고 있다면 기능 또는 자원 유형을 선택하여 다른 관련 웹 사이트에서 ServiceNow 자원을 검색합니다.

주: 아래의 많은 자원을 사용하려면 Now Learning, Now Create 또는 ServiceNow 커뮤니티와 같은 사이트에 로그인해야 합니다. 예상한 자원이 로드되지 않으면 로그인하여 자원에 다시 접근해 보십시오.

자원 링크

플랫폼 보안 기능 또는 제품	자원 유형	자원
보안 센터	시작	ServiceNow 보안 센터
보안 센터	베스트 프랙티스	• 베스트 프랙티스 - 보안 센터 • 보안 센터 강화 베스트 프랙티스
보안 센터	FAQ	ServiceNow 보안 강화 - 보안 센터
코드 서명	시작	• 강화된 심층 방어를 위한 코드 서명 • 코드 서명 및 CoT(Circle of Trust): 소개
데이터 개인정보 보호	팁 및 예시	〔워싱턴 릴리스〕 데이터 개인정보 보호를 통해 의도하지 않은 민감한 데이터 노출 위험 완화
필드 암호화	팁 및 예시	ServiceNow의 필드 수준 암호화
필드 암호화 엔터프라이즈	시작	필드 수준 암호화와 플랫폼 수준 암호화의 차이점
필드 암호화	문제 해결	• 전화 번호 데이터 유형의 필드에 필드 수준 암호화가 적용되지 않는 이유 • 직원 관계 케이스의 필드 수준을 암호화하고 있습니다. • "필드 수준 암호화"를 사용하여 첨부 파일 암호화 • 암호화된 필드 구성을 삭제할 수 없음 • 케이스 테이블은 암호화된 필드 구성에서 사용할 수 없습니다. • 암호화된 필드를 쿼리하면 예약된 작업에서 일관된 결과가 반환되지 않음
필드 암호화 엔터프라이즈	문제 해결	• 필드 수준 암호화 엔터프라이즈: 초기 설정 • 필드 수준 암호화 엔터프라이즈: 제한 사항 및 고려 사항 • 필드 수준 암호화 엔터프라이즈: 관리
에지 암호화 규칙	문제 해결	• ServiceNow의 에지 암호화 규칙 개요 • 에지 암호화 규칙: 초기 설정

기계번역

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.

자원 링크

플랫폼 보안 기능 또는 제품	자원 유형	자원
		• 에지 암호화 규칙 규칙 • 에지 암호화 규칙: 제한 사항 • 에지 암호화 규칙: 관리
에지 암호화 규칙	팁 및 예시	• 에지 암호화 규칙 자원 • 에지 암호화 규칙 프록시 로그 • 에지 암호화 규칙 인증서 만료 알림
에지 암호화 규칙	문제 해결	• 에지 암호화 규칙 성능 그래프 • 에지 암호화 규칙 필드 길이 확장
데이터베이스 암호화	팁 및 예시	ServiceNow의 데이터베이스 암호화: CCS를 사용한 TSE/DBE
접근 관리	팁 및 예시	ServiceNow를 통한 ID 및 액세스 관리
제로 트러스트 액세스	문제 해결	ServiceNow의 액세스 분석기, 제로 트러스트 액세스 및 적응형 인증 관련 도움말
서비스 제공자용 도메인 분리	문제 해결	서비스 제공자용 ServiceNow 도메인 분리
보안 속성	시작	Vancouver: 보안 속성 조건 설명
데이터 필터링	시작	"데이터 필터링" 플러그인 이해
보안 역할	팁 및 예시	보안 역할은 어떻게 작동하나요?
연결 및 자격 증명	시작	연결 및 자격 증명 개요 - Now Platform에서 통합 알아보기
ServiceNow 접근 통제	팁 및 예시	접근 제어 - 쉬운 방법
볼트	시작	ServiceNow Vault 빠른 시작 가이드

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, ServiceNow 로고, Now 및 기타 ServiceNow 표시는 미국 및/또는 기타 국가에서 ServiceNow, Inc.의 상표 및/또는 등록 상표입니다.
기타 회사 및 제품 이름은 관련이 있는 해당 회사의 상표일 수 있습니다.