Cisco Defense Orchestrator를 사용하여 SSH 장치 관리

최종 변경: 2024년 12월 31일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

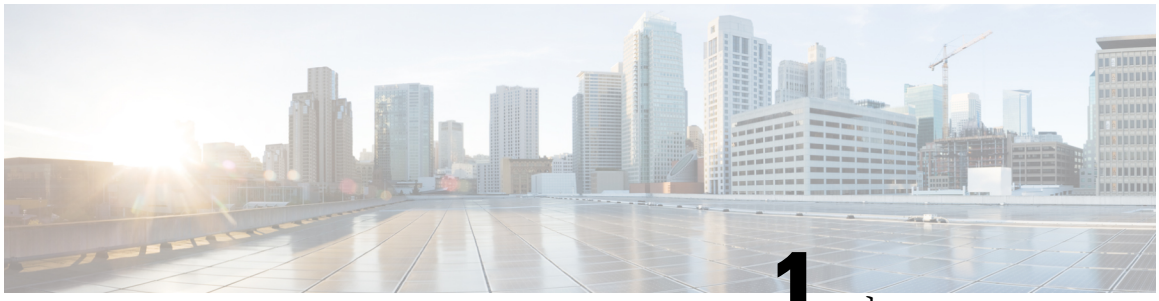
Cisco Defense Orchestrator를 사용하여 SSH 장치 관리

Cisco Defense Orchestrator를 사용하여 SSH 장치 관리

Cisco Defense Orchestrator 에서는 SSH를 통해 디바이스를 관리할 수 있습니다. 이러한 디바이스에 대해 지원되는 기능은 다음과 같습니다.

- SSH 디바이스 온보딩. SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 디바이스를 온보딩할 수 있습니다.
- CDO 디바이스 및 서비스 관리 디바이스 구성 파일을 볼 수 있습니다.
- Cisco IOS 또는 SSH에서 CDO로 변경 사항 읽기. SSH 디바이스에서 구성 파일을 읽으면 해당 파일이 CDO의 데이터베이스에 저장됩니다.
- 디바이스의 대역 외 변경 사항. 충돌 탐지를 활성화한 경우 CDO는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 변경 사항이 있는 경우 디바이스의 상태가 Conflict Detected(충돌 탐지됨)로 변경되며, 변경 충돌을 해결할 수 있습니다.
- CDO 명령줄 인터페이스. CDO의 명령줄 인터페이스를 통해 디바이스에 모든 SSH 디바이스 명령을 실행할 수 있습니다.
- 개별 CLI 명령 및 명령 그룹을 편집 및 재사용 가능한 "명령줄 인터페이스 매크로"로 전환할 수 있습니다. CDO에서 제공하는 시스템 정의 매크로를 사용하거나 자주 수행하는 작업에 대해 자신만의 매크로를 만들 수 있습니다.
- 새 지문 탐지 상태 확인. 디바이스의 자격 증명 또는 속성이 변경되어 SSH 지문이 변경되는 경우 해당 CDO는 변경 사항을 감지하고 새 지문을 검토하고 수락할 수 있는 기회를 제공합니다.
- CDO에서 변경 로그 관리. 변경 로그는 사용자가 SSH 디바이스에 실행하는 모든 명령을 캡처합니다.

Cisco Defense Orchestrator를 사용하여 SSH 장치 관리



1 장

CDO의 기본 사항

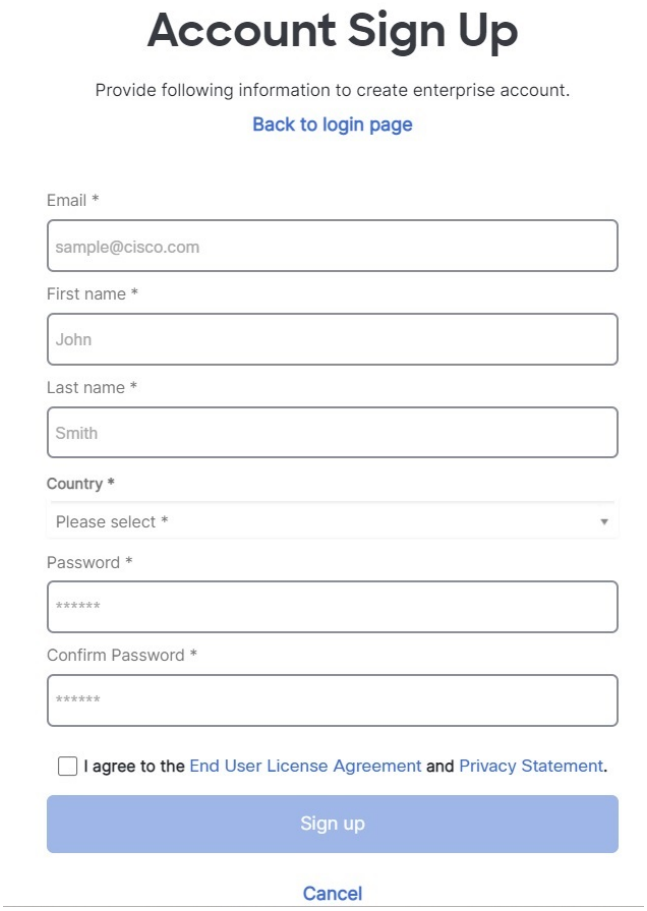
CDO는 명확하고 간결한 인터페이스를 통해 정책 관리에 대한 고유한 보기를 제공합니다. 다음은 CDO를 처음 사용할 때 기본 사항을 다루는 항목입니다.

CDO 테넌트 생성

디바이스를 온보딩하고 관리하기 위해 새 CDO 테넌트를 프로비저닝할 수 있습니다. 온프레미스 방화벽 Management Center 버전 7.2 이상을 사용하고 이를 Cisco Security Cloud와 통합하려는 경우 통합 워크플로우의 일부로 CDO 테넌트를 생성할 수도 있습니다.

절차

1. https://defenseorchestrator.com/provision로 진행합니다.
2. CDO 테넌트를 프로비저닝하려는 지역을 선택하고 **Sign Up(**등록**)**을 클릭합니다.
3. **Security Cloud Sign On(**보안 클라우드 로그인**)** 페이지에서 자격 증명을 입력합니다.
4. Security Cloud Sign On 계정이 없고 새로 생성하려는 경우, **Sign up now(**지금 등록**)**를 클릭합니다.
   a. 어카운트를 생성하기 위한 정보를 입력하십시오.



다음은 몇 가지 팁입니다.

- **Email(**이메일**)**: CDO에 로그인하는 데 사용할 이메일 주소를 입력합니다.

- **Password(암호)**: 강력한 암호를 입력하십시오.

b. **Sign up(등록하기)**을 클릭합니다. Cisco는 등록한 주소로 확인 이메일을 보냅니다.

c. 메일을 열고 메일 및 **Security Cloud Sign On(보안 클라우드 로그인)** 페이지에서 **Activate account(계정 활성화)**를 클릭합니다.

d. 선택한 디바이스에서 Duo를 사용하여 다단계 인증을 구성하고 **Log in with Duo(Duo로 로그인)**을 클릭하고 **Finish(마침)**를 클릭합니다.

Note 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 이중 인증 가이드: 등록 가이드를 참고하십시오.

5. 테넌트의 이름을 제공하고 **Create new account(새 어카운트 생성)**를 클릭합니다.
6. 선택한 지역에 새 CDO 테넌트가 생성됩니다. 생성되는 CDO 테넌트에 대한 세부 정보가 포함된 이메일도 받게 됩니다. 여러 CDO 테넌트와 이미 연결되어 있는 경우 **Choose a tenant(테넌트 선택)** 페이지에서 로그인하기 위해 방금 생성한 테넌트를 선택합니다. 처음으로 새 CDO 테넌트를 생성하는 경우 테넌트에 직접 로그인됩니다.

   CDO 테넌트에 처음으로 로그인하는 방법에 대한 자세한 내용은 새 CDO 테넌트에 대한 초기 로그인을 참조하십시오.

   CDO 테넌트 및 다양한 테넌트 설정 관리에 대한 자세한 내용은 테넌트 관리를 참조하십시오.

CDO 테넌트를 정식 버전으로 업그레이드

CDO의 무료 평가판을 사용 중인 경우 평가판 기간이 남은 기간 동안 CDO의 무료 평가판을 사용 중이라는 배너가 계속 표시됩니다. 평가판 기간 중 언제든지 CDO 테넌트를 정식 버전으로 업그레이드할 수 있습니다. 시스코 영업 담당자에게 문의하거나 시스코 영업팀에 연락하면 영업팀에서 대신 주문하고 세일즈 오더 번호를 받을 수 있습니다.

세일즈 오더 번호를 받으면 배너에서 정식 버전으로 업그레이드를 클릭하고 주문 번호를 입력하면 정식 버전의 CDO를 사용할 수 있습니다.

CDO 평가판 기간 연장 요청

평가판을 30일 동안 계속 사용하려면 **Request for an extension(연장 요청)**을 클릭합니다.

CDO에 로그인합니다.

CDO에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 CDO에서 사용자 관리가 있는 계정이 필요합니다.

IdP 어카운트에는 사용자의 자격 증명이 포함되며 IdP는 이러한 자격 증명을 기반으로 사용자를 인증합니다. 다단계 인증은 ID 보안의 추가 레이어를 제공합니다. CDO 사용자 레코드에는 주로 사용자 이름, 연결된 CDO 테넌트 및 사용자의 역할이 포함됩니다. 사용자가 로그인하면 CDO는 IdP의 사용

자 ID를 CDO의 테넌트에 있는 기존 사용자 레코드에 매핑하려고 시도합니다. CDO가 일치 항목을 찾으면 사용자는 해당 테넌트에 로그인됩니다.

엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Security Cloud Sign On입니다. Security Cloud Sign On는 다단계 인증에 Duo를 사용합니다. 고객은 원하는 경우 SAML SSO(Single Sign-On)를 과 통합할 수 있습니다.

CDO에 로그인하려면 먼저 Cisco Secure Cloud Sign-On에서 계정을 생성하고 Duo Security를 사용하여 MFA(Multi-Factor Authentication)를 구성하고 테넌트 최고 관리자가 CDO 레코드를 생성하도록 해야 합니다.

2019년 10월 14일에 CDO는 Cisco Secure Cloud Sign-On을 ID 제공자 및 MFA용 Duo로 사용하도록 기존의 모든 테넌트를 변환했습니다.

참고

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 CDO에 로그인하는 경우 Cisco Secure Cloud Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- CDO 무료 평가판을 사용 중인 경우 이 전환이 영향을 미쳤습니다.

CDO 테넌트가 2019년 10월 14일 이후에 생성된 경우 새 CDO 테넌트에 대한 초기 로그인, 4 페이지를 참조하십시오.

2019년 10월 14일 이전에 CDO 테넌트가 존재했다면 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 5 페이지를 참조하십시오.

새 CDO 테넌트에 대한 초기 로그인

시작하기 전에

DUO Security 설치. 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 이중 인증 가이드: 등록 가이드를 참고하십시오.

시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.

CDO는 Cisco Secure Cloud Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. . Cisco Security Cloud Sign On 계정이 없는 경우 https://www.defenseorchestrator.com/provision를 사용하여 새 CDO 테넌트를 생성하면 프로비저닝 플로우에는 Security Cloud Sign On 계정 생성 및 Duo를 사용한 MFA 구성 단계가 포함됩니다.

MFA는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

중요 **2019**년 **10**월 **14**일 이전에 **CDO** 테넌트가 존재했다면 이 문서 대신 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 5 페이지를 사용하여 로그인 지침을 사용합니다.

다음 작업**?**

새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 75 페이지를 계속합니다. 이는 4단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

다른 지역에서 **CDO** 로그인

다음은 다른 AWS 지역에서 CDO에 로그인하는 데 사용하는 URL입니다.

표 ***1: CDO*** 다른 지역의 ***URL***

지역	**CDO URL**
아시아 태평양 및 일본(APJ)	https://www.apj.cdo.cisco.com/
호주(AUS)	https://aus.cdo.cisco.com
유럽, 중동 및 아프리카(EMEA)	https://defenseorchestrator.eu/
인도(IN)	https://in.cdo.cisco.com
미국(US)	https://defenseorchestrator.com

로그인 실패 문제 해결

실수로 잘못된 **CDO** 지역에 로그인했기 때문에 로그인에 실패함

적절한 CDO 지역에 로그인했는지 확인합니다. https://sign-on.security.cisco.com에 로그인하면 액세스할 지역을 선택할 수 있습니다.

로그인해야 하는 지역에 대한 자세한 내용은 다른 지역에서 CDO 로그인, 5 페이지을 참조하십시오.

Cisco Secure Cloud Sign On ID 제공자로 마이그레이션

2019년 10월 14일, CDO는 모든 테넌트를 MFA(multi-factor authentication)를 위한 ID 제공자 및 Duo로 Cisco Secure Cloud Sign-On으로 변환했습니다. **CDO**에 로그인하려면 먼저 **Cisco Secure Sign-On**에서 계정을 활성화하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

CDO에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

참고

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 CDO에 로그인하는 경우 Cisco Secure Cloud Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- CDO 무료 평가판을 사용 중인 경우 이 전환이 적용됩니다.
- **CDO** 테넌트가 **2019**년 **10**월 **14**일 이후에 생성된 경우 이 문서 대신 새 CDO 테넌트에 대한 초기 로그인, 4 페이지에서 로그인 지침을 참조하십시오.

시작하기 전에

마이그레이션하기 전에 다음 단계를 수행하는 것이 좋습니다.

- **DUO Security** 설치**.** 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 이중 인증 가이드: 등록 가이드를 참고하십시오.
- 시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.
- 새 Cisco Secure Sign-On 어카운트 생성 및 Duo 다단계 인증 구성. 이는 4 단계 프로세스입니다. 4 단계를 모두 완료해야 합니다.

마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 75 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성.

- 해결 방법 새 Secure Sign-On 계정을 만든 경우 대시보드에서 테넌트가 만들어진 지역에 해당하는 CDO 타일을 클릭합니다.
  - 해결 방법 Cisco Defense Orchestrator APJ
  - 해결 방법 Cisco Defense Orchestrator 호주
  - 해결 방법 Cisco Defense Orchestrator EU
  - 해결 방법 Cisco Defense Orchestrator 인도
  - 해결 방법 Cisco Defense Orchestrator US
- 해결 방법 https://sign-on.security.cisco.com을 가리키도록 북마크를 업데이트합니다.

CDO 테넌트 시작

Procedure

단계 **1** Cisco Secure Cloud Sign-on 대시보드에서 해당 지역의 해당 CDO 버튼을 클릭합니다.

단계 **2** 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 Duo Security 또는 Google Authenticator를 선택합니다.

- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 이미 여러 포털에 사용자 레코드가 있는 경우 연결할 포털을 선택할 수 있습니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 CDO 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 CDO에 대해 자세히 알아보거나 평가판 테넌트를 요청할 수 있습니다.

포털 보기는 여러 테넌트에서 통합된 정보를 검색하고 표시합니다. 자세한 내용은 멀티 테넌트 포털 관리, on page 61를 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.

테넌트에서 슈퍼 관리자 관리

테넌트의 슈퍼 관리자 수를 제한하는 것이 가장 좋습니다. 슈퍼 관리자 권한을 가져야 하는 사용자를 결정하고 CDO에서 사용자 관리를 검토한 다음 다른 사용자의 역할을 "Admin(관리자)"으로 변경합니다.

CDO 시작하기

CDO 시작하기는 방화벽을 효율적으로 설정하고 구성하기 위한 순차적인 작업을 안내하는 직관적인 인터페이스입니다.

CDO에 로그인하고 상단 메뉴에서 ( )를 클릭합니다.

- 온프레미스 관리 페이지에 다음 링크가 제공됩니다.
  - 온프레미스 방화벽 Management Center 를 사용하여 CDOThreat Defense 디바이스를 []에 온 Onboard 합니다.
  - [] 에 의해 관리되는 온프레미스 방화벽 Management CenterThreat Defense 디바이스를 클라우드 제공 Firewall Management Center] 로 마이그레이션합니다.
  - 디바이스 템플릿을 사용하여 여러 위협 방어 디바이스를 클라우드 제공 Firewall Management Center로 대량 프로비저닝을 수행합니다.
  - 정책을 분석하고, 이상 징후를 감지하고, 선별된 교정 권장 사항을 받아보십시오.

- **Manage firewalls(**방화벽 관리**)** 페이지에 다음 링크가 제공됩니다.
  - Threat Defense 온보딩 및 관리, Cisco Secure Firewall ASA, 및 Meraki MX firewalls.
  - 사이트 간 VPN 연결 설정
  - Cisco AI Assistant를 활용하여 필요할 때 방화벽 정책과 액세스 관련 문서를 관리해 보십시오.
  - 일반적인 문제 해결을 위한 알림을 받으려면 구독하십시오.
- **Protect cloud assets(**클라우드 자산 보호**)** 페이지에 다음 링크가 제공됩니다.
  - 멀티 클라우드 방어를 사용하여 일관된 보안 조치로 멀티클라우드 환경 전반에서 데이터와 애플리케이션을 보호하여 클라우드 자산을 안전하게 보호하십시오.

CDO 라이선스 정보

CDO는 테넌트 자격에 대한 기본 구독과 디바이스 관리를 위한 디바이스 라이선스가 필요합니다. 필요한 테넌트 수에 따라 하나 이상의 CDO 기본 구독을 구입하고 디바이스 모델 번호 및 수량에 따라 디바이스 라이선스를 구입할 수 있습니다. 즉, 기본 구독을 구매하면 CDO 테넌트가 제공되며 CDO를 사용하여 관리하기로 선택한 모든 디바이스에 대해 별도의 디바이스 라이선스가 필요합니다.

배포 계획을 위해 각 CDO 테넌트는 SDC(보안 디바이스 커넥터)를 통해 약 500개의 디바이스를 관리하고 클라우드 커넥터를 사용하는 원하는 수의 디바이스를 관리할 수 있습니다. 자세한 내용은 Secure Device Connector(SDC)를 참조하십시오.

CDO에서 디바이스를 온보딩하고 관리하려면, 관리하려는 디바이스에 따라 기본 구독 및 디바이스별 기간 기반 구독을 구매해야 합니다.

서브스크립션

Cisco Defense Orchestrator 구독은 기간 기반입니다.

- 기본- 1년, 3년 및 5년 동안의 구독을 제공하고 CDO 테넌트에 액세스하고 적절하게 라이선스가 부여된 디바이스를 온보딩할 수 있는 권한을 제공합니다.
- 디바이스 라이선스 - 관리하기로 선택한 모든 지원 디바이스에 대해 1년, 3년 및 5년 구독을 제공합니다. 예를 들어 Cisco Firepower 1010 디바이스에 대한 3년 소프트웨어 구독을 구매한 경우, 3년 동안 CDO를 사용하여 Cisco Firepower 1010 디바이스를 관리하도록 선택할 수 있습니다.

CDO가 지원하는 Cisco 보안 디바이스에 대한 자세한 내용은 CDO에서 지원하는 소프트웨어 및 하드웨어를 참조하십시오.

중요 CDO에서 고가용성 디바이스 쌍을 관리하기 위해 두 개의 별도 디바이스 라이선스가 필요하지 않습니다. ASA(고가용성 쌍이 있는 경우, CDO는 고가용성 디바이스 쌍을 하나의 단일 디바이스로 간주하므로 하나의 디바이스 라이선스를 구입하는 것으로 충분합니다.

참고 Cisco 스마트 라이선스 포털을 통해 CDO 라이선스를 관리할 수 없습니다.

소프트웨어 서브스크립션 지원

CDO 기본 구독에는 구독 기간 동안 유효한 소프트웨어 구독 지원이 포함되며 추가 비용 없이 소프트웨어 업데이트, 주요 업그레이드 및 Cisco TAC(Technical Assistance Center)에 대한 액세스를 제공합니다. 소프트웨어 지원이 기본적으로 선택되어 있지만 요구 사항에 따라 CDO 솔루션 지원을 활용할 수도 있습니다.

CDO 평가 라이선스

SecureX 계정에서 30일 CDO 평가판을 요청할 수 있습니다. 자세한 내용은 CDO 테넌트 요청을 참조하십시오.

클라우드 제공 Firewall Management Center 및 Threat Defense 라이선스

CDO에서 클라우드 제공 Firewall Management Center를 사용하기 위해 별도의 라이선스를 구입할 필요가 없습니다. CDO 테넌트의 기본 구독에는 클라우드 제공 Firewall Management Center에 대한 비용이 포함됩니다.

클라우드 제공 Firewall Management Center 평가 라이선스

클라우드 제공 Firewall Management Center에 90일 평가판 라이선스가 제공되며 그 이후에는 Threat Defense 서비스가 차단됩니다.

CDO 테넌트에서 프로비저닝된 클라우드 제공 Firewall Management Center를 가져오는 방법을 알아보려면 CDO 테넌트용 클라우드 제공 Firewall Management Center 요청을 참조하십시오.

참고 클라우드 제공 Firewall Management Center는 에어갭 네트워크의 디바이스에 대한 특정 라이선스 예약(SLR)을 지원하지 않습니다.

클라우드 제공 Firewall Management Center용 Threat Defense 라이선스

클라우드 제공 Firewall Management Center에서 관리하는 각 Secure Firewall Threat Defense 디바이스에 대해 개별 라이선스가 필요합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 사용 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 라이선싱을 참조하십시오.

CDO가 클라우드 제공 Firewall Management Center으로 마이그레이션된 디바이스에 대한 라이선스를 처리하는 방법을 알아보려면 Management Center에서 Cloud로 Threat Defense 마이그레이션을 참조하십시오.

보안 디바이스 커넥터

보안 디바이스 커넥터(SDC)는 Cisco 디바이스가 CDO와 통신하도록 허용하는 인텔리전트 프록시입니다. 디바이스 자격 증명을 사용하여 인터넷을 통해 직접 연결할 수 없는 디바이스를 CDO에 온보딩하는 경우, 네트워크에서 SDC를 구축하여 디바이스와 CDO 간의 통신을 프록시할 수 있습니다. 아니면 원하는 경우 CDO에서 외부 인터페이스를 통해 직접 통신을 수신하도록 디바이스를 활성화할 수 있습니다. ASA(Adaptive Security Appliances), Meraki MXs, Secure Firewall Threat Defense 디바이스, Firepower Management Center 디바이스, 일반 SSH 및 iOS 디바이스는 모두 SDC를 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

SDC는 AES-128-GCM over HTTPS(TLS 1.3)를 사용하여 서명 및 암호화된 보안 통신 메시지를 통해 CDO와 통신합니다. 온보딩된 디바이스 및 서비스에 대한 모든 자격 증명은 브라우저에서 SDC로 직접 암호화되며, AES-128-GCM을 사용하여 저장 상태에서도 암호화됩니다. SDC만 디바이스 자격 증명에 액세스할 수 있습니다. 다른 CDO 서비스는 자격 증명에 액세스할 수 없습니다. SDC와 CDO 간의 통신을 허용하는 방법에 대한 자세한 내용은 매니지드 디바이스에 CDO 연결, 12 페이지의 내용을 참조하십시오.

SDC는 모든 Ubuntu 인스턴스에 설치할 수 있습니다. 편의를 위해 SDC CLI가 사전 설치되어 있는 강화된 Ubuntu 22 인스턴스용 OVA를 제공합니다. CLI는 가상 머신을 구성하고, 필요한 모든 시스템 패키지를 설치하며, 호스트에서 SDC를 Docker 컨테이너로 부트스트랩하는 데 도움이 됩니다. 또는 자체 Ubuntu 인스턴스(현재 테스트 중인 버전 20~24)를 롤링하고 CLI를 별도로 다운로드할 수도 있습니다.

각 CDO 테넌트에는 무제한의 SDC가 있을 수 있습니다. 이러한 SDC는 테넌트 간에 공유되지 않으며 단일 테넌트 전용입니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다.

테넌트에 대해 둘 이상의 SDC를 구축하면 다음과 같은 이점도 제공됩니다.

- 성능 저하 없이 CDO 테넌트로 더 많은 디바이스를 관리할 수 있습니다.
- 네트워크 내의 격리된 네트워크 세그먼트에 SDC를 구축하고 동일한 CDO 테넌트로 해당 세그먼트의 디바이스를 계속 관리할 수 있습니다. 여러 SDC가 없으면 서로 다른 CDO 테넌트를 사용하여 격리된 네트워크 세그먼트에서 디바이스를 관리해야 합니다.

단일 호스트에서 여러 SDC를 실행할 수 있으며, 실행하려는 각 SDC에 대해 부트스트랩 절차를 따르십시오. 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 통합하며 CDO의 **Services(**서비스**)** 페이지에 있는 **Secure Connectors(**보안 커넥터**)** 탭에 표시됩니다. 각 추가 SDC는 순서대로 번호가 매겨집니다.

자세한 내용은 CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축, 13 페이지 및 VM에 보안 디바이스 커넥터 구축, 17 페이지의 내용을 참조하십시오.

관련 정보**:**

매니지드 디바이스에 CDO 연결

CDO는 클라우드 커넥터 또는 SDC(Secure Device Connector)를 통해 관리하는 디바이스에 연결합니다.

인터넷에서 디바이스에 직접 액세스할 수 있는 경우 클라우드 커넥터를 사용하여 디바이스에 연결해야 합니다. 디바이스를 구성할 수 있는 경우 클라우드 지역의 CDO IP 주소에서 포트 443에 대한 인바운드 액세스를 허용합니다.

인터넷에서 디바이스에 액세스할 수 없는 경우 CDO가 디바이스와 통신할 수 있도록 네트워크에 온프레미스 SDC를 구축할 수 있습니다.

포트 443(또는 디바이스 관리를 위해 구성한 포트)에서 디바이스 서브넷/IP의 전체 인바운드 액세스를 허용하도록 디바이스를 구성합니다.

다음을 온보딩하려면 네트워크에 온프레미스 SDC가 필요합니다.

- SSH 액세스가 가능한 디바이스.

다른 모든 디바이스와 서비스는 CDO이 클라우드 커넥터를 사용하여 연결하므로 온프레미스 SDC가 필요하지 않습니다. 인바운드 액세스를 허용해야 하는 IP 주소를 확인하려면 다음 섹션을 참조하십시오.

클라우드 커넥터를 통해 디바이스를 CDO에 연결

클라우드 커넥터를 통해 CDO를 디바이스에 직접 연결할 때는 EMEA, 미국 또는 APJ 지역의 다양한 IP 주소에 대해 포트 443(또는 디바이스 관리를 위해 구성한 모든 포트)에서 인바운드 액세스를 허용해야 합니다.

AJP(Asia-Pacific-Japan) 고객이고, https://www.apj.cdo.cisco.com/에서 CDO에 연결하는 경우 다음 IP 주소에서 인바운드 액세스를 허용합니다.

- 54.199.195.111
- 52.199.243.0

Australia(호주**) (AUS)** 지역의 고객이고, https://aus.cdo.cisco.com에서 CDO에 연결하는 경우 다음 IP 주소에서 인바운드 액세스를 허용합니다.

- 13.55.73.159
- 13.238.226.118

유럽**,** 중동 또는 아프리카**(EMEA)** 지역의 고객이 https://defenseorchestrator.eu/에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 35.157.12.126
- 35.157.12.15

India(인도) (IN) 지역의 고객이고, https://in.cdo.cisco.com에서 CDO에 연결하는 경우 다음 IP 주소에서 인바운드 액세스를 허용합니다.

- 35.154.115.175
- 13.201.213.99

US 지역의 고객이고, https://defenseorchestrator.com에서 CDO에 연결하는 경우, 다음 IP 주소에서 인바운드 액세스를 허용합니다.

- 52.34.234.2
- 52.36.70.147

SDC에 CDO 연결

SDC를 통해 CDO를 디바이스에 연결할 때 CDO에서 관리하려는 디바이스는 포트 443(또는 디바이스 관리를 위해 구성한 포트)에서 SDC 호스트의 전체 인바운드 액세스를 허용해야 합니다. 이는 관리 액세스 제어 규칙을 사용하여 구성됩니다.

또한 SDC가 구축된 가상 머신이 매니지드 디바이스의 관리 인터페이스에 네트워크로 연결되어 있는지 확인해야 합니다.

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축

디바이스 자격 증명을 사용하여 CDO를 디바이스에 연결하는 경우 네트워크에 SDC를 다운로드하고 구축하여 CDO와 디바이스 간의 통신을 관리하는 것이 가장 좋습니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center), SSH 및 iOS 디바이스는 모두 SDC를 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다. 자세한 내용은 단일 CDO 테넌트에서 여러 SDC 사용, 32 페이지를 참조하십시오.

이 절차에서는 CDO의 VM 이미지를 사용하여 네트워크에 SDC를 설치하는 방법을 설명합니다. 이는 SDC를 생성하는 가장 쉽고 신뢰할 수 있는 방법입니다. 생성한 VM을 사용하여 SDC를 생성해야 하는 경우 VM에 보안 디바이스 커넥터 구축, 17 페이지을 수행합니다.

시작하기 전에

SDC를 구축하기 전에 다음 사전 요건을 검토합니다.

- CDO는 엄격한 인증서 확인이 필요하며 SDC(Secure Device Connector)와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC와 CDO 간의 트래픽 검사를 비활성화합니다.
- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성한 포트에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다. CDO에서 관리하는 디바이스는 이 포트의 인바운드 트래픽도 허용해야 합니다.
- 매니지드 디바이스에 CDO 연결을 검토하여 적절한 네트워크 액세스를 확인합니다.
- CDO는 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용하여 SDC VM OVF 이미지 설치를 지원합니다.
- CDO는 vSphere 데스크톱 클라이언트를 사용한 SDC VM OVF 이미지 설치를 지원하지 않습니다.
- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.
- SDC가 하나만 있는 VMware ESXi 호스트의 시스템 요구 사항:
  - VMware ESXi 호스트에는 vCPU 2개가 필요합니다.
  - VMware ESXi 호스트에는 최소 2GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- docker IP는 SDC의 IP 범위 및 디바이스 IP 범위와 다른 서브넷에 있어야 합니다.
- 설치를 시작하기 전에 다음 정보를 수집하십시오.
  - SDC에 사용할 고정 IP 주소
  - 설치 프로세스 중 생성하는 `root` 및 `cdo` 사용자의 비밀번호.
  - 조직에서 사용하는 DNS 서버의 IP 주소
  - SDC 주소가 있는 네트워크의 게이트웨이 IP 주소
  - 시간 서버의 FQDN 또는 IP 주소.
- SDC 가상 머신은 보안 패치를 정기적으로 설치하도록 구성되며, 이를 위해서는 포트 80 아웃바운드를 열어야 합니다.

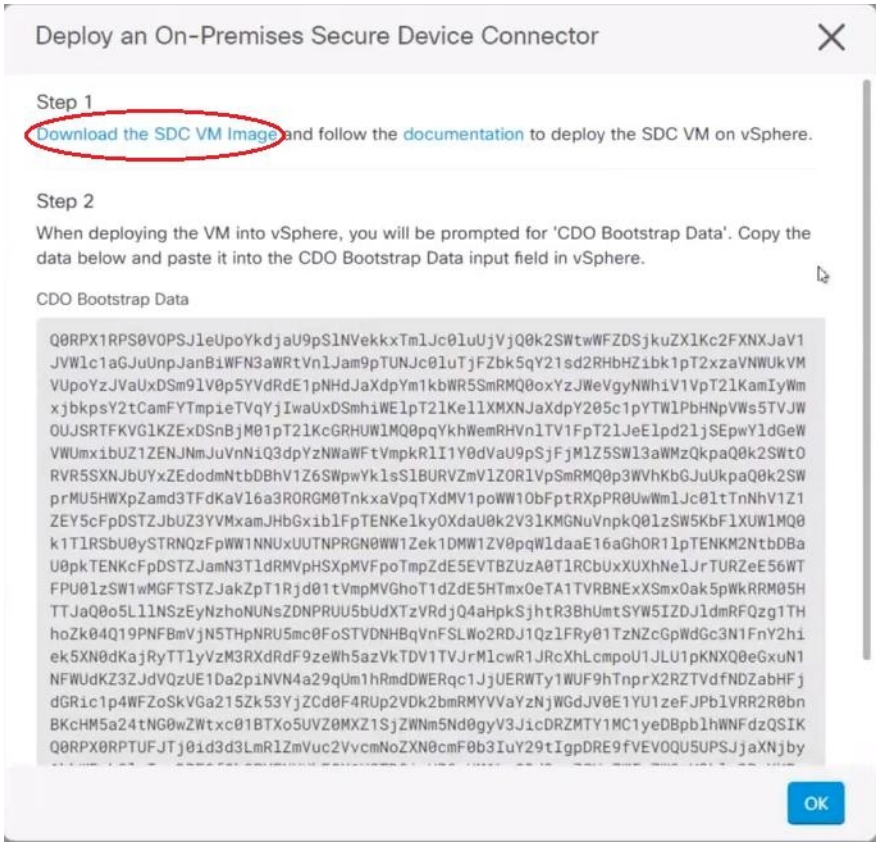
프로시저

단계 **1** SDC를 생성할 CDO 테넌트에 로그온합니다.

단계 **2** CDO 메뉴에서 **Tools & Services(**도구 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 선택합니다.

단계 **3** **Services(**서비스**)** 페이지에서 **Secure Connectors(**보안 커넥터**)** 탭을 선택하고 파란색 더하기 버튼을 클릭한 후 **Secure Device Connector(**보안 디바이스 커넥터**)**를 선택합니다.

단계 **4** 1단계에서 **Download the SDC VM image(SDC VM** 이미지 다운로드**)**를 클릭합니다. 별도의 탭에서 열립니다.



단계 **5** .zip 파일의 모든 파일을 추출합니다. 다음과 같이 표시됩니다.

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

단계 **6** vSphere 웹 클라이언트를 사용하여 VMware 서버에 관리자로 로그인합니다.

참고
ESXi 웹 클라이언트를 사용하지 마십시오.

단계 **7** 지시에 따라 OVF 템플릿에서 보안 디바이스 커넥터 가상 머신을 구축합니다.

단계 **8** 설정이 완료되면 SDC VM의 전원을 켭니다.

단계 **9** 새 SDC VM의 콘솔을 엽니다.

단계 **10** 사용자 이름 CDO로 로그인합니다. 기본 암호는 **adm123**입니다.

단계 **11** 프롬프트에 `sudo sdc-onboard setup`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 **12** 비밀번호를 물으면 `adm123`을 입력합니다.

단계 **13** 지시에 따라 `root` 사용자의 새 비밀번호를 생성합니다. 루트 사용자의 비밀번호를 입력합니다.

단계 **14** 지시에 따라 CDO 사용자의 새 암호를 생성합니다. 사용자 비밀번호를 입력합니다.

단계 **15** **Please choose the CDO domain you connect to(**연결할 도메인을 선택하십시오**)** 메시지가 표시되면 CDO 도메인 정보를 입력합니다.

단계 **16** 메시지가 표시되면 SDC VM의 다음 도메인 정보를 입력합니다.

a) IP 주소/CIDR
b) 게이트웨이
c) DNS 서버
d) NTP 서버 또는 FQDN
e) Docker 브리지

또는 docker 브리지가 적용되지 않는 경우 Enter 키를 누릅니다.

단계 **17** **Are these values valid(**이 값이 올바릅니까**?) (y/n)** 메시지가 나타나면 **y**를 사용하여 입력을 확인합니다**.**

단계 **18** 입력을 확인합니다.

단계 **19** **"Would you like to setup the SDC now?(**지금 **SDC**를 설정하시겠습니까**?) (y/n)** 메시지가 나타나면 `n`을 입력합니다.

단계 **20** VM 콘솔에서 자동으로 로그아웃됩니다.

단계 **21** SDC에 대한 SSH 연결을 생성합니다. CDO로 로그인하고 비밀번호를 입력합니다.

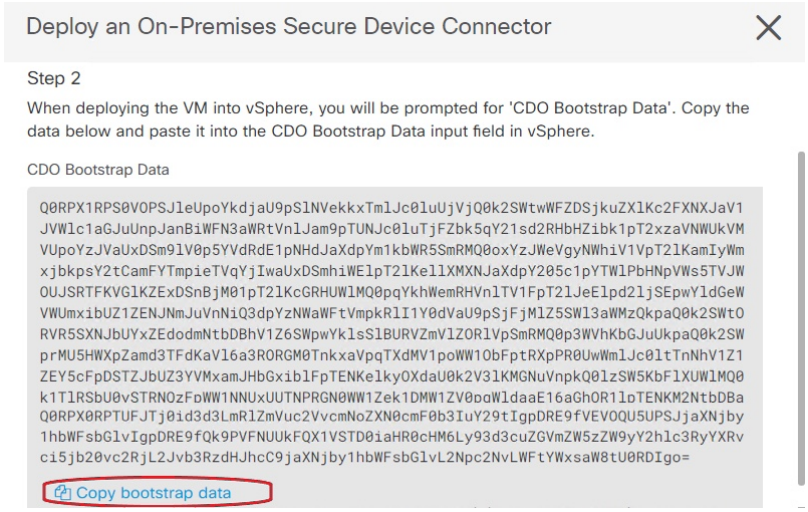
단계 **22** 프롬프트에 `sudo sdc-onboard bootstrap`을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

단계 **23** **[sudo]** 비밀번호를 묻는 메시지가 표시되면 단계 14에서 생성한 비밀번호를 입력합니다.

단계 **24** **Please copy the bootstrap data form the Secure Connector Page of CDO(**보안 커넥터 페이지에서 부트스트랩 데이터를 복사하십시오**.)** 메시지가 표시되면 다음 절차를 수행합니다.

1. CDO에 로그인합니다.
2. Actions(작업) 창에서 **Deploy an On-Premises Secure Device Connector(**온프레미스 보안 디바이스 커넥터 구축**)**를 클릭합니다.
3. 대화 상자의 2단계에서 **Copy the bootstrap data(**부트스트랩 데이터 복사**)**를 클릭하고 SSH 창에 붙여넣습니다.



단계 **25** **Do you want to update these setting(**이 설정을 업데이트하시겠습니까**?) (y/n)** 메시지가 나타나면 `n`을 입력합니다.

단계 **26** Secure Device Connector(보안 디바이스 커넥터) 페이지로 돌아갑니다. 새 SDC의 상태가 **Active(**활성**)**로 변경될 때까지 화면을 새로 고칩니다.

VM에 보안 디바이스 커넥터 구축

디바이스 자격 증명을 사용하여 CDO를 디바이스에 연결하는 경우, 네트워크에서 SDC(보안 디바이스 커넥터)를 다운로드하고 구축하여 CDO와 디바이스 간의 통신을 관리하는 것이 모범 사례입니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center) 디바이스는 모두 디바이스 자격 증명을 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다. 그러나 구축을 계획할 때는 1개의 SDC가 약 500개의 디바이스를 지원할 것으로 예상합니다. 자세한 내용은 단일 CDO 테넌트에서 여러 SDC 사용, 32 페이지를 참조하십시오.

이 절차에서는 자체 가상 머신 이미지를 사용하여 네트워크에 SDC를 설치하는 방법을 설명합니다.

참고 SDC를 설치하는 가장 쉽고 신뢰할 수 있는 방법은 CDO의 SDC OVA 이미지를 다운로드하여 설치하는 것입니다. 해당 지침은 CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축, 13 페이지의 내용을 참조하십시오.

시작하기 전에

- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- SDC가 CDO와 통신하려면 TCP 포트 443에서 인터넷에 대한 전체 아웃바운드 액세스 권한이 있어야 합니다.
- SDC를 통해 CDO에 접속하는 디바이스는 포트 443에서 SDC로부터의 인바운드 액세스를 허용해야 합니다.
- 네트워킹 지침은 매니지드 디바이스에 CDO 연결을 검토하십시오.
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트

참고 vSphere 데스크톱 클라이언트를 사용한 설치는 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Cent OS 7 게스트 운영체제.
- SDC만 있는 VM의 시스템 요구 사항:
  - VMware ESXi 호스트에는 CPU 2개가 필요합니다.
  - VMware ESXi 호스트에는 최소 2GB의 메모리가 필요합니다.
  - VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다. 이 값은 필요에 따라 필요한 디스크 공간을 확장할 수 있도록 파티션과 함께 LVM(논리적 볼륨 관리)을 사용한다고 가정합니다.
- VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 vi 시각적 편집기를 사용하는 데 익숙해야 합니다.
- CentOS 가상 머신에 온프레미스 SDC를 설치하는 경우 정기적으로 Yum 보안 패치를 설치하는 것이 좋습니다. Yum 구성에 따라 Yum 업데이트를 가져오려면 포트 80 및 443에서 아웃바운드 액세스를 열어야 할 수 있습니다. 또한 업데이트를 예약하려면 yum-cron 또는 crontab을 구성해야 합니다. 보안 운영 팀과 함께 Yum 업데이트를 받기 위해 변경해야 하는 보안 정책이 있는지 확인합니다.

참고 시작하기 전에: 절차의 명령을 복사하여 터미널 창에 붙여넣지 말고 대신 입력하십시오. 일부 명령에는 "n-대시"가 포함되며, 잘라내기 및 붙여넣기 프로세스에서 이러한 명령은 "m-대시"로 적용되어 명령이 실패할 수 있습니다.

프로시저

단계 1 SDC를 생성할 CDO 테넌트에 로그인합니다.

단계 2 왼쪽 창에서 **Tools & Services(**도구 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 클릭합니다.

단계 3 **Services(**서비스**)** 페이지에서 **Secure Connectors(**보안 커넥터**)** 탭을 선택하고 파란색 더하기 버튼을 클릭한 후 **Secure Device Connector(**보안 디바이스 커넥터**)**를 선택합니다.

단계 4 창의 2단계에서 부트스트랩 데이터를 메모장에 복사합니다.

단계 5 최소 SDC에 할당된 다음 RAM 및 디스크 공간을 사용하여 **CentOS 7** 가상 머신을 설치합니다.

- 8GB RAM
- 10GB 디스크 공간

단계 6 설치가 완료되면 SDC의 IP 주소, 서브넷 마스크 및 게이트웨이를 지정하는 등의 기본 네트워킹을 구성합니다.

단계 7 DNS(Domain Name Server) 서버를 구성합니다.

단계 8 NTP(Network Time Protocol) 서버를 구성합니다.

단계 9 SDC의 CLI와의 손쉬운 상호 작용을 위해 CentOS에 SSH 서버를 설치합니다.

단계 10 Yum 업데이트를 실행한 후 **open-vm-tools**, **nettools** 및 **bind-utils** 패키지를 설치합니다.

```
[root@sdc-vm ~]# yum update -y
                [root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

단계 11 AWS CLI 패키지를 설치합니다. https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html의 내용을 참조하십시오.

참고
--user 플래그를 사용하지 마십시오.

단계 12 Docker CE 패키지를 설치합니다. https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce의 내용을 참조하십시오.

참고
"저장소를 사용하여 설치" 방법을 사용합니다.

단계 13 Docker 서비스를 시작하고 부팅 시 시작되도록 활성화합니다.

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
    /usr/lib/systemd/system/docker.service.
```

단계 14 두 사용자("CDO" 및 "sdc")를 생성합니다. CDO 사용자는 관리 기능을 실행하기 위해 로그인하는 사용자이며(루트 사용자를 직접 사용할 필요가 없음), sdc 사용자는 SDC Docker 컨테이너를 실행하는 사용자입니다.

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc –d /usr/local/cdo
```

단계 **15** CDO 사용자의 비밀번호를 생성합니다.

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

단계 **16** CDO 사용자를 "wheel" 그룹에 추가하여 관리(sudo) 권한을 부여합니다.

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

단계 **17** Docker가 설치되면 사용자 그룹이 생성됩니다. CentOS/Docker 버전에 따라 "docker" 또는 "dockerroot"라고 부를 수 있습니다. /etc/group 파일을 확인하여 어떤 그룹이 생성되었는지 확인한 다음 sdc 사용자를 이 그룹에 추가합니다.

```
[root@sdc-vm ~]# grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

단계 **18** /etc/docker/daemon.json 파일이 없는 경우 파일을 생성하고 아래 내용을 입력합니다. 생성되면 docker 데몬을 다시 시작합니다.

참고
"group" 키에 입력한 그룹 이름이 이전 단계의 /etc/group 파일에서 찾은 그룹과 일치하는지 확인합니다.

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
        {
           "live-restore": true,
           "group": "docker"
        }
        [root@sdc-vm ~]# systemctl restart docker
        [root@sdc-vm ~]#
```

단계 **19** 현재 vSphere 콘솔 세션을 사용 중인 경우 SSH로 전환하고 "CDO" 사용자로 로그인합니다. 로그인한 후에는 "sdc" 사용자로 변경합니다. 암호를 묻는 메시지가 표시되면 "CDO" 사용자의 암호를 입력합니다.

```
[CDO@sdc-vm ~]$ sudo su sdc
              [sudo] password for cdo: <type password for cdo user>
              [sdc@sdc-vm ~]$
```

단계 **20** 디렉터리를 **/usr/local/CDO**로 변경합니다.

단계 **21** `bootstrapdata`라는 새 파일을 생성하고 온프레미스 보안 디바이스 커넥터 구축 마법사의 2단계에서 가져온 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 **Save(**저장**)**합니다. `vi` 또는 `nano`를 사용하여 파일을 생성할 수 있습니다.

단계 **22** 부트스트랩 데이터는 base64로 인코딩됩니다. 이를 디코딩하고 `extractedbootstrapdata`라는 파일로 내보냅니다.

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/ CDO/bootstrapdata >
/usr/local/CDO/extractedbootstrapdata
              [sdc@sdc-vm ~]$
```

cat 명령을 실행하여 디코딩된 데이터를 확인합니다. 명령 및 디코딩된 데이터는 다음과 같이 표시됩니다.

```
[sdc@sdc-vm ~]$ cat /usr/local/ CDO/extractedbootstrapdata
               CDO_TOKEN="<token string>"
               CDO_DOMAIN="www.defenseorchestrator.com"
               CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

단계 **23** 다음 명령을 실행하여 디코딩된 부트스트랩 데이터의 섹션을 환경 변수로 내보냅니다.

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
              [sdc@sdc-vm ~]$
```

단계 **24** CDO에서 부트스트랩 번들을 다운로드합니다.

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
               100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
               [sdc@sdc-vm ~]$ ls -l /usr/local/ CDO/*SDC
               -rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/CDO/tenant-name-SDC
```

단계 **25** SDC tarball의 압축을 풀고 `bootstrap.sh` 파일을 실행하여 SDC 패키지를 설치합니다.

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/CDO/tenant-name-SDC
               <snipped – extracted files>
               [sdc@sdc-vm ~]$
               [sdc@sdc-vm ~]$ /usr/local/ CDO/bootstrap/bootstrap.sh
               [2018-07-23 13:54:02] environment properly configured
               download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
               toolkit.sh
               common.sh
               [2018-07-23 13:54:04] startup new container
               Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
               sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
Pulling from
               ciscodefenseorchestrator/sdc_prod
               08d48e6f1cff: Pull complete
               ebbd10b629b1: Pull complete
               d14d580ef2ed: Pull complete
               45421d451ab8: Pull complete
               <snipped – downloads>
               no crontab for sdc
```

이제 SDC가 CDO에서 "Active(활성)"로 표시됩니다.

다음에 수행할 작업

-

Ubuntu 가상 머신에서 보안 디바이스 커넥터 및 보안 이벤트 커넥터 구축

디바이스 자격 증명을 사용하여 CDO를 디바이스에 연결하는 경우 네트워크에 보안 디바이스 커넥터(SDC)를 다운로드하고 구축하여 CDO와 디바이스 간의 통신을 관리하는 것이 가장 좋습니다. 일반적으로 이러한 디바이스는 경계를 기반으로 하지 않으며 공용 IP 주소가 없거나 외부 인터페이스에 대한 개방형 포트가 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center) 디바이스는 모두 디바이스 자격 증명을 사용하여 CDO에 온보딩할 수 있습니다.

SDC는 매니지드 디바이스에서 실행해야 하는 명령과 매니지드 디바이스로 전송해야 하는 메시지에 대해 CDO를 모니터링합니다. SDC는 CDO를 대신하여 명령을 실행하고, 매니지드 디바이스를 대신하여 CDO에 메시지를 전송하고, 매니지드 디바이스에서 CDO로 응답을 반환합니다.

SEC(Secure Event Connector)는 ASA 및 FTD에서 Cisco Cloud로 이벤트를 전달하므로, 라이선싱에 따라 Event Logging(이벤트 로깅) 페이지에서 해당 이벤트를 보고 Secure Cloud Analytics로 조사할 수 있습니다.

SDC를 구축한 후 SEC 컨테이너를 추가하는 것은 간단한 작업이 됩니다. SEC 서비스는 ASA, Cisco IOS 및 FDM 관리 디바이스에서 시스템 로그 메시지를 수신하고 Cisco Cloud에 안전하게 전송하도록 설계되었습니다. 이를 통해 CDO Analytics 및 Cisco XDR과 같은 이벤트 서비스를 사용하여 로그 메시지를 쉽게 저장, 기능 향상 및 분석할 수 있습니다.

CiscoDevNet 사이트에서 제공되는 스크립트를 실행하여 Linux Ubuntu 시스템에서 SDC 및 SEC를 설치할 수 있습니다.

시작하기 전에

- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시를 지원하지 않습니다.
- SDC는 TCP 포트 443에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.
- 네트워킹 지침은 매니지드 디바이스에 CDO 연결을 검토하십시오.
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트

참고 vSphere 데스크톱 클라이언트를 사용한 설치는 지원되지 않습니다.

- ESXi 5.1 하이퍼바이저.
- Ubuntu 운영 체제 버전 20.04 이상이 가상 머신에 설치되어 있습니다.

  SDC:

  - CPU: 2 코어
  - RAM: 최소 2GB

  SDC 및 SEC:

  - CPU: 4 코어

- RAM: 최소 8GB

- SDC를 실행 중인 Ubuntu 머신은 ASA 및 Cisco IOS 디바이스의 관리 인터페이스에 대한 네트워크 액세스 권한이 있어야 합니다.

프로시저

단계 **1** SDC를 생성할 CDO 테넌트에 로그인합니다.

단계 **2** 도구 및 서비스 > 보안 커넥터를 선택합니다.

단계 **3** **Services(**서비스**)** 페이지에서 **Secure Connectors(**보안 커넥터**)** 탭을 선택하고  를 클릭한 후 **Secure Device Connector(**보안 디바이스 커넥터**)**를 선택합니다.

단계 **4** 창의 2단계에서 부트스트랩 데이터를 메모장에 복사합니다.

단계 **5** SDC를 구축할 CiscoDevNet을 엽니다.

단계 **6** **Code(**코드**)**를 클릭하고 **HTTPS** 탭의 URL을 복사합니다.

단계 **7** Ubuntu 시스템에서 Ctrl+Alt+T를 눌러 터미널 창을 빠르게 엽니다.

단계 **8** 터미널에 **git** 을 입력하고 이전에 복사한 HTTPS URL을 붙여넣습니다.

```
[sdc@vm]:~$ git https://github.com/CiscoDevNet/cdo-deploy-sdc.git
Resolving deltas: 100% (22/22). done.
```

단계 **9** "cdo-deploy-sdc" 디렉터리로 이동합니다.

```
[sdc@vm]:~$ cd cdo-deploy-sdc.
```

단계 **10** **ls -la**를 실행하여 파일 및 스크립트를 확인합니다.

- **delete_sdc.sh**: 시스템에 이전에 설치된 SDC를 삭제합니다.
- **deploy_sdc.sh**: 시스템에 SDC를 구축합니다.
- **install_docker.sh**: 시스템에 권장되는 Docker 버전을 구축합니다.

단계 **11** 스크립트를 실행하여 Docker를 설치합니다.

```
[sdc@vm]:~/cdo-deploy-sdc$ ./install_docker.sh

Remove docker docker.io docker-compose docker-compose-v2 docker-doc podmand-docker {y/n] n
Active: active (running) since date time UTC; 32s ago
Adding the current user to the docker permmissions group
Done!
```

단계 **12** 스크립트를 실행하여 SDC를 구축합니다.

./deploy_sdc.sh를 입력하고 CDO UI에서 복사한 부트스트랩 데이터를 붙여넣습니다.

```
[sdc@vm]:~/cdo-deploy-sdc$ ./deploy_sdc.sh <bootstap data>.

If the docker container is up and running, the status of the SDC should go to 'Active' in
the CDO Event Connectors panel.
```

이제 보안 디바이스 커넥터가 CDO에서 "Active(활성)"로 표시됩니다.

다음에 수행할 작업

•

Terraform을 사용하여 vSphere에 보안 디바이스 커넥터 구축

시작하기 전에

이 절차에서는 vSphere용 CDO SDC Terraform 모듈을 CDO Terraform 제공자와 함께 사용하여 SDC를 vSphere에 구축하는 방법을 자세히 설명합니다. 이 작업 절차를 수행하기 전에 다음 사전 요구 사항을 검토하십시오.

- vSphere 데이터 센터 버전 7 이상이 필요합니다.
- 이 경우 데이터 센터에 대한 다음을 수행할 수 있는 권한이 있는 관리자 계정이 필요합니다.
  - VM 생성
  - 폴더 생성
  - 콘텐츠 라이브러리 생성
  - 콘텐츠 라이브러리에 파일 업로드
- Terraform 정보

프로시저

단계 **1** CDO에서 API 전용 사용자를 생성하고 API 토큰을 복사합니다. API 전용 사용자를 생성하는 방법을 알아보려면 API 전용 사용자 생성을 참조하십시오.

단계 **2** CDO Terraform 제공자의 지침에 따라 Terraform 저장소에서 CDOTerraform 제공자를 구성합니다.

예제:

```
terraform {
  required_providers {
    cdo = {
      source = "CiscoDevNet/cdo"
      version = "0.7.0"
    }
  }
}

provider "cdo" {
  base_url = “<the CDO URL you use to access CDO>”
  api_token = “<the API Token generated in step 1>”
}
```

단계 **3** CDO Terraform 제공자를 사용하여 `cdo_sdc` 리소스를 생성하는 Terraform 코드를 작성합니다. 자세한 내용은 CDO-sdc 리소스에 대한 Terraform 레지스트리를 참조하십시오.

예제:

```
Resource “cdo_sdc” “my-sdc” {
  name = “my-sdc-in-vsphere”
}
```

이 리소스의 `bootstrap_data` 속성은 CDO 부트스트랩 데이터의 값으로 채워지며 다음 단계에서 `cdo_sdc` Terraform 모듈에 제공됩니다.

단계 **4** CDO_sdc Terraform 모듈을 사용하여 vSphere에서 SDC를 생성하는 Terraform 코드를 작성합니다.

예제:

```
data "cdo_tenant" "current" {}

module "vsphere-cdo-sdc" {
  source               = "CiscoDevNet/cdo-sdc/vsphere"
  version              = "1.0.0"
  vsphere_username     = "<replace-with-username-with-admin-privileges>"
  vsphere_password     = "<super-secure-password>"
  vsphere_server       = "<replace-with-address-of-vsphere-server>"
  datacenter           = "<replace-with-datacenter-name>"
  resource_pool        = "<replace-with-resource-pool-name>"
  cdo_tenant_name      = data.cdo_tenant.current.human_readable_name
  datastore            = "<replace-with-name-of-datastore-to-deploy-vm-in>"
  network              = "<replace-with-name-of-network-to-deploy-vm-in>"
  host                 = "<replace-with-esxi-host-address>"
  allow_unverified_ssl = <boolean; set to true if your vsphere server does not have a valid
 SSL certificate>
  ip_address          = "<sdc-vm-ip-address; must be in the subnet of the assigned network
 for the VM>"
  gateway              = "<replace-with-network-gateway-address>"
  cdo_user_password    = "<replace-with-password-for-cdo-user-in-sdc-vm>"
  root_user_password   = "<replace-with-password-for-root-user-in-sdc-vm>"
  cdo_bootstrap_data   = cdo_sdc.sdc-in-vsphere.bootstrap_data
}
```

생성된 VM에는 두 명의 사용자(`root` 사용자와 `cdo`라는 사용자)가 있으며 VM의 IP 주소는 정적으로 구성됩니다. `cdo_bootstrap_data` 속성에는 `cdo_sdc` 리소스가 생성될 때 생성된 `bootstrap_data` 속성의 값이 지정됩니다.

단계 **5** `terraform 계획` 및 `terraform 적용`을 사용하여 일반적으로 Terraform을 계획하고 적용합니다.

전체 예시는 CiscoDevNet의 CDO 자동화 저장소를 참조하십시오.

SDC가 온보딩 상태를 유지한 경우 원격 콘솔을 사용하여 vSphere VM에 연결하고 CDO 사용자로 로그인한 후에 다음 명령을 실행합니다.

```
sudo su
/opt/cdo/configure.sh startup
```

참고 CDO Terraform 모듈은 Apache 2.0 라이선스에 따라 오픈 소스 소프트웨어로 게시됩니다. 지원이 필요한 경우 GitHub에서 문제를 제출할 수 있습니다.

Terraform 모듈을 사용하여 AWS VPC에 보안 디바이스 커넥터 구축

시작하기 전에

AWS VPC에서 SDC를 구축하기 전에 다음 사전 요건을 검토하십시오.

- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC(보안 디바이스 커넥터)와 CDO 간의 트래픽 검사를 비활성화합니다.
- 매니지드 디바이스에 CDO 연결을 검토하여 적절한 네트워크 액세스를 확인합니다.
- 이 경우 AWS 계정, 하나 이상의 서브넷이 있는 AWS VPC 및 AWS Route53 호스팅 영역이 필요합니다.
- CDO 부트스트랩 데이터, AWS VPC ID 및 해당 서브넷 ID가 있는지 확인합니다.
- SDC를 구축하는 프라이빗 서브넷에 NAT 게이트웨이가 연결되어 있는지 확인합니다.
- 방화벽 관리 HTTP 인터페이스가 실행 중인 포트에서 NAT 게이트웨이에 연결된 탄력적 IP로 이동하는 트래픽을 엽니다.

프로시저

단계 **1** Terraform 파일에 다음 코드 줄을 추가합니다. 변수에 대한 입력을 수동으로 입력해야 합니다.

```
module "example-sdc" {
  source             =
"git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"
  env                = "example-env-ci"
  instance_name      = "example-instance-name"
  instance_size      = "r5a.xlarge"
  cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
  vpc_id             = <replace-with-vpc-id>
  subnet_id          = <replace-with-private-subnet-id>
}
```

입력 변수 및 설명 목록은 Secure Device Connector Terraform 모듈을 참조하십시오.

단계 **2** Terraform 코드에서 `instance_id`를 출력으로 등록합니다.

```
output "example_sdc_instance_id" {
  value = module. example-sdc.instance_id
}
```

`instance_id` 를 사용하여 AWS Systems Manager 세션 관리자(SSM)를 통한 문제 해결을 위해 SDC 인스턴스에 연결할 수 있습니다. 사용 가능한 출력 목록은 Secure Device Connector Terraform 모듈의 출력을 참조하십시오.

다음에 수행할 작업

모든 SDC 문제 해결의 경우, AWS SSM을 사용하여 SDC 인스턴스에 연결해야 합니다. 인스턴스에 연결하는 방법에 대한 자세한 내용은 AWS Systems Manager 세션 관리자를 참조하십시오. SSH를 사용하여 SDC 인스턴스에 연결하는 포트는 보안상의 이유로 노출되지 않습니다.

참고 CDO Terraform 모듈은 Apache 2.0 라이선스에 따라 오픈 소스 소프트웨어로 게시됩니다. 지원이 필요한 경우 GitHub에서 문제를 제출할 수 있습니다.

프록시를 사용하도록 Secure Device Connector 구성

프록시 서버를 사용하면 아웃바운드 트래픽을 필터링하는 중개자 역할을 함으로써 보안을 강화할 수 있습니다. 네트워크 디바이스가 인터넷에 직접 노출되는 것을 방지하고 공격의 위험을 줄입니다. 프록시 서버를 SDC(보안 디바이스 커넥터)와 통합하여 SDC에서 CDO로의 모든 아웃바운드 통신을 수행할 수 있습니다. 이 절차는 호스트 Linux OS 설정이 아닌 SDC와 관련된 도커 컨테이너 구성을 수정하는 데 중점을 둡니다.

참고 변경 사항은 SDC의 도커 컨테이너에만 영향을 줍니다. 조직의 Linux 서버에 대한 표준 절차에 따라 호스트 Linux 시스템의 프록시 설정을 구성합니다.

시작하기 전에

- Linux 명령줄 인터페이스(CLI)에 익숙해야 합니다.
- config.json 파일을 편집하기 전에 백업을 만드는 것이 좋습니다.

프로시저

단계 **1** SSH를 사용하여 SDC에 액세스하고 다음 명령을 사용하여 SDC 사용자로 전환합니다.

```
$ sudo su - sdc
```

단계 **2** `usr/local/cdo/data/<your_sdc_name>/data/config.json`에서 구성 파일로 이동합니다.

단계 **3** JSON 키-값 쌍을 config.json 파일에 삽입합니다.

프록시를 프록시 서버의 IP 주소 또는 FQDN으로, 포트를 프록시 서버의 수신 포트로 바꿉니다.

```
"awsProxy":"https://proxy:port"
```

단계 **4** 변경 사항을 저장하고 SDC 컨테이너를 다시 시작합니다. 이 작업은 도커 컨테이너를 직접 다시 시작하거나 SDC를 호스팅하는 가상 머신을 재부팅하여 수행할 수 있습니다.

a) 도커 컨테이너를 다시 시작하려면 먼저 다음 명령을 사용하여 SDC 컨테이너 ID를 식별합니다.

```
[sdc@localhost cdo] $ docker ps
```

b) 이 명령을 사용하여 컨테이너를 다시 시작합니다.

```
[sdc@localhost cdo] $ docker restart <container_id>
```

여기서 <*container_id*> 는 SDC 컨테이너의 ID입니다.

단계 **5** 이 명령을 사용하여 상태를 확인하고 SDC 컨테이너가 성공적으로 다시 시작되어 작동 중인지 확인합니다.

```
[sdc@localhost cdo] $ docker ps | grep sdc
```

이 명령을 사용하여 logs/lar.log 파일에서 프록시 설정이 올바른지 확인합니다.

```
[sdc@localhost cdo] $ less /usr/local/cdo/data/<your_sdc_name>/logs/lar.log
```

SDC가 프록시 서버를 사용하여 통신하도록 성공적으로 구성되었습니다.

보안 디바이스 커넥터의 IP 주소 변경

시작하기 전에

- 이 작업을 수행하려면 관리자여야 합니다.
- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성한 포트에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다.

참고 SDC의 IP 주소를 변경한 후 디바이스를 CDO에 다시 등록할 필요가 없습니다.

프로시저

단계 **1** SDC에 대한 SSH 연결을 생성하거나 가상 머신의 콘솔을 열고 CDO 사용자로 로그인합니다.

단계 **2** IP 주소를 변경하기 전에 SDC VM의 네트워크 인터페이스 구성 정보를 보려면 `ifconfig` 명령을 사용합니다.

```
[cdo@localhost ~]$ ifconfig
```

단계 **3** 인터페이스의 IP 주소를 변경하려면 `sudo sdc-onboard setup` 명령을 입력합니다.

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

단계 **4** 프롬프트에 비밀번호를 입력합니다.

```
[sudo] password for CDO:
```

단계 **5** 루트 및 CDO 비밀번호를 재설정하라는 프롬프트에 `n`을 입력합니다.

```
Would you like to reset the root and cdo passwords? (y/n):
```

단계 **6** 네트워크 재구성 프롬프트에 `y`를 입력합니다.

```
Would you like to re-configure the network? (y/n):
```

단계 **7** 메시지가 표시되면 SDC에 할당하려는 새 IP 주소와 SDC VM의 다른 도메인 정보를 입력합니다.

a) IP Address(IP 주소)
b) 게이트웨이
c) DNS 서버
d) NTP 서버 또는 FQDN

또는 NTP 서버 또는 FQDN이 적용되지 않는 경우 Enter 키를 누릅니다.

e) Docker 브리지

또는 docker 브리지가 적용되지 않는 경우 Enter 키를 누릅니다.

단계 **8** 값의 정확성을 묻는 메시지가 표시되면 `y`로 항목을 확인합니다.

```
Are these values correct? (y/n):
```

참고
이 명령을 실행하면 이전 IP 주소에 대한 SSH 연결이 끊어지므로, `y`를 입력하기 전에 값이 정확한지 확인합니다.

단계 **9** SDC에 할당한 새 IP 주소를 사용하여 SSH 연결을 만들고 로그인합니다.

단계 **10** 연결 상태 테스트 명령을 실행하여 SDC가 실행 중인지 확인할 수 있습니다.

```
[cdo@localhost ~]$ sudo sdc-onboard status
```

모든 확인 항목은 녹색으로 `[ OK(확인) ]`이라고 표시되어야 합니다.

참고
VM의 콘솔에서 이 절차를 수행하는 경우 값이 올바른지 확인하면 연결 상태 테스트가 자동으로 실행되고 상태가 표시됩니다.

단계 **11** CDO 사용자 인터페이스를 통해 SDC의 연결을 확인할 수도 있습니다. 이렇게 하려면 CDO 애플리케이션을 열고 **Tools & Services(**도구 및 서비스**)** > **Secure Connectors(**보안 커넥터**)** 페이지로 이동합니다.

단계 **12** 페이지를 한 번 새로 고치고 IP 주소를 변경한 보안 커넥터를 선택합니다.

단계 **13** **Actions(**작업**)** 창에서 **Request Heartbeat(**하트비트 요청**)**를 클릭합니다.

하트비트 요청 성공 메시지가 표시되고, 마지막 하트비트에 현재 날짜와 시간이 표시되어야 합니다.

중요
변경한 IP 주소는 GMT 오전 3시 이후에만 SDC의 세부 정보 창에 반영됩니다.

VM에 SDC를 배포하는 방법에 대한 자세한 내용은 VM에 보안 디바이스 커넥터 구축, 17 페이지를 참조하세요.

보안 디바이스 커넥터 제거

Warning 이 절차에서는 SDC(보안 디바이스 커넥터)를 삭제합니다. 이는 되돌릴 수 없습니다. 이 작업을 수행한 후에는 새 SDC를 설치하고 디바이스를 다시 연결할 때까지 해당 SDC에 연결된 디바이스를 관리할 수 없습니다. 디바이스를 다시 연결하려면 다시 연결해야 하는 각 디바이스에 대한 관리자 자격 증명을 다시 입력해야 할 수 있습니다.

테넌트에서 SDC를 제거하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 삭제할 SDC에 연결된 모든 디바이스를 제거합니다.

- **a.** SDC에서 사용하는 모든 디바이스를 식별하려면 동일한 SDC를 사용하는 CDO 디바이스를 참조하십시오.
- **b.** **Inventory(**재고 목록**)** 페이지에서 식별한 모든 디바이스를 선택합니다.
- **c.** Device Actions(디바이스 작업) 창에서 **Remove(**제거**)**를 클릭하고 **OK(**확인**)**를 클릭하여 작업을 확인합니다.

단계 **2** 왼쪽 창에서 **Tools & Services(**도구 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 클릭합니다.

단계 **3** **Secure Connectors(**보안 커넥터**)** 탭이 선택된 **Services(**서비스**)** 페이지에서 파란색 더하기 버튼을 클릭한 후 **Secure Device Connector(**보안 디바이스 커넥터**)**를 선택합니다.

단계 **4** Secure Connector(보안 커넥터) 테이블에서 제거할 SDC를 선택합니다. 이제 디바이스 수가 0이어야 합니다.

단계 **5** 작업 창에서 **Remove(**제거**)**를 클릭합니다. 다음 경고가 표시됩니다.

Warning
<sdc_name>을 삭제하려고 합니다. SDC 삭제는 되돌릴 수 없습니다. SDC를 삭제하면 디바이스를 온보딩하거나 다시 온보딩하기 전에 새 SDC를 생성하고 온보딩해야 합니다.

현재 온보딩된 디바이스가 있으므로 SDC를 제거하려면 새 SDC를 설정한 후 해당 디바이스를 다시 연결하고 자격 증명을 다시 제공해야 합니다.

- 질문이나 우려 사항이 있는 경우 **Cancel(**취소**)**을 클릭하고 CDO 지원에 문의하십시오.
- 계속하려면 <sdc_name>을 입력란에 입력하고 **OK(**확인**)**를 클릭합니다.

단계 **6** 확인 대화 상자에서 계속 진행하려면 경고 메시지에 나와 있는 SDC의 이름을 입력합니다.

단계 **7** **OK(**확인**)**를 클릭하여 SDC 제거를 확인합니다.

SDC 간에 ASA 이동

CDO는 단일 CDO 테넌트에서 여러 SDC 사용 다음 절차를 사용하여 한 SDC에서 다른 SDC로 관리형 ASA를 이동할 수 있습니다.

프로시저

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **ASA** 탭을 클릭합니다.

단계 **3** 다른 SDC로 이동하려는 ASA를 선택합니다.

단계 **4** **Device Actions(**디바이스 작업**)** 창에서 **Update Credentials(**자격 증명 업데이트**)**를 클릭합니다.

단계 **5** 보안 디바이스 커넥터 버튼을 클릭하고 디바이스를 이동하려는 SDC를 선택합니다.

단계 **6** CDO가 디바이스에 로그인하는 데 사용하는 관리자 사용자 이름과 암호를 입력하고 **Update(**업데이트**)**를 클릭합니다. 변경되지 않은 경우 관리자 사용자 이름과 암호는 ASA 온보딩에 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항을 디바이스에 배포할 필요는 없습니다.

참고
모든 ASA가 동일한 자격 증명을 사용하는 경우 한 SDC에서 다른 SDC로 ASA를 대량으로 이동할 수 있습니다. ASA에 다른 자격 증명이 있는 경우 한 번에 하나의 SDC에서 다른 하나로 이동해야 합니다.

보안 디바이스 커넥터 이름 변경

프로시저

단계 **1** 왼쪽 창에서 **Tools & Services(**도구 및 서비스**) > > Secure Connectors(**보안 커넥터**)**를 선택합니다.

단계 **2** 이름을 바꾸려는 SDC를 선택합니다.

단계 **3** 세부 정보 창에서 SDC 이름 옆에 있는 편집 아이콘 를 클릭합니다.

단계 **4** SDC의 이름을 바꿉니다.

Inventory(재고 목록**)** 창의 보안 디바이스 커넥터 필터를 포함하여 CDO 인터페이스에 SDC 이름이 나타날 때마다 이 새 이름이 나타납니다.

보안 디바이스 커넥터 업데이트

이 절차를 문제 해결 툴로 사용합니다. 일반적으로 SDC는 자동으로 업데이트되므로 이 절차를 사용할 필요가 없습니다. 그러나 VM의 시간 구성이 잘못된 경우 SDC는 업데이트를 수신하기 위해 AWS

에 연결할 수 없습니다. 이 절차는 SDC의 업데이트를 시작하며 시간 동기화 문제로 인한 오류를 해결합니다.

Procedure

단계 **1** SDC에 연결합니다. SSH를 사용하여 연결하거나 VMware 하이퍼바이저에서 콘솔 보기를 사용할 수 있습니다.)

단계 **2** **cdo** 사용자로 SDC에 로그인합니다.

단계 **3** SDC 도커 컨테이너를 업데이트하려면 SDC 사용자로 전환합니다.

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

단계 **4** SDC 툴킷을 업그레이드합니다.

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeToolkit
                [sdc@sdc-vm ~]$
```

단계 **5** SDC를 업그레이드합니다.

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeSDC
                [sdc@sdc-vm ~]$
```

Note
SDC 가상 머신의 권장 업데이트 및 유지 관리

조직의 내부 IT 보안 및 패치 관리 정책에 따라 Ubuntu 리눅스에서 실행되는 SDC VM을 모니터링하고 업데이트를 적용해야 합니다. SDC VM이 네트워크 환경 내에서 보안을 유지하고 최적으로 작동하도록 관련 보안 패치를 정기적으로 검토하고 적용할 것을 적극 권장합니다.

단일 CDO 테넌트에서 여러 SDC 사용

테넌트에 대해 둘 이상의 SDC를 구축하면 성능 저하 없이 더 많은 디바이스를 관리할 수 있습니다. 단일 SDC에서 관리할 수 있는 디바이스의 수는 해당 디바이스에 구현된 기능 및 해당 구성 파일의 크기에 따라 달라집니다.

테넌트에 SDC를 무제한으로 설치할 수 있습니다. 각 SDC는 하나의 네트워크 세그먼트를 관리할 수 있습니다. 이러한 SDC는 해당 네트워크 세그먼트의 디바이스를 동일한 CDO 테넌트에 연결합니다. 여러 SDC가 없으면 서로 다른 CDO 테넌트를 사용하여 격리된 네트워크 세그먼트에서 디바이스를 관리해야 합니다.

두 번째 또는 후속 SDC를 구축하는 절차는 첫 번째 SDC를 구축할 때와 동일합니다. CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축하거나 VM에 보안 디바이스 커넥터 구축할 수 있습니다. 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 통합합니다. 각 추가 SDC는 순서대로 번호가 매겨집니다.

동일한 SDC를 사용하는 CDO 디바이스

동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스를 식별하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 필터 기준이 이미 지정된 경우 Inventory(재고 목록) 테이블 상단에 있는 **clear(**지우기**)** 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.

단계 **5** 필터 버튼 을 클릭하여 필터 메뉴를 확장합니다.

단계 **6** 필터의 Secure Device Connectors(보안 디바이스 커넥터) 섹션에서 원하는 SDC의 이름을 확인합니다. Inventory(재고 목록) 테이블에는 필터에서 선택한 SDC를 통해 CDO에 연결하는 디바이스만 표시됩니다.

단계 **7** (선택 사항) 필터 메뉴에서 추가 필터를 선택하여 검색을 더욱 구체화합니다.

단계 **8** (선택 사항) 작업이 완료되면 Inventory(재고 목록) 테이블 상단에 있는 **clear(**지우기**)** 버튼을 클릭하여 CDO로 관리하는 모든 디바이스 및 서비스를 표시합니다.

SDC의 오픈소스 및 서드파티 라이선스

========== ==========

*** amqplib ***

amqplib copyright (c) 2013, 2014

Michael Bridgen <mikeb@squaremobius.net>

이 패키지 **"amqplib"**는 **MIT** 라이선스에 따라 라이선스가 부여됩니다**.** 사본은 이 디렉토리의 **LICENSE-MIT** 파일에서 찾거나 다음에서 다운로드할 수 있습니다**.**

http://opensource.org/licenses/MIT

==========

*** async ***

Copyright (c) 2010-2016 Caolan McMahon

본 소프트웨어와 관련 문서 파일**(**이하 "소프트웨어"**)**의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며**,** 이에 대한 비용은 부담하지 않습니다**.** 이는 소프트웨어의 사용**,** 복제**,** 수정**,** 통합**,** 게시**,** 배포**,** 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다**.** 또한**,** 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다**.**

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** bluebird ***

The MIT License (MIT)

Copyright (c) 2013-2015 Petka Antonov

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** cheerio ***

Copyright (c) 2012 Matt Mueller <mattmuelle@gmail.com>

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** command-line-args ***

MIT 라이선스**(MIT)**

Copyright (c) 2015 Lloyd Brookes <75pound@gmail.com>

본 소프트웨어와 관련 문서 파일**(**이하 "소프트웨어"**)**의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며**,** 이에 대한 비용은 부담하지 않습니다**.** 이는 소프트웨어의 사용**,** 복제**,** 수정**,** 통합**,** 게시**,** 배포**,** 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다**.** 또한**,** 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다**.**

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다**.**

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태**("**있는 그대로"**)**로 제공됩니다**.** 이에는 상업성**,** 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다**.** 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** ip ***

이 소프트웨어는 **MIT** 라이센스에 따라 라이센스가 부여됩니다**.**

Copyright Fedor Indutny, 2012.

본 소프트웨어와 관련 문서 파일**(**이하 "소프트웨어"**)**의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며**,** 이에 대한 비용은 부담하지 않습니다**.** 이는 소프트웨어의 사용**,** 복제**,** 수정**,** 통합**,** 게시**,** 배포**,** 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다**.** 또한**,** 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다**.**

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다**.**

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태**("**있는 그대로"**)**로 제공됩니다**.** 이에는 상업성**,** 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다**.** 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** json-buffer ***

Copyright (c) 2013 Dominic Tarr

본 소프트웨어와 관련 문서 파일**(**이하 "소프트웨어"**)**의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며**,** 이에 대한 비용은 부담하지 않습니다**.** 이는 소프트웨어의 사용**,** 복제**,** 수정**,** 통합**,** 게시**,** 배포**,** 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다**.** 또한**,** 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다**.**

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다.어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 거래와 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 클레임, 손해, 또는 기타 책임에 대해서도 책임을 지지 않습니다.

==========

*** json-stable-stringify ***

이 소프트웨어는 **MIT** 라이선스에 따라 배포됩니다.

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** json-stringify-safe ***

ISC 라이선스

Copyright (c) Isaac Z. Schlueter and Contributors

위의 저작권 고지와 이 허가 고지가 모든 사본에 포함되어 있는 한, 본 소프트웨어를 비용 여부에 상관없이 어떤 목적으로든 사용, 복사, 수정 및/또는 배포할 수 있는 권한이 여기에 부여됩니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 과실 또는 기타 불법 행위로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 징벌적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

==========

*** lodash ***

Copyright JS Foundation and other contributors <https://js.foundation/>

Underscore.js, copyright Jeremy Ashkenas 기반

DocumentCloud 및 조사 리포터 및 편집자<http://underscorejs.org/>

이 소프트웨어는 많은 개인의 자발적 기여로 구성됩니다. 정확한 기여 내역은 다음에서 제공되는 https://github.com/lodash/lodash 개정 내역을 참조하십시오.

다음 라이센스는 다음을 제외하고 이 소프트웨어의 모든 부분에 적용됩니다.

아래에 문서화:

====

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

====

샘플 코드에 대한 저작권 및 관련 권리는 **CC0**을 통해 포기됩니다. 샘플 코드는 문서의 산문 내에 표시되는 모든 소스 코드로 정의됩니다.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

node_modules 및 공급업체 디렉토리에 있는 파일은 자체 라이선스가 있는 이 소프트웨어에서 사용하는 외부에서 유지 관리되는 라이브러리입니다. 용어가 위의 용어와 다를 수 있으므로 해당 용어를 읽어보는 것이 좋습니다.

==========

*** log4js ***

Copyright 2015 Gareth Jones (다른 많은 사람들의 기여 포함**)**

Apache 라이선스 버전 **2.0("**라이선스**")**에 따라 라이선스가 부여됩니다. 라이센스를 준수하지 않는 한 이 파일을 사용할 수 없습니다. 다음에서 라이센스 사본을 얻을 수 있습니다.

http://www.apache.org/licenses/LICENSE-2.0

해당 법률에서 요구하거나 서면으로 동의하지 않는 한 라이선스에 따라 배포된 소프트웨어는 명시적이든 묵시적이든 어떠한 종류의 보증이나 조건 없이 "있는 그대로" 배포됩니다.라이선스에 따른 권한 및 제한 사항을 관리하는 특정 언어는 라이선스를 참조하십시오.

==========

*** mkdirp ***

Copyright 2010 James Halliday(mail@substack.net)

이 프로젝트는 **MIT/X11** 라이선스에 따라 배포되는 무료 소프트웨어입니다.

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 소프트웨어 또는 소프트웨어의 사용 또는 기타 취급과 관련하여 계약 행위, 불법 행위 또는 기타 행위 등의 클레임, 손해, 또는 기타 책임에 대해 책임을 지지 않습니다.

==========

*** node-forge ***

새로운 **BSD** 라이선스(**3**개 조항)

Copyright (c) 2010, Digital Bazar, Inc.

All rights reserved.

다음 조건을 충족하는 경우 수정 여부에 관계없이 소스 및 바이너리 형식으로 재배포 및 사용이 허용됩니다.

***** 소스 코드의 재배포는 위의 저작권 표시, 이 조건 목록 및 다음 면책 조항을 유지해야 합니다.

***** 바이너리 형식의 재배포는 배포와 함께 제공된 설명서 및/또는 기타 자료에 위의 저작권 고지, 이 조건 목록 및 다음 면책 조항을 복제해야 합니다.

*** Digital Bazaar, Inc.**의 이름이나 기여자의 이름은 특정 사전 서면 허가 없이 이 소프트웨어에서 파생된 제품을 보증하거나 홍보하는 데 사용할 수 없습니다.

이 소프트웨어는 저작권자와 기여자에 의해 "있는 그대로" 제공되며, 명시적 또는 묵시적으로 상품성 및 특정 목적에의 적합성을 포함한 모든 보증이 거부됩니다. 어떠한 경우에도 **DIGITAL BAZAAR**는 어떠한 직접적, 간접적, 부수적, 특별, 징벌적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다. 이러한 손해가 계약, 엄격한 책임, 불법행위(과실 또는 기타 포함)에 대한 어떠한 책임 이론에 의거하여 발생하였는지 여부와 상관없이, 해당 손해의 가능성이 있음을 사전에 고지받았더라도, 이 소프트웨어의 사용으로 인해 발생하는 어떠한 방식의 책임도 지지 않습니다.

==========

*** request ***

Apache License

버전 **2.0, January 2004**

http://www.apache.org/licenses/

사용, 복제 및 배포에 대한 약관

1. 정의.

"라이선스"는 이 문서의 섹션 **1**에서 **9**까지 정의된 사용, 복제 및 배포에 대한 조건을 의미합니다.

"라이선스 제공자"는 라이센스를 부여하는 저작권 소유자 또는 저작권 소유자가 승인한 법인을 의미합니다.

"법적 실체"는 행위 실체와 해당 실체를 통제하거나 통제받거나 공통 통제하에 있는 다른 모든 실체의 조합을 의미합니다. 이 정의의 목적상 "통제"는 **(i)** 계약 또는 기타 방식으로 해당 법인의 지시 또는 관리를 유발하는 직간접적인 권한 또는 **(ii) 50%(50%)** 또는 더 많은 발행주식, 또는 **(iii)** 해당 법인의 수익적 소유권.

"귀하"(또는 "귀하의")는 계약 또는 기타 방식으로 본 라이센스에 의해 부여된 권한을 행사하는 개인 또는 법인을 의미하거나 **(ii)** 다음 중 **50%** 이상을 소유합니다. 발행주식, 또는 **(iii)** 그러한 법인의 수익적 소유권.

"소스" 형식은 소프트웨어 소스 코드, 문서 소스 및 구성 파일을 포함하되 이에 국한되지 않는 수정을 위한 기본 형식을 의미합니다.

"개체" 형식은 컴파일된 개체 코드, 생성된 문서 및 다른 미디어 유형으로의 변환을 포함하되 이에 국한되지 않는 소스 형식의 기계적 변환 또는 변환으로 인해 발생하는 모든 형식을 의미합니다.

"저작물"은 저작물에 포함되거나 첨부된 저작권 표시(예는 아래 부록에 제공됨)에 표시된 대로 라이센스에 따라 사용 가능한 소스 또는 개체 형식의 저작물을 의미합니다.

"파생 저작물"은 저작물을 기반으로 하는(또는 저작물에서 파생된) 원본 또는 개체 형식의 모든 저작물을 의미하며 편집 편집, 주석, 정교화 또는 기타 편집이 전체적으로 저자의 원본 저작물을 나타냅니다. 본 라이선스에서 파생물은 저작물 및 그 파생물과 분리된 상태를 유지하거나 인터페이스에 단순히 링크(또는 이름으로 연결)되는 저작물은 포함하지 않습니다.

"기여"는 원본 저작물과 저작물에 포함하기 위해 저작권 소유자 또는 저작권 소유자를 대신하여 제출할 권한이 있는 개인 또는 법인이 라이선스 허가자에게 의도적으로 제출된 저작물 또는 파생물에 대한 편집 또는 추가를 포함한 저작물을 의미합니다. 이 정의에서 \"제출\"은 저작물에 대해 논의하고 개선하기 위해 라이선스 허가자 또는 그 대리인에게 전송되는 모든 형태의 전자, 구두 또는 서면 제출을 의미합니다. 여기에는 저작물을 논의하고 개선할 목적으로 라이선스 허가자 또는 그 대리인이 관리하는 전자 메일 목록, 소스 코드 제어 시스템, 문제 추적 시스템을 통한 커뮤니케이션이 포함되며 이에 국한되지 않습니다. 단, 저작권 소유자가 "기고문이 아님"을 명시적으로 표시하거나 서면으로 지정한 커뮤니케이션은 제외됩니다.

"기여자"는 라이선스 제공자 및 라이선스 제공자가 대신하여 기여물을 받아 작업물에 통합한 모든 개인 또는 법인을 의미합니다.

2. 저작권 라이선스 부여. 이 라이선스의 조건에 따라 각 기여자는 이로써 귀하에게 영구적이고 전 세계적이며 비독점적이고 무료이며 로열티가 없고 취소할 수 없는 저작권 라이선스를 부여합니다. 저작물 및 그러한 파생 저작물을 소스 또는 개체 형태로 재라이선스하고 배포합니다.

3. 특허 라이선스 부여. 본 라이선스의 약관에 따라 각 기여자는 귀하에게 저작물의 제작, 사용, 판매 제안, 판매, 가져오기, 기타 방식의 이전을 위한 영구적, 세계적, 비독점적, 요금 및 로열티 무료, 철회 불가능한(본 섹션에 명시된 경우 제외) 특허 라이선스를 부여합니다. 이러한 라이선스는 기여자가 부

여할 수 있는 특허권에만 적용되며, 이는 기여물 단독으로 또는 기여물이 제출된 저작물과의 조합으로 인해 침해될 수 있습니다. 귀하가 저작물 또는 저작물에 통합된 기여가 직접적 또는 기여적 특허 침해를 구성한다고 주장하는 어떤 법인에 대해 특허 소송(소송에서 교차 청구 또는 반소 포함)을 제기하는 경우, 본 라이선스에 따라 귀하에게 부여된 모든 특허 라이선스는 작업은 그러한 소송이 제기된 날짜에 종료됩니다.

4. 재배포. 귀하는 다음 조건을 충족하는 경우 편집 여부에 관계없이 모든 매체와 소스 또는 개체 형식으로 저작물 또는 그 파생 저작물의 사본을 재생산 및 배포할 수 있습니다.

귀하는 저작물 또는 파생 저작물의 다른 수령인에게 본 라이센스의 사본을 제공해야 합니다. 그리고

귀하는 수정된 파일에 귀하가 파일을 변경했음을 알리는 눈에 띄는 통지를 전달해야 합니다. 그리고

파생 저작물의 일부와 관련되지 않은 통지를 제외하고 저작물의 소스 형식에서 가져온 모든 저작권, 특허, 상표 및 귀속 고지를 귀하가 배포하는 파생 저작물의 소스 형식으로 유지해야 합니다. 그리고

저작물이 배포의 일부로 "**NOTICE**" 텍스트 파일을 포함하는 경우 귀하가 배포하는 모든 파생 저작물에는 그러한 **NOTICE** 파일에 포함된 귀속 고지의 읽을 수 있는 사본이 포함되어야 합니다. 다음 위치 중 적어도 하나에 있는 **2**차 저작물**: 2**차 저작물의 일부로 배포되는 **NOTICE** 텍스트 파일 내에서 파생 저작물과 함께 제공되는 경우 소스 양식 또는 문서 내에서**;** 또는 파생 저작물에 의해 생성된 디스플레이 내에서 그러한 제**3**자 고지가 일반적으로 표시되는 경우**. NOTICE** 파일의 내용은 정보 제공의 목적으로만 사용되며 이에 따라 라이선스가 편집되지 않습니다. 저작물의 **NOTICE** 텍스트와 함께 또는 그 부록으로 배포하는 파생물 내 속성 고지로 인해 라이선스가 변경되지 않는 경우, 이러한 추가적인 속성 고지를 추가할 수 있습니다. 귀하는 귀하의 편집 사항에 자신의 저작권 진술을 추가할 수 있으며 편집 사항의 사용, 복제 또는 배포 또는 그러한 파생 저작물 전체에 대한 추가 또는 다른 라이선스 조건을 제공할 수 있습니다. 그렇지 않으면 저작물은 본 라이선스에 명시된 조건을 준수합니다.

5. 기여물 제출. 귀하가 달리 명시하지 않는 한, 귀하가 저작물에 포함하기 위해 라이선스 허가자에게 의도적으로 제출한 모든 기여물은 추가 약관 없이 본 라이선스의 약관에 따라야 합니다. 위의 내용에도 불구하고 여기의 어떠한 내용도 그러한 기여와 관련하여 귀하가 라이선스 제공자와 체결한 별도의 라이선스 계약 조건을 대체하거나 편집하지 않습니다.

6. 상표. 본 라이선스는 저작물의 출처를 설명하고 **NOTICE** 파일의 내용을 재생산하는 데 합당하고 관례적인 사용에 필요한 경우를 제외하고 라이선스 제공자의 상표명, 상표, 서비스 마크 또는 제품 이름을 사용할 수 있는 권한을 부여하지 않습니다.

7. 보증의 면책조항. 해당 법률에 의해 요구되는 경우나 서면으로 합의된 경우를 제외하고, 라이선서는 작업물(및 각 기여자는 자신의 기여물)을 "있는 그대로" 제공하며, 명시적이거나 묵시적으로 어떠한 종류의 보증이나 조건도 포함하지 않습니다. 이는 제목, 비침해성, 상품성 또는 특정 목적에 대한 적합성에 대한 어떠한 보증이나 조건을 포함합니다. 귀하는 저작물 사용 또는 재배포의 적합성을 판단할 전적인 책임이 있으며 본 라이선스에 따른 귀하의 권한 행사와 관련된 모든 위험을 감수합니다.

8. 책임의 제한. 어떠한 경우에도, 과실(비롯하여 과실포함 책임), 계약 또는 기타 이론에 의한, 해당 법에 의해 요구되는 경우(예: 고의적이고 중대한 과실 행위)나 서면으로 합의된 경우를 제외하고, 어떤 기여자도 본 라이선스로 인한 손해에 대해 법적으로 책임을지지 않습니다. 이는 작업물의 사용 또는 사용 불능으로 인해 발생하는 어떠한 종류의 직접적, 간접적, 특수적, 우발적 또는 결과적 손해(예: 선의의 상실, 작업 중단, 컴퓨터 고장 또는 장애, 그 외 모든 상업적 손해나 손실을 포함)에 대해서도

책임을지지 않습니다. 심지어 해당 기여자에게 그러한 손해의 가능성이 알려져 있더라도 마찬가지입니다.

9. 보증 또는 추가 책임 수락. 저작물 또는 그 파생물을 재배포하는 경우 귀하는 지원, 보증, 면책 또는 본 라이선스와 일치하는 기타 책임 의무 및/또는 권리의 수락을 제공하고 요금을 청구할 수 있습니다. 그러나 이러한 의무를 수락할 때에는 다른 기여자를 대신하여 행동하지 않고 오로지 자신의 명의로, 자신의 책임하에만 행동해야 하며, 해당 보증이나 추가적인 책임을 수락함으로써 발생하는 어떠한 책임에 대해서도 각 기여자를 면책시키고 방어하며 보호하기 위해 보증을 제공하는 경우에만 그렇게 행동할 수 있습니다.

이용 약관의 끝

==========

*** rimraf ***

ISC 라이선스

Copyright (c) Isaac Z. Schlueter and Contributors

위의 저작권 고지와 이 허가 고지가 모든 사본에 포함되어 있는 한, 본 소프트웨어를 비용 여부에 상관없이 어떤 목적으로든 사용, 복사, 수정 및/또는 배포할 수 있는 권한이 여기에 부여됩니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태**("**있는 그대로**")**로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 과실 또는 기타 불법 행위로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 징벌적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

==========

*** uuid ***

Copyright (c) 2010-2012 Robert Kieffer

MIT 라이선스- http://opensource.org/licenses/mit-license.php

==========

*** validator ***

Copyright (c) 2016 Chris O'Hara <cohara87@gmail.com>

본 소프트웨어와 관련 문서 파일**(**이하 "소프트웨어"**)**의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태**("**있는 그대로**")**로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어

의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.

==========

*** when ***

오픈 소스 이니셔티브 **OSI - MIT** 라이선스

http://www.opensource.org/licenses/mit-license.php

Copyright (c) 2011 Brian Cavalier

본 소프트웨어와 관련 문서 파일(이하 "소프트웨어")의 사본을 획득한 모든 사람은 본 소프트웨어를 제한 없이 다룰 수 있으며, 이에 대한 비용은 부담하지 않습니다. 이는 소프트웨어의 사용, 복제, 수정, 통합, 게시, 배포, 하위 라이선스 부여 및 소프트웨어의 사본을 판매하는 권리를 포함한 제한 없는 권리를 제공합니다. 또한, 소프트웨어를 제공받은 사람에게 이러한 권리를 부여함에 따라 다음의 조건에 따라야 합니다.

위의 저작권 표시와 이 허가 표시는 모든 소프트웨어의 사본 또는 실질적인 부분에 포함되어야 합니다.

본 소프트웨어는 명시적 또는 묵시적인 어떠한 종류의 보증도 포함되지 않은 상태("있는 그대로")로 제공됩니다. 이에는 상업성, 특정 목적에의 적합성 및 타인의 권리를 침해하지 않음 등의 보증이 포함되지만 이에 한정되지는 않습니다. 어떠한 경우에도 저작자 또는 저작권 보유자는 본 소프트웨어의 사용 또는 성능과 관련하여 계약, 불법 행위 등으로 인해 발생한 어떠한 직접적, 간접적, 부수적, 특별, 우발적 또는 결과적 손해(대체 상품 또는 서비스의 조달, 사용, 데이터 또는 이익의 손실, 사업 중단을 포함하되 이에 국한되지 않음)에 대해 책임을 지지 않습니다.==========

CDO에서 지원하는 디바이스, 소프트웨어 및 하드웨어

CDO는 여러 보안 플랫폼에서 보안 정책과 디바이스 구성을 관리할 수 있는 클라우드 기반 관리 솔루션입니다. CDO는 전체 정책 및 구성을 중앙에서 관리합니다.

- Cisco Secure Firewall ASA, 온프레미스 및 가상 모두
- Cisco Secure FTD(Firewall Threat Defense), 온프레미스 및 가상 모두
- Cisco Secure Firewall Management Center, 온프레미스
- Cisco Meraki MX
- Cisco IOS 디바이스
- Cisco Umbrella
- AWS 보안 그룹

이 문서에서는 CDO가 지원하는 장치, 소프트웨어 및 하드웨어에 대해 설명합니다. CDO가 지원하지 않는 소프트웨어 및 디바이스는 지적하지 않습니다. 소프트웨어 버전 또는 디바이스 유형에 대한 지원을 명시적으로 요청하지 않는 경우 지원되지 않습니다.

Cisco Secure Firewall ASA

Cisco ASA(Adaptive Security Appliance)는 방화벽, VPN, 침입 방지 기능이 통합된 보안 디바이스입니다. 무단 액세스, 사이버 위협 및 데이터 유출로부터 네트워크를 보호하고, 단일 플랫폼에서 강력한 보안 서비스를 제공합니다. CDO 는 ASA 디바이스 관리를 지원하며, 구성 관리를 간소화 하고 네트워크 인프라 전반에서 규정 준수 를 보장하는 기능을 제공합니다.

Cisco Secure Firewall Threat Defense

Firewall Threat Defense는 기존 방화벽 기능과 고급 위협 보호 기능을 통합합니다. 침입 방지, 애플리케이션 제어, URL 필터링, 고급 악성코드 보호 등 포괄적인 보안 기능을 제공합니다. FTD는 ASA 하드웨어 어플라이언스, Cisco 방화벽 하드웨어 어플라이언스 및 가상 환경에 구축할 수 있습니다. Cisco Firewall Management Center, CDO, Firewall Device Manager 등 다양한 관리 인터페이스를 통해 Threat Defense 디바이스를 관리할 수 있습니다.

소프트웨어 및 하드웨어 호환성에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense 호환성 가이드를 참조하십시오.

Firewall Device Manager는 Threat Defense 디바이스 관리를 위해 명시적으로 설계된 웹 기반 관리 인터페이스입니다. Threat Defense 디바이스를 구성하고 모니터링하는 간소화된 접근 방식을 제공하므로 소규모 구축 또는 직관적인 인터페이스를 선호하는 조직에 이상적입니다.

FDM은 네트워크 설정, 액세스 제어 정책, NAT 규칙, VPN 구성, 모니터링 및 기본 문제 해결을 위한 기본 구성 기능을 제공합니다. 일반적으로 웹 브라우저를 통해 액세스하는 FDM은 FTD 장치에서 직접 사용할 수 있으므로 추가 관리 서버나 어플라이언스가 필요하지 않습니다.

Cisco Secure Firewall Management Center

CDO는 안전한 통합을 구축하고, 디바이스 인벤토리를 검색하고, 중앙 집중식 정책 관리를 가능하게 하여 온프레미스 Firewall Management Center의 관리를 간소화합니다. 방화벽 규칙, VPN 설정, 침입 방지 정책과 같은 보안 정책을 FMC의 모든 디바이스에서 효율적으로 관리하고 구축할 수 있습니다.

Cisco Meraki MX

Meraki MX 어플라이언스는 분산 구축을 위해 설계된 엔터프라이즈급 보안 및 SD-WAN 차세대 방화벽 어플라이언스입니다. CDO는 Meraki MX 디바이스에서 레이어 3 네트워크 규칙 관리를 지원합니다. Meraki 디바이스를 CDO에 온보딩할 경우, 이는 Meraki 대시보드 와 통신하여 디바이스를 관리합니다. CDO 는 설정 요청을 Meraki 대시보드 로 안전하게 전송하며, Meraki 대시보드에서 새 설정을 디바이스에 적용합니다. 중앙 집중식 정책 관리, 백업 및 복원, 모니터링 및 보고, 규정 준수 확인, 자동화 기능 등이 CDO의 Cisco Meraki MX 지원의 주요 기능입니다.

Cisco IOS 디바이스

Cisco IOS는 라우팅, 스위칭 및 기타 네트워킹 프로토콜을 포함한 네트워크 기능을 관리하고 제어할 수 있습니다. Cisco 네트워크 장치를 구성하고 유지 관리하기 위한 일련의 기능과 명령을 제공하여 다양한 규모와 복잡한 네트워크 내에서 효율적인 커뮤니케이션과 관리를 가능하게 합니다.

Cisco Umbrella

CDO는 Umbrella ASA 통합과 같은 통합을 통해 Cisco Umbrella를 관리합니다. 이를 통해 관리자는 인터페이스별 정책을 사용하여 Umbrella 컨피그레이션에 Cisco ASA(Adaptive Security Appliance)를 포함할 수 있습니다. 이러한 통합을 통해 ASA에서는 DNS 쿼리를 Umbrella로 리디렉션할 수 있으며 Umbrella의 DNS 보안, 웹 필터링 및 위협 인텔리전스 기능을 활용하여 네트워크 보안을 강화할 수 있습니다.

AWS 보안 그룹

CDO는 AWS(Amazon Web Services) VPC(Virtual Private Clouds, 가상 프라이빗 클라우드를 위한 간소화된 관리 인터페이스를 제공합니다. 주요 기능으로는 AWS 사이트 간 VPN 연결 모니터링, AWS 장치 변경 사항 추적, AWS 사이트 간 VPN 터널 보기 등이 있습니다.

CDO에서 지원하는 브라우저

CDO는 다음 브라우저의 최신 버전을 지원합니다.

- Google Chrome
- Mozilla Firefox

CDO 플랫폼 유지 관리 일정

CDO은 새로운 기능과 품질 개선으로 매주 플랫폼을 업데이트합니다. 이 일정에 따라 업데이트가 3시간 동안 이루어집니다.

요일	시간 **(24**시간제**, UTC)**
목요일	09:00 UTC - 12:00 UTC

이 유지 관리 기간 동안 테넌트에 계속 액세스할 수 있으며 클라우드 제공 Firewall Management Center 또는 멀티 클라우드 방어 컨트롤러가 있는 경우, 해당 플랫폼에도 액세스할 수 있습니다. 또한 CDO에 온보딩한 디바이스가 보안 정책을 계속 적용합니다.

참고

- 유지 관리 기간 동안 관리하는 디바이스에 구성 변경 사항을 구축하는 데 CDO을 사용하지 않는 것이 좋습니다.
- CDO과 통신이 중단되는 문제가 발생하면 유지보수 기간이 아니더라도 영향을 받는 모든 테넌트에게 최대한 신속하게 장애를 해결합니다.

클라우드 제공 Firewall Management Center 유지 관리 일정

테넌트에 배포된 클라우드 제공 Firewall Management Center을 보유한 고객은 CDO가 클라우드 제공 Firewall Management Center 환경을 업데이트하기 약 1주일 전에 알림을 받습니다. 테넌트의 슈퍼 관리자 및 관리자 사용자에게는 이메일 알림이 전송됩니다. CDO 는 또한 모든 사용자에게 향후 업데이트를 알리는 배너를 홈페이지에 표시합니다.

참고

- 유지 관리 기간 동안 관리하는 디바이스에 구성 변경 사항을 배포하는 데 클라우드 제공 Firewall Management Center을 사용하지 않는 것이 좋습니다.
- CDO또는 클라우드 제공 Firewall Management Center과 통신이 중단되는 문제가 발생하면 유지보수 기간이 아니더라도 영향을 받는 모든 테넌트에게 최대한 신속하게 장애를 해결합니다.

CDO 테넌트 관리

CDO를 사용하면 테넌트, 사용자 및 알림 기본 설정의 특정 측면을 사용자 지정할 수 있습니다. 사용자 지정 구성에 사용할 수 있는 다음 설정을 검토하십시오.

일반 설정

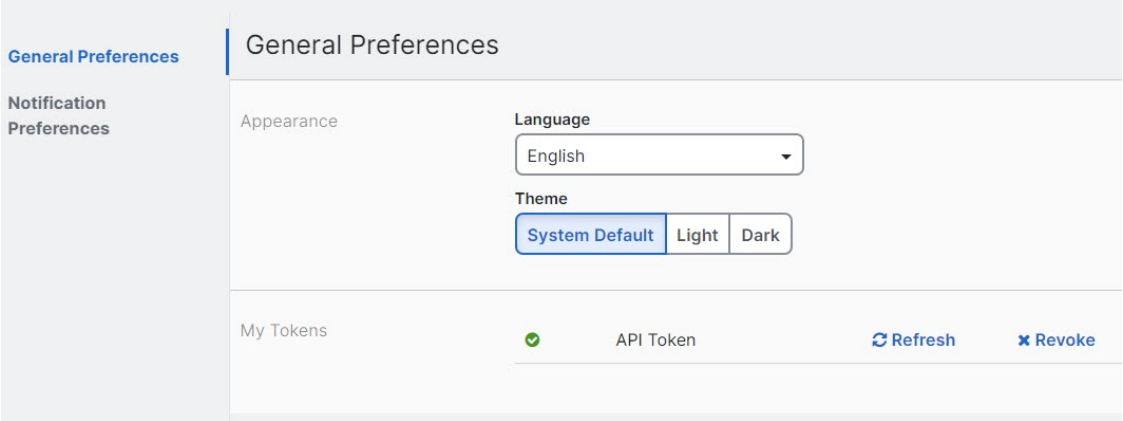
일반 CDO 설정에 관한 다음 항목을 참조하십시오.

- 일반 환경설정, on page 46
- 내 토큰은 API 토큰, on page 58를 참조하십시오.
- **Tenant Settings(**테넌트 설정**)**은 다음을 참조하십시오.
  - 변경 요청 추적 활성화, on page 47
  - Cisco 지원에서 테넌트를 볼 수 없도록 설정, on page 47
  - 디바이스 변경 사항 자동 수락 옵션 활성화, on page 47
  - 기본 충돌 탐지 간격, on page 48

- 웹 분석, on page 49
- 테넌트 ID, on page 49
- 테넌트 이름, on page 49

일반 환경설정

CDO UI를 표시할 언어와 테마를 선택합니다. 이 선택은 이 변경을 수행하는 사용자에게만 영향을 미칩니다.



CDO 웹 인터페이스 모양 변경

웹 인터페이스가 표시되는 방식을 변경할 수 있습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Preferences(**환경설정**)**를 선택합니다.

단계 **2** **General Preferences(**일반 환경설정**)** 영역에서 **Theme(**테마**)**를 선택합니다.

- 밝게
- 어두움

내 토큰

자세한 내용은 API 토큰을 참조하십시오.

테넌트 설정

변경 요청 추적 활성화

변경 요청 추적을 활성화하면 테넌트의 모든 사용자에게 영향을 미칩니다. 변경 요청 추적을 활성화하려면 다음 절차를 따르십시오.

Procedure

단계 **1** CDO 메뉴 모음에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**을 선택합니다.

단계 **2** 변경 요청 추적 아래의 슬라이더를 클릭합니다.

확인되면 인터페이스의 왼쪽 하단 모서리에 변경 요청 도구 모음이 나타나고 변경 로그의 변경 요청 드롭다운 메뉴가 나타납니다.

Cisco 지원에서 테넌트를 볼 수 없도록 설정

Cisco 지원에서는 지원 티켓을 해결하거나 두 개 이상의 고객에게 영향을 미치는 문제를 사전에 해결하기 위해 사용자를 테넌트와 연결합니다. 그러나 원하는 경우 계정 설정을 변경하여 Cisco 지원이 테넌트에 액세스하지 못하도록 할 수 있습니다. 이렇게 하려면 **Cisco** 지원에서 이 테넌트를 볼 수 없도록 방지 아래의 토글 버튼을 밀어서 녹색 확인 표시를 합니다.

Cisco 지원에서 테넌트를 볼 수 없도록 하려면 다음 절차를 따르십시오.

Procedure

단계 **1** CDO 메뉴 모음에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**을 선택합니다.

단계 **2** **Cisco** 지원팀에서 이 테넌트를 볼 수 없도록 방지 아래의 슬라이더를 클릭합니다.

디바이스 변경 사항 자동 수락 옵션 활성화

디바이스 변경에 대한 자동 수락을 활성화하면 CDO가 디바이스에서 직접 수행된 모든 변경 사항을 자동으로 수락할 수 있습니다. 이 옵션을 비활성화된 상태로 두거나 나중에 비활성화하는 경우 수락하기 전에 각 디바이스 충돌을 검토해야 합니다.

디바이스 변경 사항에 대한 자동 수락을 활성화하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**을 클릭합니다.

단계 **2** **Enable the option to auto-accept device changes(**디바이스 변경 사항을 자동으로 수락하는 옵션 활성화**)** 아래의 슬라이더를 클릭합니다.

기본 충돌 탐지 간격

이 간격은 CDO가 변경 사항을 위해 온보딩된 디바이스를 폴링하는 빈도를 결정합니다. 이 선택은 이 테넌트로 관리되는 모든 디바이스에 영향을 주며 언제든지 변경할 수 있습니다.

Note 하나 이상의 디바이스를 선택한 후 **Inventory(**재고 목록**)** 페이지에서 사용 가능한 **Conflict Detection(**충돌 탐지**)** 옵션을 통해 이 선택 항목을 오버라이드할 수 있습니다.

이 옵션을 구성하고 충돌 탐지를 위한 새 간격을 선택하려면 다음 절차를 수행합니다.

Procedure

단계 **1** CDO 메뉴 모음에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**을 선택합니다.

단계 **2** **Default Conflict Detection Interval(**기본 충돌 탐지 간격**)**의 드롭다운 메뉴를 클릭하고 시간 값을 선택합니다.

자동 구축 예약 옵션 활성화

자동 구축을 예약하는 옵션을 활성화하면 편리한 날짜와 시간에 향후 구축을 예약할 수 있습니다. 활성화되면 단일 또는 반복 자동 구축을 예약할 수 있습니다. 자동 구축을 예약하려면 자동 구축 예약을 참조하십시오.

전용 의 보류 중인 변경 사항이 있는 경우 디바이스에 대한 CDO의 변경 사항은 디바이스에 자동으로 구축되지 않습니다. 디바이스가 **Conflict Detected(**충돌 탐지됨**)** 또는 **Not Synced(**동기화되지 않음**)**와 같이 **Synced(**동기화됨**)** 상태가 아닌 경우 예약된 구축이 실행되지 않습니다. 예약된 구축이 실패한 모든 인스턴스가 작업 페이지에 나열됩니다.

Enable the Option to Schedule Automatic Deployments(자동 구축 예약 옵션 활성화**)**가 해제된 경우 예약된 모든 구축이 삭제됩니다.

Important CDO를 사용하여 디바이스에 대해 둘 이상의 예약된 구축을 생성하는 경우 새 구축이 기존 구축을 덮어씁니다. API를 사용하여 디바이스에서 둘 이상의 예약된 구축을 생성하는 경우, 새 구축을 예약하기 전에 기존 구축을 삭제해야 합니다.

자동 구축을 예약하는 옵션을 활성화하려면 다음 절차를 따르십시오.

Procedure

단계 **1** CDO 메뉴 모음에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**을 선택합니다.

단계 **2** **Enable the option to schedule automatic deployment(**자동 구축을 예약하는 옵션 활성화**)** 아래의 슬라이더를 클릭합니다.

웹 분석

웹 분석은 페이지 히트를 기반으로 익명의 제품 사용 정보를 Cisco에 제공합니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다.

웹 분석은 기본적으로 활성화됩니다. 웹 분석을 비활성화하거나 나중에 활성화하려면 다음 절차를 따르십시오.

Procedure

단계 **1** CDO 메뉴 모음에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**을 선택합니다.

단계 **2** 웹 분석 아래의 토글을 클릭합니다.

테넌트 **ID**

테넌트 ID는 테넌트를 식별합니다. 이 정보는Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다.

테넌트 이름

테넌트 이름도 테넌트를 식별합니다. 테넌트 이름은 조직 이름이 아닙니다. 이 정보는Cisco TAC(Technical Assistance Center)에 문의해야 하는 경우에 유용합니다.

CDO 알림 보기

알림 아이콘을 클릭하여 테넌트에 온보딩한 디바이스에 발생했거나 영향을 미친 최신 알림을 확인합니다. **Notification Settings(**알림 설정**)** 페이지에서 선택하는 항목은 CDO에 표시되는 알림 유형에 영향을 미칩니다. 자세한 내용을 보려면 계속 읽으십시오.

이 드롭다운 페이지는 Overview(개요), All(모두), Dismissed(해제됨)의 3개 탭으로 그룹화됩니다.

개요 탭

Overview(개요**)** 탭은 가장 최근의 우선 순위가 높은 알림 및 구독한 이벤트를 조합하여 표시합니다. 높은 우선순위 이벤트는 다음과 같습니다.

- 구축 실패
- 백업 실패
- 업그레이드 실패
- FTD를 cdFMC로 마이그레이션 실패
- 디바이스가 오프라인 상태가 됨
- 디바이스 HA 상태가 변경됨
- 디바이스 인증서 만료

Notifications(알림 설정) 창에서 Notification Settings(알림 설정)를 클릭하거나 **UserID(**사용자 **ID)** > **User Preferences(**사용자 환경 설정**)** 페이지에서 수신할 알림을 구성할 수 있습니다. 대시보드 오른쪽 상단 모서리에 있는 User ID(사용자 ID) 버튼.

All(모두**)** 탭

All(모두**)** 탭은 이메일 구독 알림 및 높은 우선 순위로 나열된 모든 항목을 포함하여 우선 순위와 상관없이 모든 알림을 표시합니다.

Dismissed(해제됨**)** 탭

Dismissed(해제됨**)** 탭에는 해제한 알림이 표시됩니다. 알림의 "**x**"를 클릭하면 개별 알림을 무시할 수 있습니다.

드롭다운 메뉴에서 알림 **Dismiss(**해제**)**를 선택하면 "개요" 및 "모두" 탭 모두 에서 알림이 해제됩니다. **Dismiss(**해제**)** 탭에 30일 동안 유지되며, 그 이후에는 CDO에서 제거됩니다.

알림 검색

알림 드롭다운 창을 보는 경우, 위에서 언급한 탭 중 하나를 사용하여 키워드나 알림을 쿼리할 수 있습니다.

사용자 알림 환경 설정

테넌트와 연결된 기기에서 특정 이벤트가 발생할 때마다 CDO에서 알림이 생성됩니다(예: 테넌트와 연결된 기기에서 특정 동작이 발생할 때마다, 기기 인증서가 만료되거나 만료된 경우, 백그라운드 로그 검색이 시작, 완료 또는 실패한 경우 등). 다음 알림은 기본적으로 활성화되어 있으며, 사용자 역할과 상관없이 테넌트와 연결된 모든 사용자에 대해 표시됩니다. 관심 있는 알림만 표시하도록 개인 알림 환경 설정을 수정할 수 있습니다. 이러한 환경 설정은 사용자만 선택할 수 있으며, 테넌트와 연결된 다른 사용자에게 영향을 미치지 않습니다.

참고 또한 아래에 나열된 알림에 대한 변경 사항은 실시간으로 자동 업데이트되며 구축이 필요하지 않습니다.

Username ID(사용자 이름 **ID)** > **Preferences(**환경 설정**)** > **Notification Preferences(**알림 환경 설정**)** 페이지에서 개인 환경 설정을 확인합니다. 사용자 이름 ID는 항상 모든 페이지에서 CDO의 오른쪽 상단에 있습니다. 이 페이지에서 아래의 "**Notify Me in CDO When(**다음의 경우 알림**)**" 알림을 구성할 수 있습니다.

디바이스 워크플로우에 대한 알림 전송

- 구축 - 이 작업은 하며, SSH 또는 IOS 디바이스에 대한 통합 인스턴스는 포함하지 않습니다.
- 백업 - 이 작업은 FDM 관리 디바이스에만 적용됩니다.
- 업그레이드 - 이 작업은 ASA 및 FDM 관리 디바이스에만 적용됩니다.
- **FTD**를 클라우드로 마이그레이션 - 이 작업은 FTD

  Device Manager를 FMC에서 CDO로 변경할 때 적용됩니다.

디바이스 이벤트에 대한 알림 전송

- 오프라인 상태 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 온라인 재전환 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- 충돌 탐지됨 - 이 작업은 테넌트와 연결된 모든 디바이스에 적용됩니다.
- **HA** 상태 변경됨 - 이 작업은 HA 또는 페일오버 쌍 내의 디바이스, 현재 상태 및 변경된 상태를 나타냅니다. 이 작업은 테넌트와 연결된 모든 HA 및 페일오버 구성에 적용됩니다.
- 사이트 간 세션 연결 끊김 - 이 작업은 테넌트에 구성된 모든 사이트 간 VPN 구성에 적용됩니다.

백그라운드 로그 검색을 위해 알림 전송

- 검색 시작 - 검색이 시작되면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다.
- 검색 완료 - 검색이 종료되면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다.
- 검색 실패 - 검색이 실패하면 알림을 받습니다. 이는 즉시 검색 및 예약된 검색에 모두 적용됩니다. 매개변수 또는 쿼리를 확인하고 다시 시도하십시오.

알림 환경 설정 선택 취소

기본적으로 모든 이벤트는 활성화되고 알림을 생성합니다. 위에서 언급한 이벤트에 의해 생성된 알림을 선택 취소하려면 알림 유형을 수동으로 선택 취소 해야 합니다. 변경 사항을 확인하려면 **Save(**저장**)**를 클릭해야 합니다.

이메일 경고

위에서 언급한 알림을 수신하려면 **Email Alerts(**이메일 알림**)** 토글을 활성화합니다. 이메일로 수신할 알림을 선택하고 **Save(**저장**)** 버튼을 클릭합니다. 기본적으로 **Use CDO notification settings above(**위의 알림 설정 사용**)**는 선택되어 있습니다. 즉, 이 페이지의 "Send Alerts When...(다음의 경우 알림 전송...)" 섹션에서 선택한 것과 동일한 모든 알림 및 이벤트에 대한 이메일 알림을 수신하게 됩니다.

위에서 언급한 이벤트 또는 경고 중 일부만 이메일로 전달하려면 **Use CDO notification settings above(**위의 알림 설정 사용**)**의 선택을 취소합니다. 이 작업은 사용 가능한 알림을 수정하고 개인화하기 위한 추가 위치를 생성합니다. 이는 리던던시(redundancy)를 줄이는 데 도움이 될 수 있습니다.

테넌트 알림 설정

왼쪽 탐색 모음에서 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

테넌트와 연결된 모든 사용자는 이러한 알림을 자동으로 수신합니다. 또한 이러한 알림의 일부 또는 모두가 특정 이메일이나 서비스로 전달될 수 있습니다.

Note 이러한 설정을 변경하려면 슈퍼 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 CDO의 사용자 역할을 참조하십시오.

이메일 가입자

CDO 테넌트의 알림을 수신하는 이메일을 추가하거나 수정합니다. 자세한 내용은 이메일 가입자 활성화, on page 52를 참조하십시오.

서비스 통합

메시징 앱에서 수신 **Webhook**를 활성화하고 앱 대시보드에서 직접 CDO 알림을 수신합니다. 자세한 내용은 CDO 알림을 위한 서비스 통합 활성화를 참조하십시오.

이메일 가입자 활성화

CDO의 이메일 알림은 작업 유형 및 영향을 받는 디바이스를 나타냅니다. 디바이스의 현재 상태 및 작업 내용에 대한 자세한 정보를 알아보려면 CDO에 로그인하여 영향을 받는 디바이스의 CDO에서 변경 로그 관리를 검토하는 것이 좋습니다.

경고! 메일러를 추가하는 경우 올바른 이메일을 입력해야 합니다. CDO는 테넌트와 연결된 알려진 사용자에 대한 이메일 주소를 확인하지 않습니다.

이메일 구독 추가

시작하기 전에

이메일 구독 목록을 보려면 관리자여야 하며, 이메일 구독을 추가, 제거 또는 편집하려면 슈퍼 관리자여야 합니다.

프로시저

단계 **1** CDO에 로그인하고 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**로 이동합니다.

단계 **2** 페이지의 오른쪽 상단에 있는 **+** 아이콘을 클릭합니다.

단계 **3** 텍스트 필드에 유효한 이메일 주소를 입력합니다.

단계 **4** 가입자에게 알리려는 이벤트 및 알림의 해당 체크 박스를 선택하고 선택 취소합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. 언제든지 **Cancel(**취소**)**을 클릭하여 테넌트에 대한 새 이메일 구독을 생성할 수 있습니다.

이메일 구독 편집

시작하기 전에

이메일 구독 목록을 보려면 관리자여야 하며, 이메일 구독을 추가, 제거 또는 편집하려면 슈퍼 관리자여야 합니다.

프로시저

단계 **1** CDO에 로그인하고 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**로 이동합니다.

단계 **2** 이메일 구독을 위해 편집하도록 활성화하려는 이메일 주소를 찾습니다.

단계 **3** 편집 아이콘을 클릭합니다.

단계 **4** 다음 속성을 편집합니다.

- 이메일 주소
- 디바이스 워크플로우가 .…일 때 알림 전송
- 다음 경우에 알림 전송... 디바이스 이벤트
- 다음 경우에 알림 전송... 백그라운드 로그 검색

단계 **5** **Ok(**확인**)**를 클릭합니다. 언제든지 **Cancel(**취소**)**을 클릭하여 이메일 구독에 대한 변경 사항을 무효화할 수 있습니다.

이메일 구독 삭제

이메일 구독 목록에서 메일러를 삭제하려면 다음 절차를 사용합니다.

시작하기 전에

이메일 구독 목록을 보려면 관리자여야 하며, 이메일 구독을 추가, 제거 또는 편집하려면 슈퍼 관리자여야 합니다.

프로시저

단계 **1** CDO에 로그인하고 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**로 이동합니다.

단계 **2** 테넌트의 이메일 구독에서 제거할 사용자를 찾습니다.

단계 **3** 제거할 사용자에 대해 **Remove(**제거**)** 아이콘을 클릭합니다.

단계 **4** 구독 목록에서 사용자를 제거할지 확인합니다. 이는 사용자 기능에 영향을 주지 않습니다.

CDO 알림을 위한 서비스 통합 활성화

서비스 통합을 활성화하여 지정된 메시징 애플리케이션 또는 서비스를 통해 CDO 알림을 전달합니다. 알림을 받으려면 메시지 프로그램에서 웹후크 URL을 생성하고 CDO의 **Notification Settings(**알림 설정**)** 페이지에서 해당 웹후크를 CDO에 지정해야 합니다.

CDO는 기본적으로 Cisco Webex 및 Slack을 서비스 통합으로 지원합니다. 이러한 서비스로 전송되는 메시지는 채널 및 자동화된 봇용으로 특별히 형식이 지정됩니다.

참고 Webhook별로 수신할 알림에 대해 해당 상자를 선택해야 합니다.

Webex Teams에 대해 수신 Webhook

시작하기 전에

CDO 알림은 지정된 작업 공간에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. 이 절차를 완료하기 전에 다음을 수행해야 합니다.

- Webex 계정.
- CDO 계정 및 테넌트.

Webex Teams에 대해 수신 웹후크를 허용하려면 다음 절차를 따르십시오.

프로시저

단계 1 Webex apphub를 엽니다.

단계 2 페이지 맨 위에서 **Connect(**연결**)**를 클릭합니다.

단계 3 페이지 하단으로 스크롤하여 다음을 구성합니다.

- **Webhook** 이름 - 이 애플리케이션에서 제공하는 메시지를 식별하기 위한 이름을 입력합니다.
- **Space(**공간**)** 선택 - 드롭다운 메뉴를 사용하여 Webex **Space(**공간**)**를 선택합니다. 공간이 이미 Webex 팀에 존재해야 하며 이 공간에 대한 액세스 권한이 있어야 합니다. 공간이 존재하지 않는 경우 Webex Teams에서 새 공간을 만들고 애플리케이션의 구성 페이지를 새로 고쳐 새 공간을 표시할 수 있습니다.

참고
과거에 Webex 수신 웹훅을 구성한 적이 있고 다시 활성화하는 경우, 이전 웹훅은 이 페이지 하단에 유지됩니다. 이전 웹훅이 더 이상 필요하지 않거나 웹엑스 공간이 더 이상 존재하지 않는 경우 삭제할 수 있습니다.

단계 4 **Add(**추가**)**를 선택합니다. 선택한 Webex Space는 애플리케이션이 추가되었다는 알림을 받게 됩니다.

단계 5 웹후크 URL을 복사합니다.

단계 6 CDO에 로그인합니다.

단계 7 왼쪽 탐색 모음에서 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 8 선택한 알림이 올바른지 검사하고 확인합니다. 그렇지 않은 경우 서비스 통합에 연결하기 전에 알림 선택을 수정할 것을 강력하게 권장합니다.

단계 9 **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 10 파란색 플러스 버튼을 클릭합니다.

단계 11 **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 12 드롭다운 메뉴를 확장하고 **Webex**를 서비스 유형으로 선택합니다.

단계 13 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 14 **OK(**확인**)**를 클릭합니다.

Slack용 수신 Webhook

CDO 알림은 지정된 채널에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. Slack이 수신 웹후크를 처리하는 방법에 대한 자세한 내용은 Slack 앱을 참조하십시오.

Slack에 대해 수신 웹후크를 허용하려면 다음 절차를 따르십시오.

프로시저

단계 **1** Slack계정에 로그인합니다.

단계 **2** 왼쪽 패널에서 아래로 스크롤하여 **Add Apps(**앱 추가**)**를 선택합니다.

단계 **3** **Incoming Webhooks(**수신 웹후크**)**에 대한 애플리케이션 디렉토리를 검색하고 앱을 찾습니다. **Add(**추가**)**를 선택합니다.

단계 **4** Slack 워크스페이스의 관리자가 아닌 경우, 조직의 관리자에게 요청을 보내고 앱이 계정에 추가될 때까지 기다려야 합니다. **Request Configuration(**요청 구성**)**을 선택합니다. 선택적 메시지를 입력하고 **Submit Request(**요청 제출**)**을 선택합니다.

단계 **5** 워크스페이스에 수신 웹후크 앱이 활성화되면 Slack 설정 페이지를 새로고침하고 **Add New Webhook to Workspace(**워크스페이스에 새 웹후크 추가**)**를 선택합니다.

단계 **6** 드롭다운 메뉴를 사용하여 CDO 알림을 표시할 Slack 채널을 선택합니다. **Authorize(**승인**)**을 선택합니다. 요청이 활성화되기를 기다리는 동안 이 페이지에서 다른 곳으로 이동하려면 Slack에 로그인하고 왼쪽 상단 모서리에서 작업 공간 이름을 선택하기만 하면 됩니다. 드롭다운 메뉴에서 **Customize Workspace(**작업 공간 사용자 지정**)**을 선택하고 **Configure Apps(**앱 구성**)**을 선택합니다. **Custom Integrations(**사용자 지정 통합**)** > **Manage (**관리**)**로 이동합니다. **Incoming Webhooks(**수신 웹후크**)**를 선택하여 앱의 랜딩 페이지를 연 다음 탭에서 **Configuration(**구성**)**을 선택합니다. 그러면 이 앱이 활성화된 작업 공간 내의 모든 사용자가 나열됩니다. 계정 구성만 보고 편집할 수 있습니다. 작업 공간 이름을 선택하여 구성을 편집하고 계속 진행합니다.

단계 **7** Slack 설정 페이지는 앱의 구성 페이지로 리디렉션됩니다. 웹후크 URL을 찾아 복사합니다.

단계 **8** CDO에 로그인합니다.

단계 **9** 왼쪽 탐색 모음에서 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **10** 선택한 알림이 올바른지 검사하고 확인합니다. 그렇지 않은 경우 서비스 통합에 연결하기 전에 알림 선택을 수정할 것을 강력하게 권장합니다.

단계 **11** **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 **12** 파란색 플러스 버튼을 클릭합니다.

단계 **13** **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 **14** 드롭다운 메뉴를 확장하고 서비스 유형으로 **Slack**을 선택합니다.

단계 **15** 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 **16** OK(확인)를 클릭합니다.

사용자 지정 통합을 위한 수신 웹후크

시작하기 전에

CDO는 사용자 지정 통합을 위한 메시지 형식을 지정하지 않습니다. 사용자 지정 서비스 또는 애플리케이션을 통합하기로 선택한 경우 CDO는 JSON 메시지를 보냅니다.

수신 웹후크를 활성화하고 웹후크 URL을 생성하는 방법에 대한 서비스 설명서를 참조하십시오. 웹후크 URL이 있으면 아래 절차를 사용하여 웹후크를 활성화합니다.

프로시저

단계 **1** 선택한 사용자 지정 서비스 또는 애플리케이션에서 웹후크 URL을 생성하고 복사합니다.

단계 **2** CDO에 로그인합니다.

단계 **3** 왼쪽 탐색 모음에서 **Settings(**설정**)** > **Notification Settings(**알림 설정**)**를 클릭합니다.

단계 **4** 선택한 알림이 올바른지 검사하고 확인합니다. 그렇지 않은 경우 서비스 통합에 연결하기 전에 알림 선택을 수정할 것을 강력하게 권장합니다.

단계 **5** **Service Integrations(**서비스 통합**)**으로 스크롤합니다.

단계 **6** 파란색 플러스 버튼을 클릭합니다.

단계 **7** **Name(**이름**)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 **8** 드롭다운 메뉴를 확장하고 서비스 유형으로 **Custom(**사용자 지정**)**을 선택합니다.

단계 **9** 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 **10** OK(확인)를 클릭합니다.

로깅 설정

월별 이벤트 로깅 한도와 한도가 재설정될 때까지 남은 일수를 확인합니다. 저장된 로깅은 Cisco cloud가 수신한 압축된 이벤트 데이터를 나타냅니다.

지난 12개월 동안 테넌트가 받은 모든 로깅을 보려면 **View Historical Usage(**기록 히스토리 보기**)** 를 클릭합니다.

추가 스토리지를 요청하는 데 사용할 수 있는 링크도 있습니다.

SAML SSO(Single Sign-On)를 과 통합

CDO는 Cisco Secure Sign-On을 SAML Single Sign-On IdP(Identity Provider) 및 MFA(다단계 인증)용 Duo Security로 사용합니다. 이는 CDO의 기본 인증 방법입니다.

그러나 고객이 자신의 SAML SSO(Single Sign-On) IdP 솔루션을 CDO와 통합하려는 경우 IdP가 SAML 2.0 및 IdP(Identity Provider) 시작 워크플로를 지원하는 경우라면 가능합니다.

자체 또는 서드파티 IdP(Identity Provider)를 Cisco Security Cloud Sign On과 통합하려면 Cisco Security Cloud Sign On ID 제공자 통합 가이드를 참조하십시오.

자체 SAML 솔루션을 CDO와 통합하는 데 추가 지원이 필요한 경우 지원팀에 문의하여 케이스를 생성하십시오.

Attention 케이스를 열 때 요청이 올바른 팀에 전달되도록 **Manually Select A Technology(**수동으로 **A** 기술 선택**)**를 선택하고 **SecureX - Sign-on and Administration(SecureX -** 로그인 및 관리**)**을 선택했는지 확인합니다.

SSO 인증서 갱신

ID 공급자(IdP)는 일반적으로 SecureX SSO와 통합됩니다. Cisco TAC 사례를 열고 metadata.xml 파일을 제공하십시오. 자세한 내용은 Cisco SecureX Sign-On 타사 ID 제공자 통합 가이드를 참조하십시오.

주의 사례를 열 때 기술 수동 선택을 선택하고 요청이 올바른 팀에 전달되도록 **SecureX -** 로그온 및 관리를 선택했는지 확인합니다.

(레거시만 해당) IdP(Identity Provider) 통합이 CDO와 직접 통합된 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법.을 열고 metadata.xml 파일을 제공하십시오.

API 토큰

개발자는 CDO REST API 호출을 할 때 CDO API 토큰을 사용합니다. 호출이 성공하려면 REST API 인증 헤더에 API 토큰을 삽입해야 합니다. API 토큰은 만료되지 않는 "장기" 액세스 토큰입니다. 그러나 이를 갱신하고 취소할 수 있습니다.

CDO 내에서 API 토큰을 생성할 수 있습니다. 이러한 토큰은 생성 직후 일반 설정 페이지가 열려 있는 동안에만 표시됩니다. CDO에서 다른 페이지를 열고 일반 설정페이지로 돌아가면, 토큰이 분명히 발급었지만 토큰이 더 이상 표시되지 않습니다.

개별 사용자는 특정 테넌트에 대한 자체 토큰을 생성할 수 있습니다. 사용자는 다른 사용자를 대신하여 토큰을 생성할 수 없습니다. 토큰은 계정-테넌트 쌍에 고유하며 다른 사용자-테넌트 조합에 사용할 수 없습니다.

API 토큰 형식 및 클레임

API 토큰은 JSON 웹 토큰(JWT)입니다. JWT 토큰 형식에 대해 자세히 알아보려면 JSON 웹 토큰 소개를 읽어보십시오.

CDO API 토큰은 다음과 같은 클레임 집합을 제공합니다.

- **id** - 사용자/디바이스 uid
- **parentId** - 테넌트 uid
- **ver** - 공개 키의 버전(초기 버전은 0, 예, **cdo_jwt_sig_pub_key.0**)
- **subscriptions** - 보안 서비스 익스체인지 구독 (선택 사항)
- **client_id** - **"api-client"**

- **jti** - 토큰 ID

토큰 관리

API 토큰 생성

Procedure

단계 **1** 왼쪽 탐색 모음에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 클릭합니다.
단계 **2** 내 토큰에서 **Generate API Token(API** 토큰 생성**)**를 클릭합니다.
단계 **3** 민감한 데이터를 유지하기 위한 기업의 모범 사례에 따라 안전한 위치에 토큰을 저장하십시오.

API 토큰 갱신

API 토큰은 만료되지 않습니다. 그러나 사용자는 토큰이 분실되거나 손상된 경우 또는 기업의 보안 지침을 준수하기 위해 API 토큰을 갱신하도록 선택할 수 있습니다.

Procedure

단계 **1** 왼쪽 탐색 모음에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 클릭합니다.
단계 **2** 내 토큰에서 **Renew(**갱신**)**을 클릭합니다. CDO에서 새 토큰을 생성합니다.
단계 **3** 민감한 데이터를 유지하기 위한 기업의 모범 사례에 따라 안전한 위치에 새 토큰을 저장하십시오.

API 토큰 취소

Procedure

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Preferences(**환경설정**)** > **General Preferences(**일반 환경설정**)**를 선택합니다.
단계 **2** 내 토큰에서 **Revoke(**취소**)**를 클릭합니다. CDO는 토큰을 취소합니다.

ID 제공자 계정과 CDO 사용자 레코드 간의 관계

CDO에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 CDO의 사용자 레코드가 있는 계정이 필요합니다. IdP 어카운트에는 사용자의 자격 증명이 포함되며 IdP는 이러한 자격 증명을 기반으로 사용자를 인증합니다. 다단계 인증은 ID 보안의 추가 레이어를 제공합니다. CDO 사용자 레코드에는 주로 사용자 이름, 연결된 CDO 테넌트 및 사용자의 역할이 포함됩니

다. 사용자가 로그인하면 CDO는 IdP의 사용자 ID를 CDO의 테넌트에 있는 기존 사용자 레코드에 매핑하려고 시도합니다. CDO가 일치하는 항목을 찾으면 사용자는 해당 테넌트에 로그인됩니다.

엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. Cisco Secure Cloud Sign-On은 다단계 인증에 Duo를 사용합니다. 고객은 원하는 경우 SAML SSO(Single Sign-On)를 과 통합할 수 있습니다.

로그인 워크플로우

다음은 IdP 계정이 CDO 사용자 레코드와 상호 작용하여 CDO 사용자에 로그인하는 방법에 대한 간략한 설명입니다.

Procedure

단계 **1** 사용자는 인증을 위해 Cisco Secure Cloud Sign-On(https://sign-on.security.cisco.com)과 같은 SAML 2.0 호환 ID 공급자(IdP)에 로그인하여 CDO에 대한 액세스를 요청합니다.

단계 **2** IdP는 사용자가 인증된 사용자라는 SAML 어설션을 발행하고 포털은 사용자가 액세스할 수 있는 애플리케이션을 표시합니다. 타일 중 하나는 CDO를 나타냅니다.

단계 **3** CDO는 SAML 어설션의 유효성을 검사하고 사용자 이름을 추출한 다음 테넌트 중에서 해당 사용자 이름에 해당하는 사용자 레코드를 찾으려고 시도합니다.

- 사용자가 CDO의 단일 테넌트에 대한 사용자 레코드를 가지고 있는 경우 CDO는 사용자에게 테넌트에 대한 액세스 권한을 부여하고 사용자의 역할에 따라 수행할 수 있는 작업이 결정됩니다.
- 사용자가 두 개 이상의 테넌트에 대한 사용자 레코드를 가지고 있는 경우 CDO는 인증된 사용자에게 선택할 수 있는 테넌트 목록을 제공합니다. 사용자는 테넌트를 선택하고 해당 테넌트에 액세스할 수 있습니다. 특정 테넌트에 대한 사용자의 역할에 따라 수행할 수 있는 작업이 결정됩니다.
- CDO에 인증된 사용자와 테넌트의 사용자 레코드에 대한 매핑이 없는 경우 CDO는 사용자에게 CDO에 대해 자세히 알아보거나 무료 평가판을 요청할 수 있는 기회를 제공하는 랜딩 페이지를 표시합니다.

CDO에 사용자 레코드를 생성해도 IdP에 계정이 생성되지 않고 IdP에 계정을 생성해도 CDO에 사용자 레코드가 생성되지 않습니다.

마찬가지로 IdP에서 계정을 삭제한다고 해서 CDO에서 사용자 기록을 삭제한 것은 아닙니다. 그러나 IdP 계정이 없는 경우 사용자를 CDO에 인증할 방법이 없습니다. CDO 사용자 기록을 삭제한다고 해서 IdP 계정이 삭제된 것은 아닙니다. 그러나 CDO 사용자 레코드가 없는 경우 인증된 사용자가 CDO 테넌트에 액세스할 수 있는 방법이 없습니다.

이 아키텍처의 의미

Cisco Security Cloud 로그인을 사용하는 고객

CDO의 Cisco Secure Cloud Sign-On ID 공급자를 사용하는 고객의 경우 슈퍼 관리자는 CDO에 사용자 레코드를 생성할 수 있으며 사용자는 CDO에 자체 등록할 수 있습니다. 두 사용자 이름이 일치하고 사용자가 올바르게 인증된 경우 사용자는 CDO에 로그인할 수 있습니다.

슈퍼 관리자가 사용자가 CDO에 액세스하지 못하도록 해야 하는 경우 CDO 사용자의 사용자 레코드를 간단히 삭제할 수 있습니다. Cisco Secure Cloud Sign-On 계정은 여전히 존재하며 슈퍼 관리자가 사용자를 복원하려는 경우 Cisco Secure Cloud Sign-On에 사용된 것과 동일한 사용자 이름으로 새 CDO 사용자 레코드를 생성하면 됩니다.

고객이 기술 지원 센터(TAC)에 전화해야 하는 CDO 문제에 직면한 경우 고객은 TAC 엔지니어를 위한 사용자 레코드를 생성하여 테넌트를 조사하고 정보와 제안을 고객에게 다시 보고할 수 있습니다.
.

자체 **ID** 제공자가 있는 고객

SAML SSO(Single Sign-On)를 과 통합의 경우 ID 공급자 계정과 CDO 테넌트를 모두 제어합니다. 이러한 고객은 CDO에서 ID 공급자 계정 및 사용자 레코드를 만들고 관리할 수 있습니다.

사용자가 CDO에 액세스하지 못하도록 해야 하는 경우, IdP 계정, CDO 사용자 레코드 또는 둘 다를 삭제할 수 있습니다.

Cisco TAC의 도움이 필요한 경우, TAC 엔지니어를 위해 읽기 전용 역할이 있는 ID 공급자 계정과 CDO 사용자 레코드를 모두 생성할 수 있습니다. 그런 다음 TAC 엔지니어는 고객의 CDO 테넌트에 액세스하여 조사하고 고객에게 정보와 제안을 보고할 수 있습니다.3

Cisco Managed Service 제공자

Cisco MSP(Managed Service Provider)가 CDO의 Cisco Secure Cloud Sign-On IdP를 사용하는 경우 Cisco Secure Cloud Sign-On에 자체 등록할 수 있으며 고객은 MSP가 고객의 테넌트를 관리할 수 있도록 CDO에 사용자 레코드를 생성할 수 있습니다. 물론 고객은 원할 때 MSP의 레코드를 삭제할 수 있는 모든 권한을 가집니다.

관련 주제

- 일반 설정
- CDO에서 사용자 관리
- CDO의 사용자 역할

멀티 테넌트 포털 관리

CDO 다중 테넌트 포털 보기는 여러 테넌트의 모든 디바이스에서 정보를 검색하고 표시합니다. 이 다중 테넌트 포털은 디바이스 상태, 디바이스에서 실행 중인 소프트웨어 버전 등을 보여줍니다.

시작하기 전에

- 다중 테넌트 포털은 해당 기능이 테넌트에서 활성화된 경우에만 사용할 수 있습니다. 테넌트에 대해 다중 테넌트 포털을 활성화하려면 Cisco TAC에서 지원 티켓을 여십시오.
- 지원 티켓이 해결되고 포털이 생성되면 포털에서 슈퍼 관리자 역할을 가진 사용자는 여기에 테넌트를 추가할 수 있습니다.
- 발생할 수 있는 특정 브라우저 관련 문제를 방지하려면 웹 브라우저에서 캐시와 쿠키를 지우는 것이 좋습니다.

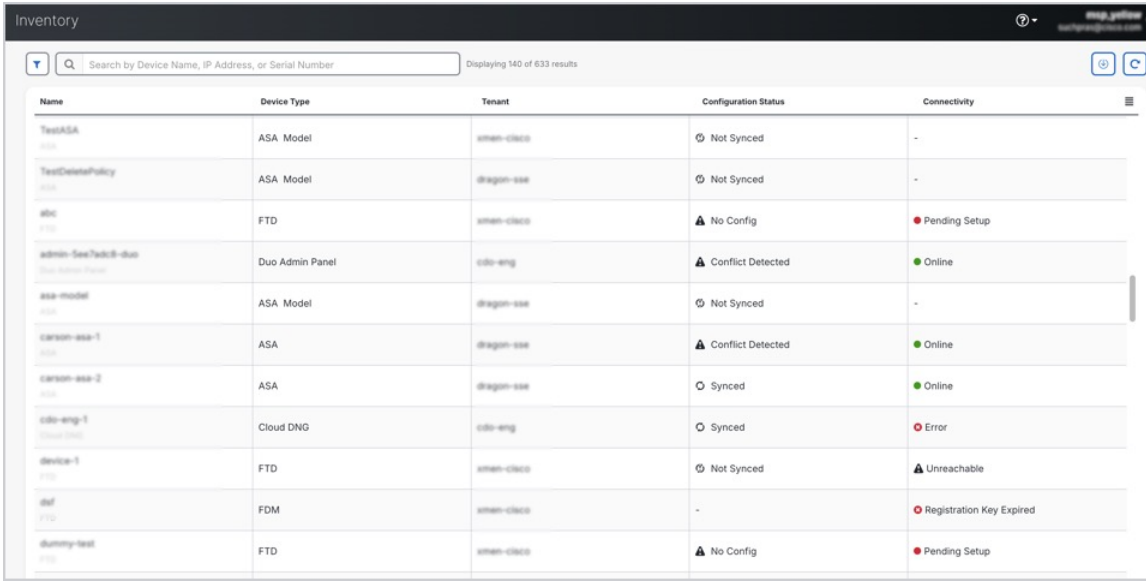
멀티 테넌트 포털

포털은 다음 메뉴를 제공합니다.

- 보안 디바이스
  - 포털에 추가된 테넌트에 온보딩된 모든 디바이스를 표시합니다. 검색 및 필터 옵션을 사용하여 디바이스를 검색합니다.
  - 디바이스를 클릭하면 모델, 온보딩 방법, 방화벽 모드, 소프트웨어 버전 등의 세부 정보를 볼 수 있습니다.
  - 디바이스를 관리하는 CDO 테넌트에서만 디바이스를 관리할 수 있습니다. 다중 테넌트 포털은 CDO 테넌트 페이지로 연결되는 장치 관리 링크를 제공합니다.

    해당 테넌트에 대한 계정이 있고 테넌트가 포털과 동일한 지역에 있는 경우 이 링크가 표시됩니다. 테넌트에 액세스할 수 있는 권한이 없는 경우 디바이스 관리 링크가 표시되지 않습니다. 권한을 얻으려면 조직의 슈퍼 관리자에게 문의하십시오.
  - 세부 정보를 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다. 이 정보는 디바이스를 분석하거나 액세스 권한이 없는 사람에게 보내는 데 도움이 됩니다. 데이터를 내보낼 때마다 CDO는 새 .csv 파일을 생성합니다. 생성된 파일에는 이름에 날짜와 시간이 포함되어 있습니다.
  - 열 선택기를 사용하면 테이블에서 볼 디바이스 속성을 선택하거나 지울 수 있습니다. 테이블을 사용자 정의하면 CDO는 다음에 로그인할 때 선택 사항을 기억합니다.

Figure 1: 보안 디바이스



Note 디바이스를 관리하는 테넌트가 다른 지역에 있는 경우 해당 지역의 CDO에 로그인할 수 있는 링크가 표시됩니다. 해당 지역의 CDO 또는 해당 지역의 테넌트에 액세스할 수 없는 경우 디바이스를 관리할 수 없습니다.

- 테넌트
  - 포털에 추가된 모든 테넌트를 표시합니다.
  - 슈퍼 관리자 역할이 있는 사용자는 포털에 테넌트를 추가할 수 있습니다.
  - 테넌트 이름으로 검색하고 테넌트 정보를 쉼표로 구분된 값(.csv) 파일로 내보낼 수 있습니다.
- 설정
  - **General Settings(**일반 설정**)**에서 **Portal Settings(**포털 설정**)** 세부 정보를 볼 수 있습니다.
  - **User Management(**사용자 관리**)**에서 모든 **User(**사용자**)**, **Active Directory** 그룹 및 **Audit Logs(**감사 로그**)**의 목록을 볼 수 있습니다. 자세한 내용은 User Management(사용자 관리)를 참조하십시오.

Note 멀티테넌트 포털 슈퍼 관리자인 경우에는 API 엔드포인트를 사용하여 다음과 같은 작업을 수행할 수 있습니다.

- CDO 테넌트 생성
- 멀티테넌트 포털에 기존 CDO 테넌트 추가

멀티 테넌트 포털에 테넌트 추가

슈퍼 관리자 역할이 있는 사용자는 포털에 테넌트를 추가할 수 있습니다. 여러 지역에 걸쳐 테넌트를 추가할 수 있습니다. 예를 들어 유럽 지역의 테넌트를 미국 지역에 추가하거나 그 반대로 추가할 수 있습니다.

Important 테넌트에 대한 API 전용 사용자 생성하고 CDO 인증을 위한 API 토큰을 생성하는 것이 좋습니다.

Note 포털에 여러 테넌트를 추가하려면 각 테넌트에서 API 토큰을 생성하고 텍스트 파일에 붙여넣습니다. 그런 다음 토큰을 생성하기 위해 매번 테넌트로 전환하지 않고도 포털에 테넌트를 차례로 쉽게 추가할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Tenants(**테넌트**)**를 클릭합니다.

단계 **2** **Add Tenant(**테넌트 추가**)**를 클릭합니다.

단계 **3** 새 테넌트를 추가하려면 **Next(**다음**)**을 클릭합니다.

Note

a. 기존 테넌트를 가져오려면 기존 테넌트를 가져오시겠습니까**?** 확인란을 선택합니다.

b. 여러 개의 API 토큰을 쉼표로 구분하여 붙여넣어 CDO에서 기존 테넌트를 추가합니다.

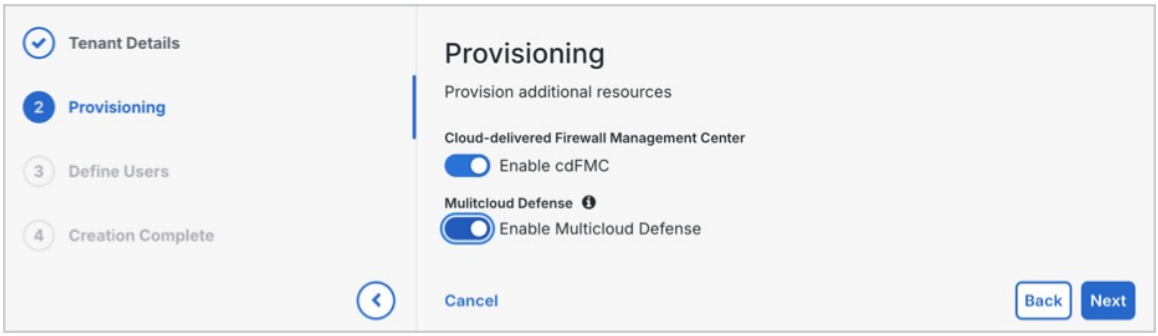
c. **Import(**가져오기**)**를 클릭합니다.

단계 **4** **Tenant Details(**테넌트 세부 정보**)**에서 **Display Name(**표시 이름**)**과 **Tenant Name(**테넌트 이름**)**을 입력합니다. **Next(**다음**)**를 클릭합니다.

단계 **5** **Provisioning(**프로비저닝**)**에서,

- 테넌트에 대한 멀티 클라우드 방어 프로비저닝을 사용하려면 멀티 클라우드 방어 토글을 활성화합니다.

- 테넌트에 대한 클라우드 제공 Firewall Management Center 프로비저닝을 사용하려면 클라우드 제공 Firewall Management Center 토글을 활성화합니다.
- **Next(**다음**)**를 클릭합니다.



단계 **6** **Define Users(**사용자 정의**)**에서 사용자를 하나씩 수동으로 추가하거나 CSV 템플릿을 다운로드하여 필요한 세부 정보를 입력한 후 파일을 업로드합니다. 추가된 사용자는 **User list(**사용자 목록**)** 섹션에 표시됩니다.

단계 **7** **Create Tenant(**테넌트 생성**)**을 클릭합니다.

테넌트 생성이 완료되었으며 프로비저닝에는 몇 분 정도 소요될 수 있습니다.

멀티 테넌트 포털에서 테넌트 삭제

Procedure

단계 **1** 왼쪽 창에서 **Tenants(**테넌트**)**를 클릭합니다.

단계 **2** 오른쪽에 나타나는 해당 삭제 아이콘을 클릭하여 원하는 테넌트를 제거합니다.

단계 **3** **Remove(**제거**)**를 클릭합니다. 참고로 연결된 디바이스도 포털에서 제거됩니다.

관리-테넌트 포털 설정

CDO를 사용하면 설정 페이지에서 다중 테넌트 포털 및 개별 사용자 계정의 특정 측면을 사용자 지정할 수 있습니다. 왼쪽 창에서 **Settings(**설정**)**를 클릭하여 설정 페이지에 액세스합니다.

설정

General Settings(일반 설정**)**

웹 분석은 페이지 히트를 기반으로 익명의 제품 사용 정보를 Cisco에 제공합니다. 이 정보에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 디바이스 호스트 이름 등이 포함됩니다. Cisco는 이 정보를 활용해 기능 사용 패턴을 확인하고 제품을 개선할 수 있습니다. 모든 사용량 데이터는 익명으로 전송되며 민감한 데이터는 전송되지 않습니다.

웹 분석은 기본적으로 활성화됩니다. 웹 분석을 비활성화하거나 나중에 활성화하려면 다음 절차를 따르십시오.

1. CDO 대시보드 왼쪽의 내비게이션 바에서 **Settings(**설정**)**를 클릭합니다.
2. **General Settings(**일반 설정**)**를 클릭합니다.
3. 웹 분석 아래의 슬라이더를 클릭합니다.

사용자 관리

User Management(사용자 관리**)** 화면에서 다중 테넌트 포털과 연결된 모든 사용자 레코드를 볼 수 있습니다. 사용자 계정을 추가, 편집 또는 삭제할 수 있습니다. 자세한 내용은 User CDO에서 사용자 관리를 참조하십시오.

테넌트 전환

포털 테넌트가 둘 이상인 경우 CDO에서 로그아웃하지 않고 다른 포털 또는 테넌트 간에 전환할 수 있습니다.

Procedure

단계 **1** 다중 테넌트 포털에서 오른쪽 상단 모서리에 나타나는 테넌트 메뉴를 클릭합니다.
단계 **2** **Switch tenant(**테넌트 전환**)**를 클릭합니다.
단계 **3** 보려는 포털 또는 테넌트를 선택합니다.

Cisco Success Network

Cisco Success Network는 사용자가 활성화하는 클라우드 서비스입니다. Cisco Success Network를 활성화하면 디바이스와 Cisco cloud간에 보안 연결이 설정되어 사용 정보 및 통계를 스트리밍합니다. 스트리밍 원격 측정은 디바이스에서 관심 있는 데이터를 선택하고 구조화된 형식으로 원격 관리 스테이션에 전송하는 메커니즘을 제공하여 다음과 같은 이점을 제공합니다.

- 네트워크에서 제품의 효율성을 향상시킬 수있는 활용 가능한 미사용 기능을 알려줍니다.
- 제품에 사용할 수 있는 추가 기술 지원 서비스 및 모니터링에 대해 알려줍니다.
- Cisco가 제품을 개선할 수 있습니다.

디바이스는 항상 보안 연결을 설정하고 유지하며 Cisco Success Network에 등록할 수 있습니다. 디바이스를 등록하고 나면 Cisco Success Network 설정을 변경할 수 있습니다.

참고

- Threat Defense 고가용성 쌍의 경우 활성 디바이스 선택이 대기 디바이스의 Cisco Success Network 설정을 오버라이드합니다.
- CDO는 Cisco Success Network 설정을 관리하지 않습니다. Firewall Device Manager 사용자 인터페이스를 통해 관리되는 설정 및 원격 분석 정보가 제공됩니다.

Cisco Success Network 활성화 또는 비활성화

초기 시스템 설정 중에 Cisco Smart Software Manager에 디바이스를 등록하라는 메시지가 표시됩니다. 90일 평가 라이선스를 대신 선택한 경우에는 평가 기간이 종료되기 전에 디바이스를 등록해야 합니다. 디바이스를 등록하려면 Cisco Smart Software Manager(Smart Licensing 페이지)에 디바이스를 등록하거나 등록 키를 입력하여 CDO에 등록합니다.

디바이스를 등록할 때는 가상 어카운트가 디바이스에 라이선스를 할당합니다. 디바이스를 등록하면 활성화한 선택 가능한 라이선스도 등록됩니다.

Firewall Device Manager UI를 통해서만 이 옵션을 비활성화할 수 있지만 Cisco Success Network를 비활성화하여 언제든지 이 연결을 끊을 수 있습니다. 비활성화하면 클라우드에서 디바이스의 연결이 끊어집니다. 연결 해제는 업데이트 수신 또는 스마트 라이선싱 기능 작동에 영향을 주지 않으므로 이러한 기능은 계속 정상적으로 작동됩니다. 자세한 내용은 Firepower 디바이스 매니저 구성 가이드, 버전 6.4.0+에서 시스템 관리 창의 **Cisco Success Network**에 연결 섹션을 참조하십시오.

CDO에서 사용자 관리

CDO에서 사용자 레코드를 생성하거나 편집하기 전에 ID 제공자 계정과 CDO 사용자 레코드 간의 관계를 읽고 IdP(Identity Provider) 계정과 사용자 레코드의 상호 작용 방식을 확인하십시오. CDO 사용자는 인증을 받고 CDO 테넌트에 액세스할 수 있도록 레코드 및 해당 IdP 계정이 필요합니다.

엔터프라이즈에 자체 IdP가 없는 경우 Cisco Secure Sign-On은 모든 CDO 테넌트에 대한 ID 제공자입니다. 이 문서의 나머지 부분에서는 Cisco Secure Sign-On을 ID 제공자로 사용한다고 가정합니다.

User Management(사용자 관리**)** 화면에서 테넌트와 연결된 모든 사용자 레코드를 볼 수 있습니다. 여기에는 지원 티켓을 해결하기 위해 사용자 어카운트와 일시적으로 연결된 모든 Cisco 지원 엔지니어가 포함됩니다.

테넌트와 연결된 사용자 기록 보기

프로시저

단계 **1** 왼쪽 창에서, **Settings(**설정**)** > > **User Management(**사용자 관리**)**를 선택합니다.

참고

Cisco 지원팀이 테넌트에 액세스하지 못하도록 하려면 일반 설정 페이지에서 **Cisco** 지원팀이 이 테넌트를 볼 수 없도록 하기를 활성화합니다.

단계 **2** 왼쪽 창에서 관리 > 사용자 관리.

참고
Cisco 지원팀이 테넌트에 액세스하지 못하도록 하려면 일반 설정 페이지에서 **Cisco** 지원팀이 이 테넌트를 볼 수 없도록 하기 토글을 활성화합니다.

사용자 관리의 Active Directory 그룹

대량의 사용자에 대해 회전율이 높은 테넌트의 경우 개별 사용자를 CDO에 추가하는 대신 CDO를 AD(Active Directory) 그룹에 매핑하여 사용자 목록 및 사용자 역할을 더 쉽게 관리할 수 있습니다. 새 사용자 추가 또는 기존 사용자 제거와 같은 모든 사용자 변경은 이제 Active Directory에서 수행할 수 있으며 더 이상 CDO에서 수행할 필요가 없습니다.

사용자 관리 페이지에서 AD(Active Directory) 그룹을 추가, 편집 또는 삭제하려면 **SuperAdmin** 사용자 역할이 있어야 합니다. 자세한 내용은 CDO의 사용자 역할을 참조하십시오.

왼쪽 창에서, **Settings(**설정**)** > **User Management(**사용자 관리**)**를 선택합니다.

Active Directory 그룹

- 왼쪽 창에서, **Settings(**설정**)** > **User Management(**사용자 관리**)** > **Active Directory Groups(**액티브 디렉토리 그룹**)**를 선택합니다. 이 페이지에는 현재 CDO에 매핑된 Active Directory 그룹이 표시됩니다.
- 이 페이지에는 Active Directory 관리자에서 할당된 Active Directory 그룹의 역할이 표시됩니다.
- Active Directory 그룹 내의 사용자는 **Active Directory** 그룹 탭이나 사용자 탭에 개별적으로 나열되지 않습니다.

감사 로그

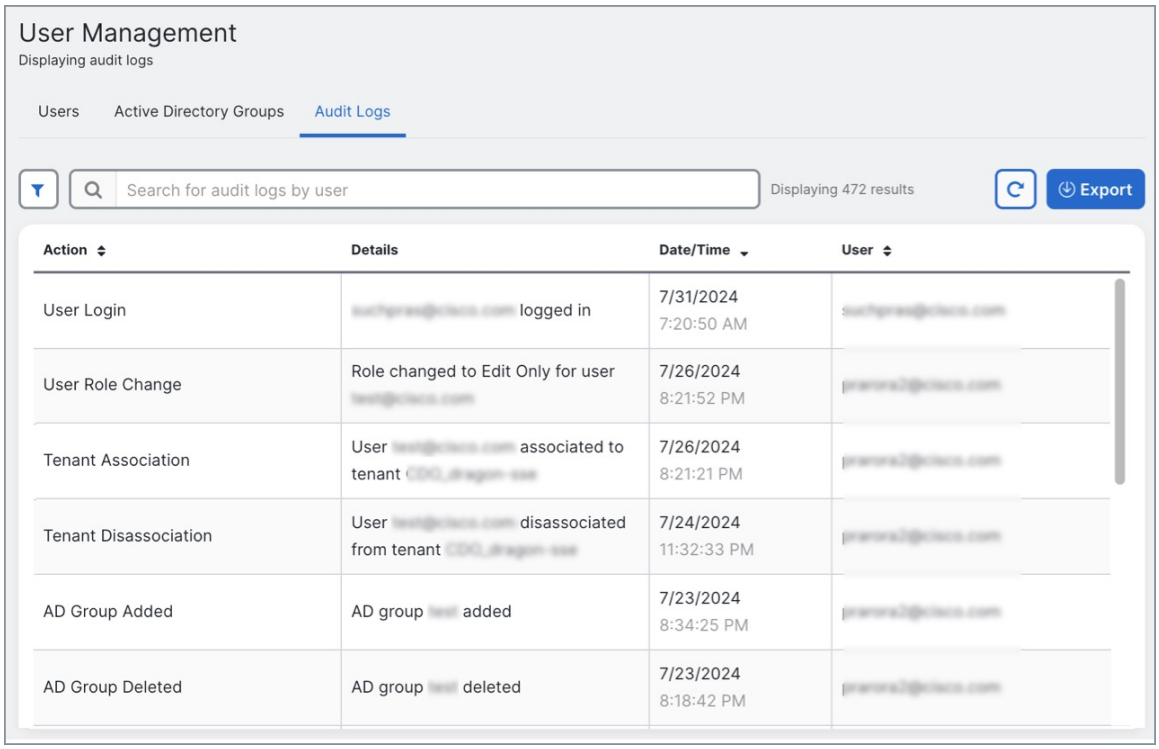
CDO에서 감사 로그는 사용자 관련 및 시스템 수준 작업을 기록합니다. 감사 로그에 캡처되는 주요 이벤트는 다음과 같습니다.

- 사용자 로그인: 사용자 인증의 모든 인스턴스를 기록합니다.
- 테넌트 연결 및 연결 해제: 테넌트와의 사용자 연결 또는 테넌트와의 연결 해제를 추적합니다.
- 사용자 역할 변경: 사용자 역할에 대한 모든 변경 사항을 기록합니다.
- **Active Directory** 그룹: AD 그룹 내의 모든 추가, 삭제 및 역할 변경 사항을 기록합니다.

절차:

1. 왼쪽 창에서 **Settings(**설정**)** > **User Management(**사용자 관리**)**를 클릭합니다.
2. **Audit Logs(**감사 로그**)** 탭을 클릭합니다. 로그인한 현재 테넌트의 이벤트 및 활동 목록이 표시됩니다.
3. **Search** (검색) 텍스트 상자를 사용하여 특정 사용자 에 대한 로그를 찾습니다.
4. 검색 결과를 구체화하고 특정 이벤트를 보려면 필터 아이콘을 클릭합니다. **Time Range(**시간 범위**)** 및 **Event Action(**이벤트 동작**)**을 기준으로 로그를 필터링할 수 있습니다.
5. CSV 형식으로 세부 정보를 다운로드하려면 **Export(**내보내기**)**를 클릭합니다.

그림 ***2:*** 감사 로그



다중 역할 사용자

CDO의 IAM 기능에 따른 확장으로 이제 사용자가 여러 역할을 가질 수 있습니다.

사용자는 Active Directory에서 여러 그룹의 일부가 될 수 있으며 각 그룹은 CDO에서 서로 다른 CDO 역할로 정의될 수 있습니다. 로그인 시 사용자가 얻는 최종 권한은 해당 사용자가 속한 CDO에 정의된 모든 Active Directory 그룹의 역할 조합입니다. 예를 들어 사용자가 두 개의 Active Directory 그룹에 속해 있고 두 그룹이 편집 전용 및 배포 전용과 같은 두 가지 다른 역할로 CDO에 추가된 경우, 사용자는 편집 전용 및 배포 전용 권한을 모두 보유하게 됩니다. 이는 여러 그룹 및 역할에 적용됩니다.

Active Directory 그룹 매핑은 CDO에서 한 번만 정의해야 하며, 이후에 다른 그룹 간에 사용자를 추가, 제거 또는 이동하여 사용자에 대한 액세스 및 권한 관리는 Active Directory에서만 독점적으로 수행할 수 있습니다.

참고 사용자가 개별 사용자이자 동일한 테넌트에 있는 Active Directory 그룹의 일부인 경우 개별 사용자의 사용자 역할이 Active Directory 그룹의 사용자 역할을 오버라이드합니다.

Active Directory 그룹에 대한 **API** 엔드포인트

슈퍼 관리자의 경우 API 엔드포인트를 사용하여 다음을 수행할 수 있습니다.

- Active Directory 그룹 생성
- Active Directory 그룹 제거
- Active Directory 그룹 수정
- Active Directory 그룹 가져오기
- Active Directory 그룹 가져오기

앞서 언급한 링크는 Cisco DevNet 웹사이트의 해당 섹션으로 연결됩니다.

CDO에 Active Directory 그룹을 추가하기 위한 사전 요건

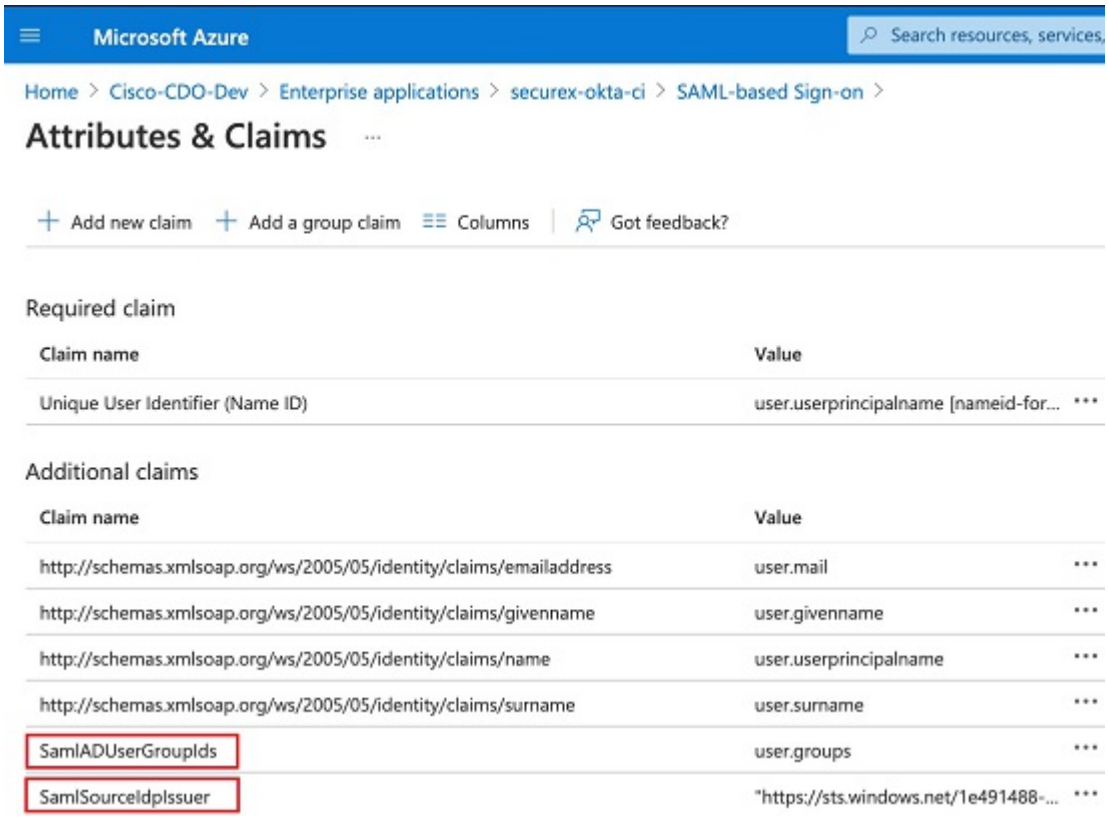
사용자 관리의 한 형태로 Active Directory 그룹 매핑을 CDO에 추가하려면 먼저 Security Cloud Sign On와 통합된 Active Directory가 있어야 합니다. Active Directory ID 공급자(IdP)가 아직 통합되어 있지 않은 경우 다음 정보를 사용하여 사용자 지정 Active Directory IdP 통합을 통합하려면 ID 공급자 통합 가이드를 참조하십시오.

- CDO 테넌트 이름 및 지역
- 사용자 지정 라우팅을 정의할 도메인(예: @cisco.com, @myenterprise.com)
- XML 형식의 인증서 및 페더레이션 메타데이터

Active Directory 통합이 완료되면 Active Directory에 다음 사용자 지정 SAML 클레임을 추가합니다. Active Directory 통합이 완료된 후 CDO 테넌트에 로그인하려면 SAML 클레임 및 속성이 필요합니다. 값은 대/소문자를 구분합니다.

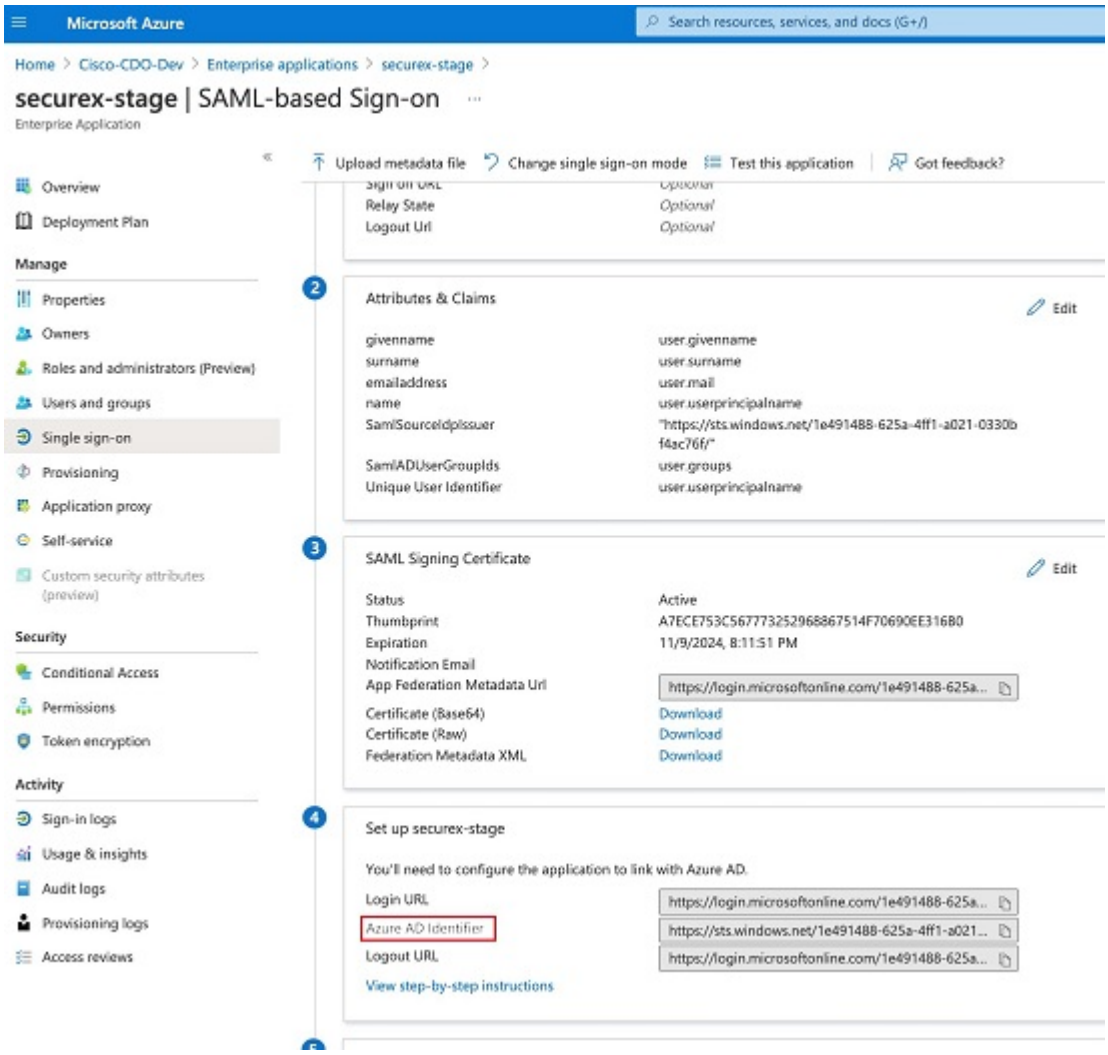
- **SamlADUserGroupIds** - 이 속성은 사용자가 Active Directory에 가지고 있는 모든 그룹 연결을 설명합니다. 예를 들어 Azure에서 아래 스크린샷과 같이 **+ Add a group claim(+** 그룹 클레임 추가**)**를 선택합니다.

그림 *3: Active Directory*에 정의된 사용자 지정 클레임



- **SamlSourceIdpIssuer** - 이 특성은 Active Directory 인스턴스를 고유하게 식별합니다. 예를 들어 Azure에서 **+ Add a group claim(+** 그룹 클레임 추가**)**를 선택하고 스크롤하여 아래 스크린샷과 같이 Azure Active Directory 식별자를 찾습니다.

그림 *4: Azure Active Directory* 식별자 찾기



사용자 관리를 위한 **Active Directory** 그룹 추가

Active Directory 그룹을 추가, 편집 또는 삭제하려면 **SuperAdmin(**슈퍼 관리자**)** 사용자 역할이 있어야 합니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** 왼쪽 창에서, **Settings(**설정**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **3** **Active Directory** 그룹 탭을 클릭합니다.

단계 **4** Active Directory 그룹 추가( ) 버튼.

단계 **5** 다음 정보를 제공합니다.

- 그룹 이름: 고유한 이름을 입력합니다. 이 이름은 Active Directory의 그룹 이름과 일치하지 않아도 됩니다. CDO에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- 그룹 **ID**: Active Directory에서 그룹 ID를 수동으로 입력합니다. 그룹 ID의 값은 사용자 지정 클레임 정의의 그룹 ID와 동일해야 합니다. 그룹의 고유 ID에 해당하는 모든 값(예: my-favorite-group, 12345 등)이 될 수 있습니다.
- **AD** 발급자: Active Directory에서 Active Directory 발급자 값을 수동으로 입력합니다.
- 역할: 사용자 역할을 선택합니다. Active Directory 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 CDO의 사용자 역할을 참조하십시오.
- (선택 사항) 참고: 이 Active Directory 그룹에 적용 가능한 참고를 추가합니다.

단계 **6** **OK(**확인**)**를 선택합니다.

사용자 관리를 위한 **Active Directory** 그룹 편집

시작하기 전에

CDO에서 Active Directory 그룹의 사용자 관리를 편집하면 CDO가 Active Directory그룹을 제한하는 방식만 편집할 수 있습니다. CDO에서 Active Directory 그룹 자체는 편집할 수 없습니다. Active Directory 그룹 내의 사용자 목록을 편집하려면 Active Directory를 사용해야 합니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** 왼쪽 창에서, **Settings(**설정**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **3** **Active Directory** 그룹 탭을 클릭합니다.

단계 **4** 편집하려는 Active Directory 그룹을 식별하고 편집 아이콘을 클릭합니다.

단계 **5** 다음 값을 편집합니다.

- **Group Name(**그룹 이름**)** - 고유한 이름을 입력합니다. CDO에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- **Group Identifier(**그룹 **ID)**: Active Directory에서 그룹 ID를 수동으로 입력합니다. 그룹 ID의 값은 사용자 지정 클레임 정의의 그룹 ID와 동일해야 합니다. 그룹의 고유 ID에 해당하는 모든 값(예: my-favorite-group, 12345 등)이 될 수 있습니다.
- **AD Issuer(AD** 발급자**)**: Active Directory에서 Active Directory 발급자 값을 수동으로 입력합니다.

- 역할: 이 Active Directory 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 사용자 역할을 참조하십시오.
- 참고: 이 Active Directory 그룹에 적용 가능한 참고를 추가합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

사용자 관리를 위한 **Active Directory** 그룹 삭제

프로시저

단계 **1** CDO에 로그인합니다.
단계 **2** 왼쪽 창에서, **Settings(**설정**)** > **User Management(**사용자 관리**)**를 선택합니다.
단계 **3** 왼쪽 창에서 관리 > 사용자 관리를 클릭합니다.
단계 **4** **Active Directory** 그룹 탭을 클릭합니다.
단계 **5** 삭제하려는 Active Directory 그룹을 식별합니다.
단계 **6** 삭제 아이콘을 클릭합니다.
단계 **7** **OK(**확인**)**를 클릭하여 Active Directory 그룹 삭제를 확인합니다.

새 **CDO** 사용자 생성

이 두 가지 작업은 새 CDO 사용자를 만드는 데 필요합니다. 순서대로 수행할 필요는 없습니다.

- 새 사용자를 위해 Cisco Secure Cloud Sign On 계정 생성
- CDO 사용자 이름으로 사용자 레코드 생성

이러한 작업이 완료되면 사용자는 새 사용자가 Cisco Secure Sign-On 대시보드에서 CDO 열기

새 사용자를 위해 **Cisco Secure Cloud Sign On** 계정 생성

새 사용자는 할당된 테넌트의 이름을 몰라도 언제든지 Cisco Security Cloud Sign On 계정을 만들 수 있습니다.

CDO에 로그인 정보

CDO는 Cisco Secure Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. **CDO**에 로그인하려면 먼저 **Cisco Security Cloud Sign On**에서 계정을 생성하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

CDO에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

Important **2019**년 **10**월 **14**일 이전에 **CDO** 테넌트가 존재했다면 이 문서 대신 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, on page 5를 사용하여 로그인 지침을 사용합니다.

로그인하기 전

DUO Security 설치

휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 이중 인증 가이드: 등록 가이드를 참고하십시오.

시간 동기화

모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.

새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성

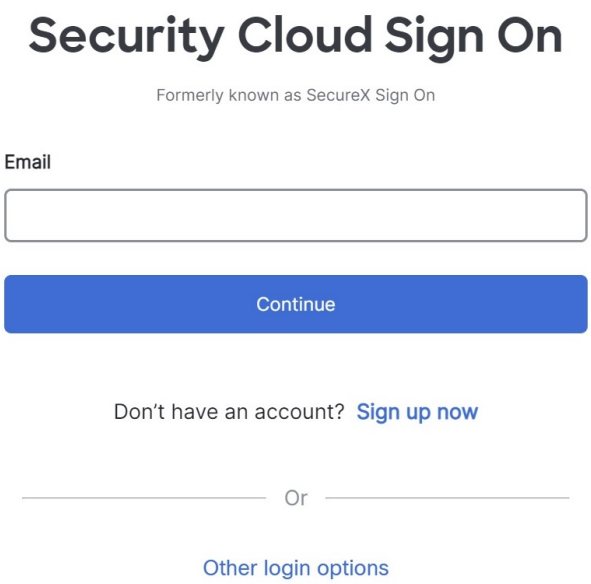
초기 로그인 워크플로우는 4단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

Procedure

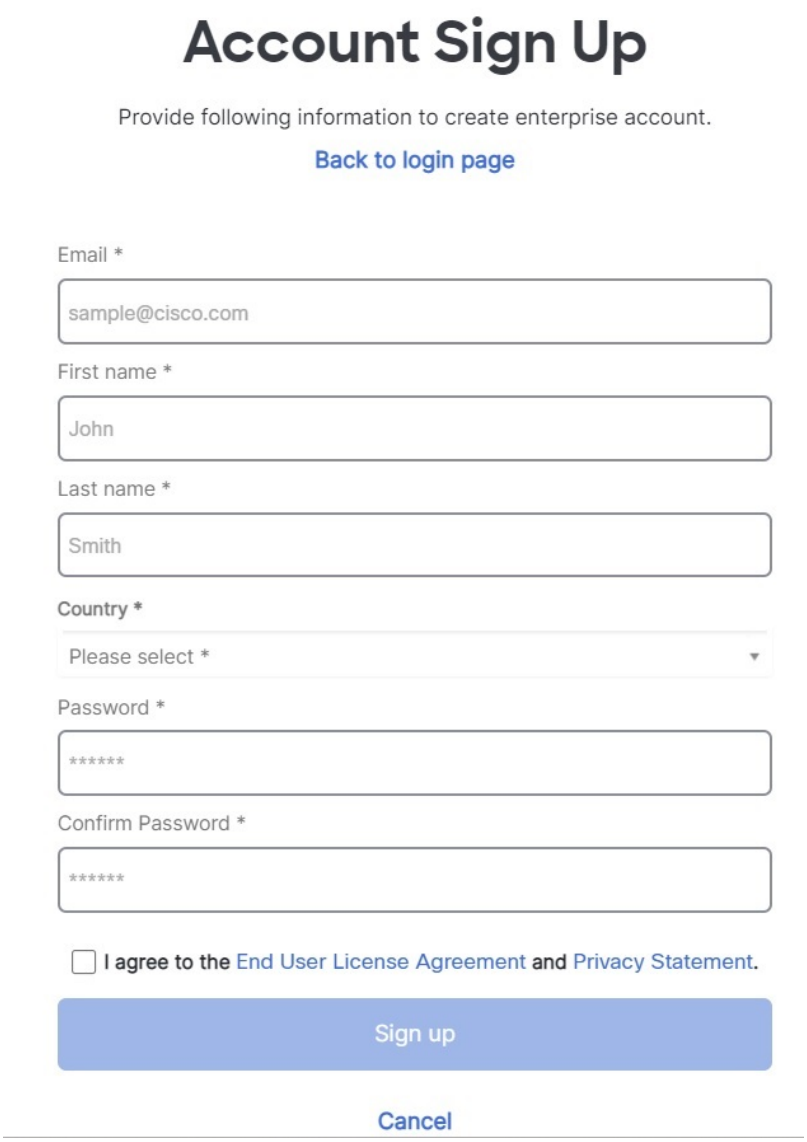
단계 **1** 새 **Cisco Security Cloud Sign On** 계정을 등록합니다.

a. https://sign-on.security.cisco.com을 엽니다.

b. 로그인 화면 하단에서 **Sign up now(**지금 등록**)**을 클릭합니다.



c. 기업 계정을 만들려면 다음 정보를 입력합니다.



다음은 몇 가지 팁입니다.

- **Email(**이메일**)**: CDO에 로그인하는 데 사용할 이메일 주소를 입력합니다.
- **Password(**암호**)**: 강력한 암호를 입력하십시오.

d. **Sign up(**등록하기**)**을 클릭합니다.

Cisco는 등록한 주소로 확인 이메일을 보냅니다. 이메일을 열고 **Activate account(**계정 활성화**)**를 클릭합니다.

단계 **2** **Duo**를 통한 다단계 인증 설정

다단계 인증을 설정할 때는 모바일 디바이스를 사용하는 것이 좋습니다.

a. **Set up multi-factor authentication(**다단계 인증 설정**)** 화면에서 **Configure factor(**요인 구성**)**를 클릭합니다.

b. **Start setup(**설정 시작**)**을 클릭하고 프롬프트에 따라 모바일 디바이스를 선택하고 해당 모바일 디바이스와 어카운트의 페어링을 확인합니다.

   자세한 내용은 Duo Guide to Two Factor Authentication: Enrollment Guide를 참조하십시오. 디바이스에 이미 Duo 앱이 있는 경우 이 어카운트에 대한 활성화 코드를 받게 됩니다. Duo는 하나의 디바이스에서 여러 계정을 지원합니다.

c. 마법사가 끝나면 **Continue to Login(**계속 로그인**)**를 클릭합니다.

d. 이중 인증을 사용하여 Cisco Security Cloud Sign On에 로그인합니다.

단계 **3** **(**선택 사항**) Google OTP**를 추가 인증자로 설정

a. Google Authenticator와 페어링할 모바일 디바이스를 선택하고 **Next(**다음**)**를 클릭합니다.

b. 설정 마법사의 프롬프트에 따라 Google 인증기를 설정합니다.

단계 **4** **Cisco Security Cloud Sign On**에 대한 계정 복구 옵션 구성

a. SMS를 사용하여 계정을 재설정하려면 복원 전화번호를 선택합니다.

b. 보안 이미지를 선택합니다.

c. **Create My Account(**내 계정 생성**)**를 클릭합니다.

CDO 사용자 이름으로 사용자 레코드 생성

슈퍼 관리자 권한이 있는 CDO 사용자만 CDO 사용자 레코드를 생성할 수 있습니다. 슈퍼 관리자는 위의 **Create Your CDO Username(**사용자 이름 생성**)** 작업에서 지정한 것과 동일한 이메일 주소로 사용자 레코드를 만들어야 합니다.

적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

Procedure

단계 **1** CDO에 로그인합니다.

단계 **2** 왼쪽 창에서, **Settings(**설정**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **3** 테넌트에 새 사용자를 추가하려면  를 클릭합니다.

단계 **4** 사용자의 이메일 주소를 입력합니다.

Note
사용자의 이메일 주소는 Cisco Secure Log-On 계정의 이메일 주소와 일치해야 합니다.

단계 5 **Role(**역할**)** 드롭다운 목록에서 사용자의 CDO의 사용자 역할을 선택합니다.

단계 6 **OK(**확인**)**를 클릭합니다.

새 사용자가 Cisco Secure Sign-On 대시보드에서 CDO 열기

Procedure

단계 1 테넌트 지역의 Cisco Secure Sign-on 대시보드에서 적절한 **CDO** 타일을 클릭합니다.

단계 2 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 Duo Security 또는 Google Authenticator를 선택합니다.

- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 이미 여러 포털에 사용자 레코드가 있는 경우 연결할 포털을 선택할 수 있습니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 CDO 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 CDO에 대해 자세히 알아보거나 평가판 테넌트를 요청할 수 있습니다.

포털 보기는 여러 테넌트에서 통합된 정보를 검색하고 표시합니다. 자세한 내용은 멀티 테넌트 포털 관리를 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.

CDO의 사용자 역할

CDO에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. CDO 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 사용자는 한 테넌트에 대해서는 읽기 전용 역할을, 다른 테넌트에서는 슈퍼 관리자 역할을 가질 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다.

읽기 전용 역할

읽기 전용 역할이 할당된 사용자는 모든 페이지에서 이 파란색 배너를 볼 수 있습니다.

Read Only User. You cannot make configuration changes.

읽기 전용 역할의 사용자는 다음을 수행할 수 있습니다.

- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 읽기 전용 사용자가 자신의 토큰을 취소하면 다시 생성할 수 없습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

읽기 전용 사용자는 다음을 수행할 수 없습니다.

- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

편집 전용 역할

편집 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- 개체, 정책, 규칙 세트, 인터페이스, VPN 등을 포함하되 이에 국한되지 않는 디바이스 구성을 편집하고 저장합니다.
- **Read Configuration(**구성 읽기**)** 작업을 통해 이루어진 구성 변경을 허용합니다.
- 변경 요청 관리 작업을 활용합니다.

편집 전용 사용자는 다음을 수행할 수 없습니다**.**

- 디바이스 또는 여러 디바이스에 변경 사항을 배포합니다.
- 단계적 변경 또는 OOB를 통해 감지된 변경을 폐기합니다.
- AnyConnect 패키지를 업로드하거나 이러한 설정을 구성합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- Snort 2와 Snort 3 버전 사이를 수동으로 전환합니다.
- 템플릿을 생성합니다.
- 기존 OOB 변경 설정을 변경합니다.
- 시스템 관리 설정을 편집합니다.
- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.
- VPN 세션 또는 사용자 세션을 삭제합니다.
- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

배포 전용 역할

배포 전용 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- 디바이스 또는 여러 디바이스에 단계적 변경 사항을 배포합니다.
- ASA 디바이스에 대한 구성 변경 사항을 되돌리거나 복원합니다.
- 디바이스에 대한 이미지 업그레이드를 예약하거나 수동으로 시작합니다.
- 보안 데이터베이스 업그레이드를 예약하거나 수동으로 시작합니다.
- 변경 요청 관리 작업을 활용합니다.

배포 전용 사용자는 다음을 수행할 수 없습니다**.**

- Snort 2와 Snort 3 버전 사이를 수동으로 전환합니다.

- 템플릿을 생성합니다.
- 기존 OOB 변경 설정을 변경합니다.
- 시스템 관리 설정을 편집합니다.
- 디바이스를 온보딩합니다.
- 디바이스를 삭제합니다.
- VPN 세션 또는 사용자 세션을 삭제합니다.
- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.
- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

VPN 세션 관리자 역할

VPN 세션 관리자 역할은 사이트 투 사이트 VPN 연결이 아닌 원격 액세스 VPN 연결을 모니터링하는 관리자를 위해 설계되었습니다.

VPN 세션 관리자 역할이 있는 사용자는 다음을 수행할 수 있습니다.

- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 RA VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 참고로 VPN 세션 관리자 사용자가 자신의 토큰을 취소하면 토큰을 다시 만들 수 없습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보냅니다.
- 기존 RA VPN 세션을 종료합니다.

VPN 세션 관리자 사용자는 다음을 수행할 수 없습니다**.**

- 모든 페이지에서 무엇이든 생성, 업데이트, 구성 또는 삭제합니다.
- 디바이스를 온보딩합니다.
- 개체 또는 정책과 같은 항목을 만드는 데 필요한 작업을 단계별로 진행하지만 저장할 수는 없습니다.

- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.
- 액세스 규칙을 정책에 연결하거나 분리합니다.

관리자 역할

관리자는 CDO의 모든 측면에 대한 완전한 액세스 권한을 갖습니다. 관리 사용자는 다음을 수행할 수 있습니다.

- CDO에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.
- 디바이스를 온보딩합니다.
- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 토큰이 취소되면 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

관리 사용자는 다음을 수행할 수 없습니다.

- CDO 사용자 레코드를 생성합니다.
- 사용자 역할을 변경합니다.

슈퍼 관리자

슈퍼 관리자는 CDO의 모든 측면에 대한 완전한 액세스 권한을 갖습니다. 슈퍼 관리자는 다음을 수행할 수 있습니다.

- 사용자 역할을 변경합니다.
- 사용자 레코드를 생성합니다.

Note 최고 관리자는 CDO 사용자 레코드를 생성할 수 있지만 사용자가 테넌트에 로그인하는 데 필요한 모든 사용자 레코드는 아닙니다. 사용자는 테넌트에서 사용하는 ID 제공자의 계정도 필요합니다. 엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Cloud Sign-on입니다. 사용자는 Cisco Secure Cloud Sign-On 계정에 자가 등록할 수 있습니다. 자세한 내용은 새 CDO 테넌트에 대한 초기 로그인, on page 4를 참조하십시오.

- CDO에서 개체 또는 정책을 생성, 읽기, 업데이트 및 삭제하고 설정을 구성합니다.

- 디바이스를 온보딩합니다.
- CDO의 모든 페이지 또는 설정을 봅니다.
- 모든 페이지의 콘텐츠를 검색하고 필터링합니다.
- 디바이스 구성을 비교하고 변경 로그를 보고 VPN 매핑을 확인합니다.
- 모든 페이지의 모든 설정 또는 개체에 관한 모든 경고를 봅니다.
- 자체 API 토큰을 생성, 새로 고침 및 취소합니다. 토큰이 취소되면 다음을 수행할 수 있습니다.
- 인터페이스를 통해 지원팀에 문의하고 변경 로그를 내보낼 수 있습니다.

사용자 역할의 기록 변경

사용자 레코드는 사용자의 현재 역할이 기록된 것입니다. 테넌트와 연결된 사용자를 보면 레코드별로 각 사용자의 역할을 확인할 수 있습니다. 사용자 역할을 변경하면 사용자 레코드가 변경됩니다. 사용자의 역할은 사용자 관리 테이블에서 해당 역할로 식별됩니다. 자세한 내용은 CDO에서 사용자 관리를 참조하십시오.

사용자 레코드를 변경하려면 슈퍼 관리자여야 합니다. 테넌트에 슈퍼 관리자가 없는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법.에 문의하십시오.

CDO에 사용자 계정 추가

CDO 사용자는 인증을 받고 CDO 테넌트에 액세스할 수 있도록 CDO 레코드 및 해당 IdP 계정이 필요합니다. 이 절차는 Cisco Secure Cloud Sign-On의 사용자 계정이 아니라 사용자의 CDO 사용자 레코드를 생성합니다. 사용자가 Cisco Security Cloud Sign On에 계정이 없는 경우, https://sign-on.security.cisco.com으로 이동하고 로그인 화면 하단에서 **Sign up(**등록**)**을 클릭하여 자가 등록할 수 있습니다. .

Note 이 작업을 수행하려면 CDO에서 슈퍼 관리자 역할이 있어야 합니다.

사용자 레코드 생성

적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

Procedure

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 내비게이션 바에서 **Settings(**설정**)** > **User Management(**사용자 관리**)**를 클릭합니다.

단계 3 테넌트에 새 사용자를 추가하려면 파란색 플러스 버튼()을 클릭합니다.

단계 4 사용자의 이메일 주소를 입력합니다.

Note
사용자의 이메일 주소는 Cisco Secure Log-On 계정의 이메일 주소와 일치해야 합니다.

단계 5 드롭다운 메뉴에서 사용자 CDO의 사용자 역할을 선택합니다.

단계 6 v를 클릭합니다.

Note
최고 관리자는 CDO 사용자 레코드를 생성할 수 있지만 사용자가 테넌트에 로그인하는 데 필요한 모든 사용자 레코드는 아닙니다. 사용자는 테넌트에서 사용하는 ID 제공자의 계정도 필요합니다. 엔터프라이즈에 자체 SSO(Single Sign-On) ID 제공자가 없는 경우 ID 제공자는 Cisco Secure Sign-on입니다. 사용자는 Cisco Secure Sign-On 계정에 자가 등록할 수 있습니다. 자세한 내용은 새 CDO 테넌트에 대한 초기 로그인, on page 4를 참조하십시오.

API 전용 사용자 생성

프로시저

단계 1 CDO에 로그인합니다.

단계 2 CDO 내비게이션 바에서 **Settings(설정)** > **User Management(사용자 관리)**를 클릭합니다.

단계 3 테넌트에 새 사용자를 추가하려면 파란색 플러스 버튼()을 클릭합니다.

단계 4 **API Only User(API** 전용 사용자**)** 확인란을 선택합니다.

단계 5 **Username(**사용자 이름**)** 필드에 사용자 이름을 입력하고 **OK(**확인**)**를 클릭합니다.

중요
사용자 이름은 이메일 주소이거나 '@yourtenant' 접미사가 사용자 이름에 자동으로 추가되므로 '@' 문자를 포함할 수 없습니다.

단계 6 드롭다운 메뉴에서 사용자 CDO의 사용자 역할을 선택합니다.

단계 7 **OK(**확인**)**를 클릭합니다.

단계 8 **User Management(**사용자 관리**)** 탭을 클릭합니다.

단계 9 새 API 전용 사용자의 토큰 열에서 **Generate API Token(API** 토큰 생성**)**을 클릭하여 API 토큰을 얻습니다.

사용자 역할에 대한 사용자 레코드 편집

이 작업을 수행하려면 슈퍼 관리자 역할이 있어야 합니다. 슈퍼 관리자가 로그인한 CDO 사용자의 역할을 변경할 경우 역할이 변경되면 해당 사용자는 자동으로 세션에서 로그아웃됩니다. 사용자가 다시 로그인하면 새 역할을 맡게 됩니다.

Note 이 작업을 수행하려면 CDO에서 슈퍼 관리자 역할이 있어야 합니다.

Caution 사용자 레코드의 역할을 변경하면 사용자 레코드와 연결된 API 토큰이 있는 경우 해당 토큰이 삭제됩니다. 사용자 역할이 변경되면 사용자는 새 API 토큰을 생성해야 합니다.

사용자 역할 편집

Note CDO 사용자가 로그인되어 있고 슈퍼 관리자가 역할을 변경하는 경우, 변경 사항을 적용하려면 사용자가 로그아웃했다가 다시 로그인해야 합니다.

사용자 레코드에 정의된 역할을 편집하려면 다음 절차를 따르십시오.

Procedure

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 내비게이션 바에서 **Settings(**설정**)** > **User Management(**사용자 관리**)**를 클릭합니다.

단계 **3** 사용자 행에서 편집 아이콘을 클릭합니다.

단계 **4** 역할 드롭다운 메뉴에서 사용자의 새 CDO의 사용자 역할을 선택합니다.

단계 **5** 사용자 레코드에 사용자와 연결된 API 토큰이 있는 것으로 표시되면 사용자의 역할을 변경하고 결과적으로 API 토큰을 삭제할 것임을 확인해야 합니다.

단계 **6** **v**를 클릭합니다.

단계 **7** CDO가 API 토큰을 삭제한 경우 사용자에게 연락하여 새 API 토큰을 생성합니다.

사용자 역할에 대한 사용자 레코드 삭제

CDO에서 사용자 레코드를 삭제하면 Cisco Secure Cloud Sign-On 계정과 사용자 레코드의 매핑이 끊어져 연결된 사용자가 CDO에 로그인할 수 없습니다. 사용자 레코드를 삭제하면 해당 사용자 레코드

와 연결된 API 토큰도 삭제됩니다. CDO에서 사용자 레코드를 삭제해도 Cisco Secure Cloud Sign-On에서 사용자의 IdP 계정은 삭제되지 않습니다.

Note 이 작업을 수행하려면 CDO에서 슈퍼 관리자 역할이 있어야 합니다.

사용자 레코드 삭제

사용자 레코드에 정의된 역할을 삭제하려면 다음 절차를 참조하십시오.

Procedure

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 내비게이션 바에서 **Settings(**설정**)** > **User Management(**사용자 관리**)**를 클릭합니다.

단계 **3** 삭제할 사용자 행에서 휴지통 아이콘를 클릭합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

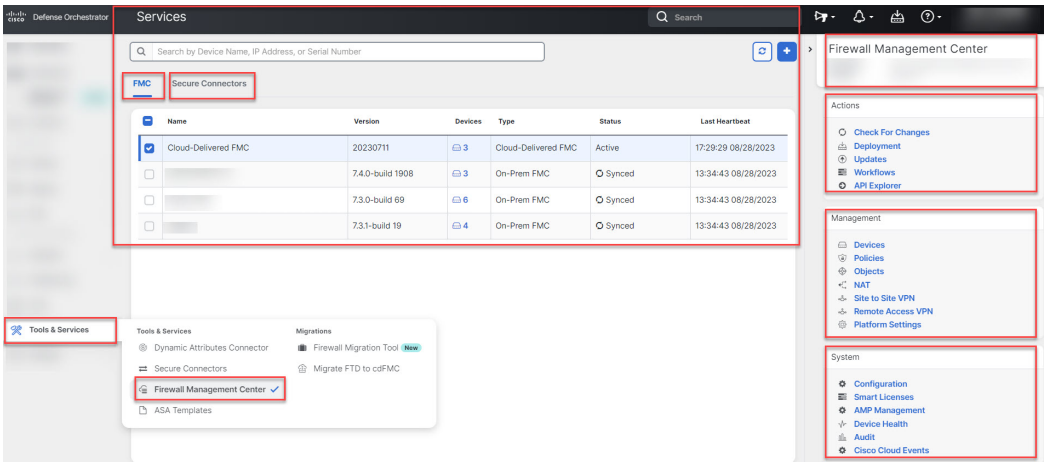
단계 **5** 확인을 클릭하여 테넌트에서 계정을 제거할 것임을 확인합니다.

CDO 서비스 페이지

Services(서비스**)** 페이지에 CDO가 제공하는 서비스 목록이 표시됩니다. **FMC** 탭을 선택하면 CDO 계정에 연결된 클라우드 제공 Firewall Management Center 및 CDO에 온보딩된 모든 온프레미스 방화벽 Management Center가 나열됩니다. 이러한 온프레미스 Management Center에서 관리하는 디바이스는 **Inventory(**재고 목록**)** 페이지에 나열됩니다. **Services(**서비스**)** 페이지의 **Secure Connector(**보안 커넥터**)** 탭 아래에도 보안 커넥터가 나열됩니다.

파란색 더하기 아이콘( )을 클릭하여 **FMC** 탭을 클릭하고 온프레미스 방화벽 Management Center를 온보딩한 후 오른쪽 창의 옵션을 사용하여 디바이스 작업을 수행할 수 있습니다. 디바이스의 버전, Management Center에서 관리하는 디바이스의 수, 디바이스 유형, 디바이스 동기화 상태 등의 디바이스 정보도 확인할 수 있습니다. 매니지드 디바이스 아이콘을 클릭하면 **Inventory(**재고 목록**)** 페이지로 이동하며, 이 페이지에는 선택된 온프레미스 방화벽 Management Center에서 관리하는 디바이스가 자동으로 필터링되어 표시됩니다. **Services(**서비스**)** 페이지에서는 하나 이상의 온프레미스 방화벽 Management Center를 동시에 선택하여 Management Center 그룹에 대한 작업을 한 번에 수행할 수 있습니다. 클라우드 제공 Firewall Management Center가 선택된 상태에서는 온프레미스 방화벽 Management Center를 선택할 수 없습니다. 새 보안 커넥터를 추가하거나 기존 보안 커넥터에 대해 작업을 수행하려면 **Secure Connector(**보안 커넥터**)** 탭을 선택하고 를 클릭합니다.

도구 및 서비스 > **Firewall Management Center**로 이동합니다.



클라우드 제공 Firewall Management Center의 경우 Services(서비스) 페이지에 다음 정보가 표시됩니다.

- 클라우드 제공 Firewall Management Center가 테넌트에 구축되지 않은 경우, **Enable Cloud-Delivered FMC(**클라우드 제공 **FMC** 활성화**)**를 클릭합니다. 자세한 내용은 CDO테넌트에서 클라우드 제공 Firewall Management Center 활성화를 참조하십시오.
- 클라우드 제공 Firewall Management Center에 구축된 Secure Firewall Threat Defense 디바이스 수.
- CDO 및 클라우드 제공 Firewall Management Center 페이지 간의 연결 상태.
- 클라우드 제공 Firewall Management Center의 마지막 하트비트. 이는 클라우드 제공 Firewall Management Center 자체의 상태와 여기에서 관리하는 디바이스 수가 이 페이지의 테이블과 마지막으로 동기화된 것을 나타냅니다.
- 선택한 클라우드 제공 Firewall Management Center의 호스트 이름.

Cloud-Delivered FMC(클라우드 제공 **FMC)**를 선택하고 **Actions(**작업**)**, **Management(**관리**)** 또는 **Settings**(설정) 창의 링크를 사용하여 클릭한 링크와 연결된 구성 작업을 수행할 수 있는 클라우드 제공 Firewall Management Center사용자 인터페이스를 엽니다.

Actions(작업**)**:

- **Check For Changes(**변경 사항 확인**)**: 테이블의 디바이스 수 및 상태 정보가 이 페이지와 클라우드 제공 Firewall Management Center가 마지막으로 동기화되었을 때 사용 가능한 정보로 업데이트됩니다. 동기화는 10분마다 이루어집니다.
- **Deployment(**구축**)**: 클라우드 제공 Firewall Management Center의 디바이스 구성 구축 페이지로 이동합니다. 구성 변경 사항 구축을 참조하십시오.
- 워크플로우: 디바이스와 통신할 때 CDO가 실행하는 모든 프로세스를 모니터링할 수 있는 워크플로우 페이지로 이동합니다. 워크플로우 페이지를 참조하십시오.
- **API Explorer**: 클라우드 제공 Firewall Management Center REST API를 나열하는 페이지로 이동합니다. Secure Firewall Management Center REST API 가이드를 참조하십시오.

Management(관리**)**:

- **Devices(**디바이스**)**: 클라우드 제공 Firewall Management Center 포털의 Threat Defense 디바이스 목록 페이지로 이동합니다. 디바이스 구성을 참조하십시오.
- **Policies(**정책**)**: 시스템에서 제공한 액세스 제어 정책을 편집하고 사용자 정의 액세스 제어 정책을 생성할 수 있는 클라우드 제공 Firewall Management Center 포털의 정책 페이지로 이동합니다. 액세스 제어 정책 관리를 참조하십시오.
- **Objects(**개체**)**: 재사용 가능한 개체를 관리할 수 있는 클라우드 제공 Firewall Management Center 포털의 정책 페이지로 이동합니다. 개체 관리를 참조하십시오.
- **NAT**: Threat Defense 디바이스에 대한 네트워크 주소 변환 정책을 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 정책 페이지로 이동합니다. NAT 정책 관리를 참조하십시오.
- **Site to Site VPN(**사이트 간 **VPN)**: 두 사이트 간에 사이트 간 VPN 정책을 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 사이트 간 VPN 대시보드 페이지로 이동합니다. 사이트 간 VPN을 참조하십시오.
- **Remote Access VPN(**원격 액세스 **VPN)**: 원격 액세스 VPN을 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 원격 액세스 VPN 대시보드 페이지로 이동합니다. 원격 액세스 VPN을 참조하십시오.
- **Platform Settings(**플랫폼 설정**)**: 값을 여러 디바이스 간에 공유하려고 할 수 있는 비 관련 기능의 범위를 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 플랫폼 설정 페이지로 이동합니다. 플랫폼 설정을 참조하십시오.

System(시스템**)**:

- **Configuration(**구성**)**: 시스템 구성 설정을 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 시스템 구성 설정 페이지로 이동합니다. 시스템 구성을 참조하십시오.
- **Smart Licenses(**스마트 라이선스**)**: 디바이스에 라이선스를 할당할 수 있는 클라우드 제공 Firewall Management Center 포털의 스마트 라이선스 페이지로 이동합니다. 디바이스에 라이선스 할당을 참조하십시오.
- **AMP Management(AMP** 관리**)**: 시스템이 네트워크에서 악성코드를 탐지하고 차단하는 데 사용하는 인텔리전스를 제공하는 클라우드 제공 Firewall Management Center 포털의 AMP 관리 페이지로 이동합니다. 악성코드 차단을 위한 클라우드 연결을 참조하십시오.
- **Device Health(**디바이스 상태**)**: 다양한 상태 표시기를 추적하고 시스템의 하드웨어 및 소프트웨어가 올바르게 작동하는지 추적하는 클라우드 제공 Firewall Management Center 포털의 상태 모니터링 페이지로 이동합니다. 상태 모니터링 정보를 참조하십시오.
- **Audit(**감사**)**: 사용자와 웹 인터페이스의 각 상호 작용에 대해 생성된 감사 레코드를 표시할 수 있는 클라우드 제공 Firewall Management Center 포털의 감사 로그 페이지로 이동합니다.
- **Cisco Cloud Events(Cisco Cloud** 이벤트**)**: SAL(SaaS)에 이벤트를 직접 전송하도록 클라우드 제공 Firewall Management Center을(를) 구성할 수 있는 CDO 포털의 Cisco Cloud 이벤트 구성 페이지로 이동합니다. SAL(SaaS)로 이벤트 전송을 참조하십시오.

클라우드 제공 Firewall Management Center 페이지가 열리면 파란색 물음표 버튼을 클릭하고 **Page-level Help(**페이지 수준 도움말**)**를 선택하여 현재 페이지와 수행 가능한 추가 작업에 대해 자세히 알아볼 수 있습니다.

다른 탭에서 **CDO** 및 클라우드 제공 **Firewall Management Center** 애플리케이션 열기 지원

클라우드 제공 Firewall Management Center에서 Threat Defense 디바이스 또는 개체를 구성할 때 추가 브라우저 탭에서 해당 구성 페이지를 열면 로그아웃하지 않고도 CDO 및 클라우드 제공 Firewall Management Center 포털에서 동시에 작업할 수 있습니다. 예를 들어, 클라우드 제공 Firewall Management Center에서 개체를 생성하고 동시에 보안 정책에서 생성된 CDO의 이벤트 로그를 모니터링할 수 있습니다.

이 기능은 클라우드 제공 Firewall Management Center 포털로 이동하는 모든 CDO 링크에서 사용할 수 있습니다. 새 탭에서 클라우드 제공 Firewall Management Center 포털을 여는 방법:

CDO 포털에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 해당 링크를 클릭합니다.

참고 한 번 클릭하면 동일한 탭에서 클라우드 제공 Firewall Management Center 페이지가 열립니다.

다음은 새 탭에서 클라우드 제공 Firewall Management Center 포털 페이지를 여는 몇 가지 예입니다.

- **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 선택하고 **Cloud-Delivered FMC(**클라우드 제공 **FMC)**를 선택합니다.

  오른쪽 창에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 액세스하려는 페이지를 클릭합니다.

- **Objects(**개체**)** > **Other FTD Objects(**기타 **FTD** 개체**)**를 선택합니다.

- CDO 페이지 오른쪽 상단 모서리에 있는 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.

  검색 결과에서 **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태로 화살표 아이콘을 클릭합니다.

- **Dashboard(**대시보드**)** > **Quick Actions(**빠른 작업**)**를 선택합니다.

  Ctrl(Windows) 또는 **Command**(Mac) 버튼을 누른 상태에서 **Manage FTD Policies(FTD** 정책 관리**)** 또는 **Manage FTD Objects(FTD** 개체 관리**)**를 클릭합니다.

참고 새 CDO 테넌트로 전환하면 새 탭에서 이미 열린 해당 클라우드 제공 Firewall Management Center 포털이 로그아웃됩니다.

관련 주제

- Cisco Defense Orchestrator를 사용하여 온프레미스 Firewall Management Center 관리
- 온프레미스 Firewall Management Center 온보딩

- CDO 테넌트에 대한 클라우드 제공 Firewall Management Center 요청
- 보안 디바이스 커넥터
- 보안 이벤트 커넥터

CDO 디바이스 및 서비스 관리

CDO는 **Inventory(**재고 목록**)** 페이지에서 온보딩된 디바이스를 보고, 관리하고, 필터링하고, 평가할 수 있는 기능을 제공합니다. **Inventory(**재고 목록**)** 페이지에서 다음을 수행할 수 있습니다.

- CDO 관리를 위한 디바이스 및 서비스를 온보딩합니다.
- 관리 디바이스 및 서비스의 구성 상태 및 연결 상태를 봅니다.
- 별도의 탭으로 분류된 온보딩된 디바이스 및 템플릿을 봅니다. CDO 재고 목록 정보, 99 페이지을 참조하십시오.
- 개별 디바이스 및 서비스를 평가하고 조치를 취합니다.
- 디바이스 및 서비스별 정보를 보고 문제를 해결합니다.
- 다음에서 관리하는 위협 방어 디바이스의 디바이스 상태를 확인합니다.
  - 클라우드 제공 Firewall Management Center
  - 온프레미스 방화벽 Management Center

  클라우드 제공 Firewall Management Center에서 관리하는 위협 방어 디바이스의 경우, 클러스터에 있는 디바이스의 노드 상태도 볼 수 있습니다.
- 이름, 유형, IP 주소, 모델 이름, 일련 번호 또는 레이블로 디바이스 또는 템플릿을 검색합니다. 검색은 대/소문자를 구분하지 않습니다. 여러 검색어를 제공하면 검색어 중 하나 이상과 일치하는 디바이스 및 서비스가 나타납니다. 페이지 레벨 검색, 102 페이지을 참조하십시오.
- 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 감지, 보안 디바이스 커넥터 및 레이블을 기준으로 디바이스 또는 템플릿 필터를 필터링합니다. 필터를 참조하십시오.

CDO에서 디바이스의 IP 주소 변경

IP 주소를 사용하여 CDO에 디바이스를 온보딩하면 CDO는 해당 IP 주소를 데이터베이스에 저장하고 해당 IP 주소를 사용하여 디바이스와 통신합니다. 디바이스의 IP 주소가 변경되면 새 주소와 일치하도록 CDO에 저장된 IP 주소를 업데이트할 수 있습니다. CDO에서 디바이스의 IP 주소를 변경해도 디바이스의 구성은 변경되지 않습니다.

CDO가 디바이스와 통신하는 데 사용하는 IP 주소를 변경하려면 다음 절차를 수행합니다.

Procedure

단계 1 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

필터 및 페이지 레벨 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 IP 주소를 변경할 디바이스를 선택합니다.

단계 5 **Device Details(**디바이스 세부 정보**)** 창 위에서 디바이스의 IP 주소 옆에 있는 편집 버튼을 클릭합니다.

단계 6 필드에 새 IP 주소를 입력하고 파란색 확인 버튼을 클릭합니다.

디바이스 자체는 변경되지 않으므로 디바이스의 Configuration Status(구성 상태)는 계속해서 Synced(동기화됨)로 표시됩니다.

관련 정보:

- 테넌트 간 디바이스 이동, on page 98
- CDO에 디바이스 대량 재연결, on page 97

CDO에서 디바이스 이름 변경

모든 디바이스, 모델, 템플릿 및 서비스는 온보딩되거나 CDO에서 생성될 때 이름이 지정됩니다. 디바이스 자체의 구성을 변경하지 않고 해당 이름을 변경할 수 있습니다.

Procedure

단계 1 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 3 이름을 변경하려는 디바이스를 선택합니다.

단계 4 **Device Details(**디바이스 세부 정보**)** 창 위에서 디바이스의 이름 옆에 있는 편집 버튼을 클릭합니다.

단계 5 필드에 새 이름을 입력하고 파란색 확인 버튼을 클릭합니다.

디바이스 자체는 변경되지 않으므로 디바이스의 Configuration Status(구성 상태)는 계속해서 Synced(동기화됨)로 표시됩니다.

디바이스 및 서비스 목록 내보내기

이 문서에서는 디바이스 및 서비스 목록을 쉼표로 구분된 값(.csv) 파일로 내보내는 방법을 설명합니다. 이 형식이 되면 Microsoft Excel과 같은 스프레드시트 애플리케이션에서 파일을 열어 목록의 항목을 정렬하고 필터링할 수 있습니다.

내보내기 버튼은 디바이스 및 템플릿 탭에서 사용할 수 있습니다. 또한 선택한 디바이스 유형 탭의 디바이스에서 세부 정보를 내보낼 수 있습니다.

디바이스 및 서비스 목록을 내보내기 전에 필터 창을 살펴보고 재고 목록 테이블에 내보내려는 정보가 표시되는지 확인합니다. 모든 필터를 지워 모든 매니지드 디바이스 및 서비스를 확인하거나 정보를 필터링하여 모든 디바이스 및 서비스의 하위 집합을 표시합니다. 내보내기 기능은 Inventory(재고 목록) 테이블에서 확인할 수 있는 내용을 내보냅니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 유형 탭을 클릭하여 해당 탭 아래의 디바이스에서 세부 정보를 내보내거나 **All(**모두**)**을 클릭하여 모든 디바이스에서 세부 정보를 내보냅니다.

필터 및 페이지 레벨 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** **Export list to CSV(CSV**로 목록 내보내기**)**를 클릭합니다.

단계 **5** 메시지가 표시되면 .csv 파일을 저장합니다.

단계 **6** 스프레드시트 애플리케이션에서 .csv 파일을 열어 결과를 정렬하고 필터링합니다.

디바이스 구성 내보내기

한 번에 하나의 디바이스 구성만 내보낼 수 있습니다. 다음 절차를 사용하여 디바이스의 구성을 JSON 파일로 내보냅니다.

프로시저

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 페이지 레벨 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

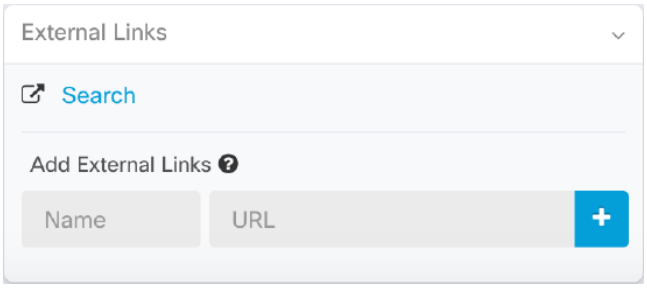
단계 **4** 원하는 디바이스를 선택하여 강조 표시하십시오.

단계 **5** **Actions(**작업**)** 창에서 **Export Configuration(**구성 내보내기**)**를 선택합니다.

단계 **6** **Confirm(**확인**)**을 선택하여 구성을 JSON 파일로 저장합니다.

디바이스의 외부 링크

외부 리소스에 대한 하이퍼링크를 생성하여 CDO로 관리하는 디바이스와 연결할 수 있습니다. 이 기능을 사용하여 디바이스 중 하나의 로컬 관리자에 대한 편리한 링크를 생성할 수 있습니다(ASA의 경우 , FTD의 경우). 또한 이를 사용하여 검색 엔진, 설명서 리소스, 회사 Wiki 또는 선택한 다른 URL에 연결할 수 있습니다. 외부 링크를 원하는 만큼 디바이스에 연결할 수 있습니다. 동일한 링크를 여러 디바이스와 동시에 연결할 수도 있습니다.



생성한 링크는 어디에나 연결할 수 있지만 회사의 보안 요구 사항은 변경되지 않습니다. 예를 들어 특정 URL에 도달하기 위해 온프레미스 또는 VPN 연결을 통해 일반적으로 기업 네트워크에 연결해야 하는 경우 이러한 요구 사항은 그대로 유지됩니다. 회사에서 특정 URL을 차단하는 경우 해당 URL은 계속 차단됩니다. 제한되지 않은 URL은 계속해서 제한되지 않습니다.

위치 변수

URL에 통합할 수 있는 {location} 변수를 생성했습니다. 이 변수는 디바이스의 IP 주소로 채워집니다. 예를 들면 다음과 같습니다.

```
https://{location}
```

또는

관련 정보**:**

- 디바이스 메모 작성, on page 99
- 디바이스 및 서비스 목록 내보내기, on page 93

장치에서 외부 링크 생성

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 장치 또는 모델을 선택합니다.

필터 및 페이지 레벨 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.

단계 **6** 링크 이름을 입력합니다.

단계 **7** URL 필드에 링크의 URL을 입력합니다. 예를 들어 Cisco의 경우 http://www.cisco.com을 입력하는 것과 같이 전체 URL을 지정해야 합니다.

단계 **8** +를 클릭하여 링크를 디바이스와 연결합니다.

에 대한 외부 링크 생성

다음은 CDO에서 직접 과 을 여는 편리한 방법입니다.

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 페이지 레벨 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 디바이스 또는 모델을 선택합니다.

단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.

단계 **6** 과 같은 링크 이름을 입력합니다.

단계 **7** URL 필드에 https://{location}을 입력합니다. {location} 변수는 디바이스의 IP 주소로 채워집니다.

단계 **8** + 상자를 클릭합니다.

여러 디바이스에 대한 외부 링크 생성

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 페이지 레벨 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 여러 디바이스 또는 모델을 선택합니다.

단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.

단계 **6** 링크 이름을 입력합니다.

단계 **7** 다음 방법 중 하나를 사용하여 도달하려는 URL을 입력하십시오.

- 입력

  ```
  https://{location}
  ```

  URL 필드에. {location} 변수는 디바이스의 IP 주소로 채워집니다. 이렇게 하면 디바이스의 ASDM에 대한 자동 링크가 생성됩니다.

- URL 필드에 링크의 URL을 입력합니다. 예를 들어 Cisco의 경우 http://www.cisco.com을 입력하는 것과 같이 전체 URL을 지정해야 합니다.

단계 **8** +를 클릭하여 링크를 디바이스와 연결합니다.

외부 링크 편집 또는 삭제

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 페이지 레벨 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 디바이스 또는 모델을 선택합니다.

단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 **6** 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.
단계 **7** 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.

여러 디바이스에 대한 외부 링크 편집 또는 삭제

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.

필터 및 페이지 레벨 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 **4** 여러 디바이스 또는 모델을 선택합니다.
단계 **5** 세부 정보 창의 오른쪽에서, **External Links(**외부 링크**)** 섹션으로 이동합니다.
단계 **6** 편집 및 삭제 아이콘을 표시하려면 링크 이름에 마우스를 올려놓습니다.
단계 **7** 해당 아이콘을 클릭하여 외부 링크를 편집하거나 삭제하고 작업을 확인합니다.

CDO에 디바이스 대량 재연결

관리자는 CDO를 통해 둘 이상의 매니지드 디바이스를 CDO에 동시에 다시 연결할 수 있습니다. CDO가 관리하는 디바이스가 "unreachable(연결할 수 없음)"로 표시되면 CDO는 더 이상 대역 외 구성 변경 사항을 탐지하거나 디바이스를 관리할 수 없습니다. 연결이 끊어지는 데에는 여러 가지 이유가 있을 수 있습니다. 디바이스에 대한 CDO 관리를 복원하는 첫 번째 단계는 디바이스를 다시 연결하는 것입니다.

Note 새 인증서가 있는 디바이스를 다시 연결하는 경우 CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다. 그러나 하나의 디바이스에만 다시 연결하는 경우 CDO는 계속해서 다시 연결하려면 인증서를 수동으로 검토하고 수락하라는 메시지를 표시합니다.

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.
단계 **2** 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

필터를 사용하여 연결 상태가 "unreachable(연결할 수 없음)"인 디바이스를 찾습니다.

단계 **4** 필터링된 결과에서 다시 연결을 시도할 디바이스를 선택합니다.

단계 **5** **Reconnect(**다시 연결**)** 을 클릭합니다. CDO는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.

단계 **6** 알림 탭에서 대량 디바이스 다시 연결 작업의 진행 상황을 확인합니다. 대량 디바이스 다시 연결 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 CDO에서 작업 모니터링, on page 159로 이동합니다.

Tip
디바이스의 인증서 또는 자격 증명이 변경되어 재연결 실패가 발생한 경우, 해당 디바이스에 개별적으로 다시 연결하여 새 자격 증명을 추가하고 새 인증서를 수락해야 합니다.

테넌트 간 디바이스 이동

디바이스를 CDO 테넌트에 온보딩하면 한 CDO 테넌트 간에 디바이스를 마이그레이션할 수 없습니다. 디바이스를 새 테넌트로 이동하려면 이전 테넌트에서 디바이스를 제거하고 새 테넌트에 다시 온보딩해야 합니다.

디바이스 인증서 만료 감지

관리 인증서는 CDO에서 FDM 관리 및 ASA 디바이스에 액세스하는 데 사용되지만, Cisco Secure Client(이전 AnyConnect)는 CDO의 ASA, FDM 관리 및 FTD 디바이스에서 가상 프라이빗 네트워크 기능을 사용하는데 필요합니다.

CDO는 이러한 인증서의 만료 상태를 적극적으로 모니터링하고 이러한 인증서가 만료 날짜에 가까워지거나 만료되면 사용자에게 알립니다. 이렇게 하면 인증서 만료로 인해 디바이스 작동이 중단되는 것을 방지할 수 있습니다. 이 문제를 해결하려면 해당 인증서를 갱신해야 합니다.

관리 인증서 만료 확인은 ASA 및 FDM 매니지드 디바이스에 적용되며, Secure Client 인증서 만료 확인은 ASA, FDM 관리 및 FTD 디바이스에 적용됩니다.

인증서 만료 알림 보기

오른쪽 상단에서 알림( ) 아이콘을 클릭하여 테넌트에 온보딩한 디바이스에 발생했거나 영향을 미친 가장 최신 알림을 확인합니다. **High Priority(**높은 우선순위**)** 섹션에는 인증서 만료 알림이 표시됩니다.

이러한 알림은 인증서 만료일 30, 14 및 7일 전에 전송되며, 그 이후에는 인증서가 만료되거나 유효한 인증서로 갱신할 때까지 매일 전송됩니다. 사용자 환경설정 페이지의 알림 설정 섹션에서 이러한 알림을 이메일로 수신하도록 구독할 수도 있습니다. 자세한 내용은 사용자 알림 환경 설정을 참조하십시오.

디바이스 메모 작성

이 절차를 사용하여 디바이스에 대한 단일 일반 텍스트 메모 파일을 생성합니다.

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 메모를 작성할 디바이스 또는 모델을 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **Notes(**메모**)**를 클릭합니다. Notes.

단계 **6** 오른쪽의 편집기 버튼을 클릭하고 기본 텍스트 편집기, Vim 또는 Emacs 텍스트 편집기를 선택합니다.

단계 **7** 메모 페이지를 편집합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.
메모가 탭에 저장됩니다.

CDO 재고 목록 정보

Inventory(재고 관리**)** 페이지에는 모든 물리적 및 가상 온보딩된 디바이스와 온보딩된 디바이스에서 생성된 템플릿이 표시됩니다. 이 페이지는 유형에 따라 디바이스 및 템플릿을 분류하고 각 디바이스 유형 전용 해당 탭에 표시합니다. 페이지 레벨 검색 기능을 사용하거나 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

이 페이지에서 다음 세부 정보를 볼 수 있습니다.

- **Device(**디바이스**)** 탭에는 CDO에 온보딩된 모든 라이브 디바이스가 표시됩니다.
- **Templates(**템플릿**(**에는 CDO로 가져온 라이브 디바이스 또는 구성 파일에서 생성된 모든 템플릿 디바이스가 표시됩니다.

CDO 레이블 및 필터링

레이블은 디바이스 또는 개체를 그룹화하는 데 사용됩니다. 온보딩 중에 또는 온보딩 후에 언제든지 하나 이상의 디바이스에 레이블을 적용할 수 있습니다. 개체를 생성한 후 개체에 레이블을 적용할 수 있습니다. 디바이스 또는 개체에 레이블을 적용한 후에는 해당 레이블을 기준으로 디바이스 테이블 또는 개체 테이블의 내용을 필터링할 수 있습니다.

참고 디바이스에 적용된 레이블은 연결된 개체로 확장되지 않으며, 공유 개체에 적용된 레이블은 연결된 개체로 확장되지 않습니다.

"group name:label" 구문을 사용하여 레이블 그룹을 생성할 수 있습니다. 예를 들어 Region:East 또는 Region:West입니다. 이 두 레이블을 생성하는 경우 그룹 레이블은 Region(지역)이 되며 해당 그룹의 East(동부) 또는 West(서부) 중에서 선택할 수 있습니다.

디바이스 및 개체에 레이블 적용

디바이스에 레이블을 적용하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** 디바이스에 레이블을 추가하려면 왼쪽 탐색 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 개체에 레이블을 추가하려면 왼쪽 탐색 창에서 **Objects(**개체**)**를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **4** 해당 디바이스 탭을 클릭합니다.

단계 **5** 생성된 테이블에서 하나 이상의 디바이스 또는 모델을 선택합니다.

단계 **6** 오른쪽의 **Add Groups and Labels(**그룹 및 레이블 추가**)** 필드에서 디바이스의 레이블을 지정합니다.

단계 **7** 파란색 + 아이콘을 클릭합니다.

필터

Security Devices(보안 디바이스**)** 및 **Objects(**개체**)** 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 Security Devices(보안 디바이스), Policies(정책) 및 Objects(개체) 탭의 왼쪽 창에서 을 클릭합니다.

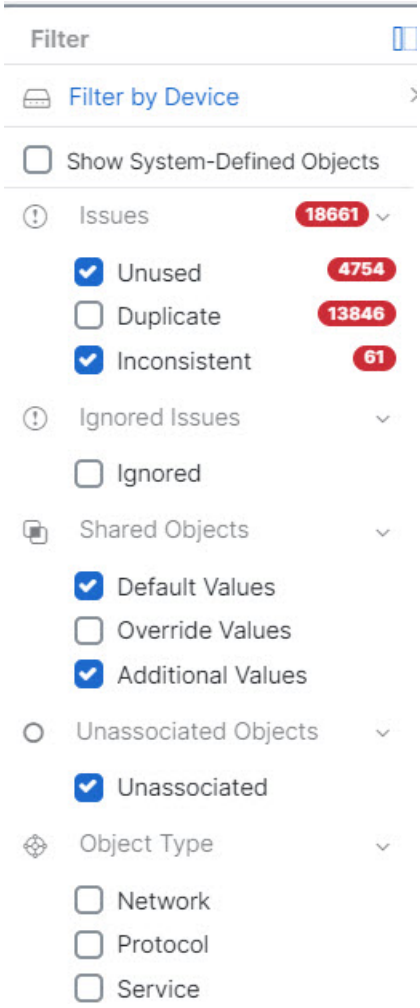
보안 디바이스 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

개체 유형 필터를 사용하면 네트워크 개체, 네트워크 그룹, URL 개체, URL 그룹, 서비스 개체, 서비스 그룹 등의 유형별로 개체를 필터링할 수 있습니다. 공유 개체 필터를 사용하면 기본값 또는 재정의 값이 있는 개체를 필터링할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유된 개체의 개체 검색에 필터를 적용합니다.



CDO 검색 기능 사용

CDO 플랫폼에는 필요한 모든 항목을 쉽게 찾을 수 있는 매우 효율적인 검색 기능이 있습니다. 각 페이지의 검색 창은 해당 페이지의 콘텐츠에 따라 맞춤화되지만, 전역 검색을 사용하면 전체 테넌트에 대한 포괄적인 검색이 가능합니다. 이렇게 하면 필요한 정보를 신속하게 찾을 수 있으므로 시간과 노력을 절약할 수 있습니다.

페이지 레벨 검색

페이지 레벨 검색을 사용하면 Inventory(재고 목록), Policies(정책), Objects(개체), VPN, Change Log(변경 로그) 및 Jobs(작업) 페이지에서 특정 항목을 검색할 수 있습니다.

- **Inventory(**재고 목록**)** 영역에서 검색 창에 입력을 시작하면 검색 기준에 맞는 디바이스가 표시됩니다. 디바이스의 일부 부분 이름, IP 주소 또는 물리적 디바이스의 일련 번호를 입력하여 디바이스를 찾을 수 있습니다.
- **Policies(**정책**)** 영역에서는 이름, 구성 요소 또는 사용된 개체를 기준으로 정책을 검색할 수 있습니다.
- **Objects(**개체**)** 영역에서는 개체 이름 또는 IP 주소 일부, 포트나 프로토콜을 입력하여 개체를 검색할 수 있습니다.
- **VPN** 영역에서는 터널 이름, 디바이스 이름 및 VPN 정책에 사용된 IP 주소를 기준으로 검색할 수 있습니다.
- **Change log(**변경 로그**)** 영역에서는 이벤트, 디바이스 이름 또는 작업을 기준으로 로그를 검색할 수 있습니다.

Procedure

단계 **1** 인터페이스 상단 근처의 검색 창으로 이동합니다.

단계 **2** 검색 표시줄에 검색 기준을 입력하면 해당 결과가 표시됩니다.

개체

개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 단일 개체를 만들고 다른 정책을 사용하고 개체를 편집할 수 있으며 해당 변경 사항은 개체를 사용하는 모든 정책에 전파됩니다. 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 편집해야 합니다.

디바이스를 온보딩하면, CDO는 해당 디바이스에서 사용하는 모든 개체를 인식하고, 저장한 다음, **Objects(**개체**)** 페이지에 나열합니다. **Objects(**개체**)** 페이지에서 기존 개체를 편집하고 보안 정책에 사용할 새 개체를 생성할 수 있습니다.

CDO은 여러 디바이스에서 사용되는 개체를 **shared object(**공유 개체**)**라고 부르고 **Objects(**개체**)** 페이지에서 이 배지 ⧉로 식별합니다.

때때로 공유 개체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다.

- **Duplicate objects(**중복 개체**)**는 이름은 다르지만 값은 같은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 일반적으로 비슷한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체는 다음 문제 아이콘로 식별됩니다.
- **Inconsistent objects(**일관성 없는 개체**)** 는 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체입니다. 때로는 사용자가 동일한 이름과 콘텐츠로 다른 구성으로 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘로 식별됩니다.
- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다. 2024년 6월 28일 이전에는 규칙 또는 정책에서 연결되지 않은 개체를 사용하는 경우 CDO는 해당 개체의 복사본을 생성하고 해당 복사본을 사용했습니다. 이 동작으로 인해 **Objects(**개체**)** 메뉴에서 동일한 개체의 인스턴스 두 개를 볼 수 있습니다. 그러나, CDO는 더 이상 이를 수행하지 않습니다. 규칙 또는 정책에서 연결되지 않은 개체를 사용할 수 있지만, CDO가 생성하는 중복 개체가 없습니다.

Objects(개체**)** 메뉴로 이동하거나 네트워크 정책의 세부 정보에서 확인하여 CDO에 의해 관리되는 개체를 볼 수 있습니다.

CDO은 한 위치에서 지원되는 디바이스 전체에 걸쳐 네트워크 및 서비스 개체를 관리할 수 있습니다. CDO에서는 다음과 같은 방법으로 개체를 관리할 수 있습니다.

- 다양한 기준에 따라 모든 개체를 검색하고 개체 필터합니다.
- 디바이스에서 중복되거나, 사용되지 않거나, 일관성이 없는 개체를 찾고 이러한 개체 문제를 통합, 삭제 또는 해결하십시오.
- 연결되지 않은 개체를 찾아 사용하지 않는 경우 삭제합니다.
- 여러 디바이스에서 공통적인 공유 개체를 검색합니다.
- 변경 사항을 커밋하기 전에 일련의 정책 및 디바이스에 대한 개체 변경 사항의 영향을 평가합니다.
- 다양한 정책 및 디바이스와 개체 및 개체의 관계 집합을 비교합니다.
- CDO에 온보딩된 후 디바이스에서 사용 중인 개체를 캡처합니다.

Note 개체에 수행된 대역 외 변경 사항은 개체에 대한 재정의로 탐지됩니다. 이러한 변경이 발생하면 편집된 값이 개체에 재정의로 추가되고 해당 개체를 선택하여 해당 값을 볼 수 있습니다. 디바이스에 대한 대역 외 변경 사항에 대해 자세히 알아보려면 디바이스의 대역 외 변경 사항, on page 143을 참조하십시오.

온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 문제 해결 CDO, on page 174를 참조하십시오.

개체 유형

다음 표에서는 CDO를 사용하여 디바이스에 대해 생성하고 관리할 수 있는 개체에 대해 설명합니다.

Table 2: 일반 개체

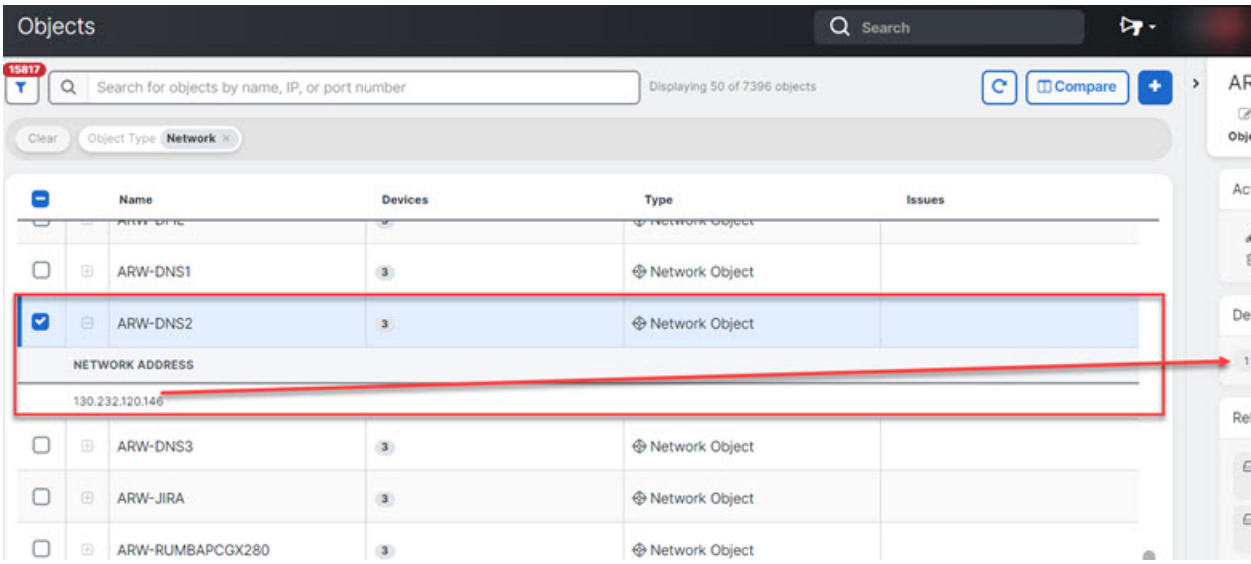
개체 유형	설명
네트워크	네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다.
URL	URL 개체 및 그룹(URL 개체로 총칭함)을 사용하여 웹 요청의 URL 또는 IP 주소를 정의합니다. 이러한 개체를 사용하여 액세스 제어 정책에서 수동 URL 필터링 또는 보안 인텔리전스 정책에서 차단 기능을 구현할 수 있습니다.

공유 개체

CDO는 이름과 콘텐츠가 동일한 여러 디바이스의 개체인 공유 개체를 호출합니다. 공유 개체는 이 아이콘으로 식별됩니다.

Objects(개체**)** 페이지에서 공유 개체를 사용하면 한 곳에서 개체를 수정할 수 있으며 변경 사항은 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 정책을 쉽게 유지 관리할 수 있습니다. 공유 개체가 없으면 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

공유 개체를 볼 때 CDO는 개체 테이블에 있는 개체의 내용을 표시합니다. 공유 개체는 정확히 동일한 내용을 갖습니다. CDO는 세부 정보 창에서 개체 요소의 결합된 보기 또는 "평평한" 보기를 보여줍니다. 세부 정보 창에서 네트워크 요소는 간단한 목록으로 병합되며 명명된 개체와 직접 연결되지 않습니다.



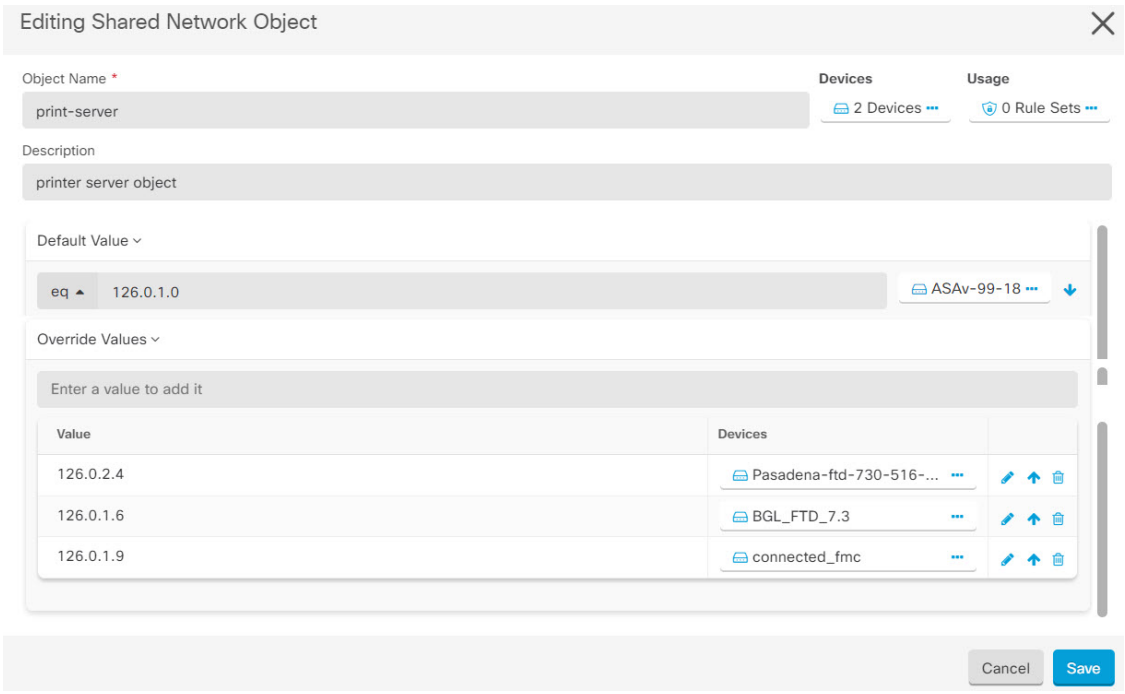
개체 재정의

개체 재정의는 특정 디바이스에서 공유 네트워크 객체의 값을 재정의할 수 있게 해줍니다. CDO는 재정의 구성 시 지정한 디바이스에 해당하는 값을 사용합니다. 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체에 대하여 CDO는 이러한 값이 재정의되기 때문에 **Inconsistent objects(**일관성 없는 개체**)**로 식별하지 않습니다.

대부분의 디바이스에 대한 정의가 해당하는 개체를 생성하고 다른 정의가 필요한 일부 디바이스의 개체에 대한 특정 변경 사항을 지정하는 오버라이드를 사용할 수 있습니다. 모든 디바이스에 오버라이드가 필요한 개체를 생성할 수도 있습니다. 하지만 이 경우 모든 디바이스에 단일 정책을 생성할 수 있습니다. 개체 재정의는 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성하도록 합니다.

예를 들어 각 사무실에 .프린터 서버가 있고, 프린터 서버 개체인 `print-server`를 만든 시나리오를 생각해 보십시오. ACL에는 프린터 서버가 인터넷에 액세스하는 것을 거부하는 규칙이 있습니다. 프린터 서버 개체에는 한 사무실에서 다른 사무실로 변경하려는 기본값이 있습니다. 값이 다를 수 있지만 개체 오버라이드를 사용하고 규칙과 "프린터-서버" 개체를 모든 위치에서 일관되게 유지함으로써 이 작업을 수행할 수 있습니다.

개체에 수행된 대역 외 변경 사항은 개체에 대한 재정의로 탐지됩니다. 이러한 변경이 발생하면 편집된 값이 개체에 재정의로 추가되고 해당 개체를 선택하여 해당 값을 볼 수 있습니다. 대역 외 변경 사항에 대해 자세히 알아보려면 디바이스의 대역 외 변경 사항, on page 143을 참조하십시오.



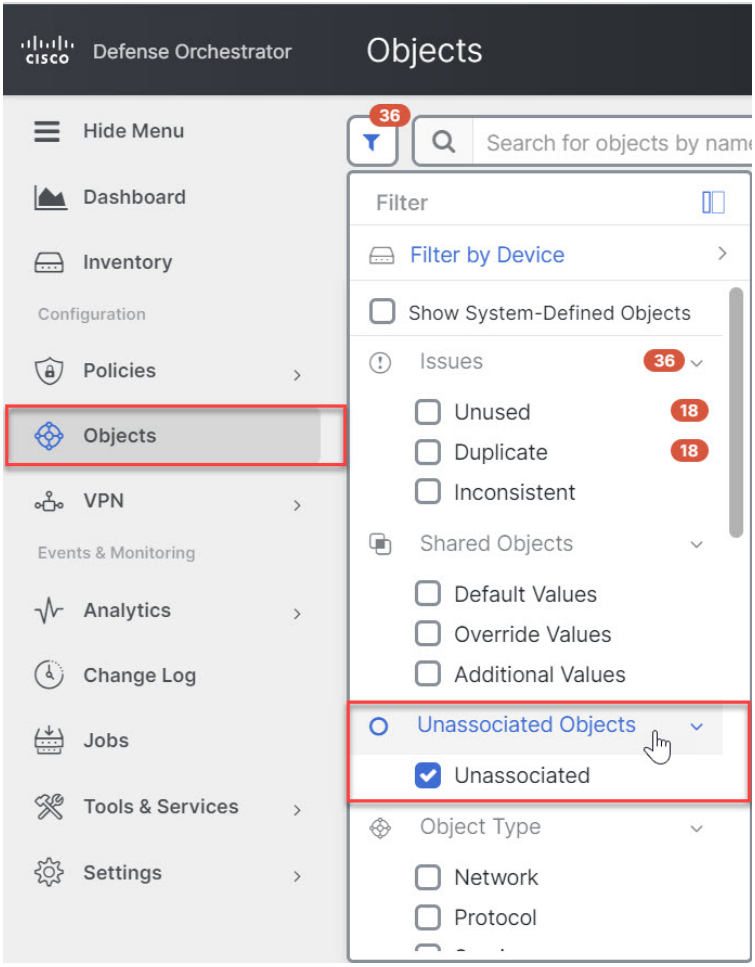
Note 일관되지 않은 개체가 있는 경우 오버라이드를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 불일치 개체 문제 해결, on page 180를 참고하십시오.

연결 해제된 개체

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수 있습니다. 규칙이나 정책과 연결되지 않은 개체를 생성할 수도 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, CDO는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다. 연결되지 않은 원래 개체는 야간 유지 관리 작업에 의해 삭제되거나 사용자가 삭제할 때까지 사용 가능한 개체 목록에 남아 있습니다.

개체와 연결된 규칙 또는 정책이 실수로 삭제된 경우 모든 구성이 손실되지 않도록 연결되지 않은 개체는 사본으로 CDO에 남아 있습니다.

연결되지 않은 개체를 보려면 개체 탭의 왼쪽 창에서 를 클릭하고 **Unassociated (**연결되지 않음**)** 확인란을 선택합니다.



개체 비교

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 페이지에서 개체를 필터링하여 비교하려는 개체를 찾습니다.

단계 **3** **Compare(**비교**)** 버튼 Compare 를 클릭합니다.

단계 **4** 비교할 개체를 최대 3개까지 선택합니다.

단계 **5** 화면 하단에서 개체를 나란히 봅니다.

- 개체 세부 정보 제목 표시줄에서 위쪽 및 아래쪽 화살표를 클릭하면 개체 세부 정보를 더 많이 또는 더 적게 볼 수 있습니다.
- 세부 정보 및 관계 상자를 확장하거나 축소하여 더 많거나 적은 정보를 확인합니다.

단계 **6** (선택 사항) 관계 상자는 개체가 사용되는 방식을 보여줍니다. 디바이스 또는 정책과 연결될 수 있습니다. 개체가 디바이스와 연결된 경우 디바이스 이름을 클릭한 다음 **View Configuration(**구성 보기**)** 을 클릭하여 디바이스 구성을 볼 수 있습니다. CDO는 디바이스의 구성 파일을 표시하고 해당 개체에 대한 항목을 강조 표시합니다.

필터

Security Devices(보안 디바이스**)** 및 **Objects(**개체**)** 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 Security Devices(보안 디바이스), Policies(정책) 및 Objects(개체) 탭의 왼쪽 창에서 을 클릭합니다.

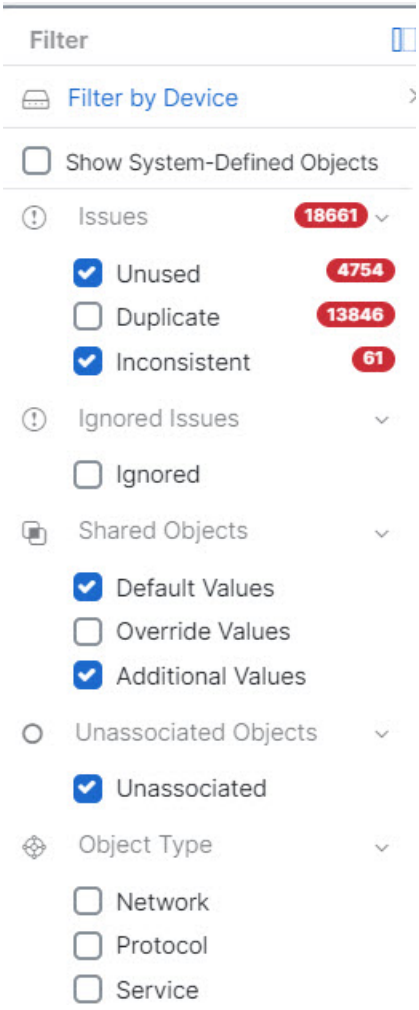
보안 디바이스 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

개체 유형 필터를 사용하면 네트워크 개체, 네트워크 그룹, URL 개체, URL 그룹, 서비스 개체, 서비스 그룹 등의 유형별로 개체를 필터링할 수 있습니다. 공유 개체 필터를 사용하면 기본값 또는 재정의 값이 있는 개체를 필터링할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(사용되었거나 일관성 없음)" 및 추가 값이 있는 공유된 개체의 개체 검색에 필터를 적용합니다.



개체 필터

필터링하려면 Objects(개체) 탭의 왼쪽 창에서 을(를) 클릭합니다.

- **Filter by Device(**디바이스별 필터**)**: 선택한 디바이스에 있는 개체를 볼 수 있도록 특정 디바이스를 선택할 수 있습니다.
- **Issues(**문제**)**: 사용하지 않거나 중복되고 일치하지 않는 개체를 선택하여 볼 수 있습니다.
- **Ignored Issues(**무시된 문제**)**: 불일치가 무시했던 모든 개체를 볼 수 있습니다.
- **Shared Objects(**공유 개체**)**: CDO가 둘 이상의 디바이스에서 공유된 것으로 확인된 모든 개체를 볼 수 있습니다. 기본값만, 재정의 값 또는 둘 다를 사용하여 공유 개체를 보도록 선택할 수 있습니다.
- **Unassociated Objects(**연결되지 않은 개체**)**: 규칙이나 정책과 연결되지 않은 모든 개체를 볼 수 있습니다.

- **Object Type(**개체 유형**)**: 개체 유형을 선택하여 네트워크 개체, 네트워크 그룹, URL 개체, URL 그룹, 서비스 개체 및 서비스 그룹과 같이 선택한 유형의 개체만 표시할 수 있습니다.

하위 필터 – 각 기본 필터에는 선택 범위를 좁히기 위해 적용할 수 있는 하위 필터가 있습니다. 이러한 하위 필터는 네트워크, 서비스, 프로토콜 등의 개체 유형을 기반으로 합니다.

이 필터 표시줄에서 선택한 필터는 다음 기준과 일치하는 개체를 반환합니다.

***** 두 디바이스 중 하나에 있는 개체. (디바이스를 지정하려면 **Filter by Device(**디바이스별 필터링**)**를 클릭합니다.) 및

***** 일치하지 않는 개체 및

***** 네트워크 개체 또는 서비스 개체 및

***** 개체 명명 규칙에 "**group**"이라는 단어가 있습니다.

Show System Objects(시스템 개체 표시**)**를 선택했으므로 결과에 시스템 개체와 사용자 정의 개체가 모두 포함됩니다.

시스템 정의 개체 표시 필터

일부 디바이스는 공통 서비스에 대해 사전 정의된 개체가 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.

Show System-Defined Objects(시스템 정의 개체 표시**)**는 기본적으로 꺼져 있습니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 **Show System-Defined Objects(**시스템 정의 개체 표시**)**를 선택합니다. 개체 테이블에서 시스템 개체를 숨기려면 필터 표시줄에서 Show System Objects(시스템 개체 표시)를 선택하지 않은 상태로 둡니다.

시스템 개체를 숨기면 검색 및 필터링 결과에 포함되지 않습니다. 시스템 개체를 표시하면 개체 검색 및 필터링 결과에 포함됩니다.

개체 필터 구성

원하는 만큼 기준을 필터링할 수 있습니다. 더 많은 범주를 필터링할수록 예상되는 결과는 줄어듭니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 페이지 상단의 필터 아이콘을 클릭하여 필터 패널을 엽니다. 선택한 필터를 선택 취소하여 실수로 필터링된 개체가 없는지 확인합니다. 또한 검색 필드를 살펴보고 검색 필드에 입력되었을 수 있는 텍스트를 삭제합니다.

단계 **3** 특정 디바이스에 있는 것으로 결과를 제한하려면 다음을 수행합니다.

a. **Filter By Device(**디바이스별 필터링**)**를 클릭합니다.

b. 모든 디바이스를 검색하거나 디바이스 탭을 클릭하여 특정 종류의 디바이스만 검색합니다.

c. 필터 기준에 포함할 디바이스를 선택합니다.

d. **OK(**확인**)**를 클릭합니다.

단계 **4** 검색 결과에 시스템 개체를 포함하려면 **Show System Objects(**시스템 개체 표시**)**를 선택합니다. 검색 결과에서 시스템 개체를 제외하려면 **Show System Objects(**시스템 개체 표시**)**의 선택을 취소합니다.

단계 **5** 필터링할 개체 **Issues(**문제**)**를 선택합니다. 두 개 이상의 문제를 선택하면 선택한 범주의 개체가 필터 결과에 포함됩니다.

단계 **6** 문제가 있었지만 관리자가 무시한 개체를 확인하려면 **Ignored(**무시됨**)** 문제를 선택합니다.

단계 **7** 두 개 이상의 디바이스 간에 공유되는 개체를 필터링하는 경우 **Shared Objects(**공유 개체**)**에서 필수 필터를 선택합니다.

- **Default Values(**기본값**)**: 기본값만 있는 개체를 필터링합니다.
- **Override Values(**값 재정의**)**: 오버라이드된 값이 있는 개체를 필터링합니다.
- **Additional Values(**추가 값**)**: 추가 값이 있는 개체를 필터링합니다.

단계 **8** 규칙 또는 정책의 일부가 아닌 개체를 필터링하는 경우 **Unassociated(**연결되지 않음**)**를 선택합니다.

단계 **9** 필터링할 개체 유형을 선택합니다.

단계 **10** Objects(개체) 검색 필드에 개체 이름, IP 주소 또는 포트 번호를 추가하여 필터링된 결과 중에서 검색 기준으로 개체를 찾을 수도 있습니다.

필터 기준에서 디바이스를 제외해야 하는 경우

필터링 기준에 디바이스를 추가하면 결과에 디바이스의 개체가 표시되지만 해당 개체와 다른 디바이스의 관계는 표시되지 않습니다. 예를 들어 **ObjectA**가 ASA1과 ASA2 간에 공유된다고 가정합니다. ASA1에서 공유 개체를 찾기 위해 개체를 필터링하는 경우 **ObjectA**를 찾을 수 있지만 **Relationships(**관계**)** 창에는 해당 개체가 ASA1에 있다는 것만 표시됩니다.

개체와 관련된 모든 디바이스를 보려면 검색 기준에 디바이스를 지정하지 마십시오. 다른 기준으로 필터링하고 원하는 경우 검색 기준을 추가하십시오. CDO가 식별하는 개체를 선택한 다음 관계 창을 살펴봅니다. 개체와 관련된 모든 디바이스 및 정책이 표시됩니다.

개체 무시

사용되지 않거나 중복되거나 일관성이 없는 개체를 해결하는 한 가지 방법은 해당 개체를 무시하는 것입니다. 사용되지 않은 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결 해당 상태에 대한 타당한 이유가 있다고 판단하고 개체 문제를 해결되지 않은 상태로 두도록 선택할 수 있습니다. 나중에 무시된 개체를 해결해야 할 수도 있습니다. CDO는 개체 문제를 검색할 때 무시된 개체를 표시하지 않으므로 무시된 개체에 대한 개체 목록을 필터링한 다음 결과에 따라 조치를 취해야 합니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 개체 필터

단계 **3** **Object(**개체**)** 테이블에서 무시를 취소할 개체를 선택합니다. 한 번에 하나의 개체를 무시 취소할 수 있습니다.

단계 **4** 세부 정보 창에서 **Unignore(**무시**)**를 클릭합니다.

단계 **5** 요청을 확인합니다. 이제 문제별로 개체를 필터링하면 이전에 무시되었던 개체를 찾아야 합니다.

개체 삭제

단일 개체 또는 여러 개체를 삭제할 수 있습니다.

단일 개체 삭제

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 개체 필터와 검색 필드를 사용하여 삭제하려는 개체를 찾아 선택합니다.

단계 **3** **Relationships(**관계**)** 창을 검토합니다. 개체가 정책 또는 개체 그룹에서 사용되는 경우 해당 정책 또는 그룹에서 개체를 제거할 때까지 개체를 삭제할 수 없습니다.

단계 **4** 작업 창에서 **Remove(**제거**)** 아이콘 를 클릭합니다.

단계 **5** **OK(**확인**)**을 클릭하여 개체 삭제를 확인합니다.

단계 **6** 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나, 한 번에 여러 변경 사항을 기다렸다가 배포합니다.

사용되지 않는 개체 그룹 삭제

디바이스를 온보딩하고 개체 문제를 해결하기 시작하면 사용하지 않는 개체를 많이 찾습니다. 한 번에 최대 50개의 사용하지 않는 개체를 삭제할 수 있습니다.

프로시저

단계 **1** **Issues(**문제**)** 필터를 사용하여 미사용 개체를 찾습니다. 디바이스 필터를 사용하여 디바이스 없음을 선택하여 디바이스와 연결되지 않은 개체를 찾을 수도 있습니다. 개체 목록을 필터링하면 개체 확인란이 나타납니다.

단계 **2** 개체 테이블 머리글에서 **Select all(**모두 선택**)** 확인란을 선택하여 개체 테이블에 나타나는 필터에 의해 발견된 모든 개체를 선택합니다. 또는 삭제할 개별 개체에 대한 개별 확인란을 선택합니다.

단계 **3** 작업 창에서 **Remove(**제거**)** 아이콘 를 클릭합니다.

단계 **4** 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

네트워크 개체

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 그룹은 그룹에 추가하는 네트워크 개체 및 기타 개별 주소 또는 서브 네트워크의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. CDO를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

동적 개체를 공유할 때 Cisco Merkai 및 멀티 클라우드 방어 등 모든 플랫폼이 네트워크 개체를 지원하는 것은 아니며, CDO는 원본 플랫폼 또는 디바이스에서 적절한 정보를 CDO이 사용할 수 있는 사용 가능한 정보 집합으로 자동으로 변환합니다.

제품 간 네트워크 개체 재사용

CDO 테넌트가 하나 있고 클라우드 제공 Firewall Management Center 및 하나 이상의 온프레미스 방화벽 Management Center가 테넌트에 온보딩된 경우:

- Secure Firewall Threat Defense, FDM 관리 Threat Defense, ASA 또는 Meraki 네트워크 개체 또는 그룹을 생성하면 클라우드 제공 Firewall Management Center를 구성할 때 사용되는 **Objects(**개체**)** > **Other FTD Objects(**기타 **FTD** 개체**)** 페이지의 개체 목록에도 개체의 복사본이 추가되며, 그 반대의 경우도 마찬가지입니다.

- Secure Firewall Threat Defense, FDM 관리 Threat Defense 또는 ASA 네트워크 개체나 그룹을 생성하면 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대해 항목이 생성됩니다. 이 목록에서 개체를 사용하려는 온프레미스 방화벽 Management Center에 개체를 선택하여 구축하고 원하지 않는 개체를 폐기할 수 있습니다. **Tools & Services(**도구 및 서비스**)** > **Firewall Management Center** , 온프레미스 방화벽 Management Center를 선택한 후 **Objects(**개체**)**를 클릭하여 온프레미스 방화벽 Management Center 사용자 인터페이스에서 개체를 확인하고 정책에 할당합니다.

한 페이지에서 네트워크 개체 또는 그룹에 대한 변경 사항은 두 페이지의 개체 또는 그룹 인스턴스에 적용됩니다. 한 페이지에서 개체를 삭제하면 다른 페이지에서도 개체의 해당 복사본이 삭제됩니다.

예외:

- 클라우드 제공 Firewall Management Center에 대해 동일한 이름의 네트워크 개체가 이미 있는 경우 Secure Firewall Threat Defense, FDM 관리 Threat Defense, ASA 또는 Meraki 네트워크 개체는 CDO의 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에서 복제되지 않습니다.
- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩된 Threat Defense 디바이스의 네트워크 개체 및 그룹은 **Objects(**개체**) > Other FTD Objects(**기타 **FTD** 개체**)** 페이지에 복제되지 않으며, 클라우드 제공 Firewall Management Center에서 사용할 수 없습니다.

  클라우드 제공 Firewall Management Center로 마이그레이션된 온프레미스 Secure Firewall Management Center 인스턴스의 경우, 네트워크 개체 및 그룹이 FTD 디바이스에 구축된 정책에서 사용되었다면 네트워크 개체 및 그룹이 CDO 개체 페이지에 복제됩니다.
- CDO와 클라우드 제공 Firewall Management Center 간에 네트워크 개체 공유는 새로운 테넌트에서 자동으로 활성화되지만 기존 테넌트에 대해서는 요청해야 합니다. 네트워크 개체를 클라우드 제공 Firewall Management Center와 공유하지 않는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법.하여 테넌트에서 기능을 활성화하십시오.
- CDO와 On-Premises Management Center간의 네트워크 개체 공유는 CDO에 온보딩된 새 온프레미스 방화벽 Management Center에 대해 CDO에서 자동으로 활성화되지 않습니다. 네트워크 개체가 On-Premises Management Center와 공유되지 않는 경우 **Settings(**설정**)**에서 온프레미스 방화벽 Management Center에 대해 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글 버튼이 활성화되어 있는지 확인하거나 CDO 고객이 TAC로 지원 티켓을 여는 방법.하여 테넌트에서 기능을 활성화하십시오.

네트워크 개체 보기

CDO를 사용하여 생성한 네트워크 개체와 온보딩된 디바이스 구성에서 CDO가 인식것이 Objects(개체) 페이지에 표시됩니다. 개체 유형으로 레이블이 지정됩니다. 이렇게 하면 개체 유형으로 필터링하여 원하는 개체를 빠르게 찾을 수 있습니다.

Objects(개체) 페이지에서 네트워크 개체를 선택하면 Details(세부 정보) 창에 개체의 값이 표시됩니다. Relationships(관계) 창에는 개체가 정책에서 사용되는지 여부와 개체가 저장된 디바이스가 표시됩니다.

네트워크 그룹을 클릭하면 해당 그룹의 콘텐츠가 표시됩니다. 네트워크 그룹은 네트워크 개체에 의해 제공되는 모든 값의 복합물입니다.

서비스 개체

프로토콜 개체

프로토콜 개체는 덜 일반적으로 사용되는 또는 레거시 프로토콜을 포함하는 서비스 개체 유형입니다. 프로토콜 개체는 이름과 프로토콜 번호로 식별됩니다. CDO는 ASA 및 Firepower(FDM 관리 디바이스) 구성에서 이러한 개체를 인식하고 사용자가 쉽게 찾을 수 있도록 자체 필터인 "프로토콜"을 제공합니다.

ICMP 개체

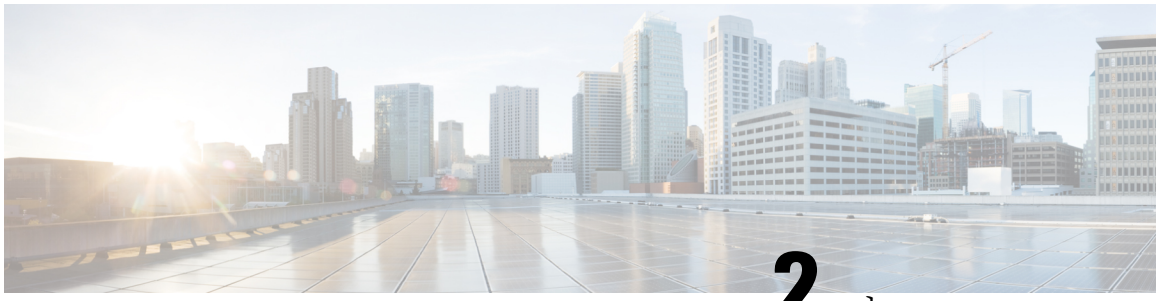
ICMP(인터넷 제어 메시지 프로토콜) 개체는 ICMP 및 IPv6-ICMP 메시지 전용 서비스 개체입니다. CDO는 ASA 및 Firepower 구성에서 해당 디바이스가 온보딩되었을 때 이러한 개체를 인식하고 CDO는 사용자가 개체를 쉽게 찾을 수 있도록 해당 디바이스에 "ICMP" 필터를 제공합니다.

CDO를 사용하면 ASA 구성에서 ICMP 개체를 제거하거나 이름을 바꿀 수 있습니다. CDO를 사용하여 Firepower 구성에서 ICMP 및 ICMPv6 개체를 생성, 업데이트 및 삭제할 수 있습니다.

Note ICMPv6 프로토콜의 경우 AWS는 특정 인수 선택을 지원하지 않습니다. 모든 ICMPv6 메시지를 허용하는 규칙만 지원됩니다.

관련 정보:

- 개체 삭제, on page 112



2 장

디바이스 및 서비스 온보딩

라이브 디바이스와 모델 디바이스를 모두 CDO에 온보딩할 수 있습니다. 모델 디바이스는 CDO를 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 보안 디바이스 커넥터가 CDO를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

SDC 및 해당 상태에 대한 자세한 내용은 보안 디바이스 커넥터, 11 페이지의 내용을 참조하십시오.

이 장에는 다음 섹션이 포함되어 있습니다.

SSH 디바이스 온보딩

SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 디바이스를 온보딩할 수 있습니다.

SSH 디바이스 온보딩

Before you begin

시작하기 전에 다음 사전 요건을 충족했는지 확인하십시오.

- Cisco SSH 디바이스가 지원하는 암호가 CDO에서 지원되는지 확인합니다. 현재 CDO는 Cisco SSH 디바이스 온보딩에 대해 제한된 암호 집합을 지원합니다. 지원되는 암호는 다음과 같습니다. `aes128-ctr`, `aes192-ctr`, `aes256-ctr`, `aes128-gcm`, `aes128-gcm@openssh.com`, `aes256-gcm`, `aes256-gcm@openssh.com` 서버에서 지원하는 암호를 확인하려면 SDC에 로그인하고 다음 명령을 실행합니다. `ssh -vv <ip_address>`.
- Cisco IOS 디바이스를 온보딩하려면 네트워크에 온프레미스 SDC(Secure Device Connector)가 있어야 합니다. SDC에 대한 설명과 구축 시나리오 링크는 보안 디바이스 커넥터, on page 11의 내용을 참조하십시오.
- 디바이스를 온보딩하기 전에 매니지드 디바이스에 CDO 연결을 검토합니다.

Procedure

단계 **1** 탐색창에서 **Inventory(**재고 목록**)** 페이지를 클릭합니다.

단계 **2** 디바이스를 온보딩하려면 파란색 플러스 버튼  를 클릭합니다.

단계 **3** **Integrations(**통합**)** 타일을 클릭합니다. 회색으로 표시되는 경우에는 네트워크에 구축되어 CDO 테넌트에서 사용하는 활성 보안 디바이스 커넥터가 없음을 의미합니다.

단계 **4** 보안 디바이스 커넥터, on page 11 버튼을 클릭하고 네트워크에서 이 디바이스가 통신할 SDC를 선택합니다. 기본 SDC가 표시되지만 SDC 이름을 클릭하여 변경할 수 있습니다.

단계 **5** 디바이스에 이름을 지정합니다.

단계 **6** Integrations(통합) 드롭다운 메뉴에서 **Generic SSH(**일반 **SSH)**를 선택합니다.

단계 **7** 디바이스의 위치를 FDQN 또는 IPv4 주소로 입력합니다. 기본 SSH 포트는 22입니다.

단계 **8** **Go(**이동**)**을 클릭합니다. CDO가 디바이스를 찾고 구성 통합을 준비합니다.

단계 **9** SSH 지문을 다운로드하고 로컬에 저장합니다. SSH를 통해 이 디바이스에 연결한 적이 없다면 이 지문을 사용하여 디바이스를 확인할 수 있습니다.

단계 **10** 온보딩하려는 디바이스에 대한 사용자 이름 및 비밀번호 로그인 자격 증명 을 입력합니다. CDO는 올바른 로그인 정보가 없으면 기존 설정을 읽을 수 없습니다.

단계 **11** (선택 사항) 이전에 이 디바이스에 대해 비밀번호 활성화를 구성한 경우 **Enable Password(**비밀번호 활성화**)**를 입력합니다.

단계 **12** (선택 사항) 드롭다운 메뉴에서 Configuration Command(구성 명령)를 선택하거나 텍스트 상자에 사용자 지정 명령을 입력합니다. 이 명령은 디바이스의 구성으로 사용됩니다. OOB가 활성화된 경우 CDO는 변경 사항을 확인하며 구성 페이지에서 현재 값을 볼 수 있습니다 디바이스가 CDO에 성공적으로 온보딩되면 이 명령을 변경할 수 있습니다.

단계 **13** **Connect(**연결**)**를 클릭합니다.

Note
로그인 자격 증명이 잘못된 경우 연결 세부 정보를 검토하라는 메시지가 표시됩니다. 여기에서 로그인 정보를 다시 입력할 수 있습니다. 자격 증명을 편집하지 않고 검토를 종료하는 경우, 디바이스는 **Inventory(**재고 목록**)** 페이지에 통합 인스턴스가 있지만 디바이스는 온보딩되거나 동기화되지 않습니다.

단계 **14** (선택 사항) 이 디바이스에 레이블을 추가합니다.

단계 **15** **Continue(**계속**)**를 클릭합니다.

단계 **16** 디바이스가 CDO에 온보딩됩니다. 마침를 클릭합니다.

단계 **17** **Inventory(**재고 목록**)** 페이지로 돌아갑니다. 디바이스가 성공적으로 온보딩되면 Configuration Status(구성 상태)가 "Synced(동기화됨)"이고 Connectivity(연결성) 상태가 "Online(온라인)"으로 표시됩니다.

Note
디바이스가 온보딩되면 실행할 구성 명령을 변경할 수 있습니다. 사용자 지정 명령을 사용하거나 CLI 매크로를 생성할 수 있습니다.

단계 **18** (선택 사항) 원하는 경우 디바이스의 참고 페이지에 입력하여 디바이스에 대한 참고를 작성할 수 있습니다. 자세한 내용은 디바이스 메모 작성을 참조하십시오.

관련 정보**:**

- 명령줄 인터페이스 매크로
-
- Cisco IOS 또는 SSH에서 CDO로 변경 사항 읽기, on page 137
- 디바이스 구성 변경 정보

CDO에서 디바이스 삭제

CDO에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

프로시저

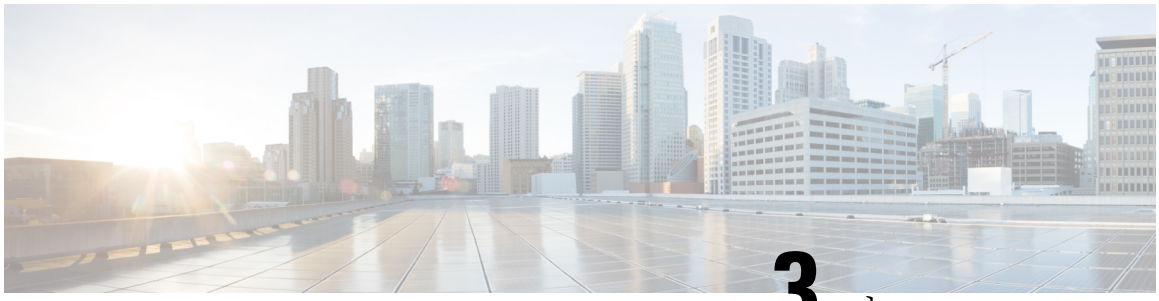
단계 **1** CDO에 로그인합니다.

단계 **2** **Inventory(**재고 목록**)** 페이지로 이동합니다.

단계 **3** 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.

단계 **4** 오른쪽에 있는 **Device Actions(**디바이스 작업**)** 패널에서 **Remove(**제거**)**를 선택합니다.

단계 **5** 메시지가 표시되면 **OK(**확인**)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel(**취소**)**을 선택합니다.



3 장

Cisco Defense Orchestrator를 사용하여 SSH 디바이스 관리

Cisco Defense Orchestrator(CDO)에서는 SSH를 통해 디바이스를 관리할 수 있습니다. 이러한 디바이스에 대해 지원되는 기능은 다음과 같습니다.

- SSH 디바이스를 온보딩합니다. SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 디바이스를 온보딩할 수 있습니다.
- 디바이스 구성 보기. 디바이스 구성 파일을 볼 수 있습니다.
- 디바이스에서 정책 및 구성 변경 사항을 검토합니다. SSH 디바이스에서 구성 파일을 읽으면 해당 파일이 CDO의 데이터베이스에 저장됩니다.
- 대역 외 변경 탐지. 충돌 탐지를 활성화한 경우 CDO는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 변경 사항이 있는 경우 디바이스의 상태가 Conflict Detected(충돌 탐지됨)로 변경되며, 변경 충돌을 해결할 수 있습니다.
- 명령줄 인터페이스 지원. CDO의 명령줄 인터페이스를 통해 디바이스에 모든 SSH 디바이스 명령을 실행할 수 있습니다.
- 개별 CLI 명령 및 명령 그룹을 편집 및 재사용 가능한 "매크로"로 전환할 수 있습니다. CDO에서 제공하는 시스템 정의 매크로를 사용하거나 자주 수행하는 작업에 대해 자신만의 매크로를 만들 수 있습니다.
- SSH 핑거프린트 변경 사항 탐지 및 관리. 디바이스의 자격 증명 또는 속성이 변경되어 SSH 지문이 변경되는 경우 해당 CDO는 변경 사항을 감지하고 새 지문을 검토하고 수락할 수 있는 기회를 제공합니다.
- 변경 로그. 변경 로그는 사용자가 SSH 디바이스에 실행하는 모든 명령을 캡처합니다.

CDO 명령줄 인터페이스

CDO는 사용자에게 , SSH-매니지드 디바이스를 관리하기 위한 CLI(명령줄 인터페이스)를 제공합니다. 사용자는 단일 디바이스 또는 여러 디바이스에 동시에 명령을 전송할 수 있습니다.

명령줄 인터페이스 사용

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 명령줄 인터페이스(CLI)를 사용하여 관리하려는 디바이스를 찾으려면 디바이스 탭과 필터 버튼을 사용합니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Device Actions(**장치 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** **Command Line Interface(**명령줄 인터페이스**)** 탭을 클릭합니다.

단계 **7** 명령 창에 명령을 입력하고 **Send(**보내기**)**를 클릭합니다. 명령에 대한 디바이스의 응답은 "응답 창" 아래에 표시됩니다.

Note
실행할 수 있는 명령에 제한 사항이 있는 경우 해당 제한 사항은 명령 창 위에 나열됩니다.

Related Topics

명령줄 인터페이스에 명령 입력, 123 페이지

명령줄 인터페이스에 명령 입력

한 줄에 하나의 명령을 입력하거나 여러 줄에 여러 명령을 순차적으로 입력할 수 있으며 CDO는 명령을 순서대로 실행합니다. 다음 ASA 예에서는 세 개의 네트워크 개체와 해당 네트워크 개체를 포함하는 네트워크 개체 그룹을 생성하는 명령 배치를 전송합니다.

명령 기록 작업

CLI 명령을 보낸 후 CDO는 **Command Line Interface(**명령줄 인터페이스**)** 페이지의 기록 창에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **5** 아직 확장되지 않은 경우 시계 아이콘 을 클릭하여 기록 창을 확장합니다.

단계 **6** 편집하거나 다시 보내려는 히스토리 창에서 명령을 Select(선택)합니다.

단계 **7** 명령 창에서 명령을 그대로 재사용하거나 편집하고 **Send(**보내기**)**를 클릭합니다. CDO는 명령의 결과를 응답 창에 표시합니다.

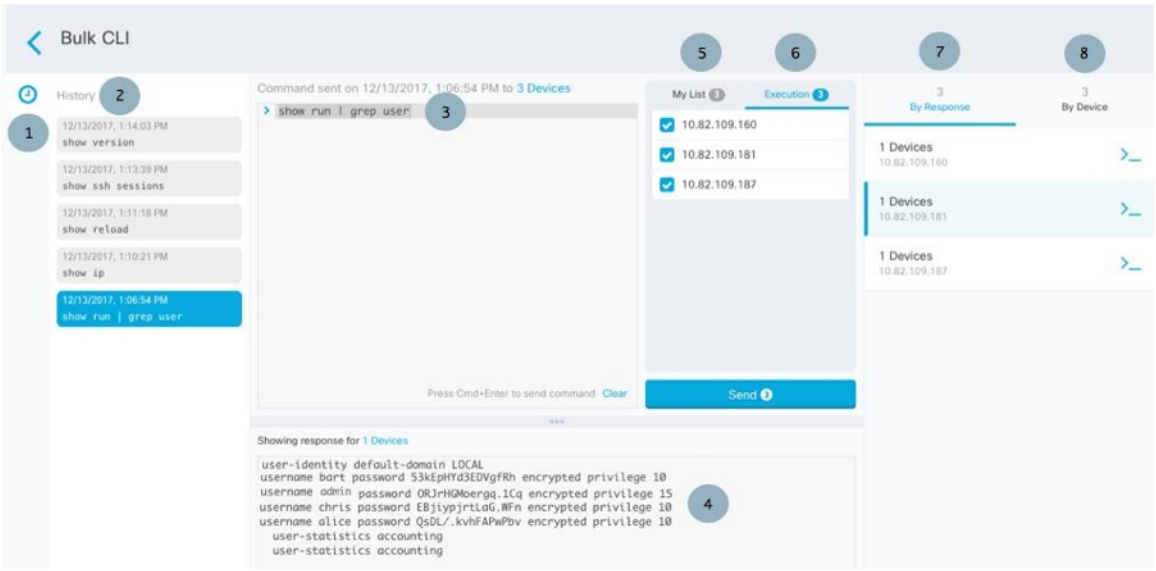
Note
CDO는 다음 두 가지 상황에서 응답창에 `Done!(완료!)` 메시지를 표시합니다.

- 명령이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 `완료!`를 반환합니다.

대량 명령줄 인터페이스

CDO는 CLI(command line interface)를 사용하여 Secure Firewall ASA, FDM 관리, Threat Defense, SSH 및 Cisco IOS 디바이스를 관리할 수 있는 기능을 사용자에게 제공합니다. 사용자는 단일 디바이스 또는 같은 종류의 여러 디바이스에 동시에 명령을 보낼 수 있습니다. 이 섹션에서는 한 번에 여러 디바이스에 CLI 명령을 보내는 방법을 설명합니다.

대량 **CLI** 인터페이스



Note CDO는 다음 두 가지 상황에서 **Done!(**완료**!)** 메시지를 표시합니다.

- 명령이 오류 없이 성공적으로 실행된 후.
- 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료**!**를 반환합니다.

숫자	설명
1	시계를 클릭하여 명령 기록 창을 확장하거나 축소합니다.
2	명령 기록. 명령을 보낸 후 CDO는 이 히스토리 창에 명령을 기록하므로 돌아가서 선택하고 다시 실행할 수 있습니다.
3	명령 창. 이 창의 프롬프트에 명령을 입력합니다.

숫자	설명
4	응답 창. CDO는 명령에 대한 디바이스의 응답과 CDO 메시지를 표시합니다. 두 개 이상의 디바이스에 대한 응답이 동일한 경우 응답 창에 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다. **Note** CDO는 다음 두 가지 상황에서 **Done!(**완료**!)** 메시지를 표시합니다. • 명령이 오류 없이 성공적으로 실행된 후. • 명령에 반환할 결과가 없는 경우. 예를 들어 특정 구성 항목을 검색하는 정규식과 함께 show 명령을 실행할 수 있습니다. 정규식 기준을 충족하는 구성 항목이 없는 경우 CDO는 완료**!**를 반환합니다.
5	**My List(**내 목록**)** 탭에는 보안 디바이스 테이블에서 선택한 디바이스가 표시되며 명령을 보낼 디바이스를 포함하거나 제외할 수 있습니다.
6	위 그림에서 강조 표시된 **Execution(**실행**)** 탭은 히스토리 창에서 선택한 명령의 디바이스를 표시합니다. 이 예에서 show run | grep user 명령이 기록 창에서 선택되고 실행 탭에 10.82.109.160, 10.82.109.181 및 10.82.10.9.187로 전송된 것으로 표시됩니다.
7	**By Response(**응답별**)** 탭을 클릭하면 명령에 의해 생성된 응답 목록이 표시됩니다. 동일한 응답은 한 행에 함께 그룹화됩니다. By Response(응답별) 탭에서 행을 선택하면 CDO는 응답 창에 해당 명령에 대한 응답을 표시합니다.
8	**By Device(**디바이스별**)** 탭을 클릭하면 각 디바이스의 개별 응답이 표시됩니다. 목록에서 디바이스 중 하나를 클릭하면 특정 디바이스에서 명령에 대한 응답을 볼 수 있습니다.

대량 명령 전송

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 탭을 선택하고 필터 버튼을 사용하여 명령줄 인터페이스를 사용하여 구성할 디바이스를 찾습니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Device Actions(**장치 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 내 목록 필드에서 명령을 보낼 디바이스를 선택하거나 선택 취소할 수 있습니다.

단계 **7** 명령 창에 명령을 입력하고 **Send(**보내기**)**를 클릭합니다. 명령 출력은 응답 창에 표시되고 명령은 변경 로그에 기록되며 CDO 명령은 대량 CLI 창의 기록 창에 명령을 기록합니다.

대량 명령 기록 작업

대량 CLI 명령을 보낸 후, CDO는 대량 CLI 인터페이스 기록에 해당 명령을 기록합니다. 기록 창에 저장된 명령을 다시 실행하거나 명령을 템플릿으로 사용할 수 있습니다. 기록 창의 명령은 명령이 실행된 원래 디바이스와 연결됩니다.

Procedure

단계 **1** 탐색창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** 디바이스를 찾으려면 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 필터 아이콘을 클릭하여 구성하려는 디바이스를 찾습니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 편집하거나 다시 보내려는 히스토리 창에서 명령을 **Select(**선택**)**합니다. 선택하는 명령은 특정 디바이스와 연결되며 반드시 첫 번째 단계에서 선택한 디바이스와 연결되지는 않습니다.

단계 **7** 내 목록 탭을 보고 전송하려는 명령이 예상하는 디바이스로 전송되는지 확인합니다.

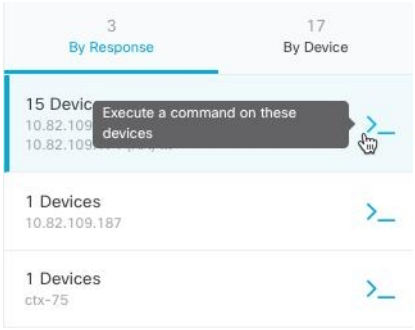
단계 **8** 명령 창에서 명령을 편집하고 **Send(**보내기**)**를 클릭합니다. CDO는 명령의 결과를 응답 창에 표시합니다.

대량 명령 필터 작업

대량 CLI 명령을 실행한 후 **By Resonse(**응답별**)** 필터 및 **By Device(**디바이스별**)** 필터를 사용하여 계속해서 디바이스를 구성할 수 있습니다.

응답 기준 필터

대량 명령을 실행한 후 CDO는 명령을 보낸 디바이스에서 반환된 응답 목록으로 **By Response(**응답별**)** 탭을 채웁니다. 응답이 동일한 디바이스는 단일 행에 통합됩니다. **By Response(**응답별**)** 탭에서 행을 클릭하면 응답 창에 디바이스의 응답이 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. **X** 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.



명령 응답과 관련된 디바이스 목록에 명령을 보내려면 다음 절차를 따르십시오.

Procedure

단계 **1** **By Response(**응답별**)** 탭에서 행의 명령 기호를 클릭합니다.

단계 **2** 명령 창에서 명령을 검토하고 **Send(**보내기**)**를 클릭하여 명령을 다시 보내거나 **Clear(**지우기**)**를 클릭하여 명령 창을 지우고 디바이스로 보낼 새 명령을 입력한 다음 **Send(**보내기**)**를 클릭합니다.

단계 **3** 명령에서 받은 응답을 검토하십시오.

단계 **4** 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send(**보내기**)**를 클릭합니다. 이렇게 하면 실행 중인 구성이 시작 구성에 저장됩니다.

디바이스 기준 필터

대량 명령을 실행한 후 CDO는 실행 탭과 디바이스별 탭을 명령을 보낸 디바이스 목록으로 채웁니다. 디바이스별 탭에서 행을 클릭하면 각 디바이스에 대한 응답이 표시됩니다.

동일한 디바이스 목록에서 명령을 실행하려면 다음 절차를 따르십시오.

Procedure

단계 **1** **By Device(**디바이스 별**)** 탭을 클릭합니다.

단계 **2** **>_Execute a command on these devices(**이 디바이스에서 명령 실행**)**를 클릭합니다.

단계 **3** **Clear(**지우기**)**를 클릭하여 명령 창을 지우고 새 명령을 입력합니다.

단계 **4** 내 목록 창에서 목록의 개별 디바이스를 선택하거나 선택 취소하여 명령을 보낼 디바이스 목록을 지정합니다.

단계 **5** **Send(**보내기**)**를 클릭합니다. 명령에 대한 응답이 응답 창에 표시됩니다. 응답 창에 두 개 이상의 디바이스에 대한 응답이 표시되면 "X 디바이스에 대한 응답 표시"라는 메시지가 표시됩니다. X 디바이스를 클릭하면 CDO가 명령에 동일한 응답을 반환한 모든 디바이스를 표시합니다.

단계 **6** 선택한 디바이스에서 실행 중인 구성 파일이 변경 사항을 반영한다고 확신하는 경우 명령 창에 `write memory`를 입력하고 **Send(**보내기**)**를 클릭합니다.

명령줄 인터페이스 매크로

CLI 매크로는 즉시 사용할 수 있는 완전한 형식의 CLI 명령이거나 실행 전에 수정할 수 있는 CLI 명령의 템플릿입니다. 모든 매크로는 하나 이상의 SSH 디바이스에서 동시에 실행할 수 있습니다.

여러 디바이스에서 동일한 명령을 동시에 실행하려면 템플릿과 유사한 CLI 매크로를 사용합니다. CLI 매크로는 디바이스 구성 및 관리의 일관성을 유지합니다. 완전한 형식의 CLI 매크로를 사용하여 디바이스에 대한 정보를 가져옵니다. SSH 디바이스에서 즉시 사용할 수 있는 다양한 CLI 매크로가 있습니다.

자주 수행하는 작업을 모니터링하기 위해 CLI 매크로를 생성할 수 있습니다. 자세한 내용은 새 명령에서 CLI 매크로 생성을 참조하십시오.

CLI 매크로는 시스템 정의 또는 사용자 정의입니다. 시스템 정의 매크로는 CDO에서 제공하며 편집하거나 삭제할 수 없습니다. 사용자 정의 매크로는 사용자가 생성하며 편집하거나 삭제할 수 있습니다.

Note 디바이스가 CDO에 온보딩된 후에만 디바이스에 대한 매크로를 생성할 수 있습니다.

ASA를 예로 들어 ASA 중 하나에서 특정 사용자를 찾으려면 다음 명령을 실행할 수 있습니다.

```
show running-config | grep username
```

명령을 실행할 때 사용자 이름을 검색할 사용자의 사용자 이름으로 대체합니다. 이 명령으로 매크로를 만들려면 동일한 명령을 사용하고 사용자 이름을 중괄호로 묶습니다.

```
> show running-config | grep {{username}}
```

매개변수의 이름은 원하는 대로 지정할 수 있습니다. 이 매개변수 이름을 사용하여 동일한 매크로를 생성할 수도 있습니다.

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

매개변수 이름은 설명적일 수 있으며 영숫자 문자와 밑줄을 사용해야 합니다. 이 경우 명령 구문은

```
show running-config | grep
```

명령의 일부이며 명령을 전송하는 디바이스에 대해 적절한 CLI 구문을 사용해야 합니다.

새 명령에서 CLI 매크로 생성

Procedure

단계 1 CLI 매크로를 생성하기 전에 CDO의 명령줄 인터페이스에서 명령을 테스트하여 명령 구문이 올바른지, 그리고 신뢰할 수 있는 결과를 반환하는지 확인합니다.

Note

단계 2 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 3 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 4 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.

단계 5 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 CLI 매크로 즐겨찾기 스타 ★를 클릭하여 이미 존재하는 매크로를 확인합니다.

단계 7 더하기 버튼  을 클릭합니다.

단계 8 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 9 **Command(**명령**)** 필드에 전체 명령을 입력합니다.

단계 10 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 11 **Create(**생성**)**를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 CLI 매크로 실행을 참조하십시오.

CLI 기록 또는 기존 CLI 매크로에서 CLI 매크로 생성

이 절차에서는 이미 실행한 명령, 다른 사용자 정의 매크로 또는 시스템 정의 매크로에서 사용자 정의 매크로를 생성합니다.

프로시저

단계 1 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

참고
CLI 기록에서 사용자 정의 매크로를 생성하려면 명령을 실행한 디바이스를 선택합니다. CLI 매크로는 동일한 계정의 디바이스 간에 공유되지만 CLI 기록은 공유되지 않습니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 온라인 및 동기화된 디바이스를 선택합니다.

단계 4 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 5 CLI 매크로를 만들려는 명령을 찾아 선택합니다. 다음 방법 중 하나를 사용합니다.

- 해당 디바이스에서 실행한 명령을 보려면 시계를 클릭합니다. 매크로로 전환할 항목을 선택하면 명령 창에 명령이 나타납니다.
- CLI 매크로 즐겨찾기 스타를 클릭하여 이미 존재하는 매크로를 확인합니다. 변경할 사용자 정의 또는 시스템 정의 CLI 매크로를 선택합니다. 명령 창에 명령이 나타납니다.

단계 6 명령 창의 명령을 사용하여 CLI 매크로 금색 별를 클릭합니다. 이 명령은 이제 새 CLI 매크로의 기본이 됩니다.

단계 7 매크로에 고유한 이름을 지정합니다. 원하는 경우 CLI 매크로에 대한 설명 및 참고 사항을 제공합니다.

단계 8 명령 필드에서 명령을 검토하고 원하는 대로 변경합니다.

단계 9 명령을 실행할 때 수정하려는 명령 부분을 중괄호로 묶인 매개변수 이름으로 교체합니다.

단계 10 **Create(**생성**)**를 클릭합니다. 생성한 매크로는 처음에 지정한 디바이스뿐만 아니라 해당 유형의 모든 디바이스에서 사용할 수 있습니다.

명령을 실행하려면 CLI 매크로 실행을 참조하십시오.

CLI 매크로 실행

Procedure

단계 1 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 적절한 디바이스 유형 탭을 클릭하고 하나 이상의 디바이스를 선택합니다.

단계 4 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

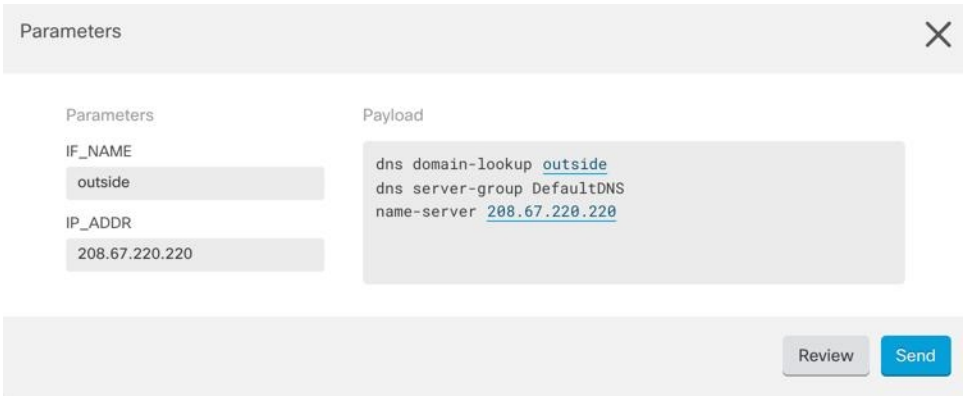
단계 5 명령 패널에서 별표를 클릭합니다.

단계 6 명령 패널에서 CLI 매크로를 선택합니다.

단계 7 다음 두 가지 방법 중 하나로 매크로를 실행합니다.

- 매크로에 정의할 매개변수가 없는 경우 **Send(**전송**)**를 클릭합니다. 명령에 대한 응답이 응답 창에 나타납니다. 다 됐습니다.
- 아래의 Configure DNS 매크로와 같은 매개변수가 매크로에 포함된 경우 **>_ View Parameters(**매개변수 보기**)**를 클릭합니다.

단계 **8** Parameters(매개변수) 창의 Parameters(매개변수) 필드에 매개변수 값을 입력합니다.



단계 **9** **Send(**보내기**)**를 클릭합니다. CDO가 성공적으로 명령을 전송하고 디바이스의 구성을 업데이트하면 완료됩니다!

단계 **10** 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

- **Write to Disk(**디스크에 쓰기**)**를 클릭하면 이 명령의 변경 사항과 실행 중인 구성의 다른 모든 변경 사항이 디바이스의 시작 구성에 저장됩니다.
- **Dismiss(**해제**)**를 클릭하면 메시지가 사라집니다.

CLI 매크로 편집

사용자 정의 CLI 매크로는 편집할 수 있지만 시스템 정의 매크로는 편집할 수 없습니다. CLI 매크로를 수정하면 모든 SSH 디바이스에 대해 변경됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 편집할 사용자 정의 매크로를 선택합니다.

단계 **7** 매크로 레이블에서 편집 아이콘을 클릭합니다.

단계 **8** Edit Macro(매크로 편집) 대화 상자에서 CLI 매크로를 편집합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

CLI 매크로를 실행하는 방법에 대한 지침은 CLI 매크로 실행를 참조하십시오.

CLI 매크로 삭제

사용자 정의 CLI 매크로는 삭제할 수 있지만 시스템 정의 매크로는 삭제할 수 없습니다. CLI 매크로를 삭제하면 모든 디바이스에서 삭제됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 디바이스를 선택합니다.

단계 **5** **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 삭제할 사용자 정의 CLI 매크로를 선택합니다.

단계 **7** CLI 매크로 레이블에서 휴지통 아이콘를 클릭합니다.

단계 **8** CLI 매크로를 제거할지 확인합니다.

CDO CLI 명령 결과 내보내기

독립형 디바이스 또는 여러 디바이스에 실행된 CLI 명령의 결과를 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다. 단일 디바이스 또는 여러 디바이스의 CLI 결과를 한 번에 내보낼 수 있습니다. 내보낸 정보에는 다음이 포함됩니다.

- 디바이스
- 날짜
- 사용자
- 명령
- 출력

CLI 명령 결과 내보내기

명령 창에서 방금 실행한 명령의 결과를 .csv 파일로 내보낼 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 디바이스를 선택하여 강조 표시하십시오.

단계 **5** 디바이스에 대한 **Device Actions(**디바이스 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 명령줄 인터페이스 창에서 명령을 입력하고 **Send(**보내기**)**를 클릭하여 디바이스에 명령을 실행합니다.

단계 **7** 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 **8** .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

CLI 매크로의 결과 내보내기

명령 창에서 실행된 매크로의 결과를 내보낼 수 있습니다. 하나 이상의 디바이스에서 실행된 CLI 매크로의 결과를 .csv 파일로 내보내려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 디바이스를 선택하여 강조 표시하십시오.

단계 **5** 디바이스에 대한 **Device Actions(**디바이스 작업**)** 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 를 선택합니다.

단계 **7** 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send(**보내기**)**를 클릭합니다.

단계 **8** 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 **9** .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

CLI 명령 기록 내보내기

다음 절차를 사용하여 하나 또는 여러 디바이스의 CLI 기록을 .csv 파일로 내보냅니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 디바이스를 선택하여 강조 표시하십시오.

단계 **5** 디바이스에 대한 디바이스 작업 창에서 >_**Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 **6** 아직 확장되지 않은 경우 시계 아이콘을 클릭하여 기록 창을 확장합니다.

단계 **7** 입력된 명령 창 오른쪽에서 내보내기 아이콘 를 클릭합니다.

단계 **8** .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다. .csv 파일에서 명령 출력을 읽을 때 모든 셀을 확장하여 명령의 모든 결과를 확인합니다.

관련 정보**:**

- CDO 명령줄 인터페이스, on page 122
- 새 명령에서 CLI 매크로 생성
- CLI 매크로 삭제
- CLI 매크로 편집
- CLI 매크로 실행
- 대량 명령줄 인터페이스

CLI 매크로 목록 내보내기

명령 창에서 실행된 매크로만 내보낼 수 있습니다. 다음 절차를 사용하여 하나 이상의 디바이스의 CLI 매크로를 .csv 파일로 내보냅니다.

프로시저

단계 1 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭합니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 디바이스를 선택하여 강조 표시하십시오.

단계 5 디바이스에 대한 디바이스 작업 창에서 **>_Command Line Interface(**명령줄 인터페이스**)**를 클릭합니다.

단계 6 CLI 창의 왼쪽 창에서 CLI 매크로 즐겨찾기 별표 ★를 선택합니다.

단계 7 내보낼 매크로 명령을 클릭합니다. 적절한 매개변수를 입력하고 **Send(**보내기**)**를 클릭합니다.

단계 8 입력된 명령 창 오른쪽에서 내보내기 아이콘  를 클릭합니다.

단계 9 .csv 파일에 설명이 포함된 이름을 지정하고 파일을 로컬 파일 시스템에 저장합니다.

디바이스 구성 변경 정보

디바이스를 관리하려면 CDO의 로컬 데이터베이스에 저장된 디바이스 구성의 자체 복사본이 있어야 합니다. CDO는 관리하는 디바이스에서 구성을 "읽을 때" 디바이스 구성의 복사본을 가져와 저장합니다. CDO가 디바이스 구성의 복사본을 처음 읽고 저장하는 경우는 디바이스가 온보딩될 때입니다. 이러한 선택 항목은 다양한 목적으로 구성을 읽는 것을 설명합니다.

- **Discard Changes(**변경 사항 취소**)**: 이 작업은 디바이스의 구성 상태가 "Not Synced(동기화되지 않음)"인 경우에 사용할 수 있습니다. Not Synced(동기화되지 않음) 상태에서는 CDO에서 보류 중인 디바이스의 구성에 대한 변경 사항이 있습니다. 이 옵션을 사용하면 보류 중인 모든 변경 사항을 취소할 수 있습니다. 보류 중인 변경 사항이 삭제되고 CDO가 디바이스에 저장된 구성의 복사본으로 구성의 복사본을 덮어씁니다.

- **Check for Changes(**변경 사항 확인**)**: 이 작업은 디바이스의 구성 상태가 동기화됨인 경우에 사용할 수 있습니다. Checking for Changes(변경 사항 확인)를 클릭하면 CDO가 디바이스의 구성 복사본을 디바이스에 저장된 구성의 복사본과 비교하게 됩니다. 차이가 있는 경우 CDO는 디바이스에 저장된 복사본으로 디바이스 구성의 복사본을 즉시 덮어씁니다.

- **Review Conflict(**충돌 검토**)** 및 **Accept Without Review(**검토 없이 수용**)**: 디바이스에서 Conflict Detection(충돌 탐지)을 활성화한 경우 CDO는 10분마다 디바이스의 구성 변경 사항을 확인합니다. 디바이스에 저장된 구성의 복사본이 변경된 경우 CDO는 "Conflict Detected(충돌 탐지됨)" 구성 상태를 표시하여 사용자에게 알립니다.

  - **Review Conflict(**충돌 검토**)**: 충돌 검토를 클릭하면 디바이스에서 직접 변경 사항을 검토하고 이를 수락하거나 거부할 수 있습니다.

- **Accept Without Review(**검토 없이 수용**)**: 이 작업은 CDO의 디바이스 구성 복사본을 디바이스에 저장된 구성의 최신 복사본으로 덮어씁니다. CDO에서는 덮어쓰기 작업을 수행하기 전에 구성의 두 복사본에서 차이점을 확인하라는 메시지를 표시하지 않습니다.

Read All(모두 읽기**)**: 대량 작업입니다. 상태에 상관없이 둘 이상의 디바이스를 선택하고 **Read All(**모두 읽기**)**을 클릭하여 CDO에 저장된 모든 디바이스의 구성을 디바이스에 저장된 구성으로 덮어쓸 수 있습니다.

- **Deploy Changes(**변경 구축**)**: 디바이스의 구성을 변경하면 CDO는 변경 사항을 구성의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 구축될 때까지 CDO에서 "보류 중"입니다. 디바이스에 구축되지 않은 설정 변경 사항이 있는 경우 디바이스는 동기화되지 않음 설정 상태가 됩니다.

  보류 중인 구성 변경 사항은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가 디바이스에 변경 사항을 구축한 후에야 적용됩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다. 구축은 단일 디바이스 또는 둘 이상의 디바이스에서 동시에 시작할 수 있습니다.

- **Discard All(**모두 취소**)**은 **Preview and Deploy(**미리보기 및 구축**)...**를 클릭한 후에만 사용할 수 있는 옵션입니다.. Preview and Deploy(미리보기 및 구축)를 클릭하면 CDO는 CDO에 보류 중인 변경 사항의 미리보기를 표시합니다. **Discard All(**모두 취소**)**을 클릭하면 CDO에서 보류 중인 모든 변경 사항이 삭제되며 선택한 디바이스에 어떤 것도 구축되지 않습니다. 위의 "변경 사항 취소"와 달리 보류 중인 변경 사항을 삭제하면 작업이 종료됩니다.

모든 디바이스 구성 읽기

CDO 외부의 디바이스에 대한 구성이 변경되면 CDO에 저장된 디바이스의 구성과 디바이스의 로컬 구성의 사본은 더 이상 동일하지 않습니다. 구성을 다시 동일하게 만들기 위해 디바이스에 저장된 구성으로 CDO의 디바이스 구성 복사본을 덮어쓰려는 경우가 많습니다. **Read All(**모두 읽기**)** 링크를 사용하여 여러 디바이스에서 동시에 이 작업을 수행할 수 있습니다.

CDO에서 디바이스 구성의 두 복사본을 관리하는 방법에 대한 자세한 내용은 디바이스 구성 변경 정보을 참조하십시오.

다음은 **Read All(**모두 읽기**)**을 클릭하면 CDO의 디바이스 구성 복사본을 디바이스의 구성 복사본으로 덮어쓰는 세 가지 구성 상태입니다.

- **Conflict Detected(**충돌 탐지**)** -충돌 탐지가 활성화된 경우 CDO는 구성 변경 사항에 대해 10분마다 관리하는 디바이스를 폴링합니다. CDO는 디바이스의 구성이 변경된 것을 발견하면 CDO는 디바이스에 대한 구성 상태를 "충돌 탐지됨"으로 표시합니다.

- **Synced(**동기화됨**)** -디바이스가 동기화된 상태인 경우 **Read All(**모두 읽기**)**을 클릭하면 CDO는 즉시 디바이스를 확인하여 구성이 직접 변경되었는지 확인합니다. **Read All(**모두 읽기**)**을 클릭하면 CDO는 디바이스 구성의 복사본을 덮어쓸 것임을 확인한 다음 CDO는 덮어쓰기를 수행합니다.

- **Not Synced(동기화되지 않음)** - 디바이스가 동기화되지 않음 상태인 경우 **Read All(모두 읽기)**을 클릭하면 CDO는 CDO를 사용하는 디바이스의 구성에 대해 보류 중인 변경 사항이 있으며 Read All(모두 읽기) 작업을 진행하면 해당 변경 사항이 삭제되고 디바이스의 구성이 포함된 CDO의 구성 복사본입니다. 이 Read All(모두 읽기)은 구성 변경 사항 취소와 같은 기능을 합니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(재고 목록)**를 클릭합니다.

단계 **2** **Devices(디바이스)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** (선택 사항) 변경 로그에서 이 대량 작업의 결과를 쉽게 식별할 수 있도록 변경 요청 관리을 생성합니다.

단계 **5** CDO를 저장할 디바이스를 선택합니다. CDO는 선택한 모든 디바이스에 적용할 수 있는 작업에 대해서만 명령 버튼을 제공합니다.

단계 **6** **Read All(모두 읽기)**을 클릭합니다.

단계 **7** CDO는 CDO에 준비된 구성 변경 사항이 있는 경우 선택한 디바이스에 대해 경고하고, 구성 대량 읽기 작업을 계속할 것인지 묻습니다. 계속하려면 **Read All(모두 읽기)**을 클릭합니다.

단계 **8** Read All(모두 읽기) 구성 작업의 진행 상황은 CDO에서 작업 모니터링에서 확인합니다. 대량 작업의 개별 작업이 성공하거나 실패한 방식에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 CDO에서 작업 모니터링 페이지로 이동합니다.

단계 **9** 변경 요청 레이블을 생성하고 활성화한 경우 실수로 다른 구성 변경 사항을 이 이벤트와 연결하지 않도록 레이블을 지워야 합니다.

관련 정보

- 디바이스 구성 변경 정보
- 구성 변경 사항 취소
- 구성 변경 사항 확인

Cisco IOS 또는 SSH에서 CDO로 변경 사항 읽기

Cisco IOS 또는 SSH 디바이스를 관리하려면 CDO에 디바이스 구성 파일의 저장된 복사본이 있어야 합니다. CDO가 디바이스 구성 파일의 복사본을 처음 읽고 저장하는 경우는 디바이스가 온보딩될 때입니다. 이후 CDO는 디바이스에서 구성을 확인할 때 디바이스 구성 파일의 복사본을 가져와 자체 데이터베이스에서 유지 관리하는 구성 파일의 복사본을 완전히 덮어씁니다. 자세한 내용은 디바이스 구성 변경 정보을 참조하십시오.

CDO 외부에서 Cisco IOS 또는 SSH 디바이스에 직접 변경된 사항을 감지하는 방법에 대한 자세한 내용은 구성 변경 사항 확인을 참조하십시오.

CDO에서 시작했지만 IOS 또는 SSH 디바이스에 구축하지 않은 구성 변경 사항을 "실행 취소"하는 방법을 알아보려면 구성 변경 사항 취소를 참조하십시오.

모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축

CDO는 테넌트의 디바이스에 대한 구성을 변경했지만 해당 변경 사항을 구축하지 않은 경우 구축 아이콘 에 주황색 점을 표시하여 알려줍니다. 이러한 변경의 영향을 받는 디바이스는 **Devices and Services(**디바이스 및 서비스**)** 페이지에서 "Not Synced(동기화되지 않음)" 상태로 표시됩니다. **Deploy(**구축**)**를 클릭하면 보류 중인 변경 사항이 있는 디바이스를 검토하고 해당 디바이스에 변경 사항을 구축할 수 있습니다.

참고 사용자가 생성하고 변경하는 모든 새로운 FDM 또는 FTD 네트워크 개체 또는 그룹에 대해 CDO는 CDO에서 관리하는 모든 온프레미스 방화벽 Management Center에 대해 이 페이지에서 항목을 생성합니다.

이 구축 방법은 지원되는 모든 디바이스에서 사용할 수 있습니다.

단일 구성 변경 사항에 이 구축 방법을 사용하거나, 기다렸다가 여러 변경 사항을 한 번에 구축할 수 있습니다.

프로시저

단계 **1** 화면의 오른쪽 상단에서 **Deploy(**구축**)** 아이콘 을 클릭합니다.

단계 **2** 구축하려는 변경 사항이 있는 디바이스를 선택합니다. 디바이스에 노란색 주의 삼각형이 있는 경우 해당 디바이스에 변경 사항을 구축할 수 없습니다. 노란색 주의 삼각형 위에 마우스를 올려놓으면 해당 디바이스에 변경 사항을 구축할 수 없는 이유를 확인할 수 있습니다.

단계 **3** (선택 사항) 보류 중인 변경 사항에 대한 자세한 정보를 보려면 **View Detailed Changelog(**자세한 변경 로그 보기**)** 링크를 클릭하여 해당 변경과 관련된 변경 로그를 엽니다. **Deploy(**구축**)** 아이콘을 클릭하여 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지로 돌아갑니다.

단계 **4** (선택 사항) **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에서 나가지 않고 변경 사항을 추적하려면 변경 요청 관리합니다.

단계 **5** 선택한 디바이스에 변경 사항을 즉시 구축하려면 **Deploy Now(**지금 구축**)**를 클릭합니다. 작업 트레이의 활성 작업 표시기에 진행 상황이 표시됩니다.

단계 **6** (선택 사항) 구축이 완료되면 CDO 탐색 모음에서 **Jobs(**작업**)**를 클릭합니다. 구축 결과를 보여주는 최근 "Deploy Changes(변경 사항 구축)" 작업이 표시됩니다.

단계 **7** 변경 요청 레이블을 생성했으며 더 이상 연결할 구성 변경 사항이 없는 경우 해당 레이블을 지웁니다.

다음에 수행할 작업

- 예약된 자동 구축 정보

디바이스 구성 대량 구축

예를 들어 공유 개체를 수정하여 여러 디바이스를 변경한 경우 해당 변경 사항을 영향을 받는 모든 디바이스에 한 번에 적용할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** CDO에서 구성을 변경한 모든 디바이스를 선택합니다. 이러한 디바이스는 "동기화되지 않음" 상태로 표시되어야 합니다.

단계 **5** 다음 방법 중 하나를 사용하여 변경 사항을 구축합니다.

- 화면 오른쪽 상단의 버튼을 클릭하여 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 창을 봅니다. 이렇게 하면 구축하기 전에 선택한 디바이스에서 보류 중인 변경 사항을 검토할 수 있습니다. **Deploy Now(**지금 구축**)**를 클릭하여 변경 사항을 구축합니다.

  Note
  Devices with Pending Changes(보류 중인 변경 사항이 있는 디바이스**)** 화면에서 디바이스 옆에 노란색 경고 삼각형이 표시되면 해당 디바이스에 변경 사항을 구축할 수 없습니다. 변경 사항을 해당 디바이스에 구축할 수 없는 이유에 대한 정보를 보려면 경고 삼각형 위에 마우스를 올려놓습니다.

- 세부 정보 창에서 **Deploy All(**모두 구축**)** 을 클릭합니다. 경고를 검토하고 **OK(**확인**)**를 클릭합니다. 대량 구축은 변경 사항을 검토하지 않고 즉시 시작됩니다.

단계 **6** (선택 사항) 탐색 모음에서 Jobs(작업) 아이콘  을 클릭하여 대량 구축의 결과를 확인합니다.

예약된 자동 구축 정보

CDO를 사용하면 CDO에서 관리하는 하나 이상의 디바이스에 대한 구성을 변경한 다음 편리한 시간에 해당 디바이스에 변경 사항을 배포하도록 예약할 수 있습니다.

Settings(설정) 페이지의 **Tenant Settings(**테넌트 설정**)** 탭에 자동 구축 예약 옵션 활성화, on page 48 있는 경우에만 배포을 예약할 수 있습니다. 이 옵션이 활성화되면 예약된 배포을 생성, 편집 또는 삭

제할 수 있습니다. 예약된 배포은 CDO에 저장된 모든 단계적 변경 사항을 설정된 날짜 및 시간에 배포합니다. Jobs(작업) 페이지에서 예약된 배포을 보고 삭제할 수도 있습니다.

CDO에서 디바이스 구성 변경 정보 않은 디바이스 변경 사항이 있는 경우 충돌이 해결될 때까지 예약된 구축을 건너뜁니다. 예약된 배포이 실패한 인스턴스가 Jobs(작업) 페이지에 나열됩니다. **Enable the Option to Schedule Automatic Deployments(**자동 구축 예약 옵션 활성화**)**가 해제된 경우 예약된 모든 구축이 삭제됩니다.

Caution 여러 디바이스에 대해 새 배포을 예약하는 경우 해당 디바이스 중 일부가 이미 배포을 예약한 경우, 새로 예약된 배포이 기존의 예약된 배포을 덮어씁니다.

Note 예약된 배포을 생성하면 디바이스의 표준 시간대가 아닌 현지 시간으로 일정이 생성됩니다. 예약된 배포은 일광 절약 시간에 맞게 자동으로 조정되지 않습니다.

자동 구축 예약

구축 일정은 단일 이벤트 또는 반복 이벤트일 수 있습니다. 반복 자동 구축을 사용하면 유지 보수 기간에 맞춰 반복 구축을 편리하게 이용할 수 있습니다. 단일 디바이스에 대해 일회성 또는 반복 구축을 예약하려면 다음 절차를 따르십시오.

Note 기존 구축이 예약된 디바이스에 대한 구축을 예약하는 경우 새로 예약된 구축이 기존 구축을 덮어씁니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 하나 이상의 디바이스를 선택합니다.

단계 **5** Device Details(디바이스 세부 정보) 창에서 Scheduled Deployments(예약된 구축) 탭을 찾아 **Schedule(**예약**)**을 클릭합니다.

단계 **6** 구축을 수행해야 하는 시기를 선택합니다.

- 일회성 구축의 경우 **Once on(**한 번**)** 옵션을 클릭하여 달력에서 날짜와 시간을 선택합니다.
- 반복 구축의 경우 **Every(**마다**)** 옵션을 클릭합니다. 매일 또는 일주일에 한 번 구축을 선택할 수 있습니다. 구축을 수행해야 하는 날짜와 시간을 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

예약된 배포 편집

예약된 배포를 편집하려면 다음 절차를 따르십시오.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.
단계 **4** 하나 이상의 디바이스를 선택합니다.
단계 **5** **Device Details(**디바이스 세부 정보**)** 창에서 예약된 배포 탭을 찾아 **Edit(**편집**)**를 클릭합니다.

단계 **6** 예약된 배포의 반복, 날짜 또는 시간을 편집합니다.
단계 **7** **Save(**저장**)**를 클릭합니다.

예약된 배포 삭제

예약된 배포를 삭제하려면 다음 절차를 따르십시오.

Note 여러 디바이스에 대한 배포를 예약한 다음 일부 디바이스에 대한 일정을 변경하거나 삭제하면 나머지 디바이스에 대한 원래 예약된 배포가 유지됩니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.
단계 **4** 하나 이상의 디바이스를 선택합니다.
단계 **5** **Device Details(**장치 세부 정보**)**창에서 예약된 배포 탭을 찾아 **Delete(**삭제**)**를 클릭합니다.

What to do next

- 디바이스 구성 변경 정보
- 모든 디바이스 구성 읽기, on page 136
- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 138

구성 변경 사항 확인

디바이스의 구성이 디바이스에서 직접 변경되었으며 CDO에 저장된 구성의 복사본과 더 이상 동일하지 않은지 확인하려면 변경 사항을 확인합니다. 디바이스가 "Synced(동기화됨)" 상태일 때 이 옵션이 표시됩니다.

변경 사항을 확인하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 구성이 디바이스에서 직접 변경되었을 가능성이 있는 디바이스를 선택합니다.

단계 **5** 오른쪽의 Synced(동기화) 창에서 **Check for Changes(**변경 사항 확인**)**를 클릭합니다.

단계 **6** 다음 동작은 디바이스에 따라 약간 다릅니다.

- 디바이스의 경우 디바이스의 구성이 변경된 경우 다음 메시지가 표시됩니다.

  디바이스에서 정책을 읽는 중입니다. 디바이스에 활성 구축이 있는 경우 완료 후 읽기가 시작됩니다.

  - 계속하려면 **OK(**확인**)**를 클릭하십시오. 디바이스의 구성이 CDO에 저장된 구성을 덮어씁니다.
  - 작업을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

- SSH 디바이스의 경우:

a. 표시되는 두 가지 구성을 비교합니다. **Continue(**계속**)**를 클릭합니다. **Last Known Device Configuration(**마지막으로 알려진 디바이스 구성**)** 레이블이 지정된 구성은 CDO에 저장된 구성입니다. **Found on Device(**디바이스에서 발견**)** 레이블이 지정된 구성은 ASA에 저장된 구성입니다.

b. 다음 중 하나를 선택합니다.

1. "마지막으로 알려진 디바이스 구성"을 유지하려면 대역 외 변경 사항을 거부합니다.
2. 대역 외 변경 사항을 수락하여 CDO에 저장된 디바이스의 구성을 디바이스에 있는 구성으로 덮어씁니다.

c. **Continue(**계속**)**를 클릭합니다.

구성 변경 사항 취소

CDO를 사용하여 디바이스의 구성에 적용한 구축 해제된 구성 변경 사항을 모두 "실행 취소"하려면 **Discard Changes(**변경 사항 취소**)**를 클릭합니다. **Discard Changes(**변경 사항 취소**)**를 클릭하면 CDO는 디바이스 구성의 로컬 복사본을 디바이스에 저장된 구성으로 완전히 덮어씁니다.

Discard Changes(변경 사항 취소**)**를 클릭하면 디바이스의 구성 상태가 **Not Synced(**동기화되지 않음**)** 상태가 됩니다. 변경 사항을 취소하면 CDO의 구성 복사본이 디바이스의 구성 복사본과 동일하게 되며 CDO의 구성 상태는 Synced(동기화)로 돌아갑니다.

디바이스에 대해 구축되지 않은 모든 구성 변경 사항을 취소하거나 "실행 취소"하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 구성을 변경한 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Not Synced(**동기화되지 않음**)** 창에서 **Discard Changes(**변경 사항 취소**)**를 클릭합니다.

- FDM 관리 디바이스의 경우 CDO는 "CDO에서 보류 중인 변경 사항이 취소되고 이 디바이스에 대한 CDO 구성이 디바이스에서 현재 실행 중인 구성으로 교체됩니다."라고 경고합니다. 변경 사항을 취소하려면 **Continue(**계속**)**를 클릭합니다.
- Meraki 디바이스의 경우 CDO가 변경 사항을 즉시 삭제합니다.
- AWS 디바이스의 경우 CDO는 삭제하려는 항목을 표시합니다. **Accept(**수락**)** 또는 **Cancel(**취소**)**을 클릭합니다.

디바이스의 대역 외 변경 사항

대역 외 변경 사항은 CDO를 사용하지 않고 디바이스에서 직접 변경한 사항을 의미합니다. 이러한 변경은 SSH 연결을 통해 디바이스의 명령줄 인터페이스를 사용하거나 ASA용 ASDM(Adaptive Security Device Manager), FDM 관리디바이스용 또는온프레미스 방화벽 Management Center사용자 인터페이스의 온프레미스 방화벽 Management Center용 FDM과 같은 로컬 관리자를 사용하여 수행할 수 있습

니다. 대역 외 변경 사항은 CDO에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

디바이스에서 대역외 변경 탐지

ASA 또는 FDM 관리 디바이스, Cisco IOS 디바이스 또는 온프레미스 방화벽 Management Center에 대해 Conflict Detection(충돌 탐지)이 활성화된 경우 CDO는 10분마다 디바이스를 확인하여 CDO외부에서 디바이스의 구성에 직접 적용된 새로운 변경 사항을 검색합니다.

CDO에 저장되지 않은 디바이스 구성 변경 사항이 있음을 발견하면 CDO는 해당 디바이스의 구성 상태를 "충돌 탐지됨" 상태로 변경합니다.

CDO에서 충돌을 탐지하는 경우 다음 두 가지 조건 중 하나가 발생할 수 있습니다.

- CDO의 데이터베이스에 저장되지 않은 디바이스에 직접 적용된 구성 변경 사항이 있습니다.
- FDM 관리 디바이스의 경우 구축되지 않은 FDM 관리 디바이스에 "보류 중인" 구성 변경 사항이 있을 수 있습니다.
- 온프레미스 방화벽 Management Center의 경우, 예를 들어 CDO 외부의 개체에 변경 사항이 있어 CDO와의 동기화를 위해 보류 중이거나CDO에서 변경 사항이 있어 온프레미스 방화벽 Management Center에 구축하기 위해 보류 중일 수 있습니다.

CDO와 디바이스 간 구성 동기화

구성 충돌 정보

Security Devices(보안 디바이스**)** 페이지에서 디바이스 또는 서비스의 상태가 "Synced(동기화됨)", "Not Synced(동기화되지 않음)" 또는 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. CDO를 사용하여 관리하는 온프레미스 방화벽 Management Center의 상태를 확인하려면 **Tools & Services(**도구 및 서비스**)** > **Firewall Management Center**로 이동하십시오.

- 디바이스가 동기화되면 CDO의 구성과 디바이스에 로컬로 저장된 구성이 동일합니다.
- 디바이스가 동기화되지 않으면 CDO에 저장된 구성이 변경되어 이제 디바이스에 로컬로 저장된 구성과 다릅니다. CDO에서 디바이스로 변경 사항을 구축하면 CDO의 버전과 일치하도록 디바이스의 구성이 변경됩니다.
- CDO 외부에서 디바이스에 적용된 변경 사항을 대역 외 변경 사항이라고 합니다. 대역 외 변경이 수행되면 디바이스에 대해 충돌 탐지가 활성화된 경우 디바이스 상태가 "Conflict Detected(충돌 탐지됨)"로 변경됩니다. 대역 외 변경 사항을 수락하면 는 CDO의 구성을 디바이스의 구성과 일치하도록 변경합니다.

충돌 탐지

충돌 탐지가 활성화된 경우 CDO는 기본 간격 동안 디바이스를 폴링하여 CDO 외부에서 디바이스의 구성이 변경되었는지 확인합니다. CDO는 변경 사항을 탐지하면 디바이스의 구성 상태를 **Conflict Detected(**충돌 탐지됨**)**로 변경합니다. CDO 외부에서 디바이스에 적용된 변경 사항을 "대역 외" 변경 사항이라고 합니다.

CDO에서 관리하는 온프레미스 방화벽 Management Center의 경우, 준비되는 변경 사항이 있고 디바이스가 **Not Synced(**동기화되지 않음**)** 상태이면 CDO는 디바이스 폴링을 중지하여 변경 사항을 확인합니다. CDO 외부에서 이루어진 변경 사항 중 CDO와의 동기화를 위해 보류 중인 변경 사항과 CDO에서 수행된 변경 사항 중 온프레미스 방화벽 Management Center에 구축되기 위해 보류 중인 사항이 있는 경우, CDO는 온프레미스 방화벽 Management Center이 **Conflict Detected(**충돌 탐지됨**)** 상태임을 선언합니다.

이 옵션이 활성화되면 디바이스별로 충돌 또는 OOB 변경 사항이 탐지되는 빈도를 구성할 수 있습니다. 자세한 내용은 디바이스 변경 사항에 대한 폴링 예약, on page 149를 참조하십시오.

충돌 탐지 활성화

충돌 탐지를 활성화하면 CDO 외부에서 디바이스가 변경된 경우 인스턴스에 알림이 표시됩니다.

Procedure

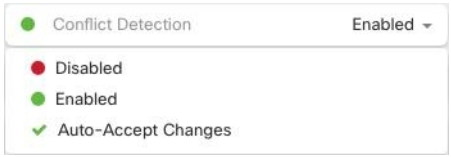
단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 선택합니다.

단계 **4** 충돌 탐지를 활성화할 디바이스를 선택합니다.

단계 **5** 디바이스 테이블 오른쪽에 있는 충돌 감지 상자의 목록에서 **Enabled(**활성화됨**)**을 선택합니다.



디바이스에서 대역외 변경 사항 자동 수락

변경 사항 자동 수락을 활성화하여 매니지드 디바이스에 대한 직접 변경 사항을 자동으로 수락하도록 CDO를 구성할 수 있습니다. CDO를 사용하지 않고 디바이스에 직접 적용된 변경 사항을 대역 외

변경 사항이라고 합니다. 대역 외 변경은 CDO에 저장된 디바이스의 구성과 디바이스 자체에 저장된 구성 간에 충돌을 일으킵니다.

자동 수락 변경 기능은 충돌 탐지를 개선한 것입니다. 디바이스에서 변경 사항 자동 수락이 활성화된 경우 CDO는 10분마다 변경 사항을 확인하여 디바이스의 구성에 대한 대역 외 변경 사항이 있는지 확인합니다. 구성이 변경된 경우 CDO는 사용자에게 확인 상자를 표시하지 않고 디바이스 구성의 로컬 버전을 자동으로 업데이트합니다.

CDO에서 아직 디바이스에 구축되지 않은 구성 변경 사항이 있는 경우 CDO는 구성 변경을 자동으로 수락하지 않습니다. 화면의 프롬프트에 따라 다음 작업을 결정합니다.

자동 수락 변경 사항을 사용하려면 먼저 테넌트가 **Security Devices(**보안 디바이스**)** 페이지의 Conflict Detection(충돌 탐지) 메뉴에서 자동 수락 옵션을 표시하도록 활성화합니다. 그런 다음 개별 디바이스에 대한 변경 사항 자동 수락을 활성화합니다.

CDO가 대역 외 변경 사항을 탐지하지만 수동으로 수락하거나 거부할 수 있는 옵션을 제공하도록 하려면 대신 충돌 탐지, on page 145를 활성화합니다.

변경 사항 자동 수락 구성

Procedure

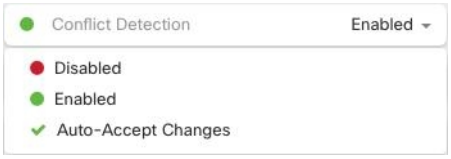
단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 **2** 왼쪽 창에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 클릭합니다.

단계 **3** **Tenant Settings(**테넌트 설정**)** 영역에서, 토글을 클릭하여 디바이스 변경 사항을 자동으로 수락하는 옵션 활성화로 전환합니다. 이렇게 하면 변경 사항 자동 수락 메뉴 옵션이 **Security Devices(**보안 디바이스**)** 페이지의 충돌 감지 메뉴에 표시됩니다.

단계 **4** 왼쪽 창에서 보안 디바이스을 클릭하고 대역 외 변경 사항을 자동으로 수락할 디바이스를 선택합니다.

단계 **5** **Conflict Detection(**충돌 감지**)** 메뉴의 드롭다운 메뉴에서 **Auto-Accept Changes(**변경 사항 자동 수락**)**을 선택합니다.



테넌트의 모든 디바이스에 대한 변경 사항 자동 수락 비활성화

Procedure

단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 **2** 왼쪽 창에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**를 클릭합니다.

단계 **3** **Tenant Settings(**테넌트 설정**)** 영역에서 회색 X가 표시되도록 토글을 왼쪽으로 밀어 "디바이스 변경 사항을 자동으로 수락하는 옵션 활성화"를 비활성화합니다. 이렇게 하면 충돌 감지 메뉴에서 변경 사항 자동 수락 옵션이 비활성화되고 테넌트의 모든 디바이스에 대한 기능이 비활성화 됩니다.

Note
"자동 수락"을 비활성화하면 CDO에 수락하기 전에 각 디바이스 충돌을 검토해야 합니다. 여기에는 이전에 변경 사항을 자동으로 수락하도록 구성된 디바이스가 포함됩니다.

구성 충돌 해결

이 섹션에서는 디바이스에서 발생하는 구성 충돌을 해결하는 방법에 대한 정보를 제공합니다.

동기화되지 않음 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

Procedure

단계 **1** 내비게이션 바에서 **Inventory(**재고 목록**)**를 클릭합니다.

Note
온프레미스 방화벽 Management Center의 경우, **Tools & Services(**도구 및 서비스**)** > **Firewall Management Center**로 이동하여 **Not Synced(**동기화되지 않음**)** 상태인 FMC를 선택하고 5단계부터 계속 진행합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

단계 **5** 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- 미리보기 및 배포... - CDO에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 한 번에 여러 변경 사항을 기다렸다가 배포하십시오.
- 변경 사항 취소 - CDO에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 CDO에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 CDO에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.

충돌 탐지됨 상태 해결

CDO를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. 충돌 탐지, on page 145이 활성화되어 있고 CDO를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected(**충돌 탐지됨**)**로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 내비게이션 바에서 **Inventory(**재고 목록**)**를 클릭합니다.

Note
온프레미스 방화벽 Management Center의 경우, **Tools & Services(**도구 및 서비스**)** > **Firewall Management Center**로 이동하여 **Not Synced(**동기화되지 않음**)** 상태인 FMC를 선택하고 5단계부터 계속 진행합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict(**충돌 검토**)**를 클릭합니다.

단계 **5** **Device Sync(**디바이스 동기화**)** 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.

- "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 CDO에 저장된 디바이스 구성입니다.
- "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.

단계 **6** 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes(**디바이스 변경 사항 수락**)**: 구성 및 CDO에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

  Note

CDO는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 구축하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review(**검토 없이 수락**)**를 선택하는 것입니다.

- **Reject Device Changes(**디바이스 변경 거부**)**: 디바이스에 저장된 구성을 CDO에 저장된 구성으로 덮어씁니다.

Note
거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

디바이스 변경 사항에 대한 폴링 예약

충돌 탐지, on page 145를 활성화했거나 Settings(설정) 페이지에서 **Enable device changes to auto-accept device changes(**디바이스 변경 자동 수락 옵션 활성화**)**를 선택한 경우 CDO은 기본 간격 동안 디바이스를 폴링하여 CDO 외부에서 디바이스의 구성이 변경되었는지 확인합니다. CDO가 디바이스별로 변경 사항을 폴링하는 빈도를 맞춤화할 수 있습니다. 이러한 변경 사항은 둘 이상의 디바이스에 적용할 수 있습니다.

디바이스에 대해 구성된 선택 항목이 없으면 "테넌트 기본값"에 대한 간격이 자동으로 구성됩니다.

Note **Security Devices(**보안 디바이스**)** 페이지에서 디바이스별 간격을 맞춤 설정하면 **General Settings(**일반 설정**)** 페이지에서 기본 충돌 탐지 간격로 선택한 폴링 간격이 재정의됩니다.

Security Devices(보안 디바이스**)** 페이지에서 **Conflict Detection(**충돌 탐지**)**을 활성화하거나 Settings(설정) 페이지에서 디바이스 변경 사항을 자동 수락하는 옵션을 활성화한 후 다음 절차를 사용하여 CDO가 디바이스를 폴링할 빈도를 예약합니다.

Procedure

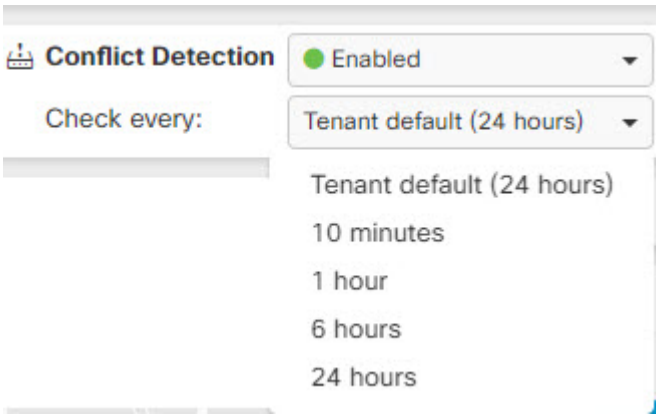
단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

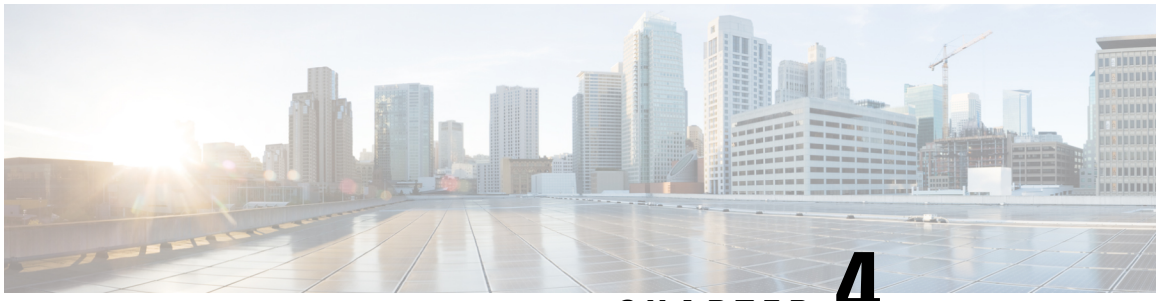
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌 탐지를 활성화할 디바이스를 선택합니다.

단계 **5** **Conflict Detection(**충돌 탐지**)**과 동일한 영역에서 **Check every(**확인 간격**)**의 드롭다운 메뉴를 클릭하고 원하는 폴링 간격을 선택합니다.


Conflict Detection
Enabled
Check every:
Tenant default (24 hours)
Tenant default (24 hours)
10 minutes
1 hour
6 hours
24 hours



CHAPTER 4

변경 로그, 워크플로우 및 작업 모니터링 및 보고

CDO는 구성 변경 로그, 대량 디바이스 작업, 디바이스와 통신할 때 실행되는 프로세스를 효과적으로 모니터링합니다. 이를 통해 네트워크의 기존 정책이 보안 상태에 어떤 영향을 미치는지 파악할 수 있습니다.

CDO에서 변경 로그 관리

변경 로그는 CDO에서 수행한 구성 변경 사항을 캡처하여, 지원되는 모든 디바이스 및 서비스의 변경 사항을 포함하는 단일 보기를 제공합니다. 다음은 변경 로그의 몇 가지 기능입니다.

- 디바이스 구성에 대한 변경 사항을 나란히 비교하여 제공합니다.
- 모든 변경 로그 항목에 대한 레이블을 제공합니다.
- 디바이스의 온보딩 및 제거를 기록합니다.
- CDO 외부에서 발생하는 정책 변경 충돌을 탐지합니다.
- 인시던트 조사 또는 문제 해결 중에 누가, 무엇을, 언제 하는지에 대한 답변을 제공합니다.
- 전체 변경 로그 또는 일부만 CSV 파일로 다운로드할 수 있습니다.

로그 용량 변경 관리

CDO는 변경 로그 정보를 1년 동안 보관하고 1년이 지난 데이터는 삭제합니다.

CDO의 데이터베이스에 저장된 변경 로그 정보와 내보낸 변경 로그에 표시되는 변경 로그 정보에는 차이가 있습니다. 자세한 내용은 변경 로그 내보내기, on page 153를 참조하십시오.

변경 로그 항목

변경 로그 항목은 단일 디바이스 구성의 변경 사항, 디바이스에서 수행된 작업 또는 CDO 외부에서 디바이스에 이루어진 변경 사항을 반영합니다.

- 구성 변경 내용이 포함된 변경 로그 항목의 경우 해당 행의 아무 곳이나 클릭하여 변경 내용에 대한 세부 정보를 볼 수 있습니다.
- CDO 외부에서 이루어진 대역 외 변경이 충돌로 감지되는 경우 시스템 사용자가 마지막 사용자로 보고됩니다.
- CDO의 디바이스 구성이 디바이스의 구성과 동기화된 후 또는 디바이스가 CDO에서 제거되면 CDO는 변경 로그 항목을 닫습니다. 구성은 디바이스에서 CDO로 구성을 읽거나 CDO에서 디바이스로 구성을 구축한 후에 동기화된 것으로 간주됩니다.
- CDO는 변경의 성공 여부와 관계없이 기존 항목을 완료한 후 즉시 새 변경 로그 항목을 만듭니다. 새 변경 로그 항목이 열리면 추가 구성 변경 사항이 추가됩니다.
- 디바이스에 대한 읽기, 구축 및 삭제 작업에 대한 이벤트가 표시됩니다. 이러한 작업은 디바이스의 변경 로그를 닫습니다.
- (읽기 또는 구축을 통해) CDO가 디바이스의 구성과 동기화된 후에 또는 CDO가 더 이상 디바이스를 관리하지 않는 경우 변경 로그가 닫힙니다.
- CDO 외부에서 디바이스를 변경하면 변경 로그에 "충돌 감지됨" 항목이 포함됩니다.

보류 중 및 완료된 변경 로그 항목

변경 로그의 상태는 보류 중 또는 완료 중 하나입니다. CDO를 사용하여 디바이스의 구성을 변경하면 이러한 변경 사항은 보류 중인 변경 로그 항목에 기록됩니다. 다음 활동으로 보류 중인 변경 로그가 완성되고, 그 후에는 향후 변경 사항을 기록하기 위한 새 변경 로그가 만들어집니다.

- 디바이스에서 CDO로 구성을 읽기
- CDO에서 디바이스로 변경 사항 구축
- CDO에서 디바이스 삭제
- 실행 중인 구성 파일을 업데이트하는 CLI 명령 실행

변경 로그 항목 검색 및 필터링

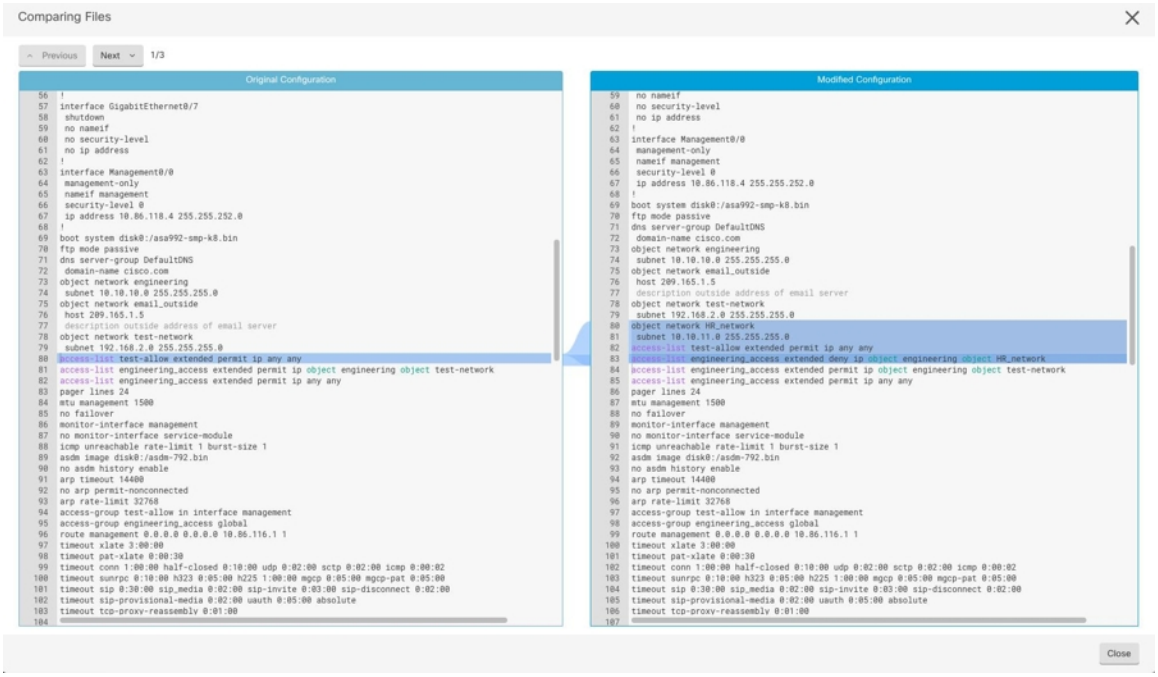
변경 로그 항목을 검색하고 필터링할 수 있습니다. 검색 필드를 사용하여 이벤트를 찾습니다. 필터( )를 사용하여 지정한 기준에 맞는 항목을 찾습니다. 변경 로그를 필터링하고 검색 필드에 키워드를 추가하여 필터링된 결과 내에서 항목을 찾는 방식으로 두 작업을 결합할 수도 있습니다.

변경 로그 차이점 보기

변경 로그에서 파란색 **Diff**를 클릭하면 디바이스의 실행 중인 구성 파일에서 변경 사항을 나란히 비교할 수 있습니다.

다음 그림에서 **Original Configuration(**원래 구성**)** 열은 ASA에 변경 사항을 기록하기 전에 실행 중인 구성 파일입니다. **Modified Configuration(**수정된 구성**)** 열에는 변경 사항이 작성된 후 실행 중인 구성 파일이 표시됩니다. 이 경우 원래 구성 열은 실행 중인 구성 파일의 행을 강조 표시하며, 이 행은 변경되지 않지만 수정된 구성 열에서 참조할 수 있는 지점을 제공합니다.

왼쪽 열에서 오른쪽 열로 가로지르는 선을 따라가면 엔지니어링 네트워크의 주소가 *HR_network* 네트워크의 주소에 도달하지 못하도록 하는 액세스 규칙과 *HR_network* 개체가 추가되는 것을 확인할 수 있습니다. **Previous(**이전**)** 및 **Next(**다음**)**를 클릭하여 파일의 변경 사항으로 이동합니다.



관련 주제

- CDO에서 변경 로그 관리, on page 151

변경 로그 내보내기

CDO 변경 로그 전체 또는 하위 집합을 쉼표로 구분된 값(.csv) 파일로 내보내 원하는 대로 정보를 필터링하고 정렬할 수 있습니다.

변경 로그를 .csv 파일로 내보내려면 다음 절차를 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 다음 작업 중 하나를 수행하여 내보낼 변경 사항을 찾습니다.

- 필터( ) 및 검색 필드를 사용하여 내보낼 항목을 찾습니다. 예를 들어 디바이스를 기준으로 필터링하면 선택한 디바이스에 대한 변경 사항만 표시됩니다.
- 변경 로그에서 모든 필터 및 검색 기준을 지웁니다. 이렇게 하면 전체 변경 로그를 내보낼 수 있습니다.

Note
CDO는 1년간의 변경 로그 데이터를 보관합니다. 1년 동안의 전체 변경 로그 기록을 다운로드하는 것보다 변경 로그 내용을 필터링하여 그 결과를 .csv 파일로 다운로드하는 것이 좋습니다.

단계 **3** 페이지 오른쪽 상단에 있는 내보내기 아이콘을 클릭합니다.

단계 **4** .csv 파일을 설명이 포함된 이름과 함께 로컬 파일 시스템에 저장합니다.

CDO의 변경 로그 용량과 내보낸 변경 로그 크기의 차이

CDO의 변경 로그 페이지에서 내보내는 정보는 CDO가 데이터베이스에 저장하는 변경 로그 정보와 다릅니다.

모든 변경 로그에 대해 CDO는 두 개의 디바이스 구성 사본을 저장합니다. 하나는 시작 구성이고, 다른 하나는 닫힌 변경 로그의 경우 종료 구성 또는 열린 변경 로그의 경우 현재 구성입니다. 이를 통해 CDO는 구성 차이를 나란히 표시할 수 있습니다. 또한 CDO는 변경한 사용자 이름, 변경한 시간 및 기타 세부 정보와 함께 모든 단계 (변경 이벤트)를 추적하고 저장합니다.

그러나 변경 로그를 내보낼 때 구성의 전체 사본 두 개가 내보내기에 포함되지 않습니다.두 여기에는 내보내기 파일이 변경 로그 CDO가 저장하는 것보다 훨씬 작은 변경 이벤트만 포함됩니다.

CDO는 변경 로그 정보를 1년 동안 저장합니다. 여기에는 두 개의 구성 사본이 포함됩니다.

변경 요청 관리

변경 요청 관리는 변경 요청과 그 비즈니스 정당성을 변경 로그 이벤트에 연결할 수 있습니다. 변경 요청은 서드파티 티켓팅 시스템에서 열립니다.

변경 요청 관리를 사용하여 CDO에서 변경 요청을 생성하고 변경 로그 이벤트와 연결합니다. 변경 로그 내에서 이름으로 이 변경 요청을 검색할 수 있습니다.

Note CDO에서 변경 요청 추적과 변경 요청 관리는 동일한 기능을 의미합니다.

변화 요청 관리 활성화

변경 요청 추적을 활성화하면 테넌트의 모든 사용자에게 영향을 미칩니다.

Procedure

단계 **1** 왼쪽 창에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**을 클릭합니다.

단계 **2** **Change Request Tracking(**변경 요청 추적**)** 토글 버튼 활성화 

이 기능을 활성화하면 변경 요청 메뉴가 왼쪽 하단에 나타나고 변경 로그 페이지에서 변경 요청 드롭다운 목록을 사용할 수 있습니다.

변경 요청 생성

Procedure

단계 **1** CDO에서 왼쪽 하단의 **Change Request** (변경 요청) 메뉴에서 변경 요청 생성(+) 아이콘을 클릭합니다.

단계 **2** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

Name(이름**)**이 조직에서 사용하려는 **Change Request(**변경 요청**)** 이름과 일치하는지, **Description(**설명**)**에 변경의 목적이 설명되어 있는지 확인합니다.

Note
Change Request(변경 요청**)**을 생성한 후에는 이름을 변경할 수 없습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

Note
Change Request(변경 요청**)**이 저장되면 CDO은 모든 새 변경 사항을 해당 **Change Request(**변경 요청**)** 이름에 연결합니다. 이 연결은 변화 요청 관리 비활성화하거나 메뉴에서 변경 요청 툴바 지우기 때까지 계속됩니다.

변경 요청을 변경 로그 이벤트와 연결

Procedure

단계 **1** 왼쪽 창에서 **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 변경 로그를 확장하여 변경 요청과 연결하려는 이벤트를 확인합니다.

단계 **3** 해당 변경 로그 항목 옆에 있는 드롭다운 목록을 클릭합니다.

Note
최신 변경 요청은 변경 요청 목록 상단에 표시됩니다.

단계 **4** 변경 요청을 선택하고 **Select(**선택**)**을 클릭합니다.

변경 요청으로 변경 로그 이벤트 검색

Procedure

단계 **1** 왼쪽 창에서 **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 이름을 입력합니다.

CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

변경 요청 검색

Procedure

단계 **1** CDO에서 왼쪽 하단의 **Change Request** (변경 요청) 메뉴에서 변경 요청 생성(+) 아이콘을 클릭합니다.

단계 **2** 검색 필드에 **Change Request(**변경 요청**)**의 이름 또는 관련 키워드를 입력합니다. 값을 입력하면 입력한 내용과 부분적으로 일치하는 결과가 이름 및 설명 필드에 모두 표시됩니다.

변경 요청 필터링

Procedure

단계 **1** 왼쪽 창에서 **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 모든 옵션을 보려면 필터 아이콘을 클릭합니다.

단계 **3** 검색 필드에 **Change Request(**변경 요청**)**의 이름을 입력합니다.

값을 입력하면 입력한 값과 부분적으로 일치하는 결과가 표시됩니다.

단계 **4** 해당 체크 박스 을 선택 하여 변경 요청 을 선택합니다.

일치하는 항목은 **Change Log(**변경 로그**)** 테이블에 표시됩니다. CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.

변경 요청 툴바 지우기

변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하려면 변경 요청 도구 모음에서 정보를 지우십시오.

Procedure

단계 **1** CDO에서 왼쪽 하단의 **Change Request** (변경 요청) 메뉴에서 변경 요청 생성(+) 아이콘을 클릭합니다.

단계 **2** **Clear(**지우기**)**를 클릭합니다.

이제 변경 요청 메뉴에 **None(**없음**)**이 표시됩니다.

변경 로그 이벤트와 관련된 변경 요청 지우기

Procedure

단계 **1** 왼쪽 창에서 **Change Log(**변경 로그**)**를 클릭합니다.

단계 **2** 변경 로그를 확장하여 변경 요청에서 연결 해제하려는 이벤트를 표시합니다.

단계 **3** 해당 변경 로그 항목 옆에 있는 드롭다운 목록을 클릭합니다.

단계 **4** **Clear(**지우기**)**를 클릭합니다.

변경 요청 삭제

변경 요청을 삭제하면 변경 요청 목록에서는 삭제되지만 변경 로그에서는 삭제되지 않습니다.

Procedure

단계 **1** 왼쪽 하단의 변경 요청 메뉴에서 변경 요청 생성(+) 아이콘을 클릭합니다.
단계 **2** 변경 요청 을 선택하고 저장소 아이콘을 클릭하여 삭제합니다.
단계 **3** 확인 표시를 클릭하여 확인합니다.

변화 요청 관리 비활성화

Change Request Management(변경 요청 관리**)**를 비활성화하거나 **Change Request Tracking(**변경 요청 추적**)**을 비활성화하면 계정의 모든 사용자에게 영향을 미칩니다.

Procedure

단계 **1** 왼쪽 창에서 **Settings(**설정**)** > **General Settings(**일반 설정**)**을 클릭합니다.
단계 **2** **Change Request Tracking(**변경 요청 추적**)** 토글 버튼 비활성화

변경 요청 관리 사용 사례

이 사용 사례에서는 변경 요청 관리를 활성화했다고 가정합니다.

외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스에 적용된 변경 사항을 추적

이 활용 사례 에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스를 변경하고 이러한 방화벽 변경에서 발생하는 변경 로그 이벤트를 변경 요청 에 연결하려는 시나리오에 대해 설명합니다. 변경 요청을 생성하고 변경 로그 이벤트를 연결하려면 다음 절차를 따르십시오.

1. 변경 요청 생성, on page 155.
2. 외부 시스템의 티켓 이름이나 번호를 변경 요청의 이름으로 사용하고 설명 필드에 변경의 정당성 및 기타 관련 정보를 추가합니다.
3. 변경 요청 도구 모음에 새 변경 요청이 표시되는지 확인합니다.

4. 방화벽 디바이스를 변경합니다.
5. 탐색창에서 변경 로그를 클릭하고 새 변경 요청과 연결된 변경 로그 이벤트를 찾습니다.
6. 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하기 위한 변경 요청 툴바 지우기, on page 157.

방화벽 디바이스 변경 후 개별 변경 로그 이벤트 수동 업데이트

이 사용 사례에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 방화벽 디바이스를 변경했지만 변경 요청 관리 기능을 사용하여 변경 요청을 변경 로그 이벤트와 연결하는 것을 잊어버린 시나리오를 설명합니다. 티켓 번호로 변경 로그 이벤트를 업데이트하려고 합니다. 변경 요청을 변경 로그 이벤트와 연결하려면 다음 절차를 따르십시오.

1. 변경 요청 생성, on page 155. 외부 시스템의 티켓 이름 또는 번호를 변경 요청 이름으로 사용합니다. 설명 필드를 사용하여 변경 및 기타 관련 정보에 대한 근거를 추가합니다.
2. 탐색창에서 **Change Log(**로그 변경**)**를 클릭하고 변경 사항과 관련된 변경 로그 이벤트를 검색합니다.
3. 변경 요청을 변경 로그 이벤트와 연결, on page 156.
4. 변경 로그 이벤트가 기존 변경 요청과 자동으로 연결되지 않도록 하기 위한 변경 요청 툴바 지우기, on page 157.

변경 요청과 관련된 변경 로그 이벤트 검색

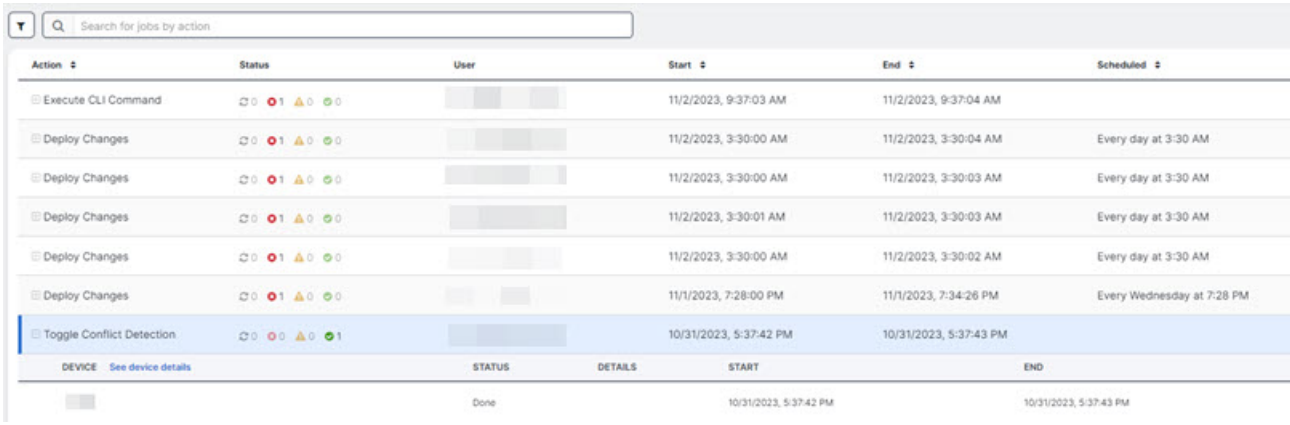
이 사용 사례에서는 외부 시스템에서 유지 관리되는 티켓을 해결하기 위해 수행한 작업으로 인해 변경 로그에 어떤 변경 로그 이벤트가 기록되었는지 확인하려는 시나리오를 설명합니다. 변경 요청과 관련된 변경 로그 이벤트를 검색하려면 다음 절차를 따르십시오.

1. 탐색창에서 **Change Log(**변경 로그**)**를 클릭합니다**.**
2. 다음 방법 중 하나를 사용하여 변경 요청과 관련된 변경 로그 이벤트를 검색합니다.
   - 해당 변경 요청과 연관된 변경 로그 이벤트를 찾기 위해 변경 로그 검색 필드에 변경 요청의 정확한 이름을 입력합니다. CDO는 정확히 일치하는 변경 로그 이벤트를 강조 표시합니다.
   - 변경 로그 이벤트를 찾기 위한 변경 요청 필터링, on page 157
3. 관련된 변경 요청을 보여주는 강조 표시된 변경 로그 이벤트를 찾으려면 각 변경 로그를 봅니다.

CDO에서 작업 모니터링

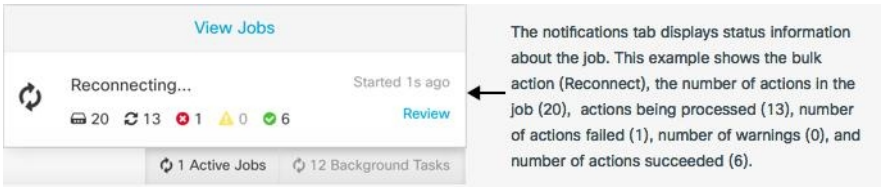
Job(작업**)** 페이지에서는 여러 디바이스 다시 연결하기, 여러 디바이스에서 구성 읽기, 여러 디바이스를 동시에 업그레이드하는 등의 대량 작업 진행 상황에 대한 개요를 제공합니다. **Job(**작업**)** 테이블은 개별 작업의 상태와 함께 색상으로 구분된 행을 사용하여 작업의 성공 또는 실패 여부를 표시합니다.

테이블의 한 행은 단일 대량 작업을 나타냅니다. 예를 들어 1개의 대량 작업이 20개의 디바이스를 다시 연결하려는 시도일 수 있습니다. **Jobs(**작업**)** 페이지에서 행을 확장하면 대량 작업의 영향을 받는 각 디바이스에 대한 결과가 표시됩니다.



Jobs(작업**)** 페이지는 다음과 같은 두 가지 방법으로 액세스할 수 있습니다.

- 새 작업 알림이 있을 때 **Notifications(**알림**)** 탭에서 **Review(**검토**)** 링크를 클릭합니다. **Jobs(**작업**)** 페이지로 리디렉션되고 해당 알림이 나타내는 특정 작업이 표시됩니다.



- 왼쪽 창에서 **Jobs(**작업**)**을 클릭합니다. 이 표에는 CDO에서 수행되는 대량 작업의 전체 목록이 나와 있습니다.

CDO에서 작업 검색

Jobs(작업**)** 페이지에서 다양한 작업, 작업을 수행한 사용자 및 작업 상태를 기준으로 필터링하고 검색할 수 있습니다.

대량 작업 재시작

Jobs(작업**)** 페이지를 검토한 후 대량 작업에서 하나 이상의 작업이 실패한 것을 발견하면 필요한 수정을 한 후 대량 작업을 다시 시도할 수 있습니다. CDO는 실패한 작업에 대해서만 작업을 다시 실행합니다. 대량 작업을 다시 실행하려면 다음을 실행합니다.

Procedure

단계 **1** **Jobs(**작업**)** 페이지에서 실패한 작업을 나타내는 행을 선택합니다.

단계 **2** **Retry(**재시도**)**( ) 아이콘을 클릭합니다.

대량 작업 취소

여러 디바이스에서 현재 진행 중인 대량 작업을 취소할 수 있습니다. 예를 들어 매니지드 디바이스 4개를 재연결하려고 시도했는데 그 중 3개가 성공적으로 재연결되었지만 네 번째 디바이스가 여전히 연결되지 않거나 연결이 끊어진 경우 대량 작업을 취소할 수 있습니다.

대량 작업을 취소하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Jobs(**작업**)**을 클릭합니다.

단계 **2** 실행 중인 대량 작업을 식별하고 오른쪽의 **Cancel(**취소**)** 링크를 클릭합니다.

Note
대량 작업의 일부가 성공하면 취소할 수 없습니다. 진행 중인 모든 작업이 취소됩니다.

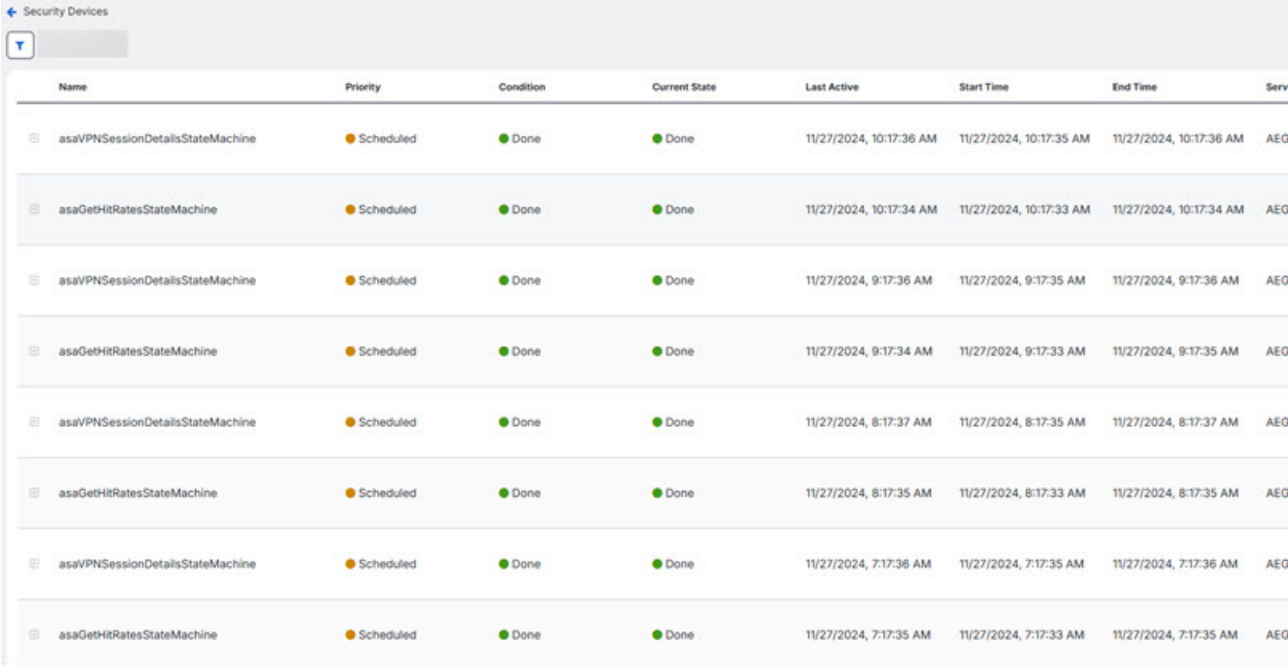
CDO에서 워크플로우 모니터링

워크플로우 페이지에서는 디바이스, 보안 디바이스 커넥터(SDC) 또는 보안 이벤트 커넥터(SEC)와 통신할 때, 디바이스에 규칙 집합 변경 사항을 적용할 때 CDO가 실행하는 모든 프로세스를 모니터링할 수 있습니다. CDO은 모든 단계에 대해 워크플로우 테이블에 항목을 만들고 이 페이지에 결과를 표시합니다. 이 항목에는 상호 작용하는 디바이스가 아니라 CDO가 수행하는 작업에만 관련된 정보가 포함되어 있습니다.

CDO는 디바이스에서 작업을 수행하지 못할 때 오류를 보고합니다. 워크플로우 페이지로 이동하여 오류가 발생한 단계를 확인하여 자세한 내용을 확인하십시오.

또한 이 페이지에서는 오류를 확인 및 해결하거나 필요한 경우 TAC와 정보를 공유할 수 있습니다.

Workflows(워크플로우**)** 페이지로 이동하려면, 왼쪽 창의 **Inventory(**재고 관리**)** 페이지에서 , **Devices(**디바이스**)** 탭을 클릭합니다. 적절한 디바이스 유형 탭을 클릭하여 디바이스를 찾고 원하는 디바이스를 선택합니다. 오른쪽 창의 **Devices and Actions(**디바이스 및 작업**)**에서 **Workflows(**워크플로우**)**를 클릭합니다. 다음 그림은 워크플로우 테이블의 항목이 있는 워크플로우 페이지를 보여줍니다.

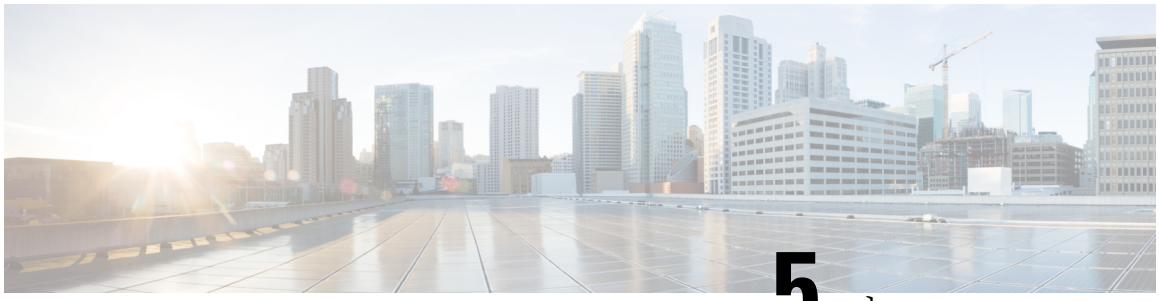


디바이스 워크플로 내보내기

전체 워크플로우 정보를 JSON 파일로 다운로드하고 TAC 팀에서 추가 분석을 요청할 때 제공할 수 있습니다. 워크플로우 정보를 내보내려면 해당 디바이스를 선택하고 해당 워크플로우 페이지로 이동하여 오른쪽 상단에 나타나는 내보내기( ) 아이콘을 클릭합니다.

스택 추적 복사

해결할 수 없는 오류가 발생하여 TAC에 문의하면 스택 추적 사본을 요청할 수 있습니다. 오류에 대한 스택 추적을 수집하려면 **Stack Trace(**스택 추적**)** 링크를 클릭하고 **Copy Stacktrace(**스택 추적 복사**)**를 클릭하여 화면에 나타나는 스택을 클립보드로 복사합니다.



5 장

Terraform

Terraform 정보

CDO 고객은 CDOTerraform 제공자 및 CDO Terraform 모듈을 통해 반복 가능하고 버전 제어되는 코드로 테넌트를 신속하게 설정할 수 있습니다. CDO Terraform 제공자를 통해 사용자는 다음을 수행할 수 있습니다.

- 사용자 관리
- 클라우드 제공 Firewall Management Centers, Cisco Secure ASA 디바이스 및 iOS 디바이스에 Secure Firewall Threat Defense 디바이스 온보딩
- vSphere 및 AWS에 보안 디바이스 커넥터 온보딩
- AWS의 보안 이벤트 커넥터 온보딩

자세한 정보는 다음 페이지를 참조하십시오.

- CDO Terraform 제공자 페이지
- vSphere 모듈 페이지의 CDO SDC
- AWS 모듈 페이지의 CDO SDC
- AWS 모듈 페이지의 CDO SEC
- Devnet 학습 랩을 통한 작업
- Cisco Defense Orchestrator Terraform 제공자를 사용하여 보안 인프라 관리 자동화 - 학습 랩
- GitHub의 CDO 자동화 예시

지원

CDO Terraform 제공자 및 모듈은 Apache 2.0 라이선스에 따라 오픈 소스 소프트웨어로 게시됩니다. 지원이 필요한 경우 아래 저장소의 GitHub에서 문제를 제출하십시오.

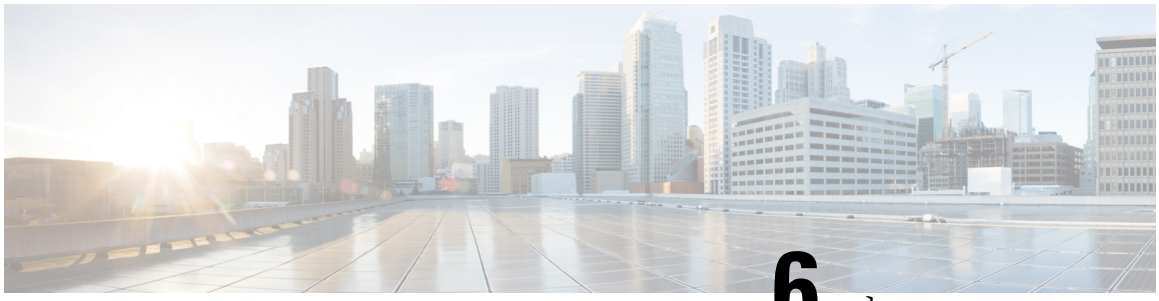
모듈	리포지토리
CDO Terraform 제공자	https://github.com/ciscodevnet/terraform-provider-CDO
CDO SDC 모듈(vSphere)	https://github.com/CiscoDevNet/terraform-vsphere-CDO-sdc
CDO SDC 모듈 (AWS)	https://github.com/CiscoDevNet/terraform-aws-CDO-sdc
CDO SEC 모듈(AWS)	https://github.com/CiscoDevNet/terraform-aws-CDO-sec

리포지토리에 대한 기여

CDO 팀은 위의 저장소에 대한 기여를 환영합니다. 제공자 및 모듈 개선에 참여하려면 이 GitHub 리포지토리에서 풀 요청을 생성하십시오.

관련 주제

- Terraform을 사용하여 vSphere에 SDC 구축
- Terraform을 사용하여 AWS VPC에 SDC 구축
- Terraform을 사용하여 AWS VPC에 SEC 구축



6 장

문제 해결

이 장에는 다음 섹션이 포함되어 있습니다.

보안 디바이스 커넥터 문제 해결

다음 주제를 사용하여 온프레미스 SDC(Secure Device Connector) 문제를 해결합니다.

이러한 시나리오와 일치하지 않는 경우 CDO 고객이 TAC로 지원 티켓을 여는 방법..

SDC에 연결할 수 없음

CDO에서 연속으로 두 개의 하트비트 요청에 응답하지 못한 경우 SDC는 "도달할 수 없음" 상태입니다. SDC에 연결할 수 없는 경우 테넌트는 온보딩한 디바이스와 통신할 수 없습니다.

CDO는 다음과 같은 방식으로 SDC에 연결할 수 없음을 나타냅니다.

- "일부 보안 디바이스 커넥터(SDC)에 연결할 수 없습니다."라는 메시지가 표시됩니다. CDO 홈페이지에서 이러한 SDC와 연결된 디바이스와 통신할 수 없습니다.
- Services(서비스) 페이지에서 SDC의 상태는 "연결할 수 없음"입니다.

먼저 이 문제를 해결하려면 SDC를 테넌트에 다시 연결해 봅니다.

1. SDC 가상 머신이 실행 중이고 해당 지역의 CDO IP 주소에 도달할 수 있는지 확인합니다. 매니지드 디바이스에 CDO 연결, 12 페이지을 참조하십시오.
2. 하트비트를 수동으로 요청하여 CDO와 SDC를 다시 연결해 봅니다. SDC가 하트비트 요청에 응답하면 "활성" 상태로 돌아갑니다. 하트비트를 수동으로 요청하려면 다음과 같이 작업합니다.
    1. 왼쪽 창에서 **Tools & Services**(도구 및 서비스) > **Secure Connectors**(보안 커넥터)를 클릭합니다.
    2. 연결할 수 없는 SDC를 클릭합니다.

3. 작업 창에서 **Request Heartbeat(**하트비트 요청**)**를 클릭합니다.
4. **Reconnect(**다시 연결**)**를 클릭합니다.

3. 테넌트에 수동으로 다시 연결하려고 시도한 후에도 SDC가 활성 상태로 돌아가지 않으면, 구축 후 SDC 상태가 CDO에서 활성화되지 않음, 166 페이지의 지침을 따르십시오.

.

구축 후 SDC 상태가 CDO에서 활성화되지 않음

CDO가 구축 후 약 10분 동안 SDC가 활성 상태임을 나타내지 않으면 SDC를 구축할 때 생성한 CDO 사용자 및 암호를 사용하여 SSH로 SDC VM에 연결합니다.

Procedure

단계 **1** `/opt/cdo/configure.log`를 검토합니다. SDC에 대해 입력한 구성 설정과 성공적으로 적용되었는지 여부를 보여줍니다. 설정 프로세스에 오류가 있거나 값이 올바르게 입력되지 않은 경우 sdc-onboard 설정을 다시 실행합니다.

a) 프롬프트에 `sudo sdc-onboard setup`을 입력합니다.
b) CDO사용자 암호를 입력합니다.
c) 프롬프트에 따라 수행합니다. 설정 스크립트는 설정 마법사에서 수행한 모든 구성 단계를 안내하고 입력한 값을 변경할 수 있는 기회를 제공합니다.

단계 **2** 로그를 검토하고 `sudo sdc-onboard setup`을 실행한 후에도 CDO가 여전히 SDC가 활성 상태임을 나타내지 않으면, CDO 지원 문의

SDC의 변경된 IP 주소가 CDO에 반영되지 않음

SDC의 IP 주소를 변경한 경우 GMT 오전 3시 이후까지는 CDO에 반영되지 않습니다.

SDC와의 디바이스 연결 문제 해결

이 도구를 사용하여 CDO에서 SDC(보안 디바이스 커넥터)를 통해 디바이스로의 연결을 테스트합니다. 디바이스가 온보딩에 실패하거나 온보딩 전에 CDO가 디바이스에 연결할 수 있는지 확인하려는 경우 이 연결을 테스트할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 **Tools & Services(**도구 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 클릭합니다.
단계 **2** SDC를 선택합니다.

단계 **3** 오른쪽의 **Troubleshooting(**문제 해결**)** 창에서 **Device Connectivity(**디바이스 연결**)**를 클릭합니다.

단계 **4** 문제 해결을 시도하거나 연결을 시도하는 디바이스의 유효한 IP 주소 또는 FQDN 및 포트 번호를 입력하고 **Go(**이동**)**를 클릭합니다. CDO는 다음 검증을 수행합니다.

a) **DNS** 확인 - IP 주소 대신 FQDN을 제공하는 경우 SDC가 도메인 이름을 확인하고 IP 주소를 가져올 수 있는지 확인합니다.

b) 연결 테스트 - 디바이스에 연결할 수 있는지 확인합니다.

c) **TLS** 지원 - 디바이스와 SDC가 모두 지원하는 TLS 버전 및 암호를 탐지합니다.

- 지원되지 않는 암호 - 디바이스와 SDC에서 모두 지원하는 TLS 버전이 없는 경우 CDO는 디바이스에서 지원하는 TLS 버전 및 암호도 테스트하지만 SDC는 테스트하지 않습니다.

d) SSL 인증서 - 문제 해결에서 인증서 정보를 제공합니다.

단계 **5** 디바이스에 대한 온보딩 또는 연결 문제가 계속 발생하는 경우 CDO 지원 문의하십시오.

간헐적으로 또는 SDC에 연결되지 않음

이 섹션에서 설명하는 솔루션은 온프레미스 SDC(보안 디바이스 커넥터)에만 적용됩니다.

증상: 간헐적으로 또는 SDC에 연결되지 않음

진단: 이 문제는 디스크 공간이 거의 찼을 때(80% 이상) 발생할 수 있습니다.

디스크 공간 사용량을 확인하려면 다음 단계를 수행합니다.

1. SDC(보안 디바이스 커넥터) VM용 콘솔을 엽니다.
2. 사용자 이름 **cdo**로 로그인합니다.
3. 최초 로그인 시 생성한 비밀번호를 입력합니다.
4. 먼저 **`df -h`**를 입력하여 사용 가능한 디스크 공간이 없는지 확인하여 디스크 여유 공간을 확인합니다.

   Docker에서 디스크 공간을 소비한 것을 확인할 수 있습니다. 정상적인 디스크 사용량은 2GB 미만일 것으로 예상됩니다.
5. **Docker** 폴더의 디스크 사용량을 보려면,

   `sudo du -h /var/lib/docker | sort -h`를 실행합니다.

   Docker 폴더의 디스크 공간 사용량을 볼 수 있습니다.

절차

Docker 폴더의 디스크 공간 사용량이 거의 가득 찬 경우 docker 구성 파일에서 다음을 정의합니다.

- 최대 크기: 현재 파일이 최대 크기에 도달하면 로그 회전을 강제합니다.
- 최대 파일: 최대 한도에 도달했을 때 초과 회전된 로그 파일을 삭제합니다.

다음을 수행하십시오.

1. **sudo vi /etc/docker/daemon.json**를 실행합니다.
2. 파일에 다음 줄을 삽입합니다.

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. **ESC** 키를 누른 다음 **:wq!**를 입력합니다. 변경 사항을 쓰고 파일을 닫습니다.

참고 **sudo cat /etc/docker/daemon.json**을 실행하여 파일의 변경 사항을 확인할 수 있습니다.

4. **sudo systemctl restart docker**를 실행하여 doker 파일을 다시 시작합니다.

   변경 사항이 적용되려면 몇 분 정도 걸립니다. **sudo du -h /var/lib/docker | sort -h**를 실행하여 docker 폴더의 업데이트된 디스크 사용량을 봅니다.
5. **df -h**를 실행하여 사용 가능한 디스크 크기가 증가했는지 확인합니다.
6. SDC 상태를 Unreachable(연결 불가)에서 Active(활성)로 변경하려면 먼저 CDO에서 **Services(**서비스**)** 페이지의 Secure Connector(보안 커넥터) 탭으로 이동하여 Actions(작업) 메뉴에서 **Request Reconnect(**재연결 요청**)**를 클릭해야 합니다.

보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 상승 취약점: cisco-sa-20190215-runc

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 **cisco-sa-20190215-runc**를 게시했습니다. 취약성에 대한 전체 설명은 전체 PSIRT 팀 자문을 참조하십시오.

이 취약성은 모든 CDO 고객에게 영향을 미칩니다.

- CDO의 클라우드 배포 SDC(보안 디바이스 커넥터)를 사용하는 고객은 CDO 운영팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 배포된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다. 다음 지침에 따라 이 작업을 수행할 수 있습니다.
  - CDO-표준 SDC 호스트 업데이트, 169 페이지
  - 사용자 지정 SDC 호스트 업데이트, 169 페이지
  - 버그 추적, 170 페이지

CDO-표준 SDC 호스트 업데이트

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축한 경우 이 지침을 사용합니다.

프로시저

단계 1 SSH 또는 하이퍼바이저 콘솔을 사용하여 SDC 호스트에 연결합니다.

단계 2 다음 명령을 실행하여 Docker 서비스 버전을 확인합니다.

```
docker version
```

단계 3 최신 VM(가상 머신) 중 하나를 실행 중인 경우 다음과 같은 출력이 표시됩니다.

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

여기에서 이전 버전을 볼 수 있습니다.

단계 4 다음 명령을 실행하여 Docker를 업데이트하고 서비스를 다시 시작하십시오.

```
> sudo yum update docker-ce
> sudo service docker restart
```

참고
Docker 서비스가 다시 시작되는 동안 CDO와 디바이스 간에 짧은 연결 중단이 발생합니다.

단계 5 docker version 명령을 다시 실행하십시오. 다음 출력이 표시되어야 합니다.

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

단계 6 마쳤습니다. 이제 패치가 적용된 최신 버전의 Docker로 업그레이드되었습니다.

사용자 지정 SDC 호스트 업데이트

자체 SDC 호스트를 생성한 경우 Docker 설치 방법에 따라 업데이트 지침을 따라야 합니다. CentOS, yum 및 Docker-ce(커뮤니티 에디션)를 사용한 경우 이전 절차가 작동합니다.

Docker-ee(엔터프라이즈 버전)를 설치했거나 다른 방법을 사용하여 Docker를 설치한 경우 Docker의 고정 버전이 다를 수 있습니다. Docker 페이지를 확인하여 설치할 올바른 버전(Docker 보안 업데이트 및 컨테이너 보안 모범 사례)을 결정할 수 있습니다.

버그 추적

Cisco는 이 취약성을 계속 평가하고 있으며 추가 정보가 제공되는 대로 권고를 업데이트할 것입니다. 권고가 최종으로 표시되면 관련 Cisco 버그에서 자세한 내용을 참조할 수 있습니다.

CSCvo33929-CVE-2019-5736: runc container breakout

올바르지 않은 시스템 시간

CDO에서는 SDC(보안 디바이스 커넥터)와의 새로운 통신 방식을 채택하고 있습니다. 이를 위해 CDO는 2024년 2월 1일까지 기존 SDC를 새 통신 방법으로 마이그레이션해야 합니다.

참고 SDC가 2024년 2월 1일까지 마이그레이션되지 않으면 CDO는 더 이상 SDC를 통해 디바이스와 통신할 수 없습니다.

CDO의 운영팀이 SDC 마이그레이션을 시도했지만 SDC 시스템 시간이 AWS 시스템 시간보다 15분 빠르거나 늦어 마이그레이션에 성공하지 못했습니다.

아래 단계에 따라 시스템 시간 문제를 해결하십시오. 이 문제가 해결되면 마이그레이션을 진행할 수 있습니다.

프로시저

단계 **1** VM 터미널을 통해 또는 SSH 연결을 통해 SDC VM에 로그인합니다.

단계 **2** 프롬프트에서 `sudo sdc-onboard setup`을 입력하고 인증합니다.

단계 **3** 이제 SDC를 처음 설정하는 것처럼 SDC 설정 질문에 응답해야 합니다. NTP 서버 주소를 제외하고는 이전과 동일한 비밀번호와 네트워크 정보를 모두 다시 입력합니다.

a) SDC를 설정하는 데 사용한 것과 동일한 비밀번호로 루트 및 CDO 사용자 비밀번호를 재설정합니다.
b) 프롬프트가 표시되면 **y** 를 입력하여 네트워크를 재설정합니다.
c) 이전과 같이 IP 주소/CIDR의 값을 입력합니다.
d) 이전과 같이 네트워크 게이트웨이의 값을 입력합니다.
e) 이전과 같이 DNS 서버 값을 입력합니다.
f) NTP 서버에 대한 프롬프트가 표시되면 유효한 NTP 서버 주소(예: `time.aws.com`)를 제공해야 합니다.
g) 제공한 값을 검토하고 값이 올바른 경우 **y**를 입력합니다.

단계 4 프롬프트에서 날짜를 입력하여 시간 서버에 연결할 수 있고 SDC와 동기화되는지 확인합니다. UTC 날짜 및 시간이 표시되며 SDC 시간과 비교할 수 있습니다.

다음에 수행할 작업

이러한 단계를 완료했거나 오류가 발생하는 경우에는 Cisco Technical Assistance Center(TAC)에 문의하십시오. 이 단계를 성공적으로 완료하면 CDO 운영팀에서 새로운 통신 방법으로의 SDC 마이그레이션을 완료할 수 있습니다.

SDC 버전이 202311****보다 낮음

CDO에서는 SDC(보안 디바이스 커넥터)와의 새로운 통신 방식을 채택하고 있습니다. 이를 위해 CDO는 2024년 2월 1일까지 기존 SDC를 새 통신 방법으로 마이그레이션해야 합니다.

참고 SDC가 2024년 2월 1일까지 마이그레이션되지 않으면 CDO는 더 이상 SDC를 통해 디바이스와 통신할 수 없습니다.

CDO의 운영팀이 SDC 마이그레이션을 시도했지만 테넌트가 202311****보다 낮은 버전을 실행하고 있어 실패했습니다.

SDC의 현재 버전은 CDO 메뉴 모음, **Tools & Services(**툴 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**로 이동하면 보안 커넥터 페이지에 나열됩니다. SDC를 선택하면 화면 오른쪽의 **Details(**세부 사항**)** 창에서 버전 번호를 확인할 수 있습니다.

SDC 버전을 업그레이드하려면 아래 단계를 따르십시오. 이 문제가 해결되면 CDO 작업에서 마이그레이션 프로세스를 다시 실행할 수 있습니다.

프로시저

단계 1 SDC VM에 로그인하고 인증합니다.

단계 2 프롬프트에 `sudo su - sdc`를 입력하고 인증합니다.

단계 3 프롬프트에 `crontab -r`을 입력합니다.

`no crontab for sdc(sdc에 대한 crontab 없음)` 메시지가 표시되는 경우 이 메시지를 무시하고 다음 단계로 이동할 수 있습니다.

단계 4 메시지가 표시되면 `./toolkit/toolkit.sh upgrade`를 입력합니다. CDO는 업그레이드가 필요한지 확인하고 툴킷을 업그레이드합니다. 콘솔에서 보고된 오류가 없는지 확인합니다.

단계 5 SDC의 새 버전을 확인합니다.

a) CDO에 로그인합니다.

b) CDO 메뉴 모음에서 **Tools & Services(**툴 및 서비스**)** > **Secure Connectors(**보안 커넥터**)**를 탐색하여 보안 커넥터 페이지로 이동합니다.

c) SDC를 선택하고 **Actions(**작업**)** 창에서 **Request Heartbeat(**하트비트 요청**)**를 클릭합니다.
d) SDC 버전이 202311**** 이상인지 확인합니다.

다음에 수행할 작업

이러한 단계를 완료했거나 오류가 발생하는 경우에는 Cisco Technical Assistance Center(TAC)에 문의하십시오. 이러한 단계를 성공적으로 완료하면 CDO 운영팀이 마이그레이션 프로세스를 다시 실행할 수 있습니다.

AWS 서버의 인증서 또는 연결 오류

CDO에서는 SDC(보안 디바이스 커넥터)와의 새로운 통신 방식을 채택하고 있습니다. 이를 위해 CDO는 2024년 2월 1일까지 기존 SDC를 새 통신 방법으로 마이그레이션해야 합니다.

참고 SDC가 2024년 2월 1일까지 마이그레이션되지 않으면 CDO는 더 이상 SDC를 통해 디바이스와 통신할 수 없습니다.

CDO의 운영팀이 SDC 마이그레이션을 시도했지만 연결 문제가 발생하여 실패했습니다.

아래 단계에 따라 연결 문제를 해결하십시오. 이 문제가 해결되면 마이그레이션을 진행할 수 있습니다.

프로시저

단계 **1** 포트 443에서 해당 지역의 도메인에 대한 아웃바운드 프록시 연결을 허용하는 방화벽 규칙을 생성합니다.

- 호주 지역의 프로덕션 테넌트:
  - cognito-identity.ap-southeast-2.amazonaws.com
  - cognito-idp.ap-southeast-2.amazonaws.com
  - sns.ap-southeast-2.amazonaws.com
  - sqs.ap-southeast-2.amazonaws.com
- 인도 지역의 프로덕션 테넌트:
  - cognito-identity.ap-south-1.amazonaws.com
  - cognito-idp.ap-south-1.amazonaws.com
  - sns.ap-south-1.amazonaws.com
  - sqs.ap-south-1.amazonaws.com

- 미국 지역의 프로덕션 테넌트:
  - cognito-identity.us-west-2.amazonaws.com
  - cognito-idp.us-west-2.amazonaws.com
  - sns.us-west-2.amazonaws.com
  - sqs.us-west-2.amazonaws.com
- EU 지역의 프로덕션 테넌트:
  - cognito-identity.eu-central-1.amazonaws.com
  - cognito-idp.eu-central-1.amazonaws.com
  - sns.eu-central-1.amazonaws.com
  - sqs.eu-central-1.amazonaws.com
- APJ 지역의 프로덕션 테넌트:
  - cognito-identity.ap-northeast-1.amazonaws.com
  - cognito-idp.ap-northeast-1.amazonaws.com
  - sqs.ap-northeast-1.amazonaws.com
  - sns.ap-northeast-1.amazonaws.com

단계 **2** 아래 명령 중 하나를 사용하여 방화벽의 "허용 목록"에 추가해야 하는 전체 IP 주소 목록을 확인할 수 있습니다.

참고
아래 명령은 **jq**가 설치되어 있는 사용자를 위한 명령입니다. IP 주소가 단일 목록에 표시됩니다.

- 미국 지역의 프로덕션 테넌트:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- EU 지역의 프로덕션 테넌트:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "eu-central-1") | .ip_prefix'
```

- APJ 지역의 프로덕션 테넌트:

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select(
(.service == "AMAZON" ) and .region == "ap-northeast-1") | .ip_prefix'
```

참고
jq가 설치되어 있지 않은 경우, 명령의 다음 단축 버전을 사용할 수 있습니다.

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

다음에 수행할 작업

이러한 단계를 완료했거나 오류가 발생하는 경우에는 Cisco Technical Assistance Center(TAC)에 문의하십시오. 이 단계를 성공적으로 완료하면 CDO 운영팀에서 새로운 통신 방법으로의 SDC 마이그레이션을 완료할 수 있습니다.

문제 해결 CDO

로그인 실패 문제 해결

실수로 잘못된 **CDO** 지역에 로그인했기 때문에 로그인에 실패함

적절한 CDO 지역에 로그인했는지 확인합니다. https://sign-on.security.cisco.com에 로그인하면 액세스할 지역을 선택할 수 있습니다.

로그인해야 하는 지역에 대한 자세한 내용은 다른 지역에서 CDO 로그인, 5 페이지을 참조하십시오.

마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 75 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성.
- 해결 방법 새 Secure Sign-On 계정을 만든 경우 대시보드에서 테넌트가 만들어진 지역에 해당하는 CDO 타일을 클릭합니다.
  - 해결 방법 Cisco Defense Orchestrator APJ

- 해결 방법 Cisco Defense Orchestrator 호주
- 해결 방법 Cisco Defense Orchestrator EU
- 해결 방법 Cisco Defense Orchestrator 인도
- 해결 방법 Cisco Defense Orchestrator US

- 해결 방법 https://sign-on.security.cisco.com을 가리키도록 북마크를 업데이트합니다.

액세스 및 인증서 문제 해결

새 지문 탐지 상태 확인

Procedure

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.
단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.
단계 **3** 해당 디바이스 탭을 클릭합니다.
단계 **4** 새 지문 감지됨 상태에서 디바이스를 선택합니다.
단계 **5** 새 지문 감지됨 창에서 지문 검토를 클릭합니다.
단계 **6** 지문을 검토하고 수락하라는 메시지가 표시되면

a. **Download Fingerprint(**지문 다운로드**)**를 클릭하고 검토합니다.

b. 지문에 만족하면 **Accept(**수락**)**를 클릭합니다. 그렇지 않은 경우 **Cancel(**취소**)**를 클릭합니다.

단계 **7** 새 지문 문제를 해결한 후 디바이스의 연결 상태가 온라인으로 표시되고 구성 상태가 "동기화되지 않음" 또는 "충돌 감지됨"으로 표시될 수 있습니다. 구성 충돌 해결을 검토하여 CDO와 디바이스 간의 구성 차이를 검토하고 해결합니다.

보안 및 분석 로깅 이벤트를 사용하여 네트워크 문제 해결

다음은 이벤트 뷰어를 사용하여 네트워크 문제를 문제 해결하는 데 사용할 수 있는 기본 프레임워크입니다.

이 시나리오에서는 네트워크 운영 팀에서 사용자가 네트워크의 리소스에 액세스할 수 없다는 보고를 받은 것으로 가정합니다. 문제를 보고하는 사용자와 해당 위치를 기반으로, 네트워크 운영 팀은 어떤 방화벽이 리소스에 대한 액세스를 제어하는지를 합리적으로 파악합니다.

Note 또한 이 시나리오에서는 FDM 관리 디바이스가 네트워크 트래픽을 관리하는 방화벽이라고 가정합니다. Security Analytics and Logging(보안 분석 및 로깅)은 다른 디바이스 유형에서 로깅 정보를 수집하지 않습니다.

Procedure

단계 **1** 기록 탭을 클릭합니다.

단계 **2** 시간 범위를 기준으로 이벤트 필터링을 시작합니다. 기본적으로 Historical(기록) 탭에는 이벤트의 마지막 시간이 표시됩니다. 올바른 시간 범위인 경우 현재 날짜와 시간을 **End(**종료**)** 시간으로 입력합니다. 올바른 시간 범위가 아닌 경우 보고된 문제의 시간을 포함하는 시작 및 종료 시간을 입력합니다.

단계 **3** **Sensor ID(**센서 **ID)** 필드에 사용자의 액세스를 제어하는 것으로 의심되는 방화벽의 IP 주소를 입력합니다. 방화벽이 두 개 이상인 경우 검색 창에서 속성**:**값 쌍을 사용하여 이벤트를 필터링합니다. 두 항목을 만들고 OR 문으로 결합합니다. 예: `SensorID:192.168.10.2 OR SensorID:192.168.20.2`.

단계 **4** Events(이벤트) 필터 표시줄의 **Source IP(**소스 **IP)** 필드에 사용자의 IP 주소를 입력합니다.

단계 **5** 사용자가 리소스에 액세스할 수 없는 경우 **Destination IP(**대상 **IP)** 필드에 해당 리소스의 IP 주소를 입력해 보십시오.

단계 **6** 결과에서 이벤트를 확장하고 세부 정보를 확인합니다. 다음은 몇 가지 세부 사항입니다.

- **AC_RuleAction** - 규칙이 트리거될 때 수행된 작업(허용, 신뢰, 차단).
- **FirewallPolicy** - 이벤트를 트리거한 규칙이 상주하는 정책입니다.
- **FirewallRule** - 이벤트를 트리거한 규칙의 이름입니다. 값이 Default Action(기본 작업)인 경우 정책의 규칙 중 하나가 아니라 이벤트를 트리거한 것은 정책의 기본 작업입니다.
- **UserName** - 이니시에이터 IP 주소와 연결된 사용자입니다. 이니시에이터 IP 주소는 소스 IP 주소와 동일합니다.

단계 **7** 규칙 작업이 액세스를 차단하는 경우 FirewallRule 및 FirewallPolicy 필드를 확인하여 액세스를 차단하는 정책의 규칙을 식별합니다.

SSL 암호 해독 문제 해결

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리**(SSL** 또는 인증 기관 피닝**)**

스마트폰 및 기타 디바이스용 일부 앱은 SSL(또는 인증 기관) 피닝이라는 기술을 사용합니다. SSL 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 Firepower Threat Defense 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때

도 연결 가능). 예를 들어 사용자는 Facebook iOS 또는 Android 앱을 사용할 수 없지만 Safari 또는 Chrome을 https://www.facebook.com으로 지정하고 성공적으로 연결할 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 SSL 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 SSL 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- Facebook 등의 그룹 1 앱은 서버에서 SH, CERT, SHD 메시지를 받는 즉시 SSL ALERT 메시지를 보냅니다. Alert는 보통 SSL 피닝을 나타내는 "Unknown CA (48)(알 수 없는 CA(48))" 알림입니다. 알림 메시지 후에는 TCP Reset(TCP 재설정)이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
  - `SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN이 포함되어 있습니다.`
  - `SSL Flow Flag(SSL 플로우 플래그)에는 APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.`
  - `SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE입니다.`
- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.
  - `SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN, APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.`
  - `SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE, CLIENT_KEY_EXCHANGE, CLIENT_CHANGE_CIPHER_SPEC, CLIENT_FINISHED, SERVER_CHANGE_CIPHER_SPEC, SERVER_FINISHED입니다.`

마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **CDO**에 로그인하지 못함

해결 방법 CDO에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 계정을 사용하려면 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 75 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **CDO**를 실행할 수 없음

해결 방법 CDO 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 계정을 만들었을 수 있습니다. CDO와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 계정을 생성하지 않은 경우 새 Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성.
- 해결 방법 새 Secure Sign-On 계정을 만든 경우 대시보드에서 테넌트가 만들어진 지역에 해당하는 CDO 타일을 클릭합니다.
  - 해결 방법 Cisco Defense Orchestrator APJ
  - 해결 방법 Cisco Defense Orchestrator 호주
  - 해결 방법 Cisco Defense Orchestrator EU
  - 해결 방법 Cisco Defense Orchestrator 인도
  - 해결 방법 Cisco Defense Orchestrator US
- 해결 방법 https://sign-on.security.cisco.com을 가리키도록 북마크를 업데이트합니다.

개체 문제 해결

중복 개체 문제 해결

중복 개체 ⧉는 이름은 다르지만 값은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 대개 실수로 생성되고 유사한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체 문제를 해결한 후 CDO는 유지된 개체 이름으로 영향을 받는 모든 개체 참조를 업데이트합니다.

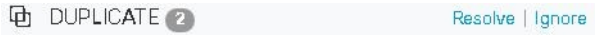
중복 개체 문제를 해결하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 개체 필터하여 중복 개체 문제를 찾습니다.

단계 **3** 결과 중 하나를 선택합니다. 개체 세부 정보 패널에 영향을 받는 중복 수가 포함된 DUPLICATE 필드가 표시됩니다.



단계 **4** **Resolve(**확인**)**를 클릭합니다. CDO는 비교할 중복 개체를 표시합니다.

단계 **5** 비교할 두 개체를 선택합니다.

단계 **6** 이제 다음과 같은 옵션이 제공됩니다.

- 개체 중 하나를 다른 개체로 교체하려면 유지할 개체에 대해 **Pick(**선택**)**을 클릭하고 **Resolve(**확인**)**를 클릭하여 영향을 받을 디바이스 및 네트워크 정책을 확인한 다음, 변경 사항이 마음에 들면 **Confirm(**확인**)**를 클릭합니다. CDO는 대체물로 선택한 개체를 유지하고 중복을 삭제합니다.
- 목록에 무시할 개체가 있는 경우 **Ignore(**무시**)**를 클릭합니다. 개체를 무시하면 CDO에 표시되는 중복 개체 목록에서 제거됩니다.
- 개체는 유지하지만 CDO가 중복 개체를 검색할 때 찾지 않도록 하려면 **Ignore All(**모두 무시**)**를 클릭합니다.

단계 **7** 중복 개체 문제가 해결되면 지금 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

사용되지 않는 개체 문제 해결

사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다.

관련 정보**:**

- 디바이스 및 서비스 목록 내보내기, 93 페이지
- CDO에 디바이스 대량 재연결, 97 페이지

사용되지 않은 개체 문제 해결

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 개체 필터하여 사용하지 않는 개체 문제를 찾습니다.

단계 **3** 하나 이상의 사용되지 않는 개체를 선택합니다.

단계 **4** 이제 다음과 같은 옵션이 제공됩니다.

- Actions(작업) 창에서 **Remove(**제거**)** 를 클릭하여 CDO에서 사용되지 않는 개체를 제거합니다.
- Issues(문제) 창에서 **Ignore(**무시**)**를 클릭합니다. 개체를 무시하면 CDO는 사용되지 않은 개체의 결과에 해당 개체를 표시하지 않습니다.

단계 **5** 사용되지 않는 개체를 제거한 경우, 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 138지금 변경한 사항을 수행하거나 대기하고 여러 변경 사항을 한 번에 구축합니다.

Note

사용되지 않는 개체 문제를 벌크로 해결하려면 대량의 개체 문제 해결을 참조하십시오.

사용되지 않는 개체 대량 제거

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 개체 필터하여 사용하지 않는 개체 문제를 찾습니다.

단계 **3** 삭제하려는 사용되지 않는 개체를 선택합니다.

- 개체 테이블 헤더 행의 확인란을 클릭하여 페이지의 모든 개체를 선택합니다.
- 개체 테이블에서 사용하지 않는 개별 개체를 선택합니다.

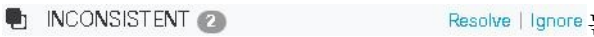
단계 **4** 오른쪽의 작업 창에서 **Remove(**제거**)** 를 클릭하여 CDO에서 선택한 사용되지 않는 개체를 모두 제거합니다. 한 번에 99개의 개체를 제거할 수 있습니다.

단계 **5** **OK(**확인**)**을 클릭하여 사용하지 않는 개체를 삭제할 것인지 확인합니다.

단계 **6** 이러한 변경 사항을 배포하기 위한 두 가지 선택 사항이 있습니다.

- 지금 변경한 내용을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.
- **Inventory(**재고 목록**)** 페이지를 열고 변경의 영향을 받은 디바이스를 찾습니다. 변경의 영향을 받는 모든 디바이스를 선택하고 관리 창에서 **Deploy All(**모두 배포**)** 를 클릭합니다. 경고를 읽고 적절한 조치를 취합니다.

불일치 개체 문제 해결

불일치 개체 

는 두 개 이상의 디바이스에서 이름은 같지만 값이 다른 개체입니다. 사용자가 동일한 이름 및 콘텐츠를 사용하여 서로 다른 구성에서 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라지므로 불일치가 발생하는 경우가 있습니다.

참고: 일관되지 않은 개체 문제를 벌크로 해결하려면 대량의 개체 문제 해결을 참고하십시오.

일치하지 않는 개체에 대해 다음을 수행할 수 있습니다.

- **Ignore(**무시**)**: CDO가 개체 간의 불일치를 무시하고 해당 값을 유지합니다. 개체가 더 이상 불일치 범주에 나열되지 않습니다.
- **Merge(**병합**)**: CDO가 선택한 모든 개체와 해당 값을 단일 개체 그룹으로 결합합니다.
- **Rename(**이름 변경**):** CDO를 사용하면 일치하지 않는 개체 중 하나의 이름을 바꾸고 새 이름을 지정할 수 있습니다.

- **Convert Shared Network Objects to Overrides(**공유 네트워크 개체를 오버라이드로 변환**)**: CDO를 사용하면 일관성이 없는 공유 개체(오버라이드가 있거나 없는)를 오버라이드가 있는 단일 공유 개체로 결합할 수 있습니다. 일치하지 않는 개체의 가장 일반적인 기본값은 새로 형성된 개체의 기본값으로 설정됩니다.

Note 공통 기본값이 여러 개인 경우 그 중 하나가 기본값으로 선택됩니다. 나머지 기본값 및 재정의 값은 해당 개체의 재정의로 설정됩니다.

- **Convert Shared Network Group to Additional Values(**공유 네트워크 그룹을 추가 값으로 변환**):** - CDO를 사용하면 일치하지 않는 공유 네트워크 그룹을 추가 값이 있는 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 이 기능의 기준은 변환할 일관되지 않은 네트워크 그룹에 동일한 값을 가진 공통 개체가 하나 이상 있어야 한다는 것입니다. 이 기준과 일치하는 모든 기본값은 기본값이 되며, 나머지 개체는 새로 형성된 네트워크 그룹의 추가 값으로 할당됩니다.

  예를 들어, 일치하지 않는 두 개의 공유 네트워크 그룹을 고려하십시오. 첫 번째 네트워크 그룹 'shared_network_group'은 'object_1'(192.0.2.x) 및 'object_2'(192.0.2.y)로 구성됩니다. 여기에는 추가 값 'object_3'(192.0.2.a)도 포함됩니다. 두 번째 네트워크 그룹 'shared_network_group'은 'object_1'(192.0.2.x) 및 추가 값 'object_4'(192.0.2.b)로 구성됩니다. 공유 네트워크 그룹을 추가 값으로 변환할 때 새로 형성된 그룹 'shared_network_group'에는 'object_1'(192.0.2.x) 및 'object_2'(192.0.2.y)'가 포함되며, 'object_3'(192.0. 2.a) 및 'object_4'(192.0.2.b)를 추가 값으로 사용합니다.

Note 새 네트워크 개체를 생성하면 CDO는 자동으로 해당 값을 동일한 이름의 기존 공유 네트워크 개체에 오버라이드로 할당합니다. 이는 새 디바이스가 CDO에 온보딩된 경우에도 적용됩니다.

자동 할당은 다음 기준을 충족하는 경우에만 발생합니다.

1. 새 네트워크 개체를 디바이스에 할당해야 합니다.
2. 이름과 유형이 같은 공유 개체는 테넌트에 하나만 있어야 합니다.
3. 공유 개체에 이미 오버라이드가 포함되어 있어야 합니다.

일관성 없는 개체 문제를 해결하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽의 CDO 탐색 모음에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 그런 다음 개체를 개체 필터하여 일관성 없는 개체 문제를 찾습니다.

단계 **3** 일치하지 않는 개체를 선택합니다. 개체 세부 정보 패널에 영향을 받는 개체의 수가 포함된 INCONSISTENT 필드가 표시됩니다.

단계 **4** **Resolve(**확인**)**를 클릭합니다. CDO는 비교할 중복 개체를 표시합니다.

단계 **5** 이제 다음과 같은 옵션이 제공됩니다.

- 모두 무시**:**
  - **a.** 표시된 개체를 비교하고 개체 중 하나에서 **Ignore(**무시**)**를 클릭합니다. 또는 모든 개체를 무시하려면 **Ignore All(**모두 무시**)**을 클릭합니다.
  - **b.** **OK(**확인**)**를 클릭하여 확인합니다.
- 개체를 병합하여 해결합니다**.**
  - **a.** **Resolve by Merging X Objects(X**개 개체를 병합하여 해결**)**를 클릭합니다.
  - **b.** **OK(**확인**)**를 클릭합니다.
- **Rename(**이름 바꾸기**):**
  - **a.** **Rename(**이름 변경**)**을 클릭합니다.
  - **b.** 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm(**확인**)**을 클릭합니다.
- **Convert to Overrides(**오버라이드로 변환**)(**일치하지 않는 공유 개체의 경우**)**: 공유 개체를 오버라이드와 비교할 때, 비교 패널의 **Inconsistent Values(**일관되지 않는 값**)** 필드에 기본값만 표시됩니다.
  - **a.** **Convert to Overrides(**재정의로 변환**)**를 클릭합니다. 일치하지 않는 모든 개체는 오버라이드가 포함된 단일 공유 개체로 변환됩니다.
  - **b.** **OK(**확인**)**를 클릭합니다. **Edit Shared Object(**공유 개체 편집**)**를 클릭하여 새로 형성된 개체의 세부 정보를 볼 수 있습니다. 위쪽 및 아래쪽 화살표를 사용하여 기본값과 재정의 간에 값을 이동할 수 있습니다.
- **Convert to Additional Values(**추가 값으로 변환**)(**일치하지 않는 네트워크 그룹의 경우**):**
  - **a.** **Convert to Additional Values(**추가 값으로 변환**)**를 클릭합니다. 일치하지 않는 모든 개체는 추가 값이 있는 단일 공유 개체로 변환됩니다.
  - **b.** 영향을 받는 네트워크 정책 및 디바이스에 변경 사항을 저장하고 **Confirm(**확인**)**을 클릭합니다.

단계 **6** 불일치를 해결한 후 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

대량의 개체 문제 해결

사용되지 않는 개체 문제 해결 중복 개체 문제 해결 불일치 개체 문제 해결, on page 180 문제가 있는 개체를 해결하는 한 가지 방법은 이러한 개체를 무시하는 것입니다. 개체에 둘 이상의 문제가 있더라도 여러 개체를 선택하고 무시할 수 있습니다. 예를 들어 개체가 일치하지 않고 사용되지 않는 경우 한 번에 하나의 문제 유형만 무시할 수 있습니다.

Important 나중에 개체가 다른 문제 유형과 연결될 경우 커밋한 무시 작업은 해당 시점에 선택한 문제에만 영향을 미칩니다. 예를 들어, 개체가 중복되었기 때문에 개체를 무시했고 개체가 나중에 일치하지 않는 것으로 표시되는 경우, 중복 개체로 무시한다고 해서 일치하지 않는 개체로 무시되는 것은 아닙니다.

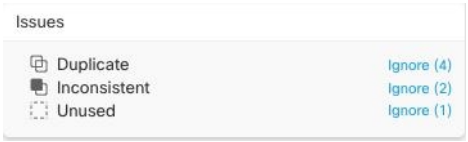
대량으로 문제를 무시하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 검색 범위를 좁히기 위해 개체 문제를 개체 필터할 수 있습니다.

단계 **3** Object(개체) 테이블에서 무시할 적용 가능한 모든 개체를 선택합니다. Issues(문제) 창은 문제 유형별로 개체를 그룹화합니다.



단계 **4** 유형별로 문제를 무시하려면 **Ignore(**무시**)**를 클릭합니다. 각 문제 유형을 개별적으로 무시해야 합니다.

단계 **5** **OK(**확인**)**를 클릭하여 해당 개체를 무시할 것임을 확인합니다.

디바이스 연결 상태

CDO 테넌트에 온보딩된 디바이스의 연결 상태를 볼 수 있습니다. 이 항목은 다양한 연결 상태를 이해하는 데 도움이 됩니다. **Inventory(**재고 목록**)** 페이지에서 **Connectivity(**연결**)** 열은 디바이스 연결 상태를 표시합니다.

디바이스 연결 상태가 '온라인'이면 디바이스의 전원이 켜져 있고 CDO에 연결되어 있음을 의미합니다. 아래 표에 설명된 다른 상태는 일반적으로 여러 가지 이유로 디바이스에 문제가 발생할 때 발생합니다. 이 표는 이러한 문제에서 복원하는 방법을 제공합니다. 연결 실패를 일으키는 문제가 두 개 이상 있을 수 있습니다. 다시 연결을 시도하면, CDO는 다시 연결을 수행하기 전에 먼저 이러한 모든 문제를 편집하라는 메시지를 표시합니다.

디바이스 연결 상태	가능한 이유	해결 방법
온라인	디바이스의 전원이 켜져 있고 CDO에 연결되어 있습니다.	해당 없음
오프라인	디바이스의 전원이 꺼졌거나 네트워크 연결이 끊겼습니다.	디바이스가 오프라인 상태인지 확인합니다.
불충분한 라이선스	디바이스에 충분한 라이선스가 없습니다.	라이선스 부족 문제 해결, on page 184
유효하지 않은 자격 증명	디바이스에 연결하기 위해 CDO에서 사용하는 사용자 이름과 암호 조합이 올바르지 않습니다.	유효하지 않은 자격 증명 문제 해결, on page 185
온보딩	디바이스 온보딩이 시작되었지만 완료되지 않았습니다.	디바이스의 연결을 확인하고 디바이스 등록을 완료해야 합니다.
새 인증서 탐지됨	디바이스의 인증서가 변경되었습니다. 디바이스가 자체 서명된 인증서를 사용하는 경우 디바이스의 전원을 껐다 켜서 이 문제가 발생했을 수 있습니다.	새 인증서 문제 해결, on page 185
온보딩 오류	CDO는 디바이스를 온보딩할 때 디바이스와의 연결이 끊어졌을 수 있습니다.	온보딩 오류 문제 해결, on page 194

라이선스 부족 문제 해결

디바이스 연결 상태가 "Insufficient License(라이선스 부족)"로 표시되면 다음을 수행합니다.

- 디바이스가 라이선스를 획득할 때까지 잠시 기다립니다. 일반적으로 Cisco Smart Software Manager가 디바이스에 새 라이선스를 적용하는 데 시간이 걸립니다.
- 디바이스 상태가 변경되지 않으면 CDO에서 로그아웃하고 다시 로그인하여 CDO 포털을 새로 고침한 후 라이선스 서버와 디바이스 간의 네트워크 통신 문제를 해결합니다.
- 포털을 새로 고침해도 디바이스 상태가 변경되지 않으면 다음을 수행합니다.

Procedure

단계 **1** Cisco Smart Software Manager에서 새 토큰을 생성하고 복사합니다. 자세한 내용은 스마트 라이선싱 생성 비디오를 참조하십시오.

단계 **2** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **3** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **4** 적절한 디바이스 유형 탭을 클릭하고 **Insufficient License(**라이선스 부족**)** 상태의 디바이스를 선택합니다.

단계 **5** **Device Details(**디바이스 세부 정보**)** 창에서 **Insufficient Licenses(**불충분한 라이선스**)**에 표시되는 **Manage Licenses(**라이선스 관리**)**를 클릭합니다. **Manage Licenses(**라이선스 관리**)** 창이 나타납니다.

단계 **6** 활성화 필드에 새 토큰을 붙여넣고 디바이스 등록를 클릭합니다.

토큰이 디바이스에 성공적으로 적용되면 연결 상태가 온라인으로 바뀝니다.

유효하지 않은 자격 증명 문제 해결

유효하지 않은 자격 증명으로 인한 디바이스 연결 끊김을 해결하려면 다음을 수행합니다.

Procedure

단계 **1** 왼쪽 창에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 **Invalid Credentials(**유효하지 않은 자격 증명**)** 상태의 디바이스를 선택합니다.

단계 **4** **Device Details(**디바이스 세부 정보**)** 창에서 **Invalid Credentials(**잘못된 자격 증명**)**에 나타나는 **Reconnect(**재연결**)**을 클릭합니다. CDO가 디바이스에 재연결을 시도합니다.

단계 **5** 프롬프트가 나타나면 Linux 사용자 이름 및 비밀번호를 입력합니다.

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** 디바이스가 온라인 상태가 되고 사용할 준비가 되면 **Close(**닫기**)**를 클릭합니다.

단계 **8** CDO가 잘못된 자격 증명을 사용하여 디바이스에 연결하려고 시도했기 때문에 CDO가 디바이스에 연결하는 데 사용해야 하는 사용자 이름 및 비밀번호 조합이 디바이스에서 직접 변경되었을 수 있습니다. 이제 디바이스가 "Online(온라인)"이지만 구성 상태가 "Conflict Detected(충돌 탐지됨)"인 것을 확인할 수 있습니다. 구성 충돌 해결를 사용하여 CDO와 디바이스 간의 구성 차이를 검토하고 해결합니다.

새 인증서 문제 해결

CDO의 인증서 사용

CDO는 디바이스에 연결할 때 인증서의 유효성을 확인합니다. 특히 CDO는 다음을 요구합니다.

1. 디바이스에서 1.0 이상의 TLS 버전을 사용합니다.
2. 디바이스에서 제시한 인증서가 만료되지 않았으며 발급 날짜가 과거입니다(즉, 이미 유효하며 나중에 유효해질 예정이 아님).

3. 인증서는 SHA-256 인증서여야 합니다. SHA-1 인증서는 허용되지 않습니다.
4. 다음 조건 중 하나가 참입니다.
   - 디바이스가 자체 서명 인증서를 사용하며, 인증된 사용자가 신뢰하는 최신 인증서와 동일합니다.
   - 디바이스는 신뢰할 수 있는 CA(Certificate Authority)에서 서명한 인증서를 사용하며, 제공된 리프 인증서를 관련 CA에 연결하는 인증서 체인을 제공합니다.

다음은 CDO가 브라우저와 다른 방식으로 인증서를 사용하는 방법입니다.

- 자체 서명 인증서의 경우 CDO는 도메인 이름 확인을 오버라이드하며, 그 대신 디바이스 온보딩 또는 재연결 중에 인증된 사용자가 신뢰하는 인증서와 인증서가 정확히 일치하는지 확인합니다.
- CDO는 아직 내부 CA를 지원하지 않습니다. 현재는 내부 CA가 서명한 인증서를 확인할 수 있는 방법이 없습니다.

  디바이스별로 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있습니다. CDO에서 ASA의 인증서를 신뢰할 수 없는 경우 해당 디바이스에 대한 인증서 검사를 비활성화할 수 있습니다. 디바이스에 대한 인증서 확인을 비활성화하려고 시도했지만 여전히 디바이스를 온보딩할 수 없는 경우, 디바이스에 대해 지정한 IP 주소 및 포트가 잘못되었거나 연결할 수 없는 것일 수 있습니다. 인증서 검사를 전역적으로 비활성화하거나 지원되는 인증서가 있는 디바이스에 대한 인증서 검사를 비활성화할 수 있는 방법은 없습니다. 비 ASA 디바이스에 대한 인증서 확인을 비활성화할 수 있는 방법은 없습니다.

  디바이스에 대한 인증서 확인을 비활성화하면 CDO는 TLS를 사용하여 디바이스에 연결하지만 연결을 설정하는 데 사용된 인증서를 검증하지 않습니다. 즉, 수동적인 중간자 공격자는 연결을 도청할 수 없지만, 활성 상태의 중간자 공격자는 CDO에 유효하지 않은 인증서를 제공하여 연결을 가로챌 수 있습니다.

인증서 문제 식별

CDO가 디바이스를 온보딩하지 못할 수 있는 몇 가지 이유가 있습니다. UI에 "CDO cannot connect to the device using the certificate presented(제공된 인증서를 사용하여 디바이스에 연결할 수 없음)"라는 메시지가 표시되면 인증서에 문제가 있는 것입니다. UI에 이 메시지가 표시되지 않으면 연결 문제(디바이스에 연결할 수 없음) 또는 기타 네트워크 오류와 관련이 있을 가능성이 높습니다.

CDO가 지정된 인증서를 거부하는 이유를 확인하려면 SDC 호스트 또는 관련 디바이스에 연결할 수 있는 다른 호스트에서 openssl 명령줄 툴을 사용할 수 있습니다. 다음 명령을 사용하여 디바이스에서 제공하는 인증서를 보여주는 파일을 생성합니다.

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

이 명령은 인터랙티브 세션을 시작하므로 몇 초 후에 종료하려면 Ctrl-c를 사용해야 합니다.

이제 다음과 같은 출력이 포함된 파일이 생성됩니다.

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
```

```
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
```

```
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

이 출력에서 가장 먼저 확인할 사항은 반환 코드 확인이 표시되는 마지막 줄입니다. 인증서 문제가 있는 경우 반환 코드는 0이 아니며 오류에 대한 설명이 표시됩니다.

일반적인 오류 및 해결 방법을 보려면 이 인증서 오류 코드 목록을 확장합니다.

0 X509_V_OK 작업에 성공했습니다.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT 신뢰할 수 없는 인증서의 발급자 인증서를 찾을 수 없습니다.

3 X509_V_ERR_UNABLE_TO_GET_CRL 인증서의 CRL을 찾을 수 없습니다.

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE 인증서 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 이는 RSA 키에만 의미가 있습니다.

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE CRL 서명을 해독할 수 없습니다. 이는 실제 서명 값이 예상 값과 일치하지 않는 것이 아니라 확인할 수 없음을 의미합니다. 사용되지 않음.

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY 인증서 SubjectPublicKeyInfo의 공개 키를 읽을 수 없습니다.

7 X509_V_ERR_CERT_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.

8 X509_V_ERR_CRL_SIGNATURE_FAILURE 인증서의 서명이 유효하지 않습니다.

9 X509_V_ERR_CERT_NOT_YET_VALID 인증서가 아직 유효하지 않습니다. notBefore 날짜가 현재 시간 이후입니다. 자세한 내용은 아래의 반환 코드 확인: 9(인증서가 아직 유효하지 않음)를 참조하십시오.

10 X509_V_ERR_CERT_HAS_EXPIRED 인증서가 만료되었습니다. 즉, notAfter 날짜는 현재 시간 이전입니다. 자세한 내용은 아래의 반환 코드 확인: 10(인증서가 만료되었습니다)을 참조하십시오.

11 X509_V_ERR_CRL_NOT_YET_VALID CRL이 아직 유효하지 않습니다.

12 X509_V_ERR_CRL_HAS_EXPIRED CRL이 만료되었습니다.

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD 인증서 notBefore 필드에 잘못된 시간이 포함되어 있습니다.

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD 인증서 notAfter 필드에 유효하지 않은 시간이 포함되어 있습니다.

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD CRL lastUpdate 필드에 잘못된 시간이 포함되어 있습니다.

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD CRL nextUpdate 필드에 유효하지 않은 시간이 포함되어 있습니다.

17 X509_V_ERR_OUT_OF_MEM 메모리를 할당하는 동안 오류가 발생했습니다. 이러한 현상은 발생해서는 안 됩니다.

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT 전달된 인증서가 자체 서명되었으며 신뢰할 수 있는 인증서 목록에서 동일한 인증서를 찾을 수 없습니다.

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN 신뢰할 수 없는 인증서를 사용하여 인증서 체인을 배포할 수 있지만 루트를 로컬에서 찾을 수 없습니다.

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 로컬로 조회된 인증서의 발급자 인증서를 찾을 수 없습니다. 이는 일반적으로 신뢰할 수 있는 인증서 목록이 완전하지 않음을 의미합니다.

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE 체인에 하나의 인증서만 포함되어 있으며 자체 서명되지 않았으므로 서명을 확인할 수 없습니다. 자세한 내용은 아래의 "반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)"를 참조하십시오. 자세한 내용은 아래의 반환 코드 확인: 21(첫 번째 인증서를 확인할 수 없음)을 참조하십시오.

22 X509_V_ERR_CERT_CHAIN_TOO_LONG 인증서 체인 길이가 제공된 최대 깊이보다 큽니다. 사용되지 않음.

23 X509_V_ERR_CERT_REVOKED 인증서가 해지되었습니다.

24 X509_V_ERR_INVALID_CA CA 인증서가 유효하지 않습니다. CA가 아니거나 확장명이 제공된 목적과 일치하지 않습니다.

25 X509_V_ERR_PATH_LENGTH_EXCEEDED basicConstraints pathlength 매개변수가 초과되었습니다.

26 X509_V_ERR_INVALID_PURPOSE 제공된 인증서를 지정된 용도로 사용할 수 없습니다.

27 X509_V_ERR_CERT_UNTRUSTED 루트 CA가 지정된 용도로 신뢰할 수 있는 것으로 표시되지 않았습니다.

28 X509_V_ERR_CERT_REJECTED 루트 CA가 지정된 용도를 거부하도록 표시되었습니다.

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH 해당 주체 이름이 현재 인증서의 발급자 이름과 일치하지 않아 현재 후보 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

30 X509_V_ERR_AKID_SKID_MISMATCH 현재 후보 발급자 인증서가 거부되었습니다. 해당 주체 키 식별자가 있고 인증 기관 키 식별자가 현재 인증서와 일치하지 않기 때문입니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH 발급자 이름 및 일련 번호가 존재하고 현재 인증서의 기관 키 식별자와 일치하지 않으므로 현재 발급자 인증서가 거부되었습니다. -issuer_checks 옵션이 설정된 경우에만 표시됩니다.

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN keyUsage 확장이 인증서 서명을 허용하지 않으므로 현재 발급자 인증서가 거부되었습니다.

50 X509_V_ERR_APPLICATION_VERIFICATION 애플리케이션 관련 오류입니다. 사용되지 않음.

새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 CDO는 **Configuration Status(**구성 상태**)** 및 **Connectivity(**연결성**)** 상태로 "New Certificate

Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. CDO에서 계속 관리하려면 이 문제를 수동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

Note 두 개 이상의 매니지드 디바이스를 CDO에 동시에 CDO에 디바이스 대량 재연결하는 경우, CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

1. **Inventory(**재고 목록**)** 페이지로 이동합니다.
2. 필터를 사용하여 **New Certificate Detected(**새 인증서 탐지됨**)** 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.
3. 작업창에서 **Review Certificate(**인증서 검토**)**를 클릭합니다. CDO에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.
4. Device Sync(디바이스 동기화) 창에서 **Accept(**수락**)**를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue(**계속**)**를 클릭합니다.

   CDO는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화된 후 디바이스를 확인하려면 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

인증서 오류 코드

반환 코드 확인**: 0 (ok)** 하지만 **CDO**에서 인증서 오류를 반환합니다**.**

CDO에 인증서가 있으면 "https://<device_ip>:<port>"에 GET 호출을 하여 URL에 연결을 시도합니다. 그래도 문제가 해결되지 않으면 CDO에 인증서 오류가 표시됩니다. 인증서가 유효한 경우(openssl에서 0 ok 반환) 연결하려는 포트에서 다른 서비스가 수신 대기하는 문제일 수 있습니다. 다음 명령을 사용할 수 있습니다.

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

ASA와 통신하고 있는지 확인하고 HTTPS 서버가 ASA의 올바른 포트에서 실행 중인지 확인합니다.

```
 # show asp table socket
Protocol         Socket         State         Local Address              Foreign Address
SSL              00019b98        LISTEN        192.168.1.5:443             0.0.0.0:*
SSL              00029e18        LISTEN        192.168.2.5:443             0.0.0.0:*
TCP              00032208        LISTEN        192.168.1.5:22              0.0.0.0:*
```

반환 코드 확인**: 9(**인증서가 아직 유효하지 않음**)**

이 오류는 제공된 인증서의 발급 날짜가 미래이므로 클라이언트가 이를 유효한 것으로 처리하지 않음을 의미합니다. 이는 잘못 구성된 인증서로 인해 발생할 수 있으며, 자체 서명 인증서의 경우 인증서를 생성할 때 잘못된 디바이스 시간이 원인일 수 있습니다.

인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
```

```
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

이 오류를 통해 인증서가 유효한 시점을 확인할 수 있습니다.

치료

인증서의 notBefore 날짜는 과거여야 합니다. 이전 날짜의 인증서를 재발급할 수 있습니다. 이 문제는 클라이언트 또는 발급 디바이스에서 시간이 올바르게 설정되지 않은 경우에도 발생할 수 있습니다.

반환 코드 확인**: 10(**인증서가 만료되었습니다**)**

이 오류는 제공된 인증서 중 하나 이상이 만료되었음을 의미합니다. 인증서의 notBefore 날짜를 포함하는 오류에 줄이 표시되어야 합니다.

```
 error 10 at 0 depth lookup:certificate has expired
```

만료 날짜는 인증서 본문에 있습니다.

치료

인증서가 실제로 만료된 경우 유일한 교정 방법은 다른 인증서를 가져오는 것입니다. 인증서의 만료 날짜가 아직 미래이지만 openssl이 만료되었다고 주장하는 경우, 컴퓨터의 시간과 날짜를 확인합니다. 예를 들어 인증서가 2020년에 만료되도록 설정되어 있지만 컴퓨터의 날짜가 2021년이면 컴퓨터는 해당 인증서를 만료된 것으로 처리합니다.

반환 코드 확인**: 21(**첫 번째 인증서를 확인할 수 없음**)**

이 오류는 인증서 체인에 문제가 있음을 나타내며, openssl은 디바이스에서 제공하는 인증서를 신뢰할 수 있는지 확인할 수 없습니다. 인증서 체인이 작동하는 방식을 확인하려면 위의 예에서 인증서 체인을 살펴보겠습니다.

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
```

```
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

인증서 체인은 서버에서 제공하는 인증서 목록으로, 서버의 자체 인증서부터 시작하여 점점 더 높은 수준의 중간 인증서를 포함하여 서버의 인증서를 인증 기관의 최상위 인증서와 연결합니다. 각 인증서에는 해당 주체(':'로 시작하는 줄) 및 발급자('i'로 시작하는 줄)가 나열됩니다.

주체는 인증서로 식별되는 엔티티입니다. 여기에는 조직 이름이 포함되며 경우에 따라 인증서가 발급된 엔티티의 공용 이름이 포함됩니다.

발급자는 인증서를 발급한 엔티티입니다. 여기에는 Organization(조직) 필드도 포함되며, 경우에 따라 Common Name(일반 이름)도 포함됩니다.

서버에 신뢰할 수 있는 인증 기관에서 직접 발급한 인증서가 있는 경우 인증서 체인에 다른 인증서를 포함할 필요가 없습니다. 다음과 같은 인증서를 제공합니다.

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

이 인증서가 제공되면 openssl은 ***.example.com**에 대한 ExampleCo 인증서가 신뢰할 수 있는 기관 인증서에 의해 올바르게 서명되었는지 확인합니다. 이 인증서는 openssl의 기본 제공 신뢰 저장소에 있습니다. 확인 후 openssl이 디바이스에 성공적으로 연결됩니다.

그러나 대부분의 서버에는 신뢰할 수 있는 CA에서 직접 서명한 인증서가 없습니다. 대신 첫 번째 예에서와 같이 서버의 인증서가 하나 이상의 중간 인증서에 의해 서명되고, 최상위 중간 인증서에는 신뢰할 수 있는 CA가 서명한 인증서가 있습니다. OpenSSL은 기본적으로 이러한 중간 CA를 신뢰하지 않으며, 신뢰할 수 있는 CA로 끝나는 완전한 인증서 체인이 제공되는 경우에만 이를 확인할 수 있습니다.

중간 기관이 인증서에 서명한 서버는 모든 중간 인증서를 포함하여 이를 신뢰할 수 있는 CA에 연결하는 모든 인증서를 제공해야 합니다. 이 전체 체인을 제공하지 않는 경우 openssl의 출력은 다음과 같습니다.

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
```

```
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

이 출력은 서버가 하나의 인증서만 제공했으며 제공된 인증서가 신뢰할 수 있는 루트가 아닌 중간 기관에 의해 서명되었음을 보여줍니다. 출력에는 특성 확인 오류도 표시됩니다.

치료

이 문제는 디바이스에서 제공하는 인증서가 잘못 구성되어 발생합니다. CDO 또는 다른 프로그램이 디바이스에 안전하게 연결할 수 있도록 이 문제를 해결하는 유일한 방법은 올바른 인증서 체인을 디바이스에 로드하여 연결하는 클라이언트에 완전한 인증서 체인을 제공하도록 하는 것입니다.

트러스트 포인트에 중간 CA를 포함하려면 아래 링크 중 하나를 따르십시오(CSR이 ASA에서 생성되었는지 여부에 따라).

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

새 인증서 탐지됨

자체 서명 인증서가 있는 디바이스를 업그레이드하고 업그레이드 프로세스 후에 새 인증서가 생성되는 경우 CDO는 **Configuration Status(**구성 상태**)** 및 **Connectivity(**연결성**)** 상태로 "New Certificate Detected(새 인증서 탐지됨)" 메시지를 생성할 수 있습니다. CDO에서 계속 관리하려면 이 문제를 수

동으로 확인하고 해결해야 합니다. 인증서가 동기화되고 디바이스가 정상 상태가 되면 디바이스를 관리할 수 있습니다.

참고 두 개 이상의 매니지드 디바이스를 CDO에 동시에 CDO에 디바이스 대량 재연결하는 경우, CDO는 디바이스에서 새 인증서를 자동으로 검토 및 수락하고 계속해서 다시 연결합니다.

다음 절차를 사용하여 새 인증서를 확인합니다.

프로시저

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭합니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 필터를 사용하여 **New Certificate Detected(**새 인증서 탐지됨**)** 연결 또는 구성 상태의 디바이스를 표시하고 원하는 디바이스를 선택합니다.

단계 **5** 작업창에서 **Review Certificate(**인증서 검토**)**를 클릭합니다. CDO에서는 검토를 위해 인증서를 다운로드하고 새 인증서를 수락할 수 있습니다.

단계 **6** Device Sync(디바이스 동기화) 창에서 **Accept(**수락**)**를 클릭하거나 Reconnecting to Device(디바이스에 다시 연결 중) 창에서 **Continue(**계속**)**를 클릭합니다.

CDO는 디바이스를 새 자체 서명 인증서와 자동으로 동기화합니다. 디바이스가 동기화된 후 디바이스를 확인하려면 페이지를 수동으로 새로 고쳐야 할 수 있습니다.

온보딩 오류 문제 해결

디바이스 온보딩 오류는 여러 가지 이유로 발생할 수 있습니다.

다음과 같은 작업을 수행할 수 있습니다.

Procedure

단계 **1** **Inventory(**재고 목록**)** 페이지에서 **Devices(**장치 **)** 탭을 클릭합니다.

단계 **2** 적절한 디바이스 유형 탭을 클릭하고 이 오류가 발생하는 디바이스를 선택합니다. 경우에 따라 오른쪽에 오류 설명이 표시됩니다. 설명에 언급된 필요한 조치를 취하십시오.

또는

단계 **3** CDO에서 디바이스 인스턴스를 제거하고 디바이스 온보딩을 다시 시도하십시오.

충돌 탐지됨 상태 해결

CDO를 사용하면 각 라이브 디바이스에서 충돌 탐지를 활성화하거나 비활성화할 수 있습니다. 충돌 탐지, on page 145이 활성화되어 있고 CDO를 사용하지 않고 디바이스의 구성을 변경한 경우, 디바이스의 구성 상태는 **Conflict Detected(**충돌 탐지됨**)**로 표시됩니다.

"충돌 탐지됨" 상태를 해결하려면 다음 절차를 수행합니다.

Procedure

단계 **1** 내비게이션 바에서 **Inventory(**재고 목록**)**를 클릭합니다.

Note
온프레미스 방화벽 Management Center의 경우, **Tools & Services(**도구 및 서비스**)** > **Firewall Management Center**로 이동하여 **Not Synced(**동기화되지 않음**)** 상태인 FMC를 선택하고 5단계부터 계속 진행합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 충돌을 보고하는 디바이스를 선택하고 오른쪽의 세부 정보 창에서 **Review Conflict(**충돌 검토**)**를 클릭합니다.

단계 **5** **Device Sync(**디바이스 동기화**)** 페이지에서 강조 표시된 차이점을 검토하여 두 구성을 비교합니다.

- "Last Known Device Configuration(마지막으로 알려진 디바이스 구성)" 패널은 CDO에 저장된 디바이스 구성입니다.
- "Found on Device(디바이스에서 발견됨)" 패널은 ASA에서 실행 중인 구성에 저장된 구성입니다.

단계 **6** 다음 중 하나를 선택하여 충돌을 해결합니다.

- **Accept Device changes(**디바이스 변경 사항 수락**)**: 구성 및 CDO에 저장된 보류 중인 변경 사항을 디바이스의 실행 중인 구성으로 덮어씁니다.

  Note
  CDO는 명령줄 인터페이스 외부에서 Cisco IOS 디바이스에 변경 사항을 구축하는 것을 지원하지 않으므로, 충돌을 해결할 때 Cisco IOS 디바이스에 대한 유일한 선택은 **Accept Without Review(**검토 없이 수락**)**를 선택하는 것입니다.

- **Reject Device Changes(**디바이스 변경 거부**)**: 디바이스에 저장된 구성을 CDO에 저장된 구성으로 덮어씁니다.

Note
거부되거나 수락된 모든 구성 변경 사항은 변경 로그에 기록됩니다.

동기화되지 않음 상태 해결

다음 절차를 사용하여 구성 상태가 "동기화되지 않음"인 디바이스를 확인합니다.

Procedure

단계 **1** 내비게이션 바에서 **Inventory(**재고 목록**)**를 클릭합니다.

Note
온프레미스 방화벽 Management Center의 경우, **Tools & Services(**도구 및 서비스**)** > **Firewall Management Center**로 이동하여 **Not Synced(**동기화되지 않음**)** 상태인 FMC를 선택하고 5단계부터 계속 진행합니다.

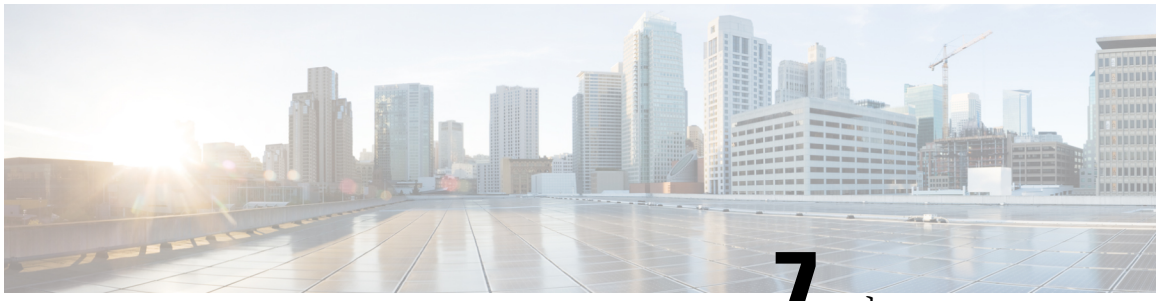
단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** 동기화되지 않은 것으로 보고된 디바이스를 선택합니다.

단계 **5** 오른쪽의 동기화되지 않음 패널에서 다음 중 하나를 선택합니다.

- 미리보기 및 배포**...** - CDO에서 디바이스로 구성 변경 사항을 푸시하려면 지금 수행한 변경 사항을 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축하거나 한 번에 여러 변경 사항을 기다렸다가 배포하십시오.
- 변경 사항 취소 - CDO에서 디바이스로 구성 변경을 푸시하지 않으려는 경우, 또는 CDO에서 시작한 구성 변경을 "취소"하려는 경우. 이 옵션은 CDO에 저장된 구성을 디바이스에 저장된 실행 중인 구성으로 덮어씁니다.



7 장

FAQ 및 지원

이 장에는 다음 섹션이 포함되어 있습니다.

Cisco Defense Orchestrator

Cisco Defense Orchestrator는 무엇입니까**?**

Cisco Defense Orchestrator는 네트워크 관리자가 다양한 보안 디바이스에서 일관된 보안 정책을 만들고 유지할 수 있도록 하는 클라우드 기반 다중 디바이스 관리자입니다.

CDO를 디바이스를 관리하는 데 사용할 수 있습니다.

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Threat Defense
- Cisco Umbrella
- Meraki
- Cisco IOS 디바이스
- 아마존 웹 서비스(AWS) 인스턴스
- SSH 연결을 사용하여 관리되는 디바이스

CDO 관리자는 단일 인터페이스를 통해 이러한 모든 디바이스 유형을 모니터링하고 유지할 수 있습니다.

CDO에 디바이스 온보딩 관련 FAQ

CDO에 Secure Firewall ASA 온보딩 관련 FAQ

자격 증명을 사용하여 어떻게 **ASA**를 온보딩합니까**?**

ASA를 한 번에 하나씩 온보딩하거나 대량 작업으로 온보딩할 수 있습니다. 고가용성 쌍의 일부인 ASA를 온보딩하는 경우 쌍의 기본 디바이스만 온보딩하는 데 ASA 디바이스 온보딩을 사용합니다. 보안 상황 또는 관리 상황을 온보딩하는 방법은 다른 ASA를 온보딩하는 방법과 동일합니다.

한 번에 하나 이상의 **ASA**를 온보딩하려면 어떻게 해야 합니까**?**

CSV 파일을 사용하여 ASA 목록을 생성할 수 있으며, CDO는 목록의 모든 ASA를 온보딩합니다. 대량 ASA 온보딩에 대한 지침은 대량 ASA 온보드를 참조하십시오.

ASA를 온보딩한 후 무엇을 해야 합니까**?**

시작하려면 Cisco Defense Orchestrator로 ASA 관리를 참조하십시오.

CDO에 FDM 매니지드 디바이스 온보딩 관련 FAQ

FDM 매니지드 디바이스를 온보딩하려면 어떻게 해야 합니까**?**

FDM 매니지드 디바이스를 온보딩하는 다양한 방법이 있습니다. 등록 키 방법을 사용하는 것이 좋습니다. 시작하려면 FDM 매니지드 디바이스 온보딩을 참조하십시오.

클라우드제공FirewallManagementCenter에SecureFirewallThreatDefense 온보딩 관련 FAQ

Secure Firewall Threat Defense를 온보딩하려면 어떻게 합니까**?**

CLI 등록 키, 제로 터치 프로비저닝 또는 일련 번호를 사용하여 FTD 디바이스를 온보딩할 수 있습니다.

Secure Firewall Threat Defense를 온보딩한 후에는 어떻게 해야 합니까**?**

디바이스가 동기화되면 Tools & Services(툴 및 서비스) > Firewall Management Center로 이동하여 Actions(작업), Management(관리) 또는 Settings(설정) 창에서 작업을 선택하여 클라우드 제공 Firewall Management Center에서 Threat Defense 디바이스의 구성을 시작합니다. 시작하려면 클라우드 사용 Firewall Management Center 애플리케이션 페이지를 참조하십시오.

Secure Firewall Threat Defense 문제를 어떻게 해결합니까**?**

Secure Firewall Threat Defense 온보딩 문제 해결을 참조하십시오.

온프레미스 Secure Firewall Management Center 관련 FAQ

온프레미스 **Management Center**를 온보딩하려면 어떻게 합니까**?**

온프레미스 Management Center를 CDO에 온보딩할 수 있습니다. 온프레미스 Management Center를 온보딩하면 온프레미스 Management Center에 등록된 모든 디바이스도 온보딩됩니다. CDO는 온프레미스 Management Center 또는 온프레미스 Management Center에 등록된 디바이스와 관련된 개체 또는 정책을 만들거나 수정하는 것은 지원하지 않습니다. 온프레미스 Management Center UI에서 이러한 변경을 수행해야 합니다. 시작하려면 온프레미스 Management Center 온보딩을 참조하십시오.

CDO에 Meraki 디바이스 온보딩 관련 FAQ

Meraki 디바이스를 온보딩하려면 어떻게 해야 합니까**?**

MX 디바이스는 CDO와 Meraki 대시보드에서 모두 관리할 수 있습니다. CDO는 구성 변경 사항을 Meraki 대시보드에 구축하며, 그러면 구성이 디바이스에 안전하게 구축됩니다. 시작하려면 Meraki MX 디바이스 온보딩을 참조하십시오.

CDO에 SSH 디바이스 온보딩 관련 FAQ

SSH 디바이스를 어떻게 온보딩합니까**?**

SSH 디바이스에 저장된 높은 권한을 가진 사용자의 사용자 이름과 암호를 사용하여 SDC(보안 디바이스 커넥터)로 디바이스를 온보딩할 수 있습니다. 시작하려면 SSH 디바이스 온보딩을 참조하십시오.

디바이스를 삭제하려면 어떻게 합니까**?**

재고 목록 페이지에서 디바이스를 삭제할 수 있습니다.

CDO에 IOS 디바이스 온보딩 관련 FAQ

Cisco IOS 디바이스를 어떻게 온보딩합니까**?**

SDC(보안 디바이스 커넥터)를 사용하여 Cisco IOS(Internetwork Operating System)를 실행하는 라이브 Cisco 디바이스를 온보딩할 수 있습니다. 시작하려면 Cisco IOS 디바이스 온보딩을 참조하십시오.

디바이스를 삭제하려면 어떻게 합니까**?**

Inventory(재고 목록) 페이지에서 디바이스를 삭제할 수 있습니다.

디바이스 유형

ASA(Adaptive Security Appliance)란 무엇입니까?

Cisco ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 디바이스 기능을 하나의 디바이스에서 제공하며 애드온 모듈과 통합된 서비스를 제공합니다. ASA에는 다중 보안 상황(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(Layer 2) 방화벽 또는 라우팅(Layer 3) 방화벽 가동, 고급 검사 엔진, IPsec VPN, SSL VPN 및 클라이언트리스 SSL VPN 지원 등의 다양한 기능이 포함되어 있습니다. ASA는 가상 머신 또는 지원되는 하드웨어에 설치할 수 있습니다.

ASA 모델이란 무엇입니까?

ASA 모델은 CDO에 온보딩한 ASA 디바이스의 실행 중인 구성 파일의 사본입니다. ASA 모델을 사용하여 디바이스 자체를 온보딩하지 않고도 ASA 디바이스의 구성을 분석할 수 있습니다.

디바이스는 언제 동기화됩니까?

CDO의 구성과 디바이스에 로컬로 저장된 구성이 동일한 경우.

디바이스가 언제 동기화되지 않습니까?

CDO에 저장된 구성이 변경되어 이제 디바이스에 로컬로 저장된 구성과 다른 경우.

디바이스가 충돌 감지 상태인 경우는 언제입니까?

디바이스의 구성이 CDO(대역 외) 외부에서 변경되어 이제 CDO에 저장된 구성과 다른 경우.

OOB(out-of-band) 변경이란 무엇입니까?

CDO 외부에서 디바이스가 변경된 경우. CLI 명령을 사용하거나 ASDM 또는 FDM과 같은 온디바이스 관리자를 사용하여 디바이스에서 직접 변경합니다. 대역 외 변경으로 인해 CDO는 디바이스에 대해 "충돌 감지" 상태를 보고합니다.

디바이스에 변경 사항을 배포한다는 것은 무엇을 의미합니까?

디바이스를 CDO에 등록한 후 CDO는 해당 구성의 복사본을 유지 관리합니다. CDO를 변경하면 CDO는 디바이스 구성의 사본을 변경합니다. 변경 사항을 디바이스에 다시 "구축"하면 CDO는 디바이스의 구성 복사본에 대한 변경 사항을 복사합니다. 다음 항목을 참조하십시오.

- 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축, on page 138

현재 지원되는 ASA 명령은 무엇입니까?

모든 명령 디바이스 활동 아래에 **Command Line Interface(**명령줄 인터페이스**)**를 클릭하여 ASA CLI를 사용합니다.

디바이스 관리에 대한 규모 제한이 있습니까?

CDO의 클라우드 아키텍처를 통해 수천 개의 디바이스로 확장할 수 있습니다.

CDO는 **Cisco Integrated Services Routers** 및 **Aggregation Services Routers**를 관리합니까?

CDO를 사용하면 ISR 및 ASR에 대한 모델 디바이스를 생성하고 해당 구성을 가져올 수 있습니다. 그런 다음 가져온 구성을 기반으로 템플릿을 생성하고 일관된 보안을 위해 신규 또는 기존 ISR 및 ASR 디바이스에 배포할 수 있는 표준화된 구성으로 구성을 내보낼 수 있습니다.

CDO가 **SMA**를 관리할 수 있습니까?

아니오, CDO는 현재 SMA를 관리하지 않습니다.

보안

CDO는 안전합니까?

CDO는 다음 기능을 통해 고객 데이터에 대한 엔드투엔드 보안을 제공합니다.

- 새 CDO 테넌트에 대한 초기 로그인, on page 4
- API 및 데이터베이스 작업에 대한 인증 호출
- 이동 중 및 유휴 상태의 데이터 격리
- 역할 분리

CDO는 사용자가 클라우드 포털에 연결할 때 다단계 인증을 요구합니다. 다단계 인증은 고객의 신원을 보호하는 데 필요한 필수 기능입니다.

이동 중이거나 유휴 상태의 모든 데이터는 암호화됩니다. 고객 프레미스 및 CDO의 디바이스와의 통신은 SSL로 암호화되며 모든 고객 테넌트 데이터 볼륨은 암호화됩니다.

CDO의 다중 테넌트 아키텍처는 테넌트 데이터를 격리하고 데이터베이스와 애플리케이션 서버 간의 트래픽을 암호화합니다. 사용자가 CDO에 액세스하기 위해 인증하면 토큰을 받습니다. 이 토큰은 키 관리 서비스에서 키를 가져오는 데 사용되며 키는 데이터베이스에 대한 트래픽을 암호화하는 데 사용됩니다.

CDO는 고객 자격 증명을 보호하면서 신속하게 고객에게 가치를 제공합니다. 이는 자격 증명 데이터가 고객 프레미스를 떠나지 않도록 모든 인바운드 및 아웃바운드 트래픽을 제어하는 클라우드 또는 고객 자체 네트워크(로드맵)에 "보안 데이터 커넥터"를 배포하여 달성됩니다.

CDO에 처음 로그인할 때 **"OTP**를 확인할 수 없음**"** 오류가 발생했습니다**.**

데스크톱 또는 모바일 디바이스 시계가 세계 시간 서버와 동기화되어 있는지 확인합니다. 시계가 1분 미만 또는 그 이상 동기화되지 않으면 잘못된 OTP가 생성될 수 있습니다.

디바이스가 **CDO** 클라우드 플랫폼에 직접 연결되어 있습니까**?**

예. 보안 연결은 디바이스와 CDO 플랫폼 간의 프록시로 사용되는 CDO SDC를 사용하여 수행됩니다 보안을 최우선으로 고려하여 설계된 CDO 아키텍처를 사용하면 디바이스를 오가는 데이터를 완전히 분리할 수 있습니다.

공용 **IP** 주소가 없는 디바이스를 어떻게 연결할 수 있습니까**?**

네트워크 내에 배포할 수 있고 외부 포트를 열 필요가 없는 CDO 보안 디바이스 커넥터를 활용할 수 있습니다. SDC가 배포되면 내부(인터넷 라우팅 불가) IP 주소로 디바이스를 온보딩할 수 있습니다.

SDC에 추가 비용이나 라이선스가 필요합니까**?**

아니요.

터널 상태를 어떻게 확인할 수 있습니까**?** 상태 옵션

CDO는 매시간 터널 연결 확인을 자동으로 수행하지만, 터널을 선택하고 연결 확인을 요청하여 임시 VPN 터널 연결 확인을 수행할 수 있습니다. 결과를 처리하는 데 몇 초가 걸릴 수 있습니다.

디바이스 이름과 피어 중 하나의 **IP** 주소를 기반으로 터널을 검색할 수 있습니까**?**

예. 이름과 피어 IP 주소 모두에서 사용 가능한 필터 및 검색 기능을 사용하여 특정 VPN 터널 세부 정보를 검색하고 피벗합니다.

문제 해결

CDO에서 관리 디바이스로 디바이스 구성을 완전히 배포하는 동안 **"**변경 사항을 디바이스에 배포할 수 없습니다**"**라는 경고가 표시됩니다**.** 해결하려면 어떻게 해야 하나요**?**

전체 구성(CDO 지원 명령 이상으로 수행된 변경 사항)을 디바이스에 배포할 때 오류가 발생하면 "변경 사항 확인"을 클릭하여 디바이스에서 사용 가능한 최신 구성을 가져옵니다. 이렇게 하면 문제가 해결될 수 있으며 계속해서 CDO를 변경하고 배포할 수 있습니다. 문제가 지속되면 **Contact Support(**지원 문의**)** 페이지에서 Cisco TAC에 문의하십시오.

대역 외 문제**(CDO** 외부에서 수행된 변경**,** 디바이스에 직접 변경**)**를 해결하는 동안 **CDO**에 있는 구성과 디바이스의 구성을 비교하는 동안 **CDO**는 내가 추가하거나 편집하지 않은 추가 메타데이터를 제공합니다**.** 왜 그럴까요**?**

CDO가 기능을 확장함에 따라 더 나은 정책 및 디바이스 관리 분석을 위해 필요한 모든 데이터를 강화하고 유지하기 위해 디바이스 구성에서 추가 정보가 수집됩니다. 이는 관리되는 디바이스에서 발생한 변경 사항이 아니라 이미 존재하는 정보입니다. 충돌 감지 상태를 해결하는 것은 디바이스에서 변경 사항을 확인하고 발생한 변경 사항을 검토하여 쉽게 해결할 수 있습니다.

CDO가 내 인증서를 거부하는 이유는 무엇입니까**?**

새 인증서 문제 해결을 참조하십시오.

제로 터치 프로비저닝에서 사용되는 용어 및 정의

- 클레임됨 - CDO에서 일련 번호 온보딩의 컨텍스트에서 사용됩니다. 일련 번호가 CDO 테넌트에 온보딩된 경우 디바이스가 "클레임"됩니다.
- 파킹됨 - CDO에서 일련 번호 온보딩의 컨텍스트에서 사용됩니다. Cisco Cloud에 연결되어 있고 CDO 테넌트가 일련 번호를 요청하지 않은 경우 디바이스는 "파킹"됩니다.
- 초기 프로비저닝 - 초기 FTD 설정의 컨텍스트에서 사용됩니다. 이 단계에서 디바이스는 EULA를 수락하고, 새 비밀번호를 생성하고, 관리 IP 주소를 구성하고, FQDN을 설정하고, DNS 서버를 설정하고, FDM을 사용하여 디바이스를 로컬로 관리하도록 선택합니다.
- 제로 터치 프로비저닝 - 공장에서 고객 사이트(일반적으로 브랜치 오피스)로 FTD를 배송하고, 사이트의 직원이 FTD를 네트워크에 연결하고, 디바이스가 Cisco Cloud에 연결하는 프로세스입니다. 이 시점에서 일련 번호가 이미 "클레임"되었거나 CDO 테넌트가 클레임할 때까지 FTD가 Cisco Cloud에 "파킹"된 경우 디바이스는 CDO 테넌트에 온보딩됩니다.

정책 최적화

두 개 이상의 액세스 목록(동일한 액세스 그룹 내)이 서로 섀도잉되는 경우를 어떻게 식별할 수 있습니까?

CDO NPM(네트워크 정책 관리)은 규칙 세트 내에서 상위 규칙이 다른 규칙을 가리고 있는지 식별하고 사용자에게 경고할 수 있습니다. 사용자는 모든 네트워크 정책 사이를 탐색하거나 필터링하여 모든 섀도우 문제를 식별할 수 있습니다.

Note CDO는 완전히 섀도우 규칙만 지원합니다.

연결성

보안 디바이스 커넥터가 IP 주소를 변경했지만 CDO에 반영되지 않았습니다. 변경 사항을 반영하려면 어떻게 해야 합니까?

CDO 내에서 새로운 SDC(보안 디바이스 커넥터)를 얻고 업데이트하려면 다음 명령을 사용하여 컨테이너를 다시 시작해야 합니다.

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh restartSDC
 <tenant-name>
```

내 디바이스(**FTD** 또는 **ASA**)를 관리하기 위해 **CDO**에서 사용하는 **IP** 주소가 변경되면 어떻게 됩니까**?**

정적 IP 주소의 변경이든 DHCP로 인한 IP 주소의 변경이든 어떤 이유로든 디바이스의 IP 주소가 변경되면, CDO가 디바이스에 연결하는 데 사용하는 IP 주소를 변경할 수 있습니다(참조 CDO에서 디바이스의 IP 주소 변경, on page 91). 그런 다음 디바이스를 다시 연결합니다(참조 CDO에 디바이스 대량 재연결, on page 97). 장치를 다시 연결할 때 장치의 새 IP 주소를 입력하고 인증 자격 증명을 다시 입력하라는 메시지가 표시됩니다.

내 **ASA**를 **CDO**에 연결하려면 어떤 네트워킹이 필요합니까**?**

- ASDM 이미지가 있고 ASA에 대해 활성화되어 있습니다.
- 52.25.109.29, 52.34.234.2, 52.36.70.147에 대한 공용 인터페이스 액세스
- ASA의 HTTPS 포트는 443 또는 1024 이상의 값으로 설정해야 합니다. 예를 들어 포트 636으로 설정할 수 없습니다.
- 관리 중인 ASA도 AnyConnect VPN 클라이언트 연결을 허용하도록 구성된 경우 ASA HTTPS 포트를 1024 이상의 값으로 변경해야 합니다.

데이터 인터페이스 정보

디바이스와의 통신에 전용 관리 인터페이스 또는 일반 데이터 인터페이스를 사용할 수 있습니다. 외부 인터페이스에서 FTD를 원격으로 관리하거나 별도의 관리 네트워크가 없는 경우 데이터 인터페이스의 CDO 액세스가 유용합니다. CDO에서는 데이터 인터페이스에서 원격으로 관리되는 FTD의 고가용성을 지원합니다.

데이터 인터페이스에서의 FTD 관리 액세스에는 다음과 같은 제한이 있습니다.

- 하나의 물리적 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 CDO를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.

CDO가 개인 정보를 처리하는 방법

CDO가 개인 식별 정보를 처리하는 방법을 알아보려면 Cisco Defense Orchestrator 프라이버시 데이터 시트를 참조하십시오.

CDO 지원 문의

이 장에는 다음 섹션이 포함되어 있습니다.

워크플로우 내보내기

지원 티켓을 열기 전에 경험 문제가 있는 디바이스의 워크플로우를 내보내는 것이 좋습니다. 이 추가 정보는 지원 팀이 문제 해결 노력을 신속하게 식별하고 편집하는 데 도움이 될 수 있습니다.

워크플로우를 내보내려면 다음 절차를 따르십시오.

프로시저

단계 **1** 탐색 모음에서 **Inventory(**재고 목록**)**를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾습니다.

단계 **3** 적절한 디바이스 유형 탭을 클릭하고 문제 해결이 필요한 디바이스를 선택합니다.

필터 또는 검색 표시줄을 사용하여 문제를 해결해야 하는 디바이스를 찾으십시오. 디바이스를 선택하여 강조 표시합니다.

단계 **4** **Device Actions(**장치 작업**)** 창에서 **Workflows(**워크플로우**)**를 선택합니다.

단계 **5** 이벤트 표 위의 페이지 오른쪽 상단에 있는 **Export(**내보내기**)** 버튼을 클릭합니다. 파일은 자동으 로 로컬에 **.json** 파일로 저장됩니다. TAC로 여는 이메일이나 티켓에 이것을 첨부하십시오.

TAC를 사용하여 지원 티켓 열기

30일 평가판 또는 라이선스가 부여된 CDO 계정을 사용하는 고객은 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 열 수 있습니다.

- CDOCDO 고객이 TAC로 지원 티켓을 여는 방법..
- CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법.

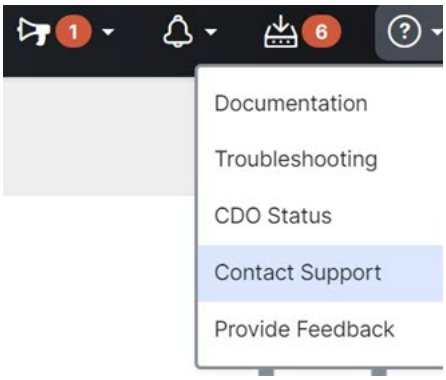
CDO 고객이 TAC로 지원 티켓을 여는 방법.

이 섹션에서는 라이선스가 부여된 CDO 테넌트를 사용하는 고객이 Cisco의 TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법을 설명합니다.

Procedure

단계 1 CDO에 로그인합니다.

단계 2 테넌트 이름 옆에 있는 help(도움말) 버튼을 클릭하고 **Contact Support(**지원 문의**)**를 선택합니다.



단계 3 지원 케이스 관리자를 클릭합니다.

단계 4 파란색 **Open New Case(**새 케이스 열기**)** 버튼을 클릭합니다.

단계 5 **Open a Case(**케이스 열기**)**를 클릭합니다.

단계 6 **Products and Services(**제품 및 서비스**)**를 선택한 다음 **Open Case(**케이스 열기**)**를 클릭합니다.

단계 7 **Request Type(**요청 유형**)**을 선택합니다.

단계 8 **Find Product by Service Agreement(**서비스 계약별 제품 찾기**)** 행을 확장합니다.

단계 9 모든 필드를 입력합니다. 많은 필드가 명확합니다. 다음은 몇 가지 추가 정보입니다.

- **Product Name(**제품 이름**) (PID)** - 이 번호가 더 이상 없는 경우 Cisco Defense Orchestrator 데이터시트를 참조하십시오.
- **Product Description(**제품 설명**)** - PID에 대한 설명입니다.
- **Site Name(**사이트 이름**)** - 사이트 이름을 입력합니다. 고객 중 한 명의 케이스를 여는 Cisco 파트너인 경우 고객의 이름을 입력합니다.
- **Service Contract(**서비스 계약**)** - 서비스 계약 번호를 입력합니다.
  - 중요: 케이스를 Cisco.com 어카운트와 연결하려면 계약 번호를 Cisco.com 프로파일에 연결해야 합니다. 이 절차를 사용하여 계약 번호를 Cisco.com 프로파일에 연결합니다.
    a. Cisco Profile Manager를 엽니다.
    b. **Access Management(**액세스 관리**)** 탭을 클릭합니다.
    c. **Add Access(**액세스 추가**)**를 클릭합니다.

d. **TAC and RMA case creation, Software Download, support tools, and entitled content on Cisco.com(TAC 및 RMA 케이스 생성, 소프트웨어 다운로드, 지원 툴, Cisco.com의 자격 콘텐츠)**를 선택하고 **Go(**이동**)**를 클릭합니다.

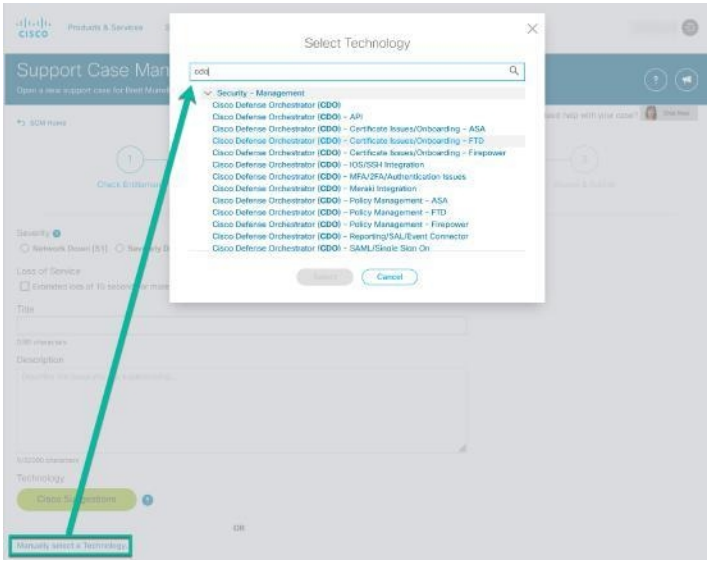
e. 제공된 공간에 서비스 계약 번호를 입력하고 **Submit(**제출**)**을 클릭합니다. 서비스 계약 연결이 완료되었다는 알림이 이메일로 전송됩니다. 서비스 계약 연결을 완료하는 데 최대 6시간이 걸릴 수 있습니다.

Important
중요: 아래 링크에 액세스할 수 없는 경우 공인 Cisco 파트너 또는 리셀러, Cisco 어카운트 담당자 또는 Cisco 서비스 계약 정보를 관리하는 회사 내 담당자에게 문의하십시오.

단계 **10** **Next(**다음**)**를 클릭합니다.

단계 **11** **Describe Problem(**문제 설명**)** 화면에서 아래로 스크롤하여 **Manually select a Technology(**수동으로 기술 선택**)**를 클릭하고 검색 필드에 **CDO**를 입력합니다.

단계 **12** 요청과 가장 일치하는 범주를 선택하고 **Select(**선택**)**를 클릭합니다.



단계 **13** 서비스 요청의 나머지 부분을 완료하고 **Submit(**제출**)**을 클릭합니다.

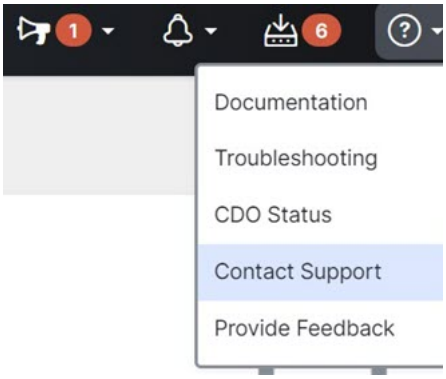
CDO 평가판 고객이 TAC를 사용하여 지원 티켓을 여는 방법

이 섹션에서는 CDO 테넌트의 무료 평가판을 사용하는 고객이 Cisco TAC(Technical Assistance Center)에서 지원 티켓을 여는 방법에 대해 설명합니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** 테넌트 및 계정 이름 옆에 있는 help(도움말) 버튼을 클릭하고 **Contact Support(**지원 문의**)**를 선택합니다.



단계 **3** 아래에 문제 또는 요청 입력 필드에서 직면한 문제 또는 요청을 지정하고 **Submit(**제출**)**를 클릭합니다.

기술 정보와 함께 귀하의 요청이 지원 팀으로 전송되고 기술 지원 엔지니어가 귀하의 질문에 응답합니다.

CDO 서비스 상태 페이지

CDO는 CDO 서비스가 작동 중이고 서비스 중단이 있었는지 여부를 보여주는 고객 대면 서비스 상태 페이지를 유지 관리합니다. 일별, 주별 또는 월별 그래프로 가동 시간 정보를 볼 수 있습니다.

CDO의 모든 페이지에 있는 도움말 메뉴에서 **CDO Status**를 클릭하면 CDO 상태 페이지에 도달할 수 있습니다.

상태 페이지에서 **Subscribe to Updates(**업데이트 구독**)**를 클릭하면 CDO 서비스가 다운될 경우 알림을 받을 수 있습니다.