



Cisco Defense Orchestrator의 기본 사항

Cisco Defense Orchestrator (CDO)는 명확하고 간결한 인터페이스를 통해 정책 관리에 대한 고유한 보기를 제공합니다. 다음은 CDO를 처음 사용할 때 기본 사항을 다루는 항목입니다.

- 네트워크 요구 사항, 2 페이지
- CDO 테넌트 요청, on page 8
- 라이선스, 8 페이지
- SDC(Secure Device Connector), 11 페이지
- CDO에 로그인, 39 페이지
- **Cisco Secure Cloud Sign On** ID 제공자로 마이그레이션, 41 페이지
- Cisco Secure Cloud Sign On 대시보드에서 CDO 실행, on page 42
- 테넌트에서 슈퍼 관리자 관리, on page 43
- CDO에서 지원하는 소프트웨어 및 하드웨어, 43 페이지
- 브라우저 지원, on page 47
- **Cisco Defense Orchestrator** 플랫폼 유지 관리 일정, 47 페이지
- 테넌트 관리, 48 페이지
- 사용자 관리, 66 페이지
- 사용자 관리의 Active Directory 그룹, 66 페이지
- 새 CDO 사용자 생성, on page 71
- Cisco Defense Orchestrator의 사용자 역할, on page 79
- 사용자 역할에 대한 사용자 레코드 생성, on page 84
- 사용자 역할에 대한 사용자 레코드 편집, on page 85
- 사용자 역할에 대한 사용자 레코드 삭제, on page 86
- 서비스 페이지 정보 보기, 87 페이지
- 디바이스 및 서비스 관리, 90 페이지
- 재고 목록 페이지 정보 보기, 97 페이지
- 레이블 및 필터링, 98 페이지
- 동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기, on page 100
- 검색, on page 101
- 글로벌 검색, 101 페이지
- CDO 명령줄 인터페이스, on page 105

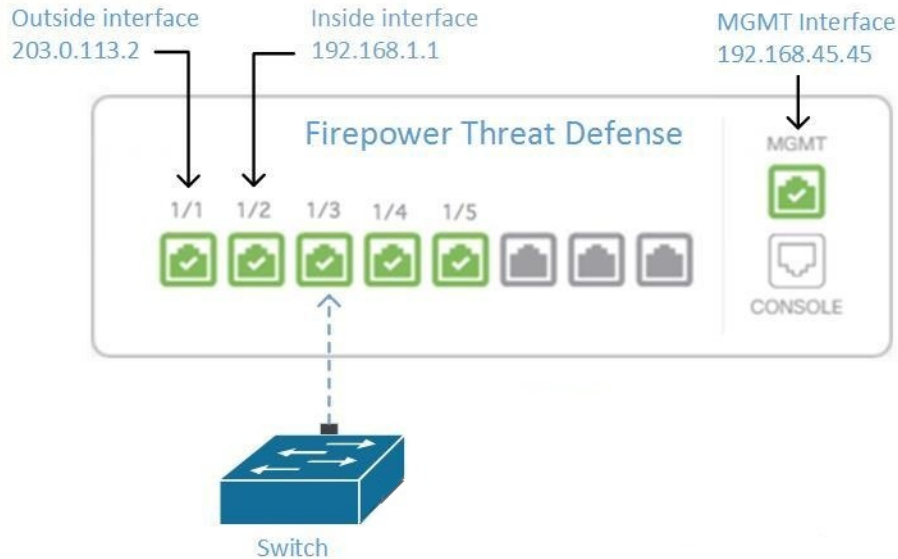
- 대량 명령줄 인터페이스, on page 107
- 디바이스 관리를 위한 CLI 매크로, on page 111
- 명령줄 인터페이스 설명서, on page 115
- CLI 명령 결과 내보내기, on page 115
- 개체, on page 118
- 네트워크 개체, on page 130
- 애플리케이션 필터 개체, on page 140
- 지리위치 개체, on page 143
- DNS 그룹 개체, 145 페이지
- 인증서 개체, on page 147
- IPsec 제안 구성, on page 153
- 글로벌 IKE 정책 구성, on page 156
- RA VPN 개체, 160 페이지
- 보안 영역 개체, on page 160
- 서비스 개체, on page 163
- 보안 그룹 태그 그룹, 166 페이지
- 시스템 로그 서버 개체, 169 페이지
- URL 개체, 172 페이지

네트워크 요구 사항

내부 인터페이스에서 **FDM**-관리 디바이스 관리

전용 MGMT 인터페이스에 조직 내에서 라우팅할 수 없는 주소가 할당된 경우, 내부 인터페이스를 사용하여 FDM 관리 디바이스를 관리하는 것이 바람직할 수 있습니다. 예를 들어 데이터 센터나 연구실 내에서만 연결할 수 있습니다.

Figure 1: 인터페이스 주소



원격 액세스 VPN 요구 사항

CDO로 관리하는 FDM 관리 디바이스가 원격 액세스 VPN(RA VPN) 연결을 관리하는 경우 CDO는 내부 인터페이스를 사용하여 디바이스를 관리해야 합니다.

다음 작업:

FDM 관리 디바이스 구성 절차를 위해 내부 인터페이스에서 FDM-관리 디바이스 관리, on page 3로 계속하십시오.

내부 인터페이스에서 FDM-관리 디바이스 관리

이 구성 방법:

- FDM 관리 디바이스가 CDO에 온보딩되지 않았다고 가정합니다.
- 데이터 인터페이스를 내부 인터페이스로 구성합니다.
- MGMT 트래픽(HTTPS)을 수신하도록 내부 인터페이스를 구성합니다.
- 클라우드 커넥터의 주소가 디바이스의 내부 인터페이스에 도달하도록 허용합니다.

Before you begin

다음 항목에서 이 구성의 사전 요구 사항을 검토합니다.

- 내부 인터페이스에서 FDM-관리 디바이스 관리, on page 2
- 매니지드 디바이스에 Cisco Defense Orchestrator 연결, on page 12

Procedure

단계 1 Secure Firewall device manager에 로그인합니다.

단계 2 **System Settings**(시스템 설정) 메뉴에서 **Management Access**(관리 액세스)를 클릭합니다.

단계 3 **Data Interfaces**(데이터 인터페이스) 탭을 클릭하고 **Create Data Interface**(데이터 인터페이스 생성)를 클릭합니다.

- a. **Interface**(인터페이스) 필드의 인터페이스 목록에서 미리 명명된 "**inside**(내부)" 인터페이스를 선택합니다.
- b. **Protocols**(프로토콜) 필드에서 아직 HTTPS가 아닌 경우 **HTTPS**를 선택합니다.
- c. **Allowed Networks**(허용된 네트워크) 필드에서 FDM 관리 디바이스의 내부 주소에 액세스할 수 있는 조직 내부의 네트워크를 나타내는 네트워크 개체를 선택합니다. SDC 또는 클라우드 커넥터의 IP 주소는 디바이스의 내부 주소에 액세스할 수 있는 주소 중 하나여야 합니다.

인터페이스 주소 다이어그램에서 SDC의 IP 주소 192.168.1.10은 192.168.1.1에 도달할 수 있어야 합니다.

단계 4 변경 사항 배포. 이제 내부 인터페이스를 사용하여 디바이스를 관리할 수 있습니다.

What to do next

클라우드 커넥터를 사용하는 경우 어떻게 됩니까?

위의 절차를 사용하고 다음 단계를 추가합니다.

- 내부 인터페이스(192.168.1.1)에 외부 인터페이스(203.0.113.2)를 "NAT"하는 단계를 추가합니다.
- 위 절차의 3c단계에서 "허용된 네트워크"는 클라우드 커넥터의 공용 IP 주소를 포함하는 네트워크 그룹 개체입니다.
- 클라우드 커넥터의 공용 IP 주소에서 외부 인터페이스(203.0.113.2)에 대한 액세스를 허용하는 액세스 제어 규칙을 생성하는 단계를 추가합니다.

유럽, 중동 또는 아프리카(EMEA) 고객이고, <https://defenseorchestrator.eu>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.

- 35.157.12.126
- 35.157.12.15

미국 고객이고, <https://defenseorchestrator.com>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.

- 52.34.234.2
- 52.36.70.147

AJPC(Asia-Pacific-Japan-China) 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

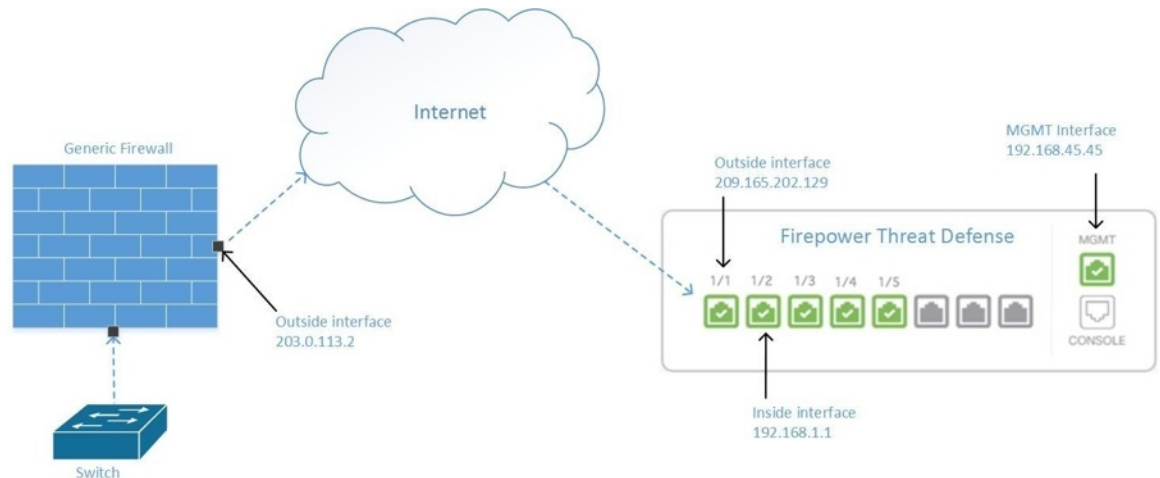
FDM-관리 디바이스 온보딩

등록 토큰 온보딩 접근 방식은 FDM 관리 디바이스를 CDO에 온보딩하는 권장 방법입니다. Cloud Connector에서 FDM 관리 디바이스로의 관리 액세스를 허용하도록 내부 인터페이스를 구성한 후, 사용자 이름과 암호를 사용하여 FDM 관리 디바이스를 온보딩합니다. 자세한 내용은 [사용자 이름, 암호 및 IP 주소를 사용하여 FDM-관리 장치 온보딩](#)을 참조하십시오. 내부 인터페이스의 IP 주소를 사용하여 연결합니다. 위의 시나리오에서 해당 주소는 192.168.1.1입니다.

외부 인터페이스에서 FDM-관리 디바이스 관리

지사에 할당된 하나의 공용 IP 주소가 있고 Cisco Defense Orchestrator가 다른 위치에서 클라우드 커넥터를 사용하여 관리되는 경우 외부 인터페이스에서 클라우드 사용 Firewall Management Center 디바이스를 관리하는 것이 바람직할 수 있습니다.

Figure 2: 외부 인터페이스에서 디바이스 관리



이 구성은 물리적 MGMT 인터페이스가 더 이상 디바이스의 관리 인터페이스가 아님을 의미하지 않습니다. 클라우드 사용 Firewall Management Center 디바이스가 있는 사무실에 있다면 MGMT 인터페이스의 주소에 연결하여 디바이스를 직접 관리할 수 있습니다.

원격 액세스 VPN 요구 사항

클라우드 사용 Firewall Management Center로 관리하는 디바이스가 원격 액세스 VPN(RA VPN) 연결을 관리하는 경우, 클라우드 사용 Firewall Management Center는 외부 인터페이스를 사용하여 클라우

드 사용 Firewall Management Center 디바이스를 관리해야 합니다. 대신 [내부 인터페이스에서 FDM-관리 디바이스 관리](#)를 참조하십시오.

다음 작업:

클라우드 사용 Firewall Management Center 디바이스 구성 절차를 위해 [FDM-관리 디바이스의 외부 인터페이스 관리](#), on page 6로 계속하십시오.

FDM-관리 디바이스의 외부 인터페이스 관리

이 구성 방법:

1. FDM 관리 디바이스가 CDO에 온보딩되지 않았다고 가정합니다.
2. 데이터 인터페이스를 외부 인터페이스로 구성합니다.
3. 외부 인터페이스에서 관리 액세스를 구성합니다.
4. 클라우드 커넥터의 공용 IP 주소(방화벽을 통해 NAT된 후)가 외부 인터페이스에 도달하도록 허용합니다.

Before you begin

다음 항목에서 이 구성의 사전 요구 사항을 검토합니다.

- [FDM-관리 디바이스의 외부 인터페이스 관리](#), on page 6
- [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#), on page 12

Procedure

단계 1 Secure Firewall device manager에 로그인합니다.

단계 2 **System Settings**(시스템 설정) 메뉴에서 **Management Access**(관리 액세스)를 클릭합니다.

단계 3 **Data Interfaces**(데이터 인터페이스) 탭을 클릭하고 **Create Data Interface**(데이터 인터페이스 생성)를 클릭합니다.

- a. **Interface**(인터페이스) 필드의 인터페이스 목록에서 미리 명명된 "**outside**(외부)" 인터페이스를 선택합니다.
- b. **Protocols**(프로토콜) 필드에서 아직 HTTPS가 아닌 경우 **HTTPS**를 선택합니다. CDO은 HTTPS 액세스만 필요합니다.
- c. **Allowed Networks**(허용된 네트워크) 필드에서 방화벽을 통해 NAT된 후 클라우드 커넥터의 공용 IP 주소를 포함하는 호스트 네트워크 개체를 생성합니다.

[Device Management from Outside Interface\(외부 인터페이스의 장치 관리\)](#) 네트워크 다이어그램에서 클라우드 커넥터의 IP 주소인 10.10.10.55는 203.0.113.2로 NAT됩니다. 허용된 네트워크의 경우 값이 203.0.113.2인 호스트 네트워크 개체를 생성합니다.

단계 4 Secure Firewall device manager에서 SDC 또는 클라우드 커넥터의 공용 IP 주소에서 FDM 관리 디바이스의 외부 인터페이스로의 관리 트래픽(HTTPS)을 허용하는 액세스 제어 정책을 생성합니다. 이 시나리오에서 소스 주소는 203.0.113.2이고 소스 프로토콜은 HTTPS입니다. 대상 주소는 209.165.202.129이고 프로토콜은 HTTPS입니다.

단계 5 변경 사항 배포. 이제 외부 인터페이스를 사용하여 디바이스를 관리할 수 있습니다.

What to do next

클라우드 커넥터를 사용하는 경우 어떻게 됩니까?

프로세스는 다음 두 가지를 제외하고 매우 유사합니다.

- 위 절차의 3c단계에서 "허용된 네트워크"는 클라우드 커넥터의 공용 IP 주소를 포함하는 네트워크 그룹 개체입니다.
 - 유럽, 중동 또는 아프리카(EMEA) 고객이고, <https://defenseorchestrator.eu/>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.
 - 35.157.12.126
 - 35.157.12.15
 - 미국 고객이고, <https://defenseorchestrator.com/>에서 CDO에 연결하는 경우 클라우드 커넥터의 공용 IP 주소는 다음과 같습니다.
 - 52.34.234.2
 - 52.36.70.147
 - AJPC(Asia-Pacific-Japan-China) 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
- 위 절차의 4단계에서는 클라우드 커넥터의 공용 IP 주소에서 외부 인터페이스에 대한 액세스를 허용하는 액세스 제어 규칙을 생성합니다.

등록 토큰 온보딩 접근 방식은 FDM 관리 디바이스를 CDO에 온보딩하는 권장 방법입니다. 클라우드 커넥터에서 관리 액세스를 허용하도록 외부 인터페이스를 구성한 후 FDM 관리 디바이스를 온보딩합니다. 외부 인터페이스의 IP 주소를 사용하여 연결합니다. 이 시나리오에서 해당 주소는 209.165.202.129입니다.

CDO 테넌트 요청

CDO 테넌트의 30일 무료 평가판을 요청하여 디바이스를 온보딩하고 관리할 수 있습니다. 그런 다음 Cisco 계정 팀에 연락하여 테넌트를 라이선스가 있는 테넌트로 업그레이드할 수 있습니다.

시작하기 전에

SecureX계정을 아직 생성하지 않았으면 생성하십시오. 새 [Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성](#)을 참조하십시오.

절차

1. <https://www.defenseorchestrator.com/new>로 진행합니다.
2. CDO 테넌트를 프로비저닝하려는 지역을 선택합니다.
3. **Sign Up with SecureX(SecureX로 가입)**를 클릭합니다.
4. SecureX 계정으로 로그인합니다.

성공적으로 로그인하면 등록된 이메일 ID로 테넌트 세부 정보가 포함된 이메일을 받게 됩니다. 선택한 지역에 새 CDO 테넌트가 생성됩니다. 이메일의 지침에 따라 새 CDO 테넌트에 액세스합니다.

CDO 테넌트에 처음으로 로그인하는 방법에 대한 자세한 내용은 [새 CDO 테넌트에 대한 초기 로그인](#)을 참조하십시오.

CDO 테넌트 및 다양한 테넌트 설정 관리에 대한 자세한 내용은 [새 CDO 테넌트에 대한 초기 로그인](#)을 참조하십시오.

추가 **CDO** 테넌트 요청

기존 테넌트를 추가로 생성하려면 어카운트 매니저에게 문의하십시오.

라이선스

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

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 관리하

고 클라우드 커넥터를 사용하는 원하는 수의 디바이스를 관리할 수 있습니다. 자세한 내용은 [Secure Device Connector\(SDC\)](#)를 참조하십시오.

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 CDO에서 클라우드 사용 Firewall Management Center를 사용하여 Cisco Firepower 1010 디바이스를 관리하도록 선택할 수 있습니다.

CDO가 지원하는 Cisco 보안 디바이스에 대한 자세한 내용은 [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 참조하십시오.



중요 CDO에서 고가용성 디바이스 쌍을 관리하기 위해 두 개의 별도 디바이스 라이선스가 필요하지 않습니다. ASA(Secure Firewall ASA) 또는 FTD(Secure Firewall Threat Defense) 고가용성 쌍이 있는 경우, CDO는 고가용성 디바이스 쌍을 하나의 단일 디바이스로 간주하므로 하나의 ASA 또는 FTD 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.

평가판 라이선스

Cisco Defense Orchestrator 평가판 라이선스

SecureX 계정에서 30일 Cisco Defense Orchestrator 평가판을 요청할 수 있습니다. 자세한 내용은 [CDO 테넌트 요청](#)을 참조하십시오.

클라우드 사용 Firewall Management Center 평가 라이선스

클라우드 사용 Firewall Management Center에 90일 평가판 라이선스가 제공되며 그 이후에는 위협 방어 서비스가 차단됩니다.

CDO 테넌트에서 프로비저닝된 클라우드 사용 Firewall Management Center를 가져오는 방법을 알아보려면 [CDO 테넌트용 클라우드 사용 Firewall Management Center 요청](#)을 참조하십시오.

클라우드 제공 Firewall Management Center 및 Threat Defense 라이선스

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



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

클라우드 제공 Firewall Management Center용 Threat Defense 라이선스

클라우드 사용 Firewall Management Center에서 관리하는 각 Secure Firewall Threat Defense 디바이스에 대해 개별 라이선스가 필요합니다. 자세한 내용은 *Cisco Defense Orchestrator*에서 클라우드 사용 Firewall Management Center로 Firewall Threat Defense 관리에서 [라이선싱](#)을 참조하십시오.

CDO가 클라우드 사용 Firewall Management Center으로 마이그레이션된 디바이스에 대한 라이선스를 처리하는 방법을 알아보려면 [Management Center에서 Cloud로 Threat Defense 마이그레이션](#)을 참조하십시오.

추가 지원 디바이스 및 라이선스

클라우드 사용 Firewall Management Center, CDO를 통해 Secure Firewall Threat Defense 디바이스를 지원하는 것 외에도 다음 디바이스도 관리합니다.

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Cloud Native
- 온프레미스 Cisco Secure Firewall Management Center
- Cisco Meraki 보안 어플라이언스
- Cisco IOS 디바이스
- SSH를 사용하여 액세스할 수 있는 디바이스
- Amazon Web Services(AWS) 가상 프라이빗 클라우드(VPC)
- Duo 관리자 패널
- Umbrella 조직

CDO 기본 인타이틀먼트 라이선스와 관리하려는 디바이스에 특정한 라이선스가 필요합니다.

SDC(Secure Device Connector)

디바이스 자격 증명을 사용하여 CDO에 디바이스를 온보딩할 때 CDO는 디바이스와 CDO 간의 프록시 통신을 위해 네트워크에서 SDC(Secure Device Connector)를 다운로드하고 구축하는 것이 모범 사례라고 간주합니다. 그러나 원하는 경우 CDO에서 외부 인터페이스를 통해 직접 통신을 수신하도록 디바이스를 활성화할 수 있습니다. ASA(Adaptive Security Appliance), FDM 관리 디바이스, FMC(Firepower Management Center), Secure Firewall Cloud Native 디바이스, 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 1.2)를 사용하여 서명 및 암호화된 보안 통신 메시지를 사용하여 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 Cisco Defense Orchestrator 연결, 12 페이지](#)의 내용을 참조하십시오.

SDC는 하이퍼바이저의 가상 머신으로 어플라이언스에 설치하거나 AWS 또는 Azure와 같은 클라우드 환경에 설치할 수 있습니다. CDO에서 제공하는 통합된 가상 머신 및 SDC 이미지를 사용하여 SDC를 설치하거나, 고유한 가상 머신을 생성하고 여기에 SDC를 설치할 수 있습니다. SDC 가상 어플라이언스는 CentOS 운영 체제를 포함하며 Docker 컨테이너 내에서 실행됩니다.

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.

두 번째 또는 후속 SDC를 구축하는 절차는 첫 번째 SDC를 구축할 때와 동일합니다. 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 통합하며 CDO의 페이지의 Secure Connectors(보안 커넥터) 탭에 표시됩니다. 각 추가 SDC는 순서대로 번호가 매겨집니다. [CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축, 14 페이지](#) 및 [자체 VM에 보안 디바이스 커넥터 구축, 18 페이지](#) 참조

관련 정보:

- [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#)
- [보안 디바이스 커넥터 문제 해결](#)
- [보안 디바이스 커넥터 업데이트, 29 페이지](#)

- [보안 디바이스 커넥터 제거, 26 페이지](#)

매니지드 디바이스에 Cisco Defense Orchestrator 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. 디바이스를 구성할 수 있는 경우 포트 443(또는 디바이스 관리를 위해 설정한 포트)에서 전체 인바운드 액세스를 허용해야 합니다.

FDM 관리 디바이스는 디바이스 자격 증명, 등록 키 또는 일련 번호를 사용하여 CDO에 온보딩할 수 있습니다(인터넷에서 직접 액세스할 수 있는지 여부). FDM 관리 디바이스가 인터넷에 직접 액세스할 수 없는 네트워크에 상주하는 경우, 디바이스의 일부로 제공되는 보안 서비스 익스체인지 커넥터는 보안 서비스 익스체인지 클라우드에 연결하여 FDM 관리 디바이스를 온보딩할 수 있습니다. 다양한 온보딩 방법에 대한 자세한 내용은 [위협 방어 디바이스 온보딩](#)의 내용을 참조하십시오.

다음은 온보딩하려면 네트워크에 온프레미스 SDC가 필요합니다.

- 클라우드에서 액세스할 수 없는 ASA 디바이스.
- 클라우드에서 액세스할 수 없는 FDM 관리 디바이스 및 "자격 증명 온보딩" 방법이 사용됩니다.
- Cisco IOS 디바이스.
- SSH 액세스가 가능한 디바이스.

다른 모든 디바이스 및 서비스에는 온프레미스 SDC가 필요하지 않습니다. CDO는 "Cloud Connector"를 사용하여 연결합니다. 인바운드 액세스를 허용해야 하는 IP 주소를 확인하려면 다음 섹션을 참조하십시오.

클라우드 커넥터를 통해 디바이스를 **CDO**에 연결

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

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

미국 지역의 고객이 https://defenseorchestrator.com에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 52.34.234.2
- 52.36.70.147

APJC(아시아-태평양-일본-중국) 지역의 고객이 <https://www.apj.cdo.cisco.com/>에서 CDO에 연결하는 경우 다음 IP 주소에서의 인바운드 액세스를 허용합니다.

- 54.199.195.111
- 52.199.243.0

SDC를 사용하여 CDO에 디바이스 연결

SDC를 통해 CDO를 디바이스에 연결할 때 CDO에서 관리하려는 디바이스는 포트 443(또는 디바이스 관리를 위해 구성된 모든 포트)에서 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.

SDC에 ASA 또는 Secure Firewall Cloud Native를 연결하기 위한 특별 고려 사항

특히 ASA 또는 Secure Firewall Cloud Native의 경우 SDC는 ASDM에서 사용하는 것과 동일한 보안 통신 채널을 사용합니다.

관리 중인 ASA 또는 Secure Firewall Cloud Native도 AnyConnect VPN 클라이언트 연결을 허용하도록 구성된 경우 ASDM HTTP 서버 포트를 1024 이상의 값으로 변경해야 합니다. 이 포트 번호는 디바이스를 ASA 또는 Secure Firewall Cloud Native 디바이스에 온보딩할 때 사용되는 포트 번호와 동일합니다.

ASA 또는 Secure Firewall Cloud Native 명령 예

다음 예에서는 ASA 또는 Secure Firewall Cloud Native 외부 인터페이스의 이름이 'outside'이고 AnyConnect 클라이언트가 ASA 또는 Secure Firewall Cloud Native에 구성되어 있으므로, ASDM HTTP 서버가 포트 8443에서 수신 대기 중이라고 가정합니다.

외부 인터페이스를 활성화하려면 다음 명령을 입력합니다.

EMEA:

http 35.157.12.126 255.255.255.255 outside

http 35.157.12.15 255.255.255.255 outside

미국:

http 52.34.234.2 255.255.255.255 outside

http 52.36.70.147 255.255.255.255 outside

아시아 태평양 일본 중국 지역:

http 54.199.195.111 255.255.255.255 outside

http 52.199.243.0 255.255.255.255 outside

AnyConnect VPN 클라이언트를 사용 중인 경우 ASDM HTTP 서버 포트를 활성화하려면 다음 명령을 입력합니다.

```
http server enable 8443
```

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축

디바이스 자격 증명을 사용하여 CDO를 디바이스에 연결하는 경우 네트워크에 SDC를 다운로드하고 배포하여 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), Secure Firewall Cloud Native 디바이스, 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, 29 페이지](#)를 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 [자체 VM에 보안 디바이스 커넥터 구축, 18 페이지](#)를 수행합니다.

시작하기 전에

SDC를 구축하기 전에 다음 사전 요건을 검토합니다.

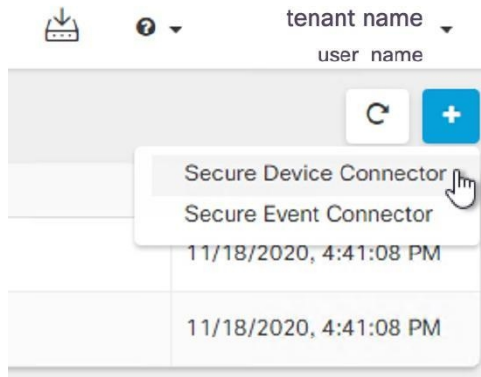
- CDO는 엄격한 인증서 확인이 필요하며 SDC와 인터넷 간의 웹/콘텐츠 프록시 검사를 지원하지 않습니다. 프록시 서버를 사용하는 경우 SDC(보안 디바이스 커넥터)와 CDO 간의 트래픽 검사를 비활성화합니다.
- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성된 포트에서 인터넷에 대한 전체 아웃바운드 액세스 권한을 가져야 합니다. CDO에서 관리하는 디바이스는 이 포트의 인바운드 트래픽도 허용해야 합니다.
- 매니지드 디바이스에 [Cisco Defense Orchestrator 연결](#)를 검토하여 적절한 네트워크 액세스를 확인합니다.
- CDO는 vSphere 웹 클라이언트 또는 ESXi 웹 클라이언트를 사용하여 SDC VM OVF 이미지를 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.
- 테넌트용 SDC 및 단일 SEC(Secure Event Connector)가 있는 VM의 시스템 요구 사항. (SEC는 [Cisco Security Analytics and Logging](#)에서 사용되는 구성 요소입니다.)
 VMware ESXi 호스트에 추가하는 각 SEC에는 4개의 CPU와 8GB의 추가 메모리가 필요합니다. 따라서 하나의 SDC와 하나의 SEC가 있는 VMware ESXi 호스트에 대한 요구 사항은 다음과 같습니다.
 - VMware ESXi 호스트에는 vCPU 6개가 필요합니다.
 - VMware ESXi 호스트에는 최소 10GB의 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.

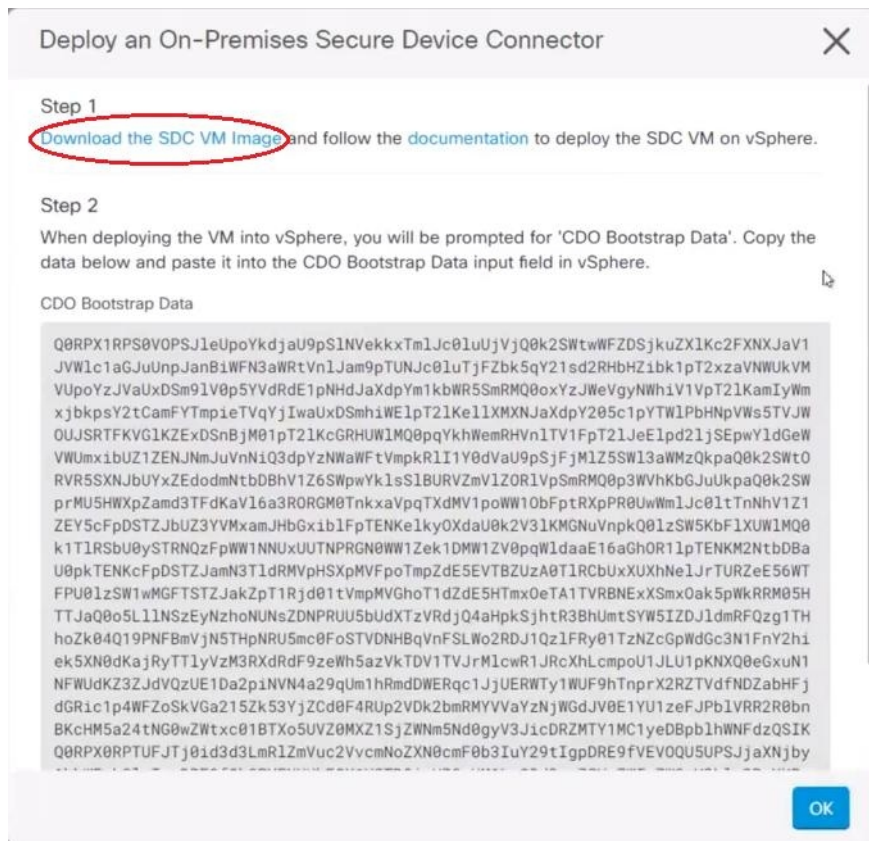
프로시저

- 단계 1 SDC를 생성할 CDO 테넌트에 로그인합니다.
- 단계 2 CDO 메뉴에서 **Tools & Services**(툴 및 서비스) > **Secure Connectors**(보안 커넥터)를 선택합니다.
- 단계 3 Secure Connectors(보안 커넥터) 페이지에서 파란색 더하기 버튼을 클릭하고 **Secure Device Connector**(보안 디바이스 커넥터)를 클릭합니다.

CDO의 VM 이미지를 사용하여 보안 디바이스 커넥터 구축



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 **cdo**로 로그인합니다. 기본 암호는 **adm123**입니다.

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

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

단계 12 비밀번호를 묻으면 `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. **cdo** 사용자의 비밀번호를 입력합니다.

단계 15 **Please choose the CDO domain you connect to**(연결할 CDO 도메인을 선택하십시오) 메시지가 표시되면 Cisco Defense Orchestrator 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 SDC를 설정하시겠습니까?) (y/n) 메시지가 나타나면 **n**을 입력합니다.

단계 20 VM 콘솔에서 자동으로 로그아웃됩니다.

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

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

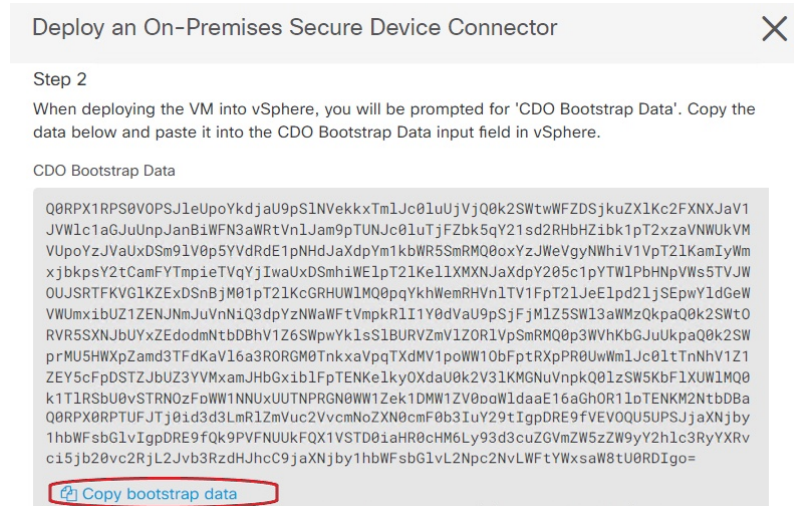
```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

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

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

1. CDO에 로그인합니다.
2. CDO 메뉴에서 **Admin**(관리) > **Secure Connector**(보안 커넥터)를 선택합니다.

3. Actions(작업) 창에서 **Deploy an On-Premises Secure Device Connector**(온프레미스 보안 디바이스 커넥터 구축)를 클릭합니다.
4. 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 n을 입력합니다.
- 단계 26 **Secure Device Connector**(보안 디바이스 커넥터) 페이지로 돌아갑니다. 새 SDC의 상태가 **Active**(활성)로 변경될 때까지 화면을 새로 고칩니다.

관련 정보:

- [보안 디바이스 커넥터 문제 해결](#)
- [SDC와의 디바이스 연결 문제 해결](#)

자체 VM에 보안 디바이스 커넥터 구축

디바이스 자격 증명을 사용하여 CDO를 디바이스에 연결하는 경우, 네트워크에서 SDC(Secure Device Connector)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 장치, FMC(Firepower Management Center) 및 Secure Firewall Cloud Native 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, 29 페이지](#)를 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 컨넥터 구축, 14 페이지](#)의 내용을 참조하십시오.

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 Cisco Defense Orchestrator 연결](#)을 검토하십시오.
- vCenter 웹 클라이언트 또는 ESXi 웹 클라이언트와 함께 설치된 VMware ESXi 호스트



참고 vSphere 데스크톱 클라이언트를 사용한 설치 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.
- 테넌트용 SDC 및 단일 SEC(Secure Event Connector)가 있는 VM의 시스템 요구 사항. (SEC는 [Cisco Security Analytics and Logging](#)에서 사용되는 구성 요소입니다.)

VMware ESXi 호스트에 추가하는 각 SEC에는 4개의 CPU와 8GB의 추가 메모리가 필요합니다.

따라서 하나의 SDC와 하나의 SEC가 있는 VMware ESXi 호스트에 대한 요구 사항은 다음과 같습니다.

- VMware ESXi 호스트에는 vCPU 6개가 필요합니다.
- VMware ESXi 호스트에는 최소 10GB의 메모리가 필요합니다.

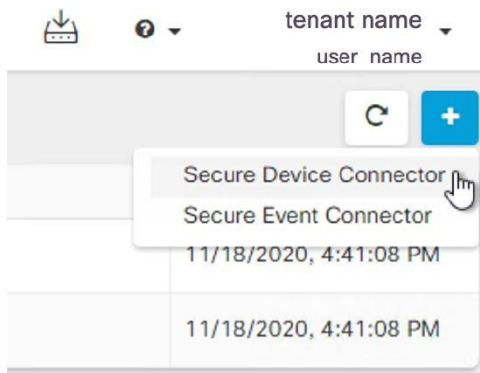
- VMware ESXi에는 프로비저닝 선택에 따라 가상 머신을 지원하기 위해 64GB의 디스크 공간이 필요합니다.
- VM의 CPU와 메모리를 업데이트한 후 VM의 전원을 켜고 Secure Connector(보안 커넥터) 페이지에 SDC가 "Active(활성)" 상태로 표시되는지 확인합니다.
- 이 절차를 수행하는 사용자는 Linux 환경에서 작업하고 파일 편집을 위해 vi 시각적 편집기를 사용하는 데 익숙해야 합니다.
- CentOS 가상 머신에 온프레미스 SDC를 설치하는 경우 정기적으로 Yum 보안 패치를 설치하는 것이 좋습니다. 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 CDO 메뉴에서 **Tools & Services(툴 및 서비스) > Secure Connectors(보안 커넥터)**를 선택합니다.
- 단계 3 Secure Connectors(보안 커넥터) 페이지에서 파란색 더하기 버튼을 클릭하고 **Secure Device Connector(보안 디바이스 커넥터)**를 클릭합니다.



- 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.html>의 내용을 참조하십시오.

참고 **--user** 플래그를 사용하지 마십시오.

- 단계 12 Docker CE 패키지를 설치합니다. <https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce>의 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 도커 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 디렉토리를 /usr/local/cdo로 변경합니다.

단계 21 bootstrapdata라는 새 파일을 생성하고 온프레미스 보안 디바이스 컨넥터 구축 마법사의 2단계에서 가져온 부트스트랩 데이터를 이 파일에 붙여넣습니다. 파일을 Save(저장)합니다. vi 또는 nano를 사용하여 파일을 생성할 수 있습니다.

단계 22 부트스트랩 데이터는 base64로 인코딩됩니다. 이를 디코딩하고 extractedbootstrapdata라는 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

- [Onboard Devices and Services\(디바이스 및 서비스 온보딩\)](#)로 이동하여 CDO로 관리하려는 디바이스를 온보딩합니다.
- 보안 이벤트 커넥터를 설치하는 경우 [SDC 가상 머신에 SEC\(Secure Event Connector\) 설치](#)로 돌아갑니다.
- 테넌트에 두 번째 이상의 보안 이벤트 커넥터를 설치하는 경우, [테넌트에 대해 여러 SEC 설치](#)로 돌아갑니다.

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 Cisco Defense Orchestrator 연결](#)를 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 모듈](#)을 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 출력](#)을 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 관리자](#)를 참조하십시오. SSH를 사용하여 SDC 인스턴스에 연결하는 포트는 보안상의 이유로 노출되지 않습니다.

보안 디바이스 커넥터의 IP 주소 변경

시작하기 전에

- 이 작업을 수행하려면 관리자여야 합니다.

- SDC는 TCP 포트 443 또는 디바이스 관리를 위해 구성된 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.
- IP Address(IP 주소)
  - 게이트웨이
  - DNS 서버
  - NTP 서버 또는 FQDN
- 또는 NTP 서버 또는 FQDN이 적용되지 않는 경우 Enter 키를 누릅니다.
- 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** 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 [자체 VM에 보안 디바이스 커넥터 구축, 18 페이지](#)를 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.

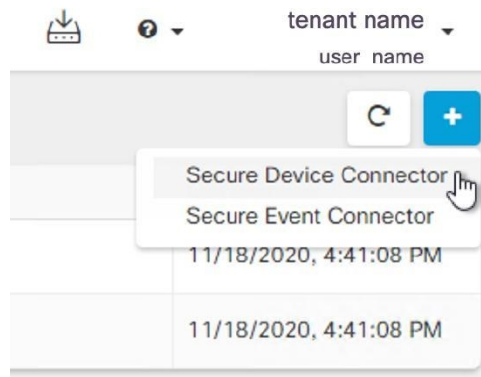
Procedure

단계 1 삭제할 SDC에 연결된 모든 디바이스를 제거합니다.

- a. SDC에서 사용하는 모든 디바이스를 식별하려면 [동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기](#)를 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 CDO 메뉴에서 **Tools & Services**(툴 및 서비스) > **Secure Connectors**(보안 커넥터)를 선택합니다.

단계 3 **Secure Connectors**(보안 커넥터) 페이지에서 파란색 더하기 버튼을 클릭하고 **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 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭한 다음 **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.

Meraki MX 연결 자격 증명 업데이트

Meraki 대시보드에서 새 API 키를 생성하는 경우 CDO에서 연결 자격 증명을 업데이트해야 합니다. 새 키를 생성하려면 **Meraki API 키 생성 및 검색**에서 자세한 내용을 확인하십시오. CDO에서는 디바이스 자체에 대한 연결 자격 증명을 업데이트할 수 없습니다. 필요한 경우 Meraki 대시보드에서 API 키를 수동으로 새로 고칠 수 있습니다. 자격 증명을 업데이트하고 통신을 다시 설정하려면 CDO UI에서 API 키를 수동으로 업데이트해야 합니다.



Note CDO가 디바이스를 동기화하지 못하면 CDO의 연결 상태에 "Invalid Credentials(유효하지 않은 자격 증명)"가 표시될 수 있습니다. 이 경우 API 키를 사용하려고 시도했을 수 있습니다. 선택한 Meraki MX의 API 키가 올바른지 확인합니다.

Meraki MX 디바이스에 대한 자격 증명을 업데이트하려면 다음 절차를 사용합니다.

Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭한 다음 **Meraki** 탭을 클릭합니다.

단계 3 연결 자격 증명을 업데이트할 Meraki MX를 선택합니다.

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


단계 5 CDO가 디바이스에 로그인하는 데 사용하는 API 키를 입력하고 **Update**(업데이트)를 클릭합니다. 변경하지 않는 한 이 API 키는 Meraki MX를 온보딩하는 데 사용한 것과 동일한 자격 증명입니다. 이러한 변경 사항을 디바이스에 구축할 필요는 없습니다.

보안 디바이스 커넥터 이름 변경

프로시저

단계 1 CDO 메뉴에서 **Tools & Services**(툴 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(인벤토리) 창의 보안 디바이스 커넥터 필터를 포함하여 CDO 인터페이스에 SDC 이름이 나타날 때마다 이 새 이름이 나타납니다.

보안 디바이스 커넥터 업데이트

이 절차를 문제 해결 톨로 사용합니다. 일반적으로 SDC는 자동으로 업데이트되므로 이 절차를 사용할 필요가 없습니다. 그러나 VM의 시간 구성이 잘못된 경우 SDC는 업데이트를 수신하기 위해 AWS에 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 ~]$
```

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 자체 VM에 보안 디바이스 커넥터 구축할 수 있습니다. 테넌트의 초기 SDC는 테넌트의 이름과 숫자 1을 포함합니다. 각 추가 SDC는 순서대로 번호가 매겨집니다.

동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기

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.
-

보안 디바이스 커넥터 오픈 소스 및 서드파티 라이선스 특성

=====

*** 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. 이에에는 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. 이에에는 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. 이에에는 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. 이에에는 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 라이선스에 따라 라이선스가 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. 이에에는 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. 이에에는 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. 이에에는 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. 이에에는 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, 징벌

적 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 라이선스는 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. 이에에는 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. 라이선스를 준수하지 않는 한 이 파일을 사용할 수 없습니다. 다음에서 라이선스 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.

* makedirs *

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. 이에에는 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(3개 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 Bazar, 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, 사

용, 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 1에서 9까지 정의된 사용, 복제 및 배포에 대한 조건을 의미합니다.

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

"법적 실체"는 행위 실체와 해당 실체를 통제하거나 통제받거나 공동 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 라이선스에 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 라이선스에 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 저작자의 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 포함

되며 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 부여할 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 라이선스의 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 **2차 저작물:** 2차 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 제3자 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 책임을 지지 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 책임을 지지 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. 이에에는 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 상실, 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. 이에에는 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.

* 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. 이에에는 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.

CDO에 로그인

Cisco Defense Orchestrator(CDO)에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 **사용자 관리**가 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 사용자 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 Cisco Secure Cloud Sign-on입니다. Cisco Secure Cloud Sign-On은 다단계 인증에 Duo를 사용합니다. 고객은 원하는 경우 SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 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, 40 페이지](#)를 참조하십시오.

2019년 10월 14일 이전에 CDO 테넌트가 존재했다면 [Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 41 페이지](#)를 참조하십시오.

새 CDO 테넌트에 대한 초기 로그인

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

v에는 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.



- 중요 2019년 10월 14일 이전에 CDO 테넌트가 존재했다면 이 문서 대신 [Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 41 페이지](#)를 사용하여 로그인 지침을 사용합니다.

시작하기 전에



DUO Security 설치. 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 [Duo 이중 인증 가이드: 등록 가이드](#)를 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.

다음 작업?

새 [Cisco Secure Cloud Sign On 계정 생성 및 Duo 다단계 인증 구성, 72 페이지](#)를 계속합니다. 이는 4단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

로그인 실패 문제 해결

실수로 잘못된 CDO 지역에 로그인했기 때문에 로그인에 실패함

적절한 CDO 지역에 로그인했는지 확인합니다. <https://sign-on.security.cisco.com>에 로그인하면 액세스할 지역을 선택할 수 있습니다. CDO타일을 클릭하여 defenceorchestrator.com에 액세스하거나 CDO(EU)를 클릭하여 defenceorchestrator.eu에 액세스합니다.

Cisco Secure Cloud Sign On ID 제공자로 마이그레이션

2019년 10월 14일, Cisco Defense Orchestrator(CDO)는 모든 테넌트를 MFA(multi-factor authentication)를 위한 ID 제공자 및 Duo로 Cisco Secure Cloud Sign-On으로 변환했습니다. CDO에 로그인하려면 먼저 **Cisco Secure Sign-On**에서 계정을 활성화하고 Duo를 사용하여 MFA를 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 2019년 10월 14일 이후에 생성된 경우 이 문서 대신 [새 CDO 테넌트에 대한 초기 로그인, 40 페이지](#)에서 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 가이드](#)를 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 CDO에 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, 72 페이지의 지침에 따라 새 Cisco Secure Cloud Sign-On 계정에 등록해야 합니다.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 CDO를 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.com>을 가리킬 수 있습니다.

해결 방법 <https://sign-on.security.cisco.com>에 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 계정을 생성한 경우 대시보드에서 Cisco Defense Orchestrator(US), Cisco Defense Orchestrator(EU) 또는 Cisco Defense Orchestrator(APJC)에 해당하는 CDO 타일을 클릭합니다.
- 해결 방법 <https://sign-on.security.cisco.com>을 가리키도록 북마크를 업데이트합니다.

Cisco Secure Cloud Sign On 대시보드에서 CDO 실행

Procedure

- 단계 1 Cisco Secure Cloud Sign-on 대시보드에서 해당 CDO 버튼을 클릭합니다. CDO 타일은 <https://defenseorchestrator.com>으로 안내하고 CDO(EU) 타일은 <https://defenseorchestrator.eu>로 안내합니다.
- 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 62을 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 [사용자 관리](#)를 검토한 다음 다른 사용자의 역할을 "Admin(관리자)"으로 변경합니다.

CDO에서 지원하는 소프트웨어 및 하드웨어

CDO 설명서에서는 CDO가 지원하는 소프트웨어 및 디바이스에 대해 설명합니다. CDO가 지원하지 않는 소프트웨어 및 디바이스는 지적하지 않습니다. 소프트웨어 버전 또는 디바이스 유형에 대한 지원을 명시적으로 요청하지 않는 경우 지원되지 않습니다.

관련 정보:

- [Secure Firewall Threat Defense 디바이스 지원 세부 사항, 44 페이지](#)
- [브라우저 지원, 47 페이지](#)

Secure Firewall Threat Defense 디바이스 지원 세부 사항



Note Secure Firewall device manager(FDM) 지원 및 기능은 요청 시에만 제공됩니다. 테넌트에서 Firewall Device Manager 지원을 아직 활성화하지 않은 경우 디바이스를 관리하거나 FDM 관리 디바이스에 구축할 수 없습니다. [이 플랫폼을 활성화하려면 지원 팀에 요청을 보냅니다.](#)

Secure Firewall Threat Defense 방화벽은 Cisco의 차세대 방화벽입니다. 이는 차세대 방화벽 서비스와 ASA 플랫폼의 장점을 결합하기 위해 노력합니다. 다양한 ASA 및 Firepower 하드웨어 디바이스 또는 가상 머신에 설치할 수 있습니다.

지원하는 기능을 검토하려면 [Cisco Defense Orchestrator로 FDM 디바이스 관리](#)를 검토하십시오. 온보딩 사전 요건 및 요구 사항에 대한 자세한 내용은 [FDM-관리 디바이스 온보딩](#)을 참조하십시오.



Note Snort 3은 버전 6.7 이상을 실행하는 FDM 관리 디바이스에서 사용할 수 있습니다. Snort 2와 Snort 3 간에 전환할 수는 있지만 구성이 호환되지 않을 수 있습니다. Snort 3, 지원되는 디바이스 및 소프트웨어, 제한 사항에 대한 자세한 내용은 [Snort 3.0으로 업그레이드](#)의 내용을 참조하십시오.

CDO에서 지원하는 하드웨어 및 소프트웨어 이미지

다음 테이블의 CDO 열은 하드웨어 플랫폼인 CDO에서 지원하는 Secure Firewall Threat Defense 소프트웨어 버전을 나타냅니다.

Table 1: Secure Firewall Threat Defense 관리자 및 버전별 하드웨어

디바이스 플랫폼	디바이스 버전: Management Center 사용		디바이스 버전: Device Manager 사용	
	고객이 구축한 관리 센터	클라우드 사용 Firewall Management Center *	Device Manager 전용	Device Manager + CDO
Firepower 1010, 1120, 1140	6.4+	7.0.3+	6.4+	6.4+
Firepower 1010E	7.2.3+ 7.3에서 지원되지 않음	7.2.3+ 7.3에서 지원되지 않음	7.2.3+ 7.3에서 지원되지 않음	7.2.3+ 7.3에서 지원되지 않음
Firepower 1150	6.5+	7.0.3+	6.5+	6.5+

디바이스 플랫폼	디바이스 버전: Management Center 사용		디바이스 버전: Device Manager 사용	
	고객이 구축한 관리 센터	클라우드 사용 Firewall Management Center *	Device Manager 전용	Device Manager + CDO
Firepower 2110, 2120, 2130, 2140	6.2.1+	7.0.3+	6.2.1+	6.4+
Secure Firewall 3110, 3120, 3130, 3140	7.1+	7.0.3+	7.1+	7.1+
Firepower 4110, 4120, 4140	6.0.1~7.2	7.2+	6.5~7.2	6.5~7.2
Firepower 4150	6.1~7.2	7.2+	6.5~7.2	6.5~7.2
Firepower 4115, 4125, 4145	6.4+	7.0.3+	6.5+	6.5+
Firepower 4112	6.6+	7.0.3+	6.6+	6.6+
Firepower 9300: SM-24, SM-36, SM-44	6.0.1~7.2	7.0.3+	6.5~7.2	6.5~7.2
Firepower 9300: SM-40, SM-48, SM-56	6.4+	7.0.3+	6.5+	6.5+
ISA 3000	6.2.3 이상	7.0.3+	6.2.3 이상	6.4+
ASA 5506-X, 5506H-X, 5506W-X	6.0.1~6.2.3	—	6.1~6.2.3	—
ASA 5508-X, 5516-X	6.0.1~7.0	7.0.3~7.0.x	6.1~7.0	6.4~7.0
ASA 5512-X	6.0.1~6.2.3	—	6.1~6.2.3	—
ASA 5515-X	6.0.1~6.4	—	6.1~6.4	6.4
ASA 5525-X, 5545-X, 5555-X	6.0.1~6.6	—	6.1~6.6	6.4 ~ 6.6

* 클라우드 사용 Firewall Management Center는 버전 7.1을 실행하는 threat defense 디바이스 또는 모든 버전을 실행하는 클래식 디바이스를 관리할 수 없습니다. 클라우드 관리 등록을 취소하고 비활성화하지 않는 한 클라우드 매니지드 디바이스를 버전 7.0.x에서 버전 7.1로 업그레이드할 수 없습니다. 디바이스를 버전 7.2 이상으로 직접 업그레이드하는 것이 좋습니다.

CDO에서 지원하는 가상 머신 플랫폼 및 소프트웨어 이미지

다음 표의 CDO 열은 가상 디바이스 플랫폼, CDO가 지원하는 Firepower Threat Defense 소프트웨어 버전을 나타냅니다.

Table 2: Threat Defense Virtual 관리자 및 버전별

디바이스 플랫폼	디바이스 버전: Management Center 사용		디바이스 버전: Device Manager 사용	
	고객이 구축한 관리 센터	클라우드 사용 Firewall Management Center *	Device Manager 전용	Device Manager + CDO
공용 클라우드				
Alibaba	7.2+	7.2%	—	—
AWS	6.0.1+	7.0.3+	6.6+	6.6+
Azure	6.2+	7.0.3+	6.5+	6.5+
GCP	6.7+	7.0.3+	7.2+	7.2%
OCI	6.7+	7.0.3+	—	—
온프레미스/프라이빗 클라우드				
HyperFlex	7.0+	7.0.3+	7.0+	7.0+
KVM	6.1+	7.0.3+	6.2.3 이상	6.4+
Nutanix	7.0+	7.0.3+	7.0+	7.0+
OpenStack	7.0+	7.0.3+	—	—
VMware 7.0	7.0+	7.0.3+	7.0+	7.0+
VMware 6.7	6.5+	7.0.3+	6.5+	6.5+
VMware 6.5	6.2.3 이상	7.0.3+	6.2.3 이상	6.4+
VMware 6.0	6.0~6.7	—	6.2.2~6.7	6.4~6.7
VMware 5.5	6.0.1~6.2.3	—	6.2.2~6.2.3	—
VMware 5.1	6.0.1만	—	—	—

* 클라우드 사용 Firewall Management Center는 버전 7.1을 실행하는 threat defense 디바이스 또는 모든 버전을 실행하는 클래식 디바이스를 관리할 수 없습니다. 클라우드 관리 등록을 취소하고 비활성화하지 않는 한 클라우드 매니지드 디바이스를 버전 7.0.x에서 버전 7.1로 업그레이드할 수 없습니다. 디바이스를 버전 7.2 이상으로 직접 업그레이드하는 것이 좋습니다.

CDO를 사용하여 Firepower 디바이스 인터페이스를 관리하는 방법에 대한 자세한 내용은 [Firepower 인터페이스 구성에 대한 지침 및 제한 사항](#)을 참조하십시오.

ASA FirePOWER 서비스 모듈

CDO는 ASA FirePOWER 서비스 모듈을 지원하지 않습니다.

브라우저 지원

CDO는 다음 브라우저의 최신 버전을 지원합니다.

- Google Chrome
- Mozilla Firefox

Cisco Defense Orchestrator 플랫폼 유지 관리 일정

Cisco Defense Orchestrator 유지 관리 일정

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

대부분의 경우 업데이트는 목요일에 완료되지만 필요한 경우 금요일 및 일요일의 유지 관리 시간이 사용됩니다.

표 3: CDO 유지 관리 일정

요일	시간 (24시간제)
목요일	09:00 UTC - 12:00 UTC
금요일	09:00 UTC - 12:00 UTC
일요일	09:00 UTC - 12:00 UTC

이 유지 관리 기간 동안 테넌트에 계속 액세스할 수 있으며 클라우드 사용 Firewall Management Center가 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 배포하는 데 CDO를 사용하지 않는 것이 좋습니다.

CDO를 중지하거나 클라우드 사용 Firewall Management Center과 통신을 중단되는 오류가 있는 경우, 해당 오류는 유지 관리 기간을 벗어나더라도 영향을 받는 모든 테넌트에서 가능한 한 빨리 해결됩니다.

클라우드 제공 **Firewall Management Center** 유지 관리 일정

테넌트에 배포된 클라우드 사용 Firewall Management Center을 보유한 고객은 CDO가 클라우드 사용 Firewall Management Center 환경을 업데이트하기 약 1주일 전에 알림을 받습니다. 테넌트의 슈퍼 관리자 및 관리 사용자는 이메일로 알림을 받습니다. CDO는 또한 모든 사용자에게 예정된 업데이트를 알리는 배너를 홈페이지에 표시합니다.

테넌트에 대한 업데이트는 최대 1시간이 걸릴 수 있으며 테넌트 지역에 할당된 유지 관리 날짜의 3시간 유지 관리 시간 내에 이루어집니다. 테넌트가 업데이트되는 동안에는 클라우드 사용 Firewall Management Center 환경에 액세스할 수 없지만, CDO의 나머지 부분에 계속 액세스할 수 있습니다.

표 4: 클라우드 제공 **Firewall Management Center** 유지 관리 일정

요일	시간 (24시간제)	지역
수요일	04:00 UTC - 07:00 UTC	유럽, 중동 또는 아프리카 (EMEA)
수요일	17:00 UTC - 20:00 UTC	아시아-태평양-일본(APJ)
목요일	09:00 UTC - 12:00 UTC	아메리카

테넌트 관리

Cisco Defense Orchestrator(CDO)는 설정 페이지에서 테넌트 및 개별 사용자 계정의 특정 측면을 사용자 지정할 수 있는 기능을 제공합니다. CDO 메뉴의 왼쪽 탐색 패널에서 **Settings**(설정)를 클릭합니다.

관련 정보:

- [일반 설정, 48 페이지](#)
- [사용자 관리](#)
- [로깅 설정](#)
- [알림 설정, 52 페이지](#)

일반 설정

오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

일반 CDO 설정에 관한 다음 항목을 참조하십시오.

- [사용자 설정, on page 49](#)
- 내 토큰은 [API 토큰, on page 58](#)를 참조하십시오.
- **Tenant Settings**(테넌트 설정)은 다음을 참조하십시오.

- 변경 요청 추적 활성화, on page 49
- Cisco 지원에서 테넌트를 볼 수 없도록 설정, on page 49
- 자동 구축 예약 옵션 활성화, on page 51
- 기본 충돌 탐지 간격, on page 50
- 웹 분석, on page 51
- 기본 반복 백업 일정 구성, on page 52
- 테넌트 ID, on page 52
- 테넌트 이름, on page 52

사용자 설정

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

내 토큰

자세한 내용은 [API 토큰](#)을 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 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.

단계 2 **General(일반)** 탭을 클릭합니다.

단계 3 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 버튼을 밀어서 녹색 확인 표시를 표시합니다.

Cisco 지원에서 테넌트를 볼 수 없도록 하려면 다음 절차를 따르십시오.

Procedure

-
- 단계 1 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
 - 단계 2 **General**(일반) 탭을 클릭합니다.
 - 단계 3 **Cisco** 지원팀에서 이 테넌트를 볼 수 없도록 방지 아래의 슬라이더를 클릭합니다.
-

디바이스 변경 사항 자동 수락 옵션 활성화

디바이스 변경에 대한 자동 수락을 활성화하면 Defense Orchestrator가 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 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
 - 단계 2 **General**(일반) 탭을 클릭합니다.
 - 단계 3 **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 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
 - 단계 2 **General Settings**(일반 설정) 탭을 클릭합니다.

단계 3 **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 예약](#)을 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 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

단계 2 **General Settings**(일반 설정) 탭을 클릭합니다.

단계 3 **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 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

단계 2 **General Settings**(일반 설정) 탭을 클릭합니다.

단계 3 웹 분석 아래의 슬라이더를 클릭합니다.

기본 반복 백업 일정 구성

여러 디바이스에서 백업 일정을 일관되게 하려면 이 설정을 사용하여 기본 반복 백업 일정을 구성하십시오. 특정 디바이스에 대한 백업을 예약할 때 기본 설정을 사용하거나 변경할 수 있습니다. 기본 반복 백업 일정을 변경해도 기존의 예약된 백업이나 반복 백업 일정은 변경되지 않습니다.

Procedure

단계 1 **Frequency**(빈도) 필드에서 매일, 매주 또는 매월을 선택합니다.

단계 2 백업을 수행할 시간을 24시간 단위로 선택합니다. UTC(Coordinated Universal Time)로 시간을 예약합니다.

- 매주 백업하는 경우: 백업을 수행할 요일을 확인합니다.
- 매월 백업하는 경우: **Days of Month**(날짜) 필드를 클릭하고 백업을 예약할 날짜를 추가합니다.
참고: 31일을 입력했지만 해당 월에 31일이 없는 경우 백업이 수행되지 않습니다. 예약된 백업 시간에 이름과 설명을 지정합니다.

단계 3 **Save**(저장)를 클릭합니다.

자세한 내용은 [단일 FTD에 대한 반복 백업 일정 구성](#)을 참조하십시오.

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.

알림 설정

테넌트와 연결된 디바이스가 특정 작업을 수행할 때마다 CDO에서 이메일 알림을 받도록 구독할 수 있습니다. 이러한 알림은 테넌트와 연결된 모든 디바이스에 적용되지만, 모든 디바이스 유형이 사용

가능한 모든 옵션을 지원하는 것은 아닙니다. 또한 아래에 나열된 CDO 알림에 대한 변경 사항은 실시간으로 자동 업데이트되며 구축이 필요하지 않습니다.

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 [변경 로그](#)를 검토하는 것이 좋습니다.

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

디바이스 워크플로우에 대한 알림 전송



Note 이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 [Cisco Defense Orchestrator의 사용자 역할](#)을 참조하십시오.

알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 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.
- **threat defense**를 클라우드로 마이그레이션 - 이 작업은 threat defense Device Manager를 Management Center에서 CDO로 변경할 때 적용됩니다.

디바이스 이벤트에 대한 알림 전송



Note 이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 [Cisco Defense Orchestrator의 사용자 역할](#)을 참조하십시오.

알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 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

이러한 설정을 변경하거나 알림을 수동으로 구독하려면 최고 관리자 사용자 역할이 있어야 합니다. 자세한 내용은 [Cisco Defense Orchestrator의 사용자 역할](#)을 참조하십시오.


테넌트에 로그인한 사용자가 백그라운드 검색을 생성하면 알림을 받습니다. 알림을 받을 디바이스 워크플로우 시나리오를 모두 선택해야 합니다. 다음 작업을 수동으로 확인합니다.

- 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.

가입자

Subscribe to receive alerts(알림 수신 구독) 토글을 활성화하여 테넌트 로그인과 연결된 이메일을 알림 목록에 추가합니다. 메일링 리스트에서 이메일을 제거하려면 토글을 선택 취소하여 회색으로 표시합니다.

특정 사용자 역할은 이 설정 페이지의 구독 작업에 제한적으로 액세스할 수 있습니다. 최고 관리자 사용자 역할의 사용자는 이메일 항목을 추가하거나 제거할 수 있습니다. 자신이 아닌 다른 사람 또는


대체 이메일 연락처를 구독 중인 사용자 목록에 추가하려면  을 클릭하고 이메일을 수동으로 입력합니다.



Warning

사용자를 수동으로 추가하는 경우 올바른 이메일을 입력해야 합니다. CDO는 테넌트와 연결된 알려진 사용자에 대한 이메일 주소를 확인하지 않습니다.

CDO 알림 보기

알림  아이콘을 클릭하여 테넌트에서 발생한 최신 알림을 확인합니다. CDO의 알림은 30일 후에 알림 목록에서 제거됩니다.



Note

Send Alerts When(알림 전송 시기) 섹션에서 선택한 사항은 CDO에 표시되는 알림 유형에 영향을 미칩니다.

서비스 통합

메시징 앱에서 수신 Webhook를 활성화하고 앱 대시보드에서 직접 CDO 알림을 수신합니다. CDO에서 이 옵션을 활성화하려면 선택한 앱에서 수신 Webhook를 수동으로 허용하고 Webhook URL을 검색해야 합니다. 자세한 내용은 [CDO 알림을 위한 서비스 통합 활성화](#)를 참조하십시오.

CDO 알람을 위한 서비스 통합 활성화

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

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



참고 알람 설정 페이지에서 선택한 **Notification Settings**(알림 설정)은 메시지 프로그램으로 전달되는 이벤트입니다.

Webex Teams에 대해 수신 Webhook

시작하기 전에

CDO 알람은 지정된 작업 공간에 표시되거나 비공개 메시지에 자동 봇으로 표시됩니다. Webex Teams이 웹훅을 처리하는 방법에 대한 자세한 정보는 [개발자용 Webex](#)를 참조하십시오.

Webex Teams에 대해 수신 웹훅을 허용하려면 다음 절차를 따르십시오.

프로시저

- 단계 1 Webex Teams 응용프로그램을 엽니다.
- 단계 2 창의 왼쪽 하단에서 **Apps**(앱) 아이콘을 클릭합니다. 이 작업은 기본 브라우저의 새 탭에서 Cisco Webex App Hub를 엽니다.
- 단계 3 수신 웹훅을 찾으려면 검색창을 사용하세요.
- 단계 4 **Connect**(연결)을 선택합니다. 이 작업은 새 탭에서 애플리케이션을 허용하는 OAuth 인증을 엽니다.
- 단계 5 **Accept**(수락)을 선택합니다. 탭은 자동으로 애플리케이션의 구성 페이지로 리디렉션됩니다.
- 단계 6 다음을 구성합니다.
 - **Webhook** 이름 - 이 애플리케이션에서 제공하는 메시지를 식별하기 위한 이름을 입력합니다.
 - 공간 선택 - 드롭다운 메뉴를 사용하여 **Space**(공간)를 선택합니다. 공간이 이미 Webex 팀에 존재해야 합니다. 공간이 존재하지 않는 경우 Webex Teams에서 새 공간을 만들고 애플리케이션의 구성 페이지를 새로 고쳐 새 공간을 표시할 수 있습니다.
- 단계 7 **Add**(추가)를 선택합니다. 선택한 Webex Space는 애플리케이션이 추가되었다는 알람을 받게 됩니다.
- 단계 8 웹훅 URL을 복사합니다.
- 단계 9 CDO에 로그인합니다.
- 단계 10 왼쪽 탐색 모음에서 **Settings**(설정) > **Notification Settings**(알림 설정)를 클릭합니다.
- 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 **Webex**를 서비스 유형으로 선택합니다.
- 단계 15 서비스에서 생성한 웹후크 URL을 붙여넣습니다.
- 단계 16 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 앱](#)을 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 **Service Integrations**(서비스 통합)으로 스크롤합니다.
- 단계 11 파란색 플러스 버튼을 클릭합니다.
- 단계 12 **Name**(이름)을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.
- 단계 13 드롭다운 메뉴를 확장하고 서비스 유형으로 **Slack**을 선택합니다.
- 단계 14 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 15 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 **Service Integrations(서비스 통합)**으로 스크롤합니다.

단계 5 파란색 플러스 버튼을 클릭합니다.

단계 6 **Name(이름)**을 입력합니다. 이 이름은 구성된 서비스 통합으로 CDO에 나타납니다. 구성된 서비스로 전달되는 이벤트에는 나타나지 않습니다.

단계 7 드롭다운 메뉴를 확장하고 서비스 유형으로 **Custom(사용자 지정)**을 선택합니다.

단계 8 서비스에서 생성한 웹후크 URL을 붙여넣습니다.

단계 9 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 Cisco Defense Orchestrator와 통합

Cisco Defense Orchestrator(CDO)는 Cisco Secure Sign-On을 SAML Single Sign-On Identity Provider(IdP) 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 SAML 솔루션을 CDO와 통합하려면 지원 부서에 문의하여 [케이스를 생성](#)해야 합니다. 지침은 [Cisco Secure Cloud Sign-On ID 제공자 통합 가이드](#)를 참조하십시오.


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 가이드](#)를 참조하십시오.



주의 사례를 열 때 기술 수동 선택을 선택하고 요청이 올바른 팀에 전달되도록 **SecureX - 로그인 및 관리**를 선택했는지 확인합니다.

(레거시만 해당) IdP(Identity Provider) 통합이 CDO와 직접 통합된 경우 [CDO TAC로 지원 티켓](#)을 열고 metadata.xml 파일을 제공하십시오.



참고 IdP를 CDO와 직접 통합하는 대신 SecureX SSO와 통합하는 것이 매우 좋습니다.

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 설정 페이지로 돌아가면, 토큰이 분명히 발급되었지만 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 소개](#)를 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 내비게이션 바에서 **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)**를 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 왼쪽 내비게이션 바에서 **Settings(설정) > General Settings(일반 설정)**를 클릭합니다.
- 단계 2 내 토큰에서 **Revoke(취소)**를 클릭합니다. CDO는 토큰을 취소합니다.

ID 제공자 계정과 Cisco Defense Orchestrator 사용자 레코드 간의 관계

Cisco Defense Orchestrator(CDO)에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 CDO의 사용자 레코드가 있는 계정이 필요합니다. IdP 어카운트에는 사용자의 자격 증명도 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 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 Cisco Defense Orchestrator와 통합할 수 있습니다.

로그인 워크플로우

다음은 IdP 계정이 CDO 사용자 레코드와 상호 작용하여 CDO 사용자에게 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 인증되었다는 SAML 어설션을 발행하고 포털은 <https://defenseorchestrator.com> 또는 <https://defenseorchestrator.eu> 또는 <https://www.apj.cdo.cisco.com/>를 나타내는 타일과 같이 사용자가 액세스할 수 있는 애플리케이션을 표시합니다.
- 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 해

서 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 공급자가 있는 고객

SAML SSO(Single Sign-On)를 Cisco Defense Orchestrator와 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](#)
- [사용자 관리](#)
- [Cisco Defense Orchestrator의 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.



Note 다중 테넌트 포털에서 여러 지역에 걸쳐 테넌트를 추가하고 해당 테넌트가 관리하는 디바이스를 볼 수 있습니다. 다중 테넌트 포털에서 테넌트를 편집하거나 디바이스를 구성할 수 없습니다.

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 최고 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.

• 디바이스:

- 포털에 추가된 테넌트에 있는 모든 디바이스를 표시합니다. 필터 및 검색 필드를 사용하여 보려는 디바이스를 검색합니다. 디바이스를 클릭하여 상태, 온보딩 방법, 방화벽 모드, 페일 오버 모드, 소프트웨어 버전 등을 볼 수 있습니다.
- 인터페이스는 테이블에서 볼 디바이스 속성을 선택하거나 지울 수 있는 열 선택기  를 제공합니다. 'AnyConnect 원격 액세스 VPN'을 제외하고 다른 모든 디바이스 속성은 기본으로 선택됩니다. 테이블을 사용자 정의하면 CDO는 다음에 CDO에 로그인할 때 선택 사항을 기억합니다.
- 디바이스를 클릭하면 오른쪽에서 세부 정보를 볼 수 있습니다.
- 포털 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.
- 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 디바이스에 이 링크가 표시됩니다. 테넌트에 액세스할 수 있는 권한이 없는 경우 디바이스 관리 링크가 표시되지 않습니다. 권한을 얻기 위해 조직의 슈퍼 관리자에게 문의할 수 있습니다.



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.

Name	Type	Region	Version	Hardware Version	Configuration	Connectivity State
52.53.207.153	ASA	Europe	9.8(3)18	ASAv (V01)	Synced	Online
Acton	Unknown	North America	16.03.07	CSR1000V	Synced	Online
Amsterdam	ASA	North America	9.13(1)7	ASAv (V01)	Synced	Online
Ayer	FTD	North America	6.4.0-44	Cisco Firepower Threat Defe	Synced	Online
Baltimore	ASA	North America	9.9(2)	ASAv (V01)	Synced	Online
Burak-crush-APUC	ASA Model	Asia-Pacific & Japan	9.1(5)		Synced	Online

- 테넌트:
 - 포털에 추가된 테넌트를 표시합니다.
 - 이를 통해 슈퍼 관리자는 포털에 테넌트를 추가할 수 있습니다.
 - 를 클릭하면 CDO 테넌트의 메인 페이지를 볼 수 있습니다.

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 생성](#) 하고 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 내비게이션 바에서 **Settings(설정)** > **General Settings(일반 설정)** > **My Tokens(내 토큰)**를 클릭합니다.
- 단계 2 **Generate API Token(API 토큰 생성)**을 클릭한 다음 복사합니다.
- 단계 3 포털로 이동하여 **Tenants(테넌트)** 탭을 클릭합니다.

단계 4 오른쪽에  테넌트 추가 버튼을 클릭합니다.

단계 5 토큰을 붙여넣고 **Save**(저장)를 클릭합니다.

멀티 테넌트 포털에서 테넌트 삭제

Procedure

단계 1 포털로 이동하여 **Tenants**(테넌트) 탭을 클릭합니다.

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

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

관리-테넌트 포털 설정

Cisco Defense Orchestrator(Defense Orchestrator)는 설정 페이지에서 다중 테넌트 포털 및 개별 사용자 계정의 특정 측면을 사용자 지정할 수 있는 기능을 제공합니다. 왼쪽 탐색 모음에서 **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 [사용자 관리](#)를 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 수 있는 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

- 위협 방어 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 끌 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.

사용자 관리

CDO에서 사용자 레코드를 생성하거나 수정하기 전에 **ID 제공자 계정과 Cisco Defense Orchestrator 사용자 레코드 간의 관계**를 읽고 IdP(Identity Provider) 계정과 사용자 레코드의 상호 작용 방식을 확인하십시오. CDO사용자는 인증을 받고 CDO테넌트에 액세스할 수 있도록 CDO레코드 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 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.

단계 2 **User Management(사용자 관리)**를 클릭합니다.

Email	Last Login	Token	Roles
sec-ops@example.com	7/23/2018 12:04:28 PM	No API Token	Admin
superadmin@example.com	8/30/2018 11:57:23 AM	No API Token	Super Admin
here2help@cisco.com	8/29/2018 2:06:42 PM	No API Token	Read Only
net-ops@example.com	8/25/2018 9:23:44 PM	No API Token	Admin

참고 Cisco 지원이 테넌트에 액세스하지 못하도록 하려면, **일반 설정** 페이지에서 계정 설정을 구성합니다.

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 그룹을 추가, 편집 또는 삭제하려면 **SuperAdmin** 사용자 역할이 있어야 합니다. 자세한 내용은 [Cisco Defense Orchestrator의 사용자 역할](#)을 참조하십시오.

Active Directory 그룹 탭

Settings(설정) 페이지의 사용자 관리 섹션에는 현재 CDO에 매핑된 Active Directory 그룹에 대한 탭이 있습니다. 가장 중요한 것은 이 페이지에 AD 관리자에서 할당된 AD 그룹의 역할이 표시된다는 것입니다.

AD 그룹 내의 사용자는 Active Directory 그룹 탭이나 사용자 탭에 개별적으로 나열되지 않습니다.

감사 로그 탭

Settings(설정) 페이지의 User Management(사용자 관리) 섹션에는 Audit Logs(감사 로그) 탭이 있습니다. 이 새 섹션에는 CDO 테넌트에 액세스한 모든 사용자의 마지막 로그인 시간과 마지막 로그인 시간에 각 사용자가 보유한 역할이 표시됩니다. 여기에는 명시적 사용자 로그인과 AD 그룹 로그인이 모두 포함됩니다.

다중 역할 사용자

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

사용자는 AD에서 여러 그룹의 일부가 될 수 있으며 각 그룹은 서로 다른 CDO 역할로 CDO에서 정의될 수 있습니다. 로그인 시 사용자가 얻는 최종 권한은 사용자가 속한 CDO에 정의된 모든 AD 그룹의 역할 조합입니다. 예를 들어 사용자가 두 개의 AD 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.

AD 그룹 매핑은 CDO에서 한 번만 정의하면 되며, 이후에 다른 그룹 간에 사용자를 추가, 제거 또는 이동하여 사용자에 대한 액세스 및 권한 관리를 AD에서만 독점적으로 수행할 수 있습니다.



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

시작하기 전에

사용자 관리의 형태로 CDO에 AD 그룹 매핑을 추가하기 전에 AD가 SecureX와 통합되어 있어야 합니다. AD ID 공급자(IdP)가 아직 통합되지 않은 경우 다음 작업을 수행해야 합니다.

1. Cisco TAC로 [지원 사례](#)를 열고 다음 정보와 함께 사용자 지정 AD IdP 통합을 요청하십시오.

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

- .XML 형식의 인증서 및 페더레이션 메타데이터.
2. AD에 다음 사용자 지정 SAML 클레임을 추가합니다. 이 값은 대소문자를 구분합니다.
- **SamlADUserGroupIds** - 이 속성은 사용자가 AD에 가지고 있는 모든 그룹 연결을 설명합니다. 예를 들어 Azure에서 아래 스크린샷과 같이 + **Add a group claim**(+ 그룹 클레임 추가)를 선택합니다.

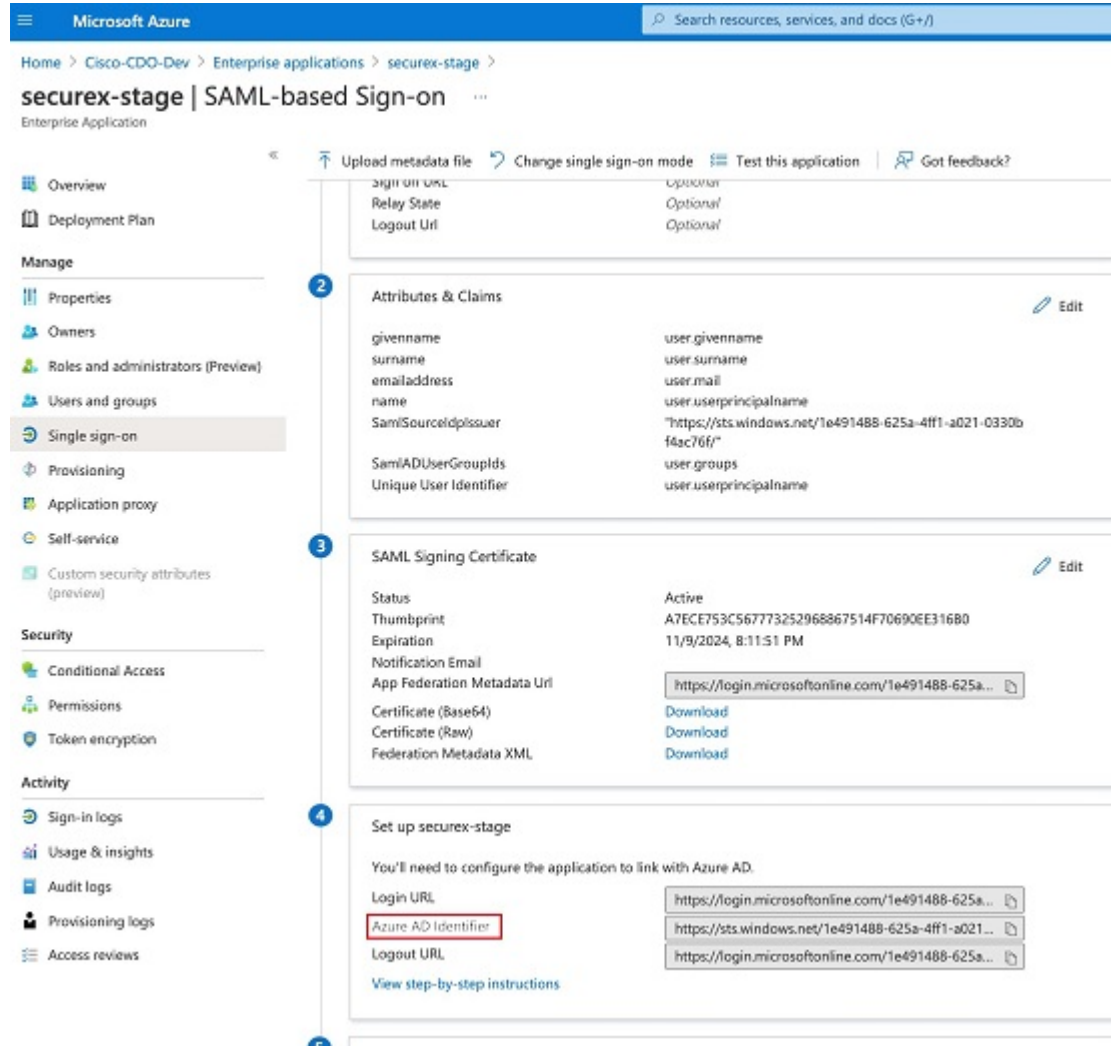
그림 3: **Active Directory**에 정의된 사용자 지정 클레임

The screenshot shows the 'Attributes & Claims' configuration page in the Microsoft Azure portal. The page title is 'Attributes & Claims' and it includes navigation links for 'Home', 'Cisco-CDO-Dev', 'Enterprise applications', 'securex-okta-ci', and 'SAML-based Sign-on'. Below the title, there are buttons for '+ Add new claim', '+ Add a group claim', 'Columns', and 'Got feedback?'. The page is divided into two sections: 'Required claim' and 'Additional claims'. The 'Required claim' section has a table with one row: 'Unique User Identifier (Name ID)' with the value 'user.userprincipalname [nameid-for... ***]'. The 'Additional claims' section has a table with five rows, each with a 'Claim name' and a 'Value'. The rows are: 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress' with value 'user.mail ***'; 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname' with value 'user.givenname ***'; 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name' with value 'user.userprincipalname ***'; 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname' with value 'user.surname ***'; and 'SamlADUserGroupIds' with value 'user.groups ***'. The 'SamlADUserGroupIds' row is highlighted with a red box. Below it is another row: 'SamlSourceIdpIssuer' with value 'https://sts.windows.net/1e491488-... ***', which is also highlighted with a red box.

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***
Additional claims	
Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***
SamlADUserGroupIds	user.groups ***
SamlSourceIdpIssuer	https://sts.windows.net/1e491488-... ***

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

그림 4: Azure Active Directory 식별자 찾기



사용자 관리를 위한 **Active Directory** 그룹 추가

프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
- 단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.
- 단계 4 테이블 상단에서 **Active Directory Groups**(활동 디렉토리 그룹) 탭을 선택합니다.
- 단계 5 현재 AD 그룹이 없는 경우 **Add AD group**(AD 그룹 추가)를 클릭합니다. 기존 항목이 있으면 Add(추가) 버튼을 클릭합니다.

단계 6 다음 정보를 입력합니다.

- **그룹 이름** - 고유한 이름을 입력합니다. 이 이름은 AD의 그룹 이름과 일치하지 않아도 됩니다. CDO에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- **그룹 ID** - AD에서 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** - AD에서 AD 발급자 값을 수동으로 입력합니다.
- **역할** - 이 AD 그룹에 포함된 모든 사용자의 역할을 결정합니다. 자세한 내용은 사용자 역할을 참조하십시오.
- (선택 사항) **참고** - 이 AD 그룹에 적용 가능한 참고를 추가합니다.

단계 7 **OK(확인)**를 선택합니다.

사용자 관리를 위한 Active Directory 그룹 편집

시작하기 전에

CDO에서 AD 그룹의 사용자 관리를 편집하면 CDO가 AD 그룹을 제한하는 방식만 편집할 수 있습니다. CDO에서 AD 그룹 자체를 편집할 수 없습니다. AD 그룹 내의 사용자 목록을 편집하려면 AD를 사용해야 합니다.

프로시저

단계 1 CDO에 로그인합니다.

단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.

단계 3 **User Management(사용자 관리)** 탭을 클릭합니다.

단계 4 테이블 상단에서 **Active Directory Groups(활동 디렉토리 그룹)** 탭을 선택합니다.

단계 5 편집할 AD 그룹을 식별하고 **Edit(편집)** 아이콘을 선택합니다.

단계 6 다음 값을 편집합니다.

- **그룹 이름** - 고유한 이름을 입력합니다. CDO에서는 이 필드에 대한 특수 문자를 지원하지 않습니다.
- **그룹 ID** - AD에서 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** - AD에서 AD 발급자 값을 수동으로 입력합니다.

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

사용자 관리를 위한 **Active Directory** 그룹 삭제

프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
- 단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.
- 단계 4 테이블 상단에서 **Active Directory Groups**(활동 디렉토리 그룹) 탭을 선택합니다.
- 단계 5 삭제할 AD 그룹을 식별합니다.
- 단계 6 **Delete**(삭제) 아이콘을 선택합니다.
- 단계 7 **OK**(확인)를 클릭하여 AD 그룹 삭제를 확인합니다.

새 **CDO** 사용자 생성

새 CDO 사용자를 생성하려면 이 두 가지 작업이 필요합니다. 순차적으로 수행할 필요는 없습니다.

- 새 사용자를 위해 [Cisco Secure Cloud Sign On 계정 생성](#)
- [CDO 사용자 이름으로 CDO 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

Cisco Secure Cloud Sign-on 계정 생성은 새 사용자가 언제든지 수행할 수 있습니다. 사용자는 할당될 테넌트의 이름을 알 필요가 없습니다.

CDO에 로그인 정보

Cisco Defense Orchestrator(CDO)는 Cisco Secure Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. CDO에 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 2019년 10월 14일 이전에 CDO 테넌트가 존재했다면 이 문서 대신 [Cisco Secure Cloud Sign On ID 제 공자로 마이그레이션](#), on page 41를 사용하여 로그인 지침을 사용합니다.

로그인하기 전에



DUO Security 설치. 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 [Duo 이중 인증 가이드: 등록 가이드](#)를 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 Secure Cloud Sign-On 계정 등록

- a. <https://sign-on.security.cisco.com>으로 이동합니다.
- b. Sign In(로그인) 화면 하단에서 **Sign up**(등록)를 클릭합니다.

Security Cloud Sign On

Formerly known as SecureX Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

- c. 계정 생성 상자의 필드를 채우십시오.

Account Sign Up

Provide following information to create enterprise account.

[Back to login page](#)

Email *

First name *

Last name *

Country *

Password *

Confirm Password *

I agree to the [End User License Agreement and Privacy Statement](#).

Sign up

[Cancel](#)

다음은 몇 가지 팁입니다.

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

d. Create Account(계정 생성)를 클릭한 후.

Cisco는 등록된 주소로 확인 이메일을 보냅니다. 이메일을 열고 어카운트 활성화를 클릭합니다.

단계 2 Duo를 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 Guide](#)를 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. 2단계 인증을 사용하여 Cisco Secure Cloud Sign-On에 로그인합니다.

단계 3 (선택 사항) Google OTP를 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 Secure Sign-On 어카운트에 대한 어카운트 복구 옵션 구성

- a. SMS를 사용하여 계정을 재설정하려면 복원 전화번호를 선택합니다.
- b. 보안 이미지를 선택합니다.
- c. **Create My Account**(내 계정 생성)를 클릭합니다. 이제 CDO 앱 타일이 있는 Cisco Security Sign-On 대시보드가 표시됩니다. 다른 앱 타일도 표시될 수 있습니다.

Tip

대시보드에서 타일을 끌어 원하는 대로 정렬하고, 탭을 생성하여 타일을 그룹화하고, 탭의 이

CDO 사용자 이름으로 CDO 사용자 레코드 생성

"슈퍼 관리자" 권한이 있는 CDO 사용자만 CDO 사용자 레코드를 생성할 수 있습니다. 슈퍼 관리자는 위의 **Create Your CDO Username**(CDO 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 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.

단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.

단계 4 파란색 더하기  버튼을 클릭하여 새 사용자를 테넌트에 추가합니다.

단계 5 사용자의 이메일 주소를 입력합니다.

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

단계 6 드롭다운 메뉴에서 사용자 **Cisco Defense Orchestrator**의 사용자 역할을 선택합니다.

단계 7 **OK**(확인)를 클릭합니다.

새 사용자가 Cisco Secure Sign-On 대시보드에서 CDO 열기

Procedure

단계 1 Cisco Secure Sign-on 대시보드에서 적절한 **CDO** 타일을 클릭합니다. **CDO** 타일은 <https://defenseorchestrator.com>으로 안내하고 **CDO(EU)** 타일은 <https://defenseorchestrator.eu>로 안내합니다.

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](#)를 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.



Cisco Defense Orchestrator의 사용자 역할

Cisco Defense Orchestrator(CDO)에는 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 버전을 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 버전을 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

관리 사용자는 대부분의 CDO 측면에 대한 완전한 액세스 권한을 가집니다. 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 40를 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 [사용자 관리](#)를 참조하십시오.

사용자 레코드를 변경하려면 슈퍼 관리자여야 합니다. 테넌트에 슈퍼 관리자가 없는 경우 [Defense Orchestrator support\(Defense Orchestrator 지원\)](#)에 문의하십시오.

사용자 역할에 대한 사용자 레코드 생성

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.com>으로 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 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.

단계 3 **User Management(사용자 관리)** 탭을 클릭합니다.

단계 4 파란색 더하기  버튼을 클릭하여 새 사용자를 테넌트에 추가합니다.

단계 5 사용자의 이메일 주소를 입력합니다.

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


단계 6 드롭다운 메뉴에서 사용자 **Cisco Defense Orchestrator의 사용자 역할**을 선택합니다.

단계 7 **v**를 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 40를 참조하십시오.

API 전용 사용자 생성

프로시저

-
- 단계 1 CDO에 로그인합니다.
 - 단계 2 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
 - 단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.
 - 단계 4 테넌트에 새 사용자를 추가하려면 파란색 플러스 버튼  를 클릭합니다.
 - 단계 5 **API Only User**(API 전용 사용자) 확인란을 선택합니다.
 - 단계 6 **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 7 드롭다운 메뉴에서 사용자 **Cisco Defense Orchestrator의 사용자 역할**을 선택합니다.
 - 단계 8 **OK**(확인)를 클릭합니다.
 - 단계 9 **User Management**(사용자 관리) 탭을 클릭합니다.
 - 단계 10 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 받게 됩니다.



Note 이 작업을 수행하려면 CDO에서 **슈퍼 관리자** 역할이 있어야 합니다.



Caution 사용자 레코드의 역할을 변경하면 사용자 레코드와 연결된 **API 토큰**이 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 오른쪽 상단의 관리자 드롭다운에서 **Settings**(설정)를 클릭합니다.
- 단계 3 **User Management**(사용자 관리) 탭을 클릭합니다.
- 단계 4 사용자 행에서 편집 아이콘을 클릭합니다.
- 단계 5 역할 드롭다운 메뉴에서 사용자의 새 **Cisco Defense Orchestrator의 사용자 역할**을 선택합니다.
- 단계 6 사용자 레코드에 사용자와 연결된 API 토큰이 있는 것으로 표시되면 사용자의 역할을 변경하고 결과적으로 API 토큰을 삭제할 것임을 확인해야 합니다.
- 단계 7 **v**를 클릭합니다.
- 단계 8 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 레코드와 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 오른쪽 상단의 관리자 드롭다운에서 **Settings(설정)**를 클릭합니다.
- 단계 3 **User Management(사용자 관리)** 탭을 클릭합니다.
- 단계 4 삭제할 사용자 행에서 휴지통 아이콘 를 클릭합니다.
- 단계 5 **OK(확인)**를 클릭합니다.
- 단계 6 확인을 클릭하여 테넌트에서 계정을 제거할 것임을 확인합니다.

서비스 페이지 정보 보기

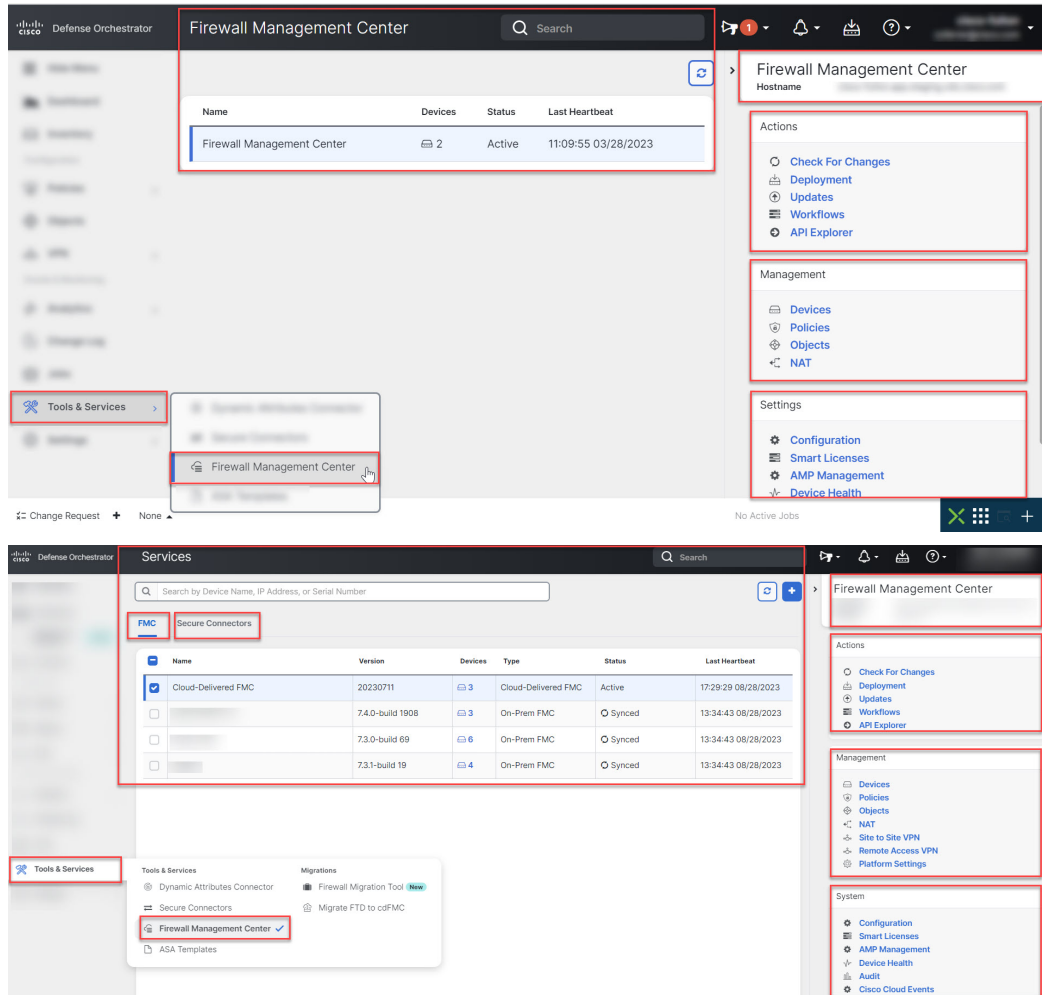
Services(서비스) 페이지에 CDO가 제공하는 서비스 목록이 표시됩니다. **FMC** 탭을 선택하면 CDO 계정에 연결된 클라우드 사용 Firewall Management Center 및 CDO에 온보딩된 모든 온프레미스 Management Center가 나열됩니다. 이러한 온프레미스 Management Center에서 관리하는 디바이스는 **Inventory(인벤토리)** 페이지에 나열됩니다. **Services(서비스)** 페이지의 **Secure Connector(보안 커넥터)** 탭 아래에도 보안 커넥터가 나열됩니다.

파란색 더하기 아이콘()을 클릭하여 **FMC** 탭을 선택하고 온프레미스 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(인벤토리)** 페이지로 이동하며, 이 페이지에는 선택된 온프레미스 Management Center에서 관리하는 디바이스가 자동으로 필터링되어 표시됩니다. **Services(서비스)** 페이지에서는 하나 이상의 온프레미스 Management Center를 동시에 선택하여 Management Center 그룹에 대한 작업을 한 번에 수행할 수 있습니다. 클라우드 사용 Firewall Management Center가 선택된 상태에서는 어떤 온프레미스 Management Center도 선택할 수 없습니다. 새 보안 커넥터를 추가하거나 기존 보안 커넥터에 대해 작업을 수행하려면 **Secure**

Connector(보안 커넥터) 탭을 선택하고 를 클릭합니다.

CDO의 메인 메뉴에서 클라우드 사용 Firewall Management Center 애플리케이션 페이지를 엽니다.

Tools & Services(툴 및 서비스) > **Firewall Management Center**로 이동합니다.



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

- 클라우드 사용 Firewall Management Center가 테넌트에 구축되지 않은 경우, **Request FMC(FMC 요청)**를 클릭합니다.
- 클라우드 사용 Firewall Management Center에 구축된 Secure Firewall Threat Defense 디바이스 수.
- CDO 및 클라우드 사용 Firewall Management Center 페이지 간의 연결 상태.
- 클라우드 사용 Firewall Management Center의 마지막 하트비트. 이는 클라우드 사용 Firewall Management Center 자체의 상태와 여기에서 관리하는 디바이스 수가 이 페이지의 테이블과 맞도록 동기화된 것을 나타냅니다.
- 선택한 클라우드 사용 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 사용 Firewall Management Center 사용자 인터페이스를 엽니다.

클라우드 사용 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.

클라우드 사용 **Firewall Management Center** 디바이스 수 및 상태 업데이트

Cloud-Delivered FMC(클라우드 제공 FMC)를 선택하고 **Actions**(작업) 창에서 **Check for Changes**(변경 사항 확인)를 클릭합니다. 테이블의 디바이스 수 및 상태 정보가 이 페이지와 클라우드 사용 Firewall Management Center가 마지막으로 동기화되었을 때 사용 가능한 정보로 업데이트됩니다. 동기화는 10분마다 이루어집니다.

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

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

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

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



참고 한번 클릭하면 동일한 탭에서 클라우드 사용 Firewall Management Center 페이지가 열립니다.

다음은 새 탭에서 클라우드 사용 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 사용 Firewall Management Center 포털이 로그아웃됩니다.

디바이스 및 서비스 관리

Cisco CDO(Defense Orchestrator)는 지원되는 디바이스 및 서비스를 보고, 관리하고, 필터링하고, 평가하는 기능을 제공합니다. **Inventory**(인벤토리) 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. [재고 목록 페이지 정보 보기, 97 페이지](#)을 참조하십시오.
- 개별 디바이스 및 서비스를 평가하고 조치를 취합니다.
- 디바이스 및 서비스별 정보를 보고 문제를 해결합니다.
- 다음에서 관리하는 위협 방어 디바이스의 디바이스 상태를 확인합니다.
 - [클라우드 사용 Firewall Management Center](#)
 - [온프레미스 Management Center](#)

클라우드 사용 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. [검색, 101 페이지](#)을 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. [필터](#)를 참조하십시오.

CDO에서 디바이스의 IP 주소 변경

IP 주소를 사용하여 CDO(Cisco Defense Orchestrator)에 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 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)를 클릭합니다.

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

단계 3 해당 디바이스 탭을 클릭합니다.

필터 및 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.

Nashua Building 1 
ASA 10.86.118.4:443 

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 97](#)
- [CDO에 디바이스 대량 다시 연결, on page 96](#)

CDO에서 디바이스의 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 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)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.

Nashua Building 1 

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

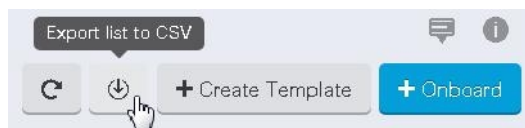
단계 1 CDO 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.

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

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

필터 및 검색 기능을 사용하여 필요한 디바이스를 찾을 수 있습니다.

단계 4 **Export list to CSV**(CSV로 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 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)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 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 Firepower FDM(Firepower Device Manager)). 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.

The screenshot shows a user interface for managing external links. At the top, there is a dropdown menu labeled 'External Links'. Below it is a search bar with a magnifying glass icon and the word 'Search'. Underneath is a section titled 'Add External Links' with a help icon. Below this section is a table with two columns: 'Name' and 'URL'. To the right of the 'URL' column is a blue button with a white plus sign, indicating where to click to add a new link.

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 FDM 매니저 디바이스의 FDM에 도달해야 합니다.

관련 정보:

- [디바이스 메모 작성, on page 97](#)

- [디바이스 및 서비스 목록 내보내기](#), on page 92

장치에서 외부 링크 생성

Procedure

-
- 단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)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 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.com>을 입력하는 것과 같이 전체 URL을 지정해야 합니다.
 - 단계 8 +를 클릭하여 링크를 디바이스와 연결합니다.
-

FDM에 대한 외부 링크 생성

다음은 CDO에서 직접 과 FTD의 FDM(Firepower Device Manager)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 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 FDM과 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 **Devices & Services**(디바이스 및 서비스)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 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.com>을 입력하는 것과 같이 전체 URL을 지정해야 합니다.

단계 8 +를 클릭하여 링크를 디바이스와 연결합니다.

외부 링크 편집 또는 삭제

Procedure

단계 1 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)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 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 **Devices & Services**(디바이스 및 서비스)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 **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 다시 연결

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 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)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 [작업 페이지](#)로 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 메모 작성

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


Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)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.

재고 목록 페이지 정보 보기

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. **검색** 기능을 사용하거나 **필터**를 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.

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:West**입니다. 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 **Devices & Services**(디바이스 및 서비스)를 클릭합니다. 개체에 레이블을 추가하려면 왼쪽 탐색 창에서 **Objects**(개체)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** 생성된 테이블에서 하나 이상의 디바이스 또는 모델을 선택합니다.
- 단계 5** 오른쪽의 **Add Groups and Labels**(그룹 및 레이블 추가) 필드에서 디바이스의 레이블을 지정합니다.
- 단계 6** 파란색 + 아이콘을 클릭합니다.

필터

Inventory(재고 목록) 및 **Objects**(개체) 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 **Devices and Services**(디바이스 및 서비스), **Policies**(정책) 및 **Objects**(개체) 탭의 왼쪽 창에서 을 클릭합니다.

Inventory(재고 목록) 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.



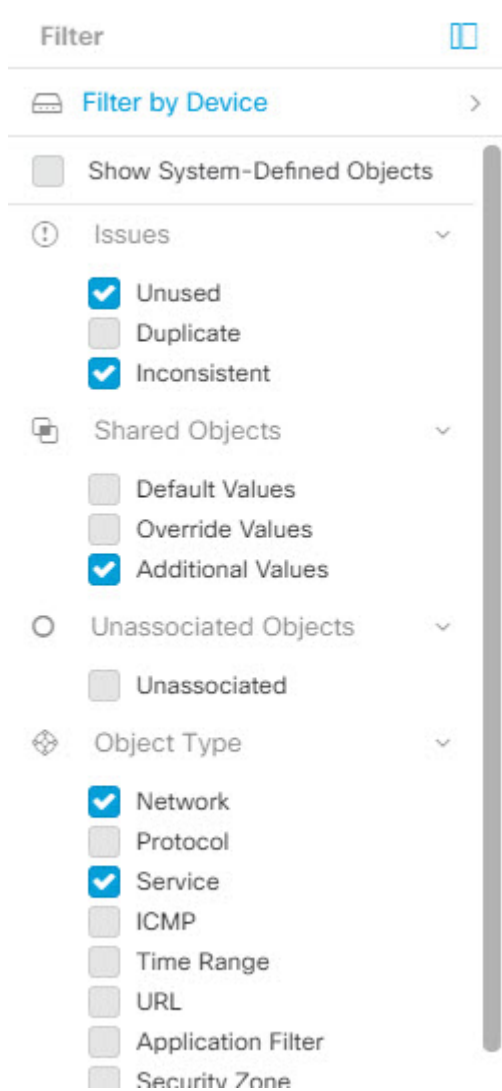
참고 **FTD** 탭이 열리면 필터 창이 CDO에서 디바이스에 액세스하는 데 사용되는 관리 애플리케이션을 기반으로 FDM 관리 디바이스를 표시하는 필터를 제공합니다.

- FDM: FTD API 또는 FDM을 사용하여 관리되는 디바이스.
- FMC-FTD: Firepower Management Center를 사용하여 관리되는 디바이스.
- FTD: FTD 관리를 사용하여 관리되는 디바이스.

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.

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 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.




동일한 SDC를 사용하여 CDO에 연결하는 모든 디바이스 찾기

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.

검색

CDO는 디바이스, 개체 및 액세스 그룹을 쉽게 찾을 수 있는 강력한 검색 기능을 제공합니다. **Devices & Service**(디바이스 및 서비스) 공간에서 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.

마찬가지로 **Objects**(개체) 공간의 검색 창을 사용하여 개체 이름의 일부를 입력하거나 IP 주소, 포트, 명명된 주소, 프로토콜의 일부를 입력하여 개체를 찾을 수 있습니다.

Procedure

단계 1 인터페이스 상단 근처의 검색 창으로 이동합니다.

단계 2 검색 표시줄에 검색 기준을 입력하면 해당 결과가 표시됩니다.

글로벌 검색

전체 검색 기능을 사용하면 CDO에서 관리하는 장치를 빠르게 찾고 탐색할 수 있습니다.

모든 검색 결과는 선택한 인덱싱 옵션을 기반으로 합니다. 인덱싱 옵션은 다음과 같습니다.

- **전체 인덱싱** - 전체 인덱싱 프로세스를 호출해야 합니다. 이 프로세스는 시스템의 모든 장치와 개체를 검색하고 인덱싱을 호출한 후에만 검색 인덱스에 표시합니다. 전체 인덱싱을 호출하려면 관리 권한이 있어야 합니다.

자세한 내용은 [전체 인덱싱 시작, 102 페이지](#)를 참고하십시오.

- **중분 인덱싱** - 장치 또는 개체가 추가, 수정 또는 삭제될 때마다 검색 인덱스가 자동으로 업데이트되는 이벤트 기반 인덱싱 프로세스입니다.

검색 필드에 입력하는 정보는 대소문자를 구분하지 않습니다. 다음 엔터티를 사용하여 전역 검색을 수행할 수 있습니다.

- 장치 이름 - 부분 장치 이름, URL, IP 주소 또는 범위를 지원합니다.
- 개체 유형 - 개체 이름, 개체 설명 및 구성된 값을 지원합니다.
- 정책 유형 - 정책 이름, 정책 설명, 규칙 이름 및 규칙 설명을 지원합니다.

CDO에서 관리되는 클라우드 제공 방화벽 관리 센터 및 온프레미스 FMC는 다음 정책 유형을 지원합니다.

- 액세스 제어 정책
- 사전 필터 정책
- 위협 방어 NAT 정책

검색식을 입력하면 인터페이스에 검색 결과가 표시되기 시작하므로 검색을 실행하기 위해 *Enter* 키를 누를 필요가 없습니다.

검색 결과에는 검색 문자열과 일치하는 모든 장치 및 개체가 표시됩니다. 검색 문자열이 디바이스 또는 개체보다 더 많이 일치하면 결과가 범주(디바이스, 개체 및 `connected_fmc`) 아래에 나타납니다.

기본적으로 검색 결과의 첫 번째 항목이 강조 표시되고 해당 항목에 대한 관련 정보가 오른쪽 창에 나타납니다. 검색 결과를 스크롤하고 항목을 클릭하면 해당 정보를 볼 수 있습니다. 항목 옆의 화살표 아이콘을 클릭하여 해당 페이지로 이동할 수 있습니다.



참고

- 전역 검색은 중복 검색 결과를 표시하지 않습니다. 개체의 경우 공유 개체의 UID는 개체 보기로 이동하는 데 사용됩니다.
- CDO에서 장치를 삭제하면, 연결된 모든 개체가 전역 검색 인덱스에서 제거됩니다.
- 정책에서 개체를 삭제하고 전체 인덱싱을 시작하기 전에 장치를 유지하면, 개체가 장치와 연결되어 있기 때문에 전역 검색 인덱스에 남아 있습니다.

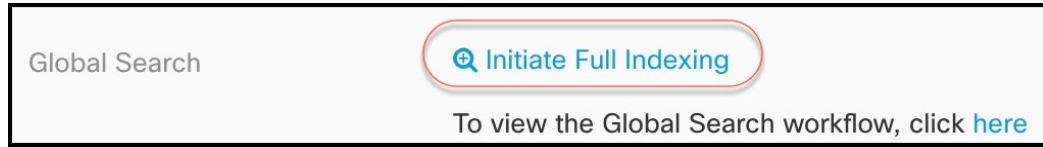
전체 인덱싱 시작

프로시저

단계 **1** 관리자 또는 슈퍼 관리자 권한이 있는 계정을 사용하여 CDO에 로그인합니다.

단계 **2** CDO 메뉴 표시줄에서 **Settings(설정) > General Settings(일반 설정)**를 탐색합니다.

단계 **3** 전역 검색에서 **Initiate Full Indexing(전체 인덱싱 시작)**을 클릭하여 인덱싱을 트리거합니다.



참고 전체 인덱싱을 시작하면 CDO 테넌트의 기존 인덱싱이 지워집니다.

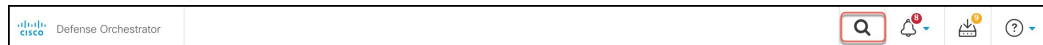
단계 4 글로벌 검색 워크플로우를 보려면 **here**(여기)를 클릭합니다.

전역 검색 수행

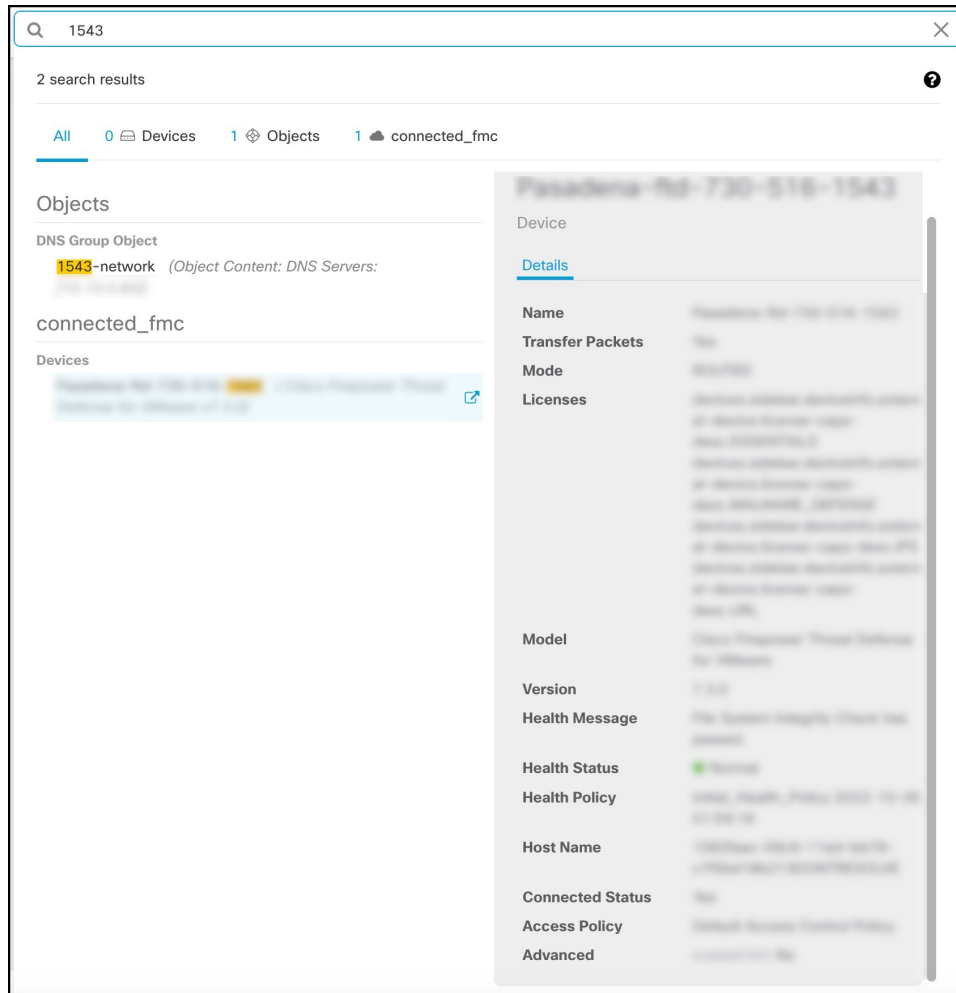
프로시저

단계 1 CDO에 로그인합니다.

단계 2 CDO 페이지 오른쪽 상단 모서리에 있는 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.



검색 문자열을 입력하기 시작하면 검색 결과에 가능한 항목 목록이 표시됩니다. 검색 결과는 All, Devices, Objects 및 connected_fmc의 네 가지 범주 아래에 나타납니다. 오른쪽 창에는 선택한 검색 결과에 대한 정보가 표시됩니다.



단계 3 검색 결과에서 디바이스 또는 개체를 선택하고 화살표 아이콘을 클릭하여 검색 결과에서 해당 디바이스 및 개체 페이지로 이동합니다. 검색 결과에서 항목을 선택하고 화살표 아이콘을 클릭하여 검색 결과에서 해당 페이지로 이동합니다.

참고 클라우드 사용 Firewall Management Center에서 디바이스 검색 결과를 선택하면, CDO에서 클라우드 사용 Firewall Management Center 사용자 인터페이스로 이동할 수 있습니다.

클라우드 사용 Firewall Management Center에 대한 자세한 내용은 [Cisco Defense Orchestrator에서 Cloud-Delivered Firewall Management Center로 Firewall Threat Defense 관리](#)를 참조하십시오.

단계 4 **X**를 클릭하여 검색 표시줄을 닫습니다.

CDO 명령줄 인터페이스

CDO는 사용자에게, FDM 관리 위협 방어 디바이스를 관리하기 위한 CLI(명령줄 인터페이스)를 제공합니다. 사용자는 단일 디바이스 또는 여러 디바이스에 동시에 명령을 전송할 수 있습니다.

관련 정보:

- FTD CLI 설명서는 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오. 참고로 FDM 관리 디바이스는 CLI 기능이 제한되어 있습니다. 이러한 디바이스에는 show, ping, traceroute, packet-tracer, failover 및 shutdown 명령만 있습니다.

명령줄 인터페이스 사용

Procedure

- 단계 1 **Inventory**(재고 목록) 페이지를 엽니다.
- 단계 2 재고 목록 테이블 위에 있는 디바이스 버튼을 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](#), 105 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.

```

> object network email_server_north
  host 192.168.10.2
  object network email_server_south
  host 192.168.20.2
  object network email_server_headquarters
  host 192.168.30.2
  object-group network email_servers_all
  network-object object email_server_north
  network-object object email_server_south
  network-object object email_server_headquarters

```

Press Cmd+Enter to send command

FDM 관리 디바이스 명령 입력: CLI 콘솔은 기본 위협 방어 CLI를 사용합니다. CLI 콘솔을 사용하여 진단 CLI, 전문가 모드 또는 FXOS CLI(FXOS를 사용하는 모델)를 시작할 수는 없습니다. 기타 CLI 모드를 시작해야 하는 경우에는 SSH를 사용합니다.

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 Inventory**(인벤토리) 페이지에서 구성할 디바이스를 선택합니다.

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 응답 창에 명령 결과를 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, 위협 방어, SSH 및 Cisco IOS Secure Firewall Cloud Native 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.

관련 정보:

- FDM 관리 디바이스 설명서의 경우 CDO는 기본 FTD CLI만 지원합니다. 이러한 디바이스에는 show, ping, traceroute, packet-tracer, failover 및 shutdown 명령만 있습니다.

위협 방어 CLI 설명서는 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오.

대량 CLI 인터페이스

The screenshot displays the Bulk CLI interface. On the left, a history list shows previous commands like 'show version', 'show ssh sessions', 'show reload', and 'show ip'. The main area shows the command 'show run | grep user' being sent to three devices. On the right, the execution results are shown, including a list of devices (10.82.109.160, 10.82.109.181, 10.82.109.187) and their respective responses, such as user statistics for 'LOCAL', 'admin', 'chris', and 'alice'.



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.

숫자	설명
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.
4	<p>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.</p> <p>Note CDO는 다음 두 가지 상황에서 Done!(완료!) 메시지를 표시합니다.</p> <ul style="list-style-type: none"> 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 Inventory (인벤토리) 테이블에서 선택한 디바이스가 표시되며 명령을 보낸 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 탐색 모음에서 **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 탐색 모음에서 **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 응답 창에 명령 결과를 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 devices**(X 디바이스)를 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 확인하는 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.

디바이스 관리를 위한 CLI 매크로

CLI 매크로는 즉시 사용할 수 있는 완전한 형식의 CLI 명령이거나 실행 전에 수정할 수 있는 CLI 명령의 템플릿입니다. 모든 매크로는 하나 이상의 FTD 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. FTD 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 생성](#)을 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

- FTD 디바이스의 경우 CDO는 FDM의 CLI 콘솔에서 실행할 수 있는 명령(show, ping, traceroute, packet-tracer, failover, reboot 및 shutdown)만 지원합니다. 이러한 명령의 구문에 대한 전체 설명은 [Cisco Firepower Threat Defense 명령 참조](#)를 참조하십시오.

단계 2 탐색 모음에서 **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 실행](#)을 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 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)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 시계 ⌚를 클릭합니다. 매크로로 전환할 항목을 선택하면 명령 창에 명령이 나타납니다.
 - CLI 매크로 즐겨찾기 스타 ★를 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 검색 별 를 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 묶은 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 실행](#)을 참조하십시오.

CLI 매크로 실행

Procedure

- 단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)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 별표 ★를 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. 다했습니다.
 - 아래의 Configure DNS 매크로와 같은 매개변수가 매크로에 포함된 경우 **>_View Parameters**(매개변수 보기)를 클릭합니다.

```

★ Using Macro: Configure DNS
> dns domain-lookup {{IF_NAME}}
dns server-group DefaultDNS
name-server {{IP_ADDR}}

```

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!

- FTD의 경우 디바이스의 활성 구성이 업데이트됩니다.

단계 10 명령을 전송한 후 "일부 명령이 실행 중인 구성을 변경했을 수 있습니다."라는 메시지와 함께 두 개의 링크가 표시될 수 있습니다.

⚠ Some commands may have made changes to the running config [Write to Disk](#) [Dismiss](#)

- **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 FTD 디바이스에 대해 변경됩니다. 매크로는 특정 디바이스에 한정되지 않습니다.

Procedure

단계 1 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)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 실행](#)를 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 내비게이션 바에서 **Devices & Services**(디바이스 및 서비스)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 아이콘 를 클릭합니다.
- 단계 8 CLI 매크로를 제거할지 확인합니다.

명령줄 인터페이스 설명서

CDO는 FDM 관리 디바이스의 명령줄 인터페이스를 부분적으로 지원합니다. 사용자가 단일 디바이스 및 여러 디바이스에 명령 및 응답 형식으로 동시에 명령을 전송할 수 있도록 CDO 내에서 터미널과 유사한 인터페이스를 제공합니다. CDO에서 지원되지 않는 명령의 경우 PuTTY 또는 SSH 클라이언트와 같은 디바이스 GUI 터미널을 사용하여 디바이스에 액세스하고, 추가 명령은 [CLI 설명서](#)를 참조하십시오.

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 탐색 모음에서 **Devices & Services**(디바이스 및 서비스)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 **Devices & Services**(디바이스 및 서비스) 페이지를 엽니다.
 - 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 탐색 창에서 **Devices & Services**(디바이스 및 서비스)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 아이콘 을 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 105](#)
- [새 명령에서 CLI 매크로 생성](#)
- [CLI 매크로 삭제](#)
- [CLI 매크로 편집](#)
- [CLI 매크로 실행](#)
- [명령줄 인터페이스 설명서](#)
- [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 탐색 창에서 **Devices & Services**(디바이스 및 서비스)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.
-


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 아이콘 로 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 시

간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘 로 식별됩니다.

- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘 로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, CDO는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다.

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 필터**합니다.
- 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.

온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 [문제 해결 Cisco Defense Orchestrator](#)를 참조하십시오.

개체 유형

다음 표에서는 CDO를 사용하여 디바이스에 대해 생성하고 관리할 수 있는 개체에 대해 설명합니다.

Table 5: FDM 관리 디바이스 개체 유형

개체	설명
애플리케이션 필터 개체	애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.

개체	설명
AnyConnect 클라이언트 프로파일	AnyConnect 클라이언트 프로파일 개체는 파일 개체이며 구성(일반적으로 원격 액세스 VPN 정책)에서 사용되는 파일을 나타냅니다. AnyConnect 클라이언트 프로파일 및 AnyConnect 클라이언트 이미지 파일을 포함할 수 있습니다.
인증서 개체	디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.
DNS 그룹 개체	www.example.com과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다. 관리 및 데이터 인터페이스에 대해서도 다른 DNS 그룹 개체를 구성할 수 있습니다.
Firepower 지리위치 필터 개체 생성 및 편집	지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소를 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.
IKEv1 정책 생성 또는 편집	IKEv1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 매개변수가 포함되어 있습니다.
IKEv2 정책	IKEv2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 매개변수가 포함되어 있습니다.
IKEv1 IPSEC 제안	IPsec 제안 개체는 IKE 1단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.
IKEv2 IPSEC 제안	IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.
네트워크 개체	네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다.

개체	설명
보안 영역 개체	보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다.
서비스 개체	서비스 개체, 서비스 그룹 및 포트 그룹은 TCP/IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다.
SGT 그룹 생성	SGT 동적 개체는 ISE에서 할당된 SGT를 기반으로 소스 또는 대상 주소를 식별하며, 그런 다음 수신 트래픽과 일치시킬 수 있습니다.
시스템 로그 서버 개체	Syslog 서버 개체는 연결 지향형 또는 진단 Syslog(Syslog) 메시지를 수신할 수 있는 서버를 식별합니다.
URL 개체	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.

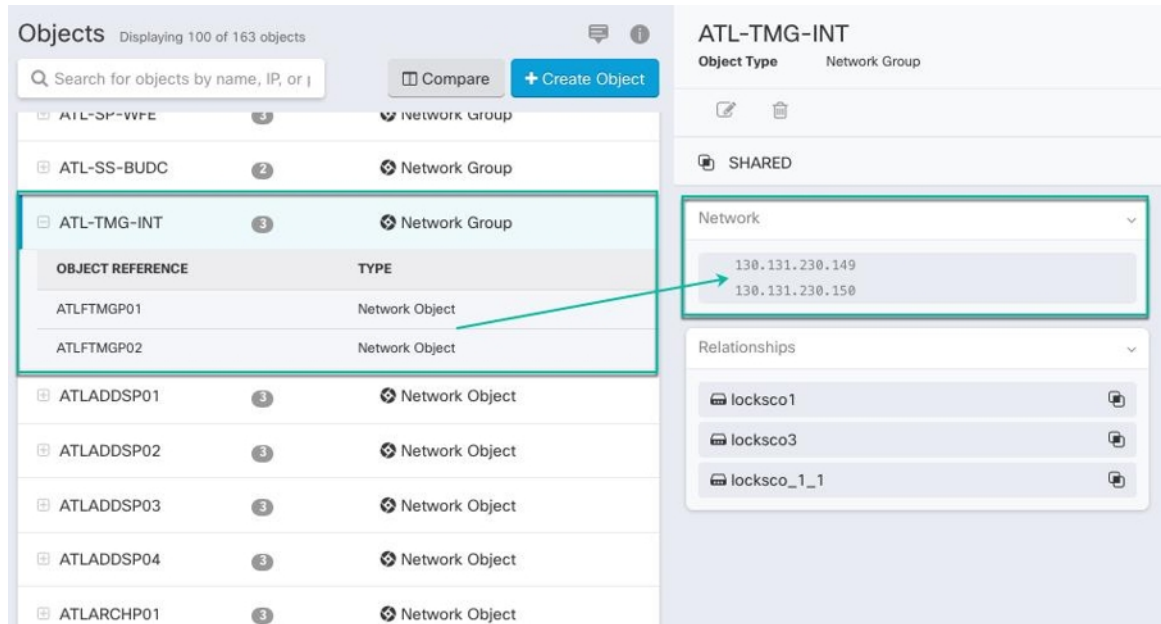
공유 개체

CDO(Cisco Defense Orchestrator)는 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 오버라이드를 사용하면 특정 디바이스에서 공유 네트워크 개체의 값을 오버라이드할 수 있습니다. CDO는 오버라이드를 구성할 때 지정한 디바이스에 해당하는 값을 사용합니다. 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체에 대하여 CDO는 이러한 값이 오버라이드 되기 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 오버라이드는 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.

Editing Shared Network Object
✕

Object Name *

Devices

2 Devices

Usage

0 Rule Sets

Description

Default Value ▾

ASAv-99-18

Override Values ▾

Value	Devices	
126.0.2.4	Pasadena-ftd-730-516-...	
126.0.1.6	BGL_FTD_7.3	
126.0.1.9	connected_fmc	

Cancel
Save



Note CDO를 사용하면 규칙 세트의 규칙과 연관된 개체를 오버라이드할 수 있습니다. 규칙에 새 개체를 추가할 때 디바이스를 규칙 세트에 연결하고 변경 사항을 저장한 후에만 오버라이드할 수 있습니다. 자세한 내용은 [Configure Rulesets for an FTD\(FTD에 대한 규칙 세트 구성\)](#)을 참조하십시오.



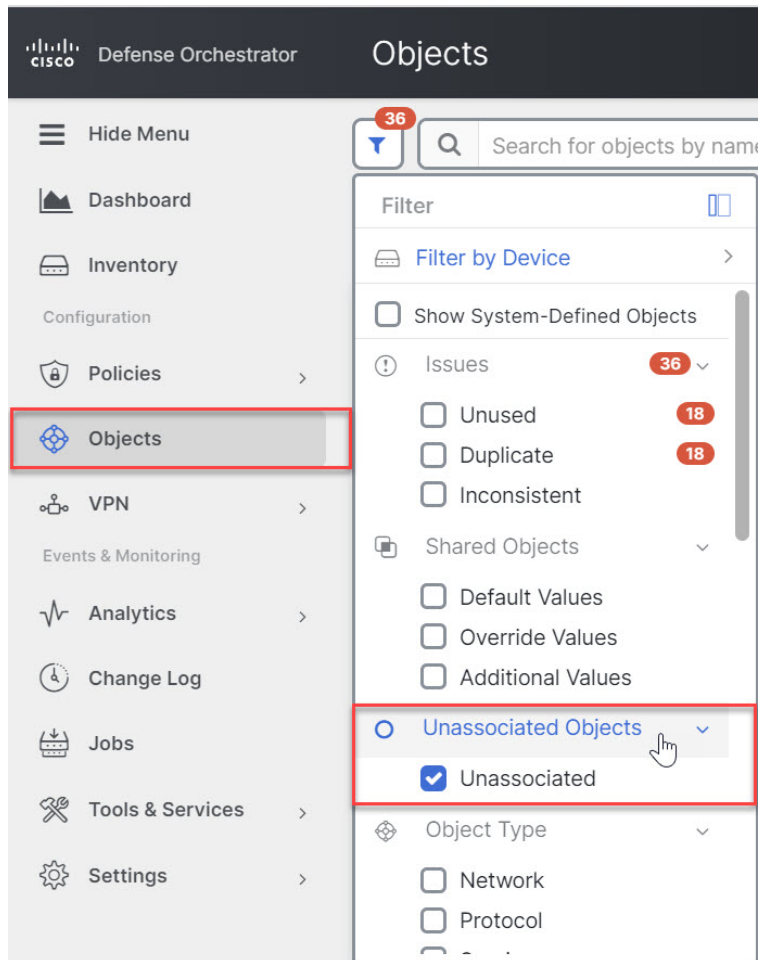
Note 일관되지 않은 개체가 있는 경우 오버라이드를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 [불일치 개체 문제 해결](#)을 참조하십시오.

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 사용할 때, CDO는 해당 개체의 사본을 생성하고 해당 사본을 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 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.

단계 2 페이지에서 개체를 필터링하여 비교하려는 개체를 찾습니다.

단계 3 **Compare**(비교) 버튼  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

Inventory(재고 목록) 및 **Objects**(개체) 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 **Devices and Services**(디바이스 및 서비스), **Policies**(정책) 및 **Objects**(개체) 탭의 왼쪽 창에서 을 클릭합니다.

Inventory(재고 목록) 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.



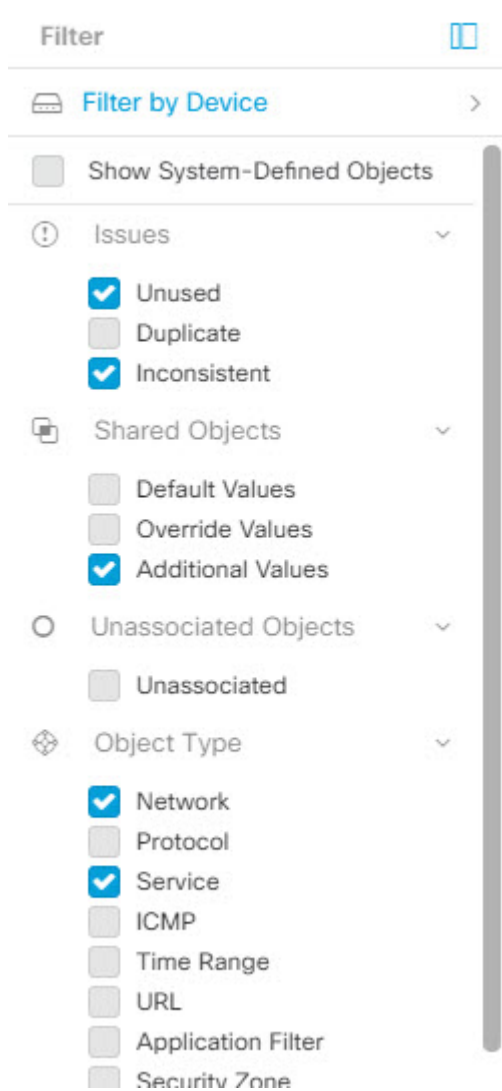
참고 **FTD** 탭이 열리면 필터 창이 CDO에서 디바이스에 액세스하는 데 사용되는 관리 애플리케이션을 기반으로 FDM 관리 디바이스를 표시하는 필터를 제공합니다.

- FDM: FTD API 또는 FDM을 사용하여 관리되는 디바이스.
- FMC-FTD: Firepower Management Center를 사용하여 관리되는 디바이스.
- FTD: FTD 관리를 사용하여 관리되는 디바이스.

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.

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 공유 개체 및 네트워크 또는 서비스 유형의 개체 검색에 필터를 적용합니다.



개체 필터

필터링하려면 Objects(개체) 탭의 왼쪽 창에서 ▼(를) 클릭합니다.

- **All Objects**(모든 개체) - 이 필터는 CDO에 온보딩된 모든 디바이스에서 사용 가능한 모든 개체를 제공합니다. 이 필터는 모든 개체를 찾아보거나 하위 필터를 검색하거나 추가로 적용하기 위한 시작점으로 유용합니다.
- **Shared Objects**(공유 개체) - 이 빠른 필터는 CDO가 두 개 이상의 디바이스에서 공유하는 것으로 확인한 모든 개체를 표시합니다.
- **Objects By Device**(디바이스별 개체) - 선택한 디바이스에 있는 개체를 볼 수 있도록 특정 디바이스를 선택할 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.) AND는

* 일치하지 않는 개체 AND는

* 네트워크 개체 또는 서비스 개체 AND

* 개체 명명 규칙에 "group"이라는 단어가 있습니다.

Show System Objects(시스템 개체 표시)를 선택했으므로 결과에 시스템 개체와 사용자 정의 개체가 모두 포함됩니다.

시스템 개체 필터 표시

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 Objects(시스템 개체 표시)는 기본적으로 꺼져 있습니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 **Show System Objects**(시스템 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 왼쪽의 CDO 탐색 바에서 **Objects**(개체)를 클릭하고 옵션을 선택합니다.
- 단계 2 페이지 상단의 필터 아이콘  을 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.

필터 기준에서 디바이스를 제외해야 하는 경우

- 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. **개체가 사용되지 않거나 중복되거나 일관성이 없더라도** 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 왼쪽의 CDO 탐색 바에서 **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 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.


한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 1 왼쪽의 CDO 탐색 모음에서 **Objects(개체)**를 선택하고 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 **Review and deploy(검토 및 배포)**하거나, 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 검토하고 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.

Table 6: 네트워크 개체의 허용되는 값

디바이스 유형	IPv4 / IPv6	단일 주소	주소 범위	전체(Fully Qualified) 도메인 이름	CIDR 표기법의 서브넷
FTD	IPv4 및 IPv6	예	예	예	예

Table 7: 네트워크 그룹의 허용되는 콘텐츠

디바이스 유형	IP 값	네트워크 개체	네트워크 그룹
FTD	아니요	예	예

제품 간 네트워크 개체 재사용

클라우드 사용 Firewall Management Center가 포함된 Cisco Defense Orchestrator 테넌트가 있는 경우:

Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체 또는 그룹을 생성하면 클라우드 사용 Firewall Management Center를 구성할 때 사용되는 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 개체 목록에도 개체의 복사본이 추가되며, 그 반대의 경우도 마찬가지입니다.

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 사용 Firewall Management Center에 대해 동일한 이름의 네트워크 개체가 이미 있는 경우 Secure Firewall Threat Defense, FDM 관리 위협 방어, ASA 또는 Meraki 네트워크 개체는 Cisco Defense Orchestrator의 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에서 복제되지 않습니다.

- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩된 위협 방어 디바이스의 네트워크 개체 및 그룹은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 복제되지 않으며, 클라우드 사용 Firewall Management Center에서 사용할 수 없습니다.

클라우드 사용 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 사용 Firewall Management Center 간에 네트워크 개체 공유는 새로운 테넌트에서 자동으로 활성화되지만 기존 테넌트에 대해서는 요청해야 합니다. 네트워크 개체를 클라우드 사용 Firewall Management Center와 공유하지 않는 경우 [TAC에 문의](#)하여 테넌트에서 기능을 활성화하십시오.

네트워크 개체 보기

CDO를 사용하여 생성한 네트워크 개체와 온보딩된 디바이스 구성에서 인식되는 CDO가 **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.

관련 정보:

- [Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집](#)

Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집

Firepower 네트워크 개체는 CIDR 표기법으로 표시된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에 사용되는 네트워크 개체 및 네트워크 그룹의 복합 그룹입니다. Cisco Defense Orchestrator(CDO)를 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

Firepower 네트워크 개체 및 그룹은 ASA, 위협 방어, FDM 관리 및 Meraki 디바이스에서 사용할 수 있습니다. [제품 간 네트워크 개체 재사용, on page 130](#)을 참조하십시오.



Note 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

**Caution**

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Table 8: 네트워크 개체에 추가할 수 있는 IP 주소

디바이스 유형	IPv4 / IPv6	단일 주소	주소 범위	PQDN(Partially Qualified Domain Name)	CIDR 표기법의 서브넷
Firepower	IPv4 / IPv6	예	예	예	예

관련 정보:

- [Firepower 네트워크 개체 생성, on page 132](#)
- [Firepower 네트워크 개체 편집, on page 134](#)
- [공유 네트워크 그룹에 값 추가, on page 137](#)
- [공유 네트워크 그룹의 추가 값 편집, on page 139](#)

Firepower 네트워크 개체 생성

**Note**

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **FTD > Network(네트워크)**를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 **Create a network object(네트워크 개체 생성)**를 선택합니다.

단계 6 **Value(값)** 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소, CIDR 표기법으로 표시된 서브넷 주소 또는 PQDN(Partially Qualified Domain Name)을 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다.

Note 호스트 비트 값을 설정하지 마십시오. 0이 아닌 호스트 비트 값을 입력하면 클라우드 사용 Firewall Management Center에서 호스트 비트가 설정되지 않은 IPv6 개체만 허용하므로 CDO가 개체를 생성하는 동안 이 값을 설정 해제합니다.

단계 7 **Add(추가)**를 클릭합니다.

주의: 새로 생성된 네트워크 개체는 규칙 또는 정책의 일부가 아니므로 FDM 관리 디바이스와 연결되지 않습니다. 이러한 개체를 보려면 개체 필터에서 **Unassociated(연결되지 않음)** 개체 범주를 선택합니다. 자세한 내용은 **개체 필터 구성**을 참고하십시오. 디바이스의 규칙 또는 정책에서 연결되지 않은 개체를 사용하면 이러한 개체는 해당 디바이스와 연결됩니다.

Firepower 네트워크 그룹 생성


네트워크 그룹은 네트워크 개체와 네트워크 그룹을 포함할 수 있습니다. 새 네트워크 그룹을 만들 때 이름, IP 주소, IP 주소 범위 또는 FQDN으로 기존 개체를 검색하고 네트워크 그룹에 추가할 수 있습니다. 개체가 없는 경우 동일한 인터페이스에서 해당 개체를 즉시 생성하고 네트워크 그룹에 추가할 수 있습니다.



Note 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지에서 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다.

Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.
- 단계 3 **FTD > Network(네트워크)**를 클릭합니다.
- 단계 4 개체 이름을 입력합니다.
- 단계 5 **Create a network group(네트워크 그룹 생성)**을 선택합니다.
- 단계 6 값 필드에 값이나 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.
- 단계 7 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 8 CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add**(추가)를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 9 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name**(이 이름의 새 개체로 추가)을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object**(새 개체로 추가)를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

참고: 편집 아이콘을 클릭하여 세부 정보를 편집할 수 있습니다. 삭제 버튼을 클릭해도 개체 자체는 삭제되지 않습니다. 대신 네트워크 그룹에서 제거됩니다.

단계 10 필요한 개체를 추가한 후 **Save**(저장)을 클릭하여 새 네트워크 그룹을 생성합니다.

단계 11 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).

Firepower 네트워크 개체 편집



Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 네트워크 개체를 선택하고 **Actions**(작업) 창에서 편집 아이콘  을 클릭합니다.

단계 4 "Firepower 네트워크 그룹 생성"에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 편집합니다.

Note 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

Firepower 네트워크 그룹 편집



Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure


단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 네트워크 그룹을 찾습니다.

단계 3 SGT 그룹을 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 필요한 경우 개체 이름과 설명을 변경합니다.

단계 5 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

- a. 개체 이름 또는 네트워크 그룹 옆에 나타나는 편집 아이콘  을 클릭하여 편집합니다.
- b. 확인 표시를 클릭하여 변경 사항을 저장합니다. 참고: 네트워크 그룹에서 값을 제거하려면 삭제 아이콘을 클릭합니다.

단계 6 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

- a. **Values(값)** 필드에 새 값이나 기존 네트워크 개체의 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다. 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.
- b. CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.
- c. 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.
 - 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
 - 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 7 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 정책이 표시됩니다.

단계 8 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 9 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

개체 오버라이드 추가



주의 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:


또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

프로시저

단계 1 왼쪽 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 오버라이드를 추가할 개체를 찾습니다.

단계 3 네트워크 개체를 선택하고 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 4 **Override Values**(오버라이드 값) 대화 상자에 값을 입력하고 + **Add Value**(+ 값 추가)를 클릭합니다.

중요 추가하려는 오버라이드에는 개체에 포함된 것과 동일한 유형의 값이 있어야 합니다. 예를 들어 네트워크 개체에 대해 호스트 값이 아닌 네트워크 값으로만 오버라이드를 구성할 수 있습니다.

단계 5 값이 추가된 것을 확인하면, 오버라이드 값에서 **Devices**(디바이스) 열의 셀을 클릭합니다.

단계 6 **Add Devices**(디바이스 추가)를 클릭하고 오버라이드를 추가할 디바이스를 선택합니다. 선택한 디바이스에는 오버라이드를 추가할 개체가 포함되어 있어야 합니다.

단계 7 **Save**(저장)를 클릭합니다. CDO는 변경의 영향을 받는 디바이스를 표시합니다.

단계 8 **Confirm**(확인)을 클릭하여 개체 및 개체의 영향을 받는 모든 디바이스에 대한 오버라이드 추가를 완료합니다.

참고 개체에 두 개 이상의 오버라이드를 추가할 수 있습니다. 그러나 오버라이드를 추가할 때마다 개체가 포함된 다른 디바이스를 선택해야 합니다.

단계 9 개체 오버라이드에 대해 자세히 알아보고 [개체 오버라이드 편집](#), 137 페이지가 기존 오버라이드를 편집하려면 [개체 재정의](#), 122 페이지를 참조하십시오.


개체 오버라이드 편집

개체가 디바이스에 있는 한 기존 오버라이드 값을 편집할 수 있습니다.


Procedure

단계 1 왼쪽 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.

단계 3 오버라이드가 있는 개체를 선택하고 작업 창에서 편집 아이콘  를 클릭합니다.

단계 4 오버라이드 값을 편집합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Override Values(오버라이드 값)의 Devices(디바이스) 열에 있는 셀을 클릭하여 새 디바이스를 할당합니다.** 이미 할당된 디바이스를 선택하고 **Remove Overrides(오버라이드 제거)**를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
- **Override Values(오버라이드 값)에서**  화살표를 클릭하여 무시하고 공유 개체의 기본값으로 생성합니다.
- 제거하려는 오버라이드 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save(저장)**를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 7 **모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.**

공유 네트워크 그룹에 값 추가

연결된 모든 디바이스에 있는 공유 네트워크 그룹의 값을 "기본값"이라고 합니다. CDO를 사용하면 공유 네트워크 그룹에 "추가 값"을 추가하고 해당 공유 네트워크 그룹과 연결된 일부 디바이스에 해당 값을 할당할 수 있습니다. CDO는 변경 사항을 디바이스에 구축할 때 콘텐츠를 확인하고 공유 네트워크 그룹과 연결된 모든 디바이스에 "기본값"을 무시하고 지정된 디바이스에만 "추가 값"을 무시합니다.

모든 사이트에서 액세스할 수 있어야 하는 본사에 4개의 AD 기본 서버가 있는 시나리오를 예로 들어 보겠습니다. 따라서 모든 사이트에서 사용할 "Active-Directory"라는 개체 그룹을 생성했습니다. 이제 지사 중 하나에 두 개의 AD 서버를 추가하려고 합니다. 개체 그룹 "Active-Directory"에서 해당 지사에 특정한 추가 값으로 세부 정보를 추가하여 이 작업을 수행할 수 있습니다. 이 두 서버는 "Active-Directory" 개체가 일관성이 있는지 또는 공유되는지를 확인하는 데 참여하지 않습니다. 따라서 모든 사이트에서 4개의 AD 기본 서버에 액세스할 수 있지만 지사(2개의 추가 서버 포함)는 2개의 AD 서버와 4개의 AD 기본 서버에 액세스할 수 있습니다.




Note 일치하지 않는 공유 네트워크 그룹이 있는 경우 추가 값을 사용하여 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 자세한 내용은 [불일치 개체 문제 해결](#)를 참조하십시오.



Caution 클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:
또는 **Objects(개체) > FDM Objects(FDM 개체)** 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects(개체) > Other FTD Objects(기타 FTD 개체)** 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.
한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 개체 필터 및 검색 필드를 사용하여 편집할 공유 네트워크 그룹을 찾습니다.
- 단계 3 **Actions(작업)** 창에서 편집 아이콘  을 클릭합니다.
 - **Devices(디바이스)** 필드에는 공유 네트워크 그룹이 있는 디바이스가 표시됩니다.
 - **Usage(사용)** 필드에는 공유 네트워크 그룹과 연결된 규칙 집합이 표시됩니다.
 - **Default Values(기본값)** 필드는 생성 중에 제공된 공유 네트워크 그룹과 연결된 기본 네트워크 개체 및 해당 값을 지정합니다. 이 필드 옆에서 이 기본값이 포함된 디바이스의 수를 볼 수 있으며, 클릭하여 해당 이름 및 디바이스 유형을 볼 수 있습니다. 이 값과 연결된 규칙 집합도 확인할 수 있습니다.
- 단계 4 **Additional Values(추가 값)** 필드에 값 또는 이름을 입력합니다. 입력을 시작하면 CDO에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.
- 단계 5 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.
- 단계 6 CDO가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(추가)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.
- 단계 7 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.
 - 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(이 이름의 새 개체로 추가)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
 - 새 개체를 생성하려면 **Add as New Object(새 개체로 추가)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

- 단계 8 **Devices**(디바이스) 열에서 새로 추가된 개체와 연결된 셀을 클릭하고 **Add Devices**(디바이스 추가)를 클릭합니다.
- 단계 9 원하는 디바이스를 선택하고 **OK**(확인)를 클릭합니다.
- 단계 10 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.
- 단계 11 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.
- 단계 12 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

공유 네트워크 그룹의 추가 값 편집




Caution

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지의 네트워크 개체 및 그룹에 대한 변경 사항은 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지의 해당 클라우드 사용 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.
- 단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 오버라이드가 있는 개체를 찾습니다.
- 단계 3 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.
- 단계 4 오버라이드 값을 편집합니다.
 - 값을 편집하려면 편집 아이콘을 클릭합니다.
 - **Devices**(디바이스) 열의 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides**(오버라이드 제거)를 클릭하여 해당 디바이스에서 오버라이드를 제거할 수 있습니다.
 - **Default Values**(기본값)의 ▼ 화살표를 클릭하여 푸시하고 공유 네트워크 그룹의 추가 값으로 설정합니다. 공유 네트워크 그룹과 연결된 모든 디바이스가 자동으로 할당됩니다.
 - **Override Values**(값 재정의)에서 ▲ 화살표를 클릭하여 공유 네트워크 그룹의 기본 개체로 푸시하고 설정합니다.
 - 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 5 **Save**(저장)를 클릭합니다. CDO에 변경의 영향을 받을 디바이스가 표시됩니다.

단계 6 **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 7 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축](#).

네트워크 개체 및 그룹 삭제

클라우드 사용 Firewall Management Center가 테넌트에 구축된 경우:

또는 **Objects**(개체) > **FDM Objects**(FDM 개체) 페이지에서 네트워크 개체나 그룹을 삭제하면 **Objects**(개체) > **Other FTD Objects**(기타 FTD 개체) 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

애플리케이션 필터 개체

애플리케이션 필터 개체는 Firepower 디바이스에서 사용됩니다. 애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.

개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

애플리케이션 필터 개체를 사용하지 않고 정책에서 애플리케이션과 애플리케이션 필터를 직접 선택할 수 있습니다. 그러나 애플리케이션 또는 필터의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다. 시스템에는 수정하거나 삭제할 수 없는 사전 정의된 여러 애플리케이션 필터가 포함되어 있습니다.



Note Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.



Note FDM 관리 FTD 디바이스가 CDO에 온보딩되면 액세스 규칙 또는 SSL 암호 해독에 정의된 규칙을 변경하지 않고 애플리케이션 필터를 애플리케이션 필터 개체로 변환합니다. 구성 변경으로 인해 디바이스의 구성 상태가 '동기화되지 않음'으로 변경되며 CDO에서 구성 구축이 필요합니다. 일반적으로 FDM은 필터를 수동으로 저장할 때까지 애플리케이션 필터를 애플리케이션 필터 개체로 변환하지 않습니다.

관련 정보:

- Firepower 애플리케이션 필터 개체 생성 및 편집
- 개체 삭제

Firepower 애플리케이션 필터 개체 생성 및 편집

애플리케이션 필터 개체를 사용하면 직접 선택한 애플리케이션 또는 필터로 식별된 애플리케이션 그룹을 대상으로 지정할 수 있습니다. 이 애플리케이션 필터 개체는 정책에서 사용할 수 있습니다.

Firepower 애플리케이션 필터 개체 생성

애플리케이션 필터 개체를 만들려면 다음 절차를 따르십시오.

Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 **Create Object(개체 생성) > FTD > Application Service(애플리케이션 서비스)**를 클릭합니다.

단계 3 개체의 개체 이름 및 설명(선택 사항)을 입력합니다.

단계 4 **Add Filter(필터 추가)**를 클릭하고 개체에 추가할 애플리케이션 및 필터를 선택합니다.

초기 목록(계속 스크롤 가능)에는 애플리케이션이 표시됩니다. 고급 필터를 클릭하면 필터 옵션을 확인하고 애플리케이션을 더 쉽게 선택할 수 있는 보기를 표시할 수 있습니다. 원하는 항목을 선택한 후 **Add(추가)**를 클릭합니다. 이 프로세스를 반복하여 애플리케이션이나 필터를 더 추가할 수 있습니다.

Note 단일 필터 기준으로 여러 선택 항목이 OR 관계를 갖습니다. 예를 들어 위험은 높음 OR 매우 높음입니다. 반면 필터 간의 관계는 AND입니다. 즉, 위험은 높음 OR 매우 높음 AND 사업 타당성은 낮음 OR 매우 낮음과 같습니다. 필터를 선택하면 디스플레이의 애플리케이션 목록이 업데이트되어 기준을 충족하는 애플리케이션만 표시됩니다. 이러한 필터를 사용하여 개별적으로 추가하려는 애플리케이션을 찾거나, 규칙에 추가할 적절한 필터를 선택하고 있는지를 확인할 수 있습니다.

Filter Applications

Risks: High, Very High

Categories: ad portal

Business Relevance: Very Low, Low

Tags: displays ads

Types: Web Application

Filter the list of applications

4 matches

Application Name	Description
MyWay	Adware and spyware, categorized as an internet browser hijacker.
Olx.pl	Platform to connect local people to buy, sell or exchange used goods and services through their mobile phone or on the web.
PopAds	Advertising network specialized in popunders on the Internet.
PopCash	Advertising platform.

Cancel OK

위험: 애플리케이션이 조직의 보안 정책에 위배되는 목적으로 사용될 가능성은 매우 낮음에서 매우 높음까지입니다.

비즈니스 관련성: 애플리케이션이 오락용이 아니라 조직의 비즈니스 운영 컨텍스트 내에서 사용될 가능성은 매우 낮음에서 매우 높음까지입니다.

유형: 애플리케이션 유형

- **애플리케이션 프로토콜:** 호스트 간의 통신을 나타내는 HTTP 및 SSH와 같은 애플리케이션 프로토콜.
- **클라이언트 프로토콜:** 호스트에서 실행 중인 소프트웨어를 나타내는 웹 브라우저 및 이메일 클라이언트와 같은 클라이언트.
- **웹 애플리케이션:** HTTP 트래픽에 대한 콘텐츠 또는 요청된 URL을 나타내는 MPEG 비디오 및 Facebook과 같은 웹 애플리케이션.

범주: 가장 필수적인 기능을 설명하는 애플리케이션의 일반적인 분류.

태그: 카테고리과 유사한 애플리케이션에 대한 추가 정보.

암호화된 트래픽의 경우, 시스템은 SSL Protocol(SSL 프로토콜) 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 암호화된 트래픽 또는 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에는 암호 해독된 트래픽 태그가 할당됩니다.

애플리케이션 목록(디스플레이 하단): 목록 위의 옵션에서 필터를 선택하면 이 목록이 업데이트되므로 현재 필터와 일치하는 애플리케이션을 볼 수 있습니다. 이 목록을 사용하여 규칙에 필터 기준을 추가하려는 경우 필터가 적절한 애플리케이션을 대상으로 하는지를 확인할 수 있습니다. 개체에 특정 애플리케이션을 추가하려면 필터링된 목록에서 선택합니다. 애플리케이션을 선택하면 필터가 더 이상 적용되지 않습니다. 필터 자체가 개체가 되도록 하려면 목록에서 애플리케이션을 선택하지 마십시오. 그런 다음 개체는 필터로 식별된 모든 애플리케이션을 나타냅니다.

단계 5 **OK**(확인)를 클릭하여 변경 사항을 저장합니다.


Firepower 애플리케이션 필터 개체 편집

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 3 편집할 개체를 선택합니다.

단계 4 세부정보 패널의 **Actions**(작업) 창에서 편집 아이콘  를 클릭합니다.

단계 5 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 6 **Save**(저장)를 클릭합니다.

단계 7 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

관련 정보:

- [개체](#)
- [개체 필터](#)
- [개체 삭제](#)

지리위치 개체

지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소만을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 지리적 위치를

사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

일반적으로는 지리위치 개체를 사용하지 않고 정책에서 직접 지리적 위치를 선택합니다. 그러나 국가와 대륙의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다.

지리위치 데이터베이스 업데이트

최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다. 현재는 Cisco Defense Orchestrator를 사용하여 수행할 수 있는 작업이 아닙니다. GeoDB 및 업데이트 방법에 대한 자세한 내용은 [디바이스가 실행 중인 버전의 Firepower Device Manager용 Cisco Firepower Threat Defense 설정 가이드](#)의 다음 섹션을 참조하십시오.

- 시스템 데이터베이스 및 피드 업데이트
- 시스템 데이터베이스 업데이트

Firepower 지리위치 필터 개체 생성 및 편집

개체 페이지에서 또는 보안 정책을 생성할 때 지리위치 개체를 생성할 수 있습니다. 이 절차에서는 개체 페이지에서 지리위치 개체를 생성합니다.

지리위치 개체를 생성하려면 다음 단계를 수행합니다.

Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > Geolocation(지리위치)**을 클릭합니다.
- 단계 3 개체의 개체 이름 및 설명(선택 사항)을 입력합니다.
- 단계 4 필터 표시줄에서 국가 또는 지역의 이름을 입력하기 시작하면 가능한 일치 목록이 표시됩니다.
- 단계 5 개체에 추가할 국가 또는 지역을 선택합니다.
- 단계 6 **Add(추가)**를 클릭합니다.

지리위치 개체 편집

Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 필터 창과 검색 필드를 사용하여 개체를 찾습니다.
- 단계 3 작업 창에서 **Edit(편집)**를 클릭합니다.
- 단계 4 개체의 이름을 변경하고 개체에 국가 및 지역을 추가하거나 제거할 수 있습니다.
- 단계 5 **Save(저장)**를 클릭합니다.

단계 6 장치가 영향을 받는 경우 알림을 받게 됩니다. **OK(확인)**를 클릭합니다.

단계 7 장치 또는 정책이 영향을 받은 경우 **Inventory(인벤토리)** 페이지를 열고 장치에 대한 변경 사항을 미리 보고 배포합니다.

DNS 그룹 개체

DNS(Domain Name System) 그룹은 DNS 서버 및 일부 관련 특성의 목록을 정의합니다. `www.example.com` 과 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인하려면 DNS 서버가 필요합니다. 관리 및 데이터 인터페이스에 대해 서로 다른 DNS 그룹 개체를 구성할 수 있습니다.

새 DNS 그룹 개체를 생성하기 전에 FDM 관리 디바이스에 DNS 서버가 구성되어 있어야 합니다. Cisco Defense Orchestrator(CDO)의 **Firepower Threat Defense 디바이스 설정**에 DNS 서버를 추가하거나 **firewall device manager**에서 DNS 서버를 생성한 다음 FDM 관리 구성을 CDO에 동기화할 수 있습니다. **firewall device manager**에서 DNS 서버 설정을 생성하거나 수정하려면 [Cisco Firepower Device Manager 구성 가이드](#), 버전 6.4 이상의 데이터 및 관리 인터페이스에 대한 **DNS** 구성을 참조하십시오.

DNS 그룹 개체 생성

CDO에서 새 DNS 그룹 개체를 생성하려면 다음 절차를 따르십시오.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **FTD > DNS Group(DNS 그룹)**을 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 (선택 사항) 설명을 추가합니다.

단계 6 **DNS** 서버의 IP 주소를 입력합니다. 최대 6개의 DNS 서버를 추가할 수 있습니다. **Add DNS Server(DNS 서버 추가)**를 클릭합니다. 서버 주소를 제거하려면 삭제 아이콘을 클릭합니다.

Note 목록은 우선순위에 따라 나열됩니다. 목록의 첫 번째 서버가 항상 사용되며, 그다음 서버는 위에 있는 서버에서 응답이 수신되지 않는 경우에만 사용됩니다. 최대 6개의 서버를 추가할 수 있지만 나열된 처음 3개의 서버만 관리 인터페이스에 사용됩니다.

단계 7 도메인 검색 이름을 입력합니다. 이 도메인은 정규화되지 않은 호스트 이름(예: `serverA.example.com` 이 아닌 `serverA`)에 추가됩니다.

단계 8 재시도 횟수를 입력합니다. 시스템이 응답을 받지 못한 경우 DNS 서버 목록을 재시도하는 횟수(0~10)입니다. 기본값은 2입니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.

단계 9 시간 초과 값을 입력합니다. 다음 DNS 서버를 시도하기 전에 기다리는 시간(1~30초)입니다. 기본값은 2초입니다. 시스템이 서버 목록을 재시도할 때마다 이 시간 초과 값이 두 배로 늘어납니다. 이 설정은 데이터 인터페이스에서 사용되는 DNS 그룹에만 적용됩니다.

단계 10 Add(추가)를 클릭합니다.


DNS 그룹 개체 편집

Cisco Defense Orchestrator 또는 firewall device manager에서 생성된 DNS 그룹 개체를 편집할 수 있습니다. 기존 DNS 그룹 개체를 편집하려면 다음 절차를 따르십시오.

Procedure

단계 1 왼쪽 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 **DNS Group Object(DNS 그룹 개체)**를 찾습니다.

단계 3 개체를 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 다음 항목을 편집합니다.

- 개체 이름
- 설명
- DNS 서버 이 목록에서 DNS 서버를 편집, 추가 또는 제거할 수 있습니다.
- 도메인 검색 이름
- 재시도.
- 시간이 초과되었습니다.

단계 5 Save(저장)를 클릭합니다.

단계 6 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.


DNS 그룹 개체 삭제

CDO에서 DNS 그룹 개체를 삭제하려면 다음 절차를 따르십시오.

Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 **DNS Group Object(DNS 그룹 개체)**를 찾습니다.

단계 3 개체를 선택하고 **Remove(제거)** 아이콘  를 클릭합니다.

단계 4 DNS 그룹 개체를 삭제할 것인지 확인하고 **Ok(확인)**를 클릭합니다.

단계 5 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

DNS 그룹 개체를 FDM-관리 DNS 서버로 추가

데이터 인터페이스 또는 관리 인터페이스에 대한 기본 설정 DNS 그룹으로 DNS 그룹 개체를 추가할 수 있습니다. 자세한 내용은 [FDM-Managed Device Settings\(FDM 매니지드 디바이스 설정\)](#)을 참조하십시오.

인증서 개체

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.

디바이스에서 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 [재사용 가능한 개체](#) 장의 인증서 정보 및 인증서 구성 섹션을 참조하십시오.

인증서 정보

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이클레먼트 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.

다음과 같은 인증서 유형을 생성할 수 있습니다.

- 내부 인증서 - 내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

시스템은 그대로 사용하거나 대체할 수 있는 사전 정의된 내부 인증서 **DefaultInternalCertificate** 및 **DefaultWebServerCertificate**와 함께 제공됩니다.

- 내부 CA(Certificate Authority) - 내부 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

시스템은 **NGFW-Default-InternalCA**와 같은 미리 정의된 내부 CA 인증서와 함께 제공되며, 이를 그대로 사용하거나 교체할 수 있습니다.

- 신뢰할 수 있는 **CA(Certificate Authority)** 인증서 - 신뢰할 수 있는 CA 인증서는 다른 인증서에 서명하는 데 사용됩니다. 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

CA(인증 증명)는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다. CA는 VeriSign과 같이 신뢰받는 서드파티이거나, 조직 내에서 설정한 전용 (내부) CA일 수 있습니다. CA는 인증서 요청을 관리하고 디지털 인증서를 발급하는 기능을 담당합니다.

시스템에는 서드파티 인증 증명에서 제공되는 수많은 신뢰할 수 있는 CA 인증서도 포함됩니다. 이러한 인증서는 Decrypt Re-Sign(암호 해독 재서명) 작업을 위한 SSL 암호 해독 정책에서 사용됩니다.

자세한 내용은 디바이스가 실행 중인 버전에 대한 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 재사용 가능한 개체 장의 기능에서 사용하는 인증서 유형 섹션을 참조하십시오.

기능에 사용되는 인증서 유형

각 기능에 대해 적절한 유형의 인증서를 생성해야 합니다. 인증서가 필요한 기능은 다음과 같습니다.

ID 정책(캡티브 포털) - 내부 인증서

(선택 사항). 캡티브 포털은 ID 정책에 사용됩니다. 사용자는 신원을 증명하고 IP 주소를 사용자 이름과 연결하기 위해 디바이스에 인증할 때 이 인증서를 수락해야 합니다. 인증서를 제공하지 않으면 디바이스는 자동으로 생성된 인증서를 사용합니다.

SSL 암호 해독 정책 — 내부, 내부 CA 및 신뢰할 수 있는 CA 인증서

(필수) SSL 암호 해독 정책은 다음 목적을 위해 인증서를 사용합니다.

- 내부 인증서는 알려진 키 암호 해독 규칙에 사용됩니다.
- 내부 CA 인증서는 클라이언트와 디바이스 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 사용됩니다.
- 신뢰할 수 있는 CA 인증서
 - 신뢰할 수 있는 CA 인증서는 디바이스와 서버 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 간접적으로 사용됩니다. 다른 인증서와 달리 이러한 인증서는 SSL 암호 해독 정책에서 직접 구성하지 않고 시스템에 업로드하기만 하면 됩니다. 시스템에는 신뢰할 수 있는 CA 인증서가 많이 포함되어 있으므로 추가 인증서를 업로드할 필요가 없을 수도 있습니다.
 - Active Directory 영역 개체를 생성하고 암호화를 사용하도록 디렉터리 서버를 구성할 때.

인증서 구성

ID 정책 또는 SSL 암호 해독 정책에 사용되는 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다. 필요한 경우 OpenSSL을 사용하여 인증서를 생성하거나 신뢰할 수 있는 인증 기관에서 가져오거나 자체 서명된 인증서를 생성할 수 있습니다.

다음 절차를 사용하여 인증서 개체를 구성합니다.

- 내부 및 내부 CA 인증서 업로드
- 신뢰할 수 있는 CA 인증서 업로드
- 자체 서명 내부 및 내부 CA 인증서 생성
- 인증서를 보거나 편집하려면 인증서의 편집 아이콘 또는 보기 아이콘을 클릭합니다.
- 참조되지 않는 인증서를 삭제하려면 해당 인증서의 삭제 아이콘을 클릭합니다. [개체 삭제](#)를 참조하십시오.

내부 및 내부 CA 인증서 업로드

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

내부 CA(Certificate Authority) 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 [기능에 사용되는 인증서 유형](#)을 참조하십시오.

절차

이 절차에서는 인증서 파일을 업로드하거나 기존 인증서 텍스트를 텍스트 상자에 붙여넣어 내부 또는 내부 CA 인증서를 생성합니다. 자체 서명된 인증서를 생성하려면 [자체 서명 내부 및 내부 CA 인증서 생성](#)을 참조하십시오.

내부 또는 내부 CA 인증서 개체를 만들거나 새 인증서 개체를 정책에 추가하려면 다음 절차를 따르십시오.

Procedure

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
 - a. 좌측의 CDO 탐색 모음에서 **Objects(개체)** > **FDM Objects(FDM 개체)**를 클릭합니다.

b. 플러스 버튼  를 클릭하고 **FTD > Certificate**(인증서)를 선택합니다.

- 정책에 새 인증서 개체를 추가할 때 **Create New Object**(새 개체 생성)를 클릭합니다.

단계 2 인증서의 **Name**(이름)을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 3 1단계에서 내부 인증서 또는 내부 **CA**를 선택합니다.

단계 4 2단계에서 **Upload**(업로드)를 선택하여 인증서 파일을 업로드합니다.

단계 5 3단계에서 서버 인증서 영역의 텍스트 상자에 인증서 내용을 붙여넣거나 마법사의 설명에 따라 인증서 파일을 업로드합니다. 텍스트 상자에 인증서를 붙여넣는 경우 인증서에 **BEGIN CERTIFICATE** 및 **END CERTIFICATE** 줄이 포함되어야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFAADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQv21kZ210
(...5 lines removed...)
shGJDRrYJQqilhHZrYTWZAYTrD7NQP HutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZ1zJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfwxUn
RV7LRfQGFYd76V/5uor4Wx2ZCjy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
v1k3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

단계 6 3단계의 인증서 키 영역에서 키 내용을 인증서 키 텍스트 상자에 붙여넣거나 마법사의 설명에 따라 키 파일을 업로드합니다. 텍스트 상자에 키를 붙여넣는 경우 키에는 **BEGIN PRIVATE KEY** 또는 **BEGIN RSA PRIVATE KEY** 및 **END PRIVATE KEY** 또는 **END PRIVATE KEY** 행이 포함되어야 합니다.

Note 키는 암호화할 수 없습니다.

단계 7 **Add**(추가)를 클릭합니다.

신뢰할 수 있는 CA 인증서 업로드

신뢰할 수 있는 CA(Certificate Authority) 인증서는 다른 인증서에 서명하는 데 사용되며, 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 [기능에 사용되는 인증서 유형](#)을 참조하십시오.

외부 인증 기관으로부터 신뢰할 수 있는 CA 인증을 획득하거나, OpenSSL 도구 등 자체 내부 CA를 사용하여 CA 인증을 생성합니다. 그런 다음, 아래 절차를 사용하여 인증서를 업로드합니다.

절차

Procedure

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
 - a. 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
 - b. 플러스 버튼  를 클릭하고 **FTD > Certificate(인증서)**를 선택합니다.
- 정책에 새 인증서 개체를 추가할 때 **Create New Object(새 개체 생성)**를 클릭합니다.

단계 2 인증서의 **Name(이름)**을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 3 1단계에서 **External CA Certificate(외부 CA 인증서)**를 선택하고 **Continue(계속)**를 클릭합니다. 마법사가 3단계로 진행합니다.

단계 4 3단계의 **Certificate Contents(인증서 내용)** 영역에서 텍스트 상자에 인증서 내용을 붙여넣거나 마법사의 설명에 따라 인증서 파일을 업로드합니다.

인증서는 다음 지침을 따라야 합니다.

- 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.
- 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.
- 붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBwUAMFcxCzAJBgNV
BAYTA1VTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAxh
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJlVUzELMAkGA1UECAwCVFgxZDZAN
BgNVBACMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
Mi4xNjguMS4xMlICIAjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GpkOQdrixn3FzeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgK1OwXbRvOdkstzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbsCF5rP71fObG9Iu6+u4EFHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

단계 5 **Add(추가)**를 클릭합니다.

자체 서명 내부 및 내부 CA 인증서 생성

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.

내부 CA(Certificate Authority) 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.

OpenSSL을 사용하여 이러한 인증서를 생성하거나, 신뢰할 수 있는 CA에서 인증서를 가져오고 업로드할 수 있습니다. 자세한 내용은 [내부 및 내부 CA 인증서 업로드](#)를 참조하십시오.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 [기능에 사용되는 인증서 유형](#)을 참조하십시오.



Note 새로운 자체 서명 인증서는 유효 기간이 5년으로 생성됩니다. 만료되기 전에 인증서를 교체하십시오.



Warning 자체 서명 인증서가 있는 디바이스를 업그레이드하면 문제가 발생할 수 있습니다. 자세한 내용은 [새 인증서 탐지](#)를 참조하십시오.


절차

이 절차는 마법사에서 적절한 인증서 필드 값을 입력하여 자체 서명된 인증서를 생성합니다. 인증서 파일을 업로드하여 내부 또는 내부 CA 인증서를 생성하려면 [내부 및 내부 CA 인증서 업로드](#)를 참조하십시오.

자체 서명된 인증서를 생성하려면 다음 절차를 따르십시오.

Procedure

단계 1 다음 중 하나를 수행합니다.

- 개체 페이지에서 인증서 개체를 생성합니다.
 - a. 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.
 - b. 플러스 버튼 를 클릭하고 **FTD > Certificate**(인증서)를 선택합니다.
- 정책에 새 인증서 개체를 추가할 때 **Create New Object**(새 개체 생성)를 클릭합니다.

단계 2 인증서의 **Name**(이름)을 입력합니다. 이름은 구성에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 3 1단계에서 내부 인증서 또는 내부 CA를 선택합니다.

단계 4 2단계에서 **Self-Signed**(자체 서명됨)을 선택하여 이 단계에서 자체 서명된 인증서를 생성합니다.

단계 5 인증서 주체와 발급자 정보에 다음 중 한 가지 이상의 정보를 구성합니다.

- 국가(C)- 드롭다운 목록에서 국가 코드를 선택합니다.
- State or Province(주/도)(ST) - 인증서에 포함할 주/도.
- Locality or City(구/군/시)(L) - 인증서에 포함할 구/군/시(예: 도시 이름).
- Organization(조직)(O) - 인증서에 포함할 조직 또는 회사 이름.
- Organizational Unit(Department)(조직 단위(부서))(OU) - 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- Common Name(공용 이름)(CN) - 인증서에 포함할 X.500 일반 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.

단계 6 **Add**(추가)를 클릭합니다.

IPsec 제안 구성

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.
- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.



Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

- [IKEv1 IPsec 제안 개체 관리](#)
- [IKEv2 IPsec 제안 개체 관리](#)

IKEv1 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 현재 CDO(Cisco Defense Orchestrator)는 IKEv1 IPsec 제안 개체를 지원합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.



Note IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

Related Topics

[IKEv1 IPsec 제안 개체 생성 또는 편집](#)

IKEv1 IPsec 제안 개체 생성 또는 편집


여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv1 Proposal**(새 IKEv1 제안 생성) 링크를 클릭하여 사이트 투 사이트 VPN 연결에서 IKEv1 IPsec 설정을 편집하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv1 IPsec Proposal**(제안)을 선택하여 새 개체를 생성합니다.
- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit**(편집)를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKEv1 IPsec 제안 개체가 작동하는 모드를 선택합니다.

- 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPsec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수 없는 네트워크

를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec이 구현되는 통상적인 방식입니다.

- 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPsec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

단계 5 이 제안에 대한 **ESP Encryption(ESP 암호화)(Encapsulating Security Protocol)** 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)를 참조하십시오.

단계 6 인증에 사용할 **ESP Hash(ESP 해시)** 또는 무결성 알고리즘을 선택합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#)를 참조하십시오.

단계 7 **Add(추가)**를 클릭합니다.

IKEv2 IPsec 제안 개체 관리

IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

Related Topics

[IKEv2 IPsec 제안 개체 생성 또는 편집](#)

IKEv2 IPsec 제안 개체 생성 또는 편집

여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 편집하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 편집할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal(새 IPsec 제안 생성)** 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 편집하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv2 IPsec Proposal(제안)**을 선택하여 새 개체를 생성합니다.

- 개체 페이지에서 편집할 IPsec 제안을 선택하고 오른쪽의 작업 창에서 **Edit(편집)**를 클릭합니다.

단계 3 새 개체의 개체 이름을 입력합니다.

단계 4 IKE2 IPsec 제안 개체 구성:

- **Encryption(암호화)** - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)를 참조하십시오.
- **Integrity Hash(무결성 해시)** - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 해시 알고리즘 결정](#)를 참조하십시오.

단계 5 **Add(추가)**를 클릭합니다.

글로벌 IKE 정책 구성

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 **Edit(수정)**을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

다음 항목에서는 각 버전에 대해 IKE 정책을 구성하는 방법에 대해 설명합니다.

- [IKEv1 정책 관리](#)
- [IKEv2 정책 관리](#)

IKEv1 정책 관리

IKEv1 정책을 생성하고 편집하는 방법을 설명합니다.

IKEv1 정책 정보

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 State(상태) 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

Related Topics

[IKEv1 정책 생성 또는 편집](#)


IKEv1 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy**(새 IKE 정책 생성) 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv1 정책을 생성할 수도 있습니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv1 Policy**(IKEv1 정책)를 선택하여 새 IKEv1 정책을 생성합니다.
- 개체 페이지에서 편집할 IKEv1 정책을 선택하고 오른쪽의 Actions(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 3 개체 이름을 최대 128자로 입력합니다.

단계 4 IKEv1 속성을 구성합니다.

- **Priority**(우선순위)-IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **Encryption**(암호화) - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정을 참조하십시오.

- **Diffie-Hellman Group(Diffie-Hellman 그룹)** - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정을 참조하십시오.
- **Lifetime(라이프타임)-SA(보안 연결)의 라이프타임(초)**으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.
- **Authentication(인증)** - 두 피어 간에 사용할 인증 방법입니다. 자세한 내용은 [사용할 인증 방법 결정](#)을 참조하십시오.
 - **Preshared Key(사전 공유 키)** - 각 디바이스에 정의된 사전 공유 키를 사용합니다. 이 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
 - **Certificate(인증서)** - 서로 식별할 피어에 대해 디바이스 ID 인증서를 사용합니다. Certificate Authority에서 각 피어를 등록하여 이 인증서를 가져와야 합니다. 또한 각 피어에서 ID 인증서 서명에 사용되는 신뢰할 수 있는 CA 루트 및 중간 CA 인증서를 업로드해야 합니다. 피어는 동일한 또는 다른 CA에 등록할 수 있습니다. 어느 피어든 간에 SSC(자가서명 인증서)를 사용할 수 없습니다.
- **Hash(해시)** - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘](#)을 참조하십시오.

단계 5 **Add(추가)**를 클릭합니다.

IKEv2 정책 관리

IKEv2 정책을 생성하고 편집하는 방법을 설명합니다.

IKEv2 정책 정보

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 **State(상태)** 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

Related Topics

[IKEv2 정책 생성 또는 편집](#)


IKEv2 정책 생성 또는 편집

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKEv2 Policy**(새 IKEv2 정책 생성) 링크를 클릭하여 사이트 간 VPN 연결에서 IKE 설정을 편집하면서 IKEv2 정책을 생성할 수도 있습니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 다음 중 하나를 수행합니다.

- 파란색 플러스 버튼  을 클릭하고 **FTD > IKEv2 Policy**(FTD IKEv2 정책)를 선택하여 새 IKEv2 정책을 생성합니다.
- 개체 페이지에서 수정할 IKEv2 정책을 선택하고 오른쪽의 **Actions**(작업) 창에서 **Edit**(편집)를 클릭합니다.

단계 3 개체 이름을 최대 128자로 입력합니다.

단계 4 IKEv2 속성을 구성합니다.

- **Priority**(우선순위)-IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에서 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- **State**(상태) - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- **Encryption**(암호화) - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는 반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 암호화 알고리즘 결정](#)를 참조하십시오.
- **Diffie-Hellman Group**(Diffie-Hellman 그룹) - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [사용할 Diffie-Hellman 모듈러스 그룹 결정](#)를 참조하십시오.
- **Integrity Hash**(무결성 해시) - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시

시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘](#)을 참조하십시오.

- **PRF(Pseudo-Random Function)** 해시 - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해서로 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 [VPN에서 사용되는 암호화 및 해시 알고리즘](#)을 참조하십시오.
- **Lifetime(라이프타임)-SA(보안 연결)**의 라이프타임(초)으로, 120~2147483647의 값이거나 비어 있습니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연결을 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다. 무제한 라이프타임을 지정하려면 아무 값도 입력하지 않고 필드를 비워 둡니다.

단계 5 Add(추가)를 클릭합니다.

RA VPN 개체

보안 영역 개체

보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 여러 영역을 정의할 수 있지만, 지정된 인터페이스는 하나의 영역에만 속할 수 있습니다.

Firepower System은 초기 구성 중에 다음 영역을 생성하며 Defense Orchestrator의 개체 페이지에 표시됩니다. 영역을 편집하여 인터페이스를 추가하거나 제거할 수도 있고, 더 이상 사용하지 않는 영역을 삭제할 수도 있습니다.

- **inside_zone** - 내부 인터페이스를 포함합니다. 이 영역은 내부 네트워크를 나타내는 데 사용됩니다.
- **outside_zone** - 외부 인터페이스를 포함합니다. 이 영역은 인터넷 등 제어 범위 외부에 있는 네트워크를 나타내는 데 사용됩니다.

일반적으로는 인터페이스가 네트워크에서 수행하는 역할별로 인터페이스를 그룹화합니다. 예를 들어 인터넷에 연결하는 인터페이스는 **outside_zone** 보안 영역에 배치하고 내부 네트워크용의 모든 인터페이스는 **inside_zone** 보안 영역에 배치합니다. 그러면 외부 영역에서 들어오는 트래픽과 내부 영역으로 이동하는 트래픽에 액세스 제어 규칙을 적용할 수 있습니다.

영역을 생성하기 전에 네트워크에 적용할 액세스 규칙 및 기타 정책을 고려하십시오. 예를 들어 모든 내부 인터페이스를 같은 영역에 배치할 필요는 없습니다. 내부 네트워크가 4개인데 그중 하나를 나머지 3개와 다른 방식으로 취급하려는 경우에는 영역을 하나가 아닌 두 개 생성할 수 있습니다. 공개 웹 서버에 대한 외부 액세스를 허용해야 하는 인터페이스가 있는 경우에는 해당 인터페이스용으로 별도의 영역을 사용할 수 있습니다.

관련 정보:

- [Firepower 보안 영역 개체 생성 또는 편집](#)
- [보안 영역에 Firepower 인터페이스 할당](#)
- [개체 삭제](#)

Firepower 보안 영역 개체 생성 또는 편집


보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 여러 영역을 정의할 수 있지만, 지정된 인터페이스는 하나의 영역에만 속할 수 있습니다. 자세한 내용은 [보안 영역 개체](#)를 참조하십시오.

보안 영역 개체는 해당 디바이스에 대한 규칙에서 사용되지 않는 한 디바이스와 연결되지 않습니다.

보안 영역 개체 생성

보안 영역 개체를 생성하려면 다음 지침을 따르십시오.

Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 파란색 플러스 버튼  을 클릭하고 **FTD > Security Zone(보안 영역)**을 선택하여 새 개체를 생성합니다.
- 단계 3 개체의 이름과 설명(선택 사항)을 입력합니다.
- 단계 4 보안 영역에 넣을 인터페이스를 선택합니다.
- 단계 5 **Add(추가)**를 클릭합니다.



보안 영역 개체 편집

FDM 관리 디바이스를 온보딩한 후 이미 두 개 이상의 보안 영역이 있음을 알 수 있습니다. 하나는 `inside_zone`이고 다른 하나는 `outside_zone`입니다. 이러한 영역은 편집하거나 삭제할 수 있습니다. 보안 영역 개체를 편집하려면 다음 지침을 따르십시오.

Procedure


단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 편집할 개체를 찾습니다.

- 개체의 이름을 알고 있는 경우 개체 페이지에서 검색할 수 있습니다.
 - 보안 영역별로 목록을 필터링합니다.
 - 검색 필드에 개체 이름을 입력합니다.
 - 개체를 선택합니다.
- 개체가 디바이스와 연결되어 있는 경우 **Inventory(인벤토리)** 페이지에서 시작하여 개체를 검색할 수 있습니다.
 - 탐색창에서 **Inventory(재고 목록)**를 클릭합니다.
 - **Devices(디바이스)** 탭을 클릭합니다.
 - 해당 탭을 클릭합니다.
 - 디바이스 **필터** 및 **검색** 표시줄을 사용하여 디바이스를 찾습니다.
 - 디바이스를 선택합니다.
- 오른쪽의 관리 창에서  **Objects(개체)**를 클릭합니다.
- 개체 필터  과 검색 표시줄을 사용하여 찾고 있는 개체를 찾습니다.

Note 생성한 보안 영역 개체가 디바이스에 대한 정책의 규칙과 연결되지 않은 경우 "연결되지 않은" 것으로 간주되어 디바이스 검색 결과에 표시되지 않습니다.

단계 3 개체를 선택합니다.

단계 4 우측의 작업 창에서 **Edit(편집)** 아이콘  를 클릭합니다.

단계 5 개체의 속성을 편집한 후, **Save(저장)**를 클릭합니다.

단계 6 저장을 클릭하면 이러한 변경 사항이 다른 디바이스에 어떤 영향을 미치는지 설명하는 메시지가 표시됩니다. **Confirm(확인)**을 클릭하여 변경 사항을 저장하거나 취소합니다.

서비스 개체

Firepower 서비스 개체

FTD 서비스 개체, 서비스 그룹 및 포트 그룹은 IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다.

FTD 서비스 그룹은 서비스 개체의 모음입니다. 서비스 그룹은 하나 이상의 프로토콜에 대한 개체를 포함할 수 있습니다. 이러한 개체 및 그룹을 보안 정책에서 사용하여 네트워크 트래픽 일치 기준(예: 특정 TCP 포트에 대한 트래픽을 허용하는 액세스 규칙을 사용하기 위한 기준)을 정의할 수 있습니다. 시스템에는 일반 서비스를 위해 사전 정의된 개체가 여러 개 포함되어 있으며, 정책에서 이러한 개체를 사용할 수 있지만 시스템 정의 개체를 편집하거나 삭제할 수는 없습니다.

Firepower Device Manager 및 Firepower Management Center는 서비스 개체를 포트 개체 및 서비스 그룹 및 포트 그룹으로 참조하십시오.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.

프로토콜 개체

프로토콜 개체는 덜 일반적으로 사용되는 또는 레거시 프로토콜을 포함하는 서비스 개체 유형입니다. 프로토콜 개체는 이름 및 [프로토콜 번호](#)로 식별됩니다. CDO는 ASA 및 Firepower(FDM 관리) 구성에서 이러한 개체를 인식하고 사용자가 쉽게 찾을 수 있도록 자체 필터인 "프로토콜"을 제공합니다.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.

ICMP 개체

ICMP(Internet Control Message Protocol) 개체는 ICMP 및 IPv6-ICMP 메시지를 위한 서비스 개체입니다. CDO는 ASA 및 Firepower 구성에서 해당 디바이스가 온보딩되고 사용자가 개체를 쉽게 찾을 수 있도록 해당 디바이스에 "ICMP" 필터를 제공할 때 이러한 개체를 인식합니다.

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.

자세한 내용은 [Firepower 서비스 개체 생성 및 편집](#)을 참조하십시오.

관련 정보:

- [개체 삭제](#), on page 129


Firepower 서비스 개체 생성 및 편집

Firepower 서비스 개체를 생성하려면 다음 단계를 수행합니다.

firewall device manager(FDM 관리) 서비스 개체는 TCP/IP 프로토콜 및 포트를 지정하는 재사용 가능한 구성 요소입니다. firewall device manager. 온프레미스 Firewall Management Center 및 클라우드 사 용 Firewall Management Center는 이러한 개체를 "포트 개체"라고 합니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 오른쪽에 있는 파란색 버튼  을 클릭하여 개체를 생성하고 **FTD > Service(FTD 서비스)**를 선택합니다.

단계 3 개체 이름과 설명을 입력합니다.

단계 4 **Create a service object(서비스 개체 생성)**를 선택합니다.

단계 5 **Service Type(서비스 유형) 버튼**을 클릭하고 개체를 생성할 프로토콜을 선택합니다.

단계 6 다음과 같이 프로토콜을 구성합니다.

- **TCP, UDP**

- **eq**를 선택하고 포트 번호 또는 프로토콜 이름을 입력합니다. 예를 들어 포트 번호로 80을 입력하거나 프로토콜 이름으로 HTTP를 입력할 수 있습니다.

- 범위를 선택한 다음 포트 번호의 범위를 입력할 수도 있습니다(예: **1 65535(모든 포트 포함)**).

- **ICMP, IPv6-ICMP-ICMP** 유형을 선택합니다. 해당 유형을 모든 ICMP 메시지에 적용하려면 모두를 선택합니다. 유형과 코드에 대한 자세한 내용은 다음 페이지를 참조하십시오.

- ICMP-<http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>

- ICMPv6-<http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml>

- 기타 - 원하는 프로토콜을 선택합니다.

단계 7 **Add(추가)**를 클릭합니다.


단계 8 지금 변경한 내용을 **검토 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Firepower 서비스 그룹 생성

서비스 그룹은 하나 이상의 프로토콜을 나타내는 하나 이상의 서비스 개체로 구성될 수 있습니다. 서비스 개체를 그룹에 추가하려면 먼저 서비스 개체를 생성해야 합니다. Firepower Device Manager 및 Firepower Management Center에서는 이러한 개체를 "포트 개체"라고 합니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 오른쪽에 있는 파란색 버튼  을 클릭하여 개체를 생성하고 **FTD > Service(서비스)**를 선택합니다.

단계 3 개체 이름과 설명을 입력합니다.

단계 4 **Create a service group(서비스 그룹 생성)**를 선택합니다.

단계 5 **Add Object(개체 추가)**를 클릭하여 그룹에 개체를 추가합니다.

- 위의 **Firepower 서비스 개체 생성 및 편집**에서 수행한 것처럼 **Create(생성)**를 클릭하여 새 개체를 생성합니다.
- 기존 서비스 개체를 그룹에 추가하려면 **Choose(선택)**를 클릭합니다. 개체를 더 추가하려면 이 단계를 반복합니다.

단계 6 서비스 그룹에 서비스 개체 추가를 완료하면 **Add(추가)**를 클릭합니다.


단계 7 지금 변경한 내용을 **검토 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Firepower 서비스 개체 또는 서비스 그룹 편집

Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 3 작업 창에서 **Edit(편집)**  를 클릭합니다.

단계 4 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 5 **Save(저장)**를 클릭합니다.

단계 6 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm(확인)**을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

단계 7 지금 변경한 내용을 **검토 및 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

보안 그룹 태그 그룹

보안 그룹 태그(Security Group Tags)

보안 그룹 태그 정보

Cisco ISE(Identity Services Engine)를 사용하여 Cisco TrustSec 네트워크에서 트래픽을 분류하기 위해 SGT(Security Group Tag)를 정의하고 사용하는 경우, SGT를 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다. 따라서 IP 주소가 아니라 보안 그룹 멤버십을 기준으로 액세스를 차단하거나 허용할 수 있습니다.

ISE에서는 SGT를 생성하고 호스트 또는 네트워크 IP 주소를 각 태그에 할당할 수 있습니다. SGT를 사용자의 계정에 할당하면 SGT가 사용자의 트래픽에 할당됩니다. ISE 서버에 연결하도록 FDM 관리 디바이스를 구성하고 SGT를 생성한 후 Cisco Defense Orchestrator에서 SGT 그룹을 생성하고 이를 중심으로 액세스 제어 규칙을 작성할 수 있습니다. SGT를 FDM 관리 디바이스에 연결하려면 먼저 ISE의 SXP(SGT Exchange Protocol) 매핑을 구성해야 합니다. 자세한 내용은 현재 실행 중인 버전의 [Cisco ISE\(Identity Services Engine\) 관리자 설명서](#)에서 보안 그룹 태그 교환 프로토콜을 참조하십시오.

FDM 관리 디바이스가 SGT를 액세스 제어 규칙에 대한 트래픽 일치 기준으로 평가하는 경우, 다음 우선순위를 사용합니다.

1. 패킷에 정의된 소스 SGT(있는 경우). 대상 일치는 이 기술을 사용하여 수행되지 않습니다. SGT를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메서드를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.
2. ISE 세션 디렉토리에서 다운로드된 대로 사용자 세션에 할당된 SGT. 이러한 유형의 SGT 일치에 대한 세션 디렉토리 정보를 수신 대기하려면 해당 옵션을 활성화해야 합니다. 그러나 이 옵션은 처음에 ISE ID 소스를 생성할 때 기본적으로 켜집니다. SGT는 소스 또는 대상과 일치할 수 있습니다. 필수 사항은 아니지만 일반적으로 사용자 ID 정보를 수집하기 위해 AD 영역과 함께 ISE ID 소스를 사용하여 패시브 인증 ID 규칙도 설정합니다.
3. SXP를 사용하여 다운로드한 SGT-IP 주소 매핑. IP 주소가 SGT 범위 내에 있는 경우 트래픽은 SGT를 사용하는 액세스 제어 규칙과 일치합니다. SGT는 소스 또는 대상과 일치할 수 있습니다.



Note ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다. SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

버전 지원

CDO는 현재 버전 6.5 이상을 FDM 관리실행하는 FDM 매니지드 디바이스에서 SGT 및 SGT 그룹을 지원합니다. FDM 관리 디바이스를 사용하면 버전 6.5 이상에서 ISE 서버를 구성하고 연결할 수 있지만 버전 6.7까지는 UI에서 SGT 구성이 지원되지 않습니다.

FDM 관리 UI에서 이는 버전 6.5 이상을 실행하는 FDM 관리 디바이스가 SGT의 SXP 매핑을 다운로드할 수 있지만, 개체 또는 액세스 제어 규칙에 수동으로 추가할 수 없음을 의미합니다. 버전 6.5 또는 버전 6.6을 실행하는 디바이스의 SGT를 변경하려면 ISE UI를 사용해야 합니다. 그러나 버전 6.5를 실행하는 디바이스가 Cisco Defense Orchestrator에 온보딩된 경우 디바이스와 연결된 현재 SGT를 확인하고 SGT 그룹을 생성할 수 있습니다.

CDO의 SGT

보안 그룹 태그(Security Group Tags)

SGT는 CDO에서 읽기 전용입니다. CDO에서 SGT를 생성하거나 편집할 수 없습니다. SGT를 생성하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 관리자 설명서](#)를 참조하십시오.

SGT 그룹



Note FDM 관리 디바이스는 SGT 그룹을 SGT 동적 개체로 지칭합니다. CDO에서는 이러한 태그 목록을 현재 SGT 그룹이라고 합니다. FDM 관리 디바이스 또는 ISE UI를 참조하지 않고 CDO에서 SGT 그룹을 생성할 수 있습니다.

SGT 그룹을 사용하여 ISE가 할당한 SGT를 기준으로 소스 또는 대상 주소를 식별합니다. 그 다음 트래픽 일치 기준을 정의하는 목적으로 액세스 제어 규칙의 개체를 사용할 수 있습니다. ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다.

SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

CDO에서 SGT 그룹을 생성하려면 하나 이상의 SGT가 이미 구성되어 있어야 하며, 사용하려는 디바이스의 FDM 관리 콘솔에 대해 ISE 서버에서 SGT 매핑이 구성되어 있어야 합니다. 둘 이상의 FDM 관리 디바이스가 동일한 ISE 서버와 연결된 경우 SGT 또는 SGT 그룹을 둘 이상의 디바이스에 적용할 수 있습니다. 디바이스가 ISE 서버와 연결되지 않은 경우, SGT 개체를 액세스 제어 규칙에 포함하거나 SGT 그룹을 해당 디바이스 설정에 적용할 수 없습니다.

규칙의 SGT 그룹

SGT 그룹을 액세스 제어 규칙에 추가할 수 있습니다. 이는 소스 또는 대상 네트워크 개체로 나타납니다. 네트워크가 규칙에서 작동하는 방식에 대한 자세한 내용은 [FDM 액세스 제어 규칙의 소스 및 대상 기준](#)을 참조하십시오.

Objects(개체) 페이지에서 SGT 그룹을 생성할 수 있습니다. 자세한 내용은 [SGT 그룹 생성, on page 167](#)를 참조하십시오.

SGT 그룹 생성

액세스 제어 규칙에 사용할 수 있는 SGT 그룹을 생성하려면 다음 절차를 사용합니다.

Before you begin

SGT(보안 그룹 태그) 그룹을 생성하기 전에 다음 구성 또는 환경을 구성해야 합니다.

- FDM 관리 디바이스는 버전 6.5 이상을 실행해야 합니다.
- SXP 매핑을 구독하고 변경 사항을 구축하도록 ISE ID 소스를 구성해야 합니다. SXP 매핑을 관리하려면 사용 중인 버전 6.7 이상에 대한 [Firepower Device Manager 구성 가이드](#)의 **ISE**에서 보안 그룹 및 **SXP** 게시 구성을 참조하십시오.
- 모든 SGT는 ISE에서 생성해야 합니다. SGT를 생성하려면 현재 실행 중인 버전의 [Cisco ISE\(Identity Services Engine\) 구성 설명서](#)를 참조하십시오.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.

단계 2 파란색 더하기 버튼  을 클릭하여 개체를 생성합니다.

단계 3 **FTD > Network(네트워크)**를 클릭합니다.

단계 4 개체 이름을 입력합니다.

단계 5 (선택 사항) 설명을 추가합니다.

단계 6 **SGT**를 클릭하고 드롭다운 메뉴를 사용하여 그룹에 포함할 모든 해당 SGT를 선택합니다. SGT 이름을 기준으로 목록을 정렬할 수 있습니다.

단계 7 **Save(저장)**를 클릭합니다.

Note CDO에서 SGT를 생성하거나 편집할 수 없으며 SGT 그룹에서 추가하거나 제거할 수만 있습니다. SGT를 생성하거나 편집하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 구성 설명서](#)를 참조하십시오.


SGT 그룹 편집

SGT 그룹을 편집하려면 다음 절차를 따르십시오.

Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.

단계 2 개체 필터 및 검색 필드를 사용하여 편집하려는 SGT 그룹을 찾습니다.

단계 3 SGT 그룹을 선택하고 **Actions(작업)** 창에서 편집 아이콘  를 클릭합니다.

단계 4 SGT 그룹을 편집합니다. 그룹과 관련된 이름, 설명 또는 SGT를 편집합니다.


단계 5 **Save(저장)**를 클릭합니다.

Note CDO에서 SGT를 생성하거나 편집할 수 없으며 SGT 그룹에서 추가하거나 제거할 수만 있습니다. SGT를 생성하거나 편집하려면 현재 실행 중인 버전의 [Cisco Identity Services Engine 구성 설명서](#)를 참조하십시오.

액세스 제어 규칙에 SGT 그룹 추가

액세스 제어 규칙에 SGT 그룹을 추가하려면 다음 절차를 따르십시오.

Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾거나 **Templates**(템플릿) 탭을 클릭하여 모델 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 SGT 그룹을 추가할 디바이스를 선택합니다.
- 단계 4 **Management**(관리) 창에서 **Policy**(정책)를 선택합니다.
- 단계 5 소스 또는 대상 개체에 대한 파란색 플러스 버튼  을 클릭하고 **SGT** 그룹을 선택합니다.
- 단계 6 개체 필터 및 검색 필드를 사용하여 편집하려는 SGT 그룹을 찾습니다.
- 단계 7 **Save**(저장)를 클릭합니다.
- 단계 8 [모든 디바이스에 대한 구성 변경 사항 미리보기 및 배포](#).

Note 추가 SGT 그룹을 생성해야 하는 경우 **Create New Object**(새 개체 생성)를 클릭합니다. [SGT 그룹 생성](#) 및 규칙에 SGT 그룹 추가에 언급된 필수 정보를 입력하고 SGT 그룹을 규칙에 추가합니다.

시스템 로그 서버 개체


FDM 관리 디바이스는 이벤트를 저장할 수 있는 용량이 제한되어 있습니다. 이벤트에 대한 스토리지를 최대화하기 위해 외부 서버를 구성할 수 있습니다. 시스템 로그(syslog) 서버 개체는 연결 지향형 또는 진단 시스템 로그 메시지를 수신할 수 있는 서버를 식별합니다. 로그 수집 및 분석을 위해 syslog 서버를 설정한 경우, Cisco Defense Orchestrator를 사용하여 개체를 생성하여 정의한 후 관련 정책에 이 개체를 사용할 수 있습니다.

시스템 로그 서버 개체 생성 및 편집

새 시스템 로그 서버 개체를 생성하려면 다음 단계를 수행합니다.

Procedure

단계 1 좌측의 CDO 내비게이션 바에서, **Objects**(개체) > **FDM Objects**(FDM 개체)을 클릭합니다.

단계 2 **Create Object**(개체 생성) 버튼  을 클릭합니다.

단계 3 FDM 관리 디바이스 개체 유형에서 **Syslog Server**(시스템 로그 서버)를 선택합니다.

단계 4 시스템 로그 서버 개체 속성을 구성합니다.

- **IP 주소** - syslog 서버의 IP 주소를 입력합니다.
- **Protocol Type**(프로토콜 유형) — 시스템 로그 서버가 메시지를 수신하는 데 사용하는 프로토콜을 선택합니다. TCP를 선택하는 경우 시스템은 syslog 서버를 사용할 수 없는 경우를 인식할 수 있으며, 서버를 다시 사용할 수 있을 때까지 이벤트 전송을 중지합니다.
- **Port Number**(포트 번호) — 시스템 로그에 사용할 유효한 포트 번호를 입력합니다. 시스템 로그 서버가 기본 포트를 사용하는 경우 기본 UDP 포트로 514를 입력하거나 기본 TCP 포트로 1470을 입력합니다. 서버에서 기본 포트를 사용하지 않는 경우 올바른 포트 번호를 입력합니다. 포트가 1025~65535 범위에 포함되어야 합니다.
- **Select an interface**(인터페이스 선택) - 진단 시스템 로그 메시지를 보내는 데 사용해야 하는 인터페이스를 선택합니다. 연결 및 침입 이벤트는 항상 관리 인터페이스를 사용합니다. 선택하는 인터페이스에 따라 syslog 메시지와 연결되는 IP 주소가 결정됩니다. 아래에 나열된 옵션 중 하나만 선택할 수 있습니다. 둘 다 선택할 수는 없습니다. 다음 옵션 중 하나를 선택합니다.
 - **Data Interface**(데이터 인터페이스) - 진단 syslog 메시지에 대해 선택하는 데이터 인터페이스를 사용합니다. 생성된 목록에서 인터페이스를 선택합니다. 브리지 그룹 멤버 인터페이스를 통해 서버에 액세스할 수 있는 경우에는 BVI(브리지 그룹 인터페이스)를 선택합니다. 진단 인터페이스(물리적 관리 인터페이스)를 통해 서버에 액세스할 수 있는 경우에는 이 옵션 대신 **Management Interface**(관리 인터페이스)를 선택하는 것이 좋습니다. 패시브 인터페이스는 선택할 수 없습니다. 연결 및 침입 시스템 로그 메시지의 경우 소스 IP 주소는 관리 인터페이스용이거나, 데이터 인터페이스를 통해 라우팅하는 경우 게이트웨이 인터페이스용입니다.
 - **Management Interface**(관리 인터페이스) - 모든 유형의 syslog 메시지에 대해 가상 관리 인터페이스를 사용합니다. 소스 IP 주소는 관리 인터페이스용이거나, 데이터 인터페이스를 통해 라우팅하는 경우 게이트웨이 인터페이스용입니다.

단계 5 **Add**(추가)를 클릭합니다.

단계 6 지금 변경 사항을 **검토하고 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

Syslog 서버 개체 편집

기존 Syslog 서버 개체를 편집하려면 다음 단계를 따르십시오.

Procedure

- 단계 1 좌측의 CDO 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 원하는 Syslog 서버 개체를 찾아 선택합니다. Syslog 서버 개체 유형별로 개체 목록을 필터링 할 수 있습니다.
- 단계 3 작업 창에서 **Edit(편집)**를 클릭합니다.
- 단계 4 원하는 대로 편집하고 **Save(저장)**를 클릭합니다.
- 단계 5 변경 사항을 확인합니다.
- 단계 6 지금 변경 사항을 **검토하고 구축**하거나 기다렸다가 여러 변경 사항을 한 번에 배포합니다.

관련 정보:

- [개체 삭제](#)

SaaS(Secure Logging Analytics)를 위한 시스템 로그 서버 개체 생성


이벤트를 전송할 SEC(Secure Event Connector)의 IP 주소, TCP 포트 또는 UDP 포트를 사용하여 시스템 로그 서버 개체를 생성합니다. 테넌트에 온보딩한 모든 SEC에 대해 하나의 시스템 로그 개체를 생성하지만, 하나의 규칙에서 하나의 SEC를 나타내는 하나의 시스템 로그 개체로만 이벤트를 전송합니다.

사전 요구 사항

이 작업은 더 큰 워크플로우의 일부입니다. 시작하기 전에 [FDM-관리 디바이스에 대한 SaaS\(Secure Logging Analytics\) 구현](#)을 참조하십시오.

절차

Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 **Create Object(개체 생성)** 버튼  을 클릭합니다.
- 단계 3 FDM 관리 장치 개체 유형에서 **Syslog Server(Syslog 서버)**를 선택합니다.
- 단계 4 시스템 로그 서버 개체 속성을 구성합니다. SEC의 이러한 속성을 찾으려면 **Admin(관리) > Secure Connector(보안 커넥터)**를 선택합니다. 그런 다음 syslog 개체를 구성할 보안 이벤트 커넥터를 선택하고 오른쪽의 세부 정보 창을 살펴봅니다.
 - IP 주소 - SEC의 IP 주소를 입력합니다.
 - 프로토콜 유형 - TCP 또는 UDP를 선택합니다.
 - 포트 번호 - TCP를 선택한 경우 포트 10125를 입력하고 UDP를 선택한 경우 10025를 입력합니다.

- 인터페이스 선택 - SEC에 도달하도록 구성된 인터페이스를 선택합니다.

Note FDM 관리 장치는 IP 주소당 하나의 syslog 개체를 지원하므로 TCP와 UDP 사용 중에서 선택해야 합니다.

단계 5 **Add(추가)**를 클릭합니다.

What to do next

기존 CDO 고객 워크플로우의 단계 3을 계속하여 SaaS(Secure Logging Analytics)를 구현하고 보안 이벤트 커넥터를 통해 이벤트를 Cisco 클라우드로 보냅니다.

URL 개체

URL 개체 및 URL 그룹은 Firepower 디바이스에서 사용됩니다. 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. URL 개체는 단일 URL 또는 IP 주소를 정의하는 반면 URL 그룹은 여러 URL 또는 IP 주소를 정의할 수 있습니다.

시작하기 전에

URL 개체를 생성할 때는 다음 사항에 유의하십시오.

- 경로를 포함하지 않는 경우(즉, URL에 / 문자가 없음), 이 일치하는 서버의 호스트 이름만을 기준으로 합니다. 호스트 이름은 // 구분자 뒷부분 또는 호스트 이름의 의 뒷부분이 같아야 일치하는 것으로 간주됩니다. 예를 들어 ign.com은 ign.com 및 www.ign.com과 일치하지만 verisign.com과는 일치하지 않습니다.
- 하나 이상의 / 문자를 포함하는 경우, 전체 URL 문자열이 서버 이름, 경로 및 쿼리 파라미터를 비롯한 부분 문자열 일치에 사용됩니다. 그러나 서버가 재구성되고 페이지가 새 경로로 이동될 수 있으므로 개별 웹 페이지 또는 사이트 일부를 차단하거나 허용하기 위해 수동 URL 필터링은 사용하지 않는 것이 좋습니다. 부분 문자열 일치하는 예기치 않은 일치로 이어질 수도 있으며, 이 경우에는 URL 개체에 포함하는 문자열도 쿼리 파라미터 내부에 있는 의도하지 않은 서버 또는 문자열의 경로와 일치됩니다.
- 시스템에서는 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹 사이트를 차단하는 경우 애플리케이션 조건을 사용하여 특정 프로토콜을 대상으로 하지 않는 한 해당 웹사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 예를 들어 <http://example.com> 대신 example.com을 사용합니다.
- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

그러나 인증서의 주체 일반 이름은 웹 사이트의 도메인 이름과 아무런 관련도 없을 수 있습니다. 예를 들어, youtube.com 인증서의 주체 일반 이름은 *.google.com입니다(언제든 변경 가능). URL 필터링 규칙이 암호 해독된 트래픽에서 작동하도록 SSL 암호 해독 정책을 사용하여 HTTPS 트래픽을 암호 해독하면 더 일관성 있는 결과를 얻게 됩니다.



참고 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

FDM-관리 URL 개체 생성 또는 편집

URL 개체는 URL 또는 IP 주소를 지정하는 재사용 가능한 구성 요소입니다.

URL 개체를 만들려면 다음 단계를 수행합니다.

Procedure

- 단계 1 왼쪽 Cisco Defense Orchestrator 탐색 모음에서 **Objects(개체) > FDM Objects(FDM 개체)**를 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > URL**을 클릭합니다.
- 단계 3 개체 이름과 설명을 입력합니다.
- 단계 4 **Create URL object(URL 개체 생성)**를 선택합니다.
- 단계 5 개체의 특정 URL 또는 IP 주소를 입력합니다.
- 단계 6 **Add(추가)**를 클릭합니다.

Firepower URL 그룹 생성

URL 그룹은 하나 이상의 URL 또는 IP 주소를 나타내는 하나 이상의 URL 개체로 구성될 수 있습니다. Firepower Device Manager 및 Firepower Management Center는 이러한 개체를 "URL 개체"라고도 합니다.

Procedure

- 단계 1 좌측의 CDO 내비게이션 바에서, **Objects(개체) > FDM Objects(FDM 개체)**을 클릭합니다.
- 단계 2 **Create Object(개체 생성) > FTD > URL**을 클릭합니다.
- 단계 3 개체 이름과 설명을 입력합니다.
- 단계 4 **Create a URL group(URL 그룹 생성)**을 선택합니다.

단계 5 **Add Object**(개체 추가)를 클릭하고, 개체를 선택하고, **Select**(선택)을 클릭하여 기존 개체를 추가합니다. 개체를 더 추가하려면 이 단계를 반복합니다.

단계 6 URL 그룹에 URL 개체 추가를 완료하면 **Add**(추가)를 클릭합니다.

Firepower URL 개체 또는 URL 그룹 편집

Procedure

단계 1 좌측의 CDO 탐색 모음에서 **Objects**(개체) > **FDM Objects**(FDM 개체)를 클릭합니다.

단계 2 개체를 필터링하여 편집할 개체를 찾은 다음 개체 테이블에서 개체를 선택합니다.

단계 3 세부 정보 창에서  를 클릭하여 편집합니다.

단계 4 위의 절차에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 CDO에 변경의 영향을 받을 정책이 표시됩니다. **Confirm**(확인)을 클릭하여 개체 및 해당 개체의 영향을 받는 정책에 대한 변경을 완료합니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.