디바이스 및 서비스 온보딩

라이브 디바이스와 모델 디바이스를 모두 CDO에 온보딩할 수 있습니다. 모델 디바이스는 CDO를 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 보안 디바이스 커넥터가 CDO를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

SDC 및 해당 상태에 대한 자세한 내용은 SDC(Secure Device Connector)의 내용을 참조하십시오.

이 장에는 다음 섹션이 포함되어 있습니다.

- 온프레미스 Management Center 온보딩, 1 페이지
- CDO에서 온프레미스 Firewall Management Center 제거, on page 7

온프레미스 **Management Center** 온보딩

자세한 내용은 매니지드 디바이스에 Cisco Defense Orchestrator 연결를 검토하십시오.

참고 CDO는 온프레미스 Management Center 또는 온프레미스 Management Center에 등록된 디바이스와 연결된 개체 또는 정책의 생성이나 수정을 지원하지 않습니다. 온프레미스 Management Center UI에서 이러한 변경을 수행해야 합니다.

지침 및 제한 사항

온프레미스 Management Center의 온보딩에 적용되는 제한 사항은 다음과 같습니다.

- 온프레미스 Management Center를 온보딩하면 온프레미스 Management Center에 등록된 모든 디바이스도 온보딩합니다. 매니지드 디바이스가 비활성화되었거나 연결할 수 없는 경우 CDO는 **Inventory(**재고 목록**)** 페이지에 디바이스를 표시할 수 있지만, 성공적으로 요청을 전송하거나 디바이스 정보를 볼 수는 없습니다.
- 특히 CDO 통신을 위해 관리자 레벨 권한이 있는 새 사용자를 온프레미스 Management Center에 생성하는 것이 좋습니다. 온프레미스 Management Center를 온보딩한 다음 동일한 로그인 자격 증명으로 온프레미스 Management Center에 동시에 로그인하면 온보딩이 실패합니다.

- CDO 통신을 위해 온프레미스 Management Center에 새 사용자를 생성하는 경우, 사용자 구성에 대한 **Maximum Number of Failed Logins(**최대 실패 로그인 횟수**)**를 "0"으로 설정해야 합니다.

네트워크 요구 사항

디바이스를 온보딩하기 전에 다음 포트에 외부 액세스 권한이 있는지 확인합니다. 통신 포트가 방화벽 뒤에서 차단된 경우 디바이스 온보딩이 실패할 수 있습니다.

포트	프로토콜/기능	플랫폼	방향	세부 사항
7/UDP	UDP/감사 로깅	FMC	아웃바운드	감사 로깅을 구성할 때 시스템 로그 서버와의 연결을 확인합니다.
25/tcp	SMTP	FMC	아웃바운드	이메일 알림 및 경고 전송
53/tcp 53/udp	DNS	FMC	아웃바운드	DNS
67/udp 68/udp	DHCP	FMC	아웃바운드	DHCP
80/tcp	HTTP	FMC	아웃바운드	대시보드에 RSS 피드 표시
80/tcp	HTTP	FMC	아웃바운드	URL 카테고리 및 평판 데이터 다운로드 또는 쿼리(포트 443도 필요)
80/tcp	HTTP	FMC	아웃바운드	HTTP를 통해 사용자 정의 보안 인텔리전스 다운로드
123/udp	NTP	FMC	아웃바운드	시간 동기화
162/udp	SNMP	FMC	아웃바운드	SNMP 경고를 원격 트랩 서버로 전송
389/tcp 636/tcp	LDAP	FMC	아웃바운드	외부 인증을 위해 LDAP 서버와 통신 감지된 LDAP 사용자의 메타데이터 가져오기(FMC 전용) 구성 가능합니다.
443/tcp	HTTPS	FMC	인바운드	FMC를 온프레미스 Secure Device Connector로 온보딩하는 경우 포트 443에 대한 인바운드 연결을 허용합니다.

포트	프로토콜/기능	플랫폼	방향	세부 사항
443/tcp	HTPS	FMC	아웃바운드	Cloud Connector를 사용하여 FMC를 CDO에 온보딩하는 경우 포트 443에서 아웃바운드 트래픽을 허용합니다.
443/tcp	HTPS	FMC	아웃바운드	SecureX를 사용하여 FMC를 온보딩하는 경우 포트 443에 대한 아웃바운드 연결을 허용합니다.
443/tcp	HTTPS	FMC	아웃바운드	인터넷에서 데이터 송수신
443	HTTPS	FMC	아웃바운드	AMP 클라우드와 통신(퍼블릭 또는 프라이빗)
514/udp	시스템 로그(알림)	FMC	아웃바운드	원격 syslog 서버에 대한 경고 전송
1812/udp 1813/udp	RADIUS	FMC	아웃바운드	외부 인증 및 어카운트 관리를 위해 RADIUS 서버와 통신 구성 가능합니다.
5222/tcp	ISE	FMC	아웃바운드	ISE ID 소스와 통신
6514/tcp	시스템 로그(감사 이벤트)	FMC	아웃바운드	TLS를 구성하면 감사 로그를 원격 시스템 로그 서버에 전송합니다.
8305/tcp	어플라이언스 통신	FMC	Both(모두)	구축 어플라이언스 간 보안 통신. 구성 가능합니다. 이 포트를 변경하는 경우 구축의 모든 어플라이언스에 대해 이 포트를 변경해야 합니다. 기본값을 유지하는 것이 좋습니다.
8989/tcp	Cisco Success Network	FMC	아웃바운드	사용 정보 및 통계를 전송합니다.

자격 증명을 사용하여 온프레미스 **Firewall Management Center**를 **CDO**로 온보딩

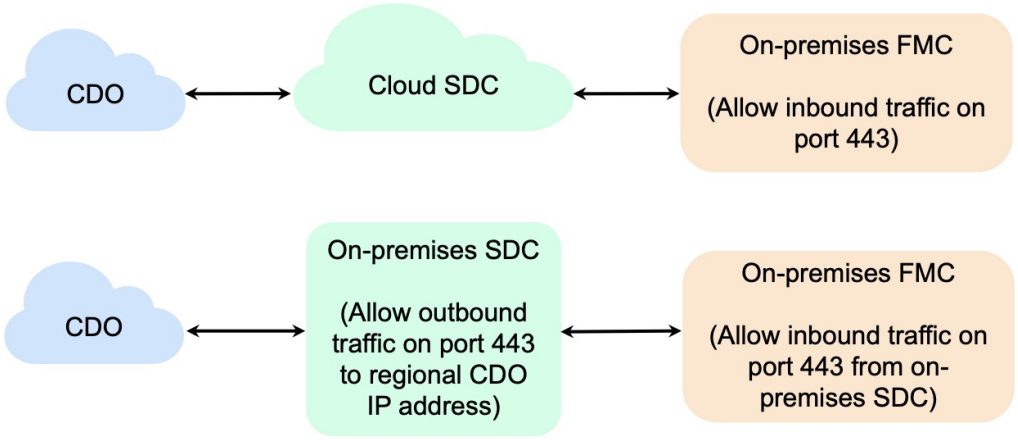
자격 증명을 사용하여 온프레미스 Firewall Management Center에 온보딩하려면 다음 절차를 수행합니다.

Before you begin

온프레미스 Management Center 온보딩, on page 1를 검토합니다.

온프레미스 Firewall Management Center에서 적절한 포트 액세스를 허용해야 합니다.

- 온프레미스 보안 디바이스 커넥터를 사용하여 온프레미스 FMC를 온보딩하는 경우 포트 443에서 인바운드 연결을 허용합니다.
- Cloud Connector를 사용하여 FMC를 온보딩하는 경우 포트 443에서 아웃바운드 연결을 허용합니다.



단계 **1** CDO 내비게이션 바에서 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 클릭합니다.

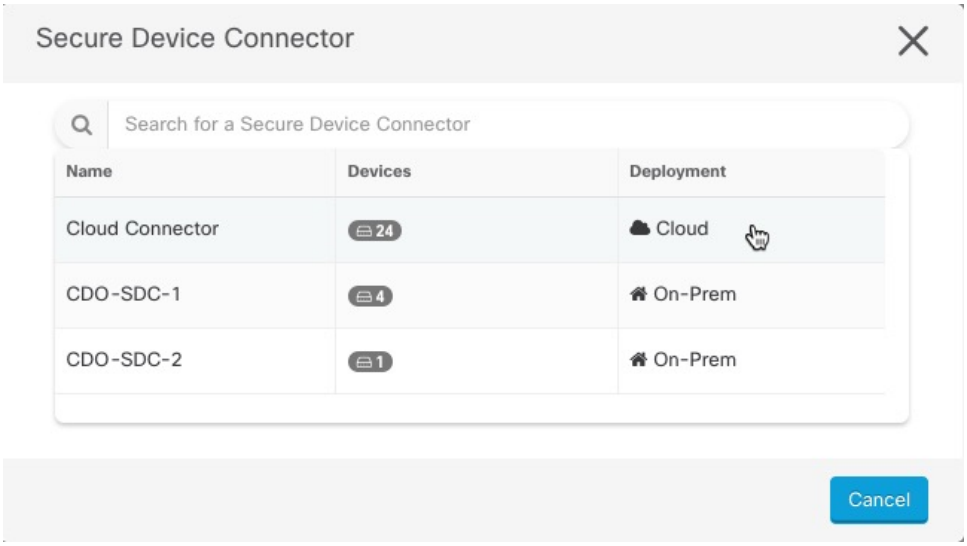
단계 **2** +을 클릭하여 온프레미스 Firewall Management Center를 온보딩합니다.

단계 **3** **On-Prem FMC(**온프레미스 **FMC)**를 클릭합니다.

단계 **4** **Use Credentials(**자격 증명 사용**)** 카드를 선택합니다.

단계 **5** **Secure Device Connector(**보안 디바이스 커넥터**)** 버튼을 클릭하고 네트워크에 설치된 SDC를 선택합니다. SDC를 사용하지 않으려는 경우 CDO는 클라우드 커넥터를 사용하여 온프레미스 Management Center에 연결할 수 있습니다. 선택은 CDO를 매니지드 디바이스에 연결하는 방법에 따라 달라집니다.

Figure 1: 보안 디바이스 커넥터 선택



단계 **6** 디바이스 이름 및 위치를 입력합니다. **Next(**다음**)**를 클릭합니다.

단계 **7** 온프레미스 Management Center에 액세스하는 데 사용할 계정 자격 증명의 **Username(**사용자 이름**)**및 **Password(**비밀번호**)**를 입력합니다. **Next(**다음**)**를 클릭합니다.

단계 **8** 디바이스가 온보딩됩니다. 여기에서 온프레미스 Management Center에 레이블을 추가하도록 선택하거나 **Go to Services(**서비스로 이동**)**를 클릭하여 온보딩된 디바이스의 페이지를 볼 수 있습니다. 정상인 경우 FMC가 **Synced(**동기화됨**)** 상태로 표시됩니다.

Note 온프레미스 Management Center에서 관리하는 디바이스의 이름은 "<*fmcname*> _<*manageddevicename*> "으로 자동 지정됩니다.

SecureX를 사용하여 온프레미스 Firepower Management Center 자동 온보딩

CDO의 슈퍼 관리자 또는 관리자 사용자는 온프레미스 Management Center의 기능에 대한 플랫폼의 자동 온보딩을 사용할 수 있습니다. 이 기능은 SecureX 테넌트에 연결된 모든 온프레미스 FMC에 대한 온보딩 프로세스를 자동으로 시작합니다. 또한 이러한 온프레미스 FMC에 연결된 위협 방어 디바이스도 온보딩합니다.

이 기능은 CDO에서 기본적으로 활성화되므로 모든 온프레미스 FMC 및 위협 방어 디바이스가 자동으로 온보딩되므로 효율성을 크게 높일 수 있습니다.

CDO는 매시간 새로운 온프레미스 Management Center에 대한 SecureX 폴링을 수행합니다. 활성 온프레미스 Management Center HA(고가용성) 쌍을 온보딩합니다.

시작하기 전에

다음 요구 사항이 충족되었는지 확인하십시오.

- 온프레미스 Management Center은 버전 7.2 이상을 실행해야 합니다.
- 활성 SecureX 계정이 있어야 합니다.
- SecureX은 온프레미스 Management Center에서 활성화되어야 합니다. 단계 및 자세한 내용은 Cisco Secure Firewall Management Center(7.0.2 및 7.2) 및 SecureX 통합 설명서를 참조하십시오.
- SecureX에 Firepower 통합 모듈을 추가해야 합니다. 단계 및 자세한 내용은 Firepower Management Center와 SecureX 통합을 참조하십시오.
- 온프레미스 Management Center에서 포트 443을 발신하는 아웃바운드 트래픽을 허용해야 합니다.
- 온프레미스 Management Center에는 모듈이 구성되어 있어야 합니다.
- 디바이스를 온보딩하기 전에 CDO 테넌트와 SecureX/CTR 계정을 병합합니다. 자세한 내용은 계정 병합을 참조하십시오.
- CDO 테넌트 및 SecureX/CTR을 병합한 후, CDO 테넌트에서 로그아웃하고 다시 로그인해야 합니다.

단계 **1** **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center** >  를 클릭하고 **FMC**를 선택합니다.

단계 **2** **Discover From(**검색 위해**) SecureX Account(**계정**)**를 방법으로 클릭합니다.

SecureX를 사용하는 온프레미스 **FMC** 자동 온보딩 기능은 기본적으로 활성화되어 있습니다. **Tools and Services(**툴 및 서비스**)** > **Firewall Management Center**로 이동하여 CDO 테넌트에 연결된 SecureX 테넌트와 연결된 새로 온보딩된 온프레미스 Management Center를 확인할 수 있습니다.

단계 **3** 사용 가능한 링크를 클릭하여 이 기능을 비활성화할 수 있습니다.

단계 **4** **General Settings(**일반 설정**)** 화면에서 **Tenant Settings(**테넌트 설정**)** 섹션으로 이동하고 **Auto onboard On-Prem FMCs using SecureX tenant(SecureX** 테넌트를 사용하여 온프레미스 **FMC** 자동 온보딩**)**을 비활성화합니다.

참고 이 기능을 비활성화하면 CDO에서 SecureX 테넌트와 연결된 온프레미스 Management Center의 추가 온보딩이 중지됩니다. 이미 온보딩된 온프레미스 FMC는 제거되지 않습니다. 기능을 비활성화한 후에는 수동으로 제거해야 합니다.

CDO을 온프레미스 Firewall Management Center로 리디렉션

온프레미스 Management Center에서 CDO로 온보딩한 후에는 온프레미스 Management Center UI에서 관리 인터페이스의 호스트 이름이 FQDN을 포함하도록 업데이트해야 합니다. 그렇지 않으면 CDO에서 교차 실행할 수 없습니다.

다음 절차를 사용하여 관리 인터페이스 호스트 이름을 업데이트하고 CDO에서 온프레미스 Management Center로 리디렉션합니다.

단계 **1** 온프레미스 Management Center UI에 로그인합니다.

단계 **2** **System(**시스템**)** > **Configuration(**컨피그레이션**)**으로 이동합니다.

단계 **3** **Management Interface(**관리 인터페이스**)** 탭을 선택합니다.

단계 **4** **Shared Settings(**공유 설정**)** 헤더를 확장하고 편집 아이콘을 클릭합니다.

단계 **5** **Hostname(**호스트 이름**)** 필드를 찾아 FMC의 FQDN을 입력합니다.

단계 **6** 변경 내용을 저장합니다.

참고: **Manage Devices in Firepower Management Center(Firepower Management Center**에서 디바이스 관리**)**를 클릭하고 온프레미스 Management Center UI를 교차 실행하려면 CDO에서 로그아웃해야 할 수 있습니다.

CDO에서 온프레미스 Firewall Management Center 제거

CDO에서 온프레미스 Management Center 제거를 선택하는 경우, CDO에서 관리되는 모든 디바이스 제거를 선택하는 것입니다. 이렇게 해도 SecureX에서 온프레미스 Management Center가 제거되지는 않습니다.

다음 절차를 사용하여 온프레미스 Management Center 및 등록된 디바이스를 CDO에서 제거합니다.

단계 **1** 탐색 창에서 **Tools & Services(**툴 및 서비스**)** > **Firewall Management Center**를 클릭합니다.

단계 **2** **FMC** 탭이 선택되어 있는지 확인하고 제거할 온프레미스 Management Center을 선택합니다.

단계 **3** 오른쪽의 **Device Actions(**디바이스 작업**)** 창에서 **Remove On-Prem FMC and its managed devices(**온프레미스 **FMC** 및 해당 매니지드 디바이스 제거**)**를 클릭합니다.

단계 **4** **OK(**확인**)**를 클릭하여 온프레미스 Management Center 및 매니지드 디바이스를 테넌트에서 제거합니다.

단계 **5** 사용 가능한 디바이스의 업데이트된 목록을 확인하려면 브라우저를 새로 고침합니다.