Security Cloud Control에 디바이스 온보딩

라이브 디바이스와 모델 디바이스를 모두 Security Cloud Control에 온보딩할 수 있습니다. 모델 디바이스는 Security Cloud Control를 사용하여 보고 편집할 수 있는 업로드된 구성 파일입니다.

대부분의 라이브 디바이스 및 서비스는 Secure Device Connector가 Security Cloud Control를 디바이스 또는 서비스에 연결할 수 있도록 개방형 HTTPS 연결을 필요로 합니다.

이 장에는 다음 섹션이 포함되어 있습니다.

지원되는 디바이스, 소프트웨어 및 하드웨어

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

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

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

Cisco Secure Firewall ASA

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

Cisco Secure Firewall Threat Defense

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

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

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

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

Cisco Catalyst SD-WAN Manager

Security Cloud Control는 Catalyst SD-WAN에 대한 중앙 집중식 관리를 제공하여 조직이 네트워크 전반에 걸쳐 보안 정책을 효율적으로 구성, 모니터링 및 시행할 수 있도록 합니다. 이 통합은 또한 Catalyst SD-WAN Manager에서의 고급 문제 해결, 규칙 최적화 및 변경 관리를 용이하게 합니다.

소프트웨어 및 하드웨어 호환성에 대한 자세한 내용은 Cisco Catalyst SD-WAN 디바이스 호환성 가이드를 참조하십시오.

Cisco Secure Firewall Management Center

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

Cisco Meraki MX

Meraki MX 어플라이언스는 분산 구축을 위해 설계된 엔터프라이즈급 보안 및 SD-WAN 차세대 방화벽 어플라이언스입니다. Security Cloud Control는 Meraki MX 디바이스에서 레이어 3 네트워크 규칙 관리를 지원합니다. Meraki 디바이스를 Security Cloud Control에 온보딩할 경우, 이는 Meraki 대시보드 와 통신하여 디바이스를 관리합니다. Security Cloud Control 는 설정 요청을 Meraki 대시보드 로 안전하게 전송하며, Meraki 대시보드에서 새 설정을 디바이스에 적용합니다. 중앙 집중식 정책 관리, 백

업 및 복원, 모니터링 및 보고, 규정 준수 확인, 자동화 기능 등이 Security Cloud Control의 Cisco Meraki MX 지원의 주요 기능입니다.

Cisco IOS 디바이스

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

Cisco Umbrella

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

AWS 보안 그룹

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

온프레미스 방화벽 Management Center 온보딩

이 장에서는 온프레미스 방화벽 Management Center를 온보딩하고 연결된 Threat Defense를 관리하는 단계를 제공합니다.

온프레미스 방화벽 Management Center을 Security Cloud Control에 온보딩

Security Cloud Control는 온프레미스 방화벽 Management Center를 온보딩하기 위한 다음 방법을 제공합니다.

- (권장) 자동 검색 및 Cisco Security Cloud과 통합된 온프레미스 방화벽 Management Center 온보딩
- 온프레미스 방화벽 Management Center 자격증명 사용

자세한 내용은 매니지드 디바이스에 Security Cloud Control 연결를 검토하십시오.

참고

Security Cloud Control는 다음을 허용하여 FMC를 보완합니다.

- FMC와 공유하는 개체 관리를 통해 정책을 일관되게 추진합니다.

  자세한 내용은 Managing On-Prem Firewall Management Center with Security Cloud Control(온프레미스 Firewall Management Center 관리)에서 **Objects(**개체**)** 섹션을 참조하십시오.

- Firewall Threat Defense 디바이스에서 제로 터치 프로비저닝 활성화

  자세한 내용은 제로 터치 프로비저닝을 사용하는 온프레미스 방화벽 Management Center에 디바이스 온보딩을 참조하십시오.

- **Security Devices(**보안 디바이스**)**의 중앙 집중식 보기를 표시합니다.

  자세한 내용은 Device and Service Management(디바이스 및 서비스 관리)를 참조하십시오.

- 클라우드 CSDC 및 클라우드 제공 Firewall Management Center 활용

  자세한 내용은 Cisco Secure Dynamic Attributes Connector를 참조하십시오.

지침 및 제한 사항

온프레미스 방화벽 Management Center의 온보딩에 적용되는 제한 사항은 다음과 같습니다.

- 온프레미스 방화벽 Management Center를 온보딩하면 온프레미스 방화벽 Management Center에 등록된 모든 디바이스도 온보딩합니다. 매니지드 디바이스가 비활성화되었거나 연결할 수 없는 경우 Security Cloud Control는 **Security Devices(**보안 디바이스**)** 페이지에 디바이스를 표시할 수 있지만, 성공적으로 요청을 전송하거나 디바이스 정보를 볼 수는 없습니다.
- 온프레미스 방화벽 Management Center를 온보딩해도 온프레미스 방화벽 Management Center의 정책이 Security Cloud Control 또는 클라우드 제공 Firewall Management Center에 연속되지 않습니다. 그러나 내장된 **FTD**를 **cdFMC**로 마이그레이션 기능을 사용하여 온프레미스 방화벽 Management Center에서 관리하는 Firewall Threat Defense를 클라우드 제공 Firewall Management Center로 마이그레이션할 수 있습니다. 그러면 모든 정책이 디바이스에 연결됩니다. 자세한 내용은 Threat Defense를 클라우드 제공 Firewall Management Center로 마이그레이션을 참조하십시오.
- 특히 Security Cloud Control 통신을 위해 관리자 레벨 권한이 있는 새 사용자를 온프레미스 방화벽 Management Center에 생성하는 것이 좋습니다. 온프레미스 방화벽 Management Center를 온보딩한 다음 동일한 로그인 자격 증명으로 온프레미스 방화벽 Management Center에 동시에 로그인하면 온보딩이 실패합니다.
- Security Cloud Control 통신을 위해 온프레미스 방화벽 Management Center에 새 사용자를 생성하는 경우, 사용자 구성에 대한 **Maximum Number of Failed Logins(**최대 실패 로그인 횟수**)**를 "0"으로 설정해야 합니다.
- 버전 7.4 이상을 실행하는 온프레미스 방화벽 Management Center의 경우, 전환이 발생하여 FMC가 더 이상 클라우드에 연결되지 않는 경우 SecureX를 비활성화했다가 다시 활성화해 보십시오.

Cisco Security Cloud와 통합된 온프레미스 방화벽 Management Center 자동 온보딩

자동 검색 및 온보딩 기능은 기본적으로 Security Cloud Control에서 활성화되어 있으므로 버전 7.2 이상을 실행하고 Cisco Security Cloud에 통합된 모든 온프레미스 방화벽 Management Center가 자동으로 검색되고 Security Cloud Control에 온보딩됩니다. 또한 연결된 Firewall Threat Defense 디바이스는 Security Cloud Control에 온보딩됩니다.

또한 Security Cloud Control은 온프레미스 방화벽 Management Center 고가용성(HA) 쌍을 온보딩합니다.

시작하기 전에

다음 사전 요건이 충족되는지 확인합니다.

- 온프레미스 방화벽 Management Center의 포트 443에서 아웃바운드 트래픽을 허용합니다.

프로시저

단계 **1** 온보딩하려는 온프레미스 방화벽 Management Center를 Cisco Security Cloud와 통합하고 Security Cloud Control 테넌트에 등록합니다. 온프레미스 방화벽 Management Center을 Cisco Security Cloud와 통합, 5 페이지을 참조하십시오.

단계 **2** 온프레미스 방화벽 Management Center에 등록된 Security Cloud Control테넌트에 로그인합니다.

단계 **3** 왼쪽 창에서 **Administration(관리)** > **Integration(통합)** > **Firewall Management Center**를 클릭합니다.

테넌트와 관련된 모든 온프레미스 방화벽 Management Center가 **FMC** 탭에 표시됩니다. 온보딩된 온프레미스 방화벽 Management Center 보기를 참조하십시오.

온프레미스 방화벽 Management Center을 Cisco Security Cloud와 통합

이 절차를 사용하여 온프레미스 방화벽 Management Center와 Cisco Security Cloud를 통합합니다. Cisco Security Cloud 통합을 활성화하면 관리 센터가 Cisco 클라우드 테넌시에 등록됩니다.

시작하기 전에

온프레미스 방화벽 Management Center을 온보딩하는 경우:

- Security Cloud Control 테넌트 이미 있는 경우 해당 기존 테넌트에 온프레미스 방화벽 Management Center를 연결할지 확인하라는 메시지가 표시됩니다.
- 테넌트 또는 어카운트가 없는 경우 등록 작업의 온보딩 프로세스 중에 온프레미스 방화벽 Management Center 통합 마법사 새 테넌트를 자동으로 생성합니다. 테넌트 는 온프레미스 방화벽 Management Center AI Assist 활성화용으로만 제공되는 프리 계층입니다. 마법사가 테넌트 생성을 관리하도록 하여 나중에 변환이 필요한 평가판 테넌트를 받지 않도록 합니다. 마법사 원활한 환경을 제공하기 위해 이 프로세스를 관리합니다.

- 클라우드 제공 Firewall Management Center를 사용하거나 Security Cloud Control를 사용하여 방화벽을 관리하려면 기본 라이선스 및 디바이스 엔타이틀먼트를 구매해야 합니다. 라이선싱 정보 및 제품 옵션에 대한 자세한 내용은 Security Cloud Control 라이선싱 개요를 참조하십시오.

프로시저

단계 **1** 온프레미스 방화벽 Management Center에서 다음을 수행합니다.

- 7.2와 7.4.x 사이의 온프레미스 방화벽 Management Center 버전은 **Integration(통합)** > **SecureX** 로 이동하십시오.
- 7.6 이상의 온프레미스 방화벽 Management Center 버전은 **Integration(통합)** > **Cisco Security Cloud**로 이동하십시오.

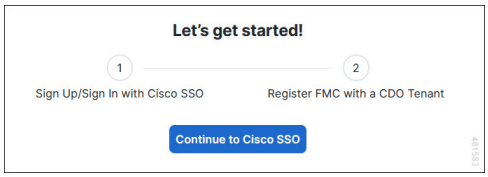
단계 **2** 온프레미스 방화벽 Management Center 버전에 따라 다음을 수행합니다.

- 7.2와 7.4.x 사이의 온프레미스 방화벽 Management Center 버전은 **Enable Secure X(Secure X 활성화)**를 클릭합니다.
- 7.6 이상의 온프레미스 방화벽 Management Center 버전은 **Cisco Security Cloud**를 클릭합니다.

Security Cloud Control 어카운트에 로그인할 수 있는 별도의 브라우저 탭이 열립니다. 이 페이지가 팝업 차단기로 차단되지 않았는지 확인하십시오.

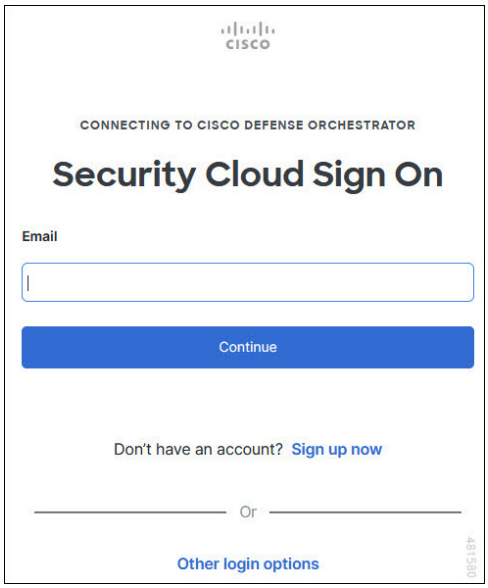
단계 **3** **Continue to Cisco SSO(Cisco SSO**로 계속 진행**)**을 클릭합니다.

그림 ***1: Cisco Security Cloud*** 시작 페이지



단계 **4** Security Cloud Control 어카운트에 로그인합니다.

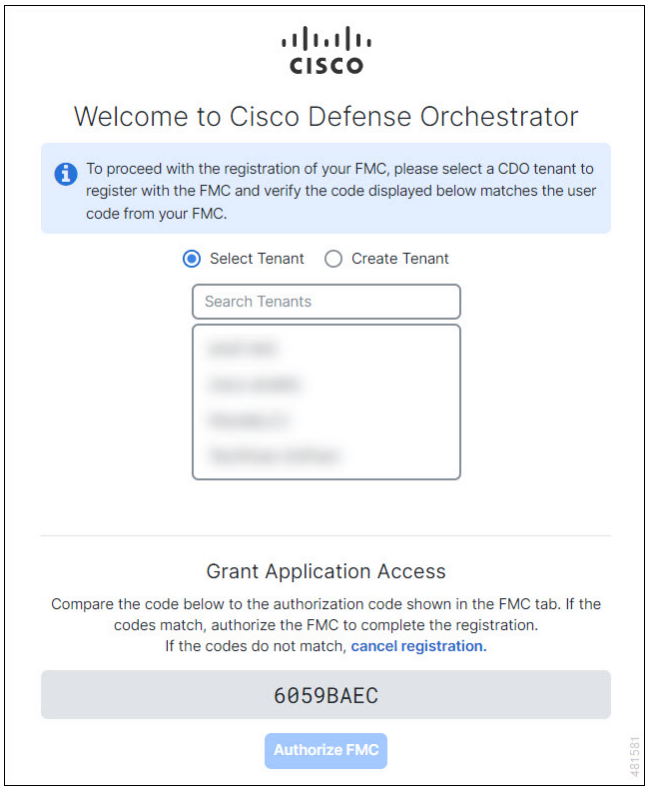
그림 *2: Cisco Security Cloud Sign On*



Security Cloud Control에 로그인할 Security Cloud 로그인 어카운트가 없고 어카운트를 생성하려면 **Security Cloud** 로그인 페이지에서 **Sign up now(**지금 가입**)**을 클릭합니다. 새 Cisco Secure Cloud Sign-On 어카운트 생성을 참조하십시오.

단계 **5** 이 통합에 사용할 Security Cloud Control 테넌트를 선택합니다. 온프레미스 방화벽 Management Center 및 매니지드 디바이스는 여기에서 선택한 Security Cloud Control 테넌트에 온보딩됩니다.

그림 *3: Security Cloud Control* 테넌트 선택



아직 Security Cloud Control 테넌트가 없거나 이 통합에 새 테넌트를 사용하려는 경우 새 테넌트를 생성합니다.

자세한 내용은 Security Cloud Control 테넌트 생성를 참조하십시오.

단계 **6** Security Cloud Control 로그인 페이지에 표시된 코드가 온프레미스 방화벽 Management Center에서 제공한 코드와 일치하는지 확인합니다.

그림 *4:* 온프레미스 방화벽 *Management Center*에서 확인 코드

단계 **7** **Authorize FMC(FMC** 권한 부여**)**를 클릭합니다.

단계 **8** 온프레미스 방화벽 Management Center UI에서 구성을 저장하려면 **Save(**저장**)**를 클릭합니다.

Notifications(알림**)** > **Tasks(**작업**)**에서 작업 진행 상황을 볼 수 있습니다.

등록 작업을 완료하는 데 최대 90초가 소요될 수 있습니다. 등록 작업이 진행되는 동안 온프레미스 방화벽 Management Center를 사용해야 하는 경우 새 창에서 온프레미스 방화벽 Management Center를 엽니다.

온프레미스 방화벽 Management Center의 자동 온보딩 비활성화

온프레미스 방화벽 Management Center의 자동 온보딩 기능을 비활성화하면 Cisco Security Cloud에서 이 Security Cloud Control 테넌트에 새로운 온프레미스 방화벽 Management Center이 자동으로 온보딩되지 않습니다.

Security Cloud Control의 슈퍼 관리자 또는 관리자 사용자만 이 기능을 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 1 왼쪽 창에서 **Administration(관리)** > **General Settings(일반 설정)**를 클릭합니다.

단계 2 **General Settings(일반 설정)** 화면에서 **Auto onboard On-Prem FMCs with Cisco Security Cloud(온프레미스 FMC 자동 온보딩)** 토글 버튼 클릭하여 온프레미스 방화벽 Management Center의 자동 온보딩 기능을 비활성화합니다.

단계 3 **OK(확인)**를 클릭합니다.

자격 증명을 사용하여 온프레미스 방화벽 Management Center를 Security Cloud Control로 온보딩

자격 증명을 사용하여 온프레미스 방화벽 Management Center을 Security Cloud Control에 온보딩하려면 다음 절차를 수행합니다.

Before you begin

다음 사전 요건을 충족해야 합니다.

- 클라우드 **SDC(Secure Device Connector)**: 온프레미스 방화벽 Management Center의 포트 443에서 인바운드 트래픽을 허용합니다.

  SDC는 포트 443의 인바운드 트래픽을 허용하여 온프레미스 방화벽 Management Center에 연결합니다.

Security Cloud Control 및 SDC는 모두 클라우드에서 호스팅됩니다.

- 온프레미스 **SDC(Secure Device Connector)**의 경우: SDC의 포트 443에서 아웃바운드 연결을 허용합니다.

  SDC는 Security Cloud Control에 대한 연결이 필요하므로, SDC에서 Security Cloud Control로의 아웃바운드 트래픽을 허용해야 합니다. 온프레미스 Firewall Management Center에 추가 포트 구성이 필요하지 않습니다.

Procedure

단계 **1** 왼쪽 창에서 **Administration(관리)** > **General Settings(일반 설정)**를 클릭합니다.

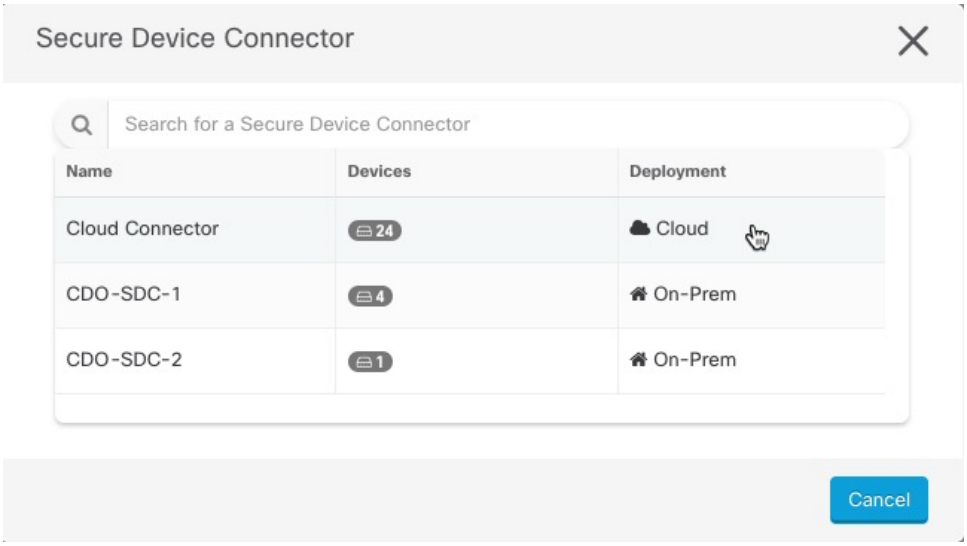
단계 **2** + 을 클릭하여 온프레미스 방화벽 Management Center를 온보딩합니다.

단계 **3** **Firewall Management Center**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 Security Cloud Control는 클라우드 커넥터를 사용하여 온프레미스 방화벽 Management Center에 연결할 수 있습니다. 선택은 Security Cloud Control를 매니지드 디바이스에 연결하는 방법에 따라 달라집니다.

Figure 5: Secure Device Connector 선택



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

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

단계 **8** 디바이스가 온보딩됩니다. 여기에서 온프레미스 방화벽 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 방화벽 Management Center에서 관리하는 디바이스의 이름은 "<*fmcname*> _<*manageddevicename*> "으로 자동 지정됩니다.

Security Cloud Control을 온프레미스 방화벽 Management Center로 리디렉션

온프레미스 방화벽 Management Center에서 Security Cloud Control로 온보딩한 후에는 온프레미스 방화벽 Management Center UI에서 관리 인터페이스의 호스트 이름이 FQDN을 포함하도록 업데이트해야 합니다. 그렇지 않으면 Security Cloud Control에서 교차 실행할 수 없습니다.

다음 절차를 사용하여 관리 인터페이스 호스트 이름을 업데이트하고 Security Cloud Control에서 온프레미스 방화벽 Management Center로 리디렉션합니다.

프로시저

단계 **1** 온프레미스 방화벽 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 Firewall Management Center의 FQDN을 입력합니다.

단계 **6** 변경 내용을 저장합니다.

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

Security Cloud Control에서 온프레미스 방화벽 Management Center 제거

Security Cloud Control에서 온프레미스 방화벽 Management Center을 제거하도록 선택하면 온프레미스 방화벽 Management Center기준의 모든 디바이스도 제거됩니다.

Before you begin

자동 온보딩 옵션을 비활성화하여 자동 온보딩 기능을 사용하여 온보딩된 하나 이상의 온프레미스 방화벽 Management Center을 제거하십시오.

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

2. **Tenant Settings(**테넌트 설정**)** 섹션에서 **Auto onboard On-Prem FMCs integrated to Cisco Security Cloud(**통합된 온프레미스 **FMC** 자동 온보딩**)**을 비활성화합니다.

Procedure

단계 **1** 왼쪽 창에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 클릭합니다.

단계 **2** **FMC** 탭이 선택되어 있는지 확인하고 제거할 온프레미스 방화벽 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 방화벽 Management Center 및 매니지드 디바이스를 테넌트에서 제거합니다.

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

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.

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.