



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.

- [위협 방어 디바이스 온보딩, on page 1](#)
- [CDO에서 디바이스 삭제, 48 페이지](#)
- [오프라인 관리를 위한 디바이스 컨피그레이션 가져오기, 49 페이지](#)
- [FDM-관리 디바이스 백업, on page 49](#)
- [FDM 소프트웨어 업그레이드 경로, on page 55](#)
- [FDM-관리 디바이스 업그레이드 사전 요건, on page 58](#)
- [단일 FTD 디바이스 업그레이드, on page 59](#)
- [대량 FDM-관리 디바이스 업그레이드, on page 61](#)
- [FDM-관리 고가용성 쌍 업그레이드, on page 64](#)
- [Snort 3.0으로 업그레이드, on page 67](#)
- [FDM-관리 디바이스용 Snort 3.0에서 되돌리기, on page 71](#)
- [보안 데이터베이스 업데이트 예약, on page 72](#)

위협 방어 디바이스 온보딩



Attention

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.](#)

위협 방어 디바이스를 온보딩하는 다양한 방법이 있습니다. 등록 키 방법을 사용하는 것이 좋습니다.

디바이스를 온보딩하는 동안 문제가 발생하는 경우 [일련 번호를 사용하여 FDM-관리 디바이스 온보딩 문제 해결](#) 또는 [라이선스 부족으로 인해 실패](#)에서 자세한 내용을 참조하십시오.

위협 방어 디바이스를 클라우드 사용 **Firewall Management Center**에 온보딩

버전 7.2 이상을 실행하는 위협 방어 디바이스를 클라우드 사용 Firewall Management Center에 온보딩할 수 있습니다. 자세한 내용은 [클라우드 사용 Firewall Management Center에 FTD 온보딩](#)을 참조하십시오.

일련 번호로 위협 방어 디바이스 온보딩

이 절차는 지원되는 버전의 소프트웨어를 실행하는 , Firepower 1000, Firepower 2100, 또는 Secure Firewall 3100 시리즈 물리적 디바이스를 온보딩하는 간소화된 방법입니다. 디바이스를 온보딩하려면 디바이스의 새시 일련 번호 또는 PCA 일련 번호가 필요하며 디바이스가 인터넷에 연결할 수 있는 네트워크에 추가되었는지 확인합니다.

공장에서 배송된 새 디바이스 또는 이미 CDO에 구성된 디바이스를 온보딩할 수 있습니다.

자세한 내용은 [디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩](#), on page 21을 참조하십시오.

등록 키를 사용하여 위협 방어 디바이스 온보딩

등록 키를 사용하여 위협 방어 디바이스를 온보딩하는 것이 좋습니다. 이는 DHCP를 사용하여 디바이스에 IP 주소가 할당된 경우 유용합니다. 등록 키로 온보딩했다면 어떤 이유로든 해당 IP 주소가 변경되더라도 위협 방어 디바이스는 CDO에 연결된 상태로 유지됩니다.

- [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩](#), on page 12
- [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#), on page 16

자격 증명을 사용하여 위협 방어 디바이스 온보딩

네트워크에서 디바이스가 구성된 방식에 따라 디바이스 자격 증명 및 디바이스 외부, 내부 또는 관리 인터페이스의 IP 주소를 사용하여 위협 방어 디바이스를 온보딩할 수 있습니다. 자격 증명을 사용하여 디바이스를 온보딩하려면 [사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩](#), on page 10의 내용을 참조하십시오. 인터페이스 주소를 사용하여 온보딩하려면 이 문서의 뒷부분에 나오는 [위협 방어 디바이스 온보딩](#)을 참조하십시오.

디바이스를 관리하려면 CDO에 디바이스에 대한 HTTPS 액세스가 필요합니다. 디바이스에 대한 HTTPS 액세스를 허용하는 방법은 네트워크에서 디바이스가 구성된 방식 및 디바이스를 온보딩하는 디바이스가 [보안 디바이스 커넥터](#)인지 클라우드 커넥터인지에 따라 달라집니다.



Note <https://www.defenseorchestrator.eu>에 연결하고 소프트웨어 버전 6.4를 사용하는 경우 이 방법으로 위협 방어 디바이스를 온보딩해야 합니다. 등록 키 방법을 사용할 수 없습니다.

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. 자격 증명으로 온보딩된 위협 방어 디바이스는 SDC를 사용하여 CDO에 온보딩할 수 있습니다.

VPN 연결을 위한 헤드엔드로도 위협 방어 디바이스를 사용하는 고객은 외부 인터페이스를 사용하여 디바이스를 관리할 수 없습니다.

위협 방어 클러스터 온보딩

CDO에 온보딩 전에 클러스터링된 위협 방어 디바이스를 온보딩할 수 있습니다. 클러스터링을 사용하면 여러 방화벽 위협 방어 유닛을 하나의 논리적 디바이스로 그룹화하여 단일 디바이스의 편의성(관리, 네트워크 통합)을 제공하는 동시에 여러 디바이스의 처리량 증가 및 이중화를 달성할 수 있습니다.

클러스터된 [Secure Firewall Threat Defense 디바이스 온보딩](#), on page 36의 내용을 참조하십시오.

온보딩을 위한 **FDM**-관리 디바이스 구성 사전 요건

FDM-관리 디바이스 관리

Secure Firewall device manager (FDM)에서 관리 중인 위협 방어 디바이스만 온보딩할 수 있습니다. Secure Firewall Management Center에서 관리 중인 위협 방어 디바이스는 클라우드 사용 Firewall Management Center에서 관리할 수 없습니다.

디바이스가 로컬 관리용으로 구성되지 않은 경우 디바이스를 온보딩하기 전에 로컬 관리로 전환해야 합니다. [Firepower Device Manager용 Secure Firewall Threat Defense 구성 가이드](#)의 로컬 및 원격 관리 간 전환 장을 참조하십시오.

라이선싱

일부 상황에서는 스마트 라이선스를 적용할 수 있지만 디바이스를 CDO에 온보딩하려면 최소한 라이선스가 설치되어 있어야 합니다.

온보딩 방법	Secure Firewall device manager 소프트웨어 버전	90일 평가판 라이선스가 허용됩니까?	온보딩 전에 디바이스에 이미 스마트 라이선스가 부여될 수 있습니까?	온보딩 전에 디바이스를 Cisco Cloud Services에 이미 등록할 수 있습니까?
자격 증명(사용자 이름 및 비밀번호)	계	예	예	예
등록 키	6.4 또는 6.5	예	아니요. 스마트 라이선스를 등록 취소한 다음 디바이스를 온보딩합니다.	해당 없음

온보딩 방법	Secure Firewall device manager 소프트웨어 버전	90일 평가판 라이선스가 허용됩니까?	온보딩 전에 디바이스에 이미 스마트 라이선스가 부여될 수 있습니까?	온보딩 전에 디바이스를 Cisco Cloud Services 에 이미 등록할 수 있습니까?
등록 키	6.6 이상	예	예	아니요. Cisco Cloud Services에서 디바이스를 등록 취소한 다음 디바이스를 온보딩합니다.
로우 터치 프로비저닝	6.7 이상	예	예	예
일련 번호로 디바이스 온보딩	6.7 이상	예	예	예

자세한 내용은 [Cisco Firepower System 기능 라이선스](#)를 참조하십시오.

디바이스 주소 지정

FDM 관리 디바이스를 온보딩하는 데 사용하는 주소는 고정 주소인 것이 가장 좋습니다. 디바이스의 IP 주소가 DHCP에 의해 할당된 경우 DDNS(동적 도메인 이름 시스템)를 사용하여 디바이스의 도메인 이름 항목이 변경되는 경우 디바이스의 새 IP 주소로 자동으로 업데이트하는 것이 가장 좋습니다.



Note FDM 관리 디바이스는 기본적으로 DDNS를 지원하지 않습니다. 사용자 고유의 DDNS를 구성해야 합니다.

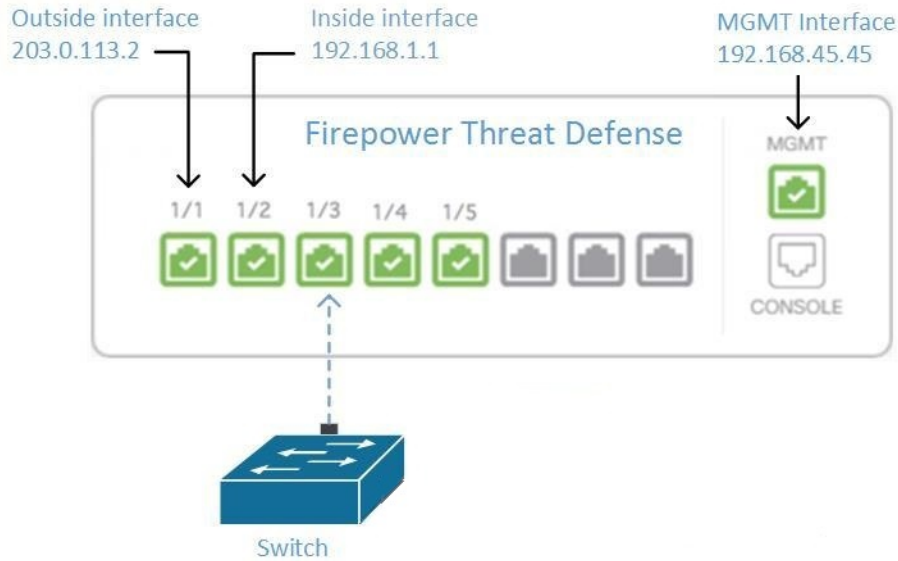


Important 디바이스가 DHCP 서버에서 IP 주소를 가져오는데 FDM 관리 디바이스의 도메인 이름 항목을 새 IP 주소로 업데이트하는 DDNS 서버가 없거나 디바이스가 새 주소를 수신하는 경우, [CDO가 디바이스에 대해 유지하는 IP 주소를 변경한 다음 디바이스를 다시 연결](#)할 수 있습니다. 등록 키를 사용하여 디바이스를 온보딩하는 것이 더 좋습니다.

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**로 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**
- 매니지드 디바이스에 **Cisco Defense Orchestrator 연결**

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

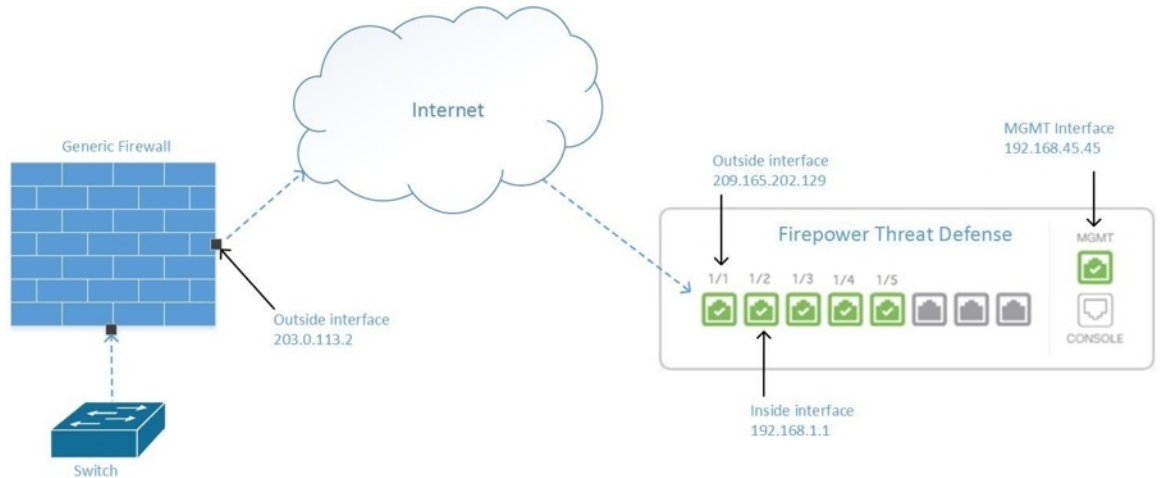
FDM-관리 디바이스 온보딩

등록 토큰 온보딩 접근 방식은 **FDM** 관리 디바이스를 CDO에 온보딩하는 권장 방법입니다. **Cloud Connector**에서 **FDM** 관리 디바이스로의 관리 액세스를 허용하도록 내부 인터페이스를 구성한 후, 사용자 이름과 암호를 사용하여 **FDM** 관리 디바이스를 온보딩합니다. 자세한 내용은 [위협 방어 디바이스 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 Orchestrator**가 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 Center**로 관리하는 디바이스가 원격 액세스 **VPN(RA VPN)** 연결을 관리하는 경우, 클라우드 사용 **Firewall Management Center**는 외부 인터페이스를 사용하여 클라우

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

다음 작업:

클라우드 사용 Firewall Management Center 디바이스 구성 절차를 위해 [FDM-관리 디바이스의 외부 인터페이스 관리](#)로 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](#)
- 매니지드 디바이스에 [Cisco Defense Orchestrator 연결](#)

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 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 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.

FDM-관리 디바이스를 CDO에 온보딩

다음 절차에 따라 아래의 방법으로 FDM 관리를 CDO로 온보딩합니다.

사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩

디바이스 자격 증명 및 디바이스의 관리 IP 주소만 사용하여 FDM 관리 디바이스를 온보딩하려면 이 절차를 사용합니다. 이는 FDM 관리 디바이스를 온보딩하는 가장 간단한 방법입니다. 그러나 FDM 관리 디바이스를 CDO에 온보딩하는 데 권장하는 방법은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)를 사용하는 것입니다.

Before you begin



Important

Cisco Defense Orchestrator에 FDM 관리 디바이스를 온보딩하기 전에 [위협 방어 디바이스 온보딩 및 매니지드 디바이스에 Cisco Defense Orchestrator 연결](#)을 읽어 보십시오. 디바이스를 온보딩하는 데 필요한 일반 디바이스 요구 사항 및 온보딩 사전 요건을 제공합니다.

- 자격 증명 방법을 사용하여 FDM 관리 디바이스를 온보딩하려면 다음 정보가 필요합니다.
 - 디바이스 자격 증명 CDO는 디바이스에 연결하는 데 사용됩니다.
 - 디바이스 관리에 사용 중인 인터페이스의 디바이스 IP 주소입니다. 이는 네트워크를 구성한 방법에 따라 관리 인터페이스, 내부 인터페이스 또는 외부 인터페이스일 수 있습니다.
 - 디바이스를 CDO에 온보딩하려면 로컬 관리를 위해 Secure Firewall device manager이 디바이스를 관리하고 구성해야 합니다. Secure Firewall Management Center에서 관리할 수 없습니다.




Note

<https://www.defenseorchestrator.eu>에 연결하고 FDM 관리 디바이스에서 소프트웨어 버전 6.4를 실행 중인 경우 이 방법을 사용해야 합니다. 소프트웨어 버전 6.5 이상을 실행하는 FDM 관리 디바이스만 온보딩할 수 있습니다.

Procedure

단계 1 CDO에 로그인합니다.

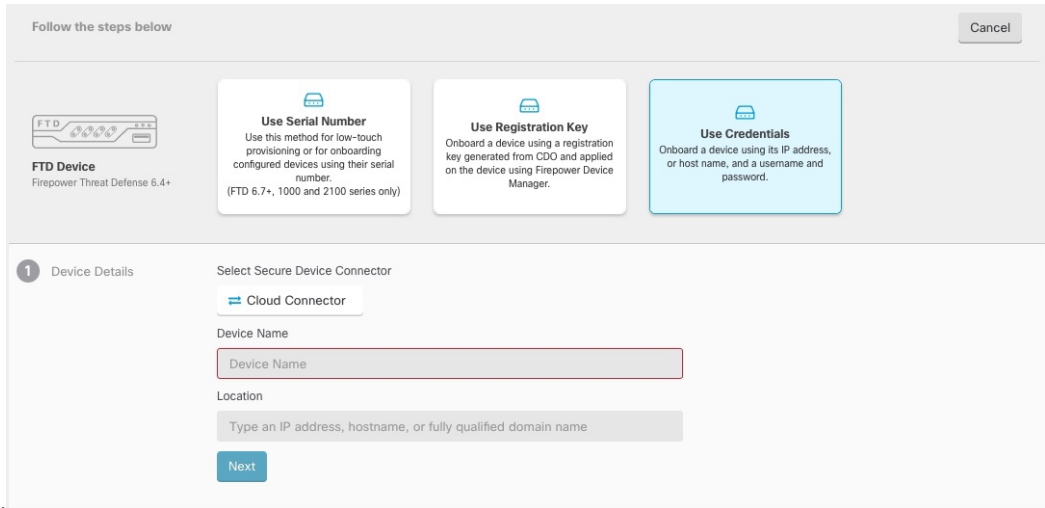
단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼 을 클릭하여 디바이스를 온보딩합니다.

단계 3 **FTD**를 클릭합니다.

Important

FDM 관리 디바이스 온보딩을 시도하면 CDO는 테넌트에 대한 일회성 활동인 Secure Firewall Threat Defense EULA(엔드 유저 라이선스 동의서)를 읽고 동의하라는 메시지를 표시합니다. EULA에 동의하면 CDO는 EULA가 변경되지 않는 한 동의하라는 메시지를 다시 표시하지 않습니다.

단계 4 온보딩 마법사에서 **Use Credentials(자격 증명 사용)**를 클릭합니



다.

단계 5 디바이스 세부 정보 단계에서 다음을 수행합니다.

- **Secure Device Connector(보안 디바이스 커넥터)** 버튼을 클릭하고 네트워크에 설치된 SDC(보안 디바이스 커넥터)를 선택합니다. SDC를 사용하지 않으려면 CDO는 Cloud Connector를 사용하여 FDM 관리 디바이스에 연결할 수 있습니다. 선택은 **CDO를 매니지드 디바이스에 연결**하는 방법에 따라 달라집니다.
- **Device Name(디바이스 이름)** 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.
- **Location(위치)** 필드에 디바이스 관리에 사용 중인 인터페이스의 IP 주소, 호스트 이름 또는 디바이스의 정규화된 도메인 이름을 입력합니다. 기본 포트는 443입니다.

Important SecureX 또는 Cisco Threat Response(CTR) 계정이 이미 있는 경우, 디바이스를 SecureX에 등록하려면 CDO 테넌트와 SecureX/CTR 계정을 병합해야 합니다. SecureX 포털을 통해 어카운트를 병합할 수 있습니다. 자세한 내용은 **CDO 및 SecureX 계정 병합**을 참조하십시오. 어카운트가 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 활용할 수 없습니다.

단계 6 Database Updates(데이터베이스 업데이트) 영역에서 **Immediately perform security updates, and enable recurring updates(즉시 보안 업데이트를 수행하고 반복 업데이트 활성화)**가 기본적으로 활성화됩니다. 이 옵션은 보안 업데이트를 즉시 트리거할 뿐 아니라 매주 월요일 오전 2시에 추가 업데이트를 확인하도록 디바이스를 자동으로 예약합니다. 자세한 내용은 **FTD 보안 데이터베이스 업데이트 및 보안 데이터베이스 업데이트 예약**을 참조하십시오.

이 옵션을 비활성화해도 FDM을 통해 구성했을 수 있는 이전에 예약된 업데이트에는 영향을 주지 않습니다.

Next(다음)를 클릭합니다.

단계 7 디바이스 관리자의 사용자 이름과 비밀번호를 입력하고 **Next(다음)**를 클릭합니다.

- 단계 8 디바이스의 Secure Firewall device manager에 보류 중인 변경 사항이 있는 경우 알림이 표시되며, 변경 사항을 되돌리거나 관리자에 로그인하여 보류 중인 변경 사항을 구축할 수 있습니다. Secure Firewall device manager에 보류 중인 변경 사항이 없으면 프롬프트가 표시되지 않습니다.
- 단계 9 (선택 사항) 디바이스의 레이블을 추가합니다. 자세한 내용은 [레이블 및 레이블 그룹](#)을 참조하십시오.

등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩

이 절차에서는 등록 키를 사용하여 FDM 관리 디바이스를 온보딩하는 방법을 설명합니다. 이 방법은 Cisco Defense Orchestrator에 FDM 관리 디바이스를 온보딩하는 데 권장되는 방법이고 DHCP를 사용하여 FDM 관리에 IP 주소를 할당한 경우 유용합니다. 어떤 이유로 해당 IP 주소가 변경되더라도 FDM 관리 디바이스는 CDO에 연결된 상태로 유지됩니다. 또한 FDM 관리 디바이스는 로컬 영역 네트워크에 주소를 가질 수 있으며 외부 네트워크에 액세스할 수 있는 한 이 방법을 사용하여 CDO에 온보딩할 수 있습니다.



Warning

이미 SecureX 또는 CTR(Cisco Threat Response) 계정이 있는 경우 디바이스를 SecureX에 등록하려면 CDO 테넌트와 SecureX/CTR 계정을 병합해야 합니다. 계정이 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 이용할 수 없습니다. SecureX에서 CDO 모듈을 생성하기 전에 계정을 병합하는 것을 강력히 권장합니다. SecureX 포털을 통해 계정을 병합할 수 있습니다. 자세한 내용은 [어카운트 병합](#)을 참조하십시오.

온보딩 전

- 버전 6.4를 실행하는 고객의 경우 이 온보딩 방법은 미국 지역(defenseorchestrator.com)에서만 지원됩니다.
- 버전 6.4를 실행하고 EU 지역(defense Orchestrator.eu)에 연결하는 고객의 경우 [사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩](#)를 사용하여 디바이스를 온보딩해야 합니다.
- 버전 6.5 이상을 실행하고 US, EU 또는 APJC 지역(apj.cdo.cisco.com) 지역에 연결하는 고객은 이 온보딩 방법을 사용할 수 있습니다.
- CDO를 FDM 관리 디바이스에 연결하는 데 필요한 네트워크 요구 사항에 대해서는 [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#)를 검토하십시오.
- Secure Firewall Management Center가 아닌 Secure Firewall device manager에서 디바이스를 관리하는지 확인합니다.
- 버전 6.4 및 6.5를 실행하는 디바이스는 등록 키로 온보딩하기 전에 Cisco Smart Software Manager에 등록하지 않아야 합니다. CDO에 온보딩하기 전에 해당 FDM 관리의 스마트 라이선스를 등록 취소해야 합니다. 아래의 "스마트 라이선스 Firewall Device Manager 등록 취소"를 참조하십시오.
- 디바이스에서 90일 평가판 라이선스를 사용 중일 수 있습니다.
- FDM 관리 디바이스에 로그인하고 디바이스에서 대기 중인 변경 사항이 없는지 확인합니다.

- DNS가 FDM 관리 디바이스에 올바르게 구성되어 있는지 확인합니다.
- FDM 관리 디바이스에서 시간 서비스가 올바르게 구성되었는지 확인합니다.
- FDM 관리 디바이스에 올바른 날짜 및 시간이 표시되는지 확인합니다. 그렇지 않으면 온보딩이 실패합니다.

다음 작업

다음 두 가지 중 하나를 수행합니다.

- 이미 스마트 라이선스가 있는 경우 Cisco Smart Software Manager에서 FDM 관리 디바이스 등록을 취소합니다. 등록 키를 사용하여 CDO에 온보딩하기 전에 Cisco Smart Software Manager에서 디바이스를 등록 취소해야 합니다. [스마트 라이선스 FDM-관리 디바이스 등록 취소, on page 13](#)를 계속합니다.
- 디바이스에 스마트 라이선스가 없는 경우 등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스를 온보딩하는 절차, [on page 14](#)을 계속 진행합니다.

스마트 라이선스 FDM-관리 디바이스 등록 취소

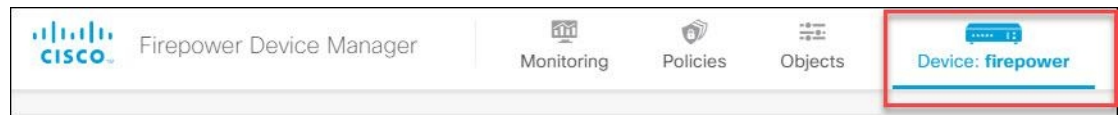
온보딩하려는 디바이스가 버전 6.4 또는 6.5를 실행 중이고, 이미 스마트 라이선스가 있는 경우, 해당 디바이스는 Cisco Smart Software Manager에 등록되어 있을 가능성이 높습니다. 등록 키를 사용하여 CDO에 온보딩하기 전에 Cisco Smart Software Manager에서 디바이스를 등록 취소해야 합니다. 등록을 취소하면 디바이스에 연결된 기본 라이선스 및 선택 가능한 모든 라이선스가 가상 어카운트에서 해제됩니다.

디바이스를 등록 취소한 후에도 디바이스의 현재 컨피그레이션 및 정책은 계속 원래대로 작동하지만 변경을 수행하거나 변경 사항을 구축할 수는 없습니다.

Procedure

단계 1 Secure Firewall device manager를 사용하여 디바이스에 로그인합니다.

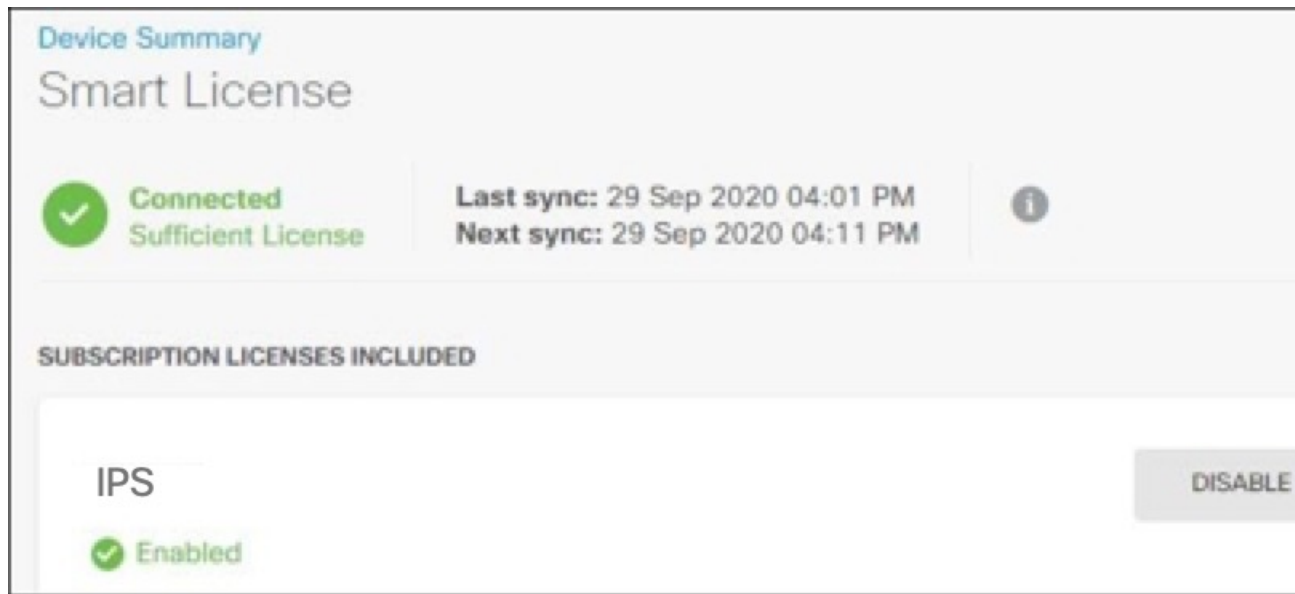
단계 2 상단 탭에서 디바이스 아이콘을 클릭합니다.



단계 3 Smart License(스마트 라이선스) 영역에서 View Configuration(구성 보기)을 클릭합니다.

단계 4 Go to Cloud Services(클라우드 서비스로 이동) 기어 메뉴를 클릭하고 Unregister Device(디바이스 등록 취소)를 선택합니다.

등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스를 온보딩하는 절차



단계 5 경고를 확인한 후에 디바이스를 등록 취소하려면 **Unregister**(등록 취소)를 클릭합니다.

What to do next


CDO에 온보딩하기 위해 등록을 취소한 경우 [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스를 온보딩하는 절차, on page 14](#)로 계속합니다.

등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스를 온보딩하는 절차
등록 키를 사용하여 FDM 관리를 온보딩하려면 다음 절차를 수행합니다.

Before you begin

[등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩, on page 12](#)에서 설명하는 사전 요건을 검토하십시오.

Procedure

- 단계 1 CDO에 로그인합니다.
- 단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.
- 단계 3 **FTD**를 클릭합니다.

Important FDM 관리 디바이스를 온보딩하려고 하면 Cisco Defense Orchestrator에서 Firepower Threat Defense EULA(최종 사용자 라이선스 계약)를 읽고 동의하라는 메시지가 표시됩니다. 이는 테넌트의 일회성 활동입니다. 이 동의서에 동의하면 CDO는 후속 FDM 관리 온보딩에서 이를 다시 확인하지 않습니다. 나중에 EULA 계약이 변경되는 경우 메시지가 표시되면 다시 동의해야 합니다.

단계 4 Onboard FTD Device(온보드 FTD 디바이스) 화면에서 Use Registration Key(등록 키 사용)를 클릭합니다.


단계 5 Device Name(디바이스 이름) 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.

단계 6 Database Updates(데이터베이스 업데이트) 영역에서 Immediately perform security updates, and enable recurring updates(즉시 보안 업데이트를 수행하고 반복 업데이트 활성화) 옵션이 기본적으로 활성화됩니다. 이 옵션은 보안 업데이트를 즉시 트리거할 뿐 아니라 매주 월요일 오전 2시에 추가 업데이트를 확인하도록 디바이스를 자동으로 예약합니다. 자세한 내용은 FTD 보안 데이터베이스 업데이트 및 보안 데이터베이스 업데이트 예약을 참조하십시오.

Note 이 옵션을 비활성화해도 Secure Firewall device manager을 통해 구성했을 수 있는 이전에 예약된 업데이트에는 영향을 주지 않습니다.

단계 7 Create Registration Key(등록 키 생성) 영역에서 CDO가 등록 키를 생성합니다.

Note 키가 생성된 후 디바이스가 완전히 온보딩되기 전에 온보딩 화면에서 나갈 경우, 온보딩 화면으로 돌아갈 수 없습니다. 그러나 CDO는 Inventory(재고 목록) 페이지에서 해당 디바이스에 대한 자리 표시자를 생성합니다. 디바이스의 자리 표시자를 선택하면 오른쪽에 있는 작업 창에서 해당 디바이스의 키를 볼 수 있습니다.

단계 8 Copy(복사) 아이콘  을 클릭하여 등록 키를 복사합니다.

Note 등록 키 복사를 건너뛰고 Next(다음)를 클릭하여 디바이스에 대한 자리 표시자 항목을 완료한 다음 나중에 디바이스를 등록할 수 있습니다. 이 옵션은 디바이스를 먼저 생성하고 나중에 디바이스를 등록하려는 경우 또는 고객 네트워크에 POV(Proof of Value) 디바이스를 설치하는 Cisco 파트너인 경우 유용합니다.

Inventory(재고 목록) 페이지에서 디바이스가 현재 연결 상태인 "Unprovisioned(프로비저닝되지 않음)"에 있음을 확인할 수 있습니다. Unprovisioned(프로비저닝되지 않음) 아래에 표시되는 등록 키를 Firewall Device Manager에 복사하여 온보딩 프로세스를 완료합니다.

단계 9 CDO에 온보딩하려는 디바이스의 Secure Firewall device manager에 로그인합니다.

단계 10 System Settings(시스템 설정)에서 Cloud Services(클라우드 서비스)를 클릭합니다.

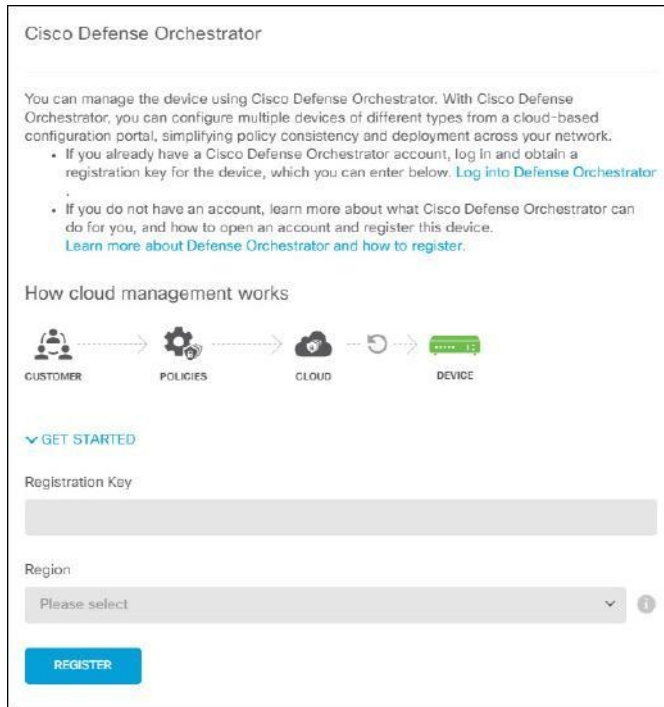
단계 11 CDO 타일에서 Get Started(시작하기)를 클릭합니다.

단계 12 Region(지역) 필드에서 테넌트가 할당된 Cisco Cloud 지역을 선택합니다.

- defenseorchestrator.com에 로그인하는 경우 US를 선택합니다.
- defenseorchestrator.eu에 로그인하는 경우 EU를 선택합니다.
- apj.cdo.cisco.com에 로그인하는 경우 APJ를 선택합니다.

Note 이 단계는 버전 6.4를 실행하는 FDM 관리 디바이스에는 적용되지 않습니다.

단계 13 Registration Key(등록 키) 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.



단계 14 Register(등록)를 클릭한 다음, **Accept Cisco Disclosure(Cisco 공개 동의)**를 클릭합니다.

단계 15 CDO으로 돌아갑니다. 디바이스에 적용할 모든 라이선스를 선택합니다.

자세한 내용은 [스마트 라이선스 적용 또는 업데이트](#)를 참조하십시오. **Skip(건너뛰기)**을 클릭하여 90일 평가 라이선스로 온보딩을 계속할 수도 있습니다.

단계 16 CDO로 돌아가 **Inventory(재고 목록)** 페이지를 열고 디바이스 상태가 "Unprovisioned(프로비저닝되지 않음)"에서 "Locating(찾기 중)", "Syncing(동기화 중)"에서 "Synced(동기화됨)"로 진행되는지 확인합니다.

등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩

이 절차에서는 등록 키를 사용하여 버전 6.6 이상을 실행하는 FDM 관리 디바이스를 온보딩하는 방법을 설명합니다. 이 방법은 FDM 관리 디바이스를 Cisco Defense Orchestrator에 온보딩하는 데 권장되는 방법이며 DHCP를 사용하여 FDM 매니지드 디바이스에 IP 주소가 할당된 경우에 유용합니다. 어떤 이유로 해당 IP 주소가 변경되더라도 FDM 관리 디바이스는 CDO에 연결된 상태로 유지됩니다. 또한 FDM 관리 디바이스는 로컬 영역 네트워크에 주소를 가질 수 있으며 외부 네트워크에 액세스할 수 있는 한 이 방법을 사용하여 CDO에 온보딩할 수 있습니다.

**Warning**

이미 SecureX 또는 CTR(Cisco Threat Response) 계정이 있는 경우 디바이스를 SecureX에 등록하려면 CDO 테넌트와 SecureX/CTR 계정을 병합해야 합니다. 계정이 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 이용할 수 없습니다. SecureX에서 CDO 모듈을 생성하기 전에 계정을 병합하는 것을 강력히 권장합니다. SecureX 포털을 통해 계정을 병합할 수 있습니다. 자세한 내용은 [어카운트 병합](#)을 참조하십시오.

버전 6.4 또는 6.5를 실행하는 FDM 관리 디바이스를 온보딩하려면 [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.

온보딩 전

- 이 온보딩 방법은 현재 버전 6.6 이상과 [defenceorchestrator.com](#), [defenceorchestrator.eu](#) 및 [apj.cdo.cisco.com](#)에 연결하는 고객이 사용할 수 있습니다.
- CDO를 FDM 관리 디바이스에 연결하는 데 필요한 네트워크 요구 사항에 대해서는 [매니지드 디바이스에 Cisco Defense Orchestrator 연결](#)를 검토하십시오.
- Secure Firewall Management Center가 아닌 Secure Firewall device manager에서 디바이스를 관리하는지 확인합니다.
- 디바이스는 90일 평가 라이선스를 사용하거나 스마트 라이선스를 사용할 수 있습니다. 버전 6.6 이상을 실행하는 디바이스는 설치된 스마트 라이선스의 등록을 취소하지 않고 등록 키를 사용하여 CDO에 온보딩할 수 있습니다.
- 디바이스를 Cisco Cloud 서비스에 이미 등록할 수 없습니다. 온보딩하기 전에 아래의 "Cisco Cloud Services에서 FDM-관리 디바이스 등록 취소"를 참조하십시오.
- 디바이스의 Secure Firewall device manager UI에 로그인하고 디바이스에서 대기 중인 변경 사항이 없는지 확인합니다.
- DNS가 FDM 관리 디바이스에 올바르게 구성되어 있는지 확인합니다.
- FDM 관리 디바이스에서 시간 서비스가 구성되었는지 확인합니다.
- FDM 관리 디바이스에 올바른 날짜 및 시간이 표시되는지 확인합니다. 그렇지 않으면 온보딩이 실패합니다.

다음 작업:

다음 중 하나를 수행합니다.

- 버전 6.6 이상을 실행하는 FDM 관리 디바이스가 이미 Cisco Cloud Services에 등록된 경우 온보딩하기 전에 디바이스 등록을 취소해야 합니다. [Cisco Cloud Services에서 FDM-관리 디바이스 등록 취소](#), [on page 18](#)를 진행합니다.
- 디바이스가 Cisco Cloud Services에 등록되지 않은 경우 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차](#), [on page 19](#)를 계속 진행합니다.

Cisco Cloud Services에서 FDM-관리 디바이스 등록 취소

다음 절차는 Cisco Cloud Services에서 디바이스를 등록 취소하기 위한 것입니다. 등록 키를 사용하여 FDM 관리 디바이스를 CDO에 온보딩하기 전에 이 방법을 사용합니다.



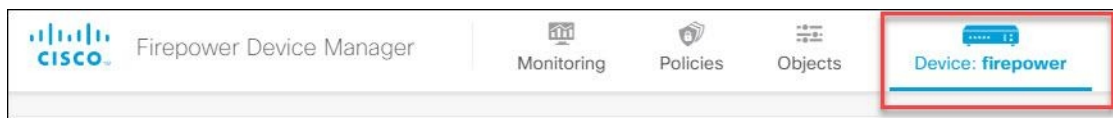
Note 버전 7.0 이상을 실행하는 가상 FDM 관리 디바이스를 온보딩하는 경우 가상 FDM 관리 디바이스를 CDO에 등록하면 성능 계층화된 스마트 라이선싱 선택 항목이 기본 계층인 **Variable(변수)**로 자동 재설정됩니다. 온보딩 후 Secure Firewall device manager UI를 통해 디바이스에 연결된 라이선스와 일치하는 계층을 수동으로 다시 선택해야 합니다.

이 절차를 사용하여 Cisco Cloud Services에 등록되지 않았는지 확인합니다.

Procedure

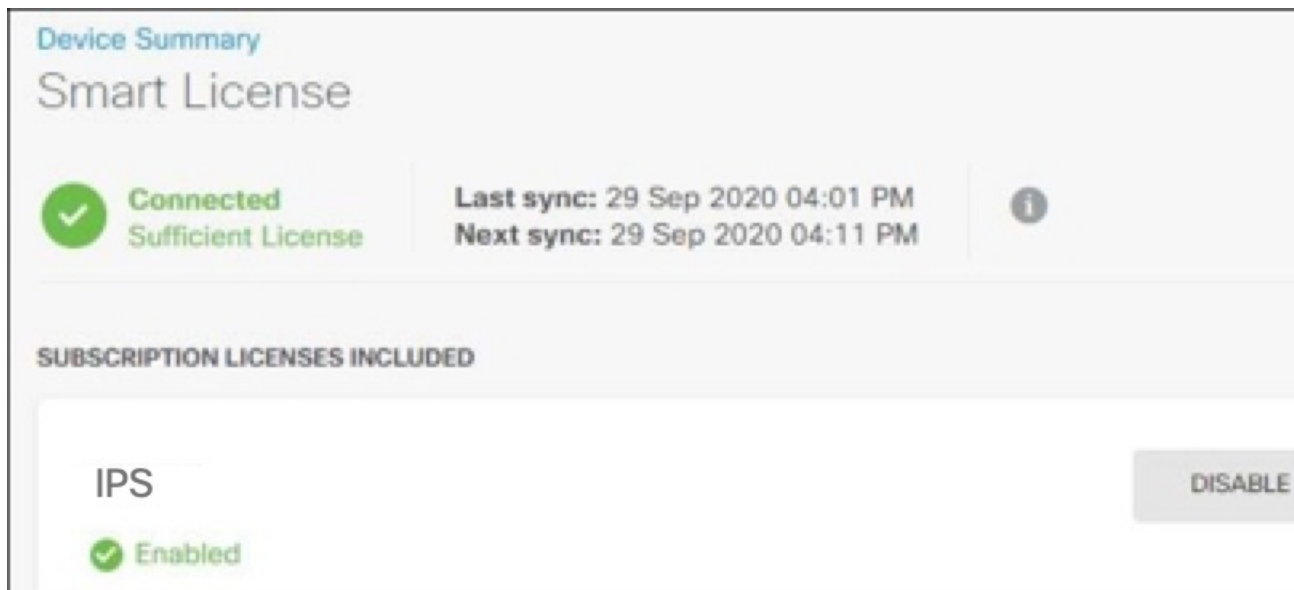
단계 1 Secure Firewall device manager를 사용하여 디바이스에 로그인합니다.

단계 2 상단 탭에서 디바이스 아이콘을 클릭합니다.



단계 3 **System Settings**(시스템 설정) 메뉴를 확장한 다음 **Cloud Services**(클라우드 서비스)를 클릭합니다.

단계 4 **Cloud Services**(클라우드 서비스) 페이지에서 기어 메뉴를 클릭하고 **Unregister Cloud Services**(클라우드 서비스 등록 취소)를 선택합니다.



단계 5 경고를 확인한 후에 디바이스를 등록 취소하려면 **Unregister**(등록 취소)를 클릭합니다.

What to do next


버전 6.6 이상을 실행하는 FDM 관리 디바이스를 온보딩하려는 경우 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차, on page 19](#)을 계속 진행하십시오.

등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차

등록 키를 사용하여 FDM 관리 디바이스를 온보딩하려면 다음 절차를 수행합니다.

Procedure

단계 1 CDO에 로그인합니다.

단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.

단계 3 **FTD**를 클릭합니다.

Important FDM 관리 디바이스 온보딩을 시도하면 Cisco Defense Orchestrator에서는 테넌트에 대한 일회성 활동인 EULA(엔드 유저 라이선스 동의서)를 읽고 동의하라는 메시지를 표시합니다. 이 동의서에 동의하면 CDO는 후속 온보딩에서 이를 다시 확인하지 않습니다. 나중에 EULA 계약이 변경되는 경우 메시지가 표시되면 다시 동의해야 합니다.

단계 4 **Onboard FTD Device**(온보드 FTD 디바이스) 화면에서 **Use Registration Key**(등록 키 사용)를 클릭합니다.


단계 5 **Device Name**(디바이스 이름) 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.

단계 6 **Database Updates**(데이터베이스 업데이트) 영역에서 **Immediately perform security updates, and enable recurring updates**(즉시 보안 업데이트를 수행하고 반복 업데이트 활성화)가 기본적으로 활성화됩니다. 이 옵션은 보안 업데이트를 즉시 트리거할 뿐 아니라 매주 월요일 오전 2시에 추가 업데이트를 확인하도록 디바이스를 자동으로 예약합니다. 자세한 내용은 [FTD 보안 데이터베이스 업데이트](#) 및 [보안 데이터베이스 업데이트 예약](#)을 참조하십시오.

Note 이 옵션을 비활성화해도 Secure Firewall device manager를 통해 구성했을 수 있는 이전에 예약된 업데이트에는 영향을 주지 않습니다.

단계 7 **Create Registration Key**(등록 키 생성) 단계에서 CDO가 등록 키를 생성합니다.

Note 키가 생성된 후 디바이스가 완전히 온보딩되기 전에 온보딩 화면에서 나갈 경우, 온보딩 화면으로 돌아갈 수 없습니다. 그러나 CDO는 **Inventory**(재고 목록) 페이지에서 해당 디바이스에 대한 자리 표시자를 생성합니다. 디바이스의 자리 표시자를 선택하면 해당 페이지에서 해당 디바이스의 키를 볼 수 있습니다.

단계 8 Copy(복사) 아이콘  을 클릭하여 등록 키를 복사합니다.

등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차

Note 등록 키 복사를 건너뛰고 **Next(다음)**를 클릭하여 디바이스에 대한 자리 표시자 항목을 완료한 다음 나중에 디바이스를 등록할 수 있습니다. 이 옵션은 디바이스를 먼저 생성하고 나중에 디바이스를 등록하려는 경우 또는 고객 네트워크에 POV(Proof of Value) 디바이스를 설치하는 Cisco 파트너인 경우 유용합니다.

Inventory(재고 목록) 페이지에서 디바이스가 현재 연결 상태인 "Unprovisioned(프로비저닝되지 않음)"에 있음을 확인할 수 있습니다. **Unprovisioned(프로비저닝되지 않음)** 아래에 표시되는 등록 키를 Firewall Device Manager에 복사하여 온보딩 프로세스를 완료합니다.

단계 9 온보딩 중인 디바이스의 Secure Firewall device manager에 로그인합니다.

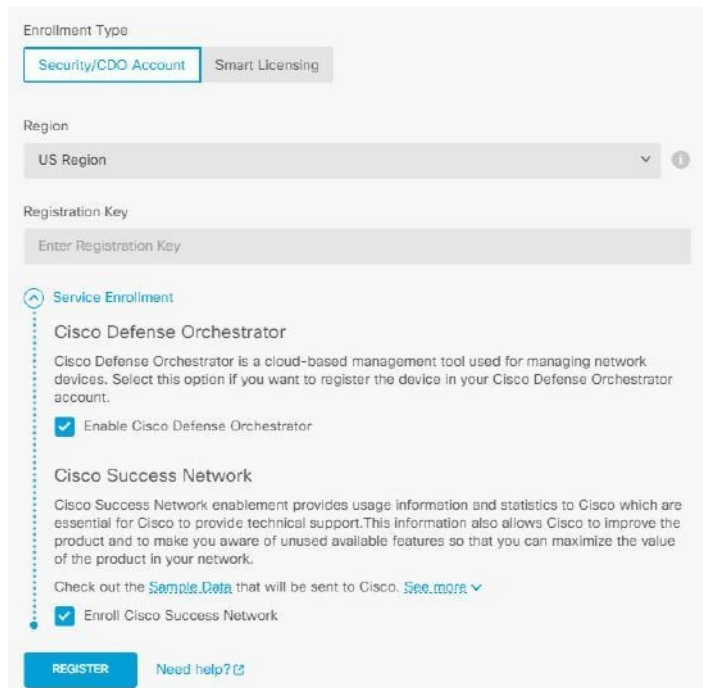
단계 10 **System Settings(시스템 설정)**에서 **Cloud Services(클라우드 서비스)**를 클릭합니다.

단계 11 **Region(지역)** 필드에서 테넌트가 할당된 Cisco Cloud 지역을 선택합니다.

- defenseorchestrator.com에 로그인하는 경우 US를 선택합니다.
- defenseorchestrator.eu에 로그인하는 경우 EU를 선택합니다.
- apj.cdo.cisco.com에 로그인하는 경우 APJ를 선택합니다.

단계 12 **Enrollment Type(등록 유형)** 영역에서 **Security Account(보안 어카운트)**를 클릭합니다.

Note 버전 6.6을 실행하는 디바이스의 경우 CDO의 Tenancy(테넌시) 탭 제목이 **Security Account(보안 계정)**이며 Secure Firewall device manager에서 CDO를 수동으로 활성화해야 합니다.



단계 13 **Registration Key(등록 키)** 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.

- 단계 14 버전 6.7 이상을 실행하는 디바이스의 경우, Service Enrollment(서비스 등록) 영역에서 **Enable Cisco Defense Orchestrator(Cisco Defense Orchestrator 활성화)**를 선택합니다.
- 단계 15 Cisco Success Network 등록에 대한 정보를 검토합니다. 참여하지 않으려면 **Enroll Cisco Success Network(Cisco Success Network 등록)** 확인란의 선택을 취소합니다.
- 단계 16 **Register(등록)**를 클릭한 다음 Cisco 고지 사항을 수락합니다. Secure Firewall device manager는 CDO에 등록 요청을 보냅니다.
- 단계 17 CDO로 돌아가 **Create Registration Key(등록 키 생성)** 영역에서 **Next(다음)**를 클릭합니다.
- 단계 18 디바이스에 적용할 모든 라이선스를 선택합니다. **Next(다음)**를 클릭합니다.
- 단계 19 CDO로 돌아가 **Inventory(재고 목록)** 페이지를 열고 디바이스 상태가 "Unprovisioned(프로비저닝되지 않음)"에서 "Locating(찾기 중)", "Syncing(동기화 중)"에서 "Synced(동기화됨)"로 진행되는지 확인합니다.

디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩

이 절차는 FDM 관리 디바이스를 Cisco Defense Orchestrator에 온보딩하고 설정하는 간소화된 방법입니다. 디바이스의 새시 일련 번호 또는 PCA 일련 번호만 있으면 됩니다. 디바이스를 온보딩할 때 스마트 라이선스를 적용하거나 90일 평가 라이선스를 사용할 수 있습니다.

[로우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건](#)을 수행하기 전에 활용 사례를 읽고 개념을 이해해야 합니다.



Important 이러한 FDM 관리 디바이스를 온보딩하는 방법은 버전 6.7 이상을 실행하는 디바이스에서만 사용할 수 있습니다.

활용 사례

- [디바이스의 일련 번호를 사용하여 FDM-관리 디바이스 온보딩, on page 21](#): 네트워크에 추가되고 인터넷에서 연결되는 새로운 공장 출하 FDM 관리 디바이스를 온보딩합니다. 디바이스에서 초기 디바이스 설정 마법사가 완료되지 않았습니다.
- [디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩, on page 28](#): 이미 구성된 FDM 관리 디바이스 또는 네트워크에 이미 추가되고 인터넷에서 연결되는 업그레이드된 디바이스를 온보딩합니다. 디바이스에서 초기 디바이스 설정 마법사가 완료되었습니다.



Important 이 방법을 사용하여 디바이스에 대해 지원되는 이전 소프트웨어 버전에서 실행 중인 디바이스를 온보딩하려면 업그레이드 대신 해당 디바이스에서 소프트웨어를 새로 설치(리이미징)해야 합니다.

관련 정보:

- [용어 및 정의](#)
- [일련 번호를 사용하여 FDM 매니저드 디바이스 온보딩 문제 해결](#)

로우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건

로우터치 프로비저닝은 새로운 Firepower 1000, Firepower 2100 또는 Secure Firewall 3100 시리즈 디바이스를 자동으로 프로비저닝 및 구성하여, CDO에 디바이스를 온보딩하는 것과 관련된 대부분의 수동 작업을 제거하는 기능입니다. 로우터치 프로비저닝은 직원이 네트워크 디바이스 사용 경험이 적은 원격 사무실 또는 기타 위치를 위한 것입니다.

로우터치 프로비저닝 프로세스를 사용하려면, 디바이스를 CDO에 온보딩하고 인터넷에 연결할 수 있는 네트워크에 연결한 다음 디바이스의 전원을 켭니다. 자세한 내용은 [디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩, on page 28](#)을 참조하십시오.



Note CDO에 온보딩하기 전이나 후에 디바이스의 전원을 켤 수 있습니다. 먼저 디바이스를 CDO에 온보딩하고 디바이스의 전원을 켜 다음 브랜치 네트워크에 연결하는 것이 좋습니다. CDO에서 디바이스를 온보딩하면 디바이스가 Cisco Cloud의 CDO 테넌트 및 CDO와 연결되고 자동으로 디바이스 구성이 동기화됩니다.

이 절차를 사용하여 외부 공급업체에서 구매한 디바이스를 온보딩하거나 다른 지역의 다른 클라우드 테넌트에서 이미 관리하는 디바이스를 온보딩할 수도 있습니다. 그러나 디바이스가 이미 외부 벤더의 클라우드 테넌트 또는 다른 지역의 클라우드 테넌트에 등록된 경우 CDO는 디바이스를 온보딩하지 않지만 "*Device serial number already claimed*(디바이스 일련 번호가 이미 클레임됨)" 오류 메시지를 표시합니다. 이러한 경우 CDO 관리자는 이전 클라우드 테넌트에서 디바이스의 일련 번호를 등록 취소한 다음 자신의 테넌트에서 CDO 디바이스를 클레임해야 합니다. 문제 해결 장에서 [디바이스 일련 번호가 이미 클레임됨](#)을 참조하십시오.

디바이스 연결 상태가 "Online(온라인)"으로 변경되고 구성 상태가 "Synced(동기화됨)"로 변경됩니다. FDM 관리 디바이스가 CDO에 온보딩됩니다.

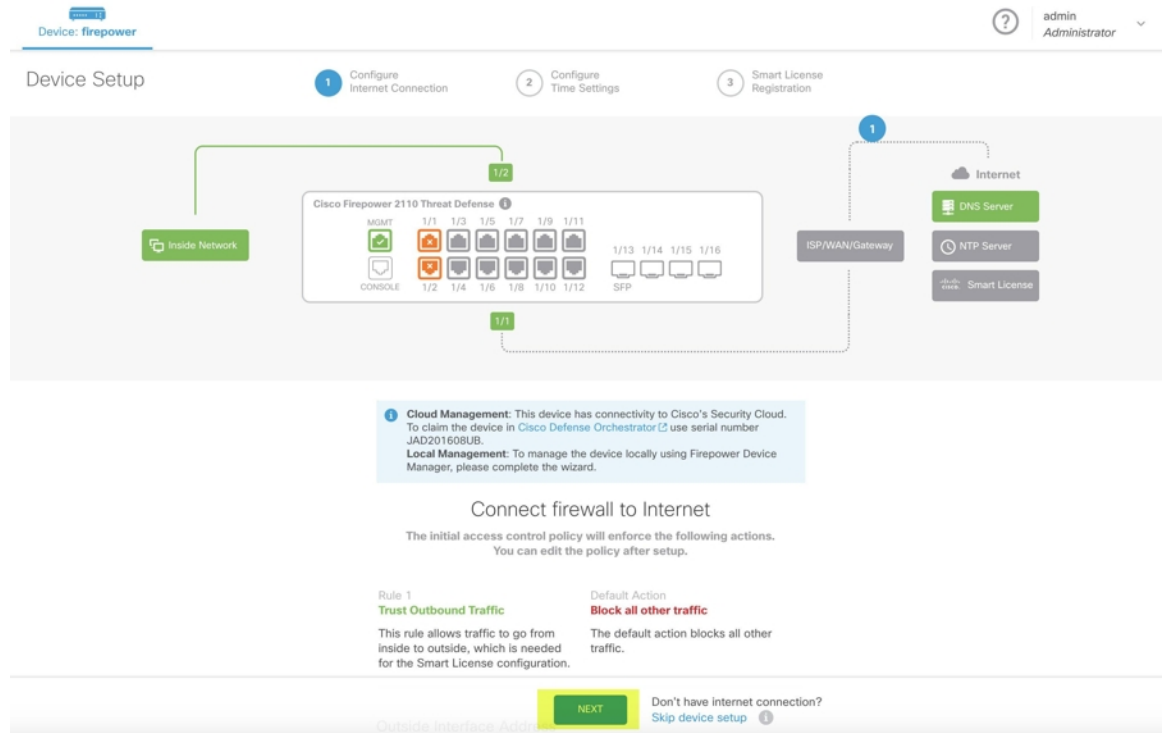
하드웨어 후면 패널에서 상태 LED(Firepower 1010), SYS LED(Firepower 2100) 또는 S LED(Secure Firewall 3100)가 녹색으로 깜박이는 것을 볼 수 있습니다. 클라우드에 연결되면 디바이스 LED가 녹색으로 계속 깜박입니다. 디바이스가 Cisco cloud에 연결할 수 없거나 연결 후 연결이 끊어지면 상태 LED(Firepower 1010), SYS LED(Firepower 2100) 또는 M LED(Secure Firewall 3100)가 녹색과 황색으로 번갈아 깜박이는 것을 볼 수 있습니다.

LED 표시등을 이해하려면 [로우터치 프로비저닝을 사용하여 Cisco Firepower 방화벽 설치](#) 비디오를 참조하십시오.



Important FDM 관리 디바이스 콘솔, SSH 또는 Secure Firewall Threat Defense에 로그인한 경우, 첫 번째 로그인 시 디바이스의 비밀번호를 변경했을 것입니다. CDO를 사용하여 디바이스를 온보딩하는 데도 로우터치 프로비저닝 프로세스를 사용할 수 있습니다. Secure Firewall Threat Defense에 로그인한 후에는 외부 인터페이스를 구성하는 디바이스 설정 마법사 단계를 완료하지 마십시오. 이 단계를 완료하면 디바이스가 클라우드에서 등록 취소되고 로우터치 프로비저닝 프로세스를 사용할 수 없습니다.

Secure Firewall Threat Defense에 로그인하면 대시보드에 다음 화면이 표시됩니다.



Secure Firewall Threat Defense UI에서 더 이상 진행하지 않고 일련 번호 온보딩 마법사로 이동하여 디바이스를 온보딩합니다. 디바이스 비밀번호가 이미 변경되었으므로, 여기서 **Default Password Changed**(기본 비밀번호 변경됨)를 선택해야 합니다.

사전 요건

소프트웨어 및 하드웨어 요구 사항

FDM 관리 디바이스는 일련 번호 온보딩을 지원하는 소프트웨어를 실행해야 합니다. 다음 표를 가이드로 사용합니다.

Table 1: 하드웨어 및 소프트웨어 지원

로우 터치(Low-Touch) 프로비저닝을 지원하는 방화벽 모델 번호	지원되는 방화벽 소프트웨어 버전	소프트웨어 패키지
Firepower 1000 시리즈 디바이스 모델: 1010, 1120, 1140, 1150	6.7 이상	SF-F1K-TDx.x-K9
Firepower 2100 시리즈 디바이스 모델: 2110, 2120, 2130, 2140	6.7 이상	SF-F2K-TDx.x-K9
Secure Firewall 3100 시리즈 디바이스 모델: 3110, 3120, 3130, 3140	7.1 이상	SF-F3K-TDx.x-K9

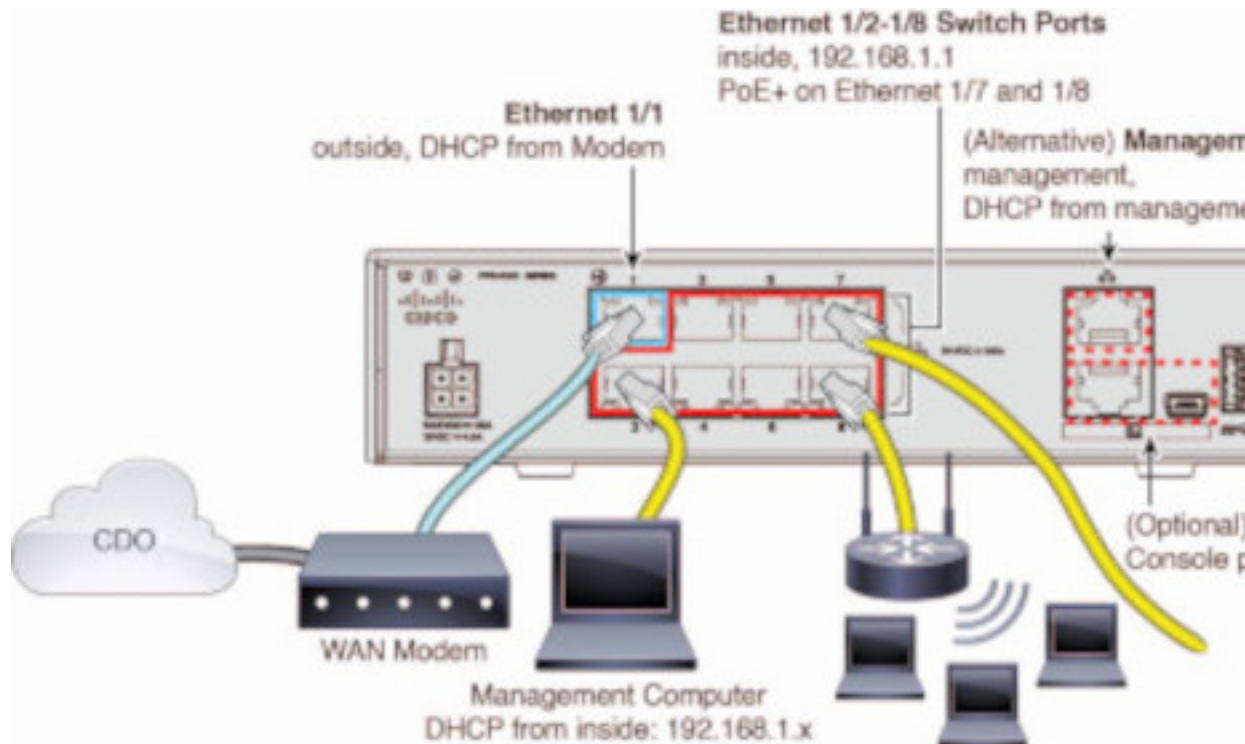
관리 플랫폼이 올바른 버전을 실행 중인지 확인합니다.

Table 2: FTD Manager 버전 지원

매니저	지원되는 버전
Secure Firewall Device Manager	7.0 이상
온프레미스 Firewall Management Center	7.2 이상
클라우드 사용 Firewall Management Center	해당 없음

하드웨어 설치를 위한 구성 사전 요건

- 브랜치 오피스에 있는 네트워크는 **192.168.1.0/24** 어드레스 스페이스를 사용할 수 없습니다. 이더넷 1/1 (외부)의 네트워크는 192.168.1.0/24 어드레스 스페이스를 사용할 수 없습니다. FTD 6.7을 실행하는 1000 및 2100 Series 디바이스에서 이더넷 1/2 "내부" 인터페이스의 기본 IP 주소는 192.168.1.1이며, 해당 서브넷에 있는 경우 WAN 모뎀이 할당한 DHCP 주소와 충돌할 수 있습니다.
 - 내부—이더넷 1/2, IP 주소 192.168.1.1
 - 외부—이더넷 1/1, DHCP의 IP 주소 또는 설정 중 지정하는 주소



외부 인터페이스 설정을 변경할 수 없는 경우, 충돌을 방지하기 위해 Secure Firewall device manager를 사용하여 이더넷 1/2 "내부" 인터페이스 설정의 서브넷을 변경합니다. 예를 들어 다음 서브넷 설정으로 변경할 수 있습니다.

- IP 주소: 192.168.95.1
- DHCP 서버 범위: 192.168.95.5-192.168.95.254

물리적 인터페이스를 구성하는 단계에 대해 알아보려면 "[Secure Firewall Device Manager 구성 가이드](#)"를 참조하십시오. "인터페이스" 장에서 "물리적 인터페이스 구성" 섹션을 참조하십시오.

- 위협 방어 디바이스를 Cisco Cloud에 설치하고 연결해야 합니다.
- 디바이스의 외부 또는 관리 인터페이스는 DHCP 주소 지정을 제공하는 네트워크에 연결해야 합니다. 일반적으로 디바이스는 외부 또는 관리 인터페이스에 기본 DHCP 클라이언트가 있습니다.



Note 관리 인터페이스가 DHCP 서버가 있는 네트워크에 연결된 경우 Linux 스택 시작 트래픽에 대해 외부 인터페이스보다 우선적으로 적용됩니다.

- 외부 또는 관리 인터페이스에서 액세스해야 직렬 온보딩 방법을 위해 다음 보안 서비스 익스체인지 도메인에 액세스할 수 있습니다.
 - 미국 지역
 - api-sse.cisco.com
 - est.sco.cisco.com(전 지역 공통)
 - mx*.sse.itd.cisco.com(현재 mx01.sse.itd.cisco.com만)
 - dex.sse.itd.cisco.com(고객 성공용)
 - eventing-ingest.sse.itd.cisco.com(CTR 및 CDO용)
 - registration.us.sse.itd.cisco.com(지역 Cisco Cloud에 디바이스 등록 허용)
 - EU 지역
 - api.eu.sse.itd.cisco.com
 - est.sco.cisco.com(전 지역 공통)
 - mx*.eu.sse.itd.cisco.com(현재 mx01.eu.sse.itd.cisco.com만)
 - dex.eu.sse.itd.cisco.com(고객 성공용)
 - eventing-ingest.eu.sse.itd.cisco.com(CTR 및 CDO용)
 - registration.eu.sse.itd.cisco.com(지역 Cisco Cloud에 디바이스 등록 허용)
 - APJ 지역
 - api.apj.sse.itd.cisco.com
 - est.sco.cisco.com(전 지역 공통)
 - mx*.apj.sse.itd.cisco.com(현재 mx01.apj.sse.itd.cisco.com만)

- dex.apj.sse.itd.cisco.com(고객 성공용)
- eventing-ingest.apj.sse.itd.cisco.com(CTR 및 CDO용)
- <http://registration.apj.sse.itd.cisco.com>(지역 Cisco Cloud에 대한 디바이스 등록 허용)

• 디바이스의 외부 인터페이스에 Cisco Umbrella DNS에 대한 DNS 액세스 권한이 있어야 합니다.

CDO에서 디바이스를 클레임하기 전에

CDO에서 디바이스를 클레임하기 전에 다음 정보가 있는지 확인합니다.

- 위협 방어 디바이스의 새시 일련 번호 또는 PCA 번호입니다. 이 정보는 하드웨어 새시 하단 또는 디바이스가 배송된 상자에 있습니다. 다음 예시 그림에서 Firepower 1010 새시 하단의 일련 번호 "*****XOR9"를 볼 수 있습니다.



- 디바이스의 기본 비밀번호입니다.
- 추가 기능을 사용하기 위해 [Cisco Smart Software Manager](#)에서 생성된 스마트 라이선스입니다. 그러나 90일 평가 라이선스를 사용하여 디바이스 온보딩을 완료하고 나중에 스마트 라이선스를 적용할 수 있습니다.



Caution 디바이스가 Cisco Defense Orchestrator에서 온보딩되는 경우 Secure Firewall device manager를 사용하여 디바이스 간편 설정을 수행하지 않는 것이 좋습니다. 이로 인해 CDO에서 임시 오류가 발생합니다.

Before you begin

온프레미스 Management Center로 관리하려는 의도로 디바이스를 온보딩하는 경우 온프레미스 Management Center는 버전 7.4 이상을 실행해야 합니다. 이전 버전은 로우터치 프로비저닝을 지원하지 않습니다.

Procedure

-
- 단계 1 외부 벤더에서 구매한 디바이스를 온보딩하는 경우 먼저 디바이스를 이미지 재설치해야 합니다. 자세한 내용은 [Cisco FXOS 문제 해결 가이드](#)의 "이미지 재설치 절차" 장을 참조하십시오.
- 단계 2 CDO에 로그인합니다.
- 단계 3 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.
- 단계 4 **FTD tile**(타일)을 클릭합니다.
- Important** 디바이스 온보딩을 시도하면 CDO는 테넌트에 대한 일회성 활동인 EULA(엔드 유저 라이선스 동의서)를 읽고 동의하라는 메시지를 표시합니다. 이 동의서에 동의하면 CDO는 후속 온보딩에서 이를 다시 확인하지 않습니다. 나중에 EULA 계약이 변경되는 경우 메시지가 표시되면 다시 동의해야 합니다.
- 단계 5 **Onboard FTD Device**(온보드 FTD 디바이스) 화면에서 **Use Serial Number**(일련 번호 사용)를 클릭합니다.
- 단계 6 **FMC** 선택단계에서 드롭다운 메뉴를 사용하여 CDO에 이미 온보딩된 온프레미스 Management Center를 선택합니다. **Next**(다음)를 클릭합니다.
- 온프레미스 Management Center에서 버전 7.4 이상을 실행해야 합니다. 온프레미스 Management Center가 온보딩되지 않은 경우 온보딩 마법사에 대해 **+Onboard**(+온프레미스 FMC)를 클릭합니다.
- 단계 7 **Connection**(연결) 단계에서 디바이스의 일련 번호와 디바이스 이름을 입력합니다. **Next**(다음)를 클릭합니다.
- 단계 8 로우터치 프로비저닝의 경우 디바이스가 새 제품이어야 하거나 이미지를 다시 설치해야 합니다. **Password Reset**(비밀번호 재설정)의 경우 **Yes, this new device has never been logged into or configured for a manager**(예, 이 새 디바이스가 관리자에 로그인하거나 구성한 적이 없습니다.)를 선택해야 합니다. 새 비밀번호를 입력하고 디바이스의 새 비밀번호를 확인한 후 **Next**(다음)를 클릭합니다.
- 단계 9 **Policy Assignment**(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 사용자 지정 정책이 없는 경우 CDO는 기본 액세스 제어 정책을 자동으로 선택합니다. **Next**(다음)를 클릭합니다.
- 단계 10 디바이스에 적용할 모든 라이선스를 선택합니다. **Next**(다음)를 클릭합니다.
- 단계 11 (선택사항) 기기에 라벨을 추가합니다. CDO는 디바이스가 성공적으로 온보딩되면 이러한 레이블을 적용합니다.
-

What to do next

CDO에서는 디바이스 클레임을 시작하고, 오른쪽에 **Claiming**(클레임 중) 메시지가 표시됩니다. CDO에서는 디바이스가 온라인 상태이고 클라우드에 등록되어 있는지 확인하기 위해 1시간 동안 지속적으로 폴링합니다. 클라우드에 등록되면 CDO에서 초기 프로비저닝을 시작하고 디바이스를 성공적으로 온보딩합니다. 디바이스에서 LED 상태가 녹색으로 깜박이면 디바이스 등록을 확인할 수 있습니다. 디바이스가 Cisco 클라우드에 연결할 수 없거나 연결 후 연결이 끊어지면 상태 LED (Firepower 1000) 또는 SYS LED (Firepower 2100)가 녹색과 황색으로 번갈아 깜박이는 것을 확인할 수 있습니다.

디바이스가 처음 1시간 이내에 클라우드에 등록되지 않으면 시간 초과가 발생하며, 이제 CDO에서 10분마다 주기적으로 폴링하여 디바이스 상태를 확인하고 **Claiming**(클레임 중) 상태를 유지합니다. 디바이스가 켜져 있고 클라우드에 연결되어 있으면 온보딩 상태를 확인하기 위해 10분 동안 기다릴 필요가 없습니다. 언제든지 **Check Status**(상태 확인) 링크를 클릭하여 상태를 확인할 수 있습니다. CDO에서는 초기 프로비저닝을 시작하고 디바이스를 온보딩합니다.



Important

디바이스 설정 마법사(디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩 참조)를 이미 완료한 경우 디바이스가 클라우드에서 등록 취소되며, 이 경우 CDO에서는 **Claiming**(클레임 중) 상태를 유지합니다. Secure Firewall device manager에서 수동 등록을 완료하여 CDO에 추가해야 합니다. (Secure Firewall device manager에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하여 **Auto-enroll with Tenancy from Cisco Defense Orchestrator**(Cisco Defense Orchestrator에서 테넌시에 자동 등록) 옵션을 선택하고 **Register**(등록)를 클릭합니다). 그런 다음 **Check Status**(상태 확인)를 클릭합니다.

디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩

이 절차는 이미 관리용으로 구성된 디바이스에 적용됩니다. 디바이스 설정 마법사가 이미 구성된 FDM 관리 디바이스에서 완료되었으므로 디바이스가 클라우드에서 등록 취소되며, 로우터치 프로비저닝 프로세스를 사용하여 이러한 디바이스를 CDO에 온보딩할 수 없습니다.

디바이스가 관리되거나 구성된 적이 없는 새로운 디바이스인 경우, 로우터치 프로비저닝을 사용하여 디바이스를 온보딩할 수 있습니다. 자세한 내용은 [로우터치 프로비저닝을 사용하여 FDM-관리 디바이스 온보딩](#), on page 26을 참조하십시오.



Note

디바이스가 Cisco 클라우드에 연결되어 있지 않으면 상태 LED(Firepower 1000), SYS LED(Firepower 2100) 또는 M LED(Secure Firewall 3100)가 녹색과 황색으로 번갈아 깜박이는 것을 볼 수 있습니다.

다음 작업을 수행하기 위해 디바이스 설정 마법사를 완료했을 수 있습니다.

- 디바이스는 버전 6.7 이상을 실행해야 합니다.
- 디바이스의 관리 인터페이스에서 고정 IP 주소를 구성합니다. 인터페이스가 필요한 동적 IP 주소를 가져올 수 없거나 DHCP 서버가 게이트웨이 경로를 제공하지 않는 경우 고정 IP 주소를 구성해야 합니다.
- PPPoE를 사용하여 주소를 가져오고 외부 인터페이스를 구성합니다.

- Secure Firewall device manager 또는 Secure Firewall Management Center를 사용하여 버전 6.7 이상 디바이스를 실행하는 디바이스를 관리합니다.




Important

Secure Firewall device manager에서 Secure Firewall Management Center으로 또는 그 반대로 Secure Firewall Threat Defense 디바이스 관리자를 전환할 수 있습니다. 디바이스가 실행하는 버전에 맞는 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 관리" 장의 로컬 및 원격 관리 간 전환 섹션에 설명된 단계를 수행합니다.

디바이스를 온보딩하려면 다음을 수행합니다.

Procedure

- 단계 1 **로우터치 프로비저닝을 사용하여 FDM-관리 디바이스를 온보딩하기 위한 워크플로우 및 전제 조건**에서 온보딩을 위한 전제 조건을 검토합니다.
- 단계 2 Secure Firewall device manager UI에서 **System Settings(시스템 설정) > Cloud Services(클라우드 서비스)**로 이동하여 **Auto-enroll with Tenancy from Cisco Defense Orchestrator(Cisco Defense Orchestrator)**에서 테넌시에 자동 등록 옵션을 선택하고 **Register(등록)**를 클릭합니다.
- 단계 3 CDO에 로그인합니다.
- 단계 4 탐색창에서 **Inventory(재고 목록)**를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.
- 단계 5 **FTD tile(타일)**을 클릭합니다.
- 단계 6 **Onboard FTD Device(온보드 FTD 디바이스)** 화면에서 **Use Serial Number(일련 번호 사용)**를 클릭합니다.
- 단계 7 **FMC** 선택단계에서 드롭다운 메뉴를 사용하여 CDO에 이미 온보딩된 온프레미스 Management Center를 선택합니다. **Next(다음)**를 클릭합니다.
온프레미스 Management Center에서 버전 7.4 이상을 실행해야 합니다. 온프레미스 Management Center이 온보딩되지 않은 경우 온보딩 마법사에 대해 +Onboard(+온프레미스 FMC)를 클릭합니다.
- 단계 8 **Connection(연결)** 단계에서 디바이스의 일련 번호와 디바이스 이름을 입력합니다. **Next(다음)**를 클릭합니다.
- 단계 9 새 기기가 아니고 관리용으로 이미 구성된 경우, **Password Reset(암호 재설정)**을 위해 예, 이 새 기기는 비밀번호 재설정을 위해 로그인하거나 관리자용으로 구성된 적이 없음을 선택합니다. **Next(다음)**를 클릭합니다.
- 단계 10 **Policy Assignment(정책 할당)** 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 사용자 지정 정책이 없는 경우 CDO는 기본 액세스 제어 정책을 자동으로 선택합니다. **Next(다음)**를 클릭합니다.
- 단계 11 디바이스에 적용할 모든 라이선스를 선택합니다. **Next(다음)**를 클릭합니다.

CDO가 디바이스 연결 상태를 "Online(온라인)"으로 변경하고 구성 상태를 "Synced(동기화됨)" 상태로 변경합니다. FDM 관리 디바이스가 CDO에 온보딩됩니다. 하드웨어 후면 패널에서 상태 LED(Firepower 1000), SYS LED(Firepower 2100) 또는 M LED가 녹색으로 깜박이는 것을 볼 수 있습니다. Cisco Cloud에 연결되면 디바이스 LED가 녹색으로 계속 깜박입니다. 디바이스가 Cisco Cloud에 연결할 수 없거나 연결 후 연결이 끊어지면 동일한 상태 LED가 녹색과 황색으로 번갈아 깜박이는 것을 볼 수 있습니다.

관련 정보:

- 용어 및 정의

FDM-관리 고가용성 쌍 온보딩

Secure Firewall Threat Defense HA 쌍을 CDO에 온보딩하려면 쌍의 각 디바이스를 개별적으로 온보딩해야 합니다. 쌍의 두 피어가 모두 온보딩되면 CDO는 **Inventory(재고 목록)** 페이지에서 단일 항목으로 자동으로 결합됩니다. 디바이스 로그인 자격 증명 또는 등록 키를 사용하여 디바이스를 온보딩합니다. 동일한 방법으로 두 디바이스를 모두 온보딩하는 것이 좋습니다. 또한 대기 모드에 있는 디바이스를 먼저 온보딩하는 경우 CDO는 해당 디바이스를 배포하거나 읽을 수 있는 기능을 비활성화합니다. HA 쌍 내의 액티브 디바이스만 읽거나 배포할 수 있습니다.



참고 CDO는 등록 키가 있는 디바이스 온보딩을 강력히 권장합니다. 등록 키를 사용한 온보딩은 특정 버전을 실행하는 Threat Defense 디바이스에서 약간 다릅니다. 자세한 내용은 [버전 6.4 또는 버전 6.5를 실행하는 FDM-관리 HA 쌍 온보딩, 31 페이지](#) 및 [버전 6.6 또는 버전 6.7 이상을 실행하는 FDM-관리 HA 쌍 온보딩, 32 페이지](#)를 참조하십시오.

CDO에 Threat Defense HA 쌍을 온보딩하기 전에 다음을 검토합니다.

- CDO에 대한 온보딩 전에 HA 쌍이 이미 형성되어 있습니다.
- 두 디바이스 모두 정상 상태입니다. 쌍은 기본/활성 및 보조/대기 또는 기본/대기 및 보조/활성 모드일 수 있습니다. 비정상 디바이스는 CDO에 동기화되지 않습니다.
- HA 쌍은 Secure Firewall Management Center가 아니라 Secure Firewall device manager이 관리합니다.
- 클라우드 커넥터는 <https://www.defenseorchestrator.com>에서 CDO에 연결됩니다.

등록 키를 사용하여 **FDM-관리 고가용성 쌍 온보딩**

등록 키를 사용하여 FDM 관리 HA(고가용성) 쌍을 온보딩하기 전에 다음 사전 요건을 확인합니다.

- 등록 키로 버전 6.4를 실행하는 디바이스 온보딩은 미국 지역(defenseorchestrator.com)에 대해서만 지원됩니다. EU 지역(defenseorchestrator.eu)에 연결하려면 사용자 이름, 비밀번호 및 IP 주소를 사용하여 HA 쌍을 온보딩해야 합니다.
- 버전 6.5 이상을 실행하고 미국, EU 또는 APJC 지역에 연결하는 고객은 이 온보딩 방법을 사용할 수 있습니다.

- 버전 6.4 및 6.5를 실행하는 디바이스는 등록 키로 온보딩하기 전에 Cisco Smart Software Manager에 등록하지 않아야 합니다. CDO에 온보딩하기 전에 해당 FDM 관리의 스마트 라이선스를 등록 취소해야 합니다. 자세한 내용은 [스마트 라이선스 FDM-관리 디바이스 등록 취소, on page 13](#)를 참조하십시오.

버전 6.4 또는 버전 6.5를 실행하는 FDM-관리 HA 쌍 온보딩

소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM 관리 HA 쌍을 온보딩하려면 디바이스를 한 번에 하나씩 온보딩해야 합니다. 액티브 또는 보조, 기본 또는 보조 디바이스를 온보딩하는지 여부는 중요하지 않습니다.




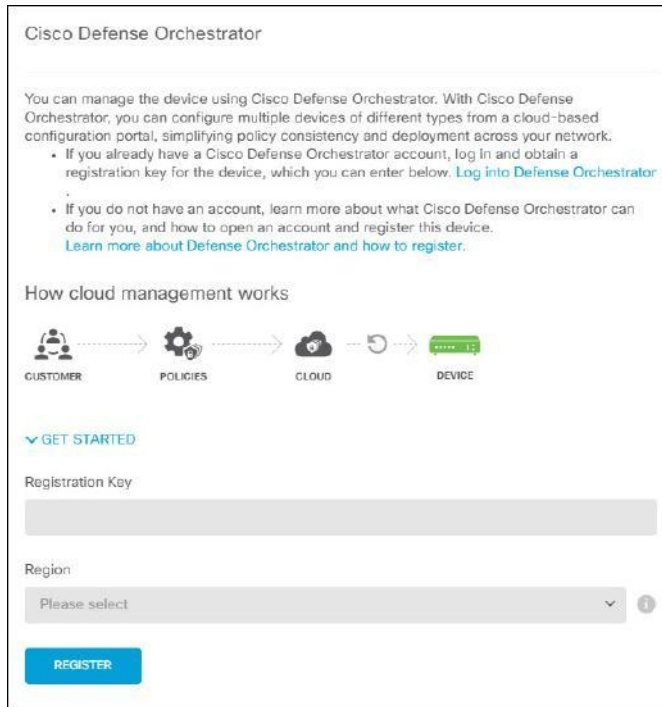
Note 등록 키를 사용하여 HA 쌍의 디바이스 중 하나를 온보딩하는 경우 동일한 방법으로 다른 피어 디바이스를 온보딩해야 합니다.

버전 6.4 또는 6.5를 실행하는 HA 쌍을 온보딩하려면 다음 단계를 사용합니다.

Procedure

- 단계 1** 피어 디바이스를 온보딩합니다. [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하여 쌍 내의 첫 번째 디바이스를 온보딩합니다.
- 단계 2** 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 3** **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 4** **FTD** 탭을 클릭합니다. 디바이스가 동기화되면 디바이스를 선택하여 강조 표시합니다. **Device Details**(디바이스 세부 정보) 바로 아래에 있는 작업 창에서 **Onboard Device**(디바이스 온보드)를 클릭합니다.
- 단계 5** 이미 온보딩된 피어 디바이스의 **HA Peer Device Name**(HA 피어 디바이스 이름) 을 입력합니다. **Next**(다음)를 클릭합니다.
- 단계 6** 첫 번째 디바이스에 대한 스마트 라이선스를 제공한 경우, CDO은 현재 디바이스를 온보딩하는 데 사용할 수 있도록 해당 라이선스를 다시 채웁니다. **Next**(다음)를 클릭합니다.

Note 디바이스 온보딩을 위해 FDM 관리 디바이스의 스마트 라이선스 등록을 취소한 경우, 여기에서 스마트 라이선스를 다시 적용합니다.
- 단계 7** CDO은 온보딩을 준비하는 디바이스에 대한 등록 키를 자동으로 생성합니다. **Copy**(복사) 아이콘  을 클릭하여 등록 키를 복사합니다.
- 단계 8** 온보딩 중인 디바이스의 Secure Firewall device manager UI에 로그인합니다.
- 단계 9** **System Settings**(시스템 설정)에서 **Cloud Services**(클라우드 서비스)를 클릭합니다.
- 단계 10** CDO 파일에서 **Get Started**(시작하기)를 클릭합니다.
- 단계 11** **Registration Key**(등록 키) 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.



단계 12 **Region**(지역) 필드에서 테넌트가 할당된 Cisco Cloud 지역을 선택합니다.

- defenseorchestrator.com에 로그인하는 경우 US를 선택합니다.
- defenseorchestrator.eu에 로그인하는 경우 EU를 선택합니다.
- apj.cdo.cisco.com에 로그인하는 경우 APJ를 선택합니다.

Note 이 단계는 버전 6.4에서 실행되는 FDM 관리 디바이스에는 적용되지 않습니다.

단계 13 **Register**(등록)를 클릭한 다음, **Accept Cisco Disclosure**(Cisco 공개 동의)를 클릭합니다.

단계 14 CDO으로 돌아가서, **Create Registration Key**(등록 키 생성) 영역에서 **Next**(다음)을 클릭합니다.

단계 15 **Go to Inventory**(재고 목록로 이동)을 클릭합니다. CDO는 자동으로 디바이스를 온보딩하고 단일 항목으로 결합합니다. 온보딩하는 첫 번째 피어 디바이스와 마찬가지로 디바이스 상태가 "Unprovisioned(프로비저닝되지 않음)"에서 "Locating(찾는 중)", "Syncing(동기화 중)"에서 "Synced(동기화됨)"로 변경됩니다.


버전 6.6 또는 6.7을 실행하는 FDM 관리 HA 쌍을 온보딩하려면 한 번에 하나씩 디바이스를 온보딩해야 합니다. 액티브 또는 보조, 기본 또는 보조 디바이스를 온보딩하는지 여부는 중요하지 않습니다.



Note 등록 키를 사용하여 HA 쌍의 디바이스 중 하나를 온보딩하는 경우 동일한 방법으로 다른 피어 디바이스를 온보딩해야 합니다.

버전 6.6 또는 6.7을 실행하는 HA 쌍을 온보딩하려면 다음 단계를 사용합니다.

Procedure

- 단계 1 피어 디바이스를 온보딩합니다. 자세한 내용은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.
- 단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 3 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 4 **FTD** 탭을 클릭합니다. 디바이스가 동기화되면 디바이스를 선택하여 강조 표시합니다. **Device Details**(디바이스 세부 정보) 바로 아래에 있는 작업 창에서 **Onboard Device**(디바이스 온보드)를 클릭합니다.
- 단계 5 이미 온보딩된 피어 디바이스의 HA 피어 디바이스 이름을 입력합니다. **Next**(다음)를 클릭합니다.
- 단계 6 첫 번째 디바이스에 대한 스마트 라이선스를 제공한 경우, CDO은 현재 디바이스를 온보딩하는 데 사용할 수 있도록 해당 라이선스를 다시 채웁니다. **Next**(다음)를 클릭합니다.
- 단계 7 CDO은 온보딩을 준비하는 디바이스에 대한 등록 키를 자동으로 생성합니다. **Copy**(복사) 아이콘 을 클릭하여 등록 키를 복사합니다.
- 단계 8 CDO에 온보딩하려는 디바이스의 Secure Firewall device manager UI에 로그인합니다.
- 단계 9 **System Settings**(시스템 설정)에서 **Cloud Services**(클라우드 서비스)를 클릭합니다.
- 단계 10 **Enrollment Type**(등록 유형) 영역에서 **Security/CDO Account**(보안/CDO 계정)를 클릭합니다.

Note 버전 6.6을 실행하는 디바이스의 경우, CDO의 Tenancy(테넌시) 탭의 제목이 **Security Account**(보안 어카운트)이며 Secure Firewall device managerUI에서 CDO를 수동으로 활성화해야 합니다.

The screenshot shows the enrollment configuration page for Cisco Defense Orchestrator. It includes fields for Enrollment Type, Region, and Registration Key. The 'Service Enrollment' section contains two options: 'Enable Cisco Defense Orchestrator' and 'Enroll Cisco Success Network', both of which are checked. A 'REGISTER' button is located at the bottom of the form.

단계 11 **Region**(지역) 필드에서 테넌트가 할당된 Cisco Cloud 지역을 선택합니다.

- defenseorchestrator.com에 로그인하는 경우 US를 선택합니다.
- defenseorchestrator.eu에 로그인하는 경우 EU를 선택합니다.
- apj.cdo.cisco.com에 로그인하는 경우 APJ를 선택합니다.

단계 12 **Registration Key**(등록 키) 필드에 CDO에서 생성한 등록 키를 붙여넣습니다.

단계 13 버전 6.7 이상을 실행하는 디바이스의 경우, **Service Enrollment**(서비스 등록) 영역에서 **Enable Cisco Defense Orchestrator**(Cisco Defense Orchestrator 활성화)를 선택합니다.

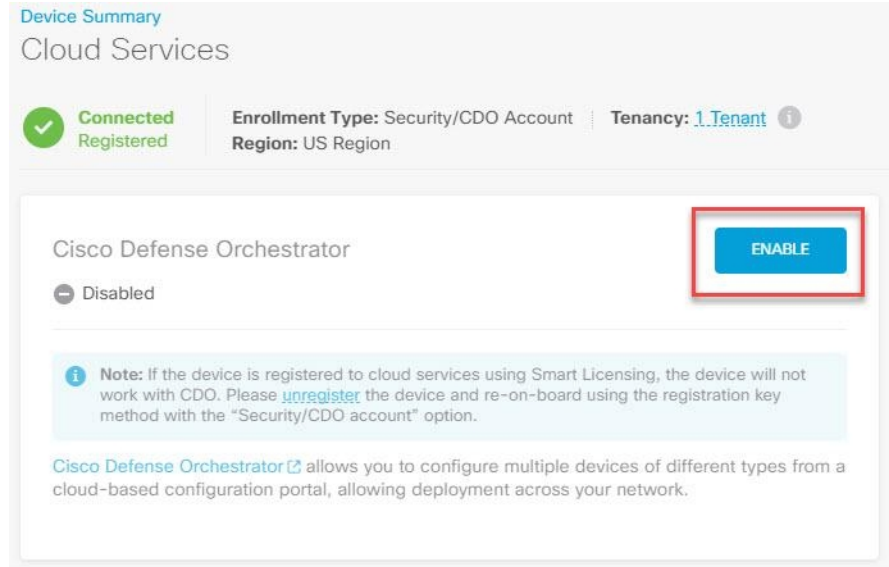
단계 14 Cisco Success Network 등록에 대한 정보를 검토합니다. 참여하지 않으려면 **Enroll Cisco Success Network**(Cisco Success Network 등록) 확인란의 선택을 취소합니다.

단계 15 **Register**(등록)를 클릭한 다음, **Accept Cisco Disclosure**(Cisco 공개 동의)를 클릭합니다. FDM에서 CDO에 등록 요청을 전송합니다.

단계 16 CDO로 돌아가 **Create Registration Key**(등록 키 생성) 영역에서 **Next**(다음)를 클릭합니다.

단계 17 **Smart License**(스마트 라이선스) 영역에서 FDM 관리 디바이스에 스마트 라이선스를 적용하고 **Next**(다음)를 클릭하거나 **Skip**(건너뛰기)를 클릭하여 90일 평가 라이선스로 온보딩을 계속할 수 있습니다.(또는 디바이스에 이미 스마트 라이선스가 있는 경우). 자세한 내용은 [FTD 디바이스의 기존 스마트 라이선스 업데이트](#)를 참조하십시오.

Note 디바이스에서 버전 6.6을 실행 중인 경우 CDO와의 통신을 수동으로 활성화해야 합니다. 디바이스의 FDM 관리 UI에서 **System Settings**(시스템 설정) > **Cloud Services**(클라우드 서비스)로 이동하여 **Cisco Defense Orchestrator** 타일에서 **Enable**(활성화)를 클릭합니다.



단계 18 CDO으로 돌아가 **Go to Inventory**(인벤토리로 이동)를 클릭합니다. CDO는 자동으로 디바이스를 온보딩하고 단일 항목으로 결합합니다. 온보딩하는 첫 번째 피어 디바이스와 마찬가지로 디바이스 상태가 "Unprovisioned(프로비저닝되지 않음)"에서 "Locating(찾는 중)", "Syncing(동기화 중)"에서 "Synced(동기화됨)"로 변경됩니다.

FDM-관리 고가용성 쌍 온보딩



참고 HA 쌍의 첫 번째 디바이스를 어떤 방법으로 온보딩하든 다른 피어 디바이스도 동일한 방법으로 온보딩해야 합니다.

CDO 외부에서 생성된 FDM 관리 HA 쌍을 온보딩하려면 다음 절차를 수행합니다.

프로시저

단계 1 HA 쌍 내의 피어 디바이스 중 하나를 온보딩합니다. 사용자 이름, 비밀번호 및 IP 주소를 사용하여 FDM-관리 디바이스 온보딩, 등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스를 온보딩하는 절차 또는 디바이스의 일련 번호를 사용하여 구성된 FDM-관리 디바이스 온보딩를 사용하여 디바이스를 온보딩합니다.

단계 2 디바이스가 동기화되면 **Inventory**(재고 목록) 페이지에서 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭합니다.

- 단계 4 디바이스를 선택합니다. **Device Details**(디바이스 세부 정보) 바로 아래에 있는 작업 창에서 **Onboard Device**(디바이스 온보드)를 클릭합니다.
- 단계 5 팝업 창에서 HA 피어의 디바이스 이름 및 위치를 입력합니다.
- 단계 6 **Onboard Device**(디바이스 온보드)를 클릭합니다. 두 디바이스가 CDO에 성공적으로 동기화되면 HA 쌍이 **Inventory**(재고 목록) 페이지에 단일 엔터티로 표시됩니다.

FTD 클러스터 온보딩

•

클러스터된 **Secure Firewall Threat Defense** 디바이스 온보딩

다음 절차를 사용하여 이미 클러스터링된 위협 방어 디바이스를 온보딩합니다.

시작하기 전에


다음 디바이스는 클러스터링을 지원합니다.

- Secure Firewall 3100 디바이스
- Firepower 4100 디바이스
- Firepower 9300 디바이스
- Threat Defense Virtual 디바이스(AWS, Azure, VMware, KVM, GCP)

클러스터된 디바이스의 경우 다음과 같은 제한 사항을 참고하십시오.

- 디바이스는 버전 6.4 이상을 실행해야 합니다.
- 디바이스는 물리적 또는 가상 Secure Firewall Management Center으로 관리해야 합니다.
- Firepower 4100 및 Firepower 9300 디바이스는 디바이스의 새시 관리자를 통해 클러스터링되어야 합니다.
- Secure Firewall 3100 디바이스, KVM 및 VMware 환경은 Secure Firewall Management Center UI를 통해 클러스터링되어야 합니다.
- Azure, AWS 및 GCP 환경 클러스터는 자체 환경을 통해 생성하고 Secure Firewall Management Center에 온보딩해야 합니다.

프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 탐색창에서 **Inventory**(재고 목록)를 클릭하고 파란색 더하기 버튼  을 클릭하여 디바이스를 온보딩합니다.
- 단계 3 **FTD**를 클릭합니다.

단계 4 Management Mode(관리 모드)에서 FTD가 선택되어 있는지 확인합니다.

FTD를 선택하면 Secure Firewall Management Center를 관리 플랫폼으로 유지하게 됩니다. FDM을 선택하면 관리자가 Secure Firewall Management Center에서 Firewall Device Manager 또는 클라우드 사용 Firewall Management Center와 같은 로컬 관리자로 전환됩니다. 관리자를 전환하면 인터페이스 구성을 제외한 모든 기존 정책 구성이 재설정되며 디바이스를 온보딩한 후 정책을 다시 구성해야 합니다.

단계 5 Onboard FTD Device(온보드 FTD 디바이스) 화면에서 Use CLI Registration Key(CLI 등록 키 사용)를 클릭합니다.

단계 6 Device Name(디바이스 이름) 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.

단계 7 Policy Assignment(정책 할당) 단계에서 드롭다운 메뉴를 사용하여 디바이스가 온보딩된 후 구축할 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy(기본 액세스 제어 정책)**를 선택합니다.

단계 8 온보딩 중인 디바이스가 물리적 디바이스인지 가상 디바이스인지 지정합니다. 가상 디바이스를 온보딩하는 경우 드롭다운 메뉴에서 디바이스의 성능 계층을 선택해야 합니다.

단계 9 디바이스에 적용할 기본 라이선스를 선택합니다. **Next(다음)**를 클릭합니다.

단계 10 CDO는 등록 키를 사용하여 명령을 생성합니다. 디바이스의 CLI에 전체 등록 키를 그대로 붙여넣습니다.

단계 11 디바이스의 온보딩이 시작됩니다. 선택적 단계로 Inventory(재고 목록) 페이지를 정렬하고 필터링하는 데 도움이 되도록 디바이스에 레이블을 추가할 수 있습니다. 레이블을 입력하고 파란색 더하기 버튼을 선택합니다. .

다음에 수행할 작업

디바이스가 동기화되면 CDO에서 디바이스가 클러스터링되었음을 자동으로 탐지합니다. 여기에서 Inventory(재고 목록) 페이지에서 방금 온보딩한 디바이스를 선택하고 오른쪽에 있는 Management(관리) 창 아래에 나열된 옵션 중 하나를 선택합니다. 다음 작업을 수행하는 것이 좋습니다.

- 아직 생성하지 않은 경우 사용자 환경에 맞게 보안을 사용자 지정하려면 사용자 지정 액세스 제어 정책을 생성합니다. 자세한 내용은 [FDM-관리 액세스 제어 정책](#)을 참조하십시오.
- Cisco SAL(Security Analytics and Logging)을 활성화하여 CDO 대시보드에서 이벤트를 보거나 보안 분석을 위해 디바이스를 Secure Firewall Management Center에 등록합니다.

스마트 라이선스 적용 또는 업데이트

FDM-관리 디바이스에 새 스마트 라이선스 적용

FTD(Firepower Threat Defense) 디바이스를 스마트 라이선싱하려면 다음 절차 중 하나를 수행합니다.

- 등록 키를 사용하여 온보딩하는 FDM 관리 디바이스의 스마트 라이선스입니다.
- 등록 키 또는 관리자 자격 증명을 사용하여 디바이스를 온보딩한 후 FDM 관리 디바이스에 스마트 라이선스를 부여합니다.



Note FDM 관리 디바이스에서 90일 평가 라이선스를 사용 중이거나 라이선스가 등록 취소되었을 수 있습니다.

등록 키를 사용하여 온보딩 시 FDM-관리 디바이스에 스마트-라이선스 부여

Procedure

단계 1 **Cisco Smart Software Manager**에 로그인하고 새 스마트 라이선스 키를 생성합니다. 새로 생성된 키를 복사합니다. 자세한 내용은 [스마트 라이선싱 생성](#) 비디오를 참조하십시오.

The screenshot shows the Cisco Smart Software Licensing interface. At the top, it displays 'Cisco Software Central > Smart Software Licensing' and the user 'Example Co admin@example.com'. The main heading is 'Smart Software Licensing'. Below this, there are navigation tabs: Alerts, Inventory, Convert to Smart Licensing, Reports, Preferences, On-Prem Accounts, and Activity. A 'Virtual Account' section shows 'Example Co' with a description 'Licenses for US Region' and 'Default Virtual Account: No'. Below this is the 'Product Instance Registration Tokens' section, which includes a 'New Token...' button and a table of existing tokens.

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
MTU2MmRiY2MTYjJhY.	2021-Jul-30 19:43:22 (in 305...	12 of 30	Allowed	CDO	admin1	Actions
NDFhZGRJNmMOTJk.	Expired		Allowed		admin2	Actions

단계 2 등록 키를 사용하여 FDM 관리 디바이스 온보딩을 시작합니다. 자세한 내용은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#) 또는 [등록 키를 사용하여 소프트웨어 버전 6.4 또는 6.5를 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.

단계 3 온보딩 마법사 4단계의 **Smart License here**(여기에 스마트 라이선스)에서 **Activate**(활성화) 필드에 스마트 라이선스를 붙여넣고 **Next**(다음)를 클릭합니다.

3 Subscription License

Please indicate if this FTD is physical or virtual:

Physical FTD Device
 Virtual FTD Device

License Type	Includes
<input checked="" type="checkbox"/> Essentials	Base Firewall Capabilities
<input type="checkbox"/> Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
<input type="checkbox"/> IPS	Intrusion Policy
<input type="checkbox"/> Malware Defense	File Policy
<input type="checkbox"/> URL	URL Reputation
<input type="checkbox"/> RA VPN VPN Only	RA VPN

Next

! Enable subscription licenses. CDO will attempt to enable the selected licenses when the device is connected to CDO and registered with the supplied Smart License.
[Learn more about Cisco Smart Accounts.](#)

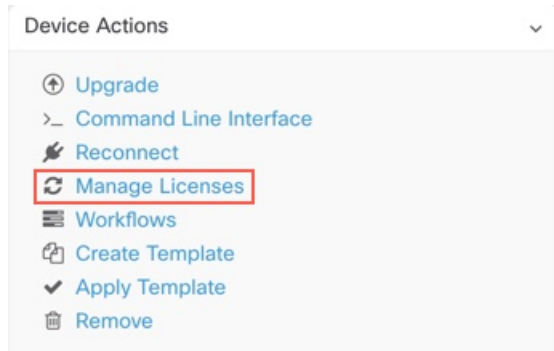
Note: All virtual FTDs require performance tier license. Make sure your subscription licensing account contains the available licenses you need. Its important to choose the tier that matches the license you have in your account. Until you choose a tier, your FTDv defaults to FTDv50 selection.

단계 4 **Go to Inventory page**(재고 목록 페이지로 이동)를 클릭합니다.

단계 5 **FTD** 탭을 클릭하고 온보딩 프로세스의 진행 상황을 확인합니다. 디바이스에서 동기화를 시작하고 스마트 라이선스를 적용합니다.

이제 디바이스가 **Online**(온라인) 연결 상태임을 확인할 수 있습니다. 디바이스가 온라인 연결 상태가 아닌 경우 오른쪽의 Device Actions(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)> **Refresh Licenses**(라이선스 새로 고침)를 클릭하여 연결 상태를 업데이트합니다.

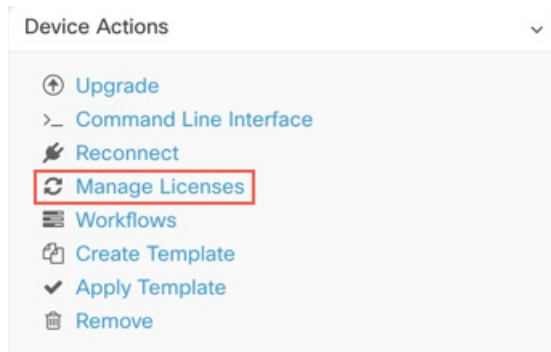
단계 6 스마트 라이선스를 FDM 관리 디바이스에 성공적으로 적용한 후 **Manage Licenses**(라이선스 관리)를 클릭합니다. 디바이스 상태에 "**Connected, Sufficient License**(연결됨, 라이선스가 충분함)"가 표시됩니다. 필요에 따라 라이선스를 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 [FDM-관리 디바이스 라이선싱 유형](#)을 참조하십시오.



등록 키 또는 자격 증명을 사용하여 디바이스 온보딩 후 FDM-관리 디바이스에 스마트-라이선스 부여

Procedure

- 단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭하고 라이선스를 부여할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭합니다.



- 단계 5 화면의 지침에 따라 Cisco Smart Software Manager에서 생성된 스마트 라이선스를 입력합니다.
- 단계 6 상자에 새 라이선스 키를 붙여넣고 **Register Device**(디바이스 등록)를 클릭합니다. 디바이스와 동기화되면 연결 상태가 'Online(온라인)'으로 변경됩니다. 스마트 라이선스를 FDM 관리 디바이스에 성공적으로 적용하면 디바이스 상태에 "**Connected, Sufficient License**(연결됨, 라이선스가 충분함)"가 표시됩니다. 필요에 따라 라이선스를 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 [FDM-관리 디바이스 라이선싱 유형](#)을 참조하십시오.

FTD 디바이스의 기존 스마트 라이선스 업데이트

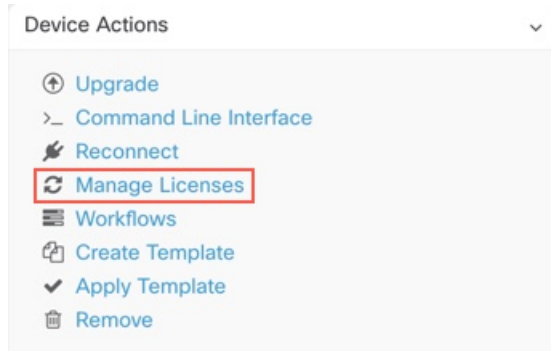
스마트 라이선스가 있는 FTD 디바이스에 새 스마트 라이선스를 적용할 수 있습니다. 디바이스 온보딩을 위해 선택한 방법에 따라 적절한 절차를 선택합니다.

등록 키를 사용하여 온보딩된 FDM-관리 디바이스에 적용되는 스마트 라이선스 변경

Procedure

- 단계 1 Cisco Defense Orchestrator에서 해당 FDM 관리 디바이스를 제거합니다.
- 단계 2 해당 디바이스의 Secure Firewall device manager에 로그인하고 스마트 라이선스를 등록 취소합니다. 자세한 내용은 [스마트 라이선스 FDM-관리 디바이스 등록 취소](#)를 참조하십시오.

- 단계 3 CDO에서 등록 키를 사용하여 FDM 관리 디바이스를 다시 온보딩합니다. 자세한 내용은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.
- 단계 4 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 5 탭을 클릭합니다.
- 단계 6 온보딩 프로세스 중에 또는 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭하여 새 스마트 라이선스를 적용합니다.



자격 증명을 사용하여 온보딩된 FDM-관리 디바이스에 적용되는 스마트 라이선스 변경

Procedure

- 단계 1 해당 디바이스의 Secure Firewall device manager에 로그인하고 스마트 라이선스를 등록 취소합니다. 자세한 내용은 [등록 키를 사용하여 소프트웨어 버전 6.6 이상을 실행하는 FDM-관리 디바이스 온보딩](#)을 참조하십시오.
- 단계 2 Secure Firewall device manager의 FDM 관리 디바이스에 새 스마트 라이선스를 적용합니다.
 - a. **Smart License**(스마트 라이선스) 영역에서 **View Configuration**(구성 보기)을 클릭합니다.
 - b. **Register Now**(지금 등록)를 클릭하고 화면의 지침을 따릅니다.
- 단계 3 CDO의 **Inventory**(재고 목록) 페이지에서 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 4 **FTD** 디바이스를 클릭합니다. CDO에서 FDM 관리 디바이스의 구축된 구성 복사본을 만들고 CDO 데이터베이스에 저장할 수 있도록 FDM 관리 디바이스 구성 변경 사항이 있는지 확인합니다. 자세한 내용은 [구성 변경 사항 읽기, 삭제, 확인 및 구축](#)을 참조하십시오.

FDM-관리 디바이스의 DHCP 주소 지정에 대한 CDO 지원

내 FDM 관리 디바이스에서 사용하는 IP 주소가 변경되면 어떻게 됩니까?

CDO(Cisco Defense Orchestrator)에는 DHCP를 사용하여 통신 사업자가 제공한 IP 주소로 디바이스를 온보딩한 많은 ASA(Adaptive Security Appliance) 및 FDM 관리 디바이스 고객이 있습니다.

고정 IP 주소가 변경되었거나 DHCP로 인해 IP 주소가 변경되는 등 어떤 이유로든 디바이스의 IP 주소가 변경되면 CDO가 디바이스에 연결하는 데 사용하는 IP 주소를 변경한 후 디바이스를 다시 연결할 수 있습니다.

이 필드는 CDO에서 관리하는 브랜치 구축 FDM 관리 디바이스의 경우와 관련하여 우려 사항을 나타냅니다. FDM 관리 디바이스의 외부 인터페이스에는 고정 IP가 필요합니다. 일부 SE의 보기에서는 FDM 관리 디바이스가 외부 인터페이스에 대해 구성된 DHCP 주소를 보유한 경우 관리 솔루션으로 CDO를 사용할 수 없습니다.

그러나 이 상황은 원격 브랜치 방화벽에 대한 VPN 터널이 있는 고객에게는 영향을 미치지 않습니다. 대다수의 고객이 브랜치에서 데이터 센터로 다시 연결되는 사이트 간 터널을 보유하고 있습니다. 사이트 간 VPN을 사용하여 디바이스에서 중앙 사이트에 연결하는 경우 외부 인터페이스의 DHCP는 CDO 및 모든 관리 플랫폼이 내부 정적 주소 지정 인터페이스(구성된 경우)를 통해 FW에 연결할 수 있기 때문에 문제가 되지 않습니다. 이는 권장되는 방법이며, 이 구축 모드를 사용하는 디바이스(+1000)를 많이 보유한 CDO 고객이 있습니다.

또한 인터페이스 IP 주소가 DHCP를 통해 발급된다고 해서 고객이 해당 IP를 사용하여 디바이스를 관리할 수 있는 것도 아닙니다. 이는 최적의 방법은 아니지만, 잠재적으로 CDO에서 IP 주소를 정기적으로 변경해야 하는 경험은 고객에게 장애로 여겨지지 않습니다. 이러한 상황은 CDO에만 해당되는 것은 아니며 ASDM, FDM 또는 SSH를 비롯한 외부 인터페이스를 사용하는 모든 관리자에서 발생합니다.

FDM-관리 디바이스 라이선싱 유형

스마트 라이선스 유형

다음 표에서는 FDM 관리 디바이스에 사용할 수 있는 라이선스에 대해 설명합니다.

FDM 관리 디바이스 구매 시 기본 라이선스가 자동으로 포함됩니다. 모든 추가 라이선스는 선택 사항입니다.

라이선스	기간	부여된 기능
라이선스(자동 포함)	영구	구독 기간 라이선스가 적용되지 않는 모든 기능. 이 토큰을 사용하여 등록된 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.

라이선스	기간	부여된 기능
	기간 기준	<p>침입 탐지 및 방지 - 침입 정책은 침입 및 익스플로잇의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다.</p> <p>파일 제어 - 파일 정책은 사용자가 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 악성코드 라이선스가 필요한 AMP for Firepower를 사용하면 악성코드가 포함된 파일을 검사하고 차단할 수 있습니다. 모든 유형의 파일 정책을 사용하려면 라이선스가 있어야 합니다.</p> <p>보안 인텔리전스 필터링 - 트래픽이 액세스 제어 규칙을 기준으로 분석 대상이 되기 전에 선택한 트래픽을 삭제합니다. 동적 피드를 사용하면 최신 인텔리전스를 기반으로 연결을 즉시 삭제할 수 있습니다.</p>
악성코드	기간 기준	<p>악성코드를 확인하는 파일 정책으로서 Cisco AMP(Advanced Malware Protection)를 AMP for Firepower(네트워크 기반 Advanced Malware Protection) 및 Cisco Threat Grid와 함께 사용합니다.</p> <p>파일 정책은 네트워크를 통해 전송된 파일에서 악성코드를 탐지하고 차단할 수 있습니다.</p>
URL 라이선스	기간 기준	<p>범주 및 평판 기반 URL 필터링</p> <p>이 라이선스가 없어도 개별 URL에 대해 URL 필터링을 수행할 수 있습니다.</p>

라이선스	기간	부여된 기능
	라이선스 유형에 따라 기간 기준 또는 영구	<p>원격 액세스 VPN 컨피그레이션 Essentials 라이선스는 RA VPN을 구성하기 위해 내보내기 제어 기능을 허용해야 합니다. 디바이스를 등록할 때 내보내기 요구사항을 충족하는지를 선택합니다.</p> <p>Firepower Device Manager는 유효한 모든 AnyConnect 라이선스를 사용할 수 있습니다. 제공되는 기능은 라이선스 유형에 따라 달라지지 않습니다. 아직 구매하지 않은 경우 원격 액세스 VPN에 대한 라이선싱 요구 사항을 참조하십시오.</p> <p>또한 Cisco AnyConnect 주문 가이드, http://www.cisco.com/zh/na/products/anyconnect/를 참조하십시오.</p>

가상 FDM-관리 디바이스 계층형 라이선스

버전 7.0에는 처리량 요구 사항 및 RA VPN 세션 제한을 기반으로 하는 가상 FDM-관리 디바이스에 대한 성능 계층형 스마트 라이선싱 지원이 추가되었습니다. 사용 가능한 성능 라이선스 중 하나로 가상 FDM-관리 디바이스에 라이선스가 부여되면 RA VPN에 대한 세션 제한이 설치된 가상 FDM-관리 디바이스 플랫폼 엔타이틀먼트 계층에 의해 결정되고 속도 제한기를 통해 적용됩니다.

CDO에서는 현재 계층형 스마트 라이선싱을 완전히 지원하지 않습니다. 다음 제한 사항을 참조하십시오.

- CDO를 통해 계층화된 라이선스를 수정할 수 없습니다. Secure Firewall device manager UI에서 변경해야 합니다.
- 클라우드 사용 Firewall Management Center에서 관리할 가상 FDM-관리 디바이스를 등록하면 계층화된 라이선스 선택이 기본 계층인 **Variable**(변수)로 자동 재설정됩니다.
- 버전 7.0 이상을 실행하는 가상 FDM-관리 디바이스를 온보딩하고 온보딩 프로세스 중에 기본 라이선스가 아닌 라이선스를 선택하면 계층화된 라이선스 선택이 자동으로 기본 계층인 **Variable**(변수)로 재설정됩니다.

위에 나열된 문제를 방지하려면 디바이스를 온보딩한 후 가상 FDM-관리 디바이스 라이선스의 계층을 선택하는 것이 좋습니다. 자세한 내용은 [스마트 라이선스 관리](#)를 참조하십시오.

디바이스용 스마트-라이선스 보기

Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 FDM 관리 디바이스를 선택하여 현재 라이선스 상태를 확인합니다.
- 단계 5 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭합니다.

Manage Licenses(라이선스 관리) 화면에는 다음 정보가 제공됩니다.

- **Smart License Agent**(스마트 라이선스 대리인) 상태: 90일 평가판 라이선스를 사용하는지 또는 Cisco Smart Software Manager에 등록했는지 여부를 표시합니다. 스마트 라이선스 대리인 상태는 다음과 같을 수 있습니다.
 - **"Connected," "Sufficient Licenses"**("연결됨", "충분한 라이선스") - 디바이스가 라이선스 기관에 연결하여 정상적으로 등록되었으며, 어플라이언스에 대한 라이선스 자격이 부여되었습니다. 디바이스는 현재 컴플라이언스 상태입니다.
 - **Out-of-Compliance**(규정 미준수) - 디바이스에 대해 사용 가능한 라이선스 자격이 없습니다. 라이선스 기능은 계속 작동합니다. 그러나 추가 자격을 구매하거나 확보하여 디바이스의 규정을 준수하는 상태가 될 수 있습니다.
 - **Authorization Expired**(권한 부여 만료됨) - 디바이스가 90일 이상 라이선스 기관과 통신하지 않았습니다. 라이선스 기능은 계속 작동합니다. 이 상태에서 스마트 라이선스 에이전트는 권한 부여 요청을 다시 시도합니다. 다시 시도가 성공하면 대리인은 **Out-of-Compliance**(규정 미준수) 또는 **Authorized**(권한 있음) 상태로 설정되며 새 권한 부여 기간이 시작됩니다. 이 경우 디바이스를 수동으로 동기화해 보십시오.
- **License Registration**(라이선스 등록): 이미 온보딩된 FDM 관리 디바이스에 스마트 라이선스를 적용할 수 있습니다. 등록된 경우 Cisco Smart Software Manager에 대한 연결 상태와 각 라이선스 유형의 상태를 확인할 수 있습니다.
- **License Status**(라이선스 상태): FDM 관리 디바이스에서 사용 가능한 라이선스(선택 사항)의 상태를 표시합니다. 라이선스를 통해 제어하는 기능을 사용하도록 라이선스를 설정할 수 있습니다.

선택 가능한 라이선스 활성화 또는 비활성화

90일 평가 라이선스 또는 전체 라이선스를 사용하는 FDM 관리 디바이스에서 필요에 따라 라이선스를 활성화(등록)할 수 있습니다. 라이선스를 통해 제어되는 기능을 사용하려면 라이선스를 활성화해야 합니다.

필요에 따라 기간별 라이선스가 적용되는 기능을 더 이상 사용하지 않으려는 경우 라이선스를 비활성화(해제)할 수 있습니다. 비활성화하는 라이선스는 Cisco Smart Software Manager 계정에서 해제되므로 다른 디바이스에 적용할 수 있습니다.

평가 모드에서는 필요에 따라 라이선스의 평가 버전을 활성화하고 모든 작업을 수행할 수도 있습니다. 이 모드에서 라이선스는 디바이스를 등록할 때까지 Cisco Smart Software Manager에 등록되지 않습니다.



Note 평가 모드에서는 라이선스를 활성화할 수 없습니다.

Before you begin

라이선스를 비활성화하기 전에 해당 라이선스를 사용하고 있지 않은지 확인합니다. 라이선스가 필요한 정책은 재작성하거나 삭제합니다.

고가용성 컨피그레이션에서 작동 중인 유닛의 경우 액티브 유닛에서만 라이선스를 활성화하거나 비활성화합니다. 다음번 구성 구축 시에 스탠바이 유닛이 필요한 라이선스를 요청하거나 해제할 때 변경사항이 스탠바이 유닛에 반영됩니다. 라이선스를 활성화하는 경우에는 Cisco Smart Software Manager 어카운트에 사용 가능한 라이선스가 충분한지 확인해야 합니다. 그렇지 않으면 각 유닛의 컴플라이언스 상태가 서로 다를 수 있습니다.

필요에 따라 라이선스를 활성화하거나 비활성화하려면 다음 절차를 수행합니다.

Procedure

- 단계 1 **Inventory**(재고 목록) 페이지에서 원하는 FDM 관리 디바이스를 선택하고 **Device Actions**(디바이스 작업) 창에서 **Manage Licenses**(라이선스 관리)를 클릭합니다. 그러면 **Manage Licenses**(라이선스 관리) 화면이 나타납니다.
- 단계 2 필요에 따라 각 라이선스의 슬라이더 컨트롤을 클릭하여 라이선스를 활성화하거나 비활성화하도록 설정합니다. 활성화되면 라이선스 상태가 OK(정상)로 표시됩니다.
 - **Enabled**(활성화됨): Cisco Smart Software Manager 계정에 라이선스를 등록하고 제어되는 기능을 활성화합니다. 이제 라이선스를 통해 제어되는 정책을 구성하고 구축할 수 있습니다.
 - **Disabled**(비활성화됨): Cisco Smart Software Manager 계정에서 라이선스를 등록 취소하고 제어되는 기능을 비활성화합니다. 이렇게 하면 새 정책에서 기능을 구성할 수 없으며 해당 기능을 사용하는 정책을 구축할 수도 없습니다.
- 단계 3 **Save**(저장)를 클릭하여 변경사항을 저장합니다.

만료되거나 비활성화된 선택 가능한 라이선스의 영향

선택 가능한 라이선스가 만료되어도 해당 라이선스를 필요로 하는 기능은 계속 사용할 수 있습니다. 그러나 라이선스는 컴플라이언스 상태가 아닌 것으로 표시되며, 라이선스를 컴플라이언스 상태로 다시 설정하려면 라이선스를 구매하여 계정에 추가해야 합니다.

선택 가능한 라이선스를 비활성화하면 시스템은 다음과 같이 대응합니다.

- 악성코드 라이선스: 시스템이 AMP 클라우드 쿼리를 중지하며 AMP 클라우드에서 전송하는 회귀적 이벤트 확인도 중지합니다. 악성코드 탐지를 적용하는 파일 정책을 포함하는 기존 액세스 제어 정책은 재구축할 수 없습니다. 악성코드 라이선스가 비활성화된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 이 기간이 만료되고 나면 시스템은 해당 파일에 사용할 수 없음 상태를 할당합니다.
- : 시스템이 더 이상 침입 또는 파일 제어 정책을 적용하지 않습니다. 보안 인텔리전스 정책의 경우 시스템은 더 이상 정책을 적용하지 않고 피드 업데이트 다운로드를 중지합니다. 라이선스가 필요한 기존 정책은 재구축할 수 없습니다.
- **URL**: URL 범주 조건이 포함된 액세스 제어 규칙의 URL 필터링이 즉시 중지되며 시스템이 URL 데이터에 대한 업데이트를 더 이상 다운로드하지 않습니다. 범주 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.
- : 원격 액세스 VPN 구성을 편집할 수는 없지만, 제거할 수는 있습니다. 사용자는 RA VPN 컨피그 레이션을 사용하여 계속 연결할 수 있습니다. 그러나 디바이스 등록을 변경하여 시스템이 더 이상 내보내기 방식을 준수하지 않는 경우에는 원격 액세스 VPN 구성이 즉시 중지되며, 원격 사용자가 VPN을 통해 연결할 수 없습니다.

Firewall Device Manager 모델 생성 및 가져오기

Cisco Defense Orchestrator는 CDO 테넌트에 있는 FDM 관리 디바이스의 전체 구성을 JSON 파일 형식으로 내보낼 수 있는 기능을 제공합니다. 그런 다음 이 파일을 다른 테넌트에 Firewall Device Manager 모델로 가져와서 해당 테넌트의 새 디바이스에 적용할 수 있습니다. 이 기능은 관리하는 여러 테넌트에서 FDM 관리 디바이스의 구성을 사용하려는 경우에 유용합니다.



Note FDM 관리 디바이스에 규칙 집합이 포함되어 있으면 구성을 내보낼 때 규칙 집합과 연결된 공유 규칙이 로컬 규칙으로 수정됩니다. 나중에 모델을 다른 테넌트로 가져와 FDM 관리 디바이스에 적용하면 디바이스에 로컬 규칙이 표시됩니다.

FDM-관리 디바이스 구성 내보내기

FDM 관리 디바이스에 다음 구성이 있는 경우 구성 내보내기 기능을 사용할 수 없습니다.


- 고가용성
- Snort 3 활성화됨

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 **FTD** 탭을 클릭합니다.
 - 단계 4 FDM 관리 디바이스를 선택하고 오른쪽 창의 **Device Actions**(디바이스 작업)에서 **Export Configuration**(구성 내보내기)을 클릭합니다.
-

FDM-관리 디바이스 구성 가져오기

Procedure

- 단계 1 **Inventory**(재고 목록) 페이지에서 과란색 더하기() 버튼을 클릭하여 구성을 가져옵니다.
- 단계 2 오프라인 관리를 위해 구성을 가져오려면 **Import**(가져오기)를 클릭합니다.
- 단계 3 **Device Type**(디바이스 유형)을 **FTD**로 선택합니다.
- 단계 4 **Browse**(찾아보기)를 클릭하고 업로드할 구성 파일(JSON 형식)을 선택합니다.
- 단계 5 구성이 확인되면 디바이스 또는 서비스에 레이블을 지정하라는 메시지가 표시됩니다. 자세한 내용은 [레이블 및 레이블 그룹](#)을 참조하십시오.
- 단계 6 모델 디바이스에 레이블을 지정한 후에는 **Inventory**(재고 목록) 목록에서 볼 수 있습니다.

Note 구성의 크기 및 다른 디바이스 또는 서비스의 수에 따라 구성을 분석하는 데 시간이 걸릴 수 있습니다.

CDO에서 디바이스 삭제

CDO에서 디바이스를 삭제하려면 다음 절차를 따르십시오.

프로시저

- 단계 1 CDO에 로그인합니다.
- 단계 2 **Inventory**(인벤토리) 페이지로 이동합니다.
- 단계 3 삭제할 디바이스를 찾아 디바이스 행에서 디바이스를 확인하고 선택합니다.
- 단계 4 오른쪽에 있는 디바이스 작업 패널에서 **Remove**(제거)를 선택합니다.

단계 5 메시지가 표시되면 **OK(확인)**를 선택하여 선택한 디바이스 제거를 확인합니다. 디바이스를 온보딩 상태로 유지하려면 **Cancel(취소)**를 선택합니다.

FDM 관리 HA 쌍의 두 디바이스를 동시에 삭제해야 합니다. 개별 피어가 아닌 FDM 관리 HA 쌍 이름을 클릭합니다.

오프라인 관리를 위한 디바이스 컨피그레이션 가져오기

오프라인 관리를 위해 디바이스의 구성을 가져오면 네트워크의 라이브 디바이스에서 작업하지 않고도 디바이스의 구성을 검토하고 최적화할 수 있습니다. CDO는 이러한 업로드된 구성 파일을 "모델"이라고도 합니다.

이러한 디바이스의 구성을 CDO로 가져올 수 있습니다.

- ASA(Adaptive Security Appliance)
- FTD(Firepower Threat Defense) FTD 모델 생성 및 가져오기를 참고하십시오.
- ASR(Aggregation Services Router) 및 ISR(Integrated Services Router)과 같은 Cisco IOS 디바이스

FDM-관리 디바이스 백업

FDM 관리 디바이스를 이전 상태로 복원할 수 있도록 디바이스의 시스템 구성을 백업하는 데 Cisco Defense Orchestrator를 사용할 수 있습니다. 백업은 구성만 포함하며 시스템 소프트웨어는 포함하지 않습니다. 디바이스를 완전히 재이미징해야 하는 경우 소프트웨어를 다시 설치해야 합니다. 그런 다음 백업을 업로드하고 구성을 복원할 수 있습니다. CDO는 디바이스에 대해 만들어진 마지막 5개의 백업을 저장합니다. 새 백업이 발생하면 최신 백업을 저장하기 위해 가장 오래된 백업이 삭제됩니다.



Note 백업에는 관리 IP 주소 구성이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 구성을 복원할 수도 있습니다.

구성 데이터베이스는 백업하는 동안 잠겨 있습니다. 백업 중에는 정책, 대시보드 등을 볼 수는 있지만 구성을 변경할 수는 없습니다. 복원 중에는 시스템을 완전히 사용할 수 없게 됩니다.

여러 디바이스에서 백업 일정을 일관되게 만들기 위해 고유한 기본 백업 일정을 구성할 수 있습니다. 특정 디바이스에 대한 백업을 예약할 때 자신의 기본 설정을 사용하거나 변경할 수 있습니다. 매일에서 월 1회 반복 백업을 예약하고 주문형 백업을 수행할 수 있습니다. 백업을 다운로드한 다음 위협 방어 디바이스 관리자를 사용하여 복원할 수도 있습니다.

CDO를 사용하여 **FDM** 관리 디바이스를 백업 및 복원하기 위한 요구 사항 및 모범 사례

- CDO는 소프트웨어 버전 6.5 이상을 실행하는 FDM 관리 디바이스를 백업할 수 있습니다.

- FDM 관리 디바이스를 등록 키를 사용하여 CDO에 온보딩해야 합니다.
- 두 디바이스가 동일한 모델이며 동일한 버전의 소프트웨어(같은 시기에 릴리스되었을 뿐만 아니라 빌드 번호도 동일해야 함)를 실행하는 경우에만 교체 디바이스에 백업을 복원할 수 있습니다. 예를 들어 소프트웨어 버전 6.6.0-90을 실행하는 FDM 관리 디바이스의 백업은 6.6.0-90을 실행하는 FDM 관리 디바이스로만 복원할 수 있습니다. 백업 및 복원 프로세스를 사용하여 어플라이언스 간에 구성을 복사하지 마십시오. 백업 파일은 어플라이언스를 고유하게 식별하는 정보를 포함하므로 이러한 방식을 통해 공유할 수 없습니다.
- CDO에서 Secure Firewall Threat Defense 백업 기능이 작동하려면, 위협 방어가 테넌트 지역을 기반으로 이러한 CDO URL 중 하나에 액세스해야 합니다.
 - edge.us.cdo.cisco.com
 - edge.eu.cdo.cisco.com
 - edge.apj.cdo.cisco.com
- 포트 443에 HTTPS 프로토콜에 대한 외부 및 아웃바운드 액세스 권한이 있는지 확인합니다. 포트가 방화벽 뒤에서 차단된 경우 백업 및 복원 프로세스가 실패할 수 있습니다.

모범 사례

백업하려는 디바이스는 CDO에서 동기화됨 상태여야 합니다. CDO는 CDO가 아닌 디바이스에서 디바이스 구성을 백업합니다. 따라서 디바이스가 동기화되지 않은 상태이면 CDO의 변경 사항이 백업되지 않습니다. 디바이스가 충돌 감지 상태이면 해당 변경 사항이 백업됩니다.

관련 정보:

- [모든 FDM 매니지드 디바이스에 대한 기본 반복 백업 일정 구성](#)
- [단일 FDM-관리 디바이스에 대한 반복 백업 일정 구성](#)
- [FDM-관리 온디맨드 디바이스 백업](#)
- [디바이스 백업 다운로드](#)
- [백업 편집](#)
- [FDM-관리 디바이스에 백업 복원, on page 54](#)

FDM-관리 온디맨드 디바이스 백업

이 절차는 필요한 경우 복원할 수 있도록 FDM 관리 디바이스를 백업하는 방법을 설명합니다.

시작하기 전에

FDM 관리 디바이스를 백업하기 전에 이러한 [FDM-관리 디바이스 백업](#)를 검토하십시오.

절차

Procedure

- 단계 1 (선택 사항) 백업에 대한 [변경 요청](#)을 생성합니다.
- 단계 2 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 3 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 4 **FTD** 탭을 클릭하고 백업할 디바이스를 선택합니다.
- 단계 5 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Backups**(백업 관리)를 클릭합니다.
- 단계 6 **Backup Now**(지금 백업)를 클릭합니다. 디바이스가 **Backing Up**(백업 중) 구성 상태로 전환됩니다.

백업이 완료되면 Cisco Defense Orchestrator는 백업이 시작되기 전의 디바이스 구성 상태를 표시합니다. 변경 로그 페이지를 열어 "**Backup completed successfully**(백업이 성공적으로 완료되었습니다)."라는 설명이 포함된 최근 변경 로그 레코드를 찾을 수도 있습니다.

1단계에서 변경 요청을 생성한 경우 해당 값으로 필터링하여 변경 로그 항목을 찾을 수도 있습니다.

- 단계 7 1단계에서 변경 요청을 생성한 경우 더 이상 예기치 않게 변경 사항을 변경 요청과 연결하지 않도록 변경 요청 값을 지우십시오.

단일 FDM-관리 디바이스에 대한 반복 백업 일정 구성

시작하기 전에

FDM 관리 디바이스를 백업하기 전에 이러한 [FDM-관리 디바이스 백업](#)를 검토하십시오.

절차

Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭하고 백업할 디바이스를 선택합니다.
- 단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Manage Backups**(백업 관리)를 클릭합니다.
- 단계 5 **Device Backups**(디바이스 백업) 페이지에서 **Set Recurring Backup**(반복 백업 설정)을 클릭하거나 **Recurring Backup**(반복 백업) 필드에서 일정을 클릭합니다. CDO는 테넌트의 모든 FDM 관리 디바이스에 대한 기본 백업 일정을 제공합니다. 자세한 내용은 [모든 FDM 매니지드 디바이스에 대한 기본 반복 백업 일정 구성](#)을 참조하십시오.
- 단계 6 백업을 수행할 시간을 24시간 단위로 선택합니다. UTC(Coordinated Universal Time) 시간대로 시간을 예약합니다.

단계 7 Frequency(빈도) 필드에서 매일, 매주 또는 매월을 선택합니다.

- Daily backups(매일 백업): 예약된 백업에 이름과 설명을 지정합니다.
- Weekly backups(매주 백업): 백업을 수행할 요일을 선택합니다. 예약된 백업 시간에 이름과 설명을 지정합니다.
- Monthly backups(매월 백업): 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 8 Save(저장)를 클릭합니다. Device Backup(디바이스 백업) 페이지에서 Recurring Backup(반복 백업) 필드가 사용자가 설정한 백업 일정으로 교체되고 로컬 시간이 반영됩니다.

디바이스 백업 다운로드

이 절차는 FDM 관리 디바이스의 백업이 포함된 .tar 파일을 다운로드하는 방법을 설명합니다.


Procedure

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

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭과 다운로드할 백업이 있는 디바이스를 클릭합니다.

단계 4 오른쪽의 작업 창에서 **Manage Backups**(백업 관리)를 클릭합니다.

단계 5 다운로드할 백업을 선택하고 해당 행에서 다운로드 링크 생성 버튼 를 클릭합니다. 버튼이 "백업 이미지 다운로드"로 변경됩니다.


단계 6 이제 버튼에 백업 이미지 다운로드가 표시됩니다. 다음 중 하나를 수행합니다.

- 복원하려는 디바이스의 Firewall Device Manager에도 연결할 수 있는 디바이스에 있는 경우 백업 이미지 다운로드 버튼을 클릭하고 다운로드한 파일을 저장합니다. 기억할 수 있는 이름으로 저장하십시오.
- 복원하려는 디바이스의 FDM에도 연결할 수 있는 디바이스에 있지 않은 경우:
 - a. 백업 이미지 다운로드 버튼을 마우스 오른쪽 버튼으로 클릭하고 링크 주소를 복사합니다.
Important 링크 주소는 다운로드 링크 생성 버튼을 클릭한 후 15분이 지나면 만료됩니다.
 - b. 이미지를 복원하려는 Secure Firewall Threat Defense의 Firewall Device Manager에 도달하는 디바이스에서도 브라우저를 엽니다.
 - c. 브라우저 주소 표시줄에 다운로드 링크를 입력하고 해당 디바이스에 백업 파일을 다운로드합니다. 기억할 수 있는 이름으로 저장하십시오.

백업 편집

이 절차를 통해 성공적인 FDM 관리 디바이스 다운로드의 이름 또는 설명을 편집할 수 있습니다.


Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭하고 편집할 디바이스를 선택합니다.
- 단계 4 오른쪽의 작업 창에서 **Manage Backups**(백업 관리)를 클릭합니다.
- 단계 5 편집할 백업과 해당 행을 선택하고 편집 아이콘  를 클릭합니다.
- 단계 6 백업의 이름이나 설명을 변경합니다. 디바이스 백업 페이지에서 새 정보를 볼 수 있습니다.

백업 삭제

CDO는 디바이스에 대해 생성된 마지막 5개의 백업을 저장합니다. 새 백업이 발생하면 최신 백업을 저장하기 위해 가장 오래된 백업이 삭제됩니다. 기존 백업을 삭제하면 보관할 백업과 삭제할 백업을 관리하는 데 도움이 될 수 있습니다.

Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭하고 삭제할 디바이스를 선택합니다.
- 단계 4 오른쪽의 Actions(작업) 창에서 **Manage Backups**(백업 관리)를 클릭합니다.
- 단계 5 삭제할 백업과 해당 행을 선택하고 휴지통  아이콘을 클릭합니다.
- 단계 6 **OK**(확인)를 클릭하여 확인합니다.

디바이스 백업 관리

Cisco Defense Orchestrator를 사용하여 생성하는 FDM 관리 디바이스의 백업은 **Device Backups**(디바이스 백업) 페이지에서 확인할 수 있습니다.

Procedure

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

단계 3 **FTD** 탭을 클릭합니다.

단계 4 디바이스 테이블에 FDM 관리 디바이스만 표시하려면 필터 아이콘을 클릭하고 **Devices/Services**(디바이스/서비스) 아래에서 **FDM**을 선택합니다.

단계 5 원하는 디바이스를 선택합니다.

단계 6 **Device Actions**(디바이스 작업) 창에서 **Manage Backups**(백업 관리)를 클릭합니다. 해당 디바이스의 최신 백업을 5개까지 볼 수 있습니다.

What to do next

백업을 복구하려면 [FDM-관리 디바이스에 백업 복원, on page 54](#)의 내용을 참조하십시오.

FDM-관리 디바이스에 백업 복원

FDM 관리 관리 위협 방어 디바이스의 백업을 복원하기 전에 이 정보를 검토하십시오.

- FDM 관리 위협 방어 디바이스를 복원하기 전에 이러한 [FDM-관리 디바이스 백업](#)를 검토하십시오.
- 복원하려는 백업 복사본이 디바이스에 아직 없는 경우 복원 전에 백업을 먼저 업로드해야 합니다.
- 복원 중에는 시스템을 완전히 사용할 수 없게 됩니다. 백업이 복원되면 디바이스가 재부팅됩니다.
- 이 절차에서는 디바이스에 복원할 준비가 된 디바이스의 기존 백업이 있다고 가정합니다.
- 디바이스가 고가용성 쌍의 일부인 경우 백업을 복원할 수 없습니다. 먼저 **Device**(디바이스) > **High Availability**(고가용성) 페이지에서 **HA**를 해제해야 백업을 복원할 수 있습니다. 백업이 **HA** 구성을 포함하는 경우 디바이스가 **HA** 그룹에 다시 조인합니다. 두 유닛에서 동일한 백업을 복원하지 마십시오. 이렇게 하면 두 유닛이 모두 액티브로 설정됩니다. 대신 액티브로 설정할 유닛에서 백업을 먼저 복원한 후에 다른 유닛에서 해당하는 백업을 복원합니다.



Note 백업에는 관리 IP 주소 구성이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 구성을 복원할 수도 있습니다.


Procedure

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

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭하고 복원할 디바이스를 선택합니다.

단계 4 오른쪽의 **Device Actions**(장치 작업)에서 **Manage Backups**(백업 관리)를 클릭합니다.

단계 5 복원하려는 백업을 선택합니다. 해당 행에서 다운로드 링크 생성 버튼 를 클릭합니다.

Note 링크 주소는 다운로드 링크 생성 버튼을 클릭한 후 15분이 지나면 만료됩니다.

단계 6 이제 버튼에 백업 이미지 다운로드가 표시됩니다. 다음 중 하나를 수행합니다.

- 복원하려는 디바이스의 Firewall Device Manager에도 연결할 수 있는 디바이스에 있는 경우 백업 이미지 다운로드 버튼을 클릭하고 다운로드한 파일을 저장합니다. 기억할 수 있는 이름으로 저장하십시오.
- 복원하려는 디바이스의 firewall device manager에도 연결할 수 있는 디바이스에 있지 않은 경우:
 - a. 백업 이미지 다운로드 버튼을 마우스 오른쪽 버튼으로 클릭하고 링크 주소를 복사합니다.
 - b. 이미지를 복원하려는 firewall device manager에 도달하는 디바이스에서도 브라우저를 엽니다.
 - c. 브라우저 주소 표시줄에 다운로드 링크를 입력하고 해당 디바이스에 백업 파일을 다운로드합니다. 기억할 수 있는 이름으로 저장하십시오.

단계 7 복원하려는 디바이스의 Firewall Device Manager에 로그인합니다.

단계 8 [Firepower Device Manager용 Cisco Firepower Threat Defense 컨피그레이션 가이드](#) 버전 6.5 이상을 엽니다. 시스템 관리 창으로 이동하여 백업 복원을 검색합니다. 해당 지침에 따라 방금 FDM 관리 디바이스에 다운로드한 이미지를 복원하십시오.

Tip 이미지를 복원하려면 firewall device manager에 이미지를 업로드해야 합니다.

단계 9 firewall device manager의 프롬프트를 따르십시오. 복원이 시작되면 브라우저와 firewall device manager의 연결이 끊어집니다. 복원이 완료되면 디바이스가 재부팅됩니다.

관련 정보:

- [FDM-관리 디바이스 백업](#)
- [FDM-관리 온디맨드 디바이스 백업](#)
- [단일 FDM-관리 디바이스에 대한 반복 백업 일정 구성](#)
- [디바이스 백업 다운로드](#)
- [백업 편집](#)

FDM 소프트웨어 업그레이드 경로

FDM 버전 업그레이드

CDO를 사용하여 FDM 관리 방화벽을 업그레이드하는 경우, CDO가 업그레이드할 수 있는 버전을 결정하며 이 항목은 필요하지 않습니다. FDM 이미지의 자체 저장소를 유지 관리하고 자체 이미지를 사

용하여 FDM 관리 디바이스를 업그레이드하는 경우, 이 주제에서는 사용할 수 있는 업그레이드 경로에 대해 설명합니다.

FDM 관리 디바이스를 하나의 주요 또는 유지 보수 버전에서 다른 버전으로 직접 업그레이드할 수 있습니다. 예를 들어 버전 6.4.0을 6.5.0으로, 또는 버전 6.4.0을 7.0.1으로 업그레이드 할 수 있습니다. 특정 패치 레벨을 실행할 필요는 없습니다.

직접 업그레이드가 불가능한 경우 업그레이드 경로에 중간 버전(예: 버전 6.4.0 > 7.0.0 > 7.1.0)이 포함되어야 합니다.

Table 3: 주요 릴리스의 업그레이드 경로

대상 버전	대상 버전으로 업그레이드할 수 있는 가장 오래된 릴리스
7.3.x	7.0.0
7.2.x	6.6.0
7.1.x	6.5.0
7.0.x	6.4.0
6.7.x	6.4.0
6.6.x	6.4.0
6.5.0	6.4.0

FDM 관리 디바이스 구성

한 버전의 패치를 다른 버전의 패치로 직접 업그레이드할 수 없습니다(예: 버전 6.4.0.1 > 6.5.0.1). 먼저 주요 릴리스로 업그레이드한 다음 해당 릴리스를 패치해야 합니다. 예를 들어 버전 6.4.0.1 > 6.5.0 > 6.5.0.1로 업그레이드해야 합니다.

Firepower 핫픽스

CDO는 핫픽스 업데이트 또는 설치를 지원하지 않습니다. 디바이스 모델 또는 소프트웨어 버전에 사용 가능한 핫픽스가 있는 경우 구성된 관리자의 대시보드 또는 UI를 사용하는 것이 좋습니다. 디바이스에 핫픽스가 설치되면 CDO가 대역 외 구성 변경 사항을 탐지합니다.

FDM 업그레이드 제거

CDO를 사용하여 주요 릴리스, 유지 보수 또는 패치 릴리스 유형을 제거하거나 다운그레이드할 수 없습니다.

Secure Firewall Threat Defense defense 버전 6.7.0부터는 Firepower Device Manager 또는 FTD CLI를 사용하여 성공적으로 업그레이드된 디바이스를 마지막 주요 또는 유지 보수 업그레이드 직전의 상태로 되돌릴 수 있습니다(스냅샷이라고도 함). 패치를 적용한 후 되돌리면 패치도 제거됩니다. 되돌린 후에는 업그레이드와 되돌리기 사이에 변경한 모든 구성을 다시 적용해야 합니다. FDM 버전 6.5.0~6.6.x로의 주요 또는 유지 보수 업그레이드를 되돌리려면 이미지를 재설치해야 합니다. 자세한 내용은

[Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 관리" 섹션을 참조하십시오.

FDM 패치 제거

CDO 또는 FDM을 사용하여 FDM 패치를 제거할 수 없습니다. 패치를 제거하려면 주 또는 유지 보수 릴리스로 이미지 재설치해야 합니다.

Snort 업그레이드

Snort는 제품의 기본 검사 엔진이며 사용자의 편의를 위해 Secure Firewall Threat Defense 소프트웨어에 패키징됩니다. 버전 6.7에는 언제든지 업그레이드하거나 되돌릴 수 있는 패키지 업데이트가 도입되었습니다. Snort 버전을 자유롭게 전환할 수는 있지만, Snort 2.0의 일부 침입 규칙은 Snort 3.0에는 없을 수 있으며 그 반대의 경우도 마찬가지입니다. 자세한 내용은 버전 6.7.0용 Firepower Device Manager 구성 가이드에서 차이점을 참조하십시오.

CDO UI에서 Snort 3을 사용하도록 FDM 관리 디바이스를 업그레이드하거나 Snort 3에서 Snort 2로 다시 되돌리려면 FTD의 경우 각각 [Snort 3.0으로 업그레이드](#) 및 [FDM-관리 디바이스용 Snort 3.0에서 되돌리기](#)를 참조하십시오.

기타 업그레이드 제한 사항

2100 시리즈

CDO는 어플라이언스 모드를 실행 중인 경우에만 Firepower 2100 Series 디바이스를 업그레이드할 수 있습니다.

- Firepower Threat Defense 디바이스는 항상 어플라이언스 모드입니다.

다음에 수행할 작업

이러한 명령에 대한 자세한 내용은 "[Cisco Firepower 2100 시작 가이드](#)"를 참조하십시오.

4100 및 9300 Series 디바이스

CDO는 4100 또는 9300 Series 디바이스에 대한 업그레이드를 지원하지 않습니다. 이러한 디바이스는 CDO 외부에서 업그레이드해야 합니다.

관련 정보:

- [FDM-관리 디바이스 업그레이드 사전 요건](#)
- [단일 FTD 디바이스 업그레이드](#).
- [대량 FDM-관리 디바이스 업그레이드](#)
- [FDM-관리 고가용성 쌍 업그레이드](#)

FDM-관리 디바이스 업그레이드 사전 요건

Cisco Defense Orchestrator(CDO)는 개별 디바이스 또는 HA 쌍에 설치된 Firewall Device Manager(FDM) 이미지를 업그레이드하는 데 도움이 되는 마법사를 제공합니다.

마법사는 호환 가능한 이미지를 선택하고 설치하고 디바이스를 재부팅하여 업그레이드를 완료하는 프로세스를 안내합니다. Cisco에서는 CDO에서 선택한 이미지가 FDM 관리 디바이스에 복사되고 설치된 이미지인지 확인하여 업그레이드 프로세스를 보호합니다. 업그레이드하는 FDM 관리 디바이스는 인터넷에 대한 아웃바운드 액세스 권한이 있어야 합니다.

FDM 관리 디바이스에 인터넷에 대한 아웃바운드 액세스 권한이 없는 경우 Cisco.com에서 원하는 이미지를 다운로드하여 자체 저장소에 저장하고 업그레이드 마법사에 해당 이미지에 대한 맞춤형 URL을 제공하면 CDO가 해당 이미지를 사용하여 업그레이드를 수행할 수 있습니다. 그러나 이 경우에는 어떤 이미지로 업그레이드할지 결정합니다. CDO는 이미지 무결성 확인 또는 디스크 공간 확인을 수행하지 않습니다.

컨피그레이션 사전 요구 사항

- FDM 관리 디바이스에서 DNS를 활성화해야 합니다. 자세한 내용은 디바이스에서 실행 중인 버전의 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)의 시스템 관리 장의 "DNS 구성" 섹션을 참조하십시오.
- CDO의 이미지 저장소에서 업그레이드 이미지를 사용하는 경우 FDM 관리 디바이스에서 인터넷에 연결할 수 있어야 합니다.
- FDM 관리 디바이스가 CDO에 성공적으로 온보딩되었습니다.
- FDM 관리 디바이스에 연결할 수 없습니다.
- FDM 관리 디바이스가 동기화됩니다.
 - CDO에서 보류 중인 변경 사항이 있는 디바이스를 업데이트하고 변경 사항을 수락하지 않으면 업그레이드가 완료된 후 보류 중인 변경 사항이 손실됩니다. 업그레이드하기 전에 보류 중인 변경 사항을 구축하는 것이 가장 좋습니다.
 - firewall device manager에서 변경 사항을 준비했으며 디바이스가 동기화되지 않은 경우 자격 확인 시 CDO에서 업그레이드가 실패합니다.

FTD를 실행하는 4100 및 9300 Series

CDO는 4100 또는 9300 Series 디바이스에 대한 업그레이드를 지원하지 않습니다. 이러한 디바이스는 CDO 외부에서 업그레이드해야 합니다.

소프트웨어 및 하드웨어 요구 사항

CDO는 클라우드 관리 플랫폼입니다. 소프트웨어 업데이트는 시간이 지남에 따라 릴리스되며 일반적으로 하드웨어에 의존하지 않습니다. 지원되는 하드웨어 유형에 대한 자세한 내용은 [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 참조하십시오.

firewall device manager 소프트웨어를 실행하는 디바이스에는 최적의 성능을 위한 권장 업그레이드 경로가 있습니다. 자세한 내용은 [FDM 소프트웨어 업그레이드 경로](#)를 참조하십시오.

업그레이드 참고 사항

업그레이드 중에는 디바이스에 변경 사항을 구축할 수 없습니다.

관련 정보:

- [FDM 소프트웨어 업그레이드 경로](#)
- [단일 FTD 디바이스 업그레이드](#)
- [대량 FDM-관리 디바이스 업그레이드](#)
- [FDM-관리 고가용성 쌍 업그레이드](#)

단일 FTD 디바이스 업그레이드

시작하기 전에

업그레이드하기 전에 [FDM-관리 디바이스 업그레이드 사전 요건](#), [FDM 소프트웨어 업그레이드 경로](#), [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 자세히 읽어보십시오. 이 문서에서는 원하는 Firepower 소프트웨어 버전으로 업그레이드하기 전에 알아야 할 모든 요구 사항 및 경고에 대해 설명합니다.

Cisco Defense Orchestrator 저장소의 이미지로 단일 FDM-관리 디바이스 업그레이드

CDO의 저장소에 저장된 소프트웨어 이미지를 사용하여 독립형 FDM 관리 디바이스를 업그레이드하려면 다음 절차를 수행합니다.

Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 업그레이드할 디바이스를 선택합니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 6 1단계에서 **Use CDO Image Repository**(CDO 이미지 저장소 사용)를 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
- 단계 7 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.

- 단계 8 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.
- Warning** 진행 중인 업그레이드를 취소하려면 **Upgrade**(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 확인하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 9 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 10 **알림** 탭에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **Jobs(작업) 페이지**로 이동합니다.
- 단계 11 시스템 데이터베이스를 업그레이드합니다. **Firewall Device Manager**에서 이 단계를 수행해야 합니다. 자세한 내용은 **Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드**의 "시스템 데이터베이스 업데이트"를 참조하십시오.

자체 저장소의 이미지로 단일 FDM-관리 디바이스 업그레이드

소프트웨어 이미지를 찾기 위해 URL 프로토콜을 사용하여 독립형 FDM 관리 디바이스를 업그레이드하려면 다음 절차를 수행합니다.

Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 업그레이드할 디바이스를 선택합니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 6 1단계에서 **Specify Image URL**(이미지 URL 지정)을 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
- 단계 7 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 8 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

Warning 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 Cisco Defense Orchestrator는 디바이스에서 변경 사항을 구축하거나 확인하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.

단계 9 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 Schedule Upgrade(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 Schedule Upgrade(업그레이드 예약) 버튼을 클릭합니다.

단계 10 알림 탭에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 Review(검토) 링크를 클릭합니다. 그러면 Jobs(작업) 페이지로 이동합니다.

단계 11 시스템 데이터베이스를 업그레이드합니다. Firewall Device Manager에서 이 단계를 수행해야 합니다. 자세한 내용은 [Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 데이터베이스 업데이트"를 참조하십시오.

업그레이드 프로세스 모니터링

Inventory(재고 목록) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 단일 디바이스의 진행 상황을 볼 수 있습니다. CDO에서 해당 디바이스의 Device Upgrade(디바이스 업그레이드) 페이지로 이동합니다.

업그레이드가 실패하면 CDO는 메시지를 표시합니다. CDO는 업그레이드 프로세스를 자동으로 다시 시작하지 않습니다.



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

대량 FDM-관리 디바이스 업그레이드

시작하기 전에

업그레이드하기 전에 [FDM-관리 디바이스 업그레이드 사전 요건](#), [FDM 소프트웨어 업그레이드 경로](#), [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 자세히 읽어보십시오. 이 문서에서는 원하는 Firepower 소프트웨어 버전으로 업그레이드하기 전에 알아야 할 모든 요구 사항 및 경고에 대해 설명합니다.



Note 모두 동일한 소프트웨어 버전으로 업그레이드하는 경우에만 FDM 관리 디바이스를 대량 업그레이드할 수 있습니다.

Cisco Defense Orchestrator 저장소의 이미지로 대량 FDM-관리 디바이스 업그레이드

CDO의 저장소에 저장된 소프트웨어 이미지를 사용하여 여러 FDM 관리 디바이스를 업그레이드하려면 다음 절차를 수행합니다.

Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 **필터**를 사용하여 대량 업그레이드에 포함할 디바이스 목록을 좁힐 수 있습니다.
- 단계 5 필터링된 디바이스 목록에서 업그레이드할 디바이스를 선택합니다.
- 단계 6 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 7 **Bulk Device Upgrade**(대량 디바이스 업그레이드) 페이지에 업그레이드할 수 있는 디바이스가 표시됩니다. 선택한 디바이스 중 업그레이드할 수 없는 디바이스가 있으면 CDO에서 업그레이드할 수 없는 디바이스를 볼 수 있는 링크를 제공합니다.
- 단계 8 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 9 1단계에서 **Use CDO Image Repository**(CDO 이미지 저장소 사용)를 클릭하여 업그레이드할 소프트웨어 이미지를 선택합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다. **Continue**(계속)를 클릭합니다.
- 단계 10 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 11 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

Warning 진행 중인 업그레이드를 취소하려면 **Upgrade**(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드를 시작한 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 롤링하지 않습니다. 업그레이드를 취소한 후에도 디바이스가 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 12 **알림** 탭에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **Jobs**(작업) 페이지로 이동합니다.
- 단계 13 시스템 데이터베이스를 업그레이드합니다. **Firewall Device Manager**에서 이 단계를 수행해야 합니다. 디바이스가 실행 중인 버전에 대한 **Firepower Device Manager**용 [Cisco Firepower Threat Defense 구성 가이드](#)의 시스템 데이터베이스 업데이트를 참조하십시오.

자체 저장소의 이미지를 사용하여 대량 FDM-관리 디바이스 업그레이드

소프트웨어 이미지를 찾기 위해 URL 프로토콜을 사용하여 여러 FDM 관리 디바이스를 업그레이드 하려면 다음 절차를 수행합니다.

Procedure

- 단계 1 내비게이션 바에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 **필터**를 사용하여 대량 업그레이드에 포함할 디바이스 목록을 좁힐 수 있습니다.
- 단계 5 필터링된 디바이스 목록에서 업그레이드할 디바이스를 선택합니다.
- 단계 6 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 7 **Bulk Device Upgrade**(대량 디바이스 업그레이드) 페이지에 업그레이드할 수 있는 디바이스가 표시됩니다. 선택한 디바이스 중 업그레이드할 수 없는 디바이스가 있으면 Cisco Defense Orchestrator에서 업그레이드할 수 없는 디바이스를 볼 수 있는 링크를 제공합니다.
- 단계 8 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 9 1단계에서 **Specify Image URL**(이미지 URL 지정)을 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다.
- 단계 10 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 11 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

Warning 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 폴링하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 12 **알림 탭**에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **Jobs**(작업) 페이지로 이동합니다.
- 단계 13 시스템 데이터베이스를 업그레이드합니다. Firewall Device Manager에서 이 단계를 수행해야 합니다. 자세한 내용은 [Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드](#)의 "시스템 데이터베이스 업데이트"를 참조하십시오.

대량 업그레이드 프로세스 모니터링

Inventory(인벤토리) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 벌크 업그레이드에 포함된 단일 디바이스의 진행 상황을 볼 수 있습니다. 탐색 창에서 **Jobs**(작업)을 클릭하고 대량 작업을 확장하여 진행 세부 정보를 볼 수도 있습니다.

업그레이드가 실패하면 CDO는 메시지를 표시합니다. CDO는 업그레이드 프로세스를 자동으로 다시 시작하지 않습니다.

FDM-관리 고가용성 쌍 업그레이드

트래픽 중단 없이 HA 쌍을 업그레이드합니다. 스탠바이 디바이스는 보조 디바이스가 업그레이드되는 동안 트래픽 탐지를 계속 처리합니다.

HA 쌍을 업그레이드할 때 CDO는 업그레이드를 시작하기 전에 자격 확인을 실행하고 이미지 위치를 복사하거나 식별합니다. 고가용성 쌍의 보조 디바이스는 현재 액티브 디바이스인 경우에도 먼저 업그레이드됩니다. 보조 디바이스가 액티브 디바이스인 경우 페어링된 디바이스는 업그레이드 프로세스의 역할을 자동으로 전환합니다. 보조 디바이스가 성공적으로 업그레이드되면 디바이스가 역할을 전환한 다음 새 스탠바이 디바이스가 업그레이드됩니다. 업그레이드가 완료되면 기본 디바이스가 액티브 상태가 되고 보조 디바이스가 스탠바이 상태가 되도록 디바이스가 자동으로 구성됩니다.

업그레이드 프로세스 중에는 HA 쌍에 구축하지 않는 것이 좋습니다.

시작하기 전에

- 업그레이드하기 전에 보류 중인 모든 변경 사항을 액티브 디바이스에 구축합니다.
- 업그레이드 중에 실행 중인 작업이 없는지 확인합니다.
- HA 쌍의 두 디바이스가 모두 정상입니다.
- 업그레이드할 준비가 되었는지 확인합니다. CDO에서는 이전 버전으로 롤백할 수 없습니다.
- [FDM-관리 디바이스 업그레이드 사전 요건](#), [FDM 소프트웨어 업그레이드 경로](#), [CDO에서 지원하는 소프트웨어 및 하드웨어](#)를 읽고 업그레이드 프로세스 중에 발생할 수 있는 요구 사항 및 경고를 검토합니다.

Cisco Defense Orchestrator 저장소의 이미지로 FDM-관리 HA 쌍 업그레이드

CDO의 저장소에 저장된 소프트웨어 이미지를 사용하여 FDM 관리 HA 쌍을 업그레이드하려면 다음 절차를 수행합니다.

Procedure

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

- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 업그레이드할 HA 쌍을 선택합니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 6 1단계에서 **Use CDO Image Repository**(CDO 이미지 저장소 사용)를 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
- 단계 7 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 8 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.
- Warning** 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 폴링하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 9 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 10 **알림 탭**에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **Jobs**(작업) 페이지로 이동합니다.
- 단계 11 시스템 데이터베이스를 업그레이드합니다. 이 단계는 FDM에서 수행해야 합니다. 자세한 내용은 **Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드**의 "시스템 데이터베이스 업데이트"를 참조하십시오.

자체 저장소의 이미지로 FDM-관리 HA 쌍 업그레이드

소프트웨어 이미지를 찾기 위해 URL 프로토콜을 사용하여 FDM 관리 HA 쌍을 업그레이드하려면 다음 절차를 수행합니다.

Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭하여 디바이스를 찾습니다.
- 단계 3 **FTD** 탭을 클릭합니다.
- 단계 4 업그레이드할 HA 쌍을 선택합니다.
- 단계 5 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.

- 단계 6** 1단계에서 **Specify Image URL**(이미지 URL 지정)을 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시 됩니다.
- 단계 7** 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
- 단계 8** 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.
- Warning** 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 Cisco Defense Orchestrator는 디바이스에서 변경 사항을 구축하거나 폴링하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.
- 단계 9** 또는 CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다. 완료되면 **Schedule Upgrade**(업그레이드 예약) 버튼을 클릭합니다.
- 단계 10** **알림 탭**에서 대량 업그레이드 작업의 진행 상황을 확인합니다. 대량 업그레이드 작업의 성공 또는 실패에 대한 자세한 내용을 보려면 파란색 **Review**(검토) 링크를 클릭합니다. 그러면 **Jobs(작업) 페이지**로 이동합니다.
- 단계 11** 시스템 데이터베이스를 업그레이드합니다. Firewall Device Manager에서 이 단계를 수행해야 합니다. 자세한 내용은 **Firepower Device Manager 버전 6.4용 Cisco Firepower Threat Defense 구성 가이드**의 "시스템 데이터베이스 업데이트"를 참조하십시오.

업그레이드 프로세스 모니터링

Inventory(재고 목록) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 단일 디바이스의 진행 상황을 볼 수 있습니다. Cisco Defense Orchestrator에서 해당 디바이스의 **Device Upgrade**(디바이스 업그레이드) 페이지로 이동합니다.

업그레이드 중에 시스템은 시스템 라이브러리를 업데이트하는 동안 HA를 일시 중단합니다. 여기에는 자동 구축이 포함되며 전체 업그레이드 프로세스 동안 정상 상태가 아닐 수 있습니다. 이것은 예상되는 동작입니다. 이 프로세스의 마지막 부분을 수행하는 동안에는 SSH 연결에 디바이스를 사용할 수 있으므로 업그레이드를 적용한 후 바로 로그인하는 경우 HA가 일시 중단된 상태로 표시될 수 있습니다. 업그레이드 프로세스 중에 시스템에 문제가 발생하고 HA 썬이 일시 중단된 것으로 보이는 경우, 액티브 디바이스의 Firewall Device Manager 콘솔에서 HA를 수동으로 재개합니다.



Note 업그레이드가 실패할 경우 CDO에서 메시지를 표시합니다. CDO는 업그레이드 프로세스를 자동으로 재시작하지 않습니다.

**Warning**

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

Snort 3.0으로 업그레이드

Snort 3은 최신 snort 엔진 또는 Firepower 버전 6.7 이상에서 사용 가능한 오픈 소스 IPS(Intrusion Prevention System)를 사용하는 강력한 전처리기입니다. Snort 엔진은 악의적인 네트워크 활동을 정의하는 데 도움이 되는 일련의 규칙을 사용하며, 이러한 규칙을 사용하여 일치하는 패킷을 찾고 사용자에게 알림을 생성하며 이상적으로는 패킷 스니퍼, 패킷 로거 또는 더 전통적으로는 독립형 네트워크 IPS로 사용됩니다.

Snort 3에서는 이제 사용자 지정 침입 정책을 생성할 수 있습니다. Snort 3를 실행하는 모든 FDM 관리 디바이스에는 Cisco의 Talos Intelligence Group(Talos)에서 사전 정의된 침입 정책 집합이 있습니다. Snort 3에서는 이러한 기본 정책을 변경할 수 있지만, 보다 강력한 정책을 위해 기반 위에 구축하는 것이 좋습니다.

Snort 2에서는 맞춤형 정책을 생성할 수 없습니다.

Snort 2에서 Snort 3으로 전환

Snort 버전을 자유롭게 전환할 수는 있지만, Snort 2.0의 일부 침입 규칙은 Snort 3.0에는 없을 수 있으며 그 반대의 경우도 마찬가지입니다. 기존 규칙에 대한 규칙 동작을 변경한 경우에는 해당 변경 사항이 유지되지 않습니다. 해당 변경 사항은 Snort 3으로 전환했다가 다시 Snort 2로 전환하거나 Snort 3으로 다시 전환하는 경우에는 유지되지 않습니다. 두 버전에 모두 있는 규칙의 규칙 동작에 대한 변경 사항은 유지됩니다. Snort 3과 Snort 2의 규칙 간 매핑은 일대일 또는 일대 다수가 될 수 있으므로 변경 사항을 가장 효과적으로 유지할 수 있습니다.

Snort 2에서 Snort 3으로 업그레이드하도록 선택하는 경우 Snort 엔진 업그레이드는 시스템 업그레이드와 유사합니다. 네트워크에 대한 트래픽 모니터링 중단을 최소화하려면 유지 보수 기간에 업그레이드하는 것이 좋습니다. Snort 버전 전환이 규칙이 트래픽을 처리하는 방식에 미치는 영향에 대해서는 *Firepower Device Manager* 구성 가이드의 [침입 정책 관리\(Snort3\)](#)를 참조하십시오.

**Tip**

Inventory(재고 목록) 페이지에서 Snort 버전으로 필터링할 수 있으며, 선택한 디바이스의 **Details**(세부 정보) 창에 디바이스에서 실행 중인 현재 버전이 표시됩니다.

Snort 3 제한 사항

라이선스 요건

Snort 엔진이 침입 및 악성코드 애널리틱스를 위해 트래픽을 처리하도록 허용하려면 FDM 관리 디바이스에 대해 활성화된 라이선스가 있어야 합니다. Firewall Device Manager를 통해 이 라이선스를 활성화하려면 Firewall Device Manager UI에 로그인하고 **Device**(디바이스) > **View Configuration**(구성 보기) > **Enable/Disable**(활성화/비활성화)로 이동하여 라이선스를 활성화합니다.

하드웨어 지원

다음 디바이스는 Snort 3을 지원합니다.

- FTD 1000 Series
- FTD 2100 Series
- FTD 4100 Series
- AWS를 사용하는 FTD 가상
- Azure를 사용하는 FTD 가상
- FTD를 사용하는 ASA 5500-X 시리즈

소프트웨어 지원

디바이스는 Firewall Device Manager 버전 6.7 이상을 실행하고 있어야 합니다. Cisco Defense Orchestrator에서는 버전 6.7 이상을 실행하는 디바이스에 대해 Snort 3 기능을 지원합니다.

FTD 1000 및 2000 Series의 경우 FXOS 패치 지원에 대한 자세한 내용은 [FXOS 번들 지원](#)을 참조하십시오.

구성 제한 사항

디바이스에 다음 구성이 있는 경우 CDO는 Snort 3으로의 업그레이드를 지원하지 않습니다.

- 디바이스가 버전 6.7 이상에서 실행되고 있지 않습니다.
- 디바이스에 보류 중인 변경 사항이 있는 경우 업그레이드하기 전에 변경 사항을 구축합니다.
- 디바이스가 현재 업그레이드 중인 경우 디바이스가 동기화될 때까지 디바이스를 업그레이드하거나 구축하지 마십시오.
- 디바이스가 가상 라우터로 구성된 경우



Note Snort 버전을 업그레이드하거나 되돌리는 경우, 시스템은 Snort 2 침입 정책과 Snort 3 침입 정책 간의 변경 사항을 구현하기 위해 자동으로 구축됩니다.

규칙 집합 및 Snort 3

현재 Snort 3은 전체 기능을 지원하지 않습니다. CDO 규칙 집합은 Snort 3 디바이스에서 지원되지 않습니다. 디바이스를 Firewall Device Manager 6.7 이상으로 동시에 업그레이드하고 Snort 2에서 Snort 3로 업그레이드하는 경우, 업그레이드 전에 구성된 모든 규칙 집합이 분리되고 그 안의 규칙이 개별 규칙으로 저장됩니다.

Snort 3에 대해 구성된 디바이스와 관련된 규칙 집합 지원의 전체 목록은 [규칙 집합](#)의 내용을 참조하십시오.

동시에 디바이스와 침입 방지 엔진 업그레이드

CDO를 사용하면 디바이스를 버전 6.7 및 Snort 3로 업그레이드할 수 있습니다. 다음 절차를 사용하여 FTD 시스템을 업그레이드합니다.

Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
 - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
 - 단계 3 **FTD** 탭을 클릭하고 업그레이드할 디바이스를 하나 이상 선택합니다.
 - 단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
 - 단계 5 업그레이드 토글을 **FTD System Upgrade**(FTD 시스템 업그레이드)로 설정합니다.
- FTD System Upgrade
 Intrusion Prevention Engine
- 단계 6 (선택 사항) CDO가 나중에 업그레이드를 수행하도록 하려면 **Schedule Upgrade**(업그레이드 예약) 확인란을 선택합니다. 미래의 날짜 및 시간을 선택하려면 필드를 클릭합니다.
 - 단계 7 1단계에서 업그레이드 방법을 선택합니다. CDO 이미지 저장소 및 자체 저장소의 이미지를 사용합니다.
 - **Use CDO Image Repository**(CDO 이미지 저장소 사용) - 이 옵션을 클릭하여 업그레이드할 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
 - **Specify Image URL**(이미지 URL 지정) - 이 옵션을 클릭하여 현재 저장소에 저장되어 있는 소프트웨어 이미지를 선택하고 **Continue**(계속)를 클릭합니다. 업그레이드할 수 있는 디바이스와 호환되는 선택 항목만 표시됩니다.
 - 단계 8 2단계에서는 선택 사항을 확인하고 디바이스에 이미지를 다운로드할지 아니면 이미지를 복사하여 설치하고 디바이스를 재부팅할지를 결정합니다.
 - 단계 9 **Upgrade to Snort 3 Engine**(Snort 3 엔진으로 업그레이드)을 선택합니다.
 - 단계 10 준비가 되면 **Perform Upgrade**(업그레이드 수행)를 클릭합니다. **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

Warning 진행 중인 업그레이드를 취소하려면 Upgrade(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 확인하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.

침입 방지 엔진 업그레이드

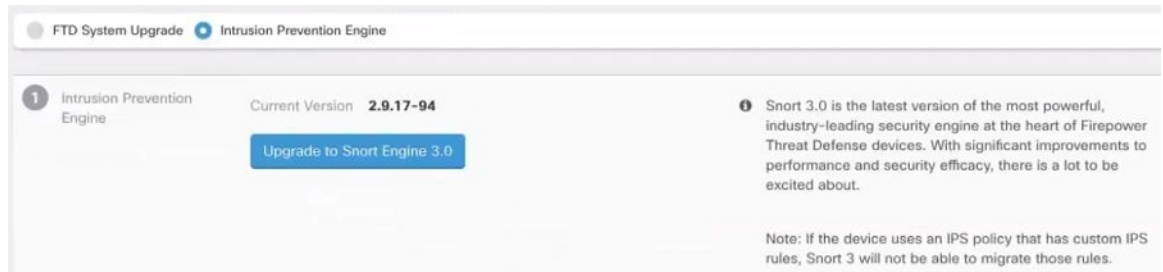
Snort 2가 설치된 버전 6.7을 이미 실행 중인 디바이스의 경우 다음 절차를 사용하여 Snort 엔진만 버전 3으로 업데이트합니다.

Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
- 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
- 단계 3 **FTD** 탭을 클릭하고 업그레이드할 디바이스를 하나 이상 선택합니다.
- 단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.
- 단계 5 업그레이드 토글을 **Intrusion Prevention Engine**(침입 방지 엔진)으로 설정합니다.



- 단계 6 **Upgrade to Snort Engine 3.0**(Snort 엔진 3.0으로 업그레이드)을 클릭합니다.



- 단계 7 **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

업그레이드 프로세스 모니터링



경고! 진행 중인 업그레이드를 취소하려면 **Upgrade**(업그레이드) 페이지에서 **Abort Upgrade**(업그레이드 중단)를 클릭합니다. 업그레이드가 시작된 후 취소하면 CDO는 디바이스에서 변경 사항을 구축하거나 확인하지 않으며 디바이스는 이전 구성으로 롤백되지 않습니다. 이로 인해 디바이스가 비정상 상태로 전환될 수 있습니다. 업그레이드 과정 중에 문제가 발생하면 Cisco TAC에 문의하십시오.

Inventory(재고 목록) 페이지에서 해당 디바이스를 선택하고 업그레이드 버튼을 클릭하여 단일 디바이스의 진행 상황을 볼 수 있습니다. CDO에서 해당 디바이스의 **Device Upgrade**(디바이스 업그레이드) 페이지로 이동합니다.

업그레이드가 실패하면 CDO는 메시지를 표시합니다. CDO는 업그레이드 프로세스를 자동으로 다시 시작하지 않습니다.



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

FDM-관리 디바이스용 Snort 3.0에서 되돌리기

Snort 2.0의 일부 침입 규칙은 Snort 3.0에 없을 수 있습니다. 2.0으로 다운그레이드하는 경우, 생성한 사용자 지정 침입 정책이 사용자 지정 정책에 사용된 기본 정책으로 변환됩니다. 가능한 한 규칙 작업 오버라이드가 유지됩니다. 두 개 이상의 사용자 지정 정책이 동일한 기본 정책을 사용하는 경우, 대부분의 액세스 제어 정책에 사용되는 사용자 지정 정책의 오버라이드는 유지되며 다른 사용자 지정 정책의 오버라이드는 손실됩니다. 이러한 "중복" 정책을 사용하는 액세스 제어 규칙은 이제 가장 많이 사용되는 사용자 지정 정책에서 생성된 기본 정책을 사용합니다. 모든 사용자 지정 정책이 삭제됩니다.

Snort 3.0에서 복귀하도록 선택하기 전에 *Firepower Device Manager* 구성 가이드의 [침입 정책 관리 \(Snort2\)](#)를 읽고 Snort 엔진 버전 전환이 현재 규칙 및 정책에 어떤 영향을 미치는지 확인합니다.



Note 버전 2로 되돌려도 Firepower 소프트웨어 버전은 제거되지 않습니다.

Snort 3.0에서 되돌리기

Snort 버전을 변경하는 경우 시스템에서는 자동 구축을 수행하여 변경을 구현합니다. 개별 디바이스는 Snort 3.0에서 버전 2로만 되돌릴 수 있습니다.

침입 방지 엔진을 되돌리려면 다음 절차를 수행합니다.

Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

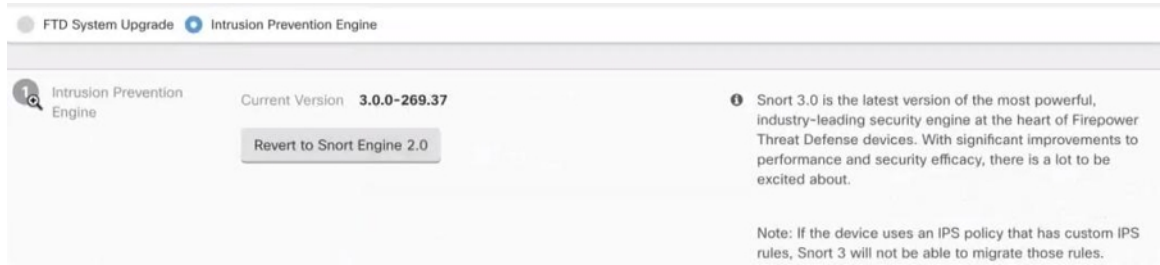
단계 3 **FTD** 탭을 클릭하고 되돌릴 디바이스를 클릭합니다.

단계 4 오른쪽의 **Device Actions**(디바이스 작업) 창에서 **Upgrade**(업그레이드)를 클릭합니다.

단계 5 업그레이드 토글을 **Intrusion Prevention Engine**(침입 방지 엔진)으로 설정합니다.



단계 6 1단계에서는 Snort 버전 3에서 되돌릴 것임을 확인하고 **Revert to Snort Engine 2**(Snort 엔진 2로 복귀)를 클릭합니다.



단계 7 **Inventory**(재고 목록) 페이지에서 업그레이드 중인 디바이스는 "Upgrade in Progress(업그레이드 진행 중)" 구성 상태로 표시됩니다.

보안 데이터베이스 업데이트 예약

FTD 디바이스에 대한 보안 데이터베이스를 확인하고 업데이트하는 예약된 작업을 생성하려면 다음 절차를 수행합니다.

Procedure

단계 1 탐색창에서 **Inventory**(재고 목록)를 클릭합니다.

단계 2 **Devices**(디바이스) 탭을 클릭합니다.

단계 3 **FTD** 탭을 클릭하고 원하는 FTD 디바이스를 선택합니다.

단계 4 **Actions**(작업) 창에서 **Security Database Updates**(보안 데이터베이스 업데이트) 섹션을 찾아 추가 + 버튼을 클릭합니다.

Note 선택한 디바이스에 대해 기존에 예약된 작업이 있는 경우 편집 아이콘을 클릭하여 새 작업을 생성합니다. 새 작업을 생성하면 기존 작업을 덮어씁니다.

단계 5 다음을 사용하여 예약된 작업을 구성합니다.

- **Frequency**(빈도) - 업데이트를 매일, 매주 또는 매월 수행하도록 선택합니다.
- **Time**(시간) - 시간을 선택합니다. 표시되는 시간은 UTC입니다.
- **Select Days**(요일 선택) - 업데이트를 수행할 요일을 선택합니다.

단계 6 **Save**(저장)를 클릭합니다.

단계 7 디바이스의 구성 상태가 "데이터베이스 업데이트 중"으로 변경됩니다.

예약된 보안 데이터베이스 업데이트 편집

FTD 디바이스에 대한 보안 데이터베이스를 확인하고 업데이트하기 위해 기존의 예약된 작업을 편집하려면 다음 절차를 따르십시오.

Procedure

- 단계 1 탐색 모음에서 **Inventory**(재고 목록)를 클릭합니다.
 - 단계 2 **Devices**(디바이스) 탭을 클릭합니다.
 - 단계 3 **FTD** 탭을 클릭하고 원하는 FTD 디바이스를 선택합니다.
 - 단계 4 **Actions**(작업) 창에서 데이터베이스 업데이트 섹션을 찾고 편집 아이콘을 클릭합니다.
 - 단계 5 다음을 사용하여 예약된 작업을 편집합니다.
 - **Frequency**(빈도) - 업데이트를 매일, 매주 또는 매월 수행하도록 선택합니다.
 - **Time**(시간) - 시간을 선택합니다. 표시되는 시간은 UTC입니다.
 - **Select Days**(요일 선택) - 업데이트를 수행할 요일을 선택합니다.
 - 단계 6 **Save**(저장)를 클릭합니다.
 - 단계 7 디바이스의 구성 상태가 "데이터베이스 업데이트 중"으로 변경됩니다.
-

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.