



Secure Firewall 200 Threat Defense : Cloud-Delivered Firewall Management Center

Cisco Secure Firewall Threat Defense
Updated NaN,

장

⋮

- 소프트웨어 버전을 확인하고, 필요한 경우 이미지를 재설치하고, 라이선스를 획득한 후 연결할 수 있는지 확인합니다.

- Cisco의 하이브리드 메시 방화벽 아키텍처를 브랜치 엣지로 확장
- AI 기반 검사 및 일관된 보안 정책 제공
- SD-WAN 기능을 통합하여 성능 및 안정적인 사용자 액세스
- 민감한 환경에 맞게 조정된 애플리케이션 및 사용자 제어, 효율적인 세그멘테이션 및 고급 보안 기능 제공

 주

이 가이드에서는 특히 외부 관리에 대해 설명하지만, 관리 인터페이스를 사용한 관리에 대해서는 [Cisco Security Cloud Control: Firewall Threat Defense용 클라우드 제공 Firewall Management Center](#)을 참조할 수 있습니다.

Secure Firewall 200의 전원을 켜는 방법을 구성하고, 전원 및 시스템 상태의 전면 패널 LED를 확인하여 성공적으로 시작되었는지 확인합니다.

이 작업을 통해 방화벽의 전원을 켜고 LED 상태 표시기를 통해 성공적인 시작을 확인할 수 있습니다.

시스템 전원은 디바이스 뒷면에 있는 전원 버튼로 제어됩니다. 전원 버튼은 부드러운 알람 기능을 제공하여 시스템의 정상적인 종료 과정을 지원함으로써 시스템 소프트웨어 및 데이터 손상 위험을 줄입니다.

주

방화벽을 처음 부팅할 때는 **Firewall Threat Defense** 초기화에 약 15~30분이 소요될 수 있습니다.

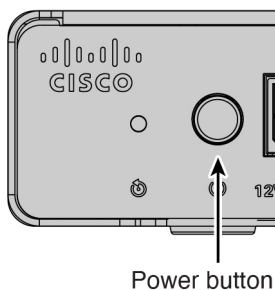
Before you begin

디바이스에 안정적인 전원을 제공하는 것이 중요합니다(예: UPS(Uninterruptable Power Supply) 사용). 먼저 켜지 않고 전력이 손실되면 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전력이 손실되면 시스템이 정상적으로 종료되지 않습니다.

방화벽의 전원을 켜려면 다음 단계를 따르십시오.

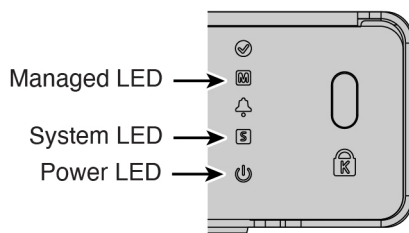
1. 전원 케이블을 디바이스에 연결하고 전기 콘센트에 꽂습니다.
2. 전원 코드 옆에 위치한 새시 후면의 전원 버튼을 사용하여 전원을 켭니다.

1:



3. LED에서 현재 상태를 확인합니다.

2: LED



- 전원 LED - 녹색으로 켜져 있으면 방화벽 전원이 켜져 있음을 의미합니다.

- 시스템 (S) LED - 다음 동작을 참조하십시오.

1: (S) LED

LED 동작	설명	디바이스 전원이 켜진 후의 시간 (분:초)
녹색으로 빠르게 깜박임	부팅	01:00
황색으로 빠르게 깜박임(오류 상태)	부팅 실패	01:00
녹색	애플리케이션 로드됨	15:00 - 30:00
황색 고정(오류 상태)	애플리케이션 로드 실패	15:00 - 30:00

- 매니지드(M) LED - 외부 인터페이스를 인터넷에 연결한 후 (방화벽 케이블 연결 페이지 13참조), 매니지드 LED를 선택하여 제로 터치 프로비저닝의 클라우드 연결 상태를 확인합니다.

2: (M) LED

M LED	설명	방화벽 전원이 켜진 후의 시간(분:초)
녹색으로 느리게 깜박임	Cisco Cloud에 연결되었으며 온보딩 준비 완료	15:00 - 30:00
녹색과 황색이 교대로 표시됨 (오류 상태)	디바이스를 Cisco Cloud에 연결하지 못했습니다.	15:00 - 30:00
녹색	온보딩됨	20:00 - 45:00

방화벽 전원이 성공적으로 켜지면 전원 LED가 녹색으로 고정되고 시스템 LED가 적절한 애플리케이션 로딩 상태를 나타냅니다. 디바이스의 설정 및 작동 준비가 완료되었습니다.

Firewall Threat Defense ASA

?

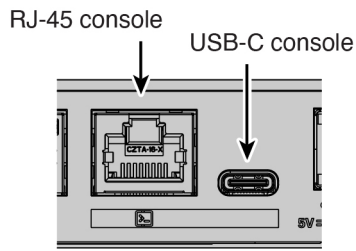
콘솔 포트에 연결하고 CLI 프롬프트를 식별하여 Secure Firewall 200에서 Firewall Threat Defense 또는 ASA가 실행 중인지를 확인합니다.

이 작업은 현재 하드웨어 플랫폼에 설치되어 있는 방화벽 애플리케이션을 식별하는 데 도움이 됩니다.

애플리케이션 Firewall Threat Defense 또는 ASA 모두 하드웨어에서 지원됩니다. 콘솔 포트에 연결하고 공장에서 설치된 애플리케이션이 무엇인지 확인합니다.

1. 두 포트 유형 중 하나를 사용하여 콘솔 포트에 연결합니다.

3:



2. CLI 프롬프트를 참조하여 방화벽 **Firewall Threat Defense** 또는 **ASA**를 실행 중인지 확인합니다.

Firewall Threat Defense

Firepower 로그인(**FXOS**) 프롬프트가 표시됩니다. 로그인하고 새 비밀번호 설정하지 않고 연결을 끊을 수 있습니다. 끝까지 로그인해야 하는 경우에는 [Firewall Threat Defense CLI에 액세스 페이지 5](#)를 참조하십시오.

```
firepower login:
```

ASA

ASA 프롬프트가 표시됩니다.

```
ciscoasa>
```

3. 잘못된 애플리케이션을 실행 중인 경우 [Cisco Secure Firewall ASA](#) 및 [Secure Firewall Threat Defense](#) 이미지 재설치 가이드를 참조하십시오.

CLI 프롬프트 모양을 기반으로 하드웨어에 설치된 방화벽 애플리케이션을 식별했습니다.

Firewall Threat Defense CLI

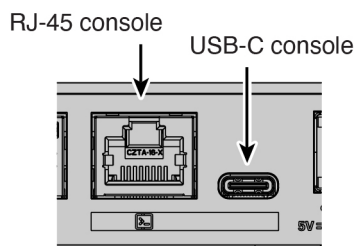
필요 시 **FXOS**에 로그인하거나 **FTD CLI**로 전환하는 등의 설정 또는 문제 해결 작업이 포함됩니다.

CLI에 액세스하여 디바이스 구성, 설정 및 문제 해결 작업을 수행합니다.

구성 또는 문제 해결을 위해 **CLI**에 액세스해야 할 수 있습니다.

1. 두 포트 유형 중 하나를 사용하여 콘솔 포트에 연결합니다.

4:



2. FXOS에 연결합니다. **admin** 사용자 이름 및 비밀번호(기본값은 **Admin123**)를 사용하여 CLI에 로그인합니다. 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다.

Example

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

3. Firewall Threat Defense CLI로 변경합니다.



주

초기 설정 에 Firewall Device Manager를 사용하려면 Firewall Threat Defense CLI에 액세스하지 마십시오. 그러면 CLI 설정이 시작됩니다.

제로 터치 프로비저닝의 경우 CLI에 액세스하고 설정 스크립트를 통해 실행해야 하는 경우, Do you want to configure IPv4? (IPv4를 설정하시겠습니까?) 라는 프롬프트가 표시되면 **n**을 선택합니다. (y/n) [y]: 및 IPv6를 구성하시겠습니까? (y/n) [y]:..또한 기본 로컬 관리자를 수락해야 합니다. 디바이스를 로컬로 관리하시겠습니까? (yes/no) [yes]:.

connect FTD

Firewall Threat Defense CLI에 처음 연결할 때는 초기 구성을 완료하라는 프롬프트가 표시됩니다.

Example

```
firepower# connect ftd
>
```

Firewall Threat Defense CLI를 종료하려면 **exit** 또는 **logout** 명령을 입력합니다. 그러면 FXOS 프롬프트로 돌아갑니다.

Example

```
> exit
```

```
firepower#
```

구성을 시작하기 전에, **Firewall Threat Defense** 소프트웨어 버전을 구성하고, **Secure Firewall 200**을(를) 대상 릴리스로 이미지 재설치합니다.

현재 소프트웨어 버전을 확인하고 필요한 경우 이미지를 재설치하여 구성 전에 방화벽이 권장 버전을 실행 중인지 확인하십시오.

방화벽을 구성하기 전에 대상 버전을 설치하는 것이 좋습니다. 또는 가동을 시작한 후 업그레이드를 수행할 수 있지만, 구성을 유지하는 업그레이드는 이 절차를 사용하는 것보다 시간이 더 오래 걸릴 수 있습니다.

어떤 버전을 실행해야 하나요?

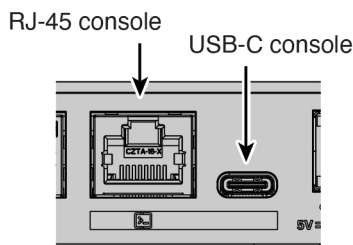
Cisco는 소프트웨어 다운로드 페이지에서 릴리스 번호 옆에 금색 별표로 표시된 **Gold Star** 릴리스를 실행할 것을 권장합니다. <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html>에 설명된 릴리스 전략을 참조할 수도 있습니다.

Before you begin

다음 단계에 따라 버전을 확인하고 디바이스의 이미지를 재설치하십시오.

1. 두 포트 유형 중 하나를 사용하여 콘솔 포트에 연결합니다.

5:



2. FXOS CLI에서 실행 중인 버전을 표시합니다.

```
scope ssa
```

```
show app-instance
```

Example

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name Slot ID Admin State Operational State Running Version Startup
Version Cluster Oper State
-----
ftd                1      Enabled      Online      7.6.0.65      7.6.0.65
```

Not Applicable

3. 새 버전을 설치하려면 다음 단계를 수행합니다.

기본적으로 관리 인터페이스는 **DHCP**를 사용합니다. 관리 인터페이스에 대한 고정 **IP** 주소를 설정해야 하는 경우 다음 명령을 입력합니다.

scope fabric-interconnect a

set out-of-band static IP /P netmask 넷마스크 **gw** 게이트웨이

commit-buffer

다음 오류가 발생하면 변경 사항을 커밋하기 전에 **DHCP** 서버를 비활성화해야 합니다. 아래 명령어를 따라 **DHCP**를 서버를 비활성화합니다.

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask>) is not
) is not
in the same network of current DHCP server IP range <ip - ip>.
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

a) **이미지 재설치 절차**는 **FXOS 문제 해결 설명서**를 참조하십시오.

관리 인터페이스에서 액세스할 수 있는 서버에서 새 이미지를 다운로드해야 합니다.

방화벽이 재부팅된 후 **FXOS CLI**에 다시 연결됩니다

b) **FXOS CLI**에서 관리자 비밀번호를 다시 설정하라는 메시지가 표시됩니다.

제로 터치 프로버저닝의 경우 디바이스를 온보딩할 때 비밀번호를 이미 설정했으므로 **Password Reset(비밀번호 재설정)** 영역에서 **No(아니요)**를 선택해야 합니다.

c) 방화벽을 종료합니다. **방화벽 전원 끄기 절차** 페이지 9의 내용을 참조하십시오.

현재 소프트웨어 버전을 확인하고, 필요한 경우 방화벽 대상 릴리스로 이미지를 재설치했습니다. 이제 방화벽이 적절한 소프트웨어 버전으로 구성할 준비가 되었습니다.

Cisco Smart Software Manager 및 **Cisco Commerce Workspace**에서 **Secure Firewall 200** 라이선스를 구성합니다. 여기에는 필요한 라이선스 유형을 파악하고, 추가 사용 권한을 주문하는 데 사용되는 라이선스 **PID**를 확인하는 작업이 포함됩니다.

Cisco 디바이스에 필요한 라이선스를 확보하고 적절한 작동과 컴플라이언스를 보장하여 다양한 기능과 성능을 활성화합니다.

Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 **Smart Software License** 어카운트에 연결되어 있어야 합니다. 초기에 제공된 라이선스 외에 추가 라이선스가 필요한 경우, **Cisco Commerce Workspace**를 통해 취득할 수 있습니다.

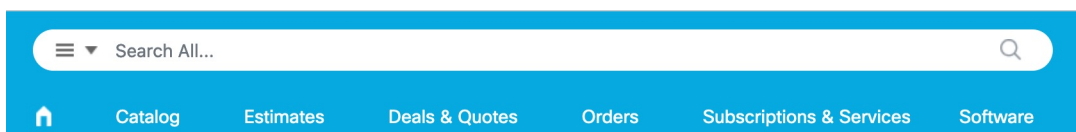
아직 등록하지 않은 경우 **Security Cloud Control**를 **Smart Software Manager**에 등록합니다. 등록하려면 **Smart Software Manager**에서 등록 토큰을 생성해야 합니다. 자세한 지침은 [Security Cloud Control 설명서](#)를 참조하십시오.

Firewall Threat Defense에는 다음 라이선스가 있습니다.

- Essentials—필수
- IPS
- 멀웨어 방어
- URL 필터링
- Cisco Secure Client

1. **Cisco Commerce Workspace**로 이동하여 **Search All**(모두 검색) 필드를 사용합니다.

6:

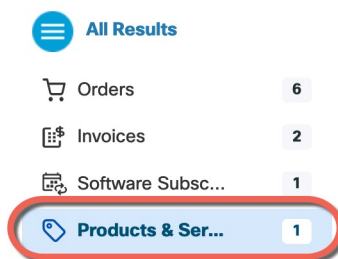


2. 라이선스 PID를 검색합니다.

원하는 PID는 주문 안내서를 확인하십시오.

3. 결과에서 **Products & Services**(제품 및 서비스)를 선택합니다.

7:



Cisco Commerce Workspace에서 필요한 라이선스 PID를 확인했으므로, 이제 해당 디바이스에 대한 추가 사용 권한을 주문할 수 있습니다.

FXOS CLI 셧다운 명령 또는 클라우드 제공 방화벽 관리 센터 셧다운 워크플로우를 사용하여 파일 시스템 손상을 방지하기 위해, 효과적으로 **Secure Firewall 200** 전원을 차단하는 방법을 설명합니다.

방화벽 전원 차단 절차란, 실행 중인 모든 프로세스가

- 정상적으로 셧다운되도록 보장하고, 부적절한 셧다운으로 인해

- 발생할 수 있는 파일 시스템 손상을 방지하며, 전원이 차단되기 전에 백그라운드 프로세스가
- 제대로 완료될 수 있도록 하는 시스템 셧다운 프로세스입니다.

시스템을 올바르게 종료하는 것이 중요합니다. 단순히 전원을 분리하거나 전원 스위치를 누르는 경우 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전원을 분리하거나 종료하면 방화벽 시스템이 정상적으로 종료되지 않습니다.

CLI

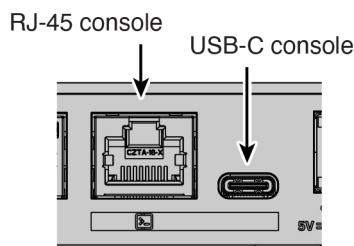
전원을 제거하거나 디바이스를 이동하기 전에 시스템을 정상적으로 중지할 수 있도록 **FXOS CLI**에서 **Secure Firewall 200** 를 종료하는 방법을 구성합니다.

명령줄 인터페이스에서 물리적으로 전원을 끄거나 디바이스를 재배치하기 전에 이 절차를 사용하여 방화벽 시스템을 안전하게 종료합니다.

FXOS를 사용하여 시스템을 안전하게 종료하고 **Firewall**의 전원을 끌 수 있습니다.

1. 두 포트 유형 중 하나를 사용하여 콘솔 포트에 연결합니다.

8:



2. **FXOS CLI** 에서 **local-mgmt**에 연결합니다.

Firepower # connect local-mgmt

3. 시스템을 종료합니다.

firepower(local-mgmt) # shutdown

Example

```
firepower(local-mgmt)# shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
```

4. 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 종료가 완료되면 다음 프롬프트가 표시됩니다.

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

5. 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

방화벽 시스템이 안전하게 종료되었으며 물리적 전원 제거 또는 재배치를 수행할 준비가 되었습니다.

Management Center Firewall

원격으로 관리하는 경우에도 디바이스의 전원을 안전하게 차단할 수 있도록, 클라우드 제공 방화벽 관리 센터를 통해 **Secure Firewall 200**의 안전 종료를 구성합니다.

이 작업을 통해 방화벽 시스템을 올바르게 종료하여 데이터 손상을 방지하고 안전한 전원 제거를 보장할 수 있습니다.

클라우드 제공 방화벽 관리 센터를 사용하여 시스템을 올바르게 종료할 수 있습니다.

1. 방화벽을 종료합니다.

- a) **Devices(디바이스) > Device Management(디바이스 관리)**를 선택합니다.
- b) 다시 시작할 디바이스 옆의 편집()을 클릭합니다.
- c) **Device(디바이스)** 탭을 클릭합니다.
- d) **System(시스템)** 섹션에서 디바이스 종료()을 클릭합니다.
- e) 메시지가 표시되면 디바이스 종료를 확인합니다.

2. 방화벽에 대한 콘솔 연결이 있는 경우 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 종료가 완료되면 이 프롬프트가 표시됩니다.

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

콘솔에 연결되지 않은 경우 시스템이 종료될 때까지 약 3분 동안 기다리십시오.

3. 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

방화벽이 안전하게 종료되며 데이터 손상 위험 없이 전원을 제거할 수 있습니다.

제

2

장

:

- [Cisco Secure Firewall 200](#)을(를) 네트워크에 연결하고 관리자에 등록합니다.
- [Cisco Secure Firewall 200](#)을(를) [Security Cloud Control](#)에 방화벽을 케이블로 연결하고 온보딩합니다.
- [Cisco Secure Firewall 200](#)을(를) [Cisco Secure Firewall 200](#) (Cisco Secure Firewall 200)에 연결합니다.

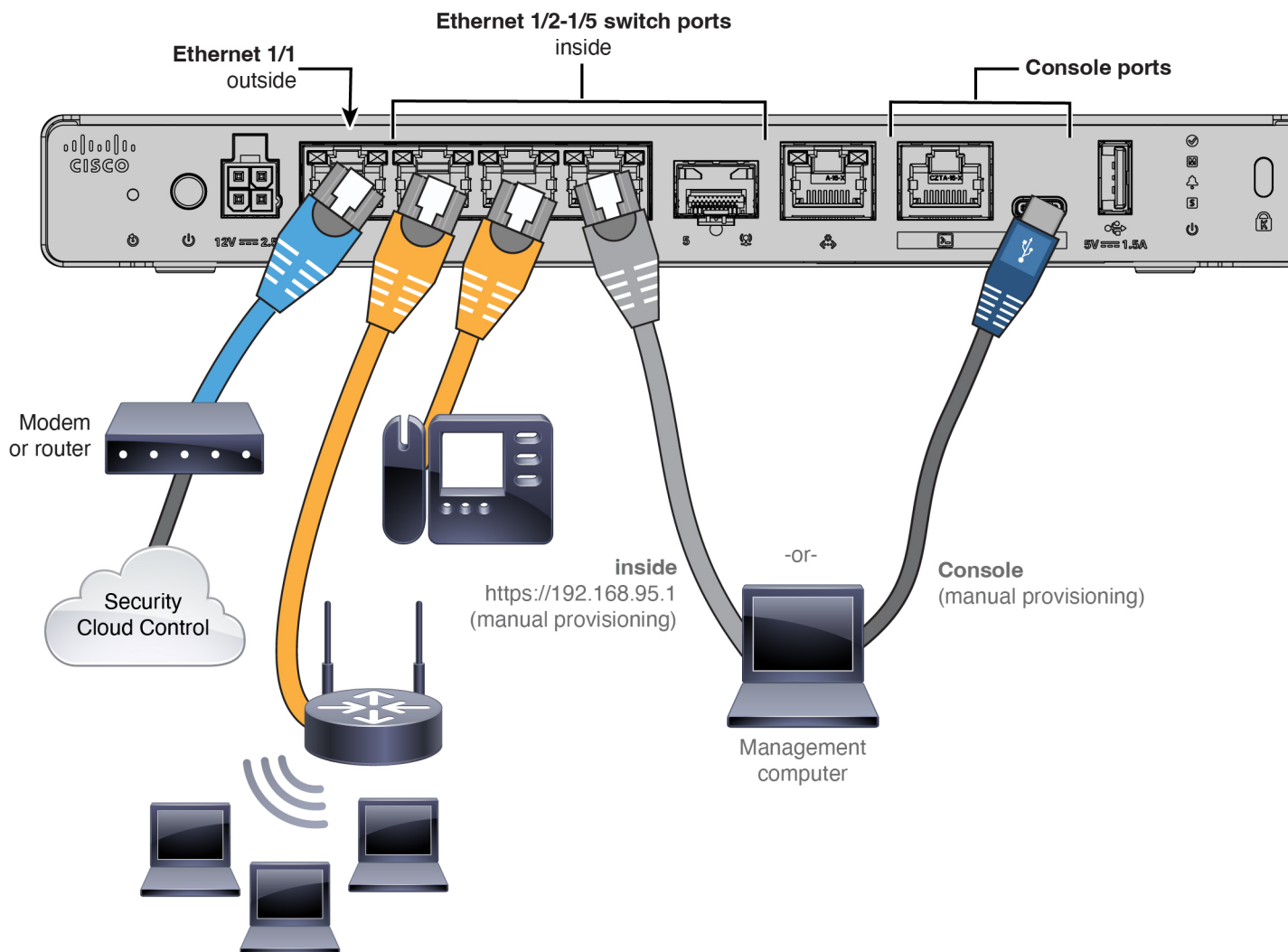
Secure Firewall 200을(를) 네트워크에 연결하고 관리자에 등록합니다.

Security Cloud Control에 방화벽을 케이블로 연결하고 온보딩합니다.

성공적인 하드웨어 설정 및 네트워크 연결성을 보장하기 위한 **Secure Firewall 200**에 대한 케이블 연결 요구 사항을 설명합니다. 이 프로세스에서는 설정에 필요한 포트를 준비합니다.

클라우드 제공 방화벽 관리 센터를 전용 관리 1/1 인터페이스에 연결하여 업데이트를 위한 인터넷 액세스를 활성화합니다.

- SFP를 Ethernet 1/5에 설치 - SFP 모듈이 필요한 1Gbps SFP 포트입니다.
- 자세한 내용은 [하드웨어 설치 가이드](#)를 참조하십시오.
- 제로 터치 프로비저닝을 사용하는 경우 외부와 관리 인터페이스를 모두 케이블로 연결하지 마십시오. 이 가이드에서는 외부 인터페이스에서의 관리에 대해 설명하지만, 고가용성을 제공하는 관리에서 제로 터치 프로비저닝을 사용하는 것이 좋습니다. 외부에서 제로 터치 프로비저닝을 사용하고 고가용성을 사용하려는 경우 등록 후 외부 IP 주소를 고정 주소로 변경해야 합니다.



Security Cloud Control .

Security Cloud Control에 Secure Firewall 200을(를) 온보딩하는 프로세스를 설명합니다. 이를 통해 클라우드 제공 Firewall Management Center를 사용하여 디바이스를 중앙 집중식으로 관리할 수 있습니다.

온보딩은 중앙 집중식 관리를 위해 방화벽을 Security Cloud Control에 연결하는 프로세스입니다.

- 제로 터치 프로비저닝 프로비저닝을 지원합니다.
- 수동 프로비저닝을 지원합니다.

<https://security.cisco.com>에서 Security Cloud Control에 로그인합니다.

빠른 원격 구축을 위해 제로 터치 프로비저닝과 디바이스 일련 번호를 사용하여 Secure Firewall 200을 Security Cloud Control에 온보딩합니다.

제로 터치 프로비저닝과 디바이스의 일련 번호를 사용하여 Firewall Threat Defense 온보딩

Before you begin

- 디바이스의 일련 번호 찾기
 - 배송 상자가 있는 경우 레이블에서 새시 일련 번호를 확인할 수 있습니다.
 - 새시 일련 번호는 후면에 있습니다.
 - PCB 일련 번호는 "S/N"이라는 새시의 레이블에 있습니다.
 - 일련 번호는 다음 CLI 명령을 사용하여 볼 수 있습니다.
 - FXOS - **show chassis detail** 는 두 일련 번호를 모두 보여줍니다.
 - Firewall Threat Defense - **show inventory** 는 새시 일련 번호를 표시합니다. **show serial-number** 는 PCB 일련 번호를 보여줍니다.
- LED를 확인하여 방화벽을 등록할 준비가 되었는지 확인합니다.

3: : (M) LED

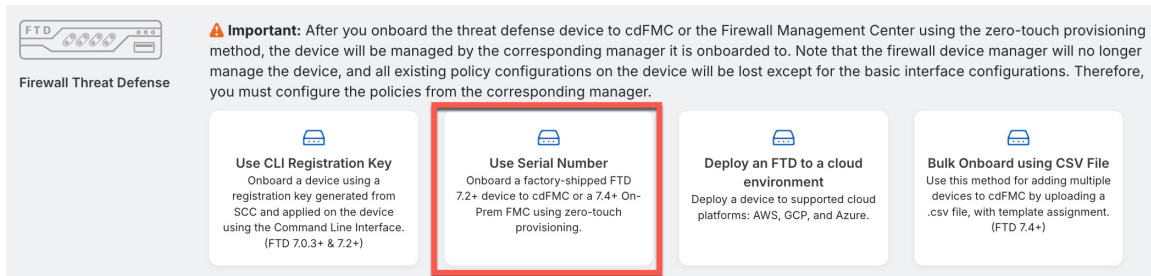
M LED	설명	방화벽 전원이 켜진 후의 시간(분:초)
녹색으로 느리게 깜박임	Cisco Cloud에 연결되었으며 온보딩 준비 완료	15:00 - 30:00
녹색과 황색이 교대로 표시됨 (오류 상태)	디바이스를 Cisco Cloud에 연결하지 못했습니다.	15:00 - 30:00
녹색	온보딩됨	20:00 - 45:00

1. Security Cloud Control 탐색 메뉴에서 보안 디바이스를 클릭한 다음 파란색 더하기 버튼()을 클릭하여 디바이스를 온보딩합니다.
2. FTD 타일을 선택합니다.
3. Management Mode(관리 모드)에서 FTD가 선택되어 있는지 확인합니다.

FTD 를 관리 모드로 선택한 후 언제든지 **Manage Smart License(스마트 라이선스 관리)**를 클릭하여 디바이스에 사용 가능한 기존 스마트 라이선스를 등록하거나 수정할 수 있습니다.

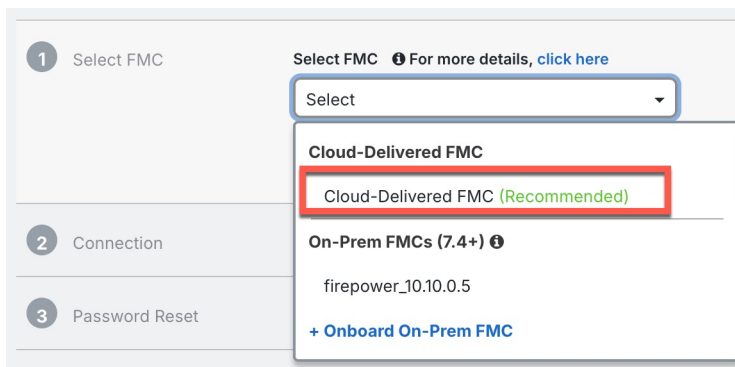
4. 온보딩 방법으로 **Use Serial Number(일련 번호 사용)**를 선택합니다.

9:



5. **Select FMC(FMC 선택)** 목록에서 **Cloud-Delivered FMC(클라우드 제공 FMC) > Cloud-Delivered FMC(클라우드 제공 FMC)**를 선택하고 **Next** 을(를) 클릭합니다.

10: FMC



6. **Connection(연결)** 영역에서 디바이스의 일련 번호와 디바이스 이름을 입력한 후 **Next(다음)**를 클릭합니다.

11:



7. **Password Reset(비밀번호 재설정)**에서 **Yes...(예)**를 클릭합니다. . 새 비밀번호를 입력하고 디바이스의 새 비밀번호를 확인한 후 **Next(다음)**를 클릭합니다.

제로 터치 프로비저닝의 경우 디바이스가 새 제품이거나 이미징을 마친 상태여야 합니다.

주

디바이스에 로그인하고 비밀번호를 재설정했지만, 제로 터치 프로비저닝을 비활성화하는 방식으로 구성을 변경하지 않았다면 아니요... 옵션을 선택해야 합니다. 제로 터치 프로비저닝 프로비저닝을 비활성화하는 구성이 많이 있으므로, 재이미징을 수행하는 등 꼭 필요한 경우가 아니라면 디바이스에는 로그인하지 않는 것이 좋습니다.

12: Password Reset()

3 Password Reset

1 Please review all the prerequisites for onboarding with a serial number. [Learn more](#)

2 Is this a new device that has never been logged into or configured for a manager?

☒ Yes, this new device has never been logged into or configured for a manager

Enter a new password for devices that have never been configured for a manager.

Important: If you select this option and the device's default password has already been changed, onboarding fails.

New Password

Confirm Password

☐ No, this device has been logged into and configured for a manager

Use this option if you already changed the password in the device CLI.

Important: If you select this option and the device's default password has not been changed, onboarding fails.

Next

1 Password must:

- Be 8-128 characters
- Have at least one lower and one upper case letter
- Have at least one digit
- Have at least one special character.
- Not contain consecutive repeated letters

8. **Policy Assignment(정책 할당)**에서 드롭다운 메뉴를 사용하여 디바이스에 대한 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy(기본 액세스 제어 정책)**를 선택합니다.

13: Policy Assignment()

4 Policy Assignment

Access Control Policy

Default Access Control Policy

Next

9. 구독 라이선스의 경우, 활성화하려는 각 기능 라이선스를 선택합니다. **Next(다음)**를 클릭합니다.

14:

5 Subscription License

License Type	Includes
☒ Essentials	Base Firewall Capabilities
☒ Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
☒ IPS	Intrusion Policy
☒ Malware Defense	File Policy
☒ URL	URL Reputation
☐ RA VPN VPNOnly ▾	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](#).

10. Security Devices(보안 디바이스) 페이지를 정렬하고 필터링하는 데 도움이 되도록 디바이스에 레이블을 추가합니다. 레이블을 입력하고 파란색 더하기 버튼(+)을 선택합니다. 레이블은 Security Cloud Control에 온보딩된 후 디바이스에 적용됩니다.

15:

6 Done

Your device is now onboarding.

This may take a long time to finish. You can check the status of the device on the Devices and Services page.

Add Labels ⓘ

Add label groups and labels +

[Go to Inventory](#)

Security Devices(보안 디바이스) 페이지에서 방금 온보딩한 디바이스를 선택하고 오른쪽에 있는 **Management** 창 아래에 나열된 옵션 중 하나를 선택합니다.

CLI 등록 키를 사용하여 Security Cloud Control에 Secure Firewall 200을(를) 등록합니다. 이 절차에서는 방화벽에 대한 수동 프로비저닝을 활성화합니다.

CLI 등록 키를 사용하여 방화벽을 본보딩합니다.

1. Security Cloud Control 탐색 메뉴에서 보안 디바이스를 클릭한 다음 파란색 더하기 버튼(+)을 클릭하여 디바이스를 온보딩합니다.
2. FTD 타일을 클릭합니다.
3. Management Mode(관리 모드)에서 FTD가 선택되어 있는지 확인합니다.
4. 온보딩 방법으로 Use CLI Registration Key(CLI 등록 키 사용)를 선택합니다.

16: CLI

Firewall Threat Defense

Important: After you onboard the threat defense device to cdFMC or the Firewall Management Center using the zero-touch provisioning method, the device will be managed by the corresponding manager it is onboarded to. Note that the firewall device manager will no longer manage the device, and all existing policy configurations on the device will be lost except for the basic interface configurations. Therefore, you must configure the policies from the corresponding manager.

Use CLI Registration Key
Onboard a device using a registration key generated from SCC and applied on the device using the Command Line Interface. (FTD 7.0.3+ & 7.2+)

Use Serial Number
Onboard a factory-shipped FTD 7.2+ device to cdFMC or a 7.4+ On-Prem FMC using zero-touch provisioning.

Deploy an FTD to a cloud environment
Deploy a device to supported cloud platforms: AWS, GCP, and Azure.

Bulk Onboard using CSV File
Use this method for adding multiple devices to cdFMC by uploading a .csv file, with template assignment. (FTD 7.4+)

5. **Device Name**(디바이스 이름)을 입력하고 **Next**(다음)를 클릭합니다.

17: **Device Name**()

1 Device Name

Device Name

ftd1

Next

6. **Policy Assignment**(정책 할당)에서 드롭다운 메뉴를 사용하여 디바이스에 대한 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy**(기본 액세스 제어 정책)를 선택합니다.

18:

2 Policy Assignment

Access Control Policy

Default Access Control Policy ▼

Next

7. 구독 라이선스의 경우, **Physical FTD Device**(물리적 FTD 디바이스) 라디오 버튼을 클릭한 다음 활성화하려는 각 기능 라이선스를 선택합니다. **Next**(다음)를 클릭합니다.

19:

3 Subscription License

Please indicate if this FTD is physical or virtual:

☒ Physical FTD Device

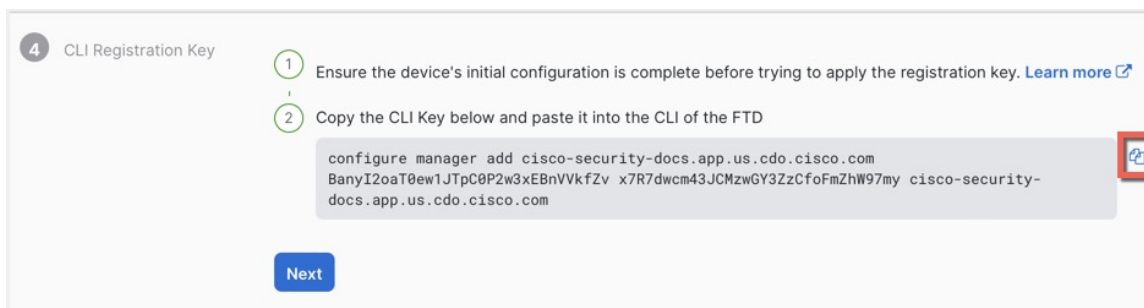
☐ Virtual FTD Device

License Type	Includes
☒ Essentials	Base Firewall Capabilities
☒ Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
☒ IPS	Intrusion Policy
☒ Malware Defense	File Policy
☒ URL	URL Reputation
☒ RA VPN	Premier ▼ RA VPN

Next

8. **CLI** 등록 키의 경우 **Security Cloud Control**는 등록 키 및 기타 매개 변수를 사용하여 명령을 생성합니다. 이 명령을 복사하여 **Firewall Threat Defense**의 초기 구성에서 사용해야 합니다.

20: **CLI**



configure manager add Security Cloud Control *_hostname registration_key nat_id display_name*

Firewall Device Manager을 사용하여 CLI에서 초기 구성 완료:

- 초기 구성: CLI 페이지 26- 시작 스크립트를 완료한 후 Firewall Threat Defense CLI에서 이 명령을 복사합니다.
- 초기 구성: Firewall Device Manager 페이지 20 - 명령의 *scc_hostname*, *registration_key* 및 *nat_id* 부분을 Management Center(관리 센터)/ Hostname(호스트 이름)/IP Address(IP 주소), Management Center(관리 센터)/ Registration Key(등록 키) 및 NAT ID 필드에 복사합니다.

Example

```
configure manager add account1.app.us.
scc

.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.
scc

.cisco.com
```

21: configure manager add

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.scc.cisco.com
```

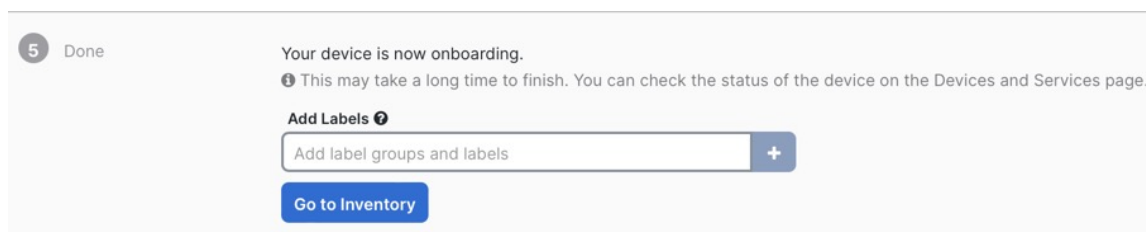
nat_id

scc_hostname registration_key

온보딩 마법사에서 **Next(다음)**를 클릭하여 디바이스 등록을 시작합니다.

9. 옵션: **Security Devices(보안 디바이스)** 페이지를 정렬하고 필터링하는 데 도움이 되도록 디바이스에 레이블을 추가합니다. 레이블을 입력하고 과란색 더하기 버튼(+)을 선택합니다. 레이블은 Security Cloud Control에 온보딩된 후 디바이스에 적용됩니다.

22:



()

디바이스가 기본 네트워크 설정을 갖추고 관리 플랫폼에 등록할 준비가 되었는지 확인하기 위해 수동 프로비저닝의 초기 설정 프로세스를 설명합니다.

초기 설정은 연결성 및 관리 등록을 활성화하기 위해 방화벽에서 기본 네트워크 설정을 설정하는 프로세스입니다.

수동 프로비저닝의 경우, **Secure Firewall Device Manager** 또는 **CLI**를 사용하여 방화벽의 초기 구성을 수행합니다.

: Firewall Device Manager

디바이스를 **Security Cloud Control**에 등록하기 전에 외부 및 관리 연결성 준비하기 위해 **Firewall Device Manager** 을(를) 사용하여 **Secure Firewall 200**에 초기 설정 마법사를 구성합니다.

이 방법을 사용하면 방화벽을 등록한 후 관리 인터페이스 외에도 다음 인터페이스가 사전 구성됩니다.

- Ethernet 1/1 — **outside** , DHCP의 IP 주소, IPv6 자동 구성
- — **inside** , 192.168.95.1/24
- 기본 경로 - 외부 인터페이스에서 DHCP를 통해 얻음
- 추가 인터페이스 - **Firewall Device Manager**의 모든 인터페이스 구성이 유지됩니다.

내부의 DHCP 서버, 액세스 제어 정책 또는 보안 영역과 같은 기타 설정은 유지되지 않습니다.

1. 컴퓨터를 내부 인터페이스에 연결합니다.
2. **Firewall Device Manager**에 로그인합니다.
 - a. <https://192.168.95.1>로 진행합니다.
 - b. 사용자 이름 **admin** 및 기본 비밀번호 **Admin123**으로 로그인합니다.
 - c. 일반 약관에 동의하고 관리자 비밀번호를 변경하라는 메시지가 표시됩니다.
3. 설정 마법사를 사용합니다.



정확한 포트 구성은 모델에 따라 다릅니다.

- a. 외부 인터페이스와 관리 인터페이스를 구성합니다.

23:

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1 Trust Outbound Traffic This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	Default Action Block all other traffic The default action blocks all other traffic.
---	---

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4
 Using DHCP

Configure IPv6
 Using DHCP

NEXT

Don't have internet connection?
[Skip device setup](#)

외부 인터페이스 주소 - 고가용성을 계획하는 경우 고정 IP 주소를 사용합니다. 설정 마법사를 사용하여 PPPoE를 구성할 수 없습니다. 마법사를 완료한 후 PPPoE를 구성할 수 있습니다.

관리 인터페이스 - 외부 인터페이스에서 관리자 액세스를 사용하여 하더라도 관리 인터페이스 네트워크 설정은 계속 사용됩니다. 예를 들어, 외부 인터페이스를 통해 백플레인으로 라우팅되는 관리 트래픽은 외부 인터페이스 DNS 서버가 아닌 관리 인터페이스 DNS 서버를 사용하여 FQDN을 확인합니다.

DNS 서버 - 시스템 관리 주소용 DNS 서버를 지정합니다. 기본값은 OpenDNS 공개 DNS 서버입니다. 외부 인터페이스에서 액세스하므로 나중에 설정하는 외부 인터페이스 DNS 서버와 일치할 수 있습니다.

방화벽 호스트 이름

- b. 시간 설정(NTP)을 구성하고 Next(다음)를 클릭합니다.

24: (NTP)

Time Setting (NTP)

System Time: 11:56:20AM October 03 2024 -06:00

Time Zone for Scheduling Tasks

(UTC+00:00) UTC

NTP Time Server

Default NTP Servers

Server Name

0.sourcefire.pool.ntp.org

1.sourcefire.pool.ntp.org

2.sourcefire.pool.ntp.org

NEXT

c. Start 90 day evaluation period without registration(등록 없이 90일 평가 기간 시작)을 선택합니다.

Register with Cisco Smart Software Manager

Register with Cisco Smart Software Manager to use the full functionality of this device and to apply subscription licenses.

[What is smart license? ↗](#)

☐ **Continue with evaluation period: Start 90-day evaluation period without registration**

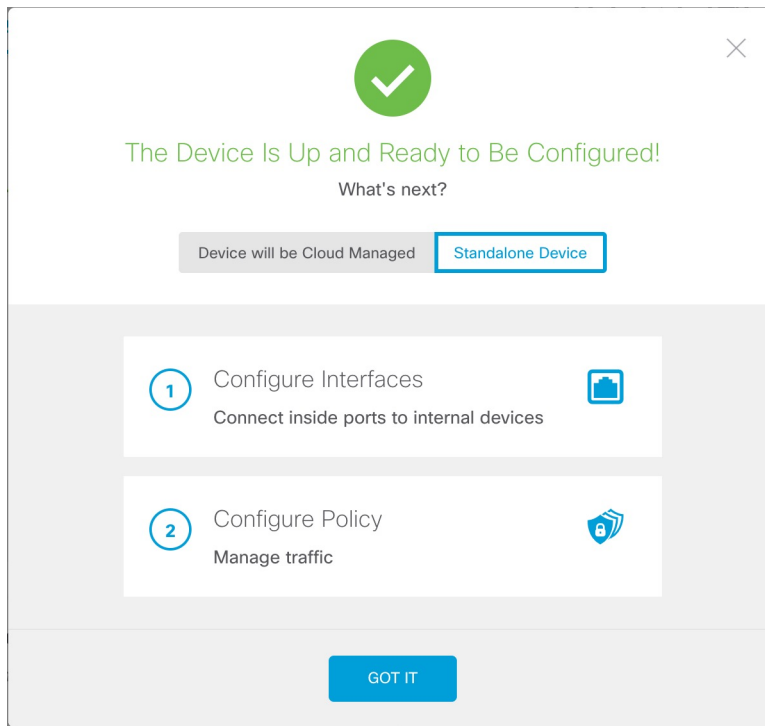
Recommended if device will be cloud managed. [Learn More ↗](#)

Please make sure you register with Cisco before the evaluation period ends.
Otherwise you will not be able to make any changes to the device configuration.

Firewall Threat Defense를 Smart Software Manager에 등록하지 마십시오. 모든 라이선싱은 Security Cloud Control에서 수행됩니다.

d. Finish(마침)를 클릭합니다.

25:



e. **Standalone Device**(독립형 디바이스)를 선택한 다음 **Got It**(확인)을 선택합니다.

4. 추가 인터페이스를 구성하려면 **Device**(디바이스)를 선택한 다음 **Interfaces**(인터페이스) 요약의 링크를 클릭합니다.
5. **Device**(디바이스) > **System Settings**(시스템 설정) > **Central Management**(중앙 관리)를 선택하고 **Proceed**(진행)를 클릭하여 Security Cloud Control에 등록합니다

Management Center/SCC/세부 정보를 구성합니다.

 주

이전 버전은 "SCC" 대신 "CDO"가 표시될 수 있습니다.

26: Management Center/SCC

Management Center/SCC Details

Do you know the Management Center/SCC hostname or IP address?

☒ Yes ☐ No

Threat Defense

 10.89.5.4
 fe80::6a87:c6ff:fea6:5480/64

→

Management Center/SCC

 10.89.5.35

Management Center/SCC Hostname or IP Address

10.89.5.35

Management Center/SCC Registration Key

.... 

NAT ID

Required when the management center/SCC hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/SCC hostname or IP address.

11204

Connectivity Configuration

Threat Defense Hostname

1120-4

DNS Server Group

CustomDNSServerGroup

Management Center/SCC Access Interface

outside (Ethernet1/1)

Type: Static | IP Address: 10.89.5.6 / 255.255.255.192 [Edit](#)

Before you connect to the management center or SCC, perform additional configuration:

- [Add a static route](#) through the data management interface so the threat defense can reach the management center. Or [review your current static routes](#).
- Optional. [Add a Dynamic DNS \(DDNS\) method](#). Or [review your current DDNS methods](#). DDNS ensures the management center can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the threat defense's IP address changes.

CANCEL
CONNECT

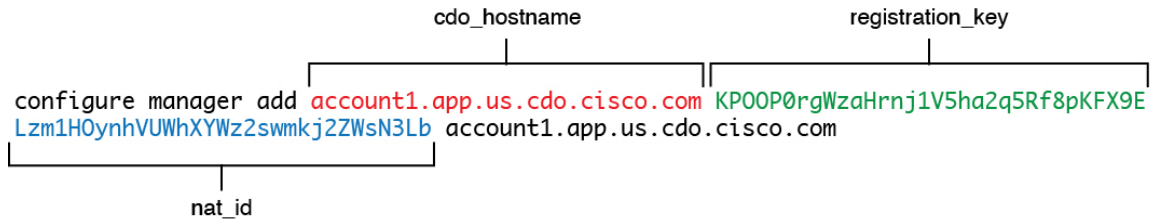
- a. Management Center/SCC 호스트 이름 또는 IP 주소를 사용하여 클라우드 제공 방화벽 관리 센터에 연결할 수 있는 경우, **Do you know the FMC hostname or IP address**(FMC 호스트 이름 또는 IP 주소를 알고 있습니까)에서 **Yes**(예).

Security Cloud Control이 **configure manager add** 명령을 생성합니다. 명령을 생성하려면 [수동 프로비저닝을 사용하여 방화벽 온보딩](#) 페이지 17의 내용을 참조하십시오.

```
configure manager add
_hostname
```

```
registration_key
nat_id
display_name
```

27: configure manager add



b. 명령의 *cdo_hostname* , *registration_key* 및 *nat_id* 부분을 다음 필드에 복사:

- Management Center/SCC 호스트 이름/IP 주소
- Management Center/SCC 등록 키
- NAT ID

6. 연결성 설정을 구성합니다.

a. **Threat Defense Hostname** 호스트 이름을 지정합니다.

이 FQDN은 외부 인터페이스에 사용됩니다.

b. **DNS** 서버 그룹을 지정합니다.

기존 그룹을 선택하거나 새로 생성합니다. 기본 DNS 그룹은 **CiscoUmbrellaDNSServerGroup**이며, 여기에는 **OpenDNS** 서버가 포함됩니다.

등록 후 외부 DNS 서버를 유지하려면 클라우드 제공 방화벽 관리 센터에서 서버 설정을 다시 구성해야 합니다.

c. **Management Center/SCC Access Interface** 의 경우 **Data Interface**(데이터 인터페이스)를 클릭하고, **outside**(외부)를 선택합니다.

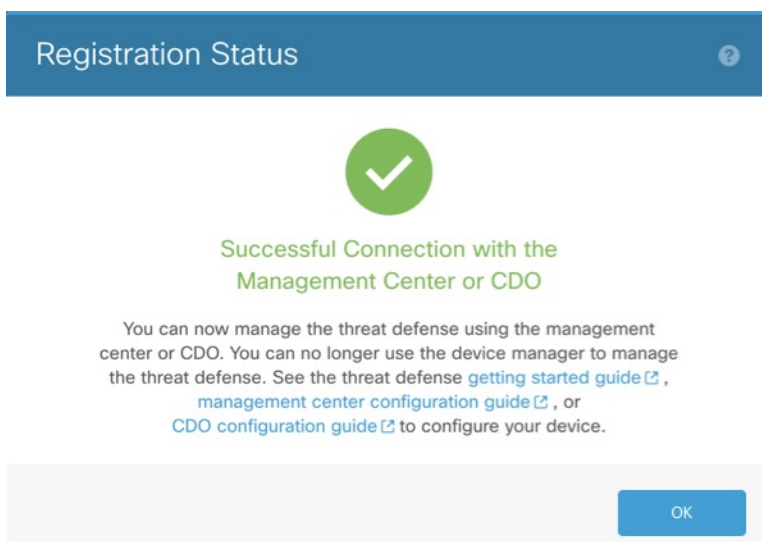
7. 옵션: DDNS(동적 DNS) 방법 추가를 클릭합니다.

DDNS는 Firewall Threat Defense의 IP 주소가 변경될 경우 클라우드 제공 방화벽 관리 센터가 FQDN에서 Firewall Threat Defense에 연결할 수 있도록 합니다.

8. Connect(연결)를 클릭합니다.

Registration Status(등록 상태) 대화 상자는 Security Cloud Control 등록에 대한 현재 상태를 보여줍니다.

28:



상태 화면의 **Saving Management Center/SCC Registration Settings**(Management Center/SCC 등록 설정 저장) 단계에서 Security Cloud Control로 이동 후 방화벽을 추가합니다. 수동 프로비저닝을 사용하여 방화벽 온보딩 페이지 17의 내용을 참조하십시오.

: CLI

CLI 설정 스크립트를 사용해 관리 주소 지정 및 외부 인터페이스 관리자 액세스를 구성하여 디바이스를 Security Cloud Control에 등록합니다.

CLI 설정 스크립트를 사용하여 전용 관리 IP 주소, 게이트웨이 및 기타 기본 네트워킹 설정을 설정합니다.

1. Firewall Threat Defense 및 ASA CLI에 액세스하기 위해 콘솔 포트에 연결 [Firewall Threat Defense CLI에 액세스](#) 페이지 5의 내용을 참조하십시오.
2. 그러면 관리 인터페이스 설정을 위한 CLI 설정 스크립트가 표시됩니다.

주

이미지 재설치 등을 통해 구성을 지우지 않으면 CLI 설정 스크립트를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network** 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. [Cisco Secure Firewall Threat Defense 명령 참조](#)의 내용을 참조하십시오.

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
System initialization in progress. Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]:
```

n

지침: 다음 주소 유형 중 하나 이상에 대해 **y** 를 입력합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다.

Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:

지침: **manual** 을 선택합니다. 관리자 액세스용 외부 인터페이스를 사용할 때는 DHCP가 지원되지 않습니다. 라우팅 문제를 방지하기 위해 이 인터페이스가 관리자 액세스 인터페이스와 다른 서브넷에 있는지 확인하십시오.

```

Enter an IPv4 address for the management interface
[192.168.45.61]:
10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]:
255.255.255.192
Enter the IPv4 default gateway for the management
interface [data-interfaces]:

```

지침: 게이트웨이를 **data-interfaces** 로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 포워딩하므로 외부 인터페이스를 통해 라우팅될 수 있습니다.

```

Enter a fully qualified hostname for this system
[firepower]:
1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []:
cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com

```

지침: 관리 인터페이스 **DNS** 서버를 설정합니다. 외부 인터페이스에서 액세스하므로 나중에 설정하는 외부 인터페이스 **DNS** 서버와 일치할 수 있습니다.

```

Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on
management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]:
no

```

지침: 클라우드 제공 방화벽 관리 센터를 사용하려면 **no** 를 입력합니다.

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on
management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

지침: **routed** 를 입력합니다. 외부 관리자 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

```
Configuring firewall mode ...
Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
  - add device configuration
  - add network discovery
  - add system policy
You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.
When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'
However, if the sensor and the Firepower Management Center are separated by
a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

3. 관리자 액세스를 위한 외부 인터페이스를 구성합니다.

configure network management-data-interface

Enter 를 누르면 외부 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

수동 IP 주소

```
>
                                configure network management-data-interface
Data interface to use for management:
                                ethernet1/1
Specify a name for the interface [outside]:
                                internet
IP address (manual / dhcp) [dhcp]:
                                manual
IPv4/IPv6 address:
                                10.10.6.7
Netmask/IPv6 Prefix:
                                255.255.255.0
Default Gateway:
                                10.10.6.1
Comma-separated list of DNS servers [none]:
```

208.67.222.222,208.67.220.220

지침: 등록 후 외부 DNS 서버를 유지하려면 클라우드 제공 방화벽 관리 센터에서 DNS 플랫폼 설정을 다시 구성해야 합니다.

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n)
[n]:
Configuration done with option to allow manager access from any network, if
you wish to change the manager access network
use the 'client' option in the command 'configure network
management-data-interface'.
Setting IPv4 network configuration.
Network settings changed.
>
```

DHCP로부터 할당된 IP 주소

```
>
configure network management-data-interface
Data interface to use for management:
ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n)
[n]:
Configuration done with option to allow manager access from any network, if
you wish to change the manager access network
use the 'client' option in the command 'configure network
management-data-interface'.
Setting IPv4 network configuration.
Network settings changed.
>
```

4. Security Cloud Control에서 생성한 **configure manager add** 명령을 사용하여 이 Firewall Threat Defense를 관리할 Security Cloud Control를 식별합니다. 명령을 생성하려면 [수동 프로비저닝을 사용하여 방화벽 온보딩](#) 페이지 17의 내용을 참조하십시오.

Example

```
>
configure manager add account1.app.us.cdo.cisco.com
KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

5. 원격 지사로 디바이스를 전송할 수 있도록 Firewall Threat Defense를 종료합니다.

시스템을 올바르게 종료하는 것이 중요합니다. 단순히 전원을 분리하거나 전원 스위치를 누르는 경우 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전원을 분리하거나 종료하면 Firepower 시스템이 정상적으로 종료되지 않는다는 점에 유의하십시오.

- a) **shutdown** 명령을 입력합니다.
 - b) 전원 **LED** 및 상태 **LED**를 관찰하여 새시의 전원이 꺼져 있는지 확인합니다(LED 꺼짐).
 - c) 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.
-

제

3

장

:

- [Cisco Firewall Management Center](#)
- [Cisco DHCP](#)
- [Cisco NAT](#)
- [Cisco SSH](#)

기본 보안 정책을 구성하여, **Secure Firewall 200**을(를) 실행합니다.

다음 설정으로 기본 보안 정책을 구성:

- 내부 및 외부 인터페이스 - 내부 인터페이스에 고정 IP 주소를 할당하고, 외부 인터페이스에 DHCP를 사용합니다.
- DHCP Server(DHCP 서버) - 클라이언트용 내부 인터페이스에서 DHCP 서버를 사용합니다.
- Default route(기본 경로) - 외부 인터페이스를 통해 기본 경로를 추가합니다.
- NAT - 외부 인터페이스에서 인터페이스 PAT를 사용합니다.
- Access control(액세스 제어) - 내부에서 외부로 향하는 트래픽을 허용합니다.

보안 정책을 사용자 지정하여 더 고급 검사를 포함시킬 수도 있습니다.

Firewall Management Center

별도의 관리 탭에서 정책을 구성하고 **Secure Firewall 200**를 관리할 수 있도록 **Security Cloud Control**에서 클라우드 제공 **Firewall Management Center**에 대한 액세스 권한을 구성합니다.

이 작업을 통해 클라우드 제공 **Firewall Management Center** 인터페이스에 액세스하여 방화벽 정책을 구성하고 디바이스를 관리할 수 있습니다.

클라우드 제공 **Firewall Management Center**는 **Security Cloud Control**의 자체 탭에서 실행됩니다.

1. **Security Cloud Control** 홈 페이지에서 방화벽을 클릭합니다.
2. **Administration(관리) > Integration(통합) > Firewall Management Center**를 선택합니다.
3. 클라우드 제공 **FMC**를 선택하고 **Actions(작업)**, **Management(관리)** 또는 **Settings(설정)** 창 링크를 클릭하여 새 탭에서 클라우드 제공 **Firewall Management Center**를 엽니다.



팁

클라우드 제공 **Firewall Management Center**에서 **Security Cloud Control**로 다시 이동하려면 **Home(홈)**를 클릭합니다.

내부 및 외부 영역 할당, 라우팅된 구축을 위한 IP 주소 설정 등을 포함하여, 인터페이스 **Secure Firewall 200**을 (를) 구성합니다.

이 작업을 통해 보안 구축에서 적절한 네트워크 세분화 및 라우팅을 위한 인터페이스 설정을 구성할 수 있습니다.

초기 설정에 대해 CLI를 사용하는 대신 제로 터치 프로비저닝 또는 **Firewall Device Manager**를 사용하는 경우, 다음 인터페이스가 사전 구성되어 있습니다.

- Ethernet 1/1 - **outside**, DHCP의 IP 주소, IPv6 자동 구성
- VLAN1 - **inside**, 192.168.95.1/24
- 기본 경로 - 외부 인터페이스에서 DHCP를 통해 얻음

클라우드 제공 방화벽 관리 센터에 등록하기 전에 **Firewall Device Manager**에서 인터페이스별 추가 구성을 수행했으면 해당 구성이 유지됩니다.

CLI를 사용하여 초기 설정을 수행한 경우, 디바이스에 사전 구성이 적용되지 않습니다.

두 경우 모두 디바이스를 등록한 후 추가 인터페이스 구성을 수행해야 합니다. CLI 초기 설정을 위해 내부 스위치 포트를 위한 **VLAN1** 인터페이스를 반드시 추가해야 합니다. 추가 구성에는 원하는 대로 스위치 포트를 방화벽 인터페이스로 변환하고, 보안 영역에 인터페이스를 할당하고, IP 주소를 변경하는 등의 작업이 포함됩니다.

이 예에서는 DHCP를 사용하는 인터페이스(**Ethernet1/1**)에서 고정 주소 및 라우팅 모드를 사용하여 내부 인터페이스(**VLAN1**)에 라우팅 모드를 구성합니다. 또한 내부 웹 서버용 **DMZ** 인터페이스를 추가합니다.

1. **Devices(디바이스) > Device Management(디바이스 관리)**를 선택하고 디바이스의 편집(✎)을 클릭합니다.
2. **Interfaces(인터페이스)**를 클릭합니다.

29: Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitor	Port Mode	VLAN Usage	SwitchPo	Virtual Router
Management1/1	management	Physical				Disabled			Global	
Ethernet1/1	outside	Physical	outside		10.89.5.29/255.255.192...	Disabled			Global	
Ethernet1/2		Physical				Disabled	Access	1		
Ethernet1/3		Physical				Disabled	Access	1		
Ethernet1/4		Physical				Disabled	Access	1		

3. 초기 설정에 CLI를 사용한 경우 스위치 포트를 활성화합니다.
 - a) 스위치 포트에 대해 편집(✎)를 클릭합니다.

30:

Edit Physical Interface

General | Hardware Configuration

Interface ID:
Ethernet1/2

☒ Enabled

Description:

Port Mode:
Access

VLAN ID:
1

(1 - 4070)

Protected:
☐

- b) **Enabled(활성화됨)** 체크 박스를 선택하여 인터페이스를 활성화합니다.
 - c) 옵션: VLAN ID를 변경합니다. 기본값은 1입니다. 그런 다음 이 ID와 일치하는 VLAN 인터페이스를 추가합니다.
 - d) **OK(확인)**를 클릭합니다.
4. **Inside(내부) VLAN 인터페이스를 추가(또는 편집)합니다.**
 - a) **Add Interfaces(인터페이스 추가) > VLAN Interface(VLAN 인터페이스 추가)**를 클릭하거나, 이 인터페이스가 이미 있는 경우, 인터페이스에 대해 편집(✎)를 클릭합니다.

31: VLAN

Add VLAN Interface ?

General
IPv4
IPv6
Advanced

Name:

☒ Enabled

Description:

Mode:

Security Zone:

MTU:

(64 - 9198)

Priority:

(0 - 65535)

VLAN ID *:

(1 - 4096)

Disable Forwarding on Interface Vlan:

Associated Interface	Port Mo...
No records to display	

- b) **Security Zone**(보안 영역) 드롭다운 목록에서 기존의 내부 보안 영역을 선택하거나 **New**(새로 만들기)를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **inside_zone**이라는 영역을 추가합니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다.

VLAN1이 사전 구성된 경우, 나머지 필드는 선택 사항입니다.

- c) **Name**(이름) 필드에 이름을 48자 이내로 입력합니다.

예를 들어 인터페이스에 **inside**라는 이름을 지정합니다.

- d) **Enable**(활성화) 확인란을 선택합니다.

- e) **Mode**(모드)는 **None**(없음) 상태로 남겨둡니다.

- f) **VLAN ID**를 1로 설정합니다.

기본적으로 모든 스위치 포트는 VLAN 1로 설정됩니다. 여기서 다른 VLAN ID를 선택하는 경우에는 각 스위치 포트를 새 VLAN ID에 맞게 수정해야 합니다.

인터페이스를 저장한 후에는 VLAN ID를 변경할 수 없습니다. VLAN ID는 사용된 VLAN 태그이자 구성의 인터페이스 ID입니다.

- g) **IPv4** 및/또는 **IPv6** 탭을 클릭 합니다.

- **IPv4** - 드롭다운 목록에서 **Use Static IP**(고정 IP 사용)를 선택하고 슬래시(/) 표기로 IP 주소와 서브넷 마스크를 입력합니다.

예를 들어 **192.168.1.56/24**를 입력합니다.

32: IP

Add VLAN Interface

General **IPv4** IPv6 Advanced

IP Type:
Use Static IP

IP Address:
192.168.1.56/24
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- **IPv6** - 상태 비저장 자동 구성을 하려면 **Autoconfiguration**(자동 구성) 확인란을 선택합니다.

h) **OK**(확인)를 클릭합니다.

5. **outside**(외부)로 사용하려는 **Ethernet1/1**에 편집(✎)를 클릭합니다.

General(일반) 페이지가 표시됩니다.

33:

Edit Physical Interface

General **IPv4** IPv6 Path Monitoring Harc

Name:
outside

☒ Enabled

☐ Management Only

Description:

Mode:
None

Security Zone:
outside_zone

Interface ID:
Ethernet1/1

MTU:
1500
(64 - 9198)

Priority:
0
(0 - 65535)

Propagate Security Group Tag: ☐

NVE Only: ☐

a) **Security Zone**(보안 영역) 드롭다운 목록에서 기존의 외부 보안 영역을 선택하거나 **New**(새로 만들기)를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **outside_zone**이라는 영역을 추가합니다.

이러한 기본 설정을 변경하면 클라우드 제공 방화벽 관리 센터 관리 연결이 중단되므로 다른 기본 설정을 변경하면 안됩니다.

b) **OK(확인)**를 클릭합니다.

6. 예를 들어 웹 서버를 호스팅하기 위해 **DMZ** 인터페이스를 구성합니다.

a) **DMZ**에 사용할 스위치 포트의 스위치 포트 모드를 비활성화하려면 **SwitchPort(스위치포트)** 열의 슬라이더를 클릭하여 비활성화(☐)로 표시되도록 합니다.

b) 인터페이스에 대해 편집(✎)를 클릭합니다.

c) **Security Zone(보안 영역)** 드롭다운 목록에서 기존의 **DMZ** 보안 영역을 선택하거나 **New(새로 만들기)**를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **dmz_zone**이라는 영역을 추가합니다.

d) **Name(이름)** 필드에 이름을 48자 이내로 입력합니다.

예를 들어 인터페이스 이름을 **dmz**로 지정합니다.

e) **Enable(활성화)** 확인란을 선택합니다.

f) **Mode(모드)**는 **None(없음)** 상태로 남겨둡니다.

g) **IPv4** 탭 및/또는 **IPv6** 탭을 클릭하고 원하는 IP 주소를 구성합니다.

h) **OK(확인)**를 클릭합니다.

7. **Save(저장)**를 클릭합니다.

DHCP

내부 클라이언트가 자동으로 IP 주소 및 관련 네트워크 설정을 수신할 수 있도록, **Secure Firewall 200** 인터페이스에서 **HCP** 서버를 구성합니다.

DHCP 서버를 활성화하여 클라이언트가 방화벽에서 IP 주소 및 네트워크 설정을 자동으로 가져올 수 있도록 합니다.

클라이언트가 **DHCP**를 사용하여 방화벽에서 IP 주소를 가져오게 하려면 **DHCP** 서버를 활성화합니다.

1. **Devices(디바이스) > Device Management(디바이스 관리)**를 선택하고 디바이스의 편집(✎)을 클릭합니다.

2. **DHCP > DHCP Server(DHCP 서버)**를 선택합니다.

34: DHCP

Device Routing Interfaces Inline Sets **DHCP** VTEP SNMP

DHCP Server

DHCP Relay

DDNS

Ping Timeout: 50 (10 - 10000 ms)

Lease Length: 3600 (300 - 10,48,575 sec)

☐ Auto-Configuration

Interface:

Override Auto Configured Settings:

Domain Name:

Primary DNS Server: + Primary WINS Server: +

Secondary DNS Server: + Secondary WINS Server: +

Server Advanced

+ Add

Interface	Address Pool	Enable DHCP Server
No records to display		

3. **Server(서버)** 페이지에서 **Add(추가)**를 클릭하고 다음 옵션을 구성합니다.

35:

Add Server ?

Interface*:

Address Pool*:
(2.2.2.10-2.2.2.20)

☒ Enable DHCP Server

Cancel OK

- **Interface(인터페이스)** - 드롭다운 목록에서 인터페이스를 선택합니다.
- **Address Pool(주소 풀)**- IP 주소의 범위를 설정합니다. 이 IP 주소는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소는 포함할 수 없습니다.
- **Enable DHCP Server(DHCP 서버 활성화)** - 선택한 인터페이스에서 DHCP 서버를 활성화합니다.

4. **OK(확인)**를 클릭합니다.

5. **Save(저장)**를 클릭합니다.

NAT

내부 클라이언트가 외부 인터페이스 IP 주소를 사용하여 외부 네트워크에 액세스할 수 있도록 **NAT(인터페이스 PAT)** 정책을 구성합니다.

NAT(인터페이스 PAT) 정책을 생성하여 내부 클라이언트가 내부 주소를 외부 인터페이스 IP 주소의 포트로 변환하여 외부 네트워크에 액세스할 수 있도록 합니다.

이 절차는 내부 클라이언트가 내부 주소를 외부 인터페이스 IP 주소의 포트에 변환하도록 하는 **NAT** 규칙을 생성합니다. 이러한 유형의 **NAT** 규칙을 인터페이스 포트 주소 변환(**PAT**)이라고 합니다.

1. **Devices(디바이스) > NAT**를 선택하고, **New Policy(새 정책)**를 클릭합니다.
2. 정책 이름을 지정하고, 정책을 사용할 디바이스를 선택한 뒤 **Save(저장)**를 클릭합니다.

36:

New Policy ⓘ

Name:
FTD_policy

Description:

Targeted Devices
Select devices to which you want to apply this policy.

Available Devices and Templates
Search by name or value

192.168.0.124
192.168.0.155

Selected Devices and Templates

192.168.0.124	✕
192.168.0.155	✕

Add to Policy

Cancel **Save**

정책이 클라우드 제공 방화벽 관리 센터를 추가합니다. 계속해서 정책에 규칙을 추가해야 합니다.

37: NAT

FTD_Policy Show Warnings Save Cancel

Enter Description

Rules NAT Exemptions Policy Assignments (1)

Filter by Device Filter Rules Add Rule

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
NAT Rules Before											
Auto NAT Rules											
NAT Rules After											

3. **Add Rule**(규칙 추가)을 클릭합니다.

4. 기본 규칙 옵션을 구성합니다.

38:

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

☒ Enable

Interface Objects **Translation**

● **NAT Rule(NAT 규칙) - Auto NAT Rule(자동 NAT 규칙)**을 선택합니다.

● **Type(유형) - Dynamic(동적)**을 선택합니다.

5. **Interface Objects**(인터페이스 개체) 페이지에서 **Available Interface Objects**(사용 가능한 인터페이스 개체) 영역의 외부 영역을 **Destination Interface objects**(대상 인터페이스 개체) 영역에 추가합니다.

39:

Interface Objects **Translation** **PAT Pool** **Advanced**

Available Interface Objects Search by name

1 inside
2 outside

Add to Source Add to Destination

Source Interface Objects (0) any

3 Destination Interface Objects (1) outside

6. **Translation**(변환) 페이지에서 다음 옵션을 설정합니다.

40:

Interface Objects	Translation	PAT Pool	Advanced
Original Packet Original Source:* all-ipv4 +		Translated Packet Translated Source: Destination Interface IP The values selected for Destination Interface Objects in 'Interface Objects' tab will be used Translated Port: 	

- **Original Source(원본 소스)**- 모든 IPv4 트래픽(0.0.0.0/0)에 대한 네트워크 개체를 추가하려면 **Add(추가)**(+)를 클릭합니다.

41:

New Network Object

Name
all-ipv4

Description

Network
☐ Host
 ☐ Range
 ☒ Network
 ☐ FQDN

0.0.0.0/0

☐ Allow Overrides

Cancel Save



주

자동 NAT 규칙은 개체 정의의 일부로 NAT를 추가하고 시스템 정의 개체를 수정할 수 없기 때문에 시스템에서 정의된 **any-ipv4** 개체를 사용할 수 없습니다.

- **Translated Source(변환된 소스) - Destination Interface IP(대상 인터페이스 IP)**를 선택합니다.

7. **Save(저장)**를 클릭하여 규칙을 저장하십시오.

규칙이 **Rules(규칙)** 테이블에 저장됩니다.

8. 변경 사항을 저장하려면 **NAT** 페이지에서 **Save(저장)**를 클릭합니다.

Secure Firewall 200에서 내부 영역에서 외부 영역으로의 트래픽을 허용하도록 액세스 제어 규칙을 구성하고, 선택적 보안 검사 정책을 적용합니다.

보안 통제를 유지하면서 신뢰할 수 있는 내부 네트워크에서 외부 네트워크로 방화벽을 통과하는 트래픽 흐름을 허용하도록 액세스 제어 규칙을 구성합니다.

방화벽을 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic**(모든 트래픽 차단)을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 액세스 제어 정책은 순서대로 평가되는 여러 규칙을 포함할 수 있습니다.

이 절차는 내부 영역에서 외부 영역으로의 모든 트래픽을 허용하는 액세스 제어 규칙을 생성합니다.

1. **Policies(정책) > Security policies(보안 정책) > Access Control(액세스 제어)**을 선택하고 편집(✎)에 할당된 액세스 제어 정책에 대해 디바이스를 클릭합니다.

2. **Add Rule(규칙 추가)**을 클릭하고 다음 매개변수를 설정합니다.

42:

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is 'inside-to-outside'. The 'Action' is 'Allow'. The 'Intrusion Policy' is 'None'. Under the 'Zones' tab, 'inside' is selected. The 'Add Source Zone' button is highlighted with a red circle and the number 3.

1. 예를 들어 이 규칙의 이름을 **inside-to-outside**로 지정합니다.

2. **Zones(영역)**에서 내부 영역을 선택합니다.

3. **Add Source Zone(소스 영역 추가)**을 클릭합니다.

43:

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is 'inside-to-outside'. The 'Action' is 'Allow'. The 'Logging' is 'OFF'. The 'Time Range' is 'None'. Under the 'Zones' tab, 'inside' and 'outside' are selected. The 'Add Source Zone' button is highlighted with a red circle and the number 4. The 'Add Destination Zone' button is highlighted with a red circle and the number 5.

4. Zones(영역)에서 외부 영역을 선택합니다.

5. Add Destination Zone(대상 영역 추가)를 클릭합니다.

기타 설정은 변경하지 않습니다.

3. 옵션: 패킷 흐름 다이어그램에서 정책 유형을 클릭하여 연결된 정책을 사용자 지정합니다.

액세스 제어 규칙보다 사전 필터, 해독, **Security Intelligence** 및 **ID** 정책이 먼저 적용됩니다. 이러한 정책을 사용자 지정할 필요는 없지만, 네트워크의 요구 사항을 파악한 후에는 신뢰할 수 있는 트래픽을 단축 경로 지정(처리 우회)하거나 트래픽을 차단하여 추가 처리가 필요 없도록 함으로써 네트워크 성능을 개선할 수 있습니다.

44:



- 사전 필터 규칙 - 기본 사전 필터 정책은 모든 트래픽을 전달하여 다른 규칙이 조치(분석)를 취하도록 합니다. 기본 정책에 대한 유일한 변경 사항은 터널 트래픽을 차단하는 것입니다. 그렇지 않으면 분석(전달), 단축 경로 지정(우회 확인 우회) 또는 차단을 수행할 수 있는 액세스 제어 정책과 연결할 새 사전 필터 정책을 생성할 수 있습니다.

사전 필터를 사용하면 트래픽이 더 이상 발생하기 전에 차단하거나 단축 경로를 지정하여 성능을 개선할 수 있습니다. 새 정책에서 터널 규칙 및 사전 필터 규칙을 추가할 수 있습니다. 터널 규칙을 사용하면 평문(비암호화) 패스트루 터널을 단축경로 처리, 차단 또는 영역을 다시 지정할 수 있습니다. 사전 필터 규칙을 사용하면 IP 주소, 포트 및 프로토콜로 식별된 비터널 트래픽을 단축경로 처리하거나 차단할 수 있습니다.

예를 들어 네트워크의 모든 FTP 트래픽을 차단하려고 하지만, 관리자로부터의 단축경로 SSH 트래픽을 차단하려는 경우 새 사전 필터 정책을 추가할 수 있습니다.

- **Decryption(해독)** - 기본적으로 해독이 적용되지 않습니다. 해독은 네트워크 트래픽을 심층 검사에 노출하는 방법입니다. 대부분의 경우 트래픽은 해독을 원하지 않으며, 법적으로 허용되는 경우에만 가능합니다. 네트워크 보호를 극대화하려면 중요한 서버로 이동하거나 신뢰할 수 없는 네트워크 세그먼트에서 오는 트래픽 해독 정책을 사용하는 것이 좋습니다.
- **Security Intelligence-** (IPS 라이선스 필요) **Security Intelligence**는 기본적으로 활성화되어 있습니다. **Security Intelligence**는 추가 처리를 위해 액세스 제어 정책에 연결을 전달하기 전에 적용되는 악의적인 활동에 대한 또 다른 초기 방어 수단입니다. **Security Intelligence**는 평판 인텔리전스를 사용하여 시스코의 위협 인텔리전스 조직인 **Talos**에서 제공하는 IP 주소, URL 및 도메인 이름과의 연결을 신속하게 차단합니다. 원하는 경우 추가 IP 주소, URL 또는 도메인을 추가하거나 삭제할 수 있습니다.

주

IPS 라이선스가 없는 경우 이 정책은 액세스 제어 정책에서 활성화된 것으로 표시되더라도 구축되지 않습니다.

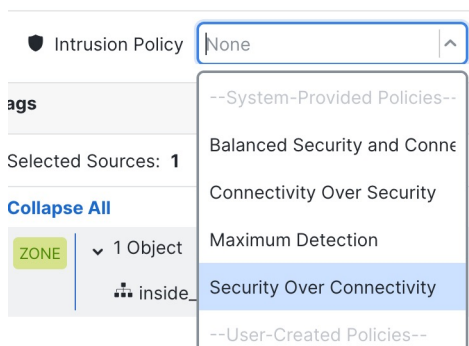
- **ID - ID**는 기본적으로 적용되지 않습니다. 액세스 제어 정책에 따라 트래픽을 처리하도록 허용하기 전에 사용자에게 인증을 요구할 수 있습니다.

4. 옵션: 액세스 제어 규칙 뒤에 적용되는 침입 정책을 추가합니다.

침입 정책은 보안 위반의 트래픽을 검사하는 침입 탐지 및 방지 설정의 정의된 집합입니다. 클라우드 제공 방화벽 관리 센터에는 있는 그대로 활성화하거나 맞춤화할 수 있는 여러 시스템 제공 정책이 포함되어 있습니다. 이 단계에서는 시스템 제공 정책을 활성화합니다.

a) **Intrusion Policy**(침입 정책) 드롭다운 목록을 클릭합니다.

45:



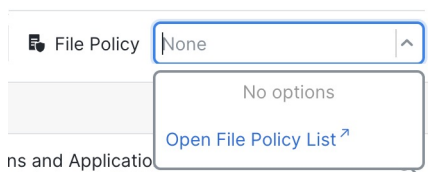
b) 목록에서 시스템 제공 정책 중 하나를 선택합니다.

대부분의 사용 사례에 균형 잡힌 보안 및 연결을 권장합니다.

5. 옵션: 액세스 제어 규칙 뒤에 적용되는 파일 정책을 추가합니다.

a) **File Policy**(파일 정책) 드롭다운 목록을 클릭하고 기존 정책을 선택하거나 **Open File Policy List**(파일 정책 목록 열기)를 선택하여 정책을 추가합니다.

46:



새 정책의 경우 **Policies**(정책) > **Security policies**(보안 정책) > **Malware & File**(멀웨어 및 파일) 페이지가 별도의 탭에 열립니다.

b) 정책 생성에 대한 자세한 내용은 [Cisco Secure Firewall Device Manager 구성 가이드](#)를 참조하십시오.

c) **Add Rule**(규칙 추가) 페이지로 돌아가 드롭다운 목록에서 새로 생성된 정책을 선택합니다.

6. **Apply**(적용)를 클릭합니다.

규칙이 **Rules**(규칙) 테이블에 추가됩니다.

7. **Save**(저장)를 클릭합니다.

SSH

승인된 IP 주소에서 원격으로 디바이스를 관리할 수 있도록 **Secure Firewall 200** 외부 인터페이스의 **SSH** 액세스를 구성합니다.

외부 인터페이스에 대한 **SSH** 액세스를 활성화하여 승인된 IP 주소에서 원격으로 방화벽을 관리합니다.

이 섹션에서는 방화벽을 원격으로 관리할 수 있도록 외부 인터페이스에 대한 **SSH** 연결을 활성화하는 방법을 설명합니다.

기본적으로 초기 설정 중에 비밀번호를 구성한 **admin** 사용자가 있습니다.

Before you begin

외부 인터페이스에서 **SSH**를 활성화하려면 다음 단계를 따르십시오.

1. **Devices(디바이스) > Platform Settings(플랫폼 설정)**를 선택하고 **Firewall Threat Defense** 정책을 생성하거나 편집합니다.
2. **Secure Shell(보안 셸)**을 선택합니다.
3. SSH 연결을 허용하는 외부 인터페이스와 IP 주소를 확인합니다.
 - a) **Add(추가)**를 클릭해 새 규칙을 추가하거나, **Edit(편집)**을 클릭해 기존 규칙을 편집합니다.
 - b) 규칙 속성을 구성합니다.
 - **IP Address(IP 주소)** - SSH 연결을 허용하는 호스트 또는 네트워크를 식별하는 네트워크 개체 또는 그룹입니다. 드롭다운 메뉴에서 개체를 선택하거나 **+**를 클릭하여 새 네트워크 개체를 추가합니다.
 - **Available Zones/Interfaces(사용할 수 있는 영역/인터페이스) - Selected Zones/Interface(선택한 영역/ 인터페이스)** 목록 아래 필드에 외부 영역을 추가하거나 외부 인터페이스 이름을 입력한 후 **Add(추가)**를 클릭합니다.

47: SSH

Edit Secure Shell Configuration ⓘ

IP Address*
any-ipv4 +

Available Zones/Interfaces C

Search

DMZ
inside
outside

Add

Selected Zones/Interface

outside Add

Cancel OK

- c) **OK(확인)**를 클릭합니다.
 4. **Save(저장)**를 클릭합니다.
- 이제 **Deploy(구축) > Deploy(구축)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

인터페이스, NAT, DHCP 및 액세스 제어 업데이트가 디바이스에 적용되도록 **Secure Firewall 200**에 대한 정책 변경을 구성합니다.

이 작업은 인터페이스, NAT, DHCP 및 액세스 제어 구성에 대한 정책 업데이트를 구축하여 디바이스에서 구성 변경 사항을 활성화합니다.

디바이스에 설정 변경 사항을 구축합니다. 구축하기 전에는 디바이스에서 변경 사항이 활성 상태가 아닙니다.

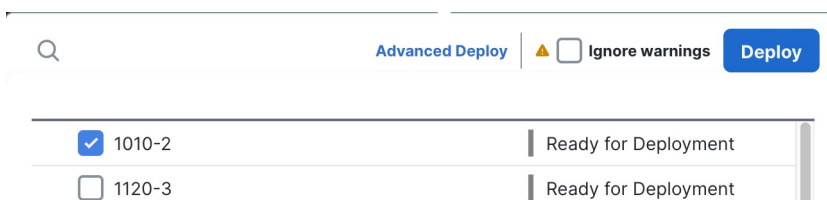
1. 우측 상단에서 **Deploy(구축)**를 클릭합니다.

48:



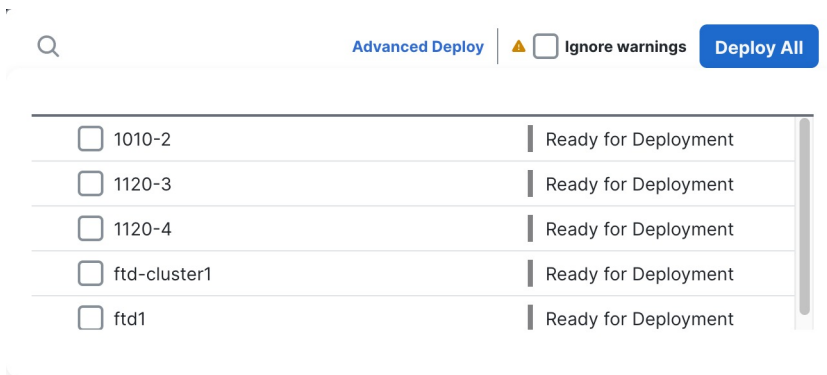
2. 빠르게 구축하려면 특정 디바이스를 선택한 다음 **Deploy(구축)**를 클릭합니다.

49:



또는 **Deploy All(모두 구축)**을 클릭하여 모든 디바이스에 구축합니다.

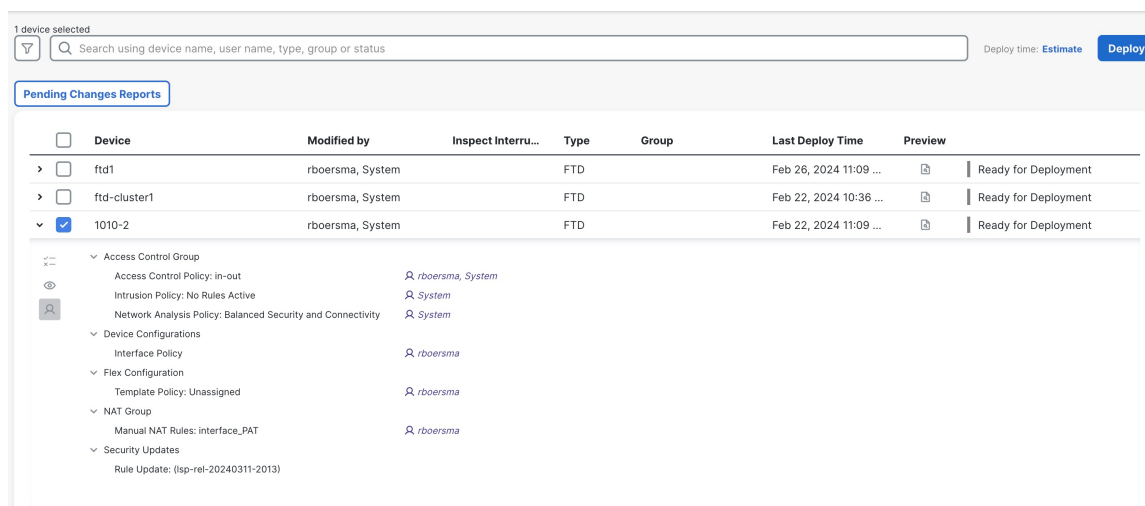
50:



5 devices are available for deployment

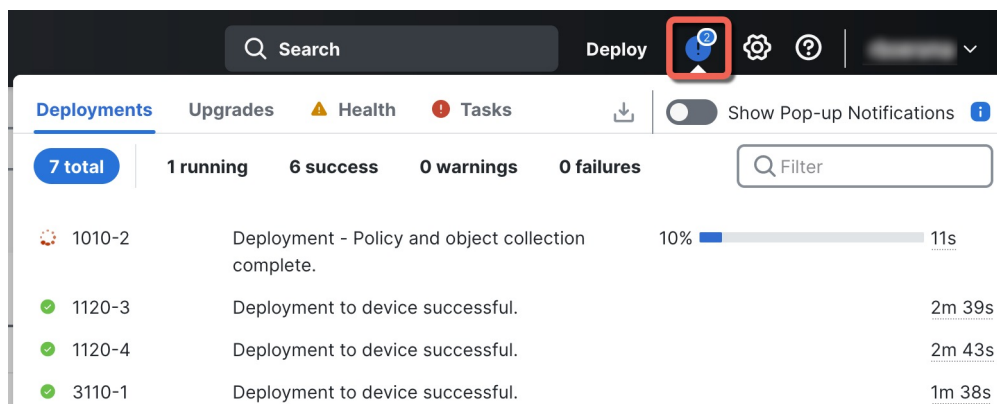
그렇지 않으면 추가 구축 옵션에 대해 **Advanced Deploy(고급 구축)**를 클릭합니다.

51:



3. 구축이 성공하는지 확인합니다. 메뉴 모음의 **Deploy(구축)** 버튼 오른쪽에 있는 아이콘을 클릭하여 구축 상태를 확인합니다.

52:





© 2026 Cisco Systems, Inc. All rights reserved.

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.

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.