



## 디바이스 관리 기본 사항

다음 주제에서는 Firepower System에서 디바이스를 관리하는 방법을 설명합니다.

- 디바이스 관리 관련 정보, 1 페이지
- 디바이스 관리 요구 사항 및 사전 요건, 9 페이지
- FTD 초기 설정 완료, on page 9
- FMC에 디바이스 추가, 15 페이지
- FMC에서 디바이스 삭제, 19 페이지
- 디바이스 그룹 추가, 19 페이지
- 디바이스 설정 구성, 20 페이지
- 디바이스의 관리자 변경, 55 페이지
- 디바이스 정보 보기, 60 페이지

## 디바이스 관리 관련 정보

Firepower Management Center를 사용하여 디바이스를 관리합니다.

### Firepower Management Center 및 디바이스 관리 관련 정보

Firepower Management Center는 디바이스를 관리할 때 자체와 디바이스 간에 양방향 SSL 암호화 통신 채널을 설정합니다. Firepower Management Center는 이 채널을 사용하여 네트워크 트래픽을 분석하고 관리하고자 하는 방법에 대한 정보를 디바이스로 전송합니다. 디바이스는 트래픽을 평가할 때 이벤트를 생성하고 동일한 채널을 사용하여 Firepower Management Center로 전송합니다.

Firepower Management Center를 사용하여 디바이스를 관리하면 다음을 수행할 수 있습니다.

- 단일 위치에서 모든 디바이스에 대한 정책을 구성하므로 설정을 좀 더 쉽게 변경할 수 있습니다.
- 디바이스에 각종 소프트웨어 업데이트를 설치할 수 있습니다.
- 관리되는 디바이스에 상태 정책을 푸시하고 에서 상태를 모니터링할 수 있습니다. Firepower Management Center

Firepower Management Center는 침입 이벤트, 네트워크 검색 정보 및 디바이스 성능 데이터를 집계하고 상호 연결하므로 사용자는 디바이스가 상호 관계에 대해 보고하는 정보를 모니터링하고 네트워크에서 발생하는 전반적인 활동을 평가할 수 있습니다.

Firepower Management Center를 사용하면 디바이스 동작의 거의 모든 부분을 관리할 수 있습니다.



참고 하지만 Firepower Management Center는 <http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html>에서 사용 가능한 호환성 매트릭스에서 지정된 일부 이전 릴리스가 실행되는 디바이스를 관리할 수 있으며 이런 이전 릴리스를 사용하는 디바이스에서는 새로운 기능을 사용할 수 없습니다.

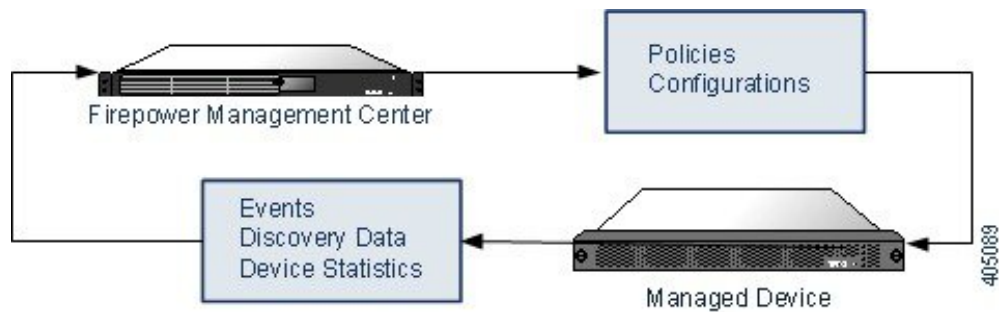
## Firepower Management Center로 관리할 수 있는 내용

Firepower Management Center를 다음과 같은 디바이스를 관리하기 위한 Firepower System 구축의 중앙 관리 지점으로 사용할 수 있습니다.

- 7000 및 8000 Series 디바이스
- ASA FirePOWER 모듈
- NGIPSv 디바이스
- Firepower Threat Defense(물리적 하드웨어 및 가상)

디바이스를 관리할 때에는 Firepower Management Center와 디바이스 간에 안전한 SSL 암호화 TCP 터널을 통해 정보가 전송됩니다.

다음 그림에서는 Firepower Management Center 및 해당 매니지드 디바이스 간에 무엇이 전송되는지를 보여줍니다. 어플라이언스 간에 전송되는 이벤트와 정책의 유형은 디바이스 유형을 기반으로 합니다.



## 정책 및 이벤트 이상

디바이스에 정책을 구축하고 디바이스에서 이벤트를 수신하는 것 외에도 Firepower Management Center에서는 다른 디바이스 관련 작업을 수행할 수 있습니다.

### 디바이스 백업

NGIPSv 디바이스 또는 ASA FirePOWER 모듈에 대한 백업 파일을 만들거나 복원할 수 없습니다.

디바이스 자체에서 관리되는 물리적 디바이스의 백업을 수행할 경우 디바이스 설정만 백업됩니다. 설정 데이터 및 선택적으로 통합된 파일을 백업하려면 관리하는 Firepower Management Center를 사용하여 디바이스의 백업을 수행할 수 있습니다.

이벤트 데이터를 백업하기 위해서는 관리하는 Firepower Management Center의 백업을 수행합니다.

### 디바이스 업데이트

Cisco는 다음과 같은 Firepower System의 업데이트를 수시로 배포합니다.

- 새로운 침입 규칙과 업데이트된 침입 규칙이 포함되는 침입 규칙 업데이트
- 취약성 데이터베이스(VDB) 업데이트
- 지리위치 업데이트
- 소프트웨어 패치 및 업데이트

관리하는 디바이스에 업데이트를 설치하려면 Firepower Management Center를 사용할 수 있습니다.

## 디바이스 관리 인터페이스

각 디바이스는 FMC와 통신하기 위한 단일 전용 관리 인터페이스를 포함합니다. 선택적으로 전용 관리 인터페이스 대신 관리용 데이터 인터페이스를 사용하도록 디바이스를 구성할 수 있습니다.

관리 인터페이스 또는 콘솔 포트에서 초기 설정을 수행할 수 있습니다.

관리 인터페이스는 Smart Licensing 서버와 통신하고, 업데이트를 다운로드하고, 기타 관리 기능을 수행하는 작업에도 사용됩니다.

### 매니지드 디바이스의 관리 인터페이스

디바이스를 설정할 때 연결할 FMC IP 주소를 지정합니다. 관리 및 이벤트 트래픽은 초기 등록 시 이 주소로 이동합니다. 참고: 일부 경우에 FMC는 다른 관리 인터페이스에서 초기 연결을 설정할 수 있습니다. 후속 연결은 지정된 IP 주소가 있는 관리 인터페이스를 사용해야 합니다.

FMC에 별도의 이벤트 전용 인터페이스가 있는 경우, 네트워크가 허용하는 경우 매니지드 디바이스에서 후속 이벤트 트래픽을 FMC 이벤트 전용 인터페이스로 보냅니다. 또한 일부 매니지드 디바이스 모델에는 이벤트 전용 트래픽에 대해 구성할 수 있는 추가 관리 인터페이스가 포함되어 있습니다. 관리를 위해 데이터 인터페이스를 구성하는 경우 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다. 이벤트 네트워크가 다운되면 이벤트 트래픽은 FMC 및/또는 매니지드 디바이스의 일반 관리 인터페이스로 되돌아갑니다.

## FTD 데이터 인터페이스를 사용하여 관리하는 방법에 대한 정보

FMC와의 통신에 전용 관리 인터페이스 또는 일반 데이터 인터페이스를 사용할 수 있습니다. 외부 인터페이스에서 원격으로 FTD를 관리하려는 경우 또는 별도의 관리 네트워크가 없는 경우 데이터 인터페이스의 FMC 액세스가 유용합니다.

데이터 인터페이스에서의 FMC 액세스에는 다음과 같은 제한이 있습니다.

- 하나의 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다.
- 이 인터페이스는 관리 전용일 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- 고가용성은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 FMC를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.

## 디바이스 모델별 관리 인터페이스 지원

관리 인터페이스 위치에 대한 모델의 하드웨어 설치 가이드를 참조하십시오.

각 매니지드 디바이스 모델에서 지원되는 관리 인터페이스는 다음 표를 참조하십시오.

표 1: 매니지드 디바이스의 관리 인터페이스 지원

모델	관리 인터페이스	선택적 이벤트 인터페이스
7000 Series	eth0	지원 안 함
8000 Series	eth0	eth1
NGIPSv	eth0	지원 안 함
ASA 5508-X 또는 5516-X의 ASA FirePOWER 서비스 모듈	eth0 참고 eth0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함

모델	관리 인터페이스	선택적 이벤트 인터페이스
ISA 3000의 ASA FirePOWER 서비스 모듈	eth0 참고 eth0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함
Firepower Threat Defense Firepower 1000	management0 참고 management0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함
Firepower Threat Defense Firepower 2100	management0 참고 management0은 Management 1/1 인터페이스의 내부 이름입니다.	지원 안 함

## 디바이스 관리 인터페이스의 네트워크 라우트

관리 인터페이스(이벤트 전용 인터페이스 포함)는 정적 경로만 지원하여 원격 네트워크에 연결할 수 있습니다. 매니지드 디바이스를 설정하면 설정 과정에서 지정한 게이트웨이 IP 주소에 대한 기본 경로가 생성됩니다. 이 경로는 삭제할 수 없으며 게이트웨이 주소만 수정할 수 있습니다.



**참고** 관리 인터페이스의 라우팅은 데이터 인터페이스에 대해 구성된 라우팅과는 완전히 분리됩니다. 전용 관리 인터페이스를 사용하는 대신 관리용 데이터 인터페이스를 설정하는 경우 데이터 라우팅 테이블을 사용하도록 트래픽이 백플레인을 통해 라우팅됩니다. 이 섹션의 정보는 적용되지 않습니다.

기본 경로는 항상 가장 낮은 번호의 관리 인터페이스(예: management0)를 사용합니다.

원격 네트워크에 액세스하기 위해서는 관리 인터페이스당 최소 1개의 정적 경로가 권장됩니다. 다른 디바이스에서 FTD 로의 라우팅 문제를 비롯하여 잠재적인 라우팅 문제를 방지하려면 각 인터페이스를 별도의 네트워크에 배치하는 것이 좋습니다. 동일한 네트워크의 인터페이스에서 문제가 발생하지 않으면 고정 경로를 올바르게 설정해야 합니다. 예를 들어 management0과 management1은 동일한 네트워크에 있지만 FMC 관리 및 이벤트 인터페이스는 서로 다른 네트워크에 있습니다. 게이트웨이는 192.168.45.1입니다. 10.6.6.1/24에서 management1을 FMC의 이벤트 전용 인터페이스에 연결하려는 경우 동일한 게이트웨이 192.168.45.1로 10.6.6.0/24에서 management1까지의 고정 경로를 생성할 수 있습니다. 10.6.6.0/24 트래픽은 기본 경로에 도달하기 전에 이 경로에 도달하므로 management1이 예상대로 사용됩니다.

또 다른 예는 FMC 및 매니지드 디바이스에 별도의 관리 및 이벤트 전용 인터페이스를 포함합니다. 이벤트 전용 인터페이스는 관리 인터페이스와 별도의 네트워크에 있습니다. 이 경우 원격 이벤트 전

용 네트워크를 대상으로 하는 트래픽에 대해 이벤트 전용 인터페이스를 통해 정적 경로를 추가할 수 있으며, 그 반대의 경우도 마찬가지입니다.

## NAT 환경

NAT(Network Address Translation)는 소스 또는 대상 IP 주소를 재할당하는 작업에 관여하는 라우터를 통해 네트워크 트래픽을 보내고 받는 방법입니다. NAT는 일반적으로 프라이빗 네트워크와 인터넷이 통신하는 데 사용됩니다. 정적 NAT는 1:1 변환을 수행하여 디바이스와 FMC의 통신에 문제를 일으키지 않지만 포트 주소 변환(PAT)이 더욱 일반적입니다. PAT를 사용하면 단일 공용 IP 주소에 고유한 포트를 사용해 공용 네트워크에 접속할 수 있습니다. 이러한 포트는 필요에 따라 동적으로 할당되므로 PAT 라우터 뒤에 있는 디바이스에 연결을 시작할 수 없습니다.

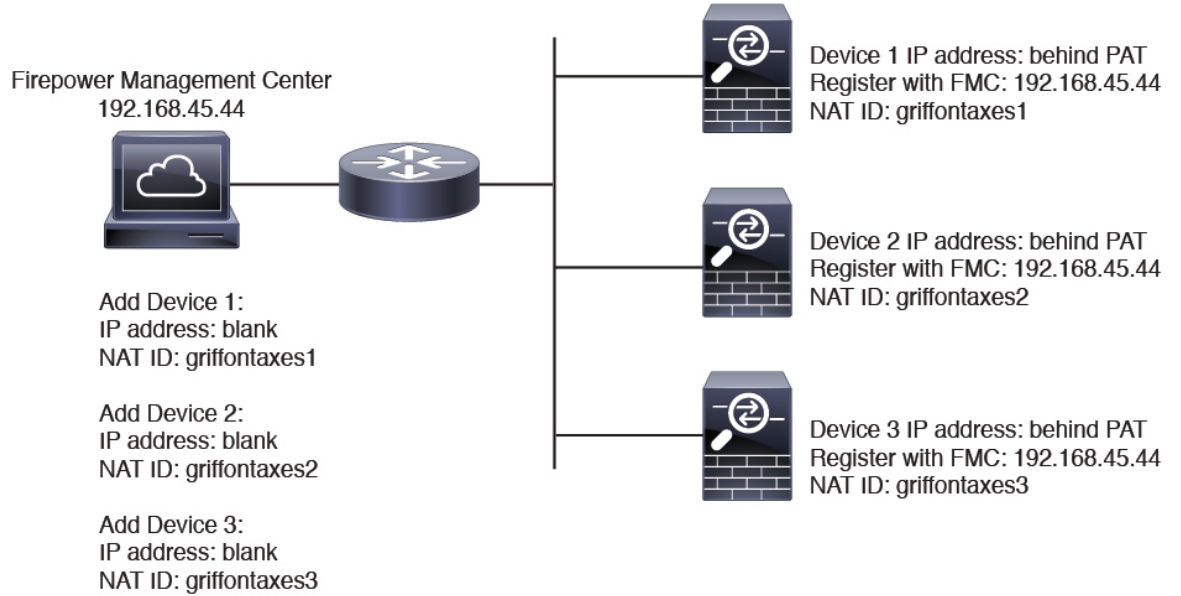
일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

예를 들어 FMC에 디바이스를 추가하지만 디바이스 IP 주소를 모르는 경우(디바이스가 PAT 라우터 뒤에 있는 경우) FMC에 NAT ID와 등록 키만 지정하고 IP 주소는 공백으로 둡니다. 디바이스에 FMC IP 주소, 동일한 NAT ID와 동일한 등록 키를 지정합니다. FMC의 IP 주소에 디바이스를 등록합니다. 이때 FMC는 IP 주소 대신 NAT ID를 사용해 디바이스를 인증합니다.

NAT 환경에서 NAT ID 사용은 일반적이지만 FMC에 많은 디바이스를 추가하려고 할 때에도 NAT ID를 선택할 수 있습니다. FMC에는 추가하려는 각 디바이스에 고유한 NAT ID를 지정하고 IP 주소를 공백으로 두고, 각 디바이스에서 FMC IP 주소 및 NAT ID를 지정하십시오. 주의: NAT ID는 디바이스별로 고유해야 합니다.

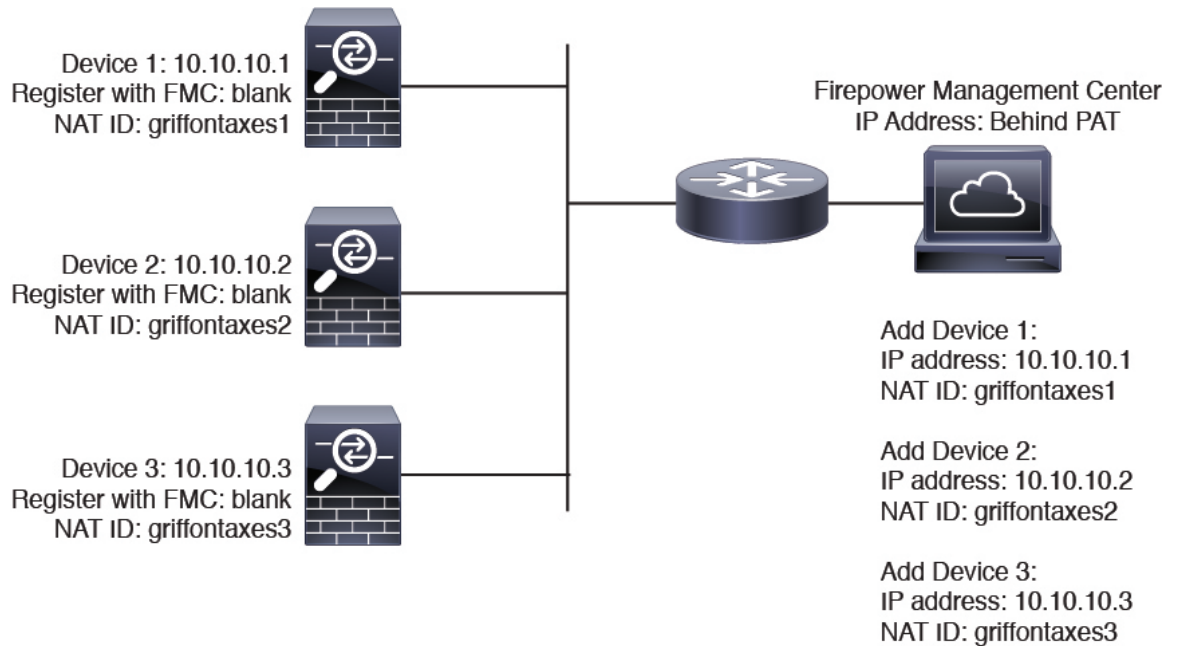
다음 예에서는 PAT IP 주소 뒤에 3개의 장치가 있음을 보여줍니다. 이 경우 FMC 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 디바이스에 FMC IP 주소를 지정하십시오.

그림 1: PAT 뒤의 관리되는 디바이스의 NAT ID



다음 예는 PAT ID 주소 뒤의 FMC를 보여줍니다. 이 경우 FMC 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 FMC에 디바이스 IP 주소를 지정하십시오.

그림 2: PAT 뒤의 FMC에 대한 NAT ID



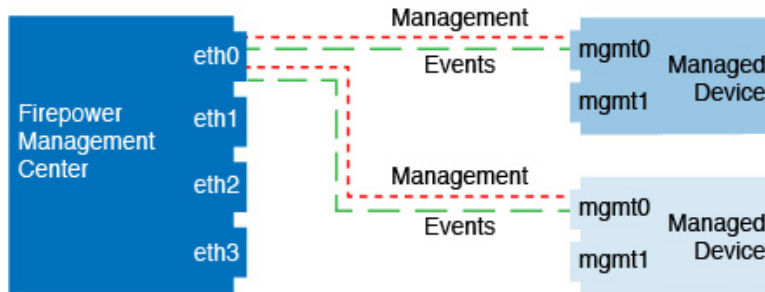
## 관리 및 이벤트 트래픽 채널 예시



참고 FTD에서 관리를 위해 데이터 인터페이스를 사용하는 경우 해당 디바이스에 대해 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다.

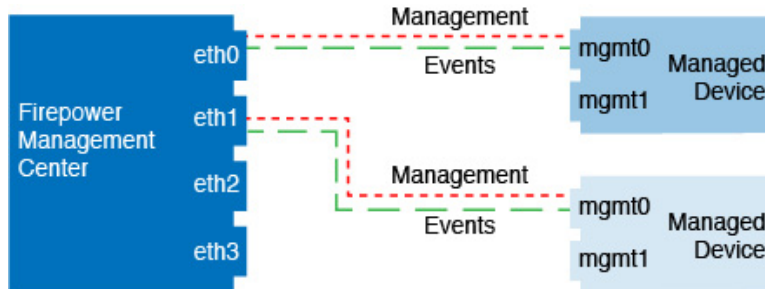
다음 예에서는 기본 관리 인터페이스만 사용하는 Firepower Management Center 및 매니지드 디바이스를 보여 줍니다.

그림 3: 단일 관리 인터페이스: **Firepower Management Center**



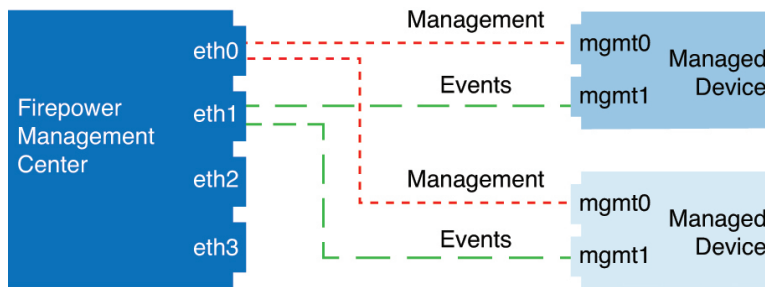
다음 예는 디바이스에 별도의 관리 인터페이스를 사용하는 Firepower Management Center를 보여 줍니다. 관리되는 각 디바이스는 1개의 관리 인터페이스를 사용합니다.

그림 4: 다중 관리 인터페이스: **Firepower Management Center**



다음 예에서는 별도의 이벤트 인터페이스를 사용하는 Firepower Management Center 및 매니지드 디바이스를 보여 줍니다.

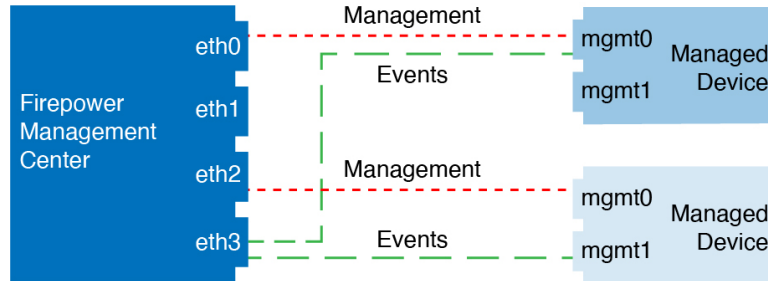
그림 5: **Firepower Management Center** 및 매니지드 디바이스에 대한 별도의 이벤트 인터페이스





다음 예는 별도의 이벤트 인터페이스를 사용하거나 단일 관리 인터페이스를 사용하는 Firepower Management Center 및 여러 매니지드 디바이스에 대한 다중 관리 인터페이스 및 별도의 이벤트 인터페이스를 보여 줍니다.

그림 6: 혼합 관리 및 이벤트 인터페이스 사용



## 디바이스 관리 요구 사항 및 사전 요건

모델 지원

모든 관리되는 디바이스(절차에 명시되지 않는 한)

지원되는 도메인

디바이스가 상주하는 도메인입니다.

사용자 역할

- 관리자
- Network Admin(네트워크 관리자)

## FTD 초기 설정 완료

FTD CLI에 연결하여 설정 마법사를 사용하여 관리 IP 주소, 게이트웨이 및 기타 기본 네트워킹 설정을 포함한 초기 설정을 수행합니다. 전용 관리 인터페이스는 자체 네트워크 설정이 있는 특수 인터페이스입니다. FMC 액세스에 관리 인터페이스를 사용하지 않으려는 경우, 대신 CLI를 사용하여 데이터 인터페이스를 설정할 수 있습니다. FMC 통신 설정도 구성합니다.

### Before you begin

이 절차는 Firepower 4100/9300을(를) 제외한 모든 FTD 디바이스에 적용됩니다. Firepower 4100/9300의 경우, [용 독립형 Firepower Threat Defense 추가](#)의 내용을 참조하십시오.

## Procedure

**단계 1** 콘솔 포트에서 또는 관리 인터페이스에 대한 SSH를 사용하여 FTD CLI에 연결합니다. 이 인터페이스는 기본적으로 DHCP 서버에서 IP 주소를 가져옵니다. 네트워크 설정을 변경하려는 경우 연결이 끊어지지 않도록 콘솔 포트를 사용하는 것이 좋습니다.

(Firepower 1000/2100) 콘솔 포트는 FXOS CLI에 연결합니다. SSH 세션은 FTD CLI에 직접 연결됩니다.

**단계 2** 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.

(Firepower 1000/2100) 콘솔 포트에서 사용자를 FXOS CLI에 연결합니다. FXOS에 처음 로그인하면 암호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 FTD 로그인에도 사용됩니다.

### 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#
```

**단계 3** (Firepower 1000/2100) 콘솔 포트에서 FXOS에 연결한 경우 FTD CLI에 연결합니다.

### connect ftd

### Example:

```
firepower# connect ftd
>
```

**단계 4** FTD에 처음 로그인할 경우, 최종 사용자 라이선스 계약(EULA)에 동의하고 SSH 연결을 사용 중인 경우 관리자 암호를 변경하라는 메시지가 표시됩니다. 그 다음에는 CLI 설정 스크립트가 표시됩니다.

**Note** 이미지 재설치 등을 통해 컨피그레이션을 지우지 않으면 CLI 설정 마법사를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network**(네트워크 구성) 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. [FTD 명령 참조](#)를 참조하십시오.

기본값 또는 이전에 입력한 값이 괄호 안에 표시됩니다. 이전에 입력한 값을 승인하려면 **Enter**를 누릅니다.

**Note** 관리 인터페이스 설정은 데이터 인터페이스에서 FMC 액세스를 활성화한 경우에도 사용됩니다. 예를 들어 데이터 인터페이스를 통해 백플레인으로 라우팅되는 관리 트래픽은 데이터 인터페이스 DNS 서버가 아닌 관리 인터페이스 DNS 서버를 사용하여 FQDN을 확인합니다.

다음 지침을 참조하십시오.

- **Configure IPv4 via DHCP or manually?(DHCP를 통해 또는 수동으로 IPv4를 설정하시겠습니까?)** - 관리 인터페이스 대신 FMC 액세스용 데이터 인터페이스를 사용하려면 **manual(수동)**을 선택합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다. 이 IP 주소는 트래픽이 데이터 인터페이스로 전달될 때 NAT 처리됩니다. 관리 인터페이스가 DHCP로 설정된 경우 관리를 위해 데이터 인터페이스를 설정할 수 없습니다. 데이터 인터페이스(데이터 인터페이스)여야 하는 기본 경로(다음 글머리 기호 참조)가 DHCP 서버에서 수신한 기본 경로를 덮어 쓸 수 있기 때문입니다.
- **Enter the IPv4 default gateway for the management interface(관리 인터페이스에 대한 IPv4 기본 게이트웨이 입력)** - 관리 인터페이스 대신 FMC 액세스에 데이터 인터페이스를 사용하려면 게이트웨이를 데이터 인터페이스(데이터 인터페이스)로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 FMC 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다. FMC 액세스에 관리 인터페이스를 사용하려면 관리 1/1 네트워크에서 게이트웨이 IP 주소를 설정해야 합니다.
- **If your networking information has changed, you will need to reconnect(네트워킹 정보가 변경된 경우 다시 연결해야 합니다)** — SSH를 통해 연결되어 있지만 최초 설정에서 IP 주소를 변경한 경우 연결이 끊깁니다. 새 IP 주소 및 비밀번호를 사용하여 다시 연결합니다. 콘솔 연결에는 영향을 미치지 않습니다.
- **Manage the device locally?(디바이스를 로컬로 관리하시겠습니까?)**—FMC을(를) 사용하려면 **no**를 입력합니다. 예를 입력하면 Firepower Device Manager를 대신 사용하게 됩니다.
- **Configure firewall mode?(방화벽 모드를 설정하시겠습니까?)**—초기 설정에서 방화벽 모드를 설정하는 것이 좋습니다. 초기 설정 후에 방화벽 모드를 변경하면 실행 중인 구성이 지워집니다. 데이터 인터페이스 FMC 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

### Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
```

```

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]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

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.
>

```

단계 5 이 FTD를 관리할 FMC을(를) 식별합니다.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
```

- {hostname | IPv4\_address | IPv6\_address | **DONTRESOLVE**}—FMC의 FQDN 또는 IP 주소를 지정합니다. FMC의 주소를 직접 지정할 수 없는 경우 **DONTRESOLVE**를 사용하고 *nat\_id*도 지정합니다. 하나 이상의 디바이스(FMC 또는 FTD)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다. 이 명령에서 **DONTRESOLVE**를 지정하는 경우 FTD에 연결할 수 있는 IP 주소 또는 호스트 이름이 있어야 합니다.
- *reg\_key* — FTD 등록시 FMC에 지정할 일회용 등록 키를 지정합니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다.
- *nat\_id* — 한쪽이 연결할 수 있는 IP 주소 또는 호스트 이름을 지정하지 않은 경우 FTD를 등록할 때 FMC에 지정할 고유한 일회용 문자열을 지정합니다. FMC를 **DONTRESOLVE**로 설정하는 경우 반드시 필요합니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 FMC에 등록하는 다른 디바이스에 사용할 수 없습니다.

**Note** 관리에 데이터 인터페이스를 사용하는 경우 등록을 위해 FTD 및 FMC 모두에서 NAT ID를 지정해야 합니다.

**Example:**

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

FMC이(가) NAT 디바이스 뒤에 있는 경우 등록 키와 고유한 NAT ID를 입력하고 호스트 이름 대신 DONTRESOLVE를 지정합니다. 예를 들면 다음과 같습니다.

**Example:**

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

FTD가 NAT 디바이스 뒤에 있는 경우 FMC IP 주소 또는 호스트 이름과 함께 고유한 NAT ID를 입력합니다. 예를 들면 다음과 같습니다.

**Example:**

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

**단계 6** (Optional) FMC 액세스를 위한 데이터 인터페이스를 설정합니다.

**configure network management-data-interface**

그러면 데이터 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

**Note** 이 명령을 사용할 때는 콘솔 포트를 사용해야 합니다. 관리 인터페이스에 SSH를 사용하는 경우 연결이 끊기고 콘솔 포트에 다시 연결해야 할 수 있습니다. SSH 사용량에 대한 자세한 내용은 아래를 참조하십시오.

이 명령 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 관리에 데이터 인터페이스를 사용하려는 경우 원래 관리 인터페이스에서 DHCP를 사용할 수 없습니다. 초기 설정 중에 IP 주소를 수동으로 설정하지 않은 경우 지금 **configure network {ipv4 | ipv6} manual** 명령을 사용하여 설정할 수 있습니다. 관리 인터페이스 게이트웨이를 아직 **data-interfaces**로 설정하지 않은 경우, 이 명령이 이제 설정합니다.
- 데이터 인터페이스에서의 FMC 액세스에는 다음과 같은 제한이 있습니다.
  - 하나의 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다.
  - 이 인터페이스는 관리 전용일 수 없습니다.
  - 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
  - 고가용성은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.
  - PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모델 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
  - 인터페이스는 전역 VRF에만 있어야 합니다.
  - 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.

- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 FMC를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.
- FMC에 FTD를 추가하면 FMC는 인터페이스 이름 및 IP 주소, 게이트웨이에 대한 고정 경로, DNS 서버 및 DDNS 서버를 포함한 인터페이스 컨피그레이션을 검색하고 유지 관리합니다. DNS 서버 설정에 관한 자세한 내용은 아래를 참조하십시오. FMC에서 나중에 FMC 액세스 인터페이스 구성을 변경할 수 있지만, FTD 또는 FMC가 관리 연결을 재설정하지 못하게 할 수 있는 변경은 수행하지 않아야 합니다. 관리 연결이 중단되면 FTD에 이전 구축을 복구하는 **configure policy rollback** 명령이 포함됩니다.
- DDNS 서버 업데이트 URL을 설정하는 경우 FTD가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 Cisco Trusted Root CA 번들에서 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. FTD는 DynDNS 원격 API 사양(<https://help.dyn.com/remote-access-api/>)을 사용하는 모든 DDNS 서버를 지원합니다.
- 이 명령은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 스크립트로 설정하거나 **configure network dns servers** 명령을 사용하여 설정한 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다.  
FMC에서 이 FTD에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. FMC에 FTD를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 구성을 포함하는 FTD에 플랫폼 설정 정책을 할당하면 해당 구성이 로컬 설정을 덮어씁니다. FMC와 FTD를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 설정하는 것이 좋습니다.  
또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 FMC에 의해 유지됩니다. 예를 들어 관리 인터페이스를 사용하여 디바이스를 등록한 다음 나중에 **configure network management-data-interface** 명령을 사용하여 데이터 인터페이스를 설정하는 경우 FTD 구성과 일치하도록 DNS 서버를 포함하여 FMC에서 이러한 모든 설정을 수동으로 설정해야 합니다.
- FTD를 FMC에 등록한 후 관리 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.
- 설정 마법사에서 설정한 FQDN이 이 인터페이스에 사용됩니다.
- 명령의 일부로 전체 디바이스 구성을 지울 수 있습니다. 복구 시나리오에서는 이 옵션을 사용할 수 있지만 초기 설정 또는 정상 작동에는 이 옵션을 사용하지 않는 것이 좋습니다.
- 데이터 관리를 비활성화하려면 **configure network management-data-interface disable** 명령을 입력합니다.

**Example:**

```
> 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://jcrichton: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 FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>

```

**Example:**

```

> 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
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 FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>

```

단계 7 (Optional) 특정 네트워크의 FMC에 대한 데이터 인터페이스 액세스를 제한합니다.

```
configure network management-data-interface client ip_address netmask
```

기본적으로 모든 네트워크가 허용됩니다.

**What to do next**

장치를 FMC에 등록합니다.

## FMC에 디바이스 추가

단일 디바이스를 FMC에 추가하려면 이 절차를 사용합니다. 디바이스를 이중화 또는 성능을 위해 연결하려는 경우 다음을 염두에 두고 이 절차를 사용합니다.

- 8000 Series스택 - 이 절차를 사용해 각 디바이스를 Firepower Management Center에 추가하고 스택을 설정할 때 [디바이스 스택 설정](#)의 내용을 참조하십시오.
- 7000 및 8000 Series고가용성 - 이 절차를 사용해 각 디바이스를 Firepower Management Center에 추가하고 고가용성을 설정할 때 [Firepower 7000/8000 시리즈 고가용성 설정](#)의 내용을 참조하십시오. 고가용성 스택의 경우 먼저 디바이스를 스택킹하고 스택 간 고가용성을 설정합니다.

- FTD 클러스터 - 클러스터 추가에 대한 자세한 내용은 [FMC: 클러스터 추가](#)의 내용을 참조하십시오.

#### 시작하기 전에

- FMC에서 관리할 수 있도록 디바이스를 설정합니다. 적절한 빠른 시작 가이드를 참조하십시오. 7000 및 8000 Series 디바이스에 대해서는 [매니지드 디바이스에서 원격 관리 구성](#)의 내용도 참조하십시오.
- FTD 디바이스를 추가하는 경우, FMC를 Smart Licensing Server(CSSM)에 등록해야 합니다. 유효한 평가 라이선스는 충분하지만, 만료되면 등록에 성공할 때까지 새 디바이스를 추가할 수 없습니다.
- FMC 및 IPv4를 사용하는 디바이스를 등록했으며 IPv6으로 전환하려는 경우, 해당 디바이스를 삭제하고 다시 등록해야 합니다.

#### 프로시저

- 
- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.
  - 단계 2 **Add**(추가) 드롭다운 메뉴에서 **Device**(디바이스)를 선택합니다.



### Add Device ?

---

Host:†

Display Name:

Registration Key:\*

Group:

Access Control Policy:\*

Smart Licensing

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

- Transfer Packets

**단계 3** 추가할 디바이스의 IP 주소 또는 호스트 이름을 호스트 필드에 입력합니다.

디바이스의 호스트 이름은 FQDN(Fully Qualified Domain Name) 또는 유효한 IP 주소에 로컬 DNS를 통해 확인하는 이름입니다. 사용자 네트워크가 IP 주소를 할당하기 위해 DHCP를 사용하는 경우 IP 주소 대신 호스트 이름을 사용합니다.

NAT 환경에서는, FMC로 관리되는 디바이스를 구성할 때 FMC의 IP 주소 또는 호스트 이름을 이미 지정한 경우 디바이스의 IP 주소 또는 호스트 이름을 지정하지 않아도 될 수 있습니다. 자세한 내용은 [NAT 환경, 6 페이지](#)의 내용을 참고하십시오.

**단계 4** FMC에 표시할 디바이스의 이름을 표시 이름 필드에 입력합니다.

- 단계 5 FMC로 관리할 디바이스를 구성할 때 사용한 것과 동일한 등록 키를 등록 키 필드에 입력합니다. 등록 키는 일회용 공유 암호입니다.
- 단계 6 다중 도메인 구축에서는 현재 도메인과 상관없이 디바이스를 리프 도메인으로 할당합니다.  
현재 도메인이 리프 도메인인 경우 디바이스는 자동으로 현재 도메인에 추가됩니다. 현재 도메인이 리프 도메인이 아닌 경우나 이후 재등록을 한 경우라면 리프 도메인으로 전환하여 디바이스를 구성합니다.
- 단계 7 (선택 사항) 디바이스 그룹에 디바이스를 추가합니다.
- 단계 8 등록 시 디바이스를 구축하기 위해 초기 액세스 제어 정책을 선택하거나 새 정책을 생성합니다.  
디바이스가 선택한 정책과 호환되지 않는 경우 구축이 실패합니다. 이러한 문제는 라이선싱 불일치, 모델 제약 조건, 수동 대 인라인 문제, 기타 잘못된 구성을 비롯한 여러 가지 이유로 인해 발생할 수 있습니다. 오류 원인을 해결한 뒤 디바이스에 수동으로 설정을 구축합니다.

- 단계 9 디바이스에 적용할 라이선스를 선택합니다.

#### 스마트 라이선싱

구축하려는 기능에 필요한 스마트 라이선스를 할당합니다.

- 악성코드(AMP 악성코드 검사를 사용하려는 경우)
- 위협(침입 방지를 사용하려는 경우)
- URL(범주 기반 URL 필터링을 구현하려는 경우)

#### Classic Licensing

- Control, Malware 및 URL Filtering 라이선스에는 Protection 라이선스가 필요합니다.
- VPN 라이선스는 하나의 7000 또는 8000 Series 디바이스를 요구합니다.
- NGIPSv와 ASA FirePOWER 디바이스에서는 제어 라이선스가 지원되지만, 8000 Series 빠른 경로 규칙, 전환, 라우팅, 스택킹, 디바이스 고가용성 구성을 허용하지 않습니다.

- 단계 10 디바이스 설정 중 NAT ID를 사용하는 경우 **Advanced**(고급) 섹션을 확장하고 **Unique NAT ID**(고유 NAT ID) 필드에 동일한 NAT ID를 입력합니다.

- 단계 11 패킷 전송 체크 박스를 선택하여 디바이스가 Firepower Management Center에 패킷을 전송하도록 합니다.

이 옵션은 기본적으로 활성화되어 있습니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 FMC에 전송합니다. 이벤트를 비활성화하면 이벤트 정보는 FMC에 전송되지만 패킷 데이터는 전송되지 않습니다.

- 단계 12 **Register**(등록)를 클릭합니다.

FMC이 디바이스의 하트비트를 확인하고 통신을 설정하는 데 최대 2분이 소요될 수 있습니다. 등록에 성공하면 디바이스가 목록에 추가됩니다. 오류가 발생하면 오류 메시지가 표시됩니다. 디바이스가 등록에 실패하면 다음 항목을 확인하십시오.

- Ping - 다음 명령을 사용해 디바이스 CLI에 액세스하고 FMC IP 주소에 Ping을 보냅니다.

**ping system ip\_address**

Ping이 실패하는 경우 **show network** 명령을 사용해 네트워크 설정을 확인합니다. 디바이스 IP 주소를 변경해야 하는 경우 **configure network {ipv4 | ipv6} manual** 명령을 사용합니다.

- 등록 키, NAT ID 및 FMC IP 주소 - 두 디바이스에서 동일한 등록 키 및 NAT ID가 사용되고 있는지 확인합니다. **configure manager add** 명령을 사용해 디바이스에서 등록 키 및 NAT ID를 설정할 수 있습니다.

자세한 문제 해결 정보는 <https://cisco.com/go/fmc-reg-error>를 참조하십시오.

## FMC에서 디바이스 삭제

디바이스를 더 이상 관리하지 않으려면 FMC에서 삭제할 수 있습니다. 디바이스 삭제

- 모든 서버는 Firepower Management Center과 디바이스 간 통신합니다.
- 디바이스 관리 페이지에서 디바이스를 제거합니다.
- 디바이스가 NTP를 통해 FMC에서 시간을 수신하도록 플랫폼 정책 설정을 통해 구성된 경우 디바이스가 로컬 시간 관리로 반환됩니다.


이후 디바이스를 관리하려면 FMC에 다시 추가합니다.



**참고** 디바이스를 삭제하고 다시 추가하는 경우 FMC 웹 인터페이스에서 액세스 제어 정책을 재적용하라는 메시지가 표시됩니다. 그러나 재등록 시 NAT 및 VPN 정책을 다시 적용하는 옵션은 없습니다. 재등록 시 이전에 적용된 모든 NAT 또는 VPN 설정이 삭제되며 등록이 완료한 뒤에 이를 다시 적용해야 합니다.

### 프로시저

**단계 1** **Devices(디바이스) > Device Management(디바이스 관리)**을(를) 선택합니다.

**단계 2** 삭제하려는 디바이스 옆에 있는 삭제(  )을 클릭합니다.

**단계 3** 디바이스를 삭제하려면 확인합니다.

## 디바이스 그룹 추가

Firepower Management Center에서는 디바이스를 그룹화하여 편리하게 정책을 구축하고 여러 디바이스에 업데이트를 설치할 수 있습니다. 그룹에 있는 디바이스의 목록을 확장 및 축소할 수 있습니다.

다중 도메인 구축의 경우 리프 도메인 내에서만 디바이스 그룹을 생성할 수 있습니다. 멀티테넌시에 Firepower Management Center을 구성하는 경우 기존 디바이스 그룹이 제거되지만 리프 도메인 레벨에서 다시 추가할 수 있습니다.

스택이나 고가용성 쌍의 기본 디바이스를 그룹에 추가하면 두 디바이스 모두 그룹에 추가됩니다. 디바이스를 스택에서 제거하거나 고가용성 쌍을 중단하는 경우에도 두 디바이스는 해당 그룹에 남아 있습니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 드롭다운 메뉴의 **Add**(추가)에서 **Add Group**(그룹 추가)를 선택합니다.

기존 그룹을 수정하려면 수정하려는 그룹에 대한 수정(✎)을 클릭합니다.

단계 3 **Name**(이름)을 입력합니다.

단계 4 **Available Devices**(사용 가능한 장치)에서 디바이스 그룹에 추가할 하나 이상의 디바이스를 선택합니다. 여러 디바이스를 선택하려면 Ctrl 또는 Shift 키를 누른 상태에서 클릭합니다.

단계 5 디바이스 그룹에서 선택한 디바이스를 포함하려면 **Add**(추가)를 클릭합니다.

단계 6 선택적으로 디바이스 그룹에서 디바이스를 제거하려면 제거하려는 디바이스 옆의 제거(삭제(🗑️))를 클릭합니다.

단계 7 디바이스 그룹에 추가하려면 **OK**(확인)를 클릭합니다.

## 디바이스 설정 구성

디바이스를 추가한 후 디바이스의 **Device**(디바이스) 페이지에서 일부 설정을 구성 할 수 있습니다.

## 시스템 종료 관리


스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	Any(모든)	ASA FirePOWER를 제외한 모든 디바이스	리프 전용	관리자/네트워크 관리자



**참고** Firepower System 사용자 인터페이스에서 ASA FirePOWER을 종료하거나 다시 시작할 수 없습니다. 각 디바이스를 종료하는 방법에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

## 프로시저


단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 다시 시작할 디바이스 옆의 수정()을 클릭합니다.


다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 **Device**(디바이스)를 클릭합니다.

팁 스택킹된 디바이스의 경우 어플라이언스 편집기의 디바이스 페이지에서 개별 디바이스를 종료하거나 다시 시작합니다.

단계 4 디바이스를 종료하려면 시스템 섹션에서 디바이스 종료()를 클릭합니다.

단계 5 메시지가 표시되면 디바이스 종료를 확인합니다.

단계 6 디바이스를 다시 시작하려면 디바이스 재시작()을 클릭합니다.

단계 7 메시지가 표시되면 디바이스 다시 시작을 확인합니다.

## 관리 설정 편집

**Management**(관리) 영역에서 관리 설정을 편집할 수 있습니다.


### FMC에서 호스트 이름 또는 IP 주소 업데이트

디바이스의 호스트 이름 또는 IP 주소를 (디바이스의 CLI 등을 사용해) FMC에 추가했다면, 아래의 절차를 사용하여 관리 FMC의 호스트 이름 또는 IP 주소를 수동으로 업데이트해야 할 수 있습니다.

디바이스에서 디바이스 관리 IP 주소를 변경하려면 참조하십시오. [CLI에서 디바이스 관리 인터페이스 수정, 31 페이지](#)

## 프로시저


단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 관리 옵션을 수정할 디바이스 옆의 수정()를 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

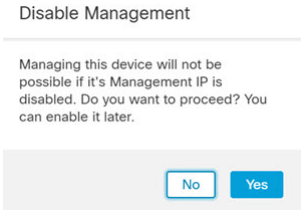
단계 3 **Device**(디바이스)를 클릭하고 **Management**(관리) 영역을 확인합니다.

팁 스택킹된 디바이스의 경우 어플라이언스 편집기의 디바이스 페이지에서 개별 디바이스의 관리 옵션을 수정할 수 있습니다.

단계 4 슬라이더 활성화됨()을(를) 클릭하여 관리를 일시적으로 비활성화합니다.



관리 비활성화를 진행하라는 메시지가 표시됩니다. **Yes(예)**를 클릭합니다.



관리를 비활성화하면 Firepower Management Center와 디바이스 간 연결이 차단되지만 Firepower Management Center에서 디바이스가 삭제되지는 않습니다.

단계 5 수정(✎)를 클릭하여 **Host(호스트)** IP 주소 또는 호스트 이름을 수정합니다.



**Management(관리)** 대화상자에서 **Host(호스트)** 필드의 이름 또는 IP 주소를 수정하고 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [권피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

## 관리에서 데이터로 FMC 액세스 인터페이스 변경

전용 관리 인터페이스 또는 데이터 인터페이스에서 FTD를 관리할 수 있습니다. 디바이스를 FMC에 추가 한 후 FMC 액세스 인터페이스를 변경하려면 다음 단계에 따라 관리 인터페이스에서 데이터 인터페이스로 마이그레이션합니다. 다른 방향으로 마이그레이션하려면 [데이터에서 관리로 FMC 액세스 인터페이스 변경, 25 페이지](#)의 내용 참조하십시오.

관리에서 데이터로의 FMC 액세스 마이그레이션을 시작하면 구축시 FTD에 차단을 적용합니다. 블록을 제거하려면 데이터 인터페이스에서 FMC 액세스를 활성화합니다.

데이터 인터페이스에서 FMC 액세스를 활성화하고 다른 필수 설정도 구성하려면 다음 단계를 참조하십시오.

시작하기 전에

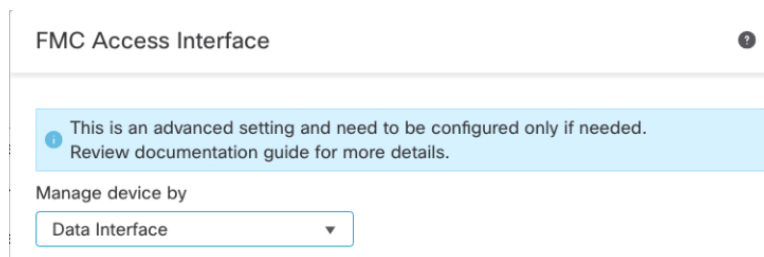
모델 지원—FTD

## 프로시저

단계 1 인터페이스 마이그레이션을 시작합니다.

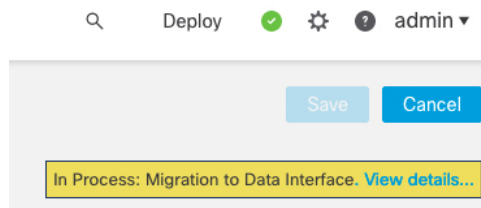
- a) **Devices(디바이스) > Device Management(디바이스 관리)** 페이지에서 디바이스에 대해 수정(✎)을 클릭합니다.
- b) **Device(디바이스) > Management(관리)** 섹션으로 이동하여 **FMC Access Interface(FMC 액세스 인터페이스)** 링크를 클릭합니다.

**FMC Access Interface(FMC 액세스 인터페이스)** 필드에는 현재 관리 인터페이스가 표시됩니다. 링크를 클릭하면 **Manage device by(디바이스 관리 기준)** 드롭 다운 목록에서 새 인터페이스 유형인 **Data Interface(데이터 인터페이스)**를 선택합니다.



- c) **Save(저장)**를 클릭합니다.

이제 데이터 인터페이스에서 FMC 액세스를 활성화하려면 이 절차의 나머지 단계를 완료해야 합니다. **Devices(디바이스)** 페이지의 오른쪽 상단에 관리 인터페이스를 마이그레이션하고 있음을 나타내는 노란색 배너가 표시됩니다.



**View Details(세부 사항 보기)**를 클릭하면 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > FMC Access Details(FMC 액세스 세부 사항)** 대화상자가 열립니다. **FMC 액세스 모드**에는 In Process(처리 중) 마이그레이션이 표시됩니다.

Configuration		
Version	7.1.0	7.1.0 (Build 1760)
Configuration Cleared		No
FMC Access Mode	Data Interface (Deploy pending)	Management Interface
Connectivity Status	Connected	Connected

단계 2 **Devices(디바이스) > Device Management(디바이스 관리) > Interfaces(인터페이스) > Edit Physical Interface(물리적 인터페이스 편집) > FMC Access(FMC 액세스)** 페이지에서 데이터 인터페이스에 대한 FMC 액세스를 활성화합니다.

라우팅 모드 인터페이스 구성을 참조하십시오. 하나의 라우팅된 데이터 인터페이스에서 FMC 액세스를 활성화할 수 있습니다. 이 인터페이스가 이름 및 IP 주소로 완전히 구성되어 있고 활성화되어 있는지 확인합니다.

**단계 3** (선택 사항) 인터페이스에 DHCP를 사용하는 경우 **Devices(디바이스) > Device Management(디바이스 관리) > DHCP > DDNS** 페이지에서 웹 유형 DDNS 방법을 활성화합니다.

동적 DNS 구성을 참조하십시오. DDNS는 FTD의 IP 주소가 변경될 경우 FMC가 FQDN(Fully-Qualified Domain Name)에서 FTD에 연결할 수 있도록 합니다.

**단계 4** FTD가 데이터 인터페이스를 통해 FMC로 라우팅될 수 있는지 확인합니다. **Device(디바이스) > Device Management(디바이스 관리) > Routing(라우팅) > Static Route(고정 경로)**에서 필요한 경우 고정 경로를 추가합니다.

고정 경로 추가의 내용을 참조하십시오.

**단계 5** (선택 사항) 플랫폼 설정 정책에서 DNS를 구성하고 **Devices(디바이스) > Platform Settings(플랫폼 설정) > DNS**에서 이 디바이스에 적용합니다.

DNS 구성을 참조하십시오. DDNS를 사용하는 경우 DNS가 필요합니다. 보안 정책에서 FQDN에 대해 DNS를 사용할 수도 있습니다.

**단계 6** (선택 사항) 플랫폼 설정 정책에서 데이터 인터페이스에 대해 SSH를 활성화하고 **Devices(디바이스) > Platform Settings(플랫폼 설정) > Secure Shell(보안 셸)**에서 이 디바이스에 적용합니다.

에서 SSH(Secure Shell) 설정을 참조하십시오. SSH는 데이터 인터페이스에서 기본적으로 활성화되어 있지 않으므로 SSH를 사용하여 FTD를 관리하려면 그를 명시적으로 허용해야 합니다.

**단계 7** 구성 변경사항을 구축합니다. **컨피그레이션 변경 사항 구축**의 내용을 참조하십시오.

FMC는 현재 관리 인터페이스를 통해 구성 변경 사항을 구축합니다. 구축 후에는 데이터 인터페이스를 사용할 수 있지만 관리에 대한 원래 관리 연결은 계속 활성화됩니다.

**단계 8** 콘솔 포트의 FTD CLI에서 관리 인터페이스가 고정 IP 주소를 사용하도록 설정하고 게이트웨이가 데이터 인터페이스를 사용하도록 설정합니다.

**configure network {ipv4 | ipv6} manual ip\_address netmask data-interfaces**

- **ip\_address netmask**-관리 인터페이스를 사용하지 않더라도 고정 IP 주소(예: 개인 주소)를 설정해야 합니다. 데이터 인터페이스 여야하는 기본 경로(다음 글 머리 기호 참조)가 DHCP 서버에서 수신한 경로로 덮어 쓰여질 수 있으므로 DHCP를 사용할 수 없습니다.
- **data-interfaces** —이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 FMC 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다.

관리 인터페이스 네트워크 설정을 변경하면 SSH 세션의 연결이 끊어 지므로 SSH 연결 대신 콘솔 포트를 사용하는 것이 좋습니다. 다음과 같은 경우

**단계 9** 필요한 경우 데이터 인터페이스에서 FMC에 연결할 수 있도록 FTD를 다시 케이블로 연결합니다.

**단계 10** FMC에서 관리 연결을 비활성화하고 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리)** 섹션에서 FTD의 호스트 IP 주소를 업데이트한 다음 연결을 다시 활성화합니다.



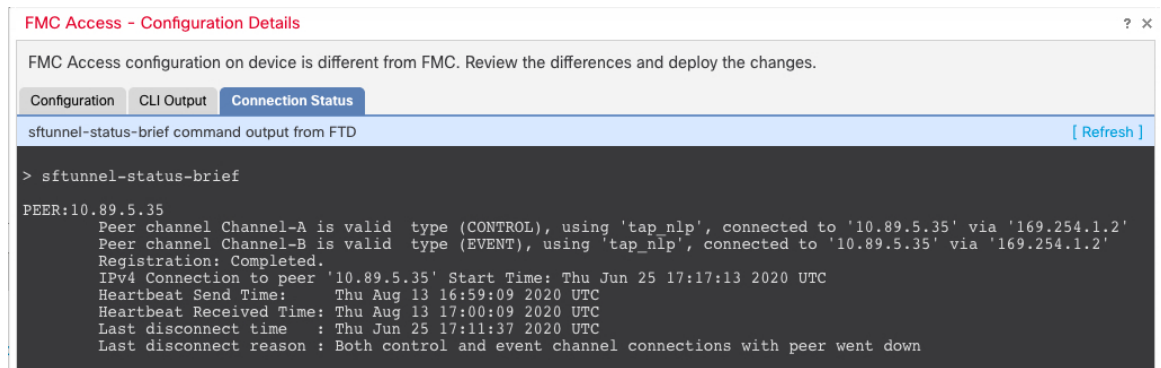
FMC에서 호스트 이름 또는 IP 주소 업데이트, 21 페이지의 내용을 참조하십시오. FTD를 FMC에 추가할 때 FTD 호스트 네임 또는 NAT ID만 사용한 경우, 값을 업데이트할 필요가 없습니다. 그러나 연결을 다시 시작하려면 관리 연결을 비활성화했다가 다시 활성화해야 합니다.

단계 11 관리 연결이 다시 설정되었는지 확인합니다.

FMC의 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > FMC Access Details(FMC 액세스 디테일) > Connection Status(연결 상태)** 페이지에서 관리 연결 상태를 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 `sftunnel-status-brief` 명령을 입력합니다.

다음 상태는 내부 "tap\_nlp" 인터페이스를 보여주는 데이터 인터페이스의 성공적인 연결을 보여줍니다.



```

FMC Access - Configuration Details
FMC Access configuration on device is different from FMC. Review the differences and deploy the changes.
Configuration  CLI Output  Connection Status
sftunnel-status-brief command output from FTD [Refresh]
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.2'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Thu Jun 25 17:17:13 2020 UTC
Heartbeat Send Time: Thu Aug 13 16:59:09 2020 UTC
Heartbeat Received Time: Thu Aug 13 17:00:09 2020 UTC
Last disconnect time : Thu Jun 25 17:11:37 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
  
```

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 41 페이지의 내용을 참조하십시오.

## 데이터에서 관리로 FMC 액세스 인터페이스 변경

전용 관리 인터페이스 또는 데이터 인터페이스에서 FTD를 관리할 수 있습니다. 디바이스를 FMC에 추가한 후 FMC 액세스 인터페이스를 변경하려면 다음 단계에 따라 데이터 인터페이스에서 관리 인터페이스로 마이그레이션합니다. 다른 방향으로 마이그레이션하려면 관리에서 데이터로 FMC 액세스 인터페이스 변경, 22 페이지의 내용 참조하십시오.

데이터에서 관리로 FMC 액세스 마이그레이션을 시작하면 FMC가 구축 시 FTD에 차단을 적용합니다. 차단을 제거하려면 데이터 인터페이스에서 FMC 액세스를 비활성화해야 합니다.

데이터 인터페이스에서 FMC 액세스를 비활성화하고 다른 필수 설정도 구성하려면 다음 단계를 참조하십시오.

시작하기 전에

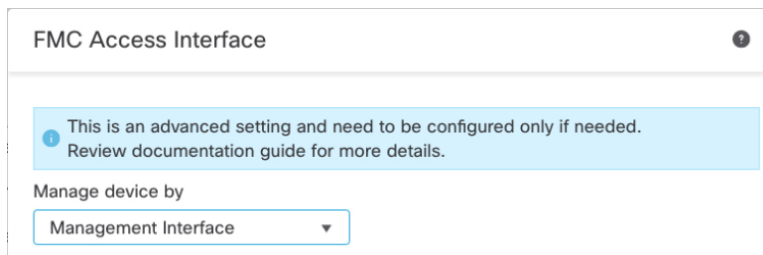
모델 지원—FTD

프로시저

단계 1 인터페이스 마이그레이션을 시작합니다.

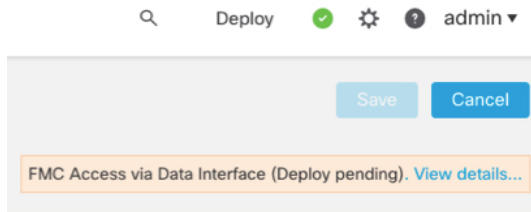
- a) **Devices**(디바이스) > **Device Management**(디바이스 관리) 페이지에서 디바이스에 대해 수정(✎)을 클릭합니다.
- b) **Device**(디바이스) > **Management**(관리) 섹션으로 이동하여 **FMC Access Interface**(FMC 액세스 인터페이스) 링크를 클릭합니다.

**FMC Access Interface**(FMC 액세스 인터페이스) 필드에는 현재 관리 인터페이스가 표시됩니다. 링크를 클릭할 때 **Manage device by**(디바이스 관리 기준) 드롭다운 목록에서 새 인터페이스 유형인 **Management Interface**(관리 인터페이스)를 선택합니다.



- c) **Save**(저장)를 클릭합니다.

이제 이 절차의 나머지 단계를 완료하여 관리 인터페이스에서 FMC 액세스를 활성화해야 합니다. **Devices**(디바이스) 페이지의 오른쪽 상단에 관리 인터페이스를 마이그레이션하고 있음을 나타내는 노란색 배너가 표시됩니다.



**View Details**(세부 사항 보기)를 클릭하면 **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Device**(디바이스) > **Management**(관리) > **FMC Access Details**(FMC 액세스 세부 사항) 대화 상자가 열립니다. FMC 액세스 모드에는 In Process(처리 중) 마이그레이션이 표시됩니다.

1. Device Summary		
<b>Configuration</b>		
Version	6.7.0	6.7.0 (Build 1974)
Configuration Cleared		No
<b>FMC Access Mode</b>	<b>Data Interface (Deploy pending)</b>	<b>Management Interface</b>
Connectivity Status	Connected	Connected

단계 2 **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Interfaces**(인터페이스) > **Edit Physical Interface**(물리적 인터페이스 편집) > **FMC Access**(FMC 액세스) 페이지에서 데이터 인터페이스에 대한 FMC 액세스를 비활성화합니다.

[라우팅 모드 인터페이스 구성](#)를 참조하십시오. 이 단계에서는 구축 시 차단을 제거합니다.

**단계 3** 아직 수행하지 않은 경우, 플랫폼 설정 정책에서 데이터 인터페이스에 대한 DNS 설정을 구성하고 **Devices(디바이스) > Platform Settings(플랫폼 설정) > DNS**에서 해당 디바이스에 적용합니다.

[DNS 구성](#)를 참조하십시오. 데이터 인터페이스에서 FMC 액세스를 비활성화하는 FMC 구축은 로컬 DNS 설정을 제거합니다. 해당 DNS 서버가 액세스 규칙의 FQDN과 같은 보안 정책에서 사용되는 경우, FMC를 통해 DNS 구성을 다시 적용해야 합니다.

**단계 4** 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

FMC는 현재 데이터 인터페이스를 통해 구성 변경 사항을 구축합니다.

**단계 5** 필요한 경우, 관리 인터페이스에서 FMC에 연결할 수 있도록 FTD를 다시 케이블로 연결합니다.

**단계 6** FTD CLI에서 고정 IP 주소 또는 DHCP를 사용하여 관리 인터페이스 IP 주소 및 게이트웨이를 설정합니다.

원래 FMC 액세스용 데이터 인터페이스를 설정하면 관리 게이트웨이가 데이터 인터페이스로 설정되었습니다. 이 인터페이스는 관리 트래픽을 백플레인을 통해 전달하여 FMC 액세스 데이터 인터페이스를 통해 라우팅할 수 있도록 지원했습니다. 이제 관리 네트워크에서 게이트웨이의 IP 주소를 설정해야 합니다.

고정 IP 주소:

```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```

DHCP:

```
configure network {ipv4 | ipv6} dhcp
```

**단계 7** FMC에서 관리 연결을 비활성화하고 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리)** 섹션에서 FTD의 호스트 IP 주소를 업데이트한 다음 연결을 다시 활성화합니다.

[FMC에서 호스트 이름 또는 IP 주소 업데이트, 21 페이지](#)의 내용을 참조하십시오. FTD를 FMC에 추가할 때 FTD 호스트네임 또는 NAT ID만 사용한 경우, 값을 업데이트할 필요가 없습니다. 그러나 연결을 다시 시작하려면 관리 연결을 비활성화했다가 다시 활성화해야 합니다.

**단계 8** 관리 연결이 다시 설정되었는지 확인합니다.

FMC의 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > Status(상태)** 필드에서 관리 연결 상태를 확인하거나 FMC에서 알림을 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 `sftunnel-status-brief` 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. [데이터 인터페이스에서 관리 연결성 문제 해결, 41 페이지](#)의 내용을 참조하십시오.

## 데이터 인터페이스 관리를 위한 FMC 액세스 세부정보 보기

모델 지원—FTD

전용 관리 인터페이스를 사용하는 대신 FMC 관리용 데이터 인터페이스를 사용하는 경우, FMC에서 FTD에 대한 인터페이스 및 네트워크 설정을 변경할 때 연결이 중단되지 않도록 주의해야 합니다. 디바이스에서 로컬로 데이터 인터페이스 설정을 변경할 수도 있습니다. 이렇게 하려면 FMC에서 이러한 변경 사항을 수동으로 조정해야 합니다. **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > FMC Access Details(FMC 액세스 세부정보)** 대화 상자를 사용하면 FMC와 FTD 로컬 구성 간의 불일치를 해결할 수 있습니다.

일반적으로 FMC에 FTD를 추가하기 전에 초기 FTD 설정의 일부로 FMC 액세스 데이터 인터페이스를 구성합니다. FMC에 FTD를 추가하면 FMC는 인터페이스 이름 및 IP 주소, 게이트웨이에 대한 고정 경로, DNS 서버 및 DDNS 서버를 포함한 인터페이스 구성을 검색하고 유지 관리합니다. DNS 서버의 경우 구성이 등록 중에 검색된 경우 로컬로 유지되지만 FMC의 플랫폼 설정 정책에 추가되지 않습니다.

FTD를 FMC에 추가한 후 **configure network management-data-interface** 명령을 사용하여 FTD의 데이터 인터페이스 설정을 로컬로 변경하면 FMC는 구성 변경 사항을 탐지하고 FTD에 대한 구축을 차단합니다. FMC는 다음 방법 중 하나를 사용하여 구성 변경을 탐지합니다.

- FTD에 구축합니다. FMC는 구축하기 전에 구성 차이를 탐지하고 구축을 중지합니다.
- **Interface(인터페이스)** 페이지의 **Sync(동기화)** 버튼
- **FMC Access Details(FMC 액세스 상세정보)** 대화 상자의 **Refresh(새로 고침)** 버튼

블록을 제거하려면 **FMC Access Details(FMC 액세스 상세정보)** 대화 상자로 이동하여 **Acknowledge(확인)**를 클릭해야 합니다. 다음에 구축할 때 FMC 컨피그레이션은 FTD의 나머지 충돌 설정을 덮어씁니다. 재구축하기 전에 FMC에서 컨피그레이션을 수동으로 수정하는 것은 사용자의 책임입니다.

이 대화 상자에서 다음 페이지를 참조하십시오.

#### 컨피그레이션

FMC 및 FTD에서 FMC 액세스 데이터 인터페이스의 구성 비교를 확인합니다.

다음 예에서는 FTD에서 **configure network management-data-interface** 명령이 입력된 FTD의 구성 세부 사항을 보여줍니다. 분홍으로 강조 표시된 부분은 차이점을 **Acknowledge(확인)** 하지만 FMC의 구성과 일치하지 않으면 FTD 구성이 제거됨을 나타냅니다. 파란색으로 강조 표시된 부분은 FTD에서 수정될 구성을 보여줍니다. 녹색으로 강조 표시된 부분은 FTD에 추가될 구성을 보여줍니다.

**FMC Access - Configuration Details** ? x

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

**Configuration** | CLI Output | Connection Status

Last updated: 2020-06-23 at 23:36:16 UTC [ Refresh ]

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
<b>DDNS - Update Methods</b>		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
<b>Interface Configuration</b>		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29 255.255.255.192
<b>Static Route Configuration</b>		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from FMC Access interface on next deploy to FTD.

다음 예는 FMC에서 인터페이스를 구성한 후의 이 페이지를 보여줍니다. 인터페이스 설정이 일치하고 분홍색 강조 표시가 제거되었습니다.

**FMC Access - Configuration Details** ? x

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

**Configuration** | CLI Output | Connection Status

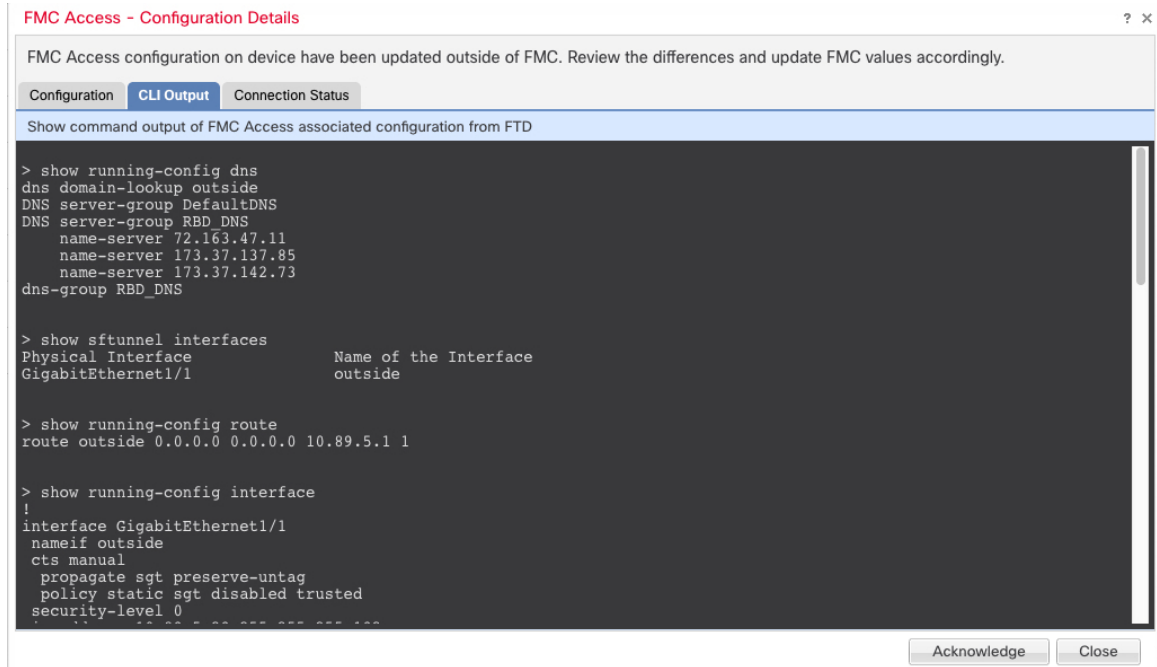
Last updated: 2020-06-23 at 23:36:16 UTC [ Refresh ]

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
<b>DDNS - Update Methods</b>		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
<b>Interface Configuration</b>		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
<b>Static Route Configuration</b>		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from FMC Access interface on next deploy to FTD.

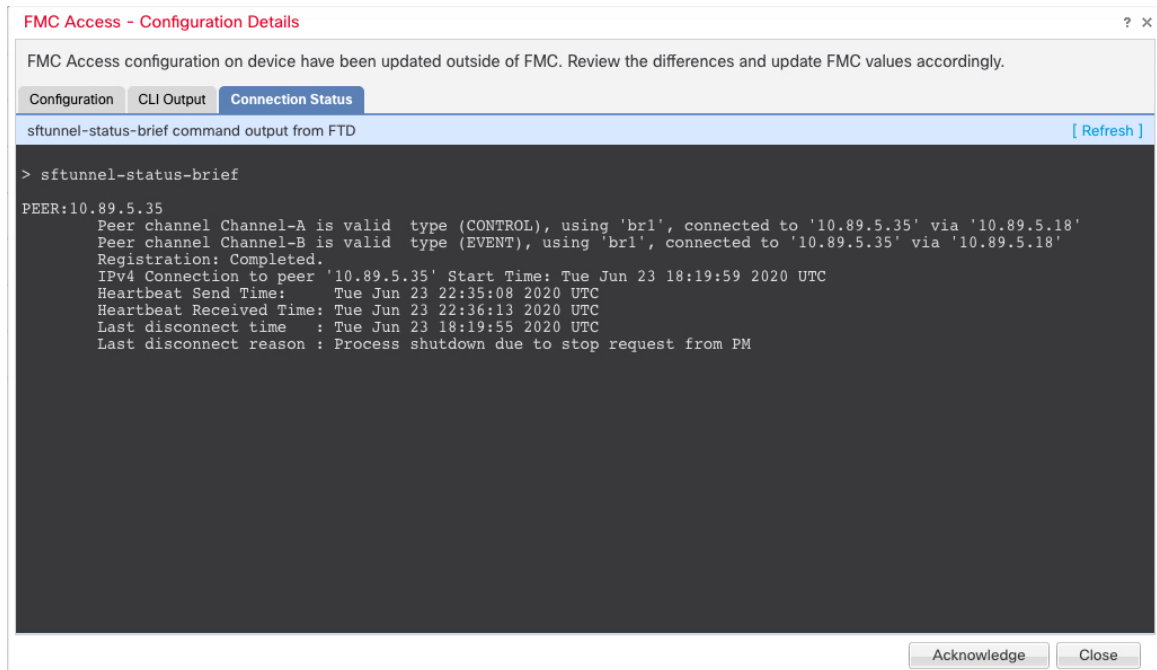
### CLI 출력

FMC 액세스 데이터 인터페이스의 CLI 구성을 확인합니다. 이는 기본 CLI에 익숙한 경우 유용합니다.



### 연결 상태

관리 연결 상태를 봅니다. 다음 예는 관리 연결이 여전히 관리 "br1" 인터페이스를 사용하고 있음을 보여줍니다.



다음 상태는 내부 "tap\_nlp" 인터페이스를 보여주는 데이터 인터페이스의 성공적인 연결을 보여줍니다.

```
FMC Access - Configuration Details
FMC Access configuration on device is different from FMC. Review the differences and deploy the changes.
Configuration CLI Output Connection Status
sftunnel-status-brief command output from FTD [Refresh]
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.2'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Thu Jun 25 17:17:13 2020 UTC
Heartbeat Send Time: Thu Aug 13 16:59:09 2020 UTC
Heartbeat Received Time: Thu Aug 13 17:00:09 2020 UTC
Last disconnect time : Thu Jun 25 17:11:37 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

작동 중지된 연결에 대해서는 다음 샘플 출력을 참조하십시오. 다음과 같은 피어 채널이나 하트비트 정보가 "연결"되지 않았습니다.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
'10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

## CLI에서 디바이스 관리 인터페이스 수정

CLI를 사용하여 매니지드 디바이스의 관리 인터페이스 설정을 수정합니다. 이러한 설정 중 대부분은 초기 설정을 수행할 때의 설정입니다. 이 절차를 통해 해당 설정을 변경하고 모델에서 지원하는 경우 이벤트 인터페이스를 활성화하거나 정적 경로를 추가하는 등의 추가 설정을 지정할 수 있습니다.



**참고** 이 항목은 전용 관리 인터페이스에 적용됩니다. 관리를 위해 데이터 인터페이스를 설정할 수도 있습니다. 해당 인터페이스의 네트워크 설정을 변경하려면 CLI가 아닌 FMC 내에서 변경해야 합니다. 중단된 관리 연결을 문제 해결해야 하고 FTD에서 직접 변경해야 하는 경우 [CLI에서 관리에 사용되는 FTD 데이터 인터페이스 수정, 38 페이지](#)의 내용을 참조하십시오.

FTD CLI에 대한 자세한 내용은 [FTD 명령 참조](#)를 참조하십시오.

클래식 디바이스 CLI에 대한 내용은 이 가이드의 [명령줄 참조](#) 섹션을 참조하십시오.



FTD 및 클래식 디바이스는 관리 인터페이스 설정에 대해 동일한 명령을 사용합니다. 다른 명령은 플랫폼에 따라 다를 수 있습니다.



**참고** SSH를 사용하여 관리 인터페이스를 변경할 때는 주의하십시오. 구성 오류로 인해 다시 연결할 수 없는 경우 디바이스 콘솔 포트에 액세스해야 합니다.



**참고** 디바이스 관리 IP 주소를 변경하는 경우 **configure manager add** 명령을 사용하여 초기 디바이스 설정 중에 FMC를 식별한 방법에 따라 FMC 연결에 대한 다음 작업을 참조하십시오(새 FMC 식별, 56 페이지 참조).

- **IP address(IP 주소)** - 작업이 없습니다. 연결 가능한 IP 주소를 사용하여 FMC를 식별한 경우 몇 분 후 관리 연결이 자동으로 다시 설정됩니다. 정보를 동기화 상태로 유지하려면 FMC에 표시되는 디바이스 IP 주소도 변경하는 것이 좋습니다. [FMC에서 호스트 이름 또는 IP 주소 업데이트, 21 페이지](#)의 내용을 참조하십시오. 이 작업은 연결을 더 빠르게 재설정하는 데 도움이 될 수 있습니다. 참고: 연결할 수 없는 FMC IP 주소를 지정한 경우 아래의 NAT ID 절차를 참조하십시오.
- **NAT ID만** - 수동으로 연결을 재설정합니다. NAT ID만 사용하여 FMC를 식별한 경우 연결을 자동으로 재설정할 수 없습니다. 이 경우 [FMC에서 호스트 이름 또는 IP 주소 업데이트, 21 페이지](#)에 따라 FMC에서 디바이스 관리 IP 주소를 변경합니다.



**참고** 고가용성 설정에서 등록된 Firepower 디바이스의 관리 IP 주소를 디바이스 CLI 또는 FMC에서 수정하면 보조 FMC는 HA 동기화가 끝나도 변경 사항을 반영하지 않습니다. 보조 FMC도 업데이트되게 하려면 두 FMC의 역할을 바꿔 보조 FMC를 액티브 유닛으로 설정해야 합니다. 현재 액티브 FMC의 디바이스 관리 페이지에 등록한 Firepower 디바이스의 관리 IP 주소를 수정합니다.

시작하기 전에

- Firepower Threat Defense 디바이스의 경우, **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. [FTD CLI용 로컬 사용자 계정 생성](#) CLI에서 [내부 사용자 추가](#) 섹션을 참조하십시오.
- 7000 및 8000 Series 디바이스의 경우, [사용자 어카운트 만들기](#)에 설명된 대로 웹 인터페이스에서 사용자 어카운트를 생성할 수 있습니다.

프로시저

- 단계 1** 콘솔 포트 또는 SSH를 사용하여 디바이스 CLI에 연결합니다.  
[7000/8000 시리즈, ASA FirePOWER, NGIPSv 디바이스에서 CLI에 로그인](#)를 참조하십시오.
- 단계 2** 관리자 사용자 이름 및 비밀번호로 로그인합니다.



단계 3 (Firepower 4100/9300만 해당) 이벤트 전용 인터페이스 사용.

**configure network management-interface enable management1**

**configure network management-interface disable-management-channel management1**

예제:

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

Firepower Management Center 이벤트 전용 인터페이스는 관리 채널 트래픽을 허용할 수 없으므로 디바이스 이벤트 인터페이스에서 관리 채널을 비활성화해야 합니다.

**configure network management-interface disable-events-channel** 명령을 사용하여 관리 인터페이스의 이벤트를 선택적으로 비활성화할 수 있습니다. 두 경우 모두에서 디바이스는 이벤트 전용 인터페이스로 이벤트를 전송하려고 시도하며 해당 인터페이스가 다운되면 이벤트 채널을 비활성화하는 경우에도 관리 인터페이스에서 이벤트를 전송합니다.

인터페이스에서 이벤트 및 관리 채널을 비활성화할 수 없습니다.

단계 4 관리 인터페이스 및/또는 이벤트 인터페이스의 네트워크 설정을 구성합니다.

*management\_interface* 인수를 지정하지 않으면 기본 관리 인터페이스에 대한 네트워크 설정을 변경하면 됩니다. 이벤트 인터페이스를 구성할 때 *management\_interface* 인수를 지정해야 합니다. 이벤트 인터페이스는 관리 인터페이스와 별도의 네트워크에 있거나 동일한 네트워크에 있을 수 있습니다. 구성 중인 인터페이스에 연결되어 있으면 연결이 끊어집니다. 새 IP 주소에 다시 연결할 수 있습니다.

a) IPv4 주소 구성:

- 수동 구성:

**configure network ipv4 manual ip\_address netmask gateway\_ip [management\_interface]**

이 명령의 *gateway\_ip*는 디바이스의 기본 경로를 만드는 데 사용됩니다. 이벤트 전용 인터페이스를 설정하는 경우 명령의 일부로 *gateway\_ip*를 입력해야 합니다. 그러나 이 항목은 사용자가 지정한 값에 대한 기본 경로만 설정하며 이벤트 인터페이스에 대해 별도의 고정 경로를 생성하지 않습니다. 관리 인터페이스와 다른 네트워크에서 이벤트 전용 인터페이스를 사용하는 경우 관리 인터페이스와 함께 사용할 *gateway\_ip*를 설정한 다음 **configure network static-routes** 명령을 사용하여 이벤트 전용 인터페이스에 대해 별도의 고정 경로를 생성하는 것이 좋습니다.

예:

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.

>
```

- DHCP(기본 관리 인터페이스에서만 지원됨):

```
configure network ipv4 dhcp
```

b) IPv6 주소 구성:

- 상태 비저장 자동 구성:

```
configure network ipv6 router [management_interface]
```

예:

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.

>
```

- 수동 구성:

```
configure network ipv6 manual ip6_address ip6_prefix_length [ip6_gateway_ip]
[management_interface]
```

이 명령의 *ip6\_gateway\_ip*는 디바이스의 기본 경로를 만드는 데 사용됩니다. 이벤트 전용 인터페이스를 설정하는 경우 명령의 일부로 *ip6\_gateway\_ip*를 입력해야 합니다. 그러나 이 항목은 사용자가 지정한 값에 대한 기본 경로만 설정하며 이벤트 인터페이스에 대해 별도의 고정 경로를 생성하지 않습니다. 관리 인터페이스와 다른 네트워크에서 이벤트 전용 인터페이스를 사용하는 경우 관리 인터페이스와 함께 사용할 *ip6\_gateway\_ip*를 설정한 다음 **configure network static-routes** 명령을 사용하여 이벤트 전용 인터페이스에 대해 별도의 고정 경로를 생성하는 것이 좋습니다.

예:

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.

>
```

- DHCPv6(기본 관리 인터페이스에서만 지원됨):

```
configure network ipv6 dhcp
```

**단계 5** IPv6의 경우 ICMPv6 Echo Reply 및 Destination Unreachable 메시지를 활성화하거나 비활성화합니다. 이러한 메시지는 기본적으로 활성화됩니다.

```
configure network ipv6 destination-unreachable {enable | disable}
```

```
configure network ipv6 echo-reply {enable | disable}
```

잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 디바이스 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다.

예제:

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

**단계 6** (FTD 전용) 기본 관리 인터페이스의 DHCP 서버가 연결된 호스트에 IP 주소를 제공할 수 있게 활성화합니다.

**configure network ipv4 dhcp-server-enable** *start\_ip\_address end\_ip\_address*

예제:

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled
>
```

관리 인터페이스 IP 주소를 수동으로 설정할 때만 DHCP 서버를 구성할 수 있습니다. 이 명령은 Firepower Threat Defense Virtual에서 지원되지 않습니다. DHCP 서버 상태를 표시하려면 **show network-dhcp-server:**를 입력합니다.

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

**단계 7** Firepower Management Center가 원격 네트워크에 있는 경우 이벤트 전용 인터페이스에 정적 경로를 추가합니다. 그렇지 않으면 모든 트래픽이 관리 인터페이스를 통해 기본 경로와 일치하게 됩니다.

**configure network static-routes** {**ipv4** | **ipv6**} **add** *management\_interface destination\_ip netmask\_or\_prefix gateway\_ip*

기본 경로의 경우 이 명령을 사용하지 마십시오. **configure network ipv4** 또는 **ipv6** 명령을 사용할 때만 기본 경로 게이트웨이 IP 주소를 변경할 수 있습니다(4단계 참조).

라우팅에 대한 내용은 [디바이스 관리 인터페이스의 네트워크 라우트, 5 페이지](#) 섹션을 참조하십시오.

예제:

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully
>
```

정적 경로를 표시하려면 **show network-static-routes**를 입력합니다(기본 경로는 표시되지 않음).

```
> show network-static-routes
-----[ IPv4 Static Routes ]-----
Interface           : management1
Destination         : 192.168.6.0
```

```
Gateway                : 10.10.10.1
Netmask                : 255.255.255.0
[...]
```

#### 단계 8 호스트네임 설정

**configure network hostname** *name*

예제:

```
> configure network hostname farscape1.cisco.com
```

시스템 로그 메시지는 리부팅될 때까지 새 호스트네임을 반영하지 않습니다.

#### 단계 9 검색 도메인 설정:

**configure network dns searchdomains** *domain\_list*

예제:

```
> configure network dns searchdomains example.com,cisco.com
```

디바이스에 대한 검색 도메인을 쉼표로 구분하여 설정합니다. 이 도메인은 명령(예: **ping system**)에서 FQDN(Fully Qualified Domain Name)을 지정하지 않은 경우 호스트 이름에 추가됩니다. 도메인은 관리 인터페이스에서 사용되거나 관리 인터페이스를 통과하는 명령에 대해서만 사용됩니다.

#### 단계 10 쉼표로 구분하여 최대 3개의 DNS 서버를 설정합니다.

**configure network dns servers** *dns\_ip\_list*

예제:

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

#### 단계 11 FMC와의 통신을 위한 원격 관리 포트를 설정합니다.

**configure network management-interface tcpport** *number*

예제:

```
> configure network management-interface tcpport 8555
```

FMC 및 매니지드 디바이스는 기본적으로 포트 8305에 있는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

참고 Cisco에서는 원격 관리 포트에 대해 기본 설정을 유지할 것을 적극 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 디바이스의 설정을 변경해야 합니다.

#### 단계 12 (FTD 전용) 관리 또는 이벤트 인터페이스 MTU를 설정합니다. MTU는 기본적으로 1500바이트입니다.

**configure network mtu** [*bytes*] [*interface\_id*]

- *bytes* - MTU를 바이트 단위로 설정합니다. 관리 인터페이스의 경우 IPv4를 활성화하는 경우 값의 범위는 64 ~ 1500이고 IPv6를 활성화하는 경우 값은 1280 ~ 1500입니다. 이벤트 인터페이스의 경우 IPv4를 활성화하는 경우 값의 범위는 64 ~ 9000이고 IPv6를 활성화하는 경우 값은 1280 ~ 9000입니다. IPv4 및 IPv6를 모두 활성화하는 경우 최소값은 1280입니다. 바이트를 입력하지 않으면 값을 입력하라는 프롬프트가 표시됩니다.
- *interface\_id* — MTU를 설정할 인터페이스 ID를 지정합니다. 플랫폼에 따라 사용 가능한 인터페이스 ID(예: management0, management1, br1, eth0)를 보려면 **show network** 명령을 사용합니다. 인터페이스를 지정하지 않으면 관리 인터페이스가 사용됩니다.

예제:

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

**단계 13** HTTP 프록시를 구성합니다. 디바이스는 TCP/443(HTTPS) 및 TCP/80(HTTP) 포트에서 직접 인터넷에 연결되도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다. 명령을 실행하면 HTTP 프록시 주소와 포트, 프록시 인증이 필요한지 여부에 대한 프롬프트가 표시되며, 해당 인증이 필요한 경우 프록시 사용자 이름, 프록시 비밀번호, 프록시 비밀번호의 확인에 대한 프롬프트가 표시됩니다.

참고 Cisco Firepower Threat Defense의 프록시 비밀번호의 경우 A-Z, a-z 및 0-9 문자만 사용할 수 있습니다.

#### configure network http-proxy

예제:

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

**단계 14** 디바이스 관리 IP 주소를 변경하는 경우 **configure manager add** 명령을 사용하여 초기 디바이스 설정 중에 FMC를 식별한 방법에 따라 FMC 연결에 대한 다음 작업을 참조하십시오(새 FMC 식별, 56 페이지 참조).

- **IP address(IP 주소)** - 작업이 없습니다. 연결 가능한 IP 주소를 사용하여 FMC를 식별한 경우 몇 분 후 관리 연결이 자동으로 다시 설정됩니다. 정보를 동기화 상태로 유지하려면 FMC에 표시되는 디바이스 IP 주소도 변경하는 것이 좋습니다. FMC에서 호스트 이름 또는 IP 주소 업데이트, 21 페이지의 내용을 참조하십시오. 이 작업은 연결을 더 빠르게 재설정하는 데 도움이 될 수 있습니다. 참고: 연결할 수 없는 FMC IP 주소를 지정한 경우 FMC에서 호스트 이름 또는 IP 주소 업데이트, 21 페이지을(를) 사용하여 연결을 수동으로 다시 설정해야 합니다.

- **NAT ID**만 - 수동으로 연결을 재설정합니다. NAT ID만 사용하여 FMC를 식별한 경우 연결을 자동으로 재설정할 수 없습니다. 이 경우 **FMC에서 호스트 이름 또는 IP 주소 업데이트**, 21 페이지에 따라 FMC에서 디바이스 관리 IP 주소를 변경합니다.

## CLI에서 관리에 사용되는 FTD 데이터 인터페이스 수정

FTD와 FMC 간의 관리 연결이 중단된 상태에서 기존 인터페이스를 대체할 새 데이터 인터페이스를 지정하려는 경우 FTD CLI를 사용하여 새 인터페이스를 설정합니다. 이 절차에서는 동일한 네트워크에서 기존 인터페이스를 새 인터페이스로 교체하려 한다고 가정합니다. 관리 연결이 활성 상태이면 FMC를 사용하여 기존 데이터 인터페이스를 변경해야 합니다. 데이터 관리 인터페이스의 초기 설정에 대해서는 **FTD 초기 설정 완료**, 9 페이지에서 **configure network management-data-interface** 명령을 참조하십시오.



**참고** 이 항목은 전용 관리 인터페이스가 아니라 관리용으로 설정한 데이터 인터페이스에 적용됩니다. 관리 인터페이스의 네트워크 설정을 변경하려면 **CLI에서 디바이스 관리 인터페이스 수정**, 31 페이지의 내용을 참조하십시오.

FTD CLI에 대한 자세한 내용은 **FTD 명령 참조**를 참조하십시오.

시작하기 전에

- **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 사용자 계정을 생성할 수 있습니다. **CLI에서 내부 사용자 추가**의 내용을 참조하십시오. **SSH에 대한 외부 인증 설정**에 따라 AAA 사용자를 구성할 수도 있습니다.

프로시저

- 단계 1** 데이터 관리 인터페이스를 새 인터페이스로 변경하는 경우 현재 인터페이스 케이블을 새 인터페이스로 이동합니다.
- 단계 2** 디바이스 CLI에 연결합니다.  
이러한 명령을 사용할 때는 콘솔 포트를 사용해야 합니다. 초기 설정을 수행하는 경우 관리 인터페이스에서 연결이 끊어질 수 있습니다. 관리 연결이 중단되어 구성을 수정하는 경우 전용 관리 인터페이스에 대한 SSH 액세스 권한이 있는 경우 해당 SSH 연결을 사용할 수 있습니다.  
**FTD 디바이스의 FTD 명령줄 인터페이스에 로그인**의 내용을 참조하십시오.
- 단계 3** 관리자 사용자 이름 및 비밀번호로 로그인합니다.
- 단계 4** FMC 액세스 인터페이스의 이름을 설정하십시오.  
**configure network management-data-interface**  
그러면 데이터 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

데이터 관리 인터페이스를 동일한 네트워크의 새 인터페이스로 변경할 때는 인터페이스 ID를 제외하고 이전 인터페이스와 동일한 설정을 사용합니다. 또한, 적용하기 전에 모든 디바이스 구성을 지우시겠습니까? (y/n) [n]: 옵션에 대해 y를 선택합니다. 이 옵션을 선택하면 이전 데이터 관리 인터페이스 구성이 지워지므로 새 인터페이스에서 IP 주소 및 인터페이스 이름을 성공적으로 재사용할 수 있습니다.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
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
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y

Configuration done with option to allow FMC access from any network, if you wish to change
the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

단계 5 (선택 사항) 특정 네트워크에서 FMC에 대한 데이터 인터페이스 액세스를 제한합니다.

```
configure network management-data-interface client ip_address netmask
```

기본적으로 모든 네트워크가 허용됩니다.

단계 6 연결은 자동으로 재설정되지만 FMC에서 연결을 비활성화했다가 다시 활성화하면 연결을 더 빠르게 재설정하는 데 도움이 됩니다. FMC에서 호스트 이름 또는 IP 주소 업데이트, 21 페이지의 내용을 참조하십시오.

단계 7 관리 연결이 재설정되었는지 확인합니다.

```
sftunnel-status-brief
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
'10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

단계 8 FMC에서 Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > FMC Access Details(FMC 액세스 세부 정보)를 선택하고 Refresh(새로 고침)를 클릭합니다.

FMC는 인터페이스 및 기본 경로 구성 변경을 탐지하고 FTD에 대한 구축을 차단합니다. 디바이스에서 로컬로 데이터 인터페이스 설정을 변경하는 경우 FMC에서 수동으로 변경 사항을 조정해야 합니다. **Configuration(구성)** 탭에서 FMC와 FTD 간의 불일치를 볼 수 있습니다.

**단계 9 Devices(디바이스) > Device Management(디바이스 관리) > Interfaces(인터페이스)**를 선택하고 다음을 변경합니다.

- a) 이전 데이터 관리 인터페이스에서 IP 주소와 이름을 제거하고 이 인터페이스에 대해 FMC 액세스를 비활성화합니다.
- b) 이전 인터페이스(CLI에서 사용한 인터페이스)의 설정으로 새 데이터 관리 인터페이스를 설정하고 FMC 액세스를 활성화합니다.

**단계 10 Devices(디바이스) > Device Management(디바이스 관리) > Routing(라우팅) > Static Route(고정 경로)**를 선택하고 기존 데이터 관리 인터페이스에서 새 경로로 기본 경로를 변경합니다.

**단계 11 FMC Access Details(FMC 액세스 세부 정보)** 대화 상자로 돌아가서 **Acknowledge(확인)**를 클릭하여 구축 블록을 제거합니다.

다음에 구축할 때 FMC 구성은 FTD의 나머지 충돌 설정을 덮어씁니다. 재구축하기 전에 FMC에서 구성을 수동으로 수정하는 것은 사용자의 책임입니다.

"Config was cleared(구성이 지워졌습니다)" 및 "FMC Access changed and acknowledged(FMC 액세스가 변경되어 승인되었습니다)"라는 메시지가 표시됩니다.

## FMC가 연결을 상실할 경우 컨피그레이션을 롤백

FMC 관리를 위해 FTD에서 데이터 인터페이스를 사용하고 네트워크 연결에 영향을 주는 FMC에서 구성 변경 사항을 구축하는 경우 관리 연결을 복원할 수 있도록 FTD의 구성을 마지막으로 구축된 구성으로 롤백할 수 있습니다. 그런 다음 네트워크 연결이 유지되도록 FMC에서 구성 설정을 조정하고 다시 구축할 수 있습니다. 연결이 끊기지 않아도 롤백 기능을 사용할 수 있습니다. 이는 이 문제 해결 상황으로 제한되지 않습니다.

다음 지침을 참조하십시오.

- 이전 구축만 FTD에서 로컬로 사용할 수 있습니다. 이전 구축으로 롤백할 수 없습니다.
- 고가용성 또는 클러스터링 구축에서는 롤백이 지원되지 않습니다.
- 롤백은 FMC에서 설정할 수 있는 구성에만 영향을 미칩니다. 예를 들어 롤백은 FTD CLI에서만 구성할 수 있는 전용 관리 인터페이스와 관련된 로컬 구성에 영향을 주지 않습니다. **configure network management-data-interface** 명령을 사용하여 마지막 FMC 구축 후 데이터 인터페이스 설정을 변경한 다음 롤백 명령을 사용하면 해당 설정이 유지되지 않습니다. 마지막으로 구축된 FMC 설정으로 롤백됩니다.
- UCAPL/CC 모드는 롤백할 수 없습니다.
- 이전 구축 중에 업데이트된 OOB(Out of Band) SCEP 인증서 데이터는 롤백할 수 없습니다.
- 롤백 중에는 현재 구성이 지워지므로 연결이 삭제됩니다.



시작하기 전에  
 모델 지원—FTD  
 프로시저

단계 1 FTD CLI에서 이전 구성으로 롤백합니다.

#### configure policy rollback

롤백 후 FTD는 롤백이 성공적으로 완료되었음을 FMC에 알립니다. FMC에서 구축 화면에는 구성이 롤백되었음을 알리는 배너가 표시됩니다.

롤백에 실패한 경우, 일반적인 구축 문제에 대한 <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html>의 내용을 참조하십시오. 경우에 따라 FMC 관리 액세스가 복원된 후 롤백이 실패할 수 있습니다. 이 경우 FMC 구성 문제를 해결하고 FMC에서 다시 구축할 수 있습니다.

예제:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....
.....
>
```

단계 2 관리 연결이 재설정되었는지 확인합니다.

FMC의 **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Device**(디바이스) > **Management**(관리) > **FMC Access Details**(FMC 액세스 디테일) > **Connection Status**(연결 상태) 페이지에서 관리 연결 상태를 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 **stunnel-status-brief** 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. [데이터 인터페이스에서 관리 연결성 문제 해결, 41 페이지](#)의 내용을 참조하십시오.

## 데이터 인터페이스에서 관리 연결성 문제 해결

모델 지원—FTD

전용 관리 인터페이스를 사용하는 대신 FMC 관리용 데이터 인터페이스를 사용하는 경우, FMC에서 FTD에 대한 인터페이스 및 네트워크 설정을 변경할 때 연결이 중단되지 않도록 주의해야 합니다.

FMC에 FTD를 추가한 후 관리 인터페이스 유형을 데이터에서 관리로 또는 관리에서 데이터로 변경하는 경우, 인터페이스 및 네트워크 설정이 올바르게 설정되지 않으면 관리 연결이 끊어질 수 있습니다.

이 주제는 관리 연결 끊김 문제를 해결하는 데 도움이 됩니다.

### 관리 연결 상태 보기

FMC의 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > FMC Access Details(FMC 액세스 디테일) > Connection Status(연결 상태)** 페이지에서 관리 연결 상태를 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다. **sftunnel-status** 명령을 사용하여 전체 정보를 볼 수도 있습니다.

작동 중지된 연결에 대해서는 다음 샘플 출력을 참조하십시오. 다음과 같은 피어 채널이나 하트비트 정보가 "연결"되지 않았습니다.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

### FTD 네트워크 정보 보기

FTD CLI에서 관리 및 FMC 액세스 데이터 인터페이스 네트워크 설정을 확인합니다.

#### show network

```
> show network
===== [ System Information ] =====
Hostname                : 5516X-4
DNS Servers             : 208.67.220.220,208.67.222.222
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ br1 ] =====
State                   : Enabled
```

```

Link                               : Up
Channels                           : Management & Events
Mode                               : Non-Autonegotiation
MDI/MDIX                           : Auto/MDIX
MTU                                 : 1500
MAC Address                         : 28:6F:7F:D3:CB:8D
-----[ IPv4 ]-----
Configuration                       : Manual
Address                             : 10.99.10.4
Netmask                             : 255.255.255.0
Gateway                             : 10.99.10.1
-----[ IPv6 ]-----
Configuration                       : Disabled

=====[ Proxy Information ]=====
State                               : Disabled
Authentication                       : Disabled

=====[ System Information - Data Interfaces ]=====
DNS Servers                         :
Interfaces                           : GigabitEthernet1/1

=====[ GigabitEthernet1/1 ]=====
State                               : Enabled
Link                                 : Up
Name                                 : outside
MTU                                 : 1500
MAC Address                         : 28:6F:7F:D3:CB:8F
-----[ IPv4 ]-----
Configuration                       : Manual
Address                             : 10.89.5.29
Netmask                             : 255.255.255.192
Gateway                             : 10.89.5.1
-----[ IPv6 ]-----
Configuration                       : Disabled

```

**FTD가 FMC에 등록되었는지 확인합니다.**

FTD CLI에서 FMC 등록이 완료되었는지 확인합니다. 이 명령은 관리 연결의 현재 상태를 표시하지 않습니다.

### show managers

```

> show managers
Type                               : Manager
Host                               : 10.89.5.35
Registration                       : Completed
>

```

### FMC ping

FTD CLI에서 다음 명령을 사용하여 데이터 인터페이스에서 FMC를 ping합니다.

#### ping fmc\_ip

FTD CLI에서 다음 명령을 사용하여 관리 인터페이스에서 FMC를 ping합니다. 이 인터페이스는 백플레인을 통해 데이터 인터페이스로 라우팅되어야 합니다.

#### ping system fmc\_ip

**FTD 내부 인터페이스에서 패킷 캡처**

FTD CLI에서 내부 백플레인 인터페이스(nlp\_int\_tap)의 패킷을 캡처하여 관리 패킷이 전송되는 지 확인합니다.

```
capture name interface nlp_int_tap trace detail match ip any any
```

```
show capture name trace detail
```

내부 인터페이스 상태, 통계 및 패킷 수 확인

FTD CLI에서 내부 백플레인 인터페이스, nlp\_int\_tap에 대한 정보를 참조하십시오.

```
show inttrace detail
```

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_ytun rev00, BW Unknown Speed-Capability, DLY 1000 usec
  (Full-duplex), (1000 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0000.0100.0001, MTU 1500
  IP address 169.254.1.1, subnet mask 255.255.255.248
  37 packets input, 2822 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  5 packets output, 370 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (0/0)
  output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
  37 packets input, 2304 bytes
  5 packets output, 300 bytes
  37 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active
```

**라우팅 및 NAT 확인**

FTD CLI에서 기본 경로(S \*)가 추가되었고 관리 인터페이스(nlp\_int\_tap)에 대한 내부 NAT 규칙이 있는지 확인합니다.

```
show route
```

```
> show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C      10.89.5.0 255.255.255.192 is directly connected, outside
L      10.89.5.29 255.255.255.255 is directly connected, outside

>

```

### show nat

```

> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface service
  tcp 8305 8305
  translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh ssh
  translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
  ipv6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0

>

```

### 다른 설정 확인

다른 모든 설정이 있는지 확인하려면 다음 명령을 참조하십시오. FMC의 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > FMC Access Details(FMC 액세스 세부 사항) > CLI Output(CLI 출력)** 페이지에서 이러한 명령을 많이 볼 수 있습니다.

### show running-config sftunnel

```

> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305

```

### show running-config ip-client

```

> show running-config ip-client
ip-client outside

```

### show conn address fmc\_ip

```

> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
  preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

```

```
TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
bytes 1630834, flags UIO
>
```

### 성공적인 DDNS 업데이트 확인

FTD CLI에서 DDNS 업데이트에 성공했는지 확인합니다.

#### debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

업데이트가 실패하면 **debug http** 및 **debug ssl** 명령을 사용합니다. 인증서 검증에 실패한 경우, 다음을 통해 루트 인증서가 디바이스에 설치되어 있는지 확인합니다.

#### show crypto ca certificates trustpoint\_name

DDNS 작업을 확인하려면 다음 명령을 사용하십시오.

#### show ddns update interface fmc\_access\_ifc\_name

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

### FMC 로그 파일 확인

<https://cisco.com/go/fmc-reg-error>를 참조하십시오.

## 일반 설정 편집

### 프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)을(를) 선택합니다.

단계 2 수정할 디바이스 옆의 수정(✍)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 **Device**(디바이스)를 클릭합니다.

단계 4 일반 섹션에서 수정(✎)을 클릭합니다.

단계 5 매니지드 디바이스의 이름을 입력합니다.

팁 스택킹된 디바이스의 경우 어플라이언스 편집기의 스택 페이지에서 스택에 할당된 디바이스 이름을 편집합니다. 어플라이언스 편집기의 디바이스 페이지에서 개별 디바이스에 할당된 디바이스 이름을 편집할 수 있습니다.

단계 6 **Transfer Packets**(패킷 전송) 설정을 변경합니다.

- 체크 박스를 선택하여 패킷 데이터가 이벤트와 함께 Firepower Management Center에 저장되도록 합니다.
- 관리되는 디바이스가 이벤트로 패킷 데이터를 전송하는 것을 방지하려면 체크 박스를 비워둡니다.

단계 7 디바이스에 현재 정책 및 디바이스 설정의 구축을 강제로 구축하려면 **Force Deploy**(강제 구축)을 클릭합니다.

참고 강제 구축은 FTD에 구축할 정책 규칙의 완전한 생성을 포함하므로 일반 구축보다 더 많은 시간을 소비합니다.

단계 8 **Deploy**(구축)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

## 다른 디바이스에 구성 복사

새로운 디바이스가 네트워크에 구축되면 새 디바이스를 수동으로 다시 구성하는 대신 사전 구성된 디바이스에서 설정 및 정책을 쉽게 복사할 수 있습니다.

시작하기 전에

다음을 확인합니다.


- 소스 및 대상 Firepower Threat Defense 디바이스가 동일한 모델이며 동일한 버전의 Firepower 소프트웨어가 실행 중입니다.
- 소스는 독립형 Firepower Threat Defense 디바이스 또는 Firepower Threat Defense 고가용성 쌍입니다.
- 대상 디바이스는 독립형 Firepower Threat Defense 디바이스입니다.
- 소스 및 대상 Firepower Threat Defense 디바이스에는 동일한 수의 물리적 인터페이스가 있습니다.
- 소스 및 대상 Firepower Threat Defense 디바이스는 동일한 방화벽 모드(라우팅됨 또는 투명)를 사용합니다.

- 소스 및 대상 Firepower Threat Defense 디바이스는 동일한 보안 인증 규정 준수 모드 상태에 있습니다.
- 소스 및 대상 Firepower Threat Defense 디바이스가 동일한 도메인에 있습니다.
- 소스 및 대상 Firepower Threat Defense 디바이스에서 구성 구축이 진행되고 있지 않습니다.

모델 지원—FTD

프로시저



단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 수정할 디바이스 옆의 수정()를 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 **Device**(디바이스)를 클릭합니다.

단계 4 일반 섹션에서 다음 중 하나를 수행합니다.

- 디바이스 컨피그레이션 가져오기()를 클릭하여 다른 디바이스에서 새 디바이스로 디바이스 설정을 복사합니다. 디바이스 설정 가져오기 페이지의 디바이스 선택 드롭다운 목록에서 소스 디바이스를 선택합니다.
- 디바이스 컨피그레이션 푸시()를 클릭하여 현재 디바이스에서 새 디바이스로 디바이스 설정을 복사합니다. 디바이스 설정 푸시 페이지의 대상 디바이스 드롭다운 목록에서 설정을 복사할 대상을 선택합니다.

단계 5 (선택 사항) 정책을 복사하려면 **Include shared policies configuration**(공유 정책 구성 포함) 확인란을 선택합니다.

AC 정책, NAT, 플랫폼 설정 및 FlexConfig 정책 같은 공유 정책은 여러 디바이스에 공유할 수 있습니다.

단계 6 **OK**(확인)를 클릭합니다.

메시지 센터의 작업에서 디바이스 설정 작업 복사 상태를 모니터링할 수 있습니다.

디바이스 설정 복사 작업이 시작되면 대상 디바이스의 설정을 삭제하고 소스 디바이스의 설정을 대상 장치에 복사합니다.



**경고!** 디바이스 설정 복사 작업을 완료하면 대상 디바이스를 원래 설정으로 되돌릴 수 없습니다.



## 라이선스 설정 편집

Firepower Management Center에 사용 가능한 라이선스가 있으면 디바이스에서 라이선스를 활성화할 수 있습니다.

프로시저

**단계 1** **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

**단계 2** 라이선스를 활성화 또는 비활성화하려는 디바이스 옆에 있는 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

**단계 3** **Device**(디바이스)를 클릭합니다.

팁 스택킹된 디바이스의 경우 어플라이언스 편집기의 스택 페이지에서 스택에 대한 라이선스를 활성화 또는 비활성화합니다.

**단계 4** 라이선스 섹션 옆에 있는 수정(✎)을 클릭합니다.

**단계 5** 관리되는 디바이스에서 활성화 또는 비활성화 하려는 라이선스 옆의 체크 박스를 선택하거나 선택 취소합니다.

**단계 6** **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

## 고급 설정 편집

다음 주제에서는 고급 디바이스 설정을 편집하는 방법에 대해 설명합니다.



참고 패킷 전송 설정에 대한 자세한 내용은 [일반 설정 편집, 46 페이지](#)를 참고하십시오.

## AAB(Automatic Application Bypass) 구성

AAB(Automatic Application Bypass)를 사용하면 Snort가 다운된 경우 또는 클래식 디바이스의 경우 패킷 처리에 시간이 너무 오래 걸리는 경우 패킷이 탐지를 우회할 수 있습니다. AAB는 장애 발생 후 10분 이내에 Snort를 재시작하고, Snort 장애의 원인을 조사하기 위해 분석할 수 있는 문제 해결 데이터를 생성합니다.



주의 AAB 활성화는 Snort 프로세스를 일부 재시작하여 일부 패킷의 검사를 일시적으로 중단합니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 [Snort® 재시작 트래픽 동작](#)을 참고하십시오.

다음 동작을 참조하십시오.

**FTD 동작:** Snort가 중단된 경우 지정된 타이머 기간 후에 AAB가 트리거됩니다. Snort가 작동하면 패킷 처리가 설정된 타이머를 초과하더라도 AAB가 트리거되지 않습니다.

**기본 디바이스 동작:** AAB는 인터페이스를 통해 패킷을 처리하는 데 허용되는 시간을 제한합니다. 패킷 처리 지연을 패킷 대기 시간을 위한 네트워크의 허용 오차와 균형을 맞춥니다.

이 기능은 모든 배포에서 기능하지만, 인라인 배포에서 특히 유용합니다.

일반적으로 레이턴시 임계값이 초과된 후 빠른 경로 패킷에 대한 침입 정책에서 **Rule Latency Thresholding**을 사용합니다. 규칙 레이턴시 임계값은 엔진을 종료하거나 문제 해결 데이터를 생성하지 않습니다.

탐지가 우회되면 디바이스는 상태 모니터링 알림을 생성합니다.

기본적으로 AAB는 비활성화되어 있습니다. AAB를 활성화하려면 단계 설명을 따릅니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 고급 디바이스 설정을 수정할 디바이스 옆에 있는 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 **Device**(디바이스)(또는 스택킹된 디바이스의 경우 **Stack**(스택))을 클릭하고, **Advanced Settings**(고급 설정) 섹션에서 수정(✎)을 클릭합니다.

단계 4 **AAB(Automatic Application Bypass)**를 선택합니다.

단계 5 250~60000밀리초 사이의 우회 임계값을 입력합니다. 기본 설정은 3000밀리초(ms)입니다.

단계 6 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [권피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

## 로컬 라우터 트래픽 검사

로컬에서 바인딩된 트래픽이 레이어 3 구축의 모니터링 규칙과 일치하면 해당 트래픽은 검사를 우회할 수 있습니다. 트래픽의 검사를 위해 로컬 라우터 트래픽 검사를 활성화합니다.

시작하기 전에

모델 지원—7000 및 8000 Series

프로시저

**단계 1** **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

**단계 2** 고급 디바이스 설정을 수정할 디바이스 옆에 있는 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

**단계 3** **Device**(디바이스)를 클릭(또는 스택된 디바이스의 경우 **Stack**(스택))한 다음 **Advanced Settings**(고급 설정) 섹션에서 수정(✎)을 클릭합니다.

**단계 4** 7000 또는 8000 Series 디바이스가 라우터로 구축된 경우 예외 트래픽을 검사하려면 로컬 라우터 트래픽 검사를 선택합니다.

**단계 5** **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

## 빠른 경로 규칙(8000 Series) 설정

초기 트래픽 처리의 형태로 8000 Series 빠른 경로 규칙은 추가 검사나 로그인 없이 8000 Series 디바이스로 트래픽을 직접 보낼 수 있습니다. (수동 배포에서 8000 Series 빠른 경로 규칙은 단순히 분석을 중지합니다.) 각 8000 Series 빠른 경로 규칙은 특정 보안 영역 또는 인라인 인터페이스 세트에 적용됩니다. 8000 Series 빠른 경로 규칙은 하드웨어 레벨에서 기능하기 때문에 간단한 외부 헤더 기준을 따르기만 하면 빠른 경로 규칙을 사용할 수 있습니다.

- 이니시에이터 또는 응답자 IP 주소 또는 주소 블록
- TCP와 UDP에 대한 프로토콜, 이니시에이터 및 응답자 포트
- VLAN ID

기본적으로 8000 Series 빠른 경로 규칙은 특정 이니시에이터부터 특정 응답자의 연결에 영향을 줍니다. 호스트가 이니시에이터이거나 응답자인 것과 관계없이 규칙의 조건을 충족하는 모든 연결에 대한 빠른 경로를 만들기 위해 규칙을 양방향으로 만들 수 있습니다.



참고 TCP 또는 UDP 트래픽에 모든 이외의 포트를 지정하면 프래그먼트 트래픽에 일치하는 첫 프래그먼트만 빠른 경로로 지정됩니다. 다른 모든 프래그먼트는 추가 검사를 위해 전달됩니다. 8000 Series은 각 프래그먼트의 IP 헤더가 빠른 경로 규칙을 일치시키는 데 필요한 모든 IP 헤더 정보를 포함하고 하위 프래그먼트가 포트를 식별하는 필드를 포함하지 않았을 때에만 프래그먼트 트래픽을 빠른 경로로 지정하기 때문입니다.

시작하기 전에

모델 지원—8000 Series

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 규칙을 설정하려는 8000 Series 디바이스 옆의 수정(✎)을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 3 **Device**(디바이스)를 클릭(또는 스택된 디바이스의 경우 **Stack**(스택))한 다음 **Advanced Settings**(고급 설정) 섹션에서 수정(✎)을 클릭합니다.

단계 4 새 **IPv4** 규칙 또는 새 **IPv6** 규칙을 클릭합니다.

단계 5 도메인 드롭다운 목록에서 인라인 집합 또는 패시브 보안 영역을 선택합니다.

단계 6 빠른 경로로 지정하고 싶은 트래픽을 설정합니다. 트래픽은 빠른 경로로 지정되기 위한 모든 조건을 충족해야 합니다.

- 이니시에이터 및 응답자(필수): 이니시에이터 및 응답자의 IP 주소 또는 주소 블록을 입력합니다.
- 프로토콜: 프로토콜을 선택하거나 **All**(전체)을 클릭합니다.
- 이니시에이터 포트 및 응답자 포트: TCP 및 UDP 트래픽의 경우 이니시에이터 및 응답자 포트를 입력합니다. 필드를 공백으로 두거나 모두를 입력하여 모든 TCP 또는 UDP 트래픽을 일치시킵니다. 쉼표로 구분된 포트 목록은 입력할 수 있지만 포트 범위는 입력할 수 없습니다.
- VLAN: VLAN ID를 입력합니다. 필드를 공백으로 두거나 모두를 입력하여 VLAN 태그와 관계없이 모든 트래픽을 일치시킵니다.

단계 7 (선택 사항) 규칙을 양방향으로 설정합니다.

단계 8 저장을 클릭하여 다시 저장합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

## 개체 그룹 검색 구성

작동하는 동안 FTD 디바이스는 액세스 규칙에 사용되는 모든 네트워크 또는 인터페이스 개체의 컨테츠에 따라 액세스 컨트롤 규칙을 여러 액세스 컨트롤 목록 항목으로 확장합니다. 개체 그룹 검색을 활성화하여 액세스 컨트롤 규칙을 검색하는 데 필요한 메모리를 줄일 수 있습니다. 개체 그룹 검색을 사용하면 시스템이 네트워크 또는 인터페이스 개체로 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. 개체 그룹 검색은 액세스 규칙이 정의된 방식 또는 Firepower 디바이스 관리자에 표시되는 방식에 영향을 주지 않습니다. 이는 액세스 컨트롤 규칙과의 연결을 일치시키는 동안 디바이스가 이를 해석 및 처리하는 방법에만 영향을 미칩니다.

개체 그룹 검색을 활성화하면 네트워크 또는 인터페이스 개체를 포함하는 액세스 컨트롤 정책에 대한 메모리 요구 사항이 감소합니다. 그러나 개체 그룹 검색은 또한 규칙 조회 성능을 저하시켜 CPU 사용률이 증가한다는 점에 유의해야 합니다. 특정 액세스 컨트롤 정책에 대한 감소된 메모리 요구 사항에 대한 CPU 영향의 균형을 유지해야 합니다. 대부분의 경우, 개체 그룹 검색을 활성화하면 네트워크 운영이 개선됩니다.

개체 그룹 검색은 기본적으로 비활성화되어 있습니다. 한 번에 하나의 디바이스에서 활성화할 수 있으며 전역적으로 활성화할 수 없습니다. 네트워크 또는 인터페이스 개체를 사용하는 액세스 규칙을 구축하는 모든 디바이스에서 이 기능을 활성화하는 것이 좋습니다.



참고

개체 그룹 검색을 활성화한 다음 잠시 동안 디바이스를 구성하고 작동할 경우 나중에 기능을 비활성화하면 원하지 않는 결과가 발생할 수 있습니다. 개체 그룹 검색을 비활성화할 경우 디바이스의 실행 중인 구성에서 기존 액세스 제어 규칙이 확장됩니다. 확장에 디바이스에서 사용할 수 있는 것보다 많은 메모리가 필요할 경우 디바이스는 일관적이지 않은 상태로 남아있을 수 있으며 성능에 영향을 미칠 수 있습니다. 디바이스가 정상적으로 작동 중인 경우 활성화한 개체 그룹 검색을 비활성화해서는 안 됩니다.

시작하기 전에

- 모델 지원—FTD
- 각 디바이스에서 트랜잭션 커밋도 활성화하는 것이 좋습니다. 디바이스 CLI에서 **asp rule-engine transactional-commit access-group** 명령을 입력합니다.
- 이 설정을 변경하면 디바이스가 ACL을 다시 컴파일하는 동안 시스템 작동이 중단될 수 있습니다. 유지 보수 기간 중에 이 설정을 변경하는 것이 좋습니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 규칙을 설정하려는 FTD 디바이스 옆의 수정(✎)을 클릭합니다.

단계 3 **Device**(디바이스) 탭을 클릭한 다음 **Advanced Settings**(고급 설정) 섹션에서 수정(✎)을 클릭합니다.

단계 4 개체 그룹 검색을 선택합니다.

단계 5 네트워크 개체 외에 인터페이스 개체에서도 개체 그룹 검색을 수행하려면 **Interface Object Optimization**(인터페이스 개체 최적화)을 선택합니다.

**Interface Object Optimization**(인터페이스 개체 최적화)을 선택하지 않으면 시스템은 각 소스/인터페이스 쌍에 대해 별도의 규칙을 구축합니다. 규칙에 사용되는 보안 영역 및 인터페이스 그룹을 사용합니다. 이는 인터페이스 그룹을 개체 그룹 검색 처리에 사용할 수 없음을 의미합니다.

단계 6 **Save**(저장)를 클릭합니다.

## 인터페이스 개체 최적화 구성

구축 중 액세스 제어 및 사전 필터 정책에서 사용하는 인터페이스 그룹 및 보안 영역은 각 소스/대상 인터페이스 쌍에 대해 별도의 규칙을 생성합니다. 인터페이스 개체 최적화를 활성화하면 시스템은 대신 액세스 제어/사전 필터 규칙에 따라 단일 규칙을 구축하여 디바이스 설정을 간소화하고 구축 성능을 개선할 수 있습니다. 이 옵션을 선택하는 경우, **Object Group Search**(개체 그룹 검색) 옵션도 선택하여 디바이스의 메모리 사용량을 줄일 수 있습니다.

인터페이스 개체 최적화는 기본적으로 비활성화되어 있습니다. 한 번에 하나의 디바이스에서 활성화할 수 있으며, 전역적으로 활성화할 수 없습니다.



참고 인터페이스 개체 최적화를 비활성화하면 인터페이스 개체를 사용하지 않고 기존 액세스 제어 규칙이 구축되므로 구축 시간이 더 오래 걸릴 수 있습니다. 또한 개체 그룹 검색을 활성화하면 인터페이스 개체에 이점이 적용되지 않으며, 디바이스의 실행 중인 설정에서 액세스 제어 규칙이 확장되어 표시될 수 있습니다. 확장에 디바이스에서 사용할 수 있는 것보다 많은 메모리가 필요할 경우 디바이스는 일관적이지 않은 상태로 남아있을 수 있으며 성능에 영향을 미칠 수 있습니다.

시작하기 전에

모델 지원—FTD

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 규칙을 설정하려는 FTD 디바이스 옆의 수정(✎)을 클릭합니다.

단계 3 **Device**(디바이스) 탭을 클릭한 다음 **Advanced Settings**(고급 설정) 섹션에서 수정(✎)을 클릭합니다.

단계 4 **Interface Object Optimization**(인터페이스 개체 최적화)을 확인합니다.

단계 5 **Save**(저장)를 클릭합니다.

## 디바이스의 관리자 변경

다음과 같은 상황에서는 디바이스에서 관리자를 변경해야 할 수 있습니다.

- 디바이스에서 **FMC IP 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다.**, [55 페이지](#) - FMC IP 주소 또는 호스트네임을 변경하는 경우, 디바이스의 새 IP 주소 또는 호스트네임과 일치하는 것이 좋습니다.
- **새 FMC 식별, 56 페이지**- 이전 FMC에서 디바이스가 있다면 이를 삭제한 후 새 FMC에 대해 디바이스를 구성한 다음 FMC에 추가할 수 있습니다.
- **Firepower Device Manager에서 FMC로 전환, 57 페이지**- 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FDM에서 FMC로 변경할 경우, FTD 설정이 지워지며 처음부터 다시 시작해야 합니다.
- **FMC에서 Firepower Device Manager로 전환, 58 페이지**- 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FMC에서 FDM으로 변경할 경우, FTD 설정이 지워지며 처음부터 다시 시작해야 합니다.

## 디바이스에서 **FMC IP** 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다.

FMC IP 주소 또는 호스트네임을 변경하는 경우, 설정이 일치하도록 디바이스 CLI의 값도 변경해야 합니다. 대부분 디바이스에서 FMC IP 주소 또는 호스트네임을 변경하지 않고 관리 연결이 다시 설정되지만, 적어도 FMC에 디바이스를 추가하고 NAT ID만 지정한 경우 연결을 다시 설정하려면 이 작업을 수행해야 합니다. 다른 경우에도 네트워크의 복원력을 높이려면 FMC IP 주소 또는 호스트네임을 최신 상태로 유지하는 것이 좋습니다.

시작하기 전에

모델 지원—FTD

프로시저

**단계 1** FMC CLI에서 FTD 명령에 지정할 수 있도록 FMC의 고유한 UUID를 확인합니다. FMC CLI에 대한 자세한 내용은 [Firepower Management Center 명령줄 참조](#)의 내용을 참조하십시오.

**show version**

FMC UUID는 FMC를 명확하게 식별합니다. 예를 들어 FMC 고가용성의 경우 FTD에서 활성 FMC를 지정해야 합니다.

예제:

```
> show version
-----[ firepower ]-----
```

```

Model                : Cisco Firepower Management Center for VMWare (66) Version 6.7.0
                    (Build 1222)
UUID                 : f2a06484-9f7f-11ea-b9f4-541a108ebbb5
Rules update version : 2020-05-26-001-vrt
VDB version          : 334
-----

```

단계 2 FTD CLI에서 FMC IP 주소 또는 호스트네임을 수정합니다.

```
configure manager edit fmc_uuid {ip_address | hostname}
```

FMC가 원래 **DONTRESOLVE** 및 NAT ID로 식별된 경우 이 명령을 사용하여 값을 호스트네임 또는 IP 주소로 변경할 수 있습니다. IP 주소 또는 호스트네임은 **DONTRESOLVE**으로 변경할 수 없습니다.

관리 연결이 중단된 다음 다시 설정됩니다. **sftunnel-status** 명령을 사용하여 연결 상태를 모니터링할 수 있습니다.

예제:

```
> configure manager edit f2a06484-9f7f-11ea-b9f4-541a108ebbb5 10.10.5.1
```

## 새 FMC 식별

이 절차에서는 매니지드 디바이스의 새 FMC를 식별하는 방법을 보여줍니다. 새 FMC에서 이전 FMC의 IP 주소를 사용하는 경우에도 이러한 단계를 수행해야 합니다.

프로시저

단계 1 기존 FMC에서 매니지드 디바이스를 삭제합니다. [FMC에서 디바이스 삭제, 19 페이지](#)를 참조하십시오.

FMC와의 활성 연결이 있는 경우 FMC IP 주소를 변경할 수 없습니다.

단계 2 예를 들어 SSH를 사용하여 디바이스 CLI에 연결합니다.

단계 3 새 FMC를 구성합니다.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE } regkey [nat_id]
```

- **{hostname | IPv4\_address | IPv6\_address}** - FMC 호스트 이름, IPv4 주소 또는 IPv6 주소를 설정합니다
- **DONTRESOLVE** - FMC에서 주소를 직접 지정할 수 없는 경우, 호스트 이름 또는 IP 주소 대신 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 **nat\_id**가 필요합니다. 이 디바이스를 FMC에 추가할 때는 디바이스 IP 주소와 **nat\_id**를 모두 지정해야 합니다. 연결의 한쪽에서 IP 주소를 지정해야 하며, 양쪽에서 동일한 고유 NAT ID를 지정해야 합니다.
- **regkey**—등록 시 FMC와 디바이스 간에 공유할 등록 키를 입력합니다. 이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.



- `nat_id` - FMC와 디바이스에서 IP 주소를 지정하지 않은 경우, 둘 사이의 등록 프로세스 동안에만 사용되는 1~37자의 영문숫자 문자열로 구성됩니다. 이 NAT ID는 등록 시에만 사용되는 일회용 비밀번호입니다. NAT ID가 고유하고 등록 대기 중인 다른 디바이스에서 사용되지 않는지 확인하십시오. FTD를 추가할 때 FMC에 동일한 NAT ID를 지정합니다.

예제:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

단계 4 FMC에 디바이스를 추가합니다. [FMC에 디바이스 추가, 15 페이지](#)의 내용을 참조하십시오.

## Firepower Device Manager에서 FMC로 전환

이 절차에서는 관리자를 FDM(Firepower Device Manager)에서 로컬 디바이스 관리자인 FMC로 변경하는 방법을 설명합니다. 소프트웨어를 다시 설치하지 않고도 FDM과 FMC 간에 전환할 수 있습니다. 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FDM에서 FMC로 변경할 경우, FTD 설정이 지워지며 처음부터 다시 시작해야 합니다.



주의 관리자를 변경하면 FTD 컨피그레이션이 공장 기본값으로 재설정됩니다. 그러나 관리 부트스트랩 컨피그레이션은 유지됩니다.

시작하기 전에

모델 지원—FTD

프로시저

단계 1 FDM에서 고가용성을 위해 고가용성 구성을 해제합니다. 액티브 유닛에서 HA를 해제하는 것이 가장 좋습니다.

단계 2 FDM에서 스마트 라이선스 서버에서 디바이스를 등록 해제합니다.

단계 3 예를 들어 SSH를 사용하여 디바이스 CLI에 연결합니다.

단계 4 현재 관리 설정을 제거합니다.

### configure manager delete

주의 로컬 관리자를 삭제하면 FTD 컨피그레이션이 공장 기본값으로 재설정됩니다. 그러나 관리 부트스트랩 컨피그레이션은 유지됩니다.

예제:

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

단계 5 새 FMC를 구성합니다.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE } regkey [nat_id]
```

- {hostname | IPv4\_address | IPv6\_address}—FMC 호스트 이름, IPv4 주소 또는 IPv6 주소를 설정합니다
- **DONTRESOLVE**—FMC에서 주소를 직접 지정할 수 없는 경우 호스트 이름 또는 IP 주소 대신 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 nat\_id가 필요합니다. 이 디바이스를 FMC에 추가할 때는 디바이스 IP 주소와 nat\_id를 모두 지정해야 합니다. 연결의 한쪽에서 IP 주소를 지정해야 하며, 양쪽에서 동일한 고유 NAT ID를 지정해야 합니다.
- regkey—등록 시 FMC와 디바이스 간에 공유할 등록 키를 입력합니다. 이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.
- nat\_id - FMC와 디바이스에서 IP 주소를 지정하지 않은 경우, 둘 사이의 등록 프로세스 동안에만 사용되는 1~37자의 영문숫자 문자열로 구성됩니다. 이 NAT ID는 등록 시에만 사용되는 일회용 비밀번호입니다. NAT ID가 고유하고 등록 대기 중인 다른 디바이스에서 사용되지 않는지 확인하십시오. FTD를 추가할 때 FMC에 동일한 NAT ID를 지정합니다.

예제:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

단계 6 FMC에 디바이스를 추가합니다. [FMC에 디바이스 추가, 15 페이지](#) 섹션을 참조하십시오.

## FMC에서 Firepower Device Manager로 전환

이 절차에서는 관리자를 FMC에서 로컬 디바이스 관리자인 FDM(Firepower Device Manager)으로 변경하는 방법을 설명합니다. 소프트웨어를 다시 설치하지 않고도 FDM과 FMC 간에 전환할 수 있습니다. 동일한 디바이스에 대해 FDM과 FMC를 동시에 사용할 수는 없습니다. FMC에서 FDM으로 변경할 경우, FTD 컨피그레이션이 지워지며 처음부터 다시 시작해야 합니다.



주의 관리자를 변경하면 FTD 구성이 공장 기본값으로 재설정됩니다. 그러나 관리 부트스트랩 구성은 유지됩니다.

시작하기 전에

모델 지원—FTD

프로시저

단계 1 FMC에서 고가용성을 위해 고가용성 구성을 해제합니다. 액티브 유닛에서 HA를 해제하는 것이 가장 좋습니다. [고가용성 쌍의 유닛 분리](#) 섹션을 참조하십시오.

단계 2 FMC에서 매니지드 디바이스를 삭제합니다. [FMC에서 디바이스 삭제](#), 19 페이지를 참조하십시오.

FMC와의 활성 연결이 있는 경우 관리자를 변경할 수 없습니다.

단계 3 예를 들어 SSH를 사용하여 디바이스 CLI에 연결합니다.

단계 4 현재 관리 설정을 제거합니다.

#### **configure manager delete**

주의 로컬 관리자를 삭제하면 FTD 구성이 공장 기본값으로 재설정됩니다. 그러나 관리 부트스트랩 컨피그레이션은 유지됩니다.

예제:

```
> configure manager delete
```

```
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes
```

```
DHCP Server Disabled
>
```

단계 5 새 FMC를 구성합니다.

**configure manager add** {hostname | IPv4\_address | IPv6\_address | **DONTRESOLVE** } regkey [nat\_id]

- {hostname | IPv4\_address | IPv6\_address}—FMC 호스트 이름, IPv4 주소 또는 IPv6 주소를 설정합니다
- **DONTRESOLVE**—FMC에서 주소를 직접 지정할 수 없는 경우 호스트 이름 또는 IP 주소 대신 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 nat\_id가 필요합니다. 이 디바이스를 FMC에 추가할 때는 디바이스 IP 주소와 nat\_id를 모두 지정해야 합니다. 연결의 한쪽에서 IP 주소를 지정해야 하며, 양쪽에서 동일한 고유 NAT ID를 지정해야 합니다.

- **regkey**—등록 시 FMC와 디바이스 간에 공유할 등록 키를 입력합니다. 이 키에 대해 1~37자의 텍스트 문자열을 선택할 수 있습니다. FTD를 추가하는 경우 FMC에 동일한 키를 입력합니다.
- **nat\_id** - FMC와 디바이스에서 IP 주소를 지정하지 않은 경우, 둘 사이의 등록 프로세스 동안에만 사용되는 1~37자의 영문숫자 문자열로 구성됩니다. 이 NAT ID는 등록 시에만 사용되는 일회용 비밀번호입니다. NAT ID가 고유하고 등록 대기 중인 다른 디바이스에서 사용되지 않는지 확인하십시오. FTD를 추가할 때 FMC에 동일한 NAT ID를 지정합니다.

예제:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

단계 6 FMC에 디바이스를 추가합니다. [FMC에 디바이스 추가, 15 페이지](#) 섹션을 참조하십시오.

## 디바이스 정보 보기

다중 도메인 구축에서 상위 도메인은 하위 도메인의 모든 디바이스에 대한 정보를 볼 수 있습니다. 디바이스를 편집하려면 리프 도메인에 있어야 합니다.

프로시저

단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

단계 2 확인할 디바이스 옆의 수정(✎)을 클릭합니다.

다중 도메인 구축 시 상위 도메인에 있는 경우, 보기(🔍)를 클릭하여 하위 도메인의 읽기 전용 모드에서 디바이스를 볼 수 있습니다.

단계 3 **Device**(디바이스)를 클릭합니다.

단계 4 다음 정보를 볼 수 있습니다.

- 일반 - 디바이스의 일반 설정을 표시합니다. [일반 정보, 61 페이지](#)의 내용을 참조하십시오.
- 라이선스 - 디바이스의 라이선스 정보를 표시합니다. [라이선스 정보, 62 페이지](#)의 내용을 참조하십시오.
- 시스템 - 디바이스에 대한 시스템 정보를 표시합니다. [시스템 정보, 62 페이지](#)의 내용을 참조하십시오.
- 상태 - 디바이스의 현재 상태에 대한 정보를 표시합니다. [상태 정보, 62 페이지](#)의 내용을 참조하십시오.
- 관리 - Firepower Management Center과 디바이스 간 통신 채널에 대한 정보를 표시합니다. [관리 정보, 63 페이지](#)를 참조하십시오.

- 고급 - 고급 기능 설정에 대한 정보를 표시합니다. [Advanced Settings\(고급 설정\)](#), 63 페이지을 참조합니다.

## 디바이스 관리 페이지 정보

Device Management(디바이스 관리) 페이지에서는 Firepower 디바이스를 관리하는 데 사용할 수 있는 다양한 정보와 옵션을 제공합니다.

이 페이지를 사용하여 디바이스를 추가, 편집, 제거 및 그룹화하고 상태를 비롯한 기본 디바이스 속성을 확인할 수 있습니다. 다양한 특성별로 디바이스를 추가로 필터링할 수 있습니다.

이 페이지에서는 클릭 한 번으로 다음에 액세스할 수 있는 기능을 제공합니다.

- 디바이스에 구축한 액세스 제어 정책
- 문제 해결 파일을 생성할 수 있는 각 디바이스의 상태 모니터링 페이지
- Firepower 4100/9300 시리즈 디바이스의 경우, Firepower Chassis Manager 웹 인터페이스로 연결되는 링크

## 일반 정보

디바이스 탭의 일반 섹션은 아래 표의 설정을 표시합니다.

표 2: 일반 섹션 표 필드

필드	설명
이름	Firepower Management Center에 표시되는 디바이스의 이름입니다.
패킷 전송	관리되는 디바이스가 Firepower Management Center에 이벤트 및 패킷 데이터를 전송할지 여부를 표시합니다.
모드	디바이스에 대한 관리 인터페이스 모드로 라우팅 또는 투명을 선택할 수 있습니다.  참고 모드 필드는 Firepower Threat Defense 디바이스에만 표시됩니다.
컴플라이언스 모드	디바이스에 대한 보안 인증서 컴플라이언스를 표시합니다. 유효한 값은 CC, UCAPL, None(없음)입니다.

## 라이선스 정보

디바이스 페이지의 라이선스 섹션은 장치에 대해 활성화된 라이선스를 표시합니다.

## 시스템 정보

디바이스 페이지의 시스템 섹션은 다음 표에 나타난 시스템 정보의 읽기 전용 표를 표시합니다.

표 3: 시스템 섹션 표 필드

필드	설명
모델	관리되는 디바이스의 모델 이름 및 번호입니다.
일련 번호	관리되는 디바이스의 새시의 일련 번호입니다.
시간	디바이스의 현재 시스템 시간입니다. 항상 UTC입니다. 아래의 시간 기반 규칙에 대한 표준 시간대 설정을 참조하십시오.
버전	매니지드 디바이스에 현재 설치된 소프트웨어 버전입니다.
시간 기반 규칙에 대한 표준 시간대 설정	디바이스 플랫폼 설정에 지정된 표준 시간대의 디바이스의 현재 시스템 시간입니다.
정책	관리되는 디바이스에 현재 구축된 플랫폼 설정 정책에 연결합니다.
인벤토리	연결된 디바이스에 대한 인벤토리 세부 정보를 연결합니다. 이 필드는 Firepower 2100 또는 Firepower 4100/9300 컨테이너 인스턴스 같은 일부 플랫폼에만 표시됩니다. 컨테이너 인스턴스에 대한 정보를 업데이트하려면 업데이트를 클릭합니다. 리소스 프로파일을 변경하면 고가용성 쌍의 불일치 문제를 방지하기 위해 인벤토리의 업데이트를 강제로 수행할 수 있습니다. 그렇지 않으면 정책 변경 사항을 구축할 때 이 정보가 업데이트됩니다.

디바이스를 종료하거나 다시 시작할 수 있습니다.

## 상태 정보

디바이스 페이지의 상태 섹션은 아래 표에서 설명한 정보를 표시합니다.

표 4: 상태 섹션 표 필드

필드	설명
상태	디바이스의 현재 상태를 나타내는 아이콘 아이콘을 클릭하면 어플라이언스에 대한 상태 모니터가 표시됩니다.
정책	디바이스에 현재 구축된 상태 정책에 대한 읽기 전용 링크입니다.
블랙리스트	상태 블랙리스트 모듈을 활성화하거나 비활성화할 수 있는 상태 블랙리스트 페이지의 링크입니다.

## 관리 정보

아래 테이블은 **Device**(디바이스) 페이지의 **Management**(관리) 섹션에 표시되는 필드를 표시합니다.

표 5: 관리 섹션 표 필드

필드	설명
호스트	디바이스의 IP 주소 또는 호스트네임입니다. 디바이스의 호스트네임 또는 IP 주소를 변경하려면 <a href="#">관리 설정 편집, 21 페이지</a> 의 내용을 참조하십시오.
상태	<b>Firepower Management Center</b> 과 매니지드 디바이스 간 채널 통신 상태를 나타내는 아이콘입니다. 커서를 상태 아이콘에 올려 놓으면 <b>Firepower Management Center</b> 이 디바이스와 연결한 마지막 시간을 볼 수 있습니다.
FMC 액세스 인터페이스	FMC 관리에 사용되는 인터페이스 유형(데이터 인터페이스 또는 관리 인터페이스)을 표시합니다. 인터페이스를 변경하려면 값을 클릭합니다. <a href="#">관리 설정 편집, 21 페이지</a> 의 내용을 참조하십시오.
FMC 액세스 세부 사항	<b>Configuration</b> (설정) 링크를 클릭하여 FMC의 데이터 인터페이스 설정 및 연결 상태를 디바이스의 값과 비교합니다. 자세한 내용은 <a href="#">데이터 인터페이스 관리를 위한 FMC 액세스 세부정보 보기, 27 페이지</a> 를 참고하십시오.

## Advanced Settings(고급 설정)

디바이스 페이지의 고급 설정 섹션은 고급 아래 표에 설명된 대로 고급 구성 설정을 표시합니다. 이러한 설정은 편집할 수 있습니다.

표 6: 고급 섹션 표 필드

필드	설명	지원되는 장치
애플리케이션 우회	디바이스에서 Automatic Application Bypass의 상태	7000 및 8000 Series
우회 임계값	밀리초로 나타낸 Automatic Application Bypass(자동 애플리케이션 우회) 임계값입니다.	NGIPSv ASA FirePOWER Firepower Threat Defense
로컬 라우터 트래픽 검사	디바이스가 라우터 인터페이스에서 수신된 ICMP, DHCP, OSFP 트래픽과 같이 스스로를 향하는 트래픽을 검사할지 여부입니다.	7000 및 8000 Series
빠른 경로(Fast-Path) 규칙	디바이스에서 생성된 8000 Series 빠른 경로 규칙의 수입니다.	8000 Series
개체 그룹 검색	디바이스에서 개체 그룹 검색의 상태입니다. 작동하는 동안 FTD 디바이스는 액세스 규칙에 사용되는 모든 네트워크 또는 인터페이스 개체의 콘텐츠에 따라 액세스 컨트롤 규칙을 여러 액세스 컨트롤 목록 항목으로 확장합니다. 개체 그룹 검색을 활성화하여 액세스 컨트롤 규칙을 검색하는 데 필요한 메모리를 줄일 수 있습니다. 개체 그룹 검색을 사용하면 시스템이 네트워크 또는 인터페이스 개체로 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. 개체 그룹 검색은 액세스 규칙이 정의된 방식 또는 Firepower 디바이스 관리자에 표시되는 방식에 영향을 주지 않습니다. 이는 액세스 컨트롤 규칙과의 연결을 일치시키는 동안 디바이스가 이를 해석 및 처리하는 방법에만 영향을 미칩니다.	Firepower Threat Defense
인터페이스 개체 최적화	디바이스에서 인터페이스 개체 최적화의 상태입니다. 구축 중 액세스 제어 및 사전 필터 정책에서 사용하는 인터페이스 그룹 및 보안 영역은 각 소스/대상 인터페이스 쌍에 대해 별도의 규칙을 생성합니다. 인터페이스 개체 최적화를 활성화하면 시스템은 대신 액세스 제어/사전 필터 규칙에 따라 단일 규칙을 구축하여 디바이스 설정을 간소화하고 구축 성능을 개선할 수 있습니다. 이 옵션을 선택하는 경우, <b>Object Group Search</b> (개체 그룹 검색) 옵션도 선택하여 디바이스의 메모리 사용량을 줄일 수 있습니다.	Firepower Threat Defense