



## 시스템 구성

---

다음 항목에서는 Firepower Management Center 및 매니지드 디바이스에 대한 시스템 구성 설정을 구성하는 방법에 대해 설명합니다.

- 시스템 컨피그레이션 요구 사항 및 전제 조건, 2 페이지
- 시스템 구성 관련 정보, 2 페이지
- 어플라이언스 정보, 5 페이지
- HTTPS 인증서, 6 페이지
- 외부 데이터베이스 액세스 설정, 11 페이지
- 데이터베이스 이벤트 제한 수, 12 페이지
- Management Interfaces(관리 인터페이스)관리 인터페이스, 15 페이지
- 종료 또는 재시작, 24 페이지
- 원격 스토리지 관리, 25 페이지
- 검증 변경, 29 페이지
- 정책 변경 코멘트, 30 페이지
- 액세스 목록, 31 페이지
- 감사 로그, 33 페이지
- 대시보드 설정, 34 페이지
- DNS 캐시, 35 페이지
- 이메일 공지, 36 페이지
- 언어 선택, 37 페이지
- 로그인 배너, 38 페이지
- SNMP 폴링, 38 페이지
- STIG 컴플라이언스, 40 페이지
- 시간 및 시간 동기화, 41 페이지
- 전역 사용자 구성, 47 페이지
- 세션 시간 초과, 50 페이지
- 취약성 매핑, 51 페이지
- 원격 콘솔 액세스 관리, 52 페이지
- VMware Tools 및 가상 시스템, 58 페이지
- 시스템 구성 기록, 59 페이지

## 시스템 컨피그레이션 요구 사항 및 전제 조건

모델 지원

FMC

일부 설정은 7000 및 8000 Series 디바이스에도 적용됩니다.

지원되는 도메인

글로벌

사용자 역할

관리자

## 시스템 구성 관련 정보

Firepower Management Center 또는 클래식 매니지드 디바이스(7000 및 8000 Series, ASA FirePOWER, NGIPSv)에 적용된 시스템 구성 설정입니다.

- Firepower Management Center의 경우 이 구성 설정은 '로컬' 시스템 구성에 포함되어 있습니다. Firepower Management Center의 시스템 구성은 단일 시스템에만 해당되며 FMC의 시스템 구성 변경은 해당 시스템에만 영향을 미칩니다.
- 클래식 관리 디바이스의 경우, Firepower Management Center의 이 구성을 플랫폼 설정 정책의 일부로 적용합니다. 공유 정책을 생성하여 매니지드 디바이스에 적합한 시스템 구성 설정의 하위 집합을 구성합니다. 이 하위 집합은 구축 전반에서 유사할 수 있습니다.



**팁** 7000 및 8000 Series 디바이스의 경우 콘솔 구성 및 원격 관리와 같은 로컬 웹 인터페이스에서 제한된 시스템 구성 작업을 수행할 수 있습니다. 이러한 구성은 플랫폼 설정 정책을 사용하는 7000 또는 8000 Series 디바이스에 적용되는 구성과 다릅니다.

## Firepower Management Center 시스템 구성 탐색

시스템 구성은 Firepower Management Center에 대한 기본적인 설정을 나타냅니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 탐색 패널을 사용하여 변경할 구성을 선택합니다. 자세한 내용은 [표 1: 시스템 구성 설정](#), 3 페이지 섹션을 참조하십시오.

## 시스템 구성 설정

매지니드 디바이스의 경우, 이러한 구성 대부분은 FMC에서 적용한 플랫폼 설정 정책으로 처리합니다. 자세한 내용은 [플랫폼 설정 정책](#)의 내용을 참조하십시오. 7000/8000 시리즈 디바이스의 경우, 비정책 기반 시스템 구성의 로컬 웹 인터페이스에 로그인할 수 있습니다. 자세한 내용은 [7000/8000 시리즈 디바이스에 대한 로컬 시스템 구성](#)의 내용을 참조하십시오.

표 1: 시스템 구성 설정

설정	설명
액세스 제어 환경 설정	액세스 제어 정책을 추가하거나 수정할 때 주석을 사용자에게 표시하도록 시스템을 구성합니다. <a href="#">정책 변경 코멘트</a> , 30 페이지 섹션을 참조하십시오.
액세스 목록	특정 포트에서 어떤 컴퓨터가 시스템에 액세스할 수 있는지 제어합니다. <a href="#">액세스 목록</a> , 31 페이지 섹션을 참조하십시오.
감사 로그	감사 로그를 외부 호스트로 보내도록 시스템을 구성합니다. <a href="#">감사 로그</a> , 33 페이지 섹션을 참조하십시오.
검증 변경	지난 24시간 동안 시스템 변경 사항에 대한 상세한 보고서를 보내도록 시스템을 구성합니다. <a href="#">검증 변경</a> , 29 페이지 섹션을 참조하십시오.
콘솔 구성	VGA 또는 시리얼 포트나 LOM(Lights-Out Management)을 통한 콘솔 액세스를 구성합니다. <a href="#">원격 콘솔 액세스 관리</a> , 52 페이지 섹션을 참조하십시오.
대시보드	대시보드에서 Custom Analysis 위젯을 활성화합니다. <a href="#">대시보드 설정</a> , 34 페이지 섹션을 참조하십시오.
데이터베이스	Firepower Management Center에서 저장할 수 있는 각 이벤트 유형의 최대 수를 지정합니다. <a href="#">데이터베이스 이벤트 제한 수</a> , 12 페이지 섹션을 참조하십시오.
DNS 캐시	이벤트 보기 페이지에서 자동으로 IP 주소를 확인하도록 시스템을 구성합니다. <a href="#">DNS 캐시</a> , 35 페이지 섹션을 참조하십시오.
이메일 알림	메일 호스트를 구성하고, 암호화 방법을 선택하고, 이메일 기반 알림 및 보고를 위한 인증 자격 증명을 제공합니다. <a href="#">이메일 공지</a> , 36 페이지 섹션을 참조하십시오.
External Database Access(외부 데이터베이스 액세스)	데이터베이스에 대한 외부 읽기 전용 액세스를 활성화하고, 다운로드할 클라이언트 드라이버를 제공합니다. <a href="#">외부 데이터베이스 액세스 설정</a> , 11 페이지 섹션을 참조하십시오.
HTTPS 인증서	필요하다면 신뢰된 권한 및 업로드 인증서에서 시스템에 HTTPS 서버 인증서를 요청합니다. <a href="#">HTTPS 인증서</a> , 6 페이지 섹션을 참조하십시오.

설정	설명
정보	어플라이언스에 대한 현재 정보를 보고 표시 이름을 편집합니다. <a href="#">어플라이언스 정보, 5 페이지</a> 섹션을 참조하십시오.
Intrusion Policy Preferences(침입 정책 환경 설정)	사용자가 침입 정책을 수정할 때 코멘트를 입력하라는 메시지를 표시하도록 시스템을 구성합니다. <a href="#">정책 변경 코멘트, 30 페이지</a> 섹션을 참조하십시오.
언어	웹 인터페이스에 대해 다른 언어를 지정합니다. <a href="#">언어 선택, 37 페이지</a> 섹션을 참조하십시오.
로그인 배너	사용자가 로그인 때 나타나는 사용자 정의 로그인 배너를 만듭니다. <a href="#">로그인 배너, 38 페이지</a> 섹션을 참조하십시오.
Management Interfaces(관리 인터페이스)	어플라이언스의 IP 주소, 호스트 이름 및 프록시 설정과 같은 옵션을 변경합니다. <a href="#">Management Interfaces(관리 인터페이스)관리 인터페이스, 15 페이지</a> 섹션을 참조하십시오.
네트워크 분석 정책 환경 설정	사용자가 네트워크 분석 정책을 수정할 때 코멘트를 입력하라는 메시지를 표시하도록 시스템을 구성합니다. <a href="#">정책 변경 코멘트, 30 페이지</a> 섹션을 참조하십시오.
프로세스	Firepower 프로세스를 종료, 리부팅 또는 다시 시작합니다. <a href="#">종료 또는 재시작, 24 페이지</a> 섹션을 참조하십시오.
원격 스토리지 디바이스	백업 및 보고서에 대한 원격 스토리지를 구성합니다. <a href="#">원격 스토리지 관리, 25 페이지</a> 섹션을 참조하십시오.
셀 시간 초과	비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유효 시간을 분 단위로 구성합니다. <a href="#">세션 시간 초과, 50 페이지</a> 섹션을 참조하십시오.
SNMP	SNMP(Simple Network Management Protocol) 폴링을 활성화합니다. <a href="#">SNMP 폴링, 38 페이지</a> 섹션을 참조하십시오.
STIG 컴플라이언스	미 국방부에서 정한 특정 요구 사항 준수 설정을 활성화합니다. <a href="#">STIG 컴플라이언스, 40 페이지</a> 섹션을 참조하십시오.
시간	현재 시간 설정을 확인하고 변경합니다. <a href="#">시간 및 시간 동기화, 41 페이지</a> 섹션을 참조하십시오.
시간 동기화	시스템에 대한 시간 동기화를 관리합니다. <a href="#">시간 및 시간 동기화, 41 페이지</a> 섹션을 참조하십시오.
사용자 구성	모든 사용자의 로그인 기록 및 비밀번호 기록을 성공적으로 추적하거나 유효하지 않은 로그인 자격 증명을 입력한 사용자에게 임시 잠금을 시행하도록 Firepower Management Center를 구성합니다. <a href="#">전역 사용자 구성, 47 페이지</a> 섹션을 참조하십시오.
VMware Tools	Firepower Management Center Virtual에서 VMware Tools를 활성화하고 사용합니다. <a href="#">VMware Tools 및 가상 시스템, 58 페이지</a> 섹션을 참조하십시오.
취약성 매핑	해당 주소에서 수신되거나 전송된 모든 애플리케이션 프로토콜 트래픽의 취약성을 호스트 IP 주소에 매핑합니다. <a href="#">취약성 매핑, 51 페이지</a> 섹션을 참조하십시오.

관련 항목

[클래식 디바이스에 대한 플랫폼 설정 관련 정보](#)

## 어플라이언스 정보

웹 인터페이스의 **System(시스템) > Configuration(구성)** 페이지에는 아래 표에 나열된 정보가 포함됩니다. 달리 명시되지 않는 한 모든 필드는 읽기 전용입니다.



**참고** **Help(도움말) > About(정보)** 페이지를 참조하십시오. 비슷하지만 약간 다른 정보를 제공합니다.

필드	설명
이름	FMC어플라이언스에 할당된 설명 이름입니다. 어플라이언스 이름으로 호스트 이름을 사용할 수 있지만 이 필드에 다른 이름을 입력해도 호스트 이름은 변경되지 않습니다.  이 이름은 특정 통합에서 사용됩니다. 예를 들어 SecureX 및 Cisco SecureX Threat Response와의 통합을 위해 디바이스 목록에 표시됩니다.
제품 모델	어플라이언스의 모델 이름입니다.
일련 번호	어플라이언스의 일련 번호입니다.
Software Version(소프트웨어 버전)	어플라이언스에 현재 설치된 소프트웨어 버전입니다.
Prohibit Packet Transfer to the Firepower Management Center	매니지드 디바이스가 이벤트와 함께 패킷 데이터를 전송하여 Firepower Management Center에 데이터를 저장할 수 있는지 여부를 지정합니다. 이 설정은 7000 및 8000 Series 디바이스의 로컬 웹 인터페이스에서 사용할 수 있습니다.
운영 체제	현재 어플라이언스에서 실행되는 운영 체제입니다.
운영 체제 버전	현재 어플라이언스에서 실행되는 운영 체제의 버전입니다.
IPv4 주소	기본(eth0) 관리 인터페이스의 IPv4 주소입니다. IPv4 관리가 비활성화된 경우, 이 필드는 이를 나타냅니다.

필드	설명
IPv6 주소	기본(eth0) 관리 인터페이스의 IPv6 주소입니다. IPv6 관리가 비활성화된 경우, 이 필드는 이를 나타냅니다.
현재 정책	현재 구축된 시스템 레벨 정책입니다. 마지막으로 구축된 후부터 정책이 업데이트된 경우, 정책 이름은 기울임 꼴로 표시됩니다.
모델 번호	내부 플래시 드라이브에 저장된 어플라이언스별 모델 번호입니다. 이 번호는 문제 해결을 위해 중요할 수 있습니다.

## 어플라이언스 정보 보기

프로시저

---

**System**(시스템) > **Configuration**(구성)을 선택합니다.

---

## 기본 시스템 정보 보기

About(정보) 페이지에는 Firepower System의 모델, 일련 번호, 다양한 구성 요소에 대한 버전 정보 등 어플라이언스에 대한 정보가 표시됩니다. 또한 Cisco 저작권 정보도 포함되어 있습니다.

프로시저

---

단계 1 페이지 상단에 있는 툴바에서 **Help**(도움말)를 클릭합니다.

단계 2 **About**(정보)를 선택합니다.

---

## HTTPS 인증서

SSL(Secure Sockets Layer)/TLS 인증서를 사용하면 Firepower Management Center 및 7000 및 8000 Series 디바이스가 시스템과 웹 브라우저 간에 암호화된 채널을 활성화할 수 있습니다. 기본 인증서는 모든 Firepower 디바이스에 포함되어 있지만 전역적으로 알려진 CA가 신뢰할 수 있는 인증 기관(CA)에서 생성되지는 않습니다. 따라서 전역적으로 알려졌거나 내부에서 신뢰할 수 있는 CA가 서명한 사용자 정의 인증서로 교체하는 것이 좋습니다.

## 기본 HTTPS 서버 인증서

어플라이언스와 함께 제공된 기본 서버 인증서를 사용하는 경우 기본 서버 인증서가 클라이언트 인증서에 서명한 CA에 의해 서명되지 않았으므로 시스템에서 웹 인터페이스 액세스에 유효한 HTTPS 클라이언트 인증서를 요구하도록 구성하지 마십시오.

기본 서버 인증서의 수명은 인증서가 생성된 시점에 따라 달라집니다. 기본 서버 인증서 만료일을 보려면 **System(시스템) > Configuration(구성) > HTTPS Certificate(HTTPS 인증서)**을 선택합니다.

일부 Firepower 소프트웨어 업그레이드는 인증서를 자동으로 갱신할 수 있습니다. 자세한 내용은 [Cisco Firepower 릴리스 노트](#)를 참조하십시오.

Firepower Management Center 및 7000 및 8000 Series 디바이스의 **System(시스템) > Configuration(구성) > HTTPS Certificate(HTTPS 인증서)** 페이지에서 기본 인증서를 갱신할 수 있습니다. 7000 및 8000 Series 디바이스에서 CLI 명령 `system renew-http-cert`를 사용하여 기본 인증서를 갱신할 수도 있습니다.

## 맞춤형 HTTPS 서버 인증서

사용자가 제공하는 시스템 정보 및 ID 정보에 따라 Firepower Management Center 웹 인터페이스를 사용하여 서버 인증서 요청을 생성할 수 있습니다. 브라우저가 신뢰하는 설치된 내부 인증 기관(CA)이 있는 경우 요청을 사용하여 인증서에 서명할 수 있습니다. 또한 인증 기관에 서버 인증서를 요청하는 결과 요청을 보낼 수 있습니다. 인증 기관(CA)으로부터 서명된 인증서를 확보한 후, 이를 가져올 수 있습니다.

## HTTPS 클라이언트 인증서

클라이언트 브라우저 인증서 확인을 사용하여 Firepower System 웹 서버에 대한 액세스를 제한할 수 있습니다. 사용자 인증서를 활성화하면, 웹 서버는 사용자의 브라우저 클라이언트가 올바른 사용자 인증서가 선택되도록 했는지 확인합니다. 해당 사용자 인증서는 반드시 서버 인증서에 사용되는 인증 기관과 동일한 신뢰 기관에서 생성된 것이어야 합니다. 브라우저는 다음과 같은 경우 웹 인터페이스를 로드할 수 없습니다.

- 사용자가 유효하지 않은 브라우저에서 인증서를 선택합니다.
- 사용자가 브라우저에서 서버 인증서에 서명한 인증 기관이 생성하지 않은 인증서를 선택합니다.
- 사용자가 브라우저에서 디바이스의 인증서 체인에 있는 인증 기관이 생성하지 않은 인증서를 선택합니다.

또한 서버에 대한 CRL(인증서 해치 목록)을 로드할 수 있습니다. CRL 목록은 인증 기관에서 해지한 모든 인증서를 나열하므로, 웹 서버는 클라이언트 브라우저 인증서가 유효한 것을 확인할 수 있습니다. 사용자가 해지된 인증서로서 CRL에 나열된 인증서를 선택한 경우, 브라우저는 웹 인터페이스를 로드할 수 없습니다.

## 현재 서버 인증서 보기

로그인한 어플라이언스의 서버 인증서만 볼 수 있습니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **HTTPS Certificate**(HTTPS 인증서)를 클릭합니다.

## 인증서 서명 요청 생성 및 제출

이 절차를 사용하여 로컬 구성 **HTTPS Certificate**(HTTPS 인증서) 페이지를 통해 인증서 요청을 생성할 때, 단일 시스템에 대해서만 인증서를 생성할 수 있습니다. 유사하게, 시스템에 연결할 때 전역으로 알려졌거나 내부적으로 신뢰할 수 있는 CA에서 서명되지 않은 인증서를 설정하는 경우 보안 경고가 표시됩니다.

인증서 요청에 대해 생성된 키는 **Base-64**로 인코딩된 PEM 형식입니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **HTTPS Certificate**(HTTPS 인증서)를 클릭합니다.

단계 3 **Generate New CSR**(새로운 CSR 생성)을 클릭합니다.

단계 4 **Country Name (two-letter code)**(국가 이름(2글자 코드)) 필드에 국가 번호를 입력합니다.

단계 5 **State or Province**(주 또는 도) 필드에 주 또는 도에 대한 우편 약자를 입력합니다.

단계 6 **Locality or City**(구/군/시)를 입력합니다.

단계 7 **Organization**(조직) 이름을 입력합니다.

단계 8 **Organizational Unit**(조직 단위)(**Department**(부서)) 이름을 입력합니다.

단계 9 **Common Name**(공용 이름) 필드에 인증서를 요청할 서버의 정규화된 도메인 이름을 올바르게 입력합니다.

참고 **Common Name**(공용 이름) 필드의 인증서에 나타나도록 서버의 정규화된 도메인 이름을 올바르게 입력해야 합니다. 공용 이름과 DNS 호스트 이름이 일치하지 않는 경우, 어플라이언스에 연결하면 경고를 받습니다.

단계 10 **Generate**(생성)를 클릭합니다.

단계 11 텍스트 편집기를 엽니다.

단계 12 **BEGIN CERTIFICATE REQUEST**(인증서 요청 시작) 및 **END CERTIFICATE REQUEST**(인증서 요청 끝)를 포함하는 인증서 요청의 전체 텍스트 블록을 복사하여 비어있는 텍스트 파일에 붙여 넣습니다.

단계 13 파일을 `servername.csr`로 저장합니다. 여기서 `servername`은 인증서 사용을 계획하고 있는 서버의 이름입니다.

단계 14 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

- 서명된 서버 인증서를 업로드합니다. [서버 인증서 업로드, 9 페이지](#) 섹션을 참조하십시오.

## 서버 인증서 업로드

인증서를 생성한 서명 기관이 중간 CA를 신뢰하기를 요청하는 경우, 또한 인증서 체인을 제공해야 하는데, 이는 때로 인증서 경로라고 합니다. 사용자 인증서를 요청하는 경우, 중간 권한이 인증서 체인에 포함된 인증 기관에서 생성된 것이어야 합니다.

## 서버 인증서 업로드

인증서를 생성한 서명 기관이 중간 CA를 신뢰하기를 요청하는 경우, 또한 인증서 체인을 제공해야 하는데, 이는 때로 인증서 경로라고 합니다. 사용자 인증서를 요청하는 경우, 중간 권한이 인증서 체인에 포함된 인증 기관에서 생성된 것이어야 합니다.

시작하기 전에

- 인증서 서명 요청을 생성합니다. [인증서 서명 요청 생성 및 제출, 8 페이지](#) 섹션을 참조하십시오.
- 인증서를 요청할 인증 기관에 CSR 파일을 업로드하거나 CSR를 사용하여 자체 서명된 인증서를 만드십시오.

프로시저

단계 1 **System(시스템) > Configuration(구성)**을(를) 선택합니다.

단계 2 **HTTPS Certificate(HTTPS 인증서)**를 클릭합니다.

단계 3 **Import HTTPS Certificate(HTTPS 인증서 가져오기)**를 클릭합니다.

단계 4 텍스트 편집기의 서버 인증서를 열어 `BEGIN CERTIFICATE` 및 `END CERTIFICATE` 문구를 포함하는 전체 텍스트 블록을 복사하여 **Server Certificate(서버 인증서)** 필드에 붙여 넣습니다.

단계 5 개인 키를 업로드하려는 경우 개인 키 파일을 열어 `BEGIN RSA PRIVATE KEY`(RSA 개인 키 시작) 및 `END RSA PRIVATE KEY`(RSA 개인 키 끝) 문구를 포함하는 전체 텍스트 블록을 복사하여 **Private Key(개인 키)** 필드에 붙여 넣습니다.

단계 6 사용자가 제공해야 하는 중간 인증서를 열어서 전체 텍스트 블록을 복사하여 각각을 **Certificate Chain(인증서 체인)** 필드에 붙여 넣습니다.

단계 7 **Save**(저장)를 클릭합니다.

## 유효한 사용자 인증서 필요

시스템은 식별 부호화 규칙(DER) 형식의 CRL 업로드를 지원합니다. 한 서버에 대해 단 하나의 CRL 만 로드할 수 있습니다.

해지된 인증서 목록이 통용되고 있음을 확인하기 위해, CRL을 업데이트하는 예약된 작업을 생성할 수 있습니다. 가장 최근 재생된 CRL이 인터페이스에 나열됩니다.



참고 반드시 사용자 브라우저(또는 관독기에 삽입된 CAC)에 유효한 사용자 인증서가 있어야 사용자 인증서를 활성화할 수 있고, 실행 후 웹 인터페이스에 액세스할 수 있습니다.

시작하기 전에

- 서버 인증서에 사용된 것과 동일한 인증 기관을 사용하여 사용자 인증서를 생성합니다.
- 인증서의 중간 인증서를 업로드합니다. [서버 인증서 업로드, 9 페이지](#) 섹션을 참조하십시오.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **HTTPS Certificate**(HTTPS 인증서)를 클릭합니다.

단계 3 **Enable User Certificates**(사용자 인증서 활성화)를 선택합니다. 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 4 CRL을 검색하려는 경우 **Enable Catching of CRL**(CRL 가져오기)을 선택합니다.

단계 5 기존 CRL 파일에 유효한 URL을 입력하고 **Refresh CRL**(CRL 새로 복구)을 클릭합니다. 제공된 URL에서 현재 CRL을 서버에 로드합니다.

참고 CRL 페칭을 활성화하면 정기적으로 CRL을 업데이트하는 예약된 작업을 생성합니다. 작업을 수정하여 업데이트의 빈도를 설정합니다.

단계 6 가지고 있는 사용자 인증서가 서버 인증서를 만든 것과 동일한 인증 기관에서 생성한 것인지 확인합니다.

주의 활성화된 사용자 인증서로 구성을 저장하면, 브라우저 인증서 스토어에 유효한 사용자 인증서가 없는 경우, 어플라이언스에 모든 웹 서버 액세스를 비활성화합니다. 구성을 저장하기 전에 설치된 사용 가능한 인증서가 있는지 확인합니다.

단계 7 **Save**(저장)를 클릭합니다.

## 기본 HTTPS 서버 인증서 갱신

로그인한 어플라이언스의 서버 인증서만 볼 수 있습니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **HTTPS Certificate**(HTTPS 인증서)를 클릭합니다.

이 버튼은 시스템이 기본 HTTPS 서버 인증서를 사용하도록 구성된 경우에만 나타납니다.

단계 3 **Renew HTTPS Certificate**(HTTPS 인증서 갱신)을 클릭합니다. (이 옵션은 시스템이 기본 HTTPS 서버 인증서를 사용하도록 구성된 경우에만 인증서 정보 아래 화면에 나타납니다.)

단계 4 (선택 사항) **Renew HTTPS Certificate**(HTTPS 인증서 갱신) 대화 상자에서 인증서에 대한 새 키를 생성하기 위한 **Generate New Key**(새 키 생성)를 선택합니다.

단계 5 **Renew HTTPS Certificate**(HTTPS 인증서 갱신) 대화 상자에서 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

**HTTPS Certificate**(HTTPS 인증서) 페이지에 표시된 인증서 유효 기간이 업데이트되었는지 확인하여 인증서가 갱신되었는지 확인할 수 있습니다.

## 외부 데이터베이스 액세스 설정

서드파티 클라이언트에 데이터베이스에 대한 읽기 전용 액세스를 허용하도록 **Firepower Management Center**를 구성할 수 있습니다. 그러면 다음 중 하나를 사용하여 SQL로 데이터베이스에 쿼리할 수 있습니다.

- Actuate BIRT, JasperSoft iReport 또는 Crystal Reports와 같은 산업 표준 보고 툴
- JDBC SSL 연결을 지원하는 기타 보고 애플리케이션(사용자 지정 애플리케이션 포함)
- 인터랙티브 방식으로 실행하거나 단일 쿼리에 대해 쉽표로 구분된 결과를 얻기 위해 사용할 수 있는 RunQuery라는 Cisco 제공 명령줄 Java 애플리케이션

**Firepower Management Center**의 시스템 구성을 사용하여 데이터베이스 액세스를 활성화하고 선택한 호스트가 데이터베이스를 쿼리할 수 있도록 액세스 목록을 만듭니다. 이 액세스 목록은 어플라이언스 액세스를 제어하지 않습니다.

다음에 포함될 패키지를 다운로드할 수도 있습니다.

- RunQuery - Cisco 제공 데이터베이스 쿼리 툴
- InstallCert - 액세스하려는 **Firepower Management Center**에서 SSL 인증서를 검색하고 승인하기 위해 사용할 수 있는 툴

- 데이터베이스에 연결하기 위해 사용해야 하는 JDBC 드라이버

데이터베이스 액세스를 구성하기 위해 다운로드한 패키지의 튜 사용에 대한 내용은 *Firepower System* 데이터베이스 액세스 설명서 섹션을 참조하십시오.

## 데이터베이스에 대한 외부 액세스 활성화

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **External Database Access**(외부 데이터베이스 액세스)를 클릭합니다.

단계 3 **Allow External Database Access**(외부 데이터베이스 액세스 허용) 확인란을 선택합니다.

단계 4 **Server Hostname**(서버 호스트네임) 필드에 적절한 값을 입력합니다. 서드파티 애플리케이션 요건에 따라 이 값은 Firepower Management Center의 QDN(정규화된 도메인 이름), IPv4 주소 또는 IPv6 주소 일 수 있습니다.

단계 5 **Client JDBC Driver**(클라이언트 JDBC 드라이버) 옆에 있는 **Download**(다운로드)를 클릭하고 브라우저의 지시에 따라 `client.zip` 패키지를 다운로드합니다.

단계 6 하나 이상의 IP 주소에 대한 데이터베이스 액세스를 추가하려면 **Add Hosts**(호스트 추가)를 클릭합니다. **Access List**(액세스 목록) 필드에 **IP Address**(IP 주소) 필드가 나타납니다.

단계 7 **IP** 주소 필드에 IP 주소 또는 어드레스 레인지 또는 모두를 입력하십시오.

단계 8 **Add**(추가)를 클릭합니다.

단계 9 **Save**(저장)를 클릭합니다.

팁        마지막으로 저장된 데이터베이스 설정으로 되돌리려면 **Refresh**(새로 고침)를 클릭합니다.

관련 항목

[Firepower System IP 주소 규칙](#)

## 데이터베이스 이벤트 제한 수

디스크 공간을 관리하기 위해서 FMC은 이벤트 데이터베이스에서 가장 오래된 침입 이벤트, 감사 기록, 보안 인텔리전스 데이터 또는 URL 필터링 데이터를 자동으로 제거합니다. 각 이벤트 유형에 대해 정리 후 FMC가 보유할 레코드 수를 지정할 수 있습니다. 해당 유형에 대해 구성된 보유 제한보다 많은 유형의 레코드를 포함하는 이벤트 데이터베이스에도 의존하지 않습니다. 성능을 높이려면 정기적으로 작업하는 이벤트 수에 대한 이벤트 제한을 조정해야 합니다. 선택적으로 정리가 발생할 때 이메일 알림을 수신하도록 선택할 수 있습니다. 일부 이벤트 유형의 경우 스토리지를 비활성화할 수 있습니다.

개별 이벤트를 수동으로 삭제하려면 이벤트 뷰어를 사용합니다. (버전 6.6.0 이상에서는 이러한 방식으로 연결 또는 보안 인텔리전스 이벤트를 수동으로 삭제할 수 없습니다.) 데이터베이스를 수동으로 제거할 수도 있습니다. [데이터 스토리지](#)의 내용을 참조하십시오.

## 데이터베이스 이벤트 제한 구성

시작하기 전에

- 이벤트가 Firepower Management Center 데이터베이스에서 정리될 때 이메일 알림을 받으려면 이메일 서버를 구성해야 합니다. [메일 릴레이 호스트 및 알림 주소 구성, 36 페이지](#) 섹션을 참조하십시오.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Database**(데이터베이스)를 선택합니다.

단계 3 각 데이터베이스에 대해 저장할 레코드의 수를 입력합니다.

각 데이터베이스가 유지 관리할 레코드 수에 대한 정보는 [데이터베이스 이벤트 제한 수, 13 페이지](#) 섹션을 참조하십시오.

단계 4 선택적으로 **Data Pruning Notification Address**(데이터 제거 알림 주소) 필드에 제거 알림을 수신할 이메일 주소를 입력합니다.

단계 5 **Save**(저장)를 클릭합니다.

## 데이터베이스 이벤트 제한 수

다음 표에는 Firepower Management Center에 저장할 수 있는 각 이벤트 유형의 최소 및 최대 레코드 수가 나열되어 있습니다.

표 2: 데이터베이스 이벤트 제한 수

이벤트 유형	상한 제한	하한 제한
침입 이벤트	1,000만(FMC Virtual) 3,000만(FMC1000, FMC1600) 6,000만(FMC2500, FMC2600, FMCv 300) 3억(FMC4500, FMC4600)	10,000
검색 이벤트	1,000만(FMC Virtual) 2,000만(FMC2500, FMC2600, FMC4500, FMC4600, FMCv 300)	0(스토리지 비활성화)

이벤트 유형	상한 제한	하한 제한
연결 이벤트 보안 인텔리전스 이벤트	5,000만(FMC Virtual) 1억(FMC1000, FMC1600) 3억(FMC2500, FMC2600, FMCv 300) 10억(FMC4500, FMC4600) 제한은 연결 이벤트와 보안 인텔리전스 이벤트 간에 공유됩니다. 구성된 최대 값의 합은 이 제한을 초과할 수 없습니다.	0(스토리지 비활성화) 이러한 설정은 연결 요약에 영향을 주지 않습니다.
연결 요약(취합된 연결 이벤트)	5,000만(FMC Virtual) 1억(FMC1000, FMC1600) 3억(FMC2500, FMC2600, FMCv 300) 10억(FMC4500, FMC4600)	0(스토리지 비활성화)
상관관계 이벤트 및 컴플라이언스 화이트 목록 이벤트	100만(FMC Virtual) 200만(FMC2500, FMC2600, FMC4500, FMC4600, FMCv 300)	1개
악성코드 이벤트	1,000만(FMC Virtual) 2,000만(FMC2500, FMC2600, FMC4500, FMC4600, FMCv 300)	10,000
파일 이벤트	1,000만(FMC Virtual) 2,000만(FMC2500, FMC2600, FMC4500, FMC4600, FMCv 300)	0(스토리지 비활성화)
상태 이벤트	100만	0(스토리지 비활성화)
감사 기록	100,000	1개
복원 상태 이벤트	1,000만	1개
화이트 리스트 위반 기록	30일 위반 기록	일일 이력
사용자 활동(사용자 이벤트)	1,000만	1개
사용자 로그인(사용자 이력)	1,000만	1개
침입 규칙 업데이트 가져오기 로그 기록	1백만	1개
VPN 문제 해결 데이터베이스	1,000만	0(스토리지 비활성화)

# Management Interfaces(관리 인터페이스)관리 인터페이스

설정 후 FMC에 관리 인터페이스, 호스트 이름, 검색 도메인, DNS 서버 및 HTTP 프록시를 추가하는 것을 포함하여 관리 네트워크 설정을 변경할 수 있습니다.

## FMC 관리 인터페이스 정보

기본적으로 FMC는 모든 디바이스를 단일 관리 인터페이스에서 관리합니다. 또한 관리 인터페이스에 대한 초기 설정을 수행하고 이 인터페이스에서 관리자로서 FMC에 로그인할 수도 있습니다. 관리 인터페이스는 Smart Licensing 서버와 통신하고, 업데이트를 다운로드하고, 기타 관리 기능을 수행하는 작업에도 사용됩니다.

디바이스 관리 인터페이스에 대한 자세한 내용은 [디바이스 관리 인터페이스](#)의 내용을 참조하십시오.

## FMC의 관리 인터페이스

FMC는 초기 설정, 관리자를 위한 HTTP 액세스, 디바이스 관리, 라이선스 및 업데이트와 같은 기타 관리 기능을 위해 eth0 인터페이스를 사용합니다.

동일한 네트워크 또는 다른 네트워크에서 추가 관리 인터페이스를 구성할 수도 있습니다. FMC에서 많은 수의 디바이스를 관리할 때 관리 인터페이스를 추가하면 처리량과 성능이 향상될 수 있습니다. 다른 모든 관리 기능에 대해 이 인터페이스를 사용할 수도 있습니다. 특정 기능을 위해 각 관리 인터페이스를 사용할 수도 있습니다. 예를 들어 HTTP 관리자 액세스용으로 하나의 인터페이스를 사용하고 디바이스 관리용으로 하나의 인터페이스를 사용할 수 있습니다.

디바이스 관리의 경우 관리 인터페이스에는 두 개의 별도 트래픽 채널이 있습니다. 즉, 관리 트래픽 채널은 모든 내부 트래픽(예: 디바이스 관리와 관련된 디바이스 간 트래픽)을 전달하고, 이벤트 트래픽 채널은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달합니다. 선택적으로 이벤트 트래픽을 처리하기 위해 FMC에 별도의 이벤트 전용 인터페이스를 구성할 수 있습니다. 하나의 이벤트 인터페이스만 구성할 수 있습니다. 이벤트 트래픽은 많은 양의 대역폭을 사용할 수 있으므로 관리 트래픽에서 이벤트 트래픽을 분리하면 FMC의 성능이 향상될 수 있습니다. 예를 들어 관리를 위해 1GigabitEthernet 인터페이스를 사용하는 경우 10GigabitEthernet 인터페이스를 이벤트 인터페이스로 할당할 수 있습니다. 예를 들어 인터넷 액세스가 포함된 네트워크의 일반 관리 인터페이스를 사용하는 동안 완전히 안전한 프라이빗 네트워크에 이벤트 전용 인터페이스를 구성할 수 있습니다. 또한 증가된 처리량만 활용하는 것이 목표인 경우 동일한 네트워크에서 관리 및 이벤트 인터페이스를 모두 사용할 수 있습니다. 매니지드 디바이스는 관리 트래픽을 FMC 관리 인터페이스로 보내고 이벤트 트래픽을 FMC 이벤트 전용 인터페이스로 보냅니다. 매니지드 디바이스가 이벤트 전용 인터페이스에 연결할 수 없는 경우 관리 인터페이스로 이벤트를 전송합니다.



**참고** 모든 관리 인터페이스는 액세스 목록 구성 ([액세스 목록 구성, 32 페이지](#))에 의해 제어되는 HTTP 관리자 액세스를 지원합니다. 반대로 인터페이스를 HTTP 액세스 전용으로 제한할 수는 없습니다. 관리 인터페이스는 항상 디바이스 관리(관리 트래픽, 이벤트 트래픽 또는 둘 다)를 지원합니다.



참고 eth0 인터페이스만 DHCP IP 주소를 지원합니다. 다른 관리 인터페이스는 고정 IP 주소만 지원합니다.

## FMC 모델별 관리 인터페이스 지원

관리 인터페이스 위치에 대한 모델의 하드웨어 설치 가이드를 참조하십시오.

각 FMC 모델에서 지원되는 관리 인터페이스는 다음 표를 참조하십시오.

표 3: FMC의 관리 인터페이스 지원

모델	Management Interfaces(관리 인터페이스)관리 인터페이스
MC1000	eth0(기본값) eth1
MC2500, MC4500	eth0(기본값) eth1 eth2 eth3
MC1600, MC2600, MC4600	eth0(기본값) eth1 eth2 eth3 CIMC(Lights-Out 관리에만 지원됨)
Firepower Management Center Virtual	eth0(기본값)

## FMC 관리 인터페이스의 네트워크 라우트

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

기본 경로는 항상 가장 낮은 번호의 관리 인터페이스(예: eth0)를 사용합니다.

원격 네트워크에 액세스하기 위해서는 관리 인터페이스당 최소 1개의 정적 경로가 권장됩니다. 다른 디바이스에서 FMC로의 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 FMC에서 eth0 및 eth1은 모두 동일한 네트워크에 있지만 각 인터페이스에서 서로 다른 디바이스 그룹을 관리하려고 합니다. 기본 게이트웨이는 192.168.45.1입니다. eth1이 원격 10.6.6.0/24 대상 네트워크에서 디바이스를 관리하도록 하려면 동일한 게이트웨이 192.168.45.1을 사용하여 eth1을 통해 10.6.6.0/24에 대한 정적 경로를 만들 수 있습니다.

니다. 10.6.6.0/24 트래픽은 기본 경로에 도달하기 전에 이 경로에 도달하므로 eth1이 예상대로 사용됩니다.

2개의 FMC 인터페이스를 사용하여 동일한 네트워크에 있는 원격 디바이스를 관리하려는 경우 디바이스 IP 주소별로 별도의 정적 경로가 필요하기 때문에 FMC의 정적 라우팅이 제대로 확장되지 않을 수 있습니다.

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 전용 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.

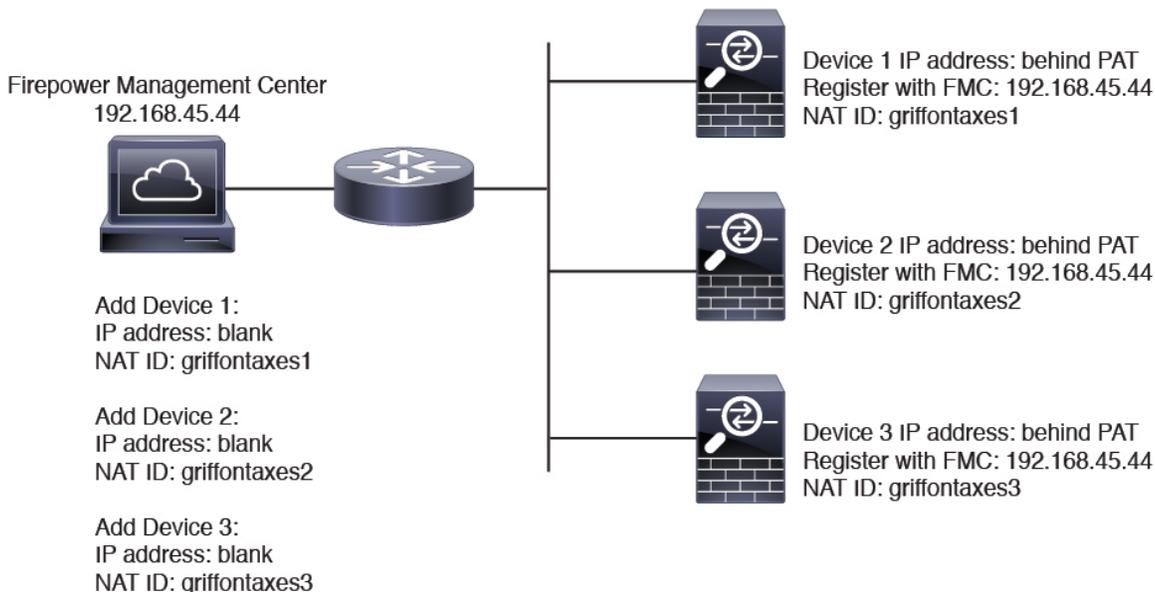
일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. FMC는 디바이스 IP 주소를 지정하고 디바이스는 FMC IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. FMC 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

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 FMC은 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.

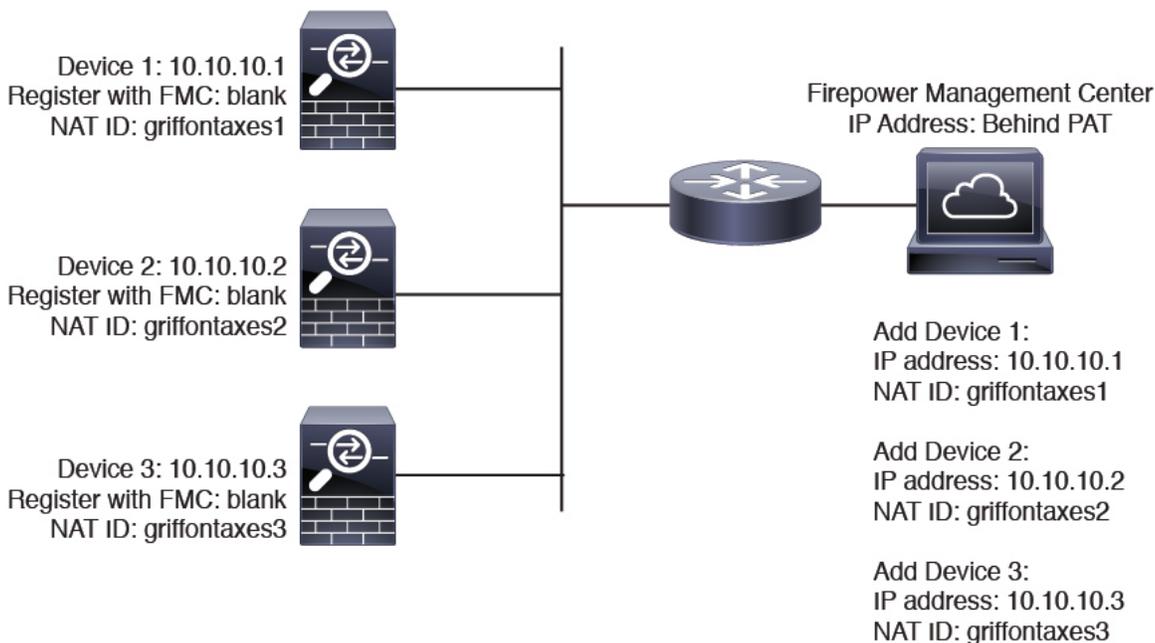
다음 예에서는 PAT IP 주소 뒤에 3개의 장치가 있음을 보여줍니다. 이 경우 FMC 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 디바이스에 FMC IP 주소를 지정하십시오.

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



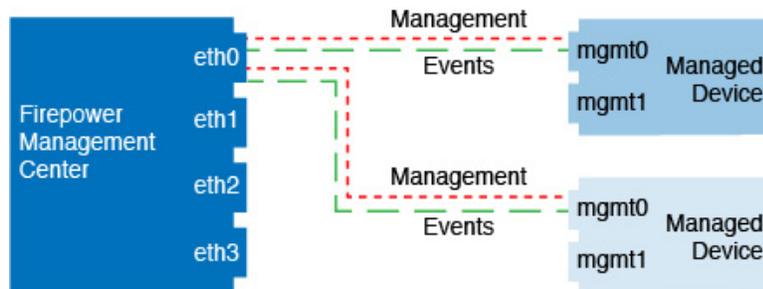
## 관리 및 이벤트 트래픽 채널 예시



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

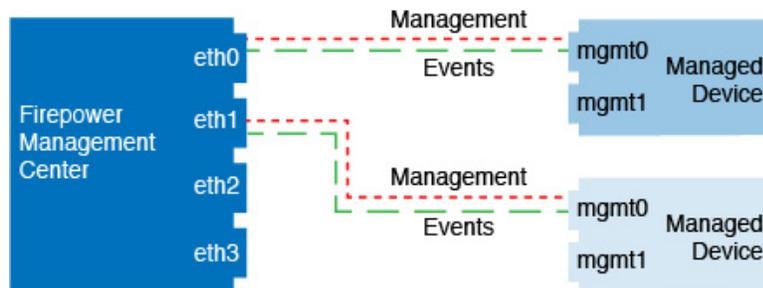
다음 예에서는 기본 관리 인터페이스만 사용하는 Firepower Management Center 및 매니지드 디바이스를 보여 줍니다.

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



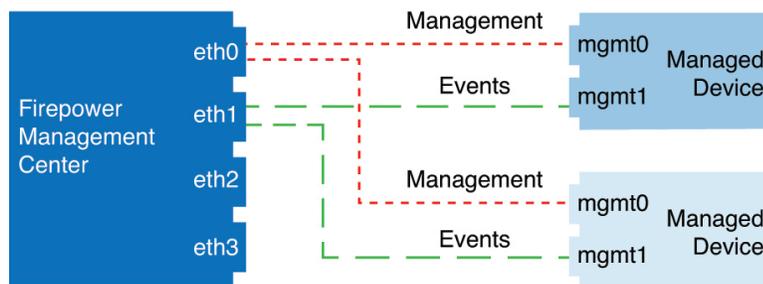
다음 예는 디바이스에 별도의 관리 인터페이스를 사용하는 Firepower Management Center를 보여 줍니다. 관리되는 각 디바이스는 1개의 관리 인터페이스를 사용합니다.

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



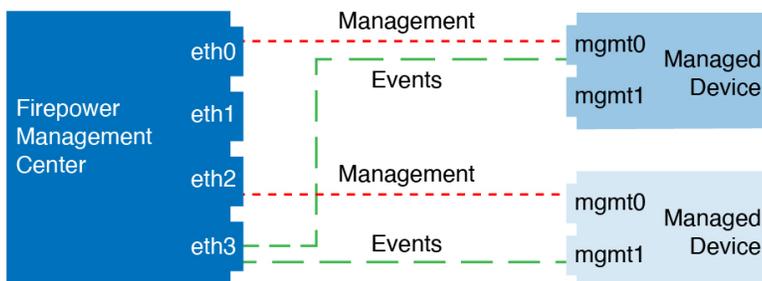
다음 예에서는 별도의 이벤트 인터페이스를 사용하는 Firepower Management Center 및 매니지드 디바이스를 보여 줍니다.

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



## FMC 관리 인터페이스 수정

Firepower Management Center에서 관리 인터페이스 설정을 수정합니다. 필요에 따라 추가 관리 인터페이스를 활성화하거나 이벤트 전용 인터페이스를 구성할 수 있습니다.



**주의** 연결된 관리 인터페이스를 변경할 때 주의하십시오. 구성 오류로 인해 다시 연결할 수 없는 경우 FMC 콘솔 포트에 액세스하여 Linux 셸의 네트워크 설정을 다시 구성해야 합니다. 이 작업에 대한 안내를 받으려면 Cisco TAC에 문의해야 합니다.



**참고** FMC IP 주소를 변경하는 경우, **디바이스에서 FMC IP 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다.**의 내용을 참조하십시오. 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.



**참고** 고가용성 설정에서 등록된 Firepower 디바이스의 관리 IP 주소를 디바이스 CLI 또는 Firepower Management Center에서 수정할 때 보조 Firepower Management Center는 HA 동기화 후에도 변경 내용을 반영하지 않습니다. 보조 Firepower Management Center도 업데이트되도록 하려면 두 Firepower Management Center 간에 역할을 전환하여 보조 Firepower Management Center를 활성 유닛으로 설정합니다. 현재 활성 Firepower Management Center의 Device Management(디바이스 관리) 페이지에 등록된 Firepower 디바이스의 관리 IP 주소를 수정합니다.

### 시작하기 전에

- 디바이스 관리의 작동 방식에 대한 자세한 내용은 [디바이스 관리 인터페이스](#)의 내용을 참조하십시오.
- 프록시를 사용하는 경우:
  - NTLM(NT LAN Manager) 인증을 사용하는 프록시는 지원되지 않습니다.
  - 스마트 라이선스를 사용하거나 사용할 예정인 경우 프록시 FQDN은 64자를 초과할 수 없습니다.

### 프로시저

**단계 1 System(시스템) > Configuration(구성)**을 선택한 다음 **Management Interface(관리 인터페이스)**를 선택합니다.

**단계 2 Interfaces(인터페이스)** 영역에서 구성하려는 인터페이스 옆에 있는 **Edit(편집)**를 클릭합니다.

이 섹션에는 사용 가능한 모든 인터페이스가 나열되어 있습니다. 다른 인터페이스를 추가할 수 없습니다.

각 관리 인터페이스에서 다음 옵션을 구성할 수 있습니다.

- **Enabled(활성화됨)** - 관리 인터페이스를 활성화합니다. 기본 eth0 관리 인터페이스를 비활성화하지 마십시오. 일부 프로세스에는 eth0 인터페이스가 필요합니다.
- **Channels(채널)** - 이벤트 전용 인터페이스를 구성합니다. FMC에 하나의 이벤트 인터페이스만 구성할 수 있습니다. 이렇게 하려면 **Management Traffic(관리 트래픽)** 확인란을 선택 취소하고 **Event Traffic(이벤트 트래픽)** 확인란을 선택한 상태로 유지합니다. 관리 인터페이스에 대한 **Event Traffic(이벤트 트래픽)**을 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.
- **Mode(모드)** - 연결 모드를 지정합니다. GigabitEthernet 인터페이스의 경우 자동 협상에 대한 변경 사항은 무시됩니다.
- **MDI/MDIX - Auto-MDIX**를 설정합니다.
- **MTU** - 최대 전송 단위(MTU)를 설정합니다. 기본값은 1500입니다. MTU 설정 가능 범위는 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.  
 시스템은 구성된 MTU 값에서 자동으로 18바이트를 잘라내므로 1298 아래의 값은 최소 IPv6 MTU 설정인 1280을 준수하지 못하며 594 아래의 값은 최소 IPv4 MTU 설정인 576을 준수하지 못합니다. 예를 들면 시스템은 구성된 값 576을 자동으로 558로 자릅니다.
- **IPv4 Configuration(IPv4 구성)** - IPv4 IP 주소를 설정합니다. 선택:
  - **Static(정적)** - 수동으로 **IPv4 Management IP(IPv4 관리 IP)** 주소 및 **IPv4 Netmask(IPv4 넷 마스크)**를 입력합니다.

- **DHCP** - DHCP를 사용하도록 인터페이스를 설정합니다(eth0 전용).
- **Disabled(비활성화됨)** - IPv4를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
- **IPv6 Configuration(IPv6 구성)** - IPv6 IP 주소를 설정합니다. 선택:
  - **Static(정적)** - 수동으로 **IPv6 Management IP(IPv6 관리 IP)** 주소 및 **IPv6 Prefix Length(IPv6 프리픽스 길이)**를 입력합니다.
  - **DHCP** - DHCPv6를 사용하도록 인터페이스를 설정합니다(eth0 전용).
  - **Router Assigned(라우터 할당)** - 상태 비저장 자동 구성을 활성화합니다.
  - **Disabled(비활성화됨)** - IPv6를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
  - **IPv6 DAD** - IPv6을 활성화할 때 DAD(Duplicate Address Detection)를 활성화 또는 비활성화합니다. DAD를 사용하면 서비스 거부(DoS) 공격 가능성이 발생하기 때문에 DAD를 비활성화하려고 할 수 있습니다. 이 설정을 비활성화하면 이 인터페이스가 이미 할당된 주소를 사용하고 있지 않은지 수동으로 확인해야 합니다.

단계 3 **Routes(경로)** 영역에서 수정(✍)을 클릭하여 정적 경로를 편집하거나 추가(+ )를 클릭하여 경로를 추가합니다.

🔍을 클릭하여 경로 테이블을 확인합니다.

각 추가 인터페이스가 원격 네트워크에 도달할 수 있는 정적 경로가 필요합니다. 새 경로가 필요한 시점에 대한 자세한 내용은 [FMC 관리 인터페이스의 네트워크 라우트, 16 페이지](#) 섹션을 참조하십시오.

참고 기본 경로의 경우 게이트웨이 IP 주소만 변경할 수 있습니다. 기본 경로는 항상 eth0 인터페이스를 사용합니다.

정적 경로에 대해 다음 설정을 구성할 수 있습니다.

- **Destination(대상)** - 경로를 생성할 네트워크의 대상 주소를 설정합니다.
- **Netmask(넷마스크)** 또는 **Prefix Length(프리픽스 길이)** - 네트워크의 넷마스크(IPv4) 또는 프리픽스 길이(IPv6)를 설정합니다.
- **Interface(인터페이스)** - 이그레스 관리 인터페이스를 설정합니다.
- **Gateway(게이트웨이)** - 게이트웨이 IP 주소를 설정합니다.

단계 4 **Shared Settings(공유 설정)** 영역의 모든 인터페이스에서 공유하는 네트워크 파라미터를 설정합니다.

참고 eth0 인터페이스에 **DHCP**를 선택한 경우 DHCP 서버에서 파생된 일부 공유 설정을 수동으로 지정할 수 없습니다.

다음 공유 설정을 구성할 수 있습니다.

- **Hostname(호스트네임)** - FMC 호스트네임을 설정합니다. 호스트 이름은 문자 또는 숫자로 시작하고 끝나야 하며 문자, 숫자 또는 하이픈만 사용할 수 있습니다. 호스트네임을 변경하는 경우 새 호스트네임을 시스템 로그 메시지에 반영하려면 FMC를 리부팅합니다. 시스템 로그 메시지는 리부팅될 때까지 새 호스트네임을 반영하지 않습니다.
- **Domains(도메인)** - FMC에 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.
- **Primary DNS Server(기본 DNS 서버), Secondary DNS Server(보조 DNS 서버)/Tertiary DNS Server(3차 DNS 서버)** - 환경설정 순서대로 사용할 DNS 서버를 설정합니다.
- **Remote Management Port(원격 관리 포트)** - 매니지드 디바이스와의 통신을 위한 원격 관리 포트를 설정합니다. 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 5 ICMPv6 영역에서 ICMPv6 설정을 구성합니다.

- **Allow Sending Echo Reply Packets(에코 응답 패킷 전송 허용)** - 에코 응답 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 FMC 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다.
- **Allow Sending Destination Unreachable Packets(대상에 연결할 수 없는 패킷 전송 허용)** - 대상에 연결할 수 없는 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다.

단계 6 Proxy(프록시) 영역에서 HTTP 프록시 설정을 구성합니다.

FMC는 TCP/443(HTTPS) 및 TCP/80(HTTP) 포트에서 직접 인터넷에 연결되도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다.

이 주제의 사전 요구 사항에서 프록시 요구 사항을 참조하십시오.

- a) **Enable(활성화)** 확인란을 선택합니다.
- b) 프록시 서버의 IP 주소 또는 정규화된 도메인 이름을 **HTTP Proxy(HTTP 프록시)** 필드에 입력합니다.

이 주제의 사전 요구 사항에서 해당 요구 사항을 참조하십시오.

- c) **Port(포트)** 필드에서 포트 번호를 입력합니다.
- d) **Use Proxy Authentication(프록시 인증 사용)**을 선택하여 인증 자격 증명을 제공하고 **User Name(사용자 이름)** 및 **Password(비밀번호)**를 제공합니다.

단계 7 **Save**(저장)를 클릭합니다.

단계 8 FMC IP 주소를 변경하는 경우, 'FMC IP 주소를 변경하는 경우'와 **디바이스에서 FMC IP 주소 또는 호스트이름을 수정하고자 할 경우 관리 연결을 재설정합니다.**의 내용을 참조하십시오.

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

## 종료 또는 재시작

웹 인터페이스를 사용하여 FMC의 프로세스 종료 및 재시작을 제어합니다. 다음 작업을 수행할 수 있습니다.

- 종료: 어플라이언스의 정상 종료를 시작합니다.



주의 전원 버튼을 사용하여 Firepower 어플라이언스를 종료하지 마십시오. 데이터가 손실될 수 있습니다. 웹 인터페이스(또는 CLI)를 사용하여 구성 데이터 손실 없이 시스템의 전원을 안전하게 끄고 재시작할 수 있도록 준비합니다.

- 재부팅: 종료한 다음 정상적으로 재시작합니다.
- 콘솔 재시작: 통신, 데이터베이스 및 HTTP 서버 프로세스를 다시 시작합니다. 이는 일반적으로 문제 해결 중에 사용됩니다.



팁 Snort 프로세스 재시작을 포함한 7000/8000 시리즈 디바이스 종료/재시작 관련 정보는 [7000/8000 시리즈 디바이스 종료 또는 재시작](#) 섹션을 참조하십시오. 가상 디바이스의 경우에는 가상 플랫폼 설명서를 참조하십시오. 특히 VMware의 경우 사용자 지정 전원 옵션을 VMware 도구로 제공합니다.

## FMC를 종료하거나 재시작합니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Process**(프로세스)를 선택합니다.

단계 3 다음 중 하나를 수행합니다.

종료	<b>Shutdown Management Center(Management Center 종료)</b> 옆에 있는 <b>Run Command(명령 실행)</b> 를 클릭합니다.
재부팅	<b>Reboot Management Center(Management Center 재부팅)</b> 옆에 있는 <b>Run Command(명령 실행)</b> 를 클릭합니다.  참고 리부팅하면 로그아웃되며, 완료하는 데 최대 1시간이 소요될 수 있는 데이터베이스 검사가 실행됩니다.
콘솔 재시작	<b>Restart Management Center Console(Management Center 콘솔 재시작)</b> 옆에 있는 <b>Run Command(명령 실행)</b> 를 클릭합니다.  참고 재시작하면 삭제된 호스트가 네트워크 맵에 다시 나타날 수 있습니다.

관련 항목

[Snort® 재시작 시나리오](#)

## 원격 스토리지 관리

Firepower Management Center에서 백업 및 보고를 위해 로컬 또는 원격 스토리지 다음을 사용할 수 있습니다.

- NFS(Network File System)
- Server Message Block (SMB)/Common Internet File System (CIFS)
- SSH(Secure Shell)

백업은 한 원격 시스템으로 전송하고 보고서는 다른 원격 시스템으로 전송할 수는 없습니다. 그러나 둘 중 하나는 원격 시스템으로 전송하고 나머지는 Firepower Management Center에 저장할 수는 있습니다.



팁 원격 스토리지를 구성 및 선택한 경우, 오직 연결 데이터베이스 한도를 높이지 않은 경우에만 로컬 스토리지로 다시 전환할 수 있습니다.

## 로컬 스토리지 설정

프로시저

- 단계 1 **System(시스템) > Configuration(구성)**을(를) 선택합니다.
- 단계 2 **Remote Storage Device(원격 스토리지 디바이스)**를 선택합니다.

단계 3 **Storage Type**(스토리지 유형) 드롭다운 목록에서 **Local (No Remote Storage)**(로컬(원격 스토리지 아님))을 선택합니다.

단계 4 **Save**(저장)를 클릭합니다.

## 원격 스토리지에 대한 NFS 설정

시작하기 전에

- 외부 원격 스토리지 시스템이 정상적으로 작동하는지와 FMC에서 액세스할 수 있는지를 확인합니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Remote Storage Device**(원격 스토리지 디바이스)를 클릭합니다.

단계 3 **Storage Type**(스토리지 유형) 드롭다운 목록에서 **NFS**를 선택합니다.

단계 4 연결 정보를 추가합니다.

- 스토리지 시스템의 IPv4 주소 또는 호스트 이름을 **Host**(호스트) 필드에 입력합니다.
- 스토리지 영역에 대한 경로를 **Directory**(디렉터리) 필드에 입력합니다.

단계 5 선택적으로 **Use Advanced Options**(고급 옵션 사용) 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. [원격 스토리지 관리 고급 옵션, 28 페이지](#) 섹션을 참조하십시오.

단계 6 **System Usage**(시스템 사용)에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups**(백업용으로 사용)를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports**(보고서용으로 사용)를 선택합니다.
- 원격 스토리지용 백업에 대해 **Disk Space Threshold**를 입력합니다. 기본값은 90%입니다.

단계 7 설정을 테스트하려면 **Test**(테스트)를 클릭합니다.

단계 8 **Save**(저장)를 클릭합니다.

## 원격 스토리지에 대한 SMB 설정

시작하기 전에

외부 원격 스토리지 시스템이 정상적으로 작동하는지 그리고 FMC에서 액세스할 수 있는지를 확인합니다.

- 시스템에서는 전체 파일 경로가 아니라 상위 레벨의 공유만 인식합니다. 사용하려는 정확한 디렉토리를 공유하려면 Windows를 사용해야 합니다.
- FMC에서 SMB 공유에 액세스하는 데 사용할 Windows 사용자에게 공유 위치에 대한 소유권과 읽기/변경 액세스 권한이 있는지 확인합니다.
- 보안을 유지하려면 SMB 2.0 이상을 설치해야 합니다.

#### 프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Remote Storage Device**(원격 스토리지 디바이스)를 클릭합니다.

단계 3 **Storage Type**(스토리지 유형) 드롭다운 목록에서 **SMB**를 선택합니다.

단계 4 연결 정보를 추가합니다.

- 스토리지 시스템의 IPv4 주소 또는 호스트 이름을 **Host**(호스트) 필드에 입력합니다.
- 스토리지 영역의 공유를 **Share**(공유) 필드에 입력합니다.
- 선택적으로, 원격 스토리지 시스템의 도메인 이름을 **Domain**(도메인) 필드에 입력합니다.
- **Username**(사용자 이름) 필드에 스토리지 시스템의 사용자 이름을 입력하고 **Password**(비밀번호) 필드에 해당 사용자의 비밀번호를 입력합니다.

단계 5 선택적으로 **Use Advanced Options**(고급 옵션 사용) 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. [원격 스토리지 관리 고급 옵션, 28 페이지](#) 섹션을 참조하십시오.

단계 6 **System Usage**(시스템 사용)에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups**(백업용으로 사용)를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports**(보고서용으로 사용)를 선택합니다.

단계 7 설정을 테스트하려면 **Test**(테스트)를 클릭합니다.

단계 8 **Save**(저장)를 클릭합니다.

## 원격 스토리지에 대한 SSH 설정



주의 어플라이언스에서 STIG 규정 준수를 활성화한 경우 해당 어플라이언스의 원격 스토리지에 SSH를 사용할 수 없습니다.

#### 시작하기 전에

- 외부 원격 스토리지 시스템이 정상적으로 작동하는지와 Firepower Management Center에서 액세스할 수 있는지를 확인합니다.

## 프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Remote Storage Device**(원격 스토리지 디바이스)를 클릭합니다.

단계 3 **Storage Type**(스토리지 유형) 드롭다운 목록에서 **SSH**를 선택합니다.

단계 4 연결 정보를 추가합니다.

- 스토리지 시스템의 IP 주소 또는 호스트네임을 **Host**(호스트) 필드에 입력합니다.
- 스토리지 영역에 대한 경로를 **Directory**(디렉터리) 필드에 입력합니다.
- **Username**(사용자 이름) 필드에 스토리지 시스템의 사용자 이름을 입력하고 **Password**(비밀번호) 필드에 해당 사용자의 비밀번호를 입력합니다. 연결 사용자 이름의 일부로 네트워크 도메인을 지정하려면 사용자 이름 앞에 슬래시(/)가 오는 도메인을 지정합니다.
- SSH 키를 사용하려면 **SSH Public Key** 필드의 내용을 복사하여 `authorized_keys` 파일에 붙여넣습니다.

단계 5 선택적으로 **Use Advanced Options**(고급 옵션 사용) 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. [원격 스토리지 관리 고급 옵션, 28 페이지](#) 섹션을 참조하십시오.

단계 6 **System Usage**(시스템 사용)에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups**(백업용으로 사용)를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports**(보고서용으로 사용)를 선택합니다.

단계 7 설정을 테스트하려면 **Test**(테스트)를 클릭해야 합니다.

단계 8 **Save**(저장)를 클릭합니다.

## 원격 스토리지 관리 고급 옵션

SFMB(보안 파일 전송 프로토콜)를 사용하여 보고서 및 백업을 저장하기 위해 NFS(Network File System) 프로토콜, SMB(Server Message Block) 프로토콜 또는 SSH를 선택하는 경우 **Use Advanced Options**(고급 옵션 사용) 확인란을 선택하여 NFS, SMB 또는 SSH 마운트 매뉴얼 페이지에 설명된 마운트 바이너리 옵션 중 하나를 사용할 수 있습니다.

SMB를 선택할 경우 다음 형식을 사용하여 **Command Line Options**(명령줄 옵션) 필드에서 보안 모드를 입력할 수 있습니다.

```
sec=mode
```

여기서 `mode`는 원격 스토리지에 사용할 보안 모드입니다.

표 4: SMB 보안 모드 설정

모드	설명
[없음]	Null 사용자(이름 없음)로서 연결을 시도합니다.
krb5	Kerberos 버전 5 인증을 사용합니다.
krb5i	Kerberos 인증 및 패킷 서명을 사용합니다.
ntlm	NTLM 비밀번호 해싱을 사용합니다. (기본값)
ntlm	서명과 함께 NTLM 비밀번호 해싱을 사용합니다 (서버에서 서명을 요구하는 경우 /proc/fs/cifs/PacketSigningEnabled가 On이면 기본값).
ntlmv2	NTLMv2 비밀번호 해싱을 사용합니다.
ntlmv2i	패킷 서명과 함께 NTLMv2 비밀번호 해싱을 사용합니다.

## 검증 변경

사용자가 변경하는 내용을 모니터링하고 그러한 변경이 회사의 기본 표준을 따르는지 확인하려면 지난 24시간 동안 변경 사항의 자세한 보고서를 이메일로 전송하도록 시스템을 구성할 수 있습니다. 사용자가 시스템 구성에 변경 사항을 저장할 때마다 변경에 대한 스냅샷이 생성됩니다. 변경 조정 보고서는 이러한 스냅샷의 정보를 결합하여 최신 시스템 변경 사항에 대한 명확한 요약を提供합니다.

다음 샘플 그림에는 예제 변경 조정 보고서의 User 페이지가 표시되며, 각 구성의 이전 값과 변경 이후의 값이 모두 나열되어 있습니다. 여러 사용자가 동일한 구성을 여러 번 변경하면 보고서에는 최근 것부터 시간순으로 각 변경 사항의 요약이 나열됩니다.

지난 24시간 동안 변경된 내용을 볼 수 있습니다.

## 검증 변경 구성

시작하기 전에

- 이메일 서버가 24시간 동안 시스템 변경 사항에 대한 이메일 보고서를 수신하도록 구성합니다. 자세한 내용은 [메일 릴레이 호스트 및 알림 주소 구성, 36 페이지](#) 섹션을 참조하십시오.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Change Reconciliation**(검증 변경)을 클릭합니다.

단계 3 **Enable**(사용) 확인란을 선택합니다.

단계 4 시스템에서 변경 검증 보고서를 전송하도록 할 시간을 **Time to Run**(실행 시간) 드롭다운 목록에서 선택합니다.

단계 5 **Email to**(수신자) 필드에 이메일 주소를 입력합니다.

팁 이메일 주소를 추가한 후 **Resend Last Report**(마지막 보고서 다시 보내기)를 클릭하여 받는 사람에게 최신 변경 검증 보고서 사본을 전송합니다.

단계 6 정책 변경 사항을 포함하려면 **Include Policy Configuration**(정책 구성 포함) 확인란을 선택합니다.

단계 7 지난 24시간 동안 모든 변경 사항을 포함하려는 경우 **Show Full Change History**(전체 변경 기록 표시) 확인란을 선택합니다.

단계 8 **Save**(저장)를 클릭합니다.

관련 항목

[감사 로그를 사용하여 변경 검사](#)

## 검증 변경 옵션

**Include Policy Configuration**(정책 구성 포함) 옵션은 시스템에 정책 변경 기록이 변경 검증 보고서에 포함되는지 여부를 제어합니다. 여기에는 액세스 제어, 침입, 시스템, 상태 및 네트워크 검색 정책에 대한 변경 사항이 포함됩니다. 이 옵션을 선택하지 않으면 정책에 대한 변경 사항이 보고서에 표시되지 않습니다. 이 옵션은 Firepower Management Center에서만 사용할 수 있습니다.

**Show Full Change History**(전체 변경 기록 표시) 옵션은 시스템이 변경 검증 보고서에 지난 24시간 동안 발생한 모든 변경 사항의 기록을 포함할지 여부를 제어합니다. 이 옵션을 선택하지 않으면 보고서에는 각 카테고리에 대한 변경 사항의 통합된 보기만 포함됩니다.



참고 변경 조정 보고서에는 Firepower Threat Defense 인터페이스 및 라우팅 설정에 대한 변경 사항이 포함되지 않습니다.

## 정책 변경 코멘트

사용자가 액세스 제어, 침입 또는 네트워크 분석 정책을 수정할 때 코멘트 기능을 사용하여 여러 정책 관련 변경 사항을 추적하도록 Firepower 시스템을 구성할 수 있습니다.

정책 변경 코멘트를 활성화하면 관리자는 배포의 중요한 정책이 수정된 이유를 신속하게 평가할 수 있습니다. 선택적으로 감사 로그에 작성된 침입 및 네트워크 분석 정책을 변경할 수 있습니다.

## 정책 변경 추적 코멘트 구성

액세스 제어 정책, 침입 정책 또는 네트워크 분석 정책을 수정할 때 사용자에게 코멘트를 요구하도록 Firepower 시스템을 구성할 수 있습니다. 코멘트를 사용하여 사용자가 정책을 변경한 이유를 추적할 수 있습니다. 정책 변경에 대한 코멘트를 활성화하는 경우, 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 정책에 대한 새로운 변경 사항이 저장될 때마다 시스템은 사용자에게 코멘트를 입력하라는 메시지를 표시합니다.

프로시저

**단계 1 System(시스템) > Configuration(구성)을(를) 선택합니다.**

왼쪽된 탐색 패널에서 시스템 구성 옵션이 나타납니다.

**단계 2** 다음 중 하나에 대한 정책 설명 환경설정을 구성합니다.

- 액세스 제어 정책에 대한 설명 환경설정을 보려면 **Access Control Preferences**(액세스 제어 환경 설정)를 클릭합니다.
- 침입 정책에 대한 설명 환경설정을 보려면 **Intrusion Policy Preferences**(침입 정책 환경 설정)를 클릭합니다.
- 네트워크 분석 정책에 대한 설명 환경설정을 보려면 **Network Analysis Policy Preferences**(네트워크 분석 정책 환경 설정)를 클릭합니다.

**단계 3** 각 정책 유형에 대해 다음과 같은 옵션을 선택할 수 있습니다.

- **Disabled**(비활성화) - 변경 코멘트를 비활성화합니다.
- **Optional**(선택 사항) - 코멘트에서 변경 사항을 설명할 수 있는 옵션을 사용자에게 제공합니다.
- **Required**(필수) - 사용자는 저장 전에 코멘트에서 변경 사항을 설명해야 합니다.

**단계 4** 선택적 침입 또는 네트워크 분석 정책 코멘트:

- 모든 침입 정책 변경 사항을 감사 로그에 기록하려면 **Write changes in Intrusion Policy to audit log**(침입 정책의 변경 사항을 감사 로그에 쓰기)를 선택합니다.
- 모든 네트워크 분석 정책 변경 사항을 감사 로그에 기록하려면 **Write changes in Network Analysis Policy to audit log**(네트워크 분석 정책의 변경 사항을 감사 로그에 쓰기)를 선택합니다.

**단계 5 Save(저장)를 클릭합니다.**

## 액세스 목록

IP 주소 및 포트를 기준으로 FMC에 대한 액세스를 제한할 수 있습니다. 기본적으로 모든 IP 주소에 대해 다음과 같은 포트가 활성화됩니다.

- 웹 인터페이스 액세스용 443(HTTPS)
- CLI 액세스용 22(SSH)

포트 161을 통해 SNMP 정보를 폴링할 수 있는 액세스 권한을 추가할 수도 있습니다. SNMP는 기본적으로 비활성화되며, 따라서 먼저 SNMP를 활성화해야 SNMP 액세스 규칙을 추가할 수 있습니다. 자세한 내용은 [SNMP 폴링 구성, 39 페이지](#)의 내용을 참고하십시오.



주의 기본적으로 액세스는 제한되지 않습니다. 더 안전한 환경에서 작동하려면 특정 IP 주소의 액세스를 추가한 후 기본 **any** 옵션을 삭제하는 것을 고려하십시오.

## 액세스 목록 구성

이 액세스 목록은 외부 데이터베이스 액세스를 제어하지 않습니다. [데이터베이스에 대한 외부 액세스 활성화, 12 페이지](#)의 내용을 참조하십시오.



주의 FMC에 연결하기 위해 현재 사용 중인 IP 주소에 대한 액세스를 삭제하면, 'IP=any port=443'에 대한 항목은 존재하지 않으며, 저장할 때 액세스 권한을 잃게 됩니다.

클래식 디바이스에 액세스 목록을 구성하려면, 디바이스 플랫폼 설정을 사용합니다. [클래식 디바이스에 대한 액세스 목록 구성](#)의 내용을 참조하십시오.

시작하기 전에

기본적으로 액세스 목록에는 HTTPS 및 SSH에 대한 규칙이 포함됩니다. SNMP 규칙을 액세스 목록에 추가하려면 먼저 SNMP를 활성화해야 합니다. 자세한 내용은 [SNMP 폴링 구성, 39 페이지](#)를 참고하십시오.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 (선택 사항) SNMP 규칙을 액세스 목록에 추가하려면 **SNMP**를 클릭해 SNMP를 구성합니다. 기본적으로 SNMP는 비활성화되어 있습니다. 자세한 내용은 [SNMP 폴링 구성, 39 페이지](#)을 참조하십시오.

단계 3 액세스 목록을 클릭합니다.

단계 4 하나 이상의 IP 주소에 대한 액세스를 추가하려면 **Add Rules**(규칙 추가)를 클릭합니다.

단계 5 **IP** 주소 필드에 IP 주소 또는 어드레스 레인지 또는 모두를 입력하세요.

단계 6 **SSH, HTTPS, SNMP** 또는 이 옵션의 조합을 선택하여 이 IP 주소에 활성화할 포트를 지정합니다.

단계 7 **Add**(추가)를 클릭합니다.

단계 8 **Save**(저장)를 클릭합니다.

관련 항목

[Firepower System IP 주소 규칙](#)

## 감사 로그

Firepower Management Center는 사용자 활동을 읽기 전용 감사 로그로 기록합니다. 여러 가지 방법으로 감사 로그 데이터를 검토할 수 있습니다.

- 웹 인터페이스인 **시스템 감사**를 사용합니다.

감사 로그는 감사 보기의 항목을 기준으로 감사 로그 메시지를 보고, 정렬하고, 필터링할 수 있는 표준 이벤트 보기에서 제공됩니다. 감사 정보를 손쉽게 삭제하고 보고할 수 있으며, 사용자가 변경한 내용에 대한 자세한 보고서를 볼 수 있습니다.

- 시스템 로그.
- HTTP 서버인에 감사 로그 메시지를 스트리밍합니다.

외부 서버로 감사 로그 메시지를 스트리밍하면 FMC의 공간을 절약할 수 있습니다. [감사 로그 스트리밍 구성, 33 페이지](#) 섹션을 참조하십시오.

여러 시스템 로그 서버로 스트리밍

감사 로그 데이터를 최대 5개의 시스템 로그 서버로 스트리밍할 수 있습니다. 그러나 보안 감사 로그 스트리밍에 대해 TLS를 활성화한 경우, 단일 시스템 로그 서버로만 스트리밍할 수 있습니다.

또한 클래식 디바이스의 감사 로그를 유지합니다. 클래식 디바이스에서 감사 로그를 스트리밍하는 방법은 [클래식 디바이스에서의 감사 로그 스트리밍](#) 섹션을 참조하십시오.

## 감사 로그 스트리밍 구성

다음은 출력 구조의 예입니다.

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

로컬 날짜, 시간 및 호스트 이름이 괄호로 묶인 선택적 태그 앞에 오는 경우, 그리고 발신 디바이스 이름이 감사 로그 메시지 앞에 오는 경우

예를 들면 다음과 같습니다.

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3500: admin@10.1.1.2, Operations > Monitoring, Page View
```

시작하기 전에

- 외부 호스트가 작동해야 하며 감사 로그를 보내는 시스템에서 액세스할 수 있어야 합니다.

프로시저

**단계 1** **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

**단계 2** **Audit Log**(로그 감사)를 클릭합니다.

단계 3 **Enabled(활성화)**를 **Send Audit Log to Syslog(감사 로그를 시스템 로그로 전송)** 드롭다운 메뉴에서 선택합니다.

단계 4 IP 주소를 사용하여 감사 정보에 대한 대상 호스트를 지정하거나 **Host(호스트)** 필드에 호스트의 FQDN(Fully Qualified Domain Name)을 지정합니다. 기본 포트(514)가 사용됩니다.

주의 감사 로그를 수신하도록 구성된 컴퓨터가 원격 메시지를 수락하도록 설정되지 않은 경우, 호스트에서 감사 로그를 허용하지 않습니다.

단계 5 시스템 로그 **Facility(시설)**를 선택합니다.

단계 6 **Severity(심각도)**를 선택합니다.

단계 7 또는, **Tag(태그)(선택 사항)** 필드에 참조 태그를 삽입합니다.

단계 8 외부 HTTP 서버에 정기 감사 로그 업데이트를 전송하려면 **Enabled(활성화)**를 **Send Audit Log to HTTP Server(HTTP 서버에 감사 로그 전송)** 드롭다운 메뉴에서 선택합니다.

단계 9 **URL to Post Audit(사후 감사 URL)** 필드에서 감사 정보를 전송할 URL을 지정합니다. 다음과 같이 나열된 대로 HPPT POST 변수를 기대하는 listener 프로그램에 해당하는 URL을 입력해야 합니다.

- subsystem
- actor
- event\_type
- message
- action\_source\_ip
- action\_destination\_ip
- result
- 시간
- tag(위와 같이 정의된 경우)

주의 암호화된 게시물을 허용하려면, HTTPS URL을 사용해야 합니다. 외부 URL에 감사 정보를 보내면 시스템 성능에 영향을 미칠 수 있음에 유의하십시오.

단계 10 **Save(저장)**를 클릭합니다.

## 대시보드 설정

대시보드는 Firepower System의 여러 부분에 대한 통찰력을 제공하는 소규모의 자족적 구성 요소인 위젯을 사용하여 현재 시스템 상태에 대한 간략한 보기를 제공합니다. Firepower System은 여러 대시보드 위젯이 사전 정의된 상태로 제공됩니다.

맞춤형 분석 위젯이 대시보드에서 활성화되도록 Firepower Management Center를 구성할 수 있습니다.

관련 항목

[대시보드 정보](#)

## 대시보드에 대한 맞춤형 분석 위젯 활성화

맞춤형 분석 대시보드 위젯을 사용하여 유연하고 사용자가 구성할 수 있는 쿼리를 기반으로 이벤트를 시각적으로 표현할 수 있습니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Dashboard**(대시보드)를 클릭합니다.

단계 3 사용자가 Custom Analysis 위젯을 대시보드에 추가하도록 허용하려면 **Enable Custom Analysis Widgets**(맞춤형 분석 위젯 활성화) 확인란을 선택합니다.

단계 4 **Save**(저장)를 클릭합니다.

## DNS 캐시

이벤트 보기 페이지에서 자동으로 IP 주소를 확인하도록 시스템을 구성할 수 있습니다. 어플라이언스가 수행하는 DNS 캐싱의 기본 등록 정보를 구성할 수도 있습니다. DNS 캐싱을 구성하면 추가 조회를 수행하지 않고도 전에 확인한 IP 주소를 식별할 수 있습니다. 이렇게 하면 네트워크의 트래픽 양을 줄이고, IP 주소 확인이 활성화된 경우 이벤트 페이지의 표시 속도를 높일 수 있습니다.

## DNS 캐시 속성 설정

DNS 확인 캐싱은 전에 확인된 DNS 조회의 캐싱을 허용하는 시스템 전체의 설정입니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **DNS Cache**(DNS 캐시)를 선택합니다.

단계 3 **DNS Resolution Caching**(DNS 확인 캐싱) 드롭다운 목록에서 다음 중 하나를 선택합니다.

- **Enabled**(활성화) - 캐싱을 활성화합니다.
- **Disabled**(비활성화) - 캐싱을 비활성화합니다.

단계 4 DNS 항목이 제거되어 비활성화되기 전 메모리에 캐시되어 머무는 시간(분)을 **DNS Cache Timeout (in minutes)** 필드에 입력합니다.

기본 설정은 300분(5시간)입니다.

단계 5 **Save**(저장)를 클릭합니다.

관련 항목

[이벤트 보기 구성](#)

## 이메일 공지

다음을 수행하려는 경우 메일 호스트를 구성합니다.

- 이벤트 기반 보고서 이메일 전송
- 예약 작업에 대한 상태 보고서 이메일 전송
- 변경 검증 보고서 이메일 전송
- 데이터 정리 알림 이메일 전송
- 검색 이벤트, 영향 플래그, 상관 이벤트 알림, 침입 이벤트 알림 및 상태 이벤트 알림에 이메일 사용

이메일 알림을 구성할 때 시스템과 메일 릴레이 호스트 간 통신을 위한 암호화 방법을 선택할 수 있고 필요한 경우 메일 서버의 인증 자격 증명을 제공할 수 있습니다. 구성한 후 연결을 테스트할 수 있습니다.

## 메일 릴레이 호스트 및 알림 주소 구성

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을 선택합니다.

단계 2 **Email Notification**(이메일 알림)을 클릭합니다.

단계 3 **Mail Relay Host**(메일 릴레이 호스트) 필드에서 사용할 메일 서버의 호스트 이름 또는 IP 주소를 입력합니다. 입력한 메일 호스트는 어플라이언스의 액세스를 허용해야 합니다.

단계 4 **Port Number**(포트 번호) 필드에 이메일 서버에서 사용할 포트 번호를 입력합니다.

일반적인 포트는 다음과 같습니다.

- 25: 암호화를 사용하지 않는 경우
- 465: SSLv3를 사용하는 경우
- 587: TLS를 사용하는 경우

단계 5 **Encryption**(암호화) 방법을 선택합니다.

- **TLS**-전송 계층 보안을 사용하여 통신을 암호화합니다
- **SSLv3-Secure Socket Layer**를 사용하여 통신을 암호화 합니다.

- **None** (없음)-암호화 되지 않은 통신을 허용 합니다.

참고 Certificate validation is not required for encrypted communication between the appliance and mail server.

- 단계 6 In the **From Address** field, enter the valid email address you want to use as the source email address for messages sent by the appliance.
- 단계 7 Optionally, to supply a user name and password when connecting to the mail server, choose **Use Authentication**. **Username**(사용자 이름) 필드에 사용자 이름을 입력합니다. **Password**(비밀번호) 필드에 비밀번호를 입력합니다.
- 단계 8 구성된 메일 서버를 사용하는 테스트 이메일을 전송하려면 **Test Mail Server Settings**(메일 서버 설정 테스트)를 클릭합니다.
- 테스트의 성공 또는 실패를 나타내는 메시지가 버튼 옆에 나타납니다.
- 단계 9 **Save**(저장)를 클릭합니다.

## 언어 선택

웹 인터페이스에 대해 다른 언어를 지정하려면 **Language** 페이지를 사용할 수 있습니다.

## 웹 인터페이스의 언어 설정

여기서 지정하는 언어는 모든 사용자에게 대한 웹 인터페이스에 사용됩니다. 다음 항목을 선택할 수 있습니다.

- 영어
- 일본어

7000/8000 시리즈 디바이스의 언어를 설정하려면 디바이스 플랫폼 설정인 **7000/8000 시리즈 웹 인터페이스 언어 설정**을(를) 사용합니다.

프로시저

- 단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.
- 단계 2 **Language**를 클릭합니다.
- 단계 3 사용하려는 언어를 선택합니다.
- 단계 4 **Save**(저장)를 클릭합니다.

## 로그인 배너

**Login Banner**(로그인 배너) 페이지를 사용하여 보안 어플라이언스 또는 공유 정책에 대한 세션, 로그인 또는 사용자 정의 메시지 배너를 지정할 수 있습니다.

ASCII 문자와 캐리지 리턴을 사용하여 사용자 정의 로그인 배너를 만들 수 있습니다. 시스템은 탭 간격을 유지하지 않습니다. 로그인 배너가 너무 크거나 오류가 발생하면 시스템에서 배너를 표시하려고 시도할 때 텔넷 또는 SSH 세션이 실패할 수 있습니다.

## 로그인 배너 사용자 지정

클래식 디바이스의 로그인 배너를 사용자 정의하려면, 디바이스 플랫폼 설정을 사용합니다. [클래식 디바이스에 대한 로그인 배너 맞춤 설정](#)의 내용을 참조하십시오.

프로시저

---

단계 **1 System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 **2 Login Banner**(로그인 배너)를 선택합니다.

단계 **3 Custom Login Banner**(사용자 정의 로그인 배너\_ 필드에서 사용하려는 로그인 배너 텍스트를 입력합니다.

단계 **4 Save**(저장)를 클릭합니다.

---

## SNMP 폴링

SNMP(Simple Network Management Protocol) 폴링을 활성화할 수 있습니다. 이 기능은 SNMP 프로토콜의 1, 2, 3 버전 사용을 지원합니다. 이 기능을 이용하면 연락처, 관리, 위치, 서비스 정보, IP 주소 지정 및 라우팅 정보, 전송 프로토콜 사용 통계 등의 시스템 세부사항을 포함하는 표준 MIB(management information base)에 액세스할 수 있습니다.




---

**참고** SNMP 프로토콜을 위한 SNMP 버전을 선택하는 경우, SNMPv2는 일기 전용 커뮤니티만 지원하며 SNMPv3는 읽기 전용 사용자만 지원한다는 사실을 유념하십시오. SNMPv3는 AES128을 이용한 암호화도 지원합니다.

---

SNMP 폴링을 활성화한다고 해서 시스템에서 SNMP 트랩을 전송하지는 않습니다. MIB의 정보를 네트워크 관리 시스템을 통한 폴링에 사용할 수 있도록 지원할 뿐입니다.

## SNMP 폴링 구성

클래식 매니지드 디바이스에서 SNMP 폴링을 구성하려면, 디바이스 플랫폼 설정을 사용합니다. [클래식 디바이스에서의 SNMP 폴링 구성](#)의 내용을 참조하십시오.

시작하기 전에

시스템 폴링에 사용할 각 컴퓨터에 대해 SNMP 액세스를 추가합니다. [액세스 목록 구성, 32 페이지](#)의 내용을 참조하십시오.



**참고** SNMP MIB에는 구축을 공격하는 데 사용할 수 있는 정보가 있습니다. Cisco에서는 MIB를 폴링하는 데 사용하는 특정 호스트에 대한 SNMP 액세스용 액세스 목록을 제한할 것을 권장합니다. 또한 SNMPv3을 사용하고 네트워크 관리 액세스에 강력한 비밀번호를 사용할 것도 권장합니다.

프로시저

- 단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.
- 단계 2 **SNMP**를 클릭합니다.
- 단계 3 **SNMP Version**(SNMP 버전) 드롭다운 목록에서, 사용할 SNMP 버전을 선택합니다.
  - **Version**(버전) 1 또는 **Version**(버전) 2: 커뮤니티 문자열 필드에 읽기 전용 SNMP 커뮤니티 이름을 넣고 절차 종료로 건너뛩니다.
    - 참고 SNMP 커뮤니티 문자열 이름에는 특수문자(<>/%#&'?, 등)를 포함하지 않습니다.
  - **Version 3**(버전 3): **Add User**(사용자 추가)를 클릭하여 사용자 정의 페이지를 표시합니다. SNMPv3는 읽기 전용 사용자 및 AES128 암호화만 지원합니다.
- 단계 4 사용자 이름을 입력합니다.
- 단계 5 **Authentication Protocol**(인증 프로토콜) 드롭다운 목록에서 인증에 사용할 프로토콜을 선택합니다.
- 단계 6 **Authentication Password**(인증 비밀번호) 필드에 SNMP 서버와 함께 인증에 필요한 비밀번호를 입력합니다.
- 단계 7 **Verify Password**(비밀번호 확인) 필드에 인증 비밀번호를 다시 입력합니다.
- 단계 8 사용할 비공개 프로토콜을 **Privacy Protocol** 목록에서 선택하거나, 비공개 프로토콜을 사용하지 않으려면 **None**을 선택합니다.
- 단계 9 **Privacy Password**(프라이버시 비밀번호) 필드에 SNMP 서버에 필요한 SNMP 프라이버시 키를 입력합니다.
- 단계 10 **Verify Password**(비밀번호 확인) 필드에 프라이버시 비밀번호를 다시 입력합니다.
- 단계 11 **Add**(추가)를 클릭합니다.
- 단계 12 **Save**(저장)를 클릭합니다.

## STIG 컴플라이언스

미국 연방 정부 내 기구는 경우에 따라 Security Technical Implementation Guides(보안 기술 구현 가이드, STIG)에 정리된 일련의 보안 검사 목록을 준수해야 합니다. Firepower는 미국 국방부가 수립한 STIG 요구 사항을 준수하도록 지원합니다.

구축의 어플라이언스에서 STIG 컴플라이언스를 활성화하는 경우 모든 어플라이언스에서 활성화해야 합니다. 비준수 매니지드 디바이스는 STIG 준수 Firepower Management Center에 등록할 수 없으며 STIG 준수 디바이스는 비준수 FMC에 등록할 수 없습니다.

STIG 규정 준수를 활성화해도 적용 가능한 모든 STIG에 대한 엄격한 규정 준수가 보장되지는 않습니다.

STIG 규정 준수를 활성화할 경우, 로컬 셸 액세스 계정의 비밀번호 복잡성 및 보관 규칙이 변경됩니다. 또한, STIG 준수 모드에서는 SSH 원격 스토리지를 사용할 수 없습니다.



주의 Cisco TAC의 도움 없이 이 설정을 비활성화해선 안 됩니다. 또한, 이 설정은 사용자 시스템의 성능에 상당한 영향을 줄 수 있습니다. Cisco에서는 국방부 보안 요구 사항 준수 이외에는 STIG 준수의 활성화를 권장하지 않습니다.

## STIG 컴플라이언스 활성화

이 구성은 Firepower Management Center 또는 기본 매니지드 디바이스(7000 및 8000 Series, ASA FirePOWER 및 NGIPSv)에 적용됩니다.

- Firepower Management Center의 경우 이 구성은 시스템 구성에 포함되어 있습니다.
- 기본 매니지드 디바이스의 경우, Firepower Management Center의 이 구성을 플랫폼 설정 정책의 일부로 적용합니다.

두 경우 모두, 시스템 구성 변경 사항을 저장하거나 공유 플랫폼 설정 정책을 구축할 때까지 구성이 적용되지 않습니다.



주의 구축의 어플라이언스에서 STIG 컴플라이언스를 활성화하는 경우 모든 어플라이언스에서 활성화해야 합니다. Support(지원팀)의 도움 없이는 이 설정을 비활성화할 수 없습니다. 또한, 이 설정은 사용자 시스템의 성능에 상당한 영향을 줄 수 있습니다. Cisco에서는 국방부 보안 요구 사항을 준수하는 경우 외에는 STIG 컴플라이언스를 활성화하지 않을 것을 권장합니다.

프로시저

단계 1 Firepower Management Center 또는 기존 매니지드 디바이스를 구성하는지 여부에 따라 다음 작업을 수행합니다.

- FMC - **System**(시스템) > **Configuration**(구성)을 선택합니다.
- 매니지드 디바이스 - **Devices**(디바이스) > **Platform Settings**(플랫폼 설정)를 선택하고 Firepower 정책을 생성하거나 수정합니다.

단계 2 **STIG Compliance**(STIG 준수)를 클릭합니다.

참고 STIG 컴플라이언스를 활성화하는 경우 어플라이언스가 재부팅됩니다. 시스템 구성을 저장할 때 Firepower Management Center가 재부팅됩니다. 매니지드 디바이스는 구성 변경 사항을 구축할 때 재부팅됩니다.

단계 3 어플라이언스에서 STIG 컴플라이언스를 영구적으로 활성화하려는 경우, **Enable STIG Compliance**(STIG 컴플라이언스 활성화)를 선택합니다.

단계 4 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.
- 어플라이언스가 5.2.0 이전 버전에서 업데이트된 경우, STIG 컴플라이언스를 활성화하면 어플라이언스 인증서가 다시 생성됩니다. 구축 전체에서 STIG 컴플라이언스를 활성화한 후 매니지드 디바이스를 Firepower Management Center에 다시 등록합니다.

## 시간 및 시간 동기화

Firepower Management Center(FMC)와 매니지드 디바이스에서 시스템 시간을 동기화하는 작업은 Firepower System의 성공적인 작업을 위해 반드시 필요합니다. Cisco에서는 FMC 초기 구성 중에 NTP 서버를 지정할 것을 권장하지만, 초기 구성이 끝난 후 이 섹션의 정보를 이용해 시간 동기화 설정을 구성하거나 변경할 수 있습니다.

FMC 및 모든 디바이스에서 시스템 시간을 동기화하려면 NTP(Network Time Protocol) 서버를 사용합니다. FMC는 MD5 또는 SHA-1 대칭 키 인증을 통해 NTP 서버와의 안전한 통신을 지원합니다. Cisco에서는 시스템 보안을 위해 이 기능을 사용하도록 권장합니다.

또한 인증된 NTP 서버에만 연결하도록 FMC를 구성할 수도 있습니다. 혼합 인증 환경을 이용 중이거나 시스템을 다른 NTP 서버로 마이그레이션할 때 이 옵션을 이용하면 보안을 강화할 수 있습니다. 연결 가능한 모든 NTP 서버가 인증된 환경에서 이 설정을 사용하는 것은 중복 행위입니다.



참고 초기 구성 중에 FMC에 NTP 서버를 지정하면, 해당 NTP 서버와의 연결은 보호되지 않습니다. 연결이 MD5 또는 SHA-1 키를 지정하도록 설정을 편집해야 합니다.



주의 시간이 FMC 및 매니지드 디바이스 간에 동기화되지 않으면 의도하지 않은 결과가 발생할 수 있습니다.

FMC 및 매니지드 디바이스의 시간을 동기화하는 방법은 다음을 참조하십시오.

- 권장: [FMC의 시간을 NTP 서버와 동기화, 42 페이지](#)

이 주제에서는 FMC를 NTP 서버 또는 서버와 동기화하도록 설정하는 데 필요한 지침을 제공하며, 동일한 NTP 서버와 동기화하도록 매니지드 디바이스를 설정하는 방법을 안내하는 링크를 제공합니다.

- 그렇지 않을 경우, [네트워크 NTP 서버에 액세스하지 않고 시간 동기화, 43 페이지](#)

이 주제에서는 FMC에서 시간을 설정하고 NTP 서버 역할을 하도록 FMC를 설정하는 방법에 대한 지침과 FMC NTP 서버와 동기화하도록 매니지드 디바이스를 설정하는 지침으로 연결되는 링크를 제공합니다.

## FMC의 시간을 NTP 서버와 동기화

시스템의 모든 구성 요소 간의 시간 동기화는 매우 중요합니다.

Firepower Management Center 및 모든 매니지드 디바이스 간의 적절한 시간 동기화를 보장하는 가장 좋은 방법은 네트워크에서 NTP 서버를 사용하는 것입니다.

FMC은(는) NTPv4를 지원합니다.

이 절차를 수행하려면 관리자 또는 네트워크 관리자 권한이 있어야 합니다.

시작하기 전에

다음에 유의하십시오.

- FMC 및 매니지드 디바이스가 네트워크 NTP 서버에 액세스할 수 없다면 이 절차를 사용하지 마십시오. 대신 [네트워크 NTP 서버에 액세스하지 않고 시간 동기화, 43 페이지](#) 섹션을 참조하십시오.
- 신뢰할 수 없는 NTP 서버를 지정하지 마십시오.
- (시스템 보안 상 권장되는) NTP 서버와의 보안 연결을 설정하려면, 해당 NTP 서버에 설정된 SHA-1 또는 MD5 키 번호 및 값을 얻어야 합니다.
- NTP 서버에 대한 연결에는 구성된 프록시 설정이 사용되지 않습니다.
- Firepower 4100 시리즈 디바이스 및 Firepower 9300 디바이스는 이 절차를 사용하여 시스템 시간을 설정할 수 없습니다. 대신 이 절차를 사용하여 설정한 것과 동일한 NTP 서버를 사용하도록 해당 디바이스를 설정합니다. 자세한 내용은 하드웨어 모델의 설명서를 참조하십시오.



주의 Firepower Management Center가 재부팅되고 DHCP 서버가 NTP 서버 레코드를 여기에 지정된 것과 다르게 설정하는 경우 DHCP 제공 NTP 서버가 대신 사용됩니다. 이 상황을 피하려면 DHCP 서버를 동일한 NTP 서버를 사용하게 설정하십시오.

프로시저

- 단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.
- 단계 2 **Time Synchronization**(시간 동기화)을 클릭합니다.
- 단계 3 **Serve Time via NTP**(NTP를 통해 시간 제공)가 **Enabled**(활성화됨)인 경우라면, **Disabled**(비활성화됨)를 선택해 FMC을(를) NTP 서버로 비활성화합니다.
- 단계 4 **Set My Clock**(내 시계 설정) 옵션에서 **Via NTP**(NTP를 통해)를 선택합니다.
- 단계 5 **Add**(추가)를 클릭합니다.
- 단계 6 **Add NTP Server**(NTP 서버 추가) 대화상자에 NTP 서버의 호스트 이름, IPv4 또는 IPv6 주소를 입력합니다.
- 단계 7 (선택 사항) FMC 및 NTP 서버 간의 통신을 보호하려면 다음을 수행합니다.
  - a) **Key Type**(키 유형) 드롭다운 목록에서 **MD5** 또는 **SHA-1**을 선택합니다.
  - b) 지정된 NTP 서버에서 해당 MD5 또는 SHA-1 키 번호와 키 값을 입력합니다.
- 단계 8 **Add**(추가)를 클릭합니다.
- 단계 9 다른 NTP 서버를 추가하려면 5~8 단계를 반복합니다.
- 단계 10 (선택 사항) FMC에서 인증에 성공한 NTP 서버만 사용하게 하려면, **Use the authenticated NTP server only**(인증된 NTP 서버만 사용) 확인란을 선택합니다.
- 단계 11 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

다음과 같이 매니지드 디바이스를 동일한 NTP 서버나 서버 모음과 동기화되도록 설정합니다.

- 디바이스 플랫폼 설정인 **Threat Defense**를 위한 **NTP 시간 동기화 구성** 및 **NTP 서버와 클래식 디바이스의 시간 동기화**을(를) 구성합니다.

FMC가 NTP 서버와 보안 연결을 구성하도록 강제하더라도(인증된 NTP 서버만 사용), 해당 서버에 대한 디바이스 연결은 인증을 사용하지 않습니다.

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

## 네트워크 NTP 서버에 액세스하지 않고 시간 동기화

디바이스에서 네트워크 NTP 서버에 직접 연결할 수 없는 경우 또는 조직에 네트워크 NTP 서버가 없는 경우, 물리적 하드웨어 Firepower Management Center가 NTP 서버 역할을 수행할 수 있습니다.



- 중요
- 다른 NTP 서버가 없는 경우가 아니면 이 절차를 사용하지 마십시오. 대신 [FMC의 시간을 NTP 서버와 동기화, 42 페이지](#)의 절차를 사용하십시오.
  - 가상 Firepower Management Center를 NTP 서버로 사용하지 마십시오.

Firepower Management Center를 NTP 서버로 설정한 후 수동으로 시간을 변경하려면 NTP 옵션을 비활성화하고 수동으로 시간을 변경한 다음 NTP 옵션을 다시 활성화해야 합니다.

#### 프로시저

단계 1 다음과 같이 Firepower Management Center에서 시스템 시간을 수동으로 설정합니다.

- a) **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.
- b) **Time Synchronization**(시간 동기화)을 클릭합니다.
- c) **Serve Time via NTP**(NTP를 통해 시간 제공)가 **Enabled**(활성화됨)인 경우 **Disabled**(비활성화됨)를 선택합니다.
- d) **Save**(저장)를 클릭합니다.
- e) **Set My Clock**(내 클릭 설정)에서 **Manually in Local Configuration**(로컬 구성에서 수동으로)을 선택합니다.
- f) **Save**(저장)를 클릭합니다.
- g) 화면 왼쪽 탐색 패널에서 **Time**(시간)을 클릭합니다.
- h) **Set Time**(시간 설정) 드롭다운 목록을 사용하여 시간을 설정합니다.
- i) 표시된 표준 시간대가 UTC가 아닌 경우, 이를 클릭하고 표준 시간대를 **UTC**로 설정합니다.
- j) **Save**(저장)를 클릭합니다.
- k) **Done**(완료)을 클릭합니다.
- l) **Apply**(적용)를 클릭합니다.

단계 2 다음과 같이 Firepower Management Center가 NTP 서버 역할을 하도록 설정합니다.

- a) 화면 왼쪽 탐색 패널에서 **Time Synchronization**(시간 동기화)을 클릭합니다.
- b) **Serve Time via NTP**(NTP를 통해 시간 제공)에 대해 **Enabled**(활성화됨)를 선택합니다.
- c) **Save**(저장)를 클릭합니다.

단계 3 다음과 같이 매니지드 디바이스를 Firepower Management Center NTP 서버와 동기화되도록 설정합니다.

- a) 매니지드 디바이스에 할당된 플랫폼 설정 정책에 대한 Time Synchronization(시간 동기화) 설정에서 **Via NTP from Management Center**(Management Center에서 NTP를 통해)를 사용하여 동기화하도록 클릭을 설정합니다.
- b) 매니지드 디바이스에 변경 사항을 구축합니다.

지침은 다음 내용을 참조하십시오.

[NTP 서버와 클래식 디바이스의 시간 동기화](#)의 내용을 참조하십시오.

## 시간 동기화 설정 변경 정보

- Firepower Management Center 및 매니지드 디바이스는 주로 정확한 시간에 의존합니다. 시스템 시계는 Firepower System의 시간을 유지하는 시스템 기능입니다. 시스템 시계는 전 세계가 시계와 시간을 규제하는 기본 시간 기준인 UTC(Universal Coordinated Time)로 설정됩니다.  
시스템 시간을 변경하지 마십시오. UTC 시스템 시간 변경은 지원되지 않으며, 변경할 경우 지원되지 않는 상태에서 복구하기 위해 디바이스 이미지를 다시 생성해야 합니다.
- NTP를 사용하여 시간을 서비스하도록 FMC를 구성한 다음 나중에 이를 비활성화하면, 매니지드 디바이스의 NTP 서비스는 계속해서 FMC와 시간을 동기화하려고 시도합니다. 새 시간 소스를 설정하려면 해당 플랫폼 설정 정책을 업데이트하고 다시 구축해야 합니다.
- Firepower Management Center를 NTP 서버로 설정한 후 수동으로 시간을 변경하려면 NTP 옵션을 비활성화하고 수동으로 시간을 변경한 다음 NTP 옵션을 다시 활성화해야 합니다.

## 현재 시스템 시간, 소스 및 NTP 서버 연결 상태 보기

시간 설정이 대부분의 페이지에서 로컬 시간으로 표시됩니다. 여기서 사용되는 시간대는 User Preferences(사용자 환경 설정)의 Time Zone(표준 시간대) 페이지에서 설정하며(기본값은 미국/뉴욕), UTC 시간을 사용해 어플라이언스에 저장합니다.



### 제한

Time Zone(표준 시간대) 기능(User Preferences(사용자 환경 설정))에서는 기본 시스템 시계가 UTC 시간으로 설정되었다고 가정합니다. 시스템 시간을 변경하지 마십시오. UTC 시스템 시간 변경은 지원되지 않으며, 그러할 경우 지원되지 않는 상태에서 복구하기 위해 디바이스 이미지를 다시 생성해야 합니다.



### 참고

7000 및 8000 하드웨어 디바이스에 대한 시간 및 시간 소스 정보를 보는 방법은 [7000/8000 시리즈 디바이스의 시스템 시간 보기](#) 섹션을 참조하십시오.

### 프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Time**(시간)을 클릭합니다.

현재 시간은 사용자 기본 설정에서 계정에 지정된 표준 시간대를 사용하여 표시됩니다.

어플라이언스에서 NTP 서버를 사용하는 경우: 테이블 항목에 대한 자세한 내용은 [NTP 서버 상태, 46 페이지](#) 섹션을 참조하십시오.

## NTP 서버 상태

NTP 서버에서 시간을 동기화한다면, **Time(시간)** 페이지에서 연결 상태를 볼 수 있습니다(**System(시스템) > Configuration(구성)**선택).

표 5: NTP 상태

열	설명
NTP 서버	구성된 NTP 서버의 IP 주소 및 이름.
상태	<p>NTP 서버 시간 동기화의 상태:</p> <ul style="list-style-type: none"> <li>• <b>Being Used(사용 중)</b> - 어플라이언스가 NTP 서버와 동기화됨을 나타냅니다.</li> <li>• <b>Available(사용 가능)</b> - NTP 서버를 사용할 수 있지만 시간이 아직 동기화되지 않았음을 나타냅니다.</li> <li>• <b>Not Available(사용 불가)</b> - NTP 서버가 설정에 있지만 NTP 디먼이 이를 사용할 수 없음을 나타냅니다.</li> <li>• <b>Pending(보류 중)</b> - NTP 서버가 새로운 것이거나 NTP 디먼이 최근에 다시 시작되었음을 나타냅니다. 시간 경과에 따라 값이 <b>Being Used(사용 중)</b>, <b>Available(사용 가능)</b> 또는 <b>Not Available(사용 불가)</b>로 변경됩니다.</li> <li>• <b>Unknown(알 수 없음)</b> - NTP 서버의 상태를 알 수 없음을 나타냅니다.</li> </ul>
인증	<p>FMC 및 NTP 서버 간의 통신에 대한 인증 상태입니다.</p> <ul style="list-style-type: none"> <li>• <b>none(없음)</b>은 인증을 구성하지 않았다는 뜻입니다.</li> <li>• <b>bad(불량)</b>은 인증을 구성했지만 실패했다는 뜻입니다.</li> <li>• <b>ok(양호)</b>는 인증에 성공했다는 뜻입니다.</li> </ul> <p>인증을 구성했다면, 시스템은 상태 값 다음에 키 번호와 키 유형(SHA-1 또는 MD5)을 표시합니다. 예: <b>bad, key 2, MD5</b>.</p>
Offset(오프셋)	어플라이언스 및 구성된 NTP 서버 간 밀리초 단위의 시간 차이. 음수 값은 어플라이언스가 NTP 서버 뒤에 있음을 나타내고, 양수 값은 그 반대를 나타냅니다.
마지막 업데이트	시간이 NTP 서버와 마지막으로 동기화된 후 경과한 기간(초). NTP 디먼은 몇 가지 조건을 기반으로 동기화 시간을 자동으로 조정합니다. 예를 들어 300초와 같이 업데이트 시간이 좀 더 긴 경우, 이는 시간이 비교적 안정적이며 NTP 디먼이 더 낮은 업데이트 증분을 사용할 필요가 없다고 결정했음을 나타냅니다.

## 전역 사용자 구성

전역 사용자 구성 설정은 Firepower Management Center에 있는 모든 사용자에게 영향을 줍니다. User Configuration(사용자 구성) 페이지(**System(시스템) > Configuration(설정) > User Configuration(사용자 설정)**)에서 이러한 설정을 구성합니다.

- **Password Reuse Limit(비밀번호 재사용 한도)**: 재사용할 수 없는 사용자의 최근 기록에 있는 비밀번호 수입니다. 이 제한은 모든 사용자의 웹 인터페이스 액세스에 적용됩니다. 관리자 사용자의 경우 이는 CLI 액세스에도 적용됩니다. 시스템은 각 액세스 형식에 대해 별도의 비밀번호 목록을 유지합니다. 한도를 0(기본값)으로 설정하면 비밀번호 재사용에 대한 제한이 없습니다. **비밀번호 재사용 한도 설정, 48 페이지**의 내용을 참조하십시오.
- **Track Successful Logins(성공적인 로그인 추적)**: 시스템이 사용자별, 액세스 방법별(웹 인터페이스 또는 CLI)로 Firepower Management Center에 대한 성공적인 로그인을 추적하는 일수입니다. 사용자가 로그인하면 사용 중인 인터페이스에 대한 로그인 성공 횟수가 표시됩니다. **Track Successful Logins(성공적인 로그인 추적)**가 0으로 설정되면(기본값) 시스템은 로그인 활동을 추적하거나 보고하지 않습니다. **성공적인 로그인 추적, 48 페이지**의 내용을 참조하십시오.
- **Max Number of Login Failures(최대 로그인 실패 횟수)**: 시스템이 구성 가능한 시간 동안 계정 액세스를 일시적으로 차단하기 전에 사용자가 잘못된 웹 인터페이스 로그인 자격 증명을 연속적으로 입력할 수 있는 횟수입니다. 임시 잠금이 적용되는 동안 사용자가 로그인 시도를 계속하는 경우:
  - 시스템은 사용자에게 임시 잠금이 적용되었음을 알리지 않고 해당 계정에 대한 액세스(유효한 비밀번호 포함)를 거부합니다.
  - 시스템은 로그인 시도가 있을 때마다 해당 계정의 로그인 실패 횟수를 계속 누적합니다.
  - 사용자가 개별 User Configuration(사용자 구성) 페이지에서 해당 계정에 대해 구성된 **Maximum Number of Failed Logins(최대 실패 로그인 횟수)**를 초과하면 관리자 사용자가 다시 활성화할 때까지 계정이 잠깁니다.
- **Set Time in Minutes to Temporarily Lockout Users(사용자에 대한 임시 잠금 시간(분) 설정)**: **Maximum Number of Failed Logins(최대 실패 로그인 횟수)**가 0이 아닌 경우 임시 웹 인터페이스 사용자 잠금 기간(분)입니다.
- **Max Concurrent Sessions Allowed(허용되는 최대 동시 세션 수)**: 동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 세션 수입니다. 세션 유형은 사용자에게 할당된 역할을 기준으로 결정됩니다. 사용자에게 읽기 전용 역할만 할당되었다면, 해당 사용자의 세션은 (읽기 전용) 세션 제한 수에 적용됩니다. 사용자에게 쓰기 권한을 제공하는 역할이 있다면, 세션은 읽기/쓰기 세션 제한 수에 적용됩니다. 예를 들어 사용자에게 관리자 역할이 할당되고 **Maximum sessions for users with Read/Write privileges/CLI users(읽기/쓰기 권한이 있는 사용자/CLI 사용자의 최대 세션 수)**를 5로 설정했다면, 사용자는 읽기/쓰기 권한이 있는 다른 사용자 5명이 로그인한 상태에서 서는 로그인할 수 없습니다.



**참고** 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할과 맞춤형 사용자 역할은 **System(시스템) > Users(사용자) > Users(사용자)** 및 **System(시스템) > Users(사용자) > User Roles(사용자 역할)**의 역할 이름에 (읽기 전용)이라고 표시됩니다. 사용자 역할의 역할 이름에 (읽기 전용)이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다. 시스템은 (읽기 전용)을 필수 기준을 충족하는 역할에 자동으로 적용합니다. 텍스트 문자열을 역할 이름에 수동으로 추가하는 방법으로는 역할을 읽기 전용을 만들 수 없습니다.

각 세션 유형에 대해 1~1024 범위의 최대 제한을 설정할 수 있습니다. **Max Concurrent Sessions Allowed**(허용되는 최대 동시 세션)을 0(기본값)으로 설정하면, 동시 세션 수는 무제한이 됩니다.

동시 세션 제한을 더 제한적인 값으로 변경하면, 시스템은 현재 열린 세션을 닫지는 않습니다. 대신 지정된 숫자 이상의 신규 세션이 열리지 않게 합니다.

## 비밀번호 재사용 한도 설정

**Password Reuse Limit**(비밀번호 재사용 한도)을 활성화하면 시스템은 FMC 사용자에게 대한 암호화된 비밀번호 기록을 유지합니다. 사용자는 기록에 있는 비밀번호는 다시 사용할 수 없습니다. 액세스 방법(웹 인터페이스 또는 CLI)별로 각 사용자에게 대해 저장된 비밀번호 수를 지정할 수 있습니다. 사용자의 현재 비밀번호도 이 숫자에 적용됩니다. 한도를 낮추면 시스템은 기록에서 이전 비밀번호를 삭제합니다. 한도를 늘려도 삭제된 비밀번호는 복원되지 않습니다.

### 프로시저

단계 1 **System(시스템) > Configuration(구성)**을(를) 선택합니다.

단계 2 **User Configuration(사용자 구성)**을 클릭합니다.

단계 3 **Password Reuse Limit(비밀번호 재사용 한도)**을 기록에서 유지할 비밀번호 수(최대 256)로 설정합니다.

비밀번호 재사용 검사를 비활성화하려면 0을 입력합니다.

단계 4 **Save(저장)**를 클릭합니다.

## 성공적인 로그인 추적

이 절차를 사용하면 지정된 일수 동안 각 사용자에게 대해 성공적인 로그인을 추적할 수 있습니다. 이 추적을 활성화하면 사용자가 웹 인터페이스 또는 CLI에 로그인할 때 로그인 성공 횟수가 표시됩니다.



**참고** 일수를 낮추면 시스템은 이전 로그인 기록을 삭제합니다. 그런 다음 한도를 늘리면 시스템은 해당 일수의 계산을 복원하지 않습니다. 이 경우 보고된 로그인 성공 횟수가 실제 수보다 일시적으로 낮을 수 있습니다.

#### 프로시저

**단계 1 System(시스템) > Configuration(구성)을(를) 선택합니다.**

**단계 2 User Configuration(사용자 구성)을 클릭합니다.**

**단계 3 Track Successful Login Days(성공적인 로그인 일수 추적):**를 성공한 로그인을 추적하는 일수로 설정합니다(최대 365일).

로그인 추적을 비활성화하려면 0을 입력합니다.

**단계 4 Save(저장)를 클릭합니다.**

## 임시 잠금 활성화

잠금이 적용되기 전에 시스템에서 허용하는 연속적인 로그인 시도 횟수를 지정하여 임시 시간 지정 잠금 기능을 활성화합니다.

#### 프로시저

**단계 1 System(시스템) > Configuration(구성)을(를) 선택합니다.**

**단계 2 User Configuration(사용자 구성)을 클릭합니다.**

**단계 3 사용자가 일시적으로 잠금 처리되기 전에 Max Number of Login Failures(최대 로그인 실패 횟수)를** 연속 로그인 실패 시도의 최대 횟수로 설정합니다.

임시 잠금을 비활성화하려면 0을 입력합니다.

**단계 4 Time in Minutes to Temporarily Lockout Users(사용자에 대한 임시 잠금 시간(분))**를 임시 잠금을 트리거한 사용자를 잠금 처리하는 시간(분)으로 설정합니다.

이 값이 0이면 **Max Number of Login Failures(최대 로그인 실패 횟수)**가 0이 아니더라도 사용자가 로그인을 다시 시도할 때까지 기다릴 필요가 없습니다.

**단계 5 Save(저장)를 클릭합니다.**

## 최대 동시 세션 수 설정

동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 최대 세션 수를 지정할 수 있습니다. 세션 유형은 사용자에게 할당된 역할을 기준으로 결정됩니다. 사용자에게 읽기 전용 역할만 할당되었다면, 해당 사용자의 세션은 읽기 전용 세션 제한 수에 적용됩니다. 사용자에게 쓰기 권한을 제공하는 역할이 있다면, 세션은 읽기/쓰기 세션 제한 수에 적용됩니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **User Configuration**(사용자 구성)을 클릭합니다.

단계 3 각 세션 유형(읽기 전용 및 읽기/쓰기)에 대해, **Max Concurrent Sessions Allowed**(허용되는 최대 동시 세션)를 해당 유형에 대해 동시에 열 수 있는 최대 세션 수로 설정합니다.

세션 유형별 동시 사용자 수를 제한하지 않으려면 0을 입력합니다.

참고 동시 세션 제한을 더 제한적인 값으로 변경하면, 시스템은 현재 열린 세션을 닫지는 않습니다. 대신 지정된 숫자 이상의 신규 세션이 열리지 않게 합니다.

단계 4 **Save**(저장)를 클릭합니다.

## 세션 시간 초과

무인 로그인 세션은 보안 위험이 될 수 있습니다. 비활성으로 인해 사용자 로그인 세션이 시간 초과 되기까지의 유효 시간을 구성할 수 있습니다.

시스템을 오랫동안 패시브 방식으로 안전하게 모니터링하려는 상황이라면, 특정 웹 인터페이스 사용자를 시간 제한에서 제외할 수 있습니다. 메뉴 옵션에 완전히 액세스할 수 있으므로 손상 시 더 큰 위험을 초래하는 Administrator 역할의 사용자는 세션 시간 초과에서 제외할 수 없습니다.

## 세션 시간 제한 구성

클래식 디바이스에 세션 시간 제한을 구성하려면, 디바이스 플랫폼 설정을 사용합니다. [클래식 디바이스에 대한 세션 시간 초과 구성](#)의 내용을 참조하십시오.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Shell Timeout**(셸 시간 초과)를 클릭합니다.

단계 3 세션 시간 제한 구성

- 웹 인터페이스(FMC에만 해당): 브라우저 세션 시간 제한(분)을 구성합니다. 기본값은 60이고 최대값은 1440(24시간)입니다.

이 세션 시간 제한에서 사용자를 제외하는 방법은 [사용자 어카운트 로그인 옵션](#)의 내용을 참조하십시오.

- CLI: 셸 시간 제한(분) 필드를 구성합니다. 기본값은 0이고 최대값은 1440(24시간)입니다.

단계 4 **Save**(저장)를 클릭합니다.

## 취약성 매핑

서버의 검색 이벤트 데이터베이스에 애플리케이션 ID가 있고 트래픽에 대한 패킷 헤더에 공급업체 및 버전이 포함된 경우, 호스트 IP 주소에서 주고받는 모든 애플리케이션 프로토콜 트래픽에 대해 Firepower System은 해당 주소에 취약성을 자동으로 매핑합니다.

패킷에 공급업체 또는 버전 정보가 포함되어 있지 않은 서버의 경우 시스템이 취약성을 해당 공급업체 및 버전 없는 서버의 서버 트래픽과 연결할지 여부를 구성할 수 있습니다.

예를 들어, 호스트가 헤더에 공급업체 또는 버전을 가지고 있지 않은 SMTP 트래픽을 서비스할 수 있습니다. 시스템 구성의 Vulnerability Mapping 페이지에서 SMTP 서버를 활성화한 다음 트래픽을 탐지하는 디바이스를 관리하는 Firepower Management Center에 해당 구성을 저장하면, SMTP 서버와 관련된 모든 취약성이 호스트의 호스트 프로파일로 추가됩니다.

탐지기는 서버 정보를 수집하여 호스트 프로파일로 추가하지만, 애플리케이션 프로토콜 탐지기는 취약성 매핑에 사용되지 않습니다. 사용자 지정 애플리케이션 프로토콜 탐지에 대해 공급업체 및 버전을 지정할 수 없으며 취약성 매핑을 위해 서버를 선택할 수 없기 때문입니다.

## 서버의 취약성 매핑

이 절차를 수행하려면 스마트 라이선스 또는 보호 클래식 라이선스가 필요합니다.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Vulnerability Mapping**(취약성 매핑)을 선택합니다.

단계 3 다음 옵션을 이용할 수 있습니다.

- 서버에 대한 취약성이 공급업체 또는 버전 정보 없는 애플리케이션 프로토콜 트래픽을 수신하는 호스트에 매핑되지 않도록 하려면 해당 서버의 확인란을 선택 취소합니다.
- 서버에 대한 취약성이 공급업체 또는 버전 정보 없는 애플리케이션 프로토콜 트래픽을 수신하는 호스트에 매핑되도록 하려면 해당 서버의 확인란을 선택합니다.

팁 **Enabled**(활성화됨) 옆에 있는 확인란을 사용하여 모든 확인란을 동시에 선택하거나 선택 취소할 수 있습니다.

단계 4 **Save**(저장)를 클릭합니다.

## 원격 콘솔 액세스 관리

VGA 포트(기본값) 또는 물리적 어플라이언스의 시리얼 포트를 통해 지원되는 시스템에 원격으로 액세스하도록 하려면 Linux 시스템 콘솔을 사용할 수 있습니다. **Console Configuration**(콘솔 구성) 페이지를 사용하여 조직 내 Firepower 구축의 실제 레이아웃에 가장 적합한 옵션을 선택합니다.

지원되는 물리적 하드웨어 기반 Firepower 시스템에서는 기본(`eth0`) 관리 인터페이스의 SOL(Serial Over LAN) 연결에서 LOM(Lights-Out Management)을 사용하여 시스템의 관리 인터페이스에 로그인하지 않고 시스템을 원격으로 모니터링하거나 관리할 수 있습니다. OOB(Out of Band) 관리 연결에서 명령줄 인터페이스를 사용하여 채시 일련 번호 보기, 팬 속도와 온도 등의 조건 모니터링 등 제한적인 작업을 수행할 수 있습니다. LOM을 지원하기 위한 케이블 연결은 FMC 모델에 따라 다릅니다.

- FMC 모델 MC1600, MC2600 및 MC4600의 경우, CIMC 포트와의 연결을 사용하여 LOM을 지원합니다. 자세한 내용은 [Cisco Firepower Management Center 1600, 2600 및 4600 시작 가이드](#)를 참조하십시오.
- 다른 모든 FMC 하드웨어 모델의 경우, 기본(`eth0`) 관리 포트가 있는 연결을 사용하여 LOM을 지원합니다. 해당 하드웨어 모델의 [Cisco Firepower Management Center 시작 가이드](#)를 참조하십시오.

시스템을 관리하려는 사용자와 시스템 모두에 대해 LOM을 활성화해야 합니다. 시스템 및 사용자를 활성화한 후 시스템에 대한 액세스 및 관리를 위해 서드파티 IPMI(Intelligent Platform Management Interface) 유틸리티를 사용합니다.

## 시스템에서 원격 콘솔 설정

이 절차를 수행하려면 관리자 사용자여야 합니다.

시작하기 전에

- 디바이스의 관리 인터페이스에 연결된 모든 서드파티 스위칭 장비에서 STP(Spanning Tree Protocol)를 비활성화해야 합니다.
- Lights-Out 관리를 활성화하려는 경우 IPMI(Intelligent Platform Management Interface) 유틸리티 설치 및 사용에 대한 정보는 어플라이언스의 [시작하기 가이드](#)를 참조하십시오.

프로시저

단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.

단계 2 **Console Configuration**(콘솔 구성)을 클릭합니다.

단계 3 원격 콘솔 액세스 옵션을 선택합니다.

- 어플라이언스의 VAG 포트를 사용하려면 **VGA**를 선택합니다.
- **Physical Serial Port**(물리적 시리얼 포트)를 선택해 어플라이언스의 시리얼 포트를 사용합니다.
- FMC의 기본 관리 포트에서 SOL 연결을 사용하려면 **Lights-Out** 관리를 선택합니다.

단계 4 SOL을 통해 LOM을 구성하려면:

- 시스템(DHCP 또는 **Manual**(수동))에 대한 주소 **Configuration**(구성)을 선택합니다.
- 수동 구성을 선택한 경우 필요한 IPv4 설정을 입력합니다.
  - LOM에 사용될 **IP Address**(IP 주소)를 입력합니다.
 

참고 LOM IP 주소는 FMC 관리 인터페이스 IP 주소와 달라야 합니다.
  - 시스템에 대한 **Netmask**(넷마스크)를 입력합니다.
  - 시스템에 대한 **Default Gateway**(기본 게이트웨이)를 입력합니다.

단계 5 **Save**(저장)를 클릭합니다.

단계 6 "다음 변경 사항을 적용하려면 시스템을 재부팅해야 합니다."라는 경고가 표시됩니다. 지금 재부팅하려면 **OK**(확인)를 클릭하고 나중에 재부팅하려면 **Cancel**(취소)을 클릭합니다.

다음에 수행할 작업

- 직렬 액세스를 구성한 경우, FMC 모델용 **시작 가이드**에 설명된 대로 이더넷을 통한 원격 직렬 액세스를 지원할 수 있는 로컬 컴퓨터, 터미널 서버 또는 기타 디바이스에 후면 패널 직렬 포트가 연결되어 있는지 확인합니다.
- Lights-Out Management를 구성한 경우 Lights-Out Management 사용자를 활성화합니다. [LOM\(Lights-Out Management\) 사용자 액세스 구성, 53 페이지](#) 섹션을 참조하십시오.

## LOM(Lights-Out Management) 사용자 액세스 구성

또한 기능을 사용할 사용자에게 Lights-Out Management 권한을 명시적으로 부여해야 합니다. 또한 LOM 사용자에는 다음과 같은 제한이 있습니다.

- 사용자에게 관리자 역할을 할당해야 합니다.
- 사용자 이름은 최대 16자의 영숫자로 지정할 수 있습니다. LOM 사용자는 16자보다 긴 사용자 이름과 하이픈을 사용할 수 없습니다.
- 사용자의 LOM 비밀번호는 해당 사용자의 시스템 비밀번호와 동일합니다. 비밀번호는 **사용자 암호**에 설명된 요구 사항을 준수해야 합니다. 어플라이언스에서 지원되는 최대 길이로 사전에 없는 복잡한 암호를 사용하고 3개월마다 변경하는 것이 좋습니다.

- LOM이 Firepower 7110, 7115, 7120 또는 7125 디바이스에서 활성화되면 비밀번호는 최대 영숫자 16자로 구성할 수 있습니다.
- 물리적 Firepower Management Center 및 8000 Series 디바이스에는 최대 13명의 LOM 사용자가 있을 수 있습니다. 7000 시리즈 디바이스에는 최대 8명의 LOM 사용자가 있을 수 있습니다.

그러한 사용자가 로그인한 상태에서 LOM으로 해당 사용자를 비활성화했다가 다시 활성화할 경우 또는 사용자의 로그인 세션 중에 백업에서 사용자를 복원할 경우, 해당 사용자가 다시 웹 인터페이스에 로그인해야 `impitool` 명령에 다시 액세스할 수 있습니다.

## LOM(Lights-Out Management) 사용자 액세스 활성화

이 절차를 수행하려면 관리자 사용자여야 합니다.

이 작업을 통해 기존 사용자에게 LOM 액세스 권한을 부여할 수 있습니다. 새 사용자에게 LOM 액세스 권한을 부여하려면 [내부 사용자 추가](#)의 내용을 참조하십시오.

각 시스템의 로컬 웹 인터페이스를 사용하여 시스템별로 LOM 및 LOM 사용자를 구성합니다. Firepower Management Center를 사용하여 매니지드 디바이스에서 LOM을 구성할 수 없습니다. 마찬가지로, 사용자는 어플라이언스별로 독립적으로 관리되므로 Firepower Management Center에서 LOM 지원 사용자를 생성할 경우 해당 기능이 매니지드 디바이스의 사용자로 전달되지 않습니다.

프로시저

단계 1 **System**(시스템) > **Users**(사용자) > **Users**(사용자)을(를) 선택합니다.

단계 2 기존 사용자에 대해 LOM 사용자 액세스 권한을 부여하려면 목록의 사용자 이름 옆에 있는 수정(✎)을 클릭합니다.

단계 3 **User Configuration**(사용자 구성) 아래에서 **Administrator** 역할을 활성화합니다.

단계 4 **Allow Lights-Out Management Access**(Lights-Out Management 액세스 허용) 확인란을 선택합니다.

단계 5 **Save**(저장)를 클릭합니다.

## SoL(Serial over LAN) 연결 구성

컴퓨터에서 타사 IPMI 유틸리티를 사용하여 어플라이언스에 대한 Serial Over LAN 연결을 만듭니다. Linux와 유사한 컴퓨터 환경 또는 Mac 환경에서는 IPMItool을 사용하고, Windows 환경에서는 Windows 버전에 따라 IPMIutil 또는 IPMItool을 사용할 수 있습니다.



참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

### Linux

IPMItool은 많은 배포의 표준이며 곧바로 사용 가능합니다.

## Mac

Mac에는 IPMItool을 설치해야 합니다. 먼저 Mac에 Apple의 XCode Developer 툴이 설치되었는지 확인하고, 명령줄 개발을 위한 선택적인 구성 요소가 설치되었는지 확인합니다(새 버전에서는 UNIX Development 및 System Tools, 이전 버전에서는 Command Line Support). 그런 다음 macports 및 IPMItool을 설치할 수 있습니다. 자세히 알아보려면 자주 사용하는 검색 엔진을 사용하거나 다음 사이트를 이용하십시오.

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
http://github.com/ipmitool/ipmitool/
```

## Windows

Linux용 Windows 하위 시스템(WSL)이 활성화된 Windows 버전 10 이상 및 일부 이전 버전의 Windows Server의 경우 IPMItool을 사용할 수 있습니다. 그렇지 않으면 Windows 시스템에서 IPMIutil을 컴파일해야 합니다. IPMIutil 자체를 사용하여 컴파일 할 수 있습니다. 자세히 알아보려면 자주 사용하는 검색 엔진을 사용하거나 다음 사이트를 이용하십시오.

```
http://ipmiutil.sourceforge.net/man.html#ipmiutil
```

## IPMI 유틸리티 명령 이해

IPMI 유틸리티에 사용되는 명령은 Mac에서 다음 IPMItool 예와 같은 세그먼트로 구성됩니다.

```
ipmitool -I lanplus -H IP_address -U user_name command
```

여기서 각 항목은 다음을 나타냅니다.

- `ipmitool`은 유틸리티를 호출합니다.
- `-I lanplus`는 세션에 대해 암호화된 IPMI v2.0 RMCP + LAN 인터페이스를 사용하도록 지정합니다.
- `-H IP_address`는 액세스하려는 어플라이언스의 LOM(Lights-Out Management)을 위해 구성된 IP 주소를 나타냅니다.
- `-U user_name`는 권한 있는 원격 세션 사용자의 이름입니다.
- `command`는 사용할 명령의 이름입니다.



참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

Windows의 IPMIutil에서는 동일한 명령이 다음과 같이 표시됩니다.

```
ipmiutil command -V 4 -J 3 -N IP_address -User_name
```

이 명령은 어플라이언스에서 실제로 존재 하는 것 처럼 로그인 할 수 있는 기기의 명령행에 연결 합니다. 비밀번호를 입력하라는 프롬프트가 표시될 수 있습니다.

## IPMItool을 사용한 SoL(Serial over LAN) 설정

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMItool을 사용하여 다음 명령을 입력하고 메시지가 표시되면 암호를 입력합니다.

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

## IPMIutil을 사용한 SoL(Serial over LAN) 설정

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMIutil을 사용하여 다음 명령을 입력하고 메시지가 표시되면 암호를 입력합니다.

```
ipmiutil -J 3 -N IP_address -U username sol -a
```

## LOM(Lights-Out Management) 개요

Lights-Out Management(LOM)를 사용하면 시스템에 로그인하지 않고도 기본(eth0) 관리 인터페이스에서 SOL 연결을 통해 제한된 작업을 수행할 수 있습니다. 이 명령을 사용하여 SOL 연결을 생성한 후 LOM 명령 중 하나를 사용합니다. 명령이 완료되면 연결이 종료됩니다. 일부 전원 제어 명령은 70xx 제품군 디바이스에서 유효합니다.



**참고** Firepower 71xx, Firepower 82xx 또는 Firepower 83xx 디바이스에 대한 BMC(baseboard management controller)는 호스트 전원이 켜져 있을 때 1Gbps 링크 속도를 통해서만 액세스할 수 있습니다. 디바이스 전원이 꺼져 있으면 BMC는 10 및 100Mbps의 이더넷 링크만 설정할 수 있습니다. 따라서 LOM을 사용하여 디바이스 전원을 원격으로 제어하는 경우 10 및 100Mbps 링크 속도만을 사용하여 디바이스를 네트워크에 연결하십시오.



**주의** 드물긴 하지만, 시스템의 관리 인터페이스와 다른 서버넷에 있으며 시스템이 DHCP로 구성되어 있는 경우 LOM 기능에 액세스하려고 시도하면 실패할 수 있습니다. 이런 일이 발생하면 시스템에서 LOM을 비활성화한 후 다시 활성화하거나, 동일한 서버넷의 컴퓨터를 시스템으로 사용하여 관리 인터페이스를 ping할 수 있습니다. 이렇게 하면 LOM을 사용할 수 있게 됩니다.



주의 Cisco에서는 IPMI(Intelligent Platform Management Interface) 표준(CVE-2013-4786)에 내재된 취약성에 대해 잘 알고 있습니다. 시스템에서 LOM(Lights-Out Management)을 활성화하면 이 취약성이 노출됩니다. 이 취약성을 완화하려면 신뢰할 수 있는 사용자만 액세스할 수 있는 안전한 관리 네트워크에 시스템을 구축하고, 시스템에서 지원되는 최대 길이로 사전에 없는 복잡한 비밀번호를 사용하고 3개월에 한 번씩 변경하십시오. 이 취약성이 노출되지 않도록 하려면 LOM을 활성화하지 마십시오.

시스템에 대한 모든 액세스 시도가 실패한 경우 LOM을 사용하여 시스템을 원격으로 재시작할 수 있습니다. SOL 연결이 활성화된 상태에서 시스템을 다시 시작하면 LOM 세션이 끊어지거나 시간이 초과될 수 있습니다.



주의 다시 시작하려는 다른 시도에 응답하지 않는 상황이 아니면 시스템을 다시 시작하지 마십시오. 원격으로 다시 시작하는 경우 시스템이 정상적으로 재부팅되지 않으며, 데이터가 손실될 수 있습니다.

표 6: Lights-Out Management 명령

IPMItool	IPMIutil	설명
(해당 없음)	-V 4	IPMI 세션의 관리자 권한을 활성화합니다.
-I lanplus	-J 3	IPMI 세션의 암호화를 활성화합니다.
-H 호스트 이름/IP 주소	-N 노드 이름/IP 주소	다음에 대한 LOM IP 주소 또는 호스트 이름을 나타냅니다.FMC
-U	-U	권한이 있는 LOM 계정의 사용자 이름을 나타냅니다.
sol activate	sol -a	SOL 세션을 시작합니다.
sol deactivate	sol -d	SOL 세션을 종료합니다.
chassis power cycle	power -c	어플라이언스를 다시 시작합니다(70xx 제품군 디바이스에서는 유효하지 않음).
chassis power on	power -u	어플라이언스 전원을 켭니다.
chassis power off	power -d	어플라이언스 전원을 끕니다(70xx 제품군 디바이스에서는 유효하지 않음).
sdr	sensor	팬 속도와 온도 등 어플라이언스 정보를 표시합니다.

예를 들어 어플라이언스 정보 목록을 표시하려면 다음 IPMItool 명령을 사용합니다.

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```



참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

IPMIutil 유틸리티에서는 동일한 명령이 다음과 같습니다.

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

## IPMItool을 사용한 LOM(Lights-Out Management) 구성

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMItool에 대해 다음 명령을 입력하고 메시지가 표시되면 비밀번호를 입력합니다.

```
ipmitool -I lanplus -H IP_address -U user_name command
```

## IPMIutil을 사용한 LOM(Lights-Out Management) 구성

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMIutil에 대해 다음 명령을 입력하고 메시지가 표시되면 비밀번호를 입력합니다.

```
ipmiutil -J 3 -N IP_address -U username command
```

## VMware Tools 및 가상 시스템

VMware Tools는 가상 머신용 성능 향상 유틸리티 모음입니다. 이러한 유틸리티를 사용하면 VMware 제품의 편리한 기능을 최대한 활용할 수 있습니다. VMware에서 실행되는 Firepower 가상 어플라이언스는 다음 플러그인을 지원합니다.

- guestInfo
- powerOps

- timeSync
- vmbackup

또한 모든 지원되는 ESXi 버전에서 VMware Tools를 활성화할 수 있습니다. 지원되는 버전 목록을 보려면 [VMware용 Cisco Firepower NGIPSv 빠른 시작 가이드](#) 섹션을 참조하십시오. VMware Tools의 전체 기능에 대한 자세한 내용은 VMware 웹 사이트(<http://www.vmware.com/>)를 참조하십시오.

## VMware용 Firepower Management Center의 VMWare Tools 활성화

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	Any(모든)	Firepower Management Center	전역만 해당	Admin(관리자)

NGIPSv에는 웹 인터페이스가 없으므로 CLI를 사용하여 해당 플랫폼에서 VMware Tools를 활성화해야 합니다. [VMware용 Cisco Firepower NGIPSv 빠른 시작 가이드](#) 섹션을 참조하십시오.

### 프로시저

- 단계 1 **System**(시스템) > **Configuration**(구성)을(를) 선택합니다.
- 단계 2 **VMware Tools**를 클릭합니다.
- 단계 3 **Enable VMware Tools**(VMware Tools 활성화)를 클릭합니다.
- 단계 4 **Save**(저장)를 클릭합니다.

## 시스템 구성 기록

기능	버전	세부 사항
SAN(Subject Alternative Name)	6.6	FMC의 HTTPS 인증서를 생성할 때 SAN 필드를 지정할 수 있습니다. 인증서가 여러 도메인 이름 또는 IP 주소를 보호하는 경우, SAN을 사용하는 것이 좋습니다. SAN에 대한 자세한 내용은 <a href="#">RFC 5280</a> , <a href="#">섹션 4.2.1.6</a> 을 참조하십시오.  신규/수정된 화면: <b>System(시스템) &gt; Configuration(구성) &gt; HTTPS Certificate(HTTPS 인증서)</b>  지원되는 플랫폼: FMC

기능	버전	세부 사항
HTTPS 인증서	6.6	<p>시스템과 함께 제공되는 기본 HTTPS 서버 인증서는 이제 800일 후에 만료됩니다. 애플 라이언스가 버전 6.6으로 업그레이드되기 전에 생성된 기본 인증서를 사용하는 경우, 인증서 수명은 인증서 생성 시 사용되던 Firepower 버전에 따라 달라집니다. 자세한 내용은 <a href="#">기본 HTTPS 서버 인증서, 7 페이지</a>를 참조하십시오.</p> <p>신규/수정된 화면: 없음</p> <p>지원되는 플랫폼: 하드웨어 FMC</p>
보안 NTP	6.5	<p>FMC은(는) SHA1 또는 MD5 대칭 키 인증을 이용해 NTP 서버와의 안전 연결을 지원합니다.</p> <p>신규/수정된 화면:</p> <p><b>System(시스템) &gt; Configuration(설정) &gt; Time Synchronization(시간 동기화)</b></p> <p>지원되는 플랫폼: FMC</p>
웹 분석	6.5	<p>EULA에 동의하면 웹 분석 데이터 수집이 시작됩니다.</p> <p>예전처럼, 데이터 공유를 계속하지 않도록 선택할 수 있습니다. (<a href="#">선택 사항</a>) <a href="#">웹 분석 추적 선택 취소</a>의 내용을 참조하십시오.</p>
다음에 대한 자동 CLI 액세스 FMC	6.5	<p>SSH를 이용해 FMC에 로그인하면, CLI에 자동으로 액세스하게 됩니다. 권장 사항은 아니지만, 이후 CLI expert 명령을 사용하면 Linux 셸에 액세스할 수 있습니다.</p> <p>참고 이 기능을 이용하면 버전 6.3 기능인 FMC에 대한 CLI 액세스 활성화/비활성화가 중단됩니다. 이 옵션이 중단되면 가상 FMC에서는 <b>System(시스템) &gt; Configuration(구성) &gt; Console Configuration(콘솔 구성)</b> 페이지가 표시되지 않습니다. 물리적 FMC에서는 계속 표시됩니다.</p>
읽기 전용 및 읽기/쓰기 액세스에 구성 가능한 세션 제한	6.5	<p><b>Max Concurrent Sessions Allowed(허용되는 최대 동시 세션)</b> 설정을 추가했습니다. 이 설정을 이용하면 관리자는 동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 최대 세션 수를 지정할 수 있습니다.</p> <p>참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할과 맞춤형 사용자 역할은 <b>System(시스템) &gt; Users(사용자) &gt; Users(사용자)</b>와 <b>System(시스템) &gt; Users(사용자) &gt; User Roles(사용자 역할)</b>의 역할 이름에 (읽기 전용)이라고 표시됩니다. 사용자 역할의 역할 이름에 (읽기 전용)이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다.</p> <p>신규/수정된 화면:</p> <p><b>System(시스템) &gt; Configuration(구성) &gt; User Configuration(사용자 구성)</b></p> <p><b>System(시스템) &gt; Users(사용자) &gt; User Roles(사용자 역할)</b></p> <p>지원되는 플랫폼: FMC</p>

기능	버전	세부 사항
관리 인터페이스에서 DAD(Duplicate Address Detection)를 비활성화하는 기능	6.4	<p>IPv6를 활성화하면 DAD를 비활성화할 수 있습니다. DAD를 사용하면 서비스 거부(DoS) 공격 가능성이 발생하기 때문에 DAD를 비활성화하려고 할 수 있습니다. 이 설정을 비활성화하면 이 인터페이스가 이미 할당된 주소를 사용하고 있지 않은지 수동으로 확인해야 합니다.</p> <p>신규/수정된 화면:</p> <p><b>System(시스템) &gt; Configuration(구성) &gt; Management Interfaces(관리 인터페이스) &gt; Interfaces(인터페이스) &gt; Edit Interface(인터페이스 편집) 대화 상자 &gt; IPv6 DAD</b> 확인란</p> <p>지원되는 플랫폼: FMC, 7000 및 8000 Series 디바이스</p>
관리 인터페이스에서 ICMPv6 Echo Reply 및 Destination Unreachable 메시지를 비활성화하는 기능	6.4	<p>IPv6를 활성화할 때 이제 ICMPv6 Echo Reply 및 Destination Unreachable 메시지를 비활성화할 수 있습니다. 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.</p> <p>신규/수정된 화면:</p> <p><b>System(시스템) &gt; Configuration(구성) &gt; Management Interfaces(관리 인터페이스) &gt; ICMPv6</b></p> <p>신규/수정된 명령: <b>configure network ipv6 destination-unreachable, configure network ipv6 echo-reply</b></p> <p>지원되는 플랫폼: FMC(웹 인터페이스에만 해당), 7000 및 8000 Series, FTD(CLI에만 해당), ASA FirePOWER 모듈(CLI에만 해당), NGIPSv(CLI에만 해당)</p>
전역 사용자 구성	6.3	<p><b>Track Successful Logins(성공적인 로그인 추적)</b> 설정을 추가했습니다. 시스템은 선택한 일수 이내에 각 FMC 계정이 수행한 성공적인 로그인 수를 추적할 수 있습니다. 이 기능을 활성화하면 로그인 사용자는 구성된 일수 전에 시스템에 성공적으로 로그인한 횟수를 나타내는 메시지를 볼 수 있습니다. (셸/CLI 액세스뿐만 아니라 웹 인터페이스에도 적용됩니다.)</p> <p><b>Password Reuse Limit(비밀번호 재사용 한도)</b> 설정을 추가했습니다. 시스템은 구성 가능한 수의 이전 비밀번호에 대해 각 계정의 비밀번호 기록을 추적할 수 있습니다. 시스템은 모든 사용자가 해당 기록에 나타나는 비밀번호를 다시 사용할 수 없게 방지합니다. (셸/CLI 액세스뿐만 아니라 웹 인터페이스에도 적용됩니다.)</p> <p><b>Max Number of Login Failures(최대 로그인 실패 횟수) 및 Set Time in Minutes to Temporarily Lockout Users(사용자에 대한 임시 잠금 시간(분) 설정)</b> 설정을 추가했습니다. 이는 시스템이 구성 가능한 시간 동안 계정을 일시적으로 차단하기 전에 사용자가 잘못된 웹 인터페이스 로그인 자격 증명을 연속적으로 입력할 수 있는 횟수를 제한하는 기능을 관리자에게 제공합니다.</p> <p>신규 화면: <b>System(시스템) &gt; Configuration(설정) &gt; User Configuration(사용자 설정)</b></p> <p>지원되는 플랫폼: FMC</p>

기능	버전	세부 사항
HTTPS 인증서	6.3	<p>시스템과 함께 제공되는 기본 HTTPS 서버 인증서는 이제 3년 후에 자동으로 만료됩니다. 어플라이언스가 버전 6.3으로 업그레이드하기 전에 생성된 기본 서버인증서를 사용하는 경우 해당 서버 인증서는 처음 생성된 시점에서 20년 후에 만료됩니다. 기본 HTTPS 서버 인증서를 사용하는 경우 시스템은 이제 이 인증서를 갱신할 수 있는 기능을 제공합니다.</p> <p>신규/수정된 화면:</p> <p><b>System(시스템) &gt; Configuration(설정) &gt; HTTPS Certificate(HTTPS 인증서) 페이지 &gt; Renew HTTPS Certificate(HTTPS 인증서 갱신)</b></p> <p>지원되는 플랫폼: FMC, 7000 및 8000 Series 디바이스</p>
CLI 액세스를 활성화 및 비활성화 하는 기능 FMC	6.3	<p>신규/수정된 화면:</p> <p>FMC 웹 인터페이스 관리자가 사용할 수 있는 새 체크박스: <b>Enable CLI Access(CLI 액세스 활성화)(System(시스템) &gt; Configuration(구성)에 위치) &gt; ( Console Configuration(콘솔 구성))</b> 페이지</p> <ul style="list-style-type: none"> <li>• 선택: SSH를 사용하여 FMC에 로그인하면 CLI에 액세스할 수 있습니다.</li> <li>• 선택 취소: SSH를 사용하여 FMC에 로그인하면 Linux 셸에 액세스할 수 있습니다. 이는 새 버전 6.3 설치 뿐만 아니라 이전 릴리스에서 버전 6.3으로 업그레이드 할 때의 기본 상태입니다.</li> </ul> <p>버전 6.3 이전에는 <b>Console Configuration(콘솔 구성)</b> 페이지에 하나의 설정만 있었으며 물리적 디바이스에만 적용되었습니다. 따라서 가상 FMC에서는 <b>Console Configuration(콘솔 구성)</b> 페이지를 사용할 수 없었습니다. 이제 이 새로운 옵션의 추가를 통해 <b>Console Configuration(콘솔 구성)</b> 페이지가 물리적 디바이스 및 가상 FMC 모두에 나타납니다. 하지만 가상 FMC의 경우 이 확인란만 페이지에 나타납니다.</p> <p>지원되는 플랫폼: FMC</p>