# Firepower System 라이선싱

버전 6.6의 Licensing(라이선싱) 챕터에서 다양한 라이선스 유형, 서비스 구독, 라이선싱 요구 사항 등의 자세한 정보를 확인할 수 있습니다. 또한 이 장에서는 에어갭 솔루션에 대한 스마트 및 기본 라이선스와 라이선싱 구축 관련 절차 및 요구 사항도 확인할 수 있습니다.

다음 주제에서는 Firepower System 라이선싱 방법을 설명합니다.


- Firepower 라이선스 정보, 1 페이지
- 라이선싱 요구 사항 및 사전 요건, 2 페이지
- Firepower Management Center 라이선스 요구 사항, 2 페이지
- 평가판 라이선스 주의 사항, 3 페이지
- 모든 디바이스 라이선싱, 3 페이지
- FTD 디바이스에서 사용할 클래식 라이선스를 변환하는 방법, 12 페이지
- 디바이스 관리 페이지에서 매니지드 디바이스에 라이선스 할당, 14 페이지
- 라이선스 만료, 15 페이지
- 이 가이드의 기타 라이선싱 정보, 18 페이지
- Firepower 라이선싱 관련 추가 정보, 20 페이지
- Cisco 지원 진단, 20 페이지
- 라이선싱 기록, 21 페이지


# Firepower 라이선스 정보

Firepower 제품(Firepower Management Center 및 매니지드 디바이스)에는 기본 작업에 대한 라이선스가 포함되지만 일부 기능은 이 장에 설명된 대로 별도 라이선싱이나 서비스 스크립션이 필요합니다.

"right-to-use(사용 권한)" 라이선스는 만료되지 않지만 서비스 서브스크립션은 주기적으로 갱신해야 합니다.

제품에서 요구하는 라이선스의 유형은 사용하는 소프트웨어에 따라 달라지며 해당 소프트웨어를 실행하는 하드웨어는 관련이 없습니다.

참고 "NGFW"는 다양한 사람에 대한 다양한 사항을 의미하기 때문에 이 문서에서는 이 용어를 사용하지 않습니다.

# 라이선싱 요구 사항 및 사전 요건

모델 지원

모두 가능하지만 모델별로 필요한 특정 라이선스는 절차에 나와 있는 것과 다릅니다.

지원되는 도메인

글로벌, 표시된 경우를 제외하고.

사용자 역할

- 관리자

# Firepower Management Center 라이선스 요구 사항

Firepower Management Center 매니지드 디바이스에 라이선스를 할당하고 시스템에 대한 라이선스를 관리할 수 있습니다.

하드웨어 **FMC**

하드웨어 Firepower Management Center는 디바이스 관리를 위한 추가 라이선스 구입이나 서비스 서브스크립션이 필요하지 않습니다.

가상 **FMC**

Firepower Management Center 가상은 추가 라이선스 요구 사항이 없습니다. Firepower Management Center Virtual 라이선스, 2 페이지의 내용을 참조하십시오.

## Firepower Management Center Virtual 라이선스

일반적으로 Firepower Management Center 가상(FMCv)은 관리하는 각 FTD 디바이스에 대해 라이선스 엔타이틀먼트가 필요합니다. FMCv에는 클래식 디바이스를 관리하는 데 Firepower MCv 라이선스가 필요하지 않습니다.

단일 FMCv가 고가용성 쌍으로 구성되는 Firepower Threat Defense 디바이스를 관리하는 경우에도 각 디바이스에 대해 하나의 엔타이틀먼트가 필요합니다(FTD 쌍마다 엔타이틀먼트 하나가 아님).

고가용성 설정의 FMCv의 경우 FMC 고가용성 설정에 대한 라이선스 요구 사항의 내용을 참조하십시오.

다중 인스턴스 구축에서 각 보안 모듈에 대해 하나의 엔타이틀먼트가 필요합니다.

스마트 라이선싱이 연결된 표준에서, 이러한 라이선스는 영구적입니다.

Specific License Reservation(특정 라이선스 예약)에서 이러한 라이선스에는 기한이 있습니다.

이 엔타이틀먼트는 Cisco Smart Software Manager에 **Firepower MCv** 디바이스 라이선스로 표시되며, 표시되는 엔타이틀먼트 수는 다양합니다.

# 평가판 라이선스 주의 사항

평가판 라이선스는 모드 기능을 사용할 수 없습니다. 평가판 라이선스의 기능을 부분적일 수 있으며 평가판 라이선싱에서 표준 라이선성으로의 전환이 원활하지 않을 수 있습니다.

예를 들어 Firepower Threat Defense 디바이스가 클러스터로 구성되어 있고 평가판 라이선스에서 스마트 라이선싱으로 전환하는 경우, 변경 사항을 배포할 때 서비스가 중단됩니다.

평가판 라이선스 주의사항에 대한 정보는 Licensing(라이선싱)에 관한 본 장 및 각 기능 배포에 관한 다른 장에 포함된 특정 기능 정보를 참조하십시오.

# 모든 디바이스 라이선싱

7000 및 8000 Series 및 NGIPSv 디바이스와 ASA FirePOWER 모듈은 기본 라이선스를 요구합니다. 이러한 디바이스를 이 문서에서는 종종 클래식 디바이스라고 합니다.

중요 Firepower 하드웨어는 실행하지만 Firepower 소프트웨어는 실행하지 않는 경우, 사용하고 있는 소프트웨어 제품에 대한 라이선싱 정보를 참조하십시오. 이 문서는 적용할 수 없습니다.

기본 라이선스는 PAK(제품 인증 키)를 활성화해야 하고 디바이스에 따라 달라집니다. 기본 라이선스는 때로 "traditional licensing(전통적 라이선싱)"이라고도 합니다.

## 제품 라이선스 등록 포털

Firepower 기능에 대해 하나 이상의 기본 라이선스를 구매하는 경우, 해당 라이선스는 Cisco Product License Registration Portal에서 관리할 수 있습니다.

https://cisco.com/go/license

이 포털을 사용에 관한 자세한 내용은 다음을 참조하십시오.

https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

이러한 링크에 액세스하려면 계정 자격 증명이 필요합니다.

# Firepower 기능에 대한 서비스 서브스크립션(클래식 라이선싱)

일부 기능은 서비스 서브스크립션이 필요합니다.

서비스 서브스크립션은 매니지드 디바이스에서 정해진 기간 동안 특정 Firepower 기능을 활성화합니다. 서비스 서브스크립션은 1년, 3년 또는 5년 기간으로 구입할 수 있습니다. 서브스크립션이 만료되는 경우, Cisco가 서브스크립션을 갱신해야 한다고 알려줍니다. 클래식 디바이스에 대한 서브스크립션이 만료되는 경우, 기능 유형에 따라 관련 기능을 사용할 수 없습니다.

표 *1:* 서비스 서브스크립션 및 해당 기본 라이선스

| 구매한 서브스크립션 | **Firepower System**에서 할당하는 기본 라이선스 |
|---|---|
| TA | 제어 + 보호 (즉, 시스템 업데이트에 필요한 "위협 & 앱") |
| TAC | 제어 + 보호 + URL 필터링 |
| TAM | 제어 + 보호 + 악성코드 |
| TAMC | 제어 + 보호 + URL 필터링 + 악성코드 |
| URL | URL 필터링 (TA가 이미 존재하는 경우 애드온) |
| AMP | 악성코드 (TA가 이미 존재하는 경우 애드온) |

기본 라이선스를 사용하는 매니지드 디바이스를 구매하는 경우 제어 및 보호 라이선스가 포함됩니다. 이러한 라이선스는 영구적이지만, TA 서비스 서브스크립션도 구입해야 서비스 업데이트를 활성화할 수 있습니다. 추가 기능에 대한 서비스 서브스크립션은 선택 사항입니다.

## 기본 라이선스 유형 및 제한 사항

이 섹션에서는 Firepower System 구축에서 사용 가능한 기본 라이선스의 유형에 대해 설명합니다. 디바이스에서 활성화할 수 있는 라이선스는 해당 모델, 버전 및 활성화된 다른 라이선스에 따라 달라질 수 있습니다.

라이선스는 7000 및 8000 Series 및 NGIPSv 디바이스와 ASA FirePOWER 모듈의 모델에 따라 다릅니다. 라이선스가 디바이스 모델과 정확히 일치하지 않는 경우 매니지드 디바이스에서 라이선스를 활성화할 수 없습니다. 예를 들어, Firepower 8250 악성코드 라이선스(FP8250-TAM-LIC =)를 사용하여 8140 디바이스의 악성코드 기능을 활성화할 수 없습니다. Firepower 8140 악성코드 라이선스 (FP8140-TAM-LIC =)를 구매해야 합니다.

참고 NGIPSv 또는 ASA FirePOWER의 경우, 제어 라이선스를 사용하면 사용자 및 애플리케이션 제어를 수행할 수 있지만 이러한 디바이스는 스위칭, 라우팅, 스태킹 또는 7000 및 8000 Series 디바이스 고가용성을 지원하지 않습니다.

Firepower System의 라이선싱된 기능에 대한 액세스 권한이 차단될 수 있는 방법이 몇 가지 있습니다.

- Firepower Management Center에서 기본 라이선스를 제거할 수 있는데, 이는 해당 매니지드 디바이스 모두에 영향을 줍니다.
- 또한 특정 매니지드 디바이스에서 라이선싱된 기능을 비활성화할 수 있습니다.

일부 예외가 있지만, 만료 또는 삭제된 라이선스와 관련된 기능을 사용할 수 없습니다.

다음 표에는 Firepower System 기본 라이선스가 요약되어 있습니다.

표 ***2: Firepower System*** 기본 라이선스

| **Firepower System**에서 할당하는 라이선스 | 구매한 서비스 서브스크립션 | 플랫폼 | 부여된 기능 | 추가 필요 항목 | 만료 가능**?** |
|---|---|---|---|---|---|
| Any(모든) | TA, TAC, TAM 또는 TAMC | 7000 및 8000 Series<br>ASA FirePOWER<br>NGIPSv | 호스트, 애플리케이션 및 사용자 검색<br>SSL 및 TLS로 암호화된 트래픽 암호 해독 및 검사 | 없음 | 라이선스에 따라 달라집니다 |
| 보호 | TA (디바이스에 포함) | 7000 및 8000 Series<br>ASA FirePOWER<br>NGIPSv | 침입 탐지 및 방지<br>파일 제어<br>보안 인텔리전스 필터링 | 없음 | 아니요 |
| 제어 | none (없음) (디바이스에 포함) | 7000 및 8000 Series | 사용자 및 애플리케이션 제어<br>스위칭 및 라우팅<br>7000 및 8000 Series 디바이스 고가용성<br>7000 및 8000 Series NAT(Network Address Translation) | 보호 | 아니요 |
| 제어 | none (없음) (디바이스에 포함) | ASA FirePOWER<br>NGIPSv | 사용자 및 애플리케이션 제어 | 보호 | 아니요 |
| 악성코드 | TAM, TAMC 또는 AMP | 7000 및 8000 Series<br>ASA FirePOWER<br>NGIPSv | AMP for Networks (네트워크 기반 고급 악성코드 보호)<br>파일 스토리지 | 보호 | 예 |
| URL 필터링 | TAC, TAMC, 또는 URL | 7000 및 8000 Series<br>ASA FirePOWER<br>NGIPSv | 카테고리 및 평판 기반 URL 필터링 | 보호 | 예 |

| Firepower System에서 할당하는 라이선스 | 구매한 서비스 서브스크립션 | 플랫폼 | 부여된 기능 | 추가 필요 항목 | 만료 가능? |
|---|---|---|---|---|---|
| VPN | none (없음) (자세한 내용은 영업팀에 문의) | 7000 및 8000 Series | 가상 사설망 구축 | 제어 | 예 |

## 보호 라이선스

보호 라이선스는 침입 탐지 및 방지, 파일 제어 및 보안 인텔리전스 필터링을 수행할 수 있습니다.

- 침입 탐지 및 방지를 사용하면 침입 및 공격의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다.
- *File control(*파일 제어*)*를 사용하면 사용자가 특정 애플리케이션 프로토콜에 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 악성코드 라이선스가 필요한 *AMP for Networks* 는 제한적인 해당 파일 유형 집합을 속성에 따라 검사 및 차단할 수 있습니다.
- *Security Intelligence filtering(*보안 인텔리전스 필터링*)*을 사용하면 트래픽이 액세스 제어 규칙에 따라 분석의 대상이 되기 전에 특정 IP 주소, URL 및 DNS 도메인 이름을 차단 목록에 추가하고 이를 오고가는 트래픽을 거부할 수 있습니다. 동적 피드를 사용하면 최신 인텔리전스를 기반으로 연결을 즉시 차단할 수 있습니다. 경우에 따라 Seurity Intelligence 필터링에 "모니터링 전용" 설정을 사용할 수 있습니다.

보호 라이선스(및 제어 라이선스)는 클래식 매니지드 디바이스를 구매하는 경우 자동으로 포함됩니다. 이러한 라이선스는 영구적이지만, TA 서비스 서브스크립션도 구입해야 서비스 업데이트를 활성화할 수 있습니다.

액세스 제어 정책을 구성하여 라이선스 없이 Protection(보호) 관련 검사를 수행할 수 있지만, 먼저 보호 라이선스를 Firepower Management Center에 추가한 후 정책의 대상이 되는 디바이스에서 활성화할 때까지 해당 정책을 적용할 수 없습니다.

보호 라이선스를 Firepower Management Center에서 삭제하거나 매니지드 디바이스에서 보호를 비활성화하면 Firepower Management Center는 영향을 받는 디바이스에서 침입 및 파일 이벤트의 인지를 중지합니다. 결과적으로, 해당 이벤트를 트리거 기준으로 사용하는 상관성 규칙이 실행을 중지합니다. 또한 Firepower Management Center은 Cisco 제공 정보나 서드파티 Security Intelligence 정보를 검색하기 위해 인터넷에 접속하지 않습니다. 보호 라이선스를 다시 활성화할 때까지 기존 정책을 다시 배포할 수 없습니다.

보호 라이선스가 URL 필터링, 악성코드 및 제어 라이선스에 필요하므로, 보호 라이선스를 삭제 또는 비활성화하는 것은 URL 필터링, 악성코드 및 제어 라이선스를 삭제 또는 비활성화하는 것과 영향이 같습니다.

# 제어 라이선스

제어 라이선스를 사용하면 액세스 제어 규칙에 사용자 및 애플리케이션 상태를 추가하여 사용자 및 애플리케이션 제어를 수행할 수 있습니다. 7000 및 8000 Series 디바이스 한정으로, 이 라이선스를 사용하면 스위칭 및 라우팅(DHCP 릴레이 및 NAT 포함), 디바이스 고가용성 쌍을 구성할 수 있습니다. 매니지드 디바이스에서 제어 라이선스를 활성화하려면 보호 라이선스도 활성화해야 합니다. 제어 라이선스(및 보호 라이선스)는 클래식 매니지드 디바이스를 구매하는 경우 자동으로 포함됩니다. 이러한 라이선스는 영구적이지만, TA 서비스 서브스크립션도 구입해야 서비스 업데이트를 활성화할 수 있습니다.

클래식 매니지드 디바이스에 대해 제어 라이선스를 활성화하지 않은 경우, 사용자 및 애플리케이션 조건을 액세스 제어 정책의 규칙에 추가할 수 있지만 해당 정책을 디바이스에 배포할 수는 없습니다. 7000 또는 8000 Series디바이스에 대해 제어 라이선스를 활성화하지 않으면, 다음도 수행할 수 없습니다.

- 스위칭, 라우팅 또는 하이브리드 인터페이스 생성
- NAT 항목 생성
- 가상 라우터에 대한 DHCP 릴레이 구성
- 디바이스 스위치 또는 라우팅을 포함하는 디바이스 구성 배포
- 디바이스 간 고가용성 설정

참고 제어 라이선스 없이 가상 스위치와 라우터를 생성할 수 있지만 이들을 채우기 위한 스위칭 및 라우팅 인터페이스가 없으면 유용하지 않습니다.

Firepower Management Center에서 제어 라이선스를 삭제하거나 개발 장치에서 제어를 비활성화하는 경우는 다음과 같습니다.

- 영향을 받는 디바이스는 스위칭 또는 라우팅 수행을 중단하지 않으며 디바이스 고가용성 쌍도 중단하지 않습니다.
- 기존 구성을 계속 편집하고 삭제할 수는 있지만, 영향을 받는 디바이스에 그러한 변경 사항을 배포할 수 없습니다.
- 새로운 스위칭, 라우팅 또는 하이브리드 인터페이스를 추가할 수 없으며, 새 NAT 항목을 추가하거나 DHCP 릴레이를 구성하거나 7000 또는 8000 Series 디바이스 고가용성을 설정할 수도 없습니다.
- 사용자 또는 애플리케이션 조건이 있는 규칙이 포함된 경우 기존 액세스 제어 정책을 다시 배포할 수 없습니다.

# 클래식 디바이스에 대한 **URL** 필터링 라이선스

URL 필터링을 사용하면 액세스 제어 규칙을 작성할 수 있습니다. 이 규칙은 모니터링된 호스트에서 요청하고 URL 정보와 상호 연결된 해당 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정

합니다. URL 필터링 라이선스를 활성화하려면 보호 라이선스도 활성화해야 합니다. 클래식 디바이스에 대한 URL 필터링 라이선스를 위협 & 앱(TAC) 또는 위협 & 앱 및 악성코드(TAMC) 서브스크립션과 결합된 서비스 서브스크립션으로 구입할 수 있습니다. 위협 & 앱(TA) 서브스크립션이 이미 활성화된 시스템의 경우 애드온 서브스크립션(URL)으로도 구입할 수 있습니다.

팁 URL 필터링 라이선스가 없는 경우, 허용하거나 차단하려는 개별 URL 또는 URL 그룹을 지정할 수 있습니다. 이를 통해 웹 트래픽에 대한 세분화된 사용자 지정 제어를 가질 수 있지만 URL 카테고리와 평판 데이터를 사용하여 네트워크 트래픽을 필터링할 수는 없습니다.

URL 필터링 라이선스 없이도 액세스 제어 규칙에 카테고리 및 평판 기반 URL 조건을 추가할 수 있지만, Firepower Management Center은 URL 정보를 다운로드하지 않습니다. URL 필터링 라이선스를 Firepower Management Center에 추가한 후 정책의 대상이 되는 디바이스에서 활성화할 때까지는 액세스 제어 정책을 배포할 수 없습니다.

Firepower Management Center에서 라이선스를 삭제하거나 매니지드 디바이스에서 URL 필터링을 비활성화하는 경우, URL 필터링에 대한 액세스가 차단될 수 있습니다. 또한 URL 필터링 라이선스가 만료될 수 있습니다. 라이선스가 만료되거나 라이선스를 비활성화하는 경우, URL 조건이 포함된 액세스 제어 규칙이 URL 필터링을 즉시 중지하고 Firepower Management Center은 더 이상 업데이트를 URL 데이터에 다운로드할 수 없습니다. 카테고리 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.

## 클래식 디바이스에 대한 악성코드 라이선스

악성코드 라이선스를 사용하면 AMP for Networks 와 Cisco Threat Grid이 포함된 Cisco AMP(고급 악성코드 보호)를 수행할 수 있습니다. 매니지드 디바이스를 사용하여 네트워크를 통해 전송된 파일에서 악성코드를 탐지 및 차단할 수 있습니다. 악성코드 라이선스를 활성화하려면 보호 라이선스도 활성화해야 합니다. 악성코드 라이선스를 위협 & 앱(TAM) 또는 위협 & 앱 및 URL 필터링(TAMC) 서브스크립션과 결합된 서브스크립션으로 구입할 수 있습니다. 위협 & 앱(TA) 서브스크립션이 이미 활성화된 시스템의 경우 애드온 서브스크립션(AMP)으로도 구입할 수 있습니다.

참고 7000 및 8000 Series 악성코드 라이선스가 활성화된 매니지드 디바이스는 사용자가 동적 분석을 구성하지 않은 경우에도 AMP 클라우드 연결을 주기적으로 시도합니다. 따라서, 디바이스의 Interface Traffic(인터페이스 트래픽) 대시보드 위젯은 전송된 트래픽을 보여주며, 이는 예상된 작업입니다.

사용자는 파일 정책의 일부로서 AMP for Networks 를 구성한 후 하나 이상의 액세스 제어 규칙과 연결합니다. 파일 정책은 사용자가 특정 애플리케이션 프로토콜을 통해 특정 유형의 파일을 업로드 또는 다운로드하는지를 탐지할 수 있습니다. AMP for Networks 을 통해 로컬 악성 코드 분석 및 파일 사전 분류를 사용하여 그러한 제한된 파일 유형의 집합에 악성코드가 있는지 검사할 수 있습니다. 또한 Cisco Threat Grid 클라우드에서 특정 파일 유형을 다운로드 및 전송하여 동적 분석과 Spero 분석으로 해당 파일에 악성코드가 포함되었는지 여부를 결정합니다. 이러한 파일에서 네트워크 파일 경로를 상세히 볼 수 있습니다. 악성코드 라이선스는 또한 특정 파일을 파일 목록에 추가하고 파일 정책 내에서 파일 목록을 활성화하며, 해당 파일이 탐지되면 자동으로 허용하거나 차단하도록 허용합니다.

AMP for Networks 구성을 포함하는 액세스 제어 정책을 배포하기 전에 반드시 악성코드 라이선스를 추가한 후, 정책의 대상이 되는 디바이스에서 이 라이선스를 활성화해야 합니다. 나중에 디바이스에서 이 라이선스를 비활성화하는 경우, 해당 디바이스에 기존 액세스 제어 정책을 다시 배포할 수 없습니다.

악성코드 라이선스가 모두 삭제되거나 만료된 경우, 시스템에서 AMP 클라우드에 대한 쿼리를 중단하며 AMP 클라우드에서 전송한 회귀적 이벤트 확인도 중지합니다. AMP for Networks 구성이 포함된 경우, 기존 액세스 제어 정책은 재적용할 수 없습니다. 악성코드 라이선스가 만료되거나 삭제된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 시간 창이 만료된 후 시스템은 해당 파일에 `Unavailable(사용 불가)` 속성을 할당합니다.

AMP for Networks 및 Cisco Threat Grid를 구축하는 경우에만 악성코드 라이선스가 필요합니다. 악성코드 라이선스가 없는 경우, Firepower Management Center은 엔드포인트 악성코드 이벤트용 AMP 및 IOC(보안 침해 지표)를 AMP 클라우드에서 받을 수 있습니다.

파일 및 악성코드 정책을 위한 라이선스 요구 사항에 있는 중요 정보도 참조하십시오.

## 7000 및 8000 시리즈 디바이스에 대한 VPN 라이선스

VPN을 사용하면 인터넷이나 기타 네트워크 등 공개 소스를 통해 엔드포인트 간 안전한 터널을 설정할 수 있습니다. 7000 및 8000 Series 디바이스의 가상 라우터 간에 안전한 VPN 터널을 구축하도록 Firepower System을 구성할 수 있습니다. VPN을 활성화하려면 보호 및 제어 라이선스도 활성화해야 합니다. VPN 라이선스를 구입하려면 영업팀에 문의하십시오.

VPN 라이선스가 없는 경우, 7000 및 8000 Series디바이스에서 VPN 구축을 구성할 수 없습니다. 구축은 생성할 수 있지만 거기에 추가할 VPN이 활성화된 라우팅 인터페이스가 없으면 효용이 없습니다.

Firepower Management Center에서 VPN 라이선스를 삭제하거나 개별 디바이스에서 VPN을 비활성화하는 경우, 영향을 받는 디바이스가 현재 VPN 구축을 중단하지 않습니다. 기존 구축을 수정 및 삭제할 수는 있지만 영향을 받는 디바이스에 변경 사항을 구축할 수는 없습니다.

# 디바이스 스택 및 고가용성 쌍의 기본 라이선스

개별 디바이스는 해당 라이선스를 보유한 후 7000 또는 8000 Series 디바이스 고가용성 쌍으로 스태킹 또는 구성될 수 있습니다. 디바이스를 스태킹한 후에는 전체 스택에 대해서만 라이선스를 변경할 수 있습니다. 그러나 7000 또는 8000 Series 디바이스 고가용성 쌍에서 활성화된 라이선스를 변경할 수 없습니다.

디바이스 스택 관련 정보 및 디바이스 고가용성 요구 사항도 참조하십시오.

# 기본 라이선스 보기

프로시저

필요에 따라 다음 중 하나를 수행합니다.

| 보려는 내용 | 수행해야 할 작업 |
|---|---|
| Firepower Management Center에 추가한 기본 라이선스 및 해당 유형, 상태, 사용, 만료 날짜를 포함하는 세부정보, 그러한 라이선스가 적용되는 매니지드 디바이스. | **System(**시스템**)** > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.<br>요약에는 구입한 라이선스의 수와 사용 중인 라이선스의 수(괄호로 표시)가 나와 있습니다. |
| 각 매니지드 디바이스에 적용된 라이선스 | **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다. |
| 상태 모니터에서 라이선스 상태 | 기본 라이선스 모니터 상태 모듈을 상태 정책에 사용합니다. 자세한 내용은 상태 모니터링, 상태 모듈 및 상태 정책 생성을 참조하십시오. |
| 대시보드의 라이선스 개요 | Product Licensing(제품 라이선싱) 위젯을 원하는 대시보드에 추가합니다. 자세한 내용은 제품 라이선싱 위젯, 대시보드에 위젯 추가 및 사용자 역할별 대시보드 위젯 가용성을 참조하십시오. |

# 라이선스 키를 식별합니다.

라이선스 키는 Cisco 라이선스 등록 포털에서 Firepower Management Center를 고유하게 식별합니다. 관리 포트 (eth0)의 MAC 주소와 제품 코드 (예를 들어, 66)의 구성 된는 Firepower Management Center; 예를 들어, 66:00:00:77:FF:CC:88 합니다.

Cisco License Registration Portal에서 라이선스 키를 사용하여 필요한 라이선스 텍스트를 가져오고 라이선스를 Firepower Management Center에 추가합니다.

프로시저

단계 **1** **System(**시스템**)** > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.

단계 **2** **Add New License(**새 라이선스 추가**)**를 클릭합니다.

단계 **3** **Add Feature License(**기능 라이선스 추가**)** 대화상자 상단에 있는 **License Key(**라이선스 키**)** 필드 값을 참조하십시오.

다음에 수행할 작업

- 라이선스를 Firepower Management Center에 추가합니다. 기본 라이선스 생성 및 추가 Firepower Management Center, 11 페이지를 참조하십시오.

  이 절차에는 라이선스 키를 사용하여 실제 라이선스 텍스트를 생성하는 과정이 포함됩니다.

# 기본 라이선스 생성 및 추가 Firepower Management Center

참고 백업이 완료된 후 라이선스를 추가할 경우, 이 라이선스는 백업이 복구된다고 해도 제거되거나 덮어써지지 않습니다. 복원 시 충돌을 방지하려면 백업을 복원하기 전에 라이선스가 어디에 사용되었는지에 유의하여 해당 라이선스를 제거합니다. 그리고 백업을 복원한 후 라이선스를 추가하고 재구성합니다. 충돌이 발생하면 Support(지원부)에 문의하십시오.

팁 또한 지원 사이트에 로그인한 후 **Licenses(**라이선스**)** 탭에서 라이선스를 요청할 수 있습니다.

시작하기 전에

- 라이선스를 구매할 때 Cisco가 제공한 소프트웨어 클레임 인증서에 PAK(제품 활성화 키)가 있는지 확인합니다. 레거시, Cisco 이전 라이선스가 있는 경우 지원팀에 문의합니다.
- Firepower Management Center에 대한 라이선스 키를 식별합니다. 라이선스 키를 식별합니다., 10 페이지를 참조하십시오.
- 이 절차를 완료하려면 사용자 계정의 자격 증명이 필요합니다.

프로시저

단계 **1** **System(**시스템**)** > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.

단계 **2** **Add New License(**새 라이선스 추가**)**를 클릭합니다.

단계 **3** 해당하는 작업을 계속 진행합니다.

- 이미 라이선스 텍스트를 가져온 경우 8단계로 건너뜁니다.
- 여전히 라이선스 텍스트를 가져와야 한다면 다음 단계로 이동합니다

단계 **4** **Get License(**라이선스 가져오기**)**를 클릭하여 Cisco 라이선스 등록 포털을 엽니다.

참고 현재 컴퓨터를 사용하여 인터넷에 액세스할 수 없는 경우, 액세스가 가능한 컴퓨터로 전환하고 http://cisco.com/go/license로 이동합니다.

단계 **5** 라이선스 등록 포털에서 PAK로 라이선스를 생성합니다.

이 단계에는 구매 과정에서 받은 PAK 뿐만 아니라 Firepower Management Center에 대한 라이선스 키도 필요합니다.

자세한 내용은 제품 라이선스 등록 포털, 3 페이지를 참조하십시오.

단계 **6** 라이선스 등록 포털이나 라이선스 등록 포털에서 발송한 이메일에서 라이선스 텍스트를 복사합니다.

중요 포털 또는 이메일 메시지에 있는 라이선스 텍스트 블록에는 하나 이상의 라이선스가 포함될 수 있습니다. 각 라이선스는 BEGIN LICENSE 행과 END LICENSE 행으로 구분됩니다. 한 번에 라이선스 하나만 복사하고 붙이도록 합니다.

단계 **7** Firepower Management Center 웹 인터페이스에서 **Add Feature License(**기능 라이선스 추가**)** 페이지로 돌아갑니다.

단계 **8** 라이선스 텍스트를 **License(**라이선스**)** 필드에 붙입니다.

단계 **9** **Verify License(**라이선스 확인**)**을 클릭합니다.

라이선스가 유효하지 않은 경우, 라이선스 텍스트를 제대로 복사했는지 확인합니다.

단계 **10** **Submit License(**라이선스 제출**)**을 클릭합니다.

다음에 수행할 작업

- 라이선스를 매니지드 디바이스로 할당합니다. 디바이스 관리 페이지에서 매니지드 디바이스에 라이선스 할당, 14 페이지을 참조하십시오. 매니지드 디바이스에서 라이선스가 부여된 기능을 사용하려면 그러한 디바이스에 라이선스를 반드시 할당해야 합니다.

# FTD 디바이스에서 사용할 클래식 라이선스를 변환하는 방법

LRP(라이선스 등록 포털) 또는 CSSM(Cisco Smart Software Manager)를 사용하여 라이선스를 전환할 수 있으며, 디바이스에 이미 할당된 미사용 PAK(제품 인증 키) 또는 기본 라이선스를 전환할 수 있습니다.

중요 이 프로세스를 취소할 수 없습니다. 라이선스가 원래 기본 라이선스였더라도 스마트 라이선스를 기본 라이선스로 전환할 수 없습니다.

Cisco.com에 있는 문서에서 기본 라이선스는 "traditional(전통적)" 라이선스라도고 합니다.

시작하기 전에

- 기본 라이선스가 아직 제품 인스턴스에 할당되지 않은 미사용 PAK인 경우, 기본 라이선스를 스마트 라이선스로 전환하는 것은 어렵지 않습니다.
- 하드웨어가 Firepower Threat Defense를 실행할 수 있어야 합니다. *Cisco Firepower* 호환성 가이드(https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html)를 참조하십시오.
- 스마트 어카운트가 있어야 합니다. 어카운트가 없는 경우 하나를 생성합니다. 스마트 어카운트를 생성하고 라이선스 보유의 내용을 참조하십시오.

- 변환하려는 PAK 또는 라이선스가 스마트 어카운트에 나타나야 합니다.
- Cisco Smart Software Manager 대신 라이선스 등록 포털을 사용하여 전환하는 경우, 스마트 어카운트 크리덴셜이 있어야 전환 프로세스를 개시할 수 있습니다.

프로시저

단계 **1** 수행할 전환 프로세스는 라이선스 사용 여부에 따라 달라집니다.

- 전환하려는 PAK가 미사용인 경우, PAK 전환에 대한 지침을 따르십시오.
- 전환하려는 PAK가 이미 디바이스에 할당된 경우, 기본 라이선스 전환에 대한 지침을 따르십시오.

  기존 기본 라이선스가 아직 디바이스에 등록되어 있는지 확인합니다.

단계 **2** 다음 문서에서 전환 유형(PAK 또는 설치된 기본 라이선스)에 대한 지침을 참조하십시오.

- LRP를 사용하여 PAK 또는 라이선스를 변환하는 경우:
  - 라이선스 등록 포털을 통한 전환 프로세스 단계에 대한 비디오를 보시려면 https://salesconnect.cisco.com/#/content-detail/7da52358-0fc1-4d85-8920-14a1b7721780를 클릭합니다.
  - 다음 https://cisco.app.box.com/s/mds3ab3fctk6pzonq5meukvcpjizt7wu 문서에서 "Convert(전환)"을 검색합니다.

    전환 절차는 세 가지가 있습니다. 상황에 맞는 전환 절차를 선택합니다.
  - LRP(라이선스 등록 포털)(https://tools.cisco.com/SWIFT/LicensingUI/Home)에 로그인하고 위 문서의 지침을 따르십시오.
- CSSM을 활용하여 PAK 또는 라이선스를 변환하는 경우:
  - 하이브리드 라이선스를 스마트 소프트웨어 라이선스 *QRG*로 전환:

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - CSSM(https://software.cisco.com/#SmartLicensing-LicenseConversion)에 로그인하고 위 다음 문서에 있는 전환 유형(PAK 또는 설치된 기본 라이선스)에 대한 지침을 따르십시오.

단계 **3** 하드웨어에 Firepower Threat Defense를 새로 설치합니다.

하드웨어에 대한 지침을 참조하십시오(https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html).

단계 **4** Firepower Device Manager을 사용하여 이 디바이스를 독립형 디바이스로 관리하려는 경우:

*Firepower Device Manager*용 *Cisco Firepower Threat Defense* 구성 가이드(https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html)에서 디바이스 라이선싱에 관한 정보를 참조하십시오.

이 절차의 나머지 부분을 건너뜁니다.

단계 **5** 이미 Firepower Management Center에 스마트 라이선싱을 구축한 경우:

a) 새 Firepower Threat Defense 디바이스에서 스마트 라이선싱을 설정합니다.

여러 매니지드 디바이스에 라이선스 할당의 내용을 참조하십시오.

b) 새 스마트 라이선스가 디바이스에 성공적으로 적용되었는지 확인합니다.

FTD 라이선스 및 라이선스 상태 보기의 내용을 참조하십시오.

단계 **6** 아직 Firepower Management Center에 스마트 라이선싱을 구축하지 않은 경우:

스마트 라이선스 등록의 내용을 참조하십시오.

# 디바이스 관리 페이지에서 매니지드 디바이스에 라이선스 할당

몇 가지 예외는 있지만 매니지드 디바이스에서 비활성화한 라이선스와 관련된 기능은 사용할 수 없습니다.

참고 동일한 보안 모듈/엔진에 있는 컨테이너 인스턴스의 경우, 각 인스턴스에 라이선스를 적용합니다. 참고로 보안 모듈/엔진는 보안 모듈/엔진의 모든 인스턴스에 대해 기능당 하나의 라이선스만 사용합니다.

시작하기 전에

- 디바이스를 Firepower Management Center에 추가합니다. FMC에 디바이스 추가의 내용을 참조하십시오.
- 이 작업을 수행하려면 관리자 또는 네트워크 관리자 권한으로 로그인해야 합니다. 여러 도메인을 사용하여 작업하는 경우 리프 도메인에서 이 작업을 수행해야 합니다.
- 스마트 라이선스를 할당하는 경우:
  - 한 번에 여러 디바이스에 스마트 라이선스를 적용 해야 하는 경우 다음 절차를 수행하는 대신 스마트 라이선스 페이지를 사용합니다. 여러 매니지드 디바이스에 라이선스 할당의 내용을 참조하십시오.
  - 스마트 라이선스를 매니지드 디바이스에 배포 준비: 스마트 라이선스 등록 참조

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 디바이스를 클릭합니다.

단계 4 License(라이선스) 섹션 옆에 있는 수정( )을 클릭합니다.

단계 5 해당 확인란을 선택하거나 지우고 디바이스에 대한 라이선스를 할당하거나 비활성화합니다.

단계 6 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 스마트 라이선스를 할당하는 경우, 라이선스 상태를 확인합니다.

  **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**로 이동하여 Smart License(스마트 라이선스) 테이블 상단에 있는 필터에 디바이스의 호스트 이름 또는 IP 주소를 입력한 후, 라이선스 유형별 각 디바이스에 녹색 원(확인 표시( ))만 표시되는지 확인합니다. 다른 아이콘이 표시되는 경우, 아이콘 위에 마우스를 놓으면 자세한 정보가 표시됩니다.

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

# 라이선스 만료


- 라이선스 만료 vs. 서비스 서브스크립션 만료
- Smart Licensing
- 특정 라이선스 예약
- Classic Licensing
- 서브스크립션 갱신


## 라이선스 만료 **vs.** 서비스 서브스크립션 만료

**Q.** Firepower 기능 라이선스가 만료되나요?

**A.** 엄밀히 말해 Firepower 기능 라이선스는 만료되지 않습니다. 대신 그러한 라이선스를 지원하는 서비스 서브스크립션이 만료됩니다. 서비스 서브스크립션에 대한 세부정보는 https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html에서 사용 가능한 *Firepower Management*

*Center* 구성 가이드의 "Service Subscriptions for Firepower Features(Firepower 기능용 서비스 서브스크립션)"을 참조하십시오.

### Smart Licensing

**Q.** 제품 인스턴스 등록 토큰이 만료될 수 있나요?

**A.** 토큰은 지정된 유효 기간 내에 제품 등록에 사용되지 않으면 만료될 수 있습니다. Cisco Smart Software Manager에서 토큰을 생성하는 경우, 토큰 유효일수를 설정합니다. 토큰을 사용하여 Firepower Management Center을 등록하기 전에 토근이 만료되는 경우, 새 토큰을 생성해야 합니다.

토큰을 사용하여 Firepower Management Center을 등록한 경우, 토큰 만료일은 더 이상 의미가 없습니다. 토큰 만료일이 경과하는 경우, 해당 토큰을 사용하여 등록한 Firepower Management Center에 아무런 영향도 주지 않습니다.

토큰 만료일은 서브스크립션 만료일에 영향을 주지 않습니다.

자세한 내용은 *Cisco Smart Software Manager* 사용자 가이드를 참조하십시오.

**Q.** 스마트 라이선스/서비스 서브스크립션이 만료되었거나 만료될 예정이라면 어떻게 알 수 있나요?

**A.** 서비스 서브스크립션이 언제 만료되는지 (또는 언제 만료되었는지) 확인하려면 Cisco Smart Software Manager에서 사용자 엔타이틀먼트를 검토합니다.

Firepower Management Center에서 **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택하여 기능 라이선스에 대한 서비스 서브스크립션이 현재 준수 상태인지 확인할 수 있습니다. 이 페이지의 테이블에서 제품 등록 토큰을 통해 Firepower Management Center와 연결된 스마트 라이선스 엔타이틀먼트를 간략히 보여줍니다. **License Status(**라이선스 상태**)**를 기준으로 기능 라이선스에 대한 서비스 서브스크립션이 현재 준수 상태인지 확인할 수 있습니다.

Firepower Device Manager에서 Smart License(스마트 라이선스) 페이지를 사용하여 시스템에 대한 현재 라이선스 상태를 확인합니다. **Device(**디바이스**)**를 클릭한 다음 Smart License(스마트 라이선스) 요약에서 **View Configuration(**구성 보기**)**를 클릭합니다.

또한 Cisco Smart Software Manager가 라이선스 만료 3개월 전에 사용자에게 알림을 보냅니다.

**Q.** 스마트 라이선스/서브스크립션이 만료되면 어떻게 되나요?

**A.** 구매한 서비스 서브스크립션이 만료되는 경우, Firepower Management Center와 스마트 어카운트에 해당 어카운트가 미준수 상태인 것으로 표시됩니다. Cisco가 서브스크립션을 갱신해야 한다고 알려줍니다. Subscription Renewals(서브스크립션 갱신)을 참조하십시오. 다른 영향은 없습니다.

### 특정 라이선스 예약

**Q.** 특정 라이선스 예약이 만료되면 어떻게 되나요?

**A.** SLR 라이선스는 기간이 정해져 있습니다.

필요한 라이선스가 사용 불가능하거나 만료된 경우, 다음 작업이 제한됩니다.

- 디바이스 등록
- 정책 구축

### Classic Licensing

**Q.** 기본 라이선스/서비스 서브스크립션이 만료되었거나 만료될 예정이라면 어떻게 알 수 있나요?

**A.** Firepower Management Center에서 **System(**시스템**)** > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.

이 페이지에서 테이블에는 Firepower Management Center에 추가된 기본 라이선스가 요약되어 있습니다.

**Status(**상태**)** 필드를 기준으로 기능 라이선스에 대한 서비스 서브스크립션이 현재 준수 상태인지 확인할 수 있습니다.

**Expires(**만료**)** 필드의 날짜를 기준으로 서비스 서브스크립션이 언제 만료되는지 (또는 언제 만료되었는지) 확인할 수 있습니다.

또한 Cisco 제품 라이선스 등록 포털에서 라이선스 정보를 검토하여 이 정보를 얻을 수 있습니다.

**Q.** 'IPS 기간 서브스크립션이 여전히 IPS에 필요한가'의 의미는 무엇일까요?

**A.** 이 메시지는 보호 및 제어 기능은 사용 권한 라이선스(영구적) 뿐만 아니라 주기적으로 갱신해야 하는 하나 이상의 관련 서비스 서브스크립션이 필요하다는 것을 알려줍니다. 사용하려는 서비스 서브스크립션이 현재 사용 중이고 만료가 임박하지 않은 경우, 아무런 작업도 필요하지 않습니다.

**Q.** 기본 라이선스/서브스크립션이 만료되면 어떻게 되나요?

**A.** 기본 라이선스를 지원하는 서비스 서브스크립션이 만료된 경우, Cisco가 해당 서브스크립션을 갱신해야 하다고 알려줍니다. Subscription Renewals(서브스크립션 갱신)을 참조하십시오.

기능 유형에 따라 관련 기능을 사용할 수 없습니다.

표 *3:* 기본 라이선스/서브스크립션 만료의 영향

| 기본 라이선스 | 가능한 지원 서브스크립션 | 만료 영향 |
|---|---|---|
| 제어 | TA, TAC, TAM, TAMC | 기존 Firepower 기능을 계속 사용할 수 있지만, 애플리케이션 서명 업데이트를 포함해 VDB 업데이트를 다운로드할 수 없습니다. |
| 보호 | TA, TAC, TAM, TAMC | 침입 검사는 계속 수행할 수 있지만, 침입 규칙 업데이트를 다운로드할 수 없습니다. |

| 기본 라이선스 | 가능한 지원 서브스크립션 | 만료 영향 |
|---|---|---|
| URL 필터링 | URL, TAC, TAMC | • URL 조건이 포함된 액세스 제어 규칙은 즉시 URL 필터링을 중지합니다.<br>• 카테고리 및 평판에 따라 트래픽을 필터링하는 다른 정책(예: SSL 정책)도 즉시 해당 작업을 중지합니다.<br>• Firepower Management Center는 더 이상 업데이트를 URL 데이터로 다운로드할 수 없습니다.<br>• URL 카테고리 및 평판 필터링을 수행하는 기존 정책을 다시 구축할 수 없습니다. |
| 악성코드 | AMP, TAM TAMC | • 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 시간 창이 만료된 후 시스템은 해당 파일에 `Unavailable`(사용 불가) 속성을 할당합니다.<br>• 시스템이 AMP 클라우드 쿼리를 중지하며 AMP 클라우드에서 전송하는 회귀적 이벤트 확인을 중지합니다.<br>• Firepower용 AMP 구성이 포함된 경우, 기존 액세스 제어 정책은 재적용할 수 없습니다. |

서브스크립션 갱신

**Q.** 만료되는 기본 라이선스를 어떻게 갱신하나요?

**A.** 만료되는 기본 라이선스를 갱신하려면, 새 PAK 키를 구매하고 동일한 프로세스를 수행하여 새로운 스크립션을 구현하면 됩니다.

**Q.** Firepower Management Center에서 Firepower 서비스 서브스크립션을 갱신할 수 있나요?

**A.** 아닙니다. Firepower 서비스 서브스크립션(클래식 또는 스마트)을 갱신하려면 Cisco Commerce Workspace 또는 Cisco Service Contract Center 중 하나를 통해 새 서브스크립션을 구입해야 합니다.

# 이 가이드의 기타 라이선싱 정보

| 대상 | 확인 |
|---|---|
| Smart Licensing authority와의 FMC 통신용 인터페이스에 대한 정보 | 디바이스 관리 인터페이스 및 하위 항목 |

| 대상 | 확인 |
| --- | --- |
| 라이선싱 방화벽 요구사항 | 인터넷 액세스 요구 사항 |
| 이 문서 각 절차의 시작 부분에 있는 테이블에 설명된 라이선스 정보 | 문서 내 라이선스 설명 |
| 백업 복원 시 중요한 라이선스 고려 사항 | 백업 및 복원 |
| 규칙 및 정책 적용 및 트리거 방식에 대한 라이선스의 효과 | 다음을 포함하는 정책 및 규칙 정보<br>• 액세스 제어 규칙 관리<br>• 액세스 제어 규칙 구성 요소조건에 대한 정보<br>• TLS/SSL 규칙 지침 및 제한 사항<br>• TLS/SSL 규칙 구성 요소<br>• QoS 정책을 사용한 속도 제한 |
| 라이선싱 관련 구축 및 정책 또는 규칙 관리 오류 | 다음을 포함해 이 가이드에 설명된 정책 및 규칙 정보<br>• 규칙 및 기타 정책 경고<br>• QoS 정책을 사용한 속도 제한 |
| SSL 라이선싱 요구 사항 | Firepower Threat Defense에 대한 SSL 설정의 사전 요구 사항 |
| SSL 프리프로세서 기능에 대한 라이선싱 요구 사항 | SSL 전처리기 |
| 엔드포인트 통합 AMP에 대한 라이선싱 | 악성코드 방지 비교: Firepower 대 AMP for Endpoints |
| 클라이언트 및 서비스 서버의 라이선싱 및 라이선스 및 스트림 리어셈블리 | TCP 스트림 전처리 옵션 |
| 라이선싱 및 Cisco Threat Intelligence Director(TID) | 플랫폼, 요소 및 라이선스 요구 사항 |
| 연결 이벤트에 대한 라이선싱 영향 | 연결 이벤트 필드 채우기 요구 사항 |
| 라이선싱 및 기타 대시보드 위젯에 대한 정보 | 사용자 역할별 대시보드 위젯 가용성<br>맞춤형 분석 위젯 |
| 라이선싱 상태 모니터에 대한 정보 | 스마트 라이선스 모니터 및 기본 라이선스 모니터에 대한 정보 상태 모듈 |

# Firepower 라이선싱 관련 추가 정보

일반 라이선싱 관련 질문 해결을 위한 자세한 내용은 다음 문서를 참조하시기 바랍니다.

- *Firepower* 라이선스 *FAQ(*자주 묻는 질문*)* 문서:

  https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html

- *Cisco Firepower System* 기능 라이선스 문서:

  https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

# Cisco 지원 진단

Cisco Support Diagnostics는 사용자가 활성화하는 클라우드 기반 TAC 지원 서비스입니다. 이 서비스를 활성화하면 FMC(Firepower Management Center)와 FTD(Firepower Threat Defense), FMC(Firepower Management Center)와 Cisco Cloud 간의 보안 연결이 설정되어 시스템 상태 관련 정보를 스트리밍합니다.

Cisco Support Diagnostics는 TAC 사례 중에 Cisco TAC가 디바이스에서 필수 데이터를 안전하게 수집하게 하여, 문제 해결 중에 향상된 사용자 경험을 제공합니다. 또한 Cisco의 자동 문제 탐지 시스템을 이용해 운영 상태 데이터를 주기적으로 수집하고 처리하여, 문제가 발생하기 전에 미리 통보합니다. TAC 사례 중의 데이터 수집 서비스는 지원 계약을 한 모든 사용자가 이용할 수 있지만, 사전 알림 서비스는 특정 서비스 계약이 있는 사용자만 사용할 수 있습니다.

Cisco Support Diagnostics나 Cisco Success Network를 활성화하면, Firepower Management Center는 Firepower Management Center와 Cisco Cloud 간의 보안 연결을 항상 설정하고 유지 관리합니다. 언제든 Cisco Success Network와 Cisco Support Diagnostics를 모두 비활성화하면 이 연결을 끌 수 있으며, 이 경우 이상의 기능과 Cisco Cloud의 연결이 끊어집니다. 그러나 Cisco Support Diagnostics를 활성화하면, Firepower Threat Defense(FTD) 및 Cisco Cloud와 함께 FMC와 Cisco Cloud 간의 보안 연결이 설정 및 유지됩니다. 따라서 Cisco Support Diagnostics가 비활성화되면 두 보안 연결이 모두 해제됩니다.

관리자는 특정 시스템 기능에 대한 문제 해결 파일 생성의 단계에 따라 FMC에서 수집하는 샘플 데이터 세트를 확인하여 문제 해결 파일을 열고, 파일을 열어 내용을 살펴볼 수 있습니다.

FMC는 수집된 데이터를 **System(**시스템**)** > **Integration(**통합**)** > **Cloud Services(**클라우드 서비스**)** 페이지에 지정된 지역 클라우드로 전송합니다. 이 설정은 Cisco Success Network에서 설명하는 Cisco Support Network와 다음을 이용한 이벤트 분석 Cisco SecureX Threat Response에서 설명하는 Cisco Threat Response 통합에도 사용합니다.

### Cisco Support Diagnostics 활성화

Cisco Support Diagnostics는 Cisco Smart Software Manager를 이용해 Firepower Management Center를 등록할 때 활성화합니다. 참고, 스마트 라이선스 등록.

**Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 페이지에서 현재 Cisco Support Diagnostics 등록 정보를 확인하고, 등록 상태를 변경할 수 있습니다. 참고, Cisco 지원 진단 등록 변경, 21 페이지.

# Cisco 지원 진단 등록 변경

Cisco Support Diagnostics는 Cisco Smart Software Manager를 이용해 Firepower Management Center를 등록할 때 활성화합니다. 그 후 다음 절차를 사용하여 등록 상태를 확인 또는 변경합니다.

프로시저

단계 **1** **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 클릭합니다.

단계 **2** Cisco Support Diagnostics 옆에 있는 Smart License Status(스마트 라이선스 상태)에서 **Enabled/Disabled(**활성화/비활성화**)** 제어를 클릭하고 설정을 적절하게 변경합니다.

참고 계속하기 전에 **Enabled/Disabled(**활성화/비활성화**)** 제어 옆에 있는 정보를 읽으십시오.

단계 **3** **Apply Changes(**변경 사항 적용**)**를 클릭합니다.

다음에 수행할 작업

Cisco Support Diagnostics를 활성화했다면, **System(**시스템**)** > **Integration(**통합**)** > **Cloud Services(**클라우드 서비스**)** > **Cisco Cloud Region(Cisco Cloud** 지역**)**에서 지역 클라우드 설정을 확인해 시스템 데이터 전송 위치를 설정합니다.

# 라이선싱 기록

| 기능 | 버전 | 세부 사항 |
|---|---|---|
| 고가용성 쌍의 FMCv(Virtual FMC) | 6.7 | FMC 고가용성 설정에 대한 라이선스 요구 사항의 내용을 참조하십시오. |
| Firepower 4100/9300의 FTD에 대한 다중 인스턴스 기능 라이선스 | 6.3 | 이제 Firepower 4100/9300에서 다중 FTD 컨테이너 인스턴스를 구축할 수 있습니다. 보안 모듈/엔진별 기능당 하나의 라이선스만 필요합니다. 기본 라이선스가 각 인스턴스에 자동으로 할당됩니다.<br>신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**<br>지원되는 플랫폼: Firepower 4100/9300에서의 FTD |

| 기능 | 버전 | 세부 사항 |
| --- | --- | --- |
| 에어 갭(Air-Gapped) 구축을 위한 특정 라이선스 예약 | 6.3 | Cisco License Authority와 통신하기 위해 인터넷에 연결할 수 없는 고객은 특정 라이선스 예약을 사용할 수 있습니다. 자세한 내용은 SLR(Specific License Reservation)을 참조하십시오.<br>신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)** (이 옵션은 기본적으로 사용할 수 없습니다.)<br>지원되는 플랫폼: FMC, FTD |
| 제한된 고객에 대한 내보내기 제어 기능 | 6.3 | 제한된 기능을 사용할 수 없는 스마트 어카운트를 보유한 특정 고객은 승인을 얻고 기간이 정해진 라이선스를 구매할 수 있습니다. 자세한 내용은 (전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화을 참조하십시오.<br>지원되는 플랫폼: FMC, FTD |
| Firepower Threat Defense 디바이스 스마트 라이선싱 구축을 위한 고급 지침 | 6.3 | 새 항목이 엔드 투 엔드 지침: Firepower Threat Defense 디바이스 라이선스를 부여하는 방법를 제공합니다. 이 항목에서 링크된 항목에서 새롭게 개선된 정보를 확인할 수도 있습니다. |
| 시스템 상태 정보를 Cisco Cloud로 스트리밍하도록 허용하는 Cisco Support Diagnostics | 6.5 | Cisco Support Diagnostics는 Firepower Management Center와 Firepower Threat Defense가 보안 연결을 통해 시스템 상태 관련 정보를 Cisco Cloud로 스트리밍할 수 있게 하는, 사용자가 활성화하는 기능입니다. 자세한 내용은 Cisco 지원 진단, 20 페이지을 참조해 주십시오.<br>신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**<br>지원되는 플랫폼: FMC, FTD |