# 라이선싱에 대한 FAQ(자주 묻는 질문)

초판: 2018년 1월 18일

최종 변경: 2023년 9월 8일

## 라이선싱에 대한 FAQ(자주 묻는 질문)

라이선싱에 대한 FAQ(자주 묻는 질문)에서는 스마트 및 클래식 라이선싱, 기능 라이선스 서비스 구독, 만료된 구독, 고가용성 및 클러스터 구축을 위한 라이선스 요구 사항 등에 대한 일반적인 질문에 대한 답변을 제공합니다.

시스코 라이선싱에 대한 자세한 내용은 cisco.com/go/licensingguide를 참조하세요.

## 이 문서는 공식 주문 가이드 또는 라이선스 계약을 대체할 수 없습니다.

이 문서의 정보는 일반 정보를 제공하기 위한 것이지만 변경될 수 있으며 라이선싱 옵션의 전체 복잡성을 파악할 수는 없습니다.

시스코 담당자와 협력하여 제품 및 구축에 적합한 라이선스를 구매하십시오.

만료되었거나 비준수 라이선스에 대한 정보의 경우, 라이선스 또는 구매 계약이 이 문서 또는 제품용 구성 가이드의 정보를 대신합니다.

## 일반 라이선스 관리

**Q.** 어떤 라이선스가 필요합니까?

**A.** 필요한 라이선스는 하드웨어에서 실행할 소프트웨어에 따라 달라집니다.

소프트웨어를 실행하려는 경우:

- 이 문서와 추가 정보, 17 페이지에 언급된 문서로 시작합니다.
- Secure Firewall Management Center 하드웨어에는 라이선스가 필요하지 않습니다.

  Management Center Virtual 어플라이언스에는 라이선스가 필요합니다.

  자세한 내용은 사용 중인 버전에 대한 Cisco Secure Firewall Management Center 관리 가이드의 라이선싱 장에서 "Management Center Virtual 라이선스" 항목을 참조하십시오.
- Secure Firewall Threat Defense 디바이스는 스마트 라이선싱을 사용합니다. 자세한 내용은 Threat Defense 기능용 스마트 라이선싱, 4 페이지를 참고하십시오.

- 다른 모든 디바이스는 클래식 라이선싱을 사용합니다. 자세한 내용은 Threat Defense 기능의 클래식 라이선싱, 7 페이지를 참고하십시오.

Secure Firewall ASA와 같은 다른 소프트웨어를 실행하려는 경우:

- 소프트웨어 제품 설명서를 참조하십시오.
- 동일한 하드웨어라도 실행하는 소프트웨어에 따라 라이선싱 요구 사항이 다를 수 있습니다.

**Q.** management center에 라이선스가 필요합니까?

**A.** 버전 6.0 이상에서 management center는 디바이스의 기능 라이선스를 관리하지만, management center 하드웨어를 사용하는 데 라이선스가 필요하지 않습니다. Management Center Virtual 어플라이언스에는 라이선스가 필요합니다. 자세한 내용은 사용 중인 버전에 대한 Cisco Secure Firewall Management Center 관리 가이드의 라이선싱 장을 참조하십시오.

버전 5.4.x 이하에서 FireSIGHT Defense Center를 사용하려면 FireSIGHT 라이선스가 필요합니다. 초기 설정 중에 이 라이선스를 Defense Center에 추가해야 합니다.

**Q.** 디바이스에 클래식 또는 스마트 라이선스가 필요합니까?

**A.** 하드웨어가 아닌 소프트웨어에 따라 제품 해당 제품에 필요한 라이선스 유형이 결정됩니다.

- Threat Defense 소프트웨어를 실행하는 디바이스에는 스마트 라이선싱이 필요합니다.
- 그 밖의 모든 디바이스 ASA with FirePOWER Services, 7000 또는 8000 시리즈, NGIPSv에는 클래식 라이선스가 필요합니다.
- Threat Defense 소프트웨어를 실행하지 않는 하드웨어의 경우 해당 소프트웨어 제품의 설명서를 참조하십시오.

  예를 들어, FirePOWER 서비스 없이 Cisco ASA(Cisco Adaptive Security) 소프트웨어를 실행하는 하드웨어의 경우 https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/licenseroadmap.html를 참조하십시오.

**Q.** 스마트 라이선스와 클래식 라이선스의 차이점은 무엇입니까?

**A.** 일부 제품은 하나 또는 다른 유형의 라이선스가 필요합니다(위의 내용 참조).

각 유형의 라이선스를 구축하는 세부 사항 및 프로세스는 서로 다릅니다.

- 스마트 라이선스에 대한 자세한 내용은 Threat Defense 기능용 스마트 라이선싱, 4 페이지를 참조하십시오.
- 클래식 라이선스("traditional(전통적)" 라이선스라고도 함)에 대한 자세한 내용은 Threat Defense 기능의 클래식 라이선싱, 7 페이지를 참조하십시오.

각 라이선스 유형 구축에 대한 추가 정보는 Cisco Secure Firewall Management Center 관리 가이드의 라이선싱 장에서 확인할 수 있습니다.

**Q.** management center가 서로 다른 라이선스 유형(스마트 및 클래식)을 사용하는 디바이스를 관리할 수 있습니까?

**A.** 예. 그러나 management center를 통해 라이선스 유형을 관리하는 단계는 약간 다릅니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드에서 라이선싱 장을 참조하십시오.

**Q.** 클래식 라이선스를 스마트 라이선스 자격으로 전환할 수 있습니까?

**A.** 일반적으로, 하드웨어에서 클래식 라이선스를 사용하는 소프트웨어 제품 또는 스마트 라이선스를 사용하는 소프트웨어 제품을 실행할 수 있는 경우 라이선스를 전환할 수 있습니다.

어카운트에서 어떤 PAK를 변환할 수 있는지 확인할 수 있습니다.

- LRP(Product License Registration Portal)에서 PAK가 스마트 어카운트에 추가되면 **PAKs or Tokens(PAK** 또는 토큰**)** 탭을 클릭하고 PAK 위에 마우스를 올려놓고 파란색 화살표가 표시되도록 한 다음 파란색 화살표를 클릭합니다. 라이선스를 변환할 수 있는 경우, **Convert to Smart Licensing(**스마트 라이선싱 으로 변환**)** 옵션이 표시됩니다. LRP는 PAK와 연결된 제품을 표시하지만, PAK의 변환 가능 여부와 관계없이 모든 PAK를 나열합니다.
- Cisco Smart Software Manager(CSSM)에서 **Convert to Smart Licensing(**스마트 라이선싱으로 변환**)** 탭을 클릭하여 전환 가능한 PAK를 확인합니다. 목록의 각 PAK와 연결된 제품을 확인하려면 PAK를 클릭하여 세부 정보를 확인합니다. (CSSM은 변환 가능한 PAK만 나열하지만, PAK가 연결된 제품을 확인하려면 각 PAK를 클릭해야 합니다.)

변환 여부는 시간이 지남에 따라 변경될 수 있습니다. PAK가 변환 자격이 되면 LRP 및 CSSM에서 PAK의 상태가 자동으로 업데이트됩니다.

라이선스 변환에 대한 정보는 Cisco Secure Firewall Management Center 관리 가이드의 라이선싱 장에 있습니다.

Cisco LRP(License Registration Portal) 사용 설명서에서 "LRP의 PAK 라이선스 SKU를 SSM(Smart Software Manager)의 스마트 라이선스 자격으로 변환"도 참조하십시오.

**Q.** 스마트 라이선스 자격을 클래식 라이선스로 전환할 수 있습니까?

**A.** 아니요. 실수로 클래식 라이선스 대신 스마트 라이선스 자격을 사용한 경우에는 Cisco TAC에 문의하십시오.

**Q.** 라이선스와 서비스 구독의 차이점은 무엇입니까?

**A.** 기능 라이선스는 사용 권한 라이선스입니다. 라이선스는 영구적입니다. 라이선스를 지원하는 서비스 구독을 구매하는지 여부와 관계없이, 기능에 처음 설치하는 버전의 기능을 계속 사용할 수 있습니다.

서비스 구독은 기능과 관련된 업데이트를 다운로드할 수 있는 자격 입니다. 예를 들어 Threat 라이선스를 지원하기 위해 T(Threat) 구독을 구매하는 경우 침입 규칙 업데이트를 다운로드할 수 있습니다. 이 자격에는 기간이 정해져 있습니다. 즉, 주기적으로 만료됩니다. 자세한 내용은 라이선스 만료, 14 페이지를 참고하십시오.

기능 라이선스를 구매하는 경우 구독 기간(예: 3년)을 지정합니다.

**Q.** 서비스 구독 기간은 언제 시작되고 종료됩니까? 시작 날짜가 구매 날짜 또는 최초 활성화 날짜와 연결되어 있습니까?

**A.** 각 서비스 구독의 시작 날짜와 종료 날짜는 세일즈 오더에 지정됩니다. 구독 시작 날짜는 최초 활성화 날짜와 연결되어 있지 않습니다.

**Q.** 내 management center를 둘 이상의 스마트 어카운트에 등록할 수 있습니까? 동일한 스마트 어카운트 내 여러 가상 어카운트에 등록할 수 있습니까?

**A.** 아니요.

참고 스마트 어카운트는 스마트 라이선스와 클래식 라이선스를 모두 관리할 수 있으므로 이 답변은 두 라이선스 유형에 모두 적용됩니다.

등록을 이동해야 하는 경우, 먼저 원래 어카운트에서 management center를 등록 취소해야 합니다. 해당 Management Center 인스턴스로 관리되는 디바이스에 할당된 라이선스는 자동으로 릴리스됩니다.

**Q.** threat defense와 ASA를 동일한 섀시에서 실행 중입니다. 어떻게 라이선싱합니까?

**A.** 하드웨어 모델이 이 구성을 지원해야 합니다. 섀시를 공유하지 않는 것처럼 각 소프트웨어 제품에 라이선스를 부여합니다.

**Q.** 시스코의 라이선스 관리 툴에 대한 도움이 되는 문서는 어디에서 찾을 수 있습니까?

**A.** https://community.cisco.com/t5/licensing-enterprise-agreements/software-on-demand-training-resources-for-customers/ta-p/3639797

**Q.** 라이선스에 대한 질문이나 문제가 있는데 회사의 어카운트 관리자가 답변할 수 없는 경우에는 어떻게 해야 합니까?

**A.** licensing@cisco.com 에 문의하십시오.

# Threat Defense 기능용 스마트 라이선싱

**Q.** 스마트 라이선스란 무엇입니까?

**A.** Cisco 스마트 라이선싱은 Cisco의 새로운 라이선스 형식입니다. 이를 통해 라이선스 풀을 중앙에서 관리할 수 있습니다. 스마트 라이선스는 클래식 라이선스와 달리 특정 일련 번호나 PAK에 묶여 있지 않습니다. Secure Firewall Management Center 또는 Secure Firewall device manager에서 스마트 라이선스를 활성화합니다.

**Q.** 어떤 디바이스가 threat defense용 스마트 라이선스 기능을 사용합니까?

**A.** threat defense 소프트웨어를 실행하는 제품은 스마트 라이선싱을 사용합니다. 이러한 디바이스의 전체 목록은 Cisco FirePOWER 호환성 가이드를 참조하십시오.

**Q.** 스마트 어카운트란 무엇이며 어떻게 받을 수 있습니까?

**A.** 스마트 어카운트에는 회사에서 구매한 라이선스(스마트 및 클래식 라이선스)가 있습니다. CSSM(Smart Software Manager)에서 스마트 라이선스를 확인하고 사용하려면 먼저 스마트 라이선스가 스마트 어카운트에 있어야 합니다.

Cisco 어카운트 담당자 또는 공인 리셀러가 구매한 라이선스를 스마트 어카운트에 보관하고 스마트 어카운트를 생성해 줄 수 있습니다.

스마트 어카운트를 생성해야 하는 경우, https://software.cisco.com/smartaccounts/setup#accountcreation-account로 이동합니다. 스마트 어카운트 설정에 대한 자세한 내용은 https://www.cisco.com/c/en/us/buy/smart-accounts.html 를 참조하십시오.

**Q.** 구매한 스마트 라이선스가 내 스마트 어카운트에 표시되지 않는 경우에는 어떻게 해야 합니까?

**A.** 다음을 순서대로 확인합니다.

- 라이선스가 조직의 스마트 어카운트 내 다른 가상 어카운트에 없는지 확인합니다. 액세스할 수 없는 가상 어카운트에 라이선스가 있을 수 있으므로 조직의 스마트 어카운트 관리자에게 문의해야 합니다.
- 라이선스를 판매한 개인 또는 조직에 문의하십시오.
- Licensing@cisco.com 에 문의하십시오.

**Q.** 설정한 스마트 어카운트에 대한 액세스 권한을 회사의 다른 사용자에게 부여하려면 어떻게 해야 합니까?

**A.** https://community.cisco.com/t5/licensing-enterprise-agreements/request-access-to-an-existing-smart-account-quick-reference/ta-p/3628587?attachment-id=144211의 내용을 참조하십시오.

**Q.** 제품 인스턴스 등록 토큰이란 무엇입니까?

**A.** 제품 인스턴스 등록 토큰을 사용하면 Cisco 스마트 소프트웨어 관리자에 management center 또는 device manager를 등록할 수 있습니다. 토큰은 Cisco Smart Software Manager에서 생성합니다. 자세한 내용은 https://www.cisco.com/web/fw/softwareworkspace/smartlicensing/SSMCompiledHelps/c_Creating_a_Product_Instance_Registration_Token.html를 참고하십시오.

내보내기 제어 기능을 활성화하거나 활성화하지 않고 토큰을 생성할 수 있습니다. 그러나 일부 중요한 Threat Defense 기능의 경우 내보내기 제어 기능을 활성화해야 합니다. 어카운트에서 내보내기 제어 기능을 사용할 수 있는 경우, 토큰을 생성하기 전에 이 기능에 권한을 부여해야 하며, 토큰을 생성할 때 옵션을 선택해야 합니다. 시스코에서는 이러한 토큰을 생성하기 전에 요구사항을 미리 파악할 것을 권장합니다. (릴리스 6.3부터는 내보내기 제어 기능을 사용할 수 없는 어카운트에서도 해당 기능을 management center별로 가져올 수 있습니다. 자세한 내용은 시스코 리셀러 또는 어카운트 담당자에게 문의하십시오. 이 솔루션의 메커니즘에는 제품 인스턴스 등록 토큰이 포함되지 않습니다.)

토큰을 생성한 후 매니지드 디바이스에 추가하여 해당 디바이스를 Cisco Smart Software Manager에 등록합니다. 관리하는 디바이스를 등록한 후에는 매니지드 디바이스에 스마트 라이선스를

할당할 수 있습니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드를 참고하십시오.

**Q.** 내 management center 또는 device manager에 대한 제품 인스턴스 등록 토큰은 어디에서 찾을 수 있습니까?

**A.** Cisco Smart Software Manager의 가상 어카운트에서 토큰을 생성하고 복사할 수 있습니다. 자세한 내용은 https://www.cisco.com/web/fw/softwareworkspace/smartlicensing/SSMCompiledHelps/c_Managing_Product_Instance_Registration_Tokens.html를 참고하십시오.

**Q.** CSSM(Cisco Smart Software Manager)에 어떻게 액세스합니까?

**A.** management center에서 **System**(시스템) > **Licenses**(라이선스) > **Smart Licenses**(스마트 라이선스)를 선택하고 **Cisco Smart Software Manager**를 클릭합니다.

브라우저에서 직접 Cisco Smart Software Manager에 액세스할 수도 있습니다.

https://software.cisco.com/#module/SmartLicensing

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

**Q.** 멀티 인스턴스 구축의 경우 몇 개의 라이선스가 필요합니까?

**A.** 모든 라이선스는 (Firepower 4100의) 보안 엔진/섀시 또는 (Firepower 9300의) 보안 모듈에 대해 소비되지만 컨테이너 라이선스에 대해서는 소비되지 않습니다. 자세한 내용은 다음을 참조하십시오.

- 기본 라이선스는 디바이스당 하나씩 자동으로 할당됩니다.
- 기능 라이선스는 각 인스턴스에 대해 수동으로 할당되지만 사용자는 디바이스의 기능당 하나의 라이선스를 소비합니다. 예를 들어 3개의 보안 모듈이 있는 Firepower 9300에 대해서는 모듈당 하나의 URL 필터링 라이선스가 필요하므로 사용 중인 인스턴스 수와 관계없이 총 3개의 라이선스가 필요합니다.

**Q.** 제품이 스마트 라이선싱 서버와 통신할 수 없는 경우 어떻게 해야 합니까?

**A.** 각 제품은 는 라이선스 기관과 30일마다 통신합니다. Smart Software Manager에서 변경할 경우 제품에서 권한 부여를 새로 고침하여 즉시 변경 사항을 적용할 수 있습니다. 또는 디바이스에서 예정대로 통신할 때까지 기다릴 수 있습니다. 선택 사항으로 HTTP 프록시를 구성할 수 있습니다.

Device Manager: 최소 90일마다 제품이 직접 또는 HTTP 프록시를 통해 인터넷에 연결되어야 합니다. 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 디바이스는 최대 90일간 콜 홈 없이 작동할 수 있습니다. 유예 기간이 지난 후 디바이스가 Licensing Authority에 연락해야 합니다. 아니면 특별 라이선스가 필요한 기능의 구성을 변경할 수 없습니다. 이를 제외하면 작동에 영향을 미치지 않습니다.

Management Center: management center가 1년 동안 Smart Software Manager와 통신하지 않을 경우, 등록 취소되며 management center은 라이선스가 필요한 기능에 대해 디바이스에 구성 변경 사항을 구축할 수 없습니다. 참고: 90일 후에 management center 권한 부여가 만료되지만 1년 이내에 통신을 성공적으로 재개하여 자동으로 다시 권한을 부여할 수 있습니다. 1년이 지나면 ID 인증서가 만료되고 management center가 어카운트에서 제거되므로 수동으로 management center를 다시 등록해야 합니다.

에어 갭 환경의 옵션을 비교하거나 Smart Software Manager 온프레미스를 구축하여 License Authority와 통신하는 방법은 Cisco Secure Firewall Management Center 관리 가이드의 라이선싱 장을 참조하십시오.

**Q.** 내 디바이스에서 PLR(Permanent License Reservation, 영구 라이선스 예약)을 사용할 수 있습니까?

**A.**

- Secure Firewall Management Center가 관리하는 Secure Firewall Threat Defense:

  특정 라이선스 예약은 6.3버전부터 도입되었습니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 Licensing(라이선싱) 장을 참조하십시오.

- Secure Firewall device manager가 관리하는 Secure Firewall Threat Defense

  PLR은 릴리스 6.6에서 도입되었으며 릴리스 6.4.0.10에서도 사용 가능합니다(6.5.x에서는 제외). 자세한 내용은 Cisco Secure Firewall Device Manager 구성 가이드에서 "시스템 라이선싱" 장을 참조하십시오.

**Q.** 제품이 규정 위반 상태인 것은 무엇을 의미하며, 이러한 현상이 발생하는지 어떻게 알 수 있습니까?

**A.** 다음과 같은 상황에서 라이선스가 규정 위반이 될 수 있습니다.

- 과다 사용—제품에서 사용 불가한 c를 사용할 경우
- 라이선스 만료—한시적인 라이선스가 만료된 경우.

어카운트가 규정 미준수 상태인지 또는 규정 미준수 상태에 근접했는지 확인하려면 Management Center 또는 스마트 어카운트의 스마트 라이선싱 페이지를 확인하십시오.

# **Threat Defense** 기능의 클래식 라이선싱

**Q.** 클래식 라이선스란 무엇입니까?

**A.** 이는 시스코의 이전 형식의 라이선스입니다. 클래식 라이선스는 PAK(product authorization key, 제품 인증 키)를 활성화해야 하고 디바이스간에 양도할 수 없습니다. 클래식 라이선스는 때로 "traditional licensing(전통적 라이선스)"이라고도 합니다.

**Q.** 어떤 디바이스가 기능에 클래식 라이선스를 사용합니까?

**A.** 7000 및 8000 Series 디바이스, ASA FirePOWER 모듈 및 NGIPSv.

**Q.** 디바이스 간에 클래식 라이선스를 양도할 수 있습니까?

**A.** 안됩니다.

**Q.** PAK(제품 인증 키)란 무엇입니까?

**A.** PAK(제품 인증 키)를 사용하면 클래식 라이선스를 활성화할 수 있습니다. PAK는 사용자가 라이선스를 구매할 때 시스코에서 제공하는 소프트웨어 클레임 인증서에 포함되어 있습니다.

Cisco Product License Registration Portal(시스코 제품 라이선스 등록 포털)에서 PAK를 라이선스 키와 함께 사용하여 management center에 라이선스를 추가하는 데 필요한 라이선스 텍스트를 생성합니다.

**Q.** Cisco LRP(License Registration Portal)에 액세스하려면 어떻게 해야 합니까?

**A.** management center에서 **System**(시스템) > **Licenses**(라이선스) > **Classic Licenses**(클래식 라이선스)를 선택하고 **Add New License**(새 라이선스 추가)를 클릭한 다음 **Get License**(라이선스 가져오기)를 클릭합니다.

브라우저에서 직접 라이선스 등록 포털에 액세스할 수도 있습니다.

https://www.cisco.com/go/license

이 포털 사용에 대한 자세한 내용은 제품 라이선스 등록 툴 및 리소스(https://www.cisco.com/web/fw/tools/swift/xui/html/help.html)를 참조하십시오.

**Q.** SCC(Software Claim Certificates, 소프트웨어 클레임 인증서)는 어떻게 제공됩니까?

**A.** 물리적 디바이스(예: Firepower 8250)를 구매하면 물리적 디바이스와 함께 상자에 관련 제어 라이선스에 대한 소프트웨어 클레임 인증서 사본을 받게 됩니다.

가상 디바이스(예: management center virtual)를 구축하는 경우, 관련 제어 라이선스에 대한 소프트웨어 클레임 인증서를 이메일 첨부 파일로 수신합니다.

물리적 또는 가상 디바이스용 기능 라이선스를 구매하는 경우(예: URL 필터링) 소프트웨어 클레임 인증서를 이메일 첨부 파일로 수신합니다.

**Q.** 시스코 제품 라이선싱 등록 포털에서 PAK를 등록하기 전에 소프트웨어 클레임 인증서를 분실하거나 잘못 두는 경우 어떻게 해야 합니까?

**A.** Cisco TAC에 문의하십시오.

**Q.** 라이선스 키란 무엇입니까?

**A.** 라이선스 키는 시스코 제품 라이선스 등록 포털에서 관리하는 디바이스를 고유하게 식별합니다. 디바이스 관리에는 ASA FirePOWER 모듈 및 management center의 로컬 관리 ASDM이 포함됩니다.

이 라이선스 키의 형식은 다음과 같습니다.

*Product_code*:주소

*Product_code* 요소는 매니지드 디바이스의 유형에 따라 달라지며, *address* 요소는 매니지드 디바이스의 MAC 주소입니다. management center에서 이는 관리 인터페이스(Eth0)의 MAC 주소입니다.

예를 들어 management center의 가능한 라이선싱 키는 "66:00:00:77:FF:CC:88"입니다.

시스코 제품 라이선스 등록 포털에서 라이선스 키를 PAK와 함께 사용하여 매니지드 디바이스에 클래식 기능 라이선스를 추가하는 데 필요한 라이선스 텍스트를 생성합니다.

**Q.** 라이선스 키는 어디에서 찾을 수 있습니까?

**A.**
- management center에서 **System**(시스템) > **Licenses**(라이선스) > **Classic Licenses**(클래식 라이선스) > **Add New License**(새 라이선스 추가)를 선택합니다. License Key(라이선스 키)가 결과 대화 상자에 나타납니다.

- ASDM에서 **Configuration**(구성) > **ASA FirePOWER Configuration**(**ASA FirePOWER** 구성) > **Licenses**(라이선스)를 선택하고 **Add New License**(새 라이선스 추가)를 클릭하여 섀시에 대한 라이선스 키를 가져옵니다. 라이선스 키는 상단 근처에 있습니다. 예: 72:78:DA:6E:D9:93:35

**Q.** management center에 클래식 라이선스를 추가하는 데 필요한 라이선스 텍스트는 어디에서 찾을 수 있습니까?

**A.** 시스코 제품 라이선스 등록 포털에서 라이선스 텍스트를 생성합니다. 라이선스 텍스트를 생성한 후에는 라이선스 등록 포털 화면 또는 라이선스 등록 포털에서 보낸 이메일에서 텍스트를 복사합니다.

중요 포털 또는 이메일 메시지에 있는 라이선스 텍스트 블록에는 하나 이상의 라이선스가 포함될 수 있습니다. 한 번에 라이선스 하나만 복사하고 붙이도록 합니다. 각 라이선스는 BEGIN LICENSE(시작 라이선스) 줄로 시작하여 END LICENSE(끝 라이선스) 줄로 끝납니다. (각 라이선스를 복사하여 붙여넣을 때 이러한 줄을 포함합니다.)

**Q.** CCW(Cisco Commerce Workspace)에서 기능 라이선스를 구매한 후 언제부터 Cisco LRP(License Registration Portal)에서 라이선스 텍스트를 생성할 수 있습니까?

**A.** 일반적으로 전자 소프트웨어 클레임 인증서는 즉시 받습니다. 그러나 Cisco Commerce Workspace에서 기능 라이선스를 구매하는 것과 PAK를 등록하고 라이선스 등록 포털에서 라이선스 텍스트를 생성할 수 없는 사이에 최대 24시간이 지연될 수 있습니다.

**Q.** 한 management center에서 라이선스를 삭제한 다음 다른 management center에서 재사용할 수 있습니까?

**A.** 직접적으로는 안됩니다. 생성된 라이선스는 각 management center에만 적용됩니다. 하지만 시스코 제품 라이선스 등록 포털에서 PAK를 재사용하여 다른 management center의 고유 ID를 사용하는 새 라이선스를 생성할 수 있습니다.

**Q.** 디바이스의 클래식 라이선스를 구매했지만 Cisco LRP(License Registration Portal)에서 등록하거나 디바이스에 할당하지 않았습니다. 이 라이선스를 다른 디바이스에 재사용할 수 있습니까?

**A.** 원래 디바이스와 새 디바이스가 동일한 모델인 경우에만 미사용 라이선스를 재사용할 수 있습니다. 예를 들어, ASA 5508-X에서 ASA FirePOWER 모듈에 대한 보호 라이선스를 구매하는 경우, 모든 ASA 5508-X에 할당할 수 있지만 ASA 5516-X에는 할당할 수 없습니다.

원래 라이선스와 동시에 구매한 서비스 구독은 재사용할 수 없습니다. 해당 구독의 타이머는 디바이스에 할당하지 않은 경우에도 발행된 날에 시작됩니다. 영업팀에 문의하여 서비스 구독의 나머지 부분에 사용할 수 있는 크레딧에 대해 문의하십시오.

# 고가용성 구성에 대한 라이선싱

- Management Center (하드웨어) 고가용성
- Management Center (가상) 고가용성
- Threat Defense 고가용성
- Firepower 7000 및 8000 Series 디바이스 고가용성

### **Management Center** (하드웨어) 고가용성

**Q.** 두 하드웨어 management center 어플라이언스를 고가용성 쌍으로 구성하려면 특별한 라이선싱이 필요합니까?

**A.** 하드웨어 management center는 독립형이든 고가용성 쌍의 일부이든 상관없이 특별한 라이선싱이 필요하지 않습니다.

**Q.** 하드웨어 Secure Firewall Management Center 고가용성 쌍으로 관리되는 디바이스에 대해 라이선스 기능을 활성화하려는 경우 라이선스를 몇 개나 구매해야 합니까?

**A.** 고가용성 구성의 management center 인스턴스로 관리되는 디바이스에는 동일한 수의 기능 라이선스 및 단일 management center로 관리되는 디바이스처럼 관련 구독이 필요합니다.

시스템은 모든 매니지드 디바이스의 기능 라이선스를 활성에서 대기 management center로 자동 복제하여 페일오버시 매니지드 디바이스에서 라이선스를 사용할 수 있습니다.

### **Management Center** (가상) 고가용성

**Q.** 고가용성 쌍의 management center virtual에 대한 라이선스 요구 사항은 무엇입니까?

**A.**

- 릴리스 **6.7**부터**:**

  10개, 25개 또는 300개의 매니지드 디바이스에 대한 자격이 있는 VMWare에서 실행되는 Management Center Virtual을 고가용성 쌍으로 구성할 수 있습니다.

  management center virtual-HA 쌍을 구성하려면 라이선스가 동일한 2개의 management center virtual이 필요합니다.

  고가용성 구성의 하드웨어 management center에 대해 위에서 설명한 것과 같이 모든 매니지드 디바이스(threat defense 및 클래식)에도 자체 라이선스가 필요합니다.

  예를 들어, management center virtual 고가용성 쌍으로 threat defense 디바이스 10개와 NGIPS 디바이스 3개를 관리하려면 FMCv25 권한 2개, threat defense 자격 10개, 클래식 자격 3개가 필요합니다.

  자세한 내용은 사용 중인 버전에 대한 Cisco Secure Firewall Management Center 관리 가이드의 "Management Center 고가용성" 장에서 라이선싱 요구 사항 항목을 참조하십시오.

- **Management Center Virtual 6.7** 이전 릴리스**:**

Secure Firewall Management Center Virtual 어플라이언스는 고가용성 쌍의 멤버가 될 수 없습니다.

### **Threat Defense** 고가용성

**Q.** 고가용성 구성에서 threat defense 디바이스에 대한 라이선스 요구 사항은 어떻게 됩니까?

**A.** 고가용성 쌍에서 threat defense 디바이스를 구성하는 데 필요한 라이선스는 없습니다. 그러나 각 디바이스에는 구축에서 사용할 각 기능에 대한 라이선스가 있어야 합니다.

**Q.** management center virtual 어플라이언스가 고가용성 쌍으로 구성된 threat defense 디바이스를 관리하는 경우 각 디바이스에 대해 하나의 자격이 필요합니까, 아니면 각 쌍에 대해 하나의 자격이 필요합니까?

**A.** 각 디바이스에 대해 하나의 자격이 필요합니다.

**Q.** 고가용성 구성에서 threat defense 디바이스에 대한 라이선스 기능을 활성화하려는 경우 라이선스를 몇 개나 구매해야 합니까?

**A.** 각 디바이스는 고가용성 쌍의 멤버인지 여부에 상관없이 사용할 모든 기능에 대해 라이선스가 부여되어야 합니다.

따라서 각 기능에 대해 해당 기능에 대한 2개의 스마트 라이선스 자격, 즉 고가용성 쌍의 각 디바이스에 대한 자격을 구매해야 합니다. 이 설정에 사용되는 라이선스의 할인 가능성에 대해 논의하려면 영업팀에 문의하십시오.

고가용성 쌍에서 threat defense 디바이스를 구성하면 management center가 Cisco Smart Software Manager와 통신하고 어카운트에서 필요한 라이선스를 가져오므로 대기 디바이스가 활성 디바이스와 동일한 기능 라이선스를 가질 수 있습니다. 스마트 라이선스에 포함되어 있는 구매한 자격이 충분하지 않으면 정확한 수의 라이선스를 구매할 때까지 어카운트는 OOC(out of compliance,

컴플라이언스 위반) 상태가 됩니다. 활성 디바이스에는 없었던 대기 디바이스 기능의 라이선스는 사용 가능한 라이선스 풀로 다시 릴리스됩니다.

**Q.** 고가용성 구성에서 threat defense 디바이스의 라이선스 변경 시 제한 사항이 있습니까?

**A.** 디바이스를 management center에 페어링한 후 쌍으로 연결된 개별 디바이스의 라이선스 옵션을 변경할 수 없지만 전체 고가용성 페어의 라이선스는 변경할 수 있습니다.

**Q.** 멀티 인스턴스 구축에서 고가용성 쌍에 몇 개의 라이선스가 필요합니까?

**A.** 고가용성 쌍은 서로 다른 두 섀시의 인스턴스 간에 형성되므로 기능 라이선스 2개를 사용합니다.

### **Firepower 7000** 및 **8000 Series** 디바이스 고가용성

**Q.** 고가용성 설정에서 Firepower 7000 및 8000 Series 디바이스에 대한 라이선스 기능을 활성화하려는 경우, 라이선스를 몇 개나 구매해야 합니까?

**A.** 해당 기능을 사용하려면 고가용성 쌍의 디바이스당 라이선스 2개를 구매해야 합니다. 이 설정에 사용되는 라이선스의 할인 가능성에 대해 논의하려면 영업팀에 문의하십시오.

**Q.** 고가용성 구성에서 Firepower 7000 및 8000 Series 디바이스에 대한 라이선스 요구 사항은 어떻게 됩니까?

**A.** 고가용성 쌍에서 7000 및 8000 Series 디바이스를 구성하는 데 필요한 추가 라이선스는 없습니다. 그러나 고가용성 쌍에서 7000 및 8000 Series 디바이스를 구성하기 전에 management center의 두 디바이스에 동일한 기능 라이선스를 할당해야 합니다.

**Q.** 고가용성 구성에서 Firepower 7000 및 8000 Series 디바이스의 라이선스 변경 시 제한 사항이 있습니까?

**A.** 디바이스를 management center에 페어링한 후 쌍으로 연결된 개별 디바이스의 라이선스 옵션을 변경할 수 없지만 전체 고가용성 페어의 라이선스는 변경할 수 있습니다.

# **Threat Defense** 디바이스 클러스터에 대한 라이선싱


- 섀시 내 클러스터링
- 섀시 간 클러스터링


## 섀시 내 클러스터링

참고 섀시 내 클러스터링은 Firepower 9300 디바이스의 threat defense 모듈에 대해서만 지원됩니다.

**Q.** 섀시 내 클러스터에서 threat defense 모듈에 대한 라이선스 기능을 활성화하려면, 라이선스를 몇 개나 구매해야 합니까?

**A.** 클러스터의 각 모듈의 해당 기능을 사용하려면 스마트 라이선스를 구매해야 합니다. 예를 들어, 클러스터에 URL 필터링을 사용하는 모듈 3개가 포함되도록 하려면 URL 필터링 라이선스 3개 및 관련 구독을 구매해야 합니다.

**Q.** threat defense 모듈의 섀시 내 클러스터링에 대한 라이선스 요구 사항은 어떻게 됩니까?

**A.** 클래식 라이선스를 사용하면 FXOS 섀시 내에서 보안 모듈을 클러스터링할 수 있습니다. 추가 라이선싱이 필요하지 않습니다. 그러나 클러스터에서 라이선스 기반 기능(예: URL 필터링)을 사용하려는 경우에는 모든 threat defense 모듈을 클러스터로 구성하기 전에 해당 모듈에 동일한 라이선스를 할당해야 합니다.

**Q.** 섀시 내 클러스터에 구성된 threat defense 모듈에 대한 라이선스 변경 시 제한 사항이 있습니까?

**A.** 디바이스를 클러스터링한 후에는 클러스터의 개별 모듈에 대한 라이선스 옵션을 변경할 수 없지만 전체 클러스터에 대한 라이선스 옵션은 변경할 수 있습니다.

### 섀시 간 클러스터링

참고 섀시 간 클러스터링은 Firepower 9300 및 Firepower 4100 Series 디바이스의 threat defense에 대해서만 지원됩니다.

**Q.** 섀시 간 클러스터의 threat defense 디바이스에 대한 라이선스 기능을 활성화하려면 라이선스를 몇 개나 구매해야 합니까?

**A.** 클러스터의 각 디바이스에 대해 해당 기능을 사용하는 스마트 라이선스를 구매해야 합니다. 예를 들어, URL 필터링을 사용하는 디바이스 4개를 클러스터에 포함하려면 URL 필터링 라이선스 4개 및 관련 구독을 구매해야 합니다.

**Q.** threat defense 디바이스의 섀시 간 클러스터링에 대한 라이선스 요구 사항은 어떻게 됩니까?

**A.** 클래식 라이선스를 사용하면 FXOS 섀시에서 실행 중인 threat defense 디바이스를 클러스터링할 수 있습니다. 추가 라이선싱이 필요하지 않습니다. 그러나 클러스터에서 라이선스 기반 기능(예:

URL 필터링)을 사용하려는 경우에는 디바이스를 클러스터로 구성하기 전에 모든 threat defense 디바이스에 동일한 라이선스를 할당해야 합니다.

**Q.** 섀시 간 클러스터에서 threat defense 디바이스에 대한 라이선스 변경 시 제한 사항이 있습니까?

**A.** 디바이스를 클러스터링한 후에는 클러스터의 개별 장치에 대한 라이선스 옵션을 변경할 수 없지만 전체 클러스터에 대한 라이선스 옵션은 변경할 수 있습니다.

# 8000 Series 디바이스 스택의 라이선싱

**Q.** 8000 Series 디바이스 스택에 대해 라이선스 기능을 활성화하려는 경우 라이선스를 몇 개 구매해야 합니까?

**A.** 스택의 각 디바이스에 대해 해당 기능을 사용하려면 클래식 라이선스를 구매해야 합니다. 예를 들어, URL 필터링을 사용하는 4개의 디바이스를 스택에 포함하려면 4개의 URL 필터링 라이선스 및 관련 구독을 구매해야 합니다.

**Q.** 8000 Series 디바이스 스택의 라이선스 요구 사항은 어떻게 됩니까?

**A.** 8000 Series 디바이스 스택을 구성하는 데 필요한 추가 라이선스는 없습니다. 그러나 스택에서 8000 Series 디바이스를 구성하려면 해당 디바이스를 스택에 포함하기 전에 모든 디바이스에 동일한 기능 라이선스를 할당해야 합니다.

**Q.** 8000 Series 스택에 구성된 디바이스에 대한 라이선스 변경에 제한이 있습니까?

**A.** 디바이스를 스택한 후에는 스택의 개별 디바이스에 대한 라이선스 옵션을 변경할 수 없지만 전체 스택에 대한 라이선스 옵션은 변경할 수 있습니다.

# 라이선스 만료


- 라이선스 만료 vs. 서비스 서브스크립션 만료
- 스마트 라이선싱
- 특정 라이선스 예약
- 클래식 라이선싱
- 서브스크립션 갱신

### 라이선스 만료 **vs.** 서비스 서브스크립션 만료

**Q.** 기능 라이선스가 만료되나요?

**A.** 엄밀히 말해 기능 라이선스는 만료되지 않습니다. 대신 그러한 라이선스를 지원하는 서비스 서브스크립션이 만료됩니다.

### 스마트 라이선싱

**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 management center을 등록하기 전에 토근이 만료되는 경우, 새 토큰을 생성해야 합니다.

토큰을 사용하여 management center을 등록한 경우, 토큰 만료일은 더 이상 의미가 없습니다. 토큰 만료일이 경과하는 경우, 해당 토큰을 사용하여 등록한 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.

management center에서 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 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.

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, 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

클래식 라이선싱

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

**A.** management center에서 시스템 ( ⚙ ) > **Licenses(**라이선스**)** > **Classic Licenses(**클래식 라이선스**)**를 선택합니다.

이 페이지에서 테이블에는 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 *1:* 기본 라이선스/서브스크립션 만료의 영향

| 기본 라이선스 | 가능한 지원 서브스크립션 | 만료 영향 |
|---|---|---|
| 제어 | TA, TAC, TAM, TAMC | 기존 기능을 계속 사용할 수 있지만, 애플리케이션 서명 업데이트를 포함하여 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>• management center는 더 이상 URL 데이터에 대한 업데이트를 다운로드할 수 없습니다.<br>• URL 카테고리 및 평판 필터링을 수행하는 기존 정책을 다시 구축할 수 없습니다. |
| 악성코드 | Secure Endpoint , 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 Secure Malware Analytics Cloud 쿼리를 중지하며 Secure Malware Analytics Cloud에서 전송하는 회귀적 이벤트 확인을 중지합니다.<br>• threat defense 구성에 대해 Secure Endpoint 가 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.** management center에서 서비스 구독을 갱신할 수 있나요?

**A.** 아니요. 서비스 구독(클래식 또는 스마트)을 갱신하려면 Cisco Commerce Workspace 또는 Cisco Service Contract Center 중 하나를 통해 새 구독을 구매해야 합니다.

# 추가 정보

자세한 내용은 다음 문서를 참조하십시오.

- 다음에서 Cisco Secure Firewall Management Center 기능 라이선스 문서:

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

- 구축에 management center이 포함된 경우, Cisco Secure Firewall Management Center 관리 가이드의 라이선스 장을 참조하십시오.

  Threat Intelligence Director 등의 일부 기능의 추가 세부정보는 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 해당 기능에 대한 장에 나와 있습니다. 제품 버전에 맞는 가이드를 사용하십시오.

- 구축이 독립형 threat defense 디바이스인 경우 Cisco Secure Firewall Management Center 관리 가이드의 라이선스 장을 참조하십시오.

- 구축이 독립 실행형 ASA with FirePOWER Services 디바이스인 경우 해당 버전에 대한 *Cisco ASA with FirePOWER Services* 로컬 관리 구성 가이드의 *"ASA FirePOWER* 모듈 라이선싱*"* 장을 참조하십시오(https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html에서 이용 가능).