라이선스

이 장에서는 다양한 라이선스 유형, 서비스 구독, 라이선스 요구 사항 등에 대한 자세한 정보를 제공합니다.

참고 Management Center는 플랫폼 라이선스에 대해 스마트 라이선스 또는 레거시 PAK(제품 활성화 키) 라이선스를 지원합니다. PAK 라이센싱에 대한 자세한 내용은 레거시 Management Center PAK 기반 라이선스 구성, 48 페이지의 내용을 참조하십시오.

라이선스 정보

시스코 스마트 라이선싱은 시스코 포트폴리오 및 조직 전체에서 소프트웨어를 보다 쉽고 빠르고 일관적인 방식으로 구매하고 관리할 수 있는 유연한 라이선싱 모델입니다. 또한 사용자가 액세스할 수 있는 항목을 제어할 수 있어 안전합니다. 스마트 라이선싱을 사용하면 다음과 같은 이점을 누릴 수 있습니다.

- 손쉬운 활성화: 스마트 라이선싱은 전체 조직에서 사용할 수 있는 소프트웨어 라이선스 풀을 설정하므로 더 이상 PAK(제품 활성화 키)가 필요하지 않습니다.
- 통합 관리: MCE(My Cisco Entitlements)는 사용하기 쉬운 포털에서 모든 시스코 제품 및 서비스에 대한 완벽한 보기를 제공하므로 무엇을 보유하고 있으며 무엇을 사용 중인지 항상 파악할 수 있습니다.

- 라이선스 유연성: 소프트웨어가 하드웨어에 노드로 고정되어 있지 않으므로 필요에 따라 라이선스를 쉽게 사용하고 전송할 수 있습니다.

스마트 라이선싱을 사용하려면 먼저 Cisco Software Central(software.cisco.com)에서 스마트 어카운트를 설정해야 합니다.

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

Smart Software Manager 및 어카운트

라이선스를 1개 이상 구매한 경우, Smart Software Manager에서 라이선스를 관리할 수 있습니다.https://software.cisco.com/#module/SmartLicensing Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다. 아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

기본적으로는 마스터 어카운트의 기본 가상 어카운트에 라이선스가 할당됩니다. 어카운트 관리자는 지역, 부서, 자회사 등에 대해 가상 어카운트를 추가로 생성할 수 있습니다. 여러 가상 어카운트가 있으면 수많은 라이선스 및 디바이스를 관리할 수 있습니다.

가상 어카운트에서 라이선스를 관리합니다. 해당 가상 어카운트의 디바이스만 어카운트에 할당된 라이선스를 사용할 수 있습니다. 추가 라이선스가 필요할 경우 다른 가상 계정의 미사용 라이선스를 이전할 수 있습니다. 또한 가상 어카운트 간에 디바이스를 이전할 수도 있습니다.

에어 갭(Air-Gapped) 구축 라이선싱 옵션

다음 표에서는 인터넷 액세스가 없는 환경에서 사용 가능한 라이선싱 옵션을 비교합니다. 영업 담당자가 특정 상황에 대한 추가적인 조언을 할 수 있습니다.

표 *1:* 에어 갭*(Air-Gapped)* 네트워크에 대한 라이선싱 옵션 비교

Smart Software Manager 온프레미스	특정 라이선스 예약
다수의 제품에 대한 확장 가능성	소수의 디바이스에 대한 최적성
자동화된 라이선싱 관리, 사용 및 자산 관리 가시성	제한된 사용 및 자산 관리 가시성
디바이스 추가 시 운영비 증가 없음	디바이스 추가 시 시간 경과에 따라 선형 운영비
유연성, 사용 용이성, 오버헤드 감소	이동, 추가 및 변경에 대한 중요한 관리 및 수동 오버헤드
규정 위반(out-of-compliance) 상태는 초기 및 여러 만료 상태로 허용됩니다.	규정 위반 상태는 시스템 기능에 영향을 줍니다.
자세한 내용은 Management Center를 Smart Software Manager 온프레미스로 등록, 27 페이지을 참조해 주십시오.	자세한 내용은 SLR(Specific License Reservation) 구성, 37 페이지을 참조해 주십시오.

Management Center 및 디바이스에 대한 라이선싱 작동 방식

management center는 Smart Software Manager에 등록한 다음 각 매니지드 디바이스에 대해 라이선스를 할당합니다. 디바이스는 Smart Software Manager에 직접 등록되지 않습니다.

물리적 management center은 자체 사용을 위한 라이선스가 필요하지 않습니다. management center virtual에는 플랫폼 라이선스가 필요합니다.

Smart Software Manager와의 정기적인 통신

제품 라이선스 엔타이틀먼트를 유지하기 위해 제품은 Smart Software Manager와 주기적으로 통신해야 합니다.

제품 인스턴스 등록 토큰을 사용하여 management center을 Smart Software Manager에 등록합니다. Smart Software Manager는 management center와 Smart Software Manager 간의 통신을 위해 ID 인증서를 발급합니다. 이 인증서는 6개월마다 갱신되지만 1년간 유효합니다. ID 인증서가 만료되면(1년 후) management center은 계정에서 제거될 수 있습니다.

management center는 주기적으로 Smart Software Manager와 통신합니다. Cisco Smart Software Manager에 변경이 있는 경우, management center에서 권한을 새로 고침하고 변경 사항을 즉시 적용할 수 있습니다. 또는 management center에서 예정대로 통신할 때까지 기다릴 수 있습니다.

management center은 Smart Software Manager에 대한 직접 인터넷 액세스 권한이 있거나 에어 갭(Air-Gapped) 구축 라이선싱 옵션, 2 페이지에 설명된 옵션 중 하나를 사용해야 합니다. 비 에어 갭(Air-Gapped) 구축에서 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 management center는 최대 90일간 Smart Software Manager에 접촉하지 않고 작동할 수 있습니다. 90일이 지나기 전에 management center가 Smart Software Manager에 접촉하는지 확인합니다. 그렇지 않으면 management center가 등록되지 않은 상태로 되돌아갑니다.

평가 모드

management center는 Smart Software Manager에 등록하기 전에 평가 모드에서 90일 동안 작동합니다. 매니지드 디바이스에 기능 라이선스를 할당할 수 있으며, 평가 모드 기간 동안 규정을 준수합니다. 이 기간이 끝나면 management center의 등록이 취소됩니다.

management center를 Smart Software Manager에 등록하면 평가 모드가 종료됩니다. 나중에 management center의 등록을 취소하면 처음에 90일을 모두 사용하지 않았더라도 평가 모드를 다시 시작할 수 없습니다.

등록되지 않은 상태에 대한 자세한 내용은 등록 취소 상태, 4 페이지의 내용을 참조하십시오.

참고 강력한 암호화(3DES/AES)를 위한 평가 라이선스를 받을 수 없습니다. 강력한 암호화(3DES/AES) 라이선스를 활성화하는 내보내기-컴플라이언스 토큰을 받으려면 Smart Software Manager에 등록해야 합니다.

규정 위반 상태

다음과 같은 상황에서 management center가 규정 위반이 될 수 있습니다.

- 과다 사용 — 매니지드 디바이스 또는 management center virtual에서 사용 불가한 라이선스를 사용할 경우.
- 라이선스 만료—매니지드 디바이스 기반 라이선스가 만료된 경우.

컴플라이언스 미준수 상태에서는 다음 효과를 확인할 수 있습니다.

- Management Center Virtual 플랫폼 라이선스 - 작업이 영향을 받지 않습니다.
- 모든 매니지드 디바이스 라이선스 - 작업은 영향을 받지 않습니다.

라이선싱 문제를 해결하면 management center에 Smart Software Manager를 통해 정기적으로 예약된 권한 부여 후 현재 컴플라이언스 상태임을 표시합니다. 권한 부여를 강제로 수행하려면 시스템 (⚙) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 페이지에서 **Re-Authorize(**재권한 부여**)**를 클릭합니다.

등록 취소 상태

다음과 같은 경우 management center가 등록 취소될 수 있습니다.

- 평가 모드 만료 - 평가 모드는 90일 후에 만료됩니다.
- management center의 수동 등록 해제
- Smart Software Manager와의 통신 부족 - management center는 1년 동안 Smart Software Manager와 통신하지 않습니다. 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.

등록되지 않은 상태에서 management center는 라이선스가 필요한 기능에 대한 구성 변경 사항을 디바이스에 구축할 수 없습니다.

최종 사용자 라이선스 계약

이 제품의 사용에 대한 Cisco EULA(최종 사용자 라이선스 계약) 및 SEULA(적용 가능한 보완 계약은 http://www.cisco.com/go/softwareterms에서 제공됩니다.

라이선스 유형 및 제한 사항

이 섹션에서는 사용할 수 있는 라이선스 유형에 대해 설명합니다.

표 2: 스마트 라이선스

사용자가 할당한 라이선스	기간	부여된 기능
Essentials	영구 또는 구독 참고 Essentials 구독 라이선스는 Threat Defense Virtual에서만 지원됩니다.	특정 라이선스 예약과 Secure Firewall 3100을 제외하고 Essentials 영구 라이선스가 모든 threat defense에 자동으로 할당됩니다. 사용자 및 애플리케이션 제어 스위칭 및 라우팅 NAT 자세한 내용은 Essentials 라이선스, 7 페이지 섹션을 참조해 주십시오.
IPS	구독	침입 탐지 및 방지 파일 제어 보안 인텔리전스 필터링 자세한 내용은 다음을 참조하십시오. IPS 라이선스, 8 페이지
악성코드 방어	구독	악성코드 방어 Secure Malware Analytics 파일 스토리지 (IPS 라이선스는 악성코드 방어 라이선스의 사전 요건입니다.) 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 악성코드 방어 라이선스, 7 페이지 및 파일 및 악성코드 정책을 위한 라이선스 요구 사항을 참조하십시오.
캐리어	Firepower 4100/9300, Secure Firewall 3100 및 Threat Defense Virtual 구독	Diameter, GTP/GPRS, M3UA 및 SCTP 검사 자세한 내용은 통신 사업자 라이선스, 9 페이지 섹션을 참조해 주십시오.
URL	구독	카테고리 및 평판 기반 URL 필터링 자세한 내용은 URL 라이선스, 10 페이지 섹션을 참조해 주십시오. (IPS 라이선스는 URL 라이선스의 사전 요건입니다.)

사용자가 할당한 라이선스	기간	부여된 기능
Management Center Virtual	• 일반 Smart Licensing - 영구 • 특정 라이선스 예약—구독	플랫폼 라이선스는 management center virtual가 관리할 수 디바이스 수를 결정합니다. 자세한 내용은 Management Center Virtual 라이선스, 6 페이지 섹션을 참조해 주십시오.
내보내기 제어 기능	영구	국가 보안, 외교 정책, 테러 방지법 및 규제의 적용을 받는 기능. 내보내기 제어 기능 라이선싱, 11 페이지를 참조하십시오.
원격 액세스 VPN: • Secure Client Premier • Secure Client Advantage • Secure Client VPN Only	구독 또는 영구	원격 액세스 VPN 컨피그레이션 계정은 원격 액세스 VPN을 구성하기 위해 내보내기 제어 기능을 허용해야 합니다. 디바이스를 등록할 때 내보내기 요구사항을 충족하는지를 선택합니다. threat defense는 유효한 Secure Client 라이선스를 사용할 수 있습니다. 제공되는 기능은 라이선스 유형에 따라 달라지지 않습니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 Secure Client 라이선스, 10 페이지 및 *VPN* 라이선싱을 참조하십시오.

참고 구독 라이선스는 조건 기반 라이선스입니다.

Management Center Virtual 라이선스

management center virtual에는 관리할 수 있는 디바이스의 수와 상관관계가 있는 플랫폼 라이선스가 필요합니다.

management center virtual는 스마트 라이선싱을 지원합니다.

일반 스마트 라이선싱에서 이러한 라이선스는 영구적입니다.

SLR(특정 라이선스 예약)에서는 이러한 라이선스가 구독 기반입니다.

참고 FMCv에 있는 새 디바이스의 애드온 라이선스 요구 사항은 추가 디바이스를 지원하는 상위 management center virtual 모델로 마이그레이션하는 것이 좋습니다.

Essentials 라이선스

Essentials 라이선스를 통해 다음을 수행할 수 있습니다.

- 디바이스를 구성하고 스위칭 및 라우팅(DHCP 릴레이 및 NAT 포함)을 수행합니다.
- 디바이스를 고가용성 쌍으로 구성합니다.
- 클러스터링 구성
- 액세스 제어 규칙에 사용자 및 애플리케이션 상태를 추가하여 사용자 및 애플리케이션 제어를 수행할 수 있습니다.
- VDB(취약점 데이터베이스) 및 GeoDB(지리적 데이터베이스)를 업데이트합니다.
- SRU/LSP와 같은 침입 규칙을 다운로드합니다. 그러나 IPS 라이선스가 활성화되어 있지 않으면 액세스 제어 정책 또는 침입 정책이 있는 규칙을 디바이스에 구축할 수 없습니다.

Secure Firewall 3100

Secure Firewall 3100을 구매하면 Essentials 라이선스를 받게 됩니다.

다른 모든 모델

Specific License Reservation(특정 라이선스 예약)을 사용하는 구축을 제외하고 Essentials 라이선스는 디바이스를 management center에 등록하면 자동으로 사용자 어카운트에 추가됩니다. 특정 라이선스 예약의 경우 Essentials 라이선스를 어카운트에 추가해야 합니다.

악성코드 방어 라이선스

악성코드 방어 라이선스를 사용하면 악성코드 대응 및 Secure Malware Analytics을 수행할 수 있습니다. 이러한 기능으로 디바이스를 사용하여 네트워크를 통해 전송된 파일에서 악성코드를 탐지 및 차단할 수 있습니다. 이러한 기능 라이선스를 지원하려면 악성코드 방어(AMP) 서비스 구독을 독립 실행형 구독으로 구매하거나 IPS(TM) 또는 IPS 및 URL(TMC) 구독과 함께 구매할 수 있습니다. IPS 라이선스는 악성코드 방어 라이선스의 사전 요건입니다.

참고 악성코드 방어 라이선스가 정기적으로 활성화되는 매니지드 디바이스는 사용자가 동적 분석을 구성하지 않은 경우에도 Secure Malware Analytics 클라우드 연결을 시도합니다. 따라서, 디바이스의 Interface Traffic(인터페이스 트래픽) 대시보드 위젯은 전송된 트래픽을 보여주며, 이는 예상된 작업입니다.

사용자는 파일 정책의 일부로서 악성코드 대응 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. 악성코드 대응 을 통해 로컬 악성 코드 분석 및 파일 사전 분류를 사용하여 그러한 제한된 파일 유형의 집합에 악성코드가 있는지 검사할 수 있습니다. 또한 Secure Malware Analytics 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 방어 라이선스는 또한 특정 파일을 파일 목록에 추가하고 파일

정책 내에서 파일 목록을 활성화하며, 해당 파일이 탐지되면 자동으로 허용하거나 차단하도록 허용합니다.

참고로 악성코드 대응 및 Secure Malware Analytics를 구축하는 경우에만 악성코드 방어 라이선스가 필요합니다. 악성코드방어라이선스가 없는 경우, management center은 엔드포인트 Secure Endpoint 악성코드 이벤트 및 보안 침해 지표(IOC)를 Secure Malware Analytics 클라우드에서 받을 수 있습니다.

Cisco Secure Firewall Management Center 디바이스 구성 가이드의 파일 및 악성코드 정책에 대한 라이선스 요구 사항의 중요 정보도 참조하십시오.

이 라이선스를 비활성화하는 경우:

- 시스템에서 Secure Malware Analytics 클라우드에 대한 쿼리를 중단하며 Secure Malware Analytics 클라우드에서 전송한 회귀적 이벤트 확인도 중지합니다.
- 악성코드 대응 구성이 포함된 경우, 기존 액세스 제어 정책은 재적용할 수 없습니다.
- 악성코드 방어 라이선스가 비활성화된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 시간대가 만료된 후 시스템은 해당 파일에 `Unavailable(사용 불가)` 속성을 할당합니다.

라이선스가 만료되면 위 기능에 대한 엔타이틀먼트가 중지되고 management center가 규정을 준수하지 않는 상태로 전환됩니다.

IPS 라이선스

IPS 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 차단 라이선스가 필요한 악성코드 대응 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.

IPS 라이선스를 독립형 서브스크립션(T) 또는 URL (TC), 악성코드 차단(TM)과 각각 결합하거나 동시에 결합(TMC)한 서브스크립션으로 구입할 수 있습니다.

이 라이선스를 비활성화하는 경우:

- management center이 영향을 받는 디바이스에서 침입 및 파일 이벤트 인지를 중단합니다. 결과적으로, 해당 이벤트를 트리거 기준으로 사용하는 상관성 규칙이 실행을 중지합니다.
- management center은 Cisco 제공 정보나 서드파티 Security Intelligence 정보를 검색하기 위해 인터넷에 접속하지 않습니다.

- IPS 라이선스를 다시 활성화할 때까지 현재 침입 정책을 다시 배포할 수 없습니다.

라이선스가 만료되면 위 기능에 대한 엔타이틀먼트가 중지되고 management center가 규정을 준수하지 않는 상태로 전환됩니다.

통신 사업자 라이선스

통신 사업자 라이선스를 사용하면 다음 프로토콜을 검사할 수 있습니다:

- Diameter - Diameter는 LTE(Long Term Evolution) 및 IMS(IP Multimedia Subsystem)용 EPS(Evolved Packet System)와 같은 차세대 모바일 및 고정 통신 네트워크에서 사용되는 AAA(Authentication, Authorization, and Accounting) 프로토콜입니다. 이는 이러한 네트워크에서 RADIUS 및 TACACS를 대체합니다.
- GTP/GPRS - GTP(GPRS Tunneling Protocol)는 GSM, UMTS 및 LTE 네트워크에서 GPRS(General Packet Radio Service) 트래픽에 사용됩니다. GTP는 SGSN에서 터널을 생성, 수정 및 삭제하여 이동 통신국용 GPRS 네트워크 액세스를 제공하는 터널 제어 및 관리 프로토콜을 제공합니다. GTP는 또한 사용자 데이터 패킷을 전송하기 위해 터널링 메커니즘을 사용합니다.
- M3UA - M3UA(MTP3 User Adaptation)는 SS7 MTP3(Message Transfer Part 3) 레이어와 인터페이스하는 IP 기반 애플리케이션에 대해 SS7(Signaling System 7) 네트워크에 대한 게이트웨이를 제공하는 클라이언트/서버 프로토콜입니다. M3UA를 사용하면 IP 네트워크를 통해 SS7 사용자 부분(예: ISUP)을 실행할 수 있습니다.
- SCTP - SCTP(Stream Control Transmission Protocol)는 IP 네트워크를 통해 SS7 프로토콜을 지원하는 전송 계층 프로토콜입니다. 4G LTE 모바일 네트워크 아키텍처를 지원합니다. SCTP는 여러 동시 스트림, 다중 스트림을 처리할 수 있으며 더 많은 보안 기능을 제공합니다.

참고 디바이스에서 이 라이선스를 활성화한 후 FlexConfig 정책을 사용하여 프로토콜 검사를 활성화합니다.

통신 사업자 라이선스 PID는 디바이스 모델이 아닌 제품군별로 사용할 수 있습니다. 평가 모드에서 또는 스마트 라이선스를 사용하여 각 디바이스에 대해 이 라이선스를 활성화할 수 있습니다.

Firepower4100/9300, Secure Firewall 3100 및 Threat Defense Virtual에 대한 통신 사업자 라이선스는 기간별입니다. 이 라이선스는 특정 라이선스 예약도 지원합니다.

지원되는 장치

통신 사업자 라이선스를 지원하는 디바이스는 다음과 같습니다.

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140

- Firepower 4112
- Firepower 4115
- Firepower 4125
- Firepower 4145
- Firepower 9300
- Threat Defense Virtual

URL 라이선스

URL 라이선스를 사용하면 액세스 제어 규칙을 작성할 수 있습니다. 이 규칙은 모니터링된 호스트에서 요청하고 URL 정보와 상호 연결된 해당 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정합니다. 이러한 기능 라이선스를 지원하려면 URL 서비스 구독을 독립 실행형 구독으로 구매하거나 IPS(TC) 또는 위협 및 악성코드 방어(TMC) 구독과 함께 구매할 수 있습니다. IPS 라이선스는 이 라이선스의 사전 요건입니다.

팁 URL 라이선스 없이, 허용하거나 차단할 개별 URL 또는 URL 그룹을 지정할 수 있습니다. 이 옵션을 통해 웹 트래픽에 대한 세분화된 사용자 지정 제어를 가질 수 있지만 URL 카테고리와 평판 데이터를 사용하여 네트워크 트래픽을 필터링할 수는 없습니다.

URL 라이선스 없이도 액세스 제어 규칙에 카테고리 및 평판 기반 URL 조건을 추가할 수 있지만, management center은 URL 정보를 다운로드하지 않습니다. 먼저 URL 라이센스를 management center에 추가한 후 정책의 대상이 되는 디바이스에서 활성화에 추가할 때까지 액세스 제어 정책을 구축할 수 없습니다.

이 라이선스를 비활성화하는 경우:

- URL 필터링에 액세스하지 못할 수 있습니다.
- URL 조건이 포함된 액세스 제어 규칙은 즉시 URL 필터링을 중지합니다.
- management center는 더 이상 URL 데이터에 대한 업데이트를 다운로드할 수 없습니다.
- 카테고리 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.

라이선스가 만료되면 위 기능에 대한 엔타이틀먼트가 중지되고 management center가 규정을 준수하지 않는 상태로 전환됩니다.

Secure Client 라이선스

Secure Client 및 표준 기반 IPSec/IKEv2를 사용하여 원격 액세스 VPN을 구성할 수 있습니다.

원격 액세스 VPN을 사용하려면 Secure Client Advantage, Secure Client Premier 또는 Secure Client VPN Only 라이선스 중 하나를 구입하여 활성화해야 합니다. 두 라이선스가 둘 다 있으며 모두 사용하려는 경우 Secure Client Advantage 및 Secure Client Premier를 선택할 수 있습니다. Secure Client VPN Only

라이선스는 **Apex** 또는 **Plus**와 사용할 수 없습니다. Secure Client 라이선스는 스마트 어카운트와 공유해야 합니다. 자세한 설명은 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf을 참조하십시오.

지정된 디바이스에 지정된 Secure Client 라이선스 유형 중 하나에 대한 최소한의 엔타이틀먼트가 없는 경우, 원격 액세스 VPN 구성을 디바이스에 배포할 수 없습니다. 등록된 라이선스를 준수하지 않거나 엔타이틀먼트가 만료된 경우, 시스템에 라이선스 경고 및 상태 이벤트가 나타납니다.

원격 액세스 VPN을 사용하는 동안 스마트 어카운트는 내보내기 제어 기능(강력한 암호화)가 활성화되어 있어야 합니다. threat defense는 원격 액세스 VPN과 Secure Client의 성공적인 연결을 위해 강력한 암호화(DES 보다 더 높은 수준)를 필요로 합니다.

다음의 경우에 원격 액세스 VPN을 구축할 수 없습니다.

- management center에서 스마트 라이선싱이 평가판 모드로 실행됩니다.
- 스마트 어카운트가 내보내기 제어 기능(강력한 암호화)를 사용하도록 구성되지 않습니다.

내보내기 제어 기능 라이선싱

내보내기 제어 기능이 필요한 기능

특정 소프트웨어 기능은 국가 보안, 외교 정책, 테러 방지법 및 규제의 적용을 받습니다. 이러한 내보내기 제어 기능은 다음을 포함합니다.

- 보안 인증서 컴플라이언스
- 원격 액세스 VPN
- 사이트 간 VPN 및 강력한 암호화
- SSH 플랫폼 정책 및 강력한 암호화
- SSL 정책 및 강력한 암호화
- SNMPv3 같은 기능 및 강력한 암호화

시스템에서 현재 내보내기 제어 기능이 활성화되어 있는지를 결정하는 방법

시스템에서 현재 내보내기 제어 기능이 활성화되어 있는지를 결정하는 방법: **System(**시스템**) > Licenses(**라이선스**) > Smart Licenses(**스마트 라이선스**)**로 이동하고 **Export-Controlled Features(**내보내기 제어 기능**)**에 **Enabled(**활성화 완료**)**로 나타나는지 확인합니다.

내보내기 제어 기능 활성화 정보

Export-Controlled Features(내보내기 제어 기능**)**이 **Disabled(**비활성화**)**로 표시되고 강력한 암호화를 필요로 하는 기능을 사용하려는 경우, 강력한 암호화 기능을 활성화하는 방법에는 두 가지가 있습니다. 해당 기관에서는 둘 중 하나를 사용할 수 있겠지만(또는 둘 다 아님) 둘 모두를 사용할 수는 없습니다.

- Smart Software Manager에서 새 Product Instance Registration(제품 인스턴스 등록)을 생성할 때 내보내기 제어 기능을 활성화하는 옵션이 없는 경우 계정 담당자에게 문의하십시오.

  Cisco에서 승인하면 내보내기 제어 기능을 사용할 수 있도록 강력한 암호화 라이선스를 계정에 수동으로 추가할 수 있습니다. 자세한 내용은 (전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화, 28 페이지을 참조해 주십시오.

- Smart Software Manager에서 새 제품 인스턴스 등록 토큰을 생성할 때 "Allow export-controlled features on the products registered with this token(이 토큰으로 등록된 제품에서 내보내기 제어 기능 허용)" 옵션이 표시되는 경우, 토큰을 생성하기 전에 해당 토큰을 선택해야 합니다.

  management center 등록에 사용한 제품 인스턴스 등록 토큰에 대해 내보내기 제어 기능을 활성화하지 않은 경우, 내보내기 제어 기능이 활성화된 상태에서 새 제품 인스턴스 등록 토큰을 사용하여 management center를 등록 취소한 다음 다시 등록해야 합니다.

평가 모드에서 또는 management center에서 강력한 암호화를 활성화하기 전에 management center에 디바이스를 등록한 경우, 각 매니지드 디바이스를 재부팅하여 강력한 암호화를 사용할 수 있게 합니다. 고가용성 구축에서, 액티브-액티브 상태를 방지하기 위해 액티브 디바이스 및 스탠바이 디바이스를 함께 재부팅해야 합니다.

엔타이틀먼트는 영구적이며 서브스크립션이 필요하지 않습니다.

추가 정보

내보내기 제어에 대한 일반 정보는 https://www.cisco.com/c/en/us/about/legal/global-export-trade.html를 참조하십시오.

Threat Defense Virtual 라이선스

이 섹션에서는 threat defense virtual에서 사용 가능한 성능 계층 라이선스 자격을 설명합니다.

모든 threat defense virtual 라이선스는 지원되는 threat defense virtual vCPU/메모리 설정에서 사용할 수 있습니다. 따라서 threat defense virtual 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다. 또한 지원되는 AWS 및 Azure 인스턴스 유형의 수가 증가합니다. threat defense virtual VM을 설정할 때 지원되는 최대 코어 수(vCPU)는 16개이고 지원되는 최대 메모리는 32GB RAM입니다.

Threat Defense Virtual 스마트 라이선싱의 성능 계층

RA VPN의 세션 제한은 설치된 threat defense virtual 플랫폼 엔타이틀먼트 계층에 따라 결정되고, 속도 제한기를 통해 적용됩니다. 다음 테이블에는 엔타이틀먼트 계층 및 속도 제한기에 따른 세션 제한이 요약되어 있습니다.

표 *3:* 자격 기준 ***Threat Defense Virtual*** 라이선스 기능 제한

성능 계층	디바이스 사양 **(Core/RAM)**	속도 제한	**RA VPN** 세션 제한
FTDv5, 100Mbps	4 코어/8GB	100Mbps	50
FTDv10, 1Gbps	4 코어/8GB	1Gbps	250

성능 계층	디바이스 사양 (Core/RAM)	속도 제한	RA VPN 세션 제한
FTDv20, 3Gbps	4 코어/8GB	3Gbps	250
FTDv30, 5Gbps	8 코어/16GB	5Gbps	250
FTDv50, 10Gbps	12 코어/24GB	10Gbps	750
FTDv100, 16Gbps	16 코어/32GB	16Gbps	10,000

FTDv 성능 계층 라이선싱 지침 및 제한

threat defense virtual 디바이스 라이선싱 시 다음 지침과 제한 사항에 유의하십시오.

- threat defense virtual에서는 구축 요건에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공하는 성능 계층 라이선싱을 지원합니다.
- 모든 threat defense virtual 라이선스는 지원되는 threat defense virtual 코어/메모리 설정에서 사용할 수 있습니다. 따라서 threat defense virtual 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다.
- 디바이스가 평가 모드인지 또는 이미 Cisco Smart Software Manager에 등록되어 있는지 여부와 무관하게 threat defense virtual 구축 시 성능 계층을 선택할 수 있습니다.

참고 Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다. 어카운트에 있는 라이선스와 일치하는 계층을 선택하는 것이 중요합니다. threat defense virtual를 버전 7.0으로 업그레이드하는 경우 **FTDv - Variable(FTDv - 변수)**를 선택하여 현재 라이선스 컴플라이언스를 유지할 수 있습니다. threat defense virtual는 디바이스 기능(코어/RAM 수)에 따라 계속 세션 제한을 수행합니다.

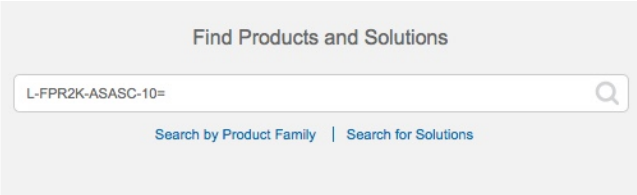
- 새 threat defense virtual 디바이스를 구축하거나 REST API를 사용한 threat defense virtual 프로비저닝 시 기본 성능 계층은 FTDv50입니다.
- Essentials 라이선스는 구독 기반이며 성능 계층에 매핑됩니다. 가상 어카운트에는 IPS, 악성코드 방어 및 URL 라이선스는 물론, threat defense virtual 디바이스에 대한 Essentials 라이센스 자격이 있어야 합니다.
- 각 HA 피어는 하나의 자격을 사용하고, Essentials 라이선스를 포함하여 각 HA 피어의 자격이 일치해야 합니다.
- HA 쌍의 성능 계층 변경 사항을 기본 피어에 적용해야 합니다.
- 개별 노드가 아니라 전체 피처 클러스터에 라이선스를 할당합니다. 그러나 클러스터의 각 노드는 각 기능에 대한 별도 라이선스를 사용합니다. 클러스터링 기능 자체에는 라이선스가 필요하지 않습니다.

- 범용 PLR 라이선싱은 HA 쌍의 각 디바이스에 개별적으로 적용됩니다. 보조 디바이스는 기본 디바이스의 성능 계층을 자동으로 미러링하지 않습니다. 수동으로 업데이트해야 합니다.

라이선스 PID

Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 Smart Software License 계정에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace에서 **Find Products and Solutions(**제품 및 솔루션 찾기**)** 검색 필드를 사용합니다. 다음 라이선스 제품 ID(PID)를 검색합니다.

그림 *1:* 라이선스 검색



Management Center Virtual PID

- VMware:
  - SF-FMC-VMW-2-K9 - 디바이스 2개
  - SF-FMC-VMW-10-K9 - 디바이스 10개
  - SF-FMC-VMW-K9 - 디바이스 25개
  - SF-FMC-VMW-300-K9 — 디바이스 300개
- KVM
  - SF-FMC-KVM-2-K9 - 디바이스 2개
  - SF-FMC-KVM-10-K9 — 디바이스 10개
  - SF-FMC-KVM-K9 - 디바이스 25개
- PAK 기반 VMware:
  - FS-VMW-2-SW-K9 - 디바이스 2개
  - FS-VMW-10-SW-K9 - 디바이스 10개
  - FS-VMW-SW-K9 - 디바이스 25개

Threat Defense Virtual PID

FTDV-SEC-SUB를 주문할 때 Essentials 라이선스 및 선택적 기능 라이선스(12개월 기간)를 선택해야 합니다.

- Essentials 라이선스:
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-30S-BSE-K9
  - FTD-V-50S-BSE-K9
  - FTD-V-100S-BSE-K9
- IPS, Malware 방어 및 URL 라이선스 조합:
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC
  - FTD-V-50S-TMC
  - FTD-V-100S-TMC
- Carrier—FTDV_CARRIER
- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 1010 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR1010T-TMC =

  위의 PID를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 1100 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR1120T-TMC =

- L-FPR1140T-TMC =
- L-FPR1150T-TMC =

위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.

- L-FPR1120T-TMC-1Y
- L-FPR1120T-TMC-3Y
- L-FPR1120T-TMC-5Y
- L-FPR1140T-TMC-1Y
- L-FPR1140T-TMC-3Y
- L-FPR1140T-TMC-5Y
- L-FPR1150T-TMC-1Y
- L-FPR1150T-TMC-3Y
- L-FPR1150T-TMC-5Y

- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 2100 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.

- FPR2110T-TMC-1Y
- L-FPR2110T-TMC-3Y
- L-FPR2110T-TMC-5Y
- L-FPR2120T-TMC-1Y
- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y

- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Secure Firewall 3100 PID

- Essentials 라이선스:
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR3110T-TMC=
  - L-FPR3120T-TMC=
  - L-FPR3130T-TMC=
  - L-FPR3140T-TMC=

  위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-FPR3105T-TMC-1Y
  - L-FPR3105T-TMC-3Y
  - L-FPR3105T-TMC-5Y
  - L-FPR3110T-TMC-1Y
  - L-FPR3110T-TMC-3Y
  - L-FPR3110T-TMC-5Y
  - L-FPR3120T-TMC-1Y
  - L-FPR3120T-TMC-3Y
  - L-FPR3120T-TMC-5Y
  - L-FPR3130T-TMC-1Y

- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- 캐리어:
  - L-FPR3K-FTD-CAR=

- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 4100 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC =
  - L-FPR4125T-TMC =
  - L-FPR4145T-TMC =

  위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y

- 캐리어:
  - L-FPR4K-FTD-CAR=
- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 9300 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR9K-40T-TMC =
  - L-FPR9K-48T-TMC =
  - L-FPR9K-56T-TMC =

  위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y
  - L-FPR9K-56T-TMC-1Y
  - L-FPR9K-56T-TMC-3Y
  - L-FPR9K-56T-TMC-5Y
- 캐리어:
  - L-FPR9K-FTD-CAR=
- Cisco Secure Client - Cisco AnyConnect 주문 가이드를 참고하십시오.

ISA 3000 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-ISA3000T-TMC=

  위의 PID를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-ISA3000T-TMC-1Y

- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- Cisco Secure Client - Cisco AnyConnect 주문 가이드를 참고하십시오.

라이선싱 요구 사항 및 사전 요건

특정 라이선스 예약 요구 사항의 경우 특정 라이센스 예약에 대한 요구 사항 및 사전 요건, 37 페이지의 내용을 참조하십시오.

일반적인 사전 요건

- management center 및 매니지드 디바이스에 NTP가 설정되어 있는지 확인합니다. 등록에 성공하려면 시간을 동기화해야 합니다.

  Firepower 4100/9300의 경우 management center와 동일한 NTP 서버를 사용하여 섀시에 NTP를 구성해야 합니다.

지원되는 도메인

글로벌, 표시된 경우를 제외하고.

사용자 역할

- 관리자

고가용성, 클러스터링 및 다중 인스턴스 라이선싱 요구 사항 및 사전 요건

이 섹션에서는 고가용성(디바이스 고가용성 및 management center virtual 고가용성), 클러스터링 및 다중 인스턴스 구축을 위한 라이선싱 요구 사항에 대해 설명합니다.

Management Center 고가용성을 위한 라이선싱

각 디바이스에는 단일 management center 또는 고가용성 쌍(하드웨어 또는 가상)의 management center로 관리되는 동일한 라이선스가 필요합니다.

예: management center 쌍으로 관리되는 두 디바이스에 대해 고급 악성코드 보호를 활성화하고 싶은 경우, 2개의 악성코드 방어 라이선스와 TM 서브스크립션을 구매하고 액티브 management center을 Smart Software Manager에 등록한 뒤 두 기기의 라이선스를 액티브 management center에 할당합니다.

액티브 management center만 Smart Software Manager에 등록됩니다. 페일오버가 발생하면 시스템은 Smart Software Manager와 통신하여 원래 활성 management center에서 라이선스 등록을 해제하고 새로운 액티브 management center에 할당합니다.

특정 라이선스 예약 구축에서는 기본 management center에서만 특정 라이선스 예약이 요구됩니다.

하드웨어 **Management Center**

고가용성 쌍의 하드웨어 management center에 필요한 특별한 라이선스는 없습니다.

Management Center Virtual

라이선스가 동일한 두 개의 management center virtual가 필요합니다.

예**:** 10개의 디바이스를 관리하는 management center virtual 고가용성 쌍의 경우 다음을 사용할 수 있습니다.

- management center virtual 10 엔타이틀먼트 2개
- 디바이스 라이선스 10개

고가용성 쌍을 분리하면 보조 management center virtual와 연결된 management center virtual 엔타이틀먼트가 해제됩니다. (이 예에서는 독립형 management center virtual 10이 2개 있습니다.)

디바이스 고가용성을 위한 라이선싱

고가용성 구성의 두 threat defense 유닛은 모두 동일한 라이선스를 가지고 있어야 합니다.

고가용성 구성에서는 디바이스 쌍의 각 디바이스에 대해 하나씩, 두 개의 라이선스 자격이 필요합니다.

고가용성을 설정하기 전에는 보조/스탠바이 디바이스에 어떤 라이선스가 할당되든 상관이 없습니다. 고가용성 설정 중에 management center은 스탠바이 유닛에 할당된 불필요한 라이선스를 해제하고 기본/액티브 유닛에 할당된 것과 동일한 라이선스로 교체합니다. 예를 들어 액티브 유닛에는 Essentials 라이선스와 IPS 라이선스가 있는데 스탠바이 유닛에 Essentials 라이선스만 있는 경우, management center은 Smart Software Manager와 통신하여 스탠바이 유닛의 어카운트에서 사용 가능한 IPS 라이선스를 가져옵니다. 라이선스에 포함되어 있는 구매한 엔타이틀먼트가 충분하지 않으면 정확한 수의 라이선스를 구매할 때까지 어카운트는 컴플라이언스 위반 상태가 됩니다.

디바이스 클러스터에 대한 라이선싱

각 threat defense virtual 클러스터 노드에는 동일한 성능 계층 라이선스가 필요합니다. 모든 멤버에 대해 동일한 수의 CPU 및 메모리를 사용하는 것이 좋습니다. 그렇지 않으면 성능이 가장 낮은 멤버와 일치하도록 모든 노드에서 제한됩니다. 처리량 레벨은 제어 노드에서 각 데이터 노드로 복제되어 일치합니다.

개별 노드가 아니라 전체 피처 클러스터에 라이선스를 할당합니다. 그러나 클러스터의 각 노드는 각 기능에 대한 별도 라이선스를 사용합니다. 클러스터링 기능 자체에는 라이선스가 필요하지 않습니다.

management center에 제어 노드를 추가하는 경우 클러스터에 사용하려는 기능 라이선스를 지정할 수 있습니다. 클러스터를 생성하기 전에는 데이터 노드에 할당된 라이선스가 중요하지 않습니다. 제어 노드의 라이선스 설정은 각 데이터 노드에 복제됩니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** > **License(**라이선스**)** 영역에서 클러스터 라이선스를 수정할 수 있습니다.

참고 management center이 라이선스 되기 전에 (평가 모드에서 실행 되기 전에) 클러스터를 추가하는 경우, management center를 라이선스하면 클러스터에 정책 변경을 구축할 때 트래픽 중단이 발생할 수 있습니다. 라이선스 모드를 변경하면 모든 데이터 유닛이 클러스터를 벗어났다가 다시 참가합니다.

다중 인스턴스 구축용 라이선싱

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

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

대표적인 예는 다음과 같습니다.

표 ***4: Firepower 9300***의 컨테이너 인스턴스에 대한 샘플 라이선스 사용

Firepower 9300	인스턴스	라이선스
보안 모듈 1	인스턴스 1	Essentials, URL, 악성코드 방어
	인스턴스 2	Essentials, URL
	인스턴스 3	Essentials, URL
보안 모듈 2	인스턴스 4	Essentials, IPS
	인스턴스 5	Essentials, URL, 악성코드 방어, IPS
보안 모듈 3	인스턴스 6	Essentials, 악성코드 방어, IPS
	인스턴스 7	Essentials, IPS

표 ***5:*** 수총 라이선스 수

Essentials	**URL**	악성코드 방어	**IPS**
3	2	3	2

스마트 어카운트 생성 및 라이선스 추가

이 어카운트를 설정하고 라이선스를 구입해야 합니다.

시작하기 전에

어카운트 담당자 또는 리셀러가 사용자 대신 스마트 어카운트를 설정했을 수도 있습니다. 그렇다면 이 절차를 사용하는 대신 해당 사용자의 어카운트에 액세스하는 데 필요한 정보를 얻은 후 해당 어카운트에 액세스할 수 있는지 확인합니다.

스마트 어카운트에 대한 일반 정보는 http://www.cisco.com/go/smartaccounts를 참조하십시오.

프로시저

단계 **1** 스마트 어카운트 요청:

자세한 내용은 https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 섹션을 참조해 주십시오.

추가 정보는 https://communities.cisco.com/docs/DOC-57261 내용을 참조하십시오.

단계 **2** 스마트 어카운트 설정 준비가 완료되었다는 이메일이 올 때까지 기다립니다. 이메일이 도착하면, 지시된 대로 거기에 포함된 링크를 클릭합니다.

단계 **3** 스마트 어카운트를 설정하빈다.

https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation로 이동합니다.

자세한 내용은 https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604 섹션을 참조해 주십시오.

단계 **4** Smart Software Manager에서 어카운트에 액세스할 수 있는지 확인합니다.

https://software.cisco.com/#module/SmartLicensing로 이동하여 로그인합니다.

단계 **5** Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다.

Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 스마트 어카운트에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace를 참조하십시오. 라이선스 PID는 라이선스 PID, 14 페이지 섹션을 참조하십시오.

Smart Licensing 구성

이 섹션에서는 Smart Software Manager 또는 Smart Software Manager On-Prem을 사용하여 스마트 라이선싱을 사용하는 방법을 설명합니다. 특정 라이선스 예약을 사용하려면 SLR(Specific License Reservation) 구성, 37 페이지의 내용을 참조하십시오.

스마트 라이선싱을 위한 **Management Center** 등록

인터넷을 통해 또는 Air-Gapped 네트워크를 사용하는 경우 Smart Software Manager On-Prem을 사용하여 Smart Software Manager에 직접 management center를 등록할 수 있습니다.

Management Center를 **Smart Software Manager**로 등록

management center를 Smart Software Manager로 등록

시작하기 전에

- Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다.

  Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 스마트 어카운트에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace를 참조하십시오. 라이선스 PID는 라이선스 PID, 14 페이지 섹션을 참조하십시오.

- management center가 Smart Software Manager(tools.cisco.com:443)에 연결할 수 있는지 확인합니다.

- NTP를 구성해야 합니다. 등록 중 스마트 에이전트 및 Smart Software Manager 간에 키 교환이 발생합니다. 따라서 시간을 해당 등록에 동기화해야 합니다.

  Firepower 4100/9300의 경우 management center와 동일한 NTP 서버를 사용하여 섀시에 NTP를 구성해야 합니다.

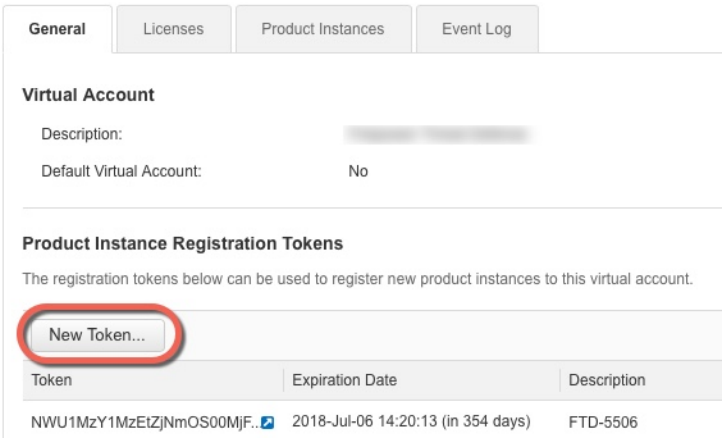
- 조직에 management center이(가) 여러 개 있다면, 각 management center의 이름이 동일한 가상 계정에 등록될 수 있는 다른 management center와(과) 명확하게 식별되는 고유한 이름인지 확인합니다. 이 이름은 스마트 라이선스 엔타이틀먼트 관리에 매우 중요하며 애매한 이름은 나중에 문제가 될 수 있습니다.

프로시저

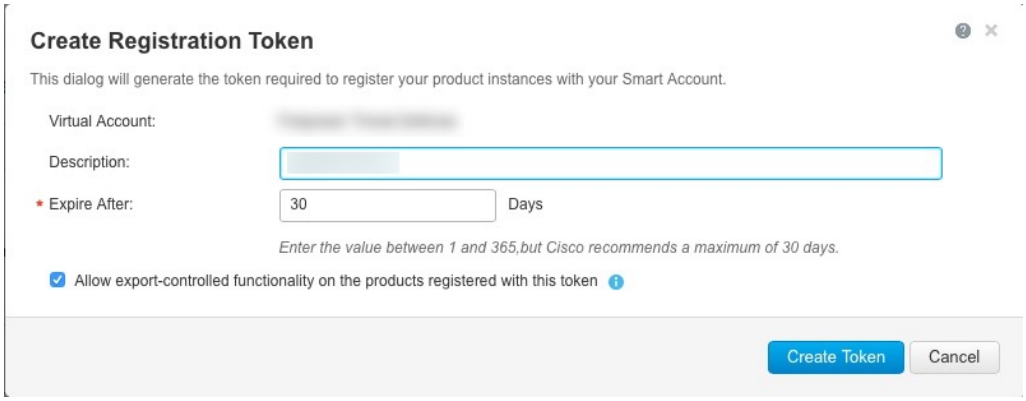
단계 **1** Smart Software Manager에서 이 디바이스를 추가할 가상 어카운트에 대한 등록 토큰을 요청 및 복사합니다.

a) **Inventory(**인벤토리**)**를 클릭합니다.

b) **General(**일반**)** 탭에서 **New Token(**새 토큰**)**을 클릭합니다.



c) **Create Registration Token(**등록 토큰 생성**)** 대화 상자에서 다음 설정을 입력한 다음 **Create Token(**토큰 생성**)**을 클릭합니다.



- 설명
- **Expire After(**다음 이후에 만료**)** — 30일로 설정하는 것이 좋습니다.
- **Allow export-controlled functionaility on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)**—강력한 암호화를 허용하는 국가에 있는 경우 내보내기-규정 준수 플래그를 활성화합니다. 해당 기능을 사용하려는 경우 이 옵션을 지금 선택해야 합니다. 나중에 이 기능을 활성화하는 경우 새 제품 키로 디바이스를 다시 등록하고 디바이스를 다시 로드해야 합니다. 이 옵션이 표시되지 않으면 계정이 내보내기 제어 기능을 지원하지 않는 것입니다.

토큰이 인벤토리에 추가됩니다.

d) 토큰의 오른쪽에 있는 화살표 아이콘을 클릭하여 **Token(**토큰**)** 대화 상자를 열면 토큰 ID를 클립보드에 복사할 수 있습니다. 나중에 절차에서 threat defense를 등록해야 하는 경우 사용하기 위해 이 토큰을 준비해 두십시오.

그림 *2:* 토큰 보기

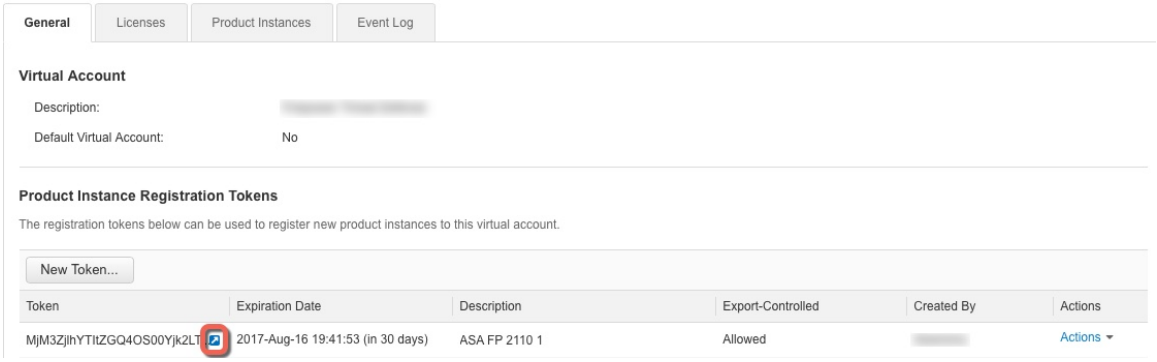
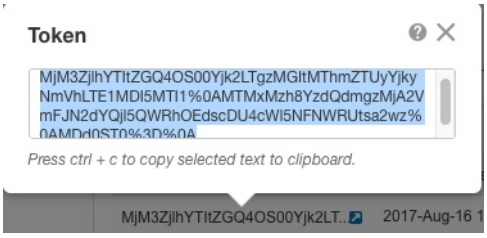


그림 *3:* 토큰 복사



단계 **2** management center에서 시스템 (⚙) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택합니다.

단계 **3** **Register(**등록**)**를 클릭합니다.

단계 **4** Smart Software Manager에서 생성한 토큰을 **Product Instance Registration Token(**제품 인스턴스 등록 토큰**)** 필드에 붙여넣기 합니다.

텍스트 시작이나 끝에 공백이나 빈 행이 없는지 확인합니다.

단계 **5** 사용량 데이터를 Cisco에 보낼지를 결정합니다.

- **Enable Cisco Success Network(Cisco Success Network** 활성화**)**는 기본적으로 활성화됩니다. 샘플 데이터를 클릭하고 Cisco에서 수집하는 데이터의 종류를 참조하십시오. 자세한 내용은 Cisco Success Network 등록 구성를 참고하십시오.
- **Cisco Support Diagnostics** 활성화는 기본적으로 비활성화됩니다. 확인란 위에 있는 링크에서 Cisco가 수집하는 데이터 종류를 확인할 수 있습니다. 자세한 내용은 Cisco 지원 진단 등록 구성를 참고하십시오.

  참고
  - 활성화하면, Cisco Support Diagnostics은 다음 동기화 주기에 디바이스에서 활성화됩니다. 디바이스와 management center 동기화는 30분마다 한 번씩 실행됩니다.
  - 활성화되면 Cisco Support Diagnostics가 이 management center에 등록된 모든 새 디바이스에서 자동으로 활성화됩니다.

단계 **6** **Apply Changes(**변경 사항 적용**)**를 클릭합니다.

다음에 수행할 작업

- 디바이스를 management center에 추가합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Management Center*에 디바이스 추가를 참조하십시오.
- 라이선스를 디바이스에 할당합니다. 여러 매니지드 디바이스에 라이선스 할당, 31 페이지의 내용을 참조하십시오.

Management Center를 Smart Software Manager 온프레미스로 등록

Smart Software Manager와의 정기적인 통신, 3 페이지에 설명된 대로, management center에서는 Cisco와 정기적으로 통신하여 라이선스 자격을 유지해야 합니다. 다음 상황 중 하나에 해당하는 경우 Smart Software Manager 온프레미스(이전 명칭: "Smart Software Satellite Server")을 Smart Software Manager에 연결하는 프록시로 사용할 수 있습니다.

- management center가 오프라인 상태이거나 연결이 제한적이거나 연결되지 않은 경우(즉, 에어 갭 네트워크에 구축).

  (공개 네트워크에 대한 대체 솔루션은 에어 갭(Air-Gapped) 구축 라이선싱 옵션, 2 페이지의 내용을 참조하십시오.)

- management center가 영구적으로 연결되어 있지만 네트워크에서 단일 연결을 통해 스마트 라이선스를 관리하려는 경우.

Smart Software Manager 온프레미스을(를) 사용하면 Smart Software Manager와의 동기화를 예약하거나 스마트 라이선스 인증을 수동으로 동기화할 수 있습니다.

Smart Software Manager 온프레미스에 대한 자세한 내용은 https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem 의 내용을 참조하십시오.

프로시저

단계 **1** Smart Software Manager 온프레미스을 구축하고 설정합니다.

- https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem에서 확인 가능한 Smart Software Manager 온프레미스에 대한 설명서를 참조하십시오.
- Smart Software Manager 온프레미스에서 TLS/SSL 인증서 CN을 메모합니다.
- http://www.cisco.com/security/pki/certs/clrca.cer로 이동한 다음, TLS/SSL 인증서 전체 본문("-----BEGIN CERTIFICATE-----" 부터 "-----END CERTIFICATE-----"까지)을 구성하는 동안 액세스할 수 있는 위치에 복사합니다.

단계 **2** management center을 Smart Software Manager 온프레미스에 등록합니다.

a) **Integration(**통합**)** > **Other Integrations(**기타 통합**)**를 선택합니다.

b) **Smart Software Satellite**를 클릭합니다.
c) **Connect to Cisco Smart Software Satellite Server(Cisco Smart Software Satellite Server**에 연결**)**을 선택합니다.
d) 이 절차의 사전 요구 사항에서 수집된 CN 값을 사용하여 Smart Software Manager 온프레미스의 **URL**을 다음 형식으로 입력합니다.

```
https://FQDN_or_hostname_of_your_SSM_On-Prem/SmartTransport
```

FQDN 또는 호스트 이름은 Smart Software Manager 온프레미스에서 제시하는 인증서의 CN 값과 일치해야 합니다.

e) 새 **SSL Certificate(SSL** 인증서**)**를 추가하고 이전에 복사한 인증서 텍스트를 붙여넣습니다.
f) **Apply(**적용**)**를 클릭합니다.
g) **System(**시스템**) > Licenses(**라이선스**) > Smart Licenses(**스마트 라이선스**)**를 선택하고 **Register(**등록**)**를 클릭합니다.
h) Smart Software Manager 온프레미스에서 신규 토큰을 생성합니다.
i) 토큰을 복사합니다.
j) 토큰을 관리 센터 페이지에 있는 양식에 붙여 넣습니다.
k) **Apply Changes(**변경 사항 적용**)**를 클릭합니다.

이제 관리 센터가 Smart Software Manager 온프레미스에 등록되었습니다.

단계 **3** 디바이스에 라이선스를 할당한 후 Smart Software Manager 온프레미스을 Smart Software Manager와 동기화합니다.

위의 Smart Software Manager 온프레미스 설명서를 참조하십시오.

단계 **4** 진행 중인 동기화 일정을 선택합니다.

(전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화

스마트 어카운트가 강력한 암호화에 대해 인증되지 않았지만 Cisco에서 강력한 암호화를 사용할 수 있다고 결정한 경우, 수동으로 어카운트에 강력한 암호화 라이선스를 추가할 수 있습니다.

시작하기 전에

- 구축에 이미 내보내기 제어 기능이 지원되지 않는지 확인합니다.

  구축에서 내보내기 제어 기능을 지원할 경우 등록 토큰 생성 페이지에는 Smart Software Manager 내보내기 제어 기능을 사용할 수 있는 옵션이 표시됩니다. 자세한 내용은 https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html를 참고하십시오.

- 구축에 평가판 라이선스가 사용되고 있지 않은지 확인합니다.
- Smart Software Manager의 **Inventory(**재고 목록**) > Licenses(**라이선스**)** 페이지에 다음과 같이 management center에 해당하는 라이선스가 있는지 확인합니다.

내보내기 제어 라이선스	**Management Center** 모델
Cisco Virtual FMC 시리즈 강력한 암호화 (3DES/AES)	모든 management center virtual
Cisco FMC 1K시리즈 강력한 암호화 (3DES/AES)	1000, 1600
Cisco FMC 2K 시리즈 강력한 암호화 (3DES/AES)	2500, 2600
Cisco FMC 4K 시리즈 강력한 암호화 (3DES/AES)	4500, 4600

프로시저

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

참고 **Request Export Key(**내보내기 키 요청**)**가 표시되는 경우, 해당 어카운트는 내보내기 제어 기능이 승인된 것이며 이 필요 기능 사용을 진행할 수 있습니다.

단계 **2** **Request Export Key(**내보내기 키 요청**)**를 클릭하고 내보내기 키를 생성합니다.

팁 내보내기 제어 키 요청이 실패하는 경우, 가상 어카운트에 유효한 내보내기 제어 라이선스가 있는지 확인합니다.

Return Export Key(내보내기 키 반환**)**를 클릭하여 내보내기 제어 라이선스를 비활성화합니다.

다음에 수행할 작업

이제 내보내기 제어 기능을 사용하는 구성이나 정책을 배포할 수 있습니다.

기억 새로운 내보내기 제어 라이선스 및 이 라이선스에 의해 활성화된 모든 기능은 디바이스가 재부팅될 때까지 threat defense 디바이스에 적용되지 않습니다. 그 때까지 이전 라이선스에서 지원하는 기능만 활성화됩니다.

고가용성 구축에서 threat defense 디바이스를 모두 동시에 재부팅해야 액티브-액티브 상태를 방지할 수 있습니다.

매니지드 디바이스에 라이선스 할당

디바이스를 management center에 등록할 때 대부분의 라이선스를 할당할 수 있습니다. 디바이스당 또는 여러 디바이스에 대해 라이선스를 할당할 수도 있습니다.

단일 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.

참고 threat defense 클러스터의 경우, 라이선스를 클러스터 전체에 적용합니다. 참고로 클러스터의 각 유닛은 기능당 별도의 라이선스를 필요로 합니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 네트워크 관리자 권한으로 로그인해야 합니다. 여러 도메인을 사용하여 작업하는 경우 리프 도메인에서 이 작업을 수행해야 합니다.

프로시저

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

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

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

단계 **3** **Device(**디바이스**)**를 클릭합니다.

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

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

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

다음에 수행할 작업

라이선스 상태 확인: 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(**Check Mark(**확인 표시**)** ( ))만 표시되는지 확인합니다. 다른 아이콘이 표시되는 경우, 아이콘 위에 마우스를 놓으면 자세한 정보가 표시됩니다.

여러 매니지드 디바이스에 라이선스 할당

management center로 관리하는 디바이스는 라이선스를 management center를 통해 얻습니다. Smart Software Manager에서 직접 하지 않습니다.

이 절차를 사용하여 여러 디바이스에서 한 번에 라이선스를 활성화합니다.

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.

참고 threat defense 클러스터의 경우, 라이선스를 클러스터 전체에 적용합니다. 참고로 클러스터의 각 유닛은 기능당 별도의 라이선스를 필요로 합니다.

프로시저

단계 **1** 시스템 ( ) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 또는 **Specific Licenses(**특정 라이선스**)**를 선택합니다.

단계 **2** **Edit Licenses(**라이선스 편집**)**을 클릭합니다.

단계 **3** 디바이스에 추가하려는 각 라이선스 유형:

a) 라이선스 유형에 대한 탭을 클릭합니다.

b) 왼쪽 목록에서 디바이스를 클릭합니다.

c) **Add(**추가**)**를 클릭하고 오른쪽 목록으로 해당 디바이스를 이동합니다.

d) 각 디바이스에 대해 이를 반복하고 라이선스 유형을 받습니다.

이제 추가하려는 모든 디바이스에 라이선스가 있는지에 대해서는 걱정하지 마십시오.

e) 추가하려는 라이선스 각 유형에 대해 라이선스의 각 유형에 대해 이 하위 절차를 반복합니다.

f) 라이선스를 제거하려면 디바이스 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

g) **Apply(**적용**)**를 클릭합니다.

다음에 수행할 작업

라이선스가 올바르게 설치되어 있는지 확인합니다. 스마트 라이선스 모니터링, 33 페이지에서 절차를 따릅니다.

스마트 라이선싱 관리

이 섹션에서는 스마트 라이선싱을 관리하는 방법을 설명합니다.

등록 취소Management Center

Smart Software Manager에서 management center의 등록을 취소하여 다른 디바이스에서 사용할 수 있도록 모든 라이선스 자격을 스마트 어카운트에 다시 릴리스합니다. 예를 들어 management center를 해제하거나 이미지를 재설치해야 하는 경우 등록을 취소합니다.

등록되지 않은 상태에서 라이선스를 시행하는 방법에 대한 자세한 내용은 등록 취소 상태, 4 페이지의 내용을 참조하십시오.

프로시저

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

단계 **2** **Deregister(**등록 해제**)**( ) 버튼을 클릭합니다.

Management Center 동기화 또는 재인증

기본적으로 ID 인증서는 6개월마다 자동으로 갱신되며, 라이선스 엔타이틀먼트는 30일마다 갱신됩니다. 예를 들어 인터넷 액세스 기간이 제한된 경우 또는 Smart Software Manager에서 라이선싱을 변경한 경우, 이러한 항목 중 하나에 대한 등록을 수동으로 갱신할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**을(를) 선택합니다.

단계 **2** ID 인증서를 갱신하려면, 동기화( )를 클릭합니다.

단계 **3** 라이센스 엔타이틀먼트를 갱신하려면 **Re-Authorize(**재승인**)**를 클릭합니다.

스마트 라이선스 상태 모니터링

System(시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 페이지의 스마트 라이선스 상태**(Smart License Status)** 섹션은 아래 설명된 대로 management center의 라이선스 사용에 대한 개요를 보여줍니다.

사용 권한 부여

가능한 상태 값:

- **In-compliance(**인 컴플라이언스**)**( ) — 매니지드 디바이스에 할당된 모든 라이선스가 준수 상태이고 management center가 Smart Software Manager와 성공적으로 통신합니다.
- **License is in compliance but communication with licensing authority has failed(**라이선스는 준수 상태이지만 **licensing authority**와의 통신은 실패하였습니다**)**— 디바이스 라이선스는 준수 상태이지만 management center가 Cisco licensing authority와 통신할 수 없습니다.

- **Out-of-compliance icon or unable to communicate with License Authority(**미준수 아이콘 또는 **License Authority**와 통신 불가**)**—하나 이상의 매니지드 디바이스는 미준수 상태의 라이선스를 사용 중이거나 management center가 Smart Software Manager와 90일 이상 통신하지 못했습니다.

제품 등록

management center이 Smart Software Manager에 연결하고 등록한 마지막 날짜를 나타냅니다.

할당된 가상 어카운트

제품 인스턴스 등록 토큰을 생성하고 management center 등록을 등록하는 데 사용한 스마트 어카운트에 속한 가상 어카운트를 나타냅니다. 이 구축이 스마트 어카운트 내의 특정 가상 어카운트와 연결되지 않는 경우, 이 정보는 표시되지 않습니다.

내보내기 제어 기능

이 옵션을 활성화하는 경우, 제한된 기능을 배포할 수 있습니다. 자세한 내용은 내보내기 제어 기능 라이선싱, 11 페이지 섹션을 참조해 주십시오.

Cisco Success Network

management center에 대해 Cisco Success Network를 활성화했는지 여부를 나타냅니다. 이 옵션을 활성화하는 경우, 기술 지원에 필요한 사용 정보 및 통계가 Cisco에 제공됩니다. 또한, 이 정보를 통해 Cisco는 제품을 개선할 수 있으며 사용 가능하지만 사용되지 않은 기능을 알려 네트워크의 제품 가치를 최대화하도록 할 수 있습니다. 자세한 내용은 Cisco Success Network 등록 구성를 참조하십시오.

스마트 라이선스 모니터링

management center 및 해당 매니지드 디바이스의 라이선스 상태를 확인하려면 Smart License(스마트 라이선스) 페이지를 사용합니다.

구축에서 라이선스의 각 유형에 대해 이 페이지는 사용된 라이선스 총 수, 라이선스 컴플라이언스 상태, 디바이스 유형, 디바이스가 구축된 도메인 및 그룹에 대한 목록을 보여줍니다. management center의 스마트 라이선스 상태도 볼 수 있습니다. 컨테이너 인스턴스는 동일한 보안 모듈/엔진에서 보안 모듈/엔진당 하나의 라이선스만 사용합니다. 따라서 management center에 각 라이선스 유형별 각 컨테이너 인스턴스 목록이 별도로 표시되지만, 기능 라이선스 유형에 대해 사용된 라이선스 수는 오직 1이 됩니다.

Smart Licenses(스마트 라이선스**)** 페이지 외에도, 라이선스를 볼 수 있는 몇 가지 다른 방법이 있습니다.

- **Product Licensing(**제품 라이선싱**)** 대시보드 위젯은 사용자 라이선스를 한눈에 볼 수 있는 개요를 제공합니다.

  대시보드에 위젯 추가, 사용자 역할별 대시보드 위젯 가용성 및 제품 라이선싱 위젯를 참조하십시오.

- **Device Management(**디바이스 관리**)** 페이지(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**)에 각 매니지드 디바이스에 적용된 라이선스 목록이 표시됩니다.

- **Smart License Monitor(**스마트 라이선스 모니터**)** 상태 모듈이 상태 정책에서 사용되는 경우 라이선스 상태를 알려줍니다.

프로시저

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

단계 **2** **Smart Licenses(**스마트 라이선스**)** 테이블에서 각 **License Type(**라이선스 유형**)** 폴더의 왼쪽에 있는 화살표를 클릭하고 해당 폴더를 확장합니다.

단계 **3** 각 폴더에서 각 디바이스의 **License Status(**라이선스 상태**)** 열에 **Check Mark(**확인 표시**)** ( )와 함께 녹색 원이 있는지 확인합니다.

참고 중복 management center virtual 라이선스가 표시되는 경우, 각각은 하나의 매니지드 디바이스를 나타냅니다.

모든 디바이스에 **Check Mark(**확인 표시**)** ( )와 함께 녹색 원이 있는 경우, 디바이스에 정상적으로 라이선스가 부여되고 사용할 준비가 된 것입니다.

녹색 원(**Check Mark(**확인 표시**)** ( )) 이외의 License Status(라이선스 상태)가 표시되는 경우, 해당 상태 아이콘 위에 마우스를 놓고 메시지를 확인합니다.

다음에 수행할 작업

- 녹색 원(**Check Mark(**확인 표시**)** ( ))이 없는 디바이스가 있는 경우, 라이선스를 추가로 구입해야 할 수도 있습니다.

스마트 라이선싱 트러블슈팅

예상했던 라이선스가 내 스마트 어카운트에 표시되지 않습니다

예상했던 라이선스가 스마트 어카운트에 없는 경우 다음을 시도하십시오.

- 해당 라이선스가 다른 가상 어카운트에 없는지 확인합니다. 조직의 라이선스 관리자가 이 문제 해결을 도와야 할 수도 있습니다.
- 라이선스 판매자에게 해당 어카운트로의 전송이 완료되었는지 확인합니다.

스마트 라이선스 서버에 연결할 수 없음

먼저 확실한 원인을 확인하십시오. 예를 들어, management center에 외부 연결이 있는지 확인합니다. 인터넷 액세스 요구 사항의 내용을 참조하십시오.

예상하지 않은 미준수 알림 또는 기타 오류

- 디바이스가 이미 다른 management center에 등록된 경우, 새 management center에서 디바이스에 라이선스를 부여하기 전에 원래 management center를 등록 취소해야 합니다. 등록 취소Management Center, 32 페이지을 참조하십시오.
- 구독 라이선스의 기간이 만료되었는지 확인합니다.

다른 문제 해결

다른 일반적인 문제에 대한 솔루션은 다음을 참조하십시오. https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html

Threat Defense에서 사용할 클래식 라이선스 변환

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

참고 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 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 어카운트 생성 및 라이선스 추가, 22 페이지의 내용을 참조하십시오.
- 변환하려는 PAK 또는 라이선스가 스마트 어카운트에 나타나야 합니다.
- 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.

- 라이선스 등록 포털을 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.
  - 라이선스 등록 포털(https://tools.cisco.com/SWIFT/LicensingUI/Home)에 로그인하고 위 문서의 지침을 따르십시오.

- Smart Software Manager를 사용하여 PAK 또는 라이선스를 변환하려면 다음을 수행합니다.
  - 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
  - Smart Software Manager(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 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** device manager을 사용하여 이 디바이스를 독립형 디바이스로 관리하려는 경우:

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html의 device manager 구성 가이드에서 디바이스 라이선싱에 대한 정보를 참조하십시오.

이 절차의 나머지 부분을 건너뜁니다.

단계 **5** 이미 management center에 스마트 라이선싱을 구축한 경우:

a) 새 threat defense에서 스마트 라이선싱을 설정합니다.

여러 매니지드 디바이스에 라이선스 할당, 31 페이지의 내용을 참조하십시오.

b) 새 스마트 라이선스가 디바이스에 성공적으로 적용되었는지 확인합니다.

스마트 라이선스 모니터링, 33 페이지의 내용을 참조하십시오.

단계 **6** 아직 management center에 스마트 라이선싱을 구축하지 않은 경우:

Smart Licensing 구성, 23 페이지의 내용을 참조하십시오. (적용되지 않거나 이미 완료한 단계를 모두 건너뜁니다.)

SLR(Specific License Reservation) 구성

에어 갭 네트워크에서 스마트 라이선싱을 배포하는 특정 라이선스 예약 기능을 사용할 수 있습니다.

참고 Cisco에서는 SLR, SPLR, PLR, 영구 라이선스 예약을 비롯한 다양한 이름이 특정 라이선스 예약에 사용됩니다. 이러한 용어는 Cisco에서 유사한 라이선싱 모델을 지칭하는 데 사용할 수 있지만, 반드시 동일한 라이선싱 모델을 나타내지는 않습니다.

특정 라이선스 예약을 활성화하는 경우, management center는 Smart Software Manager 또는 Smart Software Satellite Server에 액세스하거나 Smart Software Manager 온프레미스을 사용하지 않고 가상 어카운트에서 라이선스를 지정된 기간 동안 예약합니다.

인터넷에 액세스해야 하는 기능(예: URL 조회 또는 공용 웹 사이트 상황별 크로스 실행)이 작동하지 않습니다.

Cisco는 특정 라이선스 예약을 사용하는 배포에 대한 웹 분석 또는 텔레메트리 분석 데이터를 수집하지 않습니다.

특정 라이센스 예약에 대한 요구 사항 및 사전 요건

- 현재 일반 스마트 라이선싱을 사용하는 경우, management center를 등록 취소하고 특정 라이선스 예약을 구현합니다. 자세한 내용은 등록 취소Management Center, 32 페이지 섹션을 참조해 주십시오.

  management center에 현재 배포된 모든 스마트 라이선스는 사용자 어카운트에서 사용 가능한 라이선스 풀로 반환되며, 특정 라이선스 예약을 구현하는 경우 다시 이를 사용할 수 있습니다.

- 특정 라이선스 예약은 일반 스마트 라이선싱과 동일한 라이선스 유형을 사용합니다.
- (권장 사항) 고가용성 구성으로 management center 쌍을 구축하는 경우 라이선스를 할당하기 전에 고가용성을 구성해야 합니다. 보조 management center의 디바이스에 이미 라이선스를 할당한 경우 할당을 취소해야 합니다.

스마트 어카운트가 특정 라이선스 예약을 구축할 준비가 되었는지 확인

특정 라이선스 예약을 배포할 때 문제를 방지하기 위해 management center를 변경하기 전에 이 절차를 완료합니다.

시작하기 전에

- 특정 라이센스 예약에 대한 요구 사항 및 사전 요건, 37 페이지에서 요건을 충족했는지 확인합니다.
- Smart Software Manager 크리덴셜을 갖추도록 합니다.

프로시저

단계 **1** Smart Software Manager에 로그인합니다.

https://software.cisco.com/#SmartLicensing-Inventory

단계 **2** 해당하는 경우 페이지 오른쪽 상단에서 올바른 계정을 선택합니다.

단계 **3** 필요한 경우 **Inventory(**재고**)**를 클릭합니다.

단계 **4** **Licenses(**라이선스**)**를 클릭합니다.

단계 **5** 다음을 확인합니다.

- **License Reservation(**라이선스 예약**)** 단추가 있습니다.
- 구축하려는 디바이스와 기능을 위한 플랫폼과 기능 라이선스가 충분합니다(예: 해당되는 경우 디바이스에 대한 management center virtual 엔타이틀먼트).

단계 **6** 이러한 항목 중 하나라도 누락되었거나 잘못된 경우, 어카운트 담당자에게 문의하고 문제를 해결합니다.

참고 문제를 해결할 때까지 이 과정을 계속 진행하지 마십시오.

특정 라이선싱 메뉴 옵션 활성화

이 절차는 management center의 "Smart Licenses(스마트 라이선스)" 메뉴 옵션을 "Specific Licenses(특정 라이선스)"로 변경합니다.

프로시저

단계 **1** USB 키보드와 VGA 모니터를 사용하여 management center 콘솔에 액세스하거나 SSH를 사용하여 관리 인터페이스에 액세스합니다.

단계 **2** management center CLI 관리자 계정에 로그인합니다.

단계 **3** **expert** 명령을 입력하여 Linux 셸에 액세스합니다.

단계 **4** 다음 명령을 실행하고 특정 라이선스 예약 옵션에 액세스합니다.

sudo manage_slr.pl

예제**:**

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

단계 **5** 옵션 **2**를 선택하고 Specific License Reservation(특정 라이선스 예약)을 활성화합니다.

단계 **6** 옵션 **0**을 선택하고 manage_slr 유틸리티를 종료합니다.

단계 **7** **exit**를 입력하고 Linux 셸을 종료합니다.

단계 **8** **exit**를 입력하여 명령줄 인터페이스를 종료합니다.

단계 **9** management center 웹 인터페이스의 **Specific License Reservation(**특정 라이선스 예약**)** 페이지에 액세스할 수 있는지 확인합니다.

- **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**페이지가 현재 표시된 경우, 페이지를 새로 고칩니다.
- 아니면 **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

특정 라이선스 예약 인증 코드를 **Management Center**에 입력

프로시저

단계 **1** 예약 요청 코드를 생성합니다.

a) management center에서 **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

b) **Generate(**생성**)**를 클릭합니다.

c) **Reservation Request Code(**예약 요청 코드**)**를 메모합니다.

단계 **2** 예약 인증 코드를 생성합니다.

a) Cisco Smart Software Manager로 이동합니다.https://software.cisco.com/#SmartLicensing-Inventory

b) 필요한 경우 페이지 오른쪽 상단에서 올바른 계정을 선택합니다.

c) 필요한 경우 **Inventory(**재고**)**를 클릭합니다.

d) **Licenses(**라이선스**)**를 클릭합니다.

e) **License Reservation(**라이선스 예약**)**을 클릭합니다.

f) management center에서 생성한 코드를 **Reservation Request Code(**예약 요청 코드**)** 상자에 입력합니다.

g) **Next(**다음**)**를 클릭합니다.

h) **Reserve a specific license(**특정 라이선스 예약**)**를 선택합니다.

i) 아래로 스크롤하여 전체 라이선스 그리드를 표시합니다.

j) **Quantity To Reserve(**예약 수량**)**에 구축에 필요한 각 플랫폼 및 기능 라이선스의 수를 입력합니다.

참고

- 각 매니지드 디바이스 또는 다중 인스턴스 구축의 경우 각 컨테이너에 대한 Essentials 라이선스를 명시적으로 포함해야 합니다.
- management center virtual를 사용하는 경우, 각 컨테이너(다중 인스턴스 구축의 경우)이나 각 매니지드 디바이스(그 외 모든 구축의 경우)에 대한 자격을 포함해야 합니다.
- 강력한 암호화 기능을 사용하는 경우:
  - 내보내기 제어 기능에서 Smart Account(스마트 어카운트) 전체를 활성화하는 경우, 여기서 어떠한 작업도 수행할 필요가 없습니다.
  - 해당 조직의 자격이 management center에 따르는 경우, 적절한 라이선스를 선택해야 합니다.

  management center에 대한 정확한 라이선스 이름은 (전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화, 28 페이지에서 해당 사전 요구 사항을 참조하십시오.

k) **Next(**다음**)**를 클릭합니다.

l) **Generate Authorization Code(**인증 코드 생성를 클릭합니다.

이 시점에서는 Smart Software Manager에 따라 라이선스가 사용됩니다.

m) 인증 코드를 다운로드하고 management center에 입력할 준비를 합니다.

단계 **3** management center에 인증 코드를 입력합니다.

a) management center에서 **Browse(**찾아보기**)** 를 클릭하여 Smart Software Manager에서 생성한 인증 코드로 텍스트 파일을 업로드합니다.

b) **Install(**설치**)**을 클릭합니다.

c) **Specific License Reservation(**특정 라이선스 예약**)** 페이지에 **Usage Authorization(**사용 권한 부여**)** 상태가 authorized(권한 있음)로 표시되는지 확인합니다.

d)

단계 **4** **Reserved License(**예약된 라이선스**)** 탭을 클릭하고 선택된 라이선스를 확인하는 한편 **Authorization Code(**인증 코드**)**를 생성합니다.

필요한 라이선스가 표시되지 않는 경우, 필요한 라이선스를 추가합니다. 자세한 정보는 특정 라이선스 예약 업데이트를 참조하십시오.

매니지드 디바이스에 특정 라이선스 할당

이 절차를 사용하여 한 번에 여러 매니지드 디바이스에 라이선스를 신속하게 할당합니다.

또한 이 절차를 사용하여 라이선스를 비활성화하거나 디바이스 간에 라이선스를 이동시킬 수 있습니다. 디바이스에 대한 라이선스를 비활성화하는 경우, 해당 디바이스에서 그 라이선스와 관련된 기능을 사용할 수 없습니다.

프로시저

단계 **1** **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

단계 **2** **Edit Licenses(**라이선스 편집**)**을 클릭합니다.

단계 **3** 각 탭을 클릭하고 필요에 따라 디바이스에 라이선스를 할당합니다.

단계 **4** **Apply(**적용**)**를 클릭합니다.

단계 **5** **Assigned Licenses(**할당된 라이선스**)** 탭을 클릭하고 각 디바이스에 라이선스가 올바르게 설치되어 있는지 확인합니다.

단계 **6** 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

특정 라이선스 예약 관리

이 섹션에서는 특정 라이선스 예약을 관리하는 방법을 설명합니다.

중요! 특정 라이선스 예약 구축 유지 관리

위협 데이터 및 소프트웨어를 업데이트하고 구축을 효과적으로 유지하려면 에어-갭(Air-Gapped) 구축 유지 관리을 참조하십시오.

모든 기능이 중단 없이 계속 작동되도록 하려면 라이선스 만료 날짜를 모니터링합니다(**Reserved Licenses(**예약된 라이선스**)** 탭).

특정 라이선스 예약 업데이트

management center에 특정 라이선스를 성공적으로 구축한 경우, 이 절차를 사용하여 엔타이틀먼트를 언제든 추가 또는 제거할 수 있습니다.

라이선스가 만료된 후 라이선스를 갱신해야 하는 경우 이 절차를 사용합니다. 필요한 라이선스가 없는 경우 다음 작업이 제한됩니다.

- 디바이스 등록
- 정책 구축

프로시저

단계 **1** management center에서 management center의 고유한 제품 인스턴스 식별자를 가져옵니다.

a) **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

b) **Product Instance(**제품 인스턴스**)** 값을 메모합니다.

이 프로세스가 진행되는 동안 이 값이 여러 번 필요합니다.

단계 **2** Smart Software Manager에서 업데이트할 management center를 식별합니다.

a) Smart Software Manager로 이동합니다.

https://software.cisco.com/#SmartLicensing-Inventory

b) 필요한 경우 **Inventory(**재고**)**를 클릭합니다.

c) **Product Instances(**제품 인스턴스**)**를 클릭합니다.

d) **Type(**유형**)** 열에 **FT**, **Name(**이름**)** 열에 일반 SKU(호스트네임 아님)로 되어 있는 제품 인스턴스를 찾습니다. 다른 테이블 열에 있는 값을 사용하여 어떤 management center가 올바른 management center인지 결정할 수 있습니다. 이름을 클릭합니다.

e) **UUID**를 보고 수정하려는 management center의 UUID인지 확인합니다.

그렇지 않으면 올바른 management center를 찾을 때까지 이러한 단계를 반복해야 합니다.

단계 **3** 올바른 management center를 Smart Software Manager에서 찾은 경우, 예약된 라이선스를 업데이트하고 새 인증 코드를 생성합니다.

a) 올바른 UUID를 나타내는 페이지에서 **Actions(**작업**)** > **Update Reserved Licenses(**예약된 라이선스 업데이트**)**를 선택합니다.

b) 필요에 따라 예약된 라이선스를 업데이트합니다.

참고

- 각 매니지드 디바이스 또는 다중 인스턴스 구축의 경우 각 컨테이너에 대한 Essentials 라이선스를 명시적으로 포함해야 합니다.
- management center virtual를 사용하는 경우, 각 컨테이너(다중 인스턴스 구축의 경우)이나 각 매니지드 디바이스(그 외 모든 구축의 경우)에 대한 자격을 포함해야 합니다.
- 강력한 암호화 기능을 사용하는 경우:
  - 내보내기 제어 기능에서 Smart Account(스마트 어카운트) 전체를 활성화하는 경우, 여기서 어떠한 작업도 수행할 필요가 없습니다.
  - 해당 조직의 자격이 management center에 따르는 경우, 적절한 라이선스를 선택해야 합니다.

  management center에 대한 정확한 라이선스 이름은 (전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화, 28 페이지에서 해당 사전 요구 사항을 참조하십시오.

c) **Next(**다음**)**를 클릭하고 상세정보를 확인합니다.

d) **Generate Authorization Code(**인증 코드 생성**)**를 클릭합니다.
e) 인증 코드를 다운로드하고 management center에 입력할 준비를 합니다.
f) **Update Reservation(**예약 업데이트**)** 페이지를 열어 둡니다. 이 절차의 뒷부분에서 해당 페이지로 돌아갑니다.

단계 **4** management center에서 특정 라이선스를 업데이트합니다.

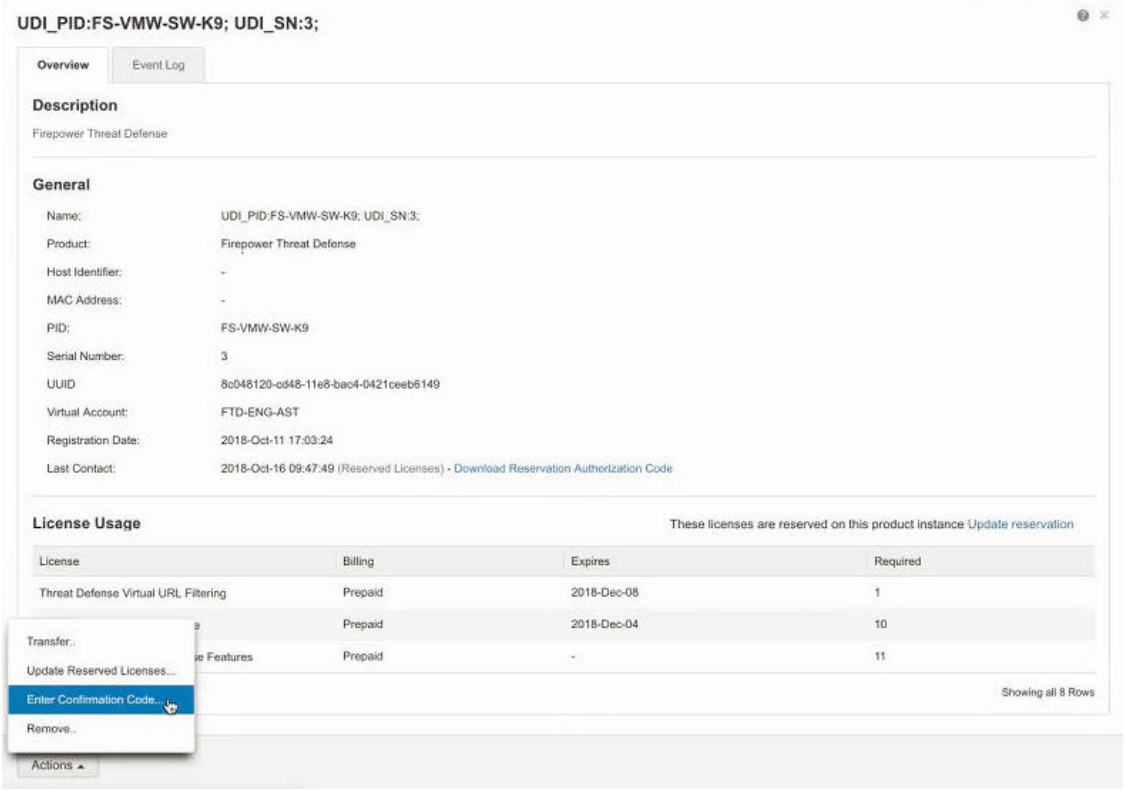
a) **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.
b) **Edit SLR(SLR** 편집**)**을 클릭합니다.
c) **Browse(**브라우저**)**를 클릭하고 새로 생성된 인증 코드를 업로드합니다.
d) **Install(**설치**)**을 클릭하고 라이선스를 업데이트합니다.

인증 코드가 성공적으로 설치된 경우, management center의 **Reserved**(예약된 라이선스) 열에 표시된 라이선스가 Smart Software Manager에 예약한 라이선스와 일치하는지 확인합니다.

e) **Confirmation Code(**인증 코드**)**를 메모합니다.

단계 **5** Smart Software Manager에서 인증 코드를 입력합니다.

a) 이 절차의 앞부분에서 열어 둔 Smart Software Manager 페이지를 돌아갑니다.
b) **Actions(**작업**)** >**Enter Confirmation Code(**인증 코드 입력**)**을 선택합니다.



c) management center에서 생성된 인증 코드를 입력합니다.

단계 **6** management center에서 라이선스가 예상대로 예약이 되었는지 그리고 각 매니지드 디바이스의 각 기능에 **Check Mark(**확인 표시**)** (✔)가 있는 녹색 원이 있는지 확인합니다.

필요한 경우, 자세한 내용은 특정 라이선스 예약 상태 모니터링, 46 페이지를 참조하십시오.

단계 **7** 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

특정 라이선스 예약 비활성화 및 반환

특정 라이선스가 더 이상 필요하지 않은 경우, 반드시 스마트 어카운트로 반환해야 합니다. 스마트 라이선싱 계정을 등록하려면 특정 라이선스 예약을 비활성화해야 합니다(아래 절차의 6단계).

중요 이 절차의 모든 단계를 수행하지 않는 경우, 라이선스는 사용 중 상태로 남게 되고 다시 사용할 수 없습니다.

이 절차는 management center와 연결되는 모든 라이선스 엔타이틀먼트를 가상 계정에 다시 릴리스합니다. 등록 취소 후에는 라이선스된 기능에 대한 업데이트나 변경은 허용되지 않습니다.

프로시저

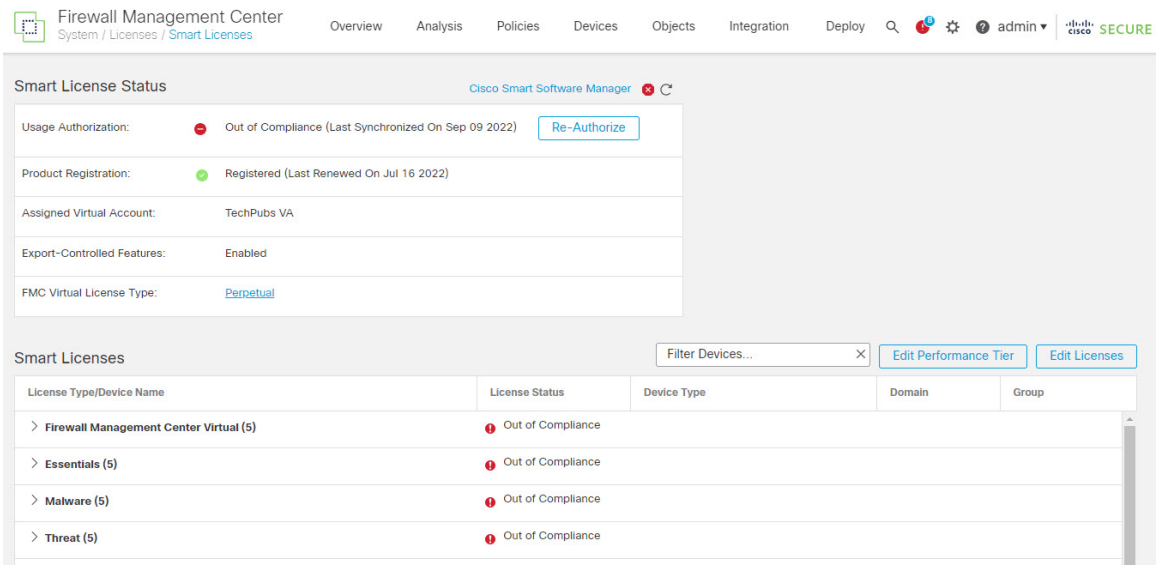
단계 **1** management center 웹 인터페이스에서 **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

단계 **2** management center에 대한 **Product Instance(**제품 인스턴스**)** 식별자를 메모합니다.

단계 **3** management center에서 반환 코드를 생성합니다.

a) **SLR(SLR**로 돌아가기**)**를 클릭합니다.

다음 그림에는 Return SLR(SLR 반환)이 나와 있습니다.



디바이스의 라이선스가 해제되고 management center은 등록 취소 상태로 전환됩니다.

b) **Return Code(**코드 반환**)**을 메모합니다.

단계 **4** Smart Software Manager에서 등록을 취소할 management center을 식별합니다.

a) Smart Software Manager로 이동합니다.

https://software.cisco.com/#SmartLicensing-Inventory

b) 필요한 경우 **Inventory(**재고**)**를 클릭합니다.

c) **Product Instances(**제품 인스턴스**)**를 클릭합니다.

d) **Type(**유형**)** 열에 **FT**, **Name(**이름**)** 열에 일반 SKU(호스트네임 아님)로 되어 있는 제품 인스턴스를 찾습니다. 다른 테이블 열에 있는 값을 사용하여 어떤 management center가 올바른 management center인지 결정할 수 있습니다. 이름을 클릭합니다.

e) **UUID**를 보고 수정하려는 management center의 UUID인지 확인합니다.

그렇지 않으면 올바른 management center를 찾을 때까지 이러한 단계를 반복해야 합니다.

단계 **5** 올바른 management center를 찾은 경우, 다음과 같이 스마트 어카운트에 라이선스를 반환합니다.

a) 올바른 UUID를 나타내는 페이지에서 **Actions(**작업**)** > **Remove(**제거**)**를 선택합니다.

b) management center에서 생성한 예약 반환 코드를 **Remove Product Instance(**제품 인스턴스 제거**)** 대화 상자에 입력합니다.

c) **Remove Product Instance(**제품 인스턴스 제거**)**를 클릭합니다.

특정 예약된 라이선스는 스마트 어카운트에서 사용 가능한 풀로 반환되고, 이 management center는 Smart Software Manager 제품 인스턴스 목록에서 제거됩니다.

단계 **6** management center Linux 셸에서 특정 라이선스 비활성화:

a) USB 키보드와 VGA 모니터를 사용하여 management center 콘솔에 액세스하거나 SSH를 사용하여 관리 인터페이스에 액세스합니다.

b) management center CLI 관리자 계정에 로그인합니다. 이렇게 하면 명령줄 인터페이스에 액세스할 수 있습니다.

c) **expert** 명령을 입력하여 Linux 셸에 액세스합니다.

d) 다음 명령을 실행합니다.

sudo manage_slr.pl

예제**:**

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) 특정 라이선스 예약을 비활성화 하려면 메뉴 옵션 **3**을 선택합니다.
f) 옵션 **0**을 선택하고 manage_slr 유틸리티를 종료합니다.
g) **exit**을(를) 입력하여 Linux 셸을 종료합니다.
h) **exit**를 입력하여 명령줄 인터페이스를 종료합니다.

특정 라이선스 예약 상태 모니터링

System(시스템) > **Licenses**(라이선스) > **Specific Licenses**(특정 라이선스) 페이지는 아래 설명된 대로 management center의 라이선스 사용에 대한 개요를 보여줍니다.

사용 권한 부여

가능한 상태 값:

- **Authorized**(권한 있음) — management center가 준수 상태이고, 어플라이언스에 대한 라이선스 엔타이틀먼트를 부여하는 License Authority에 정상적으로 등록됩니다.
- **Out-of-compliance**(미준수) — 라이선스가 만료되거나 management center가 예약되지 않은 라이선스를 과다하게 사용한 경우, 상태가 Out-of-Compliance(미준수)로 표시됩니다. 라이선스 엔타이틀먼트는 특정 라이선스 예약에 적용되므로 반드시 작업을 수행해야 합니다.

제품 등록

등록 상태 및 인증 코드가 management center에 마지막으로 설치되거나 갱신된 날짜를 나타냅니다.

내보내기 제어 기능

management center에 대해 내보내기 제어 기능을 활성화했는지 여부를 나타냅니다.

내보내기 제어 기능에 대한 자세한 내용은 내보내기 제어 기능 라이선싱, 11 페이지을 참조하십시오.

제품 인스턴스

management center의 UUID(Universally Unique Identifier). 이 값은 Smart Software Manager에서 디바이스를 식별합니다.

확인 코드

Confirmation Code(확인 코드)는 특정 라이선스를 업데이트 또는 비활성화하고 반환하는 경우 필요합니다.

Assigned Licenses(할당된 라이선스) 탭

각 디바이스에 할당된 라이선스와 각각의 상태를 표시합니다.

Reserved Licenses(예약된 라이선스) 탭

사용된 라이선스 및 할당이 가능한 라이선스의 수와 라이선스 만료 날짜를 표시합니다.

특정 라이선스 예약 문제 해결

Smart Software Manager의 제품 인스턴스 목록에서 특정 **management center** 항목을 식별하려면 어떻게 해야 합니까**?**

Smart Software Manager의 Product Instances(제품 인스턴스) 페이지에서 한 테이블 열의 값을 기반으로 제품 인스턴스를 식별할 수 없는 경우, **FP** 유형의 각 일반 제품 인스턴스의 이름을 클릭하고 제품 인스턴스 상세정보 페이지를 확인해야 합니다. 이 페이지의 **UUID** 값은 하나의 관리 센터를 고유하게 식별합니다.

management center 웹 인터페이스에서 Management Center의 UUID는 **System(**시스템**) > Licenses(**라이선스**) > Specific Licenses(**특정 라이선스**)** 페이지에 표시된 **Product Instance(**제품 인스턴스**)** 값입니다.

Smart Software Manager에서 **License Reservation(**라이선스 예약**)** 버튼이 보이지 않는 경우

License Reservation(라이선스 예약**)** 버튼이 표시되지 않으면 어카운트가 특정 라이선스 예약에 대해 인증되지 않은 것입니다. Linux 셸에서 이미 Specific License Reservation(특정 라이선스 예약)을 활성화하고 요청 코드를 생성했다면, 다음을 수행합니다.

1. 관리 센터 웹 인터페이스에서 이미 **Request Code(**요청 코드**)**를 생성한 요청 코드를 취소합니다.
2. 섹션 특정 라이선스 예약 비활성화 및 반환, 44 페이지의 설명에 따라 관리 센터 Linux 셸에서 Specific License Reservation(특정 라이선스 예약)을 비활성화합니다.
3. 스마트 토큰을 사용하여 일반 모드에서 Smart Software Manager에 관리 센터를 등록합니다.
4. Cisco TAC에 문의하고 스마트 어카운트에 대한 Specific License(특정 라이선스)를 활성화합니다.

라이선스 프로세스 중간에 중단된 경우 남은 부분을 어떻게 계속 진행할 수 있을까요**?**

Smart Software Manager에서 인증 코드를 생성은 했지만 아직 다운로드하지 않은 경우, Smart Software Manager에 있는 **Product Instance(**제품 인스턴스**)** 페이지로 이동하고 제품 인스턴스를 클릭한 후 **Download Reservation Authorization Code(**예약 인증 코드**)** 다운로드를 클릭합니다.

management center virtual에 디바이스를 등록할 수 없습니다**.**

스마트 어카운트에 등록하려는 디바이스에 대한 충분한 management center virtual 엔타이틀먼트가 있는지 확인한 후, 구축을 업데이트하여 필요한 엔타이틀먼트를 추가합니다.

특정 라이선스 예약 업데이트, 41 페이지의 내용을 참조하십시오.

Specific Licensing(특정 라이선싱**)**을 활성화했지만 **Smart License(**스마트 라이선스**)** 페이지가 보이지 않는 경우

이는 정상적인 동작입니다. Specific Licensing(특정 라이선싱)을 활성화하는 경우, Smart Licensing(스마트 라이선싱)이 비활성화됩니다. Specific License(특정 라이선스) 페이지를 사용하여 라이선싱 작업을 수행할 수 있습니다.

스마트 라이선싱을 사용하려는 경우, 특정 라이선스를 반환해야 합니다. 자세한 내용은 특정 라이선스 예약 비활성화 및 반환, 44 페이지를 참조하십시오.

management center virtual에서 **Specific License(**특정 라이선스**)** 페이지가 보이지 않는 경우

Specific License(특정 라이선스)를 활성화해야 Specific License(특정 라이선스) 페이지를 볼 수 있습니다. 자세한 내용은 특정 라이선싱 메뉴 옵션 활성화, 38 페이지를 참조하십시오.

Specific Licensing(특정 라이선싱**)**을 비활성화했지만 **Return Code(**반환 코드**)** 복사를 잊어버린 경우 어떻게 해야 합니까**?**

반환 코드는 management center virtual에 저장됩니다. Linux 셸에서 Specific License(특정 라이선스)를 다시 활성화하고(특정 라이선싱 메뉴 옵션 활성화, 38 페이지 참조), management center virtual 웹 인터페이스를 새로 고침해야 합니다. **Return Code(**반환 코드**)**가 표시됩니다.

레거시 Management Center PAK 기반 라이선스 구성

management center는 플랫폼 라이선스에 대해 스마트 라이선스 또는 레거시 PAK(제품 활성화 키) 라이선스를 지원합니다. 이 절차에서는 PAK 기반 라이선스를 적용하는 방법을 설명합니다.

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.

프로시저

단계 **1** 라이선스 키는 Smart Software Manager에서 management center를 고유하게 식별합니다. 관리 포트(eth0)의 MAC 주소와 제품 코드 (예를 들어, 66)의 구성 된는 management center; 예를 들어, 66:00:00:77:FF:CC:88 합니다.

a) 시스템 (⚙) > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.
b) **Add New License(**새 라이선스 추가**)**를 클릭합니다.
c) **Add Feature License(**기능 라이선스 추가**)** 대화상자 상단에 있는 **License Key(**라이선스 키**)** 필드 값을 참조하십시오.

단계 **2** 시스템 (⚙) > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.

단계 **3** **Add New License(**새 라이선스 추가**)**를 클릭합니다.

단계 **4** 해당하는 작업을 계속 진행합니다.

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

단계 **5** **Get License(**라이선스 가져오기**)**를 클릭하여 라이선스 등록 포털을 엽니다.

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

단계 **6** 라이선스 등록 포털: https://cisco.com/go/license에서 PAK로 라이선스를 생성합니다.

이 단계에는 구매 과정에서 받은 PAK 뿐만 아니라 management center에 대한 라이선스 키도 필요합니다.

이 포털을 사용에 관한 자세한 내용은 다음을 참조하십시오.

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

이러한 링크에 액세스하려면 계정 자격 증명이 필요합니다.

단계 **7** 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 **8** management center virtual 웹 인터페이스에서 **Add Feature License(**기능 라이선스 추가**)** 페이지로 돌아갑니다.

단계 **9** 라이선스 텍스트를 **License(**라이선스**)** 필드에 붙입니다.

단계 **10** **Verify License(**라이선스 확인**)**을 클릭합니다.

라이선스가 유효하지 않은 경우, 라이선스 텍스트를 제대로 복사했는지 확인합니다.

단계 **11** **Submit License(**라이선스 제출**)**을 클릭합니다.

라이선싱 관련 추가 정보

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

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

라이센스 내역

기능	버전	세부정보
스마트 라이선싱 표준화	7.3	management center GUI에서 다음 라이선스 이름을 변경했습니다. • 기본은 이제 필수입니다 • 위협은 이제 IPS입니다. • 악성코드는 이제 악성코드 방어입니다 • RA VPN/AnyConnect 라이선스가 이제 Cisco Secure Client임 • AnyConnect Plus는 이제 Secure Client Advantage입니다 • AnyConnect Apex는 이제 Secure Client Premier입니다 • AnyConnect Apex 및 Plus는 이제 Secure Client Premier 및 Advantage입니다 • AnyConnect VPN Only는 이제 Secure Client VPN Only입니다
통신 사업자 라이선스 지원	7.3	통신 사업자 라이선스는 Diameter, GTP/GPRS, SCTP 및 M3UA 프로토콜의 검사를 활성화합니다. 신규/수정된 화면: **System(**시스템**)** > **Smart Licenses(**스마트 라이선스**)**
threat defense virtual의 성능 계층 라이선싱	7.0	성능 계층 라이센싱은 배포 요구 사항에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공합니다. 라이선스 계층은 새 threat defense virtual 모델에 매핑됩니다.
Firepower 4100/9300의 threat defense에 대한 다중 인스턴스 기능 라이선스	6.3	이제 Firepower 4100/9300에서 다중 threat defense 컨테이너 인스턴스를 구축할 수 있습니다. 보안 모듈/엔진별 기능당 하나의 라이선스만 필요합니다. 기본 라이선스가 각 인스턴스에 자동으로 할당됩니다. 신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 지원되는 플랫폼: Firepower 4100/9300에서의 threat defense
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. 신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)** (이 옵션은 기본적으로 사용할 수 없습니다.) 지원되는 플랫폼: management center, threat defense
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. 지원되는 플랫폼: management center, threat defense