시스템 라이선싱

다음 주제에서는 threat defense 디바이스 라이선싱 방법을 설명합니다.

Firewall System 스마트 라이선싱

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.

Cisco Smart Software Manager

threat defense 디바이스 라이선스를 1개 이상 구매한 경우, Cisco Smart Software Manager(https://software.cisco.com/#SmartLicensing-Inventory)에서 라이선스를 관리할 수 있습니다. Cisco Smart Software Manager에서는 조직의 기본 어카운트를 생성할 수 있습니다.

기본적으로는 기본 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 어플라이언스를 관리할 수 있습니다.

라이선스 및 어플라이언스는 가상 어카운트별로 관리됩니다. 해당 가상 어카운트의 어플라이언스만 어카운트에 할당된 라이선스를 사용할 수 있습니다. 추가 라이선스가 필요할 경우 다른 가상 계정의 미사용 라이선스를 이전할 수 있습니다. 또한 가상 어카운트 간에 어플라이언스를 전송할 수도 있습니다.

Cisco Smart Software Manager를 사용하여 디바이스를 등록할 때는 Smart Software Manager에서 제품 인스턴스 등록 토큰을 생성한 다음 device manager에 입력합니다. 등록된 디바이스는 사용하는 토큰에 따라 가상 어카운트와 연결됩니다.

Cisco Smart Software Manager에 대한 자세한 내용은 Smart Software Manager 온라인 도움말을 참조하십시오.

License Authority와의 정기적인 통신

제품 인스턴스 등록 토큰을 사용하여 threat defense 디바이스를 등록하면 디바이스가 Cisco License Authority에 등록됩니다. License Authority에서는 디바이스와 License Authority의 통신을 위해 ID 인증서를 발급합니다. 이 인증서는 6개월마다 갱신되지만 1년간 유효합니다. ID 인증서가 만료되면(대개 9개월 후 또는 통신을 수행하지 않는 경우 1년 후) 디바이스는 등록 취소된 상태로 돌아가며 라이선스 기능의 사용이 일시 중단됩니다.

디바이스는 주기적으로 License Authority와 통신합니다. Cisco Smart Software Manager에 변경이 있는 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다. 또는 디바이스에서 예정대로 통신할 때까지 기다릴 수 있습니다. 일반 라이선스 통신은 12시간마다 이루어지지만, 유예 기간이 있으면 디바이스는 최대 90일간 콜 홈 없이 작동할 수 있습니다. 90일이 지나기 전에 License Authority에 접속해야 합니다.

스마트 라이선스 유형

다음 표에서는 threat defense 디바이스에 사용할 수 있는 라이선스에 관해 설명합니다.

threat defense 디바이스 구매 시 Base 라이선스가 자동으로 포함됩니다. 모든 추가 라이선스는 선택 사항입니다.

표 *1:* 스마트 라이선스 유형

라이선스	기간	부여된 기능
Base	영구	선택적 기간 라이선스가 적용되지 않는 모든 기능. Base 라이선스는 등록 시 어카운트에 자동으로 추가됩니다. 보안 방화벽 3100은 예외입니다. 방화벽을 구매하면 Base 라이선스를 받게 되며, 라이선스는 어카운트의 다른 라이선스처럼 관리됩니다. 예를 들어 등록할 때 라이선스가 올바른 가상 어카운트에 있는지 확인해야 합니다. 이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.
위협	기간 기준	다음 정책을 사용하는 데 필요합니다. • 침입 • 파일(악성코드도 필요함) • 보안 인텔리전스
악성코드	기간 기준	파일 정책(위협도 필요함).
URL	기간 기준	URL 정책 - 범주 및 평판 기반 URL 필터링 또는 DNS 조회 요청 필터링. 이 라이선스가 없어도 개별 URL에 대해 URL 필터링을 수행할 수 있습니다.
RA VPN: • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN Only	라이선스 유형에 따라 기간 기준 또는 영구	원격 액세스 VPN 컨피그레이션 기본 라이선스는 RA VPN 구성을 위한 내보내기 제어 기능을 허용해야 합니다. 디바이스를 등록할 때 내보내기 요구사항을 충족하는지를 선택합니다. device manager는 유효한 Secure Client 라이선스를 사용할 수 있습니다. 제공되는 기능은 라이선스 유형에 따라 달라지지 않습니다. 라이선스를 아직 구매하지 않은 경우에는 원격 액세스 VPN에 대한 라이선싱 요구 사항를 참조하십시오. *Cisco AnyConnect* 주문 가이드, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf도 참조하십시오.

Threat Defense Virtual 라이선싱

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 ***2:*** 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
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

Threat Defense Virtual 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.
- Base 라이선스는 구독 기반이며 성능 계층에 매핑됩니다. 가상 어카운트에는 위협, 악성코드 및 URL 필터링 라이선스는 물론 threat defense virtual 디바이스에 대한 Base 라이선스 자격이 있어야 합니다.
- 각 HA 피어는 하나의 자격을 사용하고, Base 라이선스를 포함하여 각 HA 피어의 자격이 일치해야 합니다.
- HA 쌍의 성능 계층 변경 사항을 기본 피어에 적용해야 합니다.
- 범용 PLR 라이선싱은 HA 쌍의 각 디바이스에 개별적으로 적용됩니다. 보조 디바이스는 기본 디바이스의 성능 계층을 자동으로 미러링하지 않습니다. 수동으로 업데이트해야 합니다.

내보내기 제어 설정이 암호화 기능에 미치는 영향

디바이스를 등록할 때 이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.

평가 모드는 내보내기와 호환되지 않는 계정을 사용하여 등록하는 것과 동일하게 처리됩니다. 즉, 평가 모드에서 실행할 때는 원격 액세스 VPN을 구성하거나 고급 암호화 알고리즘을 사용할 수 없습니다.

특히 DES 표준은 평가 또는 내보내기와 호환되지 않는 모드에서만 사용할 수 있습니다.

따라서 사이트 간 VPN과 같은 암호화된 기능을 구성하거나 고가용성 그룹에서 페일오버 연결을 암호화하는 경우 내보내기 호환 계정에 등록한 후 연결 문제가 발생할 수 있습니다. 기능이 평가 모드에서 DES를 사용 중인 경우 계정을 등록한 후에 해당 구성이 중단됩니다.

암호화 관련 문제를 방지하려면 다음 권장 사항을 고려하십시오.

- 디바이스를 등록할 때까지 사이트 간 VPN 및 암호화된 페일오버 연결과 같은 암호화된 기능을 구성하지 마십시오.
- 내보내기 호환 계정을 사용하여 디바이스를 등록한 후 평가 모드에서 구성한 모든 암호화된 기능을 편집하고 더 안전한 암호화 알고리즘을 선택합니다. 각 기능을 테스트하고 확인하여 기능이 올바르게 작동하는지 확인합니다.

참고 평가 모드에서 HA 페일오버 암호화를 구성한 경우, 더 강력한 암호화를 사용하려면 HA 그룹의 두 디바이스를 모두 재부팅해야 합니다. 두 디바이스가 모두 활성 유닛으로 간주되는 스플릿 브레인 상황을 방지하려면 먼저 암호화를 제거하는 것이 좋습니다.

만료되거나 비활성화된 선택 가능한 라이선스의 영향

다음의 선택 가능한 라이선스 중 하나가 만료된 경우 라이선스가 필요한 기능을 계속 사용할 수 있습니다. 그러나 라이선스는 컴플라이언스 상태가 아닌 것으로 표시되며, 라이선스를 컴플라이언스 상태로 다시 설정하려면 라이선스를 구매하여 어카운트에 추가해야 합니다.

선택 가능한 라이선스를 비활성화하면 시스템은 다음과 같이 대응합니다.

- 악성코드 - 시스템에서 Secure Malware Analytics 클라우드에 대한 쿼리를 중단하며 Secure Malware Analytics 클라우드에서 전송한 회귀적 이벤트 확인도 중지합니다. 파일 정책이 포함된 경우, 기존 액세스 제어 정책은 재구축할 수 없습니다. 악성코드 라이선스가 비활성화된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 이 기간이 만료되고 나면 시스템은 해당 파일에 사용할 수 없음 상태를 할당합니다.
- 위협 - 시스템이 더 이상 침입 또는 파일 정책을 적용하지 않습니다. 보안 인텔리전스 정책의 경우 시스템은 더 이상 정책을 적용하지 않고 피드 업데이트 다운로드를 중지합니다. 라이선스가 필요한 기존 정책은 재구축할 수 없습니다.
- URL - URL 범주 조건이 포함된 액세스 제어 규칙의 URL 또는 DNS 조회 요청 필터링이 즉시 중지되며 시스템이 URL 데이터에 대한 업데이트를 더 이상 다운로드하지 않습니다. 범주 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.
- RA VPN - 원격 액세스 VPN 컨피그레이션을 수정할 수는 없지만, 제거할 수는 있습니다. 사용자는 RA VPN 컨피그레이션을 사용하여 계속 연결할 수 있습니다. 그러나 디바이스 등록을 변경하여 시스템이 더 이상 내보내기 방식을 준수하지 않는 경우에는 원격 액세스 VPN 컨피그레이션이 즉시 중지되며 원격 사용자가 VPN을 통해 연결할 수 없습니다.

스마트 라이선스 관리

스마트 라이선스 페이지를 사용하여 시스템의 현재 라이선스 상태를 확인합니다. 시스템에 라이선스가 있어야 합니다.

이 페이지에는 90일 평가 라이선스를 사용 중인지 아니면 Cisco Smart Software Manager에 등록되었는지가 표시됩니다. 등록한 경우 Cisco Smart Software Manager에 대한 연결 상태와 각 라이선스 유형의 상태를 확인할 수 있습니다.

사용 권한 부여에서 스마트 라이선스 에이전트 상태를 식별합니다.

- 권한 있음("연결됨", "충분한 라이선스") - 디바이스가 License Authority에 연결하여 정상적으로 등록되었으며, 어플라이언스에 대한 라이선스 자격이 부여되었습니다. 디바이스는 현재 컴플라이언스 상태입니다.

- 규정 미준수 - 디바이스에 대해 사용 가능한 라이선스 자격이 없습니다. 라이선스 기능은 계속 작동합니다. 그러나 추가 자격을 구매하거나 확보해야 디바이스의 컴플라이언스 상태가 될 수 있습니다.
- 권한 부여 만료됨 - 디바이스가 90일 이상 Licensing Authority와 통신하지 않았습니다. 라이선스 기능은 계속 작동합니다. 이 상태에서 스마트 라이선스 에이전트는 권한 부여 요청을 다시 시도합니다. 다시 시도가 성공하면 에이전트는 규정 미준수 또는 권한 있음 상태로 설정되며 새 권한 부여 기간이 시작됩니다. 이 경우 디바이스를 수동으로 동기화해 보십시오.

참고 스마트 라이선스 상태 옆의 **i** 버튼을 클릭하여 가상 어카운트와 내보내기 제어 기능을 확인하고 Cisco Smart Software Manager를 여는 링크를 확인합니다. 내보내기 제어 기능은 국가별 보안, 해외 정책 및 테러 방지법과 규정이 적용되는 소프트웨어를 제어합니다.

다음 절차에서는 시스템의 라이선스를 관리하는 방법을 간략하게 설명합니다.

시작하기 전에

시스템에 인터넷에 대한 경로가 없는 경우 스마트 라이선싱을 사용할 수 없습니다. 그 대신 영구 라이선스 예약(PLR) 모드로 전환합니다. 자세한 내용은 에어 갭(Air-Gapped) 네트워크에서 영구 라이선스 적용, 12 페이지를 참조하십시오.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 디바이스를 등록합니다.

Cisco Smart Software Manager에 등록해야 선택 가능한 라이선스를 할당할 수 있습니다. 평가 기간이 종료되기 전에 등록하십시오.

디바이스 등록, 8 페이지의 내용을 참조하십시오.

참고 등록 시 Cisco에 사용량 데이터를 보낼지를 선택하십시오. 기어 아이콘 옆에 있는 **Go To Cisco Success Network(Cisco Success Network**로 이동**)** 링크를 클릭하여 선택을 변경할 수 있습니다.

단계 **3** 선택 가능한 기능 라이선스를 요청하고 관리합니다.

라이선스를 통해 제어되는 기능을 사용하려면 선택 가능한 라이선스를 등록해야 합니다. 선택 가능한 라이선스 활성화 또는 비활성화, 10 페이지의 내용을 참조하십시오.

단계 **4** 시스템 라이선싱을 유지합니다.

다음과 같은 작업을 수행할 수 있습니다.

- Cisco Smart Software Manager와 동기화, 11 페이지

• 디바이스 등록 취소, 11 페이지

디바이스 등록

threat defense 디바이스 구매 시 Base 라이선스가 자동으로 포함됩니다. Base 라이선스는 선택 가능한 라이선스에 포함되지 않는 모든 기능을 포함합니다. 영구 라이선스입니다.

초기 시스템 설정 중에 Cisco Smart Software Manager에 디바이스를 등록하라는 메시지가 표시됩니다. 90일 평가 라이선스를 대신 선택한 경우에는 평가 기간이 종료되기 전에 디바이스를 등록해야 합니다.

디바이스를 등록할 때는 가상 어카운트가 디바이스에 라이선스를 할당합니다. 디바이스를 등록하면 활성화한 선택 가능한 라이선스도 등록됩니다.

시작하기 전에

디바이스를 등록하면 해당 디바이스만 등록됩니다. 디바이스가 고가용성을 제공하도록 구성된 경우에는 고가용성 쌍의 다른 유닛에 로그인하여 해당 유닛을 등록해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Register Device(**디바이스 등록**)**를 클릭하고 지침을 따릅니다.

a) 링크를 클릭하여 Cisco Smart Software Manager를 열고 어카운트에 로그인하거나 필요한 경우 새 어카운트를 생성합니다.

b) 새 토큰을 생성합니다.

토큰을 생성할 때는 토큰을 사용할 수 있는 유효 기간을 지정합니다. 권장 만료 기간은 30일입니다. 이 기간은 토큰 자체의 만료 날짜를 정의하며 토큰을 사용하여 등록하는 디바이스에는 영향을 주지 않습니다. 토큰이 사용하기 전에 만료되는 경우 새 토큰을 생성하면 됩니다.

이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.

c) 토큰을 복사하여 스마트 라이선스 등록 대화 상자의 수정 상자에 붙여넣습니다.

d) (**Threat Defense Virtual** 전용) threat defense virtual 디바이스에 대한 성능 계층을 선택하거나 기본 선택을 유지합니다.

성능 계층을 선택하지 않은 경우 threat defense virtual 디바이스는 4코어/8GB의 기본 설정으로 레거시 모드에서 실행됩니다. 자세한 내용은 Threat Defense Virtual 성능 계층 변경, 9 페이지의 내용을 참조하십시오.

e) Cisco Cloud Services 등록을 위한 지역을 선택합니다.

등록 후 이 지역을 변경해야 하는 경우, 디바이스를 등록 취소한 다음 다시 등록하고 새 지역을 선택해야 합니다.

f) 사용량 데이터를 Cisco에 보낼지를 결정합니다.

Cisco Success Network 단계에 나와 있는 정보를 읽고 **Sample Data(**샘플 데이터**)** 링크를 클릭하여 수집된 실제 데이터를 확인한 다음 **Enable Cisco Success Network(Cisco Success Network** 활성화**)** 옵션을 선택한 상태로 둘지를 결정합니다.

g) **Register Device(**디바이스 등록**)**를 클릭합니다.

Threat Defense Virtual 성능 계층 변경

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. Threat Defense Virtual 스마트 라이선싱의 성능 계층, 4 페이지의 내용을 참조하십시오.

threat defense virtual의 버전 7.0 이상으로 업그레이드 시 디바이스는 "FTDv 변수" 계층으로 자동 이동하고 자격 레벨을 선택할 때까지 계층 없는 자격을 계속 사용하게 됩니다.

참고 처리량 또는 RA VPN 요구 사항에 따라 구축 요건에 맞춰 성능 계층을 변경할 수 있습니다. threat defense virtual의 경우 조정 가능한 코어 및 메모리 리소스를 사용하여 구축합니다. 선택한 성능 계층이 디바이스 사양을 초과해서는 안 됩니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Performance Tier(**성능 계층**)** 드롭다운 목록에서 원하는 옵션을 선택합니다.

- FTDv5(4코어/8GB)
- FTDv10(8코어/8GB)
- FTDv20(8코어/8GB)
- FTDv30(8코어/16GB)
- FTDv50(12코어/24GB)
- FTDv100(16코어/24GB)

참고 시스템은 현재 디바이스 사양에 따라 최적의 계층을 강조 표시합니다.

단계 **3** 선택 및 디바이스 사양을 검토합니다.

참고 threat defense virtual VM을 설정할 때 지원되는 최대 코어 수(vCPU)는 12개(VMware 및 KVM의 FTDv100의 경우 16개)입니다. 지원되는 최대 메모리는 24GB RAM입니다. 선택한 성능 계층이 디바이스 사양을 초과해서는 안 됩니다.

단계 **4** **YES(**예**)**를 클릭하여 성능 계층을 변경합니다.

선택 가능한 라이선스 활성화 또는 비활성화

선택 가능한 라이선스는 활성화(등록)하거나 비활성화(해제)할 수 있습니다. 라이선스를 통해 제어되는 기능을 사용하려면 라이선스를 활성화해야 합니다.

선택적 기간 라이선스가 적용되는 기능을 더 이상 사용하지 않으려는 경우 라이선스를 비활성화할 수 있습니다. 비활성화하는 라이선스는 Cisco Smart Software Manager 어카운트에서 해제되므로 다른 디바이스에 적용할 수 있습니다.

평가 모드에서 실행 중인 경우 이러한 라이선스의 평가 버전을 활성화할 수도 있습니다. 평가 모드에서 라이선스는 디바이스를 등록할 때까지 Cisco Smart Software Manager에 등록되지 않습니다. 그러나 평가 모드에서는 RA VPN 라이선스를 활성화할 수 없습니다.

시작하기 전에

라이선스를 비활성화하기 전에 해당 라이선스를 사용하고 있지 않은지 확인합니다. 라이선스가 필요한 정책은 재작성하거나 삭제합니다.

고가용성 컨피그레이션에서 작동 중인 유닛의 경우 액티브 유닛에서만 라이선스를 활성화하거나 비활성화합니다. 다음번 컨피그레이션 구축 시에 스탠바이 유닛이 필요한 라이선스를 요청하거나 해제할 때 변경 사항이 스탠바이 유닛에 반영됩니다. 라이선스를 활성화하는 경우에는 Cisco Smart Software Manager 어카운트에 사용 가능한 라이선스가 충분한지 확인해야 합니다. 그렇지 않으면 각 유닛의 컴플라이언스 상태가 서로 다를 수 있습니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 선택 가능한 각 라이선스에 대해 **Enable(**활성화**)/Disable(**비활성화**)** 컨트롤을 필요한 대로 클릭합니다.

- **Enable(**활성화**)** - Cisco Smart Software Manager 어카운트에 라이선스를 등록하고 제어되는 기능을 활성화합니다. 이제 라이선스를 통해 제어되는 정책을 구성하고 구축할 수 있습니다.
- **Disable(**비활성화**)** - Cisco Smart Software Manager 어카운트에서 라이선스를 등록 취소하고 제어되는 기능을 비활성화합니다. 이렇게 하면 새 정책에서 기능을 구성할 수 없으며 해당 기능을 사용하는 정책을 구축할 수도 없습니다.

단계 **3** **RA VPN** 라이선스를 활성화한 경우 어카운트에서 사용 가능한 라이선스의 유형을 선택합니다.

모든 AnyConnect 라이선스(**Plus**, **Apex** 또는 **VPN** 전용)를 사용할 수 있습니다. Plus 라이선스와 Apex 라이선스가 둘 다 있으며 모두 사용하려는 경우 **Plus** 및 **Apex**를 선택할 수 있습니다.

Cisco Smart Software Manager와 동기화

시스템은 Cisco Smart Software Manager와 주기적으로 라이선스 정보를 동기화합니다. 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 어플라이언스는 최대 90일간 콜 홈 없이 작동할 수 있습니다.

그러나 Cisco Smart Software Manager에서 변경을 수행할 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다.

동기화 시에는 라이선스의 현재 상태를 가져오며 권한 부여와 ID 인증서가 갱신됩니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 기어 드롭다운 목록에서 **Resync Connection(**연결 재동기화**)**를 선택합니다.

디바이스 등록 취소

더 이상 디바이스를 사용하지 않으려는 경우 Cisco Smart Software Manager에서 디바이스를 등록 취소할 수 있습니다. 등록을 취소하면 디바이스에 연결된 Base 라이선스 및 선택 가능한 모든 라이선스가 가상 어카운트에서 해제됩니다. 선택 가능한 라이선스는 다른 디바이스에 할당할 수 있습니다. 또한 디바이스는 클라우드 및 클라우드 서비스에서도 등록이 취소됩니다.

디바이스를 등록 취소한 후에도 디바이스의 현재 컨피그레이션 및 정책은 계속 원래대로 작동하지만 변경을 수행하거나 변경 사항을 구축할 수는 없습니다.

시작하기 전에

디바이스 등록을 취소하면 해당 디바이스만 등록 취소됩니다. 디바이스가 고가용성을 제공하도록 구성된 경우에는 고가용성 쌍의 다른 유닛에 로그인하여 해당 유닛을 등록 취소해야 합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 기어 드롭다운 목록에서 **Unregister Device(**디바이스 등록 취소**)**를 선택합니다.

단계 **3** 경고를 확인한 후에 디바이스를 등록 취소하려면 **Unregister(**등록 취소**)**를 클릭합니다.

에어 갭(Air-Gapped) 네트워크에서 영구 라이선스 적용

에어 갭(air-gapped) 네트워크는 인터넷에 대한 경로가 없는 네트워크입니다. 이러한 네트워크는 외부 입력 및 공격의 가능성을 방지하려는 상위 보안 네트워크입니다. 인터넷에 대한 경로가 없으므로 Cisco Smart Software Manager를 사용하여 디바이스를 직접 등록할 수 없습니다. 대신 영구 라이선스 예약(PLR) 모드를 사용하여 디바이스에 적용할 수 있는 라이선스를 얻을 수 있습니다.

PLR 모드를 사용해야 하는 경우에는 다음 사항에 유의하십시오.

- 인터넷에 액세스해야 하는 기능(예: 파일 정책, URL 조회 또는 공용 웹 사이트 상황별 크로스 실행)이 작동하지 않습니다.
- Web Analytics 및 Cisco Success Network를 활성화한다 해도, 인터넷 액세스가 없기 때문에 연결된 데이터를 Cisco에서 수집하지 않습니다.
- 지리위치 데이터베이스, 침입 규칙, VDB(Vulnerability Database)에 업데이트를 수동으로 업로드해야 합니다. 예를 들어 플래시 드라이브에 업데이트를 다운로드한 다음, 드라이브를 보안 구축 환경으로 가져와 보안 워크스테이션에서 이를 업로드할 수 있습니다.

참고 Cisco Smart Software Manager는 디바이스의 일련 번호를 사용하여 영구 라이선스를 할당합니다. 디바이스의 등록을 취소해야 하는 경우 일반 등록 취소 또는 취소 프로세스에서 라이선스 할당을 제거하지 못하면 Cisco 기술 지원에 문의하여 Cisco Smart Software Manager에서 등록을 제거해야 합니다. 디바이스를 다시 이미징하면 라이선스 등록이 제거되지 않습니다.

다음 주제에서는 다양한 유형의 영구 라이선스에 대해 자세히 설명하고, 이러한 라이선스를 적용하는 방법, 그리고 등록을 취소하거나 디바이스 등록을 해제하는 방법에 대해 자세히 설명합니다.

범용 대 특정 영구 라이선스 예약

영구 라이선스 예약은 별도의 두 가지 유형이 있습니다.

- 범용 영구 라이선스 예약(범용 PLR, 즉 UPLR) — 범용 영구 라이선스를 사용하면 모든 옵션 라이선스를 포함하여, 지원되는 방화벽 제품을 영구적으로 무제한 사용할 수 있습니다. 범용 영구 라이선스를 구매한 후 적용하면, 일반적으로 시간을 기반으로 적용되는 기능 라이선스를 영구적으로 적용할 수 있습니다. 그러나 교체 라이선스는 스마트 라이선스 어카운트에서 만료되므로 계속 구매해야 합니다. ISA 3000은 승인된 고객에 대해 범용 PLR을 지원합니다.
- 특정 영구 라이선스 예약(특정 PLR, 즉 SPLR) — 특정 영구 라이선스 예약에는 표준 스마트 라이선싱과 동일한 번호 및 라이선스 유형이 필요합니다. 이 라이선스를 취득하면 기본 라이선스 외에 원하는 선택적인 기능 라이선스를 선택할 수 있습니다. 라이선스가 만료될 때 해당 라이선스를 주기적으로 업데이트해야 합니다.

Device Manager은 범용 PLR만 지원합니다. device manager를 사용하여 특정 PLR을 적용할 수 없습니다.

Cisco 담당자와 협력하여 CSSM(Cisco Smart Software Manager) 어카운트에서 범용 영구 라이선스 예약(PLR) 모드를 활성화해야 합니다.

스마트 어카운트가 범용 라이선스를 제공할 수 있는지 확인

영구 라이선스를 획득하고 적용할 수 있는지 확인하려면 CSSM 어카운트에 로그인하고 **Smart Software Licensing(**스마트 소프트웨어 라이선싱**)** > **Inventory(**인벤토리**)** 페이지로 이동한 다음, **Licenses(**라이선스**)** 탭을 클릭합니다. **License Reservation(**라이선스 예약**)** 버튼이 표시되면 영구 라이선스 예약을 받을 수 있는 권한이 있는 것입니다.

그러나 이 버튼을 누르면 범용 및 특정 영구 라이선스 두 가지 모두에 대해 작동하는 마법사가 시작됩니다.

또한, 사용 가능한 라이선스 목록을 검토하여 디바이스에 대한 범용 라이선스가 있는지 확인해야 합니다. 이 라이선스는 **License Reservation(**라이선스 예약**)** 버튼을 사용하여 실행된 마법사의 2단계에서 선택 가능한 항목으로 표시됩니다.

License Reservation(라이선스 예약**)** 버튼이 표시되고 범용 라이선스를 받을 수 있는 경우, 영구 라이선스를 사용하도록 시스템을 전환하는 작업을 계속 진행할 수 있습니다. 이 버튼이 표시되지 않거나 특정 라이선스만 예약할 수 있는 경우, Cisco 담당자에게 전화하여 해당 어카운트에 대해 범용 PLR 모드가 활성화되도록 요청하십시오.

PLR 모드로 전환하고 범용 라이선스 적용

스마트 어카운트가 범용 라이선스를 제공할 수 있는지 확인, 13 페이지에 설명된 것처럼 영구 라이선스를 받을 수 있는지 확인하고, 필요한 범용 라이선스를 구매한 후에는 영구 라이선스 예약(PLR) 모드로 전환하고 라이선스를 적용할 수 있습니다.

⚠

주의 현재 평가 모드에 있는 경우 PLR 모드로 전환하면 다시 평가 모드로 전환할 수 없습니다.

시작하기 전에

디바이스가 고가용성으로 구성된 경우, HA 그룹의 두 디바이스에 대해 이 작업을 개별적으로 완료해야 합니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 스마트 라이선싱을 사용하여 디바이스를 이미 등록한 경우, 톱니바퀴 모양 드롭다운 목록에서 **Unregister Device(**디바이스 등록 해제**)**를 선택한 다음 등록 해제를 확인합니다. 계속 진행하려면 우선 등록 해제 작업이 완료될 때까지 기다려야 합니다.

단계 **3** 톱니바퀴 모양 드롭다운 목록에서 **Switch to Universal PLR(**범용 **PLR**로 전환**)**을 선택하여 범용 영구 라이선스 예약(PLR) 모드로 전환합니다.

경고 메시지를 읽고 **Yes(**예**)**를 클릭하여 전환을 확인합니다.

시스템이 PLR 모드로 변환된 다음 PLR 등록 프로세스가 시작됩니다.

단계 **4** PLR 등록을 완료합니다.

a) Universal Permanent License Reservation(범용 영구 라이선스 예약) 대화 상자가 열리면 첫 번째 단계에 사용자에게 필요한 요청 코드가 포함되어 있습니다. **Save As TXT(TXT**로 저장**)**를 클릭하여 이 코드를 텍스트 파일로 저장하거나, **Print(**인쇄**)**를 클릭하여 인쇄할 수 있습니다. 문자열을 강조 표시하고 Ctrl+C를 눌러 클립보드에 복사할 수도 있습니다.

모드 전환 후 프로세스를 취소한 경우, Licensing(라이선싱) 페이지의 **Continue Reservation(**예약 계속 진행**)** 버튼을 클릭하여 이 단계에서 다시 시작할 수 있습니다.

b) CSSM 어카운트에 로그인하고 **Smart Software Licensing(**스마트 소프트웨어 라이선싱**)** > **Inventory(**인벤토리**)** 페이지로 이동한 다음, **Licenses(**라이선스**)** 탭을 클릭합니다.

c) **License Reservation(**라이선스 예약**)** 버튼을 클릭하고 마법사의 지침을 따릅니다. 생성한 요청 코드를 입력하라는 메시지가 표시되며, 이렇게 하면 인증 코드가 제공됩니다.

마법사에는 다음 단계가 포함됩니다.

1. 라이선스 요청 코드를 입력하거나, 코드가 포함된 텍스트 파일을 업로드하고 **Next(**다음**)**를 클릭합니다.
2. 2단계에서는 라이선스를 부여하려는 시스템에 대한 제품 세부 정보, 그리고 사용 가능한 라이선스 목록이 표시됩니다. FDM에서 관리되는 threat defense 디바이스에 대한 범용 라이선스를 선택하고 **Next(**다음**)**를 클릭합니다.
3. 3단계에서는 올바른 라이선스를 선택했는지 확인했는지 확인하고 **Generate Authorization Code(**인증 코드 생성**)**를 클릭합니다.
4. 4단계에서는 인증 코드가 표시됩니다. **Download as File(**파일로 다운로드**)** 또는 **Copy to Clipboard(**클립보드에 복사**)**를 클릭하여 코드를 저장합니다.
5. **Close(**닫기**)**를 클릭하여 마법사를 종료합니다.

d) device manager으로 다시 돌아간 후, 인증 코드를 적절한 필드에 붙여넣습니다.

범용 라이선스에 대한 유효한 인증 코드 형식은 XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXX입니다. 여기서 X는 영숫자 문자입니다. 인증 코드가 XML 파일인 경우, 특정 라이선스를 보유한 것이며 이 시스템에서는 사용할 수 없습니다. PLR 등록 취소, 15 페이지에 설명된 대로 등록을 취소하여 CSSM에서 예약된 라이선스를 해제하십시오. 그런 다음, Cisco 담당자와 협력하여 스마트 어카운트를 범용 PLR로 변환하십시오.

e) **Register(**등록**)**를 클릭합니다.

시스템에서 등록 프로세스를 시작합니다. Licensing(라이선싱) 페이지를 새로 고침하여 등록 상태를 확인합니다.

단계 **5** 필요에 따라 선택적인 기능 라이선스를 활성화합니다.

범용 라이선스는 Base 라이선스에 대해서만 디바이스를 등록합니다. 이제 필요한 각 기능 라이선스에 대해 **Enable(**활성화**)**을 클릭할 수 있습니다.

PLR 등록 취소

범용 영구 라이선스 예약(PLR) 요청이 완료되기 전에 이를 취소할 수 있습니다. 예를 들어 PLR 등록 프로세스를 시작한 후 Smart Software Manager 어카운트가 PLR에 설정되지 않은 것을 확인한 경우, PLR 모드에 대한 인증을 받고 스마트 라이선스 어카운트가 올바르게 설정될 때까지 이러한 등록 프로세스를 취소할 수 있습니다.

PLR 등록 프로세스를 완료한 경우에는 이를 취소할 수 없습니다. 대신 PLR 모드에서 디바이스 등록 해제, 16 페이지 섹션을 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 톱니바퀴 모양 드롭다운 목록에서 **Cancel PLR(PLR** 취소**)**을 선택하여 취소 프로세스를 시작합니다.

단계 **3** 상황에 맞는 옵션을 선택합니다.

- **I have a license in CSSM(CSSM**에 라이선스가 있습니다**.)** — CSSM(Cisco Smart Software Manager)에서 라이선스 등록 마법사를 완료했고 인증 코드를 받은 경우 이 옵션을 사용합니다. 이 단계에서 CSSM에 예약된 라이선스가 있다면 해당 라이선스를 해제해야 합니다.
- **I do not have a license in CSSM(CSSM**에 라이선스가 없습니다**.)** — 인증 코드를 받은 시점에 CSSM 마법사를 완료하지 않은 경우 이 옵션을 사용합니다. 예를 들어, device manager에서 PLR 등록을 시작한 후 스마트 어카운트에서 **License Reservation(**라이선스 예약**)** 버튼이 제공되지 않는다는 걸 확인한 경우 이 옵션을 사용합니다.

단계 **4** (**I have a license in CSSM(CSSM**에 라이선스가 있습니다**.)**을 선택한 경우.) CSSM에서 해제 코드를 받아 라이선스가 더 이상 사용 중으로 표시되지 않도록 해야 합니다. 그러지 않으면 다른 디바이스에서 해당 라이선스를 사용할 수 없습니다.

a) 등록 시 CSSM에서 받은 인증 코드를 취소 대화 상자에 붙여넣고 **Generate Release Code(**해제 코드 생성**)**를 클릭합니다.

b) **Release License Code(**라이선스 코드 해제**)** 필드에 코드가 있을 경우, **Save As TXT(TXT**로 저장**)**를 클릭하여 이를 텍스트 파일로 저장하거나 **Print(**인쇄**)**를 클릭하여 인쇄합니다. 코드를 선택하고 Ctrl+C를 눌러 클립보드에 복사할 수도 있습니다.

c) CSSM의 **Smart Software Licensing(**스마트 소프트웨어 라이선싱**)** > **Inventory(**인벤토리**)** 페이지에서 디바이스(디바이스 일련 번호가 이름임)를 찾고, **Action(**작업**)** > **Remove(**제거**)**를 클릭한 후 해제 코드를 입력합니다.

CSSM에 제품이 제거되었다는 메시지가 표시될 때까지 기다립니다.

단계 **5** **OK(**확인**)**를 클릭하여 취소 프로세스를 완료합니다.

시스템이 스마트 라이선스 모드로 돌아갑니다. 그러나 디바이스는 등록 해제되어 평가 모드를 다시 시작할 수 없습니다. 이 단계에서는 스마트 라이선스를 사용하여 디바이스를 등록하거나, PLR 모드로 다시 전환한 후 다시 등록하여 사용해야 합니다.

PLR 모드에서 디바이스 등록 해제

예를 들어 디바이스를 디커미션하거나 별도로 라이선스를 부여하는 다른 시설로 디바이스를 옮기는 경우처럼 디바이스에 라이선스가 더 이상 필요하지 않은 경우, 디바이스를 등록 해제할 수 있습니다.

디바이스 등록을 해제하면 라이선스가 사용되지 않은 상태로 돌아갑니다. 디바이스를 등록 해제하지 않을 경우 라이선스가 계속 사용 중으로 표시되며 이를 다른 용도로 사용할 수 없습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 톱니바퀴 모양 드롭다운 목록에서 **Unregister Universal PLR(**범용 **PLR** 등록 해제**)**을 선택한 후 경고 메시지를 읽고 **Yes(**예**)**를 클릭하여 프로세스를 시작합니다.

단계 **3** Unregister Universal Permanent License Reservation(범용 영구 라이선스 예약 등록 해제) 대화 상자가 열리면, **Release License Code(**라이선스 코드 해제**)** 필드에 CSSM 어카운트에 현재 할당된 라이선스를 해제해야 할 코드가 채워져 있습니다. **Save as TXT(TXT**로 저장**)** 또는 **Print(**인쇄**)**를 클릭하여 이 코드의 복사본을 보관합니다. 코드를 선택하고 Ctrl+C를 사용하여 클립보드에 복사할 수도 있습니다.

단계 **4** CSSM 어카운트로 이동하여 **Smart Software Licensing(**스마트 소프트웨어 라이선싱**)** > **Inventory(**인벤토리**)** 페이지에서 디바이스(디바이스 일련 번호가 이름임)를 찾고, **Action(**작업**)** > **Remove(**제거**)**를 클릭한 후 해제 코드를 입력합니다.

CSSM에 제품이 제거되었다는 메시지가 표시될 때까지 기다립니다.

단계 **5** device manager으로 돌아가 Unregister Device(디바이스 등록 해제)에서 **Unregister(**등록 해제**)**를 클릭합니다.

이렇게 하면 프로세스가 완료됩니다. 이제 CSSM의 라이선스를 다른 디바이스에 자유롭게 할당할 수 있으며, threat defense 디바이스에는 라이선스가 없습니다.