ASA의 라이선스 관리

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.

참고 이 섹션은 Firepower 4100/9300 섀시의 ASA 논리적 디바이스에만 적용됩니다. FTD 논리적 디바이스의 라이선싱에 대한 자세한 내용은 FMC 컨피그레이션 가이드를 참조하십시오.

Smart Software Licensing 정보

이 섹션에서는 Smart Software Licensing이 적용되는 방법에 관해 설명합니다.

참고 이 섹션은 Firepower 4100/9300 섀시의 ASA 논리적 디바이스에만 적용됩니다. FTD 논리적 디바이스의 라이선싱에 대한 자세한 내용은 FMC 컨피그레이션 가이드를 참조하십시오.

ASA의 Smart Software Licensing

Firepower 4100/9300 섀시의 ASA 애플리케이션의 경우, Smart Software Licensing 구성은 Firepower 4100/9300 섀시 수퍼바이저와 애플리케이션으로 나뉩니다.

- Firepower 4100/9300 섀시— 수퍼바이저에 모든 Smart Software Licensing 인프라를 구성하며 여기에는 License Authority와 통신하는 데 필요한 파라미터가 포함됩니다. Firepower 4100/9300 섀시 자체는 작동하기 위한 라이선스가 필요하지 않습니다.

참고 섀시 간 클러스터링에서는 클러스터의 각 섀시에서 동일한 Smart Licensing 방법을 활성화해야 합니다.

- ASA 애플리케이션 — 애플리케이션의 모든 라이선스 엔타이틀먼트를 구성합니다.

참고 Cisco 전송 게이트웨이는 Firepower 4100/9300 보안 어플라이언스에서 지원되지 않습니다.

Smart Software Manager 및 어카운트

디바이스 라이선스를 1개 이상 구매한 경우, Cisco Smart Software Manager에서 라이선스를 관리할 수 있습니다.

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

Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

참고 아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

기본적으로 마스터 계정의 기본 가상 계정에 라이선스가 지정됩니다. 계정 관리자는 선택적으로 추가 가상 계정을 만들 수 있습니다. 이를테면 지역, 부서, 자회사를 위한 계정을 만들 수 있습니다. 여러 가상 계정이 있으면 많은 수의 라이선스 및 디바이스를 더 편리하게 관리할 수 있습니다.

오프라인 관리

디바이스에서 인터넷에 액세스할 수 없으며 License Authority에 등록할 수 없는 경우, 오프라인 라이선싱을 구성할 수 있습니다.

영구 라이선스 예약

보안상의 이유로 디바이스에서 인터넷에 액세스할 수 없는 경우 선택적으로 각 ASA에 대한 영구 라이선스를 요청할 수 있습니다. 영구 라이선스 사용 시에는 License Authority에 주기적으로 액세스할 필요가 없습니다. PAK 라이선스와 마찬가지로 라이선스를 구매한 후 ASA용 라이선스 키를 설치하면 됩니다. 그러나 PAK 라이선스와는 달리 Smart Software Manager를 사용하여 라이선스를 받고 관리합니다. 일반 Smart Licensing 모드와 영구 라이선스 예약 모드 간을 쉽게 전환할 수 있습니다.

Carrier 라이선스 및 최대 보안 컨텍스트를 갖춘 표준 Tier 등 모든 기능을 활성화하는 라이선스를 얻을 수 있습니다. 이 라이선스는 Firepower 4100/9300 섀시에서 관리되지만 ASA에서 엔타이틀먼트 사용을 허용하도록 ASA 구성의 엔타이틀먼트도 요청해야 합니다.

Satellite 서버

보안상의 이유로 디바이스가 인터넷에 액세스할 수 없는 경우 선택적으로 로컬 Smart Software Manager Satellite 서버를 VM(가상 머신)으로 설치할 수 있습니다. Smart Software Manager 기능의 하위 집합을 제공하는 이 Satellite을 통해 모든 로컬 디바이스에 필수 라이선싱 서비스를 제공할 수 있습니다. Satellite는 라이선스 사용량 동기화를 위해 메인 License Authority에 주기적으로 연결하기만 하면 됩니다. 일정에 따라 동기화하거나 수동으로 동기화할 수 있습니다.

Satellite 애플리케이션을 다운로드하고 구축하면 인터넷을 사용하여 Cisco SSM에 데이터를 전송하지 않고 다음 기능을 수행할 수 있습니다.

- 라이선스 활성화 또는 등록
- 회사의 라이선스 보기
- 회사 엔터티 간 라이선스 양도

자세한 내용은 Smart Account Manager Satellite의 Smart Software Manager Satellite 설치 및 환경 설정 가이드를 참고하십시오.

가상 어카운트별로 관리되는 라이선스 및 디바이스

라이선스 및 디바이스는 가상 어카운트별로 관리됩니다. 가상 계정의 디바이스에서만 해당 계정에 지정된 라이선스를 사용할 수 있습니다. 추가 라이선스가 필요할 경우 다른 가상 계정의 미사용 라이선스를 이전할 수 있습니다. 또한 가상 어카운트 간에 디바이스를 이전할 수도 있습니다.

Firepower 4100/9300 섀시만 디바이스로 등록되며 섀시의 ASA 애플리케이션은 고유한 라이선스를 요청합니다. 예를 들어, 보안 모듈이 3개 있는 Firepower 9300 섀시의 경우 섀시는 디바이스 1개로 간주되지만 모듈은 개별 라이선스 3개를 사용합니다.

평가판 라이선스

Firepower 4100/9300 섀시는 두 가지 유형의 평가판 라이선스를 지원합니다.

- 섀시 레벨 평가 모드 — Firepower 4100/9300 섀시가 Licensing Authority에 등록되기 전에 평가 모드로 90일(총 사용량) 동안 작동됩니다. 이 모드에서 ASA는 특정 엔타이틀먼트를 요청할 수 없으며 기본 엔타이틀먼트만 활성화됩니다. 이 기간이 종료되면 Firepower 4100/9300 섀시는 컴플라이언스 미준수 상태가 됩니다.
- 엔타이틀먼트 기반 평가 모드 - Firepower 4100/9300 섀시가 Licensing Authority에 등록되고 나면 ASA에 할당할 수 있는 시간 기반 평가판 라이선스를 받을 수 있습니다. ASA에서는 평소대로 엔타이틀먼트를 요청합니다. 시간 기반 라이선스가 만료되면 시간 기반 라이선스를 갱신하거나 영구 라이선스를 받아야 합니다.

참고 Strong Encryption(3DES/AES)용 평가판 라이선스를 받을 수는 없으며 영구 라이선스만 이 엔타이틀먼트를 지원합니다.

Smart Software Manager 통신

이 섹션에서는 디바이스가 Smart Software Manager와 통신하는 방법을 설명합니다.

디바이스 등록 및 토큰

각 가상 어카운트에서 등록 토큰을 만들 수 있습니다. 이 토큰은 기본적으로 30일간 유효합니다. 각 섀시를 구축할 때 또는 기존 섀시를 등록할 때 이 토큰 ID와 엔타이틀먼트 레벨을 입력합니다. 기존 토큰이 만료되면 새 토큰을 생성할 수 있습니다.

구축 후 시작 시 또는 기존 섀시에서 이 파라미터를 직접 구성한 이후에 섀시는 Cisco License Authority에 등록됩니다. 섀시를 토큰과 함께 등록하면 License Authority는 섀시와 License Authority 간의 통신을 위한 ID 인증서를 발급합니다. 이 인증서는 6개월마다 갱신되지만 1년간 유효합니다.

License Authority와의 정기적인 통신

디바이스는 30일마다 License Authority와 통신합니다. Smart Software Manager에서 변경할 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다. 또는 디바이스에서 예정대로 통신할 때까지 기다릴 수 있습니다.

선택 사항으로 HTTP 프록시를 구성할 수 있습니다.

최소 90일마다 Firepower 4100/9300 섀시가 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 Licensing Authority에 연락해야 합니다. 아니면 특별 라이선스가 필요한 기능의 구성을 변경할 수 없습니다. 이를 제외하면 작동에 영향을 미치지 않습니다.

참고 디바이스가 1년 동안 License Authority와 통신할 수 없는 경우, 디바이스는 등록되지 않은 상태로 전환되지만 이전에 활성화된 강력한 암호화 기능은 손실되지 않습니다.

규정 위반 상태

디바이스는 다음과 같은 상황에서 규정 위반이 될 수 있습니다.

- 과다 사용 — 디바이스에서 사용 불가한 라이선스를 사용할 경우.
- 라이선스 만료—한시적인 라이선스가 만료된 경우.
- 통신 부재 — 디바이스에서 권한 재부여를 위해 Licensing Authority에 연결하지 못한 경우.

어카운트가 컴플라이언스 미준수 상태인지 또는 컴플라이언스 미준수 상태에 근접한지를 확인하려면 Firepower 4100/9300 섀시에서 현재 사용 중인 엔타이틀먼트와 Smart Account의 엔타이틀먼트를 비교해야 합니다.

컴플라이언스 미준수 상태에서는 특수 라이선스가 필요한 기능의 구성을 변경할 수는 없지만 작업은 달리 영향을 받지 않습니다. 예를 들어 표준 라이선스 한도를 초과하는 기존 컨텍스트를 계속 실행할 수 있으며 해당 구성을 수정할 수는 있지만 새 컨텍스트를 추가할 수는 없습니다.

Smart Call Home 인프라

기본적으로, Smart Call Home 프로파일은 Licensing Authority의 URL을 지정하는 FXOS 구성에 있습니다. 이 프로필을 제거할 수 없습니다. License 프로필의 유일한 구성 옵션은 License Authority의 대상 주소 URL입니다. Cisco TAC에서 지시하지 않는 한 License Authority URL을 변경해서는 안 됩니다.

참고 Cisco 전송 게이트웨이는 Firepower 4100/9300 보안 어플라이언스에서 지원되지 않습니다.

Cisco Success Network

Cisco Success Network는 사용자가 활성화하는 클라우드 서비스입니다. Cisco Success Network를 활성화하는 경우, Firepower 4100/9300 섀시과 Cisco Cloud 사이에 보안 연결이 설정되어 사용 정보와 통계가 스트리밍됩니다. 스트리밍 텔레메트리는 ASA에서 관심 있는 데이터를 선택하고 이를 구조화된 형식으로 원격 관리 스테이션에 전송하여 다음을 수행하는 메커니즘을 제공합니다.

- 네트워크에서 제품의 효율성을 향상시킬 수있는 활용 가능한 미사용 기능을 알려줍니다.
- 제품에 사용할 수 있는 추가 기술 지원 서비스 및 모니터링에 대해 알려줍니다.

- Cisco가 제품을 개선하도록 돕습니다.

Firepower 4100/9300을 Cisco Smart Software Manager에 등록할 때 Cisco Success Network를 활성화하십시오. 라이센스 기관에 Firepower 4100/9300 섀시을 등록합니다., 18 페이지의 내용을 참조하십시오.

다음 조건이 모두 충족되는 경우에만 Cisco Success Network에 등록할 수 있습니다.

- 스마트 소프트웨어 라이선스가 등록되었습니다.
- 스마트 라이선스 위성 모드가 비활성화되었습니다.
- 영구 라이선스가 비활성화되었습니다.

Cisco Success Network에 등록하면 섀시가 항상 보안 연결을 설정하고 유지합니다. Cisco Success Network를 비활성화하여 언제든지 이 연결을 끌 수 있으며, 이 경우 디바이스와Cisco Success Network 클라우드의 연결이 끊어집니다.

Cisco Success Network 현재 등록 상태를 시스템 > 라이센싱 > **Cisco Success Network**페이지에서 볼 수 있으며, 등록 상태를 변경할 수 있습니다. Cisco Success Network 등록 변경, 19 페이지의 내용을 참조하십시오.

Cisco Success Network 텔레메트리 데이터

Cisco Success Network를 사용하면 등록된 섀시가 구성 및 운영 상태 정보를 24시간마다 Cisco Success Network 클라우드로 스트리밍할 수 있습니다. 수집 및 모니터되는 데이터는 다음과 같습니다.

- 등록 디바이스 정보— Firepower 4100/9300 섀시 모델명, 제품 ID, 일련번호, UUID, 시스템 가동 시간 및 스마트 라이선싱 정보를 포함합니다. 등록된 디바이스 데이터, 7 페이지의 내용을 참조하십시오.
- 소프트웨어 정보 - Firepower 4100/9300 섀시에서 실행 중인 소프트웨어의 유형 및 버전 번호입니다. 소프트웨어 버전 데이터, 7 페이지의 내용을 참조하십시오.
- **ASA** 디바이스 정보 — Firepower 4100/9300의 보안 모듈/엔진에서 실행 중인 ASA 디바이스에 대한 정보. Firepower 4100 Series의 경우 단일 ASA 디바이스에 대한 정보만 포함된다는 점에 유의하십시오. ASA 디바이스 정보에는 각 디바이스, 디바이스 모델, 일련 번호 및 소프트웨어 버전에 사용 중인 스마트 라이선스가 포함됩니다. ASA 디바이스 데이터, 8 페이지의 내용을 참조하십시오.
  - 성능 정보 — ASA 디바이스의 시스템 가동 시간, CPU 사용량, 메모리 사용량, 디스크 공간 사용량 및 대역폭 사용량 정보입니다. 성능 데이터, 8 페이지의 내용을 참조하십시오.
  - 사용 정보 — 기능 상태, 클러스터, 장애 조치 및 로그인 정보:
    - 기능 상태 — 사용자가 구성했거나 기본적으로 활성화되어 있는 활성화된 ASA 기능의 목록입니다.
    - 클러스터 정보 — ASA 디바이스가 클러스터 모드인 경우 클러스터 정보를 포함합니다. ASA 디바이스가 클러스터 모드가 아닌 경우 이 정보가 표시되지 않습니다. 클러스터 정보에는 ASA 디바이스의 클러스터 그룹 이름, 클러스터 인터페이스 모드, 유닛 이름

및 상태가 포함됩니다. 동일한 클러스터에 있는 다른 피어 ASA 디바이스의 경우, 이름, 상태 및 일련 번호가 정보에 포함됩니다.

- 장애 조치 정보 — ASA가 장애 조치 모드인 경우 장애 조치 정보를 포함합니다. ASA가 장애 조치 모드가 아닌 경우 이 정보가 표시되지 않습니다. 장애 조치 정보에는 ASA의 역할 및 상태, 피어 ASA 디바이스의 역할, 상태 및 일련 번호가 포함됩니다.
- 로그인 기록 — 사용자 로그인 빈도, 로그인 시간 및 ASA 디바이스에서 가장 최근에 성공한 로그인 날짜 스탬프입니다. 그러나 로그인 기록에는 사용자 로그인 이름, 자격 증명 또는 기타 개인 정보가 포함되지 않습니다.

자세한 내용은 사용량 데이터, 9 페이지를 참조하십시오.

등록된 디바이스 데이터

Firepower 4100/9300 섀시를 Cisco Success Network에 등록한 경우, 섀시에 대한 일부 텔레메트리 데이터가 Cisco 클라우드로 스트리밍됩니다. 다음 표는 수집 및 모니터링된 소프트웨어 정보에 관해 설명합니다.

표 *1:* 등록된 디바이스 텔레메트리 데이터

데이터 포인트	예제 값
디바이스 모델	Cisco Firepower FP9300 Security 어플라이언스
Serial number(일련 번호)	GMX1135L01K
스마트 라이선스 PIID	752107e9-e473-4916-8566-e26d0c4a5bd9
스마트 라이선스 가상 어카운트 이름	FXOS-일반
시스템 가동 시간	32115
UDI 제품 ID	FPR-C9300-AC

소프트웨어 버전 데이터

Cisco Success Network는 유형 및 소프트웨어 버전을 포함하여 섀시와 관련된 소프트웨어 정보를 수집합니다. 다음 표는 수집 및 모니터링된 소프트웨어 정보에 관해 설명합니다.

표 *2:* 소프트웨어 버전 텔레메트리 데이터

데이터 포인트	예제 값
Type(유형)	package_version
버전	2.7(1.52)

ASA 디바이스 데이터

Cisco Success Network는 Firepower 4100/9300의 보안 모듈/엔진에서 실행 중인 ASA 디바이스에 대한 정보를 수집합니다. 다음 표는 ASA 디바이스에 대해 수집 및 모니터링된 소프트웨어 정보를 설명합니다.

표 *3: ASA* 디바이스 텔레메트리 데이터

데이터 포인트	예제 값
ASA 디바이스 PID	FPR9K-SM-36
ASA 디바이스 모델	Cisco Adaptive Security Appliance
ASA 디바이스 일련 번호	XDQ311841WA
구축 유형(기본 또는 컨테이너)	네이티브
보안 상황 모드(단일 또는 다중)	단일

ASA 소프트웨어 버전	{
	type: "asa_version",
	ersion: "9.13.1.5"
	}

디바이스 매니저 버전	{
	type: "device_mgr_version",
	version: "7.10.1"
	}

활성화된 스마트 라이선스 사용 중	{
	"type": "Strong encryption",
	"tag":
	"regid.2016-05.com.cisco.ASA-GEN-STRONG-ENCRYPTION,
	5.7_982308k4-74w2-5f38-64na-707q99g10cce",
	"count": 1
	}

성능 데이터

Cisco Success Network는 ASA 디바이스에 대한 성능 관련 정보를 수집합니다. 정보에는 시스템 가동 시간, CPU 사용량, 메모리 사용량, 디스크 공간 사용량 및 대역폭 사용량 정보가 포함됩니다.

- **CPU usage** - 지난 5분 동안의 CPU 사용량 정보
- 메모리 사용량 - 시스템의 여유, 사용 및 총 메모리
- 디스크 사용량 - 여유 공간, 사용된 공간, 총 디스크 공간 정보
- 시스템 **uptime(**실행시간**)** - 시스템 uptime(실행시간) 정보
- **Bandwidth(**대역폭**)** 사용량 - 시스템 Bandwidth 사용량. 모든 nameif-ed 인터페이스에서 집계 시스템 가동 이후 초당 수신 및 전송된 패킷(또는 바이트)에 대한 통계를 보여줍니다.

다음 표는 수집 및 모니터링된 소프트웨어 정보에 관해 설명합니다.

표 4: 성능 텔레메트리 데이터

데이터 포인트	예제 값

지난 5분 동안의 시스템 CPU 사용량	{
	“fiveSecondsPercentage”:0.2000000,
	“oneMinutePercentage”: 0,
	“fiveMinutesPercentage”: 0
	
	}

시스템 메모리 사용량	{
	“freeMemoryInBytes”:225854966384,
	“usedMemoryInBytes”: 17798281616,
	“totalMemoryInBytes”:243653248000
	
	}

시스템 디스크 사용량	{
	"freeGB": 21.237285,
	"usedGB": 0.238805,
	"totalGB": 21.476090
	
	}

시스템 가동 시간	99700000

시스템 bandwidth(대역폭) 사용량	{
	"receivedPktsPerSec": 3,
	"receivedBytesPerSec": 212,
	"transmittedPktsPerSec": 3,
	"transmittedBytesPerSec": 399
	}

사용량 데이터

Cisco Success Network는 섀시의 보안 모듈/엔진에서 실행 중인 ASA 디바이스에 대한 기능 상태, 클러스터, 장애 조치 및 로그인 정보를 수집합니다. 다음 표는 ASA 디바이스 사용에 대해 수집 및 모니터링된 데이터를 설명합니다.

표 5: 텔레메트리 데이터 사용

데이터 포인트	예제 값

Feature status(기능 상태)	[{
	“name”: “cluster”,
	“status”: “enabled”
	},
	{
	“name”: “webvpn”,
	“status”: “enabled”
	},
	{
	“name”: “logging-buffered”,
	“status”: “debugging”
	}]

데이터 포인트	예제 값
Cluster information(클러스터 정보)	{ "clusterGroupName": "asa-cluster", "interfaceMode": "spanned", "unitName": "unit-3-3", "unitState": "SLAVE", "otherMembers": { "items": [{ "memberName": "unit-2-1", "memberState": "MASTER", "memberSerialNum": "DAK391674E" }] } }
Failover information(장애 조치 정보)	{ myRole: "Primary", peerRole: "Secondary", myState: "active", peerState: "standby", peerSerialNum: "DAK39162B" }
로그인 기록	{ "loginTimes": "1 times in last 1 days", "lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019" }

텔레메트리 예시 파일

Firepower 4100/9300 섀시는 데이터를 Cisco 클라우드로 전송하기 전에 텔레메트리가 활성화되고 섀시 관련 정보 및 추가 필드와 함께 온라인 상태인 모든 ASA 디바이스에서 수신한 데이터를 집계합니다. 텔레메트리 데이터가 포함된 애플리케이션이 없는 경우에도 섀시 정보와 함께 텔레메트리가 Cisco 클라우드로 전송됩니다.

다음은 Firepower 9300의 ASA 디바이스 2개에 대해 Cisco 클라우드로 전송된 정보를 포함하는 Cisco Success Network 텔레메트리 파일의 예입니다.

```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json",
    "msgID": "2227"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1560868270055,
    "FXOS": {
      "FXOSdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "HNY4475P01K",
```

```
    "smartLicenseProductInstanceIdentifier": "413509m0-f952-5822-7492-r62c0a5h4gf4",
    "smartLicenseVirtualAccountName": "FXOS-general",
    "systemUptime": 32115,
    "udiProductIdentifier": "FPR-C9300-AC"
  },
  "versions": {
    "items": [
      {
        "type": "package_version",
        "version": "2.7(1.52)"
      }
    ]
  }
},
"asaDevices": {
  "items": [
    {
      "CPUUsage": {
        "fiveMinutesPercentage": 0,
        "fiveSecondsPercentage": 0,
        "oneMinutePercentage": 0
      },
      "bandwidthUsage": {
        "receivedBytesPerSec": 1,
        "receivedPktsPerSec": 0,
        "transmittedBytesPerSec": 1,
        "transmittedPktsPerSec": 0
      },
      "deviceInfo": {
        "deploymentType": "Native",
        "deviceModel": "Cisco Adaptive Security Appliance",
        "securityContextMode": "Single",
        "serialNumber": "ADG2158508T",
        "systemUptime": 31084,
        "udiProductIdentifier": "FPR9K-SM-24"
      },
      "diskUsage": {
        "freeGB": 19.781810760498047,
        "totalGB": 20.0009765625,
        "usedGB": 0.21916580200195312
      },
      "featureStatus": {
        "items": [
          {
            "name": "aaa-proxy-limit",
            "status": "enabled"
          },
          {
            "name": "firewall_user_authentication",
            "status": "enabled"
          },
          {
            "name": "IKEv2 fragmentation",
            "status": "enabled"
          },
          {
            "name": "inspection-dns",
            "status": "enabled"
          },
          {
            "name": "inspection-esmtp",
            "status": "enabled"
          },
          {
```

```
    "name": "inspection-ftp",
    "status": "enabled"
  },
  {
    "name": "inspection-hs232",
    "status": "enabled"
  },
  {
    "name": "inspection-netbios",
    "status": "enabled"
  },
  {
    "name": "inspection-rsh",
    "status": "enabled"
  },
  {
    "name": "inspection-rtsp",
    "status": "enabled"
  },
  {
    "name": "inspection-sip",
    "status": "enabled"
  },
  {
    "name": "inspection-skinny",
    "status": "enabled"
  },
  {
    "name": "inspection-snmp",
    "status": "enabled"
  },
  {
    "name": "inspection-sqlnet",
    "status": "enabled"
  },
  {
    "name": "inspection-sunrpc",
    "status": "enabled"
  },
  {
    "name": "inspection-tftp",
    "status": "enabled"
  },
  {
    "name": "inspection-xdmcp",
    "status": "enabled"
  },
  {
    "name": "management-mode",
    "status": "normal"
  },
  {
    "name": "mobike",
    "status": "enabled"
  },
  {
    "name": "ntp",
    "status": "enabled"
  },
  {
    "name": "sctp-engine",
    "status": "enabled"
  },
  {
```

```
        "name": "smart-licensing",
        "status": "enabled"
      },
      {
        "name": "static-route",
        "status": "enabled"
      },
      {
        "name": "threat_detection_basic_threat",
        "status": "enabled"
      },
      {
        "name": "threat_detection_stat_access_list",
        "status": "enabled"
      }
    ]
  },
  "licenseActivated": {
    "items": []
  },
  "loginHistory": {
    "lastSuccessfulLogin": "05:53:18 UTC Jun 18 2019",
    "loginTimes": "1 times in last 1 days"
  },
  "memoryUsage": {
    "freeMemoryInBytes": 226031548496,
    "totalMemoryInBytes": 241583656960,
    "usedMemoryInBytes": 15552108464
  },
  "versions": {
    "items": [
      {
        "type": "asa_version",
        "version": "9.13(1)248"
      },
      {
        "type": "device_mgr_version",
        "version": "7.13(1)31"
      }
    ]
  }
},
{
  "CPUUsage": {
    "fiveMinutesPercentage": 0,
    "fiveSecondsPercentage": 0,
    "oneMinutePercentage": 0
  },
  "bandwidthUsage": {
    "receivedBytesPerSec": 1,
    "receivedPktsPerSec": 0,
    "transmittedBytesPerSec": 1,
    "transmittedPktsPerSec": 0
  },
  "deviceInfo": {
    "deploymentType": "Native",
    "deviceModel": "Cisco Adaptive Security Appliance",
    "securityContextMode": "Single",
    "serialNumber": "RFL21764S1D",
    "systemUptime": 31083,
    "udiProductIdentifier": "FPR9K-SM-24"
  },
  "diskUsage": {
    "freeGB": 19.781543731689453,
```

```
  "totalGB": 20.0009765625,
  "usedGB": 0.21943283081054688
},
"featureStatus": {
  "items": [
    {
      "name": "aaa-proxy-limit",
      "status": "enabled"
    },
    {
      "name": "call-home",
      "status": "enabled"
    },
    {
      "name": "crypto-ca-trustpoint-id-usage-ssl-ipsec",
      "status": "enabled"
    },
    {
      "name": "firewall_user_authentication",
      "status": "enabled"
    },
    {
      "name": "IKEv2 fragmentation",
      "status": "enabled"
    },
    {
      "name": "inspection-dns",
      "status": "enabled"
    },
    {
      "name": "inspection-esmtp",
      "status": "enabled"
    },
    {
      "name": "inspection-ftp",
      "status": "enabled"
    },
    {
      "name": "inspection-hs232",
      "status": "enabled"
    },
    {
      "name": "inspection-netbios",
      "status": "enabled"
    },
    {
      "name": "inspection-rsh",
      "status": "enabled"
    },
    {
      "name": "inspection-rtsp",
      "status": "enabled"
    },
    {
      "name": "inspection-sip",
      "status": "enabled"
    },
    {
      "name": "inspection-skinny",
      "status": "enabled"
    },
    {
      "name": "inspection-snmp",
      "status": "enabled"
```

```
      },
      {
        "name": "inspection-sqlnet",
        "status": "enabled"
      },
      {
        "name": "inspection-sunrpc",
        "status": "enabled"
      },
      {
        "name": "inspection-tftp",
        "status": "enabled"
      },
      {
        "name": "inspection-xdmcp",
        "status": "enabled"
      },
      {
        "name": "management-mode",
        "status": "normal"
      },
      {
        "name": "mobike",
        "status": "enabled"
      },
      {
        "name": "ntp",
        "status": "enabled"
      },
      {
        "name": "sctp-engine",
        "status": "enabled"
      },
      {
        "name": "smart-licensing",
        "status": "enabled"
      },
      {
        "name": "static-route",
        "status": "enabled"
      },
      {
        "name": "threat_detection_basic_threat",
        "status": "enabled"
      },
      {
        "name": "threat_detection_stat_access_list",
        "status": "enabled"
      }
    ]
  },
  "licenseActivated": {
    "items": []
  },
  "loginHistory": {
    "lastSuccessfulLogin": "05:53:16 UTC Jun 18 2019",
    "loginTimes": "1 times in last 1 days"
  },
  "memoryUsage": {
    "freeMemoryInBytes": 226028740080,
    "totalMemoryInBytes": 241581195264,
    "usedMemoryInBytes": 15552455184
  },
  "versions": {
```

```
            "items": [
              {
                "type": "asa_version",
                "version": "9.13(1)248"
              },
              {
                "type": "device_mgr_version",
                "version": "7.13(1)31"
              }
            ]
          }
        }
      ]
    }
  }
}
```


Smart Software Licensing 사전 요구 사항

- 이 장은 Firepower 4100/9300 섀시의 ASA 논리적 디바이스에만 적용됩니다. FTD 논리적 디바이스의 라이선싱에 대한 자세한 내용은 FMC 구성 가이드를 참조하십시오.
- Cisco Smart Software Manager에서 마스터 계정을 만듭니다.

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

  아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.
- Cisco Commerce Workspace에서 라이선스를 1개 이상 구매합니다. 홈 페이지의 **Find Products and Solutions(**제품 및 솔루션 찾기**)** 검색 필드에서 사용 중인 플랫폼을 검색합니다. 일부 라이선스는 무료이지만 Smart Software Licensing 어카운트에 추가해야 합니다.
- 섀시가 Licensing Authority에 연결할 수 있도록 섀시에서 인터넷 액세스 또는 HTTP 프록시 액세스가 가능한지 확인합니다.
- 섀시에서 Licensing Authority의 이름을 확인할 수 있도록 DNS 서버를 구성합니다.
- 섀시의 시간을 설정합니다.
- ASA 라이선싱 엔타이틀먼트를 구성하기 전에 Firepower 4100/9300 섀시에 Smart Software Licensing 인프라를 구성합니다.

스마트 소프트웨어 라이센싱을 위한 지침

페일오버 및 클러스터링을 위한 **ASA** 지침

각 Firepower 4100/9300 섀시를 License Authority 또는 Satellite 서버에 등록해야 합니다. 보조 유닛에 대한 추가 비용은 없습니다. 영구 라이선스를 예약하려면 각 섀시용으로 별도의 라이선스를 구매해야 합니다.

Smart Software Licensing의 기본값

Firepower 4100/9300 섀시 기본 구성은 Smart Call Home 프로필인 "SLProf"를 포함하며, 이는 Licensing Authority의 URL을 지정합니다.

일반 Smart Software Licensing 구성

Cisco License Authority와 통신하기 위해 HTTP 프록시를 선택적으로 구성할 수 있습니다. License Authority에 등록하려면 Smart Software 라이선스 어카운트에서 얻은 Firepower 4100/9300 섀시에 등록 토큰 ID를 입력해야 합니다.

프로시저

단계 **1** (선택 사항) HTTP 프록시 구성, 17 페이지.

단계 **2** (선택 사항) Call Home URL 삭제, 18 페이지

단계 **3** 라이센스 기관에 Firepower 4100/9300 섀시을 등록합니다., 18 페이지.

(선택 사항) HTTP 프록시 구성

네트워크에서 인터넷 액세스에 HTTP 프록시를 사용할 경우 스마트 소프트웨어 라이선싱에 대해 프록시 주소를 구성해야 합니다. 일반적으로 이 프록시는 Smart Call Home에도 사용됩니다.

참고 인증이 있는 HTTP 프록시는 지원되지 않습니다.

프로시저

단계 **1** **System**(시스템) > **Licensing**(라이선싱) > **Call Home**을 선택합니다.

Call Home 페이지는 License Authority의 대상 주소 URL 구성 및 HTTP 프록시 구성을 위한 필드를 제공합니다.

참고 Cisco TAC에서 지시하지 않는 한 License Authority URL을 변경해서는 안 됩니다.

단계 **2** Server Enable(서버 활성화) 드롭다운 목록에서 **on**(설정)을 선택합니다.

단계 **3** **Server URL**(서버 **URL**) 및 **Server Port**(서버 포트) 필드에 프록시 IP 주소와 포트를 입력합니다. 이를테면 HTTPS 서버에 대해 포트 443을 입력합니다.

단계 4 **Save(**저장**)**를 클릭합니다.

(선택 사항) Call Home URL 삭제

앞에서 구성한 Call Home URL을 삭제하려면 다음 절차를 사용하십시오.

프로시저

단계 1 **System(**시스템**)** > **Licensing(**라이선싱**)** > **Call Home**을 선택합니다.

단계 2 **Call home Configuration(Call home** 구성**)** 영역에서 Delete(삭제)를 선택합니다.

라이센스 기관에 Firepower 4100/9300 섀시을 등록합니다.

Firepower 4100/9300 섀시를 등록할 때 License Authority에서는 Firepower 4100/9300 섀시와 License Authority의 통신을 위해 ID 인증서를 발급합니다. 또한 Firepower 4100/9300 섀시를 적절한 가상 계정에 지정합니다. 일반적으로 이 절차는 1회 수행됩니다. 그러나 이를테면 통신 문제 때문에 ID 인증서가 만료되면 나중에 Firepower 4100/9300 섀시를 다시 등록해야 할 수 있습니다.

프로시저

단계 1 Smart Software Manager 또는 Smart Software Manager Satellite에서 이 Firepower 4100/9300 섀시를 추가하려는 가상 어카운트에 대한 등록 토큰을 요청 및 복사합니다.

Smart Software Manager Satellite를 사용하여 등록 토큰을 요청하는 방법에 대한 자세한 내용은 Cisco Smart Software Manager Satellite 사용 설명서(https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html)를 참조하십시오.

단계 2 Firepower Chassis Manager에서 **System(**시스템**)** > **Licensing(**라이선싱**)** > **Smart License(**스마트 라이선스**)**를 선택합니다.

단계 3 **Enter Product Instance Registration Token(**제품 인스턴스 등록 토큰 입력**)** 필드에 등록 토큰을 입력합니다.

단계 4 (선택 사항) **Enable Cisco Success Network** 체크 박스의 선택을 취소하여 Cisco Success Network 기능을 비활성화할 수 있습니다.

자세한 내용은 Cisco Success Network, 5 페이지를 참조하십시오.

단계 5 **Register(**등록**)**를 클릭합니다.

Firepower 4100/9300 섀시에서 License Authority 등록을 시도합니다.

디바이스의 등록을 취소하려면 **Unregister(**등록 취소**)**를 클릭합니다.

Firepower 4100/9300 섀시를 등록 취소하면 계정에서 디바이스가 제거됩니다. 디바이스의 모든 라이선스 엔타이틀먼트 및 인증서가 제거됩니다. 새 Firepower 4100/9300 섀시의 라이선스를 확보하기 위해 등록을 취소하는 경우가 있습니다. 또는 Smart Software Manager에서 해당 디바이스를 제거할 수 있습니다.

Cisco Success Network 등록 변경

Firepower 4100/9300을 Cisco Smart Software Manager에 등록할 때 Cisco Success Network를 활성화하십시오. 그 후 다음 절차를 사용하여 등록 상태를 확인 또는 변경합니다.

참고 Cisco Success Network는 평가판 모드에서 작동하지 않습니다.

프로시저

단계 1 시스템 > 라이선싱 > **Cisco Success Network**를 선택합니다.

단계 2 **Cisco Success Network** 기본 설정 아래에서, Cisco에서 제공하는 정보를 읽고 Cisco로 전송될 샘플 데이터를 확인하려면 여기를 클릭을 클릭합니다.

단계 3 **Cisco Success Network** 활성화 여부를 선택하고 **Save(**저장**)**를 클릭합니다.

Smart License Satellite Server 구성 Firepower 4100/9300 섀시

다음 절차는 Smart Licence Satellite 서버를 사용하도록 Firepower 4100/9300 섀시를 구성하는 방법을 보여줍니다.

시작하기 전에

- Smart Software Licensing 사전 요구 사항, 16 페이지에 나열된 모든 전제 조건을 완료합니다.
- Smart Software Satellite Server를 구축하고 설정합니다.

  Cisco.com에서 Smart License Satellite OVA 파일을 다운로드하고 VMwareESXi 서버에 이 파일을 설치 및 구성합니다. 자세한 내용은 Smart Software Manager Satellite 설치 가이드를 참고하십시오.
- Smart Software Satellite Server의 FQDN을 내부 DNSserver에서 확인할 수 있는지 확인합니다.
- 위성 트러스트 포인트가 이미 있는지를 확인합니다.

  scope security

  show trustpoint

트러스트 포인트는 FXOS 버전 2.4(1) 이상에서 기본적으로 추가됩니다. 트러스트 포인트가 없는 경우 다음 단계를 사용하여 트러스트 포인트 하나를 직접 추가해야 합니다.

1. http://www.cisco.com/security/pki/certs/clrca.cer로 이동한 다음, 구성하는 동안 액세스할 수 있는 위치에 SSL 인증서("-----BEGIN CERTIFICATE-----"부터 "-----END CERTIFICATE-----"까지)의 전체 본문을 복사합니다.
2. 보안 모드를 입력합니다.

   scope security
3. Trust Point를 생성하고 이름을 지정합니다.

   create trustpoint *trustpoint_name*
4. Trust Point의 인증서 정보를 지정합니다. 참고: 인증서는 Base64 암호화 X.509(CER) 형식이어야 합니다.

   set certchain *certchain*

   *certchain*변수의 경우 1단계에서 복사한 인증서 텍스트를 붙여넣습니다.

   명령에 인증서 정보를 지정하지 않은 경우, 루트 CA(Certificate Authority)에 인증 경로를 정의하는 신뢰 지점 목록 또는 인증서를 입력하라는 프롬프트가 표시됩니다. 해당 정보를 입력한 후 다음 행에 **ENDOFBUF** 를 입력하여 완료합니다.
5. 구성을 커밋합니다.

   commit-buffer

프로시저

단계 **1** **System(**시스템**)** > **Licensing(**라이선싱**)** > **Call Home**을 선택합니다.

단계 **2** **Call home Configuration(Call Home** 구성**)** 영역에서 **Address(**주소**)** 필드의 기본 URL을 이 절차의 사전 요구 사항에서 수집한 정보를 사용하는 Smart Software Satellite Server의 URL로 교체합니다 (**https://***[Satellite* 서버의 *FQDN]***/Transportgateway/services/DeviceRequestHandler** 형식 사용).

단계 **3** 라이센스 기관에 Firepower 4100/9300 섀시을 등록합니다., 18 페이지. Smart License Manager Satellite에서 등록 토큰을 요청하고 복사해야 합니다.

영구 라이선스 예약 구성

Firepower 4100/9300 섀시에 영구 라이선스를 할당할 수 있습니다. 이 범용 예약을 사용하면 디바이스에서 어떤 엔타이틀먼트라도 무제한 사용할 수 있습니다.

참고 시작하기 전에 Smart Software Manager에서 사용할 수 있도록 영구 라이선스를 구매해야 합니다. 모든 계정에 대해 영구 라이선스 예약이 승인되는 것은 아닙니다. 구성을 시도하기 전에 Cisco에서 이 기능에 대한 승인을 받았는지 확인하십시오.

영구 라이선스 설치

다음 절차는 Firepower 4100/9300 섀시에 영구 라이선스를 할당하는 방법을 보여줍니다.

프로시저

단계 **1** **System** > **Licensing** > **Permanent License**를 선택합니다.

단계 **2** **Generate**를 클릭하여 예약 요청 코드를 생성합니다. 예약 요청 코드를 클립보드에 복사합니다.

단계 **3** Cisco Smart Software Manager 포털의 Smart Software Manager Inventory(인벤토리) 화면으로 이동하여 **Licenses** 탭을 클릭합니다.

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

Licenses 탭에는 계정과 연결된 모든 기존 라이선스(일반 및 영구)가 표시됩니다.

단계 **4** **License Reservation**을 클릭하고, 생성된 예약 요청 코드를 상자에 붙여넣습니다.

단계 **5** **Reserve License** 버튼을 클릭합니다.

Smart Software Manager에서 인증 코드를 생성합니다. 코드를 다운로드하거나 클립보드로 복사할 수 있습니다. 이 시점에서는 Smart Software Manager에 따라 라이선스가 사용됩니다.

License Reservation 버튼이 표시되지 않으면 계정이 영구 라이선스 예약에 대해 인증되지 않은 것입니다. 이 경우 영구 라이선스 예약을 비활성화하고 일반 smart license 명령을 다시 입력해야 합니다.

단계 **6** Firepower Chassis Manager에서 **Authorization Code** 입력란에 생성된 인증 코드를 입력합니다.

단계 **7** **Install** 버튼을 클릭합니다.

Firepower 4100/9300 섀시에 PLR로 완전히 라이선스가 부여되면, Permanent License(영구 라이선스) 페이지에 라이선스 상태가 표시되고 영구 라이선스를 반환할 수 있는 옵션이 제공됩니다.

단계 **8** ASA 논리적 디바이스에서 기능 엔타이틀먼트를 활성화합니다. 엔타이틀먼트를 활성화하려면 ASA 라이선싱 장을 참조하십시오.

(선택 사항) 영구 라이선스 반환

영구 라이선스가 더 이상 필요하지 않으면 다음 절차를 사용하여 공식적으로 Smart Software Manager에 반환해야 합니다. 모든 단계를 수행하지 않으면 라이선스가 사용 중 상태로 유지되므로 다른 곳에서 사용할 수 없습니다.

프로시저

단계 **1** **System** > **Licensing** > **Permanent License**를 선택합니다.

단계 **2** **Return**을 클릭하여 반환 코드를 생성합니다. 반환 코드를 클립보드에 복사합니다.

Firepower 4100/9300 섀시의 라이선스가 즉시 취소되고 Evaluation(평가) 상태로 전환됩니다.

단계 **3** Smart Software Manager Inventory(인벤토리) 화면으로 이동하여 **Product Instances** 탭을 클릭합니다.

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

단계 **4** UDI(universal device identifier)를 사용하여 Firepower 4100/9300 섀시를 검색합니다.

단계 **5** **Actions** > **Remove**를 선택하고, 생성된 반환 코드를 상자에 붙여넣습니다.

단계 **6** **Remove Product Instance** 버튼을 클릭합니다.

영구 라이선스가 사용 가능한 풀로 반환됩니다.

단계 **7** 시스템을 재부팅합니다. Firepower 4100/9300 섀시 리부팅 방법에 대한 자세한 내용은 Firepower 4100/9300 섀시 리부팅 섹션을 참조하십시오.

Smart Software Licensing 기록

기능 이름	플랫폼 릴리스	설명
Cisco Success Network	2.7.1	Cisco Success Network는 사용자가 활성화하는 클라우드 서비스입니다. Cisco Success Network를 활성화하는 경우, Firepower 4100/9300 섀시과 Cisco Cloud 사이에 보안 연결이 설정되어 사용 정보와 통계가 스트리밍됩니다. 스트리밍 텔레메트리는 ASA에서 관심 있는 데이터를 선택하고 이를 구조화된 형식으로 원격 관리 스테이션에 전송하여 다음을 수행하는 메커니즘을 제공합니다. • 네트워크에서 제품의 효율성을 향상시킬 수있는 활용 가능한 미사용 기능을 알려줍니다. • 제품에 사용할 수 있는 추가 기술 지원 서비스 및 모니터링에 대해 알려줍니다. • Cisco가 제품을 개선하도록 돕습니다. Cisco Success Network에 등록하면 섀시가 항상 보안 연결을 설정하고 유지합니다. Cisco Success Network를 비활성화하여 언제든지 이 연결을 끌 수 있으며, 이 경우 디바이스와Cisco Success Network 클라우드의 연결이 끊어집니다. 다음 명령을 도입했습니다. **scope telemetry {enable | disable}** 추가된 화면: 시스템 > 라이센싱 > **Cisco Success Network**

기능 이름	플랫폼 릴리스	설명
Firepower 4100/9300 섀시의 Cisco 스마트 소프트웨어 라이선싱	1.1(1)	스마트 소프트웨어 라이선싱에서는 라이선스 풀을 구매하여 관리할 수 있습니다. 스마트 라이선스는 특정 일련 번호에 연결되지 않습니다. 각 유닛의 라이선스 키를 관리할 필요 없이 손쉽게 디바이스를 구축하거나 사용 중단할 수 있습니다. 또한 스마트 소프트웨어 라이선싱에서는 라이선스 사용량 및 필요량을 한눈에 볼 수 있습니다. Smart Software 라이선싱 구성은 Firepower 4100/9300 섀시 Supervisor(관리자)와 보안 모듈로 나뉩니다. 추가된 화면: **System(**시스템**)** > **Licensing(**라이선싱**)** > **Call Home** **System(**시스템**)** > **Licensing(**라이선싱**)** > **Smart License(**스마트 라이선스**)**