Catalyst 플랫폼에서 Smart Licensing 문제 해결

목차

- 소개
  - Cisco Smart Licensing이란?
  - 스마트 라이선싱 구현 방법
  - 지원되는 Cisco IOS XE 플랫폼
  - 레거시 라이선스에서 스마트 라이선스로 마이그레이션
    - DLC(Device LED Conversion)를 통한 변환
    - CSSM(Cisco Smart Software Manager) 또는 LRP(License Registration Portal)를 통한 변환
    - Cisco GLO(Global Licensing Operations) 부서에 전환 및 문의
  - 16.9에서 16.12.3으로 Catalyst 9500 고성능 동작 변화
    - Cisco IOS XE 버전 16.11.x 이전
    - Cisco IOS XE 버전 16.12.3 이상
    - C9500 고성능 변경 FAQ
- 설정
  - 기본 설정
  - 등록 토큰/디바이스 ID 토큰
  - 등록 및 라이선스 상태
- 고려 사항 및 주의 사항
- 문제 해결
  - 디바이스 등록 실패
- 일반적인 실패 시나리오
  - 시나리오 #1: 스위치 등록 "Failure Reason: Product Already Registered"
  - 시나리오 #2: 스위치 등록 "실패 사유: 요청을 지금 처리할 수 없습니다. 다시 시도하여 주십시오"
  - 시나리오 #3: 실패 사유 "디바이스 일자 152613526865 3이 허용 한도 초과로 오프셋되었습니다.
  - 시나리오 #4: 스위치 등록 "실패 사유: 통신 전송을 사용할 수 없습니다."
  - 시나리오 #5: 스위치 라이센스 권한 부여 "실패 사유: Call Home HTTP 메시지를 전송하지 못했습니다."
  - 시나리오 #6: 실패 이유 "Id 인증서 일련 번호 필드 누락; 서명 인증서 일련 번호 필드 누락; 서명된 데이터와 인증서가 일치하지 않음" 로그
  - 시나리오 #7: 스위치 라이센스 권한 부여 "실패 사유: 응답 대기 중"
  - 시나리오 #8: "OUT OF COMPLIANCE" 상태의 라이센스
  - 시나리오 #9: 스위치 라이센스 권한 부여 "실패 사유: 데이터와 서명이 일치하지 않음 "

소개

이 문서에서는 Cisco Smart Licensing(클라우드 기반 시스템)을 사용하여 Catalyst 스위치에서 소프트웨어 라이선스 관리를 작동하는 방법을 설명합니다.

Cisco Smart Licensing이란?

Cisco Smart Licensing은 Cisco 제품 전체의 모든 소프트웨어 라이센스를 관리하는 클라우드 기반

통합 라이센스 관리 시스템입니다. Cisco Software 라이센스를 구매, 구축, 관리, 추적, 갱신할 수 있습니다. 이는 단일 사용자 인터페이스에서 라이선스 보유 및 사용에 관한 정보도 제공합니다.

이 솔루션은 Cisco 소프트웨어 자산을 추적하는 데 사용되는 온라인 Smart Account(Cisco Smart Licensing Portal)와 Smart Account 관리에 사용되는 Cisco Smart Software Manager(CSSM)로 구성됩니다. CSSM에서는 라이선스 등록, 등록 취소, 이동 및 전송과 같은 모든 라이선싱 관리 관련 작업을 수행할 수 있습니다. 사용자에게 스마트 어카운트 및 특정 가상 어카운트에 대한 액세스 권한을 부여하고 추가할 수 있습니다.

Cisco 스마트 라이선싱에 대해 자세히 알아 보려면 다음을 방문하십시오.

a) Cisco 스마트 라이선싱 홈 페이지

b) Cisco Community - 온디맨드 교육

Cisco IOS® XE 17.3.2 이상 버전에서 정책 방법을 사용하는 새로운 Smart Licensing에 대한 자세한 내용은 Catalyst 스위치에서 정책을 사용하는 Smart Licensing을 참고하십시오.

스마트 라이선싱 및/또는 스마트 어카운트 관리를 처음 사용하십니까? 새로운 관리자 교육 과정 및 녹화 과정을 방문하여 등록하십시오.
Cisco Community - Cisco 스마트 어카운트/스마트 라이선싱 및 My Cisco 엔타이틀먼트로 스마트해지기

스마트 어카운트는 다음에서 생성할 수 있습니다. Smart Accounts

스마트 어카운트는 다음에서 관리할 수 있습니다. Smart Software Licensing

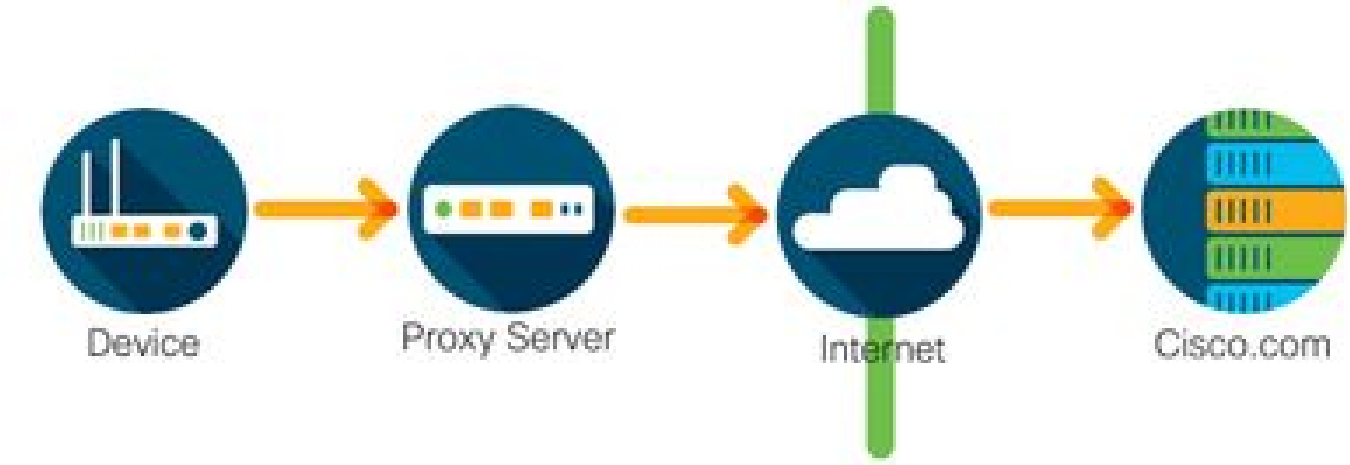
스마트 라이선싱 구현 방법

다음과 같은 회사의 보안 프로파일에 따라 활용할 수 있는 Cisco 스마트 라이선싱 구축에는 여러 가지 방법이 있습니다.

직접 클라우드 액세스

Cisco 제품은 안전하게 HTTPS를 사용하여 인터넷을 통해 직접 사용 정보를 전송합니다. 추가 구성 요소는 필요하지 않습니다.

HTTP 프록시를 통한 액세스



Cisco 제품은 HTTPS를 사용하여 HTTP 프록시 서버를 통해 사용량 정보를 안전하게 전송합니다. 기존 프록시 서버를 사용하거나 Cisco Transport Gateway를 통해 구축할 수 있습니다. (추가 정보를 보려면 여기를 클릭)

온프레미스 라이선스 서버(Cisco Smart Software Manager Statellite이라고도 함)

Cisco 제품은 사용 정보를 인터넷을 통해 직접 전송하지 않고 온프레미스 서버로 전송합니다. 한 달에 한 번 서버가 HTTPS를 통해 인터넷을 통해 모든 디바이스에 접속하거나 데이터베이스를 동기화하기 위해 수동으로 전송할 수 있습니다. CSSM On-prem(위성)은 VM(Virtual Machine)으로 제공되며 여기에서 다운로드할 수 있습니다. 자세한 내용은 Smart Software Manager Satellite 페이지를 방문하십시오.

지원되는 Cisco IOS XE 플랫폼

- Cisco IOS XE 버전 16.9.1 릴리스부터는 Catalyst 3650/3850 및 Catalyst 9000 시리즈 스위치 플랫폼이 유일한 라이선싱 방법으로 Cisco Smart Licensing 방법을 지원합니다.
- Cisco IOS XE 버전 16.10.1 릴리스부터는 ASR1K, ISR1K, ISR4K 및 가상 라우터(CSRv / ISRv)와 같은 라우터 플랫폼이 유일한 라이선싱 방법으로 Cisco Smart Licensing 방법을 지원

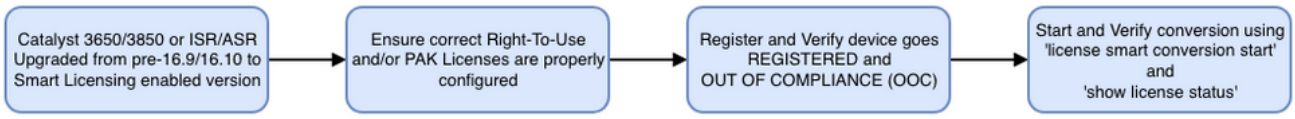
합니다.

레거시 라이선스에서 스마트 라이선스로 마이그레이션

레거시 라이센스를 변환하는 방법에는 RTU(Right-To-Use) 또는 PAK(Product Activation Key)와 같은 두 가지가 있습니다. 어떤 방법을 따라야 하는지에 대한 자세한 내용은 특정 Cisco 장치에 대한 관련 릴리스 노트 및/또는 컨피그레이션 가이드를 참조하십시오.

DLC(Device LED Conversion)를 통한 변환

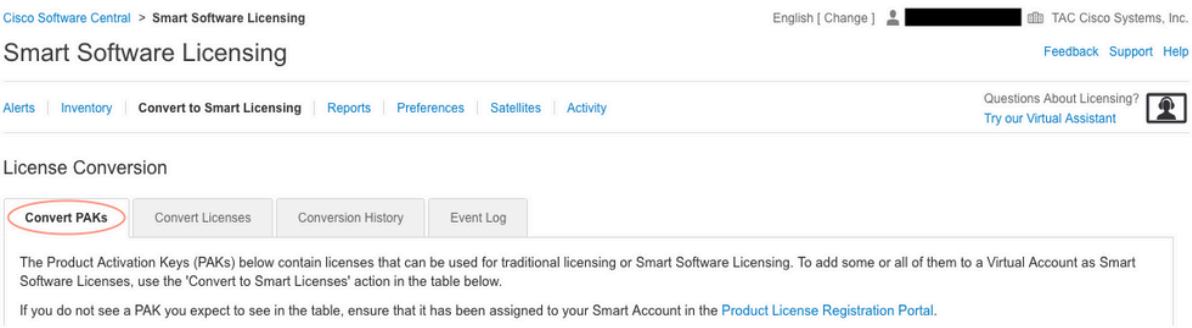
- DLC(Device Led Conversion)는 Cisco 제품이 어떤 라이센스를 사용하는지 보고할 수 있으며, 라이센스가 CSSM(Cisco Smart Software Manager)의 해당 Smart Account에 자동으로 저장되는 일회성 방법입니다. DLC 절차는 특정 Cisco 디바이스의 CLI(Command Line Interface)에서 직접 수행됩니다.
- DLC 프로세스는 Catalyst 3650/3850 및 선택한 라우터 플랫폼에서만 지원됩니다. 특정 라우터 모델은 개별 플랫폼 컨피그레이션 가이드 및 릴리스 정보를 참조하십시오. 예: Fuji 16.9.x 릴리스를 실행 중인 Catalyst 3850의 DLC 절차



CSSM(Cisco Smart Software Manager) 또는 LRP(License Registration Portal)를 통한 변환

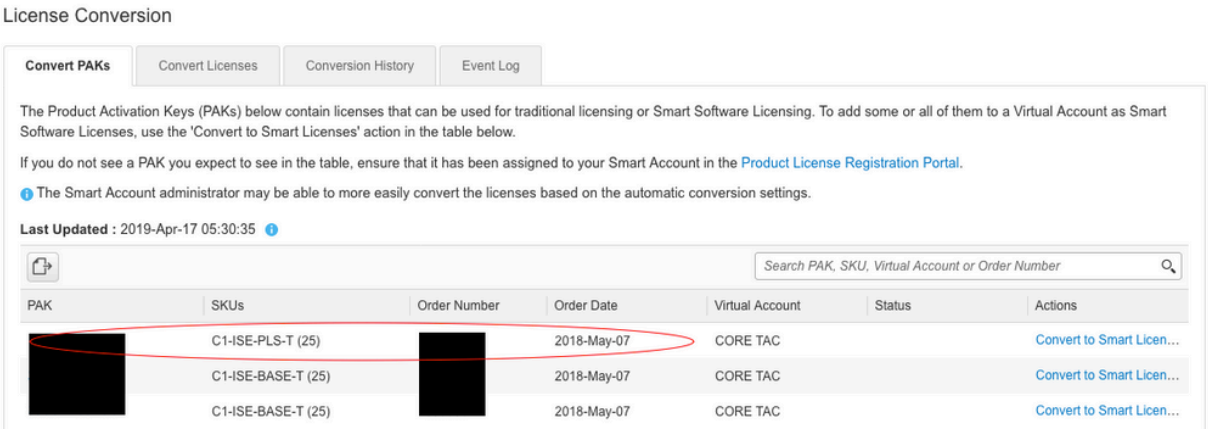
CSSM(Cisco Smart Software Manager) 방법:

1. CSSM(Cisco Smart Software Manager)에 로그인합니다(https://software.cisco.com/).
2. Smart Software 라이선싱으로 이동 > 스마트 라이선싱으로 변환
3. Convert PAK 또는 Convert Licenses를 선택합니다

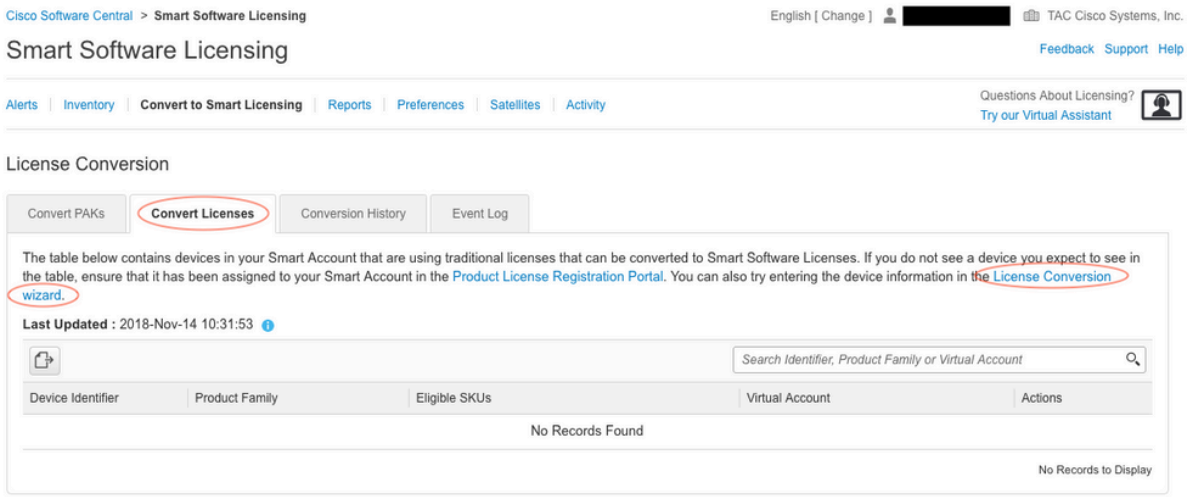


4. PAK 라이센스를 변환하려면 이 표에서 라이센스를 찾습니다. 비 PAK 라이센스를 변환하려면 단계별 지침에 라이센스 변환 마법사를 사용합니다.

어카운트와 관련된 알려진 PAK 파일의 위치:

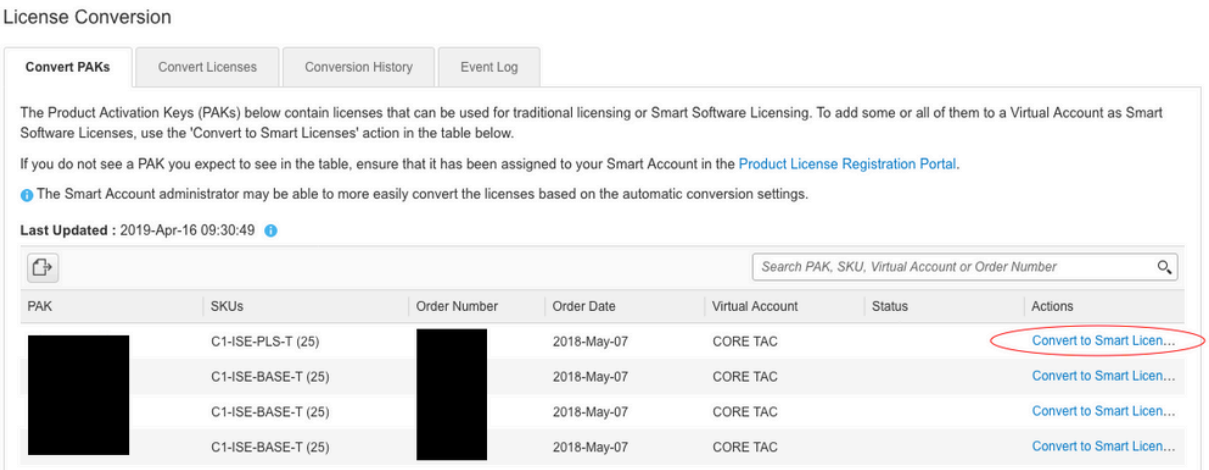


"라이선스 변환 마법사" 링크의 위치:

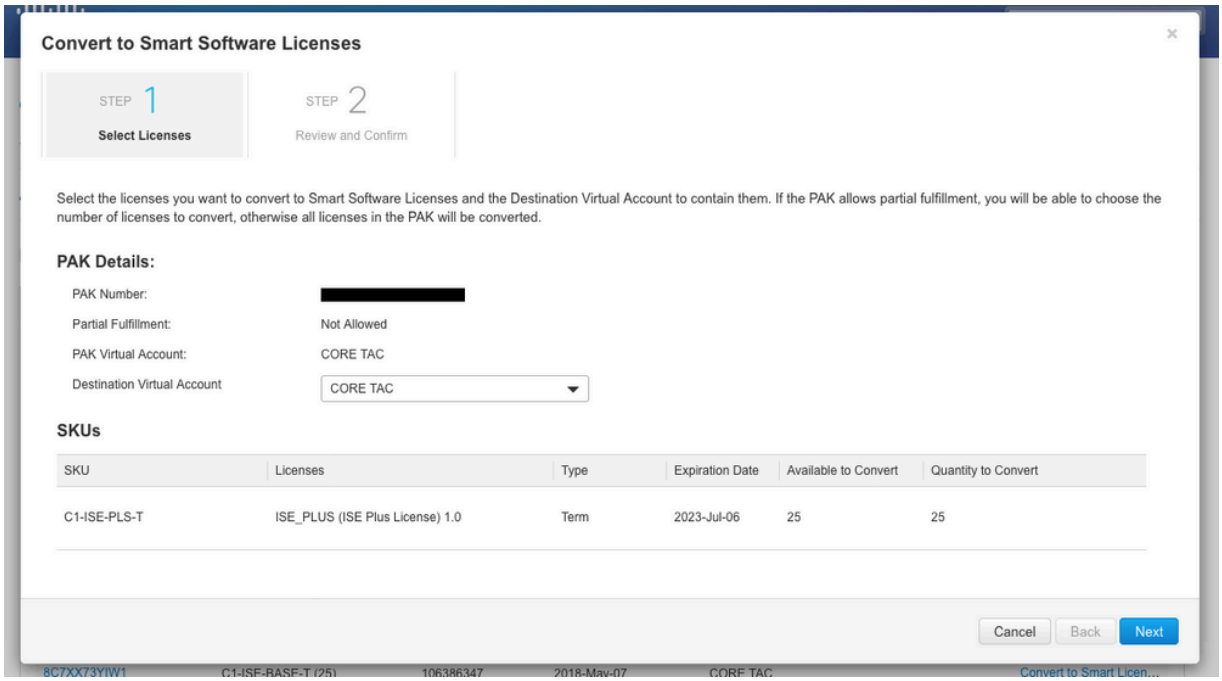


5. 원하는 라이선스 및 제품 조합 찾기.

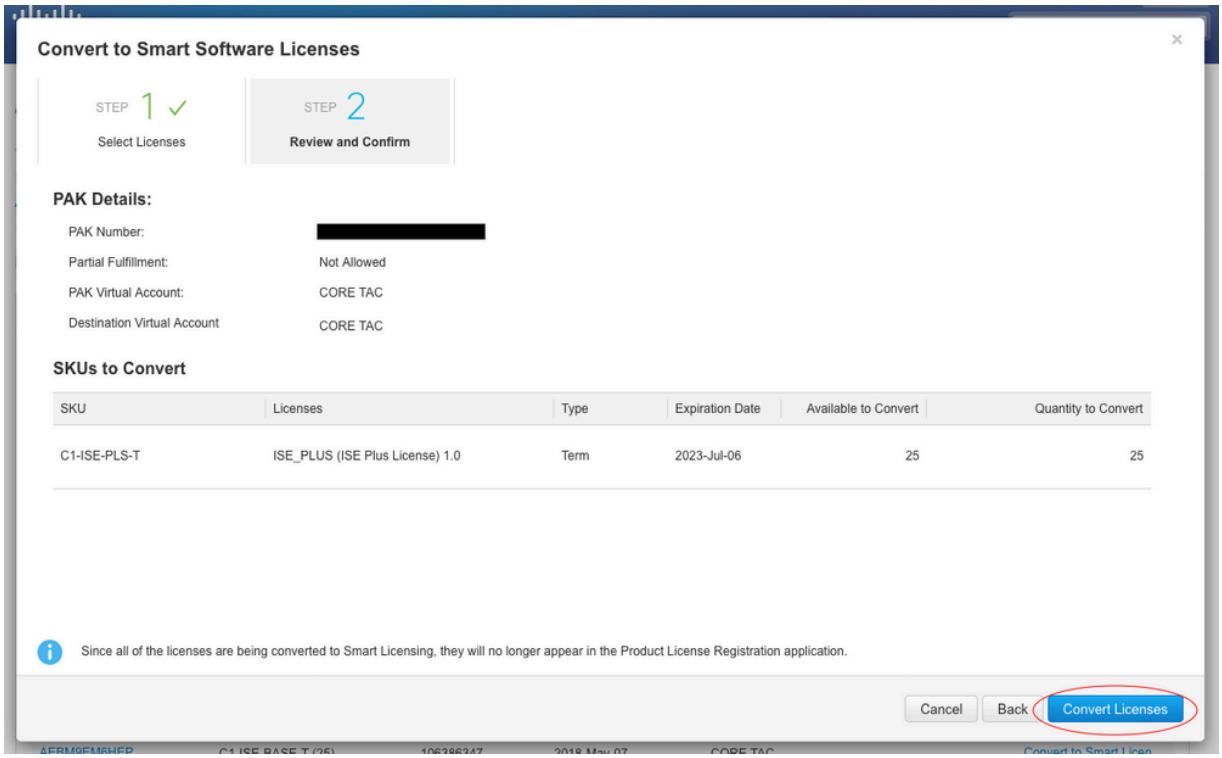
6. (Actions(작업) 아래의 Convert to Smart Licensing(Smart Licensing으로 변환)을 클릭합니다.



7. 가상 어카운트, 라이센스를 선택하고 다음을 클릭합니다.



8. 선택 사항을 검토한 다음 라이선스 변환 클릭.

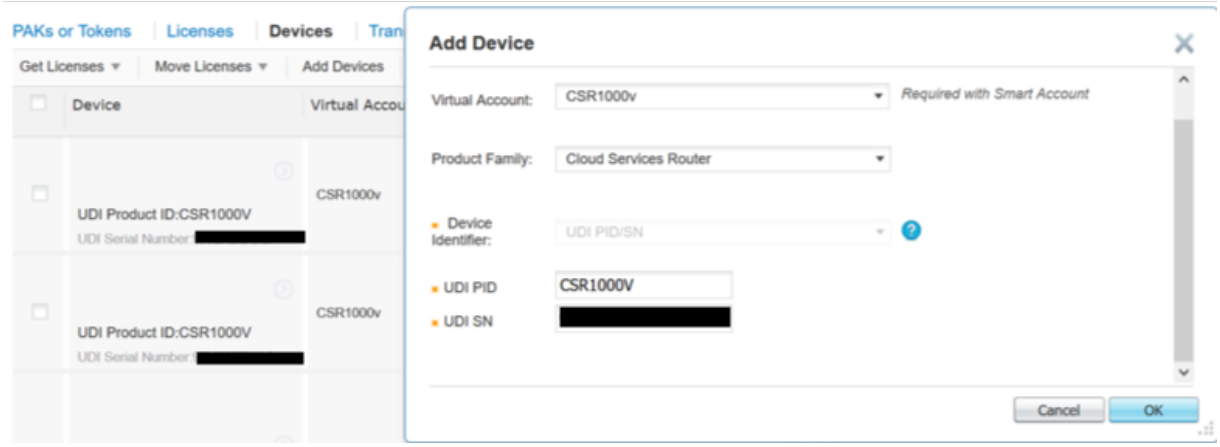


LRP(License Registration Portal) 방법:

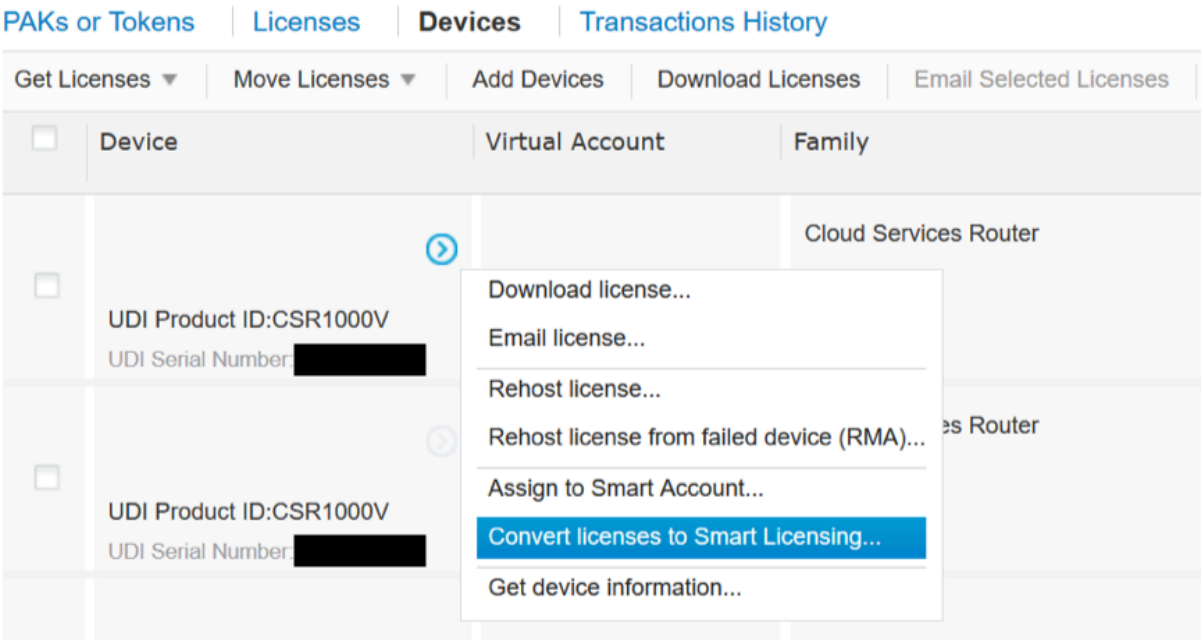
1. LRP(License Registration Portal)에 로그인합니다.
http://tools.cisco.com/SWIFT/LicensingUI/Home

2. 디바이스로 이동 > 디바이스 추가.

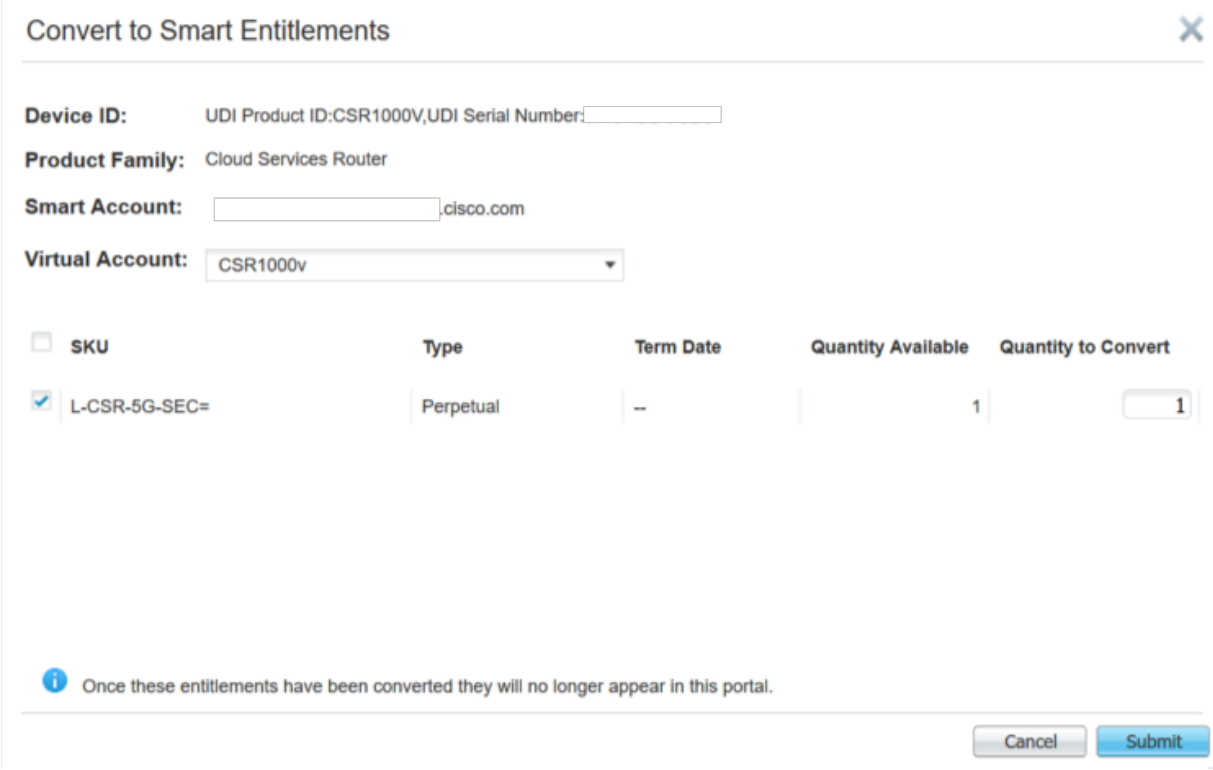
3. 적절한 제품군 및 UDI(고유 장치 식별자) 제품 ID와 일련 번호를 입력한 다음 확인을 클릭합니다. UDI 정보는 Cisco 디바이스의 CLI(Command Line Interface)에서 가져온 show version 또는 show inventory에서 얻을 수 있습니다.



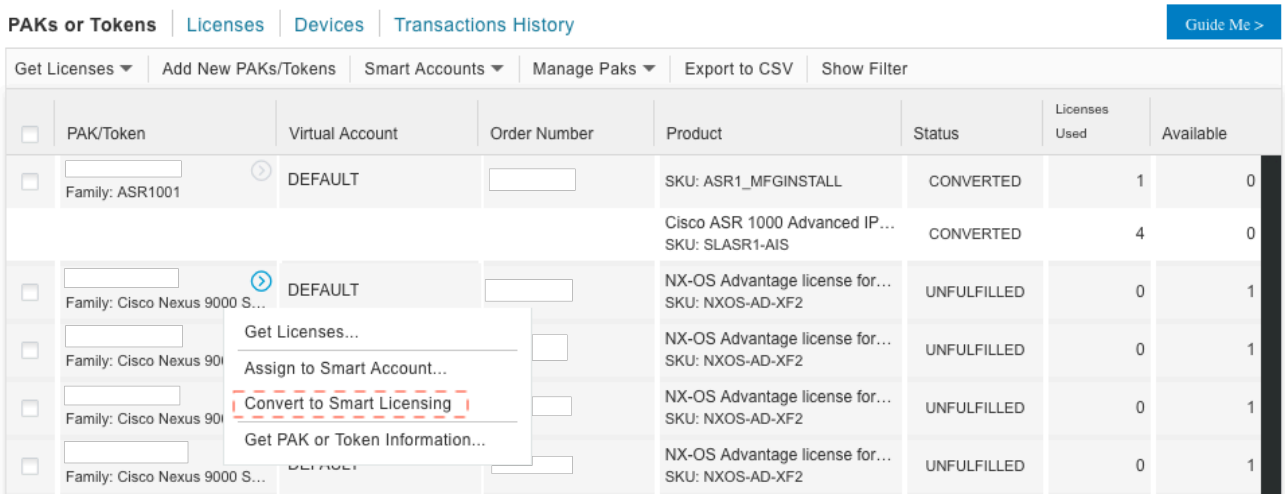
4. 추가된 디바이스를 선택하고 라이선스를 스마트 라이선싱으로 변환



5. 적절한 Virtual Account에 할당한 후 변환할 라이센스를 선택하고 Submit(제출)을 클릭합니다.



팁: PAKs 또는 Tokens(토큰) 탭에서 라이센스/제품군을 조회하여 LRP 툴을 사용할 수도 있습니다. PAK/Token 옆에 있는 원 드롭다운을 클릭하고 Convert to Smart Licensing을 선택합니다.



Cisco GLO(Global Licensing Operations) 부서에 전환 및 문의

Global Licensing Operations 부서는 전 세계 컨택 센터의 이곳으로 문의할 수 있습니다.

16.9에서 16.12.3으로 Catalyst 9500 고성능 동작 변화

다른 Catalyst 9000 모델과 마찬가지로 Catalyst 9500 고성능 모델은 Cisco IOS XE 버전 16.9 이상의 Smart Licensing에서 활성화되었습니다. 그러나 Catalyst 9500 고성능 모델의 경우 각 모델에는 고유한 라이선스 엔타이틀먼트 태그가 있습니다. C9500 플랫폼 엔타이틀먼트 태그는 나중에 제품 및 마케팅 팀에서 통합하기로 결정했습니다. 이 결정으로 C9500 고성능 모델의 동작이 특정 엔타이틀먼트 태그 사용에서 일반 C9500 라이선스로 변경되었습니다.

이러한 행동 변화는 다음과 같은 결함에 기록되어 있습니다.

a) Cisco 버그 ID CSCvp30661

b) Cisco 버그 ID CSCvt01955

C9500 High Performance 모델에 대한 위의 변경 라이센스 변경 전후의 변경 사항은 다음과 같습니다.

Cisco IOS XE 버전 16.11.x 이전

각 C9600 High Performance 모델에는 고유한 자격 태그가 있습니다.

모델	라이선스
C9500-32C	C9500 32C NW Essentials C9500 32C NW Advantage C9500 32C DNA Essentials C9500 32C DNA Advantage
C9500-32QC	C9500 32QC NW Essentials C9500 32C NW Advantage C9500 32C DNA Essentials C9500 32QC DNA Advantage
C9500-24Y4C	C9500 24Y4C NW Essentials C9500 24Y4C NW Advantage C9500 24Y4C DNA Essentials C9500 24Y4C DNA Advantage
C9500-48Y4C	C9500 48Y4C NW Essentials C9500 48Y4C NW Advantage C9500 48Y4C DNA Essentials C9500 48Y4C DNA Advantage

참고: Cisco IOS XE 버전 16.12.1 및 16.12.2에는 Cisco 버그 ID CSCvp30661 및 Cisco 버그 ID CSCvt01955에 결함이 있습니다. 이러한 결함은 16.12.3a 이상에서 해결됩니다.

Cisco IOS XE 버전 16.12.3 이상

Catalyst 9500 High Performance 플랫폼은 이제 일반 네트워크 라이센스 태그와 별도의 DNA 라이센스 태그를 사용합니다. 다음 표는 Cisco IOS XE 버전 16.12.3 이상에서 강조 표시된 자격 변경 사항을 보여줍니다.

모델	라이선스
C9500-32C	C9500 Network Essentials C9500 Network Advantage C9500 32C DNA Essentials C9500 32C DNA Advantage
C9500-32QC	C9500 Network Essentials C9500 Network Advantage C9500 32C DNA Essentials C9500 32QC DNA Advantage
C9500-24Y4C	C9500 Network Essentials C9500 Network Advantage C9500 24Y4C DNA Essentials C9500 24Y4C DNA Advantage
C9500-48Y4C	C9500 Network Essentials C9500 Network Advantage C9500 48Y4C DNA Essentials C9500 48Y4C DNA Advantage

참고: Cisco IOS XE 버전 16.12.1 및 16.12.2에서 업그레이드하면 이 라이센스 동작이 표시됩

니다. Cisco IOS XE 버전 16.9.x, 16.10.x, 16.11.x에서 16.12.3으로 업그레이드하면 이전 라이센스 구성이 인식됩니다.

C9500 고성능 변경 FAQ

1. 장치가 장치별 네트워크 라이센스를 사용하고 있는데 Cisco에서 일반 네트워크 라이센스를 할당하는 이유는 무엇입니까?

일반 태그는 네트워크 디바이스에 적합한 엔타이틀먼트 태그이므로 제공됩니다. 따라서 특정 C9500 고성능 모델이 아니라 전체 Cat9500 플랫폼에서 엔타이틀먼트 태그를 사용할 수 있습니다. 디바이스별 라이선스 태그를 요청하는 16.12.3 이전 이미지는 라이선싱 계층 구조의 일반 라이선스에 해당하므로 일반 라이선스 태그를 준수합니다.

2. Smart Account에 두 개의 네트워크 태그가 표시되는 이유는 무엇입니까?

이 동작은 라이선싱 계층 구조로 인해 발생하며 디바이스별 라이선싱 태그를 사용하는 이전 이미지에서 디바이스를 실행할 때 발생합니다. 디바이스별 라이선스 태그를 요청하는 이전 이미지는 라이선스 계층 구조의 일반 라이선스에 포함되므로 더 구체적인 태그가 일반 라이선스 태그를 준수합니다.

설정

기본 설정

Smart Licensing 구성 방법에 대한 정확한 절차는 각 릴리스/플랫폼에 제공되는 시스템 관리 컨피그레이션 가이드에서 확인할 수 있습니다.

예: 시스템 관리 설정가이드, Cisco IOS XE Fuji 16.9.x(Catalyst 9300 Switches)

등록 토큰/디바이스 ID 토큰

디바이스를 등록하기 전에 토큰을 생성해야 합니다. 디바이스 ID 토큰이라고도 하는 등록 토큰은 Cisco 디바이스를 처음 해당 스마트 어카운트에 등록할 때 스마트 라이센싱 포털 또는 Cisco Smart Software Manager 온프레미스에서 생성되는 고유한 토큰입니다. 개별 토큰을 사용하여 생성 중에 사용된 매개변수에 따라 여러 Cisco 디바이스를 등록할 수 있습니다.

등록 토큰은 Cisco 디바이스를 Cisco 백엔드로 call-home하고 올바른 스마트 어카운트에 연결하기 위해 디바이스에 정보를 제공하므로 Cisco 디바이스를 처음 등록하는 동안에만 필요합니다. Cisco 디바이스가 등록된 후에는 더 이상 토큰이 필요하지 않습니다.

등록 토큰 및 생성 방법에 대한 자세한 내용은 여기를 클릭하여 일반 가이드를 참조하십시오. 자세한 내용은 특정 Cisco 디바이스의 설정 가이드를 참조하십시오.

등록 및 라이선스 상태

Smart Licensing을 구축하고 구성하는 동안 Cisco 디바이스가 포함될 수 있는 상태는 여러 가지입

니다. Cisco 디바이스의 CLI(Command Line Interface)에서 show license all 또는 show license status를 확인하여 이러한 상태를 표시할 수 있습니다.

다음은 모든 상태의 목록 및 설명 입니다.

평가(미확인) 상태

- 평가는 처음 부팅할 때 디바이스의 기본 상태입니다.
- 일반적으로 이 상태는 Cisco 디바이스가 아직 Smart Licensing에 대해 구성되지 않았거나 Smart Account에 등록되지 않은 경우에 나타납니다.
- 이 상태에서는 모든 기능을 사용할 수 있으며, 디바이스는 라이센스 레벨을 자유롭게 변경할 수 있습니다.
- 평가 기간은 디바이스가 미확인 상태일 때 사용됩니다. 디바이스는 이 상태에서 Cisco와 통신을 시도하지 않습니다.
- 이 평가 기간은 90일 사용이며 90일이 아닙니다. 평가 기간이 만료되면 재설정되지 않습니다.
- 전체 디바이스에 대해 하나의 평가 기간이 있으며, 엔타이틀먼트 당 하나의 평가 기간이 아닙니다.
- 평가 기간이 90일의 끝에 만료되면 장치는 EVAL EXPIRY 모드로 전환됩니다. 그러나 다시 로드한 후에도 기능에 영향을 주거나 기능을 방해하지 않습니다. 현재 시행은 이루어지지 않고 있습니다.
- 카운트다운 시간은 재부팅 시 유지됩니다.
- 평가 기간은 디바이스가 아직 Cisco에 등록되지 않았고 Cisco 백엔드에서 다음 두 메시지를 수신하지 않은 경우 사용됩니다.
    1. 등록 요청에 대한 성공적인 응답.
    2. 엔타이틀먼트 권한 부여 요청에 성공적으로 응답했습니다.

등록된 상태

- Registered는 등록이 성공적으로 완료된 후 예상되는 상태입니다.
- 이 상태는 Cisco 디바이스가 Cisco Smart Account와 성공적으로 통신하고 등록했음을 나타냅니다.
- 디바이스는 향후 통신에 사용되는 1년 유효 ID 인증서를 받습니다.
- 디바이스에서 사용 중인 라이센스에 대한 엔타이틀먼트를 인증하도록 CSSM에 요청을 보냅니다.
- CSSM 응답에 따라 디바이스는 Authorized(승인됨) 또는 Out of Compliance(컴플라이언스 위반) 상태로 전환됩니다.
- ID 인증서는 1년 말에 만료됩니다. 6개월 후 소프트웨어 에이전트 프로세스에서 인증서를 갱신하려고 시도합니다. 에이전트가 CSSM과 통신할 수 없는 경우 만료 날짜(1년)까지 ID 인증서를 계속 갱신합니다. 1년이 지나면 상담원은 비식별 상태로 되돌아가 평가 기간을 활성화하려고 시도합니다. CSSM은 데이터베이스에서 제품 인스턴스를 제거합니다.

- 권한 부여된 상태
- Authorized(권한 부여됨)는 디바이스가 엔타이틀먼트를 사용하고 있고 규정 준수 상태일 때의 예상 상태입니다(음수 잔액 없음).
- 이 상태는 CSSM의 Virtual Account가 이 디바이스에 대한 라이센스 사용을 승인하는 데 필요한 올바른 유형 및 라이센스 수를 가지고 있음을 나타냅니다.
- 30일이 지나면 디바이스가 CSSM에 새 요청을 보내 권한 부여를 갱신합니다.

- 이 상태의 기간은 90일입니다. 90일 후(성공적으로 갱신되지 않은 경우) 디바이스가 Authorization Expired 상태로 전환됩니다.

규정 준수 위반

- Out of Compliance는 디바이스가 엔타이틀먼트를 사용 중이고 컴플라이언스 상태가 아닌 상태입니다(마이너스 잔액).
- 이 상태는 Cisco 디바이스가 Cisco 스마트 어카운트에 등록된 해당 가상 어카운트에서 디바이스에 사용 가능한 라이선스가 없는 경우 표시됩니다.
- Compliance/Authorized(컴플라이언스/권한 부여) 상태로 들어가려면 올바른 라이센스 수 및 유형을 Smart Account에 추가해야 합니다.
- 디바이스가 Out of Compliance 상태에 있으면 매일 자동으로 권한 부여 갱신 요청을 보냅니다.
- 라이센스와 기능은 계속 작동하며 기능에는 영향을 미치지 않습니다.

권한 부여 만료 상태

- Authorization Expired(권한 부여 만료됨)는 디바이스가 자격을 사용 중이며 90일 이상 연결된 Cisco Smart Account와 통신할 수 없는 상태입니다.
- 이 상태는 일반적으로 Cisco 장치가 인터넷 액세스를 잃거나 초기 등록 후 tools.cisco.com에 연결할 수 없는 경우에 나타납니다.
- 스마트 라이선싱의 온라인 방법을 사용하려면 Cisco 디바이스에서 이 상태를 방지하기 위해 최소 90일마다 통신해야 합니다.
- CSSM은 90일 동안 디바이스와 통신하지 않았으므로 이 디바이스에 대해 사용 중인 모든 라이센스를 풀로 다시 반환합니다.
- 이 상태에서 디바이스는 등록 기간(ID 인증서)이 만료될 때까지 권한 부여 갱신을 위해 매시간 Cisco에 연락을 시도합니다.
- 소프트웨어 에이전트는 Cisco와의 통신을 재설정하고 권한 부여 요청을 받은 경우 정상적으로 회신하는 절차를 거쳐 설정된 상태 중 하나로 들어갑니다.

고려 사항 및 주의 사항

스위치의 경우 16.9.1, 라우터의 경우 16.10.1부터 CiscoTAC-1이라는 기본 Call-Home 프로필이 생성되어 Smart Licensing으로의 마이그레이션을 지원합니다. 기본적으로 이 프로파일은 Direct Cloud Access 방법에 대해 설정됩니다.

<#root>

#show call-home profile CiscoTAC-1

```
Profile Name: CiscoTAC-1
Profile status: ACTIVE
Profile mode: Full Reporting
Reporting Data: Smart Call Home, Smart Licensing
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: http
HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Other address(es): default
<snip>
```

Cisco Smart Software Manager 온프레미스 서버를 사용하는 경우 활성 Call-Home 설정의 대상 주소가 해당 주소를 가리켜야 합니다.(대/소문자 구분).

<#root>

```
(config)#call-home
(cfg-call-home)#profile "CiscoTAC-1"
(cfg-call-home-profile)#destination address http https://
```

<IP/FQDN>

```
/Transportgateway/services/DeviceRequestHandler
```

Tools.cisco.com을 확인하려면 DNS가 필요합니다. DNS 서버 연결이 VRF에 있는 경우 적절한 소스 인터페이스 및 VRF가 정의되어 있는지 확인합니다.

```
Global Routing Table Used:
(config)#ip domain-lookup [source-interface <INTERFACE>]
(config)#ip name-server <IP>

VRF Routing Table Used:
(config)#ip domain-lookup [source-interface <INTERFACE>]     <<-- "ip vrf forwarding <VRF-NAME>" define
(config)#ip name-server vrf <VRF-NAME> <SERVER-IP>
```

또는 DNS를 사용할 수 없는 경우 로컬 DNS-IP 매핑을 정적으로 구성하거나(최종 장치의 로컬 DNS 확인 기준) call-home 컨피그레이션의 DNS 이름을 IP 주소로 교체합니다. 직접 클라우드 액세스는 예를 참조하십시오(Cisco Smart Software Manager 온프레미스의 경우 tools.cisco.com 대신 고유한 DNS 이름 사용).

```
(config)#ip host tools.cisco.com <x.x.x.x>
```

tools.cisco.com에 대한 통신을 특정 VRF(예: Mgmt-vrf)의 인터페이스에서 시작해야 하는 경우 이 CLI를 구성해야 합니다.

```
(config)#ip http client source-interface <VRF_INTERFACE>
```

StackWise 또는 StackWise Virtual에서 실행되는 Catalyst 스위치와 같이 Cisco 디바이스의 컨피그레이션에 따라 서로 다른 수의 라이센스를 사용할 수 있습니다.

기존 스택 방식 지원 스위치(예: Catalyst 9300 Series):

네트워크 라이센스: 스택에서 스위치당 1개의 라이센스가 소비됨

DNA 라이센스: 스택에서 스위치당 1개의 라이센스가 소비됨

모듈형 섀시(예: Catalyst 9400 Series):

네트워크 라이센스: 섀시의 수퍼바이저당 라이센스 1개가 소비됨

DNA 라이센스: 섀시당 1개의 라이센스가 사용됨

고정 스택 방식의 가상 지원 스위치(예: Catalyst 9500 Series):

네트워크 라이센스: 스택에서 스위치당 1개의 라이센스가 소비됨

DNA 라이센스: 스택에서 스위치당 1개의 라이센스가 소비됨

- Smart Licensing에 대해 하나의 call-home 프로파일만 활성화할 수 있습니다.
- 라이선스는 해당 기능이 구성된 경우에만 사용됩니다.
- Smart Licensing용으로 구성된 Cisco 디바이스는 해당 Cisco Smart Account와 올바르게 동기화되도록 올바른 시스템 시간 및 날짜로 구성해야 합니다. Cisco 디바이스의 시간 오프셋이 너무 멀면 디바이스를 등록하지 못할 수 있습니다. 시계는 NTP(Network Time Protocol) 또는 PTP(Precision Time Protocol)와 같은 타이밍 프로토콜을 통해 수동으로 설정 또는 구성해야 합니다. 이러한 변경 사항을 구현하는 데 필요한 정확한 단계는 특정 Cisco 디바이스의 컨피그레이션 가이드를 참조하십시오.
- Cisco 디바이스 등록 중에 생성된 PKI(Public Key Infrastructure) 키는 등록 후 자동으로 저장되지 않는 경우 저장해야 합니다. 디바이스에서 PKI 키를 저장하지 못하면 copy running-config startup-config 또는 write memory 명령을 통해 컨피그레이션을 저장하라는 메시지를 표시하는 syslog가 생성됩니다.
- Cisco 디바이스의 PKI 키가 제대로 저장되지 않으면 장애 조치 또는 재로드 시 라이선스 상태가 손실될 수 있습니다.
- Smart Licensing은 HTTPS 프록시 방법에 서드파티 프록시를 사용할 때 기본적으로 HTTPS 프록시 SSL 인증서 가로채기를 지원하지 않습니다. 이 기능을 지원하려면 프록시에서 SSL 인터셉를 비활성화하거나 프록시에서 전송한 인증서를 수동으로 가져올 수 있습니다.

<#root>

How to Manually Import Certification as a TrustPoint:

```
The certificate will need be in a BASE64 format to be copied and pasted onto the device as a TrustPoint

The following example shown below uses "LicRoot" as the TrustPoint name, however, this name can be chan

Device#conf t
Device(config)#crypto pki trustpoint LicRoot
Device(ca-trustpoint)#enrollment terminal
Device(ca-trustpoint)#revocation-check none
Device(ca-trustpoint)#exit
Device(config)#crypto pki authenticate LicRoot
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
Certificate has the following attributes:
     Fingerprint MD5: XXXXXXXX
   Fingerprint SHA1: XXXXXXX
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

전송 게이트웨이 HTTP 프록시를 사용하는 경우 다음 예와 같이 IP 주소를 tools.cisco.com에서 프록시로 변경해야 합니다.

대상 주소 http https://tools.cisco.com/its/service/oddce/services/DDCEService

수신

대상 주소 http https://<TransportGW-IP_Address>:<port_number>/Transportgateway/services/DeviceRequestHandler

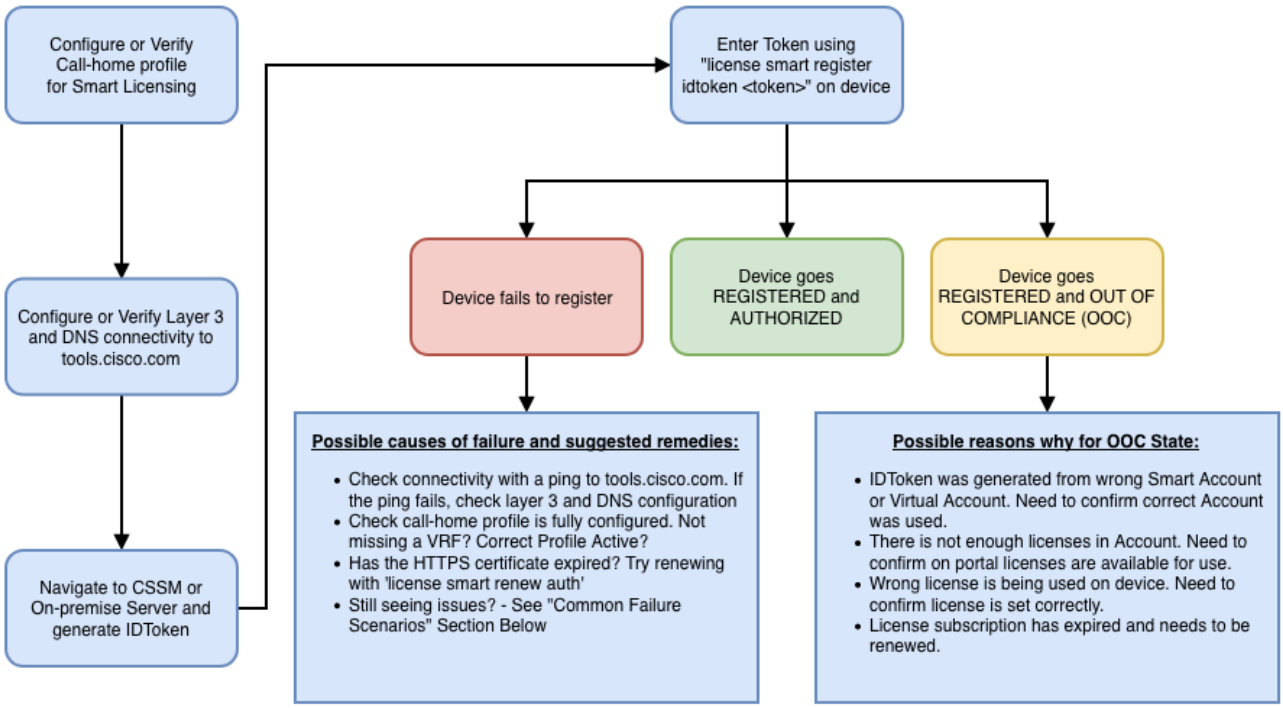
전송 게이트웨이 IP 주소는 HTTP 설정으로 이동하여 Cisco Transport Gateway GUI의 HTTP Service URL(HTTP 서비스 URL) 아래에서 확인할 수 있습니다.

자세한 내용은 여기서 Cisco Transport Gateway의 컨피그레이션 가이드를 참조하십시오.

문제 해결

Cisco 디바이스를 Smart Licensing 지원 소프트웨어 버전으로 마이그레이션할 때 이 순서도를 세 가지 방법(Direct Cloud Access, HTTPS Proxy, Cisco Smart Software Manager On-prem) 모두에 대한 일반 설명서로 사용할 수 있습니다.

디바이스가 업그레이드되거나 Smart Licensing을 지원하는 소프트웨어 릴리스와 함께 제공됨(지원되는 Cisco IOS XE 릴리스 목록은 섹션 1.3 참조)



이러한 트러블슈팅 단계는 주로 디바이스가 등록되지 않는 시나리오를 중점적으로 다룹니다.

디바이스 등록 실패

초기 설정 후 스마트 라이선싱을 활성화하려면 CSSM/Cisco Smart Software Manager 온프레미스에서 생성되는 토큰을 CLI를 통해 디바이스에 등록해야 합니다.

```
license smart register idtoken <TOKEN>
```

이 작업은 다음 이벤트를 생성합니다.

```
<#root>
! Smart licensing process starts

!

Registration process is in progress. Use the 'show license status' command to check the progress and re

!

! Crypto key is automatically generated for HTTPS communication

!

Generating 2048 bit RSA keys, keys will be exportable... [OK] (elapsed time was 1 seconds)
%CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or imported by crypto-engine
%PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write memory" to save new IOS PKI configur

!

! Call-home start registration process

!

%CALL_HOME-6-SCH_REGISTRATION_IN_PROGRESS: SCH device registration is in progress. Call-home will poll

!

! Smart Licensing process connects with CSSM and check entitlement.

!
```

```
%SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed
%SMART_LIC-6-AGENT_REG_SUCCESS: Smart Agent for Licensing Registration with the Cisco Smart Software Ma
%SMART_LIC-4-CONFIG_NOT_SAVED: Smart Licensing configuration has not been saved

%SMART_LIC-5-IN_COMPLIANCE: All entitlements and licenses in use on this device are authorized

%SMART_LIC-6-AUTH_RENEW_SUCCESS: Authorization renewal with the Cisco Smart Software Manager or satelli
```

Call-home 컨피그레이션을 확인하려면 다음 CLI를 실행합니다.

<#root>

```
#show call-home profile all


Profile Name: CiscoTAC-1

    Profile status: ACTIVE

    Profile mode: Full Reporting


Reporting Data: Smart Call Home, Smart Licensing

    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes


Transport Method: http
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Other address(es): default

    Periodic configuration info message is scheduled every 1 day of the month at 09:15

    Periodic inventory info message is scheduled every 1 day of the month at 09:00

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               warning
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    APF-.-WLC_.*              warning
    .*                        major
```

Smart Licensing 상태를 확인하려면 다음 CLI를 실행합니다.

<#root>

```
#show license summary

Smart Licensing is ENABLED
```

```
Registration:


Status: REGISTERED

  Smart Account: TAC Cisco Systems, Inc.
  Virtual Account: Krakow LAN-SW
  Export-Controlled Functionality: ALLOWED
  Last Renewal Attempt: None
  Next Renewal Attempt: Nov 22 21:24:32 2019 UTC

License Authorization:


Status: AUTHORIZED



Last Communication Attempt: SUCCEEDED


 Next Communication Attempt: Jun 25 21:24:37 2019 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  C9500 Network Advantage (C9500 Network Advantage)         1 AUTHORIZED
  C9500-DNA-40X-A         (C9500-40X DNA Advantage)         1 AUTHORIZED
```

디바이스 등록에 실패한 경우(및 상태가 REGISTERED(등록됨)와 다른 경우) 컴플라이언스 미준수는 스마트 가상 어카운트의 라이선스 누락, 잘못된 매핑(예: 다른 가상 어카운트의 토큰이 라이선스를 사용할 수 없는 경우) 등의 문제를 암시합니다. 다음 항목을 확인합니다:

1. 설정 및 일반적인 실패 시나리오 확인

기본 설정 단계는 섹션 2.1을 참조하십시오. 또한 현장에서 관찰되는 일반적인 장애 시나리오에 대해서는 섹션 5를 참조하십시오.

2. 기본 연결 확인

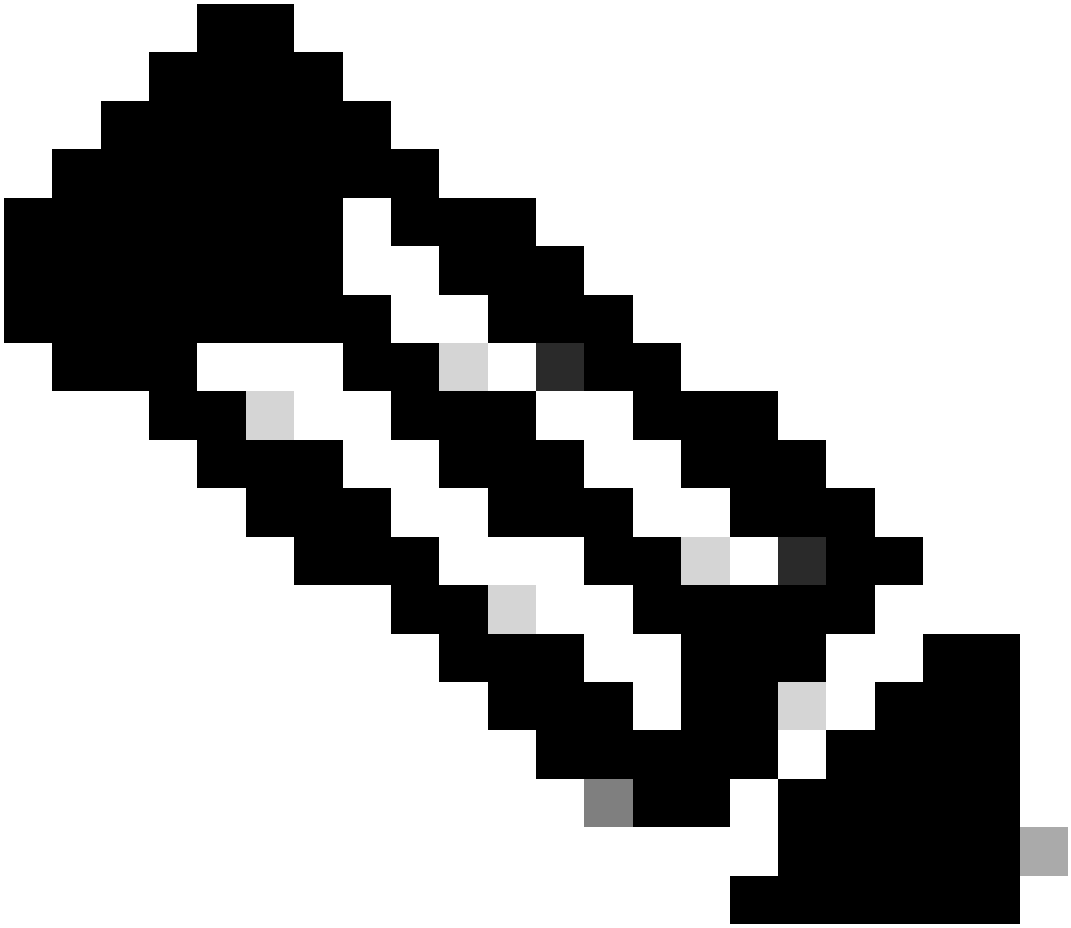
디바이스가 tools.cisco.com(직접 액세스의 경우) 또는 Cisco Smart Software Manager 온프레미스 서버에 연결(및 TCP 포트 열기)할 수 있는지 확인합니다.

<#root>

```
#show run all | in destination address http

  destination address http

https://tools.cisco.com

/its/service/oddce/services/DDCEService
!
! check connectivity
!

#telnet tools.cisco.com 443 /source-interface gi0/0

Trying tools.cisco.com (x.x.x.x, 443)... Open
```

```
[Connection to tools.cisco.com closed by foreign host]
```

이러한 명령이 작동하지 않을 경우 라우팅 규칙, 소스 인터페이스 및 방화벽 설정을 다시 확인하십시오.



> 참고: HTTP(TCP/80)는 더 이상 사용되지 않으며 권장 프로토콜은 HTTPS(TCP/443)입니다.

섹션 3을 참조하십시오. DNS 및 HTTP 세부사항을 구성하는 방법에 대한 추가 지침은 이 문서에서 고려해야 할 사항과 유의사항을 참조하십시오.

3. 스마트 라이선스 설정 확인

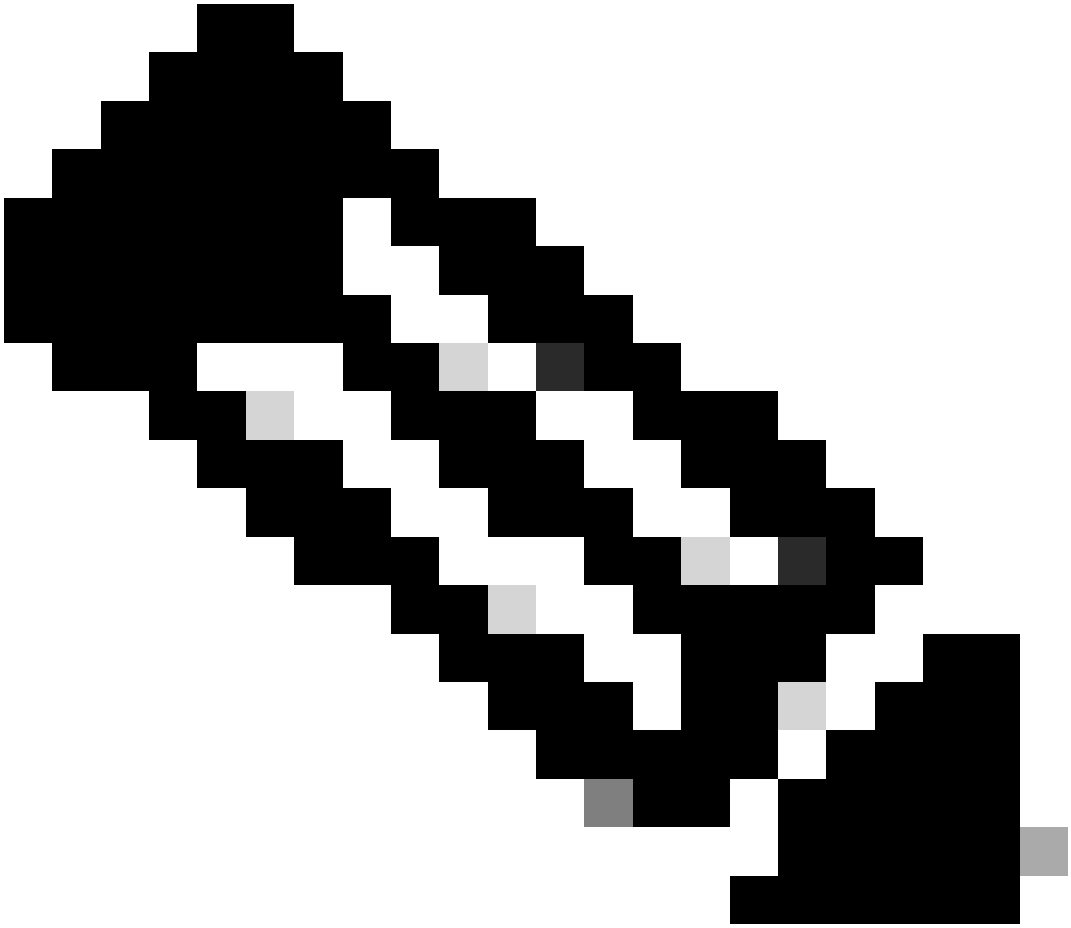
다음의 출력을 수집합니다.

```
#show tech-support license
```

및 수집된 설정/로그를 검증합니다(추가 조사를 위해 Cisco TAC 케이스를 열 경우 이 출력 첨부).

4. 디버그 활성화

이러한 디버그를 활성화하여 스마트 라이센싱 프로세스에 대한 추가 정보를 수집합니다.



> 참고: 디버그를 활성화한 후에는 4.1 지점에서 언급한 대로 CLi를 통해 라이센스를 다시 등록해야 합니다.

```
#debug call-home smart-licensing [all | trace | error]
#debug ip http client [all | api | cache | error | main | msg | socket]
```

내부 디버그의 경우 이진 추적을 활성화하고 읽습니다.

```
! enable debug
#set platform software trace ios [switch] active R0 infra-sl debug
!
! read binary traces infra-sl process logs
#show platform software trace message ios [switch] active R0
```

일반적인 실패 시나리오

이 섹션에서는 Cisco 디바이스 등록 도중 또는 이후에 발생할 수 있는 몇 가지 일반적인 장애 시나리오에 대해 설명합니다.

시나리오 #1: 스위치 등록 "Failure Reason: Product Already Registered"

"모든 라이선스 보기"의 일부:

등록:

상태: 등록되지 않음 - 등록 실패

내보내기 제어 기능: 허용되지 않음

초기 등록 실패: 10월 22일 14:25:31 2018 EST

실패 사유: 제품이 이미 등록되었습니다.

다음 등록 시도: 10월 22일 14:45:34 2018 EST

다음 단계:

- Cisco 디바이스를 다시 등록해야 합니다.

- CSSM에 Cisco 장치가 표시되는 경우 force 매개 변수를 사용해야 합니다(즉, license smart register idtoken <TOKEN> force).

참고: 실패 사유는 다음과 같이 표시될 수도 있습니다.
- 실패 사유: udiSerialNumber:<SerialNumber>,udiPid:<Product>이(가) 포함된 <X> 및 sudi가 이미 등록되었습니다.
- 실패 사유: 기존 제품 인스턴스에 소비량이 있으며 Force Flag가 False임

시나리오 #2: 스위치 등록 "실패 사유: 요청을 지금 처리할 수 없습니다. 다시 시도하여 주십시오"

"모든 라이선스 보기"의 일부:

등록:

상태: 등록 - 등록 진행 중

내보내기 제어 기능: 허용되지 않음

초기 등록 실패: 10월 24일 15:55:26 2018 EST

실패 이유: 요청을 지금 처리할 수 없습니다. 다시 시도하여 주십시오

다음 등록 시도: 10월 24일 16:12:15 2018 EST

다음 단계:

- 섹션 4에서 설명한 대로 디버그를 활성화하여 문제에 대한 더 많은 통찰력을 얻습니다.

- 스마트 라이선싱에서 CSSM으로 새 토큰을 생성하고 다시 시도하십시오.

시나리오 #3: 실패 사유 "디바이스 일자 15261352686533이 허용 한도 초과로 오프셋 되었습니다.

"모든 라이선스 보기"의 일부:

등록:

상태: 등록 - 등록 진행 중

내보내기 제어 기능: 허용되지 않음

초기 등록: 11월 1117:55:46 2018 EST 실패

실패 이유: {"timestamp":["The device date '1526135268653' is offset beyond the allowed tolerance limit."]}

다음 등록 시도: 11월 11일 18:12:17 2018 EST

가능한 로그 확인:

%PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: 인증서 체인 검증에 실패했습니다. 인증서(SN: XXXXXX)가 아직 유효하지 않습니다. 유효 기간은 2018-12-12:43Z에 시작됩니다.

다음 단계:

- Cisco 장치 시계가 올바른 시간(시계 표시)을 표시하는지 확인합니다.

- 가능한 경우 시계가 올바르게 설정되도록 NTP(Network Time Protocol)를 구성합니다.

- NTP를 사용할 수 없는 경우, 시계 달력 유효(calendar-valid)가 구성되어 있는지 확인하여 수동으로 설정된 시계(시계 집합)가 정확하고(시계 표시) 신뢰할 수 있는 시간 원본으로 구성되어 있는지 확인합니다

참고: 기본적으로 시스템 클럭은 신뢰되지 않습니다. 유효한 시계 달력은 필수입니다.

시나리오 #4: 스위치 등록 "실패 사유: 통신 전송을 사용할 수 없습니다."

"모든 라이선스 보기"의 일부:

등록: 상태: 등록되지 않음 - 등록 실패

내보내기 제어 기능: 허용되지 않음

Initial Registration(초기 등록): FAILED on Mar 09 21:42:02 2019 CST

실패 이유: 통신 전송을 사용할 수 없습니다.

가능한 로그 확인:

%CALL_HOME-3-CALL_HOME_FAILED_TO_ENABLE: Smart Agent for Licensing에서 Call-Home을 사용하도록 설정하지 못했습니다. 기존 활성 사용자 프로필로 인해 명령이 Smart Call-Home을 사용하도록 설정하지 못했습니다. CiscoTAC-1 프로필 이외의 사용자 프로필을 사용하여 Cisco의 SCH 서버로 데이터를 보내는 경우 프로필 모드에서 reporting smart-licensing-data를 입력하여 해당 프로필을 스마트 라이센싱에 맞게 구성합니다. SCH에 대한 자세한 내용은 http://www.cisco.com/go/smartcallhome을 참조하십시오.
%SMART_LIC-3-AGENT_REG_FAILED: Cisco Smart Software Manager 또는 Satellite에 대한 라이선스 등록용 Smart Agent 실패: 통신 전송을 사용할 수 없습니다.
%SMART_LIC-3-COMM_FAILED: Cisco Smart Software Manager 또는 위성 통신 실패: 통신 전송을 사용할 수 없습니다.

다음 단계:

- Cisco 디바이스의 show running-config 출력에서 call-home이 service call-home과 함께 활성화되었는지 확인합니다.

- 올바른 call-home 프로필이 활성화되었는지 확인합니다.

- 활성 call-home 프로필에 reporting smart-licensing-data가 구성되어 있는지 확인합니다.

시나리오 #5: 스위치 라이센스 권한 부여 "실패 사유: Call Home HTTP 메시지를 전송하지 못했습니다."

"모든 라이선스 보기"의 일부:

라이선스 인증:

상태: OUT OF COMPLIANCE ON Jul 26 09:24:09 2018 UTC

마지막 통신 시도: 8월 2일 14:26:23 2018 UTC에 실패

실패 이유: Call Home HTTP 메시지를 전송하지 못했습니다.

다음 통신 시도: 8월 2일 14:26:53 2018 UTC

커뮤니케이션 마감 날짜: 10월 25일 09:21:38 2018 UTC

가능한 로그가 표시됩니다.

%CALL_HOME-5-SL_MESSAGE_FAILED: Smart Licensing 메시지를 https://<ip>/its/service/oddce/services/DDCEService로 보내지 못했습니다(오류 205: 요청 중단됨).

%SMART_LIC-3-COMM_FAILED:Cisco Smart Software Manager 또는 Satellite와의 통신 실패: Call Home HTTP 메시지를 전송하지 못했습니다.

%SMART_LIC-3-AUTH_RENEW_FAILED: Cisco Smart Software Manager 또는 Satellite를 사용한 인증 갱신: 통신 메시지 udi PID 전송 오류: XXX, SN: XXX

다음 단계:

- Cisco 디바이스가 tools.cisco.com에 ping할 수 있는지 확인합니다.

- DNS가 구성되지 않은 경우 tools.cisco.com에 대한 로컬 nslookup IP에 대해 DNS 서버 또는 ip host 문을 구성합니다.

- TCP 포트 443(HTTPS에서 사용하는 포트)에서 Cisco 디바이스에서 tools.cisco.com으로 텔넷을 시도합니다.

- HTTPs 클라이언트 소스 인터페이스가 정의되어 있고 올바른지 확인합니다.

- show call-home profile all을 통해 콜 홈 프로필의 URL/IP가 Cisco 디바이스에서 올바르게 설정되었는지 확인합니다.

- ip 경로가 올바른 다음 홉을 가리키는지 확인합니다.

- TCP 포트 443이 Cisco 디바이스, Smart Call Home 서버 경로 또는 Cisco Smart Software Manager 온프레미스(위성)에서 차단되지 않도록 합니다.

- 해당되는 경우 call-home에서 올바른 VRF(Virtual Routing and Forwarding) 인스턴스가 구성되어 있는지 확인합니다.

시나리오 #6: 실패 이유 "Id 인증서 일련 번호 필드 누락; 서명 인증서 일련 번호 필드 누락; 서명된 데이터와 인증서가 일치하지 않음" 로그

이 동작은 Cisco 버그 ID CSCvr41393에 설명된 대로 암호화 인증서가 만료된 CSSM 온프레미스 서버에서 작업할 때 나타납니다. 이는 CSSM 온프레미스(on-prem)에서 인증서를 동기화하고 갱신할 수 있어야 등록 디바이스에서 인증서 동기화 문제를 방지할 수 있기 때문에 예상되는 동작입니다.

"모든 라이선스 보기"의 일부:

```
등록:
  상태: 등록되지 않음
  Smart Account: 예 어카운트
  내보내기 제어 기능: 허용됨
```

라이선스 인증:
상태: 평가 모드
남은 평가 기간: 65일, 18시간, 43분, 0초

가능한 로그 확인:

이 오류는 show logging 또는 show license eventlog 아래에 표시됩니다.
SAEVT_DEREGISTER_STATUS msgStatus="LS_INVALID_DATA" error="Missing Id cert serial number field; Missing signing cert serial number field; Signed data and certificate does does not match"

다음 단계:

- Cisco 디바이스가 CSSM 온프레미스 서버에 IP 연결되어 있는지 확인합니다.
- HTTPS를 사용하는 경우 디바이스 call-home 컨피그레이션에서 인증 C-Name이 사용되고 있는지 확인합니다.
- DNS 서버를 사용하여 인증 C-Name을 확인할 수 없는 경우, 도메인 이름과 IP 주소를 매핑하도록 고정 ip host 문을 구성합니다.

- CSSM 온프레미스 인증서의 상태가 여전히 유효한지 확인합니다.
- CSSM 온프레미스 인증서가 만료된 경우 Cisco 버그 ID CSCvr에 문서화된 해결 방법 중 하나를 사용합니다41393

참고: 기본적으로 HTTPS는 SSL 핸드셰이크 중에 서버 ID 검사를 수행하여 URL 또는 IP가 서버에서 제공한 인증서와 동일한지 확인합니다. 이로 인해 호스트 이름과 IP가 일치하지 않으면 DNS 항목 대신 IP 주소를 사용할 때 문제가 발생할 수 있습니다. DNS를 사용할 수 없거나 고정 ip host 문인 경우 이 인증 검사를 비활성화하도록 http secure server-identity-check를 구성할 수 없습니다.

시나리오 #7: 스위치 라이센스 권한 부여 "실패 사유: 응답 대기 중"

"모든 라이선스 보기"의 일부:

라이선스 인증:
상태: OUT OF COMPLIANCE ON Jul 26 09:24:09 2018 UTC
마지막 통신 시도: 8월 2일 14:34:51 2018 UTC
실패 사유: 회신 대기 중
다음 통신 시도: 8월 2일 14:53:58 2018 UTC
커뮤니케이션 마감 날짜: 10월 25일 09:21:39 2018 UTC

가능한 로그가 표시됩니다.

%PKI-3-CRL_FETCH_FAIL: 신뢰 지점 SLA-TrustPoint에 대한 CRL 가져오기 실패 이유: 소켓을 선택하지 못했습니다. 시간 초과: 5(연결 시간 초과)
%PKI-3-CRL_FETCH_FAIL: 신뢰 지점 SLA-TrustPoint에 대한 CRL 가져오기 실패 이유: 소켓을 선택하지 못했습니다. 시간 초과: 5(연결 시간 초과)

다음 단계:

- 이 문제를 해결하려면 실행 중인 컨피그레이션에서 SLA-TrustPoint를 none으로 구성해야 합니다

show running-config

<omitted>

crypto pki trustpoint SLA-TrustPoint

revocation-check 없음

CRL이란?

CRL(Certificate Revocation List)은 폐기된 인증서의 목록입니다. CRL은 처음에 인증서를 발급한 CA(인증 기관)에 의해 생성되고 디지털로 서명됩니다. CRL에는 각 인증서가 발급된 날짜 및 만료 날짜가 포함됩니다. CRL 관련 추가 정보는 여기에서 확인할 수 있습니다.

시나리오 #8: "OUT OF COMPLIANCE" 상태의 라이센스

"모든 라이선스 보기"의 일부:

라이선스 인증:
상태: OUT OF COMPLIANCE ON Jul 26 09:24:09 2018 UTC
마지막 통신 시도: 8월 2일 14:34:51 2018 UTC
실패 사유: 회신 대기 중
다음 통신 시도: 8월 2일 14:53:58 2018 UTC
커뮤니케이션 마감 날짜: 10월 25일 09:21:39 2018 UTC

가능한 로그가 표시됩니다.

%SMART_LIC-3-OUT_OF_COMPLIANCE: 하나 이상의 자격이 규정을 준수하지 않습니다.

다음 단계:

- 적절한 Smart Virtual Account의 토큰이 사용되었는지 확인합니다.

- 사용 가능한 라이선스의 양을 여기에서 확인합니다.

시나리오 #9: 스위치 라이센스 권한 부여 "실패 사유: 데이터와 서명이 일치하지 않음"

"모든 라이선스 보기"의 일부:

라이선스 인증:

상태: AUTHORIZED on 3월 12일 09:17:45 2020 EDT

마지막 통신 시도: 3월 12일 09:17:45 2020 EDT 실패

실패 이유: 데이터와 서명이 일치하지 않습니다.

다음 통신 시도: 3월 12일 09:18:15 2020 EDT

커뮤니케이션 마감 날짜: 5월 09일 21:22:43 2020 EDT

가능한 로그가 표시됩니다.

%SMART_LIC-3-AUTH_RENEW_FAILED: CSSM(Cisco Smart Software Manager)을 사용하여 권한 부여 갱신: Smart Software Manager에서 오류 수신: 데이터 및 서명이 udi PID에 대해 일치하지 않음: C9000,SN:XXXXXXXXXXXXX

다음 단계:

- License smart deregister를 사용하여 스위치를 등록 취소합니다.

- 그런 다음 라이센스 smart register idtoken <TOKEN> force를 사용하여 새 토큰을 사용하여 스위치를 등록합니다.

참조

1) Cisco 스마트 라이선싱 홈페이지

2) Cisco Community - 온디맨드 교육

3) 스마트 어카운트 - 관리 포털: 스마트 소프트웨어 라이선싱

4) 스마트 어카운트 - 새 어카운트 생성: 스마트 어카운트

5) 설정 가이드(예) - 시스템 관리 설정 가이드, Cisco IOS XE Fuji 16.9.x(Catalyst 9300 Switches)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.