

오프라인 Catalyst 9300X Series 스위치에서 SLP를 사용하여 HSEC 라이선스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[Smart Licensing 전송을 설정 해제합니다.](#)

[Trust ACK 요청 설치](#)

[Cisco SSM에 신뢰 요청 파일을 업로드하고 ACK 파일을 다운로드합니다.](#)

[CopyTrust ACK 파일](#)

[제품 인스턴스에 파일을 가져와 설치합니다.](#)

[모든 필수 정보가 포함된 Authorization Request를 설치합니다.](#)

[Cisco SSM에 권한 부여 요청 파일을 업로드하고 ACK 파일을 다운로드합니다.](#)

[CopyAuthorization RequestACK 파일](#)

[InstallAuthorization RequestACK 파일](#)

[다음을 확인합니다.](#)

소개

이 문서에서는 Offline Catalyst 9300X Series 스위치에서 SLP를 사용하여 HSEC 라이선스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SLP(Cisco Smart Licensing Using Policy) 개념 이해
- Cisco Catalyst 9300X Series 스위치 하드웨어 및 소프트웨어 관리 속지
- CSSM(Cisco Smart Software Manager)에서 라이선스 탐색 및 관리 경험
- Cisco IOS XE 디바이스에서 CLI 사용 가능
- Cisco DNA 라이선스 자격 유형 지식
- 디바이스 등록 및 라이선스 예약 절차

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 하드웨어: Cisco Catalyst C9300X-24Y
- 소프트웨어: Cisco IOS XE 17.12.04
- 스마트 라이선싱 인프라: CSSM(Cisco Smart Software Manager)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

HSEC(High-Security) 라이선스는 Cisco 플랫폼에서 고급 보안 기능을 활성화하여 네트워크 보호, 데이터 무결성 및 개인 정보를 강화합니다. 엄격한 보안 요구 사항을 준수하고 안전한 커뮤니케이션을 위한 강력한 툴을 제공합니다.

HSEC에서 지원하는 주요 기능은 다음과 같습니다.

- VPN 지원은 사이트 간 및 원격 액세스를 위해 IPsec 및 SSL VPN과 같은 공용 네트워크 전반에서 암호화된 보안 통신을 지원합니다.
- 암호화 기능은 기밀성, 무결성 및 인증을 보장하기 위해 AES 및 SHA를 비롯한 데이터 보호를 위한 강력한 암호화 알고리즘을 지원합니다.
- WAN MACsec은 WAN 링크 전반에 걸쳐 MACsec(Layer 2 Encryption) 기능을 확장하여 신뢰할 수 없는 네트워크에서 엔드 투 엔드 데이터 보안을 보장합니다.
- 확장성 개선 사항은 대규모 구축을 지원하기 위해 VPN 세션과 같은 암호화된 터널에 대한 더 높은 확장성의 잠금을 해제합니다.
- 보안 통신을 통해 FlexVPN 및 DMVPN과 같은 동적, 확장 가능한 보안 연결 기능을 사용할 수 있습니다.

구성

C9300X CLI를 사용하여 스마트 라이선싱을 구성합니다.

Smart Licensing 전송을 설정 해제합니다.

CLI 구성:

```
device#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
device(config)#license smart transport off
```

Trust ACK 요청 설치

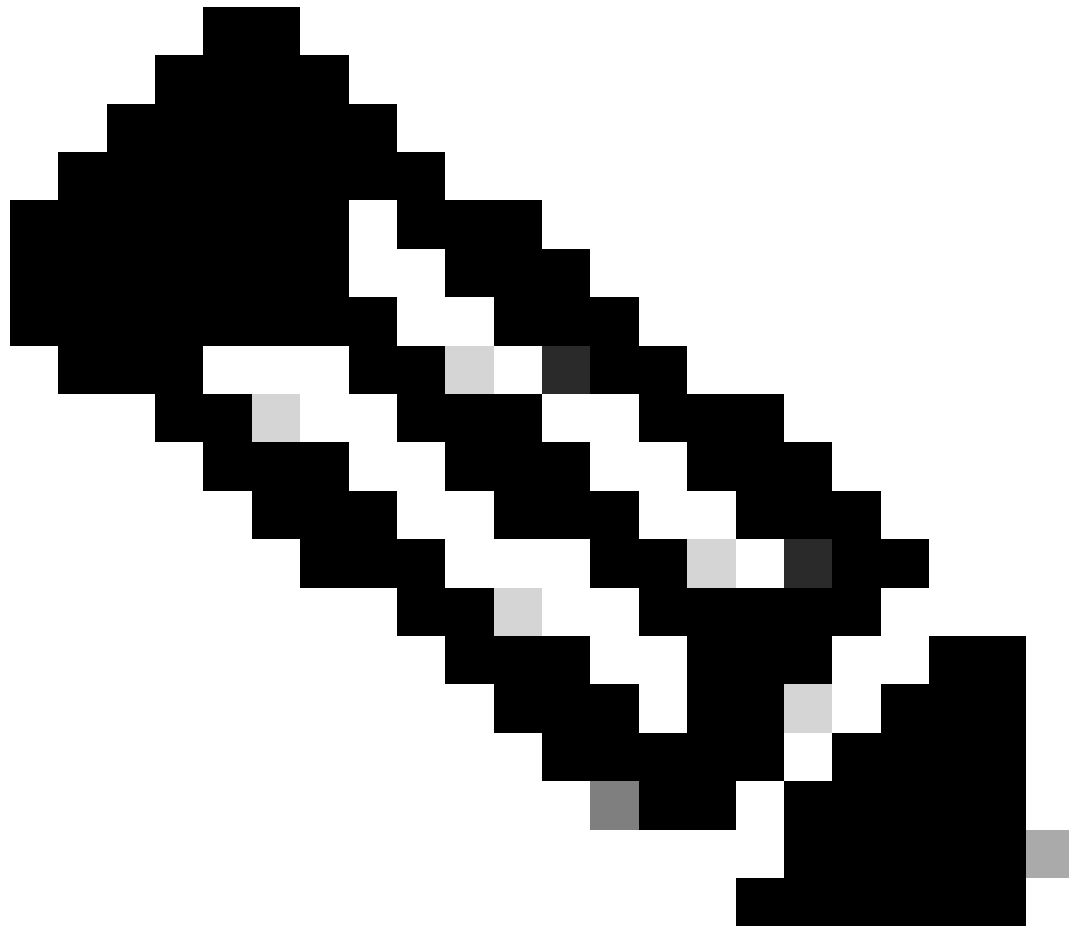
플래시의 활성 제품 인스턴스에 대한 신뢰 코드 요청을 생성하고 저장합니다.

CLI 구성:

```
device#license smart save trust-request flash:trust_request.txt
```

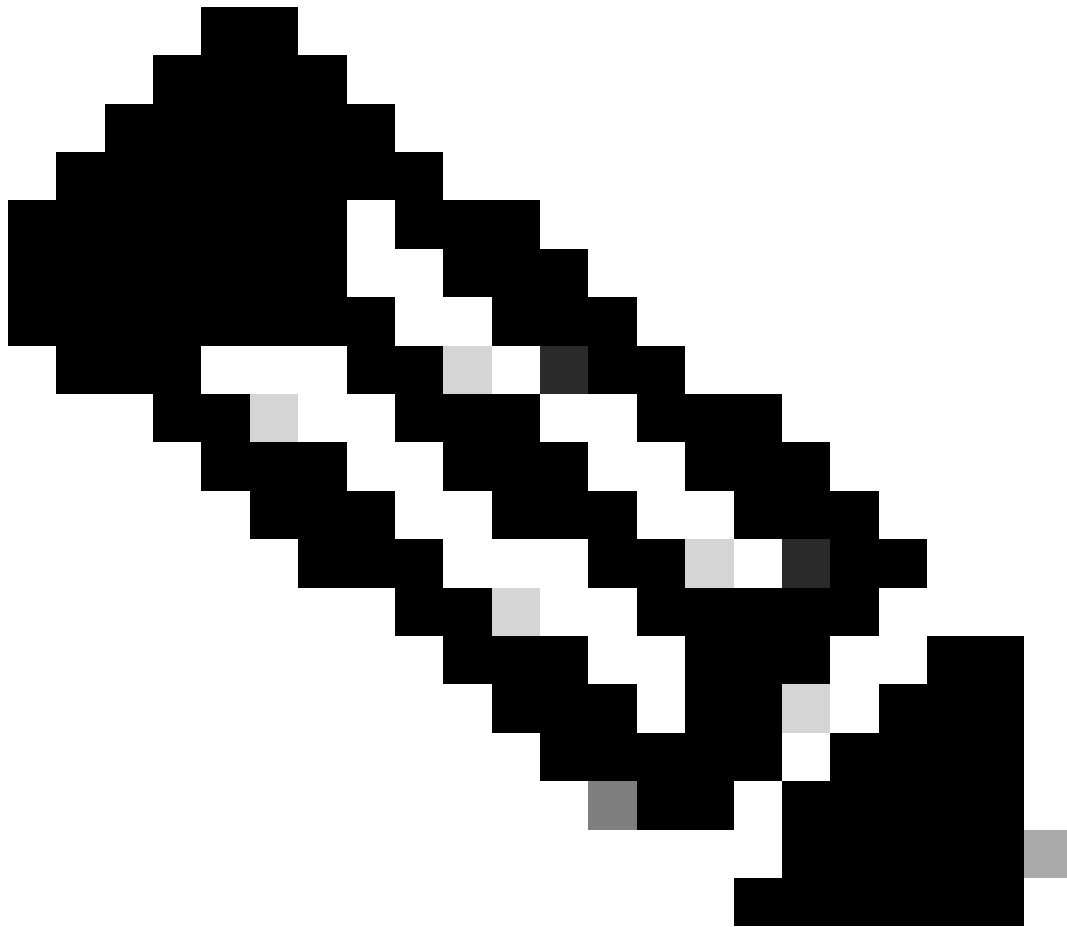
Cisco SSM에 신뢰 요청 파일을 업로드하고 ACK 파일을 다운로드합니다.

1. <https://software.cisco.com>에서 Cisco SSM 웹 UI에 [로그인합니다](#). Smart Software Licensing 아래에서 Manage licenses(라이선스 관리) 링크를 클릭합니다.
2. 보고서를 수신하는 Smart Account를 선택합니다.
3. Smart Software Licensing > Reports > Usage Data Files를 선택합니다.
4. CClick Upload Usage Data(사용량 데이터 업로드). 파일 위치(tar 형식의 RUM 보고서)를 찾은 다음 Upload Data(데이터 업로드)를 선택하고 CClick 업로드합니다.



참고: 파일을 업로드한 후에는 삭제할 수 없습니다. 그러나 필요한 경우 다른 파일을 업로드할 수 있습니다.

-
5. [가상 어카운트 선택] 팝업창에서 업로드된 파일을 받을 가상 어카운트를 선택합니다.
 6. 파일이 업로드되고 [보고서] 화면의 [사용 데이터 파일] 테이블에 나열됩니다. 표시되는 세부 정보에는 파일 이름, 보고 시간, 업로드된 가상 어카운트, 보고 상태, 보고된 제품 인스턴스 수, 승인 상태 등이 있습니다.
 7. Acknowledgement(확인 응답) 열에서 CClick Download(CClick 다운로드)를 클릭하여 보고서 또는 업로드한 요청의 ACK 파일을 저장합니다.



참고: Acknowledgement 열에 파일이 나타날 때까지 기다려야 합니다. RUM 보고서 또는 처리할 요청이 많은 경우 Cisco SSM은 몇 분 정도 소요되어야 합니다.

파일을 다운로드한 후 파일을 가져와 제품 인스턴스에 설치합니다

신뢰 ACK 파일 복사

소스 위치 또는 디렉토리에서 제품 인스턴스의 플래시 메모리로 파일을 복사합니다.

CLI 구성:

```
device#copy ftp: flash:
```

```
Address or name of remote host []? 192.168.1.1
```

```
Source filename []? ACK_trust_request.txt
```

```
Destination filename [ACK_trust_request.txt]?
```

Accessing ftp://192.168.1.1/ACK_ trust_request.txt...!

[OK - 5254/4096 bytes]

5254 bytes copied in 0.045 secs (116756 bytes/sec)

제품 인스턴스에 파일을 가져와 설치합니다.

CLI 구성:

```
device#license smart import flash:ACK_ trust_request.txt
```

```
Import Data Successful
```

```
device#
```

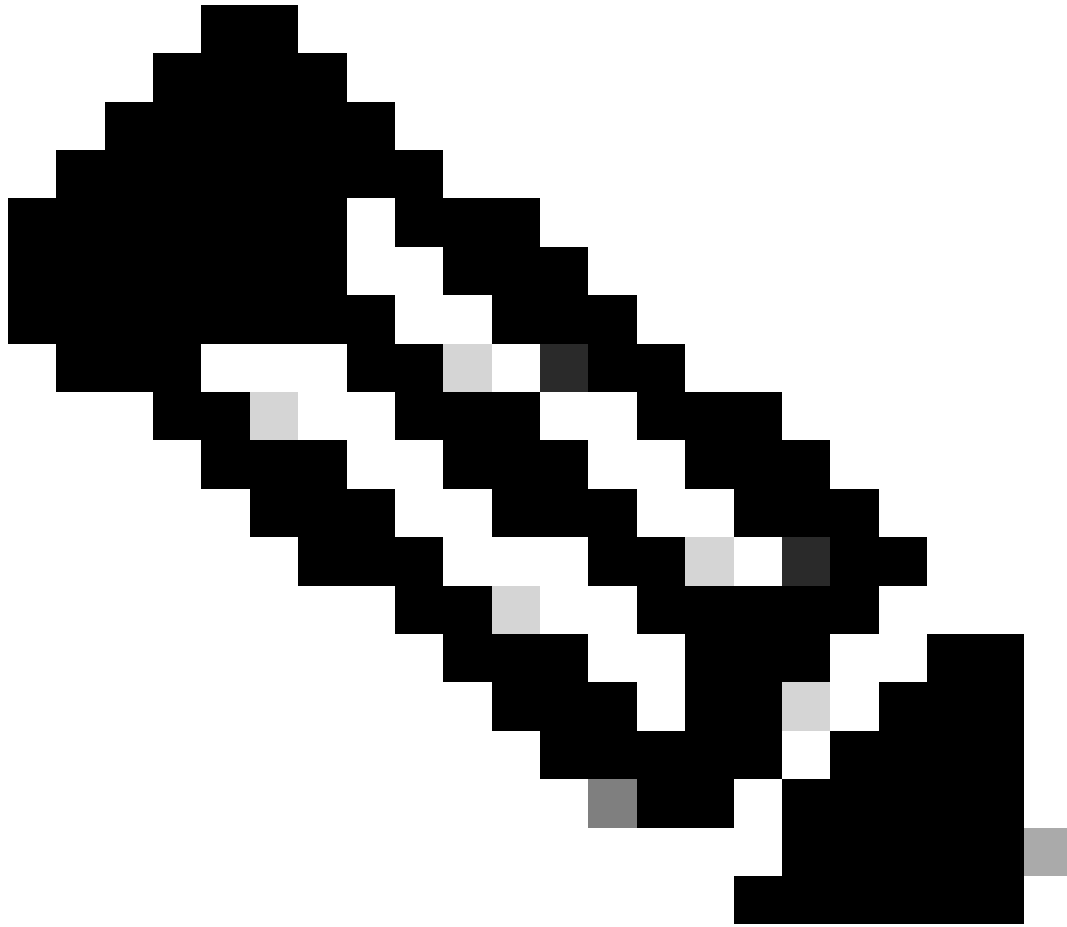
```
*Jun 12 20:01:07.348: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully i
```

모든 필수 정보가 포함된 Authorization Request를 설치합니다.

플래시에 활성 제품 인스턴스에 대한 권한 부여 요청을 생성하고 저장합니다.

CLI 구성:

```
device#license smart authorization request add hseck9 all
```



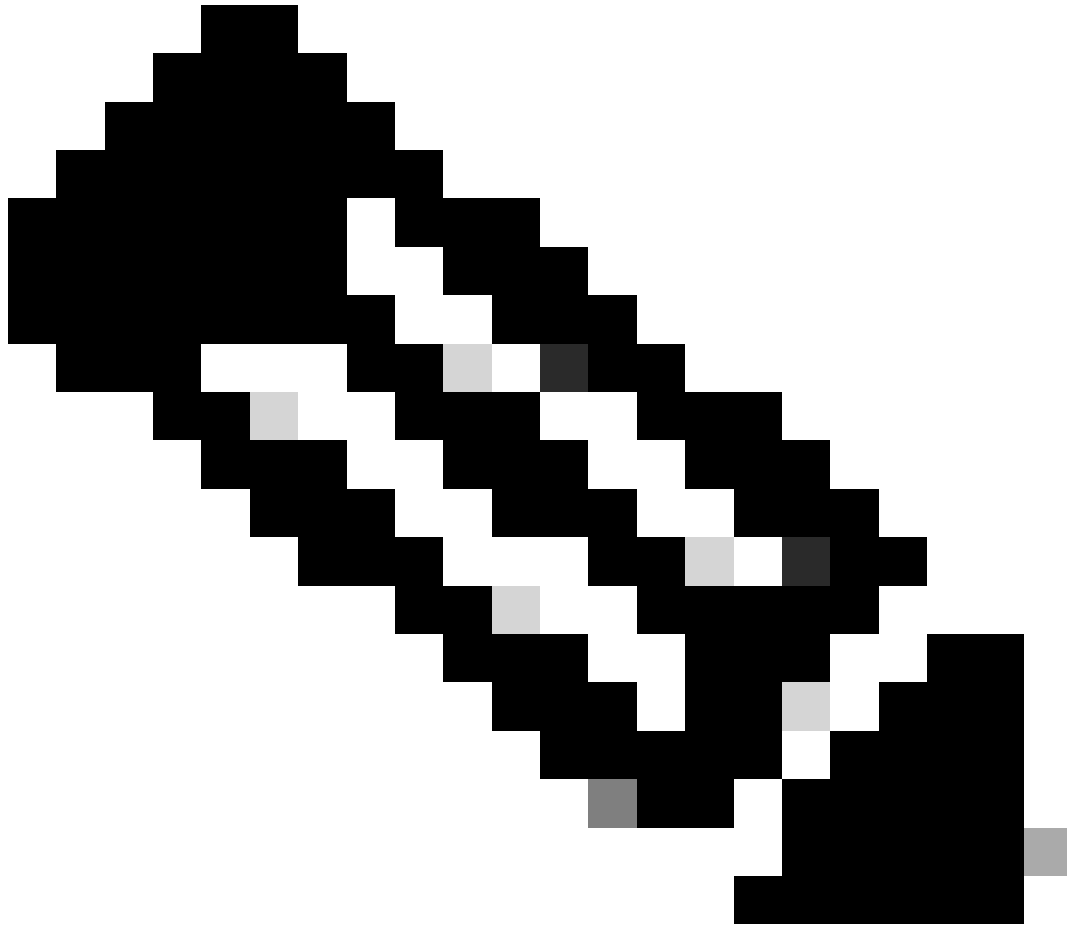
참고: HSEC: 높은 보안.

플래시에 활성 제품 인스턴스에 대한 권한 부여 코드 요청을 저장합니다.

```
device#license smart authorization request save bootflash:auth3.txt
```

Cisco SSM에 권한 부여 요청 파일을 업로드하고 ACK 파일을 다운로드합니다.

1. <https://software.cisco.com>에서 Cisco SSM 웹 UI에 [로그인합니다](#). Smart Software Licensing 아래에서 Manage licenses(라이선스 관리) 링크를 클릭합니다.
2. 보고서를 수신하는 Smart Account를 선택합니다.
3. Smart Software Licensing > Reports > Usage Data Files를 선택합니다.
4. CClick Upload Usage Data(사용량 데이터 업로드). 파일 위치(tar 형식의 RUM 보고서)를 찾은 다음 Upload Data(데이터 업로드)를 선택하고 CClick 업로드합니다.

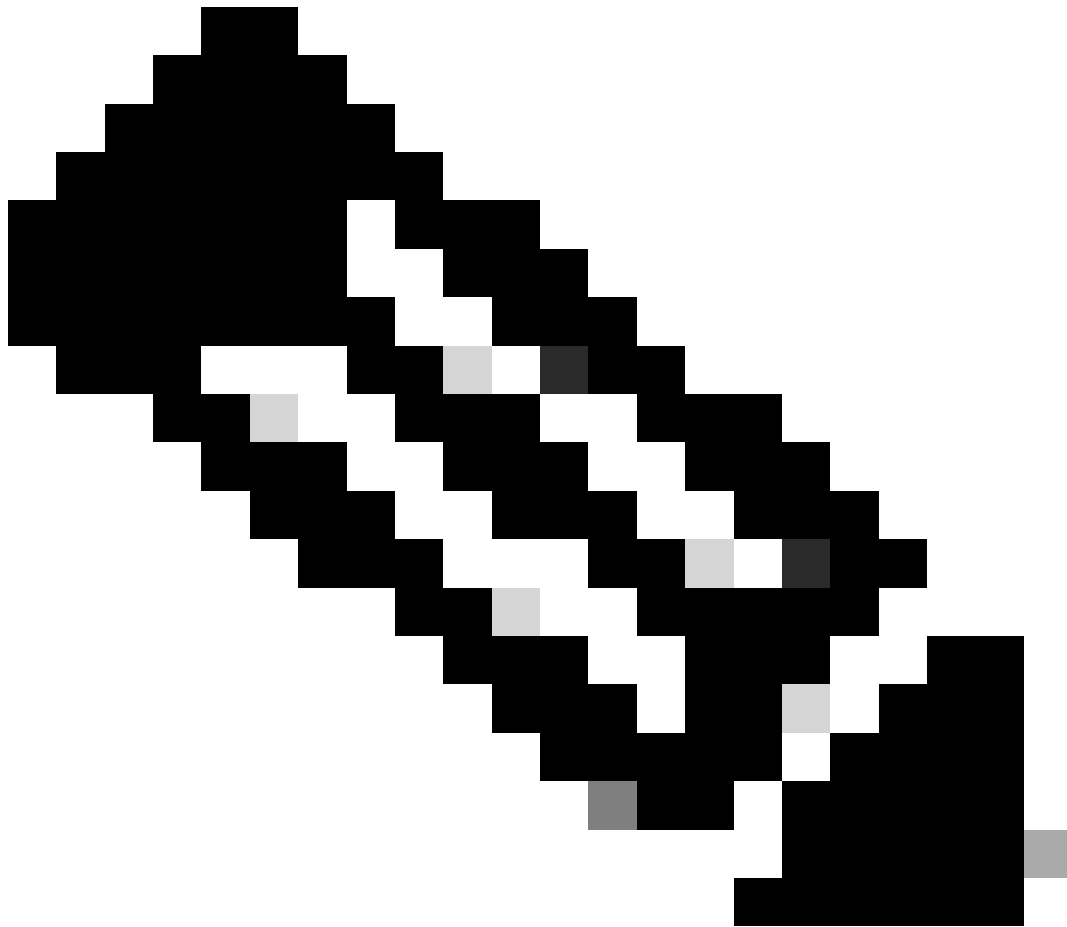


참고: 파일을 업로드한 후에는 삭제할 수 없습니다. 그러나 필요한 경우 다른 파일을 업로드할 수 있습니다.

5. [가상 어카운트 선택] 팝업창에서 업로드된 파일을 받을 가상 어카운트를 선택합니다.

파일이 업로드되고 Reports(보고서) 화면의 Usage Data Files(사용 데이터 파일) 테이블에 나열됩니다. 표시되는 세부 정보에는 파일 이름, 보고 시간, 업로드된 가상 어카운트, 보고 상태, 보고된 제품 인스턴스 수, 승인 상태 등이 있습니다.

6. 승인 열에서 다운로드를 눌러 업로드한 보고서나 요청에 대한 ACK 파일을 저장합니다.



참고: Acknowledgement 열에 파일이 나타날 때까지 기다려야 합니다. RUM 보고서 또는 처리할 요청이 많은 경우 Cisco SSM은 몇 분 정도 소요되어야 합니다.

파일을 다운로드한 후 파일을 가져와 제품 인스턴스에 설치합니다

CopyAuthorization 요청 ACK 파일

소스 위치 또는 디렉토리에서 제품 인스턴스의 플래시 메모리로 파일을 복사합니다.

```
device#copy ftp flash
```

```
Address or name of remote host [192.168.1.1]? 192.168.1.1
```

```
Source filename [ACK_auth3.txt]? ACK_auth3.txt
```

```
Destination filename [ACK_auth3.txt]?
```

```
Accessing ftp://192.168.1.1/ACK_auth3.txt ...!
```

[OK - 1543/4096 bytes]

1543 bytes copied in 0.041 secs (37634 bytes/sec)

InstallAuthorization 요청 ACK 파일

```
device#license smart import flash:ACK_auth3.txt

Last Confirmation code UDI: PID:C9300X-24Y,SN:XXXXXXXXXX

    Confirmation code: a4a85361

Import Data Completed

Last Confirmation code UDI: PID:C9300X-24Y,SN:XXXXXXXXXX

    Confirmation code: a4a85361

device#

*Jun 12 20:05:33.968: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa
```

다음을 확인합니다.

다음 명령을 사용하여 라이선스 상태를 확인할 수 있습니다.

```
device#sh license sum

Account Information:

    Smart Account: Cisco Systems, TAC As of Jun 12 20:03:03 2025 UTC

    Virtual Account: LANSW

License Usage:
```

License	Entitlement Tag	Count	Status
network-advantage	(C9300X-12/24Y Network ...)	1	IN USE
dna-advantage	(C9300X-12/24Y DNA Adva...)	1	IN USE
C9K HSEC	(Cat9K HSEC)	0	NOT IN USE

device#show license authorization

Overall status:

Active: PID:C9300X-24Y,SN:XXXXXXXXXX

Status: SMART AUTHORIZATION INSTALLED on Jun 12 20:05:33 2025 UTC

Last Confirmation code: a4a85361

Authorizations:

C9K HSEC (Cat9K HSEC):

Description: HSEC Key for Export Compliance on Cat9K Series Switches

Total available count: 4

Enforcement type: EXPORT RESTRICTED

Term information:

Active: PID:C9300X-24Y,SN:FJC28281AE2

Authorization type: SMART AUTHORIZATION INSTALLED

License type: PERPETUAL

Term Count: 4

device#sh license all | i Trust

Trust Code Installed: Jun 12 20:01:07 2025 UTC

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.