

HSEC-licenties configureren met behulp van SLP op offline Switches van de Catalyst 9300X-reeks

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Slimme transportlicenties configureren.](#)

[Een Trust ACK-aanvraag installeren](#)

[Upload het vertrouwensaanvraagbestand naar Cisco SSM en download het ACK-bestand.](#)

[CopyTrust ACK-bestand](#)

[Importeer en installeer het bestand op de productinstantie.](#)

[Installeer een autorisatieaanvraag met alle vereiste informatie.](#)

[Upload het autorisatieaanvraagbestand naar Cisco SSM en download het ACK-bestand.](#)

[CopyAuthorization RequestACK-bestand](#)

[InstallAuthorization RequestACK-bestand](#)

[Verifiëren](#)

Inleiding

In dit document wordt beschreven hoe u HSEC-licenties kunt configureren met behulp van SLP op Switches uit de Offline Catalyst 9300X-reeks.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van Cisco Smart Licensing Using Policy (SLP) concepten
- Vertrouwdheid met Cisco Catalyst 9300X Series switch hardware- en softwarebeheer
- Ervaring met het navigeren en beheren van licenties in Cisco Smart Software Manager (CSSM)
- Mogelijkheid om de CLI te gebruiken op Cisco IOS XE-apparaten
- Kennis van Cisco DNA-licentietypen
- Procedures voor apparaatregistratie en licentiereservering

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Hardware: Cisco Catalyst C9300X-24Y
- Software: Cisco IOS XE 17.12.04
- Slimme licentie-infrastructuur: Cisco Smart Software Manager (CSSM)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De HSEC-licentie (High-Security) maakt geavanceerde beveiligingsmogelijkheden op Cisco-platforms mogelijk, waardoor netwerkbeveiliging, gegevensintegriteit en privacy worden verbeterd. Het biedt robuuste tools voor veilige communicatie en naleving van strenge beveiligingseisen.

De belangrijkste functies van HSEC zijn:

- VPN Support faciliteert veilige, versleutelde communicatie via openbare netwerken, zoals IPsec en SSL VPN's, voor site-to-site en externe toegang.
- Encryption Capabilities ondersteunt sterke cryptografische algoritmen voor gegevensbescherming, waaronder AES en SHA voor het waarborgen van vertrouwelijkheid, integriteit en authenticatie.
- WAN MACsec breidt Layer 2-coderingsmogelijkheden (MACsec) uit over WAN-koppelingen en zorgt voor end-to-end gegevensbeveiliging via niet-vertrouwde netwerken.
- Met de uitbreidingen voor schaalbaarheid wordt schaalvergroting mogelijk voor versleutelde tunnels, zoals VPN-sessies, om grote implementaties te ondersteunen.
- Veilige communicatie maakt functies zoals FlexVPN en DMVPN mogelijk voor dynamische, schaalbare en veilige connectiviteit.

Configureren

Gebruik de C9300X CLI om slimme licenties te configureren.

Slimme transportlicenties configureren.

CLI-configuratie:

```
device#conf t
```

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

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

Een Trust ACK-aanvraag installeren

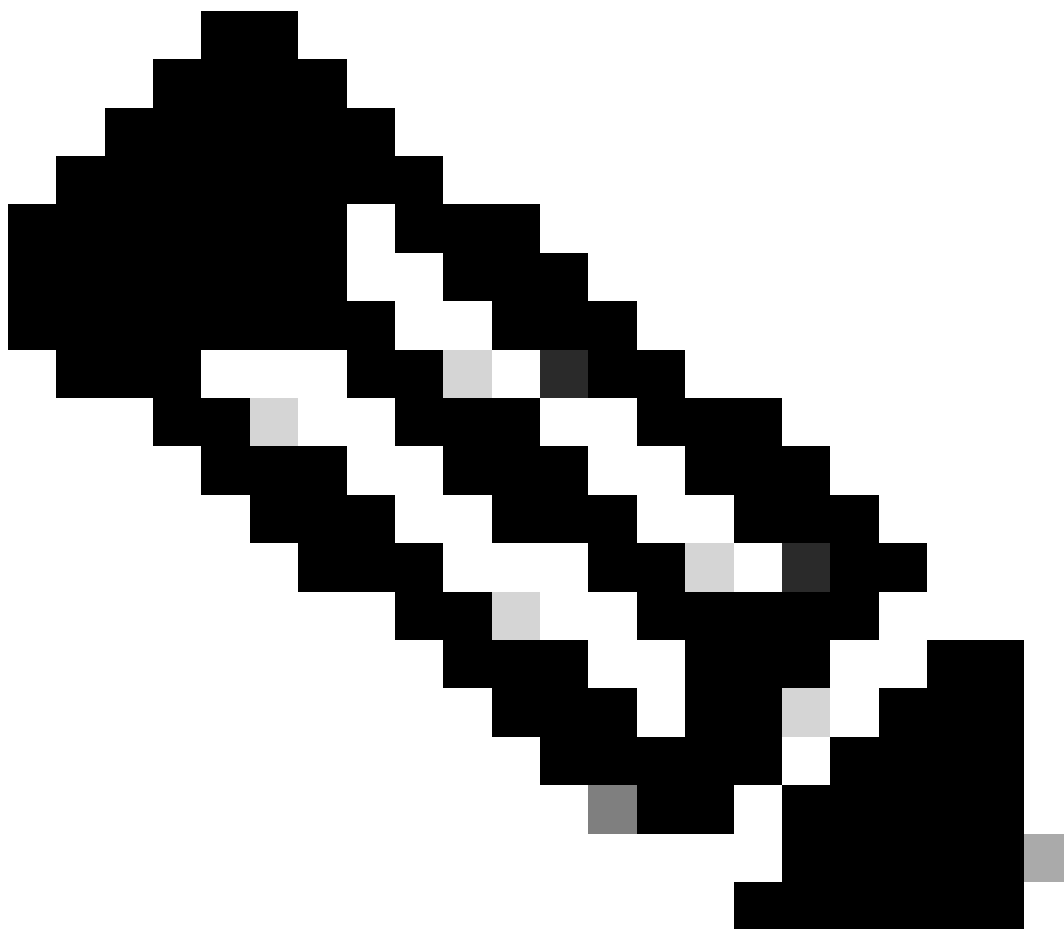
Genereer en sla de aanvraag voor de vertrouwenscode voor de actieve productinstantie op in Flash.

CLI-configuratie:

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

Upload het vertrouwensaanvraagbestand naar Cisco SSM en download het ACK-bestand.

1. Meld u aan bij de Cisco SSM Web UI op <https://software.cisco.com>. Klik onder Slimme softwarelicenties op de link Licenties beheren.
2. Selecteer de slimme account die het rapport ontvangt.
3. Selecteer Slimme softwarelicenties > Rapporten > Gebruiksgegevens.
4. Klik op Gebruiksgegevens uploaden. Blader naar de bestandslocatie (RUM-rapport in tar-indeling), selecteer en klik op Gegevens uploaden.



Opmerking: u kunt een bestand niet verwijderen nadat het is geüpload. U kunt echter een ander bestand uploaden, indien nodig.

-
5. Selecteer in het pop-upvenster Virtuele accounts selecteren de virtuele account die het geüploade bestand ontvangt.
 6. Het bestand wordt geüpload en weergegeven in de tabel Gebruiksgegevens in het scherm Rapporten. De weergegeven details omvatten de bestandsnaam, het tijdstip waarop de melding is gedaan, de virtuele account waarnaar de melding is geüpload, de rapportagestatus, het aantal gerapporteerde productinstanties en de erkenningsstatus.
 7. Klik in de kolom Bevestiging op Downloaden om het ACK-bestand op te slaan voor het rapport of de aanvraag die u hebt geüpload.



Opmerking: u moet wachten totdat het bestand in de kolom Bevestiging wordt weergegeven. Als er veel RUM-rapporten of -verzoeken zijn om te verwerken, moet Cisco SSM enkele minuten in beslag nemen.

Nadat u het bestand hebt gedownload, importeert en installeert u het bestand op de productinstantie

ACK-bestand voor vertrouwen kopiëren

Kopieer het bestand van de bronlocatie of directory naar het flashgeheugen van de productinstantie.

CLI-configuratie:

```
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)

Importeer en installeer het bestand op de productinstantie.

CLI-configuratie:

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

```
Import Data Successful
```

```
device#
```

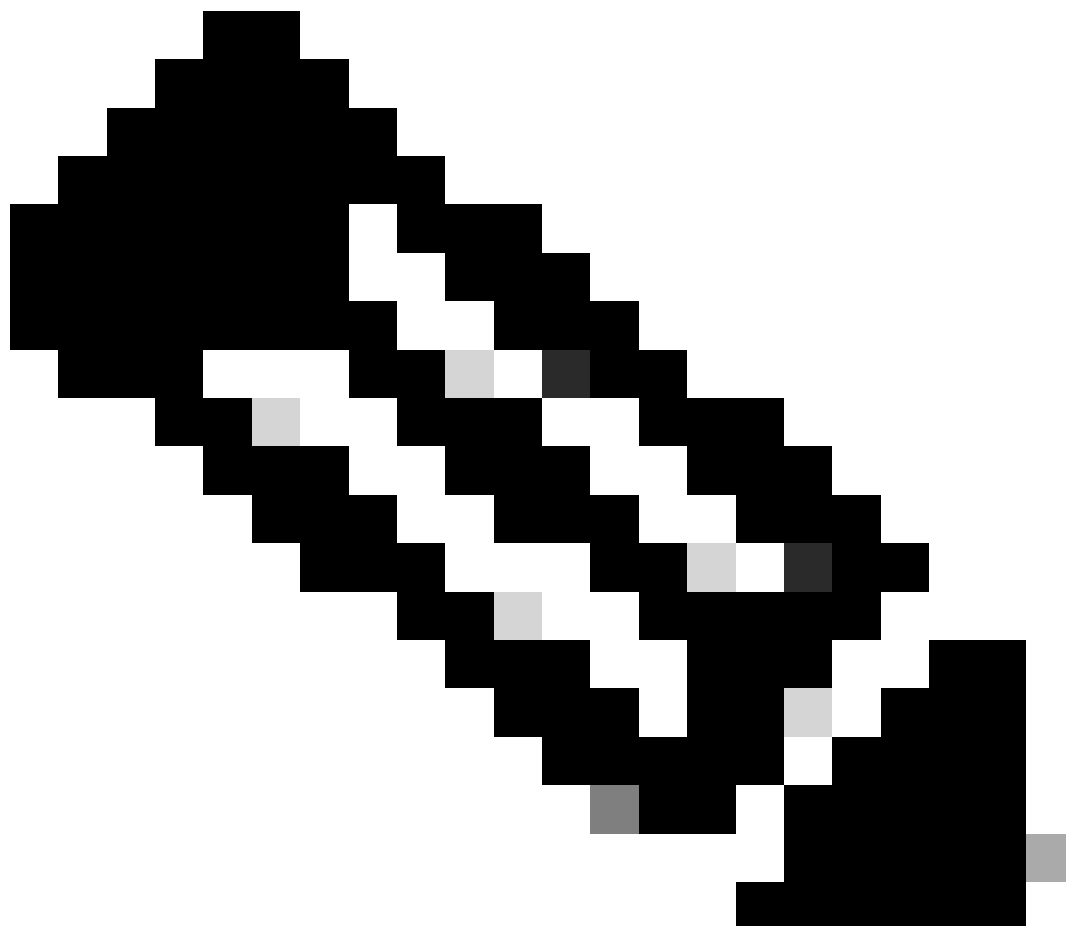
```
*Jun 12 20:01:07.348: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully i
```

Installeer een autorisatieaanvraag met alle vereiste informatie.

Genereer en sla de autorisatieaanvraag voor het actieve product op in de flash.

CLI-configuratie:

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



Opmerking: HSEC: High Security.

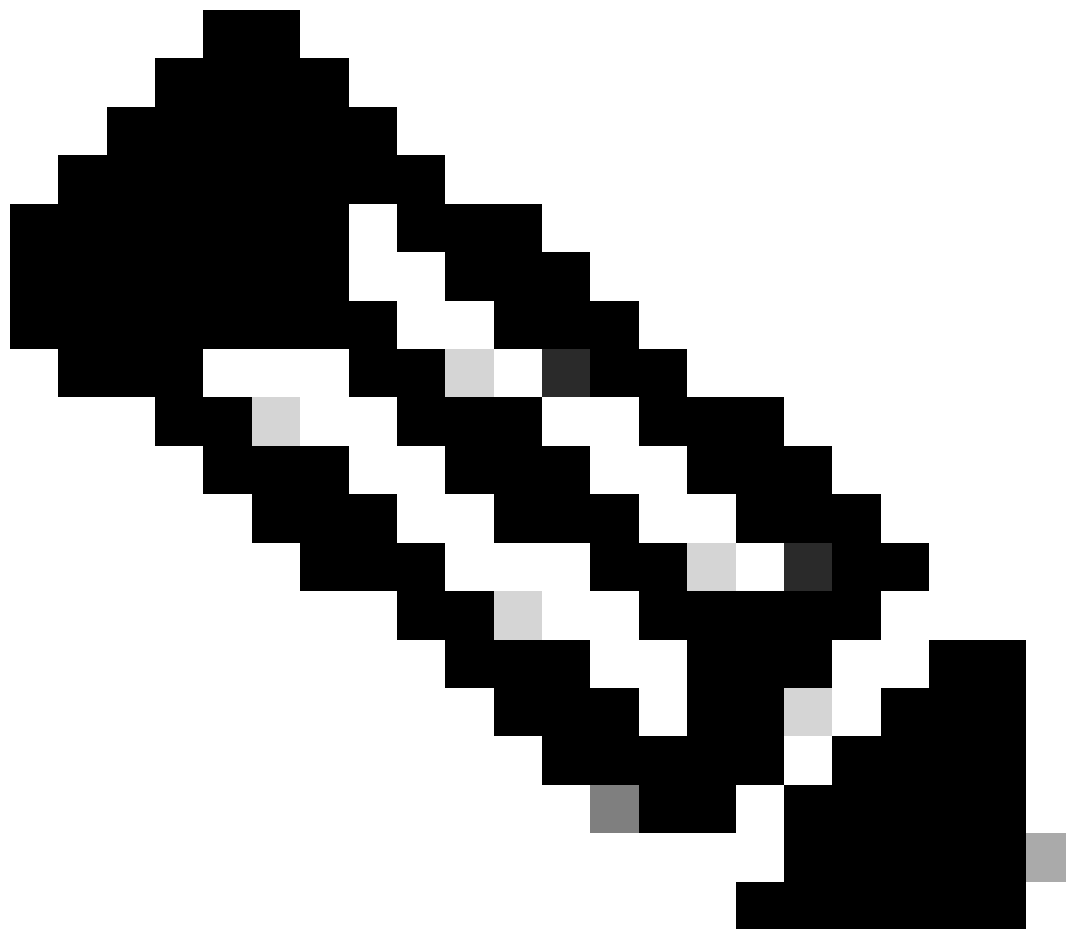
Sla de aanvraag voor de autorisatiecode voor de actieve productinstantie op in Flash.

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

Upload het autorisatieaanvraagbestand naar Cisco SSM en download het ACK-bestand.

1. Meld u aan bij de Cisco SSM Web UI op <https://software.cisco.com>. Klik onder Slimme softwarelicenties op de link Licenties beheren.
2. Selecteer de slimme account die het rapport ontvangt.
3. Selecteer Slimme softwarelicenties > Rapporten > Gebruiksgegevens.
4. Klik op Gebruiksgegevens uploaden. Blader naar de bestandslocatie (RUM-rapport in tar-

indeling), selecteer en klik op Gegevens uploaden.



Opmerking: u kunt een bestand niet verwijderen nadat het is geüpload. U kunt echter een ander bestand uploaden, indien nodig.

5. Selecteer in het pop-upvenster Virtuele accounts selecteren de virtuele account die het geüploade bestand ontvangt.

Het bestand wordt geüpload en weergegeven in de tabel Gebruiksgegevens in het scherm Rapporten. De weergegeven details omvatten de bestandsnaam, het tijdstip waarop de melding is gedaan, de virtuele account waarnaar de melding is geüpload, de rapportagestatus, het aantal gerapporteerde productinstanties en de erkenningsstatus.

6. Klik in de kolom Bevestiging op Downloaden om het ACK-bestand op te slaan voor het rapport of de aanvraag die u hebt geüpload.



Opmerking: u moet wachten totdat het bestand in de kolom Bevestiging wordt weergegeven. Als er veel RUM-rapporten of -verzoeken zijn om te verwerken, moet Cisco SSM enkele minuten in beslag nemen.

Nadat u het bestand hebt gedownload, importeert en installeert u het bestand op de productinstantie

ACK-bestand voor autorisatieaanvraag kopiëren

Kopieer het bestand van de bronlocatie of directory naar het flashgeheugen van de productinstantie.

```
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)

ACK-bestand voor InstallAuthorization Request

```
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 was installed.

Verifiëren

U kunt deze opdracht gebruiken om de licentiestatus te controleren:

```
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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.