Configuration des licences HSEC à l'aide de SLP sur les commutateurs hors ligne de la gamme Catalyst 9300X

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Informations générales

Configurer

- Désactivez la fonction Smart Licensing Transport.
- Installer une demande ACK de confiance
- Téléchargez le fichier de demande d'approbation sur Cisco SSM et téléchargez le fichier ACK.
- Fichier ACK CopyTrust
- Importez et installez le fichier sur l'instance de produit.
- Installez une demande d'autorisation avec toutes les informations requises.
- Téléchargez le fichier de demande d'autorisation sur Cisco SSM et téléchargez le fichier ACK.
- Fichier CopyAuthorization RequestACK
- Fichier InstallAuthorization RequestACK

Vérifier

Introduction

Ce document décrit comment configurer des licences HSEC à l'aide de SLP sur des commutateurs hors ligne de la gamme Catalyst 9300X.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension des concepts de Cisco Smart Licensing Using Policy (SLP)
- Connaissance de la gestion matérielle et logicielle des commutateurs Cisco Catalyst 9300X
- Expérience de navigation et de gestion des licences dans Cisco Smart Software Manager (CSSM)
- Possibilité d'utiliser la CLI sur les périphériques Cisco IOS XE
- Connaissance des types de licences Cisco DNA
- Procédures d'enregistrement et de réservation de licence

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Matériel : Cisco Catalyst C9300X-24Y
- le logiciel Cisco IOS: Cisco IOS XE 17.12.04
- Infrastructure de licence intelligente : Cisco Smart Software Manager (CSSM)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La licence HSEC (High-Security) offre des fonctionnalités de sécurité avancées sur les plates-formes Cisco, améliorant ainsi la protection du réseau, l'intégrité des données et la confidentialité. Il fournit des outils robustes pour une communication sécurisée et la conformité aux exigences de sécurité strictes.

Fonctionnalités clés activées par HSEC :

- La prise en charge VPN facilite les communications sécurisées et cryptées sur les réseaux publics, tels que les VPN IPsec et SSL, pour l'accès site à site et à distance.
- Les fonctions de cryptage prennent en charge des algorithmes cryptographiques puissants pour la protection des données, notamment AES et SHA pour garantir la confidentialité, l'intégrité et l'authentification.
- WAN MACsec étend les capacités de cryptage de couche 2 (MACsec) sur les liaisons WAN, assurant ainsi la sécurité de bout en bout des données sur les réseaux non fiables.
- Les améliorations de l'évolutivité permettent une évolutivité plus élevée pour les tunnels cryptés, tels que les sessions VPN, afin de prendre en charge les déploiements à grande échelle.
- La communication sécurisée offre des fonctionnalités telles que FlexVPN et DMVPN pour une connectivité dynamique, évolutive et sécurisée.

Configurer

Utilisez l'interface de ligne de commande C9300X pour configurer les licences Smart.

Désactivez la fonction Smart Licensing Transport.

Configuration CLI :

```
device#conf t

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

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

Installer une demande ACK de confiance

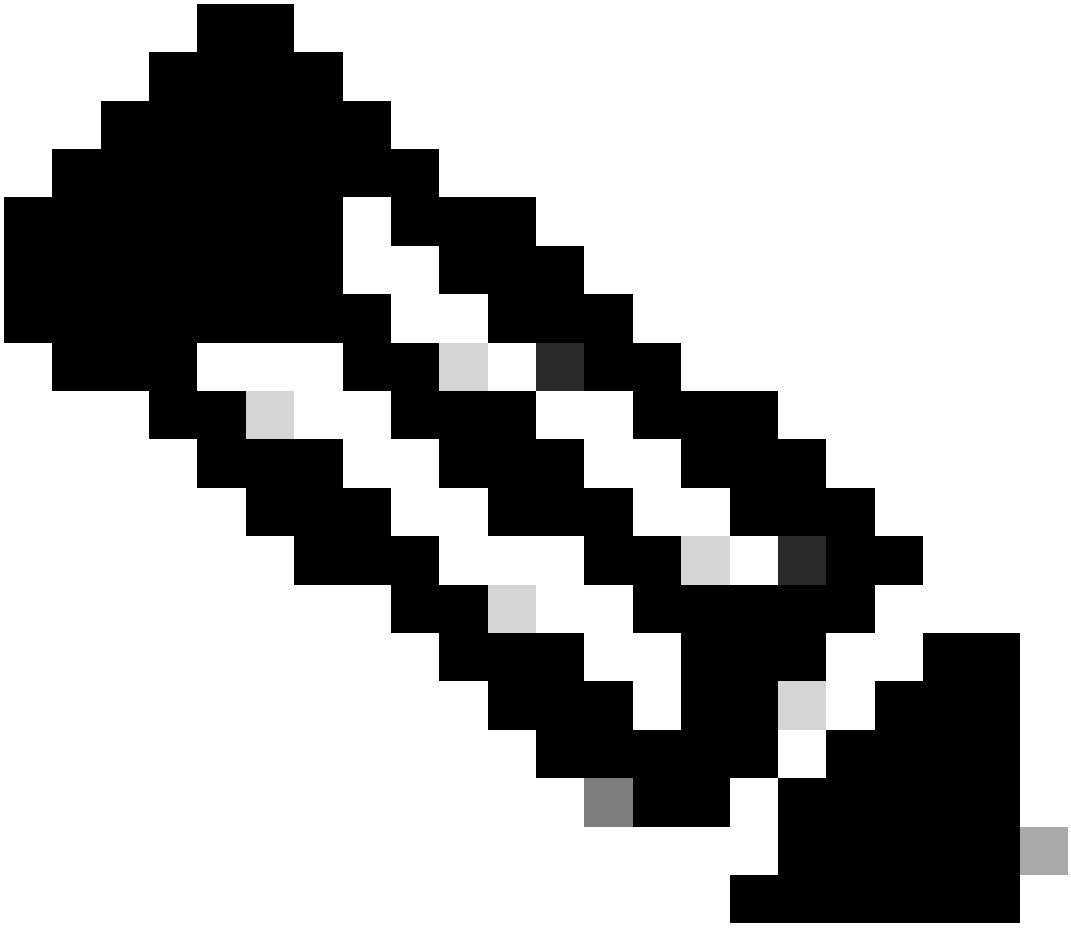
Générez et enregistrez la demande de code d'approbation pour l'instance de produit active dans la mémoire Flash.

Configuration CLI :

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

Téléchargez le fichier de demande d'approbation sur Cisco SSM et téléchargez le fichier ACK.

1. Connectez-vous à l'interface utilisateur Web de Cisco SSM à l'adresse https://software.cisco.com. Sous Smart Software Licensing, cliquez sur le lien Manage licenses.
2. Sélectionnez le compte Smart qui reçoit le rapport.
3. Sélectionnez Smart Software Licensing > Reports > Usage Data Files.
4. CLIck Télécharger les données d'utilisation. Accédez à l'emplacement du fichier (rapport RUM au format tar), sélectionnez, puis cliquez sur CLIck Upload Data.

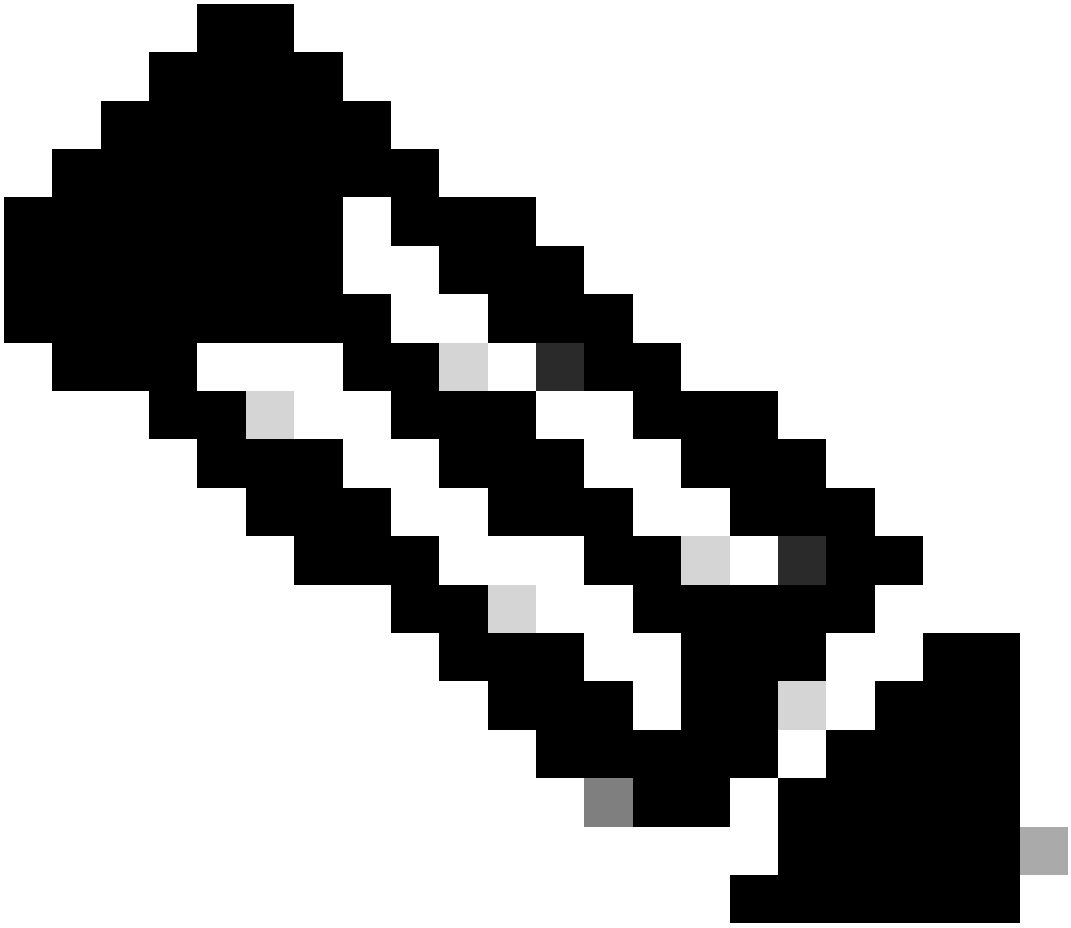


Remarque : Vous ne pouvez pas supprimer un fichier après l'avoir téléchargé. Vous pouvez toutefois télécharger un autre fichier, si nécessaire.

5. Dans la fenêtre contextuelle Sélectionner des comptes virtuels, sélectionnez le compte virtuel qui reçoit le fichier téléchargé.

6. Le fichier est téléchargé et figure dans le tableau Fichiers de données d'utilisation de l'écran Rapports. Les détails affichés incluent le nom du fichier, l'heure à laquelle il a été signalé, le compte virtuel vers lequel il a été téléchargé, l'état du rapport, le nombre d'instances de produit signalées et l'état de l'accusé de réception.

7. Dans la colonne Acknowledgement, cliquez sur Download pour enregistrer le fichier ACK pour le rapport ou la demande que vous avez téléchargé.



Remarque : Vous devez attendre que le fichier apparaisse dans la colonne Accusé de réception. S'il y a beaucoup de rapports RUM ou de demandes à traiter, Cisco SSM doit prendre quelques minutes.

Après avoir téléchargé le fichier, importez-le et installez-le sur l'instance du produit

Copier le fichier ACK de confiance

Copiez le fichier de son emplacement ou répertoire source vers la mémoire flash de l'instance de produit.

Configuration CLI :

```
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)
```

Importez et installez le fichier sur l'instance de produit.

Configuration CLI :

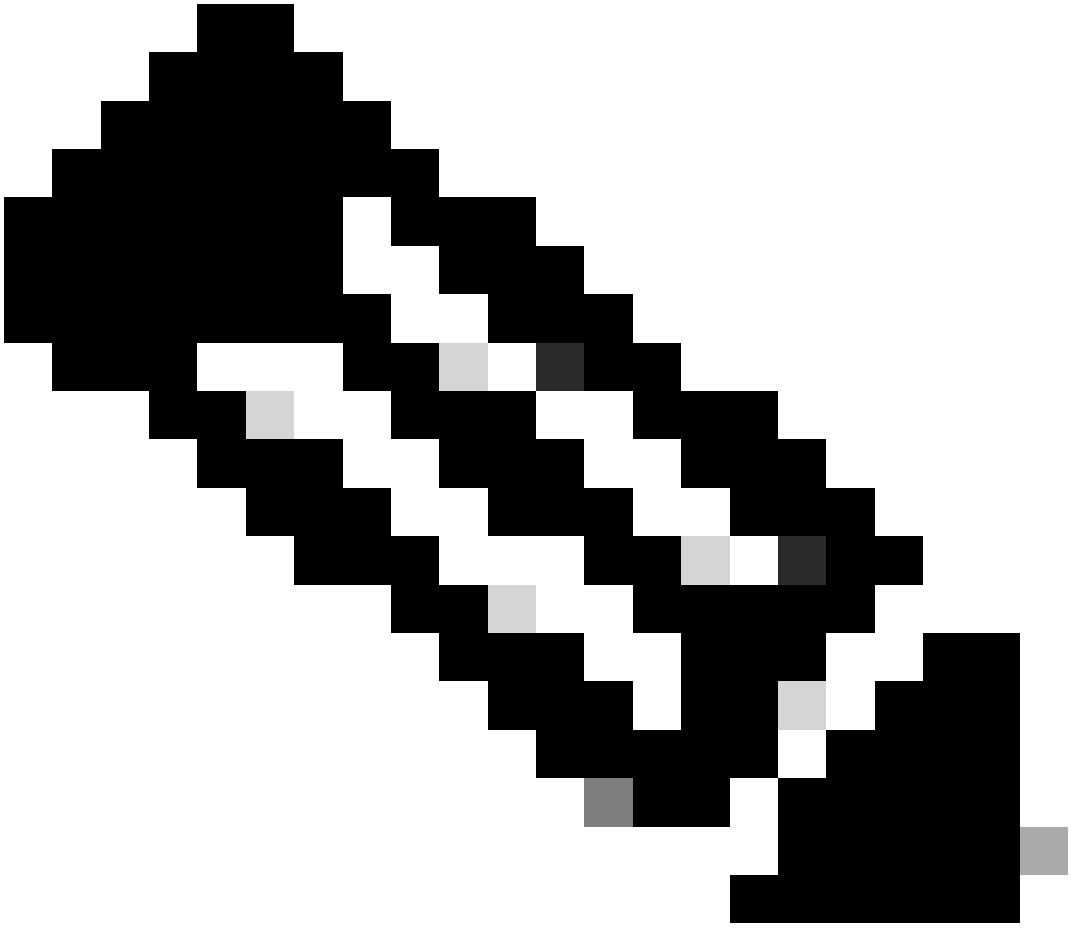
```
device#license smart import flash:ACK_ trust_request.txt

Import Data Successful


device#

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

Installez une demande d'autorisation avec toutes les informations requises.

Générez et enregistrez la demande d'autorisation pour l'instance de produit active dans la mémoire Flash.

Configuration CLI :

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



Remarque : HSEC : Haute sécurité.

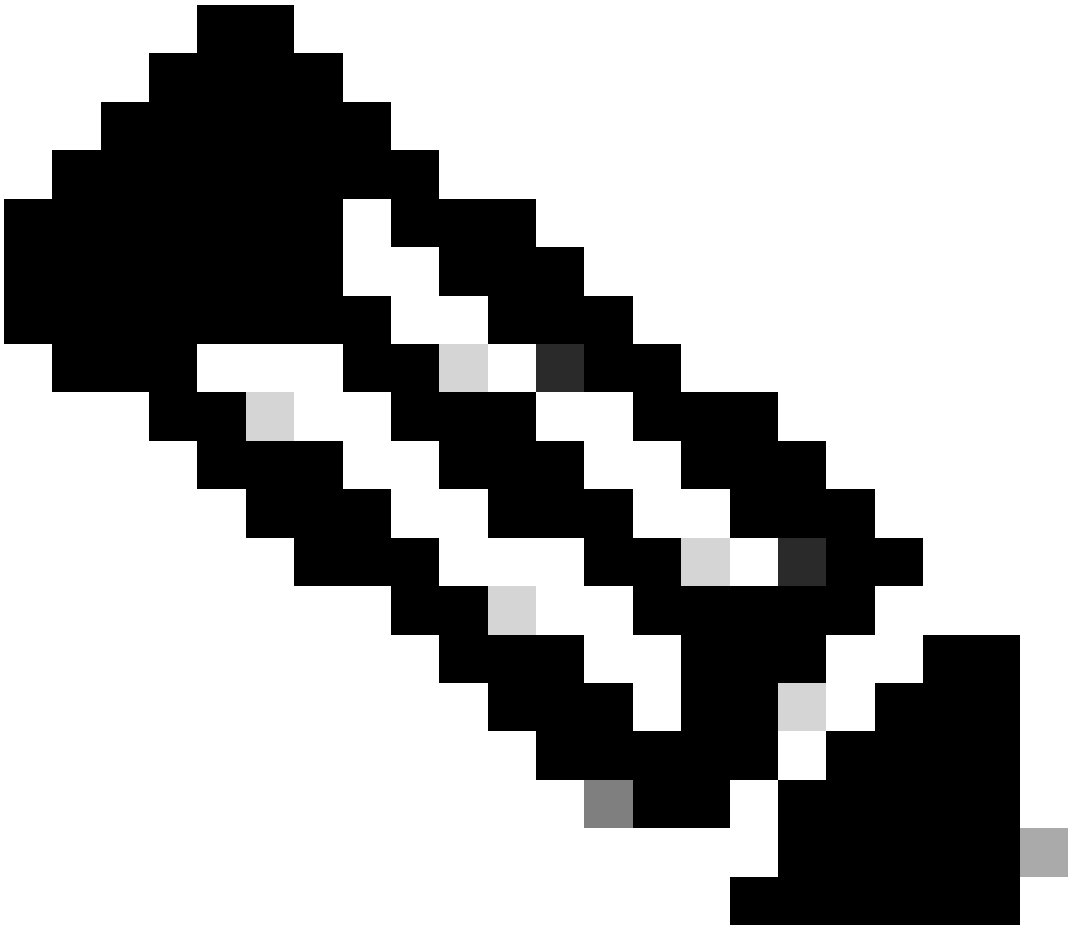
Enregistrez la demande de code d'autorisation pour l'instance de produit active dans la mémoire Flash.

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

Téléchargez le fichier de demande d'autorisation sur Cisco SSM et téléchargez le fichier ACK.

1. Connectez-vous à l'interface utilisateur Web de Cisco SSM à l'adresse https://software.cisco.com. Sous Smart Software Licensing, cliquez sur le lien Manage licenses.
2. Sélectionnez le compte Smart qui reçoit le rapport.

3. Sélectionnez Smart Software Licensing > Reports > Usage Data Files.
4. CLIck Télécharger les données d'utilisation. Accédez à l'emplacement du fichier (rapport RUM au format tar), sélectionnez, puis cliquez sur CLIck Upload Data.



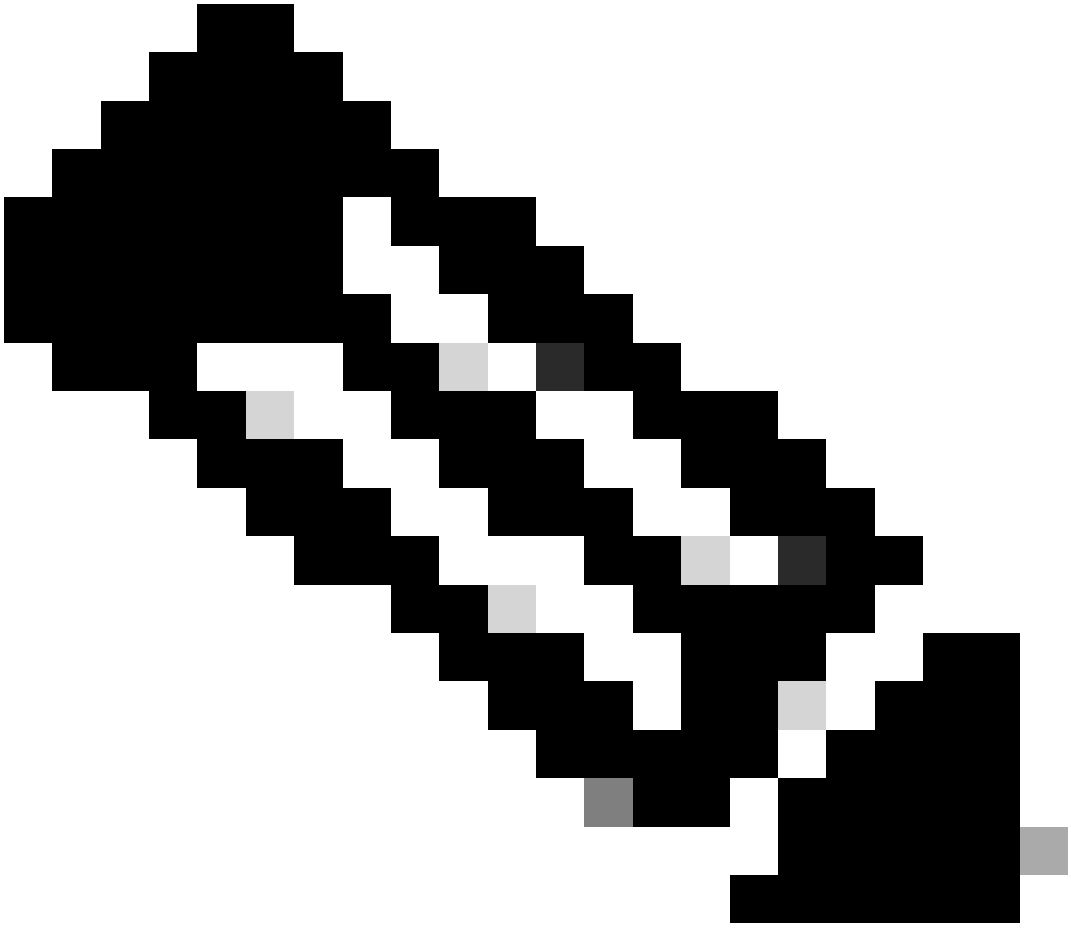
Remarque : Vous ne pouvez pas supprimer un fichier après l'avoir téléchargé. Vous pouvez toutefois télécharger un autre fichier, si nécessaire.

---

5. Dans la fenêtre contextuelle Sélectionner des comptes virtuels, sélectionnez le compte virtuel qui reçoit le fichier téléchargé.

Le fichier est téléchargé et est répertorié dans le tableau Fichiers de données d'utilisation dans l'écran Rapports. Les détails affichés incluent le nom du fichier, l'heure à laquelle il a été signalé, le compte virtuel vers lequel il a été téléchargé, l'état du rapport, le nombre d'instances de produit signalées et l'état de l'accusé de réception.

6. Dans la colonne Acknowledgement, cliquez sur Download pour enregistrer le fichier ACK pour le rapport ou la demande que vous avez téléchargé.



Remarque : Vous devez attendre que le fichier apparaisse dans la colonne Accusé de réception. S'il y a beaucoup de rapports RUM ou de demandes à traiter, Cisco SSM doit prendre quelques minutes.

Après avoir téléchargé le fichier, importez-le et installez-le sur l'instance du produit

Fichier ACK de demande CopyAuthorization

Copiez le fichier de son emplacement ou répertoire source vers la mémoire flash de l'instance de produit.

```
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)
```

Fichier ACK de demande InstallAuthorization

```
device#license smart import flash:ACK_auth3.txt
Last Confirmation code UDI: PID:C9300X-24Y,SN:XXXXXXXXX
    Confirmation code: a4a85361
Import Data Completed
Last Confirmation code UDI: PID:C9300X-24Y,SN:XXXXXXXXX
    Confirmation code: a4a85361
device#
*Jun 12 20:05:33.968: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa
```

Vérifier

Vous pouvez utiliser ces commandes pour vérifier l'état de la licence :

```
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.