Konfigurieren von HSEC-Lizenzen mithilfe von SLP auf Offline-Switches der Catalyst Serie 9300X

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie HSEC-Lizenzen mithilfe von SLP auf Offline-Catalyst-Switches der Serie 9300X konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes zu den Konzepten von Cisco Smart Licensing Using Policy (SLP)
- Vertrautheit mit der Hardware- und Softwareverwaltung für Cisco Catalyst Switches der Serie 9300X
- Erfahrung bei der Verwaltung von Lizenzen im Cisco Smart Software Manager (CSSM)
- Verwendung der CLI auf Cisco IOS XE-Geräten
- Kenntnisse der Berechtigungstypen für Cisco DNA-Lizenzen

- Verfahren zur Geräteregistrierung und Lizenzreservierung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Hardware: Cisco Catalyst C9300X - 24 Jahre
- Software: Cisco IOS XE 17.12.04
- Smart Licensing-Infrastruktur: Cisco Smart Software Manager (CSSM)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die HSEC-Lizenz (High-Security) ermöglicht erweiterte Sicherheitsfunktionen auf Cisco Plattformen und verbessert so den Netzwerkschutz, die Datenintegrität und den Datenschutz. Es bietet robuste Tools für eine sichere Kommunikation und die Einhaltung strenger Sicherheitsanforderungen.

Zu den wichtigsten Funktionen von HSEC gehören:

- Die VPN-Unterstützung ermöglicht eine sichere, verschlüsselte Kommunikation über öffentliche Netzwerke wie IPsec und SSL VPNs für Site-to-Site- und Remote-Zugriff.
- Verschlüsselungsfunktionen unterstützen starke Verschlüsselungsalgorithmen für den Datenschutz, einschließlich AES und SHA zur Gewährleistung von Vertraulichkeit, Integrität und Authentifizierung.
- WAN MACsec erweitert die Funktionen zur Layer-2-Verschlüsselung (MACsec) auf WAN-Links und gewährleistet End-to-End-Datensicherheit über nicht vertrauenswürdige Netzwerke.
- Verbesserte Skalierbarkeit ermöglicht höhere Skalierbarkeit für verschlüsselte Tunnel, wie z. B. VPN-Sitzungen, um große Bereitstellungen zu unterstützen.
- Secure Communication ermöglicht Funktionen wie FlexVPN und DMVPN für dynamische, skalierbare und sichere Verbindungen.

Konfigurieren

Verwenden Sie die C9300X-CLI, um Smart Licensing zu konfigurieren.

Smart Licensing-Transport deaktivieren

CLI-Konfiguration:

```
device#conf t

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


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

Installieren einer Trust ACK-Anforderung

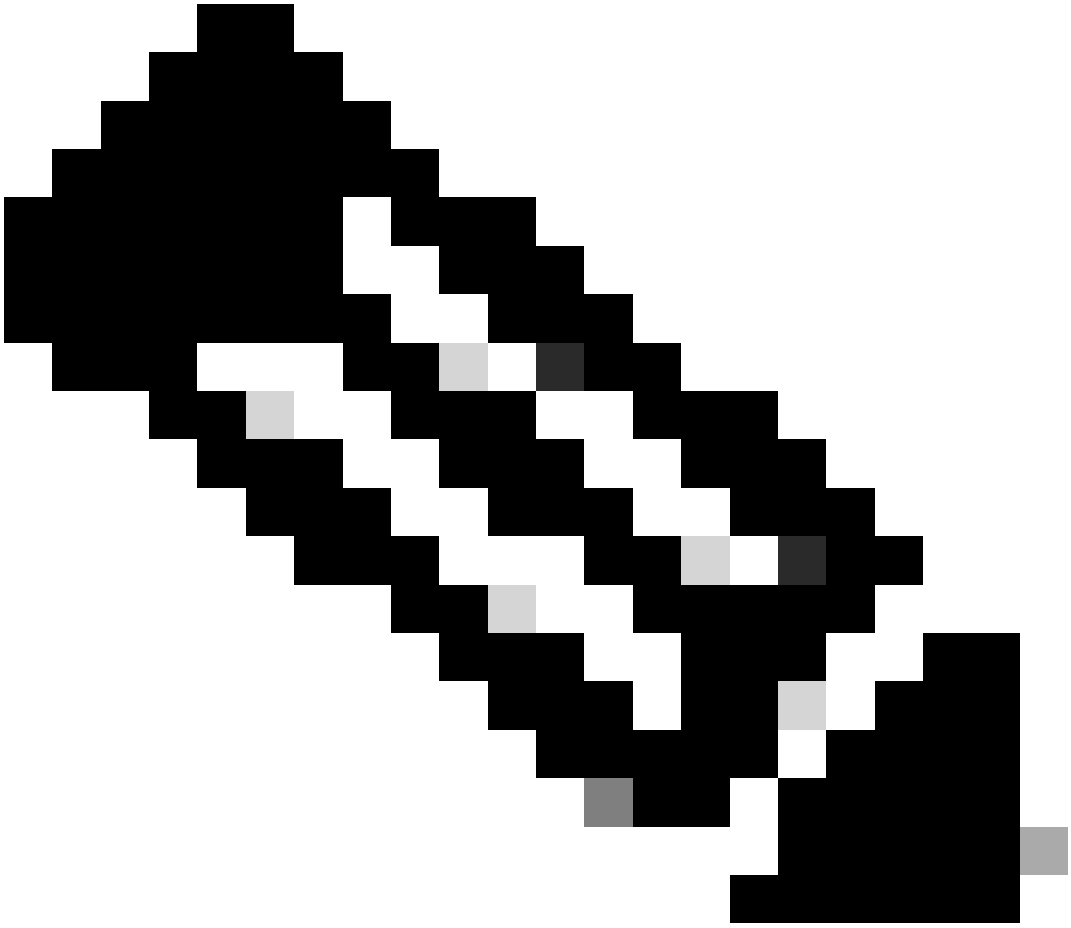
Generieren und speichern Sie die Anforderung für den Vertrauenscode für die aktive Produktinstanz im Flash.

CLI-Konfiguration:

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

Laden Sie die Datei für die Vertrauenswürdigkeit in Cisco SSM hoch, und laden Sie die ACK-Datei herunter.

1. Melden Sie sich unter https://software.cisco.com bei der Cisco SSM-Webbenutzeroberfläche an. Klicken Sie unter Smart Software Licensing auf den Link Manage licenses (Lizenzen verwalten).
2. Wählen Sie den Smart Account aus, der den Bericht empfängt.
3. Wählen Sie Smart Software Licensing > Reports > Usage Data Files aus.
4. CLIck-Nutzungsdaten hochladen. Navigieren Sie zum Dateispeicherort (RUM-Bericht im TAR-Format), wählen Sie und klicken Sie auf Daten hochladen.

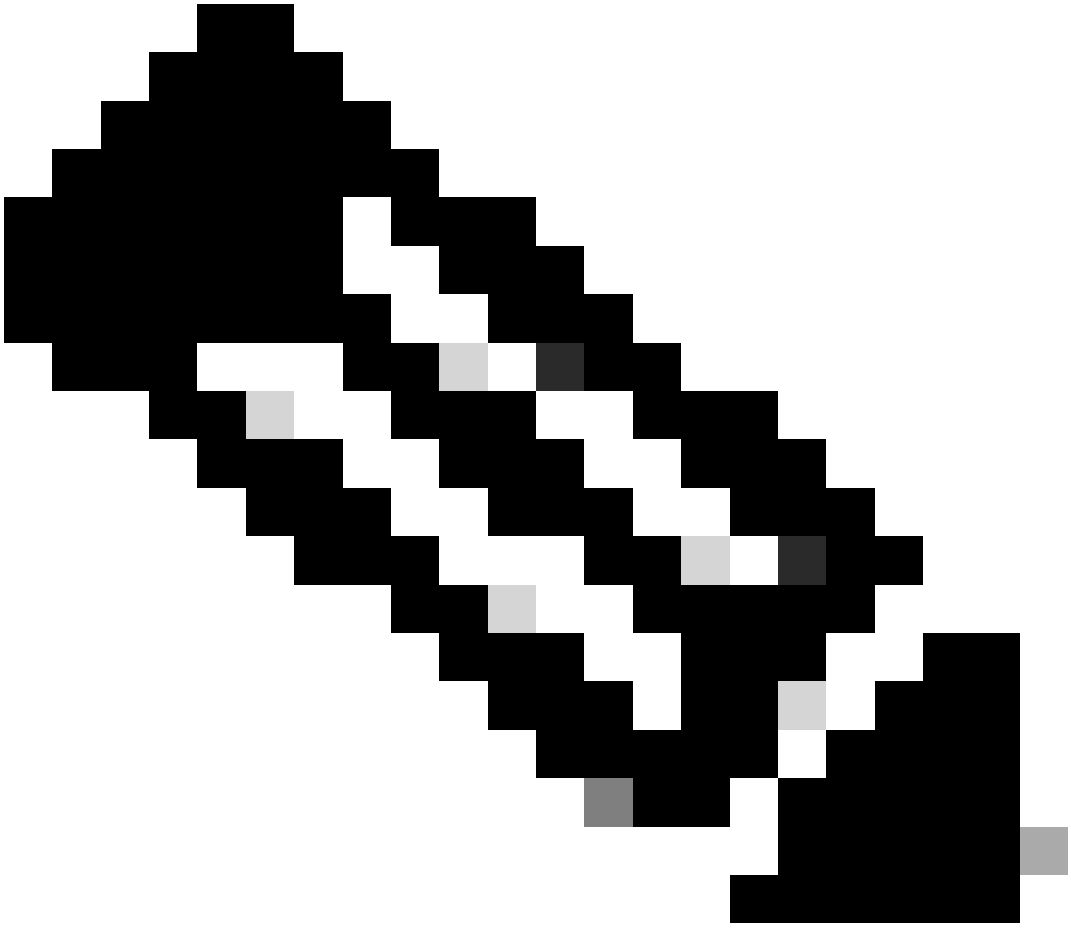


Anmerkung: Sie können eine Datei nicht löschen, nachdem sie hochgeladen wurde. Sie können jedoch bei Bedarf eine weitere Datei hochladen.

5. Wählen Sie aus dem Popup-Fenster "Virtuelle Konten auswählen" das virtuelle Konto aus, das die hochgeladene Datei empfängt.

6. Die Datei wird hochgeladen und in der Tabelle Verwendungsdatendateien im Bildschirm "Berichte" aufgeführt. Zu den angezeigten Details gehören der Dateiname, der Zeitpunkt, zu dem er gemeldet wurde, in welches Virtual Account er hochgeladen wurde, der Berichtsstatus, die Anzahl der gemeldeten Produktinstanzen und der Bestätigungsstatus.

7. Klicken Sie in der Spalte "Bestätigung" auf "Herunterladen", um die ACK-Datei für den Bericht zu speichern oder eine hochgeladene Anforderung zu senden.



Anmerkung: Sie müssen warten, bis die Datei in der Spalte Bestätigung angezeigt wird. Wenn viele RUM-Berichte oder -Anfragen verarbeitet werden, benötigt Cisco SSM einige Minuten.

Importieren und installieren Sie die Datei nach dem Herunterladen in der Produktinstanz.

Vertrauenswürdige ACK-Datei kopieren

Kopieren Sie die Datei aus dem Quellverzeichnis in den Flash-Speicher der Produktinstanz.

CLI-Konfiguration:

```
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)
```

Importieren und installieren Sie die Datei in der Produktinstanz.

CLI-Konfiguration:

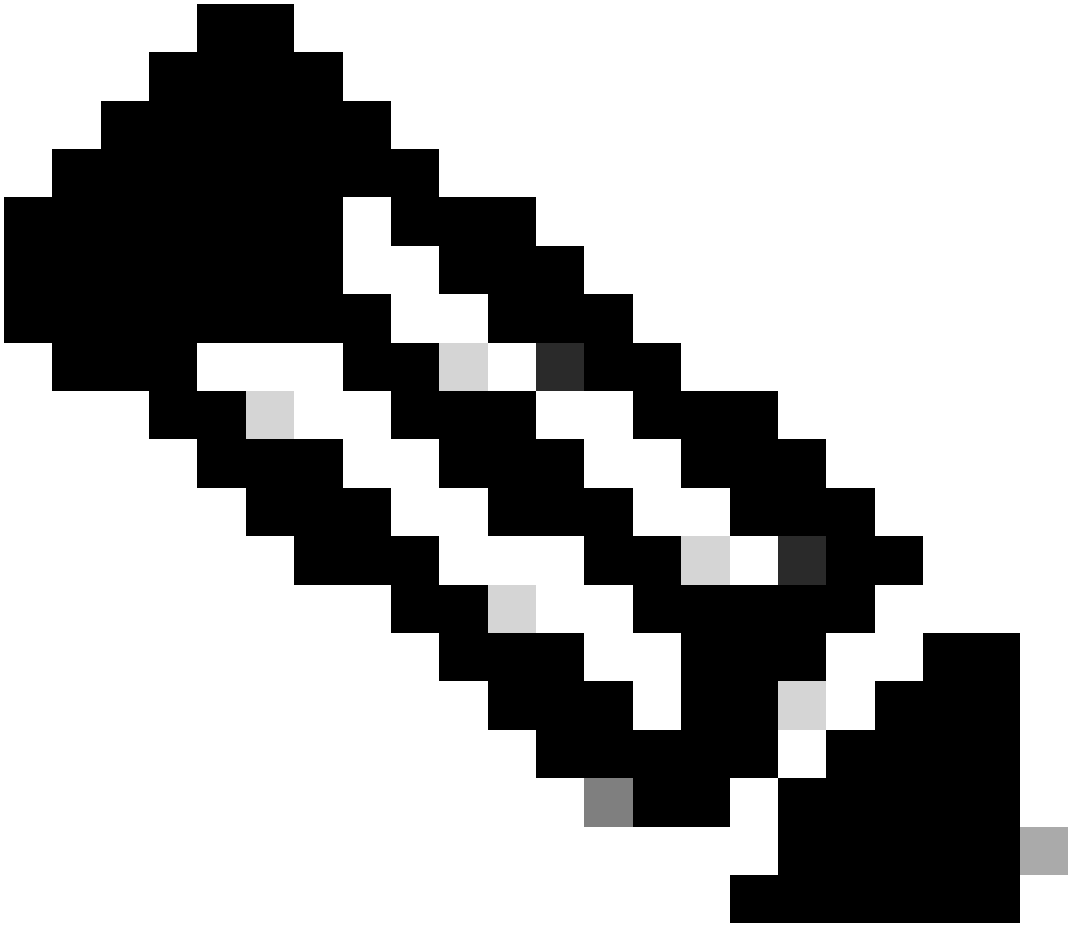
```
device#license smart import flash:ACK_ trust_request.txt

Import Data Successful


device#

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

Installieren einer Autorisierungsanfrage mit allen erforderlichen Informationen

Generieren und speichern Sie die Autorisierungsanfrage für die aktive Produktinstanz im Flash-Speicher.

CLI-Konfiguration:

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



Anmerkung: HSEC: Hohe Sicherheit.

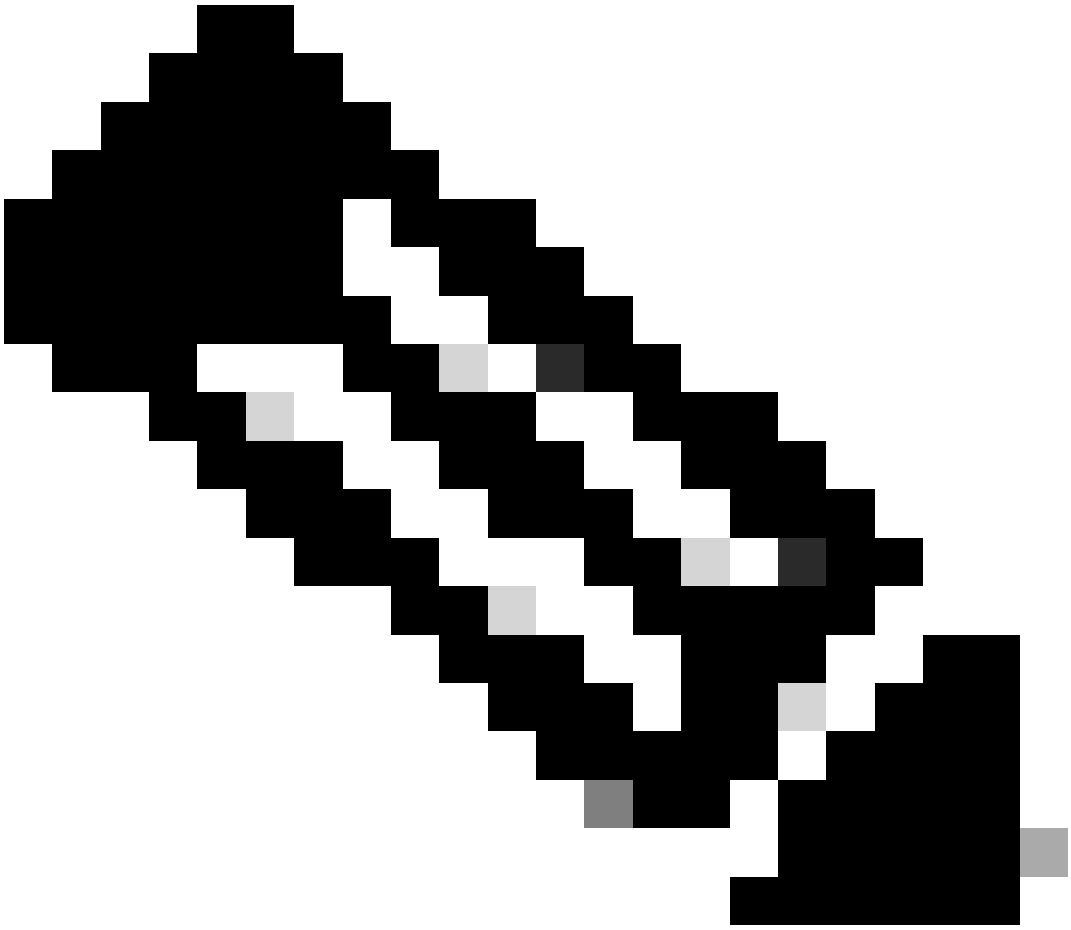
Speichern Sie die Autorisierungscodeanforderung für die aktive Produktinstanz im Flash-Speicher.

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

Laden Sie die Datei für die Autorisierungsanfrage in Cisco SSM hoch, und laden Sie die ACK-Datei herunter.

1. Melden Sie sich unter https://software.cisco.com bei der Cisco SSM-Webbenutzeroberfläche an. Klicken Sie unter Smart Software Licensing auf den Link Manage licenses (Lizenzen verwalten).
2. Wählen Sie den Smart Account aus, der den Bericht empfängt.
3. Wählen Sie Smart Software Licensing > Reports > Usage Data Files aus.

4. CLIck-Nutzungsdaten hochladen. Navigieren Sie zum Dateispeicherort (RUM-Bericht im TAR-Format), wählen Sie und klicken Sie auf Daten hochladen.



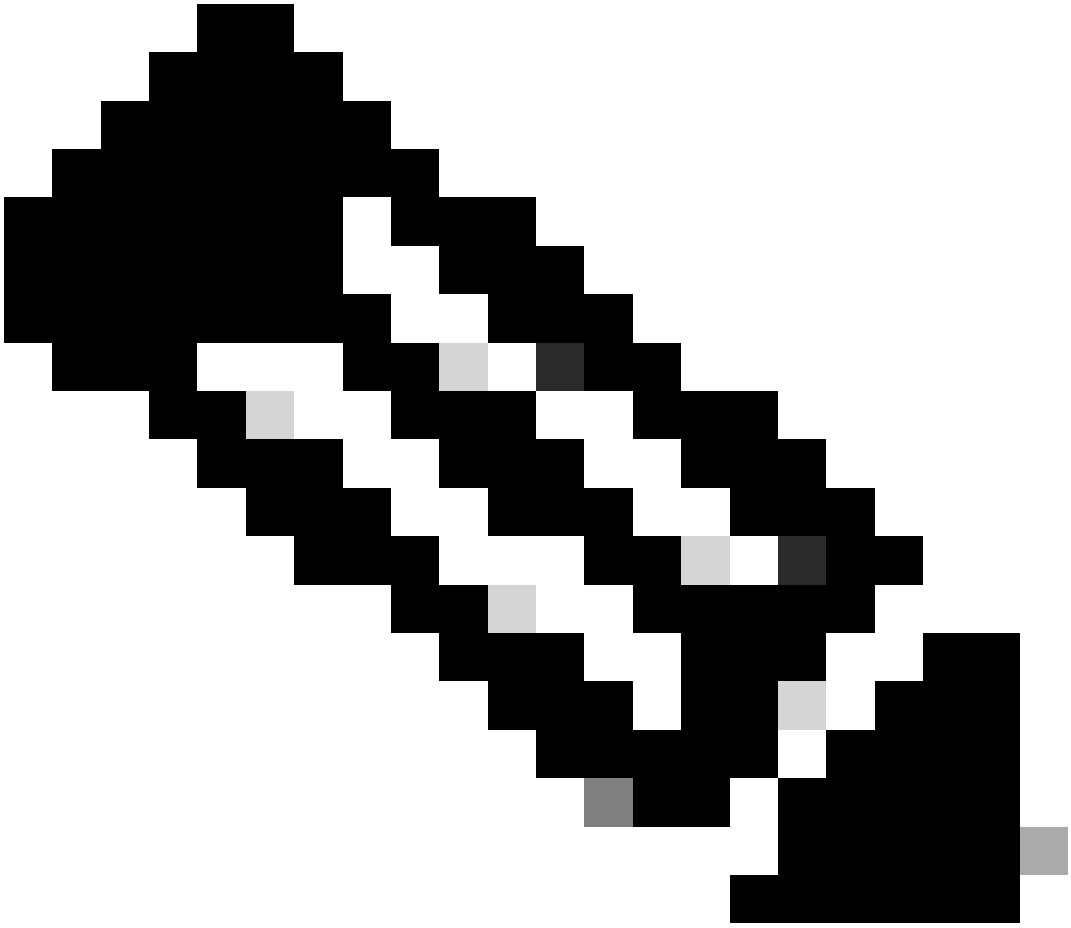
Anmerkung: Sie können eine Datei nicht löschen, nachdem sie hochgeladen wurde. Sie können jedoch bei Bedarf eine weitere Datei hochladen.

---

5. Wählen Sie aus dem Popup-Fenster "Virtuelle Konten auswählen" das virtuelle Konto aus, das die hochgeladene Datei empfängt.

Die Datei wird hochgeladen und in der Tabelle Verwendungsdatendateien im Bildschirm "Berichte" aufgeführt. Zu den angezeigten Details gehören der Dateiname, der Zeitpunkt, zu dem er gemeldet wurde, in welches Virtual Account er hochgeladen wurde, der Berichtsstatus, die Anzahl der gemeldeten Produktinstanzen und der Bestätigungsstatus.

6. Klicken Sie in der Spalte "Bestätigung" auf Herunterladen, um die ACK-Datei für den Bericht oder die hochgeladene Anforderung zu speichern.



Anmerkung: Sie müssen warten, bis die Datei in der Spalte Bestätigung angezeigt wird. Wenn viele RUM-Berichte oder -Anfragen verarbeitet werden, benötigt Cisco SSM einige Minuten.

Importieren und installieren Sie die Datei nach dem Herunterladen in der Produktinstanz.

ACK-Datei für Autorisierungsanforderung kopieren

Kopieren Sie die Datei aus dem Quellverzeichnis in den Flash-Speicher der Produktinstanz.

```
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-Datei für die Installationsautorisierungsanforderung

```
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
```

Überprüfung

Sie können die folgenden Befehle verwenden, um den Lizenzstatus zu überprüfen:

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.