Configuración de licencias HSEC mediante SLP en switches Catalyst serie 9300X sin conexión

Contenido

Introducción

Este documento describe cómo configurar licencias HSEC usando SLP en switches Catalyst serie 9300X sin conexión.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Descripción de los conceptos de Cisco Smart Licensing Using Policy (SLP)
- Familiaridad con la gestión de hardware y software de los switches Catalyst de Cisco serie 9300X
- Experimente la navegación y la gestión de licencias en Cisco Smart Software Manager (CSSM)
- Posibilidad de utilizar la CLI en dispositivos Cisco IOS XE
- Conocimiento de los tipos de derechos de licencia DNA de Cisco
- Procedimientos para el registro de dispositivos y la reserva de licencias

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Hardware Cisco Catalyst C9300X-24Y
- Software: Cisco IOS XE 17.12.04
- Infraestructura de licencias inteligentes: Cisco Smart Software Manager (CSSM)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La licencia HSEC (High-Security) habilita funciones de seguridad avanzadas en las plataformas de Cisco, lo que mejora la protección de la red, la integridad de los datos y la privacidad. Proporciona herramientas robustas para una comunicación segura y el cumplimiento de estrictos requisitos de seguridad.

Las funciones clave habilitadas por HSEC incluyen:

- La compatibilidad con VPN facilita la comunicación segura y cifrada a través de redes públicas, como VPN IPsec y SSL, para el acceso remoto y de sitio a sitio.
- Las funciones de cifrado admiten potentes algoritmos criptográficos para la protección de datos, incluidos AES y SHA para garantizar la confidencialidad, la integridad y la autenticación.
- WAN MACsec amplía las funciones de cifrado de capa 2 (MACsec) a través de los enlaces WAN, lo que garantiza una seguridad de datos integral en redes no fiables.
- Las mejoras en la escalabilidad permiten una mayor escalabilidad de los túneles cifrados, como las sesiones VPN, para admitir implementaciones de gran tamaño.
- La comunicación segura habilita funciones como FlexVPN y DMVPN para una conectividad dinámica, escalable y segura.

Configurar

Utilice la CLI de C9300X para configurar las licencias inteligentes.

Configure el transporte de licencias inteligentes desactivado.

Configuración de CLI:

```
device#conf t

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

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

Instalar una solicitud ACK de confianza

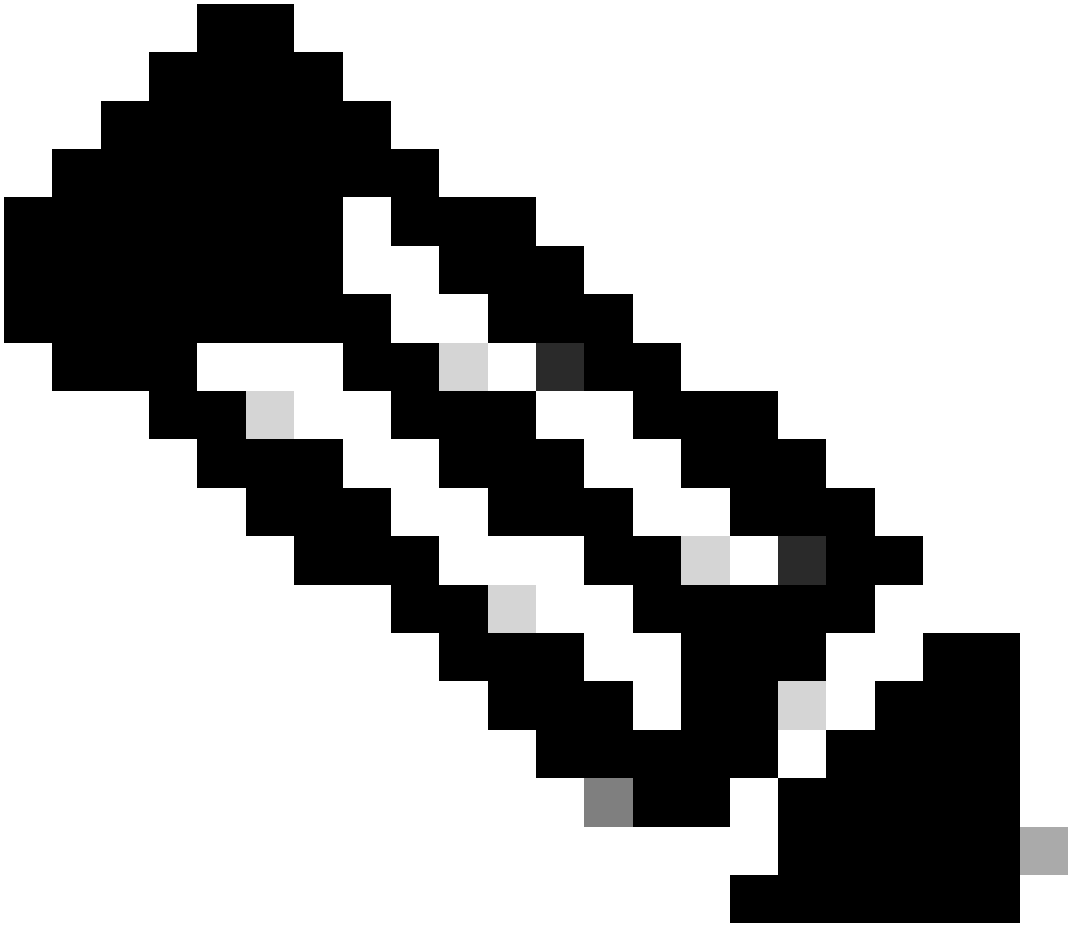
Genere y guarde la solicitud de código de confianza para la instancia de producto activa en la memoria flash.

Configuración de CLI:

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

Cargue el archivo de solicitud de confianza en Cisco SSM y descargue el archivo ACK.

1. Inicie sesión en Cisco SSM Web UI en https://software.cisco.com. En Licencias de software inteligente, haga clic en el enlace Administrar licencias.
2. Seleccione la cuenta inteligente que recibe el informe.
3. Seleccione Smart Software Licensing > Reports > Usage Data Files .
4. CLIck Cargar datos de uso. Busque la ubicación del archivo (informe de RUM en formato .tar), seleccione y haga clic en CLI para cargar datos.

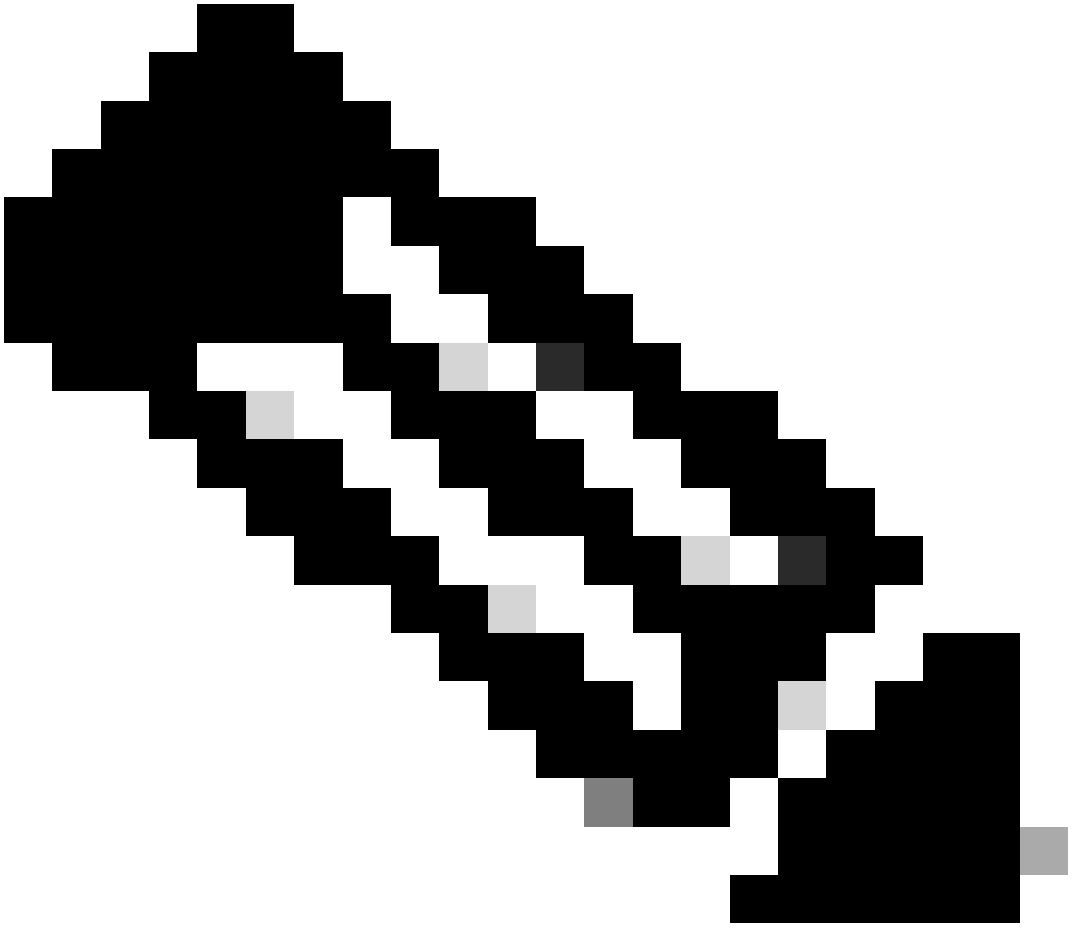


Nota: No puede eliminar un archivo después de haberlo cargado. Sin embargo, puede cargar otro archivo si es necesario.

5. En la ventana emergente Seleccionar cuentas virtuales, seleccione la cuenta virtual que recibe el archivo cargado.

6. El archivo se carga y aparece en la tabla Archivos de datos de uso de la pantalla Informes. Los detalles que se muestran incluyen el nombre del archivo, la hora a la que se notificó, la cuenta virtual en la que se cargó, el estado de los informes, el número de instancias de productos notificadas y el estado de la confirmación.

7. En la columna Reconocimiento, haga clic en Descargar para guardar el archivo ACK para el informe o la solicitud que ha cargado.



Nota: Debe esperar a que el archivo aparezca en la columna Reconocimiento. Si hay muchos informes o solicitudes RUM para procesar, Cisco SSM debe tardar unos minutos.

Después de descargar el archivo, importe e instale el archivo en la instancia del producto

Copiar archivo ACK de confianza

Copie el archivo desde su ubicación o directorio de origen a la memoria flash de la instancia del producto.

Configuración de 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)
```

Importe e instale el archivo en la instancia del producto.

Configuración de CLI:

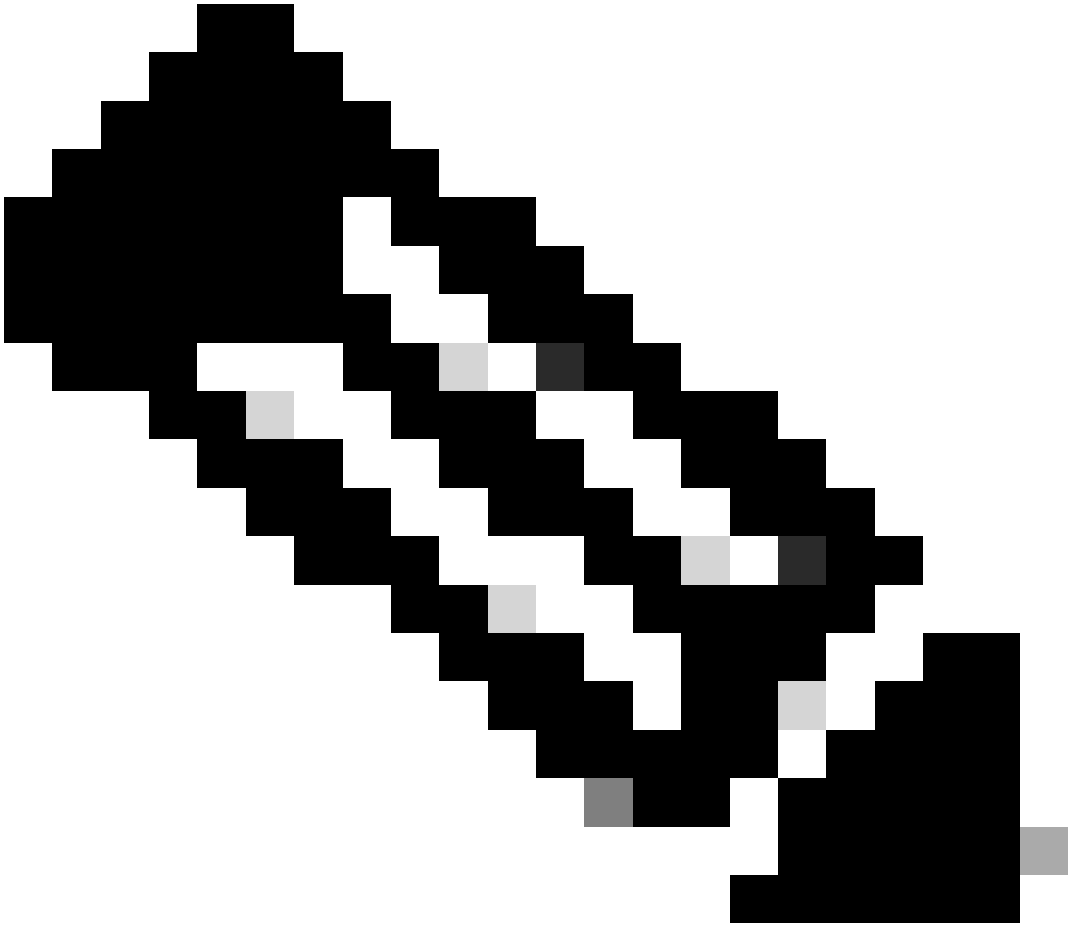
```
device#license smart import flash:ACK_ trust_request.txt

Import Data Successful


device#

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

Instale una solicitud de autorización con toda la información necesaria.

Genere y guarde la solicitud de autorización para la instancia del producto activo en la memoria flash.

Configuración de CLI:

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



Nota: HSEC: Gran seguridad.

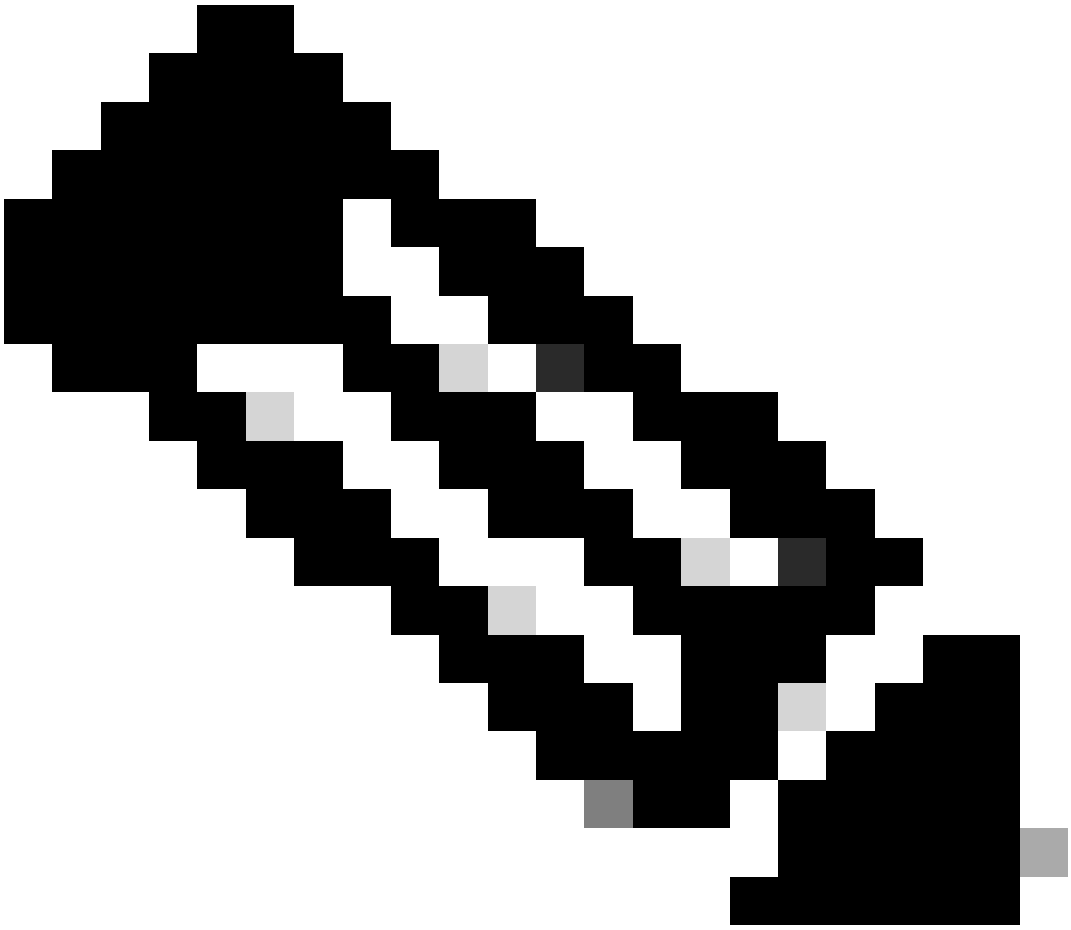
Guarde la solicitud de código de autorización para la instancia de producto activa en la memoria flash.

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

Cargue el archivo de solicitud de autorización en Cisco SSM y descargue el archivo ACK.

1. Inicie sesión en Cisco SSM Web UI en https://software.cisco.com. En Licencias de software inteligente, haga clic en el enlace Administrar licencias.
2. Seleccione la cuenta inteligente que recibe el informe.
3. Seleccione Smart Software Licensing > Reports > Usage Data Files .

4. CLIck Cargar datos de uso. Busque la ubicación del archivo (informe de RUM en formato .tar), seleccione y haga clic en CLI para cargar datos.



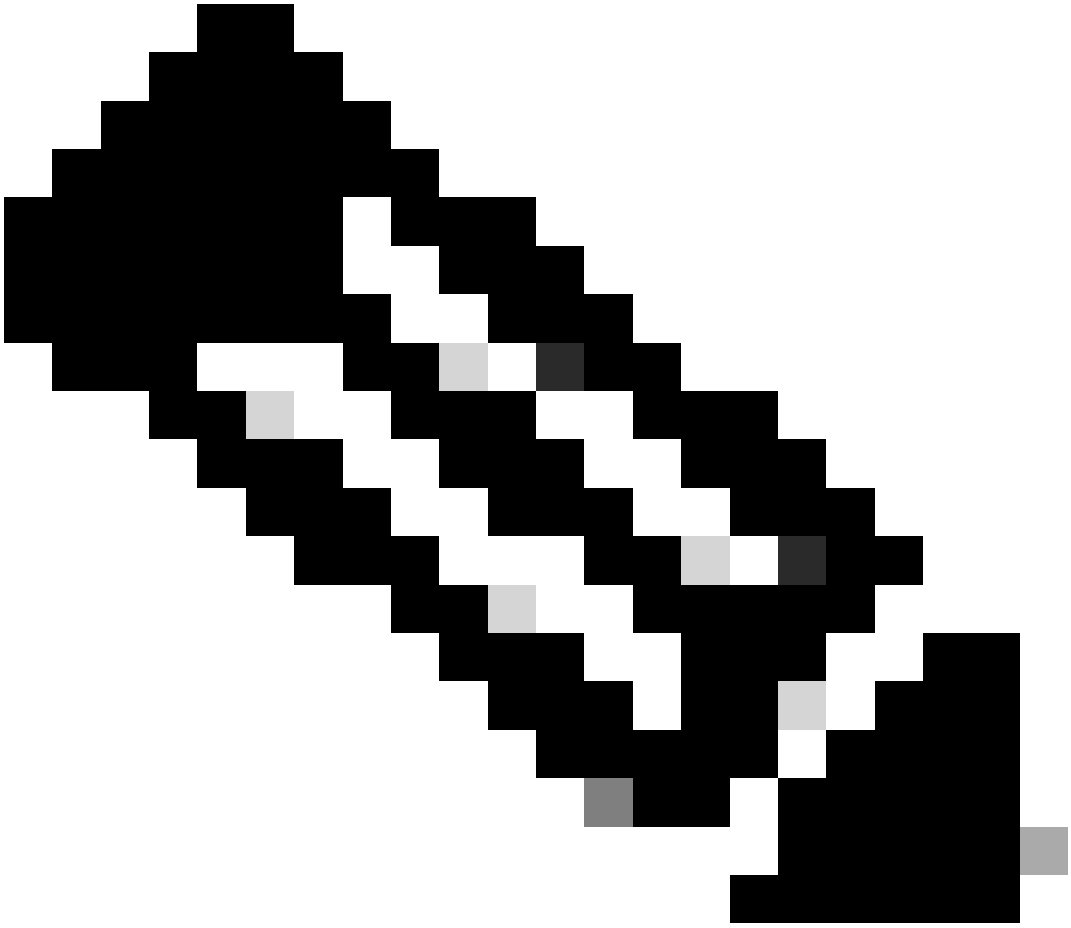
Nota: No puede eliminar un archivo después de haberlo cargado. Sin embargo, puede cargar otro archivo si es necesario.

---

5. En la ventana emergente Seleccionar cuentas virtuales, seleccione la cuenta virtual que recibe el archivo cargado.

El archivo se carga y se muestra en la tabla Archivos de datos de uso de la pantalla Informes. Los detalles que se muestran incluyen el nombre del archivo, la hora a la que se notificó, la cuenta virtual en la que se cargó, el estado de los informes, el número de instancias de productos notificadas y el estado de la confirmación.

6. En la columna Reconocimiento, haga clic en Descargar para guardar el archivo ACK del informe o la solicitud que ha cargado.



Nota: Debe esperar a que el archivo aparezca en la columna Reconocimiento. Si hay muchos informes o solicitudes RUM para procesar, Cisco SSM debe tardar unos minutos.

Después de descargar el archivo, importe e instale el archivo en la instancia del producto

CopyAuthorization Request ACK file

Copie el archivo desde su ubicación o directorio de origen a la memoria flash de la instancia del producto.

```
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)
```

Archivo ACK de solicitud de autorización de instalación

```
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
```

Verificación

Puede utilizar estos comandos para verificar el estado de la licencia:

```
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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).