Configurar licenças HSEC usando SLP em switches Catalyst 9300X Series off-line

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
  - Informações de Apoio
- Configurar
  - Configure o transporte do Smart Licensing como desativado.
  - Instalar uma solicitação ACK confiável
  - Carregue o arquivo de solicitação de confiança para o Cisco SSM e baixe o arquivo ACK.
  - Arquivo CopyTrust ACK
  - Importe e instale o arquivo na instância do produto.
  - Instale uma Solicitação de Autorização com todas as informações necessárias.
  - Carregue o arquivo de solicitação de autorização para o Cisco SSM e baixe o arquivo ACK.
  - Arquivo CopyAuthorization RequestACK
  - arquivo InstallAuthorization RequestACK
- Verificar

Introdução

Este documento descreve como configurar licenças HSEC usando SLP em Switches Catalyst 9300X Series off-line.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão dos conceitos do Cisco Smart Licensing Using Policy (SLP)
- Familiaridade com o gerenciamento de hardware e software do switch Cisco Catalyst 9300X Series
- Experiência de navegação e gerenciamento de licenças no Cisco Smart Software Manager (CSSM)
- Capacidade de usar o CLI em dispositivos Cisco IOS XE
- Conhecimento dos tipos de direitos de licença do Cisco DNA
- Procedimentos para registro de dispositivos e reserva de licenças

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Hardware: Cisco Catalyst C9300X-24Y
- Software: Cisco IOS XE 17.12.04
- Infraestrutura do Smart Licensing: Cisco Smart Software Manager (CSSM)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A licença HSEC (High-Security) permite recursos de segurança avançados em plataformas Cisco, melhorando a proteção de rede, integridade de dados e privacidade. Ele fornece ferramentas robustas para comunicação segura e conformidade com requisitos de segurança rigorosos.

Os principais recursos habilitados pelo HSEC incluem:

- O suporte a VPN facilita a comunicação segura e criptografada em redes públicas, como VPNs IPsec e SSL, para acesso remoto e de site a site.
- Os recursos de criptografia suportam algoritmos criptográficos fortes para proteção de dados, incluindo AES e SHA para garantir confidencialidade, integridade e autenticação.
- O WAN MACsec estende os recursos de criptografia da camada 2 (MACsec) através dos links da WAN, garantindo a segurança de dados de ponta a ponta em redes não confiáveis.
- Aprimoramentos de escalabilidade liberam maior escala para túneis criptografados, como sessões VPN, para suportar grandes implantações.
- A comunicação segura permite recursos como FlexVPN e DMVPN para conectividade dinâmica, escalável e segura.

Configurar

Use a CLI do C9300X para configurar o licenciamento inteligente.

Configure o transporte do Smart Licensing como desativado.

Configuração de CLI:

```
device#conf t

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


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

Instalar uma solicitação ACK confiável

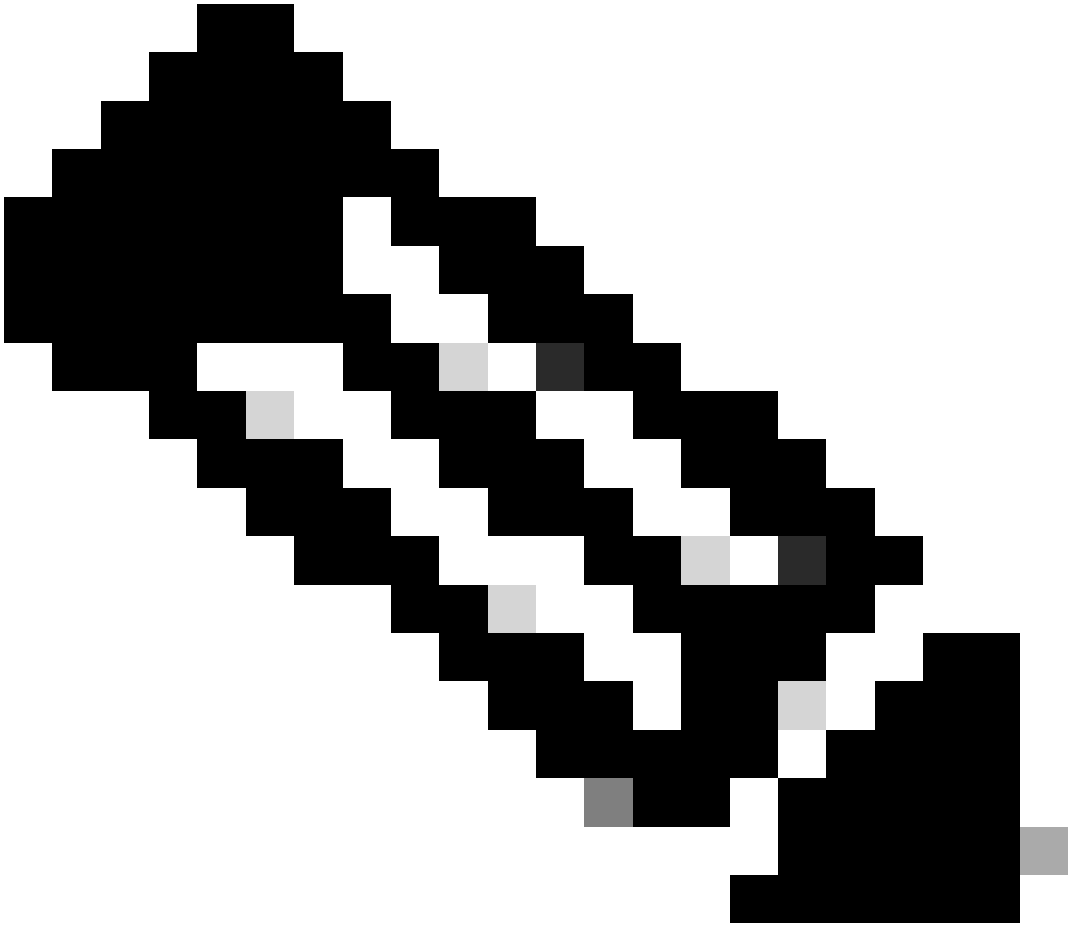
Gere e salve a solicitação de código de confiança para a instância ativa do produto na memória flash.

Configuração de CLI:

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

Carregue o arquivo de solicitação de confiança para o Cisco SSM e baixe o arquivo ACK.

1. Faça login na interface do usuário da Web do Cisco SSM em https://software.cisco.com. Em Smart Software Licensing, clique no link Manage licenses.
2. Selecione a Smart Account que recebe o relatório.
3. Selecione Licenciamento de software inteligente > Relatórios > Arquivos de dados de uso.
4. CLIck Carregar Dados de Uso. Navegue até o local do arquivo (relatório RUM no formato tar), selecione e CLIck Upload Data.

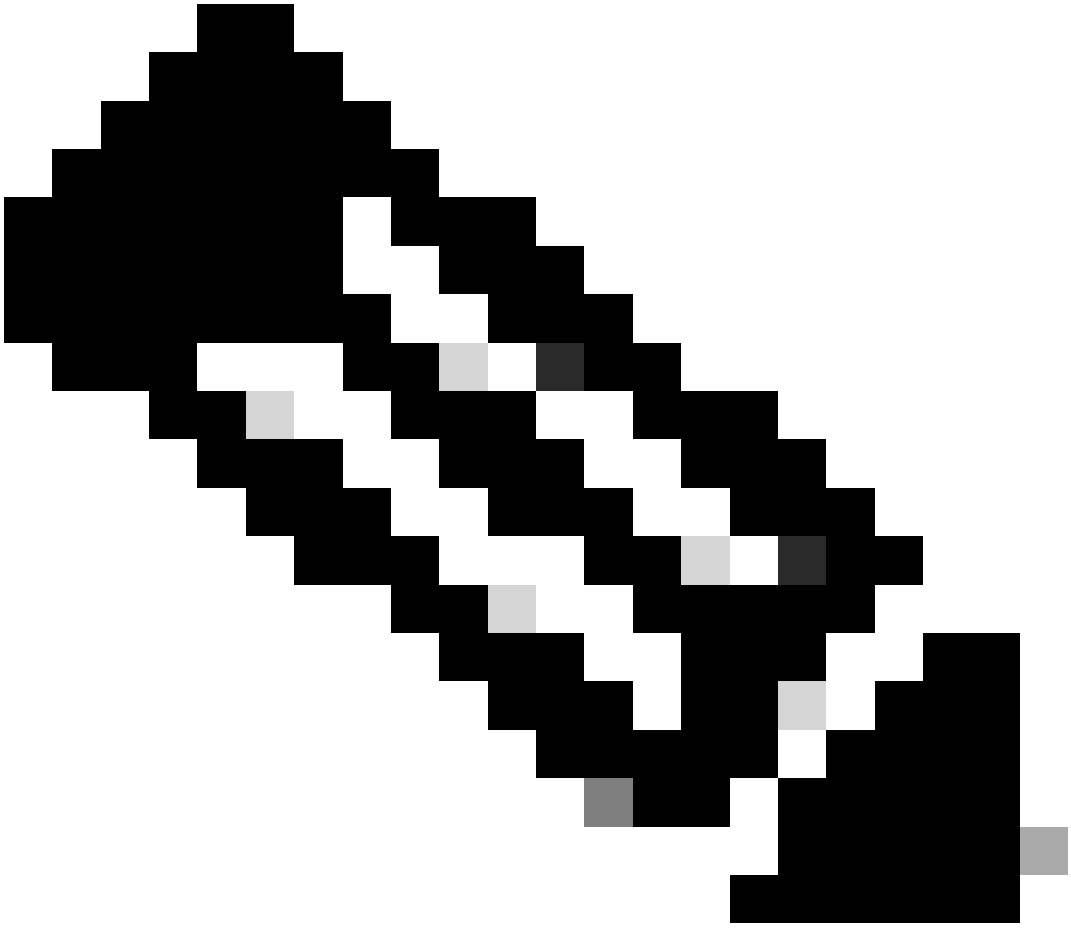


Note: Não é possível excluir um arquivo depois que ele é carregado. No entanto, você pode fazer upload de outro arquivo, se necessário.

5. No pop-up Selecionar Contas Virtuais, selecione a Conta Virtual que recebe o arquivo carregado.

6. O arquivo é carregado e está listado na tabela Arquivos de Dados de Uso na tela Relatórios. Os detalhes exibidos incluem o nome do arquivo, a hora em que ele foi relatado, em que Virtual Account ele foi carregado, o status do relatório, o número de instâncias de produto relatadas e o status da confirmação.

7. Na coluna Confirmação, clique em Download para salvar o arquivo ACK para o relatório ou solicitação que você fez upload.



Note: Você deve aguardar até que o arquivo seja exibido na coluna Confirmação. Se houver muitos relatórios ou solicitações de RUM a serem processados, o Cisco SSM deverá levar alguns minutos.

Depois de fazer o download do arquivo, importe e instale o arquivo na instância do produto

Copiar arquivo ACK confiável

Copie o arquivo do local ou diretório de origem para a memória flash da instância do produto.

Configuração 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 o arquivo na instância do produto.

Configuração de CLI:

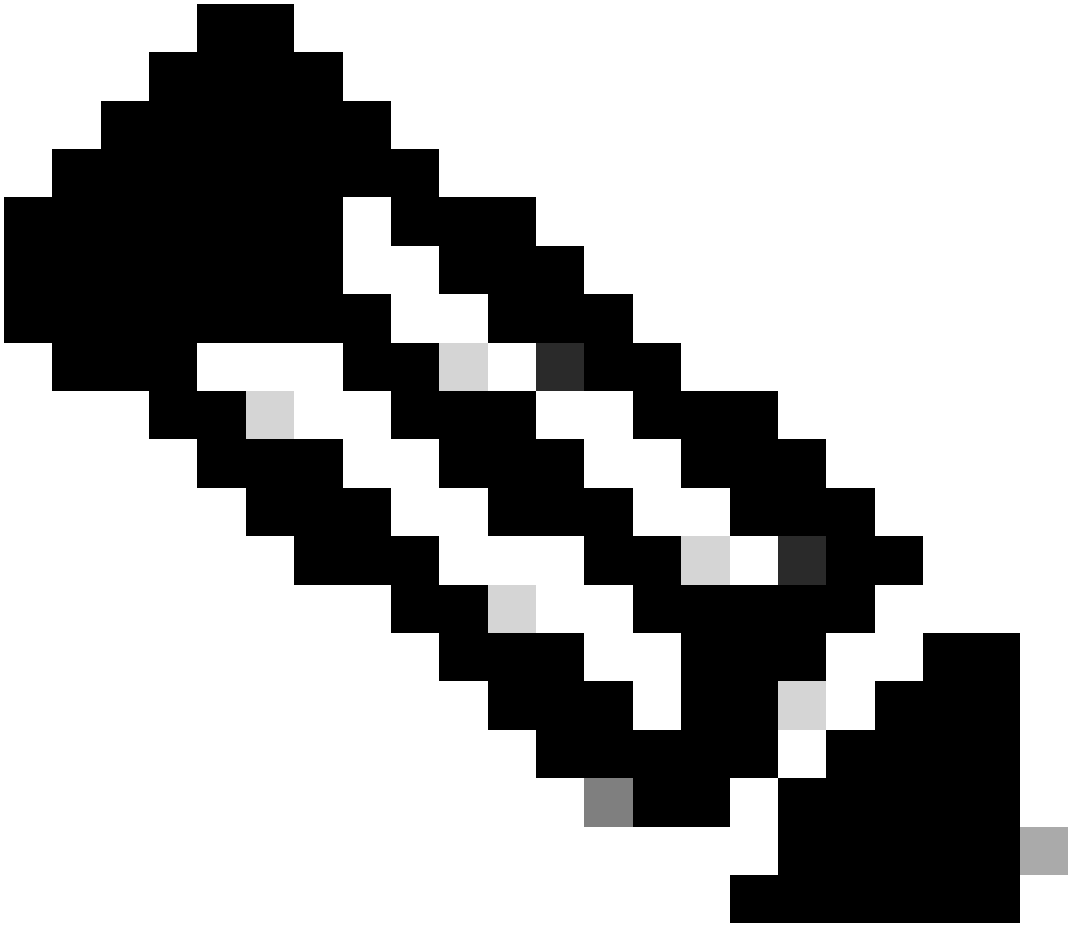
```
device#license smart import flash:ACK_ trust_request.txt

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 uma Solicitação de Autorização com todas as informações necessárias.

Gere e salve a solicitação de autorização para a instância ativa do produto na memória flash.

Configuração de CLI:

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



Note: HSEC: Alta segurança.

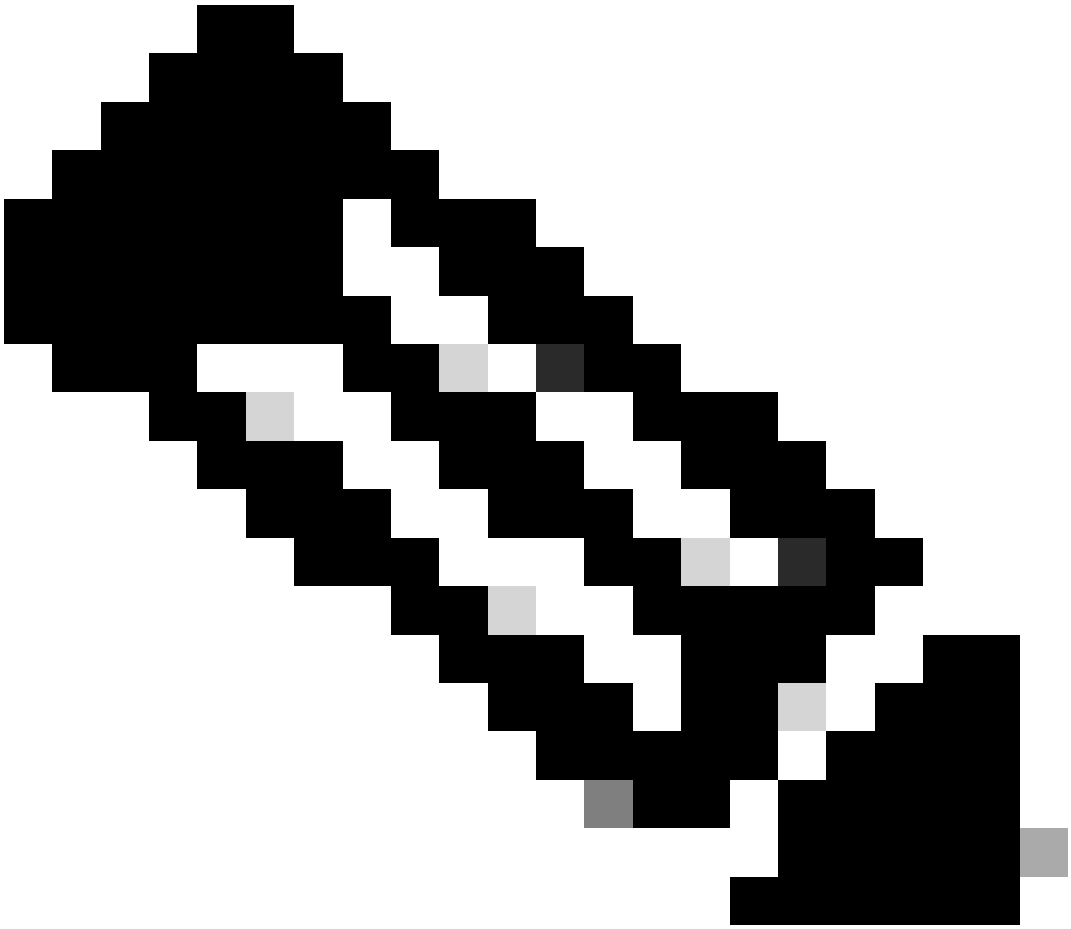
Salve a solicitação de código de autorização para a instância ativa do produto na memória flash.

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

Carregue o arquivo de solicitação de autorização para o Cisco SSM e baixe o arquivo ACK.

1. Faça login na interface do usuário da Web do Cisco SSM em https://software.cisco.com. Em Smart Software Licensing, clique no link Manage licenses.
2. Selecione a Smart Account que recebe o relatório.
3. Selecione Licenciamento de software inteligente > Relatórios > Arquivos de dados de uso.
4. CLIck Carregar Dados de Uso. Navegue até o local do arquivo (relatório RUM no formato

tar), selecione e CLIck Upload Data.

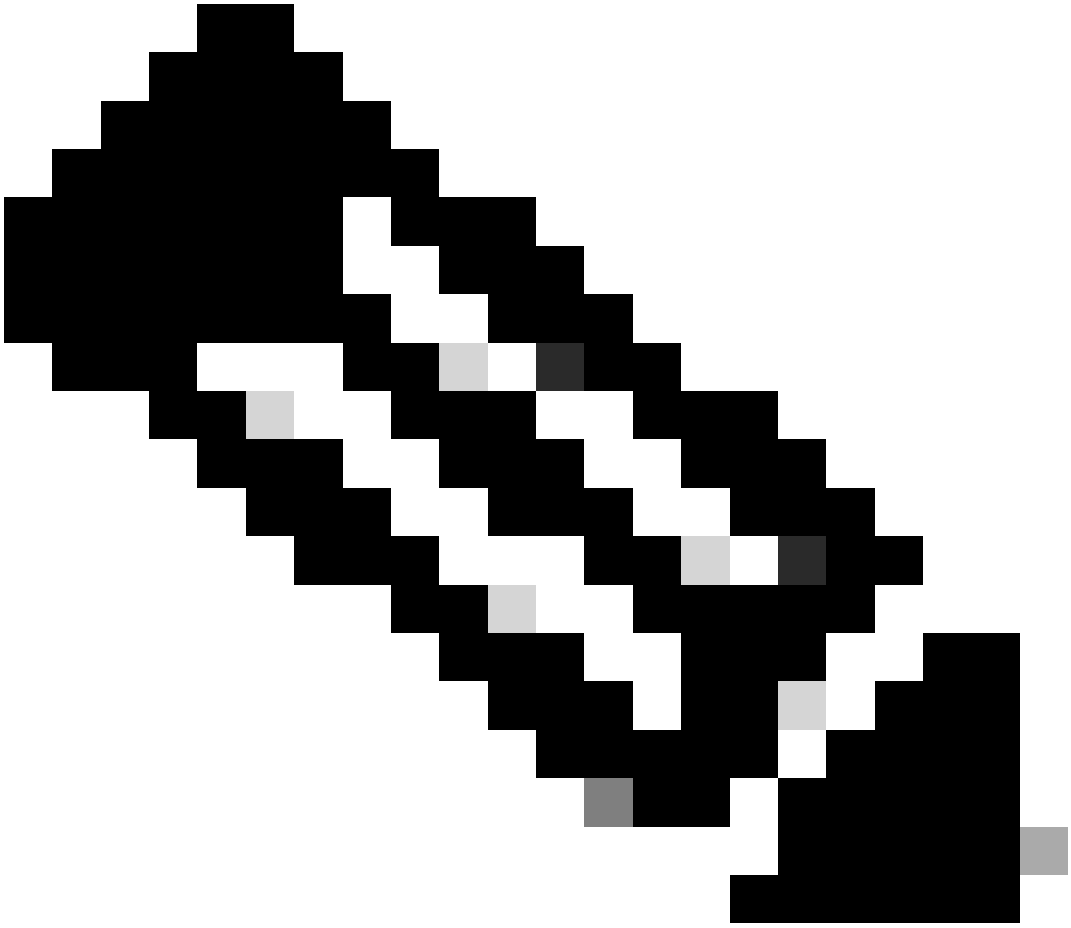


Note: Não é possível excluir um arquivo depois que ele é carregado. No entanto, você pode fazer upload de outro arquivo, se necessário.

5. No pop-up Selecionar Contas Virtuais, selecione a Conta Virtual que recebe o arquivo carregado.

O arquivo é carregado e está listado na tabela Arquivos de dados de uso na tela Relatórios. Os detalhes exibidos incluem o nome do arquivo, a hora em que ele foi relatado, em que Virtual Account ele foi carregado, o status do relatório, o número de instâncias de produto relatadas e o status da confirmação.

6. Na coluna Confirmação, clique em Download para salvar o arquivo ACK para o relatório ou solicitação carregada.



Note: Você deve aguardar até que o arquivo seja exibido na coluna Confirmação. Se houver muitos relatórios ou solicitações de RUM a serem processados, o Cisco SSM deverá levar alguns minutos.

Depois de fazer o download do arquivo, importe e instale o arquivo na instância do produto

Arquivo CopyAuthorization Request ACK

Copie o arquivo do local ou diretório de origem para a memória flash da instância do produto.

```
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)
```

Arquivo InstallAuthorization Request ACK

```
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
```

Verificar

Você pode usar estes comandos para verificar o status da licença:

```
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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.