Configurazione delle licenze HSEC con SLP sugli switch Catalyst serie 9300X non in linea

Sommario

Introduzione

In questo documento viene descritto come configurare le licenze HSEC con SLP sugli switch Catalyst serie 9300X.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Informazioni sui concetti di Cisco Smart Licensing basato su criteri (SLP)
- Familiarità con la gestione hardware e software dello switch Cisco Catalyst serie 9300X
- Esperienza nella navigazione e nella gestione delle licenze in Cisco Smart Software Manager (CSSM)
- Possibilità di utilizzare la CLI sui dispositivi Cisco IOS XE
- Conoscenza dei tipi di autorizzazione per le licenze Cisco DNA
- Procedure per la registrazione dei dispositivi e la prenotazione delle licenze

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La licenza HSEC (High-Security) offre funzionalità di sicurezza avanzate sulle piattaforme Cisco, migliorando la protezione della rete, l'integrità dei dati e la privacy. Fornisce strumenti affidabili per una comunicazione sicura e la conformità ai rigidi requisiti di sicurezza.

Le funzionalità principali abilitate da HSEC includono:

- Il supporto VPN semplifica la comunicazione protetta e crittografata tra le reti pubbliche, ad esempio IPsec e VPN SSL, per l'accesso da sito a sito e remoto.
- Le funzionalità di crittografia supportano algoritmi di crittografia affidabili per la protezione dei dati, tra cui AES e SHA per garantire la riservatezza, l'integrità e l'autenticazione.
- WAN MACsec estende le funzionalità di crittografia di livello 2 (MACsec) sui collegamenti WAN, garantendo la sicurezza dei dati end-to-end su reti non attendibili.
- I miglioramenti della scalabilità sbloccano una scalabilità più elevata per i tunnel crittografati, ad esempio le sessioni VPN, al fine di supportare installazioni di grandi dimensioni.
- Secure Communication consente funzionalità quali FlexVPN e DMVPN per una connettività dinamica, scalabile e sicura.

Configurazione

Utilizzare la CLI di C9300X per configurare le licenze intelligenti.

Configurare il trasporto di Smart Licensing disattivato.

Configurazione dalla CLI:

```
device#conf t

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


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

Installa una richiesta di ACK di trust

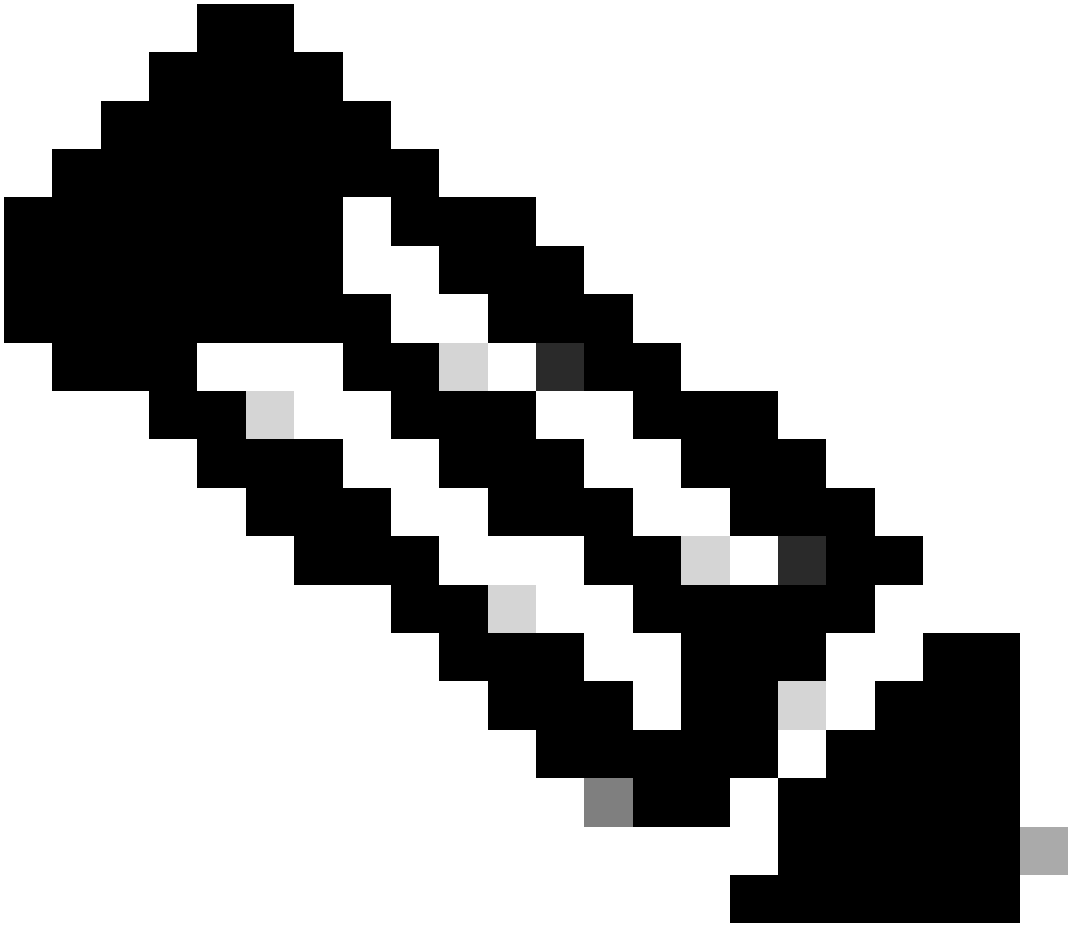
Generare e salvare la richiesta del codice di attendibilità per l'istanza del prodotto attivo nella memoria flash.

Configurazione dalla CLI:

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

Caricare il file di richiesta di trust in Cisco SSM e scaricare il file ACK.

1. Accedere all'interfaccia utente Web di Cisco SSM all'indirizzo https://software.cisco.com. In Smart Software Licensing, fare clic sul collegamento Gestisci licenze.
2. Selezionare lo Smart Account che riceve il report.
3. Selezionare Smart Software Licensing > Report > File di dati di utilizzo.
4. CLIck Carica dati di utilizzo. Individuare la posizione del file (report RUM in formato tar), selezionare e fare clic su CLIck Upload Data.

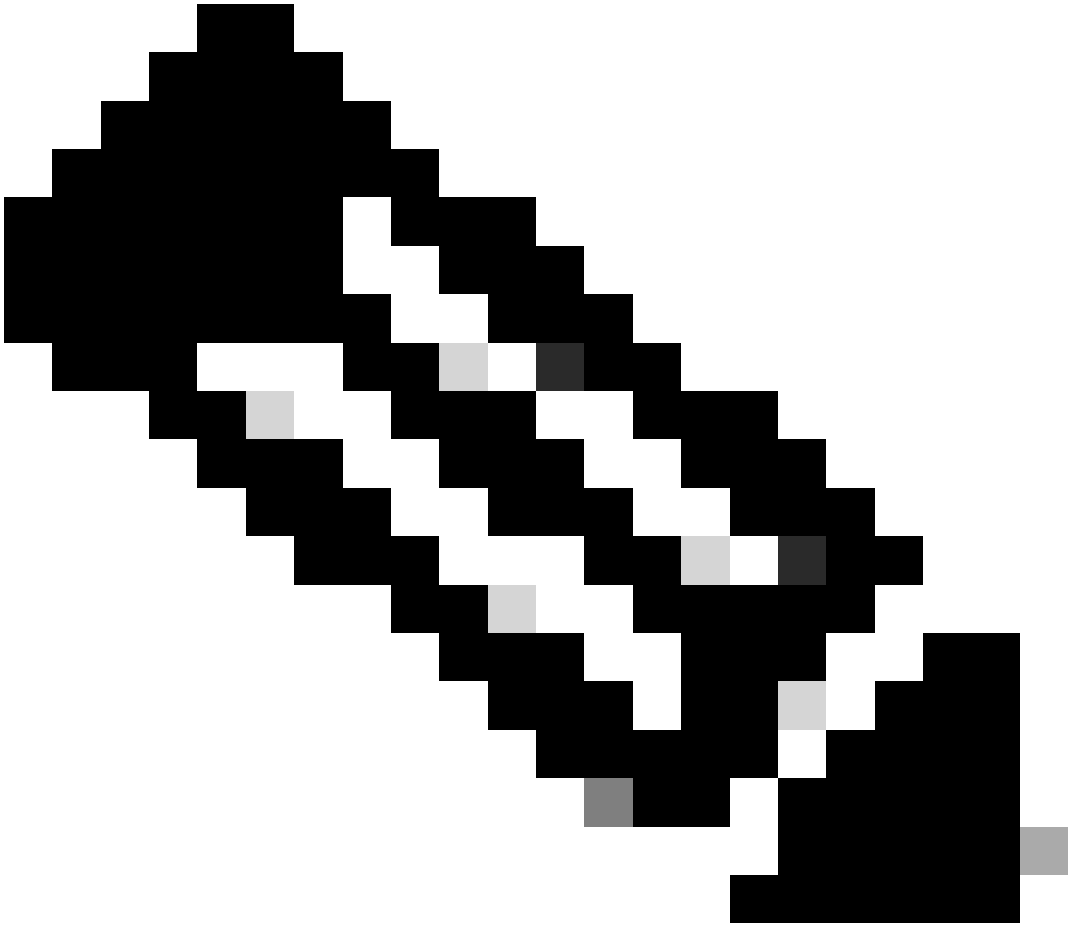


Nota: Non è possibile eliminare un file dopo che è stato caricato. È tuttavia possibile caricare un altro file, se necessario.

5. Dal popup Seleziona account virtuali, selezionare l'account virtuale che riceve il file caricato.

6. Il file viene caricato ed è elencato nella tabella File di dati di utilizzo nella schermata Report. I dettagli visualizzati includono il nome del file, l'ora in cui è stato segnalato, l'account virtuale in cui è stato caricato, lo stato della segnalazione, il numero di istanze del prodotto segnalate e lo stato della conferma.

7. Nella colonna Conferma, fare clic su CLIck Download per salvare il file ACK per il report o la richiesta caricati.



Nota: È necessario attendere che il file venga visualizzato nella colonna Conferma. Se sono presenti molti report o richieste RUM da elaborare, Cisco SSM deve richiedere alcuni minuti.

Dopo aver scaricato il file, importarlo e installarlo nell'istanza del prodotto

Copia file ACK di trust

Copiare il file dal percorso o dalla directory di origine nella memoria flash dell'istanza del prodotto.

Configurazione dalla 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)
```

Importare e installare il file nell'istanza del prodotto.

Configurazione dalla CLI:

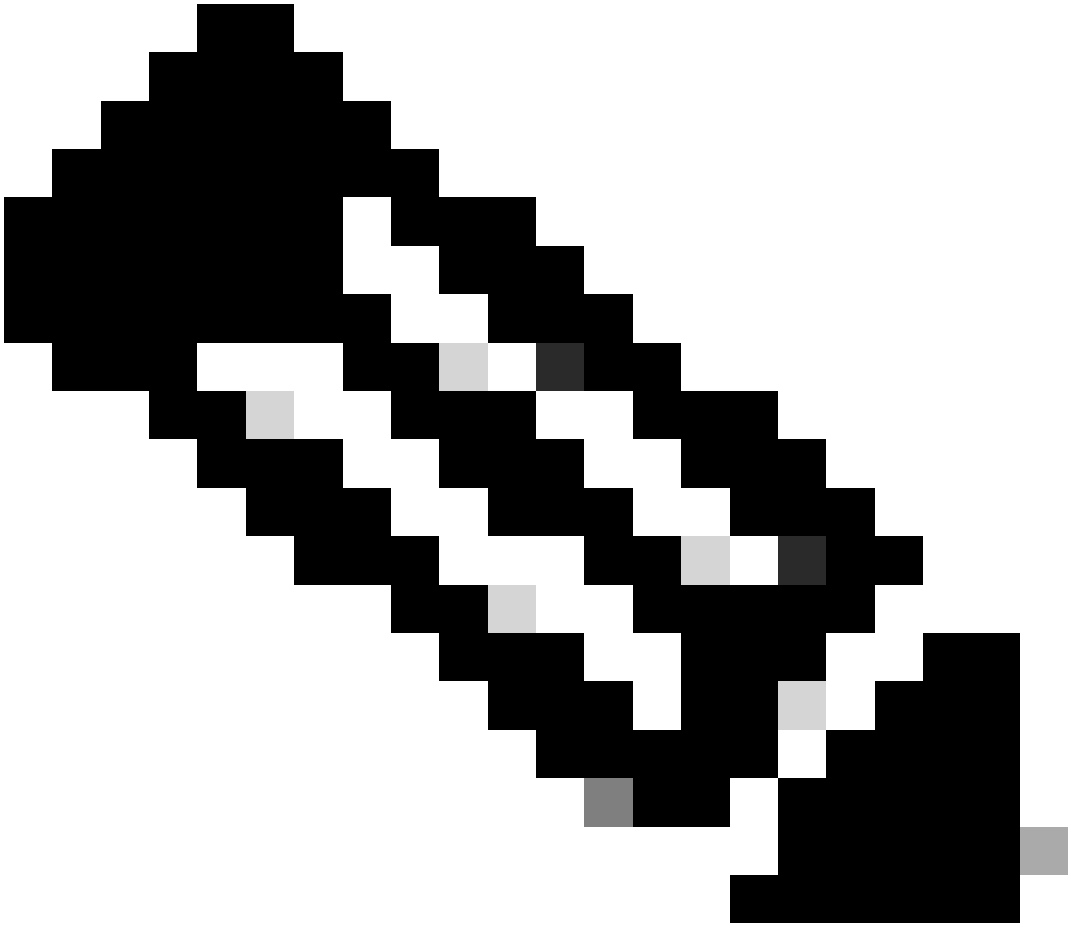
```
device#license smart import flash:ACK_ trust_request.txt

Import Data Successful


device#

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

Installare una richiesta di autorizzazione con tutte le informazioni necessarie.

Generare e salvare la richiesta di autorizzazione per l'istanza di prodotto attiva nella memoria flash.

Configurazione dalla CLI:

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



Nota: HSEC Sicurezza elevata.

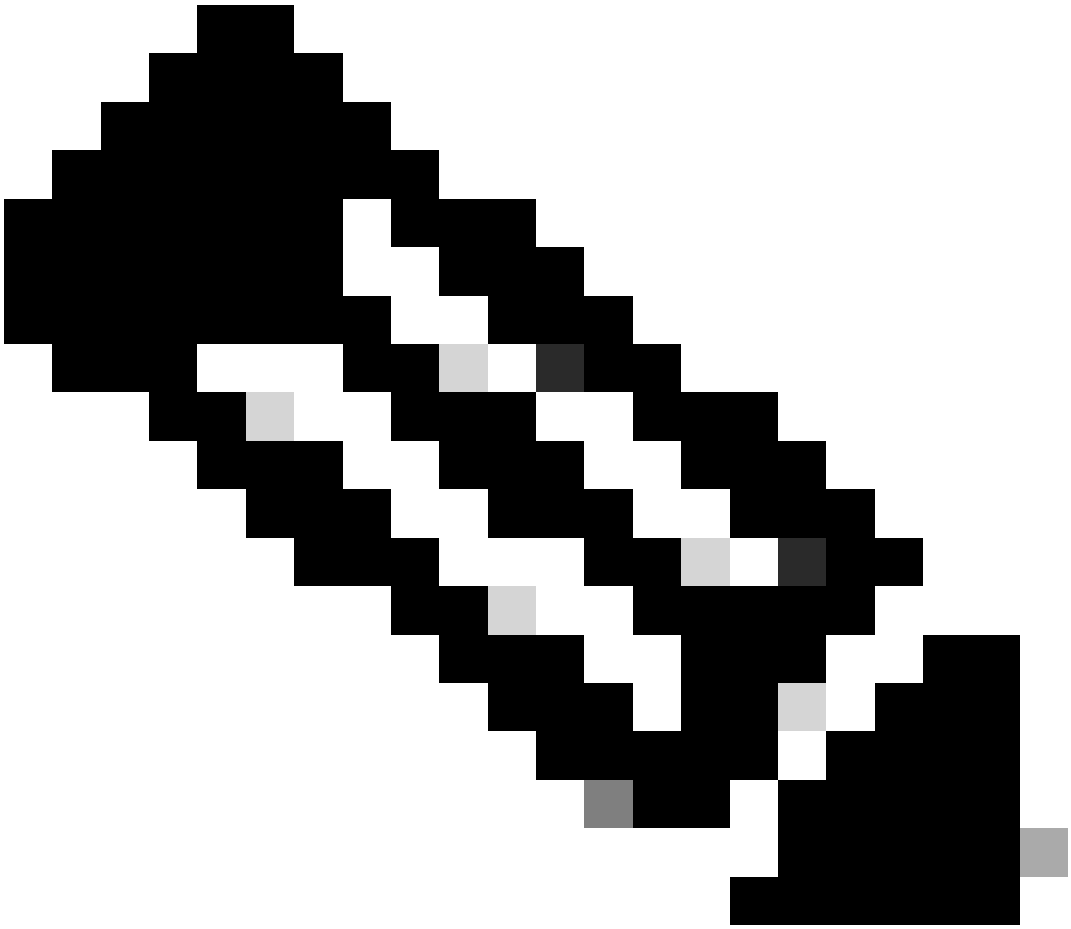
Salvare la richiesta del codice di autorizzazione per l'istanza del prodotto attivo nella memoria flash.

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

Caricare il file di richiesta di autorizzazione in Cisco SSM e scaricare il file ACK.

1. Accedere all'interfaccia utente Web di Cisco SSM all'indirizzo https://software.cisco.com. In Smart Software Licensing, fare clic sul collegamento Gestisci licenze.
2. Selezionare lo Smart Account che riceve il report.
3. Selezionare Smart Software Licensing > Report > File di dati di utilizzo.
4. CLIck Carica dati di utilizzo. Individuare la posizione del file (report RUM in formato tar),

selezionare e fare clic su CLIck Upload Data.

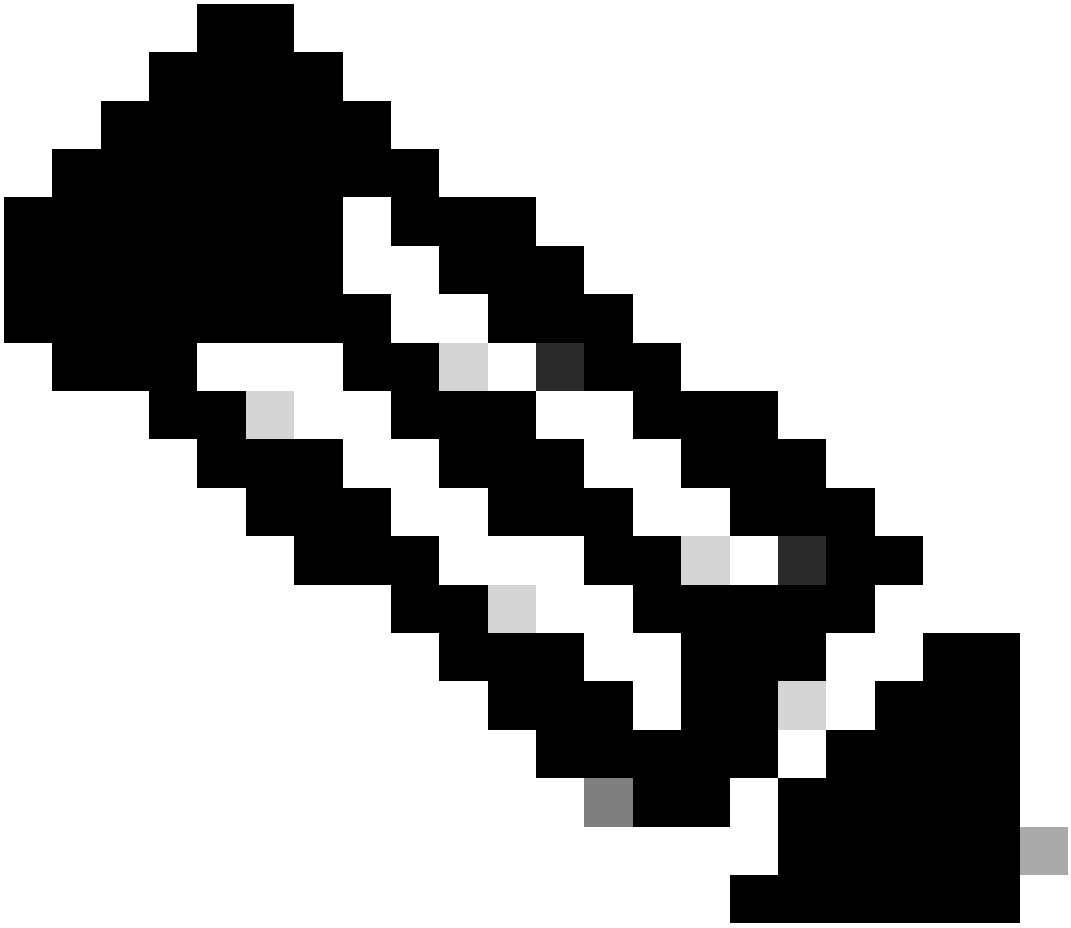


Nota: Non è possibile eliminare un file dopo che è stato caricato. È tuttavia possibile caricare un altro file, se necessario.

5. Dal popup Seleziona account virtuali, selezionare l'account virtuale che riceve il file caricato.

Il file viene caricato ed elencato nella tabella File di dati di utilizzo della schermata Report. I dettagli visualizzati includono il nome del file, l'ora in cui è stato segnalato, l'account virtuale in cui è stato caricato, lo stato della segnalazione, il numero di istanze del prodotto segnalate e lo stato della conferma.

6. Nella colonna Conferma, fare clic su Scarica per salvare il file ACK per il rapporto o la richiesta caricata.



Nota: È necessario attendere che il file venga visualizzato nella colonna Conferma. Se sono presenti molti report o richieste RUM da elaborare, Cisco SSM deve richiedere alcuni minuti.

Dopo aver scaricato il file, importarlo e installarlo nell'istanza del prodotto

File ACK richiesta CopyAuthorization

Copiare il file dal percorso o dalla directory di origine nella memoria flash dell'istanza del prodotto.

```
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)
```

File ACK richiesta 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
```

Verifica

È possibile utilizzare questi comandi per verificare lo stato della licenza:

```
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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).