

オフラインのCatalyst 9300XシリーズスイッチでSLPを使用してHSECライセンスを設定する

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[スマートライセンスの転送をオフに設定します。](#)

[Trust ACK要求のインストール](#)

[信頼要求ファイルをCisco SSMにアップロードし、ACKファイルをダウンロードします。](#)

[CopyTrust ACKファイル](#)

[製品インスタンスにファイルをインポートしてインストールします。](#)

[必要なすべての情報を指定して許可要求をインストールします。](#)

[許可要求ファイルをCisco SSMにアップロードし、ACKファイルをダウンロードします。](#)

[CopyAuthorization RequestACKファイル](#)

[InstallAuthorization RequestACKファイル](#)

[確認](#)

はじめに

このドキュメントでは、オフラインのCatalyst 9300XシリーズスイッチでSLPを使用してHSECライセンスを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Smart Licensing Using Policy(SLP)の概念の理解
- Cisco Catalyst 9300Xシリーズスイッチのハードウェアおよびソフトウェア管理に精通していること
- Cisco Smart Software Manager(CSSM)でのライセンスのナビゲートと管理の経験
- Cisco IOS XEデバイスでCLIを使用する機能
- Cisco DNAライセンスの権限付与タイプに関する知識
- デバイス登録とライセンス予約の手順

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ハードウェア : Cisco Catalyst C9300X-24Y
- ソフトウェア : Cisco IOS XE 17.12.04
- Smart Licensingインフラストラクチャ : Cisco Smart Software Manager(CSSM)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

HSEC(High-Security)ライセンスは、シスコプラットフォーム上で高度なセキュリティ機能を有効にし、ネットワーク保護、データ整合性、プライバシーを強化します。セキュアな通信を実現する堅牢なツールと、厳格なセキュリティ要件へのコンプライアンスを提供します。

HSECによって実現される主な機能は次のとおりです。

- VPNサポートにより、サイト間およびリモートアクセス用に、IPsec VPNやSSL VPNなどのパブリックネットワークを介した安全で暗号化された通信が促進されます。
- 暗号化機能は、機密性、整合性、および認証を確保するためのAESやSHAなど、データ保護のための強力な暗号化アルゴリズムをサポートします。
- WAN MACsecは、レイヤ2暗号化(MACsec)機能をWANリンク全体に拡張し、信頼できないネットワーク上でのエンドツーエンドのデータセキュリティを確保します。
- 拡張性の強化により、VPNセッションなどの暗号化されたトンネルの拡張性が向上し、大規模な導入をサポートできます。
- セキュア通信は、FlexVPNやDMVPNなどの機能を使用して、動的でスケーラブルなセキュアな接続を実現します。

設定

C9300X CLIを使用してスマートライセンスを設定します。

スマートライセンスの転送をオフに設定します。

CLI による設定 :

```
device#conf t
```

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

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

Trust ACK要求のインストール

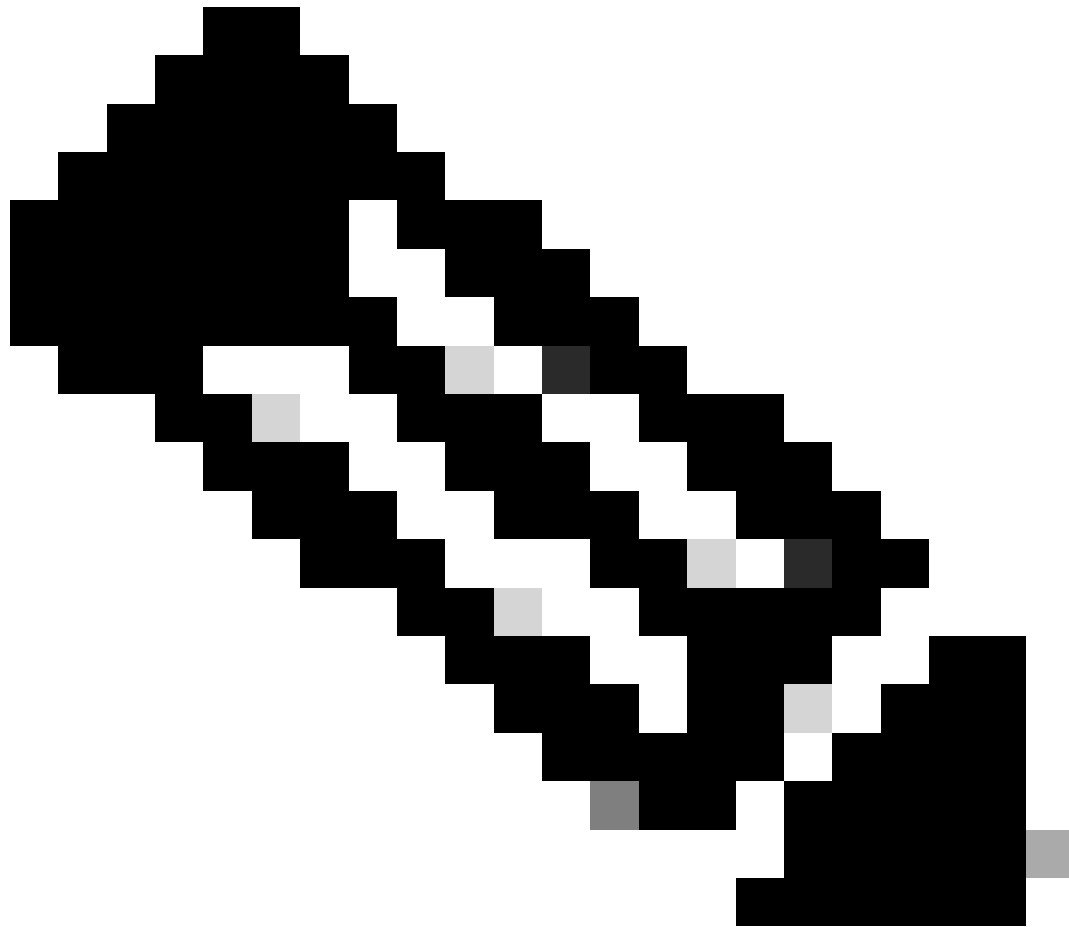
アクティブな製品インスタンスの信頼コード要求を生成してフラッシュに保存します。

CLI による設定：

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

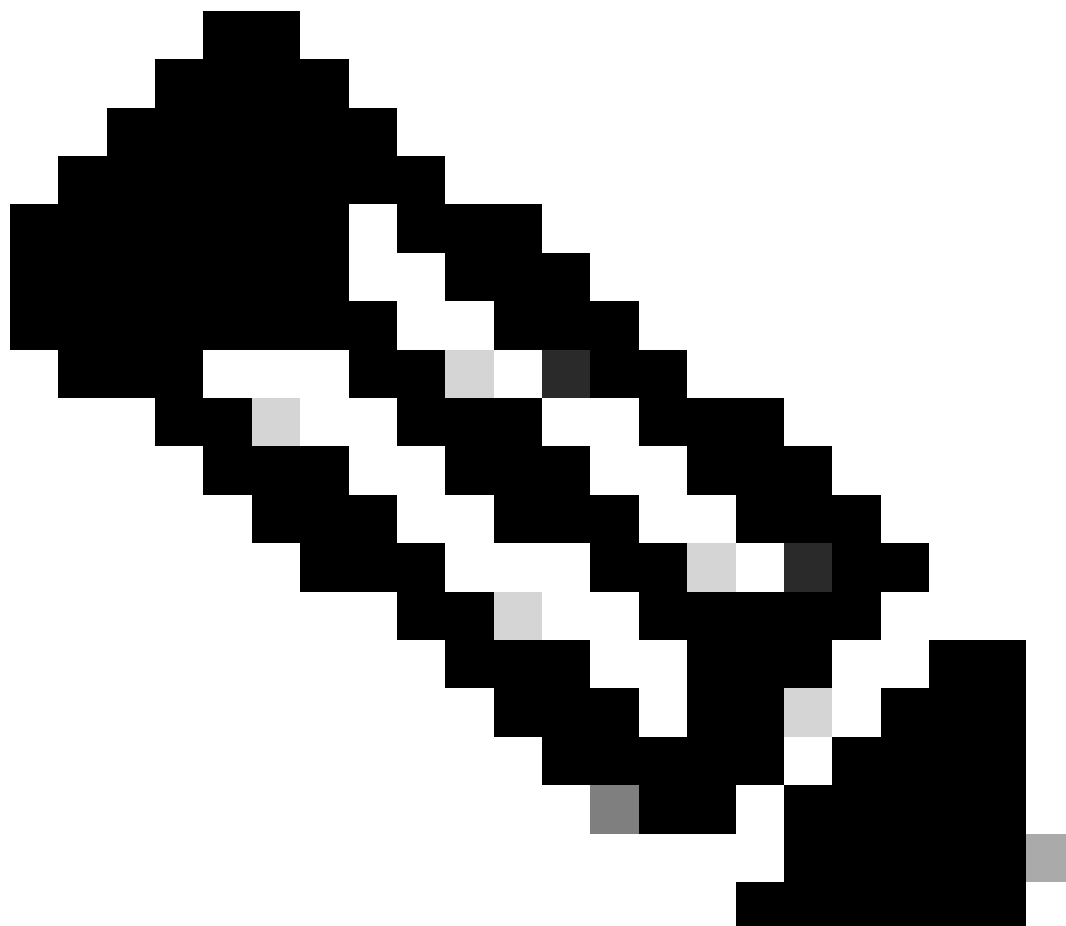
信頼要求ファイルをCisco SSMにアップロードし、ACKファイルをダウンロードします。

1. <https://software.cisco.com>でCisco SSM Web UIにログインします。Smart Software Licensingで、Manage licensesリンクをCLIでクリックします。
2. レポートを受信するスマートアカウントを選択します。
3. Smart Software Licensing > Reports > Usage Data Filesの順に選択します。
4. Click Upload Usage Dataを参照してください。ファイルの場所 (tar形式のRUMレポート) を参照し、を選択して、「データのアップロード」をクリックします。



注：アップロードされたファイルは削除できません。ただし、必要に応じて別のファイルをアップロードすることもできます。

-
5. Select Virtual Accountsポップアップから、アップロードされたファイルを受信する仮想アカウントを選択します。
 6. ファイルがアップロードされ、「レポート」画面の「使用状況データファイル」テーブルに表示されます。表示される詳細には、ファイル名、報告時刻、アップロード先の仮想アカウント、報告ステータス、報告された製品インスタンスの数、および確認ステータスが含まれます。
 7. 「確認」列で「ダウンロード」をクリックし、アップロードしたレポートまたはリクエストのACKファイルを保存します。



注：確認応答の列にファイルが表示されるまで待つ必要があります。RUMレポートまたは処理要求が多数ある場合、Cisco SSMには数分かかる必要があります。

ファイルをダウンロードしたら、製品インスタンスにファイルをインポートしてインストールします

Trust ACKファイルのコピー

ファイルをコピー元の場所またはディレクトリから製品インスタンスのフラッシュメモリにコピーします。

CLI による設定：

```
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)
```

製品インスタンスにファイルをインポートしてインストールします。

CLI による設定 :

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

```
device#
```

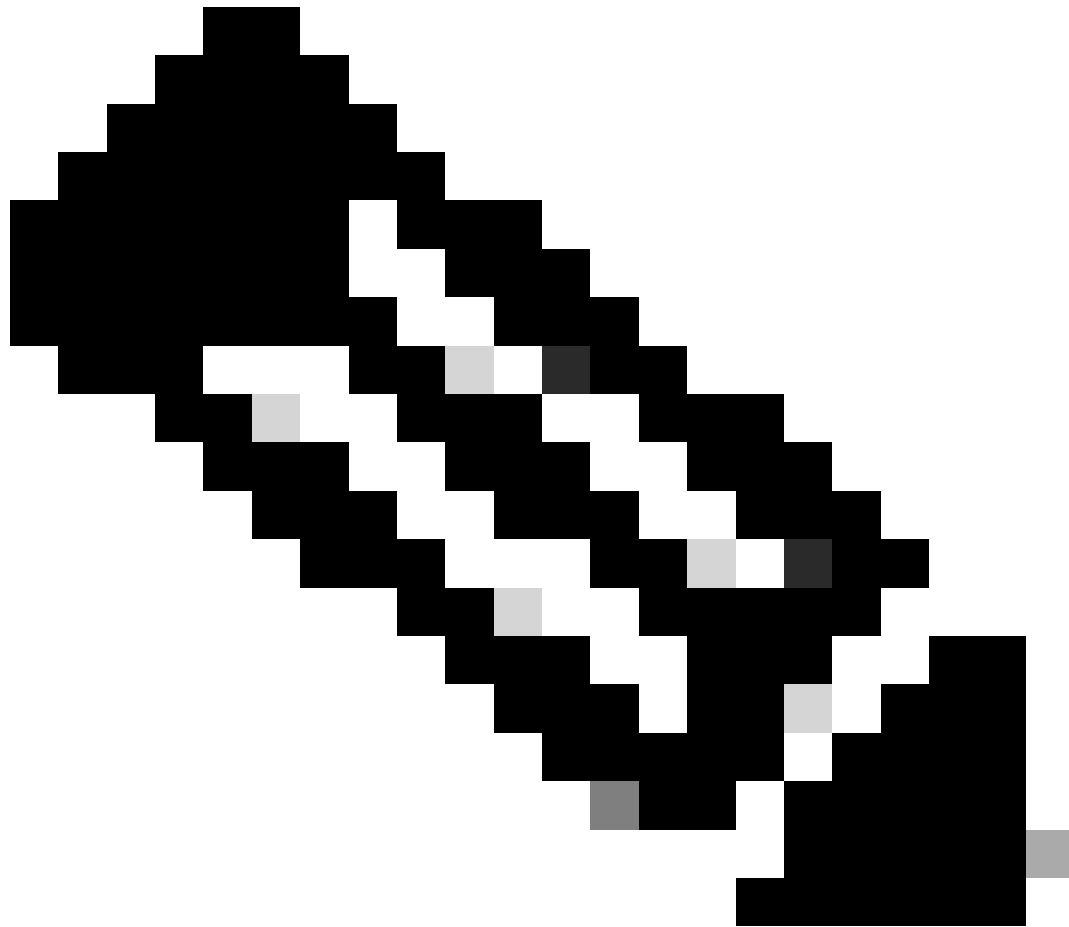
```
*Jun 12 20:01:07.348: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully i
```

必要なすべての情報を指定して許可要求をインストールします。

アクティブな製品インスタンスの許可要求を生成し、フラッシュに保存します。

CLI による設定 :

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



注:HSEC:High Security

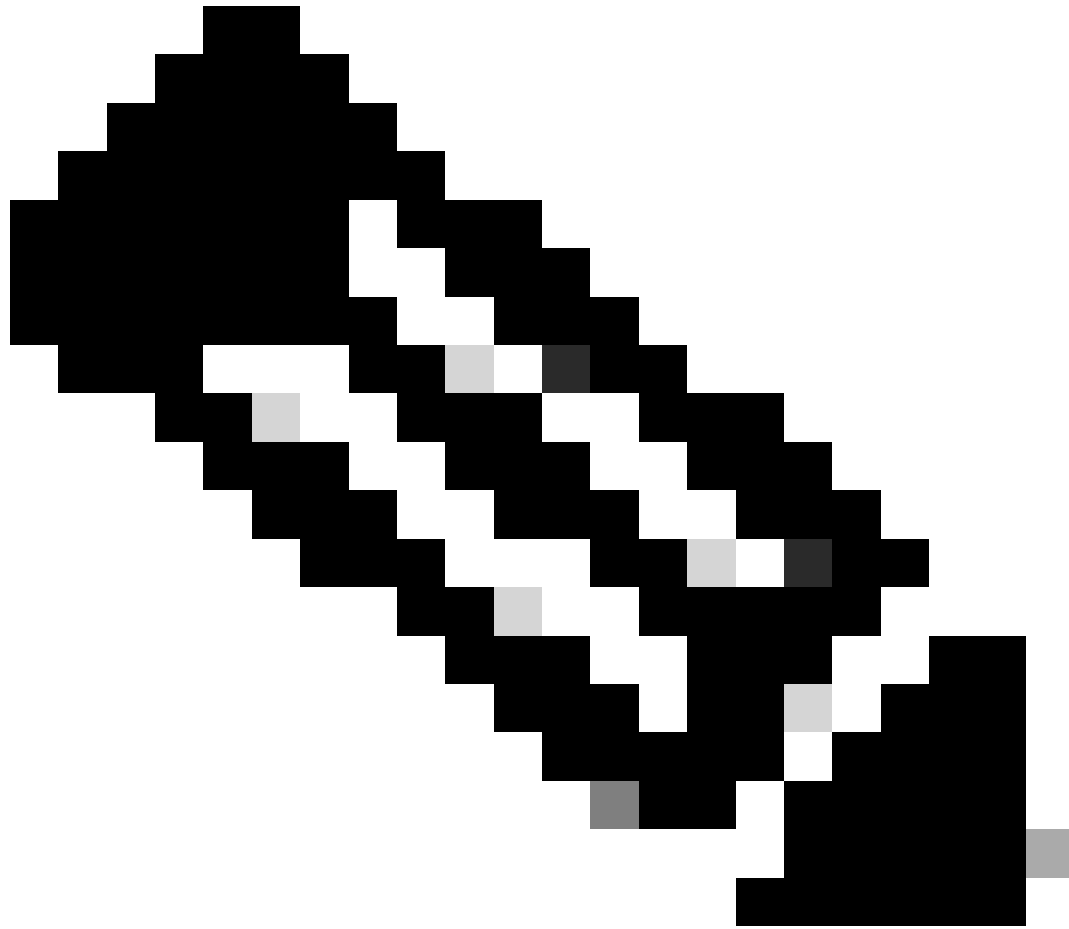
アクティブな製品インスタンスの認証コード要求をフラッシュに保存します。

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

許可要求ファイルをCisco SSMにアップロードし、ACKファイルをダウンロードします。

1. <https://software.cisco.com>でCisco SSM Web UIにログインします。Smart Software Licensingで、Manage licensesリンクをCLIでクリックします。
2. レポートを受信するスマートアカウントを選択します。
3. Smart Software Licensing > Reports > Usage Data Filesの順に選択します。
4. Click Upload Usage Dataを参照してください。ファイルの場所 (tar形式のRUMレポート

)を参照し、を選択して、「データのアップロード」をクリックします。

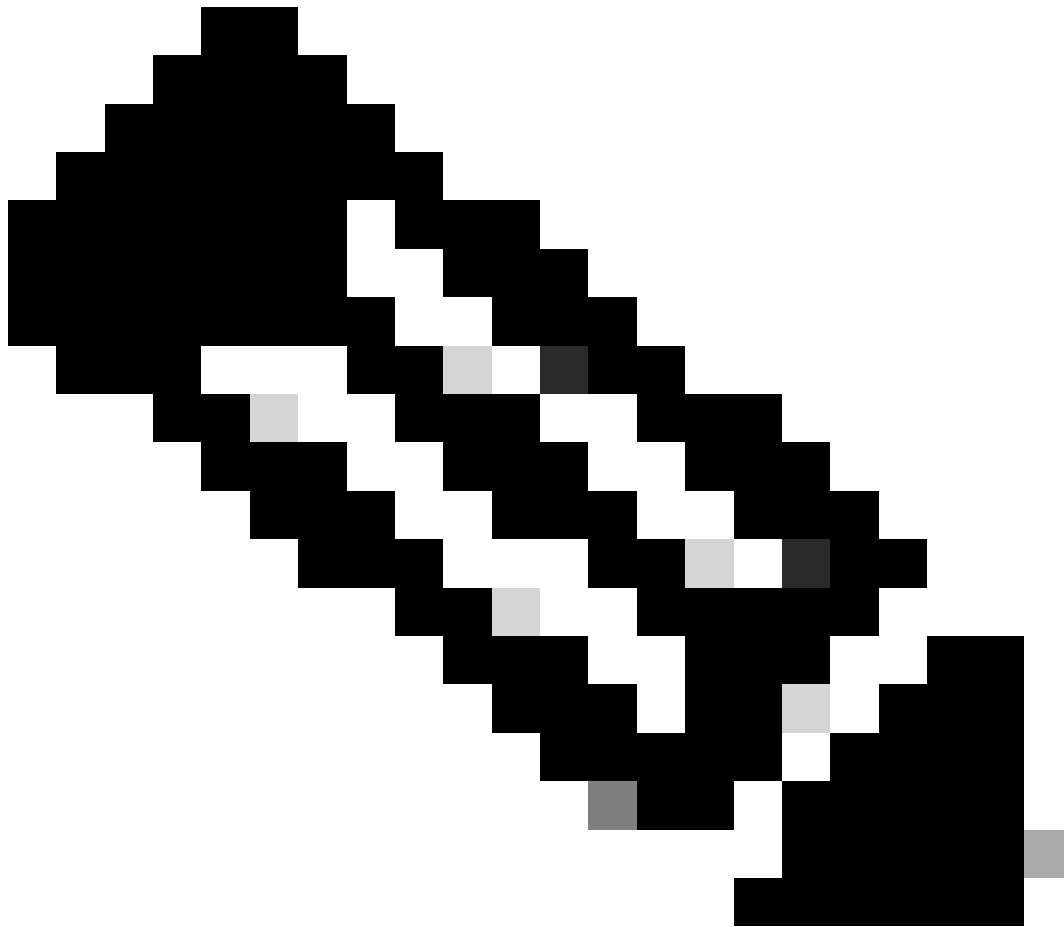


注：アップロードされたファイルは削除できません。ただし、必要に応じて別のファイルをアップロードすることもできます。

5. Select Virtual Accountsポップアップから、アップロードされたファイルを受信する仮想アカウントを選択します。

ファイルがアップロードされ、レポート画面の「使用状況データファイル」テーブルに表示されます。表示される詳細には、ファイル名、報告時刻、アップロード先の仮想アカウント、報告ステータス、報告された製品インスタンスの数、および確認ステータスが含まれます。

6. 「確認」列で「ダウンロード」をクリックし、アップロードしたレポートまたはリクエストのACKファイルを保存します。



注：確認応答の列にファイルが表示されるまで待つ必要があります。RUMレポートまたは処理要求が多数ある場合、Cisco SSMには数分かかる必要があります。

ファイルをダウンロードしたら、製品インスタンスにファイルをインポートしてインストールします

CopyAuthorization Request ACKファイル

ファイルをコピー元の場所またはディレクトリから製品インスタンスのフラッシュメモリにコピーします。

```
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)

InstallAuthorization Request ACKファイル

device#license smart import flash:ACK_auth3.txt

Last Confirmation code UDI: PID:C9300X-24Y,SN:XXXXXXXXXX

Confirmation code: a4a85361

Import Data Completed

Last Confirmation code UDI: PID:C9300X-24Y,SN:XXXXXXXXXX

Confirmation code: a4a85361

device#

*Jun 12 20:05:33.968: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code wa

確認

ライセンスのステータスを確認するには、次のコマンドを使用できます。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。