Configure HSEC Licenses Using SLP on Offline Catalyst 9300X Series Switches

Contents

Introduction

This document describes how to configure HSEC licenses using SLP on Offline Catalyst 9300X Series Switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Understanding of Cisco Smart Licensing Using Policy (SLP) concepts
- Familiarity with Cisco Catalyst 9300X Series switch hardware and software management
- Experience navigating and managing licenses in Cisco Smart Software Manager (CSSM)
- Ability to use the CLI on Cisco IOS XE devices
- Knowledge of Cisco DNA license entitlement types
- Procedures for device registration and license reservation

Components Used

The information in this document is based on these software and hardware versions:

- Hardware: Cisco Catalyst C9300X-24Y

- Software: Cisco IOS XE 17.12.04
- Smart Licensing infrastructure: Cisco Smart Software Manager (CSSM)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The HSEC (High-Security) license enables advanced security capabilities on Cisco platforms, enhancing network protection, data integrity, and privacy. It provides robust tools for secure communication and compliance with stringent security requirements.

Key features enabled by HSEC include:

- **VPN Support** facilitates secure, encrypted communication across public networks, such as IPsec and SSL VPNs, for site-to-site and remote access.
- **Encryption Capabilities** supports strong cryptographic algorithms for data protection, including AES and SHA for ensuring confidentiality, integrity, and authentication.
- **WAN MACsec** extends Layer 2 encryption (MACsec) capabilities across WAN links, ensuring end-to-end data security over untrusted networks.
- **Scalability Enhancements** unlocks higher scale for encrypted tunnels, such as VPN sessions, to support large deployments.
- **Secure Communication** enables features like FlexVPN and DMVPN for dynamic, scalable, and secure connectivity.

Configure

Use the C9300X CLI to configure smart licensing.

Configure smart licensing transport off.

CLI configuration:

```
device#conf t

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


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

Install a Trust ACK request

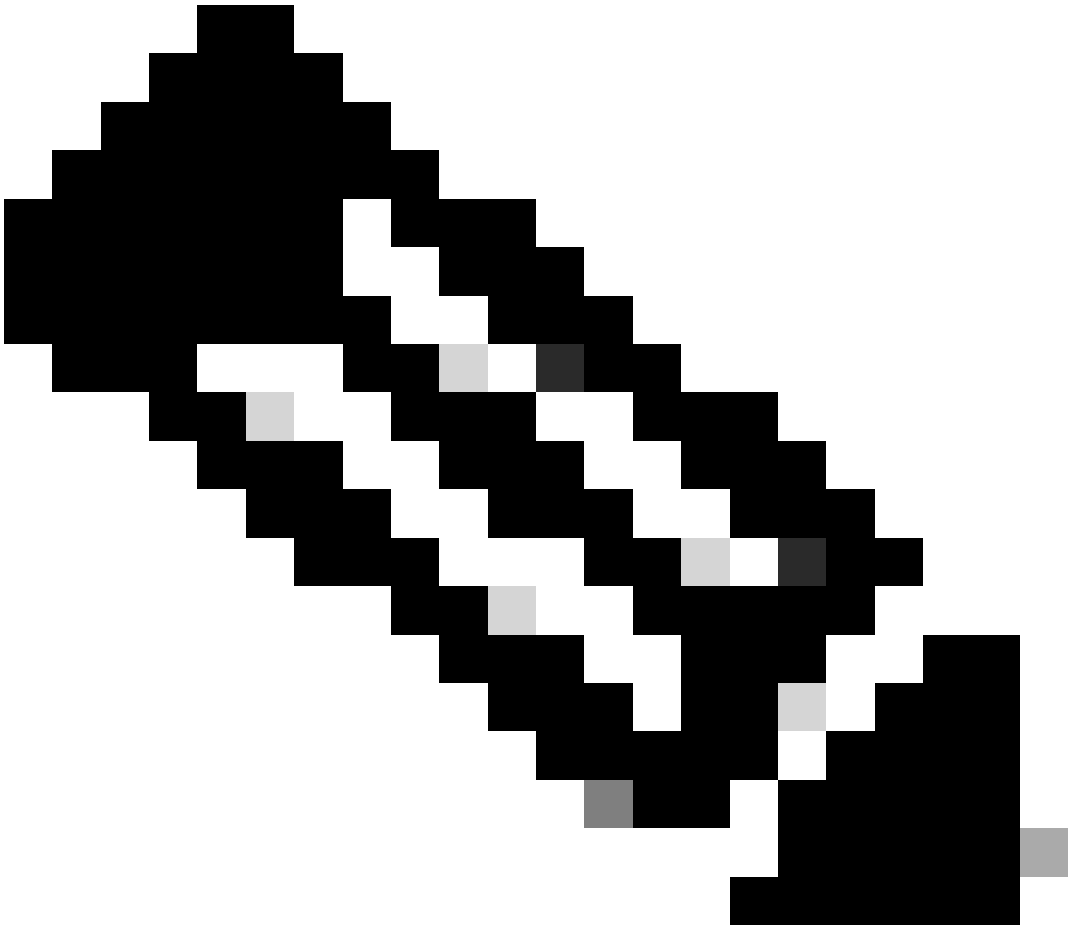
Generate and save the trust code request for the active product instance in the flash.

CLI configuration:

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

Upload the trust request file to Cisco SSM and download the ACK file.

1. Log in to the Cisco SSM Web UI at https://software.cisco.com. Under Smart Software Licensing, CLIck the Manage licenses link.
2. Select the **Smart Account** that receives the report.
3. Select **Smart Software Licensing > Reports > Usage Data Files.**
4. CLIck **Upload Usage Data**. Browse to the file location (RUM report in tar format), select, and CLIck **Upload Data.**



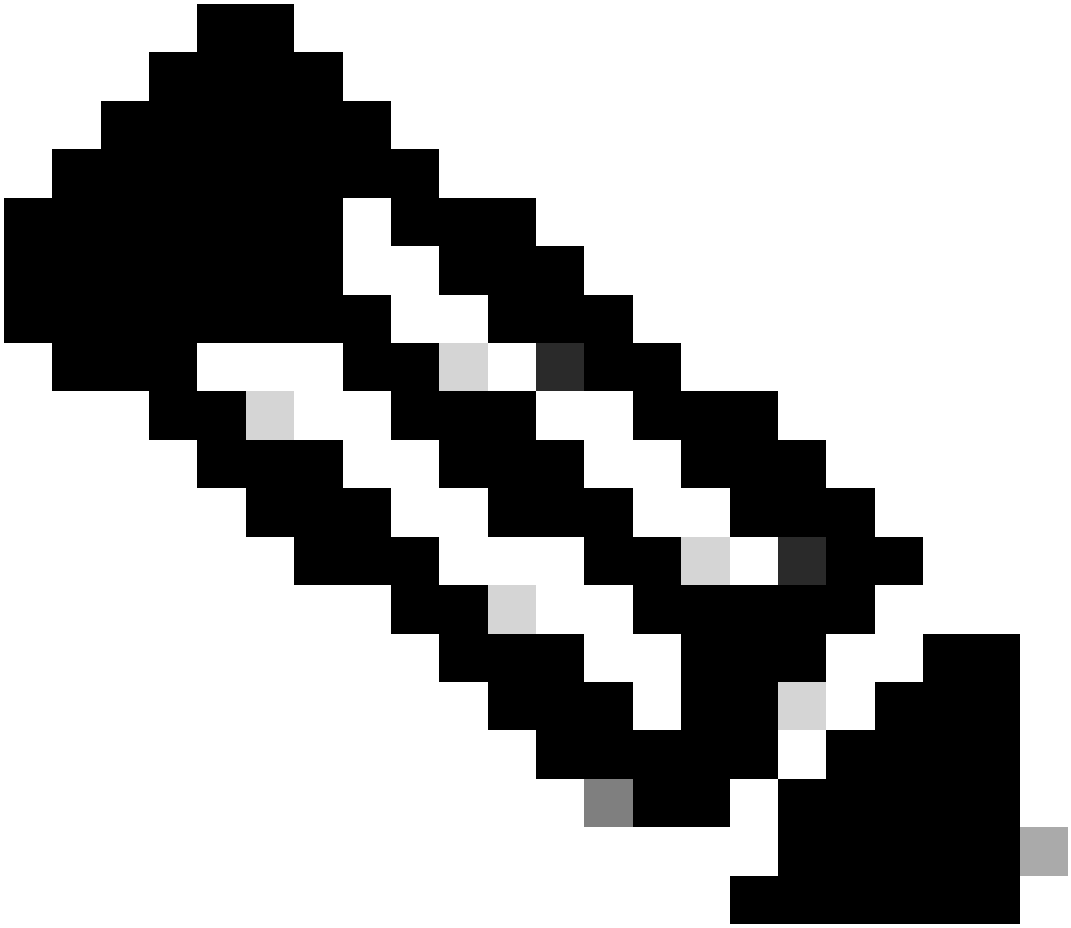
Note: You cannot delete a file after it has been uploaded. You can however upload another file, if required.

---

5. From the **Select Virtual Accounts** pop-up, select the Virtual Account that receives the uploaded file.

6. The file is uploaded and is listed in the **Usage Data Files** table in the Reports screen. Details displayed include the file name, the time at which it was reported, which Virtual Account it was uploaded to, the reporting status, number of product instances reported, and the acknowledgement status.

7. In the Acknowledgement column, CLIck **Download** to save the ACK file for the report or request you uploaded.



> **Note**: You must wait for the file to appear in the Acknowledgement column. If there many RUM reports or requests to process, Cisco SSM must take a few minutes.

After you download the file, import and install the file on the product instance

Copy Trust ACK file

Copy the file from its source location or directory to the flash memory of the product instance.

CLI configuration:

```
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)
```

Import and install the file on the product instance.

CLI configuration:

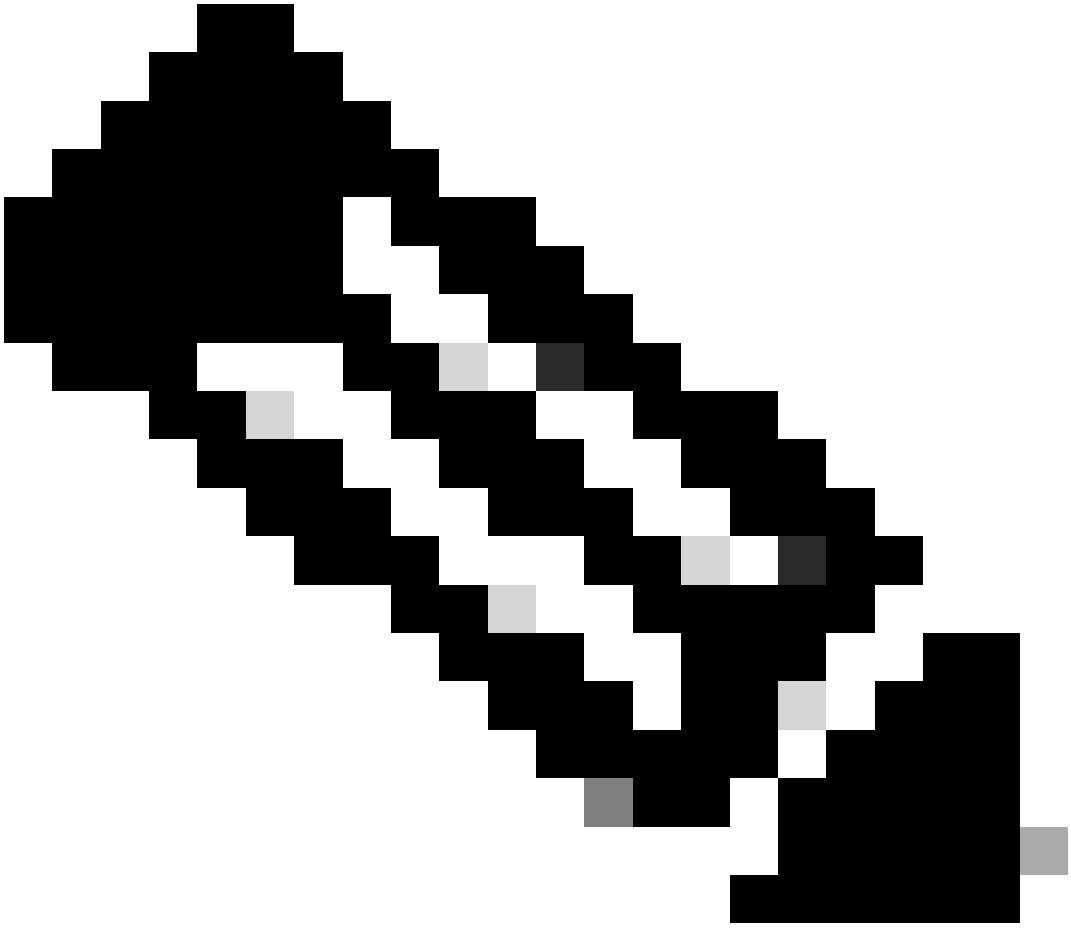
```
device#license smart import flash:ACK_ trust_request.txt

Import Data Successful


device#

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

Install an Authorization Request with all the required information.

Generate and save the Authorization request for the active product instance in the flash.

CLI configuration:

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



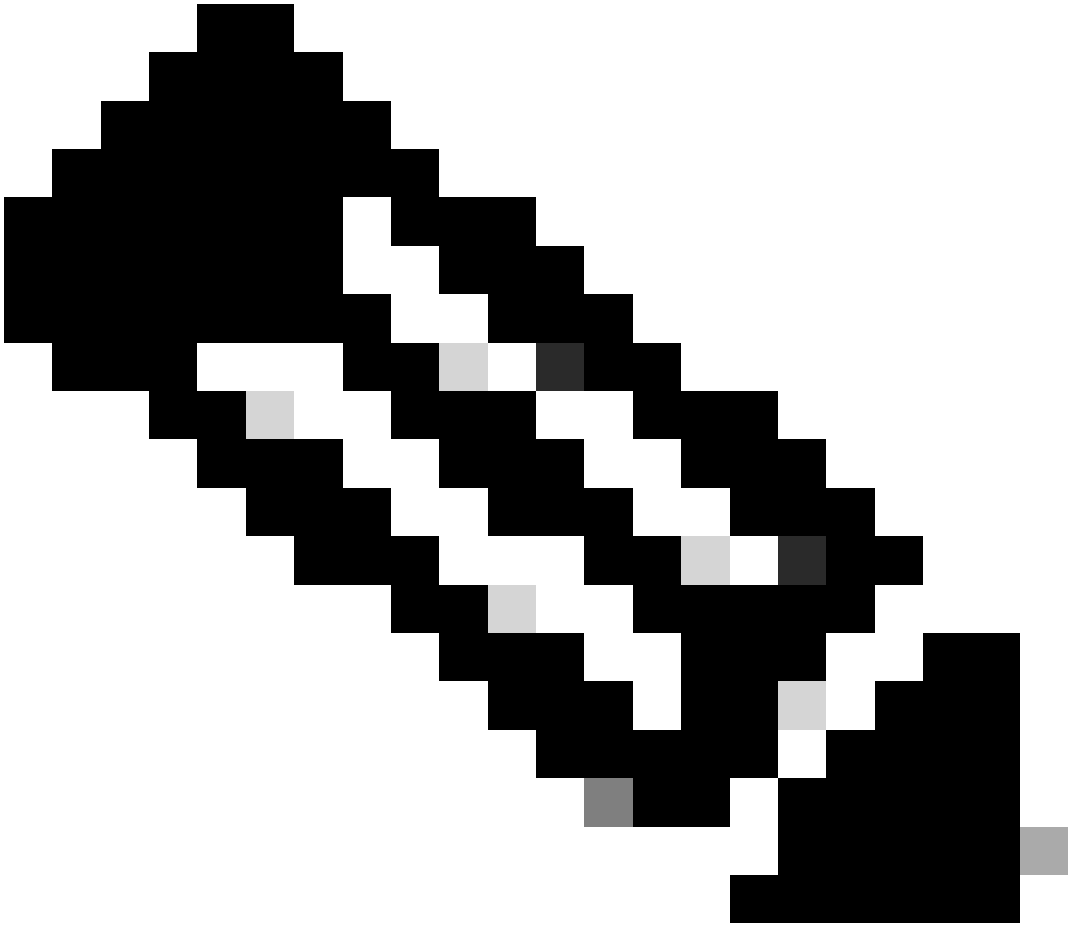
Note: HSEC: High Security.

Save the authorization code request for the active product instance in the flash.

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

Upload the Authorization Request file to Cisco SSM and download the ACK file.

1. Log in to the Cisco SSM Web UI at https://software.cisco.com. Under Smart Software Licensing, CLIck the Manage licenses link.
2. Select the **Smart Account** that receives the report.
3. Select **Smart Software Licensing > Reports > Usage Data Files.**
4. CLIck **Upload Usage Data**. Browse to the file location (RUM report in tar format), select, and CLIck **Upload Data.**

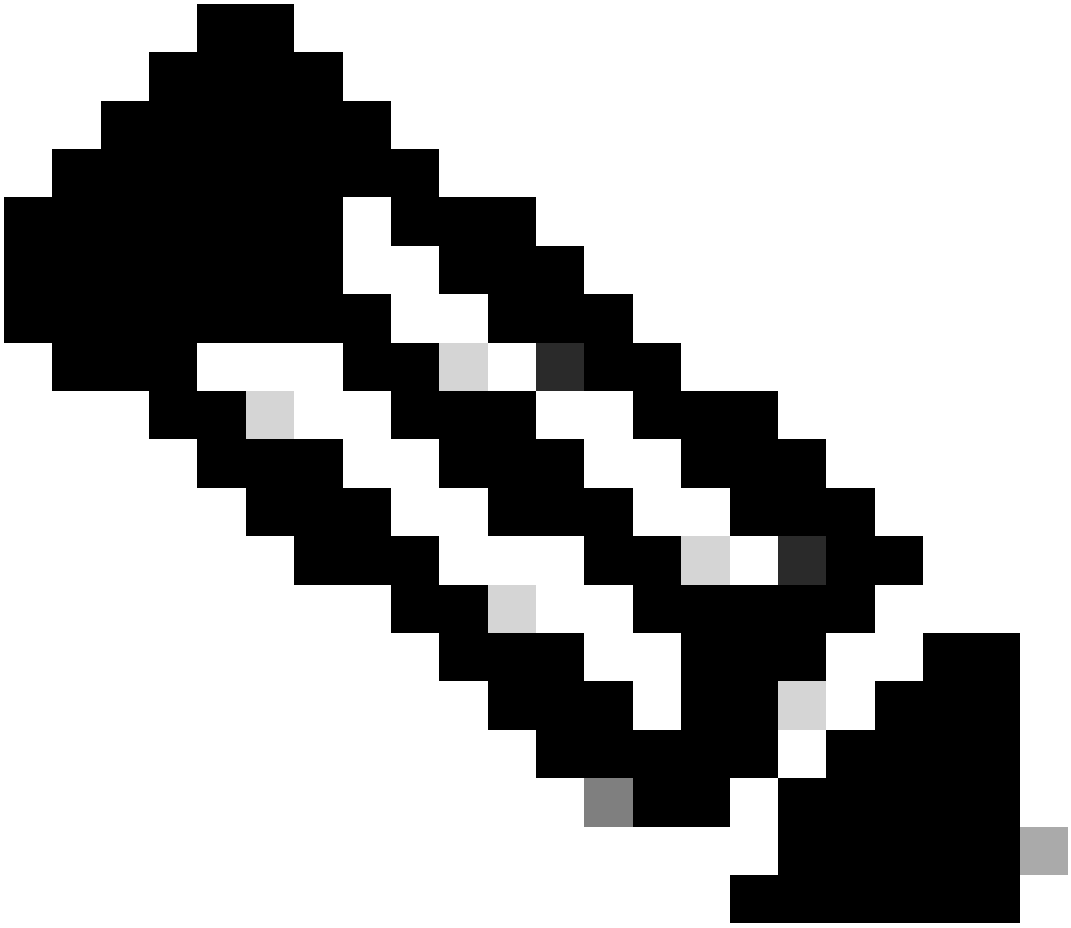


Note: You cannot delete a file after it has been uploaded. You can however upload another file, if required.

5. From the **Select Virtual Accounts** pop-up, select the Virtual Account that receives the uploaded file.

The file is uploaded and is listed in the **Usage Data Files** table in the Reports screen. Details displayed include the file name, the time at which it was reported, which Virtual Account it was uploaded to, the reporting status, number of product instances reported, and the acknowledgement status.

6. In the Acknowledgement column, Click **Download** to save the ACK file for the report or request you uploaded.



Note: You must wait for the file to appear in the Acknowledgement column. If there many RUM reports or requests to process, Cisco SSM must take a few minutes.

After you download the file, import and install the file on the product instance

CopyAuthorization Request ACK file

Copy the file from its source location or directory to the flash memory of the product instance.

```
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 file

```
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
```

Verify

You can use these command to verify License status:

```
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
```