Revised: September 8, 2025

Configuring Licenses on Cisco Catalyst 9000 Series Switches

Configuring Licenses on Cisco Catalyst 9000 Series Switches

This document provides information about the licenses that are available on Cisco Catalyst 9000 Series Switches running Cisco IOS-XE software. It shows how to configure the available licenses, and outlines how to report usage for the licenses you use, to ensure compliance.

Available Licenses

This section lists all the licenses that are available on Cisco Catalyst 9000 Series Switches, license usage guidelines, and ordering considerations.

Base and Add-On Licenses

A base license is a perpetually valid, or permanent license. There is no expiration date for such a license.

An add-on license provides Cisco innovations on the switch, and on the Cisco Catalyst Center. This license has a defined validity period - it is available for a three, five, or seven year subscription period.

This table clarifies the availability of base and add-on licenses across the Cisco Catalyst 9000 Series Switches.

Product	Available Base Licenses	Available Add-on Licenses
Cisco Catalyst 9200 Series Switches	Network Essentials Network Advantage	DNA Essentials DNA Advantage
Cisco Catalyst 9300 Series Switches		
Cisco Catalyst 9400 Series Switches		
Cisco Catalyst 9500 Series Switches		
Cisco Catalyst 9600 Series Switches	Network Advantage	DNA Advantage

For more information, see Cisco Catalyst and Cisco DNA Software Subscription Matrix for Switching.

License and Feature Mapping Information

The software features available on Cisco Catalyst 9000 Series Switches require either a base, or an add-on license.

To know which license levels a feature is available with, use Cisco Feature Navigator at https://cfnng.cisco.com. An account on cisco.com is not required.

Ordering Guidelines for Base and Add-On Licenses

- A base license is ordered and fulfilled only with a perpetual or permanent license type.
- An add-on license is ordered and fulfilled only with a subscription or term license type.

- An add-on license level is included when you choose a network license level. Add-on licenses must be renewed before term expiry, to continue using DNA features.

  Add-on licenses can be deactivated, followed by a switch reload, to discontinue use. The switch then continues operating with base license capabilities.

- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not.

Figure 1: Permitted Base and Add-On License Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes	Yes

Note

The **Network Advantage and DNA Essentials** combination is available only at the time of DNA license renewal, and not with the initial or first-time purchase of DNA Essentials.

For more detailed information about ordering these licenses, refer to the corresponding ordering guide:

Cisco Catalyst 9200 Series Switches Ordering Guide

Cisco Catalyst 9300 Series Switches Ordering Guide

Cisco Catalyst 9400 Series Switches Ordering Guide

Cisco Catalyst 9500 Series Switches Ordering Guide

Cisco Catalyst 9600 Series Switches Ordering Guide

Export Control Key for High Security or HSECK9 key

Products and features that provide cryptographic functionality are within the purview of U.S. export control laws (the U.S. Government Encryption and Export Administration Regulations (EAR)).

The Export Control Key for High Security (HSECK9 key) is an export-controlled license, which authorizes the use of cryptographic functionality.

These sections provide information about the Cisco Catalyst 9000 Series Switches that support the HSECK9 key, the cryptographic features on these products that require the HSECK9 key, what to consider when ordering it, prerequisites, and how to configure it on supported platforms.

When an HSECK9 Key Is Required and Which Products Support It

An HSECK9 key is required only if you want to use certain cryptographic features that are restricted by U.S. export control laws. You cannot enable restricted cryptographic features without it.

This table clarifies the products that support the HSECK9 key, when support is introduced, and which cryptographic feature supported on the product requires the HSECK9 key.

Table 1: HSECK9 Key Product Support and Releases

The HSECK9 is supported on these products…	**Starting with this release…**	**And for this cryptographic feature…**
Cisco Catalyst 9300X Series Switches For information about the SKUs in this series, see the Switch Models in the hardware installation guide.	Cisco IOS XE Bengaluru 17.6.2	IPsec
Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2) and associated line cards	Cisco IOS XE Cupertino 17.8.1	WAN MACsec More specifically, on *customer edge devices* in a point-to-point (P2P) and point-to-multipoint (P2MP) network where the WAN MACsec feature is configured
Cisco Catalyst 9500X Series Switches For information about the SKUs in this series, see the Switch Models in the hardware installation guide.	Cisco IOS XE Cupertino 17.8.1	
Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules (C9400X-SUP-2 and C9400X-SUP-2XL)	Cisco IOS XE Dublin 17.11.1	IPSec

Prerequisites for Using an HSECK9 Key

- Check platform support.

  Ensure that the device on which you want to use an HSECK9 key is one that supports the HSECK9 key. See When an HSECK9 Key Is Required and Which Products Support It.

- Check that the prerequisite license is configured.

  Ensure that the DNA Advantage license is configured on the device. You cannot use an HSECK9 key without DNA Advantage configured.

- Check availability of the required number of HSECK9 keys.

  Ensure that you have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in Cisco Smart Software Manager (Cisco SSM). These platform-specific guidelines help you assess the required number of HSECK9 keys:

Platform	**How to Assess the Required Number of HSECK9 keys**
Cisco Catalyst 9300X Series Switches	One HSECK9 key is required for each UDI where you want to use a cryptographic feature. To understand and evaluate this requirement in the context of a stacking set-up, see Stacking Considerations.

Platform	How to Assess the Required Number of HSECK9 keys
Cisco Catalyst 9500X Series Switches	One HSECK9 key is required for each UDI where you want to use a cryptographic feature. **Note** On Cisco Catalyst 9500X Series Switches, the HSECK9 key is supported only in a standalone setup.
Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules and Cisco Catalyst 9600 Series Supervisor Engine 2	For modular switches, the HSECK9 key is tied to the chassis. Regardless of the number of supervisor modules installed in the chassis, a separate HSECK9 key is required only for each *chassis* UDI where you want to use a cryptographic feature. To understand and evaluate this requirement in the context of a High Availability setup, see High Availability Considerations.

- Implement a Smart Licensing Using Policy topology.

  An HSECK9 key requires authorization before use, because it is restricted by U.S. trade-control laws (export-controlled). This authorisation is provided by a Smart Licensing Authorization Code (SLAC) which must be obtained from Cisco SSM and installed on the device.

  Installing SLAC on the device enables activation and use of the HSECK9 key.

  There are multiple ways in which a device can be connected to Cisco SSM, to obtain a SLAC. Each way of connecting to Cisco SSM is referred to as a *topology,* and is within the framework of the Smart Licensing Using Policy solution.

  Implement one of the supported Smart Licensing Using Policy topologies, so that you can obtain a SLAC.

  Note

  To obtain and install SLAC on supported platforms that are within the scope of this document, refer to the configuration section in this document. There are differences in the configuration process when compared to other Cisco products.

- Follow the right sequence.

  First install SLAC on the device, and only then configure the cryptographic feature. If not, you will have to reconfigure the cryptographic feature after installing SLAC.

- Configure the right interface (only Cisco Catalyst 9600 Series Supervisor Engine 2).

  The interface on which you configure the cryptographic feature must correspond with a line card slot where a line card supporting the cryptographic feature is installed.

Ordering Considerations for an HSECK9 Key

If you plan to use cryptographic functionality on new hardware that you are ordering (supported platforms), provide your Smart Account and Virtual Account information with the order. This enables Cisco to factory-install SLAC, so that you don't have to.

Stacking Considerations for Cisco Catalyst 9300X Series Switches

This section covers HSECK9 considerations and requirements that apply to a device stack with an active, a standby, and one or more members. This is therefore applicable only to Cisco Catalyst 9300X Series Switches.

- Mixed stacking is not support. All the devices in the stack must be Cisco Catalyst 9300X Series Switches. For information about the available C9300X SKUs in the series, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.
- At a minimum, obtain an HSECK9 key and install SLAC for the active device in a stack. For uninterrupted use of the cryptographic feature in the event of a switchover, we recommend that you obtain an HSECK9 key for the standby also. Consider the following scenarios:

  Scenario 1: If the standby device in a stack also uses an HSECK9 key and has SLAC insalled, when a switchover occurs, the system continues operation of the cryptographic functionality on the new active without any interruptions.

  Scenario 2: If the standby device in a stack does not use an HSECK9 key, system messages are displayed - daily and during the switchover.

  A daily system message, which alerts you to the fact that the current standby does not have the requisite HSECK9 key and cryptographic functionality may be disabled when a switchover occurs. It does not affect the functioning of HSECK9-enabled features on the currently active device.

  ```
  IOSXE_SMART_AGENT-6-STANDBY_NOT_AUTHORIZED: Standby is in 'not authorized' state for license hseck9
  ```

  When a switchover occurs and the standby, which does not have an HSCECK9 key becomes the new active, these system messages are displayed, before the device is reloaded.

  ```
  %PLATFORM_IPSEC_HSEC-3-UNAUTHORIZED_HSEC: Switchover happened with IPSec configured but HSEC unauthorized,
   reloading.
  %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp action requested
  %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes exit with reload switch code
  ```

  There are two possible outcomes when the stack comes up, after reload:

  If the *next* new active selected at stack bootup after reload has an HSECK9 key, then the cryptographic functionality in the startup configuration is applied or accepted and the system resumes operation of the cryptographic functionality.

  If the *next* new active selected at stack bootup after reload does not have an HSECK9 key either, then the cryptographic functionality in the startup configuration is rejected and cryptographic functionality is disabled in the entire stack.
- To add a device to an existing stack where cryptographic functionality is already being used, follow either sequence.

  Add the device to the stack, and request SLAC for the entire stack again. See: Example for C9300X: Adding a Member to a Stack Where HSECK9 Keys are in Use, on page 24.

  or

  Install SLAC on the standalone, configure the cryptographic functionality on the standalone device, and finally add the device to the existing stack. See: Example for C9300X: Requesting SLAC on a Standalone and Then Adding it to a Stack Where HSECK9 Keys are In Use, on page 28

High Availability Considerations for Cisco Catalyst 9400 and 9600 Series Switches

This section covers High Availability considerations that apply when using the HSECK9 key and is applicable to Cisco Catalyst 9400 and 9600 Series Switches.

Supported High Availability Setups	Supported Platforms
Dual supervisor setup In this setup, two supervisor modules are installed in a chassis, one being the active and the other, the standby	Supported on Cisco Catalyst 9600 Series Switches and Cisco Catalyst 9400 Series Switches.

Supported High Availability Setups	Supported Platforms
Cisco StackWise Virtual Setup In this setup two chassis are involved. One supervisor module is installed in each chassis, one being the active and the other, the standby.	Supported on Cisco Catalyst 9400 Series Switches.

In both High Availability setups, all licensing information, such as trust codes, SLAC, and RUM reports, are stored on the active supervisor (active product instance) and synchronised with the standby.

Note

When using the HSECK9 key on Cisco Catalyst 9500X Series Switches, a High Availability setup is not supported.

Number of HSECK9 Keys Required in High Availability Setups

The HSECK9 key is tied to the chassis UDI and regardless of the number of supervisors installed, one HSECK9 key is required for each chassis UDI. This requirement translates as follows for the supported High Availability setups.

Dual Supervisor Setup

In a dual supervisor setup, one HSECK9 key is required for each chassis UDI where you want to use a cryptographic feature.

The following sample output shows you how the chassis UDI is displayed in a dual supervisor setup. Note how the same chassis UDI is displayed for the active and standby as well.

```
Device# show license udi
UDI: PID:C9606R,SN:FXS241201WP <<< chassis UDI

HA UDI List:
    Active:PID:C9606R,SN:FXS241201WP
    Standby:PID:C9606R,SN:FXS241201WP
```

Cisco StackWise Virtual Setup

In a Cisco StackWise Virtual setup, at a minimum, you must obtain an HSECK9 key for the chassis with the active supervisor module. But for uninterrupted use of the cryptographic feature in the event of a switchover, we recommend that you obtain an HSECK9 key for both the chassis.

This sample output shows you how the chassis UDI is displayed in a Cisco StackWise Virtual setup. The minimum requirement here is to obtain an HSECK9 key for chassis UDI `C9407R,SN:FXS221500CT`. For uninterrupted use of the cryptographic feature in the event of a switchover, an HSECK9 key must be obtained for `C9407R,SN:FXS221500BN` as well.

```
Device# show license udi
UDI: PID:C9407R,SN:FXS221500CT        <<<<< UDI of chassis with active supervisor

HA UDI List:
    Active:PID:C9407R,SN:FXS221500CT
    Standby:PID:C9407R,SN:FXS221500BN <<<<< UDI of chassis with standby supervisor
```

SLACs Required in High Availability Setups

Each HSECK9 key requires one SLAC.

Dual Supervisor Setup

In a dual supervisor setup, the same SLAC confirmation code is displayed for the active and standby supervisor module, because they are in the same chassis and have the same UDI.

This sample output shows how SLAC information is displayed. Because they have the same UDI, note how the same SLAC confirmation code is displayed for all connected devices. Also note the Total available count, for HSECK9 key - only one is required for each chassis.

```
Device# show license authorization
Overall status:
  Active: PID:C9606R,SN:FXS241201WP
      Status: SMART AUTHORIZATION INSTALLED on Dec 13 05:18:07 2021 UTC
      Last Confirmation code: 7cf1f54a  <<<<<< Confirmation code on active.
  Standby: PID:C9606R,SN:FXS241201WP
      Status: SMART AUTHORIZATION INSTALLED on Dec 13 05:18:07 2021 UTC
      Last Confirmation code: 7cf1f54a  <<<<<< Same confirmation code on standby.

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1

<output truncated>
```

Cisco StackWise Virtual Setup

In a Cisco StackWise Virtual setup, each chassis UDI requires its own HSECK9 key and its own SLAC. Accordingly, the confirmation codes of the active and standby are different.

```
Device# show license authorization
Overall status:
  Active: PID:C9407R,SN:FXS221500CT           <<<<<< UDI of the chassis with active supervisor
      Status: SMART AUTHORIZATION INSTALLED on Jul 07 10:14:04 2022 PDT
      Last Confirmation code: 40ba43d2  <<<<<< Confirmation code for chassis with active supervisor

  Standby: PID:C9407R,SN:FXS221500BN          <<<<<< UDI of the chassis with standby supervisor
      Status: SMART AUTHORIZATION INSTALLED on Jul 07 10:13:45 2022 PDT
      Last Confirmation code: 649e8b1d  <<<<<< Confirmation code for chassis with standby supervisor

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 2
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9407R,SN:FXS221500CT
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9407R,SN:FXS221500BN
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

System Behaviour During Switchover

System behaviour in the event of a switchover depends on the High Availability setup.

Dual Supervisor Setup

In a dual supervisor setup, the system continues uninterrupted operation of the cryptographic feature in case of a switchover.

Since the HSECK9 key is tied to the *chassis* UDI and not a supervisor module, and licensing information on the active is synchronized with the standby, a switchover in this High Availability setup can never result in an interruption in the operation of the cryptographic feature.

Cisco StackWise Virtual Setup

In a Cisco StackWise Virtual setup, system behaviour in the event of a switchover is determined by whether the chassis with the standby supervisor module has an HSECK9 key or not.

Consider the following scenarios.

Scenario 1: If the standby has an HSECK9 key and a switchover occurs, the system continues operation of the cryptographic functionality on the new active, without any interruptions.

Scenario 2: If the standby does not have an HSECK9 key and a switchover occurs, these events occur.

- A daily system message, to alert you to the fact that the current standby does not have the requisite HSECK9 key and cryptographic functionality may be disabled when a switchover occurs. It does not affect the functioning of HSECK9-enabled features on the currently active device.

  ```
  %IOSXE_SMART_AGENT-6-STANDBY_NOT_AUTHORIZED: Standby is in 'not authorized' state
  for license hseck9
  ```

- After a switchover occurs, the standby, which does not have an HSECK9 key, comes up as the new active, and system messages are displayed to alert you to the fact that the new active does not have an HSECK9 key and that the device is reloading.

  ```
  %PLATFORM_IPSEC_HSEC-3-UNAUTHORIZED_HSEC: Switchover happened with IPSec configured
  but HSEC unauthorized, reloading.
  %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp action requested
  %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes exit with reload switch code
  ```

  There are two possible outcomes at bootup, after reload:

  If the *next* new active selected at bootup after reload has an HSECK9 key, then the cryptographic functionality in the startup configuration is applied or accepted and the system resumes operation of the cryptographic functionality.

  If the *next* new active selected at bootup after reload does not have an HSECK9 key either, then the cryptographic functionality in the startup configuration is rejected and cryptographic functionality is disabled.

Hardware Removal and Replacement Considerations for Cisco Catalyst 9400 and 9600 Series Switches

This section covers hardware removal and replacement considerations that apply when using the HSECK9 key and is applicable to Cisco Catalyst 9400 and 9600 Series Switches.

- On Cisco Catalyst 9400 and 9600 Series Switches:

  The HSECK9 key is tied to the chassis.

  Licensing information is saved on the active product instance (active supervisor module). In a High Availability setup, licensing information is synchronized with the standby.

- On Cisco Catalyst 9600 Series Switches:

  The cryptographic feature is configured in interface configuration mode. It corresponds with the line card slot where a linecard supporting the cryptographic feature is installed.

  You can remove and replace a linecard without any interruptions in the operation of the cryptographic functionality, as long as the replacement line card is installed in the *same line card slot*.

When you remove and replace a supervisor module or a linecard, observe these guidelines.

Single Supervisor Setup

In a single supervisor setup, if you remove the active supervisor module and replace it with another one, you must install SLAC again.

If you remove and reinstall the *same* supervisor module, you do not have to reinstall SLAC.

Dual Supervisor Setup and Cisco StackWise Virtual Setup

In a dual supervisor setup (Cisco Catalyst 9400 and 9600 Series Switches) and Cisco StackWise Virtual setup (only Cisco Catalyst 9400 Series Switches), remove and replace one supervisor module at-a-time.

You can start with the active followed by the standby or vice versa. Removing and replacing supervisor modules one at-a-time enables the required licensing information to be retained on the device at all times. It also ensures the operation of the cryptographic feature without any interruptions. If you remove both supervisor modules simultaneously and replace them with other supervisor modules, required licensing information will no longer be available on the device, and you will have to install SLAC again.

If you remove and reinstall the *same* supervisor module, you do not have to reinstall SLAC.

Line Card Removal and Replacement

You can remove and replace a linecard without any interruptions in the operation of the cryptographic functionality, as long as the replacement line card is installed in the *same line card slot*.

If you remove a linecard where cryptographic functionality is configured and install the replacement linecard in a different slot, you may have to reconfigure the cryptographic feature.

For information about the removal and replacement procedures, refer to the corresponding hardware documentation.

Cisco Catalyst 9400 Series Supervisor Module Installation Note.

Cisco Catalyst 9600 Series Supervisor Engine Installation Note and Cisco Catalyst 9600 Series Line Card Installation Note.

Configure Base and Add-On Licenses

After you order and purchase a base or add-on license, you must configure the license on the device before you can use it.

This task sets a license level and requires a reload before the configured changes are effective. Follow these steps to add a license and change the current license.

Step 1 **enable**

Enables privileged EXEC mode. Enter your password, if prompted.

Example:

```
Device> enable
```

Step 2 **configure terminal**

Enters global configuration mode.

Example:

```
Device# configure terminal
```

Step 3 **license boot level** { **network-advantage** [**addon dna-advantage**] | **network-essentials** [**addon dna-essentials**] }

Activates the configured license on the product instance.

- **network-advantage** [**addon dna-advantage**]: Configures the Network Advantage license. Optionally, you can also configure the Digital Networking Architecture (DNA) Advantage license.

- **network-advantage** [**addon dna-advantage**]: Configures the Network Essentials license. Optionally, you can also configure the Digital Networking Architecture (DNA) Essentials license.

In the accompanying example, the DNA Advantage license will be activated on the product instance after reload.

Example:

```
Device(config)# license boot level network-advantage add-on dna-advantage
```

Step 4 **exit**

Returns to the privileged EXEC mode.

Example:

```
Device(config)# exit
```

Step 5 **copy running-config startup-config**

Saves changes in the configuration file.

Example:

```
Device# copy running-config startup-config
```

Step 6 **show version**

Shows currently configured license information and the license that is applicable after reload.

The "`Technology-package Next reboot`" column displays the change in the configured license that is effective after reload, only if you save the configuration change.

In the accompanying example, the current license level is Network Advantage. Because the configuration change was saved, the "`Technology-package Next reboot`" column shows that the DNA Advantage license will be activated after reload.

Example:

```
Device# show version

<output truncated>
Technology Package License Information:

------------------------------------------------------------------
Technology-package                          Technology-package
Current              Type                   Next reboot
------------------------------------------------------------------
network-advantage    Smart License          network-advantage
                     Subscription Smart License dna-advantage

<output truncated>
```

Step 7 **reload**

Reloads the device.

Example:

```
Device# reload
```

Step 8 **show version**

Shows currently configured license information and the license that is applicable after reload.

Example:

```
Device# show version

<output truncated>
Technology Package License Information:

------------------------------------------------------------------------
Technology-package                          Technology-package
Current              Type                   Next reboot
------------------------------------------------------------------------
network-advantage    Smart License          network-advantage
dna-advantage        Subscription Smart License dna-advantage

<output truncated>
```

What's next

Complete usage reporting - if required. To know if reporting is required, you can wait for a system message or refer to the policy, by using **show** commands.

- The system message, which indicates that reporting is required:

  ```
  %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgment will be required in [dec] days.
  ```

  [dec] is the amount of time (in days) left to meet reporting requirements.

- To check reporting requirements in a **show** command, refer to the output of the **show license status** privileged EXEC command and check the `Next ACK deadline` field. This means a RUM report must be sent and the ACK must be installed by this date.

  The method that you can use to send the RUM report, depends on the topology you have implemented. For more information, see: Smart Licensing Using Policy for Cisco Catalyst 9000 Series Switches.

Install SLAC for an HSECK9 Key

This section lists the various methods of installing SLAC for an HSECK9 key for Cisco Catalyst 9300, 9400, 9500, and 9600 series switches.

Prerequisites for Installing SLAC

Ensure that you meet these prerequisites:

The device on which you want to install SLAC is one that supports the HSECK9 key. See When an HSECK9 Key Is Required and Which Products Support It, on page 2.

You have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in Cisco SSM.

You have configured the initial setup as per the applicable Smart Licensing Using Policy topology. For information about all the supported topologies, see Smart Licensing Using Policy for Cisco Catalyst 9000 Series Switches.

Restrictions for Installing SLAC

The only topology that you *cannot* implement if you want to use an HSECK9 key, is one where the product instance is connected to Cisco SSM through a controller. The "controller" here is Cisco Catalyst Center. Cisco Catalyst Center does not provide an option to generate a SLAC for Cisco Catalyst 9000 Sereis Switches that support the HSECK9 key.

Install SLAC When Connected to Cisco SSM Over the Internet

This task shows you how to request and install SLAC when the device (product instance) is connected to Cisco SSM. The product instance may be connected in any one of these ways.

- Directly connected to Cisco SSM, over the internet.
- Connected to Cisco SSM through CSLU, and the product instance initiates communication, that is, the product instance is configured to *push* the required information to CSLU.
- Connected to Cisco SSM through SSM On-Prem, and the product instance initiates communication.

Step 1 **enable**

Enables privileged EXEC mode. Enter your password, if prompted.

Example:

```
Device> enable
```

Step 2 **license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**}

Requests a SLAC from Cisco SSM, CSLU, or SSM On-Prem.

- Specify if you want to add to or replace an existing SLAC:
  - **add**: This adds the requested key to an existing SLAC. The new SLAC will contain all the keys of the existing SLAC, and the requested key.
  - **replace**: This replaces the existing SLAC. The new SLAC will contain only the requested key. All HSECK9 keys in the existing SLAC are returned. When you enter this keyword, the product instance checks if these existing keys are in-use. If they are, an error message is displayed, telling you to first disable the corresponding cryptographic feature.

    On Cisco Catalyst 9300X Series Switches in a stacking setup: If you have added a device where SLAC is not installed, to a stack where SLAC is already installed, use the **replace** and **all** keywords. This returns all HSECK9 keys in the existing SLAC and requests SLAC for all the devices in the stack. You cannot request SLAC for a particular member. Your only options are: either the active, or the entire stack.

    On Cisco Catalyst 9400 Series Supervisor Modules in a Cisco StackWise Virtual set-up: This keyword is not supported . If SLAC is installed only on the active and you want to install it on the standby as well, return the SLAC which is on the active and then request and install SLAC on the active and standby again.

- *feature_name*: Enter `hseck9`, to request and install SLAC for the HSECK9 key.
- Specify the device by entering one of these options:
  - **all**: Gets the authorization code for *all* devices in a High Availability and stacking set-up.

    In case of a stacking setup or a Cisco StackWise Virtual setup, we recommend that you use this option and install SLAC for the active and the standby. This ensures uninterrupted use of the cryptographic feature in the event of a switchover.
  - **local**: Gets the authorization code for the *active* device in a High Availability and stacking set-up. This is the default option.

Example:

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

Step 3 (Optional) **license smart sync** {**all** | **local**}

Triggers the product instance to synchronize with Cisco SSM, CSLU, or SSM On-Prem - as the case may be, to send and receive any pending data.

By synchronizing right-away, you can ensure that the SLAC installation process is completed soon after. Otherwise, SLAC is applied to the product instance only the next time the product instance is *scheduled* to contact Cisco SSM, CSLU, or SSM On-Prem.

Example:

```
Device# license smart sync all
```

What's next

See Required Tasks After Installing SLAC

No Connectivity to CSSM and No CSLU

This task shows you how to request and install SLAC in an air-gapped network, where a device (product instance) cannot communicate online, with anything outside its network.

You generate and save the SLAC request to a file, upload it to the CSSM Web UI, download the SLAC code from the CSSM Web UI, and finaly, install it on the product instance.

Ensure that you have completed Step 1 of the *No Connectivity to CSSM and No CSLU* topology. See Workflow for Topology: No Connectivity to Cisco SSM and No CSLU.

Step 1 **enable**

Enables privileged EXEC mode. Enter your password, if prompted.

Example:

```
Device> enable
```

Step 2 **license smart authorization request** {**add** | **replace**} *feature_name* {**all**| **local**}

Generates a SLAC request with all the required information.

Specify if you want to add to or replace an existing SLAC:

- **add**: Adds the requested key to an existing SLAC. The new authorization code will contain all the keys of the existing SLAC, and the requested license.
- **replace**: Replaces the existing SLAC. The new SLAC will contain only the requested HSECK9 key. All keys in the existing SLAC are returned. When you enter this keyword, the product instance checks if these existing keys are in-use. If they are, an error message is displayed, telling you to first disable the corresponding feature.

Note For a stacking scenario (Cisco Catalyst 9300X Series Switches): If you have added a device (where SLAC is not installed) to an existing stack where SLAC is already installed, use the **replace** and **all** keywords. This returns all HSECK9 keys in the existing SLAC and requests SLAC for all the devices in the stack. You cannot request SLAC for a particular member. Your only options are: either the active, or the entire stack.

Note This keyword is not supported on Cisco Catalyst 9400 Series Supervisor Modules in a Cisco StackWise Virtual set-up. If SLAC is installed only on the active and you want to install it on the standby as well, return the SLAC which is on the active and then request and install SLAC on the active and standby again.

For *feature_name*, enter the name of the export-controlled license for which you want to request an addition or a replacement of the SLAC. Enter "hseck9" to request and install SLAC for the HSECK9 key.

Specify the device by entering one of these options:

- **all**: Gets the SLAC for *all* devices in a High Availability set-up

  In case of a stacking setup or a Cisco StackWise Virtual setup, we recommend that you use this option and install SLAC for the active and the standby. This ensures uninterrupted use of the cryptographic feature in the event of a switchover.

- **local**: Gets the SLAC for the *active* device in a High Availability set-up. This is the default option.

Example:

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

Step 3 **license smart authorization request save***path*

Saves the required UDI information for the SLAC request in a .txt file, in the specified location.

Example:

```
Device# license smart authorization request save bootflash:slac.txt
```

Step 4 Upload the request file to Cisco SSM and download the SLAC file.

This part of the task is performed on the Cisco SSM Web UI.

Note This provision to upload a SLAC *request* file and to then download a SLAC file is supported starting with Cisco IOS XE Cupertino 17.7.1 only. With earlier releases, you have to enter the required information in the Cisco SSM Web UI, generate a SLAC code in the Cisco SSM Web UI, and then download and install it. The older method continues to be available, but the new method is prone to fewer manual errors and is the recommended way for this topology.

a) Log in to the Cisco SSM Web UI at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses** link.
b) Select the **Smart Account** that will receive the report.
c) Select **Smart Software Licensing** > **Reports** > **Usage Data Files**.
d) Click **Upload Usage Data**. Browse to the file location (RUM report in tar format), select, and click **Upload Data**.

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

e) From the **Select Virtual Accounts** pop-up, select the Virtual Account that will receive 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.

f) In the Acknowledgement column, click **Download** to save the ACK or SLAC file for the report or request you uploaded.

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

   After you download the file, import and install the file on the product instance, or transfer it to CSLU or SSM On-Prem.

Step 5 **copy** *source filename* **bootflash:**

(Optional) Copies the file from its source location or directory to the flash memory of the product instance. You can also import the file *directly* from a remote location and install it on the product instance (next step).

- *source*: This is the source location of file. The source can be either local or remote.
- **bootflash:**: This is the destination for boot flash memory.

Example:

```
Device# copy tftp://10.8.0.6/user01/example.txt bootflash:
```

Step 6 **license smart import** *filepath_filename*

Imports and installs the file on the product instance. For *filepath_filename*, specify the location, including the filename. After installation, a system message displays the type of file you installed.

Note If you generated SLAC for multiple product instances (as in a stacking set-up) in the CSSM Web UI, ensure that you download a separate .txt SLAC file for each UDI. Import and install one file at a time.

Example:

```
Device# license smart import bootflash:example.txt
```

What's next

See Required Tasks After Installing SLAC

Install SLAC When Connected to Cisco SSM Through CSLU: CSLU-Initiated Communication

This task shows you how to request and install SLAC when the device (product instance) is connected to Cisco SSM through CSLU and where CSLU initiates communication, that is, CSLU is configured to *pull* the required information from the product instance.

This task requires you to perform certain tasks in Cisco SSM, and certain tasks in the CSLU interface.

Step 1 In CSLU, request authorization codes for one or more devices.

a) Log in to CSLU and navigate to the **Inventory** tab.
b) Select one or more product instances for authorization code request.
c) Select **Actions for Selected** > **Authorization Code Request** > **Accept**

Another modal opens to select a local .csv file for uploading.

Step 2 Log in to Cisco SSM at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses** link.

Step 3 Click **Inventory** > **Product Instances** > **Authorize License Enforced Features**

Step 4 Generate SLAC for a single product instance or for multiple product instances (*choose one*).
Choose from:

- **Generating SLAC for a single product instance:**

  a. Enter the **PID** and **Serial Number**.

  Note Do not populate any of the other fields.

  b. Choose the license, and in the corresponding **Reserve** column, and enter `1`.

Ensure that you choose the correct license for a PID. For Cisco Catalyst Access, Core, and Aggregation Switches where the HSECK9 is supported, select "C9K HSEC".

c. Click **Next**

d. Click **Generate Authorization Code**.

e. Download the authorization code and save as a .csv file.

- **Generating SLAC for multiple product instances (you should have a .csv file to upload in this case)**:

a. From the dropdown list that says “Single Device” (by default), change the selection to “Multiple Devices”.

At this point, a "Download a template" link is displayed. If you don't already have the required template or file, you can download it. Only the serial number and PID are mandatory.

b. Click **Choose File** and navigate to the .csv file, which contains the list of product instances that require SLAC.

c. Once uploaded, the list of devices is displayed in Cisco SSM. All the devices will have the checkbox enabled (implying that you want to request a SLAC for all of them), and click **Next**.

d. Specify the license quantity required for each product instance, and click **Next**.

Note For the "C9K HSEC" license, one SLAC is required for each UDI.

e. Click **Reserve Licenses**.

f. Click **Download Authorization Codes** > **Close**

A.csv file containing all the authorization codes is downloaded.

Step 5 Return to the CSLU interface and go to **Data** > **Import from CSSM**

Drag and drop a file that resides on your local drive, or browse and select the appropriate *.xml file.

If the upload is successful, you will get a message indicating that the file was successfully sent to the server. If the upload is not successful, you will get an import error.

If uploaded successfully, the codes are applied to the product instances, the next time the CSLU runs an update.

What's next

See Required Tasks After Installing SLAC

Install SLAC When Connected to Cisco SSM Through SSM On-Prem: SSM On-Prem-Initiated Communication

This task shows you how to request and install SLAC when the device (product instance), is connected to SSM On-Prem and where SSM On-Prem initiates communication, that is, SSM On-Prem is configured to *pull* the required information from the product instance.

Here you create a request file in SSM On-Prem, upload the request in the Cisco SSM Web UI, generate SLAC, import it into the SSM On-Prem server. Finally, synchronize SSM On-Prem with the product instance.

Step 1 Log into SSM On-Prem and navigate to **Smart Licensing** > **Inventory** > **SL Using Policy**.

a) Select all the product instances for which you want to request SLAC.

b) Click **Actions for Selected…** > **Authorization Code Request** > **Accept**.

The saved .csv file contains the list of selected product instances along with required device information, in the required format, to generate the SLAC in Cisco SSM. Save this file in a location that is accessible when you are in Cisco SSM in the next step.

Step 2 Log in to Cisco SSM at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses** link.

Step 3 Click **Inventory** > **Product Instances** > **Authorize License Enforced Features**

Step 4 Generate SLAC for multiple product instances

a) From the dropdown list that says “Single Device” (by default), change the selection to “Multiple Devices”.

At this point, a "Download a template" link is displayed. If you don't already have the required template or file, you can download it. Only the serial number and PID are mandatory.

b) Click **Choose File** and navigate to the .csv file, which contains the list of product instances that require SLAC.

c) Once uploaded, the list of devices is displayed in Cisco SSM. All the devices will have the checkbox enabled (implying that you want to request a SLAC for all of them), and click **Next**.

d) Specify the license quantity required for each product instance, and click **Next**.

Note For the "C9K HSEC" license, one SLAC is required for each UDI.

e) Click **Reserve Licenses** > **Download Authorization Codes** > **Close**

A.csv file containing all the authorization codes is downloaded.

Step 5 Return to the SSM On-Prem UI to import the file containing all the authorization codes.

a) Navigate to **Inventory** > **SL Using Policy**

b) Click **Export/Import All…** > **Import From Cisco**.

Go to **Inventory** > **SL Using Policy**, and see the Alerts column to verify import status: `Authorization message received from CSSM`.

Step 6 Apply SLAC on all the product instances, by navigating to **Reports** > **Synchronisation pull schedule with the devices** > **Synchronise now with the device**.

If you don't synchronize immediately after importing the codes, the uploaded codes are applied to the product instances the next time SSM On-Prem runs an update.

What's next

See Required Tasks After Installing SLAC

Required Tasks After Installing

This task shows you the activities that you must complete after installing SLAC. The information here applies to all methods of installing SLAC.

Step 1 Verify SLAC installation and HSECK9 key usage.

a) Note the system messages that are displayed after SLAC installation:

```
%SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was successfully
installed on: [chars].
```

[chars] is the UDI where the SLAC was installed

```
%SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed for feature hseck9
```

b) Check that the output of the **show license authorization** privileged EXEC command displays a timestamp and a last confirmation code.

In the `Overall Status` section of the output, look for `Status: SMART AUTHORIZATION INSTALLED on <timestamp>` and `Last Confirmation code: <code>`. This means SLAC is installed.

Example:

For Cisco Catalyst 9300X Series Switches, if you have installed more than one SLAC in a stacking setup, the status, timestamp, and confirmation code is displayed for each UDI where SLAC is installed. In the sample output below, SLAC is installed only on the active and not the standby or member switch.

```
Device# show license authorization

Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC
      Last Confirmation code: 6746c5b5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: NOT INSTALLED
  Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: NOT INSTALLED

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Device# show license summary
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-24 Network Advan...)       1 IN USE
  dna-advantage           (C9300-24 DNA Advantage)          1 IN USE
  network-advantage       (C9300-48 Network Advan...)       2 IN USE
  dna-advantage           (C9300-48 DNA Advantage)          2 IN USE
  C9K HSEC                (Cat9K HSEC)                      0 NOT IN USE
```

For Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules, if you have installed SLAC in a Cisco StaskWise Virtual setup, a different confirmation code is displayed for each connected device.

```
Device# show license authorization
Overall status:
  Active: PID:C9407R,SN:FXS2115054R
      Status: SMART AUTHORIZATION INSTALLED on Sep 07 22:56:57 2022 UTC
      Last Confirmation code: dc206d9d
  Standby: PID:C9407R,SN:FXS2115054R
      Status: SMART AUTHORIZATION INSTALLED on Sep 07 22:56:57 2022 UTC
      Last Confirmation code: dc206d9d

Authorizations:
```

```
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9407R,SN:FXS2115054R
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9407R,SN:FXS2115054R
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Device# show license summary

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9400 Network Advantage)         2 IN USE
  dna-advantage           (C9400 DNA Advantage)             1 IN USE
  C9K HSEC                (Cat9K HSEC)                      0 NOT IN USE
```

If you have installed SLAC in a dual supervisor setup, note that the same confirmation code is displayed for all connected devices. In the sample output below, SLAC is installed in such a dual-supervisor setup.

```
Device# show license authorization
Overall status:
  Active: PID:C9606R,SN:FXS241201WP
      Status: SMART AUTHORIZATION INSTALLED on Dec 13 05:18:07 2021 UTC
      Last Confirmation code: 7cf1f54a
  Standby: PID:C9606R,SN:FXS241201WP
      Status: SMART AUTHORIZATION INSTALLED on Dec 13 05:18:07 2021 UTC
      Last Confirmation code: 7cf1f54a

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9606R,SN:FXS241201WP
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9606R,SN:FXS241201WP
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Oct 07 05:13:33 2021 UTC
  Virtual Account: Eg-VA
```

```
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9600-NW-A)                      2 IN USE
  dna-advantage           (C9600-DNA-A)                     1 IN USE
  C9K HSEC                (Cat9K HSEC)                      0 NOT IN USE
```

c) Check that the *usage* count and status for "C9K HSEC" in the output of the **show license summary** privileged EXEC command displays `0` and `NOT IN USE`, respectively. This means that the HSECK9 key is available but is not in-use yet.

Step 2 Configure the cryptographic feature.

For information about configuring the feature, refer to the corresponding platform's configuration guide.

For Cisco Catalyst 9300X Series Switches, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)*.

For Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)*

For Cisco Catalyst 9500X Series Switches, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9500 Switches)* .

For Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2) and associated line cards, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9600 Switches)* .

Step 3 Again check HSECK9 key usage.

After you configure the cryptographic feature, the usage count and status of HSECK9 key in the output of the **show license summary** privileged EXEC command changes to `1` and `IN USE`, respectively.

Example:

Even if you have obtained more than one HSECK9 key in stacking set-ups or in Cisco StackWise Virtual setups, the *usage* count in the output of the **show license summary** command displays only 1. This is because only one HSECK9 key is used at a given point in time - the one on the active. The HSECK9 key on the standby is used when a switchover occurs. When the standby becomes the new active, usage count remains 1, because it is still only one key that is used.

For Cisco Catalyst 9300X Series Switches.

```
Device# show license summary
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-24 Network Advan...)       1 IN USE
  dna-advantage           (C9300-24 DNA Advantage)          1 IN USE
  network-advantage       (C9300-48 Network Advan...)       2 IN USE
  dna-advantage           (C9300-48 DNA Advantage)          2 IN USE
  hseck9                  (Cat9K HSEC)                      1 IN USE
```

For Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules, in a Cisco StackWise Virtual setup.

```
Device# show license summary

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9400 Network Advantage)         2 IN USE
```

```
  dna-advantage           (C9400 DNA Advantage)             1 IN USE
  C9K HSEC                (Cat9K HSEC)                      1 IN USE
```

For Cisco Catalyst 9500X Series Switches.

```
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Sep 27 10:04:01 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9500X_NW_A)                     1 IN USE
  dna-advantage           (C9500X_DNA_A)                    1 IN USE
  C9K HSEC                (Cat9K HSEC)                      1 IN USE
```

For Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2) and associated line cards in a dual supervisor setup.

```
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Oct 07 05:13:33 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9600-NW-A)                      2 IN USE
  dna-advantage           (C9600-DNA-A)                     1 IN USE
  C9K HSEC                (Cat9K HSEC)                      1 IN USE
```

What's next

Complete usage reporting - if required. To know if reporting is required, you can wait for a system message or refer to the policy, by using **show** commands.

- The system message, which indicates that reporting is required:

  ```
  %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgment will be required in [dec] days.
  ```

  [dec] is the amount of time (in days) left to meet reporting requirements.

- To check reporting requirements in a **show** command, refer to the output of the **show license status** privileged EXEC command and check the `Next ACK deadline` field. This means a RUM report must be sent and the ACK must be installed by this date.

  The method that you can use to send the RUM report, depends on the topology you have implemented. For more information, see: Smart Licensing Using Policy for Cisco Catalyst 9000 Series Switches.

Returning a SLAC

You can use this task to remove a SLAC and return the HSECK9 key, for all topologies.

You may want to return a SLAC and HSECK9 key under these circumstances:

- You no longer want to use the cryptographic feature, which requires an HSECK9 key.
- You want to return the device for Return Material Authorization (RMA), or decommission it permanently. When you return a device to Cisco, you have to configure the licence smart factory reset privileged EXEC command, which removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports and so on. *Before* you perform a factory reset, return the SLAC code. We also recommend that you send a RUM report to Cisco SSM before removing licensing information from the product instance.

1. Disable or unconfigure the cryptographic feature for which you used the HSECK9 key. For information about disabling the feature, refer to the corresponding platform's configuration guide.

   For information about disabling the feature, refer to the corresponding platform's configuration guide.

   For Cisco Catalyst 9300X Series Switches, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)*.

   For Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)*

   For Cisco Catalyst 9500X Series Switches, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9500 Switches)* .

   For Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2) and associated line cards, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9600 Switches)* .

2. Check the license usage status of the HSECK9 key by using the **show license summary** privileged EXEC command.

   If the status of the HSECK9 key is displayed as `NOT IN USE` proceed with the steps in the task.

   If the status of the HSECK9 key is displayed as `IN USE` even after the cryptographic feature is disabled, then first enter the required command to release the HSECK9 key.

For this platform...	**Enter this command to release the HSECK9 key forcibly**

Cisco Catalyst 9300X Series Switches
Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules.
	platform hsec-license-release
	`Device# configure terminal`
	`Device(config)# platform hsec-license-release`
	`HSEC license is released`
	`Device(config)# exit`

Cisco Catalyst 9500X Series Switches
Cisco Catalyst 9600 Series Supervisor Engine 2 and associated line cards.
	platform wanmacsec hsec-license-release
	`Device# configure terminal`
	`Device(config)# platform wanmacsec hsec-license-release`
	`HSEC license is released`
	`Device(config)# exit`

Follow these steps to remove a SLAC and return the HSECK9 key to your license pool in Cisco SSM.

Step 1 **show license summary**

(Optional) Displays license usage summary. This step applies only if you are returning a SLAC.

Ensure that the status of the license that you want to return is `NOT IN USE`.

Example:

```
Device# show license summary
License Usage:
  License             Entitlement Tag             Count Status
  -----------------------------------------------------------
  network-advantage   (C9300-24 Network Advan...)     1 IN USE
  dna-advantage       (C9300-24 DNA Advantage)        1 IN USE
  network-advantage   (C9300-48 Network Advan...)     2 IN USE
  dna-advantage       (C9300-48 DNA Advantage)        2 IN USE
  C9K HSEC            (Cat9K HSEC)                    0 NOT IN USE
```

Step 2 **license smart authorization return** {**all** |**local**} {**offline** [*path*] |**online**}

Example:

```
Device# license smart authorization return all online

OR

Device# license smart authorization return all offline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9300X-24HX,SN:FOC2519L8R7
Return code: Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7

OR
Device# license smart authorization return all offline bootflash:return-code.txt
```

Returns an authorization code back to the license pool in Cisco SSM. A return code is displayed after you enter this command.

Specify the product instance:

- **all**: Performs the action for all connected product instances in a High Availability or stacking set-up.
- **local**: Performs the action for the active product instance. This is the default option.

Specify if you are connected to Cisco SSM or not:

- If the product instance is directly connected to Cisco SSM, or it is connected to Cisco SSM through CSLU or SSM On-Prem and the product instance-initiates communication, enter **online**. The code is automatically returned to Cisco SSM and a confirmation is returned and installed on the product instance. If you choose this option, the return code is automatically submitted to Cisco SSM.
- If the product instance is not connected to Cisco SSM, or if you have implemented a topology with CSLU-initiated or SSM On-Prem initiated communication, enter **offline** [*filepath_filename*].

  If you choose the offline option, you must complete the additional step of submitting this to Cisco SSM.

Step 3 If you choose the **offline** option, upload the return information in Cisco SSM.

a) Log in to the CSSM Web UI at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses** link.

   Log in using the username and password provided by Cisco.

b) Select the **Smart Account** that will receive the report.

c) Select **Smart Software Licensing** > **Reports** > **Usage Data Files** > **Upload Usage Data**.

d) Browse to the file location (RUM report in tar format), select, and click **Upload Data**

e) Click ... to upload the SLAC return request file (`.txt` format)

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

f) From the **Select Virtual Accounts** pop-up, select the Virtual Account that will receive the uploaded file.

   The file is uploaded to Cisco SSM and is listed under **Reports** > **Usage Data Files** with the file name, the time is was reported, and the Virtual Account it was uploaded to, and so on.

g) In the **Acknowledgement** column, click **Download** to save the ACK.

   You may have to wait for the file to appear in the Acknowledgement column. If there many RUM reports or requests to process, CSSM may take a few minutes.

   After you download the file, import and install the file on the product instance by using the **license smart import***filepath_filename* command in privileged EXEC mode or import it to CSLU or SSM On-Prem.

Step 4 **show license authorization**

Displays licensing information. If the return process is completed correctly, the `Last return code:` field displays the return code.

Example:

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: NOT INSTALLED
      Last return code: Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-
babWeL-FABPt9-Wr1Dn7-Rp7
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: NOT INSTALLED
  Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: NOT INSTALLED

<output truncated>
```

Configuration Examples

Example for C9300X: Adding a Member to a Stack Where HSECK9 Keys are in Use

This example shows one way of adding a device to an existing stack where a cryptographic feature is configured and HSECK9 keys are IN USE.

This is the overall sequence of tasks for this method: **Add a new member to the existing stack** > **Request and install SLAC for the entire stack again**.

1. Display and check information about the existing stack.

   The output of the **show switch detail** command shows that this is a two-member stack.

   The output of the **show license authorisation** command shows that SLAC is installed on the active (C9300X-24HX,SN:FOC2519L8R7) and the standby (PID:C9300X-48HXN,SN:FOC2524L39P).

   The output of the **show license summary** command shows that the cryptographic functionality has been configured (C9K HSEC - IN USE).

   The output of the **show license all** command (truncated output) shows that the device is directly connected to Cisco SSM and the **smart** transport option is used for communication with Cisco SSM.

```
Device# show switch detail
Switch/Stack Mac Address : b08b.d02b.5b80 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------------------
*1       Active   b08b.d02b.5b80     15     P2B     Ready
 2       Standby  b08b.d08d.bb00     14     P2B     Ready
 3       Member   0000.0000.0000     0      PP      Removed

         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
---------------------------------------------------------
  1       DOWN          OK             None       2
  2         OK        DOWN               1      None
```

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
      Last Confirmation code: 72ad37d5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
      Last Confirmation code: 842584db


Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 2
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9300X-48HXN,SN:FOC2524L39P
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

```
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Dec 03 18:51:59 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-24 Network Advan...)       1 IN USE
  dna-advantage           (C9300-24 DNA Advantage)          1 IN USE
  network-advantage       (C9300-48 Network Advan...)       1 IN USE
  dna-advantage           (C9300-48 DNA Advantage)          1 IN USE
  C9K HSEC                (Cat9K HSEC)                      1 IN USE
```

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

<output truncated>

Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

<output truncated>
```

2. Add a new member to the stack.

The syslogs show the sequence of events after the new member is added to the stack. Note the successful trust code installation on the newly added member (%SMART_LIC-6-TRUST_INSTALL_SUCCESS).

The output of the **show switch stack-ports** and **show switch detail** commands show the status of switch 3, which is the newly added member.

The output of the **show license udi** command shows the PIDs of all the connected devices in the stacking set-up including the new member, C9300X-48HX,SN:FOC2516LC92.

The output of the **show license authorisation** command shows that SLAC is installed on the active (C9300X-24HX,SN:FOC2519L8R7) and the standby (PID:C9300X-48HXN,SN:FOC2524L39P), but not on the newly added member.

```
<output truncated>
Dec  3 18:42:49.885: %STACKMGR-6-STACK_LINK_CHANGE: Switch 2 R0/0: stack_mgr: Stack port 2 on Switch 2 is
up
Dec  3 18:42:57.213: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port 1 on Switch 1 is
up
Dec  3 18:42:57.229: %STACKMGR-4-SWITCH_ADDED: Switch 1 R0/0: stack_mgr: Switch 3 has been added to the
stack.
Dec  3 18:42:57.228: %STACKMGR-4-SWITCH_ADDED: Switch 2 R0/0: stack_mgr: Switch 3 has been added to the
stack.
Applying config on Switch 3...[DONE]
Dec  3 18:42:59.179: %STACKMGR-4-SWITCH_ADDED: Switch 2 R0/0: stack_mgr: Switch 3 has been added to the
stack.
.
.
.
Dec  3 18:42:36.633: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 1 on Switch 3 is
down
Dec  3 18:42:36.633: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 2 on Switch 3 is
down
Dec  3 18:42:50.369: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 1 on Switch 3 is
up
Dec  3 18:42:57.067: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 2 on Switch 3 is
up
Dec  3 18:42:57.070: %STACKMGR-4-SWITCH_ADDED: Switch 3 R0/0: stack_mgr: Switch 3 has been added to the
stack.
.
.
.
Dec  3 18:43:04.079: Slot add triggered 3
Dec  3 18:43:06.233: ILP:: switch 3 POE mode : IEEE BT
Dec  3 18:43:06.233: ILP:: POE POST detail for switch 3: PASS
Dec  3 18:43:06.233: ILP::   Able to get POE POST from switch 3 MCU
.
.
.
Dec  3 18:43:29.665: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully installed
 on P:C9300X-48HX,S:FOC2516LC92.
Dec  3 18:43:45.239: %LINK-3-UPDOWN: Interface TenGigabitEthernet3/0/4, changed state to up
Dec  3 18:43:46.239: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet3/0/4, changed state
 to up
<output truncated>
```

```
Device# show switch stack-ports
Switch#   Port1     Port2
---------------------------
1         OK        OK
2         OK        OK
3         OK        OK

Device# show switch detail
Switch/Stack Mac Address : b08b.d02b.5b80 - Local Mac Address
```

```
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------------------------------------
*1       Active   b08b.d02b.5b80     15     P2B     Ready
 2       Standby  b08b.d08d.bb00     14     P2B     Ready
 3       Member   f87a.414b.5580     1      PP      Ready

         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
  1         OK         OK               3        2
  2         OK         OK               1        3
  3         OK         OK               2        1
```

```
Device# show license udi
UDI: PID:C9300X-24HX,SN:FOC2519L8R7

HA UDI List:
    Active:PID:C9300X-24HX,SN:FOC2519L8R7
    Standby:PID:C9300X-48HXN,SN:FOC2524L39P
    Member:PID:C9300X-48HX,SN:FOC2516LC92
```

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
      Last Confirmation code: 72ad37d5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
      Last Confirmation code: 842584db
  Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: NOT INSTALLED

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 2
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9300X-48HXN,SN:FOC2524L39P
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

3. Request SLAC for the entire stack again.

   The method of requesting and installing SLAC here corresponds with the topology where the device is directly connected to Cisco SSM. Follow the method that applies to the topology you implement.

   The system messages show that SLAC is installed on all the connected devices in the set-up - the active (SN:FOC2519L8R7), the standby (SN:FOC2524L39P), and the member (SN:FOC2516LC92).

   The output of the **show license authorisation** command displayes the updated timestamp and the *new* confirmation codes for SLAC installation.

The confirmation codes for SN:FOC2519L8R7 and SN:FOC2524L39P , which are the existing devices in the stack, have changed from `72ad37d5` and `842584db`, to `f6c6978d` and `7ae69c8c`, respectively.

The confirmation code for the new member, which is SN:FOC2516LC92, is e3fd6642.

```
Device# license smart authorization request replace hseck9 all

Dec  3 18:45:33.145: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was
successfully installed on PID:C9300X-24HX,SN:FOC2519L8R7
Dec  3 18:45:33.235: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was
successfully installed on PID:C9300X-48HXN,SN:FOC2524L39P
Dec  3 18:45:33.319: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was
successfully installed on PID:C9300X-48HX,SN:FOC2516LC92
```

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:45:33 2021 UTC
      Last Confirmation code: f6c6978d
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:45:33 2021 UTC
      Last Confirmation code: 7ae69c8c
  Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:45:33 2021 UTC
      Last Confirmation code: e3fd6642

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 3
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9300X-48HXN,SN:FOC2524L39P
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Member: PID:C9300X-48HX,SN:FOC2516LC92
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

There is another way of adding a member to a stack where HSECK9 keys are in use, see Example for C9300X: Requesting SLAC on a Standalone and Then Adding it to a Stack Where HSECK9 Keys are In Use, on page 28.

Example for C9300X: Requesting SLAC on a Standalone and Then Adding it to a Stack Where HSECK9 Keys are In Use

This example shows you one way of adding a device to an existing stack where cryptographic functionality is being used.

This is the overall sequence of tasks for this method: **Install SLAC on the standalone** > **Configure the cryptographic functionality on the standalone** > **Add the device to the existing stack where cryptographic functionality is being used**.

1. Display and check information about the existing stack.

   The output of the **show switch detail** command shows that this is a two-member stack.

The output of the **show license authorisation** command shows that SLAC is installed on the active (C9300X-24HX,SN:FOC2519L8R7) and the standby (PID:C9300X-48HXN,SN:FOC2524L39P).

The output of the **show license summary** command shows that the cryptographic functionality has been configured (C9K HSEC - IN USE).

The output of the **show license all** command (truncated output) shows that the device is directly connected to Cisco SSM. The **smart** transport option is used for communication with Cisco SSM.

```
Device# show switch detail
Switch/Stack Mac Address : b08b.d02b.5b80 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-------------------------------------------------------------------
*1       Active   b08b.d02b.5b80     15     P2B     Ready
 2       Standby  b08b.d08d.bb00     14     P2B     Ready
 3       Member   0000.0000.0000     0      PP      Removed

         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------
  1       DOWN         OK              None       2
  2         OK       DOWN                1      None
```

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
      Last Confirmation code: 72ad37d5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:34:03 2021 UTC
      Last Confirmation code: 842584db


Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 2
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9300X-48HXN,SN:FOC2524L39P
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

```
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Dec 03 18:51:59 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-24 Network Advan...)       1 IN USE
  dna-advantage           (C9300-24 DNA Advantage)          1 IN USE
  network-advantage       (C9300-48 Network Advan...)       1 IN USE
```

```
  dna-advantage           (C9300-48 DNA Advantage)          1 IN USE
  C9K HSEC                (Cat9K HSEC)                      1 IN USE

Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

<output truncated>

Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

<output truncated>
```

2. Boot the third switch as a standalone.

The syslogs show the boot-up sequence.

The output of the **show switch detail** command shows that this is a standalone set-up.

```
<output truncated>

switch:boot
boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
Waiting for 120 seconds for other switches to boot
##############################################################################################################################
Switch number is 3
.
.
.
Press RETURN to get started!
*Dec  3 18:29:30.097: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled
*Dec  3 18:29:30.145: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is not allowed
*Dec  3 18:29:41.412: %SYS-5-RESTART: System restarted —
<output truncated>

Device# show switch detail
Switch/Stack Mac Address : f87a.414b.5580 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-------------------------------------------------------------------------------
 1       Member   0000.0000.0000     0              Provisioned
 2       Member   0000.0000.0000     0              Provisioned
*3       Active   f87a.414b.5580     1      PP      Ready


         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
---------------------------------------------------------
  3       DOWN       DOWN             None     None
```

3. Configure a Smart Licensing Using Policy topology on the standalone.

   The sample configuration shows that the *No Connectivity to Cisco SSM and No CSLU* topology is implemented. Configure the applicable commands depending on the topology you implement.

   The output of the **show license authorisation** command shows that SLAC is not installed on the standalone.

```
Device(config)# license smart transport off
Device(config)# exit
Device# copy running-config startup-config

Device# show license authorization

Overall status:
  Active: PID:C9300X-48HX,SN:FOC2516LC92
      Status: NOT INSTALLED
Purchased Licenses:
  No Purchase Information Available
```

4. Import and install SLAC

   The SLAC file is obtained from Cisco SSM and not shown here. The sample configuration shows how the SLAC file is installed on the device by using the **license smart import** command.

   The output of the **show license authorisation** command shows that SLAC is installed.

```
Device# license smart import tftp://10.8.0.6/user-01/SLAC-standalone.txt
Import Data Successful
Last Confirmation code UDI: PID:C9300X-48HX,SN:FOC2516LC92
    Confirmation code: 59e155ae
Device#
*Dec  3 18:58:39.026: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was
successfully installed on PID:C9300X-48HX,SN:FOC2516LC92

Device# show license authorization
Overall status:
  Active: PID:C9300X-48HX,SN:FOC2516LC92
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:58:39 2021 UTC
      Last Confirmation code: 59e155ae


Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-48HX,SN:FOC2516LC92
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

5. Configure the cryptographic feature

   The outputs of the **show license summary** commands show the status of the HSECK9 key before (NOT IN USE) and after (IN USE) configuration of the cryptographic feature.

```
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Dec 03 18:57:27 2021 UTC
  Virtual Account: Eg-VA
```

```
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-48 Network Advan...)       1 IN USE
  dna-advantage           (C9300-48 DNA Advantage)          1 IN USE
  C9K HSEC                (Cat9K HSEC)                      0 NOT IN USE

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface tu10
Device(config-if)# tunnel mode ipsec ipv4
Device(config-if)# end


*Dec  3 18:59:29.309: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is allowed for
feature hseck9

Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Dec 03 18:57:27 2021 UTC
  Virtual Account: Eg-VA


License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-48 Network Advan...)       1 IN USE
  dna-advantage           (C9300-48 DNA Advantage)          1 IN USE
  C9K HSEC                (Cat9K HSEC)                      1 IN USE
```

6. Add the standalone switch to the existing stack

The output of the **show switch detail** command shows that a new member has been added to the stack.

The output of the **show license all** command shows that the SLAC on the new member is retained. Compare the "Status" and "Last Confirmation code" fields in the output here, with the output of the **show license authorization** command after SLAC installation on the standalone (above).

The output of the **show license summary** shows that the cryptographic feature continues to be operational (the HSECK9 key is IN-USE).

```
Chassis 3 reloading, reason - stack merge
*Dec  3 19:00:59.575: %STACKMGR-6-STACK_LINK_CHANGE: Switch 3 R0/0: stack_mgr: Stack port 1 on Switch 3 is
 up
*Dec  3 19:00:59.577: %STACKMGR-1-RELOAD: Switch 3 R0/0: stack_mgr: Reloading due to reason stack merge
Dec  3 19:01:08.683: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp action requested
Dec  3 19:01:10.171: %PMAN-5-EXITACTION: R0/vp: Process manager is exiting: rp processes exit with reload
switch code

Initializing Hardware......

<output truncated>

Device# show switch detail
Switch/Stack Mac Address : b08b.d02b.5b80 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-------------------------------------------------------------------------------------
*1       Active   b08b.d02b.5b80     15     P2B     Ready
 2       Standby  b08b.d08d.bb00     14     P2B     Ready
 3       Member   f87a.414b.5580     1      PP      Ready
```

```
         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------
  1         OK         OK               3        2
  2         OK         OK               1        3
  3         OK         OK               2        1


Device# show license all

Smart Licensing Status
======================


Smart Licensing is ENABLED


Export Authorization Key:
  Features Authorized:
    <none>


Utility:
  Status: DISABLED


Smart Licensing Using Policy:
  Status: ENABLED


Account Information:
  Smart Account: Eg-SA As of Dec 03 18:51:59 2021 UTC
  Virtual Account: Eg-VA


Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED


Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured


Miscellaneous:
  Custom Id: <empty>


Policy:
  Policy in use: Installed On Dec 03 18:32:37 2021 UTC
  Policy name: Custom Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (Customer Policy)
    Reporting frequency (days): 0 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
```

```
    First report requirement (days): 90 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 365 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 365 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)


Usage Reporting:
  Last ACK received: Dec 03 18:37:21 2021 UTC
  Next ACK deadline: Mar 03 18:37:21 2022 UTC
  Reporting push interval: 30  days
  Next ACK push check: Dec 03 19:04:55 2021 UTC
  Next report push: Dec 03 19:05:03 2021 UTC
  Last report push: Dec 03 18:52:53 2021 UTC
  Last report file write: <none>


Trust Code Installed:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
    INSTALLED on Dec 03 18:32:37 2021 UTC
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
    INSTALLED on Dec 03 18:32:37 2021 UTC
  Member: PID:C9300X-48HX,SN:FOC2516LC92
    INSTALLED on Dec 03 18:43:29 2021 UTC


License Usage
=============


network-advantage (C9300-24 Network Advantage):
  Description: C9300-24 Network Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9300-24 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual


dna-advantage (C9300-24 DNA Advantage):
  Description: C9300-24 DNA Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9300-24 DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription


network-advantage (C9300-48 Network Advantage):
  Description: C9300-48 Network Advantage
  Count: 2
  Version: 1.0
```

```
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9300-48 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual


dna-advantage (C9300-48 DNA Advantage):
  Description: C9300-48 DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9300-48 DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription


C9K HSEC (Cat9K HSEC):
  Description: HSEC Key for Export Compliance on Cat9K Series Switches
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Export


Product Information
===================
UDI: PID:C9300X-24HX,SN:FOC2519L8R7


HA UDI List:
    Active:PID:C9300X-24HX,SN:FOC2519L8R7
    Standby:PID:C9300X-48HXN,SN:FOC2524L39P
    Member:PID:C9300X-48HX,SN:FOC2516LC92


Agent Version
=============
Smart Agent for Licensing: 5.3.15_rel/49


License Authorizations
======================
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:51:56 2021 UTC
      Last Confirmation code: fa4c0d80
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:51:56 2021 UTC
      Last Confirmation code: 450243e2
  Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: SMART AUTHORIZATION INSTALLED on Dec 03 18:58:39 2021 UTC
      Last Confirmation code: 59e155ae


Authorizations:
  C9K HSEC (Cat9K HSEC):
```

```
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 3
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9300X-48HXN,SN:FOC2524L39P
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Member: PID:C9300X-48HX,SN:FOC2516LC92
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1


Purchased Licenses:
  No Purchase Information Available


Usage Report Summary:
=====================
Total: 58,  Purged: 0
Total Acknowledged Received: 20,  Waiting for Ack: 33
Available to Report: 5  Collecting Data: 0



Device# show license summary
Load for five secs: 1%/0%; one minute: 9%; five minutes: 5%
Time source is NTP, 19:05:29.741 UTC Fri Dec 3 2021

Account Information:
  Smart Account: Eg-SA As of Dec 03 19:04:56 2021 UTC
  Virtual Account: Eg-VA


License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-24 Network Advan...)       1 IN USE
  dna-advantage           (C9300-24 DNA Advantage)          1 IN USE
  network-advantage       (C9300-48 Network Advan...)       2 IN USE
  dna-advantage           (C9300-48 DNA Advantage)          2 IN USE
  C9K HSEC                (Cat9K HSEC)                      1 IN USE
```

To see the other method of adding a member to a stack where HSECK9 keys are in use, see Example for C9300X: Adding a Member to a Stack Where HSECK9 Keys are in Use, on page 24.

Example: SLAC Installation Failure Because of an Insufficient Number of HSECK9 Keys

This example shows what happens if the required number of HSECK9 keys are not available in the applicable Smart Account and Virtual Account in Cisco SSM, when attempting SLAC installation.

This is a Cisco StackWise Virtual setup where SLAC is being installed on both chassis UDIs (SN:FXS221500CT and SN:FXS221500BN), for uninterrupted use the cryptographic feature in case of switchover.

```
Device# show license udi
UDI: PID:C9407R,SN:FXS221500CT

HA UDI List:
```

```
Active:PID:C9407R,SN:FXS221500CT
Standby:PID:C9407R,SN:FXS221500BN
```

The product instance is directly connected to Cisco SSM, and the **license smart authorization request add hseck9 all** command is configured to request and install SLAC for all connected devices, that is, the active and the standby.

The first system message shows that SLAC was successfully installed on the active.

The second system message shows that SLAC was not installed on the standby (SN:FXS221500BN). The `ERROR_ALL_COUNTS_IN_USE` code in the message shows that installation failed, because a sufficient number of HSECK9 keys were not available in the Smart Account and Virtual Account in Cisco SSM.

```
Device# license smart authorization request add hseck9 all
*Sep  6 16:58:25.528 PDT: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code
was successfully installed on PID:C9407R,SN:FXS221500CT

*Sep  6 16:58:25.575 PDT: %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED: The install of a new licensing
authorization code has failed on PID:C9407R,SN:FXS221500BN: ERROR_ALL_COUNTS_IN_USE.
```

To resolve the above problem and install SLAC on all connected devices:

- Ensure that the required number of HSECK9 keys are available the applicable Smart Account and Virtual Account in Cisco SSM. In the above example, one HSECK9 is required for each chassis UDI.
- Return the SLAC which is on the active product instance.
- Lastly, request and install SLAC on the active and standby again.

Feature History for Available Licenses

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.5.1a	Base and Add-On Licenses	Enables the use of software features on the device. See: Base and Add-On Licenses, on page 1 and Configure Base and Add-On Licenses, on page 9. This feature was introduced on • Cisco Catalyst 9300 Series Switches, and • C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Everest 16.6.1	Base and Add-On Licenses	This feature was implemented on Cisco Catalyst 9400 Series Switches.
Cisco IOS XE Fuji 16.8.1a	Base and Add-On Licenses	This feature was implemented on the High Performance models of the Cisco Catalyst 9500 Series Switches, that is C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C.
Cisco IOS XE Fuji 16.9.2	Base and Add-On Licenses	This feature was implemented on Cisco Catalyst 9200 Series Switches.

Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.11.1	Base and Add-On Licenses	This feature was implemented on Cisco Catalyst 9600 Series Switches.
Cisco IOS XE Bengaluru 17.6.2	Export Control Key for High Security (HSECK9 key)	Authorizes the use of cryptographic features that are restricted by U.S. export control laws. If you want to use a restricted cryptographic feature, an HSECK9 key is required. See: Export Control Key for High Security or HSECK9 key, on page 2 and Install SLAC for an HSECK9 Key, on page 11. This feature was introduced on the Cisco Catalyst 9300X Series Switches. It is required for the IPsec feature. The HSECK9 key is supported only on the Cisco Catalyst 9300X Series Switches and not on any of the other models in the Cisco Catalyst 9300 Series Switches.
Cisco IOS XE Cupertino 17.7.1	Ability to save SLAC request in a file.	Introduces the option to saves the required UDI information for a SLAC request and a SLAC return request, in a .txt file, in the specified location. The SLAC request file must then be uploaded to Cisco SSM in the same location and in the same way as a RUM report. Use the **license smart authorization request save** *path* command in privileged EXEC mode.
	Base and Add-On Licenses	This feature was implemented on • C9400X-SUP-2 and C9400X-SUP-2XL supervisor modules, and • the C9500X-28C8D model of Cisco Catalyst 9500X Series Switches.
Cisco IOS XE Cupertino 17.8.1	HSECK9 key	This feature was implemented on these platforms, and is required for the WAN MACsec feature. • Cisco Catalyst 9500X Series Switches. The HSECK9 is supported only on the Cisco Catalyst 9500X Series Switches and not on any of the other models in the Cisco Catalyst 9500 Series Switches. • Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2) and associated line cards.
Cisco IOS XE Dublin 17.11.1	HSECK9 key	This feature was implemented on the C9400X-SUP-2 and C9400X-SUP-2XL on supervisor modules and is required for the IPsec feature.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com.