Available Licenses

Information About Available Licenses

This section provides information about the licenses that are available on Cisco Catalyst 9600 Series Switches running Cisco IOS-XE software. The information applies to all models in the series, unless indicated otherwise.

Base and Add-On Licenses

The software features available on the switch fall under base or add-on license levels.

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 Digital Network Architecture Center (Cisco DNA Center). An add-on license is valid only until a certain date. You can purchase an add-on license for a three, five, or seven year subscription period.

The following base and add-on licenses are available:

Base Licenses

Network Advantage

Add-On Licenses

DNA Advantage

Guidelines for Using Base and Add-On Licenses

- A base license (Network-Advantage) is ordered and fulfilled only with a perpetual or permanent license type.
- An add-on license (DNA Advantage) 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. If you use DNA features, renew the license before term expiry, to continue using it. If you don't want to continue using DNA features, deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- To know which license level a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to https://cfnng.cisco.com. An account on cisco.com is not required.

Export Control Key for High Security

Products and features that provide cryptographic functionality are within the purview of U.S. export control laws [1]. The Export Control Key for High Security (HSECK9 key) is an export-controlled license, which authorizes the use of cryptographic functionality.

This subsection provides information about the Cisco Catalyst 9600 Series Switches that support the HSECK9 key, the cryptographic features that require the HSECK9 key, what to consider when ordering it, prerequisites, and how to configure it on supported platforms.

Supported Platforms and Releases

The HSECK9 key is supported on the Cisco Catalyst 9600 Series 40-Port 50G, 2-Port 200G, 2-Port 400G Line Card (C9600-LC-40YL4CD), starting with Cisco IOS XE Cupertino 17.8.1. This line card is compatible only with Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2).

For more information about the line card and compatibility, see Cisco Catalyst 9600 Series Line Card Installation Note and Cisco Catalyst 9600 Series Switches Hardware Installation Guide.

When an HSECK9 Key Is Required

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.

The WAN MACsec feature requires an HSECK9 key. More specifically, the HSECK9 key is required on *customer edge devices* in a point-to-point (P2P) and point-to-multipoint (P2MP) network where the WAN MACsec feature is configured.

Prerequisites for Using an HSECK9 Key

Ensure you meet the following requirements:

- The device is one that supports the HSECK9 key. See Supported Platforms and Releases, on page 2.
- You have configured the DNA Advantage license on the device. You cannot use an HSECK9 key without DNA Advantage configured.
- You have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in Cisco Smart Software Manager (CSSM).

  The HSECK9 key is tied to the *chassis*. Each *chassis* UDI where you want to use a cryptographic feature requires one HSECK9 key. To understand this requirement in the context of a High Availability setup, see High Availability Considerations, on page 3.

[1] the U.S. Government Encryption and Export Administration Regulations (EAR)

- You have implemented one of the supported Smart Licensing Using Policy topologies. This enables you to install a Smart Licensing Authorization Code (SLAC) for each HSECK9 key you want to use.

  An HSECK9 key requires authorization *before* use, because it is restricted by U.S. trade-control laws (export-controlled). A SLAC provides this authorization and allows activation and continued use of an export-controlled license. A SLAC is generated in and obtained from CSSM. There are multiple ways in which a device can be connected to CSSM, to obtain a SLAC. Each way of connecting to CSSM is called a topology. The configuration section shows you how to obtain a SLAC with each topology (Installing SLAC for an HSECK9 Key, on page 7).

Note To obtain and install SLAC on supported platforms that are within the scope of this document (Supported Platforms and Releases, on page 2), refer to the configuration section in *this* document. There are differences in the configuration process when compared to other Cisco products.

- You configure the cryptographic feature only after you have installed SLAC. If not, you have to reconfigure the cryptographic feature after installing SLAC.
- The interface on which you configure the cryptographic feature must correspond with a linecard slot where a line card supporting the cryptographic feature is installed.

Ordering Considerations

This section covers important ordering considerations for an HSECK9 key.

The HSECK9 key is tied to the chassis UDI. Regardless of whether you have a single or dual supervisor set-up, and regardless of the number of linecards where the cryptographic feature is configured, only one license is required for a chassis. A separate HSECK9 key is required for each *chassis* UDI where you want to use a cryptographic feature.

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.

For information about ordering the key, see the Cisco Catalyst 9600 Series Switches Ordering Guide.

High Availability Considerations

This section covers the High Availability considerations that apply *when using the HSECK9 key*.

- Supported High Availability setups:

  A dual-supervisor setup, where two supervisor modules are installed in a chassis, one being the active and the other, the standby.

  All licensing information, such as trust codes, SLAC, RUM reports, are stored on the active supervisor (active product instance) and synchronised with the standby.

Note You cannot use the HSECK9 key in any other High Availability setup. For example, it is not supported in a Cisco Stackwise Virtual setup and in a Quad-Supervisor setup (Quad-Supervisor with Route Processor Redundancy).

- The number of HSECK9 keys required in a High Availability setup:

  The HSECK9 key is tied to the chassis UDI and regardless of the number of supervisors installed, only one HSECK9 key is required for each chassis UDI. The following sample output shows you how the chassis UDI is displayed. The same chassis UDI is also displayed for the active and standby:

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

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

- The number of SLACs required in a High Availability setup:

  Each HSECK9 key requires one SLAC.

  The following sample output shows you 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
  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

<output truncated>
```

- Behavior in the event of a switchover:

  The system continues uninterrupted operation of the cryptographic feature in case of a switchover.

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

- Hardware removal and replacement in High Availability setup:

  See Hardware Removal and Replacement, on page 4.

Hardware Removal and Replacement

The following constitues the basis of what you must consider when removing and replacing a supervisor module or linecard:

- 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.
- 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.

The above principles have the following implications when you remove and replace a supervisor module or a linecard:

- In a single supervisor set-up, 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.

- In a dual supervisor set-up, 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.

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

How to Configure Available Licenses

This section provides information about how to configure available licenses.

Configuring 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. You can use this task to

- Change the current license.
- Add another license. For example, if you are currently using Network Advantage and you also want to use features available with the corresponding Digital Networking Architecture (DNA) Advantage license.
- Remove a license.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license boot level** { **network-advantage** [**addon dna-advantage**] | **network-essentials** [**addon dna-essentials**] } **Example:** `Device(config)# license boot level network-advantage add-on dna-advantage`	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.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to the privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves changes in the configuration file.

Step 6	**show version**
	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>`
		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.

	Command or Action	Purpose
Step 7	**reload** **Example:** `Device# reload`	Reloads the device.

Step 8	**show version**
	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>`
		Shows currently configured license information and the license that is applicable after reload.

What to do next

After you configure a license level, the change is effective after a reload. To know if reporting is required, you can wait for a system message or refer to the policy-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.

- If using **show** commands, 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. Refer to the workflow for the applicable topology in the How to Configure Smart Licensing Using Policy: Workflows by Topology section of the *Smart Licensing Using Policy* chapter in this guide.

Installing SLAC for an HSECK9 Key

This section shows you the various methods of installing SLAC for an HSECK9 key. Each method corresponds with a particular topology in the Smart Licensing Using Policy environment.

For information about all the supported topologies, see the Supported Topologies section of the *Smart Licensing Using Policy* chapter in this guide.

Note The only topology that you *cannot* implement if you want to use an HSECK9 key, is *Connected to CSSM Through a Controller*. The "controller" here is Cisco DNA Center. The Cisco DNA Center GUI does not provide an option to generate a SLAC for Cisco Catalyst switches that support HSECK9.

Installing SLAC: Connected Directly to CSSM

This task shows you how to request and install SLAC when the device (product instance), is directly connected to CSSM.

Before you begin

- Ensure that the device is one that supports HSECK9. See Supported Platforms and Releases, on page 2.
- Ensure you have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in CSSM.
- Ensure that you have completed Steps from 1 through 3 of the *Connected Directly to CSSM* topology. See Workflow for Topology: Connected Directly to CSSM.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**} **Example:** `Device# license smart authorization request add hseck9 all`	Requests a SLAC from CSSM or 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

	Command or Action	Purpose
		the corresponding cryptographic feature. **Note** On Cisco Catalyst 9300X Series Switches in a stacking setup: 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. • *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:

	Command or Action	Purpose
		• **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.
Step 3	(Optional) **license smart sync** {**all** | **local**} **Example:** `Device# license smart sync all`	Triggers the product instance to synchronize with CSSM, or CSLU, or SSM On-Prem, to send and receive any pending data. This step applies only to topologies where the product instance is connected to CSSM, or CSLU or SSM On-Prem, and where the product instance initiates communication. The topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated), and SSM On-Prem Deployment (product instance-initiated). By triggering an on-demand synchronization, you can ensure that the SLAC installation process is completed soon after you request SLAC. Otherwise, SLAC is applied to the product instance only the next time the product instance is *scheduled* to contact CSSM, or CSLU or SSM On-Prem.

What to do next

Required Tasks After Installing SLAC, on page 23

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.

Here 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.

Before you begin

- Ensure that the device is one that supports HSECK9. See Supported Platforms and Releases, on page 2.
- Ensure you have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in CSSM.
- Ensure that you have completed Step 1 of the *No Connectivity to CSSM and No CSLU* topology. See Workflow for Topology: No Connectivity to CSSM and No CSLU.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all**| **local**} **Example:** `Device# license smart authorization request add hseck9 all`	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.

	Command or Action	Purpose
		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.

	Command or Action	Purpose
		• **local**: Gets the SLAC for the *active* device in a High Availability set-up. This is the default option.
Step 3	**license smart authorization request save***path* **Example:** `Device# license smart authorization request save bootflash:slac.txt`	Saves the required UDI information for the SLAC request in a .txt file, in the specified location.
Step 4	Uploading Data or Requests to CSSM and Downloading a File	This task is performed on the CSSM 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 CSSM Web UI, generate a SLAC code in the CSSM 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.
Step 5	**copy** *source filename* **bootflash:** **Example:** `Device# copy tftp://10.8.0.6/user01/example.txt 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.
Step 6	**license smart import** *filepath_filename* **Example:** `Device# license smart import bootflash:example.txt`	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.

What to do next

Required Tasks After Installing SLAC, on page 23

Installing SLAC: Connected to CSSM Through CSLU (Product Instance-Initiated)

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

Before you begin

- Ensure that the device is one that supports the HSECK9 key. See Supported Platforms and Releases, on page 2.
- Ensure you have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in CSSM.
- Ensure that you have completed Steps 1 through 3 of the *Connected to CSSM Through CSLU* (Product Instance-Initiated Communication) topology. See Workflow for Topology: Connected to CSSM Through CSLU → Tasks for Product Instance-Initiated Communication.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

Step 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**}
	Example:
	`Device# license smart authorization request add hseck9 all`
		Requests a SLAC from CSSM or 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.

	Command or Action	Purpose
		Note On Cisco Catalyst 9300X Series Switches in a stacking setup: 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. • *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:

	Command or Action	Purpose
		• **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.
Step 3	(Optional) **license smart sync** {**all** | **local**} **Example:** `Device# license smart sync all`	Triggers the product instance to synchronize with CSSM, or CSLU, or SSM On-Prem, to send and receive any pending data. This step applies only to topologies where the product instance is connected to CSSM, or CSLU or SSM On-Prem, and where the product instance initiates communication. The topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated), and SSM On-Prem Deployment (product instance-initiated). By triggering an on-demand synchronization, you can ensure that the SLAC installation process is completed soon after you request SLAC. Otherwise, SLAC is applied to the product instance only the next time the product instance is *scheduled* to contact CSSM, or CSLU or SSM On-Prem.

What to do next

Required Tasks After Installing SLAC, on page 23

Installing SLAC: Connected to CSSM Through CSLU (CSLU-Initiated)

This task shows you how to request and install SLAC when the device (product instance) is connected to CSSM 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 configure certain commands on the product instance, certain tasks in the CSSM Web UI, and certain tasks in the CSLU interface.

Before you begin

- Ensure that the device is one that supports the HSECK9 key. See Supported Platforms and Releases, on page 2.
- Ensure you have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in CSSM.
- Ensure that you have completed Steps 1 through 3 of the *Connected to CSSM Through CSLU* (Product Instance-Initiated Communication) topology. See Workflow for Topology: Connected to CSSM Through CSLU → Tasks for CSLU-Initiated Communication.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

Step 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**}
	Example:
	`Device# license smart authorization request add hseck9 all`
		Requests a SLAC from CSSM or 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.

	Command or Action	Purpose
		Note On Cisco Catalyst 9300X Series Switches in a stacking setup: 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. • *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:

	Command or Action	Purpose
		• **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.
Step 3	Requesting SLAC for One or More Product Instance (CSLU Interface)	This task is performed on the CSLU interface.
Step 4	Generating and Downloading SLAC from CSSM to a File	This task is performed on the CSSM Web UI.
Step 5	Import from CSSM (CSLU Interface)	This task is performed on the CSLU interface. After you have completed it, the uploaded codes are applied to the product instances the next time CSLU runs an update.

What to do next

Required Tasks After Installing SLAC, on page 23

Installing SLAC: SSM On-Prem Deployment (Product Instance-Initiated)

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

Here you first create a request file in SSM On-Prem, upload the request in the CSSM Web UI, generate SLAC, import the SLAC into the SSM On-Prem server. Finally configure the commands on the product instance to request and install SLAC.

Before you begin

- Ensure that the device is one that supports the HSECK9 key. See Supported Platforms and Releases, on page 2.
- Ensure you have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in CSSM.

- Ensure that you have completed Steps 1 through 3 c. of the *SSM On-Prem Deployment* (Product Instance-Initiated) topology. See Workflow for Topology: SSM On-Prem Deployment → Tasks for Product Instance-Initiated Communication.

Procedure

	Command or Action	Purpose
Step 1	Submitting an Authorization Code Request (SSM On-Prem UI)	This task is performed on the SSM On-Prem UI.
Step 2	Generating and Downloading SLAC from CSSM to a File	This task is performed on the CSSM Web UI.
Step 3	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 4	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**} **Example:** `Device# license smart authorization request add hseck9 all`	Requests a SLAC from CSSM or 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.

	Command or Action	Purpose
		Note On Cisco Catalyst 9300X Series Switches in a stacking setup: 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. • *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:

	Command or Action	Purpose
		• **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.
Step 5	(Optional) **license smart sync** {**all** | **local**} **Example:** `Device# license smart sync all`	Triggers the product instance to synchronize with CSSM, or CSLU, or SSM On-Prem, to send and receive any pending data. This step applies only to topologies where the product instance is connected to CSSM, or CSLU or SSM On-Prem, and where the product instance initiates communication. The topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated), and SSM On-Prem Deployment (product instance-initiated). By triggering an on-demand synchronization, you can ensure that the SLAC installation process is completed soon after you request SLAC. Otherwise, SLAC is applied to the product instance only the next time the product instance is *scheduled* to contact CSSM, or CSLU or SSM On-Prem.

What to do next

Required Tasks After Installing SLAC, on page 23

Installing SLAC: SSM On-Prem Deployment (SSM On-Prem-Initiated)

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 CSSM Web UI, generate SLAC, import it into the SSM On-Prem server. Finally, synchronize SSM On-Prem with the product instance.

Before you begin

- Ensure that the device is one that supports the HSECK9 key. See Supported Platforms and Releases, on page 2.
- Ensure you have the required number of the HSECK9 keys in the applicable Smart Account and Virtual Account in CSSM.
- Ensure that you have completed Steps 1 through 3 a. of the *SSM On-Prem Deployment* (Product Instance-Initiated) topology. See Workflow for Topology: SSM On-Prem Deployment → Tasks for SSM On-Prem Instance-Initiated Communication.

Procedure

	Command or Action	Purpose
Step 1	Submitting an Authorization Code Request (SSM On-Prem UI).	This task is performed in the SSM On-Prem UI.
Step 2	In the SSM On-Prem UI, navigate to **Reports** > **Synchronisation pull schedule with the devices** > **Synchronise now with the device**.	This step is optional. 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 to do next

Required Tasks After Installing SLAC, on page 23

Required Tasks After Installing SLAC

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

Procedure

Step 1 Verify SLAC installation and HSECK9 key usage.

- The following system messages 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.`
- 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.

If you have installed SLAC in a High Availability setup, note that the same SLAC installation timestamp and last confirmation code is displayed for all connected devices. In the sample output below, SLAC is installed in a High Availability setup.

- 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.

Example:

```
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
```

Step 2 Configure the cryptographic feature.

The following WAN MACsec configuration is for example purposes only. For information about configuring the feature, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9600 Switches)*

Example:

```
Device# show module
Chassis Type: C9606R

Mod Ports Card Type                                  Model          Serial No.
---+-----+--------------------------------------+--------------+--------------
2   24   24-Port 40GE / 100GE                     C9600-LC-24C     FDO24300SBD
```

```
3   0    Supervisor 2 Module                          C9600X-SUP-2     FDO24410996
4   0    Supervisor 2 Module                          C9600X-SUP-2     FDO2441090F
5   44   40x10/25/50GE + 2x200GE + 2x400GE            C9600-LC-40YL4CD FDO245106QU

<output truncated>

Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface FourHundredGigE5/0/44
Device(config-if)# macsec dot1q-in-clear 1
Device(config-if)#
*Dec  13 05:20:04.221: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
 is
 allowed for feature hseck9
Device(config-if)#

Device# show running-config interface FourHundredGigE5/0/44
Building configuration...

Current configuration : 160 bytes
!
interface FourHundredGigE5/0/44
 no switchport
 no ip address
 macsec dot1q-in-clear 1
 eapol destination-address broadcast-address
 eapol eth-type 876F
end
```

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:

```
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
```

Step 4 Check if reporting is required. The method that you can use to send the RUM report, depends on the topology you have implemented. Refer to the workflow for the applicable topology in the How to Configure Smart Licensing Using Policy: Workflows by Topology section of the *Smart Licensing Using Policy* chapter in this guide.

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

- The system message, which indicates that reporting is required: `%SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will be required in [dec] days.`

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

- If using **show** commands, refer to the output of the **show license status** privileged EXEC command. Check the `Next ACK deadline` field. You must send the RUM report and ensure that the ACK is installed by this date.

Returning a SLAC

This task shows you how to return a SLAC and return the HSECK9 key to your license pool in CSSM. You can use this task with 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 CSSM before removing licensing information from the product instance.

Before you begin

Disable or unconfigure the cryptographic feature for which you used the HSECK9 key.

Procedure

	Command or Action	Purpose
Step 1	Disable or unconfigure the cryptographic feature for which you used the HSECK9 key.	For information about disabling the WANMACsec feature, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9600 Switches)* If the cryptographic feature you are disabling is the WAN MACsec feature, note the following: Even after disabling the cryptographic feature, the output of the **show license summary** command displays the usage count and status for the HSECK9 key as `1` and `IN USE`. This is as expected. The steps in this task show you how to *release* the key, which changes the count and status to `0` and `NOT IN USE`. But you must disable the WAN MACsec feature before you try to release the HSECK9 key.
Step 2	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	

Step 3	**show license summary**
	Example:
	`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`
		(Optional) Displays license usage summary. This step applies only if you are returning a SLAC.
		If the status of the HSECK9 key is displayed as `NOT IN USE` skip to Step 5.
		If the status of the HSECK9 key is displayed as `IN USE` even after the cryptographic feature is disabled, then perform the next step. This is the case in the accompanying example.

Step 4	**platform wanmacsec hsec-license-release**
	Example:
	`Device# configure terminal`
	`Device(config)# platform wanmacsec hsec-license-release`
	`HSEC license is released`
	`Device(config)# exit`
		Enters the global configuration mode, releases the HSECK9 license, and returns to privileged EXEC mode.

Step 5	**show license summary**
	Example:
	`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`
		(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`.

Step 6	**license smart authorization return** {**all** |**local**} {**offline** [*path*] |**online**} **Example:**	Returns an authorization code back to the license pool in CSSM. A return code is displayed after you enter this command. Specify the product instance:

	Command or Action	Purpose

	`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:C9606R,SN:FXS241201WP`
	`Return code:`
	`Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7`
	
	`OR`
	
	`Device# license smart authorization return all`
	`offline bootflash:return-code.txt`
		• **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 CSSM or not:
		• If connected to CSSM, or if you have implemented a topology where the product instance-initiates communication (CSLU or SSM On-Prem), enter **online**. The code is automatically returned to CSSM and a confirmation is returned and installed on the product instance. If you choose this option, the return code is automatically submitted to CSSM.
		• If not connected to CSSM, or if you have implemented a topology with CSLU-initiated or SSM On-Prem initiated communication, enter **offline** [*filepath_filename*].
		  • If you enter only the **offline** keyword, copy the return code that is displayed on the CLI and enter it in the CSSM Web UI.
		
		  Complete this task to enter the return code in the CSSM Web UI: Entering a SLAC Return Code in CSSM and Removing a Product Instance.
		  • If you save the return code to a file, upload the file to CSSM Web UI.
		
		  For example: `Device# license smart authorization return local offline bootflash:return-code.txt`
		
		  Note This method of returning SLAC is supported starting with Cisco IOS XE Cupertino 17.7.1 only.
		
		  Complete this task to upload the return request in the CSSM Web UI: Uploading Data or Requests to CSSM and Downloading a File.

	Command or Action	Purpose

Step 7	**show license authorization**
	Example:
	`Device# show license authorization`
	`Overall status:`
	`  Active: PID:C9606R,SN:FXS241201WP`
	`  Status: NOT INSTALLED`
	`  Last return code:`
	`Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-`
	`babWeL-FABPt9-Wr1Dn7-Rp7`
	`  Standby: PID:C9606R,SN:FXS241201WP`
	`  Status: NOT INSTALLED`
	`  Last return code:`
	`Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-`
	`babWeL-FABPt9-Wr1Dn7-Rp7`
	
	`<output truncated>`
		Displays licensing information. Check under the `License Authorizations` header in the output. If the return process is completed correctly, the `Last return code:` field displays the return code.

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 Gibraltar 16.11.1	Base and Add-On Licenses	This feature was introduced. The software features available on Cisco Catalyst 9600 Series Switches fall under base and add-on license levels. See Base and Add-On Licenses, on page 1 and Configuring Base and Add-On Licenses, on page 5.
Cisco IOS XE Cupertino 17.7.1	Base and Add-On Licenses	This feature was implemented on Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2), which was introduced in this release. See Base and Add-On Licenses, on page 1 and Configuring Base and Add-On Licenses, on page 5.

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	Export Control Key for High Security (HSECK9)	Support for the HSECK9 key was introduced on the Cisco Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2) and associated line cards. The HSECK9 key is an export-controlled license, which 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, on page 2 and Installing SLAC for an HSECK9 Key, on page 7.

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