Available Licenses

Information About Available Licenses

This section provides information about the licenses that are available on Cisco Catalyst 9300 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 Essentials
- Network Advantage: Includes features available with the Network Essentials license and more.

Add-On Licenses

- DNA Essentials
- DNA Advantage: Includes features available with the DNA Essentials license and more.

Guidelines for Using Base and Add-On Licenses

- A base license (Network Essentials and Network-Advantage) is ordered and fulfilled only with a perpetual or permanent license type.
- An add-on license (DNA Essentials and 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.

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

  Table 1: Table 4. Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[1]	Yes

  [1] You will be able to purchase this combination only at the time of DNA license renewal and not when you purchase DNA-Essentials the first time

- 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 [2]. 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 9300 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 available only on Cisco Catalyst 9300X Series Switches, starting with Cisco IOS XE Bengaluru 17.6.2.

For information about the available SKUs in the series, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.

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

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 IPsec feature requires an HSECK9 key.

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).

  Each UDI where you want to use a cryptographic feature requires one HSECK9 key. Ensure that you have read the stacking considerations to evaluate the number of keys you require. See Stacking Considerations, on page 4.
- 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.

Ordering Considerations

This section covers important ordering considerations for an HSECK9 key.

A separate HSECK9 key is required for each UDI where you want to use a cryptographic feature. If you have a device stack see the Stacking Considerations, on page 4 section for information about the number of keys you require.

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 9300 Series Ordering Guide.

Stacking Considerations

This section covers HSECK9 considerations and requirements that apply to a device stack with an active, a standby, and one or more members.

- Mixed stacking is not supported - 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, you must 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: Device stack where the standby has an HSECK9 key and SLAC. When a switchover occurs, the system continues operation of the cryptographic functionality on the new active without any interruptions.

  Scenario 2: Device stack where the standby does not have an HSECK9 key.

  - A daily system message is displayed 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 the switchover occurs and the standby (without an HSCECK9 key) becomes the new active, the following system messages are displayed. They 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 stack bootup 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 one of these sequences:
  - Add the device to the stack, and request SLAC for the entire stack again. See Example: Requesting and Installing SLAC - Adding a Member and Requesting SLAC Again, on page 25.
  - Install SLAC on the standalone, configure the cryptographic functionality on the standalone device, and finally add the device to the existing stack. See Example: Requesting and Installing SLAC - Requesting SLAC on a Standalone Then Adding Member, on page 29.

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.
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.

	Command or Action	Purpose
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.

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 local`
		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.
		• *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 authorization code for *all* devices in a High Availability and stacking set-up.

	Command or Action	Purpose
		Note For stacking scenarios only: 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** options. This 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. • **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 local`	Triggers the product instance to synchronize with CSSM, or CSLU, or SSM On-Prem, to send and receive any pending data. This step is optional and applies only to scenarios where the product instance is connected to CSSM, or CSLU or SSM On-Prem, and where the product instance initiates communication. The corresponding topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated), and SSM On-Prem Deployment (product instance-initiated communication). Here, the command manually triggers synchronization and completes the SLAC installation process. Otherwise SLAC is applied to the product instance the next time the product instance contacts CSLU or SSM On-Prem.

What to do next

Required Tasks After Installing SLAC, on page 19

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 local`	Generates a SLAC request with the required HSECK9 key and UDI details. 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. 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.

	Command or Action	Purpose
		Specify the device by entering one of these options: • **all**: Gets the SLAC for *all* devices in a High Availability set-up **Note** 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** options. This 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. • **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 and HSECK9 key details 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:**	(Optional) Copies the file from its source location or directory to the flash memory of the product instance. You can also import the file

	Command or Action	Purpose
	`Device# copy tftp://10.8.0.6/user01/example.txt bootflash:`	*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 19

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 where 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 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 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 local`	Requests a SLAC from CSSM or CSLU or SSM On-Prem. • Specify if you want to add to or replace an existing SLAC:

	Command or Action	Purpose
		• **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. • *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 authorization code for *all* devices in a High Availability and stacking set-up. **Note** For stacking scenarios only: 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** options. This 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. • **local**: Gets the authorization code for the *active* device in a High

	Command or Action	Purpose
		Availability and stacking set-up. This is the default option.
Step 3	(Optional) **license smart sync** {**all** | **local**} **Example:** `Device# license smart sync local`	Triggers the product instance to synchronize with CSSM, or CSLU, or SSM On-Prem, to send and receive any pending data. This step is optional and applies only to scenarios where the product instance is connected to CSSM, or CSLU or SSM On-Prem, and where the product instance initiates communication. The corresponding topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated), and SSM On-Prem Deployment (product instance-initiated communication). Here, the command manually triggers synchronization and completes the SLAC installation process. Otherwise SLAC is applied to the product instance the next time the product instance contacts CSLU or SSM On-Prem.

What to do next

Required Tasks After Installing SLAC, on page 19

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 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 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 local`
		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.
		• *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 authorization code for *all* devices in a High Availability and stacking set-up.

	Command or Action	Purpose
		Note For stacking scenarios only: 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** options. This 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. • **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 19

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 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 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 local`
		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.
		• *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"

	Command or Action	Purpose
		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. **Note** For stacking scenarios only: 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** options. This 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. • **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 local`	Triggers the product instance to synchronize with CSSM, or CSLU, or SSM On-Prem, to send and receive any pending data. This step is optional and applies only to scenarios where the product instance is connected to CSSM, or CSLU or SSM On-Prem, and where the product instance initiates communication. The corresponding topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated), and SSM On-Prem Deployment (product instance-initiated communication). Here, the command manually triggers synchronization and completes the SLAC installation process. Otherwise SLAC is applied

	Command or Action	Purpose
		to the product instance the next time the product instance contacts CSLU or SSM On-Prem.

What to do next

Required Tasks After Installing SLAC, on page 19

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 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 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 19

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.

- 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 more than one SLAC (in a stacking setup), the status, timestamp, and last confirmation code is displayed for each UDIs where SLAC is installed. In the sample output below, SLAC is installed only on the active and not the standby or member switch.

- Check that the *usage* count and status 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.

- The following system messages are displayed after SLAC installation:

  - `Error Message %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.`

Example:

```
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
```

Step 2 Configure the cryptographic feature.

The following IPsec configuration is for example purposes only. For information about configuring the feature, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)*.

Example:

```
 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
```

Step 3 Again check HSECK9 key usage.

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

Note The system counts only one HSECK9 key as IN USE at a given point in time.

Even if you have installed SLAC on more than one device in a stacking step-up, 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.

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
  hseck9                  (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.

When 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.

Procedure

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

Step 2	**show license summary**
	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) 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.

	Command or Action	Purpose

Step 3	**platform hsec-license-release**
	Example:
	`Device# configure terminal`
	`Device(config)# platform hsec-license-release`
	`HSEC license is released`
	`Device(config)# exit`
		(Optional) Enters the global configuration mode, releases the HSECK9 license, and returns to privileged EXEC mode.
		If you have already disabled or unconfigured the cryptographic feature using the HSECK9 key, and the usage status of the HSECK9 key is still displayed as `IN USE`, this command forces the system to change the HSECK9 key status to `NOT IN USE`.

Step 4	**show license summary**
	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`
		(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 5	**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 CSSM. 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 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.

	Command or Action	Purpose
		• 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.

Step 6	**show license authorization**
	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>`
		Displays licensing information. If the return process is completed correctly, the `Last return code:` field displays the return code.

Examples for Configuring Available Licenses

Example: Requesting and Installing SLAC - Adding a Member and Requesting SLAC Again

This example shows you how to add a device to an existing stack where cryptographic functionality is being used. The overall sequence with this method is as follows: Add new member to the existing device → Request and install SLAC for the entire stack again.

Displaying 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 *Connected Directly to CSSM* topology is implemented here. The Smart transport option is used for communication with CSSM.

```
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>
```

Adding 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
```

Requesting SLAC for the entire stack again

The method of requesting and installing SLAC here corresponds with the *Connected Directly to CSSM* topology. 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 (the existing devices in the stack), have changed from 72ad37d5 and 842584db to f6c6978d and 7ae69c8c, respectively.

There is also confirmation code e3fd6642, on the new member, SN:FOC2516LC92.

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

Example: Requesting and Installing SLAC - Requesting SLAC on a Standalone Then Adding Member

This example shows you how to add a device to an existing stack where cryptographic functionality is being used. The overall sequence with this method is as follows: Install SLAC on the standalone → Configure the cryptographic functionality on the standalone → Add the device to the existing stack.

Displaying 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 *Connected Directly to CSSM* topology is implemented here. The Smart transport option is used for communication with CSSM.

```
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>
```

Booting 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
```

Configuring the *No Connectivity to CSSM and No CSLU* topology on the standalone

The example shows configuration that applied to the device used in the example. 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
```

Importing and installing SLAC

Note Note: In this example, SLAC is generated in the CSSM Web UI and not shown here. For detailed steps, see Generating and Downloading SLAC from CSSM to a File.

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
```

Configuring 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
```

Adding 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: SA-Switching-Polaris As of Dec 03 19:04:56 2021 UTC
  Virtual Account: SLE_Adoption_Switching


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
```

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	This feature was introduced. The software features available on Cisco Catalyst 9300 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.

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.6.2	Export Control Key for High Security (HSECK9)	Support for the HSECK9 key was introduced on the Cisco Catalyst 9300X Series Switches. **Note** The HSECK9 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. 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.
Cisco IOS XE Cupertino 17.7.1	Ability to save SLAC request and return in a file in an air-gapped network.	Option to save a SLAC request file on the product instance. The SLAC request file must be uploaded to CSSM and the file containing the SLAC code can then be downloaded and installed it on the product instance. Similarly, an authorization code that is saved to a file can also be uploaded the same way as a RUM report. With this new method you do not have to gather and enter the required details on the CSSM Web UI to generate a SLAC. You also do not have to locate the product instance in the CSSM Web UI to return an authorization code. In the CSSM Web UI, you must upload the SLAC request or return file in the same way as you upload a RUM report. See Installing SLAC: No Connectivity to CSSM and No CSLU, on page 10 and Returning a SLAC, on page 22. For command syntax changes, in the command reference of the corresponding release, see the **license smart** privileged EXEC command.

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.