

Task Library for Smart Licensing Using Policy

This section is a group of tasks that apply to Smart Licensing Using Policy.

If you are implementing a particular topology, refer to the corresponding workflow. See *How to Configure Smart Licensing Using Policy: Workflows by Topology* to know the sequential order of tasks that apply.

- Logging into Cisco (CSLU Interface), on page 2
- Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 2
- Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 3
- Ensuring Network Reachability for Product Instance-Initiated Communication, on page 3
- Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 5
- Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 6
- Ensuring Network Reachability for CSLU-Initiated Communication, on page 7
- Export to CSSM (CSLU Interface), on page 11
- Import from CSSM (CSLU Interface), on page 12
- Requesting SLACs for Multiple Product Instances (CSLU Interface), on page 12
- Setting Up a Connection to CSSM , on page 13
- Configuring Smart Transport Through an HTTPs Proxy, on page 16
- Configuring the Call Home Service for Direct Cloud Access, on page 17
- Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server, on page 20
- Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 21
- Validating Devices (SSM On-Prem UI), on page 22
- Ensuring Network Reachability for Product Instance-Initiated Communication, on page 22
- Retrieving the Transport URL (SSM On-Prem UI), on page 25
- Submitting an Authorization Code Request (SSM On-Prem UI, Connected Mode), on page 26
- Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 27
- Exporting and Importing Usage Data (SSM On-Prem UI), on page 28
- Adding One or More Product Instances (SSM On-Prem UI), on page 29
- Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 30
- Generating and Downloading SLAC from CSSM to a File, on page 35
- Manually Requesting and Auto-Installing a SLAC , on page 37
- Generating and Saving a SLAC Request on the Product Instance, on page 39
- Removing and Returning an Authorization Code, on page 40
- Returning SLAC for an HSECK9 License That Is In-Use, on page 45
- Entering a Return Code in CSSM and Removing the Product Instance, on page 46

• Generating a New Token for a Trust Code from CSSM, on page 47
• Establishing Trust with an ID Token, on page 48
• Downloading a Policy File from CSSM, on page 49
• Uploading Data or Requests to CSSM and Downloading a File, on page 50
• Installing a File on the Product Instance, on page 51
• Setting the Transport Type, URL, and Reporting Interval, on page 52
• Enabling the Utility Mode, on page 55
• Continue Using a PAK License, on page 57
• Removing a PAK License, on page 59
• Removing a PAK License on a Failed Product Instance, on page 60
• Activating a PLR, on page 61
• Upgrading a PLR, on page 64
• Deactivating a PLR, on page 66
• HSECK9 License Mapping Table for Routing Product Instances, on page 67
• Converting a Device-Specific HSECK9 License, on page 75
• Sample Resource Utilization Measurement Report, on page 83

Logging into Cisco (CSLU Interface)

Depending on your needs, when working in CSLU, you can either be in connected or disconnected mode. To work in the connected mode, complete these steps to connect with Cisco.

Procedure

Step 1 From the CSLU Main screen, click **Login to Cisco** (located at the top right corner of the screen).

Step 2 Enter: **CCO User Name** and **CCO Password**.

Step 3 In the CSLU Preferences tab, check that the Cisco connectivity toggle displays “Cisco Is Available”.

Configuring a Smart Account and a Virtual Account (CSLU Interface)

Both the Smart Account and Virtual Account are configured through the Preferences tab. Complete the following steps to configure both Smart and Virtual Accounts for connecting to Cisco.

Procedure

Step 1 Select the **Preferences Tab** from the CSLU home screen.

Step 2 Perform these steps for adding both a Smart Account and Virtual Account:

a) In the Preferences screen navigate to the **Smart Account** field and add the **Smart Account Name**.

b) Next, navigate to the **Virtual Account** field and add the **Virtual Account Name**.

If you are connected to CSSM (In the Preferences tab, **Cisco is Available**), you can select from the list of available SA/VAs.

If you are not connected to CSSM (In the Preferences tab, **Cisco Is Not Available**), enter the SA/VAs manually.

Note
SA/VA names are case sensitive.

Step 3 Click **Save**. The SA/VA accounts are saved to the system

Only one SA/VA pair can reside on CSLU at a time. You cannot add multiple accounts. To change to another SA/VA pair, repeat Steps 2a and 2b then Save. A new SA/VA account pair replaces the previous saved pair

Adding a Product-Initiated Product Instance in CSLU (CSLU Interface)

Complete these steps to add a device-created Product Instance using the Preferences tab.

Procedure

Step 1 Select the **Preferences** tab.

Step 2 In the Preferences screen, de-select the **Validate Device** check box.

Step 3 Set the **Default Connect Method** to **Product Instance Initiated** and then click **Save**.

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps my be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (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	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding SLP_VRF`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 8	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface gigabitethernet0/0`	Configures a source interface for the HTTP client.
Step 9	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf SLP_VRF 192.168.0.1 255.255.0.0 192.168.255.1`	(Required) Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.

	Command or Action	Purpose
Step 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf SLP_VRF 173.37.137.85`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**license smart vrf** *vrf_string* **Example:** `Device(config)# Device(config)# license smart vrf SLP_VRF`	Configures the VRF name that is used by the product instance. The product instance uses the VRF to send licensing-related data to CSSM, CSLU, or SSM On-Prem. Ensure that the product instance is one that supports VRF and that you configure the transport type as **smart** or **cslu**, with the corresponding URL.
Step 12	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Configures the source interface for the DNS domain lookup. **Note** If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 13	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configure DNS discovery of your domain. In accompanying example, the name-server creates entry `cslu-local.example.com`.

Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface)

Using the CSLU interface, you can configure the connect method to be CSLU Initiated. This connect method (mode) enables CSLU to retrieve product instance information from the product instance.

Note The default Connect Method is set in the **Preferences** tab.

Complete these steps to add a product instance from the **Inventory** tab

Procedure

Step 1 Go to the **Inventory** tab and from the Product Instances table, select **Add Single Product**.

Step 2 Enter the **Host** (IP address of the Host).

Step 3 Select the **Connect Method** and select one of the CSLU Initiated connect methods.

Step 4 In the right panel, click **Product Instance Login Credentials**. The left panel of the screen changes to show the User Name and Password fields.

Step 5 Enter the product instance **User Name** and **Password**.

Step 6 Click **Save**.

The information is saved to the system and the device is listed in the Product Instances table with the Last Contact listed as never.

Collecting Usage Reports: CSLU Initiated (CSLU Interface)

CSLU also allows you to manually trigger the gathering of usage reports from devices.

After configuring and selecting a product instance (selecting **Add Single Product**, filling in the **Host** name and selecting a CSLU-initiated connect method), click **Actions for Selected** > **Collect Usage**. CSLU connects to the selected product instances and collects the usage reports. These usage reports are stored in CSLU's local library. These reports can then be transferred to Cisco if CSLU is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Data** > **Export to CSSM**.

If you are working in CSLU-initiated mode, complete these steps to configure CSLU to collect RUM reports from product instances.

Procedure

Step 1 Click the **Preference** tab and enter a valid **Smart Account** and **Virtual Account**, and then selectan appropriate CSLU-initiated collect method. (If there have been any changes in Preferences, make sure you click **Save**).

Step 2 Click the **Inventory** tab and select one or more product instances.

Step 3 Click **Actions for Selected** > **Collect Usage**.

RUM reports are retrieved from each selected device and stored in the CSLU local library. The Last Contacted column is updated to show the time the report was received, and the Alerts column shows the status.

If CSLU is currently logged into Cisco the reports will be automatically sent to the associated Smart Account and Virtual Account in Cisco and Cisco will send an acknowledgement to CSLU as well as to the product instance. The acknowledgement will be listed in the alerts column of the Product Instance table. To manually transfer usage reports Cisco, from the CSLU main screen select **Data** > **Export to CSSM**.

Step 4 From the **Export to CSSM** modal, select the local directory where the reports are to be stored. (<CSLU_WORKING_Directory>/data/default/rum/unsent)

At this point, the usage reports are saved in your local directory (library). To upload these usage reports to Cisco, follow the steps described in Uploading Data or Requests to CSSM and Downloading a File, on page 50.

Note
The Windows operating system can change the behavior of a usage report file properties by dropping the extension when that file is renamed. The behavior change happens when you rename the downloaded file and the renamed file drops the extension. For example, the downloaded default file named `UD_xxx.tar` is renamed to `UD_yyy`. The file loses its TAR extension and cannot function. To enable the usage file to function normally, after re-naming a usage report file, you must also add the TAR extension back to the file name, for example `UD_yyy.tar`.

Ensuring Network Reachability for CSLU-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for CSLU-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (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	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new model** **Example:** `Device(config)# aaa new model`	(Required) Enable the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	(Required) Sets AAA authentication to use the local username database for authentication.

	Command or Action	Purpose
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.
Step 6	ip routing **Example:** `Device(config)# ip routing`	Enables IP routing.
Step 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	(Optional) Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 8	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS). **Note** Note If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 9	**ip domain name** *name* **Example:** `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 10	**no username** *name* **Example:** `Device(config)# no username admin`	(Required) Clears the specified username, if it exists. For *name* , enter the same username you will create in the next step. This ensures that a duplicate of the username you are going to create in the next step does not exist.

	Command or Action	Purpose
		If you plan to use REST APIs for CSLU-initiated retrieval of RUM reports, you have to log in to CSLU. Duplicate usernames may cause the feature to work incorrectly if there are duplicate usernames in the system.

Step 11	**username** *name* **privilege** *level* **password** *password*
	Example:
	`Device(config)# username admin privilege 15`
	`password 0 lab`
		(Required) Establishes a username-based authentication system.
		The **privilege** keyword sets the privilege level for the user. A number between 0 and 15 that specifies the privilege level for the user.
		The password allows access to the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
		This enables CSLU to use the product instance native REST.
		Note
		Enter this username and password in CSLU (Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 6 → *Step 4. f.* CSLU can then collect RUM reports from the product instance.

Step 12	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 13	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 15	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 16	**no shutdown** **Example:**	Restarts a disabled interface.

	Command or Action	Purpose
	`Device(config-if)# no shutdown`	
Step 17	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 18	**ip http server** **Example:** `Device(config)# ip http server`	(Required) Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. The HTTP server uses the standard port 80, by default.

Step 19	**ip http authentication local**
	Example:
	`ip http authentication local`
	`Device(config)#`
		(Required) Specifies a particular authentication method for HTTP server users.
		The **local** keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.

Step 20	**ip http secure-server** **Example:** `Device(config)# ip http server`	(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.
Step 21	**ip http max-connections** **Example:** `Device(config)# ip http max-connections 16`	(Required) Configures the maximum number of concurrent connections allowed for the HTTP server. Enter an integer in the range from 1 to 16. The default is 5.
Step 22	**ip tftp source-interface** *interface-type-number* **Example:** `Device(config)# ip tftp source-interface GigabitEthernet0/0`	Specifies the IP address of an interface as the source address for TFTP connections.
Step 23	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.

Step 24	**logging host**
	Example:
	`Device(config)# logging host 172.25.33.20`
	`vrf Mgmt-vrf`
		Logs system messages and debug output to a remote host.

Step 25	**end** **Example:**	Exits the global configuration mode and enters priveleged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	
Step 26	**show ip http server session-module** **Example:** `Device# show ip http server session-module`	(Required) Verifies HTTP connectivity. In the output, check that `SL_HTTP` is active. Additionally, you can also perform the following checks : • From device where CSLU is installed, verify that you can ping the product instance. A successful ping confirms that the product instance is reachable. • From a Web browser on the device where CSLU is installed verify `https://<product-instance-ip>/`. This ensures that the REST API from CSLU to the product instance works as expected.

Export to CSSM (CSLU Interface)

This option can be used as a part of a manual download procedure when you want the workstation isolated for security purposes.

Procedure

Step 1 Go to the **Preferences** tab, and turn off the **Cisco Connectivity** toggle switch.

The field switches to “Cisco Is Not Available”.

Step 2 From the main menu in the CSLU home screen navigate to **Data** > **Export to CSSM**.

Step 3 Select the file from the modal that opens and click **Save**. You now have the file saved.

Note
At this point you have a DLC file, RUM file, or both.

Step 4 From a workstation that has connectivity to Cisco, and complete the following: Uploading Data or Requests to CSSM and Downloading a File, on page 50.

Once the file is downloaded, you can import it into CSLU, see Import from CSSM (CSLU Interface), on page 12

Import from CSSM (CSLU Interface)

Once you have received the ACK or other file (such as an authorization code) from Cisco, you are ready to upload that file to your system. This procedure can be used for workstations that are offline. Complete these steps to select and upload files from Cisco.

Procedure

Step 1 Ensure that you have downloaded the file to a location that is accessible to CSLU.

Step 2 From the main menu in the CSLU home screen, navigate to **Data** > **Import from CSSM**.

Step 3 An Import from CSSM modal open for you to either:

- Drag and Drop a file that resides on your local drive, or
- Browse for the appropriate *.xml file, select the file and click **Open**.

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

Step 4 When you have finished uploading, click the **x** at the top right corner of the modal to close it.

Requesting SLACs for Multiple Product Instances (CSLU Interface)

The **Authorization Code Request** menu option is specifically used to manually request SLACs for multiple Product Instances.

Before you begin

Supported topologies:

- Connected to CSSM Through CSLU
- CSLU Disconnected from CSSM

Procedure

Step 1 From the Product Instance table, select the **Product Instances** for authorization code request.

Step 2 With one or more Product Instances selected, select the **Authorization Code Request** option from the Available Actions menu.

Step 3 In the modal it describes that steps to take, click **Accept**

The upload modal opens to select a CSV file for uploading. (local)

Step 4 Next, follow these steps that are also described in the modal.

a) Upload the file to Cisco by following this directory path: **software.cisco.com** > **Smart Software Licensing** > **Inventory** > **Product Instances** > **Authorize License Enforced Features**

b) Follow the steps shown on the screen:

1. Select **Multiple Product Instances**.

   If multiple Product Instances, you can click **Choose File** to upload or **Download a Template** (csv file template) for future uploads.

2. In the next panel, **select licenses**.

3. Review and Confirm your **license selections**

4. Create the **Authorization Code** to be downloaded

c) After the file and selected licenses have uploaded to Cisco, **download the authorization codes** (as a file) for those Product Instances selected back to CSLU.

Step 5 Select **Upload From Cisco (in the CSLU interface)**

If CSLU is In Product-Initiated mode: The uploaded codes are now applied to the Product Instances the next time the Product Instance contacts CSLU.

If CSLU is in a CSLU initiated mode: The uploaded codes are now applied to the Product Instances the next time the CSLU runs an update.

Setting Up a Connection to CSSM

The following steps show how to set up a Layer 3 connection to CSSM to verify network reachability. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

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	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:**	Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The

	Command or Action	Purpose
	`Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	**ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6* **Example:** `Device(config)# ip name-server vrf SLP_VRF 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	(Optional) Configures DNS on the VRF interface. You can specify up to six name servers. Separate each server address with a space. **Note** This command is an alternative to the **ip name-server** command.
Step 5	**license smart vrf** *vrf_string* **Example:** `Device(config)# Device(config)# license smart vrf SLP_VRF`	Configures the VRF name that is used by the product instance. The product instance uses the VRF to send licensing-related data to CSSM, CSLU, or SSM On-Prem. Ensure that the product instance is one that supports VRF and that you configure the transport type as **smart** or **cslu**, with the corresponding URL.
Step 6	**ip domain lookup source-interface** *interface-type interface-number* **Example:** `Device(config)# ip domain lookup source-interface Vlan100`	Configures the source interface for the DNS domain lookup.
Step 7	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configures the domain name.
Step 8	**ip host tools.cisco.com** *ip-address* **Example:** `Device(config)# ip host tools.cisco.com 209.165.201.30`	Configures static hostname-to-address mappings in the DNS hostname cache if automatic DNS mapping is not available.

Step 9	**interface** *interface-type-number*
	Example:
	`Device(config)# interface Vlan100`
	`Device(config-if)# ip address 192.0.2.10 255.255.255.0`
	`Device(config-if)# exit`
		Configures a Layer 3 interface. Enter an interface type and number or a VLAN.

Step 10	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] **Example:**	(Required) Activates the NTP service (if it has not already been activated) and enables the system to synchronize the system software

	Command or Action	Purpose

	`Device(config)# ntp server 198.51.100.100 version 2 prefer`	clock with the specified NTP server. This ensures that the device time is synchronized with CSSM.
		Use the **prefer** keyword if you need to use this command multiple times and you want to set a preferred server. Using this keyword reduces switching between servers.
		Tip
		After you complete this configuration, use the **show license tech** to verify if the clock has actually synchronized. If successfully synchronized, the `Clock sync-ed with NTP` field is set to `True`. If not synchronized, this field is set to `False`.
		If the clock is not synchronized, your **attempts** at trust establishment or requesting SLAC and so on, are not reflected in the **show license tech** output. For example:
		`Trust Establishment:`
		`  Attempts: Total=0, Success=0, Fail=0`
		`  Ongoing Failure: Overall=0`
		`Communication=0`

Step 11	**switchport access vlan** *vlan_id*
	Example:
	`Device(config)# interface GigabitEthernet1/0/1`
	`Device(config-if)# switchport access vlan 100`
	`Device(config-if)# switchport mode access`
	`Device(config-if)# exit`
	`OR`
	`Device(config)#`
		Enables the VLAN for which this access port carries traffic and sets the interface as a nontrunking nontagged single-VLAN Ethernet interface.
		Note
		This step is to be configured only if the switchport access mode is required. The **switchport access vlan** command may apply to Catalyst switching product instances, for example, and for routing product instances you may want to configure the **ip address** *ip-address mask* command instead.

Step 12	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route 192.0.2.0 255.255.255.255 192.0.2.1`	Configures a route on the device. You can configure either a static route or a dynamic route.
Step 13	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface Vlan100`	(Required) Configures a source interface for the HTTP client. Enter an interface type and number or a VLAN.

	Command or Action	Purpose
Step 14	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 15	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Configuring Smart Transport Through an HTTPs Proxy

To use a proxy server to communicate with CSSM when using the Smart transport mode, complete the following steps:

Note *Authenticated* HTTPs proxy configurations are not supported.

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 smart transport smart** **Example:** `Device(config)# license smart transport smart`	Enables Smart transport mode.
Step 4	**license smart url default** **Example:** `Device(config)# license smart transport default`	Automatically configures the Smart URL (https://smartreceiver.cisco.com/licservice/license). For this option to work as expected, the transport mode in the previous step must be configured as **smart**.
Step 5	**license smart proxy** {**address** *address_hostname* | **port** *port_num*} **Example:**	Configures a proxy for the Smart transport mode. When a proxy is configured, licensing messages are sent to the proxy along with the final destination URL (CSSM). The proxy sends

	Command or Action	Purpose
	`Device(config)# license smart proxy address 192.168.0.1` `Device(config)# license smart proxy port 3128`	the message on to CSSM. Configure the proxy IP address and port information separately: • **address** *address_hostname*: Specifies the proxy address. Enter the IP address or hostname of the proxy server. • **port** *port_num*: Specifies the proxy port. Enter the proxy port number. Note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`. For more information about the status line, see section 3.1.2 of RFC 7230.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Configuring the Call Home Service for Direct Cloud Access

The Call Home service provides email-based and web-based notification of critical system events to CSSM. To configure the transport mode, enable the Call Home service, and configure a destination profile (A destination profile contains the required delivery information for an alert notification. At least one destination profile is required.), complete the following steps:

Note All steps are required unless specifically called-out as "(Optional)".

Procedure

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart transport callhome** **Example:** `Device(config)# license smart transport callhome`	Enables Call Home as the transport mode.
Step 4	**license smart url** *url* **Example:** `Device(config)# license smart url https://tools.cisco.com/its/service/oddce/services/DDCEService`	For the **callhome** transport mode, configure the CSSM URL exactly as shown in the example.
Step 5	**service call-home** **Example:** `Device(config)# service call-home`	Enables the Call Home feature.
Step 6	**call-home** **Example:** `Device(config)# call-home`	Enters Call Home configuration mode.
Step 7	**contact-email-address** *email-address* **Example:** `Device(config-call-home)# contact-email-addr username@example.com`	Assigns customer's email address and enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process. You can enter up to 200 characters in email address format with no spaces.

Step 8	**profile** *name*
	Example:
	`Device(config-call-home)# profile CiscoTAC-1`
	`Device(config-call-home-profile)#`
		Enters the Call Home destination profile configuration submode for the specified destination profile.
		By default:
		• The CiscoTAC-1 profile is inactive. To use this profile with the Call Home service, you must enable the profile.
		• The CiscoTAC-1 profile sends a full report of all types of events subscribed in the profile. The alternative is to additionally configure `Device(cfg-call-home-profile)# anonymous-reporting-only` anonymous-reporting-only. When this is

	Command or Action	Purpose
		set, only crash, inventory, and test messages will be sent. Use the **show call-home profile all** command to check the profile status.
Step 9	**active** **Example:** `Device(config-call-home-profile)# active`	Enables the destination profile.

Step 10	**destination transport-method http** {**email** |**http**}
	Example:
	`Device(config-call-home-profile)# destination transport-method http`
	AND
	`Device(config-call-home-profile)# no destination transport-method email`
		Enables the message transport method. In the example, Call Home service is enabled via HTTP and transport via email is disabled.
		
		The **no** form of the command disables the method.

Step 11	**destination address** { **email** *email_address* |**http** *url*}
	Example:
	`Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
	AND
	`Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
		Configures the destination e-mail address or URL to which Call Home messages are sent. When entering a destination URL, include either **http://** (default) or **https://**, depending on whether the server is a secure server.
		
		In the example provided here, a **http://** destination URL is configured; and the **no** form of the command is configured for **https://**.

Step 12	**exit** **Example:** `Device(config-call-home-profile)# exit`	Exits Call Home destination profile configuration mode and returns to Call Home configuration mode.
Step 13	**exit** **Example:** `Device(config-call-home)# end`	Exits Call Home configuration mode and returns to privileged EXEC mode.
Step 14	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.
Step 15	**show call-home profile** {*name* |**all**}	Displays the destination profile configuration for the specified profile or all configured profiles.

Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server

The Call Home service can be configured through an HTTPs proxy server. This configuration requires no user authentication to connect to CSSM.

Note Authenticated HTTPs proxy configurations are not supported.

To configure and enable the Call Home service through an HTTPs proxy, complete the following steps:

Note All steps are required unless specifically called-out as "(Optional)".

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 smart transport callhome** **Example:** `Device(config)# license smart transport callhome`	Enables Call Home as the transport mode.
Step 4	**service call-home** **Example:** `Device(config)# service call-home`	Enables the Call Home feature.
Step 5	**call-home** **Example:** `Device(config)# call-home`	Enters Call Home configuration mode.
Step 6	**http-proxy** *proxy-address* **proxy-port** *port-number* **Example:**	Configures the proxy server information to the Call Home service. Note the change in the criteria for the acceptance of proxy servers, starting with Cisco

	Command or Action	Purpose
	`Device(config-call-home)# http-proxy 198.51.100.10 port 5000`	IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`. For more information about the status line, see section 3.1.2 of RFC 7230.
Step 7	**exit** **Example:** `Device(config-call-home)# exit`	Exits Call Home configuration mode and enters global configuration mode.
Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 9	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Assigning a Smart Account and Virtual Account (SSM On-Prem UI)

You can use this procedure to import one or more product instances along with corresponding Smart Account and Virtual Account information, into the SSM On-Prem database. This enables SSM On-Prem to map product instances that are part of local virtual accounts (other than the default local virtual account), to the correct license pool in CSSM:

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 Log into the SSM On-Prem and select the **Smart Licensing** workspace.

Step 2 Navigate to **Inventory** > **SL Using Policy** > **Export/Import All** > **Import Product Instances List**

The **Upload Product Instances** window is displayed.

Step 3 Click **Download** to download the .csv template file and enter the required information for all the product instances in the template.

Step 4 Once you have filled-out the template, click **Inventory** > **SL Using Policy** > **Export/Import All** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

Step 5 Now, click **Browse** and upload the filled-out .csv template.

Smart Account and Virtual Account information for all uploaded product instances is now available in SSM On-Prem.

Validating Devices (SSM On-Prem UI)

When device validation is enabled, RUM reports from unknown product instances (not in the SSM On-Prem database) are rejected.

By default, devices are not validated. Complete the following steps to enable it:

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 In the **On-Prem License Workspace** window, click **Admin Workspace** and log in, if prompted.

The **On-Prem Admin Workspace** window is displayed.

Step 2 Click the **Settings** widget.

The **Settings** window is displayed.

Step 3 Navigate to the **CSLU** tab and turn-on the **Validate Device** toggle switch.

RUM reports from unknown product instances will now be rejected. If you haven't already, you must now add the required product instances to the SSM On-Prem database before sending RUM reports. See Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 21

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps my be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Note Ensure that you configure steps 14, 15, and 16 exactly as shown below. These commands must be configured to ensure that the correct trustpoint is used and that the necessary certificates are accepted for network reachability.

Before you begin

Supported topologies: SSM On-Prem Deployment(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	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding SLP_VRF`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 8	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface gigabitethernet0/0`	Configures a source interface for the HTTP client.
Step 9	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf SLP_VRF 192.168.0.1 255.255.0.0 192.168.255.1`	(Required) Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf SLP_VRF 198.51.100.1`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**license smart vrf** *vrf_string* **Example:** `Device(config)# Device(config)# license smart vrf SLP_VRF`	Configures the VRF name that is used by the product instance. The product instance uses the VRF to send licensing-related data to CSSM, CSLU, or SSM On-Prem. Ensure that the product instance is one that supports VRF and that you configure the transport type as **smart** or **cslu**, with the corresponding URL.
Step 12	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Configures the source interface for the DNS domain lookup.
Step 13	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configure DNS discovery of your domain. In the accompanying example, the name-server creates entry `cslu-local.example.com`.

Step 14	**crypto pki trustpoint SLA-TrustPoint**
	Example:
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		(Required) Declares that the product instance should use trustpoint "SLA-TrustPoint" and enters the ca-trustpoint configuration mode. The product instance does not recognize any trustpoints until you declare a trustpoint using this command.

Step 15	enrollment terminal **Example:**	(Required) Specifies the certificate enrollment method.

	Command or Action	Purpose
	`Device(ca-trustpoint)# enrollment terminal`	
Step 16	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	(Required) Specifes a method that is to be used to ensure that the certificate of a peer is not revoked. For the SSM On-Prem Deployment topology, enter the **none** keyword. This means that a revocation check will not be performed and the certificate will always be accepted.

Step 17	**exit**
	Example:
	`Device(ca-trustpoint)# exit`
	`Device(config)# exit`
		Exits the ca-trustpoint configuration mode and then the global configuration mode and returns to privileged EXEC mode.

Step 18	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Retrieving the Transport URL (SSM On-Prem UI)

You must configure the transport URL on the product instance when you deploy the product instance-initiated communication with SSM On-Prem deployment. This task show you how to easily copy the complete URL including the tenant ID from SSM On-Prem.

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 Log into SSM On-Prem and select the **Smart Licensing** workspace.

Step 2 Navigate to the **Inventory** tab and from the dropdown list of local virtual accounts (top right corner), select the *default local virtual account*. When you do, the area under the **Inventory** tab displays **Local Virtual Account: Default**.

Step 3 Navigate to the **General** tab.

The **Product Instance Registration Tokens** area is displayed.

Step 4 In the **Product Instance Registration Tokens** area click **CSLU Transport URL**.

The **Product Registration URL** pop-window is displayed.

Step 5 Copy the entire URL and save it in an accessible place.

You will require the URL when you configure the transport type and URL on the product instance.

Step 6 Configure the transport type and URL. See: Setting the Transport Type, URL, and Reporting Interval, on page 52.

Submitting an Authorization Code Request (SSM On-Prem UI, Connected Mode)

This procedure shows you how to install SLAC for export-controlled and enfored licenses when SSM On-Prem is connected to CSSM. Here you begin by sending the SLAC request from the product instance, to SSM On-Prem. You must then synchronize SSM On-Prem with CSSM. CSSM processes the request and the response is send back to SSM On-Prem. Finally, the response is sent from SSM On-Prem to the product instance and the SLAC is installed on the device.

Before you begin

Supported topologies: SSM On-Prem Deployment (Product instance-initiated communication).

Ensure that you have an adequate positive balance of the necessary export-controlled or enforced licenses in your Smart Account and Virtual Account in CSSM.

Procedure

Step 1 On the product instance, configure the following command: **license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local** }

This sends the SLAC request to SSM On-Prem.

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

- **add**: Adds the requested license to an existing SLAC. The new authorization code will contain all the licences of the existing SLAC, and the requested license.
- **replace**: Replaces the existing SLAC. The new SLAC will contain only the requested license. All licenses in the existing SLAC are returned. When you enter this keyword, the product instance checks if these existing licenses 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 license for which you want to request an addition or a replacement of the SLAC. For example, enter `hseck9` for the HSECK9 license.

Specify the device by entering one of these options:

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

Step 2 Log into SSM On-Prem.

Step 3 In the SSM On-Prem UI, Smart Licensing workspace, nagivate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**

The SLAC request is sent to CSSM. CSSM processes the request and sends a SLAC response back to SSM On-Prem, which sends the response to the product instance. It is automatically installed on the product instance.

You can monitor the event log in SSM On-Prem UI to know when the SLAC has been sent to the product instance.

Step 4 On the product instance, enter the **show license authorization** command in privileged EXEC mode to display SLAC information.

Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode)

With the SSM On-Prem Deployment topology, if SSM On-Prem is not connected to CSSM, the authorization codes required for export-controlled and enfored licenses must be generated in CSSM and imported into SSM On-Prem before the product instance can request the same.

This procedure shows you the steps you have to complete in SSM On-Prem (to submit the request and then import SLAC), points you to the procedure you have to complete in CSSM (to generate and download SLAC), and to the procedure you have to complete on the product instance (to finally request and install SLAC).

Before you begin

Supported topologies:

- SSM On-Prem Deployment (SSM On-Prem-initiated communication)
- SSM On-Prem Deployment (Product instance-initiated communication).

Ensure that you have an adequate positive balance of the necessary export-controlled or enforced licenses in your Smart Account and Virtual Account in CSSM.

Procedure

Step 1 Log into SSM On-Prem and select **Smart Licensing**.

Step 2 Navigate to **Inventory** > **SL Using Policy**. Select all the product instances for which you want to request SLAC.

Step 3 Click **Actions for Selected…** > **Authorization Code Request**.

The **Authorization Request Information** pop-up window is displayed.

Step 4 Click **Accept** and save the .csv file when prompted.

The generated .csv file contains the list of selected product instances along with required device information, in the required format, to generate the SLAC in CSSM. Save this file in a location that is accessible when you are working on the CSSM Web UI (in the next step).

Step 5 Complete this task in CSSM: Uploading Data or Requests to CSSM and Downloading a File, on page 50.

You can use the above procedure to generate SLAC for a single product instance and for multiple product instances. For the SSM On-Prem Deployment topology, follow the steps to generate SLAC for multiple product instances.

Step 6 Return to the SSM On-Prem UI and navigate to **Inventory** > **SL Using Policy**.

Step 7 Click **Export/Import All…** > **Import From Cisco**.

Import the file download from CSSM at the end of the procedure in Step 5 above.

To verify import, under **Inventory** > **SL Using Policy**, see the Alerts column. The following message is displayed: Authorization message received from CSSM.

Step 8 Complete this task on the product instance: Manually Requesting and Auto-Installing a SLAC , on page 37.

This task shows you how to request and install SLAC from SSM On-Prem.

Exporting and Importing Usage Data (SSM On-Prem UI)

You can use this procedure to complete usage synchronization between SSM On-Prem and CSSM when SSM On-Prem is disconnected from CSSM.

Before you begin

Supported topologies:

- SSM On-Prem Deployment (SSM On-Prem-initiated communication)
- SSM On-Prem Deployment (product instance-initiated communication).

Reporting data must be available in SSM On-Prem. You must have either pushed the nessary reporting data from the product instance to SSM On-Prem (product instance-initiated communication) or retrieved the necessary reporting data from the product instance (SSM On-Prem-initiated communication).

Procedure

Step 1 Log into SSM On-Prem and select **Smart Licensing**.

Step 2 Navigate to **Inventory** > **SL Using Policy** tab.

Step 3 In the **SL Using Policy** tab area, click **Export/Import All...** > **Export Usage to Cisco**.

This generates one .tar file with *all* the usage reports available in the SSM On-Prem server.

Step 4 Complete this task in CSSM: Uploading Data or Requests to CSSM and Downloading a File, on page 50.

At the end of this task you will have an ACK file to import into SSM On-Prem.

Step 5 Again navigate to the **Inventory** > **SL Using Policy** tab.

Step 6 In the **SL Using Policy** tab area, click **Export/Import All...** > **Import From Cisco** . Upload the .tar ACK file.

To verify ACK import, in the **SL Using Policy** tab area check the **Alerts** column of the corresponding product instance. The following message is displayed: Acknowledgement received from CSSM.

Adding One or More Product Instances (SSM On-Prem UI)

You can use this procedure to add one product instance or to import and add multiple product instances. It enables SSM On-Prem to retrieve information from the product instance.

Before you begin

Supported topologies: SSM On-Prem Deployment (SSM On-Prem-initiated communication).

Procedure

Step 1 Log into the SSM On-Prem UI and click **Smart Licensing**.

Step 2 Navigate to **Inventory** tab. Select a local virtual account from the drop-down list in the top right corner.

Step 3 Navigate to the **SL Using Policy** tab.

Step 4 Add a single product or import multiple product instances (*choose one*).

- **To add a single product instance**:
  - **a.** In the **SL Using Policy** tab area, click **Add Single Product**.
  - **b.** In the **Host** field, enter the IP address of the host (product instance).
  - **c.** From the **Connect Method** dropdown list, select an appropriate SSM On-Prem-initiated connect method.

    The available connect methods for SSM On-Prem-initiated communication are: NETCONF, RESTCONF, and REST API.
  - **d.** In the right panel, click **Product Instance Login Credentials**.

    The **Product Instance Login Credentials** window is displayed

    Note
    You need the login credentials if a product instance requires a SLAC. Further, you must have also added a valid Smart Account and Virtual Account before any SLAC requests can be serviced.
  - **e.** Enter the **User ID** and **Password**, and click **Save**.

    This is the same user ID and password that you configured as part of commands required to establish network reachability (Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 30).

    Once validated, the product instance is displayed in the listing in the **SL Using Policy** tab area.
- **To import multiple product instances:**
  - **a.** In **SL Using Policy** tab, click **Export/Import All...** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

b. Click **Download** to download the predefined .csv template.

c. Enter the required information for all the product instances in the .csv template.

In the template, ensure that you provide **Host**, **Connect Method** and **Login Credentials** for all product instances.

The available connect methods for SSM On-Prem-initiated communication are: NETCONF, RESTCONF, and REST API.

Login credentials refer to the user ID and password that you configured as part of commands required to establish network reachability (Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 30).

d. Again navigate to **Inventory** > **SL Using Policy** tab. Click **Export/Import All....** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

e. Now upload the filled-out .csv template.

Once validated, the product instances are displayed in the listing in the **SL Using Policy** tab.

Ensuring Network Reachability for SSM On-Prem-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for SSM On-Prem-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Note Ensure that you configure steps 25, 26, and 27 exactly as shown below. These commands must be configured to ensure that the correct trustpoint is used and that the necessary certificates are accepted for network reachability.

Before you begin

Supported topologies: SSM On-Prem Deployment (SSM On-Prem-initiated communication).

Procedure

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new model** **Example:** `Device(config)# aaa new model`	(Required) Enable the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	(Required) Sets AAA authentication to use the local username database for authentication.
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.
Step 6	ip routing **Example:** `Device(config)# ip routing`	Enables IP routing.
Step 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	(Optional) Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 8	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS). **Note** If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port

	Command or Action	Purpose
		mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 9	**ip domain name** *name* **Example:** `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 10	**no username** *name* **Example:** `Device(config)# no username admin`	(Required) Clears the specified username, if it exists. For *name* , enter the same username you will create in the next step. This ensures that a duplicate of the username you are going to create in the next step does not exist. If you plan to use REST APIs for SSM On-Prem-initiated retrieval of RUM reports, you have to log in to SSM On-Prem. Duplicate usernames may cause the feature to work incorrectly if there are present in the system.

Step 11	**username** *name* **privilege** *level* **password** *password*
	Example:
	`Device(config)# username admin privilege 15`
	`password 0 lab`
		(Required) Establishes a username-based authentication system.
		The **privilege** keyword sets the privilege level for the user. A number between 0 and 15 that specifies the privilege level for the user.
		The password allows access to the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
		This enables SSM On-Prem to use the product instance native REST.
		Note
		Enter this username and password in SSM On-Prem (Adding One or More Product Instances (SSM On-Prem UI), on page 29). This enables SSM On-Prem to collect RUM reports from the product instance.

Step 12	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.

	Command or Action	Purpose
Step 13	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 15	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 16	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts a disabled interface.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 18	**ip http server** **Example:** `Device(config)# ip http server`	(Required) Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. The HTTP server uses the standard port 80, by default.

Step 19	**ip http authentication local**
	Example:
	`ip http authentication local`
	`Device(config)#`
		(Required) Specifies a particular authentication method for HTTP server users.
		The **local** keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.

Step 20	**ip http secure-server** **Example:** `Device(config)# ip http server`	(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.
Step 21	**ip http max-connections** **Example:** `Device(config)# ip http max-connections 16`	(Required) Configures the maximum number of concurrent connections allowed for the HTTP server. Enter an integer in the range from 1 to 16. The default is 5.

	Command or Action	Purpose
Step 22	**ip tftp source-interface** *interface-type-number* **Example:** `Device(config)# ip tftp source-interface GigabitEthernet0/0`	Specifies the IP address of an interface as the source address for TFTP connections.
Step 23	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 24	**logging host** **Example:** `Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	Logs system messages and debug output to a remote host.

Step 25	**crypto pki trustpoint SLA-TrustPoint**
	Example:
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		(Required) Declares that the product instance should use trustpoint "SLA-TrustPoint" and enters the ca-trustpoint configuration mode. The product instance does not recognize any trustpoints until you declare a trustpoint using this command.

Step 26	enrollment terminal **Example:** `Device(ca-trustpoint)# enrollment terminal`	Required) Specifies the certificate enrollment method.
Step 27	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	(Required) Specifes a method that is to be used to ensure that the certificate of a peer is not revoked. For the SSM On-Prem Deployment topology, enter the **none** keyword. This means that a revocation check will not be performed and the certificate will always be accepted.

Step 28	**end**
	Example:
	`Device(ca-trustpoint)# exit`
	`Device(config)# end`
		Exits the ca-trustpoint configuration mode and then the global configuration mode and returns to privileged EXEC mode.

Step 29	**show ip http server session-module** **Example:** `Device# show ip http server session-module`	(Required) Verifies HTTP connectivity. In the output, check that `SL_HTTP` is active. Additionally, you can also perform the following checks : • From device where SSM On-Prem is installed, verify that you can ping the product instance. A successful ping

	Command or Action	Purpose
		confirms that the product instance is reachable. • From a Web browser on the device where SSM On-Prem is installed verify `https://<product-instance-ip>/`. This ensures that the REST API from SSM On-Prem to the product instance works as expected.
Step 30	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Generating and Downloading SLAC from CSSM to a File

To generate a SLAC in CSSM and download it to a file, perform the following steps in CSSM:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM
- SSM On-Prem Deployment (product instance-initiated and SSM On-Prem-initiated communication)

You can use this procedure to generate SLAC for a single product instance and for multiple product instances.

If it is for a single product instance, you will require the PID and Serial number to complete this task. On the product instance, enter the **show license udi** command in privileged EXEC mode and keep this information handy.

If it is for multiple product instances, have the .csv file (with necessary product instance information) saved in an accessible location.

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Click the **Inventory** tab.

Step 3 Click the **Product Instances** tab.

Step 4 Click the **Authorize License Enforced Features** tab.

Step 5 Generate SLAC for a single product instance or for multiple product instances (*choose one*).

- **To generate SLAC for a single product instance:**
  a. Enter the **PID** and **Serial Number**.

     Note
     Do not populate any of the other fields.

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

     Ensure that you choose the correct license for a PID. See the HSECK9 License Mapping Table for Routing Product Instances, on page 67 for reference.

  c. Click **Next**

  d. Click **Generate Authorization Code**.

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

  f. Install the file on the product instance. See Installing a File on the Product Instance, on page 51.

- **To generate SLAC for multiple product instances (you will have a .csv file to upload in this case)**:
  a. From the dropdown list that says “Single Device” (by default), change the selection to “Multiple Devices”.

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

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

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

     Note
     If you are requesting SLAC for export-controlled or enforced licenses in the Smart Licensing Using Policy environment only one SLAC is required for each product instance.

  e. From the **Device Type** dropdown list, select **DNA On-Prem**, and click **Continue**.

  f. Click **Reserve Licenses**.

     The **Download Authorization Codes** button is displayed.

  g. Click **Download Authorization Codes** to download this .csv file, which has SLACs for all product insances in step c. above. Click **Close**.

  h. You can now import this .csv file to SSM On-Prem. Return to Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 27 and complete the remaining steps to import this file.

Manually Requesting and Auto-Installing a SLAC

To request CSSM, or CSLU, or SSM On-Prem for a SLAC and have it automatically installed on the product instance, perform the following steps on the product instance:

Before you begin

Supported topologies:

- Connected to CSSM Through CSLU
- Connected Directly to CSSM
- SSM On-Prem Deployment (product instance-initiated communication)

Before you proceed, check the following as well:

- The product instance on which you are requesting the SLAC is connected CSSM, CSLU, or SSM On-Prem.
- The transport type is set accordingly (**smart** for CSSM, and **cslu** for CSLU). Enter the **show license all** command in privileged EXEC mode. In the output, check field `Transport: .`
- If you are directly connected to CSSM, a trust code is installed. Enter the **show license all** command in privileged EXEC mode. In the output check field `Trust Code Installed:`
- In case of an SSM On-Prem Deployment where SSM On-Prem is in a disconnected mode, the product instance requests SSM On-Prem for SLAC in this task, so the required SLAC file must be available in the SSM On-Prem server before you begin with this task. See Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 27

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 replace hseck9 local`	The **license smart authorization request** command requests a SLAC from CSSM or CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem. A SLAC is returned and automatically installed on the product instance. Specify if you want to add to or replace an existing SLAC: • **add**: Adds the requested license to an existing SLAC. The new authorization code will contain all the licences of the existing SLAC, and the requested license.

	Command or Action	Purpose
		Do not use this option even though it is available on the CLI, for any of the supported product instances that are within the scope of this document. Use the replace option in all scenarios. • **replace**: Requests SLAC if it is not already installed, or replaces an existing SLAC. When you enter this keyword, the product instance checks if these existing licenses are in-use. If they are, an error message is displayed, telling you to first disable the corresponding feature. A device requires only one SLAC. For *feature_name*, enter the name of the license for which you want to request an addition or a replacement of the SLAC. Specify the device by entering one of these options: • **all**: Gets the authorization code for *all* devices in a High Availability set-up • **local**: Gets the authorization code for the *active* device in a High Availability set-up. This is the default option. Alternatively, use one of the following methods to request and install a SLAC - note the supported platforms for each option: • Only on Cisco 1000, 4000 Series Integrated Services Routers, Catalyst 8200 Edge Platforms, and 8300 Edge Platforms: **license feature** *feature_name*: Enables the feature and automatically request the code. `Device(config)# license feature hseck9` • Only on Catalyst 8000V Edge Software, Cisco Cloud Services Router 1000v, Cisco Integrated Services Virtual Routers: **platform hardware throughput level MB** {**500** |**1000** | **2500** | **5000**}: Requests and installs the requisite SLAC. This is supported only with the throughput value keywords specified here (greater than 250 MB).

	Command or Action	Purpose
		`Device(config)# platform hardware throughput level MB 5000`
Step 3	**show license authorization** **Example:** `Device# show license authorization`	Displays the authorization code (SLAC) installed on the product instance.

Generating and Saving a SLAC Request on the Product Instance

To generate and then save a SLAC request for an HSECK9 key to a file on the product instance, complete the following task:

Note This method of requesting a SLAC is supported starting with Cisco IOS XE Cupertino 17.7.1a only.

Before you begin

Supported topologies: 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 replace hseck9 local`	Generates a SLAC request with the required license and UDI details. Specify if you want to add to or replace an existing SLAC: • **add**: Adds the requested license to an existing SLAC. The new authorization code will contain all the licences of the existing SLAC, and the requested license. **Note** Do not use this option even though it is available on the CLI, for any of the supported product instances that are within the scope of this document. Use the replace option in all scenarios. • **replace**: Requests an authorization code (SLAC) if it is not already installed, or

	Command or Action	Purpose
		replaces an existing one. When you enter this keyword, the product instance checks if these existing licenses are in-use. If they are, an error message is displayed, telling you to first disable the corresponding feature. A device requires only one SLAC. For *feature_name*, enter the name of the license for which you want to request an addition or a replacement of the SLAC. Specify the device by entering one of these options: • **all**: Gets the SLAC for *all* devices in a High Availability set-up • **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 license details for the SLAC request in a .txt file, in the specified location.
Step 4	Upload the file to the CSSM Web UI, and then download the file containing the SLAC code.	Complete this task: Uploading Data or Requests to CSSM and Downloading a File, on page 50.
Step 5	Install the file on the product instance.	Complete this task: Installing a File on the Product Instance, on page 51.

Removing and Returning an Authorization Code

This task shows how you can remove an authorization code for a license and return it to your license pool in CSSM. The authorization code on the device can be any one of the following: a Smart Licensing Authorization Code (SLAC), a Specific License Reservation (SLR) authorization code, a Product Activation Key (PAK), a Permanent License Reservation (PLR) authorization code.

You may want to remove and return an authorization code on a product instance under these circumstances:

- You no longer want to use the cryptographic feature, which requires an HSECK9 license.
- You want to return a device for Return Material Authorization (RMA), or decommission it permanently. As part of the RMA or decommision process you must perform a factory reset. But before you perform a factory reset, remove the authorization code and return the license to your license pool in CSSM.

Note Not all authorization codes require you to perform the entire procedure. Further, on some product instances, you cannot remove and return the code yourself. Note the specific guidelines provided under "**Before you begin**" for each kind of authorization code and the differences in the prerequisites between product instances.

Before you begin

Supported topologies: all

- To return *a SLAC* for an HSECK9 license:
  - On Cisco 1000, 4000 Series Integrated Services Routers, first disable the HSECK9 license for which SLAC is installed. Next, save configuration changes and reload the device for the status of the HSECK9 license to be displayed as NOT IN USE.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no license feature hseck9
% use 'write' command to disable 'hseck9' license on next boot
Device(config)# end
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Device# reload
Proceed with reload? [confirm]
.
.
.
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Jan 29 07:10:00 2023 UTC
  Virtual Account: Eg-VA
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  hseck9                  (ISR_4331_Hsec)                   0 NOT IN USE
  booster_performance     (ISR_4331_BOOST)                  1 IN USE
  appxk9                  (ISR_4331_Application)            1 IN USE
  uck9                    (ISR_4331_UnifiedCommun...)       1 IN USE
  securityk9              (ISR_4331_Security)               1 IN USE
```

  After the above prerequsite is met, perform the remaining steps to remove and return the SLAC as show in the procedure below.

  - On Cisco Catalyst 8200 and 8300 Edge Platforms, first configure the throughput to lesser than 250 Mbps. This can be a tier-based value or a numeric value. Next, disable the HSECK9 license for which SLAC is installed. Lastly, save configuration changes and reload the device for the status of the HSECK9 license to be displayed as NOT IN USE.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
```

```
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
  T0    T0(up to 15 mbps) bidirectional thput
  T1    T1(up to 100 mbps) bidirectional thput
  T2    T2(up to 2 gbps) aggregate thput
  T3    T3(up to 5 gbps) aggregate thput
Device(config)# platform hardware throughput crypto 10M

Device(config)# no license feature hseck9
% use 'write' command to disable 'hseck9' license on next boot
Device(config)# end
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
*Jan 31 05:13:22.556: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
 config file
*Jan 31 05:13:22.563: %CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE: Setting crypto bidir
throughput to: 10000 kbps

Device# reload
Proceed with reload? [confirm]
.
.
.
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Jan 29 07:10:00 2023 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag     Count Status
  -----------------------------------------------------------
  network-advantage_10M   (ESR_P_10M_A)           1 IN USE
  dna-advantage_10M       (DNA_P_10M_A)           1 IN USE
  Router US Export Lic... (DNA_HSEC)              0 NOT IN USE
```

After the above prerequsite is met, perform the remaining steps to remove and return the SLAC as show in the procedure below.

- On Catalyst 8000V Edge Software, (including Cisco Cloud Services Router 1000v and Cisco Integrated Services Virtual Routers where the .bin image is upgraded to a Catalyst 8000V software image), first configure the throughput to lesser than 250 Mbps. This can be a tier-based value or a numeric value. You do not have to reload the device for the changes to take effect.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# platform hardware throughput level MB ?
  100    Mbps
  1000   Mbps
  10000  Mbps
  15     Mbps
  25     Mbps
  250    Mbps
  2500   Mbps
  50     Mbps
  500    Mbps
  5000   Mbps
  T0     Tier0(up to 15M throughput)
  T1     Tier1(up to 100M throughput)
  T2     Tier2(up to 1G throughput)
```

```
  T3      Tier3(up to 10G throughput)
  T4      Tier4(unthrottled)

Device(config)# platform hardware throughput level MB T1
The current throughput level is 100000 kb/s
Device(config)# end
```

After the above prerequsite is met, perform the remaining steps to remove and return the SLAC as show in the procedure below.

- On Catalyst 8500 Edge Platforms, you cannot disable the HSECK9 license yourself. To return a SLAC, you must open a case instead. Go to Support Case Manager. Click **Open New Case** and select **Software Licensing**. Select the applicable category and click **Open Case**. Ensure that you provide the Smart Account, Virtual Account, device UDI information in the case. The licensing team will contact you to start the process or for any additional information.

  The steps in the procedure below do not apply to this platform.

- To return *an SLR authorization code*, complete the procedure below. The steps are the same regardless of whether the SLR authorization code includes an HSECK9 license or not.
- To return *a PAK*, see: Removing a PAK License, on page 59.
- To return *a PLR authorization code*, see: Deactivating a PLR, on page 66.

Procedure

	Command or Action	Purpose

Step 1	**license smart authorization return** {**all** | **local**} {**offline** [*path*] | **online**}
	Example:
	`Device# license smart authorization return local online`
	
	`OR`
	
	`Device# license smart authorization return local offline`
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C8300-1N1S-4T2X,SN:FDO2349A00R`
	`Return code: CrMfaJ-9odPW7-gr2DzP-t3srpf-ATqzGS-wGF3c6-U3Kg77-GdiABx-gud`
	`*Jan 31 05:18:00.804: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has been removed from PID:C8300-1N1S-4T2X,SN:FDO2349A00R.`
	
	`OR`
	
	`Device# license smart authorization return local 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 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, 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, enter **offline**.
		If you choose the offline option, you must complete the additional step of submitting this to CSSM.

	Command or Action	Purpose
		• Copy the return code from the CLI or from a saved file and enter it in CSSM: Entering a Return Code in CSSM and Removing the Product Instance, on page 46. For software versions prior to 17.7.1a, you can use only this procedure to return the code. • Specify a path to save the file and upload the file to CSSM. This procedure to return the code is available starting with 17.7.1a: Uploading Data or Requests to CSSM and Downloading a File, on page 50. The file format can be any readable format. For example: `Device# license smart authorization return local offline bootflash:return-code.txt`. **Note** In case of an SSM On-Prem Deployment, use only the **online** option; the **offline** option is not supported.

Step 2	**show license all**
	Example:
	`Device# show license all`
	`.`
	`.`
	`.`
	`License Authorizations`
	`==========`
	`Overall status:`
	`Active:`
	`PID:C8300-1N1S-4T2X,SN:FDO2349A00R`
	`Status: NOT INSTALLED`
	`Last return code:`
	`CrMfaJ-9odPW7-gr2DzP-t3srpf-ATqzGS-wGF3c6-U3Kg77-GdiABx-gud`
	`.`
	`.`
	`.`
		Displays licensing information. Check the `License Authorizations` header in the output. If the return process is completed correctly, the `Last return code:` field displays the return code.

Step 3	**show license summary**
	Example:
	`Device# show license summary`
	`Account Information:`
	`Smart Account: Eg-SA As of Jan 31 05:31:20 2023 UTC`
	`Virtual Account: Eg-VA`
		Displays all the licenses available on the product instance. In the accompanying example, the HSECK9 license is no longer displayed.

	Command or Action	Purpose
	License Usage: License Tag Count Status Entitlement network-advantage_10M (ESR_P_10M_A) 1 IN USE dna-advantage_10M (DNA_P_10M_A) 1 IN USE	

Returning SLAC for an HSECK9 License That Is In-Use

To return an HSECK9 license that is being used (license status is IN-USE), you have to initiate a forced return of the Smart Licensing Authorization Code (SLAC).

Note Returning an HSECK9 license, throttles throughput on the device to 250 Mbps.

Before you begin

Supported topologies: all

The forced return option for SLAC is available only on these devices: Catalyst 8000V Edge Software, Catalyst 8200 Series Edge Platforms, Catalyst 8300 Series Edge Platforms, and Cisco 1000 Series Integrated Services Routers.

This option is not available on Catalyst 8500 Series Edge Platforms. This option is also not available on devices that do not support the HSECK9 license.

Follow these steps to initiate a forced return:

Procedure

	Command or Action	Purpose

Step 1	**license smart authorization return force-reload**
	Example:
	`Device# license smart authorization return force-reload`
	`Attention!!! This command will forcibly remove HSECK9 authorization code. Device will reload automatically if you continue.`
	`Do you want to continue? [yes/no]:yes`
		Forces the the device to return the SLAC. A return code is displayed after you enter this command.
		Note
		On a Catalyst 8000V Edge device the keyword is **force**. This is because a reload is not required on virtual platforms.

Step 2	Check that the return process is completed	• If the device has connectivity to the internet and Cisco SSM:

	Command or Action	Purpose

		For virtual platforms, the return code is automatically updated in Cisco SSM, and the device does not reload.
		
		For physical platforms, after reload is complete and connectivity is restored, the return code is automatically updated in Cisco SSM.
		
		Verify the return by accessing the coressponding Smart Account and Virtual Account in Cisco SSM.
		
		• If the device is offline and has no connectivity to the internet, then you must manually copy and enter the return code in Cisco SSM, to complete the return process. See Entering a Return Code in CSSM and Removing the Product Instance, on page 46.
		
		You can find the code in the output of the **show license authorization** privileged EXEC command.
		
		`Device# show license authorization`
		`Overall status:`
		`  Active:`
		`PID:C8300-1N1S-4T2X,SN:FDO2349A00R`
		`  Status: NOT INSTALLED`
		`  Last return code:`
		`CtMfaJ-9odRW7-gr2DzP-t3srpf-AKpqGS-wGF3c6-U3Kg77-GdiABx-gud`
		`<output truncated>`
		
		Once the SLAC return process is complete, the HSECK9 license is automatically returned to the license pool in Cisco SSM and throughput on the device is throttled to 250 Mbps.

Entering a Return Code in CSSM and Removing the Product Instance

If you return an authorization code by configuring configured **license smart authorization return** {**all** | **local**} **offline**, you must manully enter the return code in CSSM, to complete the return process.

You can use this procedure for all authorization codes (SLAC, SLR, PLR, etc.)

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose your virtual account.

Step 4 Click the **Product Instances** tab.

The list of product instances that are available is displayed.

Step 5 Locate the required product instance from the product instances list. Optionally, you can enter a name or product type string in the search tab to locate the product instance.

Step 6 In the **Actions** column of the product instance, from the Actions dropdown list, select **Remove**.

The **Remove Reservation** window is displayed.

Step 7 In the **Reservation Return Code** field, enter the return code.

The license is returned to the license pool. The Remove Reservation window is automatically closed and you return to the Product Instances tab.

Note
If you want to only return the license, your task ends here. If you also want to remove the product instance from CSSM, continue to the next step.

Step 8 In the **Actions** column of the product instance, from the Actions dropdown list, *again* select **Remove**.

The **Confirm Remove Product** Instance window is displayed.

Step 9 Click **Remove Product Instance**.

The product instance is removed from CSSM and no longer consumes any licenses.

Generating a New Token for a Trust Code from CSSM

To generate a token to request a trust code, complete the following steps.

Generate one token for each *Virtual Account* you have. You can use same token for all the product instances that are part of one Virtual Account.

Before you begin

Supported topologies: Connected Directly to CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose the required virtual account

Step 4 Click the **General** tab.

Step 5 Click **New Token**. The **Create Registration Token** window is displayed.

Step 6 In the **Description** field, enter the token description

Step 7 In the **Expire After** field, enter the number of days the token must be active.

Step 8 (Optional) **In the Max. Number of Uses** field, enter the maximum number of uses allowed after which the token expires.

Note
If you enter a value here, ensure that you stagger the installation of the trust code during the next part of the process. If you want to simultaneously install the trust code on a large number of product instances, we recommend that you leave this field blank. Entering a limit here and simultaneously installing it on a large number of devices causes a bottleneck in the processing of these requests in CSSM and installation on some devices may fail, with the following error: `Failure Reason: Server error occurred: LS_LICENGINE_FAIL_TO_CONNECT`.

Step 9 Click **Create Token**.

Step 10 You will see your new token in the list. Click **Actions** and download the token as a `.txt` file.

Establishing Trust with an ID Token

To establish a trusted connection with CSSM, complete the following steps:

Before you begin

Supported topologies: Connected Directly to CSSM

Before you peform this task, ensure that you have generated and downloaded an ID token file from CSSM: Generating a New Token for a Trust Code from CSSM, on page 47.

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	**license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] **Example:** `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	Submits the trust request and establishes a trusted connection with CSSM. For *id_token_value*, enter the token you generated in CSSM. Enter one of following options: • **local**: Submits the trust request only for the active device in a High Availability set-up. This is the default option. • **all**: Submits the trust request for all devices in a High Availability set-up. Enter the **force** keyword to submit a trust code request despite an existing trust code on the product instance. Trust codes are node-locked to the UDI of the product instance. If a UDI already has a trust code (a trusted connection with CSSM), CSSM does not allow a new trust code for same UDI. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one already exists.

Step 3	**show license status**
	Example:
	`<output truncated>`
	`Trust Code Installed:`
	`  Active: PID:C9500-24Y4C,SN:CAT2344L4GH`
	`    INSTALLED on Sep 04 01:01:46 2020 EDT`
	`  Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ`
	`    INSTALLED on Sep 04 01:01:46 2020 EDT`
		Displays date and time if trust code is installed. Date and time are in the local time zone. See field `Trust Code Installed:`.

Downloading a Policy File from CSSM

If you have requested a custom policy or if you want to apply a policy that is different from the default that is applied to the product instance, complete the following task:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Follow this directory path: **Reports** > **Reporting Policy**.

Step 3 Click **Download**, to save the `.xml` policy file.

You can now install the file on the product instance. See Installing a File on the Product Instance, on page 51

Uploading Data or Requests to CSSM and Downloading a File

You can use this task to:

- To upload a RUM report to CSSM and download an ACK.
- To upload a SLAC request file and download a SLAC code file.

  This method is supported starting with Cisco IOS XE Cupertino 17.7.1a
- To upload a SLAC return file.

  This method is supported starting with Cisco IOS XE Cupertino 17.7.1a

To upload a file to CSSM and download file when the product instance is not connected to CSSM or when CSLU or SSM On-Prem are not connect to CSSM, complete the following task:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM
- SSM On-Prem Deployment (Product instance-initiated communication and SSM On-Prem-initiated communication)

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Select the **Smart Account** (upper left-hand corner of the screen) that will receive the report.

Step 3 Select **Smart Software Licensing** → **Reports** → **Usage Data Files**.

Step 4 Click **Upload Usage Data**. Browse to the file location (RUM report in tar format), select, and click **Upload Data**.

Upload a RUM report (`.tar` format), or a SLAC request file (`.txt` format), or a SLAC return request file (`.txt` format).

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

Step 5 From the Select Virtual Accounts pop-up, select the **Virtual Account** that will receive the uploaded file. The file is uploaded to Cisco and is listed in the Usage Data Files table in the Reports screen showing the File Name, time is was Reported, which Virtual Account it was uploaded to, the Reporting Status, Number of Product Instances reported, and the Acknowledgement status.

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

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

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

Installing a File on the Product Instance

To install a SLAC, or policy, or ACK on the product instance, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

You must have the corresponding file saved in a location that is accessible to the product instance.

- For a SLAC, see Generating and Downloading SLAC from CSSM to a File, on page 35 or Uploading Data or Requests to CSSM and Downloading a File, on page 50 (There are multiple ways to obtain a SLAC file in an air-gapped network).
- For a policy, see Downloading a Policy File from CSSM, on page 49.
- For an ACK, see Uploading Data or Requests to CSSM and Downloading a File, on page 50.

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	**copy** *source* **bootflash:***file-name* **Example:** `Device# copy tftp://10.8.0.6/user01/example.txt bootflash:`	Copies the file from its source location or directory to the flash memory of the product instance. • *source*: This is the location of the source file or directory to be copied. The source can be either local or remote • **bootflash:**: This is the destination for boot flash memory.
Step 3	**license smart import bootflash:** *file-name* **Example:** `Device# license smart import bootflash:example.txt`	Imports and installs the file on the product instance. After installation, a system message displayed - this indicates the type of file you just installed. For a SLAC, the product instance ensures that this new file correctly accounts for all the licenses in-use. On successful installation, the new code replaces any existing code.
Step 4	**show license all** **Example:** `Device# show license all`	Displays license authorization, policy and reporting information for the product instance.

Setting the Transport Type, URL, and Reporting Interval

To configure the mode of transport for a product instance, complete the following task:

Before you begin

Supported topologies: all

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`	

	Command or Action	Purpose
Step 3	**license smart transport** {**automatic** | **callhome** | **cslu** | **off** | **smart**} **Example:** `Device(config)# license smart transport cslu`	Selects the type of message transport the product instance will use. Choose from the following options: • **automatic**: Sets the transport mode to default, which is CSLU. • **callhome**: Enables Call Home as the transport mode. • **cslu**: This is the default transport mode. Enter this keyword if you are using CSLU *or* SSM On-Prem, with product instance-initiated communication. **Note** The same transport mode applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu_or_on-prem_url* in the next step. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport. **Note** If you are changing the transport method from **callhome** to **smart** you do not have to disable the call-home profile "CiscoTAC-1" for Smart Licensing Using Policy to work as expected.
Step 4	**license smart url** {*url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *smart_url*} **Example:** `Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi`	Sets the URL that is used for the configured transport mode. Depending on the transort mode you've chosen in the previous step, configure the corresponding URL here: • *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows: `https://tools.cisco.com/its/service/oddce/services/DDCEService` The **no license smart url** *url* command reverts to the default URL. • **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable: • If you are using CSLU, enter the URL as follows:

	Command or Action	Purpose

		`http://<cslu_ip_or_host>:8182/cslu/v1/pi`
		
		For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.
		
		The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`
		
		• If you are using SSM On-Prem, enter the URL as follows:
		
		`http://<ip>/cslu/v1/pi/<tenant ID>`
		
		For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.
		
		Tip
		You can retrieve the entire URL from SSM On-Prem. See Retrieving the Transport URL (SSM On-Prem UI), on page 25
		
		The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`
		
		• **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.
		
		If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically (`https://cslu-local:8182/cslu/v1/pi`).
		
		If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`).

	Command or Action	Purpose
		• **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows: `https://smartreceiver.cisco.com/licservice/license` When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required. The **no license smart url smart***smart_url* command reverts to the default URL. • **utility** *smart_url*: Although available on the CLI, this option is not supported.
Step 5	**license smart usage interval** *interval_in_days* **Example:** `Device(config)# license smart usage interval 40`	(Optional) Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650. If you are using the utility mode, we recommend a reporting interval of seven days or less. This ensures that the 30- day ACK requirement, which applies to a product instance in the utility mode, is met in timely manner. If you do not configure an interval, the reporting interval is determined entirely by the policy.

Enabling the Utility Mode

You must enable this mode on the product instance for all supported topologies - only if you have an MSLA.

Before you begin

Supported topologies:

- Connected Directly to CSSM
- Connected to CSSM Through CSLU, CSLU Disconnected from CSSM (Product Instance-Initiated and CSLU-Initiated Communication)
- SSM On-Prem Deployment (Product Instance-Initiated and SSM On-Prem-Initiated Communication)
- 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	**configure terminal** **Example:** `Device# configure terminal`	
Step 3	**license smart utility** **Example:** `Device (config)# license smart utility`	Enables the utility mode on the product instance to indicate that an MSLA will be used. Enabling it causes the following to occur: • The system checks the transport type and URL. The %SMART_LIC-4-UTILITY_TRANSPORT_NOT_CONFIG system message is displayed if this settings is not configured correctly. • RUM reports include a flag to indicate that the product instance is in the utility mode. When utility mode is first enabled, the RUM report has the utility flag set. If a subscription exists in the Smart Account and Virtual Account, the subscription IDs are returned in the RUM ACK. Subsequent RUM reports include the subscription IDs. The subscription IDs are also returned in every RUM ACK. The %SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE message is displayed if the utility mode is enabled and a license without a subscription ID is being used on the product instance. • A policy that is specific to the utility mode is set on the product instance. The utility policy states that a RUM ACK must be installed every 30 days. The %SMART_LIC-4-UTILITY_NO_ACK system message is displayed if an ACK is past due.

	Command or Action	Purpose
		• An informational message, %SMART_LIC-3-UTILITY_STARTED is displayed; it indicates that the utility mode is enabled and a subscription ID is available.
Step 4	**exit** **Example:** `Device (config)# exit`	Exits the global configuration mode and returns to the privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Continue Using a PAK License

If you have a PAK license and you want to continue using it on the product instance, complete the following steps:

Note This procedure is applicable to all licenses that are PAK-fufilled - including HSECK9.

Before you begin

Supported topologies: all

Procedure

Step 1 Upgrade the software version on the product instance to a release where the system takes a snapshot of the PAK license.

For the system to take snapshot of the PAK license, you must upgrade to one of the following releases:

- Cisco IOS XE Amsterdam 17.3.5 and later releases of the 17.3.x train.
- Cisco IOS XE Bengaluru 17.6.2 and later releases of the 17.6.x train.
- Cisco IOS XE Cupertino 17.7.1 and later releases of the 17.7.x train, and all releases of subsequent trains, that is, Cisco IOS XE Cupertino 17.8.x, Cisco IOS XE Cupertino 17.9.x, and until Cisco IOS XE Dublin 17.10.x.

For upgrade information, see:

Product Series	Supports PAK ?	Link to Upgrade Information
Cisco 1000 Series Integrated Services Routers	Yes	How to Install and Upgrade the Software
Cisco 4000 Series Integrated Services Routers	Yes	How to Install and Upgrade the Software
Cisco ASR 1000 Series Aggregation Services Routers	Yes	Software Upgrade Processes Supported by Cisco ASR 1000 Series Routers
Cisco Cloud Services Router 1000v	Yes	Upgrading the Cisco IOS XE Software
Catalyst 8000V Edge Software	Yes - but, only in case of a .bin upgrade from a CSR1000v to Catalyst 8000V Edge Software	Upgrading the Cisco IOS XE Software

After upgrade, enter the **show platform software sl-infra pak-info** command in privileged EXEC mode to display and verify that a snapshot has been taken.

Step 2 Verify that DLC is completed.

The system triggers the DLC. After DLC, the PAK-fulfilled license is available in your Smart Account. On the product instance, enter the **show license all** command to verify that it continues to be *identified* as a PAK-fulfilled license. For example, an HSECK9 PAK that has been snapshotted, continues to be displayed with `Status:PAK`.

The DLC process is triggered automatically on the product instance when you upgrade to a release that supports Smart Licensing Using Policy. DLC data is collected one hour after the product instance is upgraded to a software version that supports Smart Licensing Using Policy.

The DLC process is completed after an ACK is installed on the product instance. (The ACK is available once usage synchronization is completed - this is the next step.)

```
Device# show platform software license dlc

<output truncated>

DLC Process Status: Completed

DLC Conversion Status: SUCCESS
```

Step 3 Synchronize license usage with CSSM.

Follow the method that applies to the topology you have implemented and ensure that a RUM report is sent to CSSM.

Results:

- A snaphot of the PAK license is available and continues to be honored even after the PAK-managing library is discontinued.

- The license count is deposited in the Smart Account and Virtual Account in CSSM.
- Usage of the license is reported to CSSM.

Removing a PAK License

If you have a PAK license on a product instance and you want to remove the license, complete the following steps:

Note This procedure is applicable to all licenses that are PAK-fufilled - including HSECK9.

After you have completed this task, multiple options are available with respect to what you can do with the device and the license that is returned to the license pool in CSSM. These are described in the "**Results**" section at the end of the task.

Before you begin

Supported topologies: all

Procedure

Step 1 Verify that DLC is completed.

The system triggers the DLC. After DLC, the PAK-fulfilled license is available in your Smart Account. On the product instance, enter the **show license all** command to verify that it continues to be *identified* as a PAK-fulfilled license. For example, an HSECK9 PAK, continues to be displayed with `Status:PAK`.

The DLC process is triggered automatically on the product instance when you upgrade to a release that supports Smart Licensing Using Policy. DLC data is collected one hour after the product instance is upgraded to a software version that supports Smart Licensing Using Policy.

The DLC process is completed after an ACK is installed on the product instance. (The ACK is available once usage synchronization is completed - this is the next step.)

```
Device# show platform software license dlc

<output truncated>

DLC Process Status: Completed

DLC Conversion Status: SUCCESS
```

Step 2 Perform factory reset

Depending on your product instance, refer to the corresponding link:

Product Series	Link to Factory Reset Information
Cisco 1000 Series Integrated Services Routers	Using the factory reset Commands
Cisco 4000 Series Integrated Services Routers	Factory Reset

Product Series	Link to Factory Reset Information
Cisco ASR 1000 Series Aggregation Services Routers	Factory Reset
Cisco Cloud Services Router 1000v	Performing a Factory Reset
Catalyst 8000V Edge Software	Performing a Factory Reset

Step 3 Reload the product instance if the PAK license included an HSECK9 license.

This step is not required if the PAK license did not include an HSECK9 license.

After you have performed factory reset in the previous step, this reload enables the device to come-up without the HSECK9 license.

Step 4 Synchronize license usage with CSSM

Follow the method that applies to the topology you have implemented and ensure that a RUM report is sent to CSSM. Sending the RUM report accomplishes the following:

- Notifies CSSM that no licenses are being consumed on the product instance.
- The PAK-fulfilled license is returned to the license pool in CSSM and is *available* as a Smart license. For example, if what you had was a "PAK-fulfilled securityk9" license, it is now available for use as a "securityk9" license.

Results:

You now have the following options:

- Use the PAK-fulfilled license, on *the same* product instance, as a regular Smart license.

  To use the license on the product instance, configure the license using the applicable commands. Reporting requirements for the license will be the same as any other license - as per the policy, or, if system messages indicate that it is.

- Use the PAK-fulfilled license, on *another* product instance, as a regular Smart license.

  To use the license on another product instance, configure the license using the applicable commands for that product instance. Reporting requirements for the license will be the same as any other license - as per the policy, or, if system messages indicate that it is.

- Continue using the product instance.
- Remove the product instance from CSSM if you want to decommission the product instance or perform a Return Material Authrization (RMA).

Removing a PAK License on a Failed Product Instance

This task shows you how to return a PAK license on a product instance, which is not working at all (you cannot access the console to configure any Cisco IOS commands).

To return a PAK license on a failed product instance, you must open a case. Go to Support Case Manager. Click **OPEN NEW CASE** > Select **Software Licensing**.

After you have opened a case, the support team will contact you to initiate the return process and remove the product instance from CSSM.

Activating a PLR

To activate PLR on a supporting product instance, complete the following steps:

Some of the steps in this procedure must be performed on the product instance and some of them, on the CSSM Web UI. Steps that must be performed on the CSSM Web UI are prefixed with "(CSSM)" to avoid confusion. All other steps must be performed on the product instance.

Before you begin

- Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts in CSSM.
- Ensure that your Smart Account is enabled for PLR.

  To check if it is enabled, login to CSSM https://software.cisco.com, and click **Manage licenses**. Click the **Inventory** tab. Select your Virtual Account. Click the **Licenses** tab. If the **License Reservation** button is enabled, then your Smart account is enabled for PLR. If it is greyed-out or not available, open a case in Support Case Manager (SCM).
- Ensure that the software version running on the product instance is Cisco IOS XE Dublin 17.10.1a or later. Enter the **show version** command in privileged EXEC mode, to confirm.

Procedure

Step 1 **configure terminal**

Example:

```
Device#configure terminal
```

Enters the global configuration mode.

Step 2 **license smart reservation**

Example:

```
Device(config)# license smart reservation
```

Enables the reservation mode.

Step 3 **exit**

Example:

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

Exits the global configuration mode and enters the privileged EXEC mode.

Step 4 **license smart reservation request local**

Example:

```
Device# license smart reservation request local
Enter this request code in the Cisco Smart Software Manager portal:
UDI: PID:C8000V,SN:96QKIABBZ1H
Request code: DB-ZC8000V:96QKIABBZ1H-AYk3ndtp6-F1
```

Generates a reservation request code on the product instance.

You have to paste this in the CSSM Web UI, in a later step. You can save it in a .txt or other accessible file.

Step 5 (CSSM) Go to https://software.cisco.com and click **Manage licenses**. Log in using the username and password provided by Cisco.

The **Smart Software Licensing** page is displayed.

Step 6 (CSSM) Click the **Inventory** tab. Select your Virtual Account. Click the **Licenses** tab, and then click the **License Reservation** button.

The system displays the **Smart License Reservation** dialog box.

Tip
If the Smart Account and Virtual Account are not enabled for PLR, then the **License Reservation** button is not enabled. If this is the case, you must open a support case in Support Case Manager (SCM), to get it enabled.

Step 7 (CSSM) For **Step 1: Enter Request Code**, enter the request code in the **Reservation Request Code** text box. Click **Next**.

Enter the reservation request code that you generated on the product instance in Step 3.

After you click **Next**, the system displays the **Step 2: Select Licenses** dialog box.

Step 8 (CSSM) For **Step 2: Select Licenses**, select **C8000v PLR**. Click **Next**.

After you click **Next**, the system displays a list of licenses for selection.

Step 9 (CSSM) Enter the **Quantity to Reserve** as `1` and leave the **Expires** column blank. Click **Next**.

After you click **Next**, the system displays the **Step 3: Review and Confirm** dialog box.

Step 10 (CSSM) In the **Step 3: Review and Confirm** dialog box, click the **Generate Authorization Code** button.

After you click the **Generate Authorization Code**button, the system displays the **Step 4: Authorization Code** dialog box.

Step 11 (CSSM) In the **Step 4: Authorization Code** dialog box, either click **Copy to Clipboard** or **Download as File**. Click **Close**.

Copies the PLR authorization code to clipboard or downloads it as a file.

If you download it to a file, you must transfer the saved file to a flash drive or network resource (for example, a TFTP server), because you must install it on the product instance in the next step.

Step 12 **license smart reservation install** *PLR-Code*

Example:

```
Device# license smart reservation install
DA3Ks9-WM4yzT-Y7UAbh-GGXUwr-qARDsq-sjJs9e-Z3Xqix-TKcsy9-z6
Reservation install successful
```

Installs Version 3 of the PLR code and displays a success message.

Tip

Version 3 of the PLR code always starts with the letter “D” and is 58 characters long.

Step 13 **show license reservation**

Example:

```
Device# show license reservation
License reservation: ENABLED
Overall status:
   Active: PID:C8000V,SN:96QKIABBZ1H
   Reservation status: UNIVERSAL INSTALLED on Oct 25 17:50:48 2022 UTC
```

Displays license reservation information.

When a PLR code is installed on the product instance, the reservation status in the output of this command displays `UNIVERSAL INSTALLED`.

Step 14 **configure terminal**

Example:

```
Device# configure terminal
```

Enters the global configuration mode.

Step 15 **platform hardware throughput level MB** {**100** | **1000** | **10000** | **15** | **25** | **50** | **250** | **2500** | **50** | **500** | **5000**}

Example:

```
Device(config)# platform hardware throughput level MB 1000
```

Configures the throughput level.

At a minimum, you must have configured a network-stack license already. Otherwise the command is not recognized as a valid one on the command line interface.

Note
If you configure a throughput that is greater than 250 Mbps, you do not have to install SLAC. The PLR code authorizes a throughput of greater than 250 Mbps.

Step 16 **exit**

Example:

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

Exits the global configuration mode and enters the privileged EXEC mode.

Step 17 **show platform hardware throughput level MB**

Example:

```
Device# show platform hardware throughput level MB
The current throughput level is 2000000 kb/s
```

Displays the currently running throughput on the device.

Upgrading a PLR

To upgrade the PLR version code to continue using PLR in the Smart Licensing Using Policy environement, complete the following steps:

Some of the steps in this procedure must be performed on the product instance and some of them, on the CSSM Web UI. Steps that must be performed on the CSSM Web UI are prefixed with "(CSSM)" to avoid confusion. All other steps must be performed on the product instance.

Before you begin

- Supported topologies: Not applicable
- The following settings are assumed because you have an existing, older version of the PLR code:
  - You have a user role with proper access rights to a Smart Account and the required Virtual Accounts in CSSM.
  - Your Smart Account is enabled for PLR.
- Ensure that you have performed a .bin upgrade of the software version on the product instance to Cisco IOS XE Dublin 17.10.1a or later. Enter the **show version** command in privileged EXEC mode, to confirm.



Note If the throughput level on the product instance was greater than 250 Mbps before upgrade, then on upgrade, it is set *to* 250 Mbps. A system message as shown below is also displayed, but you can ignore it. The procedure below shows you how to upgrade the PLR code to Version 3, which automatically restores throughput.

```
%SMART_LIC-6-RESERVE_AUTH_FAILED: Failed to validate the Universal
 Reservation
Authorization Code for udi PID:CSR1000V,SN:9QLBLATKXM4. Changing to
 the unregistered state.
```

Procedure

Step 1 (CSSM) Go to https://software.cisco.com and click **Manage licenses**. Log in using the username and password provided by Cisco.

Logs in to the CSSM Web UI.

Step 2 (CSSM) Click the **Inventory** tab. Select your Virtual Account. Click the **Product Instances** tab.

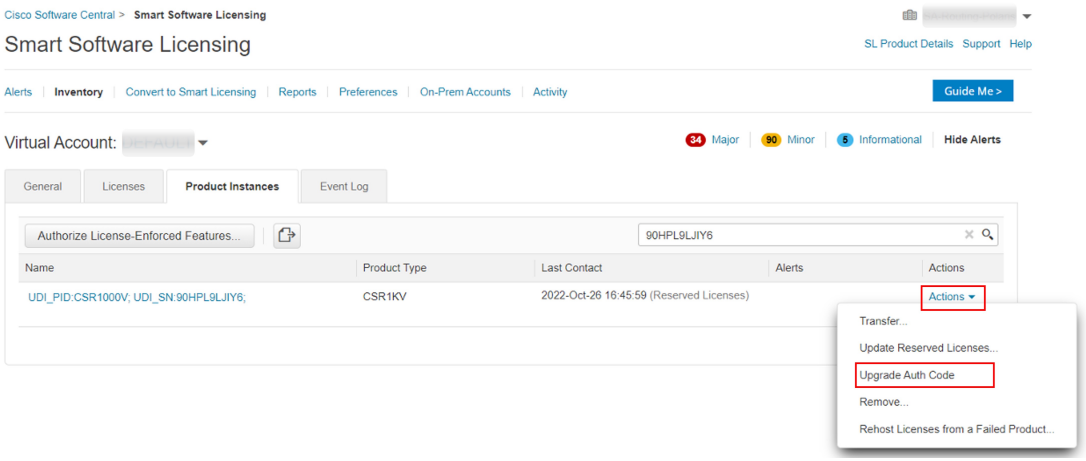
A list of product instances is displayed.

Step 3 (CSSM) Locate the product instance for which you are upgrading the PLR code and click on the corresponding **Actions** dropdown.

A list of available actions is displayed.

Step 4 (CSSM) Select **Upgrade Auth Code**.

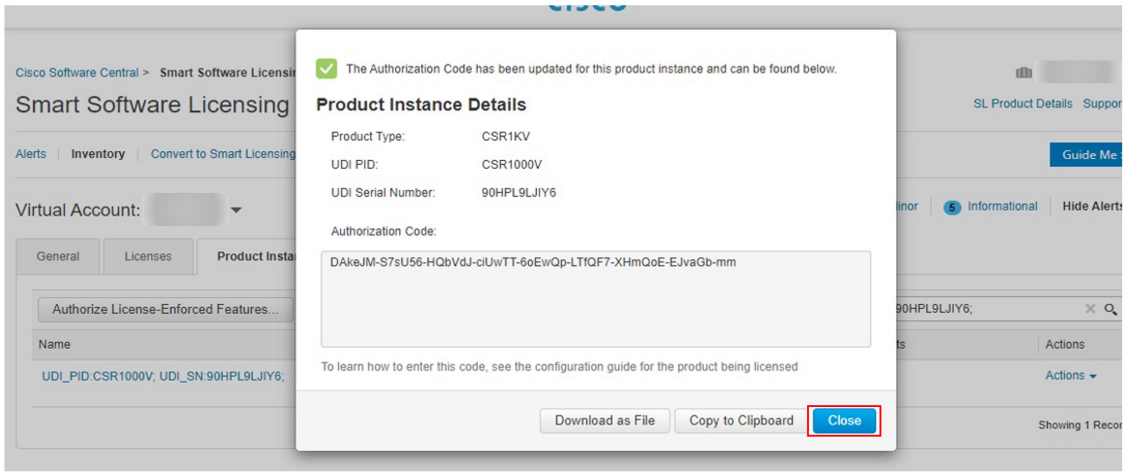
Example:



The **Product Instance Details** pop-up window is displayed.

Step 5 (CSSM) either click **Copy to Clipboard** or **Download as File**. Click **Close**.

Example:



Copies the PLR authorization code to clipboard or downloads it as a file.

If you download it to a file, you must transfer the saved file to a flash drive or network resource (for example, a TFTP server), because you must install it on the product instance in the next step.

Step 6 **license smart reservation install** *PLR-Code*

Example:

```
Device# license smart reservation
DA3Ks9-WM4yzT-Y7UAbh-GGXUwr-qARDsq-sjJs9e-Z3Xqix-TKcsy9-z6

Reservation install successful
```

Installs Version 3 of the PLR code and displays a success message. Any existing older PLR code version is deleted during the process.

If the throughput level on the product instance was greater than 250 Mbps before software version upgrade, the throughput level is now restored.

Tip
Version 3 of the PLR code always starts with the letter “D” and is 58 characters long.

Step 7 **show platform hardware throughput level MB**

Example:

```
Device# show platform hardware throughput level MB
The current throughput level is 2000000 kb/s
```

Displays the currently running throughput on the device.

Step 8 **show license reservation**

Example:

```
Device# show license reservation
License reservation: ENABLED
Overall status:
      Active: PID:CSR1000V,SN:9QLBLATKXM4
      Status: UNIVERSAL INSTALLED on Oct 25 20:54:08 2022 UTC
```

Displays license reservation information.

When a PLR code is installed on the product instance, the reservation status in the output of this command displays `UNIVERSAL INSTALLED`.

Deactivating a PLR

To deactivate PLR on a supporting product instance, complete the following steps:

Some of the steps in this procedure must be performed on the product instance and some of them, on the CSSM Web UI. Steps that must be performed on the CSSM Web UI are prefixed with "(CSSM)" to avoid confusion. All other steps must be performed on the product instance.

Before you begin

Supported topologies: Not applicable

Procedure

Step 1 **license smart reservation return local**

Example:

```
Device# license smart reservation return local
This command will remove the license authorization code.
Some features may not function properly.

Do you want to continue? [yes/no]:
Enter this return code in Cisco Smart Software Manager portal:
```

```
UDI: PID:CSR1000V,SN:9QLBLATKXM4
    Return code: CNcjZD-aGrAPP-SpCkkD-nZtES8-46zCDq-jZP
```

Generates a reservation return request code on the product instance.

You have to paste this in the CSSM Web UI, in a later step. You can save it in a .txt or other accessible file.

Step 2 (CSSM) Go to https://software.cisco.com and click **Manage licenses**. Log in using the username and password provided by Cisco.

Logs in to the CSSM Web UI.

Step 3 (CSSM) Click the **Inventory** tab. Select your Virtual Account. Click the **Product Instances** tab.

A list of product instances is displayed.

Step 4 (CSSM) Locate the product instance for which you are upgrading the PLR code and click on the corresponding **Actions** dropdown.

Step 5 (CSSM) Select **Remove Product Instance**. Paste the return code you generated in Step 1 in the text box. Click **Remove**.

If greater than 250 Mbps throughput was running with PLR, then throughput is set to 250 Mbps. It throughput was less than or equal to 250 Mbps, it remains unchanged.

Step 6 **configure terminal**

Example:

```
Device# configure terminal
```

Enters the global configuration mode.

Step 7 **no license smart reservation**

Example:

```
Device (config)# no license smart reservation
```

Disables the reservation mode.

Step 8 **exit**

Example:

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

Exits the global configuration mode and enters the privileged EXEC mode.

HSECK9 License Mapping Table for Routing Product Instances

When you generate a SLAC in CSSM (Generating and Downloading SLAC from CSSM to a File, on page 35), you must select the correct license name for the PID. This table is provides a ready reference of the PID ↔ license name mapping for Cisco Aggregation, Integrated, and Cloud Service Routers.

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR1K -8P	C1111-8P	ISR_1100_8P_Hsec	Use **ISR_1100_8P_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, If the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses
	C1111-8PLTEEA		
	C1111-8PLTELA		
	C1111-8PWE		
	C1111-8PWB		
	C1111-8PWA		
	C1111-8PWZ		
	C1111-8PWN		
	C1111-8PWQ		
	C1111-8PWC		
	C1111-8PWR		
	C1111-8PWK		
	C1111-8PWS		
	C1111-8PLTEEAWE		
	C1111-8PLTEEAWB		
	C1111-8PLTEEAWA		
	C1111-8PLTEEAWR		
	C1111-8PLTELAWZ		
	C1111-8PLTELAWN		
	C1111-8PLTELAWQ		
	C1111-8PLTELAWC		
	C1111-8PLTELAWK		
	C1111-8PLTELAWD		
	C1111-8PLTELAWA		
	C1111-8PLTELAWE		
	C1111-8PLTELAWS		
	C1116-8P		
	C1116-8PLTEEA		
	C1117-8P		
	C1117-8PM		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
	C1117-8PLTEEA		
	C1117-8PLTELA		
	C1117-8PMLTEEA		
	C1117-8PWE		
	C1117-8PWA		
	C1117-8PWZ		
	C1117-8PMWE		
	C1117-8PLTEEAWE		
	C1117-8PLTELAWE		
	C1117-8PLTELAWZ		
	C1111X-8P		
	C1112-8P		
	C1112-8PLTEEA		
	C1113-8P		
	C1113-8PM		
	C1113-8PLTEEA		
	C1113-8PLTELA		
	C1113-8PMLTEEA		
	C1113-8PWE		
	C1113-8PWA		
	C1113-8PWZ		
	C1113-8PMWE		
	C1113-8PLTEEAWE		
	C1113-8PLTELAWE		
	C1113-8PLTELAWZ		
	C1114-8P		
	C1114-8PLTEEA		
	C1115-8P		
	C1115-8PLTEEA		
	C1115-8PM		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
	C1115-8PMLTEEA		
	C1118-8P		
	C1121-8PLTEPWE		
	C1121-8PLTEPWB		
	C1121-8PLTEPWZ		
	C1121-8PLTEPWQ		
	C1121-8PLTEP		
	C1121X-8PLTEP		
	C1121-8P		
	C1121X-8P		
	C1161-8P		
	C1161X-8P		
	C1161-8PLTEP		
	C1161X-8PLTEP		
	C1126-8PLTEP		
	C1127-8PLTEP		
	C1127-8PMLTEP		
	C1126X-8PLTEP		
	C1127X-8PLTEP		
	C1127X-8PMLTEP		
	C1128-8PLTEP		
	C1121X-8PLTEPWE		
	C1121X-8PLTEPWB		
	C1121X-8PLTEPWZ		
	C1121X-8PLTEPWA		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR1K - 4P	C1111-4P	ISR_1100_4P_Hsec	Use **ISR_1100_4P_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses
	C1111-4PLTEEA		
	C1111-4PLTELA		
	C1111-4PWE		
	C1111-4PWB		
	C1111-4PWA		
	C1111-4PWZ		
	C1111-4PWN		
	C1111-4PWQ		
	C1111-4PWC		
	C1111-4PWR		
	C1111-4PWK		
	C1111-4PWD		
	C1111X-4P		
	C1116-4P		
	C1116-4PLTEEA		
	C1116-4PLTEEAWE		
	C1116-4PWE		
	C1117-4P		
	C1117-4PLTEEA		
	C1117-4PLTELA		
	C1117-4PLTEEAWE		
	C1117-4PLTEEAWA		
	C1117-4PLTELAWZ		
	C1117-4PWE		
	C1117-4PWA		
	C1117-4PWZ		
	C1117-4PM		
	C1117-4PMLTEEA		
	C1117-4PMLTEEAWE		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
	C1117-4PMWE		
	C1101-4P		
	C1101-4PLTEP C1101-4PLTEPWE		
	C1101-4PLTEPWB		
	C1101-4PLTEPWD		
	C1101-4PLTEPWZ		
	C1101-4PLTEPWA		
	C1101-4PLTEPWH		
	C1101-4PLTEPWQ		
	C1101-4PLTEPWR		
	C1101-4PLTEPWN		
	C1101-4PLTEPWF		
	C1109-4PLTE2P		
	C1109-4PLTE2PWB		
	C1109-4PLTE2PWD		
	C1109-4PLTE2PWE		
	C1109-4PLTE2PWZ		
	C1109-4PLTE2PWA		
	C1109-4PLTE2PWH		
	C1109-4PLTE2PWQ		
	C1109-4PLTE2PWR		
	C1109-4PLTE2PWN		
	C1109-4PLTE2PWF		
	C1118-4P		
	C1121-4P		
	C1121-4PLTEP		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR1K-2P	C1109-2PLTEGB	ISR_1100_2P_Hsec	Use **ISR_1100_2P_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses
	C1109-2PLTEUS		
	C1109-2PLTEVZ		
	C1109-2PLTEJN		
	C1109-2PLTEAU		
	C1109-2PLTEIN		
ISR4200	ISR4221/K9	ISR4220_HSEC	Use **ISR4220_HSEC**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses
	ISR4221X/K9		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR4300	ISR4321/K9	ISR_4321_Hsec	Use **ISR_4321_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses
	ISR4331/K9	ISR_4331_Hsec	Use **ISR_4331_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses
	ISR4351/K9	ISR_4531_Hsec	Use **ISR_4531_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR4400	ISR4431/K9	ISR_4400_Hsec	Use **ISR_4400_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses
	ISR4451/K9		
	ISR4451-X/K9		
	ISR4461/K9		
C8300	C8300-1N1S-4T2X	Router US Export Lic for DNA	Router US Export Lic for DNA (No change)
	C8300-1N1S-6T		
	C8300-2N2S-4T2X		
	C8300-2N2S-6T		
	C8300-1N1S-4G2X		
	C8300-1N1S-6G		
	C8300-2N2S-4G2X		
	C8300-2N2S-6G		
C8200	C8200-1N-4T		
	C8200-1N-1G		
ISR1100	ISR1100-6G		
	ISR1100X-6G		
C8500	C8500-12X4QC		
	C8500-12X		
	C8500L-8S4X		
C8000V	C8000V		
CSR1000V	CSR1000V		
ISRV	ISRV		

Converting a Device-Specific HSECK9 License

This task shows you how to convert *unused* device-specific HSECK9 licenses like *ISR_1100_8P_Hsec* or *ISR_4321_Hsec* to *Router US Export Lic for DNA* (DNA_HSEC) license. For the complete list of device-specific

HSECK9 licenses that you can convert, see: HSECK9 License Mapping Table for Routing Product Instances, on page 67.

To perform this task you will require a device from which you can access the internet.

Before you begin

Depending on the number of device-specific HSECK9 licenses you want to convert, order the corresponding number of spare upgrade-license PIDs on Cisco commerce workspace (CCW). Use part number DNA-HSEC-UPGD=. The unit list price for this PID is USD 0.00.

Note Ensure that the correct Smart Account and Virtual Account is mentioned in the order. The account must be the same as the Virtual Account where the device-specific HSECK9 license (which you are going to convert) is deposited.

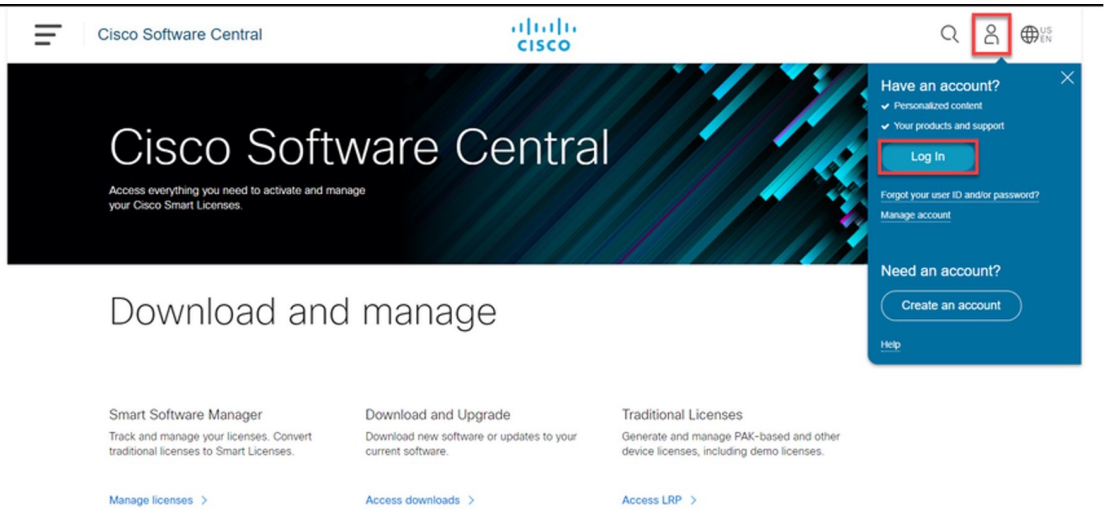
Procedure

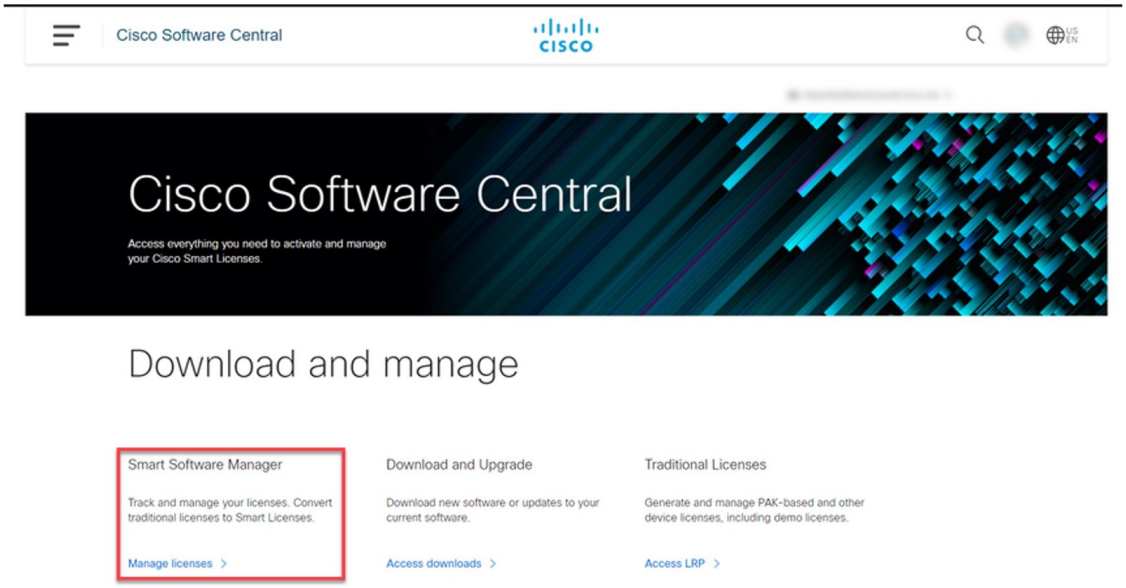
Step 1 Go to https://software.cisco.com and click **Manage licenses**.

Log in by the using username and password provided by Cisco.

The **Smart Software Licensing** page is displayed.

Example:



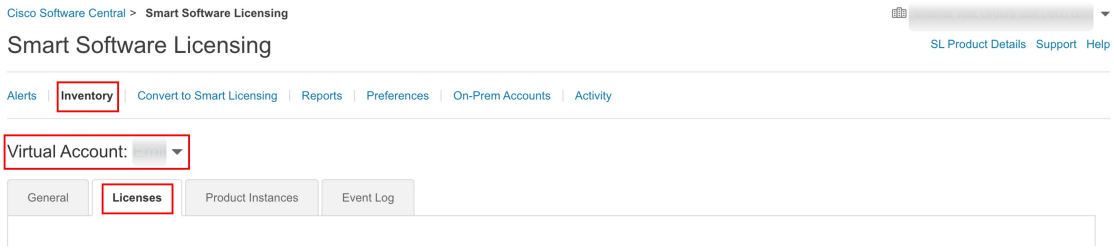


Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose the applicable Virtual Account.

Step 4 Click the **Licenses** tab.

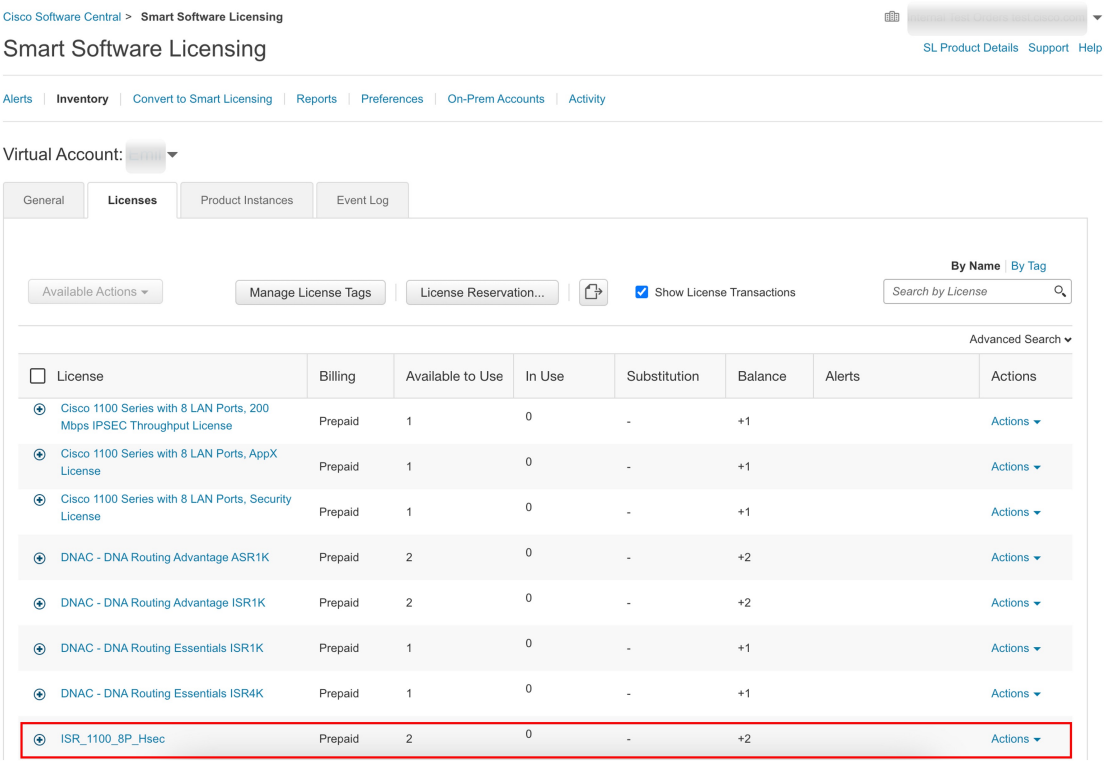
Example:



Step 5 Ensure that the device-specific HSECK9 license and the *Router US Export Lic for DNA* licenses are in this same Virtual Account.

Use the search bar and locate the device-specific HSECK9 license. In the accompanying sample screenshot this is the “ISR_1100_8P_Hsec” HSECK9 license and there are two of them.

Example:

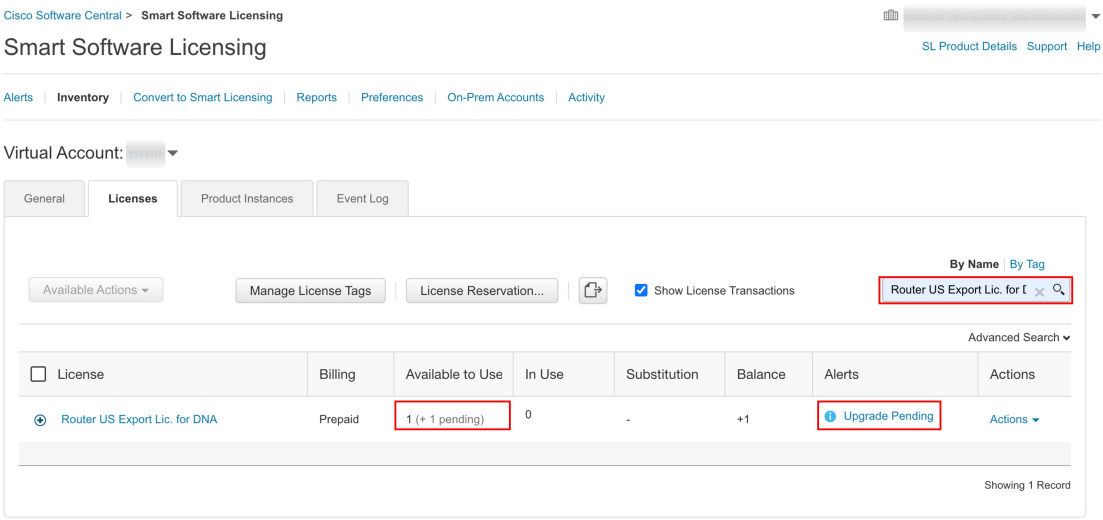


Again use the search bar and locate *Router US Export Lic for DNA*. In the **Alerts** column for this license check that "Upgrade Pending" is displayed. This confirms that you have the correct spare upgrade-license PID. Further, the **Available to Use** column displays the number of PIDs that are pending upgrade, within parentheses. In the accompanying sample screenshot there is one license pending.

step

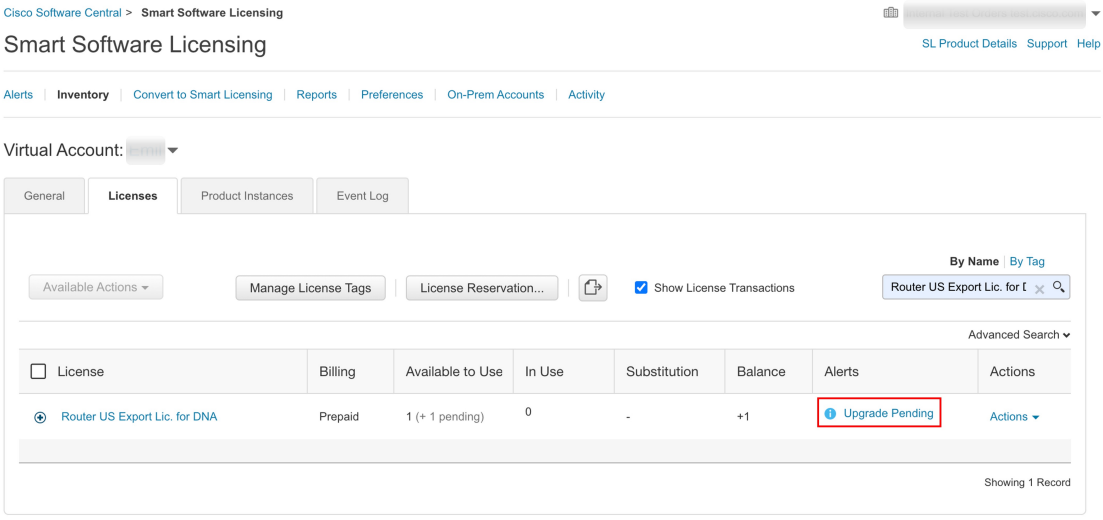
Note
Although there are two device-specific HSECK9 licenses in the sample screenshot, only one of them is converted in this example, because only one upgrade-license PID is available. Also note that if there are different device-specific HSECK9 licenses in your virtual account (for example, ISR_1100_8P_Hsec *and* ISR4220_HSEC) you can choose the one you want to convert to DNA_HSEC.

Example:



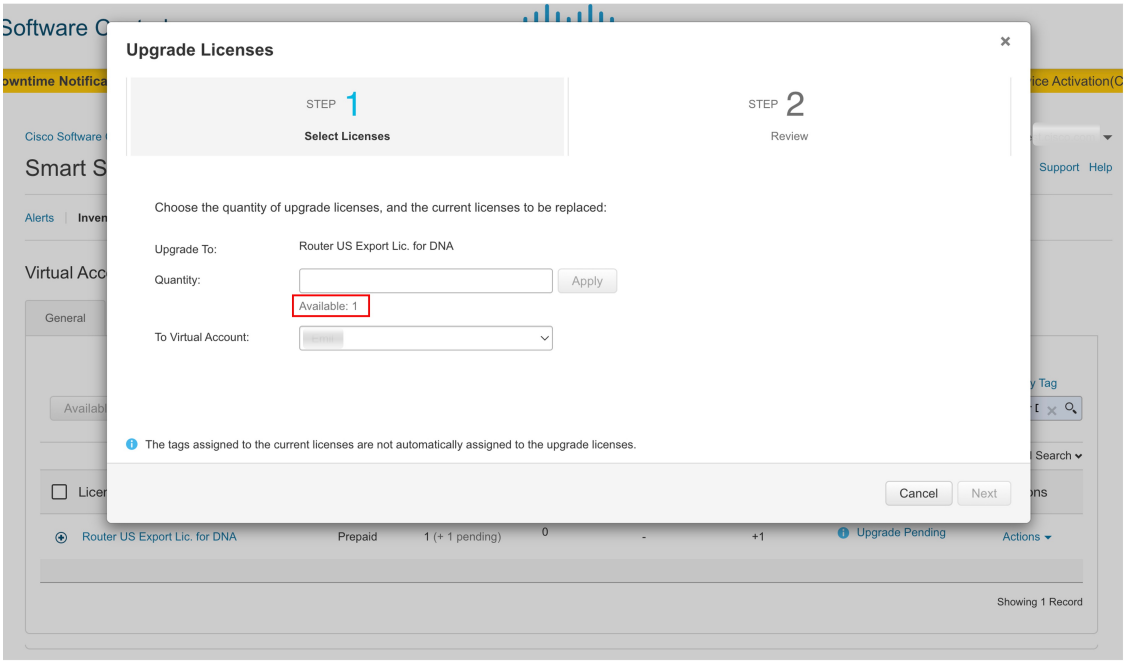
Step 6 Click **Upgrade Pending**.

Example:



The **Upgrade Licences** pop-up window is displayed. Below the *Quantity* field, the number of available upgrade licenses is displayed.

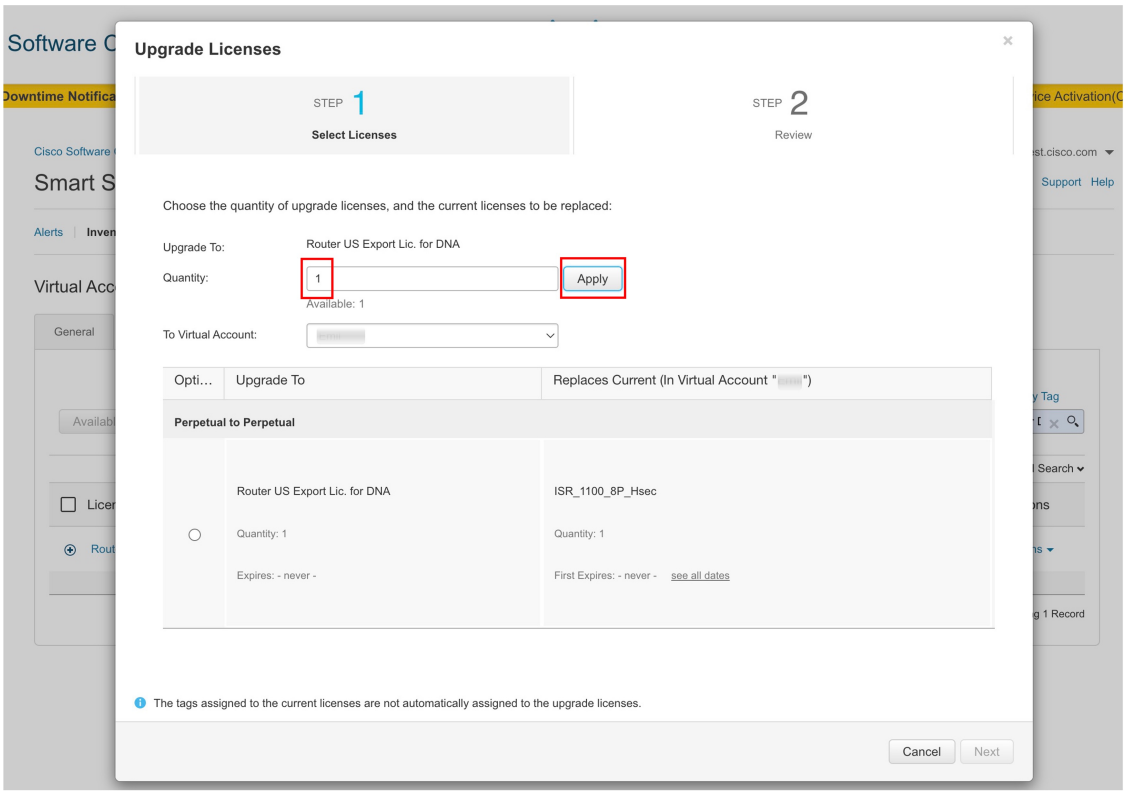
Example:



Step 7 In the **Quantity** field, enter the number of upgrade licenses that you want to convert and then click **Apply**.

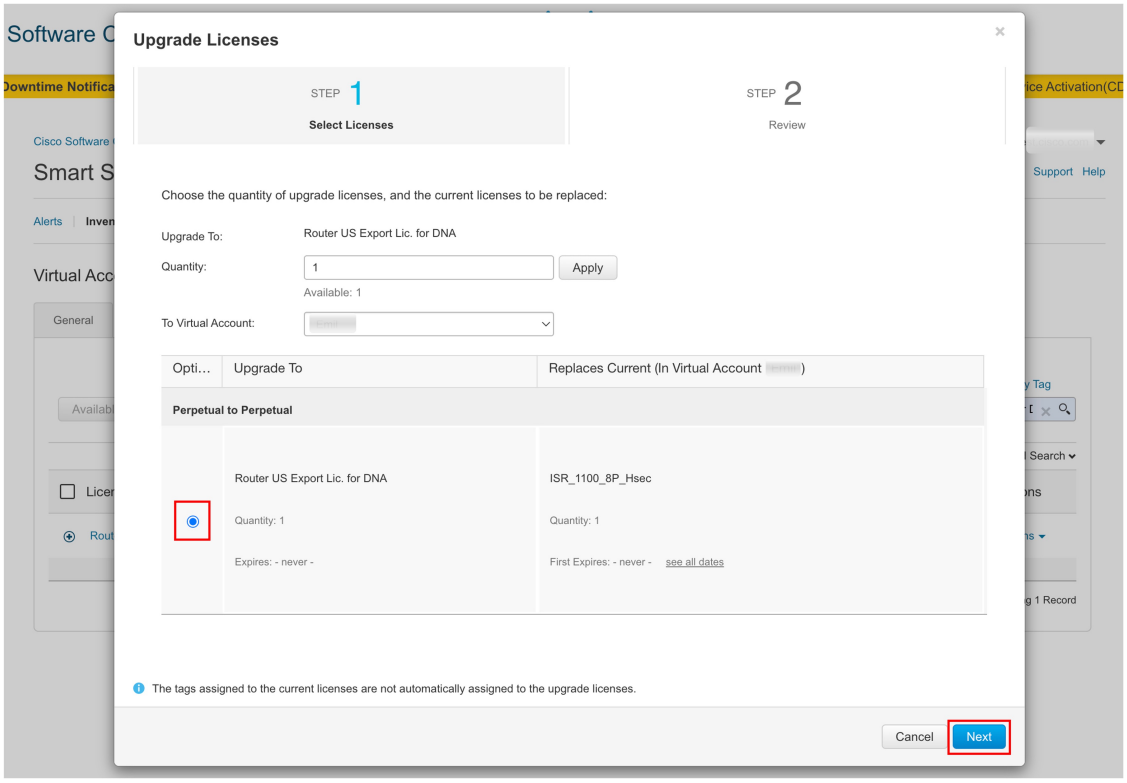
The quantity of *Router US Export Lic for DNA* licenses and number of device-specific HSECK9 licenses that will be replaced are displayed in a table in the same window.

Example:



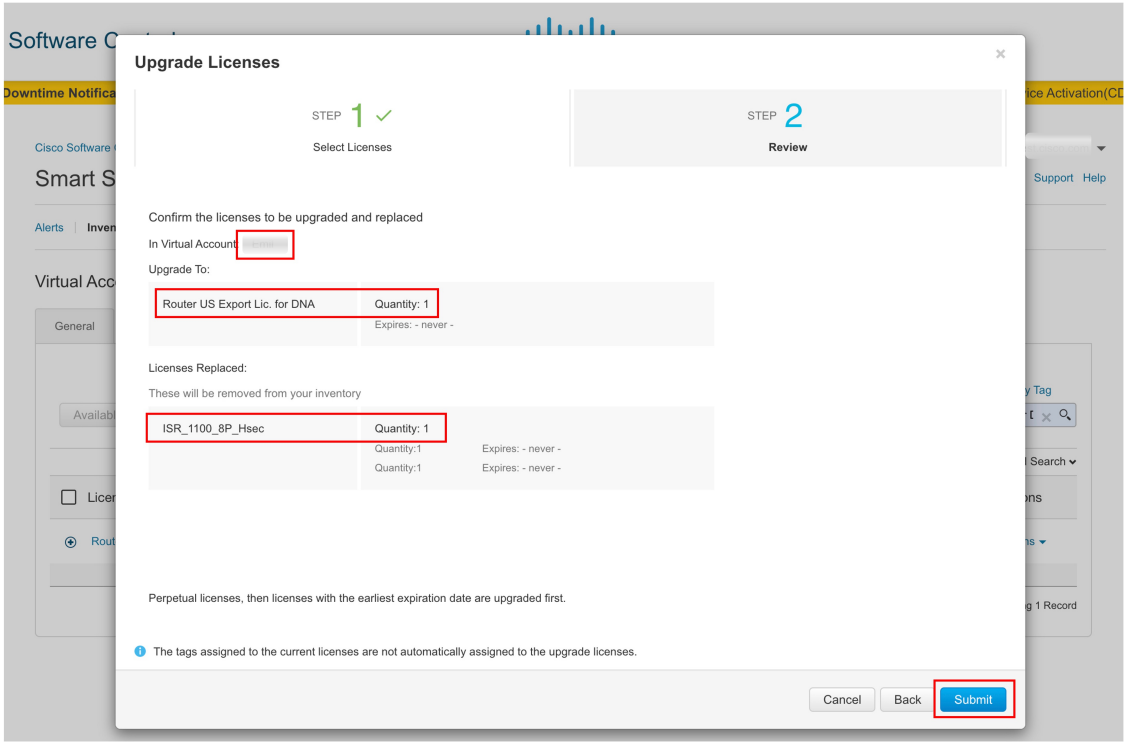
Step 8 Select the radio button and click **Next**.

Example:



Step 9 Review all the information and click **Submit**.

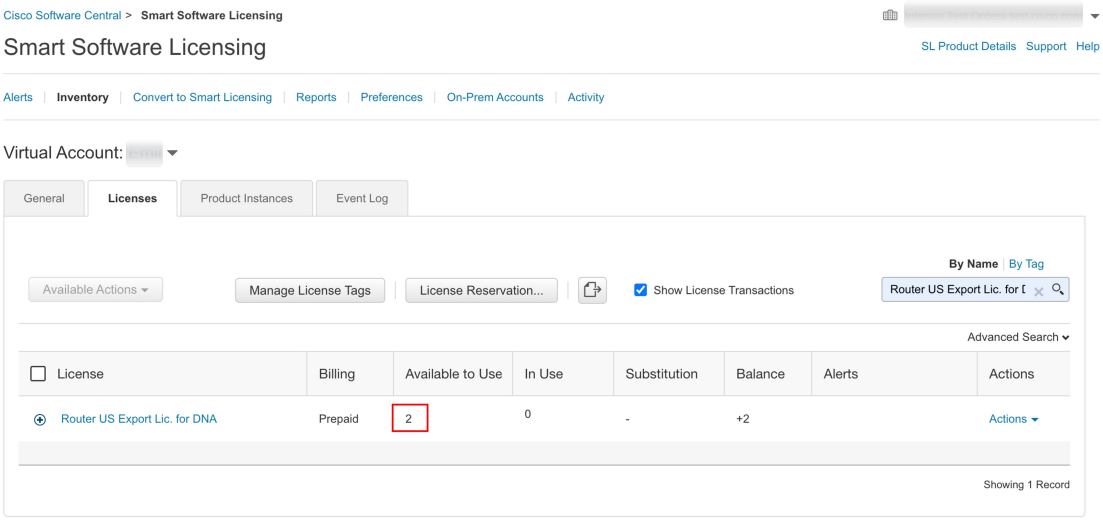
Example:



Step 10 In the **Licenses** tab, again use the search bar and locate *Router US Export Lic for DNA*. Check the **Available to Use** column for an updated count.

In the accompanying sample screenshot the number of *Router US Export Lic for DNA* licenses has increased from one to two.

Example:



What to do next

To use the *Router US Export Lic for DNA* HSECK9 license, install SLAC (on the device) according to the topology you have implemented.

Sample Resource Utilization Measurement Report

The following is a sample Resource Utilization Measurement (RUM) report, in XML format (See RUM Report and Report Acknowledgement). Several such reports may be concatenated to form one report.

```
<?xml version="1.0" encoding="UTF-8"?>
  <smartLicense>
```

[redacted]

```
  </smartLicense>
```