Task Library for Smart Licensing Using Policy

This section is a grouping of tasks that apply to Smart Licensing Using Policy. It includes tasks performed on a product instance, on the CSLU interface, and on the CSSM Web UI.

To implement a particular topology, refer to the corresponding workflow to know the sequential order of tasks that apply. See Implementing Smart Licensing Using Policy.

To perform any additional configuration tasks, for instance, to configure a different license, or use an add-on license, or to configure a narrower reporting interval, refer to the corresponding task here. Check the "Supported Topologies" where provided, before you proceed.

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.

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.

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 Cisco SSM (In the Preferences tab, **Cisco is Available**), you can select from the list of available SA/VAs.

If you are not connected to Cisco SSM (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.

Step 1 Click 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 Cisco SSM Through CSLU (product instance-initiated communication).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type-number*
4. **vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **negotiation auto**
7. **end**
8. **ip http client source-interface** *interface-type-number*
9. **ip route** *ip-address ip-mask subnet mask*
10. {**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*]
11. **ip domain lookup source-interface** *interface-type-number*
12. **ip domain name** *domain-name*

DETAILED STEPS

	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 Mgmt-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 mgmt-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)# Device(config)# ip name-server vrf mgmt-vrf 173.37.137.85`	Configures Domain Name System (DNS) on the VRF interface.

	Command or Action	Purpose
Step 11	**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 12	**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.

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

Complete these steps to add a Product Instance from the Inventory tab

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 an appropriate CSLU Initiated connect method.

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 Instance**, filling in the host name and selecting a CSLU Initiated connect method), select **Actions for Selected** > **Collect Usage**. CSLU connects to the selected product instances and collects 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 Cisco SSM**.

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

Step 1 Click the **Preferences** tab and enter a valid Smart Account and Virtual Account, and then select an 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 Contact 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 Cisco SSM**.

Step 4 From the **Export to Cisco SSM** modal, you can 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 Cisco SSM 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`.

Export to Cisco SSM (CSLU Interface)

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

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 CSLU home screen, navigate to **Data** > **Export to Cisco SSM**.

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 Cisco SSM and Downloading a File, on page 50

Once the file is downloaded, you can import it into CSLU. See: Import from Cisco SSM (CSLU Interface), on page 7

Import from Cisco SSM (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.

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

Step 2 From the CSLU home screen, navigate to **Data** > **Import from Cisco SSM**.

Step 3 An Import from Cisco SSM 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 a 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.

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 Cisco SSM Through CSLU (CSLU-initiated communication).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new model**
4. **aaa authentication login default local**
5. **aaa authorization exec default local**
6. ip routing

7. {**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*]
8. **ip domain lookup source-interface** *interface-type-number*
9. **ip domain name** *name*
10. **no username** *name*
11. **username** *name* **privilege** *level* **password** *password*
12. **interface** *interface-type-number*
13. **vrf forwarding** *vrf-name*
14. **ip address** *ip-address mask*
15. **negotiation auto**
16. **no shutdown**
17. **end**
18. **ip http server**
19. **ip http authentication local**
20. **ip http secure-server**
21. **ip http max-connections**
22. **ip tftp source-interface** *interface-type-number*
23. **ip route** *ip-address ip-mask subnet mask*
24. **logging host**
25. **end**
26. **show ip http server session-module**

DETAILED STEPS

	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.
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.

	Command or Action	Purpose
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 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 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.

	Command or Action	Purpose
		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 5 → *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:** `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

	Command or Action	Purpose
		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:** `Device(config)# end`	Exits the global configuration mode and enters priveleged EXEC mode.
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.

Requesting SLAC for One or More Product Instance (CSLU Interface)

This task shows you how to manually request SLAC for one or more product instances in CSLU.

Before you begin

Supported topologies:

- Connected to Cisco SSM Through CSLU (Product instance-initiated and CSLU-initiated)
- CSLU Disconnected from Cisco SSM (Product instance-initiated and CSLU-initiated)

Step 1 Navigate to the **Inventory** tab. From the Product Instance table, select the one or more product instances for authorization code request.

Step 2 From the **Actions for Selected** menu, select the **Authorization Code Request** option.

The **Authorization Request Information** modal pops up.

Step 3 Click **Accept**.

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

Step 4 Upload the file to Cisco SSM, generate authorization codes and download the file containing the codes. See Generating and Downloading SLAC from Cisco SSM to a File, on page 39.

Step 5 Return to the CSLU interface.

Step 6 Apply the authorization codes by selecting **Data** > **Import from Cisco SSM**. See Import from Cisco SSM (CSLU Interface), on page 7

If CSLU is in the product instance-initiated mode: The uploaded codes are applied to the product instance the next time the product instance contacts CSLU.

If CSLU is in the CSLU-initiated mode: The uploaded codes are now applied to the product instance the next time the CSLU runs an update.

Setting Up a Connection to Cisco SSM

The following steps show how to set up a Layer 3 connection to Cisco SSM 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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. {**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*]

4. **ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6*
5. **ip domain lookup source-interface** *interface-type interface-number*
6. **ip domain name** *domain-name*
7. **ip host tools.cisco.com** *ip-address*
8. **interface** *interface-type-number*
9. **ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**]
10. **switchport access vlan** *vlan_id*
11. **ip route** *ip-address ip-mask subnet mask*
12. **ip http client source-interface** *interface-type-number*
13. **exit**
14. **copy running-config startup-config**

DETAILED STEPS

	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:** `Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	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 4	**ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6* **Example:** `Device(config)# ip name-server vrf Mgmt-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	**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 6	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configures the domain name.

	Command or Action	Purpose
Step 7	**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 8	**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 9	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Device(config)# ntp server 198.51.100.100 version 2 prefer`	(Required) Activates the NTP service (if it has not already been activated) and enables the system to synchronize the system software clock with the specified NTP server. This ensures that the device time is synchronized with Cisco SSM. 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.

Step 10	**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 11	**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 12	**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.
Step 13	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 14	**copy running-config startup-config** **Example:**	Saves your entries in the configuration file.

	Command or Action	Purpose
	`Device# copy running-config startup-config`	

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license smart transport smart**
4. **license smart url default**
5. **license smart proxy** {**address** *address_hostname* | **port** *port_num*}
6. **exit**
7. **copy running-config startup-config**

DETAILED STEPS

	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

	Command or Action	Purpose
	`Device(config)# license smart proxy address 192.168.0.1` `Device(config)# license smart proxy port 3128`	sends the message on to CSSM. Configure the proxy address and port number 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 Cisco SSM. 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)".

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license smart transport callhome**
4. **license smart url** *url*
5. **service call-home**
6. **call-home**
7. **contact-email-address** *email-address*
8. **profile** *name*

9. **active**
10. **destination transport-method http**{**email** |**http**}
11. **destination address** { **email** *email_address* |**http** *url*}
12. **exit**
13. **exit**
14. **copy running-config startup-config**
15. **show call-home profile** {*name* |**all**}

DETAILED STEPS

	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	**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 Cisco SSM 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:

	Command or Action	Purpose
		• 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 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:**	Saves your entries in the configuration file.

	Command or Action	Purpose
	`Device# copy running-config startup-config`	
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 Cisco SSM.

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)".

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license smart transport callhome**
4. **service call-home**
5. **call-home**
6. **http-proxy** *proxy-address* **proxy-port** *port-number*
7. **exit**
8. **exit**
9. **copy running-config startup-config**

DETAILED STEPS

	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.

	Command or Action	Purpose
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:** `Device(config-call-home)# http-proxy 198.51.100.10 port 5000`	Configures the proxy server information to the Call Home service.
Step 7	**exit** **Example:** `Device(config-call-home)# exit`	Exits Call Home configuration mode and enters global configuration mode. 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 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 Cisco SSM:

Before you begin

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

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 an unknown product instance (not in the SSM On-Prem database) are rejected.

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

Before you begin

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

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 an unknown product instance 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 20.

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 13, 14, and 15 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).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type-number*
4. **vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **negotiation auto**
7. **end**
8. **ip http client source-interface** *interface-type-number*
9. **ip route** *ip-address ip-mask subnet mask*
10. {**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*]
11. **ip domain lookup source-interface** *interface-type-number*
12. **ip domain name** *domain-name*
13. **crypto pki trustpoint SLA-TrustPoint**
14. enrollment terminal
15. **revocation-check none**
16. **exit**
17. **copy running-config startup-config**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**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 Mgmt-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 mgmt-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)# Device(config)# ip name-server vrf mgmt-vrf 198.51.100.1`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**ip domain lookup source-interface** *interface-type-number* **Example:**	Configures the source interface for the DNS domain lookup.

	Command or Action	Purpose
	`Device(config)# ip domain lookup source-interface gigabitethernet0/0`	**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 12	**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 13	**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 14	enrollment terminal **Example:** `Device(ca-trustpoint)# enrollment terminal`	(Required) Specifies the certificate enrollment method.
Step 15	**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 16	**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 17	**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 product instance-initiated communication in an SSM On-Prem deployment. This task shows 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).

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.

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

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

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).

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 Cisco SSM: Uploading Data or Requests to Cisco SSM 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 Cisco SSM.

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).

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 only if a product instance requires a SLAC.
  - **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 27).

    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 27).

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).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new model**
4. **aaa authentication login default local**
5. **aaa authorization exec default local**
6. ip routing
7. {**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*]
8. **ip domain lookup source-interface** *interface-type-number*
9. **ip domain name** *name*
10. **no username** *name*
11. **username** *name* **privilege** *level* **password** *password*

12. **interface** *interface-type-number*
13. **vrf forwarding** *vrf-name*
14. **ip address** *ip-address mask*
15. **negotiation auto**
16. **no shutdown**
17. **end**
18. **ip http server**
19. **ip http authentication local**
20. **ip http secure-server**
21. **ip http max-connections**
22. **ip tftp source-interface** *interface-type-number*
23. **ip route** *ip-address ip-mask subnet mask*
24. **logging host**
25. **crypto pki trustpoint SLA-TrustPoint**
26. enrollment terminal
27. **revocation-check none**
28. **end**
29. **show ip http server session-module**
30. **copy running-config startup-config**

DETAILED STEPS

	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.
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.

	Command or Action	Purpose
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 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:** d `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:**	(Required) Establishes a username-based authentication system.

	Command or Action	Purpose
	`Device(config)# username admin privilege 15 password 0 lab`	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 26). 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.
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.

	Command or Action	Purpose

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	**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.

	Command or Action	Purpose

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 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.

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

With the SSM On-Prem Deployment topology, the authorization codes required for export-controlled and enfored licenses must be generated in Cisco SSM 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 Cisco SSM (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 balace of the necessary export-controlled or enforced licenses in your Smart Account and Virtual Account in Cisco SSM.

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 Cisco SSM. Save this file in a location that is accessible when you are working on the Cisco SSM Web UI (in the next step).

Step 5 Complete this task in Cisco SSM: Generating and Downloading SLAC from Cisco SSM to a File, on page 39.

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 Again navigate to **Inventory** > **SL Using Policy**.

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

Import the .csv file download at the end of the procedure in Step 4 above.

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

Step 8 Complete the final step depending on whether the product instance or SSM On-Prem initiates communication.

- For product instance-initiated communication, configure the product instance to request and install SLAC from SSM On-Prem. See: Manually Requesting and Auto-Installing a SLAC , on page 33
- For SSM On-Prem-initiated communication, the uploaded codes are applied to the product instances the next time SSM On-Prem runs an update.

Manually Requesting and Auto-Installing a SLAC

To request Cisco SSM 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 Cisco SSM Through CSLU (product instance-initiated and CSLU-initiated communication)
- Connected Directly to Cisco SSM
- CSLU Disconnected from Cisco SSM (product instance-initiated and CSLU-initiated communication)
- SSM On-Prem Deployment (product instance-initiated communication)

Before you proceed, check the following as well:

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

  Each UDI where you want to use a cryptographic feature requires one HSECK9 key. Each HSECK9 key requires a SLAC. When you follow this task to request and install SLAC on the product instance, the usage count of the HSECK9 key is updated accordingly in Cisco SSM.

Note The following restriction applies only to Cisco Catalyst 9400 Series Supervisor Modules supporting the HSECK9 key: In a Cisco StackWise Virtual set-up, when requesting SLAC for a product instance that is connected to CSLU or SSM On-Prem, even if you use the option to request SLAC only for the active (the **local** keyword), SLAC is requested and installed for the active *and* standby. You must therefore ensure that you have two available HSECK9 keys - one for each chassis UDI - in the Smart Account and Virtual Account in Cisco SSM. A corresponding SLAC is then installed for each chassis UDI.

This restriction does not affect a single or a dual-supervisor setup, because only one HSECK9 and one corresponding SLAC is required in these setups.

- The product instance on which you are requesting the SLAC is connected Cisco SSM, or CSLU, or SSM On-Prem.
- The transport type and URL are configured accordingly. In the **show license all** command in privileged EXEC mode. In the output, check field `Transport: .`
- You have installed a trust code by generating a token, if you are directly connected to Cisco SSM. 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, the product instance requests SSM On-Prem for SLAC, so ensure that you have made the required number of SLACs available in the SSM On-Prem server before you can begin with this task.

SUMMARY STEPS

1. **enable**
2. **license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**}
3. (Optional) **license smart sync** {**all** | **local**}
4. Complete remaining steps for applicable topologies.
5. **show license authorization**
6. Configure the cryptographic feature.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local**} **Example:** `Device# license smart authorization request add hseck9 all`	Requests a SLAC from Cisco SSM or CSLU or SSM On-Prem. • Specify if you want to add to or replace an existing SLAC:

	Command or Action	Purpose
		• **add**: This adds the requested key to an existing SLAC. The new SLAC will contain all the keys of the existing SLAC, and the requested key. • **replace**: This replaces the existing SLAC. The new SLAC will contain only the requested key. All HSECK9 keys in the existing SLAC are returned. When you enter this keyword, the product instance checks if these existing keys are in-use. If they are, an error message is displayed, telling you to first disable the corresponding cryptographic feature. **Note** On Cisco Catalyst 9300X Series Switches in a stacking setup: If you have added a device (where SLAC is not installed) to an existing stack where SLAC is already installed, use the **replace** and **all** keywords. This returns all HSECK9 keys in the existing SLAC and requests SLAC for all the devices in the stack. You cannot request SLAC for a particular member. Your only options are: either the active, or the entire stack. **Note** This keyword is not supported on Cisco Catalyst 9400 Series Supervisor Modules in a Cisco StackWise Virtual set-up. If SLAC is installed only on the active and you want to install it on the standby as well, return the SLAC which is on the active and then request and install SLAC on the active and standby again. • *feature_name*: Enter the name of the export-controlled license for which you want to request an addition or a replacement of the SLAC. Enter "hseck9" to request and install SLAC for the HSECK9 key. • Specify the device by entering one of these options: • **all**: Gets the authorization code for *all* devices in a High Availability and stacking set-up. In case of a stacking setup or a Cisco StackWise Virtual setup, we recommend that you use this option and install SLAC for the active and the standby. This ensures uninterrupted use of the cryptographic feature in the event of a switchover.

	Command or Action	Purpose
		• **local**: Gets the authorization code for the *active* device in a High Availability and stacking set-up. This is the default option.
Step 3	(Optional) **license smart sync** {**all** | **local**} **Example:** `Device# license smart sync all`	Triggers the product instance to synchronize with Cisco SSM, or CSLU, or SSM On-Prem, to send and receive any pending data. This step applies only to topologies where the product instance is connected to Cisco SSM, or CSLU or SSM On-Prem, and where the product instance initiates communication. The topologies are: *Connected Directly to Cisco SSM*, *Connected to Cisco SSM Through CSLU* (product instance-initiated), and SSM On-Prem Deployment (product instance-initiated). By triggering an on-demand synchronization, you can ensure that the SLAC installation process is completed soon after you request SLAC. Otherwise, SLAC is applied to the product instance only the next time the product instance is *scheduled* to contact Cisco SSM, or CSLU or SSM On-Prem.
Step 4	Complete remaining steps for applicable topologies.	• For *Connected to Cisco SSM Through CSLU* (CSLU-initiated communication), see Tasks for CSLU-Initiated Communication. • For *CSLU Disconnected from Cisco SSM* (product instance-initiated and CSLU-initiated communication), see Workflow for Topology: CSLU Disconnected from Cisco SSM. • For *SSM On-Prem Deployment* (product instance-initiated communication), see Workflow for Topology: SSM On-Prem Deployment

Step 5	**show license authorization**
	Example:
	`Device# show license authorization`
	`Overall status:`
	`  Active: PID:C9300X-24HX,SN:FOC2519L8R7`
	`  Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC`
	`  Last Confirmation code: 6746c5b5`
	`  Standby: PID:C9300X-48HXN,SN:FOC2524L39P`
	`  Status: NOT INSTALLED`
	`  Member: PID:C9300X-48HX,SN:FOC2516LC92`
	`  Status: NOT INSTALLED`
	
	`Authorizations:`
	`  C9K HSEC (Cat9K HSEC):`
	`  Description: HSEC Key for Export Compliance on`
		Displays the SLAC that is installed on the product instance.

	Command or Action	Purpose
	Cat9K Series Switches Total available count: 1 Enforcement type: EXPORT RESTRICTED Term information: Active: PID:C9300X-24HX,SN:FOC2519L8R7 Authorization type: SMART AUTHORIZATION INSTALLED License type: PERPETUAL Term Count: 1 Purchased Licenses: No Purchase Information Available	
Step 6	Configure the cryptographic feature. **Example:** Device# **show license summary** License Usage: License Entitlement Tag Count Status --- network-advantage (C9300-24 Network Advan...) 1 IN USE dna-advantage (C9300-24 DNA Advantage) 1 IN USE network-advantage (C9300-48 Network Advan...) 2 IN USE dna-advantage (C9300-48 DNA Advantage) 2 IN USE hseck9 (Cat9K HSEC) 1 IN USE	After you configure the cryptographic feature, the usage count and status of HSECK9 key in the output of the **show license summary** privileged EXEC command changes to `1` and `IN USE`, respectively Depending on the cryptopgraphic feature and the product instance, refer to the correspoding document: For information about disabling the IPsec feature on Cisco Catalyst 9300X Series Switches, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)*. For information about disabling the IPsec feature on Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9400 Switches)*. For information about disabling the WANMACsec feature on Cisco Catalyst 9500X Series Switches, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9500 Switches)* For information about disabling the WANMACsec feature on Cisco Catalyst 9600 Series 40-Port 50G, 2-Port 200G, 2-Port 400G Line Card, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9600 Switches)*

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 17.7.1 only.

Before you begin

Supported topologies: No Connectivity to Cisco SSM and No CSLU

Also ensure that you have the required number of HSECK9 keys in the applicable Smart Account and Virtual Account in Cisco SSM. Each UDI where you want to use a cryptographic feature requires one HSECK9 key. Each HSECK9 key requires a SLAC. After you complete this task you have to upload the SLAC request file in Cisco SSM. Once this is processed in Cisco SSM, the usage count of the HSECK9 key is updated accordingly in Cisco SSM.

SUMMARY STEPS

1. **enable**
2. **license smart authorization request** {**add** | **replace**} *feature_name* {**all**| **local**}
3. **license smart authorization request save***path*
4. Upload the file to Cisco SSM, and then download the file containing the SLAC code.
5. Install the file on the product instance.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all**| **local**} **Example:** `Device# license smart authorization request add hseck9 all`	Generates a SLAC request with all the required information. Specify if you want to add to or replace an existing SLAC: • **add**: Adds the requested key to an existing SLAC. The new authorization code will contain all the keys of the existing SLAC, and the requested license. • **replace**: Replaces the existing SLAC. The new SLAC will contain only the requested HSECK9 key. All keys in the existing SLAC are returned. When you enter this keyword, the product instance checks if these existing keys are in-use. If they are, an error message is displayed, telling you to first disable the corresponding feature. **Note** For a stacking scenario (Cisco Catalyst 9300X Series Switches): If you have added a device (where SLAC is not installed) to an existing stack where SLAC is already installed, use the **replace** and **all** keywords. This returns all HSECK9 keys in the existing SLAC and requests SLAC for all the devices in the stack. You cannot request SLAC for a particular member. Your only options are: either the active, or the entire stack.

	Command or Action	Purpose
		Note This keyword is not supported on Cisco Catalyst 9400 Series Supervisor Modules in a Cisco StackWise Virtual set-up. If SLAC is installed only on the active and you want to install it on the standby as well, return the SLAC which is on the active and then request and install SLAC on the active and standby again. For *feature_name*, enter the name of the export-controlled license for which you want to request an addition or a replacement of the SLAC. Enter "hseck9" to request and install SLAC for the HSECK9 key. Specify the device by entering one of these options: • **all**: Gets the SLAC for *all* devices in a High Availability set-up In case of a stacking setup or a Cisco StackWise Virtual setup, we recommend that you use this option and install SLAC for the active and the standby. This ensures uninterrupted use of the cryptographic feature in the event of a switchover. • **local**: Gets the SLAC for the *active* device in a High Availability set-up. This is the default option.
Step 3	**license smart authorization request save***path* **Example:** `Device# license smart authorization request save bootflash:slac.txt`	Saves the required UDI information for the SLAC request in a .txt file, in the specified location.
Step 4	Upload the file to Cisco SSM, and then download the file containing the SLAC code.	Complete this task: Uploading Data or Requests to Cisco SSM 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.

Generating and Downloading SLAC from Cisco SSM to a File

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 containing the PIDs and serial numbers of all applicable product instances saved in an accessible location.

Before you begin

Supported topologies:

- Connected to Cisco SSM Through CSLU (Product instance-initiated and CSLU-initiated)
- CSLU Disconnected from Cisco SSM (Product instance-initiated and CSLU-initiated)
- No Connectivity to Cisco SSM and No CSLU
- SSM On-Prem Deployment (product instance-initiated and SSM On-Prem-initiated communication)

Step 1 Log in to the Cisco SSM Web UI at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses** link.

Log in using the username and password provided by Cisco.

Step 2 Click the **Inventory** tab.

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

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

Step 5 Click the **Authorize License Enforced Features** tab.

Step 6 Generate SLAC for a single product instance or for multiple product instances (*choose one*).

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

     Note Do not populate any of the other fields.

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

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

  3. Click **Next**
  4. Click **Generate Authorization Code**.
  5. Download the authorization code and save as a .csv file.
  6. 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 should have a .csv file to upload in this case)**:
  1. From the dropdown list that says “Single Device” (by default), change the selection to “Multiple Devices”.

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

  2. Click **Choose File** and navigate to the .csv file, which contains the list of product instances that require SLAC.
  3. Once uploaded, the list of devices is displayed in Cisco SSM. All the devices will have the checkbox enabled (implying that you want to request a SLAC for all of them), and click **Next**.
  4. Specify the license quantity required for each product instance, and click **Next**.

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

e. Click **Reserve Licenses**.

f. Download accordingly to topology:

- For the *Connected to Cisco SSM Through CSLU*, *CSLU Disconnected from Cisco SSM*, *SSM On-Prem Deployment* topologies, click **Download Authorization Codes** to download a.csv file containing all the authorization codes. Click **Close**.

  You can now import this .csv file to CSLU or SSM On-Prem. Return to the CSLU or SSM On-Prem interface to complete the remaining steps to import this file.

- For the *No Connectivity to Cisco SSM and No CSLU* topology (in an air-gapped network), where you have to import the code into the product instance, download the authorization code for each product instance to a separate .txt file. Do not download the .csv file which has all the codes.

  In the Cisco SSM Web UI, return to the **Inventory**> **Product Instances** tab. Locate each product instance by its PID or serial number. Click on the UDI to display the **Overview** tab. The **Last Contact** field displays a link called *Download Reservation Authorization Code*. Click on the link to download the authorization code of only the selected product instance, in .txt format.

  Import each SLAC into the product instance, see Installing a File on the Product Instance, on page 51.

Returning an Authorization Code

This task shows you how to return an authorization code for a license and to then return the license to your license pool in Cisco SSM. You can use this procedure for all authorization codes - SLAC and SLR.

Before you begin

Supported topologies: all

SUMMARY STEPS

1. Disable or unconfigure the cryptographic feature for which you used the HSECK9 key.
2. **enable**
3. **show license summary**
4. Depending on the cryptographic feature you were using, enter the applicable command to release the HSECK9 key.
   - For IPSec: **platform hsec-license-release**
   - For WAN MACsec: **platform wanmacsec hsec-license-release**
5. **show license summary**
6. **license smart authorization return** {**all** |**local**} {**offline**[*path*] |**online**}
7. **no license smart reservation**
8. **show license authorization**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Disable or unconfigure the cryptographic feature for which you used the HSECK9 key.	Depending on the cryptopgraphic feature and the product instance, refer to the correspoding document: For information about disabling the IPsec feature on Cisco Catalyst 9300X Series Switches, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9300 Switches)*. For information about disabling the IPsec feature on Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules, see the *Configuring IPsec* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9400 Switches)*. For information about disabling the WANMACsec feature on Cisco Catalyst 9500X Series Switches, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9500 Switches)* For information about disabling the WANMACsec feature on Cisco Catalyst 9600 Series 40-Port 50G, 2-Port 200G, 2-Port 400G Line Card, see the *MACsec Encryption* chapter of the *Security Configuration Guide, Cisco IOS XE <applicable release number> (Catalyst 9600 Switches)* If the cryptographic feature you are disabling is the WAN MACsec feature, also note the following: Even after disabling the cryptographic feature, the output of the **show license summary** command displays the usage count and status for the HSECK9 key as `1` and `IN USE`. This is as expected. The steps in this task show you how to *release* the key, which changes the count and status to `0` and `NOT IN USE`. But you must disable the WAN MACsec feature before you try to release the HSECK9 key.
Step 2	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

Step 3	**show license summary**
	Example:
	`Device# show license summary`
	`License Usage:`
	`License Entitlement Tag Count Status`
	`----------`
	`network-advantage (C9300-24 Network Advan...) 1 IN USE`
		(Optional) Displays license usage summary. This step applies only if you are returning a SLAC.
		If the status of the HSECK9 key is displayed as `NOT IN USE` skip to Step 5.
		If the status of the HSECK9 key is displayed as `IN USE` even after the cryptographic feature is disabled, then perform the next step. This is the case in the accompanying example.

	Command or Action	Purpose
	dna-advantage (C9300-24 DNA Advantage) 1 IN USE network-advantage (C9300-48 Network Advan...) 2 IN USE dna-advantage (C9300-48 DNA Advantage) 2 IN USE **C9K HSEC (Cat9K HSEC)** **1 IN USE**	

Step 4	Depending on the cryptographic feature you were using, enter the applicable command to release the HSECK9 key.
	• For IPSec: **platform hsec-license-release**
	• For WAN MACsec: **platform wanmacsec hsec-license-release**
	Example:
	`Device# configure terminal`
	`Device(config)# platform hsec-license-release`
	`HSEC license is released`
	`Device(config)# exit`
		(Optional) Enters the global configuration mode, releases the HSECK9 key, and returns to privileged EXEC mode. This step applies only if you are returning a SLAC.
		If the cryptographic feature using the HSECK9 key has been disabled or unconfigured, and the license is still displayed as `IN USE`, this command forces the HSECK9 key to be marked as `NOT IN USE`. If the status of the HSECK9 key is still displayed as `IN USE`, repeat Step 1.

Step 5	**show license summary**
	Example:
	`Device# show license summary`
	`License Usage:`
	`License Entitlement Tag Count Status`
	`---`
	network-advantage (C9300-24 Network Advan...)
	1 IN USE
	dna-advantage (C9300-24 DNA Advantage)
	1 IN USE
	network-advantage (C9300-48 Network Advan...)
	2 IN USE
	dna-advantage (C9300-48 DNA Advantage)
	2 IN USE
	C9K HSEC (Cat9K HSEC)
	0 NOT IN USE
		(Optional) Displays license usage summary. This step applies only if you are returning a SLAC.
		Ensure that the status of the license that you want to return is `NOT IN USE`.

Step 6	**license smart authorization return** {**all** |**local**} {**offline**[*path*] |**online**}
	Example:
	`Device# license smart authorization return all online`
	`OR`
	`Device# license smart authorization return all offline`
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C9300X-24HX,SN:FOC2519L8R7`
	`Return code:`
	`Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7`
		Returns an authorization code back to the license pool in Cisco SSM. A return code is displayed after you enter this command.
		Specify the product instance:
		• **all**: Performs the action for all connected product instances in a High Availability or stacking set-up.
		• **local**: Performs the action for the active product instance. This is the default option.
		Specify if you are connected to Cisco SSM or not:
		• If the product instance is directly connected to Cisco SSM, or it is connected to Cisco SSM through CSLU

	Command or Action	Purpose
	OR `Device# license smart authorization return all offline bootflash:return-code.txt`	or SSM On-Prem and the product instance-initiates communication, enter **online**. The code is automatically returned to Cisco SSM and a confirmation is returned and installed on the product instance. If you choose this option, the return code is automatically submitted to Cisco SSM. • If the product instance is not connected to Cisco SSM, or if you have implemented a topology with CSLU-initiated or SSM On-Prem initiated communication, enter **offline** [*filepath_filename*]. If you choose the offline option, you must complete the additional step of submitting this to Cisco SSM. • For software versions Cisco IOS XE Cupertino 17.7.1 and later only: Specify a path to save the SLAC return request in a file and upload the file to Cisco SSM: Uploading Data or Requests to Cisco SSM 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`. • For software versions prior to 17.7.1: If you are returning a SLAC, copy the return code that is displayed on the CLI and complete this task to enter the return code in Cisco SSM: Entering a SLAC Return Code in Cisco SSM and Removing a Product Instance, on page 45. • For all software versions, if you are returning an SLR authorization code, copy the return code that is displayed on the CLI and complete this task to enter the return code in Cisco SSM: #unique_86. Proceed with the next step only after you complete this step.

Step 7	**no license smart reservation**
	Example:
	`Device# configure terminal`
	`Device(config)# no license smart reservation`
	`Device(config)# exit`
		Enter the global configuration mode, disables SLR configuration on the product instance, and returns to privileged EXEC mode.
		This step is required only if the authorization code you are returning is an SLR authorization code. Skip this step if the code you are returning is a SLAC for an HSECK9 key.

	Command or Action	Purpose
		Note You must complete the authorization code return process (**license smart authorization return**), online or offline, before you enter the **no license smart reservation** command in this step. Otherwise, the return may not be reflected in Cisco SSM or in the **show** command, and you will have to contact your Cisco technical support representative to rectify the problem.

Step 8	**show license authorization**
	Example:
	`Device# show license authorization`
	`Overall status:`
	`  Active: PID:C9300X-24HX,SN:FOC2519L8R7`
	`  Status: NOT INSTALLED`
	`  Last return code:`
	`Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-`
	`babWeL-FABPt9-Wr1Dn7-Rp7`
	`  Standby: PID:C9300X-48HXN,SN:FOC2524L39P`
	`  Status: NOT INSTALLED`
	`  Member: PID:C9300X-48HX,SN:FOC2516LC92`
	`  Status: NOT INSTALLED`
	
	`<output truncated>`
		Displays licensing information. If the return process is completed correctly, the `Last return code:` field displays the return code.

Entering a SLAC Return Code in Cisco SSM and Removing a Product Instance

You can use this task to complete the return procedure for a SLAC when the product instance is not connected to Cisco SSM. This returns the HSECK9 keys to the license pool. Additionally, you also have the option of removing the product instance from Cisco SSM.

Before you begin

Supported topologies: all

Follow this procedure only if you are returning a SLAC.

Ensure that you have generated a return code as shown in Returning an Authorization Code, on page 41. (Enter it in Step 7 in this task).

Step 1 Log in to the Cisco SSM Web UI at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses**link.

Log in using the username and password provided by Cisco.

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. You can enter the PID or serial number in the search tab to locate it.

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 SLAC return code you generated.

Step 8 Click **Remove Reservation**.

The HSECK9 key 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 SLAC, your task ends here. If you also want to remove the product instance from Cisco SSM, continue to the next step.

Step 9 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 10 Click **Remove Product Instance**.

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

Entering an SLR Return Code in Cisco SSM and Removing the Product Instance

You can use this task to complete the return prcedure for an SLR authorization code. This returns the licenses to the license pool and removes the product instance.

Before you begin

Supported topologies: all

Follow this procedure only if you are returning an SLR authorization code.

Ensure that you have generated a return code as shown in Returning an Authorization Code, on page 41. (Enter it in Step 7 in this task).

Step 1 Log in to the Cisco SSM Web UI at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses**link.

Log in using the username and password provided by Cisco.

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. You can enter the PID or serial number in the search tab to locate it.

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

- If the product instance is *not* using a license with an SLR authorization code then the **Confirm Remove Product Instance** window is displayed.
- If the product instance *is* using a license with an SLR authorization code, then the **Remove Product Instance** window, with a field for return code entry is displayed.

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

Note This step applies only if the product instance is using a license with an SLR authorization code.

Step 8 Click **Remove Product Instance**.

The license is returned to the license pool and the product instance is removed.

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

Step 1 Log in to the CSSM Web UI at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses**link.

Log in using the username and password provided by Cisco.

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

This task shows you how to establish trust. Here, you use the ID token downloaded from Cisco SSM and submit a trust request. Cisco SSM responds with the trust code, which is automatically installed on the product instance.

Before you begin

Supported topologies: Connected Directly to Cisco SSM

You must have already generated and downloaded an ID token file from Cisco SSM: Generating a New Token for a Trust Code from CSSM, on page 47.

SUMMARY STEPS

1. **enable**
2. **license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**]
3. **show license status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted
Step 2	**license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] **Example:** `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	Establishes a trusted connection with Cisco SSM. For *id_token_value*, enter the token you generated in Cisco SSM. 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.

	Command or Action	Purpose
		Enter the **force** keyword to submit the trust code request in spite of an existing trust code on the product instance. Trust codes are node-locked to the UDI of the product instance. If a UDI is already registered, Cisco SSM does not allow a new registration for the same UDI. Entering the **force** keyword sets a force flag in the message sent to Cisco SSM to create a new trust code even if one already exists. You may for example need to use the **force** keyword if there is already a factory-installed trust code on the product instance. A trust code is factory-installed starting with Cisco IOS XE Cupertino 17.7.1. Since a factory-installed trust code cannot be used for secure communication with Cisco SSM, you must use the **force** keyword to overwrite it with the trust code obtained using the ID token. Also see: Trust Code.

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 Cisco SSM

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 Cisco SSM and No CSLU
- CSLU Disconnected from Cisco SSM

Step 1 Log in to the Cisco SSM Web UI at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses**link.

Log in using the username and password provided by Cisco.

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 Cisco SSM and Downloading a File

You can use this task to:

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

  This applies only to the *No Connectivity to Cisco SSM and No CSLU* topology and is supported starting with Cisco IOS XE Cupertino 17.7.1.
- To upload a SLAC or SLR authorization code return request.

  This applies only to the *No Connectivity to Cisco SSM and No CSLU* topology and is supported starting with Cisco IOS XE Cupertino 17.7.1.

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

Before you begin

Supported topologies:

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

Step 1 Log in to the Cisco SSM Web UI at https://software.cisco.com. Under **Smart Software Licensing**, click the **Manage licenses** link.

Log in using the username and password provided by Cisco.

Step 2 Select the **Smart Account** 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, Cisco SSM may take a few minutes.

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

Installing a File on the Product Instance

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

Before you begin

Supported topologies: No Connectivity to Cisco SSM and No CSLU

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

- For a policy, see Downloading a Policy File from Cisco SSM, on page 49.
- For an ACK, see Uploading Data or Requests to Cisco SSM and Downloading a File, on page 50.
- For a SLAC, see Generating and Downloading SLAC from Cisco SSM to a File, on page 39 or Uploading Data or Requests to Cisco SSM and Downloading a File, on page 50 (There are multiple ways to obtain a SLAC).

SUMMARY STEPS

1. **enable**
2. **copy** *source filename* **bootflash:**
3. **license smart import** *filepath_filename*
4. **show license all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**copy** *source filename* **bootflash:** **Example:** `Device# copy tftp://10.8.0.6/user01/example.txt bootflash:`	(Optional) Copies the file from its source location or directory to the flash memory of the product instance. You can also import the file *directly* from a remote location and install it on the product instance (next step). • *source*: This is the source location of file. The source can be either local or remote. • **bootflash:**: This is the destination for boot flash memory.

	Command or Action	Purpose
Step 3	**license smart import** *filepath_filename* **Example:** `Device# license smart import bootflash:example.txt`	Imports and installs the file on the product instance. For *filepath_filename*, specify the location, including the filename. After installation, a system message displays the type of file you installed. **Note** If you generated SLAC for multiple product instances (as in a stacking set-up) in the Cisco SSM Web UI, that is, you followed the method described here: Generating and Downloading SLAC from Cisco SSM to a File, on page 39, ensure that you download a separate .txt SLAC file for each UDI. Import and install one file at a time.
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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license smart transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** }
4. **license smart url** { *url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *smart_url* }
5. **license smart usage interval** *interval_in_days*
6. **exit**
7. **copy running-config startup-config**

DETAILED STEPS

	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`	Configures a mode of transport for the product instance to use. Choose from the following options: • **automatic**: Sets the transport mode **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. While the transport mode keyword is the same for CSLU and SSM On-Prem, the transport URLs are different. See **license smart url cslu** *cslu_or_on-prem_url* in the next step. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport.

Step 4	**license smart url** {*url* | **cslu** *cslu_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 a URL for the configured transport mode. Depending on the transort mode you have chosen to configure in the previous step, configure the corresponding URL here:
		• *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the Cisco SSM 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:
		`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_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

	Command or Action	Purpose
		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 24 The **no license smart url cslu** *cslu_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`). • **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 set the value to zero, RUM reports are not sent, regardless of what the applied policy specifies - this applies to topologies where CSLU or Cisco SSM may be on the receiving end. If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval_in_days* and the policy value for `Ongoing reporting`

	Command or Action	Purpose
		`frequency(days):`, the lower of the two values is applied. For example, if *interval_in_days* is set to 100, and the value in the in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days. If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent.
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 a Base or Add-On License

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

This task sets a license level and requires a reload before the configured changes are effective. You can use this task to:

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

Before you begin

Supported topologies: all

For information about the available base and add-on licenses, see Base and Add-On Licenses.

Information about the licenses that you have purchased can be found in the Smart Account and Virtual Account of the product instance in the Cisco Smart Software Manager (CSSM) Web UI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license boot level** { **network-advantage** [**addon dna-advantage**] | **network-essentials** [**addon dna-essentials**] }
4. **exit**

5. **copy running-config startup-config**
6. **show version**
7. **reload**
8. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license boot level** { **network-advantage** [**addon dna-advantage**] | **network-essentials** [**addon dna-essentials**] } **Example:** `Device(config)# license boot level network-advantage add-on dna-advantage`	Activates the configured license on the product instance. • **network-advantage** [**addon dna-advantage**]: Configures the Network Advantage license. Optionally, you can also configure the Digital Networking Architecture (DNA) Advantage license. • **network-advantage** [**addon dna-advantage**]: Configures the Network Essentials license. Optionally, you can also configure the Digital Networking Architecture (DNA) Essentials license. In the accompanying example, the DNA Advantage license will be activated on the product instance after reload.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to the privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves changes in the configuration file.

Step 6	**show version**
	Example:
	`Device# show version`
	
	`<output truncated>`
	`Technology Package License Information:`
	
	`------------------------------------------------------`
	`Technology-package`
	`Technology-package`
		Shows currently configured license information and the license that is applicable after reload.
		The "`Technology-package Next reboot`" column displays the change in the configured license that is effective after reload, only if you save the configuration change.
		In the accompanying example, the current license level is Network Advantage. Because the configuration change was saved, the "`Technology-package Next reboot`" column

	Command or Action	Purpose

	`Current Type`
	`Next reboot`
	`——————————————————————`
	`network-advantage Smart License`
	`network-advantage`
	`Subscription Smart License`
	`dna-advantage`
	
	`<output truncated>`
		shows that the DNA Advantage license will be activated after reload.

Step 7	**reload** **Example:** `Device# reload`	Reloads the device.

Step 8	**show version**
	Example:
	`Device# show version`
	
	`<output truncated>`
	`Technology Package License Information:`
	
	`——————————————————————`
	`Technology-package`
	`Technology-package`
	`Current Type`
	`Next reboot`
	`——————————————————————`
	`network-advantage Smart License`
	`network-advantage`
	`dna-advantage Subscription Smart License`
	`dna-advantage`
	
	`<output truncated>`
		Shows currently configured license information and the license that is applicable after reload.

What to do next

After you configure a license level, the change is effective after a reload. To know if reporting is required, refer to the output of the **show license status** privileged EXEC command and check the `Next ACK deadline:` and `Next report push:` fields.

Note The change in license usage is recorded on the product instance. The next steps relating to reporting - if required - depend on your current topology.

- Connected to CSSM Through CSLU
  - Product Instance-initiated communication: No action required. Since the product instance initiates communication, it automatically sends out the RUM report at the scheduled time, as per the policy (**show license status** —> `Next report push`), to CSLU. (To manually trigger this on the product instance, enter the **license smart sync** {**all**| **local**} privileged EXEC command. This synchronizes the product instance with CSLU, to send and receive any pending data.) CSLU forwards the RUM report to CSSM and retrieves the ACK. The ACK is applied to the product instance the next time the product instance contacts CSLU.

- CSLU-initiated communication: In the CSLU interface, collect usage from the product instance: Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 5. CSLU sends the RUM report to CSSM and retrieves the ACK from CSSM. The ACK is applied to the product instance the next time CSLU runs an update.

- Connected Directly to CSSM: No action required. Since the product instance initiates communication, it automatically sends out the RUM report at the scheduled time, as per the policy (**show license status** —> `Next report push`), to CSSM. (To manually trigger this on the product instance, enter the **license smart sync** {**all**| **local**} privileged EXEC command. This synchronizes the product instance with CSSM, to send and receive any pending data.) Once the ACK is available, CSSM sends this back to the product instance.
- CSLU Disconnected from CSSM
  - Product Instance-initiated communication: No action required. Since the product instance initiates communication, it automatically sends out the RUM report at the scheduled time, as per the policy (**show license status** —> `Next report push`), to CSLU. (To manually trigger this on the product instance, enter the **license smart sync** {**all**| **local**} privileged EXEC command. This synchronizes the product instance with CSLU, to send and receive any pending data.)

    Since CSLU is disconnected from CSSM, in the CSLU interface and then the CSSM Web UI, complete these tasks Export to Cisco SSM (CSLU Interface), on page 6 > Uploading Data or Requests to Cisco SSM and Downloading a File, on page 50 > Import from Cisco SSM (CSLU Interface), on page 7. The ACK is applied to the product instance the next time the product instance contacts CSLU.
  - CSLU-initiated communication: In the CSLU interface, collect usage from the product instance: Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 5.

    Since CSLU is disconnected from CSSM, in the CSLU interface and then the CSSM Web UI, complete these tasks Export to Cisco SSM (CSLU Interface), on page 6 > Uploading Data or Requests to Cisco SSM and Downloading a File, on page 50 > Import from Cisco SSM (CSLU Interface), on page 7. The ACK is applied to the product instance the next time CSLU runs an update.

- Connected to CSSM Through a Controller: No action is required (if you have already completed the first ad hoc report in the Cisco DNA Center GUI). Cisco DNA Center handles all subsequent reporting and returns the ACK to the product instance.
- No Connectivity to CSSM and No CSLU: Save RUM reports to a file (on your product instance) and upload it to CSSM (from a workstation that has connectivity to the Internet, and Cisco). Enter the **license smart save usage** command in privileged EXEC mode, to save RUM reports to a file. Then to upload the file to CSSM and download the ACK, complete this task: Uploading Data or Requests to Cisco SSM and Downloading a File, on page 50. Lastly, to install the ACK on the product instance, complete this task: Installing a File on the Product Instance, on page 51.
- SSM On-Prem Deployment:
  - Product Instance-initiated communication: No action required. Since the product instance initiates communication, it automatically sends out the RUM report at the scheduled time, as per the policy (**show license status** —> `Next report push`), to SSM On-Prem. (To manually trigger this on the product instance, enter the **license smart sync** {**all**| **local**} privileged EXEC command. This synchronizes the product instance with SSM On-Prem, to send and receive any pending data.)

- If SSM On-Prem is connected to CSSM, in the SSM On-Prem interface, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**.
- If SSM On-Prem is disconnected from CSSM, upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 25.

- SSM On-Prem initiated communication: In the SSM On-Prem interface, collect usage information from the product instance. Navigate to **Reports** > **Synchronisation pull schedule with the devices** > **Synchronise now with the device**.
  - If SSM On-Prem is connected to CSSM, in the SSM On-Prem interface, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**.
  - If SSM On-Prem is disconnected from CSSM, upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 25.

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>
```

```
  </smartLicense>
```